Mathematisches
Forschungsinstitut
Oberwolfach

Member of the Leibniz
Leibniz
Association

# Oberwolfach Preprints

OWP 2020 - 15

DARIJ GRINBERG AND VICTOR REINER

## Hopf Algebras in Combinatorics

Volume 2

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

## Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.
Copyright of the content is held by the authors.

DOI 10.14760/OWP-2020-15

# Hopf Algebras in Combinatorics

## Volume 2 of 2

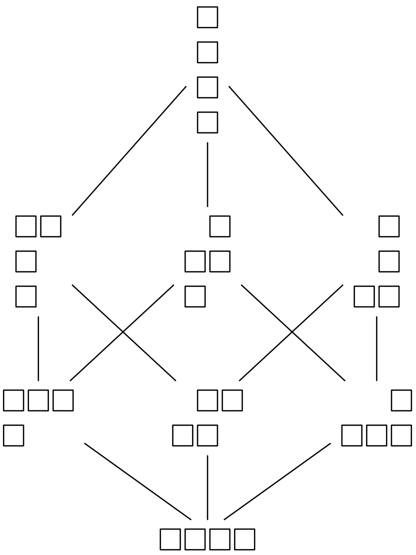
*Version of July 27, 2020*

Darij Grinberg

*Drexel University*

Victor Reiner

*University of Minnesota, Twin Cities*



Oberwolfach Preprints, 2020

**Hopf Algebras in Combinatorics**, volume **2** of 2.

Version of 27 July 2020,
equivalent to `arXiv:1409.8356v7` up to editorial changes.

Darij Grinberg:
Drexel University
Korman Center, Room 263
15 S 33rd Street
Philadelphia PA, 19104
USA
(temporary:)
Mathematisches Forschungsinstitut Oberwolfach,
Schwarzwaldstrasse 9–11
77709 Oberwolfach
Germany
darijgrinberg@gmail.com
https://www.cip.ifi.lmu.de/~grinberg/

Victor Reiner:
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
USA
reiner@math.umn.edu
https://www-users.math.umn.edu/~reiner/

**Keywords:** Hopf algebra, combinatorics, symmetric functions, quasisymmetric functions.

Typeset with LaTeX.

Future versions of this text will be available from the first author's website:
https://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb.pdf
https://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf
(version with solutions).

# Note to the Reader

This is the second volume of the July 2020 edition of "Hopf Algebras in Combinatorics", an introduction to combinatorial Hopf algebras with particular focus on symmetric and quasisymmetric functions.

This text surveys some of the most fundamental Hopf algebras appearing in combinatorics. After introducing coalgebras, bialgebras and Hopf algebras in general, we study the Hopf algebra of *symmetric functions*; we prove Zelevinsky's axiomatic characterization of it as a "PSH" (*positive self-adjoint Hopf algebra*) and its application to the *representation theory* of symmetric and (briefly) finite general linear groups. We then continue with the *quasisymmetric* and the *noncommutative symmetric functions*, some Hopf algebras formed from graphs, posets and matroids, and the *Malvenuto–Reutenauer Hopf algebra of permutations.* Among other results, we survey the Littlewood–Richardson rule and other symmetric function identities, Zelevinsky's structure theorem for PSHs, the antipode formula for P-partition enumerators, the Aguiar–Bergeron–Sottile universal property of QSym, the theory of Lyndon words, the Gessel–Reutenauer bijection, and Hazewinkel's polynomial freeness of QSym.

The text is written with a graduate student reader in mind (and originates from a one-semester graduate class held by the second author at the University of Minnesota). It assumes a good familiarity with multilinear algebra and – for the representation-theoretical applications – basic group representation theory; otherwise it is meant to be rather self-contained.

The text has been edited over 9 years; it is still likely to be rough at some edges, but has proven useful at least to its authors. It may still grow (note the strategic gap in the numbering between Chapters 8 and 11) and improve. The authors will appreciate any comments and corrections sent to `darijgrinberg@gmail.com` and `reiner@math.umn.edu`.

This version of the text is essentially the version posted on the arXiv as `arXiv:1409.8356v7`; it differs only in some minor editorial changes (spacing, display of formulas, and the occasional trivial rewording of a sentence) and in the page numbering. The numbering of results and equations is identical between this and the arXiv version.

For printing reasons, this version of the text is split into two volumes. Volume 1 covers general Hopf algebra theory and the symmetric functions (including their PSH-characterization and representation-theoretical applications), while Volume 2 (this one) covers the "larger" combinatorial Hopf algebras (and includes the bibliography, the index and a short section containing hints to the exercises from Chapter 1.

Parts of this text have been written during stays at the Mathematisches Forschungsinstitut Oberwolfach (2019 and 2020)[1] and at the Institut

[1] This research was supported through the programme "Oberwolfach Leibniz Fellows" by the Mathematisches Forschungsinstitut Oberwolfach in 2019 and 2020.

Mittag–Leffler Djursholm (Spring 2020, supported by the Swedish Research Council under grant no. 2016-06596); DG thanks both for their hospitality.

*Darij Grinberg*
*July 27, 2020*

*Victor Reiner*
*July 27, 2020*

## 5. Quasisymmetric functions and $P$-partitions

We discuss here our next important example of a Hopf algebra arising in combinatorics: the *quasisymmetric functions* of Gessel [79], with roots in work of Stanley [203] on $P$-partitions. Other treatments of quasisymmetric functions can be found in [206, Section 7.19] and [187, Chapter 8] (with focus on their enumerative applications rather than on their Hopf structure) and in [153, Chapter 6] (with a focus on their representation-theoretical meaning). Quasisymmetric functions have found applications in combinatorial enumeration ([187, Chapter 8], [206, Section 7.19]), topology ([12]) and algebraic geometry ([158], [163]).

### 5.1. Definitions, and Hopf structure.

The definitions of quasisymmetric functions require a totally ordered variable set. Usually we will use a variable set denoted $\mathbf{x} = (x_1, x_2, \ldots)$ with the usual ordering $x_1 < x_2 < \cdots$. However, it is good to have some flexibility in changing the ordering, which is why we make the following definition.

**Definition 5.1.1.** Given any totally ordered set $I$, create a totally ordered variable set $\{x_i\}_{i \in I}$, and then let $R(\{x_i\}_{i \in I})$ denote the power series of bounded degree in $\{x_i\}_{i \in I}$ having coefficients in $\mathbf{k}$.

The *ring of quasisymmetric functions* $\mathrm{QSym}(\{x_i\}_{i\in I})$ *over the alphabet* $\{x_i\}_{i\in I}$ will be the $\mathbf{k}$-submodule consisting of the elements $f$ in $R(\{x_i\}_{i\in I})$ that have the same coefficient on the monomials $x_{i_1}^{\alpha_1} \cdots x_{i_\ell}^{\alpha_\ell}$ and $x_{j_1}^{\alpha_1} \cdots x_{j_\ell}^{\alpha_\ell}$ whenever both $i_1 < \cdots < i_\ell$ and $j_1 < \cdots < j_\ell$ in the total order on $I$. We write $\mathrm{QSym}_{\mathbf{k}}(\{x_i\}_{i\in I})$ instead of $\mathrm{QSym}(\{x_i\}_{i\in I})$ to stress the choice of base ring $\mathbf{k}$.

It immediately follows from this definition that $\mathrm{QSym}(\{x_i\}_{i\in I})$ is a free $\mathbf{k}$-submodule of $R(\{x_i\}_{i\in I})$, having as $\mathbf{k}$-basis elements the *monomial quasisymmetric functions*

$$M_\alpha(\{x_i\}_{i\in I}) := \sum_{i_1 < \cdots < i_\ell \text{ in } I} x_{i_1}^{\alpha_1} \cdots x_{i_\ell}^{\alpha_\ell}$$

for all compositions[251] $\alpha$ satisfying $\ell(\alpha) \leq |I|$. When $I$ is infinite, this means that the $M_\alpha$ for all compositions $\alpha$ form a basis of $\mathrm{QSym}(\{x_i\}_{i\in I})$.

Note that $\mathrm{QSym}(\{x_i\}_{i\in I}) = \bigoplus_{n\geq 0} \mathrm{QSym}_n(\{x_i\}_{i\in I})$ is a graded $\mathbf{k}$-module of finite type, where $\mathrm{QSym}_n(\{x_i\}_{i\in I})$ is the $\mathbf{k}$-submodule of quasisymmetric functions which are homogeneous of degree $n$. Letting Comp denote the set of all compositions $\alpha$, and $\mathrm{Comp}_n$ the compositions $\alpha$ of $n$ (that is, compositions whose parts sum to $n$), the subset $\{M_\alpha\}_{\alpha\in\mathrm{Comp}_n;\ \ell(\alpha)\leq|I|}$ gives a $\mathbf{k}$-basis for $\mathrm{QSym}_n(\{x_i\}_{i\in I})$.

[251] Recall that compositions were defined in Definition 4.3.1, along with related concepts such as length and size.

**Example 5.1.2.** Taking the variable set $\mathbf{x} = (x_1 < x_2 < \cdots)$ to define $\operatorname{QSym}(\mathbf{x})$, for $n = 0, 1, 2, 3$, one has these basis elements in $\operatorname{QSym}_n(\mathbf{x})$:

$$M_{()} = M_\varnothing = 1,$$

$$\begin{aligned}
M_{(1)} &= x_1 + x_2 + x_3 + \cdots & &= m_{(1)} = s_{(1)} = e_1 = h_1 = p_1,\\[1em]
M_{(2)} &= x_1^2 + x_2^2 + x_3^2 + \cdots & &= m_{(2)} = p_2,\\
M_{(1,1)} &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots & &= m_{(1,1)} = e_2,\\[1em]
M_{(3)} &= x_1^3 + x_2^3 + x_3^3 + \cdots & &= m_{(3)} = p_3,\\
M_{(2,1)} &= x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + \cdots\ , & &\\
M_{(1,2)} &= x_1x_2^2 + x_1x_3^2 + x_2x_3^2 + \cdots\ , & &\\
M_{(1,1,1)} &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + \cdots & &= m_{(1,1,1)} = e_3.
\end{aligned}$$

It is not obvious that $\operatorname{QSym}(\mathbf{x})$ is a subalgebra of $R(\mathbf{x})$, but we will show this momentarily. For example,

$$\begin{aligned}
&M_{(a)}M_{(b,c)}\\
&= (x_1^a + x_2^a + x_3^a + \cdots)(x_1^bx_2^c + x_1^bx_3^c + x_2^bx_3^c + \cdots)\\
&= x_1^{a+b}x_2^c + \cdots + x_1^bx_3^{a+c} + \cdots + x_1^ax_2^bx_3^c + \cdots + x_1^bx_2^ax_3^c + \cdots + x_1^bx_2^cx_3^a + \cdots\\
&= M_{(a+b,c)} + M_{(b,a+c)} + M_{(a,b,c)} + M_{(b,a,c)} + M_{(b,c,a)}.
\end{aligned}$$

**Proposition 5.1.3.** *For any infinite totally ordered set $I$, one has that $\operatorname{QSym}(\{x_i\}_{i\in I})$ is a $\mathbf{k}$-subalgebra of $R(\{x_i\}_{i\in I})$, with multiplication in the $\{M_\alpha\}$-basis as follows: Fix three disjoint chain posets $(i_1 < \cdots < i_\ell)$, $(j_1 < \cdots < j_m)$ and $(k_1 < k_2 < \cdots)$. Now, if $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_m)$ are two compositions, then*

$$M_\alpha M_\beta = \sum_f M_{\operatorname{wt}(f)} \tag{5.1.1}$$

*in which the sum is over all $p \in \mathbb{N}$ and all maps $f$ from the disjoint union of two chains to a chain*

$$(i_1 < \cdots < i_\ell) \sqcup (j_1 < \cdots < j_m) \xrightarrow{f} (k_1 < \cdots < k_p) \tag{5.1.2}$$

*which are both surjective and strictly order-preserving (that is, if $x$ and $y$ are two elements in the domain satisfying $x < y$, then $f(x) < f(y)$), and where the composition $\operatorname{wt}(f) := (\operatorname{wt}_1(f), \ldots, \operatorname{wt}_p(f))$ is defined by $\operatorname{wt}_s(f) := \sum_{i_u\in f^{-1}(k_s)} \alpha_u + \sum_{j_v\in f^{-1}(k_s)} \beta_v$.*

**Example 5.1.4.** For this example, set $\alpha = (2, 1)$ and $\beta = (3, 4, 2)$. Let us compute $M_\alpha M_\beta$ using (5.1.1). Indeed, the length of $\alpha$ is $\ell = 2$, and the length of $\beta$ is $m = 3$, so the sum on the right hand side of (5.1.1) is a sum over all $p \in \mathbb{N}$ and all surjective strictly order-preserving maps $f$ from the disjoint union $(i_1 < i_2) \sqcup (j_1 < j_2 < j_3)$ of two chains to the chain $(k_1 < k_2 < \cdots < k_p)$. Such maps can exist only when $p \leq 5$ (due to having to be surjective) and only for $p \geq 3$ (since, being strictly order-preserving, they have to be injective when restricted to $(j_1 < j_2 < j_3)$). Hence, enumerating them is a finite problem. The reader can check that the value obtained fo $M_\alpha M_\beta$ is

$$\begin{aligned}
&M_{(2,1,3,4,2)} + M_{(2,3,1,4,2)} + M_{(2,3,4,1,2)} + M_{(2,3,4,2,1)} + M_{(3,2,1,4,2)} \\
&+ M_{(3,2,4,1,2)} + M_{(3,2,4,2,1)} + M_{(3,4,2,1,2)} + M_{(3,4,2,2,1)} + M_{(3,4,2,2,1)} \\
&+ M_{(2,3,4,3)} + M_{(2,3,5,2)} + M_{(2,4,4,2)} + M_{(3,2,4,3)} + M_{(3,2,5,2)} + M_{(3,4,2,3)} \\
&+ M_{(3,4,4,1)} + M_{(3,6,1,2)} + M_{(3,6,2,1)} + M_{(5,1,4,2)} + M_{(5,4,1,2)} + M_{(5,4,2,1)} \\
&+ M_{(5,4,3)} + M_{(5,5,2)} + M_{(3,6,3)}.
\end{aligned}$$

Here, we have listed the addends corresponding to $p = 5$ on the first two rows, the addends corresponding to $p = 4$ on the next two rows, and those corresponding to $p = 3$ on the fifth row. The reader might notice that the first two rows (i.e., the addends with $p = 5$) are basically a list of shuffles of $\alpha$ and $\beta$: In general, the maps (5.1.2) for $p = \ell + m$ are in bijection with the elements of $\mathrm{Sh}_{\ell,m}$ [252], and the corresponding compositions $\mathrm{wt}(f)$ are the shuffles of $\alpha$ and $\beta$. Therefore the name "overlapping shuffle product".

*Proof of Proposition 5.1.3.* It clearly suffices to prove the formula (5.1.1). Let $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_m)$ be two compositions. Fix three disjoint chain posets $(i_1 < \cdots < i_\ell)$, $(j_1 < \cdots < j_m)$ and $(k_1 < k_2 < \cdots)$.

Thus, multiplying $M_\alpha = \sum_{u_1<\cdots<u_\ell} x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}$ with $M_\beta = \sum_{v_1<\cdots<v_m} x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}$, we obtain

$$\begin{aligned}
M_\alpha M_\beta &= \sum_{u_1<\cdots<u_\ell} \sum_{v_1<\cdots<v_m} \left(x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}\right)\left(x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}\right) \\
&= \sum_{\gamma=(\gamma_1,\ldots,\gamma_p)\in\mathrm{Comp}} \sum_{w_1<\cdots<w_p \text{ in } I} N_{w_1,\ldots,w_p}^{\gamma} x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p}, \qquad (5.1.3)
\end{aligned}$$

where $N_{w_1,\ldots,w_p}^{\gamma}$ is the number of all pairs

$$((u_1 < \cdots < u_\ell), (v_1 < \cdots < v_m)) \in I^\ell \times I^m \qquad (5.1.4)$$

of two strictly increasing tuples satisfying

$$\left(x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}\right)\left(x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}\right) = x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p}. \qquad (5.1.5)$$

[253] Thus, we need to show that $N_{w_1,\ldots,w_p}^{\gamma}$ (for a given $\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathrm{Comp}$ and a given $(w_1 < \cdots < w_p) \in I^p$) is also the number of all surjective strictly order-preserving maps

(5.1.6)

$$(i_1 < \cdots < i_\ell) \sqcup (j_1 < \cdots < j_m) \xrightarrow{f} (k_1 < \cdots < k_p) \text{ satisfying } \mathrm{wt}(f) = \gamma$$

(because then, (5.1.3) will simplify to (5.1.1)).

In order to show this, it suffices to construct a bijection from the set of all pairs (5.1.4) satisfying (5.1.5) to the set of all surjective strictly order-preserving maps (5.1.6). This bijection is easy to construct: Given a pair

[252] The bijection takes a map $f$ to the inverse of the permutation $\sigma \in \mathfrak{S}_p$ which sends every $x \in \{1, 2, \ldots, \ell\}$ to the index $y$ satisfying $f(i_x) = k_y$, and sends every $x \in \{\ell+1, \ell+2, \ldots, \ell+m\}$ to the index $y$ satisfying $f(j_{x-\ell}) = k_y$.

[253] In the second equality in (5.1.3), we have used the fact that each monomial can be uniquely written in the form $x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p}$ for some composition $\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathrm{Comp}$ and some strictly increasing tuple $(w_1 < \cdots < w_p) \in I^p$.

(5.1.4) satisfying (5.1.5), the bijection sends it to the map (5.1.6) determined by:

$$i_g \overset{f}{\mapsto} k_h, \text{ where } h \text{ is chosen such that } u_g = w_h;$$
$$j_g \overset{f}{\mapsto} k_h, \text{ where } h \text{ is chosen such that } v_g = w_h.$$

Proving that this bijection is well-defined and bijective is straightforward[254]. □

The multiplication rule (5.1.1) shows that the $\mathbf{k}$-algebra $\operatorname{QSym}(\{x_i\}_{i\in I})$ does not depend much on $I$, as long as $I$ is infinite. More precisely, all such $\mathbf{k}$-algebras are mutually isomorphic. We can use this to define a $\mathbf{k}$-algebra of quasisymmetric functions without any reference to $I$:

**Definition 5.1.5.** Let QSym be the $\mathbf{k}$-algebra defined as having $\mathbf{k}$-basis $\{M_\alpha\}_{\alpha\in\mathrm{Comp}}$ and with multiplication defined $\mathbf{k}$-linearly by (5.1.1). This is called the *$\mathbf{k}$-algebra of quasisymmetric functions*. We write $\operatorname{QSym}_{\mathbf{k}}$ instead of QSym to stress the choice of base ring $\mathbf{k}$.

The $\mathbf{k}$-algebra QSym is graded, and its $n$-th graded component $\operatorname{QSym}_n$ has $\mathbf{k}$-basis $\{M_\alpha\}_{\alpha\in\mathrm{Comp}_n}$.

For every infinite totally ordered set $I$, the $\mathbf{k}$-algebra QSym is isomorphic to the $\mathbf{k}$-algebra $\operatorname{QSym}(\{x_i\}_{i\in I})$. The isomorphism sends $M_\alpha \longmapsto M_\alpha(\{x_i\}_{i\in I})$.

In particular, we obtain the isomorphism $\operatorname{QSym} \cong \operatorname{QSym}(\mathbf{x})$ for $\mathbf{x}$ being the infinite chain $(x_1 < x_2 < x_3 < \cdots)$. We will identify QSym with $\operatorname{QSym}(\mathbf{x})$ along this isomorphism. This allows us to regard quasisymmetric functions either as power series in a specific set of variables ("alphabet"), or as formal linear combinations of $M_\alpha$'s, whatever is more convenient.

For any infinite alphabet $\{x_i\}_{i\in I}$ and any $f \in \operatorname{QSym}$, we denote by $f\left(\{x_i\}_{i\in I}\right)$ the image of $f$ under the algebra isomorphism $\operatorname{QSym} \to \operatorname{QSym}\left(\{x_i\}_{i\in I}\right)$ defined in Definition 5.1.5.

The comultiplication of QSym will extend the one that we defined for $\Lambda$, but we need to take care about the order of the variables this time. We consider the linear order from (2.3.2) on two sets of variables $(\mathbf{x}, \mathbf{y}) = (x_1 < x_2 < \cdots < y_1 < y_2 < \cdots)$, and we embed the $\mathbf{k}$-algebra $\operatorname{QSym}(\mathbf{x}) \otimes \operatorname{QSym}(\mathbf{y})$ into the $\mathbf{k}$-algebra $R(\mathbf{x}, \mathbf{y})$ by identifying every $f \otimes g \in \operatorname{QSym}(\mathbf{x}) \otimes \operatorname{QSym}(\mathbf{y})$ with $fg \in R(\mathbf{x}, \mathbf{y})$ (this embedding is indeed injective[255]). It can then be seen that

$$\operatorname{QSym}(\mathbf{x}, \mathbf{y}) \subset \operatorname{QSym}(\mathbf{x}) \otimes \operatorname{QSym}(\mathbf{y})$$

[254] The inverse of this bijection sends each map (5.1.6) to the pair (5.1.4) determined by

$$u_g = w_h, \text{ where } h \text{ is chosen such that } f(i_g) = k_h;$$
$$v_g = w_h, \text{ where } h \text{ is chosen such that } f(j_g) = k_h.$$

[255] This is because it sends the basis elements $M_\beta(\mathbf{x}) \otimes M_\gamma(\mathbf{y})$ of the former $\mathbf{k}$-algebra to the linearly independent power series $M_\beta(\mathbf{x}) M_\gamma(\mathbf{y})$.

(where the right hand side is viewed as $\mathbf{k}$-subalgebra of $R(\mathbf{x},\mathbf{y})$ via said embedding)[256], so that one can define $\mathrm{QSym} \xrightarrow{\Delta} \mathrm{QSym}\otimes\mathrm{QSym}$ as the composite of the maps in the bottom row here:

(5.1.7)
$$\begin{tikzcd}
 & R(\mathbf{x},\mathbf{y}) \arrow[r, phantom, "="] & R(\mathbf{x},\mathbf{y}) & \\
\mathrm{QSym} \arrow[r, phantom, "\cong"] & \mathrm{QSym}(\mathbf{x},\mathbf{y}) \arrow[u, phantom, sloped, "\subset"] \arrow[r, hook] & \mathrm{QSym}(\mathbf{x})\otimes\mathrm{QSym}(\mathbf{y}) \arrow[u, phantom, sloped, "\subset"] \arrow[r, phantom, "\cong"] & \mathrm{QSym}\otimes\mathrm{QSym}, \\
f \arrow[r, mapsto] & f(\mathbf{x},\mathbf{y}). & &
\end{tikzcd}$$

(Recall that $f(\mathbf{x},\mathbf{y}) = f(x_1,x_2,\ldots,y_1,y_2,\ldots)$ is formally defined as the image of $f$ under the algebra isomorphism $\mathrm{QSym}\to\mathrm{QSym}(\mathbf{x},\mathbf{y})$ defined in Definition 5.1.5.)

**Example 5.1.6.** For example,

$$\begin{aligned}
\Delta M_{(a,b,c)} &= M_{(a,b,c)}(x_1,x_2,\ldots,y_1,y_2,\ldots)\\
&= x_1^a x_2^b x_3^c + x_1^a x_2^b x_4^c + \cdots\\
&\quad + x_1^a x_2^b\cdot y_1^c + x_1^a x_2^b \cdot y_2^c + \cdots\\
&\quad + x_1^a \cdot y_1^b y_2^c + x_1^a\cdot y_1^b y_3^c + \cdots\\
&\quad + y_1^a y_2^b y_3^c + y_1^a y_2^b y_4^c + \cdots\\
&= M_{(a,b,c)}(\mathbf{x}) + M_{(a,b)}(\mathbf{x})M_{(c)}(\mathbf{y}) + M_{(a)}(\mathbf{x})M_{(b,c)}(\mathbf{y}) + M_{(a,b,c)}(\mathbf{y})\\
&= M_{(a,b,c)}\otimes 1 + M_{(a,b)}\otimes M_{(c)} + M_{(a)}\otimes M_{(b,c)} + 1\otimes M_{(a,b,c)}.
\end{aligned}$$

Defining the *concatenation* $\beta\cdot\gamma$ of two compositions $\beta=(\beta_1,\ldots,\beta_r),\gamma=(\gamma_1,\ldots,\gamma_s)$ to be the composition $(\beta_1,\ldots,\beta_r,\gamma_1,\ldots,\gamma_s)$, one has the following description of the coproduct in the $\{M_\alpha\}$ basis.

**Proposition 5.1.7.** *For a composition $\alpha=(\alpha_1,\ldots,\alpha_\ell)$, one has*

$$\Delta M_\alpha = \sum_{k=0}^{\ell} M_{(\alpha_1,\ldots,\alpha_k)}\otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)} = \sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha}} M_\beta\otimes M_\gamma.$$

*Proof.* We work with the infinite totally ordered set $I=\{1<2<3<\cdots\}$. The definition of $\Delta$ yields

$$\Delta M_\alpha = M_\alpha(\mathbf{x},\mathbf{y}) = \sum_{p_1<p_2<\cdots<p_\ell \text{ in } (\mathbf{x},\mathbf{y})} p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\ell^{\alpha_\ell}, \tag{5.1.8}$$

where the sum runs over strictly increasing $\ell$-tuples $(p_1<p_2<\cdots<p_\ell)$ of variables in the variable set $(\mathbf{x},\mathbf{y})$. But every such $\ell$-tuple $(p_1<p_2<\cdots<p_\ell)$ can be expressed uniquely in the form $\left(x_{i_1},\ldots,x_{i_k},y_{j_1},\ldots,y_{j_{\ell-k}}\right)$ for some $k\in\{0,1,\ldots,\ell\}$ and some subscripts $i_1<\cdots<i_k$ and $j_1<\cdots<j_{\ell-k}$ in $I$. The corresponding monomial $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\ell^{\alpha_\ell}$ then rewrites as $x_{i_1}^{\alpha_1}\cdots x_{i_k}^{\alpha_k}\cdot y_{j_1}^{\alpha_{k+1}}\cdots y_{j_{\ell-k}}^{\alpha_\ell}$. Thus, the sum on the right hand side of (5.1.8)

[256] This is not completely obvious, but can be easily checked by verifying that $M_\alpha(\mathbf{x},\mathbf{y}) = \sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha}} M_\beta(\mathbf{x})\otimes M_\gamma(\mathbf{y})$ for every composition $\alpha$ (see the proof of Proposition 5.1.7 for why this holds).

rewrites as

$$\begin{aligned}
&\sum_{k=0}^{\ell} \sum_{i_1<\cdots<i_k} \sum_{j_1<\cdots<j_{\ell-k}} x_{i_1}^{\alpha_1}\cdots x_{i_k}^{\alpha_k} \cdot y_{j_1}^{\alpha_{k+1}}\cdots y_{j_{\ell-k}}^{\alpha_\ell} \\
&= \sum_{k=0}^{\ell} \underbrace{\left(\sum_{i_1<\cdots<i_k} x_{i_1}^{\alpha_1}\cdots x_{i_k}^{\alpha_k}\right)}_{=M_{(\alpha_1,\ldots,\alpha_k)}(\mathbf{x})} \cdot \underbrace{\left(\sum_{j_1<\cdots<j_{\ell-k}} y_{j_1}^{\alpha_{k+1}}\cdots y_{j_{\ell-k}}^{\alpha_\ell}\right)}_{=M_{(\alpha_{k+1},\ldots,\alpha_\ell)}(\mathbf{y})} \\
&= \sum_{k=0}^{\ell} M_{(\alpha_1,\ldots,\alpha_k)}(\mathbf{x}) M_{(\alpha_{k+1},\ldots,\alpha_\ell)}(\mathbf{y}).
\end{aligned}$$

Thus, (5.1.8) becomes

$$\begin{aligned}
\Delta M_\alpha &= \sum_{p_1<p_2<\cdots<p_\ell \text{ in } (\mathbf{x},\mathbf{y})} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \sum_{k=0}^{\ell} M_{(\alpha_1,\ldots,\alpha_k)}(\mathbf{x}) M_{(\alpha_{k+1},\ldots,\alpha_\ell)}(\mathbf{y}) \\
&= \sum_{k=0}^{\ell} M_{(\alpha_1,\ldots,\alpha_k)} \otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)} = \sum_{\substack{(\beta,\gamma): \\ \beta\cdot\gamma=\alpha}} M_\beta \otimes M_\gamma.
\end{aligned}$$

□

**Proposition 5.1.8.** *The quasisymmetric functions* QSym *form a connected graded Hopf algebra of finite type, which is commutative, and contains the symmetric functions* $\Lambda$ *as a Hopf subalgebra.*

*Proof.* To prove coassociativity of $\Delta$, we need to be slightly careful. It seems reasonable to argue by $(\Delta \otimes \mathrm{id}) \circ \Delta f = f(\mathbf{x},\mathbf{y},\mathbf{z}) = (\mathrm{id} \otimes \Delta) \circ \Delta f$ as in the case of $\Lambda$, but this would now require further justification, as terms like $f(\mathbf{x},\mathbf{y})$ and $f(\mathbf{x},\mathbf{y},\mathbf{z})$ are no longer directly defined as evaluations of $f$ on some sequences (but rather are defined as images of $f$ under certain homomorphisms). However, it is very easy to see that $\Delta$ is coassociative by checking $(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta$ on the $\{M_\alpha\}$ basis: Proposition 5.1.7 yields

$$\begin{aligned}
((\Delta \otimes \mathrm{id}) \circ \Delta) M_\alpha &= \sum_{k=0}^{\ell} \Delta(M_{(\alpha_1,\ldots,\alpha_k)}) \otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)} \\
&= \sum_{k=0}^{\ell} \left( \sum_{i=0}^{k} M_{(\alpha_1,\ldots,\alpha_i)} \otimes M_{(\alpha_{i+1},\ldots,\alpha_k)} \right) \otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)} \\
&= \sum_{k=0}^{\ell} \sum_{i=0}^{k} M_{(\alpha_1,\ldots,\alpha_i)} \otimes M_{(\alpha_{i+1},\ldots,\alpha_k)} \otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)}
\end{aligned}$$

and the same expression for $((\mathrm{id} \otimes \Delta) \circ \Delta) M_\alpha$.

The coproduct $\Delta$ of QSym is an algebra morphism because it is defined as a composite of algebra morphisms in the bottom row of (5.1.7). To prove that the restriction of $\Delta$ to the subring $\Lambda$ of QSym is the comultiplication of $\Lambda$, it thus is enough to check that it sends the elementary symmetric function $e_n$ to $\sum_{i=0}^{n} e_i \otimes e_{n-i}$ for every $n \in \mathbb{N}$. This again follows from Proposition 5.1.7, since $e_n = M_{(1,1,\ldots,1)}$ (with $n$ times 1).

The counit is as usual for a connected graded coalgebra, and just as in the case of $\Lambda$, sends a quasisymmetric function $f(\mathbf{x})$ to its constant term $f(0,0,\ldots)$. This is an evaluation, and hence an algebra morphism. Hence QSym forms a bialgebra, and as it is graded and connected, also a Hopf algebra by Proposition 1.4.16. It is clearly of finite type and contains $\Lambda$ as a Hopf subalgebra. □

We will identify the antipode in QSym shortly, but we first deal with another slightly subtle issue. In addition to the counit evaluation $\epsilon(f) = f(0,0,\ldots)$, starting in Section 7.1, we will want to specialize elements in $\mathrm{QSym}(\mathbf{x})$ by making other variable substitutions, in which all but a finite list of variables are set to zero. We justify this here.

**Proposition 5.1.9.** *Fix a totally ordered set $I$, a commutative* $\mathbf{k}$*-algebra $A$, a finite list of variables $x_{i_1},\ldots,x_{i_m}$, say with $i_1<\cdots<i_m$ in $I$, and an ordered list of elements $(a_1,\ldots,a_m)\in A^m$.*

*Then there is a well-defined evaluation homomorphism*

$$\begin{array}{rcl}\mathrm{QSym}(\{x_i\}_{i\in I}) & \longrightarrow & A, \\ f & \longmapsto & [f]_{\substack{x_{i_1}=a_1,\ldots,x_{i_m}=a_m \\ x_j=0 \text{ for } j\notin\{i_1,\ldots,i_m\}}} .\end{array}$$

*Furthermore, this homomorphism depends only upon the list $(a_1,\ldots,a_m)$, as it coincides with the following:*

$$\begin{array}{rcl}\mathrm{QSym}(\{x_i\}_{i\in I}) \cong \mathrm{QSym}(x_1,x_2,\ldots) & \longrightarrow & A, \\ f(x_1,x_2,\ldots) & \longmapsto & f(a_1,\ldots,a_m,0,0\ldots).\end{array}$$

*(This latter statement is stated for the case when $I$ is infinite; otherwise, read "$x_1,x_2,\ldots,x_{|I|}$" for "$x_1,x_2,\ldots$", and interpret $(a_1,\ldots,a_m,0,0\ldots)$ as an $|I|$-tuple.)*

*Proof.* One already can make sense of evaluating $x_{i_1}=a_1,\ldots,x_{i_m}=a_m$ and $x_j=0$ for $j\notin\{i_1,\ldots,i_m\}$ in the ambient ring $R(\{x_i\}_{i\in I})$ containing $\mathrm{QSym}(\{x_i\}_{i\in I})$, since a power series $f$ of bounded degree will have finitely many monomials that only involve the variables $x_{i_1},\ldots,x_{i_m}$. The last assertion follows from quasisymmetry of $f$, and is perhaps checked most easily when $f=M_\alpha(\{x_i\}_{i\in I})$ for some $\alpha$. □

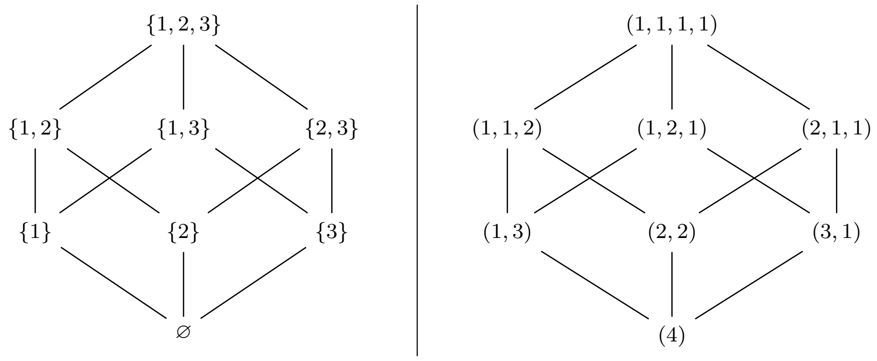
The antipode in QSym has a reasonably simple expression in the $\{M_\alpha\}$ basis, but requiring a definition.

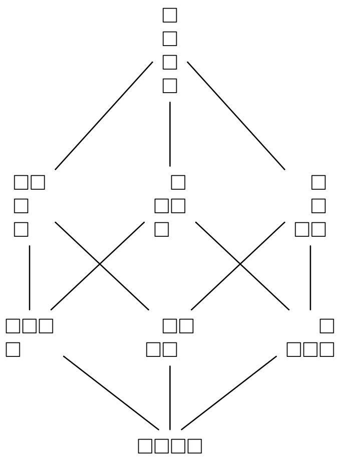
**Definition 5.1.10.** For $\alpha,\beta$ in $\mathrm{Comp}_n$, say that $\alpha$ *refines* $\beta$ or $\beta$ *coarsens* $\alpha$ if, informally, one can obtain $\beta$ from $\alpha$ by combining some of its adjacent parts. Alternatively, this can be defined as follows: One has a bijection $\mathrm{Comp}_n\to 2^{[n-1]}$ where $[n-1]:=\{1,2,\ldots,n-1\}$ which sends $\alpha=(\alpha_1,\ldots,\alpha_\ell)$ having length $\ell(\alpha)=\ell$ to its subset of partial sums

$$D(\alpha):=\{\alpha_1,\alpha_1+\alpha_2,\ldots,\alpha_1+\cdots+\alpha_{\ell-1}\},$$

and this sends the refinement ordering to the inclusion ordering on the Boolean algebra $2^{[n-1]}$ (to be more precise: a composition $\alpha\in\mathrm{Comp}_n$ refines a composition $\beta\in\mathrm{Comp}_n$ if and only if $D(\alpha)\supset D(\beta)$).

There is also a bijection sending every composition $\alpha$ to its *ribbon* diagram $\mathrm{Rib}\,(\alpha)$: the skew diagram $\lambda/\mu$ having rows of sizes $\alpha_1,\ldots,\alpha_\ell$ read from bottom to top with exactly one column of overlap between adjacent rows. These bijections and the refinement partial order are illustrated here for $n = 4$:





(where we have drawn each ribbon diagram with its boxes spaced out).

Given $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, its *reverse* composition is

$$\operatorname{rev}(\alpha) = (\alpha_\ell, \alpha_{\ell-1}, \ldots, \alpha_2, \alpha_1).$$

Note that $\alpha \mapsto \operatorname{rev}(\alpha)$ is a poset automorphism of $\mathrm{Comp}_n$ for the refinement ordering.

**Theorem 5.1.11.** *For any composition $\alpha$ in* Comp,

$$S(M_\alpha) = (-1)^{\ell(\alpha)} \sum_{\substack{\gamma \in \mathrm{Comp}: \\ \gamma \text{ coarsens } \operatorname{rev}(\alpha)}} M_\gamma.$$

For example,

$$S(M_{(a,b,c)}) = -\left(M_{(c,b,a)} + M_{(b+c,a)} + M_{(c,a+b)} + M_{(a+b+c)}\right).$$

*Proof.* We give Ehrenborg's proof[257] [64, Prop. 3.4] via induction on $\ell = \ell(\alpha)$. One has easy base cases when $\ell(\alpha) = 0$, where $S(M_\varnothing) = S(1) = 1 = (-1)^0 M_{\operatorname{rev}(\varnothing)}$, and when $\ell(\alpha) = 1$, where $M_{(n)}$ is primitive by Proposition 5.1.7, so Proposition 1.4.17 shows $S(M_{(n)}) = -M_{(n)} = (-1)^1 M_{\operatorname{rev}((n))}$.

[257] A different proof was given by Malvenuto and Reutenauer [146, Cor. 2.3], and is sketched in Remark 5.4.4 below.

For the inductive step, apply the inductive definition of $S$ from the proof of Proposition 1.4.16:

$$\begin{aligned} S(M_{(\alpha_1,\ldots,\alpha_\ell)}) &= -\sum_{i=0}^{\ell-1} S(M_{(\alpha_1,\ldots,\alpha_i)})M_{(\alpha_{i+1},\ldots,\alpha_\ell)} \\ &= \sum_{i=0}^{\ell-1} \sum_{\substack{\beta \text{ coarsening} \\ (\alpha_i,\alpha_{i-1},\ldots,\alpha_1)}} (-1)^{i+1} M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}. \end{aligned}$$

The idea will be to cancel terms of opposite sign that appear in the expansions of the products $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$. Note that each composition $\beta$ appearing above has first part $\beta_1$ of the form $\alpha_i + \alpha_{i-1} + \cdots + \alpha_h$ for some $h \leq i$ (unless $\beta = \varnothing$), and hence each term $M_\gamma$ in the expansion of the product $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$ has $\gamma_1$ (that is, the first entry of $\gamma$) a sum that can take one of these three forms:

- $\alpha_i + \alpha_{i-1} + \cdots + \alpha_h$,
- $\alpha_{i+1} + (\alpha_i + \alpha_{i-1} + \cdots + \alpha_h)$,
- $\alpha_{i+1}$.

Say that the *type* of $\gamma$ is $i$ in the first case, and $i+1$ in the second two cases[258]; in other words, the type is the largest subscript $k$ on a part $\alpha_k$ which was combined in the sum $\gamma_1$. It is not hard to see that a given $\gamma$ for which the type $k$ is strictly smaller than $\ell$ arises from exactly two pairs $(\beta,\gamma), (\beta',\gamma)$, having opposite signs $(-1)^k$ and $(-1)^{k+1}$ in the above sum[259]. For example, if $\alpha = (\alpha_1, \ldots, \alpha_8)$, then the composition $\gamma = (\alpha_6 + \alpha_5 + \alpha_4, \alpha_3, \alpha_7, \alpha_8 + \alpha_2 + \alpha_1)$ of type 6 can arise from either of

$$\begin{aligned} \beta &= (\alpha_6 + \alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 6 \text{ and sign } (-1)^7, \\ \beta' &= (\alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 5 \text{ and sign } (-1)^6. \end{aligned}$$

Similarly, $\gamma = (\alpha_6, \alpha_5 + \alpha_4, \alpha_3, \alpha_7, \alpha_8 + \alpha_2 + \alpha_1)$ can arise from either of

$$\begin{aligned} \beta &= (\alpha_6, \alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 6 \text{ and sign } (-1)^7, \\ \beta' &= (\alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 5 \text{ and sign } (-1)^6. \end{aligned}$$

Thus one can cancel almost all the terms, excepting those with $\gamma$ of type $\ell$ among the terms $M_\gamma$ in the expansion of the last $(i = \ell - 1)$ summand $M_\beta M_{(\alpha_\ell)}$. A bit of thought shows that these are the $\gamma$ coarsening $\operatorname{rev}(\alpha)$, and all have sign $(-1)^\ell$. □

5.2. **The fundamental basis and $P$-partitions.** There is a second important basis for QSym which arose originally in Stanley's $P$-partition theory [203].[260]

[258] We imagine that we label the terms obtained by expanding $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$ by distinct labels, so that each term knows how exactly it was created (i.e., which $i$, which $\beta$ and which map $f$ as in (5.1.2) gave rise to it). Strictly speaking, it is these triples $(i, \beta, f)$ that we should be assigning types to, not terms.

[259] Strictly speaking, this means that we have an involution on the set of our $(i, \beta, f)$ triples having type smaller than $\ell$, and this involution switches the sign of $(-1)^i M_{\mathrm{wt}(f)}$.

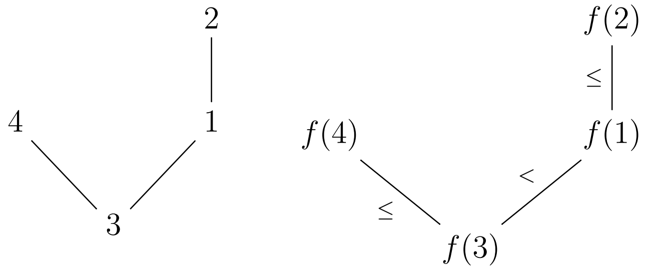
[260] See [80] for a history of $P$-partitions; our notations, however, strongly differ from those in [80].

**Definition 5.2.1.** A *labelled poset* will here mean a partially ordered set $P$ whose underlying set is some finite subset of the integers. A *$P$-partition* is a function $P \xrightarrow{f} \{1, 2, \ldots\}$ with the following two properties:

- If $i \in P$ and $j \in P$ satisfy $i <_P j$ and $i <_{\mathbb{Z}} j$, then $f(i) \leq f(j)$.
- If $i \in P$ and $j \in P$ satisfy $i <_P j$ and $i >_{\mathbb{Z}} j$, then $f(i) < f(j)$.

Denote by $\mathcal{A}(P)$ the set of all $P$-partitions $f$, and let $F_P(\mathbf{x}) := \sum_{f \in \mathcal{A}(P)} \mathbf{x}_f$ where $\mathbf{x}_f := \prod_{i \in P} x_{f(i)}$. This $F_P(\mathbf{x})$ is an element of $\mathbf{k}\,[[\mathbf{x}]] := \mathbf{k}\,[[x_1, x_2, \ldots]]$.

**Example 5.2.2.** Depicted is a labelled poset $P$, along with the relations among the four values $f = (f(1), f(2), f(3), f(4))$ that define its $P$-partitions $f$:



*Remark* 5.2.3. Stanley's treatment of $P$-partitions in [206, §3.15 and §7.19] uses a language different from ours. First, Stanley works not with labelled posets $P$, but with pairs $(P, \omega)$ of a poset $P$ and a bijective labelling $\omega : P \to [n]$. Thus, the relation $<_{\mathbb{Z}}$ is not given on $P$ a priori, but has to be pulled back from $[n]$ using $\omega$ (and it depends on $\omega$, whence Stanley speaks of "$(P, \omega)$-partitions"). Furthermore, what we call "$P$-partition" is called a "reverse $P$-partition" in [206]. Finally, Stanley uses the notations $F_P$ and $F_{P,\omega}$ for something different from what we denote by $F_P$, whereas what we call $F_P$ is dubbed $K_{P,\omega}$ in [206, §7.19].

The so-called *fundamental quasisymmetric functions* are an important special case of the $F_P(\mathbf{x})$. We shall first define them directly and then see how they are obtained as $P$-partition enumerators $F_P(\mathbf{x})$ for some special labelled posets $P$.

**Definition 5.2.4.** Let $n \in \mathbb{N}$ and $\alpha \in \operatorname{Comp}_n$. We define the *fundamental quasisymmetric function* $L_\alpha = L_\alpha(\mathbf{x}) \in \operatorname{QSym}$ by

$$L_\alpha := \sum_{\substack{\beta \in \operatorname{Comp}_n: \\ \beta \text{ refines } \alpha}} M_\beta. \tag{5.2.1}$$

**Example 5.2.5.** The extreme cases for $\alpha$ in $\operatorname{Comp}_n$ give quasisymmetric functions $L_\alpha$ which are symmetric:

$$\begin{aligned} L_{(1^n)} &= M_{(1^n)} = e_n, \\ L_{(n)} &= \sum_{\alpha \in \operatorname{Comp}_n} M_\alpha = h_n. \end{aligned}$$

Before studying the $L_\alpha$ in earnest, we recall a basic fact about finite sets, which is sometimes known as the "principle of inclusion and exclusion" (although it is more general than the formula for the size of a union of sets that commonly goes by this name):

**Lemma 5.2.6.** *Let $G$ be a finite set. Let $V$ be a $\mathbf{k}$-module. For each subset $A$ of $G$, we let $f_A$ and $g_A$ be two elements of $V$.*

(a) *If*

$$\text{every } A \subset G \text{ satisfies } g_A = \sum_{B \subset A} f_B,$$

*then*

$$\text{every } A \subset G \text{ satisfies } f_A = \sum_{B \subset A} (-1)^{|A \setminus B|} g_B.$$

(b) *If*

$$\text{every } A \subset G \text{ satisfies } g_A = \sum_{B \subset G;\ B \supset A} f_B,$$

*then*

$$\text{every } A \subset G \text{ satisfies } f_A = \sum_{B \subset G;\ B \supset A} (-1)^{|B \setminus A|} g_B.$$

*Proof.* This can be proven by elementary arguments (easy exercise). Alternatively, Lemma 5.2.6 can be viewed as a particular case of the Möbius inversion principle (see, e.g., [206, Propositions 3.7.1 and 3.7.2]) applied to the Boolean lattice $2^G$ (whose Möbius function is very simple: see [206, Example 3.8.3]). (This is spelled out in [138, Example 4.52], for example.) □

Lemma 5.2.6 can be translated into the language of compositions:

**Lemma 5.2.7.** *Let $n \in \mathbb{N}$. Let $V$ be a $\mathbf{k}$-module. For each $\alpha \in \operatorname{Comp}_n$, we let $f_\alpha$ and $g_\alpha$ be two elements of $V$.*

(a) *If*

$$\text{every } \alpha \in \operatorname{Comp}_n \text{ satisfies } g_\alpha = \sum_{\beta \text{ coarsens } \alpha} f_\beta,$$

*then*

$$\text{every } \alpha \in \operatorname{Comp}_n \text{ satisfies } f_\alpha = \sum_{\beta \text{ coarsens } \alpha} (-1)^{\ell(\alpha)-\ell(\beta)} g_\beta.$$

(b) *If*

$$\text{every } \alpha \in \operatorname{Comp}_n \text{ satisfies } g_\alpha = \sum_{\beta \text{ refines } \alpha} f_\beta,$$

*then*

$$\text{every } \alpha \in \operatorname{Comp}_n \text{ satisfies } f_\alpha = \sum_{\beta \text{ refines } \alpha} (-1)^{\ell(\beta)-\ell(\alpha)} g_\beta.$$

*Proof.* Set $[n-1] = \{1, 2, \ldots, n-1\}$. Recall (from Definition 5.1.10) that there is a bijection $D : \operatorname{Comp}_n \to 2^{[n-1]}$ that sends each $\alpha \in \operatorname{Comp}_n$ to $D(\alpha) \subset [n-1]$. This bijection $D$ has the properties that:

- a composition $\beta$ refines a composition $\alpha$ if and only if $D(\beta) \supset D(\alpha)$;
- a composition $\beta$ coarsens a composition $\alpha$ if and only if $D(\beta) \subset D(\alpha)$;
- any composition $\alpha \in \operatorname{Comp}_n$ satisfies $|D(\alpha)| = \ell(\alpha) - 1$ (unless $n = 0$), and thus
- any compositions $\alpha$ and $\beta$ in $\operatorname{Comp}_n$ satisfy $|D(\alpha)| - |D(\beta)| = \ell(\alpha) - \ell(\beta)$.

This creates a dictionary between compositions in $\operatorname{Comp}_n$ and subsets of $[n-1]$. Now, apply Lemma 5.2.6 to $G = [n-1]$, $f_A = f_{D^{-1}(A)}$ and $g_A = g_{D^{-1}(A)}$, and translate using the dictionary. □

Now, we can see the following about the fundamental quasisymmetric functions:

**Proposition 5.2.8.** *The family $\{L_\alpha\}_{\alpha\in\operatorname{Comp}}$ is a $\mathbf{k}$-basis for* QSym, *and each $n \in \mathbb{N}$ and $\alpha \in \operatorname{Comp}_n$ satisfy*

$$M_\alpha = \sum_{\substack{\beta\in\operatorname{Comp}_n: \\ \beta \text{ refines } \alpha}} (-1)^{\ell(\beta)-\ell(\alpha)} L_\beta. \tag{5.2.2}$$

*Proof.* Fix $n \in \mathbb{N}$. Recall the equality (5.2.1). Thus, Lemma 5.2.7(b) (applied to $V = \operatorname{QSym}$, $f_\alpha = M_\alpha$ and $g_\alpha = L_\alpha$) yields (5.2.2).

Recall that the family $(M_\alpha)_{\alpha\in\operatorname{Comp}_n}$ is a basis of the $\mathbf{k}$-module $\operatorname{QSym}_n$. The equality (5.2.1) shows that the family $(L_\alpha)_{\alpha\in\operatorname{Comp}_n}$ expands invertibly triangularly[261] with respect to the family $(M_\alpha)_{\alpha\in\operatorname{Comp}_n}$ (where $\operatorname{Comp}_n$ is equipped with the refinement order).[262] Thus, Corollary 11.1.19(e) (applied to $\operatorname{QSym}_n$, $\operatorname{Comp}_n$, $(M_\alpha)_{\alpha\in\operatorname{Comp}_n}$ and $(L_\alpha)_{\alpha\in\operatorname{Comp}_n}$ instead of $M$, $S$, $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$) shows that the family $(L_\alpha)_{\alpha\in\operatorname{Comp}_n}$ is a basis of the $\mathbf{k}$-module $\operatorname{QSym}_n$. Combining this fact for all $n \in \mathbb{N}$, we conclude that the family $(L_\alpha)_{\alpha\in\operatorname{Comp}}$ is a basis of the $\mathbf{k}$-module QSym. This completes the proof of Proposition 5.2.8. □

**Proposition 5.2.9.** *Let $n \in \mathbb{N}$. Let $\alpha$ be a composition of $n$. Let $I$ be an infinite totally ordered set. Then,*

$$L_\alpha\left(\{x_i\}_{i\in I}\right) = \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I; \\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n},$$

*where $L_\alpha\left(\{x_i\}_{i\in I}\right)$ is defined as the image of $L_\alpha$ under the isomorphism* $\operatorname{QSym} \to \operatorname{QSym}\left(\{x_i\}_{i\in I}\right)$ *obtained in Definition 5.1.5. In particular, for the standard (totally ordered) variable set $\mathbf{x} = (x_1 < x_2 < \cdots)$, we obtain*

$$L_\alpha = L_\alpha(\mathbf{x}) = \sum_{\substack{(1\le)i_1\le i_2\le\cdots\le i_n; \\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n}. \tag{5.2.3}$$

*Proof.* Every composition $\beta = (\beta_1, \ldots, \beta_\ell)$ of $n$ satisfies

$$\begin{aligned} M_\beta\left(\{x_i\}_{i\in I}\right) &= \sum_{k_1<\cdots<k_\ell \text{ in } I} x_{k_1}^{\beta_1}\cdots x_{k_\ell}^{\beta_\ell} \\ &= \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I; \\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n}. \end{aligned} \tag{5.2.4}$$

[261] See Section 11.1 for a definition of this concept.

[262] In fact, it expands unitriangularly with respect to the latter family.

Applying the ring homomorphism $\operatorname{QSym} \to \operatorname{QSym}\left(\{x_i\}_{i\in I}\right)$ to (5.2.1), we obtain

$$\begin{aligned}
L_\alpha\left(\{x_i\}_{i\in I}\right) &= \sum_{\substack{\beta\in\operatorname{Comp}_n:\\ \beta \text{ refines } \alpha}} M_\beta\left(\{x_i\}_{i\in I}\right)\\
&\overset{(5.2.4)}{=} \sum_{\substack{\beta\in\operatorname{Comp}_n:\\ \beta \text{ refines } \alpha}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n}\\
&= \sum_{\substack{\beta\in\operatorname{Comp}_n:\\ D(\alpha)\subset D(\beta)}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n}\\
&= \sum_{\substack{Z\subset[n-1]:\\ D(\alpha)\subset Z}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in Z}} x_{i_1}x_{i_2}\cdots x_{i_n}\\
&= \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n}. \qquad \square
\end{aligned}$$

**Proposition 5.2.10.** *Assume that the labelled poset $P$ is a total or linear order $w = (w_1 < \cdots < w_n)$ (that is, $P = \{w_1, w_2, \ldots, w_n\}$ as sets, and the order $<_P$ is given by $w_1 <_P w_2 <_P \cdots <_P w_n$). Let* $\operatorname{Des}(w)$ *be the* descent set *of $w$, defined by*

$$\operatorname{Des}(w) := \{i : w_i >_{\mathbb{Z}} w_{i+1}\} \subset \{1, 2, \ldots, n-1\}.$$

*Let $\alpha \in \operatorname{Comp}_n$ be the unique composition in $\operatorname{Comp}_n$ having partial sums $D(\alpha) = \operatorname{Des}(w)$. Then, the generating function $F_w(\mathbf{x})$ equals the fundamental quasisymmetric function $L_\alpha$. In particular, $F_w(\mathbf{x})$ depends only upon the descent set* $\operatorname{Des}(w)$.

E.g., total order $w = 35142$ has $\operatorname{Des}(w) = \{2, 4\}$ and composition $\alpha = (2, 2, 1)$, so

$$\begin{aligned}
F_{35142}(\mathbf{x}) &= \sum_{f(3)\le f(5)<f(1)\le f(4)<f(2)} x_{f(3)}x_{f(5)}x_{f(1)}x_{f(4)}x_{f(2)}\\
&= \sum_{i_1\le i_2<i_3\le i_4<i_5} x_{i_1}x_{i_2}x_{i_3}x_{i_4}x_{i_5}\\
&= L_{(2,2,1)} = M_{(2,2,1)} + M_{(2,1,1,1)} + M_{(1,1,2,1)} + M_{(1,1,1,1,1)}.
\end{aligned}$$

*Proof of Proposition 5.2.10.* Write $F_w(\mathbf{x})$ as a sum of monomials $x_{f(w_1)} \cdots x_{f(w_n)}$ over all $w$-partitions $f$. These $w$-partitions are exactly the maps $f : w \to \{1, 2, 3, \ldots\}$ satisfying $f(w_1) \le \cdots \le f(w_n)$ and having strict inequalities $f(w_i) < f(w_{i+1})$ whenever $i$ is in $\operatorname{Des}(w)$ (because if two elements $w_a$ and $w_b$ of $w$ satisfy $w_a <_w w_b$ and $w_a >_{\mathbb{Z}} w_b$, then they must satisfy $a < b$ and $i \in \operatorname{Des}(w)$ for some $i \in \{a, a+1, \ldots, b-1\}$; thus, the conditions "$f(w_1) \le \cdots \le f(w_n)$" and "$f(w_i) < f(w_{i+1})$ whenever $i$ is in $\operatorname{Des}(w)$" ensure that $f(w_a) < f(w_b)$ in this case). Therefore, they are in bijection with the weakly increasing sequences $(i_1 \le i_2 \le \cdots \le i_n)$ of positive integers having strict inequalities $i_j < i_{j+1}$ whenever $i \in \operatorname{Des}(w)$ (namely, the bijection sends any $w$-partition $f$ to the sequence

$(f(w_1) \leq f(w_2) \leq \cdots \leq f(w_n)))$. Hence,

$$F_w(\mathbf{x}) = \sum_{f \in \mathcal{A}(w)} \mathbf{x}_f = \sum_{\substack{(1\leq) i_1 \leq i_2 \leq \cdots \leq i_n; \\ i_j < i_{j+1} \text{ if } j \in \operatorname{Des}(w)}} x_{i_1} x_{i_2} \cdots x_{i_n}$$
$$= \sum_{\substack{(1\leq) i_1 \leq i_2 \leq \cdots \leq i_n; \\ i_j < i_{j+1} \text{ if } j \in D(\alpha)}} x_{i_1} x_{i_2} \cdots x_{i_n} \qquad (\text{since } \operatorname{Des}(w) = D(\alpha)).$$

Comparing this with (5.2.3), we conclude that $F_w(\mathbf{x}) = L_\alpha$. □

The next proposition ([206, Cor. 7.19.5], [140, Cor. 3.3.24]) is an algebraic shadow of Stanley's main lemma [206, Thm. 7.19.4] in $P$-partition theory. It expands any $F_P(\mathbf{x})$ in the $\{L_\alpha\}$ basis, as a sum over the set $\mathcal{L}(P)$ of all *linear extensions* $w$ of $P$ [263]. E.g., the poset $P$ from Example 5.2.2 has $\mathcal{L}(P) = \{3124, 3142, 3412\}$.

**Theorem 5.2.11.** *For any labelled poset $P$,*

$$F_P(\mathbf{x}) = \sum_{w \in \mathcal{L}(P)} F_w(\mathbf{x}).$$

*Proof.* We give Gessel's proof [79, Thm. 1], via induction on the number of pairs $i, j$ which are incomparable in $P$. When this quantity is 0, then $P$ is itself a linear order $w$, so that $\mathcal{L}(P) = \{w\}$ and there is nothing to prove.

In the inductive step, let $i, j$ be incomparable elements. Consider the two posets $P_{i<j}$ and $P_{j<i}$ which are obtained from $P$ by adding in an order relation between $i$ and $j$, and then taking the transitive closure; it is not hard to see that these transitive closures cannot contain a cycle, so that these really do define two posets. The result then follows by induction applied to $P_{i<j}, P_{j<i}$, once one notices that $\mathcal{L}(P) = \mathcal{L}(P_{i<j}) \sqcup \mathcal{L}(P_{j<i})$ since every linear extension $w$ of $P$ either has $i$ before $j$ or vice-versa, and $\mathcal{A}(P) = \mathcal{A}(P_{i<j}) \sqcup \mathcal{A}(P_{j<i})$ since, assuming that $i <_{\mathbb{Z}} j$ without loss of generality, every $f$ in $\mathcal{A}(P)$ either satisfies $f(i) \leq f(j)$ or $f(i) > f(j)$. □

**Example 5.2.12.** To illustrate the induction in the above proof, consider the poset $P$ from Example 5.2.2, having $\mathcal{L}(P) = \{3124, 3142, 3412\}$. Then

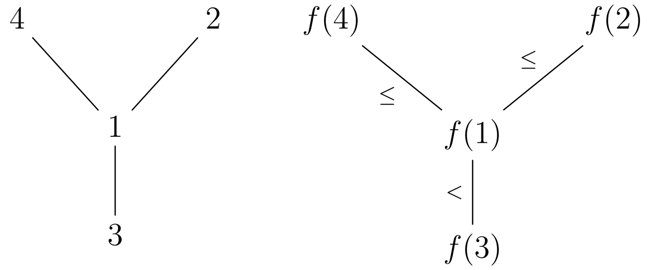
[263] Let us explain what we mean by linear extensions and how we represent them.

If $\mathbf{P}$ is a finite poset, then a *linear extension* of $\mathbf{P}$ denotes a total order $w$ on the set $\mathbf{P}$ having the property that every two elements $i$ and $j$ of $\mathbf{P}$ satisfying $i <_{\mathbf{P}} j$ satisfy $i <_w j$. (In other words, it is a linear order on the ground set $\mathbf{P}$ which extends $\mathbf{P}$ as a poset; therefore the name.) We identify such a total order $w$ with the list $(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n)$ containing all elements of $\mathbf{P}$ in $w$-increasing order (that is, $\mathbf{p}_1 <_w \mathbf{p}_2 <_w \cdots <_w \mathbf{p}_n$).

(Stanley, in [206, §3.5], defines linear extensions in a slightly different way: For him, a linear extension of a finite poset $\mathbf{P}$ is an order-preserving bijection from $\mathbf{P}$ to the subposet $\{1, 2, \ldots, |\mathbf{P}|\}$ of $\mathbb{Z}$. But this is equivalent to our definition, since a bijection like this can be used to transport the order relation of $\{1, 2, \ldots, |\mathbf{P}|\}$ back to $\mathbf{P}$, thus resulting in a total order on $\mathbf{P}$ which is a linear extension of $\mathbf{P}$ in our sense.)

choosing as incomparable pair $(i, j) = (1, 4)$, one has

$P_{i<j} =$

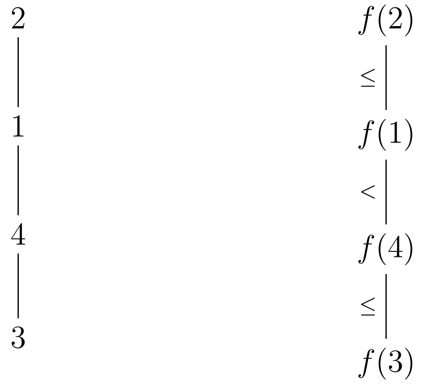


,

thus $\mathcal{L}(P_{i<j}) = \{3124, 3142\}$

and

$P_{j<i} =$



, thus $\mathcal{L}(P_{j<i}) = \{3412\}$.

**Exercise 5.2.13.** Give an alternative proof for Theorem 5.2.11.

[**Hint:** For every $f : P \to \{1, 2, 3, \ldots\}$, we can define a binary relation $\prec_f$ on the set $P$ by letting $i \prec_f j$ hold if and only if

$$(f(i) < f(j) \text{ or } (f(i) = f(j) \text{ and } i <_{\mathbb{Z}} j)).$$

Show that this binary relation $\prec_f$ is (the smaller relation of) a total order. When $f$ is a $P$-partition, then endowing the set $P$ with this total order yields a linear extension of $P$. Use this to show that the set $\mathcal{A}(P)$ is the union of its disjoint subsets $\mathcal{A}(w)$ with $w \in \mathcal{L}(P)$.]

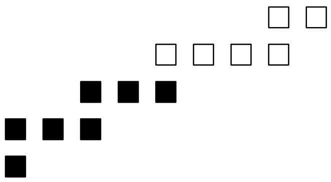
Various other properties of the quasisymmetric functions $F_P(\mathbf{x})$ are studied, e.g., in [152].

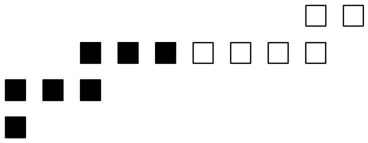
We next wish to describe the structure maps for the Hopf algebra QSym in the basis $\{L_\alpha\}$ of fundamental quasisymmetric functions. For this purpose, two more definitions are useful.

**Definition 5.2.14.** Given two nonempty compositions $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_m)$, their *near-concatenation* is

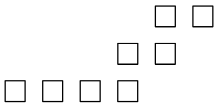
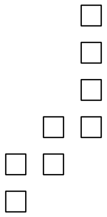
$$\alpha \odot \beta := (\alpha_1, \ldots, \alpha_{\ell-1}, \alpha_\ell + \beta_1, \beta_2, \ldots, \beta_m).$$

For example, the figure below depicts for $\alpha = (1, 3, 3)$ (black squares) and $\beta = (4, 2)$ (white squares) the concatenation and near-concatenation as ribbons:[264]

$\mathrm{Rib}\,(\alpha \cdot \beta) =$ 

$\mathrm{Rib}\,(\alpha \odot \beta) =$ 

Lastly, given $\alpha$ in $\mathrm{Comp}_n$, let $\omega(\alpha)$ be the unique composition in $\mathrm{Comp}_n$ whose partial sums $D(\omega(\alpha))$ form the complementary set within $[n-1]$ to the partial sums $D(\mathrm{rev}(\alpha))$; alternatively, one can check this means that the ribbon for $\omega(\alpha)$ is obtained from that of $\alpha$ by conjugation or transposing, that is, if $\mathrm{Rib}\,(\alpha) = \lambda/\mu$ then $\mathrm{Rib}\,(\omega(\alpha)) = \lambda^t/\mu^t$. E.g. if $\alpha = (4,2,2)$ so that $n = 8$, then $\mathrm{rev}(\alpha) = (2,2,4)$ has $D(\mathrm{rev}(\alpha)) = \{2,4\} \subset [7]$, complementary to the set $\{1,3,5,6,7\}$ which are the partial sums for $\omega(\alpha) = (1,2,2,1,1,1)$, and the ribbon diagrams of $\alpha$ and $\omega(\alpha)$ are

$\mathrm{Rib}\,(\alpha) =$  and $\mathrm{Rib}\,(\omega(\alpha)) =$ 

**Proposition 5.2.15.** *The structure maps for the Hopf algebra* QSym *in the basis $\{L_\alpha\}$ of fundamental quasisymmetric functions are as follows:*

$$\Delta L_\alpha = \sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha \text{ or } \beta\odot\gamma=\alpha}} L_\beta \otimes L_\gamma, \tag{5.2.5}$$

$$L_\alpha L_\beta = \sum_{w \in w_\alpha \sqcup\!\sqcup\, w_\beta} L_{\gamma(w)}, \tag{5.2.6}$$

$$S(L_\alpha) = (-1)^{|\alpha|} L_{\omega(\alpha)}. \tag{5.2.7}$$

*Here we are making use of the following notations in* (5.2.6) *(recall also Definition 1.6.2):*

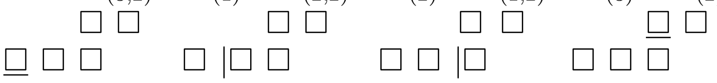
- *A* labelled linear order *will mean a labelled poset $P$ whose order $<_P$ is a total order. We will identify any labelled linear order $P$ with the word (over the alphabet $\mathbb{Z}$) obtained by writing down the elements of $P$ in increasing order (with respect to the total order $<_P$). This way, every word (over the alphabet $\mathbb{Z}$) which has no two equal letters becomes identified with a labelled linear order.*
- *$w_\alpha$ is any labelled linear order with underlying set $\{1, 2, \ldots, |\alpha|\}$ such that* $\mathrm{Des}\,(w_\alpha) = D\,(\alpha)$.
- *$w_\beta$ is any labelled linear order with underlying set $\{|\alpha|+1, |\alpha|+2, \ldots, |\alpha|+|\beta|\}$ such that* $\mathrm{Des}\,(w_\beta) = D\,(\beta)$.
- *$\gamma(w)$ is the unique composition of $|\alpha|+|\beta|$ with* $D(\gamma(w)) = \mathrm{Des}(w)$.

[264] The ribbons are drawn with their boxes spaced out in order to facilitate counting.

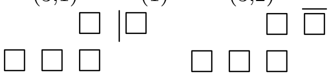
*(The right hand side of* (5.2.6) *is to be read as a sum over all $w$, for a fixed choice of $w_\alpha$ and $w_\beta$.)*

At first glance the formula (5.2.5) for $\Delta L_\alpha$ might seem more complicated than the formula of Proposition 5.1.7 for $\Delta M_\alpha$. However, it is equally simple when viewed in terms of ribbon diagrams: it cuts the ribbon diagram $\operatorname{Rib}(\alpha)$ into two smaller ribbons $\operatorname{Rib}(\beta)$ and $\operatorname{Rib}(\gamma)$, in all $|\alpha|+1$ possible ways, via *horizontal* cuts ($\beta\cdot\gamma=\alpha$) or *vertical* cuts ($\beta\odot\gamma=\alpha$). For example,

$$\Delta L_{(3,2)} = 1\otimes L_{(3,2)} + L_{(1)}\otimes L_{(2,2)} + L_{(2)}\otimes L_{(1,2)} + L_{(3)}\otimes L_{(2)}$$



$$+L_{(3,1)}\otimes L_{(1)} + L_{(3,2)}\otimes 1.$$



**Example 5.2.16.** To multiply $L_{(1,1)}L_{(2)}$, one could pick $w_\alpha=21$ and $w_\beta=34$, and then

$$\begin{aligned} L_{(1,1)}L_{(2)} &= \sum_{w\in 21\sqcup\!\sqcup 34} L_{\gamma(w)} \\ &= L_{\gamma(2134)} + L_{\gamma(2314)} + L_{\gamma(3214)} + L_{\gamma(2341)} + L_{\gamma(3241)} + L_{\gamma(3421)} \\ &= L_{(1,3)} + L_{(2,2)} + L_{(1,1,2)} + L_{(3,1)} + L_{(1,2,1)} + L_{(2,1,1)}. \end{aligned}$$

Before we prove Proposition 5.2.15, we state a simple lemma:

**Lemma 5.2.17.** *Let $Q$ and $R$ be two labelled posets whose underlying sets are disjoint. Let $Q\sqcup R$ be the disjoint union of these posets $Q$ and $R$; this is again a labelled poset. Then,*

$$F_Q(\mathbf{x})\,F_R(\mathbf{x}) = F_{Q\sqcup R}(\mathbf{x}).$$

*Proof.* We identify the underlying set of $Q\sqcup R$ with $Q\cup R$ (since the sets $Q$ and $R$ are already disjoint). If $f : Q\sqcup R\to\{1,2,3,\ldots\}$ is a $Q\sqcup R$-partition, then its restrictions $f\mid_Q$ and $f\mid_R$ are a $Q$-partition and an $R$-partition, respectively. Conversely, any pair of a $Q$-partition and an $R$-partition can be combined to form a $Q\sqcup R$-partition. Thus, there is a bijective correspondence between the addends in the expanded sum $F_Q(\mathbf{x})\,F_R(\mathbf{x})$ and the addends in $F_{Q\sqcup R}(\mathbf{x})$. □

*Proof of Proposition 5.2.15.* To prove formula (5.2.5) for $\alpha$ in $\operatorname{Comp}_n$, note that

$$\begin{aligned} \Delta L_\alpha &= L_\alpha(\mathbf{x},\mathbf{y}) \\ &= \sum_{k=0}^{n} \sum_{\substack{1\le i_1\le\cdots\le i_k,\\ 1\le i_{k+1}\le\cdots\le i_n:\\ i_r<i_{r+1}\text{ for } r\in D(\alpha)\setminus\{k\}}} x_{i_1}\cdots x_{i_k}\cdot y_{i_{k+1}}\cdots y_{i_n} \qquad (5.2.8) \end{aligned}$$

by Proposition 5.2.9 (where we identify $\operatorname{QSym}\otimes\operatorname{QSym}$ with a $\mathbf{k}$-subalgebra of $R(\mathbf{x},\mathbf{y})$ by means of the embedding $\operatorname{QSym}\otimes\operatorname{QSym}\overset{\cong}{\to}\operatorname{QSym}(\mathbf{x})\otimes\operatorname{QSym}(\mathbf{y})\hookrightarrow R(\mathbf{x},\mathbf{y})$ as in the definition of the comultiplication on QSym). One then realizes that the inner sums corresponding to values of $k$ that lie (resp. do not lie) in $D(\alpha) \cup \{0, n\}$ correspond to the terms $L_\beta(\mathbf{x})L_\gamma(\mathbf{y})$ for pairs $(\beta, \gamma)$ in which $\beta \cdot \gamma = \alpha$ (resp. $\beta \odot \gamma = \alpha$).

For formula (5.2.6), let $P$ be the labelled poset which is the disjoint union of linear orders $w_\alpha, w_\beta$. Then

$$L_\alpha L_\beta = F_{w_\alpha}(\mathbf{x})F_{w_\beta}(\mathbf{x}) = F_P(\mathbf{x}) = \sum_{w \in \mathcal{L}(P)} F_w(\mathbf{x}) = \sum_{w \in w_\alpha \sqcup\!\sqcup\, w_\beta} L_{\gamma(w)}$$

where the first equality used Proposition 5.2.10, the second equality comes from Lemma 5.2.17, the third equality from Theorem 5.2.11, and the fourth from the equality $\mathcal{L}(P) = w_\alpha \sqcup\!\sqcup\, w_\beta$.

To prove formula (5.2.7), compute using Theorem 5.1.11 that

$$S(L_\alpha) = \sum_{\beta \text{ refining } \alpha} S(M_\beta) = \sum_{\substack{(\beta,\gamma): \\ \beta \text{ refines } \alpha, \\ \gamma \text{ coarsens } \operatorname{rev}(\beta)}} (-1)^{\ell(\beta)} M_\gamma = \sum_\gamma M_\gamma \sum_\beta (-1)^{\ell(\beta)}$$

in which the last inner sum is over $\beta$ for which

$$D(\beta) \supset D(\alpha) \cup D(\operatorname{rev}(\gamma)).$$

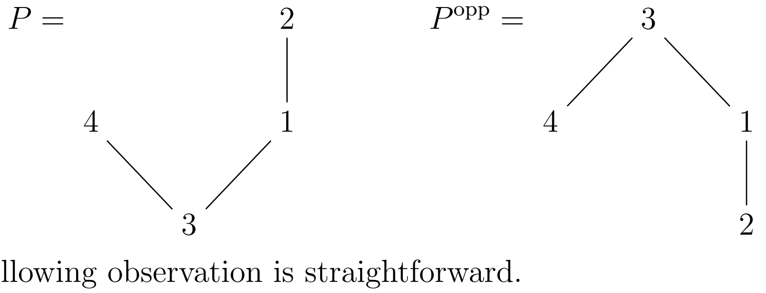
The alternating signs make such inner sums vanish unless they have only the single term where $D(\beta) = [n-1]$ (that is, $\beta = (1^n)$). This happens exactly when $D(\operatorname{rev}(\gamma)) \cup D(\alpha) = [n-1]$ or equivalently, when $D(\operatorname{rev}(\gamma))$ contains the complement of $D(\alpha)$, that is, when $D(\gamma)$ contains the complement of $D(\operatorname{rev}(\alpha))$, that is, when $\gamma$ refines $\omega(\alpha)$. Thus

$$S(L_\alpha) = \sum_{\substack{\gamma \in \mathrm{Comp}_n: \\ \gamma \text{ refines } \omega(\alpha)}} M_\gamma \cdot (-1)^n = (-1)^{|\alpha|} L_{\omega(\alpha)}. \qquad \square$$

The antipode formula (5.2.7) for $L_\alpha$ leads to a general interpretation for the antipode of QSym acting on $P$-partition enumerators $F_P(\mathbf{x})$.

**Definition 5.2.18.** Given a labelled poset $P$ on $\{1, 2, \ldots, n\}$, let the *opposite* or *dual* labelled poset $P^{\mathrm{opp}}$ be the labelled poset on $\{1, 2, \ldots, n\}$ that has $i <_{P^{\mathrm{opp}}} j$ if and only if $j <_P i$.

For example,



The following observation is straightforward.

**Proposition 5.2.19.** *When $P$ is a linear order corresponding to some permutation $w = (w_1, \ldots, w_n)$ in $\mathfrak{S}_n$, then $w^{\mathrm{opp}} = ww_0$ where $w_0 \in \mathfrak{S}_n$ is the permutation that swaps $i \leftrightarrow n+1-i$ (this is the so-called* longest permutation, *thus named due to it having the highest "Coxeter length" among all permutations in $\mathfrak{S}_n$). Furthermore, in this situation one has $F_w(\mathbf{x}) = L_\alpha$, that is, $\mathrm{Des}(w) = D(\alpha)$ if and only if $\mathrm{Des}(w^{\mathrm{opp}}) = D(\omega(\alpha))$, that is $F_{w^{\mathrm{opp}}}(\mathbf{x}) = L_{\omega(\alpha)}$. Thus,*

$$S(F_w(\mathbf{x})) = (-1)^n F_{w^{\mathrm{opp}}}(\mathbf{x}).$$

For example, given the compositions considered earlier:

$$\alpha = (4,2,2) = \begin{array}{cccccc} &&&&\square&\square\\ &&&\square&\square&\\ \square&\square&\square&\square&& \end{array} \qquad \text{and} \qquad \omega(\alpha) = (1,2,2,1,1,1) = \begin{array}{ccc} &&\square\\ &&\square\\ &&\square\\ &\square&\square\\ \square&\square&\\ \square&& \end{array}$$

if one picks $w = 1235 \cdot 47 \cdot 68$ (with descent positions marked by dots) having $\text{Des}(w) = \{4,6\} = D(\alpha)$, then $w^{\text{opp}} = ww_0 = 8 \cdot 67 \cdot 45 \cdot 3 \cdot 2 \cdot 1$ has $\text{Des}(w^{\text{opp}}) = \{1,3,5,6,7\} = D(\omega(\alpha))$.

**Corollary 5.2.20.** *For any labelled poset $P$ on $\{1,2,\ldots,n\}$, one has*

$$S\left(F_P(\mathbf{x})\right) = (-1)^n F_{P^{\text{opp}}}(\mathbf{x}).$$

*Proof.* Since $S$ is linear, one can apply Theorem 5.2.11 and Proposition 5.2.19, obtaining

$$S\left(F_P(\mathbf{x})\right) = \sum_{w\in\mathcal{L}(P)} S(F_w(\mathbf{x})) = \sum_{w\in\mathcal{L}(P)} (-1)^n F_{w^{\text{opp}}}(\mathbf{x}) = (-1)^n F_{P^{\text{opp}}}(\mathbf{x}),$$

as $\mathcal{L}(P^{\text{opp}}) = \{w^{\text{opp}} : w \in \mathcal{L}(P)\}$. □

*Remark* 5.2.21. Malvenuto and Reutenauer, in [147, Theorem 3.1], prove an even more general antipode formula, which encompasses our Corollary 5.2.20, Proposition 5.2.19, Theorem 5.1.11 and (5.2.7). See [85, Theorem 4.2] for a restatement and a self-contained proof of this theorem (and [85, Theorem 4.7] for an even further generalization).

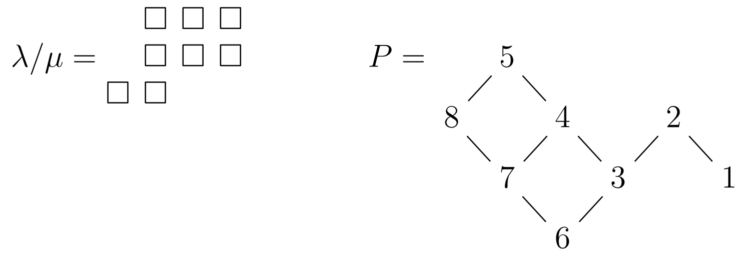
We remark on a special case of Corollary 5.2.20 to which we alluded earlier, related to skew Schur functions.

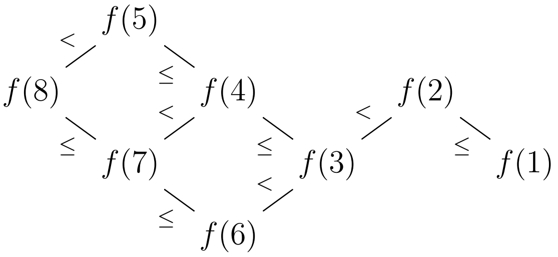
**Corollary 5.2.22.** *In $\Lambda$, the action of $\omega$ and the antipode $S$ on skew Schur functions $s_{\lambda/\mu}$ are as follows:*

$$\omega(s_{\lambda/\mu}) = s_{\lambda^t/\mu^t}, \tag{5.2.9}$$

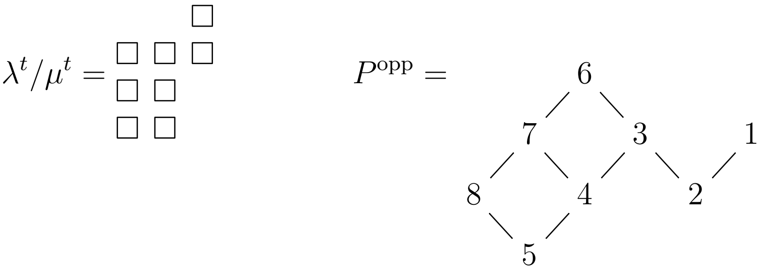
$$S(s_{\lambda/\mu}) = (-1)^{|\lambda/\mu|} s_{\lambda^t/\mu^t}. \tag{5.2.10}$$

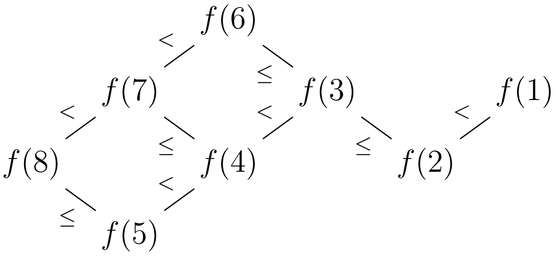
*Proof.* Given a skew shape $\lambda/\mu$, one can always create a labelled poset $P$ which is its *skew Ferrers poset*, together with one of many *column-strict labellings*, in such a way that $F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x})$. An example is shown here for $\lambda/\mu = (4,4,2)/(1,1,0)$:





The general definition is as follows: Let $P$ be the set of all boxes of the skew diagram $\lambda/\mu$. Label these boxes by the numbers $1, 2, \ldots, n$ (where $n = |\lambda/\mu|$) row by row from bottom to top (reading every row from left to right), and then define an order relation $<_P$ on $P$ by requiring that every box be smaller (in $P$) than its right neighbor and smaller (in $P$) than its lower neighbor. It is not hard to see that in this situation, $F_{P^{\text{opp}}}(\mathbf{x}) = \sum_T \mathbf{x}^{\text{cont}(T)}$ as $T$ ranges over all *reverse semistandard tableaux* or *column-strict plane partitions* of $\lambda^t/\mu^t$:





But this means that $F_{P^{\text{opp}}}(\mathbf{x}) = s_{\lambda^t/\mu^t}(\mathbf{x})$, since the fact that skew Schur functions lie in $\Lambda$ implies that they can be defined either as generating functions for column-strict tableaux or reverse semistandard tableaux; see Remark 2.2.5 above, or [206, Prop. 7.10.4].

Thus we have

$$F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x}),$$
$$F_{P^{\text{opp}}}(\mathbf{x}) = s_{\lambda^t/\mu^t}(\mathbf{x}).$$

Corollary 1.4.27 tells us that the antipode for QSym must specialize to the antipode for $\Lambda$ (see also Remark 5.4.11 below), so (5.2.10) is a special case of Corollary 5.2.20. Then (5.2.9) follows from the relation (2.4.11) that $S(f) = (-1)^n \omega(f)$ for $f$ in $\Lambda_n$. □

*Remark* 5.2.23. Before leaving $P$-partitions temporarily, we mention two open questions about them.

The first is a conjecture of Stanley from his thesis [203]. As mentioned in the proof of Corollary 5.2.22, each skew Schur function $s_{\lambda/\mu}(\mathbf{x})$ is a special instance of $P$-partition enumerator $F_P(\mathbf{x})$.

**Conjecture 5.2.24.** *A labelled poset $P$ has $F_P(\mathbf{x})$ symmetric, and not just quasisymmetric,* if and only if *$P$ is a column-strict labelling of some skew Ferrers poset $\lambda/\mu$.*

A somewhat weaker result in this direction was proven by Malvenuto in her thesis [145, Thm. 6.4], showing that if a labelled poset $P$ has the stronger property that its set of linear extensions $\mathcal{L}(P)$ is a union of *plactic* or *Knuth equivalence classes*, then $P$ must be a column-strict labelling of a skew Ferrers poset.

The next question is due to P. McNamara, and is suggested by the obvious factorizations of $P$-partition enumerators $F_{P_1 \sqcup P_2}(\mathbf{x}) = F_{P_1}(\mathbf{x}) F_{P_2}(\mathbf{x})$ (Lemma 5.2.17).

*Question* 5.2.25. If $\mathbf{k}$ is a field, does a *connected* labelled poset $P$ always have $F_P(\mathbf{x})$ *irreducible* within the ring QSym?

The phrasing of this question requires further comment. It is assumed here that $\mathbf{x} = (x_1, x_2, \ldots)$ is infinite; for example when $P$ is a 2-element chain labelled "against the grain" (i.e., the bigger element of the chain has the smaller label), then $F_P(\mathbf{x}) = e_2(\mathbf{x})$ is irreducible, but its specialization to two variables $\mathbf{x} = (x_1, x_2)$ is $e_2(x_1, x_2) = x_1 x_2$, which is reducible. If one wishes to work in finitely many variables $\mathbf{x} = (x_1, \ldots, x_m)$ one can perhaps assume that $m$ is at least $|P| + 1$.

When working in QSym = QSym($\mathbf{x}$) in infinitely many variables, it is perhaps not so clear where factorizations occur. For example, if $f$ lies in QSym and factors $f = g \cdot h$ with $g, h$ in $R(\mathbf{x})$, does this imply that $g, h$ also lie in QSym? The answer is "Yes" (for $\mathbf{k} = \mathbb{Z}$), but this is not obvious, and was proven by P. Pylyavskyy in [175, Chap. 11].

One also might wonder whether $\mathrm{QSym}_{\mathbb{Z}}$ is a unique factorization domain, but this follows from the result of M. Hazewinkel ([89] and [93, Thm. 6.7.5], and Theorem 6.4.3 further below) who proved a conjecture of Ditters that $\mathrm{QSym}_{\mathbb{Z}}$ is a polynomial algebra; earlier Malvenuto and Reutenauer [146, Cor. 2.2] had shown that $\mathrm{QSym}_{\mathbb{Q}}$ is a polynomial algebra. In fact, one can find polynomial generators $\{P_\alpha\}$ for $\mathrm{QSym}_{\mathbb{Q}}$ as a subset of the dual basis to the $\mathbb{Q}$-basis $\{\xi_\alpha\}$ for $\mathrm{NSym}_{\mathbb{Q}}$ which comes from taking products $\xi_\alpha := \xi_{\alpha_1} \cdots \xi_{\alpha_\ell}$ of the elements $\{\xi_n\}$ defined in Remark 5.4.4 below. Specifically, one takes those $P_\alpha$ for which the composition $\alpha$ is a *Lyndon composition*; see the First proof of Proposition 6.4.4 for a mild variation on this construction.

Hazewinkel's proof [93, Thm. 6.7.5] of the polynomiality of $\mathrm{QSym}_{\mathbb{Z}}$ also shows that QSym is a polynomial ring over $\Lambda$ (see Corollary 6.5.33); in particular, this yields that QSym is a free $\Lambda$-module.[265]

[265] The latter statement has an analogue in finitely many indeterminates, proven by Lauve and Mason in [125, Corollary 13]: The quasisymmetric functions QSym $\left(\{x_i\}_{i \in I}\right)$

An affirmative answer to Question 5.2.25 is known at least in the special case where $P$ is a connected column-strict labelling of a skew Ferrers diagram, that is, when $F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x})$ for some connected skew diagram $\lambda/\mu$; see [13].

### 5.3. **Standardization of $n$-tuples and the fundamental basis.**

Another equivalent description of the fundamental quasisymmetric functions $L_\alpha$ (Lemma 5.3.6 below) relies on the concept of words and of their standardizations. We shall study words in detail in Chapter 6; at this point, we merely introduce the few notions that we will need:

**Definition 5.3.1.** We fix a totally ordered set $\mathfrak{A}$, which we call the *alphabet*.

We recall that a *word over* $\mathfrak{A}$ is just a (finite) tuple of elements of $\mathfrak{A}$. A word $(w_1, w_2, \ldots, w_n)$ can be written as $w_1 w_2 \cdots w_n$ when this incurs no ambiguity.

If $w \in \mathfrak{A}^n$ is a word and $i \in \{1, 2, \ldots, n\}$, then the *$i$-th letter* of $w$ means the $i$-th entry of the $n$-tuple $w$. This $i$-th letter will be denoted by $w_i$.

Our next definition relies on a simple fact about permutations and words:[266]

**Proposition 5.3.2.** *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be any word. Then, there exists a unique permutation $\sigma \in \mathfrak{S}_n$ such that for every two elements $a$ and $b$ of $\{1, 2, \ldots, n\}$ satisfying $a < b$, we have*

$$(\sigma(a) < \sigma(b) \text{ if and only if } w_a \leq w_b).$$

**Definition 5.3.3.** Let $w \in \mathfrak{A}^n$ be any word. The unique permutation $\sigma \in \mathfrak{S}_n$ defined in Proposition 5.3.2 is called the *standardization* of $w$, and is denoted by $\operatorname{std} w$.

**Example 5.3.4.** If $\mathfrak{A}$ is the alphabet $\{1 < 2 < 3 < \cdots\}$, then $\operatorname{std}(41211424)$ is the permutation which is written (in one-line notation) as 61423758.

A simple method to compute the standardization of a word $w \in \mathfrak{A}^n$ is the following: Replace all occurrences of the smallest letter appearing in $w$ by the numbers $1, 2, \ldots, m_1$ (where $m_1$ is the number of these occurrences); then replace all occurrences of the second-smallest letter appearing in $w$ by the numbers $m_1 + 1, m_1 + 2, \ldots, m_1 + m_2$ (where $m_2$ is the number of these occurrences), and so on, until all letters are replaced by numbers.[267] The result is the standardization of $w$, in one-line notation.

Another method to compute the standardization $\operatorname{std} w$ of a word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ is based on sorting. Namely, consider the total order on the set $\mathfrak{A} \times \mathbb{Z}$ given by

$$(a, i) \leq (b, j) \text{ if and only if } (\text{either } a < b \text{ or } (a = b \text{ and } i \leq j)).$$

(In other words, two pairs in $\mathfrak{A} \times \mathbb{Z}$ are compared by first comparing their first entries, and then, in the case of a tie, using the second entries as tiebreakers.) Now, in order to compute $\operatorname{std} w$, we sort the $n$-tuple

are free as a $\Lambda\left(\{x_i\}_{i\in I}\right)$-module for any totally ordered set $I$, infinite or not. In the case of finite $I$, this cannot be derived by Hazewinkel's arguments, as the ring $\operatorname{QSym}\left(\{x_i\}_{i\in I}\right)$ is not in general a polynomial ring (e.g., when $\mathbf{k} = \mathbb{Q}$ and $I = \{1, 2\}$, this ring is not even a UFD, as witnessed by $\left(x_1^2 x_2\right) \cdot \left(x_1 x_2^2\right) = \left(x_1 x_2\right)^3$).

[266] See Exercise 5.3.7 below for a proof of Proposition 5.3.2.

[267] Here, a number is not considered to be a letter; thus, a number that replaces a letter will always be left in peace afterwards.

$((w_1, 1), (w_2, 2), \ldots, (w_n, n)) \in (\mathfrak{A} \times \mathbb{Z})^n$ into increasing order (with respect to the total order just described), thus obtaining a new $n$-tuple of the form $\left(\left(w_{\tau(1)}, \tau(1)\right), \left(w_{\tau(2)}, \tau(2)\right), \ldots, \left(w_{\tau(n)}, \tau(n)\right)\right)$ for some $\tau \in \mathfrak{S}_n$; the standardization $\operatorname{std} w$ is then $\tau^{-1}$.

**Definition 5.3.5.** Let $n \in \mathbb{N}$. Let $\sigma \in \mathfrak{S}_n$. Define a subset $\operatorname{Des} \sigma$ of $\{1, 2, \ldots, n-1\}$ by

$$\operatorname{Des} \sigma = \{i \in \{1, 2, \ldots, n-1\} \mid \sigma(i) > \sigma(i+1)\}.$$

(This is a particular case of the definition of $\operatorname{Des} w$ in Exercise 2.9.11, if we identify $\sigma$ with the $n$-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. It is also a particular case of the definition of $\operatorname{Des} w$ in Proposition 5.2.10, if we identify $\sigma$ with the total order $(\sigma(1) < \sigma(2) < \cdots < \sigma(n))$ on the set $\{1, 2, \ldots, n\}$.)

There is a unique composition $\alpha$ of $n$ satisfying $D(\alpha) = \operatorname{Des} \sigma$ (where $D(\alpha)$ is defined as in Definition 5.1.10). This composition will be denoted by $\gamma(\sigma)$.

The following lemma (equivalent to [182, Lemma 9.39]) yields another description of the fundamental quasisymmetric functions:

**Lemma 5.3.6.** *Let $\mathfrak{A}$ denote the totally ordered set $\{1 < 2 < 3 < \cdots\}$ of positive integers. For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$.*

*Let $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Then,*

$$L_{\gamma(\sigma)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w.$$

**Exercise 5.3.7.** Prove Proposition 5.3.2 and Lemma 5.3.6.

5.4. **The Hopf algebra** NSym **dual to** QSym**.** We introduce here the (graded) dual Hopf algebra to QSym. This is well-defined, as QSym is connected graded of finite type.

**Definition 5.4.1.** Let NSym := QSym$^o$, with dual pairing

$$\mathrm{NSym} \otimes \mathrm{QSym} \xrightarrow{(\cdot,\cdot)} \mathbf{k}.$$

Let $\{H_\alpha\}$ be the $\mathbf{k}$-basis of NSym dual to the $\mathbf{k}$-basis $\{M_\alpha\}$ of QSym, so that

$$(H_\alpha, M_\beta) = \delta_{\alpha,\beta}.$$

When the base ring $\mathbf{k}$ is not clear from the context, we write $\mathrm{NSym}_{\mathbf{k}}$ in lieu of NSym.

The Hopf algebra NSym is known as the *Hopf algebra of noncommutative symmetric functions*. Its study goes back to [77].

**Theorem 5.4.2.** *Letting $H_n := H_{(n)}$ for $n = 0, 1, 2, \ldots$, with $H_0 = 1$, one has that*

$$\mathrm{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots \rangle, \tag{5.4.1}$$

*the free associative (but not commutative) algebra on generators* $\{H_1, H_2, \ldots\}$ *with coproduct determined by*[268]

$$\Delta H_n = \sum_{i+j=n} H_i \otimes H_j. \tag{5.4.2}$$

*Proof.* Since Proposition 5.1.7 asserts that $\Delta M_\alpha = \sum_{(\beta,\gamma):\beta\cdot\gamma=\alpha} M_\beta \otimes M_\gamma$, and since $\{H_\alpha\}$ are dual to $\{M_\alpha\}$, one concludes that for any compositions $\beta, \gamma$, one has

$$H_\beta H_\gamma = H_{\beta\cdot\gamma}.$$

Iterating this gives

$$H_\alpha = H_{(\alpha_1,\ldots,\alpha_\ell)} = H_{\alpha_1} \cdots H_{\alpha_\ell}. \tag{5.4.3}$$

Since the $H_\alpha$ are a $\mathbf{k}$-basis for NSym, this shows NSym $\cong \mathbf{k}\langle H_1, H_2, \ldots\rangle$.

Note that $H_n = H_{(n)}$ is dual to $M_{(n)}$, so to understand $\Delta H_n$, one should understand how $M_{(n)}$ can appear as a term in the product $M_\alpha M_\beta$. By (5.1.1) this occurs only if $\alpha = (i), \beta = (j)$ where $i + j = n$, where

$$M_{(i)} M_{(j)} = M_{(i+j)} + M_{(i,j)} + M_{(j,i)}$$

(where the $M_{(i,j)}$ and $M_{(j,i)}$ addends have to be disregarded if one of $i$ and $j$ is 0). By duality, this implies the formula (5.4.2). □

**Corollary 5.4.3.** *The algebra homomorphism defined by*

$$\begin{array}{rcl} \text{NSym} & \xrightarrow{\pi} & \Lambda, \\ H_n & \longmapsto & h_n \end{array}$$

*is a Hopf algebra surjection, and adjoint to the inclusion* $\Lambda \overset{i}{\hookrightarrow}$ QSym *(with respect to the dual pairing* NSym $\otimes$ QSym $\xrightarrow{(\cdot,\cdot)} \mathbf{k}$*).*

*Proof.* As an algebra morphism, $\pi$ may be identified with the surjection $T(V) \to \mathrm{Sym}(V)$ from the tensor algebra on a graded free $\mathbf{k}$-module $V$ with basis $\{H_1, H_2, \ldots\}$ to the symmetric algebra on $V$, since

$$\text{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots\rangle,$$
$$\Lambda \cong \mathbf{k}[h_1, h_2, \ldots].$$

As (5.4.2) and Proposition 2.3.6(iii) assert that

$$\Delta H_n = \sum_{i+j=n} H_i \otimes H_j,$$
$$\Delta h_n = \sum_{i+j=n} h_i \otimes h_j,$$

this map $\pi$ is also a bialgebra morphism, and hence a Hopf morphism by Corollary 1.4.27.

[268] The abbreviated summation indexing $\sum_{i+j=n} t_{i,j}$ used here is intended to mean

$$\sum_{\substack{(i,j)\in\mathbb{N}^2;\\ i+j=n}} t_{i,j}.$$

To check $\pi$ is adjoint to $i$, let $\lambda(\alpha)$ denote the partition which is the weakly decreasing rearrangement of the composition $\alpha$, and note that the bases $\{H_\alpha\}$ of NSym and $\{m_\lambda\}$ of $\Lambda$ satisfy

$$\begin{aligned}(\pi(H_\alpha), m_\lambda) = (h_{\lambda(\alpha)}, m_\lambda) = \left\{\begin{matrix} 1 & \text{if } \lambda(\alpha) = \lambda \\ 0 & \text{otherwise} \end{matrix}\right\} = \left( H_\alpha, \sum_{\beta:\lambda(\beta)=\lambda} M_\beta \right) \\ = (H_\alpha, i(m_\lambda)). \end{aligned} \qquad \square$$

*Remark* 5.4.4. For those who prefer generating functions to sign-reversing involutions, we sketch here Malvenuto and Reutenauer's elegant proof [146, Cor. 2.3] of the antipode formula (Theorem 5.1.11). One needs to know that when $\mathbb{Q}$ is a subring of $\mathbf{k}$, and $A$ is a $\mathbf{k}$-algebra (possibly noncommutative), in the ring of power series $A[[t]]$ where $t$ commutes with all of $A$, one still has familiar facts, such as

$$a(t) = \log b(t) \quad \text{if and only if} \quad b(t) = \exp a(t)$$

and whenever $a(t), b(t)$ commute in $A[[t]]$, one has

$$\exp\left(a(t) + b(t)\right) = \exp a(t) \exp b(t), \tag{5.4.4}$$

$$\log\left(a(t)b(t)\right) = \log a(t) + \log b(t). \tag{5.4.5}$$

Start by assuming WLOG that $\mathbf{k} = \mathbb{Z}$ (as $\mathrm{NSym}_{\mathbf{k}} = \mathrm{NSym}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbf{k}$ in the general case). Now, define in $\mathrm{NSym}_{\mathbb{Q}} = \mathrm{NSym} \otimes_{\mathbb{Z}} \mathbb{Q}$ the elements $\{\xi_1, \xi_2, \ldots\}$ via generating functions in $\mathrm{NSym}_{\mathbb{Q}}[[t]]$:

$$\begin{aligned} \widetilde{H}(t) &:= \sum_{n\geq 0} H_n t^n, \\ \xi(t) &:= \sum_{n \geq 1} \xi_n t^n = \log \widetilde{H}(t). \end{aligned} \tag{5.4.6}$$

One first checks that this makes each $\xi_n$ primitive, via a computation in the ring $(\mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}})[[t]]$ (into which we "embed" the ring $(\mathrm{NSym}_{\mathbb{Q}}[[t]]) \otimes_{\mathbb{Q}[[t]]} (\mathrm{NSym}_{\mathbb{Q}}[[t]])$ via the canonical ring homomorphism from the latter into the former [269]):

$$\begin{aligned} \Delta\xi(t) &= \Delta\left(\log \sum_{n\geq 0} H_n t^n\right) = \log \sum_{n \geq 0} \Delta(H_n) t^n = \log \sum_{n\geq 0} \left( \sum_{i+j=n} H_i \otimes H_j \right) t^n \\ &= \log\left( \left(\sum_{i\geq 0} H_i t^i\right) \otimes \left(\sum_{j \geq 0} H_j t^j\right)\right) \\ &= \log\left( \left(\sum_{i\geq 0} H_i t^i \otimes 1\right) \left(1 \otimes \sum_{j \geq 0} H_j t^j\right)\right) \\ &\overset{(5.4.5)}{=} \log \widetilde{H}(t) \otimes 1 + 1 \otimes \log \widetilde{H}(t) = \xi(t) \otimes 1 + 1 \otimes \xi(t). \end{aligned}$$

[269] This ring homomorphism might fail to be injective, whence the "embed" stands in quotation marks. This does not need to worry us, since we will not draw any conclusions in $(\mathrm{NSym}_{\mathbb{Q}}[[t]]) \otimes_{\mathbb{Q}[[t]]} (\mathrm{NSym}_{\mathbb{Q}}[[t]])$ from our computation.

We are also somewhat cavalier with the notation $\Delta$: we use it both for the comultiplication $\Delta : \mathrm{NSym}_{\mathbb{Q}} \to \mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}}$ of the Hopf algebra $\mathrm{NSym}_{\mathbb{Q}}$ and for the continuous $\mathbf{k}$-algebra homomorphism $\mathrm{NSym}_{\mathbb{Q}}[[t]] \to \left(\mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}}\right)[[t]]$ it induces.

Comparing coefficients in this equality yields $\Delta(\xi_n) = \xi_n \otimes 1 + 1 \otimes \xi_n$. Thus $S(\xi_n) = -\xi_n$, by Proposition 1.4.17. This allows one to determine $S(H_n)$ and $S(H_\alpha)$, after one first inverts the relation (5.4.6) to get that $\widetilde{H}(t) = \exp \xi(t)$, and hence

$$\begin{aligned} S(\widetilde{H}(t)) &= S(\exp \xi(t)) = \exp S(\xi(t)) = \exp\left(-\xi(t)\right) \overset{(5.4.4)}{=} \left(\exp \xi(t)\right)^{-1} \\ &= \widetilde{H}(t)^{-1} = \left(1 + H_1 t + H_2 t^2 + \cdots\right)^{-1}. \end{aligned}$$

Upon expanding the right side, and comparing coefficients of $t^n$, this gives

$$S(H_n) = \sum_{\beta \in \operatorname{Comp}_n} (-1)^{\ell(\beta)} H_\beta$$

and hence

$$\begin{aligned} S(H_\alpha) = S(H_{\alpha_\ell}) \cdots S(H_{\alpha_2}) S(H_{\alpha_1}) &= \sum_{\substack{\gamma: \\ \gamma \text{ refines } \operatorname{rev}(\alpha)}} (-1)^{\ell(\gamma)} H_\gamma \\ &= \sum_{\substack{\gamma: \\ \operatorname{rev}(\gamma) \text{ refines } \alpha}} (-1)^{\ell(\gamma)} H_\gamma \end{aligned}$$

(because if $\mu$ and $\nu$ are two compositions, then $\mu$ refines $\nu$ if and only if $\operatorname{rev}(\mu)$ refines $\operatorname{rev}(\nu)$). As $S_{\mathrm{NSym}}, S_{\mathrm{QSym}}$ are adjoint, and $\{H_\alpha\}, \{M_\alpha\}$ are dual bases, this is equivalent to saying that

$$S(M_\alpha) = (-1)^{\ell(\alpha)} \sum_{\substack{\gamma: \\ \operatorname{rev}(\alpha) \text{ refines } \gamma}} M_\gamma \qquad \text{for all } \alpha \in \operatorname{Comp}.$$

But this is precisely the claim of Theorem 5.1.11. Thus, Theorem 5.1.11 is proven once again.

Let us say a bit more about the elements $\xi_n$ defined in (5.4.6) above. The elements $n\xi_n$ are noncommutative analogues of the power sum symmetric functions $p_n$ (and, indeed, are lifts of the latter to NSym, as Exercise 5.4.5 below shows). They are called the *noncommutative power sums of the second kind* in [77][270], and their products form a basis of NSym. They are furthermore useful in studying the so-called *Eulerian idempotent* of a cocommutative Hopf algebra, as shown in Exercise 5.4.6 below.

**Exercise 5.4.5.** Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Define a sequence of elements $\xi_1, \xi_2, \xi_3, \ldots$ of $\mathrm{NSym} = \mathrm{NSym}_{\mathbf{k}}$ by (5.4.6).

(a) For every $n \geq 1$, show that $\xi_n$ is a primitive homogeneous element of NSym of degree $n$.

(b) For every $n \geq 1$, show that $\pi(n\xi_n)$ is the $n$-th power sum symmetric function $p_n \in \Lambda$.

(c) For every $n \geq 1$, show that

$$\xi_n = \sum_{\alpha \in \operatorname{Comp}_n} (-1)^{\ell(\alpha)-1} \frac{1}{\ell(\alpha)} H_\alpha. \tag{5.4.7}$$

(d) For every composition $\alpha$, define an element $\xi_\alpha$ of NSym by $\xi_\alpha = \xi_{\alpha_1}\xi_{\alpha_2}\cdots\xi_{\alpha_\ell}$, where $\alpha$ is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$

[270] See Exercise 5.4.12 for the ones of the first kind.

with $\ell = \ell(\alpha)$. Show that

$$H_n = \sum_{\alpha \in \mathrm{Comp}_n} \frac{1}{\ell(\alpha)!} \xi_\alpha \tag{5.4.8}$$

for every $n \in \mathbb{N}$.

Use this to prove that $(\xi_\alpha)_{\alpha \in \mathrm{Comp}_n}$ is a $\mathbf{k}$-basis of $\mathrm{NSym}_n$ for every $n \in \mathbb{N}$.

**Exercise 5.4.6.** Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $A$ be a cocommutative connected graded $\mathbf{k}$-bialgebra. Let $A = \bigoplus_{n \geq 0} A_n$ be the decomposition of $A$ into homogeneous components. If $f$ is any $\mathbf{k}$-linear map $A \to A$ annihilating $A_0$, then $f$ is locally $\star$-nilpotent[271], and so the sum $\log^\star(f + u\epsilon) := \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}$ is a well-defined endomorphism of $A$ [272]. Let $\mathfrak{e}$ denote the endomorphism $\log^\star(\mathrm{id}_A)$ of $A$ (obtained by setting $f = \mathrm{id}_A - u\epsilon : A \to A$). Show that $\mathfrak{e}$ is a projection from $A$ to the $\mathbf{k}$-submodule $\mathfrak{p}$ of all primitive elements of $A$ (and thus, in particular, is idempotent).

**Hint:** For every $n \geq 0$, let $\pi_n : A \to A$ be the projection onto the $n$-th homogeneous component $A_n$. Since NSym is the free $\mathbf{k}$-algebra with generators $H_1, H_2, H_3, \ldots$, we can define a $\mathbf{k}$-algebra homomorphism $\mathfrak{W} : \mathrm{NSym} \to (\mathrm{End}\, A, \star)$ by sending $H_n$ to $\pi_n$. Show that:

(a) The map $\mathfrak{e} : A \to A$ is graded. For every $n \geq 0$, we will denote the map $\pi_n \circ \mathfrak{e} = \mathfrak{e} \circ \pi_n : A \to A$ by $\mathfrak{e}_n$.

(b) We have $\mathfrak{W}(\xi_n) = \mathfrak{e}_n$ for all $n \geq 1$, where $\xi_n$ is defined as in Exercise 5.4.5.

(c) If $w$ is an element of NSym, and if we write $\Delta(w) = \sum_{(w)} w_1 \otimes w_2$ using the Sweedler notation, then

$$\Delta \circ (\mathfrak{W}(w)) = \left( \sum_{(w)} \mathfrak{W}(w_1) \otimes \mathfrak{W}(w_2) \right) \circ \Delta.$$

(d) We have $\mathfrak{e}_n(A) \subset \mathfrak{p}$ for every $n \geq 0$.

(e) We have $\mathfrak{e}(A) \subset \mathfrak{p}$.

(f) The map $\mathfrak{e}$ fixes any element of $\mathfrak{p}$.

*Remark* 5.4.7. The endomorphism $\mathfrak{e}$ of Exercise 5.4.6 is known as the *Eulerian idempotent* of $A$, and can be contrasted with the Dynkin idempotent of Remark 1.5.15. It has been studied in [166], [169], [31] and [60], and relates to the Hochschild cohomology of commutative algebras [134, §4.5.2].

[271] See the proof of Proposition 1.4.24 for what this means.

[272] This definition of $\log^\star(f + u\epsilon)$ is actually a particular case of Definition 1.7.17. This can be seen as follows:

We have $f(A_0) = 0$. Thus, Proposition 1.7.11(h) (applied to $C = A$) yields $f \in \mathfrak{n}(A, A)$ (where $\mathfrak{n}(A, A)$ is defined as in Section 1.7), so that $(f + u\epsilon) - u\epsilon = f \in \mathfrak{n}(A, A)$. Therefore, Definition 1.7.17 defines a map $\log^\star(f + u\epsilon) \in \mathfrak{n}(A, A)$. This map is identical to the map $\log^\star(f + u\epsilon) := \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}$ we have just defined, because Proposition 1.7.18(f) (applied to $C = A$) shows that the map $\log^\star(f + u\epsilon)$ defined using Definition 1.7.17 satisfies

$$\log^\star(f + u\epsilon) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} f^{\star n} = \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}.$$

**Exercise 5.4.8.** Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $A$, $A_n$ and $\mathfrak{e}$ be as in Exercise 5.4.6.

(a) Show that $\mathfrak{e}^{\star n} \circ \mathfrak{e}^{\star m} = n!\delta_{n,m}\mathfrak{e}^{\star n}$ for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$.
(b) Show that $\mathfrak{e}^{\star n} \circ \operatorname{id}_A^{\star m} = \operatorname{id}_A^{\star m} \circ \mathfrak{e}^{\star n} = m^n \mathfrak{e}^{\star n}$ for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

We next explore the basis for NSym dual to the $\{L_\alpha\}$ in QSym.

**Definition 5.4.9.** Define the *noncommutative ribbon functions* $\{R_\alpha\}_{\alpha \in \mathrm{Comp}}$ to be the $\mathbf{k}$-basis of NSym dual to the fundamental basis $\{L_\alpha\}_{\alpha\in\mathrm{Comp}}$ of QSym, so that

$$(R_\alpha, L_\beta) = \delta_{\alpha,\beta} \qquad \text{for all } \alpha, \beta \in \mathrm{Comp}.$$

**Theorem 5.4.10.** (a) *One has that*

$$H_\alpha = \sum_{\beta \text{ coarsens } \alpha} R_\beta; \tag{5.4.9}$$

$$R_\alpha = \sum_{\beta \text{ coarsens } \alpha} (-1)^{\ell(\beta)-\ell(\alpha)} H_\beta. \tag{5.4.10}$$

(b) *The surjection* NSym $\xrightarrow{\pi} \Lambda$ *sends* $R_\alpha \longmapsto s_{\mathrm{Rib}(\alpha)}$, *the skew Schur function associated to the ribbon* $\mathrm{Rib}\,(\alpha)$.
(c) *Furthermore,*

$$R_\alpha R_\beta = R_{\alpha\cdot\beta} + R_{\alpha\odot\beta} \qquad \text{if } \alpha \text{ and } \beta \text{ are nonempty}; \tag{5.4.11}$$

$$S(R_\alpha) = (-1)^{|\alpha|} R_{\omega(\alpha)}. \tag{5.4.12}$$

*Finally,* $R_\varnothing$ *is the multiplicative identity of* NSym.

*Proof.* (a) For (5.4.9), note that

$$H_\alpha = \sum_\beta (H_\alpha, L_\beta) R_\beta = \sum_\beta \left( H_\alpha, \sum_{\substack{\gamma: \\ \gamma \text{ refines } \beta}} M_\gamma \right) R_\beta = \sum_{\substack{\beta: \\ \beta \text{ coarsens } \alpha}} R_\beta.$$

The equality (5.4.10) follows from (5.4.9) by Lemma 5.2.7(a).

(b) Write $\alpha$ as $(\alpha_1, \ldots, \alpha_\ell)$. To show that $\pi(R_\alpha) = s_{\mathrm{Rib}(\alpha)}$, we instead examine $\pi(H_\alpha)$:

$$\pi(H_\alpha) = \pi(H_{\alpha_1} \cdots H_{\alpha_\ell}) = h_{\alpha_1} \cdots h_{\alpha_\ell} = s_{(\alpha_1)} \cdots s_{(\alpha_\ell)} = s_{(\alpha_1)\oplus\cdots\oplus(\alpha_\ell)}$$

where $(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$ is some skew shape which is a horizontal strip having rows of lengths $\alpha_1, \ldots, \alpha_\ell$ from bottom to top. We claim

$$s_{(\alpha_1)\oplus\cdots\oplus(\alpha_\ell)} = \sum_{\substack{\beta: \\ \beta \text{ coarsens } \alpha}} s_{\mathrm{Rib}(\beta)},$$

because column-strict tableaux $T$ of shape $(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$ biject to column-strict tableaux $T'$ of some ribbon $\mathrm{Rib}\,(\beta)$ with $\beta$ coarsening $\alpha$, as follows: Let $a_i, b_i$ denote the leftmost, rightmost entries of the $i$-th row from the bottom in $T$, of length $\alpha_i$, and

- if $b_i \leq a_{i+1}$, merge parts $\alpha_i, \alpha_{i+1}$ in $\beta$, and concatenate the rows of length $\alpha_i, \alpha_{i+1}$ in $T'$, or
- if $b_i > a_{i+1}$, do not merge parts $\alpha_i, \alpha_{i+1}$ in $\beta$, and let these two rows overlap in one column in $T'$.

E.g., if $\alpha = (3,3,2,3,2)$, then the tableau

$$T = \begin{array}{ccccccccccccc} &&&&&&&&&&&3&4\\ &&&&&&&&&4&4&5&\\ &&&&&&&4&4&&&&\\ &&&&2&2&3&&&&&&\\ 1&1&3&&&&&&&&&& \end{array}$$

of shape $(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$ maps to the tableau

$$T' = \begin{array}{ccccccccccc} &&&&&&&&&3&4\\ &&2&2&3&4&4&4&4&5&\\ 1&1&3&&&&&&&& \end{array}$$

of shape Rib$\,(\beta)$ for $\beta = (3,8,2)$.

The reverse bijection breaks the rows of $T'$ into the rows of $T$ of lengths dictated by the parts of $\alpha$. Having shown $\pi(H_\alpha) = \sum_{\beta:\beta \text{ coarsens } \alpha} s_{\mathrm{Rib}(\beta)}$, we can now apply Lemma 5.2.7(a) to obtain

$$s_{\mathrm{Rib}(\alpha)} = \sum_{\beta:\beta \text{ coarsens } \alpha} (-1)^{\ell(\alpha)-\ell(\beta)} \pi(H_\beta) = \pi(R_\alpha) \qquad \text{(by (5.4.10))};$$

thus, $\pi(R_\alpha) = s_{\mathrm{Rib}(\alpha)}$ is proven.

(c) Finally, (5.4.11) and (5.4.12) follow from (5.2.5) and (5.2.7) by duality. □

*Remark* 5.4.11. Since the maps

$$\begin{tikzcd} \mathrm{NSym} \arrow[dr, "\pi"'] & & \mathrm{QSym} \\ & \Lambda \arrow[ur, hook, "i"'] & \end{tikzcd}$$

are Hopf morphisms, they must respect the antipodes $S_\Lambda, S_{\mathrm{QSym}}, S_{\mathrm{NSym}}$, but it is interesting to compare them explicitly using the fundamental basis for QSym and the ribbon basis for NSym.

On one hand (5.2.7) shows that $S_{\mathrm{QSym}}(L_\alpha) = (-1)^{|\alpha|} L_{\omega(\alpha)}$ extends the map $S_\Lambda$ since $L_{(1^n)} = e_n$ and $L_{(n)} = h_n$, as observed in Example 5.2.5, and $\omega((n)) = (1^n)$.

On the other hand, (5.4.12) shows that $S_{\mathrm{NSym}}(R_\alpha) = (-1)^{|\alpha|} R_{\omega(\alpha)}$ lifts the map $S_\Lambda$ to $S_{\mathrm{NSym}}$: Theorem 5.4.10(b) showed that $R_\alpha$ lifts the skew Schur function $s_{\mathrm{Rib}(\alpha)}$, while (2.4.15) asserted that $S(s_{\lambda/\mu}) = (-1)^{|\lambda/\mu|} s_{\lambda^t/\mu^t}$, and a ribbon Rib$\,(\alpha) = \lambda/\mu$ has Rib$\,(\omega(\alpha)) = \lambda^t/\mu^t$.

**Exercise 5.4.12.** (a) Show that any integers $n$ and $i$ with $0 \leq i < n$ satisfy

$$R_{(1^i,n-i)} = \sum_{j=0}^{i} (-1)^{i-j} R_{(1^j)} H_{n-j}.$$

(Here, as usual, $1^i$ stands for the number 1 repeated $i$ times.)

(b) Show that any integers $n$ and $i$ with $0 \leq i < n$ satisfy

$$(-1)^i R_{(1^i,n-i)} = \sum_{j=0}^{i} S(H_j) H_{n-j}.$$

(c) For every positive integer $n$, define an element $\Psi_n$ of NSym by
$$\Psi_n = \sum_{i=0}^{n-1} (-1)^i R_{(1^i, n-i)}.$$
Show that $\Psi_n = (S \star E)(H_n)$, where the map $E : \mathrm{NSym} \to \mathrm{NSym}$ is defined as in Exercise 1.5.14 (for $A = \mathrm{NSym}$). Conclude that $\Psi_n$ is primitive.

(d) Prove that
$$\sum_{k=0}^{n-1} H_k \Psi_{n-k} = n H_n$$
for every $n \in \mathbb{N}$.

(e) Define two power series $\psi(t)$ and $\widetilde{H}(t)$ in $\mathrm{NSym}[[t]]$ by
$$\psi(t) = \sum_{n \geq 1} \Psi_n t^{n-1};$$
$$\widetilde{H}(t) = \sum_{n \geq 0} H_n t^n.$$
Show that[273] $\dfrac{d}{dt} \widetilde{H}(t) = \widetilde{H}(t) \cdot \psi(t)$.

(The functions $\Psi_n$ are called *noncommutative power sums of the first kind*; they are studied in [77]. The power sums of the second kind are the $n\xi_n$ in Remark 5.4.4.)

(f) Show that $\pi(\Psi_n)$ equals the power sum symmetric function $p_n$ for every positive integer $n$.

(g) Show that every positive integer $n$ satisfies
$$p_n = \sum_{i=0}^{n-1} (-1)^i s_{(n-i, 1^i)} \qquad \text{in } \Lambda.$$

(h) For every nonempty composition $\alpha$, define a positive integer $\mathrm{lp}(\alpha)$ by $\mathrm{lp}(\alpha) = \alpha_\ell$, where $\alpha$ is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$. (Thus, $\mathrm{lp}(\alpha)$ is the last part of $\alpha$.)

Show that every positive integer $n$ satisfies
$$\Psi_n = \sum_{\alpha \in \mathrm{Comp}_n} (-1)^{\ell(\alpha)-1} \mathrm{lp}(\alpha) H_\alpha. \tag{5.4.13}$$

(i) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$.

For every composition $\alpha$, define an element $\Psi_\alpha$ of NSym by $\Psi_\alpha = \Psi_{\alpha_1} \Psi_{\alpha_2} \cdots \Psi_{\alpha_\ell}$, where $\alpha$ is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$.

For every composition $\alpha$, define $\pi_u(\alpha)$ to be the positive integer $\alpha_1(\alpha_1 + \alpha_2) \cdots (\alpha_1 + \alpha_2 + \cdots + \alpha_\ell)$, where $\alpha$ is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$.

Show that
$$H_n = \sum_{\alpha \in \mathrm{Comp}_n} \frac{1}{\pi_u(\alpha)} \Psi_\alpha \tag{5.4.14}$$

[273] The derivative $\frac{d}{dt} Q(t)$ of a power series $Q(t) \in R[[t]]$ over a noncommutative ring $R$ is defined just as in the case of $R$ commutative: by setting $\frac{d}{dt} Q(t) = \sum_{i \geq 1} i q_i t^{i-1}$, where $Q(t)$ is written in the form $Q(t) = \sum_{i \geq 0} q_i t^i$.

for every $n \in \mathbb{N}$.

Use this to prove that $(\Psi_\alpha)_{\alpha \in \mathrm{Comp}_n}$ is a $\mathbf{k}$-basis of $\mathrm{NSym}_n$ for every $n \in \mathbb{N}$.

(j) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $V$ be the free $\mathbf{k}$-module with basis $(\mathfrak{b}_n)_{n \in \{1,2,3,\ldots\}}$. Define a $\mathbf{k}$-module homomorphism $f : V \to \mathrm{NSym}$ by requiring that $f(\mathfrak{b}_n) = \Psi_n$ for every $n \in \{1,2,3,\ldots\}$. Let $F$ be the $\mathbf{k}$-algebra homomorphism $T(V) \to \mathrm{NSym}$ induced by this $f$ (using the universal property of the tensor algebra $T(V)$). Show that $F$ is a Hopf algebra isomorphism (where the Hopf algebra structure on $T(V)$ is as in Example 1.4.18).

(k) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $V$ be as in Exercise 5.4.12(j). Show that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ (defined as in Proposition 1.6.7) as Hopf algebras.

(l) Solve parts (a) and (b) of Exercise 2.9.14 again using the ribbon basis functions $R_\alpha$.

One might wonder whether the Frobenius endomorphisms of $\Lambda$ (defined in Exercise 2.9.9) and the Verschiebung endomorphisms of $\Lambda$ (defined in Exercise 2.9.10) generalize to analogous operators on either QSym or NSym. The next two exercises (whose claims mostly come from [90, §13]) answer this question: The Frobenius endomorphisms extend to QSym, and the Verschiebung ones lift to NSym.

**Exercise 5.4.13.** For every $n \in \{1,2,3,\ldots\}$, define a map $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ by setting

$$\mathbf{F}_n(a) = a(x_1^n, x_2^n, x_3^n, \ldots) \qquad \text{for every } a \in \mathrm{QSym}.$$

(So what $\mathbf{F}_n$ does to a quasi-symmetric function is replacing all variables $x_1, x_2, x_3, \ldots$ by their $n$-th powers.)

(a) Show that $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ is a $\mathbf{k}$-algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.

(b) Show that $\mathbf{F}_n \circ \mathbf{F}_m = \mathbf{F}_{nm}$ for any two positive integers $n$ and $m$.

(c) Show that $\mathbf{F}_1 = \mathrm{id}$.

(d) Prove that $\mathbf{F}_n\left(M_{(\beta_1,\beta_2,\ldots,\beta_s)}\right) = M_{(n\beta_1,n\beta_2,\ldots,n\beta_s)}$ for every $n \in \{1,2,3,\ldots\}$ and $(\beta_1,\beta_2,\ldots,\beta_s) \in \mathrm{Comp}$.

(e) Prove that $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ is a Hopf algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.

(f) Consider the maps $\mathbf{f}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.9. Show that $\mathbf{F}_n \mid_\Lambda = \mathbf{f}_n$ for every $n \in \{1,2,3,\ldots\}$.

(g) Assume that $\mathbf{k} = \mathbb{Z}$. Prove that $\mathbf{f}_p(a) \equiv a^p \bmod p\,\mathrm{QSym}$ for every $a \in \mathrm{QSym}$ and every prime number $p$.

(h) Give a new solution to Exercise 2.9.9(d).

**Exercise 5.4.14.** For every $n \in \{1,2,3,\ldots\}$, define a $\mathbf{k}$-algebra homomorphism $\mathbf{V}_n : \mathrm{NSym} \to \mathrm{NSym}$ by

$$\mathbf{V}_n(H_m) = \begin{cases} H_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases} \qquad \text{for every positive integer } m$$

[274].

[274] This is well-defined, since NSym is (isomorphic to) the free associative algebra with generators $H_1, H_2, H_3, \ldots$ (according to (5.4.1)).

(a) Show that any positive integers $n$ and $m$ satisfy

$$\mathbf{V}_n \left(\Psi_m\right) = \begin{cases} n\Psi_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases},$$

where the elements $\Psi_m$ and $\Psi_{m/n}$ of NSym are as defined in Exercise 5.4.12(c).

(b) Show that if $\mathbb{Q}$ is a subring of $\mathbf{k}$, then any positive integers $n$ and $m$ satisfy

$$\mathbf{V}_n \left(\xi_m\right) = \begin{cases} \xi_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases},$$

where the elements $\xi_m$ and $\xi_{m/n}$ of NSym are as defined in Exercise 5.4.5.

(c) Prove that $\mathbf{V}_n \circ \mathbf{V}_m = \mathbf{V}_{nm}$ for any two positive integers $n$ and $m$.

(d) Prove that $\mathbf{V}_1 = \operatorname{id}$.

(e) Prove that $\mathbf{V}_n : \operatorname{NSym} \to \operatorname{NSym}$ is a Hopf algebra homomorphism for every $n \in \{1, 2, 3, \ldots\}$.

Now, consider also the maps $\mathbf{F}_n : \operatorname{QSym} \to \operatorname{QSym}$ defined in Exercise 2.9.9. Fix a positive integer $n$.

(f) Prove that the maps $\mathbf{F}_n : \operatorname{QSym} \to \operatorname{QSym}$ and $\mathbf{V}_n : \operatorname{NSym} \to \operatorname{NSym}$ are adjoint with respect to the dual pairing $\operatorname{NSym} \otimes \operatorname{QSym} \xrightarrow{(\cdot,\cdot)} \mathbf{k}$.

(g) Consider the maps $\mathbf{v}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.10. Show that the surjection $\pi : \operatorname{NSym} \to \Lambda$ satisfies $\mathbf{v}_n \circ \pi = \pi \circ \mathbf{V}_n$ for every $n \in \{1, 2, 3, \ldots\}$.

(h) Give a new solution to Exercise 2.9.10(f).

# 6. Polynomial generators for QSym and Lyndon words

In this chapter, we shall construct an algebraically independent generating set for QSym as a $\mathbf{k}$-algebra, thus showing that QSym is a polynomial ring over $\mathbf{k}$. This has been done by Malvenuto [145, Cor. 4.19] when $\mathbf{k}$ is a field of characteristic 0, and by Hazewinkel [89] in the general case. We will begin by introducing the notion of *Lyndon words* (Section 6.1), on which both of these constructions rely; we will then (Section 6.2) elucidate the connection of Lyndon words with shuffles, and afterwards (Section 6.3) apply it to prove *Radford's theorem* stating that the shuffle algebra of a free $\mathbf{k}$-module over a commutative $\mathbb{Q}$-algebra is a polynomial algebra (Theorem 6.3.4). The shuffle algebra is not yet QSym, but Radford's theorem on the shuffle algebra serves as a natural stepping stone for the study of the more complicated algebra QSym. We will prove – in two ways – that QSym is a polynomial algebra when $\mathbb{Q}$ is a subring of $\mathbf{k}$ in Section 6.4, and then we will finally prove the general case in Section 6.5. In Section 6.6, we will explore a different aspect of the combinatorics of words: the notion of necklaces (which are in bijection with Lyndon words, as Exercise 6.1.34 will show) and the *Gessel-Reutenauer bijection*, which help us define and understand the *Gessel-Reutenauer symmetric functions*. This will rely on Section 6.1, but not on any of the other sections of Chapter 6.

Strictly speaking, this whole Chapter 6 is a digression, as it involves almost no coalgebraic or Hopf-algebraic structures, and its results will not be used in further chapters (which means it can be skipped if so desired). However, it sheds additional light on both quasisymmetric and symmetric functions, and serves as an excuse to study Lyndon words, which are a combinatorial object of independent interest (and are involved in the study of free algebras and Hopf algebras, apart from QSym – see [177] and [182][275]).

We will take a scenic route to the proof of Hazewinkel's theorem. A reader only interested in the proof proper can restrict themselves to reading only the following:

- from Section 6.1, everything up to Corollary 6.1.6, then from Definition 6.1.13 up to Proposition 6.1.18, then from Definition 6.1.25 up to Lemma 6.1.28, and finally Theorem 6.1.30. (Proposition 6.1.19 and Theorem 6.1.20 are also relevant if one wants to use a different definition of Lyndon words, as they prove the equivalence of most such definitions.)
- from Section 6.2, everything except for Exercise 6.2.25.
- from Section 6.3, Definition 6.3.1, Lemma 6.3.7, and Lemma 6.3.10.
- from Section 6.4, Definition 6.4.1, Theorem 6.4.3, then from Proposition 6.4.5 up to Definition 6.4.9, and Lemma 6.4.11.
- all of Section 6.5.

Likewise, Section 6.6 can be read immediately after Section 6.1.

## 6.1. **Lyndon words.**

Lyndon words have been independently defined by Shirshov [202], Lyndon [141], Radford [177, §2] and de Bruijn/Klarner [29] (though using different and sometimes incompatible notations). They have

[275] They also are involved in indexing basis elements of combinatorial Hopf algebras other than QSym. See Bergeron/Zabrocki [18].

since been surfacing in various places in noncommutative algebra (particularly the study of free Lie algebras); expositions of their theory can be found in [139, §5], [182, §5.1] and [124, §1] (in German). We will follow our own approach to the properties of Lyndon words that we need.

**Definition 6.1.1.** We fix a totally ordered set $\mathfrak{A}$, which we call the *alphabet*. Throughout Section 6.1 and Section 6.2, we will understand "word" to mean a word over $\mathfrak{A}$.

We recall that a *word* is just a (finite) tuple of elements of $\mathfrak{A}$. In other words, a word is an element of the set $\bigsqcup_{n\geq 0} \mathfrak{A}^n$. We denote this set by $\mathfrak{A}^*$.

The *empty word* is the unique tuple with 0 elements. It is denoted by $\varnothing$. If $w \in \mathfrak{A}^n$ is a word and $i \in \{1, 2, \ldots, n\}$, then the *i-th letter* of $w$ means the $i$-th entry of the $n$-tuple $w$. This $i$-th letter will be denoted by $w_i$.

The *length* $\ell(w)$ of a word $w \in \bigsqcup_{n\geq 0} \mathfrak{A}^n$ is defined to be the $n \in \mathbb{N}$ satisfying $w \in \mathfrak{A}^n$. Thus, $w = \left(w_1, w_2, \ldots, w_{\ell(w)}\right)$ for every word $w$.

Given two words $u$ and $v$, we say that $u$ is *longer* than $v$ (or, equivalently, $v$ is *shorter* than $u$) if and only if $\ell(u) > \ell(v)$.

The *concatenation* of two words $u$ and $v$ is defined to be the word $\left(u_1, u_2, \ldots, u_{\ell(u)}, v_1, v_2, \ldots, v_{\ell(v)}\right)$. This concatenation is denoted by $uv$ or $u \cdot v$. The set $\mathfrak{A}^*$ of all words is a monoid with respect to concatenation, with neutral element $\varnothing$. It is precisely the free monoid on generators $\mathfrak{A}$. If $u$ is a word and $i \in \mathbb{N}$, we will understand $u^i$ to mean the $i$-th power of $u$ in this monoid (that is, the word $\underbrace{uu \cdots u}_{i \text{ times}}$).

The elements of $\mathfrak{A}$ are called *letters*, and will be identified with elements of $\mathfrak{A}^1 \subset \bigsqcup_{n\geq 0} \mathfrak{A}^n = \mathfrak{A}^*$. This identification equates every letter $u \in \mathfrak{A}$ with the one-letter word $(u) \in \mathfrak{A}^1$. Thus, every word $(u_1, u_2, \ldots, u_n) \in \mathfrak{A}^*$ equals the concatenation $u_1 u_2 \cdots u_n$ of letters, hence allowing us to use $u_1 u_2 \cdots u_n$ as a brief notation for the word $(u_1, u_2, \ldots, u_n)$.

If $w$ is a word, then:

- a *prefix* of $w$ means a word of the form $(w_1, w_2, \ldots, w_i)$ for some $i \in \{0, 1, \ldots, \ell(w)\}$;
- a *suffix* of $w$ means a word of the form $\left(w_{i+1}, w_{i+2}, \ldots, w_{\ell(w)}\right)$ for some $i \in \{0, 1, \ldots, \ell(w)\}$;
- a *proper suffix* of $w$ means a word of the form $\left(w_{i+1}, w_{i+2}, \ldots, w_{\ell(w)}\right)$ for some $i \in \{1, 2, \ldots, \ell(w)\}$.

In other words,

- a *prefix* of $w \in \mathfrak{A}^*$ is a word $u \in \mathfrak{A}^*$ such that there exists a $v \in \mathfrak{A}^*$ satisfying $w = uv$;
- a *suffix* of $w \in \mathfrak{A}^*$ is a word $v \in \mathfrak{A}^*$ such that there exists a $u \in \mathfrak{A}^*$ satisfying $w = uv$;
- a *proper suffix* of $w \in \mathfrak{A}^*$ is a word $v \in \mathfrak{A}^*$ such that there exists a nonempty $u \in \mathfrak{A}^*$ satisfying $w = uv$.

Clearly, any proper suffix of $w \in \mathfrak{A}^*$ is a suffix of $w$. Moreover, if $w \in \mathfrak{A}^*$ is any word, then a proper suffix of $w$ is the same thing as a suffix of $w$ distinct from $w$.

We define a relation $\leq$ on the set $\mathfrak{A}^*$ as follows: For two words $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$, we set $u \leq v$ to hold if and only if

**either** there exists an $i \in \{1, 2, \ldots, \min\{\ell(u), \ell(v)\}\}$
such that $(u_i < v_i$, and every $j \in \{1, 2, \ldots, i-1\}$ satisfies $u_j = v_j)$,

**or** the word $u$ is a prefix of $v$.

This order relation (taken as the smaller-or-equal relation) makes $\mathfrak{A}^*$ into a poset (by Proposition 6.1.2(a) below), and we will always be regarding $\mathfrak{A}^*$ as endowed with this poset structure (thus, notations such as $<$, $\leq$, $>$ and $\geq$ will be referring to this poset structure). This poset is actually totally ordered (see Proposition 6.1.2(a)).

Here are some examples of words compared by the relation $\leq$:

$$113 \leq 114, \qquad 113 \leq 132, \qquad 19 \leq 195, \qquad 41 \leq 412,$$
$$41 \leq 421, \qquad 539 \leq 54, \qquad \varnothing \leq 21, \qquad \varnothing \leq \varnothing$$

(where $\mathfrak{A}$ is the alphabet $\{1 < 2 < 3 < \cdots\}$).

Notice that if $u$ and $v$ are two words of the same length (i.e., we have $u, v \in \mathfrak{A}^n$ for one and the same $n$), then $u \leq v$ holds if and only if $u$ is lexicographically smaller-or-equal to $v$. In other words, the relation $\leq$ is an extension of the lexicographic order on every $\mathfrak{A}^n$ to $\mathfrak{A}^*$. This is the reason why this relation $\leq$ is usually called the *lexicographic order* on $\mathfrak{A}^*$. In particular, we will be using this name.[276] However, unlike the lexicographic order on $\mathfrak{A}^n$, it does not always respect concatenation from the right: It can happen that $u, v, w \in \mathfrak{A}^*$ satisfy $u \leq v$ but not $uw \leq vw$. (For example, $u = 1$, $v = 13$ and $w = 4$, again with $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$.) We will see in Proposition 6.1.2 that this is rather an exception than the rule and the relation $\leq$ still behaves mostly predictably with respect to concatenation.

Some basic properties of the order relation $\leq$ just defined are collected in the following proposition:

**Proposition 6.1.2.** (a) *The order relation $\leq$ is (the smaller-or-equal relation of) a total order on the set $\mathfrak{A}^*$.*

(b) *If $a, c, d \in \mathfrak{A}^*$ satisfy $c \leq d$, then $ac \leq ad$.*
(c) *If $a, c, d \in \mathfrak{A}^*$ satisfy $ac \leq ad$, then $c \leq d$.*
(d) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $a \leq c$, then either we have $ab \leq cd$ or the word $a$ is a prefix of $c$.*
(e) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $ab \leq cd$, then either we have $a \leq c$ or the word $c$ is a prefix of $a$.*
(f) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $ab \leq cd$ and $\ell(a) \leq \ell(c)$, then $a \leq c$.*
(g) *If $a, b, c \in \mathfrak{A}^*$ satisfy $a \leq b \leq ac$, then $a$ is a prefix of $b$.*
(h) *If $a \in \mathfrak{A}^*$ is a prefix of $b \in \mathfrak{A}^*$, then $a \leq b$.*
(i) *If $a$ and $b$ are two prefixes of $c \in \mathfrak{A}^*$, then either $a$ is a prefix of $b$, or $b$ is a prefix of $a$.*
(j) *If $a, b, c \in \mathfrak{A}^*$ are such that $a \leq b$ and $\ell(a) \geq \ell(b)$, then $ac \leq bc$.*
(k) *If $a \in \mathfrak{A}^*$ and $b \in \mathfrak{A}^*$ are such that $b$ is nonempty, then $a < ab$.*

**Exercise 6.1.3.** Prove Proposition 6.1.2.

[276] The relation $\leq$ is also known as the *dictionary order*, due to the fact that it is the order in which words appear in a dictionary.

[**Hint:** No part of Proposition 6.1.2 requires more than straightforward case analysis. However, the proof of (a) can be simplified by identifying the order relation $\leq$ on $\mathfrak{A}^*$ as a restriction of the lexicographic order on the set $\mathfrak{B}^\infty$, where $\mathfrak{B}$ is a suitable extension of the alphabet $\mathfrak{A}$. What is this extension, and how to embed $\mathfrak{A}^*$ into $\mathfrak{B}^\infty$ ?]

Proposition 6.1.2 provides a set of tools for working with the lexicographic order without having to refer to its definition; we shall use it extensively. Proposition 6.1.2(h) (and its equivalent form stating that $a \leq ac$ for every $a \in \mathfrak{A}^*$ and $c \in \mathfrak{A}^*$) and Proposition 6.1.2(k) will often be used without explicit mention.

Before we define Lyndon words, let us show two more facts about words which will be used later. First, when do words commute?

**Proposition 6.1.4.** *Let $u, v \in \mathfrak{A}^*$ satisfy $uv = vu$. Then, there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers $n$ and $m$ such that $u = t^n$ and $v = t^m$.*

*Proof.* We prove this by strong induction on $\ell(u)+\ell(v)$. We assume WLOG that $\ell(u)$ and $\ell(v)$ are positive (because otherwise, one of $u$ and $v$ is the empty word, and everything is trivial). It is easy to see that either $u$ is a prefix of $v$, or $v$ is a prefix of $u$ [277]. We assume WLOG that $u$ is a prefix of $v$ (since our situation is symmetric). Thus, we can write $v$ in the form $v = uw$ for some $w \in \mathfrak{A}^*$. Consider this $w$. Clearly, $\ell(u) + \ell(w) = \ell\left(\underbrace{uw}_{=v}\right) = \ell(v) < \ell(u) + \ell(v)$ (since $\ell(v)$ is positive). Since $v = uw$, the equality $uv = vu$ becomes $uuw = uwu$. Cancelling $u$ from this equality, we obtain $uw = wu$. Now, we can apply Proposition 6.1.4 to $w$ instead of $v$ (by the induction assumption, since $\ell(u)+\ell(w) < \ell(u)+\ell(v)$), and obtain that there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers $n$ and $m$ such that $u = t^n$ and $w = t^m$. Consider this $t$ and these $n$ and $m$. Of course, $u = t^n$ and $v = \underbrace{u}_{=t^n}\underbrace{w}_{=t^m} = t^n t^m = t^{n+m}$. So the induction step is complete, and Proposition 6.1.4 is proven. □

**Proposition 6.1.5.** *Let $u, v, w \in \mathfrak{A}^*$ be nonempty words satisfying $uv \geq vu$, $vw \geq wv$ and $wu \geq uw$. Then, there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers $n$, $m$ and $p$ such that $u = t^n$, $v = t^m$ and $w = t^p$.*

*Proof.* We prove this by strong induction on $\ell(u) + \ell(v) + \ell(w)$. Clearly, $\ell(u)$, $\ell(v)$ and $\ell(w)$ are positive (since $u$, $v$ and $w$ are nonempty). We assume WLOG that $\ell(u) = \min\{\ell(u), \ell(v), \ell(w)\}$ (because there is a cyclic symmetry in our situation). Thus, $\ell(u) \leq \ell(v)$ and $\ell(u) \leq \ell(w)$. But $vu \leq uv$. Hence, Proposition 6.1.2(e) (applied to $a = v$, $b = u$, $c = u$ and $d = v$) yields that either we have $v \leq u$ or the word $u$ is a prefix of $v$. But Proposition 6.1.2(f) (applied to $a = u$, $b = w$, $c = w$ and $d = u$) yields $u \leq w$ (since $uw \leq wu$ and $\ell(u) \leq \ell(w)$). Furthermore, $wv \leq vw$. Hence, Proposition 6.1.2(e) (applied to $a = w$, $b = v$, $c = v$ and $d = w$) yields that either we have $w \leq v$ or the word $v$ is a prefix of $w$.

[277] *Proof.* The word $u$ is a prefix of $uv$. But the word $v$ is also a prefix of $uv$ (since $uv = vu$). Hence, Proposition 6.1.2(i) (applied to $a = u$, $b = v$ and $c = uv$) yields that either $u$ is a prefix of $v$, or $v$ is a prefix of $u$, qed.

From what we have found so far, it is easy to see that $u$ is a prefix of $v$ [278]. In other words, there exists a $v' \in \mathfrak{A}^*$ such that $v = uv'$. Consider this $v'$.

If the word $v'$ is empty, then the statement of Proposition 6.1.5 can be easily deduced from Proposition 6.1.4[279]. Thus, we assume WLOG that this is not the case. Hence, $v'$ is nonempty.

Using $v = uv'$, we can rewrite $uv \geq vu$ as $uuv' \geq uv'u$. That is, $uv'u \leq uuv'$, so that $v'u \leq uv'$ (by Proposition 6.1.2(c), applied to $a = u$, $c = v'u$ and $d = uv'$). That is, $uv' \geq v'u$. But $\ell(uw) = \ell(u) + \ell(w) = \ell(w) + \ell(u) = \ell(wu) \geq \ell(wu)$. Hence, Proposition 6.1.2(i) (applied to $a = uw$, $b = wu$ and $c = v'$) yields $uwv' \leq wuv'$ (since $uw \leq wu$). Now, $\underbrace{uv'}_{=v} w = vw \geq w \underbrace{v}_{=uv'} = wuv' \geq uwv'$ (since $uwv' \leq wuv'$), so that $uwv' \leq uv'w$. Hence, $wv' \leq v'w$ (by Proposition 6.1.2(c), applied to $a = u$, $c = wv'$ and $d = v'w$), so that $v'w \geq wv'$. Now, we can apply Proposition 6.1.5 to $v'$ instead of $v$ (by the induction hypothesis, because $\underbrace{\ell(u) + \ell(v')}_{\substack{=\ell(uv')=\ell(v)\\ (\text{since } uv'=v)}} + \ell(w) = \ell(v) + \ell(w) < \ell(u) + \ell(v) + \ell(w)$). As a result, we see that there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers $n$, $m$ and $p$ such that $u = t^n$, $v' = t^m$ and $w = t^p$. Clearly, this $t$ and these $n, m, p$ satisfy $v = \underbrace{u}_{=t^n}\underbrace{v'}_{=t^m} = t^n t^m = t^{n+m}$, and so the statement of Proposition 6.1.5 is satisfied. The induction step is thus complete. □

**Corollary 6.1.6.** *Let $u, v, w \in \mathfrak{A}^*$ be words satisfying $uv \geq vu$ and $vw \geq wv$. Assume that $v$ is nonempty. Then, $uw \geq wu$.*

*Proof.* Assume the contrary. Thus, $uw < wu$, so that $wu \geq uw$.

If $u$ or $w$ is empty, then everything is obvious. We thus WLOG assume that $u$ and $w$ are nonempty. Thus, Proposition 6.1.5 shows that there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers $n$, $m$ and $p$ such that $u = t^n$, $v = t^m$ and $w = t^p$. But this yields $wu = t^p t^n = t^{p+n} = t^{n+p} = \underbrace{t^n}_{=u}\underbrace{t^p}_{=w} = uw$, contradicting $uw < wu$. This contradiction finishes the proof. □

**Exercise 6.1.7.** Find an alternative proof of Corollary 6.1.6 which does not use Proposition 6.1.5.

The above results have a curious consequence, which we are not going to use:

[278] *Proof.* Assume the contrary. Then, $u$ is not a prefix of $v$. Hence, we must have $v \leq u$ (since either we have $v \leq u$ or the word $u$ is a prefix of $v$), and in fact $v < u$ (because $v = u$ would contradict to $u$ not being a prefix of $v$). Thus, $v < u \leq w$. But recall that either we have $w \leq v$ or the word $v$ is a prefix of $w$. Thus, $v$ must be a prefix of $w$ (because $v < w$ rules out $w \leq v$). In other words, there exists a $q \in \mathfrak{A}^*$ such that $w = vq$. Consider this $q$. We have $v < u \leq w = vq$. Thus, Proposition 6.1.2(g) (applied to $a = v$, $b = u$ and $c = q$) yields that $v$ is a prefix of $u$. In light of $\ell(u) \leq \ell(v)$, this is only possible if $v = u$, but this contradicts $v < u$. This contradiction completes this proof.

[279] *Proof.* Assume that the word $v'$ is empty. Then, $v = uv'$ becomes $v = u$. Therefore, $vw \geq wv$ becomes $uw \geq wu$. Combined with $wu \geq uw$, this yields $uw = wu$. Hence, Proposition 6.1.4 (applied to $w$ instead of $v$) yields that there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers $n$ and $m$ such that $u = t^n$ and $w = t^m$. Clearly, $v = u = t^n$ as well, and so the statement of Proposition 6.1.5 is true.

**Corollary 6.1.8.** *We can define a preorder on the set $\mathfrak{A}^* \setminus \{\varnothing\}$ of all nonempty words by defining a nonempty word $u$ to be greater-or-equal to a nonempty word $v$ (with respect to this preorder) if and only if $uv \geq vu$. Two nonempty words $u, v$ are equivalent with respect to the equivalence relation induced by this preorder if and only if there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers $n$ and $m$ such that $u = t^n$ and $v = t^m$.*

*Proof.* The alleged preorder is transitive (by Corollary 6.1.6) and reflexive (obviously), and hence is really a preorder. The claim in the second sentence follows from Proposition 6.1.4. □

As another consequence of Proposition 6.1.5, we obtain a classical property of words [139, Proposition 1.3.1]:

**Exercise 6.1.9.** Let $u$ and $v$ be words and $n$ and $m$ be positive integers such that $u^n = v^m$. Prove that there exists a word $t$ and positive integers $i$ and $j$ such that $u = t^i$ and $v = t^j$.

Here is another application of Corollary 6.1.6:

**Exercise 6.1.10.** Let $n$ and $m$ be positive integers. Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words. Prove that $uv \geq vu$ holds if and only if $u^n v^m \geq v^m u^n$ holds.

**Exercise 6.1.11.** Let $n$ and $m$ be positive integers. Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words satisfying $n\ell(u) = m\ell(v)$. Prove that $uv \geq vu$ holds if and only if $u^n \geq v^m$ holds.

We can also generalize Propositions 6.1.4 and 6.1.5:

**Exercise 6.1.12.** Let $u_1, u_2, \ldots, u_k$ be nonempty words such that every $i \in \{1, 2, \ldots, k\}$ satisfies $u_i u_{i+1} \geq u_{i+1} u_i$, where $u_{k+1}$ means $u_1$. Show that there exist a word $t$ and nonnegative integers $n_1, n_2, \ldots, n_k$ such that $u_1 = t^{n_1}$, $u_2 = t^{n_2}$, …, $u_k = t^{n_k}$.

Now, we define the notion of a Lyndon word. There are several definitions in literature, some of which will be proven equivalent in Theorem 6.1.20.

**Definition 6.1.13.** A word $w \in \mathfrak{A}^*$ is said to be *Lyndon* if it is nonempty and satisfies the following property: Every nonempty proper suffix $v$ of $w$ satisfies $v > w$.

For example, the word 113 is Lyndon (because its nonempty proper suffixes are 13 and 3, and these are both $>$ 113), and the word 242427 is Lyndon (its nonempty proper suffixes are 42427, 2427, 427, 27 and 7, and again these are each $>$ 242427). The words 2424 and 35346 are not Lyndon (the word 2424 has a nonempty proper suffix 24 $\leq$ 2424, and the word 35346 has a nonempty proper suffix 346 $\leq$ 35346). Every word of length 1 is Lyndon (since it has no nonempty proper suffixes). A word $w = (w_1, w_2)$ with two letters is Lyndon if and only if $w_1 < w_2$. A word $w = (w_1, w_2, w_3)$ of length 3 is Lyndon if and only if $w_1 < w_3$ and $w_1 \leq w_2$. A four-letter word $w = (w_1, w_2, w_3, w_4)$ is Lyndon if and only if $w_1 < w_4$, $w_1 \leq w_3$, $w_1 \leq w_2$ and (if $w_1 = w_3$ then $w_2 < w_4$). (These rules only get more complicated as the words grow longer.)

We will show several properties of Lyndon words now. We begin with trivialities which will make some arguments a bit shorter:

**Proposition 6.1.14.** *Let $w$ be a Lyndon word. Let $u$ and $v$ be words such that $w = uv$.*

(a) *If $v$ is nonempty, then $v \geq w$.*
(b) *If $v$ is nonempty, then $v > u$.*
(c) *If $u$ and $v$ are nonempty, then $vu > uv$.*
(d) *We have $vu \geq uv$.*

*Proof.* (a) Assume that $v$ is nonempty. Clearly, $v$ is a suffix of $w$ (since $w = uv$). If $v$ is a proper suffix of $w$, then the definition of a Lyndon word yields that $v > w$ (since $w$ is a Lyndon word); otherwise, $v$ must be $w$ itself. In either case, we have $v \geq w$. Hence, Proposition 6.1.14(a) is proven.

(b) Assume that $v$ is nonempty. From Proposition 6.1.14(a), we obtain $v \geq w = uv > u$ (since $v$ is nonempty). This proves Proposition 6.1.14(b).

(c) Assume that $u$ and $v$ are nonempty. Since $u$ is nonempty, we have $vu > v \geq w$ (by Proposition 6.1.14(a)). Since $w = uv$, this becomes $vu > uv$. This proves Proposition 6.1.14(c).

(d) We need to prove that $vu \geq uv$. If either $u$ or $v$ is empty, $vu$ and $uv$ are obviously equal, and thus $vu \geq uv$ is true in this case. Hence, we can WLOG assume that $u$ and $v$ are nonempty. Assume this. Then, $vu \geq uv$ follows from Proposition 6.1.14(c). This proves Proposition 6.1.14(d). □

**Corollary 6.1.15.** *Let $w$ be a Lyndon word. Let $v$ be a nonempty suffix of $w$. Then, $v \geq w$.*

*Proof.* Since $v$ is a nonempty suffix of $w$, there exists $u \in \mathfrak{A}^*$ such that $w = uv$. Thus, $v \geq w$ follows from Proposition 6.1.14(a). □

Our next proposition is [93, Lemma 6.5.4]; its part (a) is also [182, (5.1.2)]:

**Proposition 6.1.16.** *Let $u$ and $v$ be two Lyndon words such that $u < v$. Then:*

(a) *The word $uv$ is Lyndon.*
(b) *We have $uv < v$.*

*Proof.* (b) The word $u$ is Lyndon and thus nonempty. Hence, $uv \neq v$ [280]. If $uv \leq v\varnothing$, then Proposition 6.1.16(b) easily follows[281]. Hence, for the rest of this proof, we can WLOG assume that we don't have $uv \leq v\varnothing$. Assume this.

We have $u < v$. Hence, Proposition 6.1.2(d) (applied to $a = u$, $b = v$, $c = v$ and $d = \varnothing$) yields that either we have $uv \leq v\varnothing$ or the word $u$ is a prefix of $v$. Since we don't have $uv \leq v\varnothing$, we thus see that the word $u$ is a prefix of $v$. In other words, there exists a $t \in \mathfrak{A}^*$ satisfying $v = ut$. Consider this $t$. Then, $t$ is nonempty (else we would have $v = u\underbrace{t}_{=\varnothing} = u$ in contradiction to $u < v$).

Now, $v = ut$. Hence, $t$ is a proper suffix of $v$ (proper because $u$ is nonempty). Thus, $t$ is a nonempty proper suffix of $v$. Since every nonempty

[280] *Proof.* Assume the contrary. Then, $uv = v$. Thus, $uv = v = \varnothing v$. Cancelling $v$ from this equation, we obtain $u = \varnothing$. That is, $u$ is empty. This contradicts the fact that $u$ is nonempty. This contradiction proves that our assumption was wrong, qed.

[281] *Proof.* Assume that $uv \leq v\varnothing$. Thus, $uv \leq v\varnothing = v$. Since $uv \neq v$, this becomes $uv < v$, so that Proposition 6.1.16(b) is proven.

proper suffix of $v$ is $> v$ (because $v$ is Lyndon), this shows that $t > v$. Hence, $v \leq t$. Thus, Proposition 6.1.2(b) (applied to $a = u$, $c = v$ and $d = t$) yields $uv \leq ut = v$. Combined with $uv \neq v$, this yields $uv < v$. Hence, Proposition 6.1.16(b) is proven.

(a) The word $v$ is nonempty (since it is Lyndon). Hence, $uv$ is nonempty. It thus remains to check that every nonempty proper suffix $p$ of $uv$ satisfies $p > uv$.

So let $p$ be a nonempty proper suffix of $uv$. We must show that $p > uv$. Since $p$ is a nonempty proper suffix of $uv$, we must be in one of the following two cases (depending on whether this suffix begins before the suffix $v$ of $uv$ begins or afterwards):

*Case 1:* The word $p$ is a nonempty suffix of $v$. (Note that $p = v$ is allowed.)

*Case 2:* The word $p$ has the form $qv$ where $q$ is a nonempty proper suffix of $u$.

Let us first handle Case 1. In this case, $p$ is a nonempty suffix of $v$. Since $v$ is Lyndon, this yields that $p \geq v$ (by Corollary 6.1.15, applied to $v$ and $p$ instead of $w$ and $v$). But Proposition 6.1.16(b) yields $uv < v$, thus $v > uv$. Hence, $p \geq v > uv$. We thus have proven $p > uv$ in Case 1.

Let us now consider Case 2. In this case, $p$ has the form $qv$ where $q$ is a nonempty proper suffix of $u$. Consider this $q$. Clearly, $q > u$ (since $u$ is Lyndon and since $q$ is a nonempty proper suffix of $u$), so that $u \leq q$. Thus, Proposition 6.1.2(d) (applied to $a = u$, $b = v$, $c = q$ and $d = v$) yields that either we have $uv \leq qv$ or the word $u$ is a prefix of $q$. Since $u$ being a prefix of $q$ is impossible (in fact, $q$ is a proper suffix of $u$, thus shorter than $u$), we thus must have $uv \leq qv$. Since $uv \neq qv$ (because otherwise we would have $uv = qv$, thus $u = q$ (because we can cancel $v$ from the equality $uv = qv$), contradicting $q > u$), this can be strengthened to $uv < qv = p$. Thus, $p > uv$ is proven in Case 2 as well.

Now that $p > uv$ is shown to hold in both cases, we conclude that $p > uv$ always holds.

Now, let us forget that we fixed $p$. We have thus shown that every nonempty proper suffix $p$ of $uv$ satisfies $p > uv$. Since $uv$ is nonempty, this yields that $uv$ is Lyndon (by the definition of a Lyndon word). Thus, the proof of Proposition 6.1.16(a) is complete. □

Proposition 6.1.16(b), combined with Corollary 6.1.6, leads to a technical result which we will find good use for later:

**Corollary 6.1.17.** *Let $u$ and $v$ be two Lyndon words such that $u < v$. Let $z$ be a word such that $zv \geq vz$ and $uz \geq zu$. Then, $z$ is the empty word.*

*Proof.* Assume the contrary. Then, $z$ is nonempty. Thus, Corollary 6.1.6 (applied to $z$ and $v$ instead of $v$ and $w$) yields $uv \geq vu$. But Proposition 6.1.16(b) yields $uv < v \leq vu$, contradicting $uv \geq vu$. This contradiction completes our proof. □

We notice that the preorder of Corollary 6.1.8 becomes particularly simple on Lyndon words:

**Proposition 6.1.18.** *Let $u$ and $v$ be two Lyndon words. Then, $u \geq v$ if and only if $uv \geq vu$.*

*Proof.* We distinguish between three cases:

*Case 1:* We have $u < v$.

*Case 2:* We have $u = v$.

*Case 3:* We have $u > v$.

Let us consider Case 1. In this case, we have $u < v$. Thus,

$$\begin{aligned} uv &< v && \text{(by Proposition 6.1.16(b))} \\ &\leq vu. \end{aligned}$$

Hence, we have neither $u \geq v$ nor $uv \geq vu$ (because we have $u < v$ and $uv < vu$). Thus, Proposition 6.1.18 is proven in Case 1.

In Case 2, we have $u = v$. Therefore, in Case 2, both inequalities $u \geq v$ and $uv \geq vu$ hold (and actually are equalities). Thus, Proposition 6.1.18 is proven in Case 2 as well.

Let us finally consider Case 3. In this case, we have $u > v$. In other words, $v < u$. Thus, Proposition 6.1.16(b) (applied to $v$ and $u$ instead of $u$ and $v$) yields $vu < u \leq uv$. Hence, we have both $u \geq v$ and $uv \geq vu$ (because we have $v < u$ and $vu < uv$). Thus, Proposition 6.1.18 is proven in Case 3.

Proposition 6.1.18 is now proven in all three possible cases. □

**Proposition 6.1.19.** *Let $w$ be a nonempty word. Let $v$ be the (lexicographically) smallest nonempty suffix of $w$. Then:*

(a) *The word $v$ is a Lyndon word.*

(b) *Assume that $w$ is not a Lyndon word. Then there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$, $u \geq v$ and $uv \geq vu$.*

*Proof.* (a) Every nonempty proper suffix of $v$ is $\geq v$ (since every nonempty proper suffix of $v$ is a nonempty suffix of $w$, but $v$ is the smallest such suffix) and therefore $> v$ (since a proper suffix of $v$ cannot be $= v$). Combined with the fact that $v$ is nonempty, this yields that $v$ is Lyndon. Proposition 6.1.19(a) is proven.

(b) Assume that $w$ is not a Lyndon word. Then, $w \neq v$ (since $v$ is Lyndon (by Proposition 6.1.19(a)) while $w$ is not). Now, $v$ is a suffix of $w$. Thus, there exists an $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this $u$. Clearly, $u$ is nonempty (since $uv = w \neq v$). Assume (for the sake of contradiction) that $u < v$. Let $v'$ be the (lexicographically) smallest nonempty suffix of $u$. Then, $v'$ is a Lyndon word (by Proposition 6.1.19(a), applied to $u$ and $v'$ instead of $w$ and $v$) and satisfies $v' \leq u$ (since $u$ is a nonempty suffix of $u$, whereas $v'$ is the smallest such suffix). Thus, $v'$ and $v$ are Lyndon words such that $v' \leq u < v$. Proposition 6.1.16(a) (applied to $v'$ instead of $u$) now yields that the word $v'v$ is Lyndon. Hence, every nonempty proper suffix of $v'v$ is $> v'v$. Since $v$ is a nonempty proper suffix of $v'v$, this yields that $v > v'v$.

But $v'$ is a nonempty suffix of $u$, so that $v'v$ is a nonempty suffix of $uv = w$. Since $v$ is the smallest such suffix, this yields that $v'v \geq v$. This contradicts $v > v'v$. Our assumption (that $u < v$) therefore falls. We conclude that $u \geq v$.

It remains to prove that $uv \geq vu$. Assume the contrary. Then, $uv < vu$. Thus, there exists at least one suffix $t$ of $u$ such that $tv < vt$ (namely, $t = u$). Let $p$ be the **minimum-length** such suffix. Then, $pv < vp$. Thus, $p$ is nonempty.

Since $p$ is a suffix of $u$, it is clear that $pv$ is a suffix of $uv = w$. So we know that $pv$ is a nonempty suffix of $w$. Since $v$ is the smallest such suffix, this yields that $v \leq pv < vp$. Thus, Proposition 6.1.2(g) (applied to $a = v$, $b = pv$ and $c = p$) yields that $v$ is a prefix of $pv$. In other words, there exists a $q \in \mathfrak{A}^*$ such that $pv = vq$. Consider this $q$. This $q$ is nonempty (because otherwise we would have $pv = v \underbrace{q}_{=\varnothing} = v$, contradicting the fact that $p$ is nonempty). From $vq = pv < vp$, we obtain $q \leq p$ (by Proposition 6.1.2(c), applied to $a = v$, $c = q$ and $d = p$).

We know that $q$ is a suffix of $pv$ (since $vq = pv$), whereas $pv$ is a suffix of $w$. Thus, $q$ is a suffix of $w$. So $q$ is a nonempty suffix of $w$. Since $v$ is the smallest such suffix, this yields that $v \leq q$. We now have $v \leq q \leq p \leq pv < vp$. Hence, $v$ is a prefix of $p$ (by Proposition 6.1.2(g), applied to $a = v$, $b = p$ and $c = p$). In other words, there exists an $r \in \mathfrak{A}^*$ such that $p = vr$. Consider this $r$. Clearly, $r$ is a suffix of $p$, while $p$ is a suffix of $u$; therefore, $r$ is a suffix of $u$. Also, $pv < vp$ rewrites as $vrv < vvr$ (because $p = vr$). Thus, Proposition 6.1.2(c) (applied to $a = v$, $c = rv$ and $d = vr$) yields $rv \leq vr$. Since $rv \neq vr$ (because otherwise, we would have $rv = vr$, thus $v \underbrace{rv}_{=vr} = vvr$, contradicting $vrv < vvr$), this becomes $rv < vr$.

Now, $r$ is a suffix of $u$ such that $rv < vr$. Since $p$ is the minimum-length such suffix, this yields $\ell(r) \geq \ell(p)$. But this contradicts the fact that $\ell\left(\underbrace{p}_{=vr}\right) = \ell(vr) = \underbrace{\ell(v)}_{>0} + \ell(r) > \ell(r)$. This contradiction proves our assumption wrong; thus, we have shown that $uv \geq vu$. Proposition 6.1.19(b) is proven. □

**Theorem 6.1.20.** *Let $w$ be a nonempty word. The following four assertions are equivalent:*

- *Assertion $\mathcal{A}$: The word $w$ is Lyndon.*
- *Assertion $\mathcal{B}$: Any nonempty words $u$ and $v$ satisfying $w = uv$ satisfy $v > w$.*
- *Assertion $\mathcal{C}$: Any nonempty words $u$ and $v$ satisfying $w = uv$ satisfy $v > u$.*
- *Assertion $\mathcal{D}$: Any nonempty words $u$ and $v$ satisfying $w = uv$ satisfy $vu > uv$.*

*Proof. Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{B}$:* If Assertion $\mathcal{A}$ holds, then Assertion $\mathcal{B}$ clearly holds (in fact, whenever $u$ and $v$ are nonempty words satisfying $w = uv$, then $v$ is a nonempty proper suffix of $w$, and therefore $> w$ by the definition of a Lyndon word).

*Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{C}$:* This implication follows from Proposition 6.1.14(b).

*Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{D}$:* This implication follows from Proposition 6.1.14(c).

*Proof of the implication $\mathcal{B} \Longrightarrow \mathcal{A}$:* Assume that Assertion $\mathcal{B}$ holds. If $v$ is a nonempty proper suffix of $w$, then there exists an $u \in \mathfrak{A}^*$ satisfying $w = uv$. This $u$ is nonempty because $v$ is a proper suffix, and thus Assertion $\mathcal{B}$ yields $v > w$. Hence, every nonempty proper suffix $v$ of $w$ satisfies $v > w$.

By the definition of a Lyndon word, this yields that $w$ is Lyndon, so that Assertion $\mathcal{A}$ holds.

*Proof of the implication* $\mathcal{C} \Longrightarrow \mathcal{A}$*:* Assume that Assertion $\mathcal{C}$ holds. If $w$ was not Lyndon, then Proposition 6.1.19(b) would yield nonempty words $u$ and $v$ such that $w = uv$ and $u \geq v$; this would contradict Assertion $\mathcal{C}$. Thus, $w$ is Lyndon, and Assertion $\mathcal{A}$ holds.

*Proof of the implication* $\mathcal{D} \Longrightarrow \mathcal{A}$*:* Assume that Assertion $\mathcal{D}$ holds. If $w$ was not Lyndon, then Proposition 6.1.19(b) would yield nonempty words $u$ and $v$ such that $w = uv$ and $uv \geq vu$; this would contradict Assertion $\mathcal{D}$. Thus, $w$ is Lyndon, and Assertion $\mathcal{A}$ holds.

Now we have proven enough implications to conclude the equivalence of all four assertions. □

Theorem 6.1.20 connects our definition of Lyndon words with some of the definitions appearing in literature. For example, Lothaire [139, §5.1], Shirshov [202] and de Bruijn/Klarner [29, §4] define Lyndon words using Assertion $\mathcal{D}$ (note, however, that Shirshov takes $<$ instead of $>$ and calls Lyndon words "regular words"; also, de Bruijn/Klarner call Lyndon words "normal words"). Chen-Fox-Lyndon [38, §1], Reutenauer [182] and Radford [177] use our definition (but Chen-Fox-Lyndon call the Lyndon words "standard sequences", and Radford calls them "primes" and uses $<$ instead of $>$).

Theorem 6.1.20 appears (with different notations) in Zhou-Lu [229, Proposition 1.4]. The equivalence $\mathcal{D} \Longleftrightarrow \mathcal{A}$ of our Theorem 6.1.20 is equivalent to [139, Proposition 5.12] and to [38, $\mathfrak{A}'' = \mathfrak{A}'''$].

The following exercise provides a different (laborious) approach to Theorem 6.1.20:

**Exercise 6.1.21.** (a) Prove that if $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ are two words satisfying $uv < vu$, then there exists a nonempty suffix $s$ of $u$ satisfying $sv < v$.

(b) Give a new proof of Theorem 6.1.20 (avoiding the use of Proposition 6.1.19).

[**Hint:** For (a), perform strong induction on $\ell(u) + \ell(v)$, assume the contrary, and distinguish between the case when $u \leq v$ and the case when $v$ is a prefix of $u$. For (b), use part (a) in proving the implication $\mathcal{D} \Longrightarrow \mathcal{B}$, and factor $v$ as $v = u^m v'$ with $m$ maximal in the proof of the implication $\mathcal{C} \Longrightarrow \mathcal{B}$.]

The following two exercises are taken from [91][282].

**Exercise 6.1.22.** Let $w$ be a nonempty word. Prove that $w$ is Lyndon if and only if every nonempty word $t$ and every positive integer $n$ satisfy (if $w \leq t^n$, then $w \leq t$).

**Exercise 6.1.23.** Let $w_1, w_2, \ldots, w_n$ be $n$ Lyndon words, where $n$ is a positive integer. Assume that $w_1 \leq w_2 \leq \cdots \leq w_n$ and $w_1 < w_n$. Show that $w_1 w_2 \cdots w_n$ is a Lyndon word.

The following exercise is a generalization (albeit not in an obvious way) of Exercise 6.1.23:

[282] Exercise 6.1.22 is more or less [91, Lemma 4.3] with a converse added; Exercise 6.1.23 is [91, Lemma 4.2].

**Exercise 6.1.24.** Let $w_1$, $w_2$, $\ldots$, $w_n$ be $n$ Lyndon words, where $n$ is a positive integer. Assume that $w_i w_{i+1} \cdots w_n \geq w_1 w_2 \cdots w_n$ for every $i \in \{1, 2, \ldots, n\}$. Show that $w_1 w_2 \cdots w_n$ is a Lyndon word.

We are now ready to meet one of the most important features of Lyndon words: a bijection between all words and multisets of Lyndon words[283]; it is clear that such a bijection is vital for constructing polynomial generating sets of commutative algebras with bases indexed by words, such as QSym or shuffle algebras. This bijection is given by the *Chen-Fox-Lyndon factorization*:

**Definition 6.1.25.** Let $w$ be a word. A *Chen-Fox-Lyndon factorization* (in short, *CFL factorization*) of $w$ means a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$ and $a_1 \geq a_2 \geq \cdots \geq a_k$.

**Example 6.1.26.** The tuple $(23, 2, 14, 13323, 13, 12, 12, 1)$ is a CFL factorization of the word 23214133231312121 over the alphabet $\{1, 2, 3, \ldots\}$ (ordered by $1 < 2 < 3 < \cdots$), since 23, 2, 14, 13323, 13, 12, 12 and 1 are Lyndon words satisfying $23214133231312121 = 23 \cdot 2 \cdot 14 \cdot 13323 \cdot 13 \cdot 12 \cdot 12 \cdot 1$ and $23 \geq 2 \geq 14 \geq 13323 \geq 13 \geq 12 \geq 12 \geq 1$.

The bijection is given by the following *Chen-Fox-Lyndon theorem* ([93, Theorem 6.5.5], [139, Thm. 5.1.5], [177, part of Thm. 2.1.4]):

**Theorem 6.1.27.** *Let $w$ be a word. Then, there exists a unique CFL factorization of $w$.*

Before we prove this, we need to state and prove a lemma (which is [139, Proposition 5.1.6]):

**Lemma 6.1.28.** *Let $(a_1, a_2, \ldots, a_k)$ be a CFL factorization of a nonempty word $w$. Let $p$ be a nonempty suffix of $w$. Then, $p \geq a_k$.*

*Proof.* We will prove Lemma 6.1.28 by induction over the (obviously) positive integer $k$.

*Induction base:* Assume that $k = 1$. Thus, $(a_1, a_2, \ldots, a_k) = (a_1)$ is a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$. We have $w = a_1 a_2 \cdots a_k = a_1$ (since $k = 1$), so that $w$ is a Lyndon word (since $a_1$ is a Lyndon word). Thus, Corollary 6.1.15 (applied to $v = p$) yields $p \geq w = a_1 = a_k$ (since $1 = k$). Thus, Lemma 6.1.28 is proven in the case $k = 1$. The induction base is complete.

*Induction step:* Let $K$ be a positive integer. Assume (as the induction hypothesis) that Lemma 6.1.28 is proven for $k = K$. We now need to show that Lemma 6.1.28 holds for $k = K + 1$.

So let $(a_1, a_2, \ldots, a_{K+1})$ be a CFL factorization of a nonempty word $w$. Let $p$ be a nonempty suffix of $w$. We need to prove that $p \geq a_{K+1}$.

By the definition of a CFL factorization, $(a_1, a_2, \ldots, a_{K+1})$ is a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_{K+1}$ and $a_1 \geq a_2 \geq \cdots \geq a_{K+1}$. Let $w' = a_2 a_3 \cdots a_{K+1}$; then, $w = a_1 a_2 \cdots a_{K+1} = a_1 \underbrace{(a_2 a_3 \cdots a_{K+1})}_{=w'} = a_1 w'$. Hence, every nonempty suffix of $w$ is either a nonempty suffix of $w'$, or has the form $qw'$ for a nonempty suffix $q$ of $a_1$. Since $p$ is a nonempty suffix of $w$, we thus must be in one of the following two cases:

[283] And it is not even the only such bijection: we will see another in Subsection 6.6.1.

*Case 1:* The word $p$ is a nonempty suffix of $w'$.

*Case 2:* The word $p$ has the form $qw'$ for a nonempty suffix $q$ of $a_1$.

Let us first consider Case 1. In this case, $p$ is a nonempty suffix of $w'$. The $K$-tuple $(a_2, a_3, \ldots, a_{K+1})$ of Lyndon words satisfies $w' = a_2 a_3 \cdots a_{K+1}$ and $a_2 \geq a_3 \geq \cdots \geq a_{K+1}$; therefore, $(a_2, a_3, \ldots, a_{K+1})$ is a CFL factorization of $w'$. We can thus apply Lemma 6.1.28 to $K$, $w'$ and $(a_2, a_3, \ldots, a_{K+1})$ instead of $k$, $w$ and $(a_1, a_2, \ldots, a_k)$ (because we assumed that Lemma 6.1.28 is proven for $k = K$). As a result, we obtain that $p \geq a_{K+1}$. Thus, $p \geq a_{K+1}$ is proven in Case 1.

Let us now consider Case 2. In this case, $p$ has the form $qw'$ for a nonempty suffix $q$ of $a_1$. Consider this $q$. Since $a_1$ is a Lyndon word, we have $q \geq a_1$ (by Corollary 6.1.15, applied to $a_1$ and $q$ instead of $w$ and $v$). Thus, $q \geq a_1 \geq a_2 \geq \cdots \geq a_{K+1}$, so that $p = qw' \geq q \geq a_{K+1}$. Thus, $p \geq a_{K+1}$ is proven in Case 2.

We have now proven $p \geq a_{K+1}$ in all cases. This proves that Lemma 6.1.28 holds for $k = K + 1$. The induction step is thus finished, and with it the proof of Lemma 6.1.28. □

*Proof of Theorem 6.1.27.* Let us first prove that there exists a CFL factorization of $w$.

Indeed, there clearly exists a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$ [284]. Fix such a tuple with **minimum** $k$. We claim that $a_1 \geq a_2 \geq \cdots \geq a_k$.

Indeed, if some $i \in \{1, 2, \ldots, k-1\}$ would satisfy $a_i < a_{i+1}$, then the word $a_i a_{i+1}$ would be Lyndon (by Proposition 6.1.16(a), applied to $u = a_i$ and $v = a_{i+1}$), whence $(a_1, a_2, \ldots, a_{i-1}, a_i a_{i+1}, a_{i+2}, a_{i+3}, \ldots, a_k)$ would also be a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_{i-1} (a_i a_{i+1}) a_{i+2} a_{i+3} \cdots a_k$ but having length $k - 1 < k$, contradicting the fact that $k$ is the minimum length of such a tuple. Hence, no $i \in \{1, 2, \ldots, k-1\}$ can satisfy $a_i < a_{i+1}$. In other words, every $i \in \{1, 2, \ldots, k-1\}$ satisfies $a_i \geq a_{i+1}$. In other words, $a_1 \geq a_2 \geq \cdots \geq a_k$. Thus, $(a_1, a_2, \ldots, a_k)$ is a CFL factorization of $w$, so we have shown that such a CFL factorization exists.

It remains to show that there exists at most one CFL factorization of $w$. We shall prove this by induction over $\ell(w)$. Thus, we fix a word $w$ and assume that

$$\begin{aligned} &\text{for every word } v \text{ with } \ell(v) < \ell(w), \\ &\text{there exists at most one CFL factorization of } v. \end{aligned} \tag{6.1.1}$$

We now have to prove that there exists at most one CFL factorization of $w$.

Indeed, let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_m)$ be two CFL factorizations of $w$. We need to prove that $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_m)$. If $w$ is empty, then this is obvious, so we WLOG assume that it is not; thus, $k > 0$ and $m > 0$.

Since $(b_1, b_2, \ldots, b_m)$ is a CFL factorization of $w$, we have $w = b_1 b_2 \cdots b_m$, and thus $b_m$ is a nonempty suffix of $w$. Thus, Lemma 6.1.28 (applied to $p = b_m$) yields $b_m \geq a_k$. The same argument (but with the roles of

[284] For instance, the tuple $(w_1, w_2, \ldots, w_{\ell(w)})$ of one-letter words is a valid example (recall that one-letter words are always Lyndon).

$(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_m)$ switched) shows that $a_k \geq b_m$. Combined with $b_m \geq a_k$, this yields $a_k = b_m$. Now let $v = a_1 a_2 \cdots a_{k-1}$. Then, $(a_1, a_2, \ldots, a_{k-1})$ is a CFL factorization of $v$ (since $a_1 \geq a_2 \geq \cdots \geq a_{k-1}$).

Since $(a_1, a_2, \ldots, a_k)$ is a CFL factorization of $w$, we have $w = a_1 a_2 \cdots a_k = \underbrace{a_1 a_2 \cdots a_{k-1}}_{=v} \underbrace{a_k}_{=b_m} = v b_m$, so that

$$v b_m = w = b_1 b_2 \cdots b_m = b_1 b_2 \cdots b_{m-1} b_m.$$

Cancelling $b_m$ yields $v = b_1 b_2 \cdots b_{m-1}$. Thus, $(b_1, b_2, \ldots, b_{m-1})$ is a CFL factorization of $v$ (since $b_1 \geq b_2 \geq \cdots \geq b_{m-1}$). Since $\ell(v) < \ell(w)$ (because $v = a_1 a_2 \cdots a_{k-1}$ is shorter than $w = a_1 a_2 \cdots a_k$), we can apply (6.1.1) to obtain that there exists at most one CFL factorization of $v$. But we already know two such CFL factorizations: $(a_1, a_2, \ldots, a_{k-1})$ and $(b_1, b_2, \ldots, b_{m-1})$. Thus, $(a_1, a_2, \ldots, a_{k-1}) = (b_1, b_2, \ldots, b_{m-1})$, which, combined with $a_k = b_m$, leads to $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_m)$. This is exactly what we needed to prove. So we have shown (by induction) that there exists at most one CFL factorization of $w$. This completes the proof of Theorem 6.1.27. □

The CFL factorization allows us to count all Lyndon words of a given length if $\mathfrak{A}$ is finite:

**Exercise 6.1.29.** Assume that the alphabet $\mathfrak{A}$ is finite. Let $q = |\mathfrak{A}|$. Let $\mu$ be the number-theoretic Möbius function (defined as in Exercise 2.9.6). Show that the number of Lyndon words of length $n$ equals $\frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$ for every positive integer $n$ (where "$\sum_{d|n}$" means a sum over all positive divisors of $n$). [285]

Exercise 6.1.29 is a well-known result and appears, e.g., in [38, Theorem 1.5] or in [139, Section 5.1].

We will now study another kind of factorization: not of an arbitrary word into Lyndon words, but of a Lyndon word into two smaller Lyndon words. This factorization is called *standard factorization* ([139, §5.1]) or *canonical factorization* ([93, Lemma 6.5.33]); we only introduce it from the viewpoint we are interested in, namely its providing a way to do induction over Lyndon words[286]. Here is what we need to know:

**Theorem 6.1.30.** *Let $w$ be a Lyndon word of length $> 1$. Let $v$ be the (lexicographically) smallest nonempty* **proper** *suffix of $w$. Since $v$ is a proper suffix of $w$, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this $u$. Then:*

(a) *The words $u$ and $v$ are Lyndon.*
(b) *We have $u < w < v$.*

*Proof.* Every nonempty proper suffix of $v$ is $\geq v$ (since every nonempty proper suffix of $v$ is a nonempty proper suffix of $w$, but $v$ is the smallest such suffix) and therefore $> v$ (since a proper suffix of $v$ cannot be $= v$). Combined with the fact that $v$ is nonempty, this yields that $v$ is Lyndon.

[285] In particular, $\frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$ is an integer.

[286] e.g., allowing to solve Exercise 6.1.24 in a simpler way

Since $w$ is Lyndon, we know that every nonempty proper suffix of $w$ is $> w$. Applied to the nonempty proper suffix $v$ of $w$, this yields that $v > w$. Hence, $w < v$. Since $v$ is nonempty, we have $u < uv = w < v$. This proves Theorem 6.1.30(b).

Let $p$ be a nonempty proper suffix of $u$. Then, $pv$ is a nonempty proper suffix of $uv = w$. Thus, $pv > w$ (since every nonempty proper suffix of $w$ is $> w$). Thus, $pv > w = uv$, so that $uv < pv$. Thus, Proposition 6.1.2(e) (applied to $a = u$, $b = v$, $c = p$ and $d = v$) yields that either we have $u \leq p$ or the word $p$ is a prefix of $u$.

Let us assume (for the sake of contradiction) that $p \leq u$. Then, $p < u$ (because $p$ is a proper suffix of $u$, and therefore $p \neq u$). Hence, we cannot have $u \leq p$. Thus, the word $p$ is a prefix of $u$ (since either we have $u \leq p$ or the word $p$ is a prefix of $u$). In other words, there exists a $q \in \mathfrak{A}^*$ such that $u = pq$. Consider this $q$. We have $w = \underbrace{u}_{=pq} v = pqv = p(qv)$, and thus $qv$ is a proper suffix of $w$ (proper because $p$ is nonempty). Moreover, $qv$ is nonempty (since $v$ is nonempty). Hence, $qv$ is a nonempty proper suffix of $w$. Since $v$ is the smallest such suffix, this entails that $v \leq qv$. Proposition 6.1.2(b) (applied to $a = p$, $c = v$ and $d = qv$) thus yields $pv \leq pqv$. Hence, $pv \leq pqv = w$, which contradicts $pv > w$. This contradiction shows that our assumption (that $p \leq u$) was false. We thus have $p > u$.

We now have shown that $p > u$ whenever $p$ is a nonempty proper suffix of $u$. Combined with the fact that $u$ is nonempty, this shows that $u$ is a Lyndon word. This completes the proof of Theorem 6.1.30(a). □

Another approach to the standard factorization is given in the following exercise:

**Exercise 6.1.31.** Let $w$ be a Lyndon word of length $> 1$. Let $v$ be the longest proper suffix of $w$ such that $v$ is Lyndon[287]. Since $v$ is a proper suffix of $w$, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this $u$. Prove that:

(a) The words $u$ and $v$ are Lyndon.
(b) We have $u < w < v$.
(c) The words $u$ and $v$ are precisely the words $u$ and $v$ constructed in Theorem 6.1.30.

Notice that a well-known recursive characterization of Lyndon words [38, $\mathfrak{A}' = \mathfrak{A}''$] can be easily derived from Theorem 6.1.30 and Proposition 6.1.16(a). We will not dwell on it.

The following exercise surveys some variations on the characterizations of Lyndon words[288]:

**Exercise 6.1.32.** Let $w$ be a nonempty word. Consider the following nine assertions:

- *Assertion $\mathcal{A}'$:* The word $w$ is a power of a Lyndon word.

[287] This is well-defined, because there exists at least one proper suffix $v$ of $w$ such that $v$ is Lyndon. (Indeed, the last letter of $w$ forms such a suffix, because it is a proper suffix of $w$ (since $w$ has length $> 1$) and is Lyndon (since it is a one-letter word, and since every one-letter word is Lyndon).)

[288] Compare this with [112, §7.2.11, Theorem Q].

- *Assertion $\mathcal{B}'$:* If $u$ and $v$ are nonempty words satisfying $w = uv$, then either we have $v \geq w$ or the word $v$ is a prefix of $w$.
- *Assertion $\mathcal{C}'$:* If $u$ and $v$ are nonempty words satisfying $w = uv$, then either we have $v \geq u$ or the word $v$ is a prefix of $u$.
- *Assertion $\mathcal{D}'$:* If $u$ and $v$ are nonempty words satisfying $w = uv$, then we have $vu \geq uv$.
- *Assertion $\mathcal{E}'$:* If $u$ and $v$ are nonempty words satisfying $w = uv$, then either we have $v \geq u$ or the word $v$ is a prefix of $w$.
- *Assertion $\mathcal{F}'$:* The word $w$ is a prefix of a Lyndon word in $\mathfrak{A}^*$.
- *Assertion $\mathcal{F}''$:* Let $m$ be an object not in the alphabet $\mathfrak{A}$. Let us equip the set $\mathfrak{A} \cup \{m\}$ with a total order which extends the total order on the alphabet $\mathfrak{A}$ and which satisfies ($a < m$ for every $a \in \mathfrak{A}$). Then, the word $wm \in (\mathfrak{A} \cup \{m\})^*$ (the concatenation of the word $w$ with the one-letter word $m$) is a Lyndon word.
- *Assertion $\mathcal{G}'$:* There exists a Lyndon word $t \in \mathfrak{A}^*$, a positive integer $\ell$ and a prefix $p$ of $t$ (possibly empty) such that $w = t^\ell p$.
- *Assertion $\mathcal{H}'$:* There exists a Lyndon word $t \in \mathfrak{A}^*$, a nonnegative integer $\ell$ and a prefix $p$ of $t$ (possibly empty) such that $w = t^\ell p$.

(a) Prove the equivalence $\mathcal{A}' \Longleftrightarrow \mathcal{D}'$.
(b) Prove the equivalence $\mathcal{B}' \Longleftrightarrow \mathcal{C}' \Longleftrightarrow \mathcal{E}' \Longleftrightarrow \mathcal{F}'' \Longleftrightarrow \mathcal{G}' \Longleftrightarrow \mathcal{H}'$.
(c) Prove the implication $\mathcal{F}' \Longrightarrow \mathcal{B}'$.
(d) Prove the implication $\mathcal{D}' \Longrightarrow \mathcal{B}'$. (The implication $\mathcal{B}' \Longrightarrow \mathcal{D}'$ is false, as witnessed by the word 11211.)
(e) Prove that if there exists a letter $\mu \in \mathfrak{A}$ such that ($\mu > a$ for every letter $a$ of $w$), then the equivalence $\mathcal{F}' \Longleftrightarrow \mathcal{F}''$ holds.
(f) Prove that if there exists a letter $\mu \in \mathfrak{A}$ such that ($\mu > a$ for some letter $a$ of $w$), then the equivalence $\mathcal{F}' \Longleftrightarrow \mathcal{F}''$ holds.

The next exercise (based on work of Hazewinkel [92]) extends some of the above properties of Lyndon words (and words in general) to a more general setting, in which the alphabet $\mathfrak{A}$ is no longer required to be totally ordered, but only needs to be a poset:

**Exercise 6.1.33.** In this exercise, we shall loosen the requirement that the alphabet $\mathfrak{A}$ be a totally ordered set: Instead, we will only require $\mathfrak{A}$ to be a poset. The resulting more general setting will be called the *partial-order setting*, to distinguish it from the *total-order setting* in which $\mathfrak{A}$ is required to be a totally ordered set. All results in Chapter 6 so far address the total-order setting. In this exercise, we will generalize some of them to the partial-order setting.

All notions that we have defined in the total-order setting (the notion of a word, the relation $\leq$, the notion of a Lyndon word, etc.) are defined in precisely the same way in the partial-order setting. However, the poset $\mathfrak{A}^*$ is no longer totally ordered in the partial-order setting.

(a) Prove that Proposition 6.1.2 holds in the partial-order setting, as long as one replaces "a total order" by "a partial order" in part (a) of this Proposition.

(b) Prove (in the partial-order setting) that if $a, b, c, d \in \mathfrak{A}^*$ are four words such that the words $ab$ and $cd$ are comparable (with respect to the partial order $\leq$), then the words $a$ and $c$ are comparable.

(c) Prove that Proposition 6.1.4, Proposition 6.1.5, Corollary 6.1.6, Corollary 6.1.8, Exercise 6.1.9, Exercise 6.1.10, Exercise 6.1.11, Exercise 6.1.12, Proposition 6.1.14, Corollary 6.1.15, Proposition 6.1.16, Corollary 6.1.17, Proposition 6.1.18, Theorem 6.1.20, Exercise 6.1.21(a), Exercise 6.1.23, Exercise 6.1.24, Exercise 6.1.31(a) and Exercise 6.1.31(b) still hold in the partial-order setting.

(d) Find a counterexample to Exercise 6.1.22 in the partial-order setting.

(e) Salvage Exercise 6.1.22 in the partial-order setting (i.e., find a statement which is easily equivalent to this exercise in the total-order setting, yet true in the partial-order setting).

(f) In the partial-order setting, a *Hazewinkel-CFL factorization* of a word $w$ will mean a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words such that $w = a_1 a_2 \cdots a_k$ and such that no $i \in \{1, 2, \ldots, k-1\}$ satisfies $a_i < a_{i+1}$. Prove that every word $w$ has a unique Hazewinkel-CFL factorization (in the partial-order setting).[289]

(g) Prove that Exercise 6.1.32 still holds in the partial-order setting.

The reader is invited to try extending other results to the partial-order setting (it seems that no research has been done on this except for Hazewinkel's [92]). We shall now, however, return to the total-order setting (which has the most known applications).

Another extension of the notion of Lyndon words has been introduced in 2018 by Dolce, Restivo and Reutenauer [53]; it is based on a generalized version of the lexicographic order, in which different letters are compared differently depending on their positions in the word (i.e., there is one total order for comparing first letters, another for comparing second letters, etc.).

Lyndon words are related to various other objects in mathematics, such as free Lie algebras (Subsection 6.1.1 below), shuffles and shuffle algebras (Sections 6.2 and 6.3 below), QSym (Sections 6.4 and 6.5), Markov chains on combinatorial Hopf algebras ([52]), de Bruijn sequences ([72], [159], [160], [112, §7.2.11, Algorithm F]), symmetric functions (specifically, the transition matrices between the bases $(h_\lambda)_{\lambda \in \mathrm{Par}}$, $(e_\lambda)_{\lambda \in \mathrm{Par}}$ and $(m_\lambda)_{\lambda \in \mathrm{Par}}$; see [117] for this), and the Burrows-Wheeler algorithm for data compression (see Remark 6.6.31 below for a quick idea, and [45], [81], [116] for more). They are also connected to *necklaces* (in the combinatorial sense) – a combinatorial object that also happens to be related to a lot of algebra ([185, Chapter 5], [48]). Let us survey the basics of this latter classical connection in an exercise:

**Exercise 6.1.34.** Let $\mathfrak{A}$ be any set (not necessarily totally ordered). Let $C$ denote the infinite cyclic group, written multiplicatively. Fix a generator $c$ of $C$. [290] Fix a positive integer $n$. The group $C$ acts on $\mathfrak{A}^n$ from the

[289] This result, as well as the validity of Proposition 6.1.16 in the partial-order setting, are due to Hazewinkel [92].

[290] So $C$ is a group isomorphic to $(\mathbb{Z}, +)$, and the isomorphism $(\mathbb{Z}, +) \to C$ sends every $n \in \mathbb{Z}$ to $c^n$. (Recall that we write the binary operation of $C$ as $\cdot$ instead of $+$.)

left according to the rule

$$c \cdot (a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_n, a_1) \qquad \text{for all } (a_1, a_2, \ldots, a_n) \in \mathfrak{A}^n.$$

[291] The orbits of this $C$-action will be called *$n$-necklaces*[292]; they form a set partition of the set $\mathfrak{A}^n$.

The $n$-necklace containing a given $n$-tuple $w \in \mathfrak{A}^n$ will be denoted by $[w]$.

(a) Prove that every $n$-necklace $N$ is a finite nonempty set and satisfies $|N| \mid n$. (Recall that $N$ is an orbit, thus a set; as usual, $|N|$ denotes the cardinality of this set.)

The *period* of an $n$-necklace $N$ is defined as the positive integer $|N|$. (This $|N|$ is indeed a positive integer, since $N$ is a finite nonempty set.)[293]

An $n$-necklace is said to be *aperiodic* if its period is $n$.

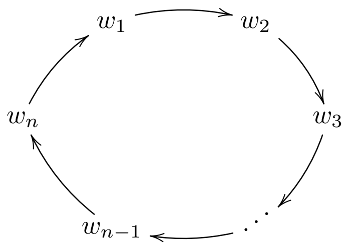
(b) Given any $n$-tuple $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, prove that the $n$-necklace $[w]$ is aperiodic if and only if every $k \in \{1, 2, \ldots, n-1\}$ satisfies $(w_{k+1}, w_{k+2}, \ldots, w_n, w_1, w_2, \ldots, w_k) \neq w$.

From now on, we assume that the set $\mathfrak{A}$ is totally ordered. We use $\mathfrak{A}$ as our alphabet to define the notions of words, the lexicographic order, and Lyndon words. All notations that we introduced for words will thus be used for elements of $\mathfrak{A}^n$.

(c) Prove that every aperiodic $n$-necklace contains exactly one Lyndon word.

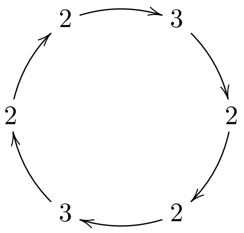
[291] In other words, $c$ rotates any $n$-tuple of elements of $\mathfrak{A}$ cyclically to the left. Thus, $c^n \in C$ acts trivially on $\mathfrak{A}^n$, and so this action of $C$ on $\mathfrak{A}^n$ factors through $C / \langle c^n \rangle$ (a cyclic group of order $n$).

[292] Classically, one visualizes them as necklaces of $n$ beads of $|\mathfrak{A}|$ colors. (The colors are the elements of $\mathfrak{A}$.) For example, the necklace containing an $n$-tuple $(w_1, w_2, \ldots, w_n)$ is visualized as follows:



with $w_1, w_2, \ldots, w_n$ being the colors of the respective beads. The intuition behind this is that a necklace is an object that doesn't really change when we rotate it in its plane. However, to make this intuition match the definition, we need to think of a necklace as being stuck in its (fixed) plane, so that we cannot lift it up and turn it around, dropping it back to its plane in a reflected state.

[293] For example, the 6-necklace [232232] – or, visually,



– has period 3, as it is a set of size 3 (with elements 232232, 322322 and 223223). The word "period" hints at the geometric meaning: If an $n$-necklace $N$ is represented by coloring the vertices of a regular $n$-gon, then its period is the smallest positive integer $d$ such that the colors are preserved when the $n$-gon is rotated by $2\pi d/n$.

(d) If $N$ is an $n$-necklace which is not aperiodic, then prove that $N$ contains no Lyndon word.

(e) Show that the aperiodic $n$-necklaces are in bijection with Lyndon words of length $n$.

From now on, we assume that the set $\mathfrak{A}$ is finite. Define the number-theoretic Möbius function $\mu$ and the Euler totient function $\phi$ as in Exercise 2.9.6.

(f) Prove that the number of all aperiodic $n$-necklaces is
$$\frac{1}{n}\sum_{d\mid n}\mu\left(d\right)\left|\mathfrak{A}\right|^{n/d}.$$

(g) Prove that the number of all $n$-necklaces is
$$\frac{1}{n}\sum_{d\mid n}\phi\left(d\right)\left|\mathfrak{A}\right|^{n/d}.$$

(h) Solve Exercise 6.1.29 again.

(i) Forget that we fixed $\mathfrak{A}$. Show that every $q \in \mathbb{Z}$ satisfies $n \mid \sum_{d\mid n}\mu\left(d\right)q^{n/d}$ and $n \mid \sum_{d\mid n}\phi\left(d\right)q^{n/d}$.

[**Hint:** For (c), use Theorem 6.1.20. For (i), either use parts (f) and (g) and a trick to extend to $q$ negative; or recall Exercise 2.9.8.]

We will pick up the topic of necklaces again in Section 6.6, where we will connect it back to symmetric functions.

6.1.1. *Free Lie algebras.* In this brief subsection, we shall review the connection between Lyndon words and free Lie algebras (following [124, Kap. 4], but avoiding the generality of Hall sets in favor of just using Lyndon words). None of this material shall be used in the rest of these notes. We will only prove some basic results; for more thorough and comprehensive treatments of free Lie algebras, see [182], [27, Chapter 2] and [124, Kap. 4].

We begin with some properties of Lyndon words.

**Exercise 6.1.35.** Let $w \in \mathfrak{A}^*$ be a nonempty word. Let $v$ be the longest Lyndon suffix of $w$ [294]. Let $t$ be a Lyndon word. Then, $t$ is the longest Lyndon suffix of $wt$ if and only if we do not have $v < t$.

(We have written "we do not have $v < t$" instead of "$v \geq t$" in Exercise 6.1.35 for reasons of generalizability: This way, Exercise 6.1.35 generalizes to the partial-order setting introduced in Exercise 6.1.33, whereas the version with "$v \geq t$" does not.)

**Exercise 6.1.36.** Let $w \in \mathfrak{A}^*$ be a word of length $> 1$. Let $v$ be the longest Lyndon proper suffix of $w$ [295]. Let $t$ be a Lyndon word. Then, $t$ is the longest Lyndon proper suffix of $wt$ if and only if we do not have $v < t$.

(Exercise 6.1.36, while being a trivial consequence of Exercise 6.1.35, is rather useful in the study of free Lie algebras. It generalizes both [38, Lemma (1.6)] (which is obtained by taking $w = c$, $v = b$ and $t = d$) and [139, Proposition 5.1.4] (which is obtained by taking $v = m$ and $t = n$).)

[294] Of course, a Lyndon suffix of $w$ just means a suffix $p$ of $w$ such that $p$ is Lyndon.

[295] Of course, a Lyndon proper suffix of $w$ just means a proper suffix $p$ of $w$ such that $p$ is Lyndon.

**Definition 6.1.37.** For the rest of Subsection 6.1.1, we let $\mathfrak{L}$ be the set of all Lyndon words (over the alphabet $\mathfrak{A}$).

**Definition 6.1.38.** Let $w$ be a Lyndon word of length $> 1$. Let $v$ be the longest proper suffix of $w$ such that $v$ is Lyndon. (This is well-defined, as we know from Exercise 6.1.31.) Since $v$ is a proper suffix of $w$, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this $u$. (Clearly, this $u$ is unique.) Theorem 6.1.30(a) shows that the words $u$ and $v$ are Lyndon. In other words, $u \in \mathfrak{L}$ and $v \in \mathfrak{L}$. Hence, $(u, v) \in \mathfrak{L} \times \mathfrak{L}$. The pair $(u, v) \in \mathfrak{L} \times \mathfrak{L}$ is called the *standard factorization* of $w$, and is denoted by $\operatorname{stf} w$.

For the sake of easier reference, we gather a few basic properties of the standard factorization:

**Exercise 6.1.39.** Let $w$ be a Lyndon word of length $> 1$. Let $(g, h) = \operatorname{stf} w$. Prove the following:

(a) The word $h$ is the longest Lyndon proper suffix of $w$.
(b) We have $w = gh$.
(c) We have $g < gh < h$.
(d) The word $g$ is Lyndon.
(e) We have $g \in \mathfrak{L}$, $h \in \mathfrak{L}$, $\ell(g) < \ell(w)$ and $\ell(h) < \ell(w)$.
(f) Let $t$ be a Lyndon word. Then, $t$ is the longest Lyndon proper suffix of $wt$ if and only if we do not have $h < t$.

**Exercise 6.1.40.** Let $\mathfrak{g}$ be a Lie algebra. For every Lyndon word $w$, let $b_w$ be an element of $\mathfrak{g}$. Assume that for every Lyndon word $w$ of length $> 1$, we have

$$b_w = [b_u, b_v], \qquad \text{where } (u, v) = \operatorname{stf} w. \tag{6.1.2}$$

Let $B$ be the $\mathbf{k}$-submodule of $\mathfrak{g}$ spanned by the family $(b_w)_{w \in \mathfrak{L}}$.

(a) Prove that $B$ is a Lie subalgebra of $\mathfrak{g}$.
(b) Let $\mathfrak{h}$ be a $\mathbf{k}$-Lie algebra. Let $f : B \to \mathfrak{h}$ be a $\mathbf{k}$-module homomorphism. Assume that whenever $w$ is a Lyndon word of length $> 1$, we have

$$f([b_u, b_v]) = [f(b_u), f(b_v)], \qquad \text{where } (u, v) = \operatorname{stf} w. \tag{6.1.3}$$

Prove that $f$ is a Lie algebra homomorphism.

[**Hint:** Given two words $w$ and $w'$, write $w \sim w'$ if and only if $w'$ is a permutation of $w$. Part (a) follows from the fact that for any $(p, q) \in \mathfrak{L} \times \mathfrak{L}$ satisfying $p < q$, we have $[b_p, b_q] \in B_{pq,q}$, where $B_{h,s}$ denotes the $\mathbf{k}$-linear span of $\{b_w \mid w \in \mathfrak{L}, w \sim h \text{ and } w < s\}$ for any two words $h$ and $s$. Prove this fact by a double induction, first inducting over $\ell(pq)$, and then (for fixed $\ell(pq)$) inducting over the rank of $q$ in lexicographic order (i.e., assume that the fact is already proven for every $q' < q$ instead of $q$). In the induction step, assume that $(p, q) \neq \operatorname{stf}(pq)$ (since otherwise the claim is rather obvious) and conclude that $p$ has length $> 1$; thus, set $(u, v) = \operatorname{stf} p$, so that $\left[\underbrace{b_p}_{=[b_u, b_v]}, b_q\right] = [[b_u, b_v], b_q] = [[b_u, b_q], b_v] - [[b_v, b_q], b_u]$, and use Exercise 6.1.36 to obtain $v < q$.

The proof of (b) proceeds by a similar induction, piggybacking on the $[b_p, b_q] \in B_{pq,q}$ claim.]

**Exercise 6.1.41.** Let $V$ be the free $\mathbf{k}$-module with basis $(x_a)_{a\in\mathfrak{A}}$. For every word $w \in \mathfrak{A}^*$, let $x_w$ be the tensor $x_{w_1} \otimes x_{w_2} \otimes \cdots \otimes x_{w_{\ell(w)}}$. As we know from Example 1.1.2, the tensor algebra $T(V)$ is a free $\mathbf{k}$-module with basis $(x_w)_{w\in\mathfrak{A}^*}$. We regard $V$ as a $\mathbf{k}$-submodule of $T(V)$.

The tensor algebra $T(V)$ becomes a Lie algebra via the commutator (i.e., its Lie bracket is defined by $[\alpha, \beta] = \alpha\beta - \beta\alpha$ for all $\alpha \in T(V)$ and $\beta \in T(V)$).

We define a sequence $(\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \ldots)$ of $\mathbf{k}$-submodules of $T(V)$ as follows: Recursively, we set $\mathfrak{g}_1 = V$, and for every $i \in \{2, 3, 4, \ldots\}$, we set $\mathfrak{g}_i = [V, \mathfrak{g}_{i-1}]$. Let $\mathfrak{g}$ be the $\mathbf{k}$-submodule $\mathfrak{g}_1 + \mathfrak{g}_2 + \mathfrak{g}_3 + \cdots$ of $T(V)$.

Prove the following:

(a) The $\mathbf{k}$-submodule $\mathfrak{g}$ is a Lie subalgebra of $T(V)$.
(b) If $\mathfrak{k}$ is any Lie subalgebra of $T(V)$ satisfying $V \subset \mathfrak{k}$, then $\mathfrak{g} \subset \mathfrak{k}$.

Now, for every $w \in \mathfrak{L}$, we define an element $b_w$ of $T(V)$ as follows: We define $b_w$ by recursion on the length of $w$. If the length of $w$ is 1 [296], then we have $w = (a)$ for some letter $a \in \mathfrak{A}$, and we set $b_w = x_a$ for this letter $a$. If the length of $w$ is $> 1$, then we set $b_w = [b_u, b_v]$, where $(u, v) = \operatorname{stf} w$ [297].

Prove the following:

(c) For every $w \in \mathfrak{L}$, we have
$$b_w \in x_w + \sum_{\substack{v\in\mathfrak{A}^{\ell(w)};\\ v>w}} \mathbf{k}x_v.$$
(d) The family $(b_w)_{w\in\mathfrak{L}}$ is a basis of the $\mathbf{k}$-module $\mathfrak{g}$.
(e) Let $\mathfrak{h}$ be any $\mathbf{k}$-Lie algebra. Let $\xi : \mathfrak{A} \to \mathfrak{h}$ be any map. Then, there exists a unique Lie algebra homomorphism $\Xi : \mathfrak{g} \to \mathfrak{h}$ such that every $a \in \mathfrak{A}$ satisfies $\Xi(x_a) = \xi(a)$.

*Remark* 6.1.42. Let $V$ and $\mathfrak{g}$ be as in Exercise 6.1.41. In the language of universal algebra, the statement of Exercise 6.1.41(e) says that $\mathfrak{g}$ (or, to be more precise, the pair $(\mathfrak{g}, f)$, where $f : \mathfrak{A} \to \mathfrak{g}$ is the map sending each $a \in \mathfrak{A}$ to $x_a \in \mathfrak{g}$) satisfies the universal property of the free Lie algebra on the set $\mathfrak{A}$. Thus, this exercise allows us to call $\mathfrak{g}$ the *free Lie algebra* on $\mathfrak{A}$. Most authors define the free Lie algebra differently, but all reasonable definitions of a free Lie algebra[298] lead to isomorphic Lie

[296] The length of any $w \in \mathfrak{L}$ must be at least 1. (Indeed, if $w \in \mathfrak{L}$, then the word $w$ is Lyndon and thus nonempty, and hence its length must be at least 1.)

[297] This is well-defined, because $b_u$ and $b_v$ have already been defined. [*Proof.* Let $(u, v) = \operatorname{stf} w$. Then, Exercise 6.1.39(e) (applied to $(g, h) = (u, v)$) shows that $u \in \mathfrak{L}$, $v \in \mathfrak{L}$, $\ell(u) < \ell(w)$ and $\ell(v) < \ell(w)$. Recall that we are defining $b_w$ by recursion on the length of $w$. Hence, $b_p$ is already defined for every $p \in \mathfrak{L}$ satisfying $\ell(p) < \ell(w)$. Applying this to $p = u$, we see that $b_u$ is already defined (since $u \in \mathfrak{L}$ and $\ell(u) < \ell(w)$). The same argument (but applied to $v$ instead of $u$) shows that $b_v$ is already defined. Hence, $b_u$ and $b_v$ have already been defined. Thus, $b_w$ is well-defined by $b_w = [b_u, b_v]$, qed.]

[298] Here, we call a definition "reasonable" if the "free Lie algebra" it defines satisfies the universal property.

algebras (because the universal property determines the free Lie algebra uniquely up to canonical isomorphism).

Notice that the Lie algebra $\mathfrak{g}$ does not depend on the total order on the alphabet $\mathfrak{A}$, but the basis $(b_w)_{w\in\mathfrak{L}}$ constructed in Exercise 6.1.41(d) does. There is no known basis of $\mathfrak{g}$ defined without ordering $\mathfrak{A}$.

It is worth noticing that our construction of $\mathfrak{g}$ proves not only that the free Lie algebra on $\mathfrak{A}$ exists, but also that this free Lie algebra can be realized as a Lie subalgebra of the (associative) algebra $T(V)$. Therefore, if we want to prove that a certain identity holds in every Lie algebra, we only need to check that this identity holds in every associative algebra (if all Lie brackets are replaced by commutators); the universal property of the free Lie algebra (i.e., Exercise 6.1.41(e)) will then ensure that this identity also holds in every Lie algebra $\mathfrak{h}$.

There is much more to say about free Lie algebras than what we have said here; in particular, there are connections to symmetric functions, necklaces, representations of symmetric groups and NSym. See [139, §5.3], [182], [27, Chapter 2], [124, §4] and [24] for further developments[299].

## 6.2. Shuffles and Lyndon words.

We will now connect the theory of Lyndon words with the notion of shuffle products. We have already introduced the latter notion in Definition 1.6.2, but we will now study it more closely and introduce some more convenient notations (e.g., we will need a notation for single shuffles, not just the whole multiset).[300]

**Definition 6.2.1.** (a) Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Then, $\operatorname{Sh}_{n,m}$ denotes the subset

$$\left\{\sigma \in \mathfrak{S}_{n+m} \ : \ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n) ; \right. \\ \left. \sigma^{-1}(n+1) < \sigma^{-1}(n+2) < \cdots < \sigma^{-1}(n+m)\right\}$$

of the symmetric group $\mathfrak{S}_{n+m}$.

(b) Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_m)$ be two words. If $\sigma \in \operatorname{Sh}_{n,m}$, then, $u \underset{\sigma}{\sqcup\!\sqcup} v$ will denote the word $\left(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n+m)}\right)$, where $(w_1, w_2, \ldots, w_{n+m})$ is the concatenation

$$u \cdot v = (u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_m).$$

We notice that the multiset of all letters of $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the disjoint union of the multiset of all letters of $u$ with the multiset of all letters of $v$. As a consequence, $\ell\left(u \underset{\sigma}{\sqcup\!\sqcup} v\right) = \ell(u) + \ell(v)$.

(c) Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_m)$ be two words. The *multiset of shuffles of $u$ and $v$* is defined as the multiset

$$\left\{\left(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n+m)}\right) \ : \ \sigma \in \operatorname{Sh}_{n,m}\right\}_{\text{multiset}},$$

[299] The claim made in [24, page 2] that "$\{x_1, \ldots, x_n\}$ generates freely a Lie subalgebra of $A_R$" is essentially our Exercise 6.1.41(e).

[300] Parts (a) and (c) of the below Definition 6.2.1 define notions which have already been introduced in Definition 1.6.2. Of course, the definitions of these notions are equivalent; however, the variables are differently labelled in the two definitions (for example, the variables $u$, $v$, $w$ and $\sigma$ of Definition 6.2.1(c) correspond to the variables $a$, $b$, $c$ and $w$ of Definition 1.6.2). The labels in Definition 6.2.1 have been chosen to match with the rest of Section 6.2.

where $(w_1, w_2, \ldots, w_{n+m})$ is the concatenation

$$u \cdot v = (u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_m).$$

In other words, the multiset of shuffles of $u$ and $v$ is the multiset

$$\left\{ u \underset{\sigma}{\sqcup\!\sqcup} v \ : \ \sigma \in \operatorname{Sh}_{n,m} \right\}_{\text{multiset}}.$$

It is denoted by $u \sqcup\!\sqcup v$.

The next fact provides the main connection between Lyndon words and shuffles:

**Theorem 6.2.2.** *Let $u$ and $v$ be two words.*

*Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of $u$. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of $v$.*

(a) *Let $(c_1, c_2, \ldots, c_{p+q})$ be the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order*[301]*. Then, the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $c_1 c_2 \cdots c_{p+q}$ (and $(c_1, c_2, \ldots, c_{p+q})$ is the CFL factorization of this element).*

(b) *Let $\mathfrak{L}$ denote the set of all Lyndon words. If $w$ is a Lyndon word and $z$ is any word, let $\operatorname{mult}_w z$ denote the number of terms in the CFL factorization of $z$ which are equal to $w$. The multiplicity with which the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ appears in the multiset $u \sqcup\!\sqcup v$ is $\prod_{w \in \mathfrak{L}} \dbinom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$. (This product is well-defined because almost all of its factors are 1.)*

(c) *If $a_i \geq b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$, then the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $uv$.*

(d) *If $a_i > b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$, then the multiplicity with which the word $uv$ appears in the multiset $u \sqcup\!\sqcup v$ is 1.*

(e) *Assume that $u$ is a Lyndon word. Also, assume that $u \geq b_j$ for every $j \in \{1, 2, \ldots, q\}$. Then, the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $uv$, and the multiplicity with which this word $uv$ appears in the multiset $u \sqcup\!\sqcup v$ is $\operatorname{mult}_u v + 1$.*

**Example 6.2.3.** For this example, let $u$ and $v$ be the words $u = 23232$ and $v = 323221$ over the alphabet $\mathfrak{A} = \{1, 2, 3, \ldots\}$ with total order given by $1 < 2 < 3 < \cdots$. The CFL factorizations of $u$ and $v$ are $(23, 23, 2)$ and $(3, 23, 2, 2, 1)$, respectively. Thus, using the notations of Theorem 6.2.2, we have $p = 3$, $(a_1, a_2, \ldots, a_p) = (23, 23, 2)$, $q = 5$ and $(b_1, b_2, \ldots, b_q) = (3, 23, 2, 2, 1)$. Thus, Theorem 6.2.2(a) predicts that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8$, where $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8$ are the words $23, 23, 2, 3, 23, 2, 2, 1$ listed in decreasing order (in other words, $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) = (3, 23, 23, 23, 2, 2, 2, 1)$). In other words, Theorem 6.2.2(a) predicts that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is 32323232221. We could verify this by brute force, but this would be laborious since the multiset $u \sqcup\!\sqcup v$ has $\dbinom{5+6}{5} = 462$ elements (with multiplicities). Theorem 6.2.2(b) predicts that this lexicographically

[301] with respect to the total order on $\mathfrak{A}^*$ whose greater-or-equal relation is $\geq$

highest element 32323232221 appears in the multiset $u \sqcup\!\sqcup v$ with a multiplicity of $\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$. This product $\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$ is infinite, but all but finitely many of its factors are 1 and therefore can be omitted; the only factors which are not 1 are those corresponding to Lyndon words $w$ which appear both in the CFL factorization of $u$ and in the CFL factorization of $v$ (since for any other factor, at least one of the numbers $\operatorname{mult}_w u$ or $\operatorname{mult}_w v$ equals 0, and therefore the binomial coefficient $\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$ equals 1). Thus, in order to compute the product $\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$, we only need to multiply these factors. In our example, these are the factors for $w = 23$ and for $w = 2$ (these are the only Lyndon words which appear both in the CFL factorization $(23, 23, 2)$ of $u$ and in the CFL factorization $(3, 23, 2, 2, 1)$ of $v$). So we have

$$\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} = \underbrace{\binom{\operatorname{mult}_{23} u + \operatorname{mult}_{23} v}{\operatorname{mult}_{23} u}}_{=\binom{2+1}{2}=3} \underbrace{\binom{\operatorname{mult}_2 u + \operatorname{mult}_2 v}{\operatorname{mult}_2 u}}_{=\binom{1+2}{1}=3}$$
$$= 3 \cdot 3 = 9.$$

The word 32323232221 must thus appear in the multiset $u \sqcup\!\sqcup v$ with a multiplicity of 9. This, too, could be checked by brute force.

Theorem 6.2.2 (and Theorem 6.2.22 further below, which describes more precisely how the lexicographically highest element of $u \sqcup\!\sqcup v$ emerges by shuffling $u$ and $v$) is fairly close to [177, Theorem 2.2.2] (and will be used for the same purposes), the main difference being that we are talking about the shuffle product of two (not necessarily Lyndon) words, while Radford (and most other authors) study the shuffle product of many Lyndon words.

In order to prove Theorem 6.2.2, we will need to make some stronger statements, for which we first have to introduce some more notation:

**Definition 6.2.4.** (a) If $p$ and $q$ are two integers, then $[p : q]^+$ denotes the interval $\{p+1, p+2, \ldots, q\}$ of $\mathbb{Z}$. Note that $\left|[p : q]^+\right| = q - p$ if $q \geq p$.

(b) If $I$ and $J$ are two nonempty intervals of $\mathbb{Z}$, then we say that $I < J$ if and only if every $i \in I$ and $j \in J$ satisfy $i < j$. This defines a partial order on the set of nonempty intervals of $\mathbb{Z}$. (Roughly speaking, $I < J$ if the interval $I$ ends before $J$ begins.)

(c) If $w$ is a word with $n$ letters (for some $n \in \mathbb{N}$), and $I$ is an interval of $\mathbb{Z}$ such that $I \subset [0 : n]^+$, then $w[I]$ will denote the word $(w_{p+1}, w_{p+2}, \ldots, w_q)$, where $I$ is written in the form $I = [p : q]^+$ with $q \geq p$. Obviously, $\ell(w[I]) = |I| = q - p$. A word of the form $w[I]$ for an interval $I \subset [0 : n]^+$ (equivalently, a word which is a prefix of a suffix of $w$) is called a *factor* of $w$.

(d) Let $\alpha$ be a composition. Then, we define a tuple $\operatorname{intsys} \alpha$ of intervals of $\mathbb{Z}$ as follows: Write $\alpha$ in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ (so that $\ell =$

$\ell(\alpha)$). Then, set $\operatorname{intsys}\alpha = (I_1, I_2, \ldots, I_\ell)$, where

$$I_i = \left[\sum_{k=1}^{i-1} \alpha_k : \sum_{k=1}^{i} \alpha_k\right]^+ \qquad \text{for every } i \in \{1, 2, \ldots, \ell\}.$$

This $\ell$-tuple $\operatorname{intsys}\alpha$ is a tuple of nonempty intervals of $\mathbb{Z}$. This tuple $\operatorname{intsys}\alpha$ is called the *interval system corresponding to* $\alpha$. (This is precisely the $\ell$-tuple $(I_1, I_2, \ldots, I_\ell)$ constructed in Definition 4.3.4.) The length of the tuple $\operatorname{intsys}\alpha$ is $\ell(\alpha)$.

**Example 6.2.5.** (a) We have $[2:4]^+ = \{3,4\}$ and $[3:3]^+ = \varnothing$.

(b) We have $[2:4]^+ < [4:5]^+ < [6:8]^+$, but we have neither $[2:4]^+ < [3:5]^+$ nor $[3:5]^+ < [2:4]^+$.

(c) If $w$ is the word 915352, then $w\left[[0:3]^+\right] = (w_1, w_2, w_3) = 915$ and $w\left[[2:4]^+\right] = (w_3, w_4) = 53$.

(d) If $\alpha$ is the composition $(4,1,4,2,3)$, then the interval system corresponding to $\alpha$ is

$$\begin{aligned}\operatorname{intsys}\alpha &= \left([0:4]^+, [4:5]^+, [5:9]^+, [9:11]^+, [11:14]^+\right)\\ &= (\{1,2,3,4\}, \{5\}, \{6,7,8,9\}, \{10,11\}, \{12,13,14\}).\end{aligned}$$

The following properties of the notions introduced in the preceding definition are easy to check:

*Remark* 6.2.6. (a) If $I$ and $J$ are two nonempty intervals of $\mathbb{Z}$ satisfying $I < J$, then $I$ and $J$ are disjoint.

(b) If $I$ and $J$ are two disjoint nonempty intervals of $\mathbb{Z}$, then either $I < J$ or $J < I$.

(c) Let $\alpha$ be a composition. Write $\alpha$ in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ (so that $\ell = \ell(\alpha)$). The interval system $\operatorname{intsys}\alpha$ can be described as the unique $\ell$-tuple $(I_1, I_2, \ldots, I_\ell)$ of nonempty intervals of $\mathbb{Z}$ satisfying the following three properties:
   - The intervals $I_1$, $I_2$, $\ldots$, $I_\ell$ form a set partition of the set $[0:n]^+$, where $n = |\alpha|$.
   - We have $I_1 < I_2 < \cdots < I_\ell$.
   - We have $|I_i| = \alpha_i$ for every $i \in \{1, 2, \ldots, \ell\}$.

**Exercise 6.2.7.** Prove Remark 6.2.6.

The following two lemmas are collections of more or less trivial consequences of what it means to be an element of $\mathrm{Sh}_{n,m}$ and what it means to be a shuffle:

**Lemma 6.2.8.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\sigma \in \mathrm{Sh}_{n,m}$.*

(a) *If $I$ is an interval of $\mathbb{Z}$ such that $I \subset [0:n+m]^+$, then $\sigma(I) \cap [0:n]^+$ and $\sigma(I) \cap [n:n+m]^+$ are intervals.*

(b) *Let $K$ and $L$ be nonempty intervals of $\mathbb{Z}$ such that $K \subset [0:n]^+$ and $L \subset [0:n]^+$ and $K < L$ and such that $K \cup L$ is an interval. Assume that $\sigma^{-1}(K)$ and $\sigma^{-1}(L)$ are intervals, but $\sigma^{-1}(K) \cup \sigma^{-1}(L)$ is not an interval. Then, there exists a nonempty interval $P \subset [n:n+m]^+$ such that $\sigma^{-1}(P)$, $\sigma^{-1}(K) \cup \sigma^{-1}(P)$ and $\sigma^{-1}(P) \cup \sigma^{-1}(L)$ are intervals and such that $\sigma^{-1}(K) < \sigma^{-1}(P) < \sigma^{-1}(L)$.*

(c) *Lemma 6.2.8(b) remains valid if "$K \subset [0:n]^+$ and $L \subset [0:n]^+$" and "$P \subset [n:n+m]^+$" are replaced by "$K \subset [n:n+m]^+$ and $L \subset [n:n+m]^+$" and "$P \subset [0:n]^+$", respectively.*

**Exercise 6.2.9.** Prove Lemma 6.2.8.

**Lemma 6.2.10.** *Let $u$ and $v$ be two words. Let $n = \ell(u)$ and $m = \ell(v)$. Let $\sigma \in \operatorname{Sh}_{n,m}$.*

(a) *If $I$ is an interval of $\mathbb{Z}$ satisfying either $I \subset [0:n]^+$ or $I \subset [n:n+m]^+$, and if $\sigma^{-1}(I)$ is an interval, then*

$$\left(u \underset{\sigma}{\sqcup\!\sqcup} v\right)\left[\sigma^{-1}(I)\right] = (uv)[I]. \tag{6.2.1}$$

(b) *Assume that $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Let $I \subset [0:n]^+$ and $J \subset [n:n+m]^+$ be two nonempty intervals. Assume that $\sigma^{-1}(I)$ and $\sigma^{-1}(J)$ are also intervals, that $\sigma^{-1}(I) < \sigma^{-1}(J)$, and that $\sigma^{-1}(I) \cup \sigma^{-1}(J)$ is an interval as well. Then, $(uv)[I] \cdot (uv)[J] \geq (uv)[J] \cdot (uv)[I]$.*

(c) *Lemma 6.2.10(b) remains valid if "$I \subset [0:n]^+$ and $J \subset [n:n+m]^+$" is replaced by "$I \subset [n:n+m]^+$ and $J \subset [0:n]^+$".*

**Exercise 6.2.11.** Prove Lemma 6.2.10.

[**Hint:** For (b), show that there exists a $\tau \in \operatorname{Sh}_{n,m}$ such that $u \underset{\tau}{\sqcup\!\sqcup} v$ differs from $u \underset{\sigma}{\sqcup\!\sqcup} v$ only in the order of the subwords $(uv)[I]$ and $(uv)[J]$.]

We are still a few steps away from stating our results in a way that allows comfortably proving Theorem 6.2.2. For the latter aim, we introduce the notion of *$\alpha$-clumping permutations*, and characterize them in two ways:

**Definition 6.2.12.** Let $n \in \mathbb{N}$. Let $\alpha$ be a composition of $n$. Let $\ell = \ell(\alpha)$.

(a) For every set $S$ of positive integers, let $\overrightarrow{S}$ denote the list of all elements of $S$ in increasing order (with each element appearing exactly once). Notice that this list $\overrightarrow{S}$ is a word over the set of positive integers.

(b) For every $\tau \in \mathfrak{S}_\ell$, we define a permutation $\operatorname{iper}(\alpha, \tau) \in \mathfrak{S}_n$ as follows:

The interval system corresponding to $\alpha$ is an $\ell$-tuple of intervals (since $\ell(\alpha) = \ell$); denote this $\ell$-tuple by $(I_1, I_2, \ldots, I_\ell)$. Now, define $\operatorname{iper}(\alpha, \tau)$ to be the permutation in $\mathfrak{S}_n$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\,\overrightarrow{I_{\tau(2)}} \cdots \overrightarrow{I_{\tau(\ell)}}$ (a concatenation of $\ell$ words). This is well-defined[302]; hence, $\operatorname{iper}(\alpha, \tau) \in \mathfrak{S}_n$ is defined.

(c) The interval system corresponding to $\alpha$ is an $\ell$-tuple of intervals (since $\ell(\alpha) = \ell$); denote this $\ell$-tuple by $(I_1, I_2, \ldots, I_\ell)$.

A permutation $\sigma \in \mathfrak{S}_n$ is said to be *$\alpha$-clumping* if every $i \in \{1, 2, \ldots, \ell\}$ has the two properties that:

– the set $\sigma^{-1}(I_i)$ is an interval;

[302] In fact, from the properties of interval systems, we know that the intervals $I_1$, $I_2$, $\ldots$, $I_\ell$ form a set partition of the set $[0:n]^+$. Hence, the intervals $I_{\tau(1)}$, $I_{\tau(2)}$, $\ldots$, $I_{\tau(\ell)}$ form a set partition of the set $[0:n]^+$. As a consequence, the word $\overrightarrow{I_{\tau(1)}}\,\overrightarrow{I_{\tau(2)}} \cdots \overrightarrow{I_{\tau(\ell)}}$ is a permutation of the word $12\ldots n$, and so there exists a permutation in $\mathfrak{S}_n$ which (in one-line notation) is this word, qed.

– the restriction of the map $\sigma^{-1}$ to the interval $I_i$ is increasing.

**Example 6.2.13.** For this example, let $n = 7$ and $\alpha = (2, 1, 3, 1)$. Then, $\ell = \ell(\alpha) = 4$ and $(I_1, I_2, I_3, I_4) = (\{1, 2\}, \{3\}, \{4, 5, 6\}, \{7\})$ (where we are using the notations of Definition 6.2.12). Hence, $\overrightarrow{I_1} = 12$, $\overrightarrow{I_2} = 3$, $\overrightarrow{I_3} = 456$ and $\overrightarrow{I_4} = 7$.

(a) If $\tau \in \mathfrak{S}_\ell = \mathfrak{S}_4$ is the permutation $(2, 3, 1, 4)$, then $\operatorname{iper}(\alpha, \tau)$ is the permutation in $\mathfrak{S}_7$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\overrightarrow{I_{\tau(3)}}\overrightarrow{I_{\tau(4)}} = \overrightarrow{I_2}\,\overrightarrow{I_3}\,\overrightarrow{I_1}\,\overrightarrow{I_4} = 3456127$.

If $\tau \in \mathfrak{S}_\ell = \mathfrak{S}_4$ is the permutation $(3, 1, 4, 2)$, then $\operatorname{iper}(\alpha, \tau)$ is the permutation in $\mathfrak{S}_7$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\overrightarrow{I_{\tau(3)}}\overrightarrow{I_{\tau(4)}} = \overrightarrow{I_3}\,\overrightarrow{I_1}\,\overrightarrow{I_4}\,\overrightarrow{I_2} = 4561273$.

(b) The permutation $\sigma = (3, 7, 4, 5, 6, 1, 2) \in \mathfrak{S}_7$ (given here in one-line notation) is $\alpha$-clumping, because:
  - every $i \in \{1, 2, \ldots, \ell\} = \{1, 2, 3, 4\}$ has the property that $\sigma^{-1}(I_i)$ is an interval (namely, $\sigma^{-1}(I_1) = \sigma^{-1}(\{1, 2\}) = \{6, 7\}$, $\sigma^{-1}(I_2) = \sigma^{-1}(\{3\}) = \{1\}$, $\sigma^{-1}(I_3) = \sigma^{-1}(\{4, 5, 6\}) = \{3, 4, 5\}$ and $\sigma^{-1}(I_4) = \sigma^{-1}(\{7\}) = \{2\}$), and
  - the restrictions of the map $\sigma^{-1}$ to the intervals $I_i$ are increasing (this means that $\sigma^{-1}(1) < \sigma^{-1}(2)$ and $\sigma^{-1}(4) < \sigma^{-1}(5) < \sigma^{-1}(6)$, since the one-element intervals $I_2$ and $I_4$ do not contribute anything to this condition).

Here is a more or less trivial observation:

**Proposition 6.2.14.** *Let $n \in \mathbb{N}$. Let $\alpha$ be a composition of $n$. Let $\ell = \ell(\alpha)$. Write $\alpha$ in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$. The interval system corresponding to $\alpha$ is an $\ell$-tuple of intervals (since $\ell(\alpha) = \ell$); denote this $\ell$-tuple by $(I_1, I_2, \ldots, I_\ell)$. Let $\tau \in \mathfrak{S}_\ell$. Set $\sigma = \operatorname{iper}(\alpha, \tau)$.*

(a) *We have $\sigma^{-1}\left(I_{\tau(j)}\right) = \left[\sum_{k=1}^{j-1} \alpha_{\tau(k)} : \sum_{k=1}^{j} \alpha_{\tau(k)}\right]^+$ for every $j \in \{1, 2, \ldots, \ell\}$.*

(b) *For every $j \in \{1, 2, \ldots, \ell\}$, the restriction of the map $\sigma^{-1}$ to the interval $I_{\tau(j)}$ is increasing.*

(c) *The permutation $\operatorname{iper}(\alpha, \tau)$ is $\alpha$-clumping.*

(d) *Let $i \in \{1, 2, \ldots, \ell - 1\}$. Then, the sets $\sigma^{-1}\left(I_{\tau(i)}\right)$, $\sigma^{-1}\left(I_{\tau(i+1)}\right)$ and $\sigma^{-1}\left(I_{\tau(i)}\right) \cup \sigma^{-1}\left(I_{\tau(i+1)}\right)$ are nonempty intervals. Also, $\sigma^{-1}\left(I_{\tau(i)}\right) < \sigma^{-1}\left(I_{\tau(i+1)}\right)$.*

**Exercise 6.2.15.** Prove Proposition 6.2.14.

**Proposition 6.2.16.** *Let $n \in \mathbb{N}$. Let $\alpha$ be a composition of $n$. Let $\ell = \ell(\alpha)$.*

(a) *Define a map*

$$\begin{aligned} \operatorname{iper}_\alpha : \mathfrak{S}_\ell &\longrightarrow \{\omega \in \mathfrak{S}_n \mid \omega \text{ is } \alpha\text{-clumping}\}, \\ \tau &\longmapsto \operatorname{iper}(\alpha, \tau) \end{aligned}$$

[303]. *This map $\operatorname{iper}_\alpha$ is bijective.*

[303] This map is well-defined because for every $\tau \in \mathfrak{S}_\ell$, the permutation $\operatorname{iper}(\alpha, \tau)$ is $\alpha$-clumping (according to Proposition 6.2.14(c)).

(b) *Let $\sigma \in \mathfrak{S}_n$ be an $\alpha$-clumping permutation. Then, there exists a unique $\tau \in \mathfrak{S}_\ell$ satisfying $\sigma = \operatorname{iper}(\alpha, \tau)$.*

**Exercise 6.2.17.** Prove Proposition 6.2.16.

Next, we recall that the concatenation $\alpha \cdot \beta$ of two compositions $\alpha$ and $\beta$ is defined in the same way as the concatenation of two words; if we regard compositions as words over the alphabet $\{1, 2, 3, \ldots\}$, then the concatenation $\alpha \cdot \beta$ of two compositions $\alpha$ and $\beta$ **is** the concatenation $\alpha\beta$ of the words $\alpha$ and $\beta$. Thus, we are going to write $\alpha\beta$ for the concatenation $\alpha \cdot \beta$ of two compositions $\alpha$ and $\beta$ from now on.

**Proposition 6.2.18.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\alpha$ be a composition of $n$, and $\beta$ be a composition of $m$. Let $p = \ell(\alpha)$ and $q = \ell(\beta)$. Let $\tau \in \mathfrak{S}_{p+q}$. Notice that* $\operatorname{iper}(\alpha\beta, \tau) \in \mathfrak{S}_{n+m}$ *(since $\alpha\beta$ is a composition of $n+m$ having length $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta) = p+q$). Then, $\tau \in \operatorname{Sh}_{p,q}$ if and only if* $\operatorname{iper}(\alpha\beta, \tau) \in \operatorname{Sh}_{n,m}$.

**Exercise 6.2.19.** Prove Proposition 6.2.18.

Here is one more simple fact:

**Lemma 6.2.20.** *Let $u$ and $v$ be two words. Let $n = \ell(u)$ and $m = \ell(v)$. Let $\alpha$ be a composition of $n$, and let $\beta$ be a composition of $m$. Let $p = \ell(\alpha)$ and $q = \ell(\beta)$. The concatenation $\alpha\beta$ is a composition of $n+m$ having length $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta) = p+q$. Thus, the interval system corresponding to $\alpha\beta$ is a $(p+q)$-tuple of intervals which covers $[0 : n+m]^+$. Denote this $(p+q)$-tuple by $(I_1, I_2, \ldots, I_{p+q})$.*

*Let $\tau \in \operatorname{Sh}_{p,q}$. Set $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Then,*

$$u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right].$$

**Exercise 6.2.21.** Prove Lemma 6.2.20.

Having these notations and trivialities in place, we can say a bit more about the lexicographically highest element of a shuffle product than what was said in Theorem 6.2.2:

**Theorem 6.2.22.** *Let $u$ and $v$ be two words. Let $n = \ell(u)$ and $m = \ell(v)$.*

*Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of $u$. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of $v$.*

*Let $\alpha$ be the $p$-tuple $(\ell(a_1), \ell(a_2), \ldots, \ell(a_p))$. Then, $\alpha$ is a composition*[304] *of length $p$ and size $\sum_{k=1}^{p} \ell(a_k) = \ell\left(\underbrace{a_1 a_2 \cdots a_p}_{=u}\right) = \ell(u) = n$.*

*Let $\beta$ be the $q$-tuple $(\ell(b_1), \ell(b_2), \ldots, \ell(b_q))$. Then, $\beta$ is a composition of length $q$ and size $\sum_{k=1}^{q} \ell(b_k) = m$.* [305]

*Now, $\alpha$ is a composition of length $p$ and size $n$, and $\beta$ is a composition of length $q$ and size $m$. Thus, the concatenation $\alpha\beta$ of these two tuples is a composition of length $p+q$ and size $n+m$. The interval system corresponding to this composition $\alpha\beta$ is a $(p+q)$-tuple (since said composition has length $p+q$); denote this $(p+q)$-tuple by $(I_1, I_2, \ldots, I_{p+q})$.*

[304] since Lyndon words are nonempty, and thus $\ell(a_i) > 0$ for every $i$

[305] The proof of this is the same as the proof of the fact that $\alpha$ is a composition of length $p$ and size $\sum_{k=1}^{p} \ell(\alpha_k) = n$.

(a) *If* $\tau \in \operatorname{Sh}_{p,q}$ *satisfies* $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$, *and if we set* $\sigma = \operatorname{iper}(\alpha\beta, \tau)$*, then* $\sigma \in \operatorname{Sh}_{n,m}$*, and the word* $u \underset{\sigma}{\sqcup\!\sqcup} v$ *is the lexicographically highest element of the multiset* $u \sqcup\!\sqcup v$.

(b) *Let* $\sigma \in \operatorname{Sh}_{n,m}$ *be a permutation such that* $u \underset{\sigma}{\sqcup\!\sqcup} v$ *is the lexicographically highest element of the multiset* $u \sqcup\!\sqcup v$*. Then, there exists a unique permutation* $\tau \in \operatorname{Sh}_{p,q}$ *satisfying* $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ *and* $\sigma = \operatorname{iper}(\alpha\beta, \tau)$.

*Proof.* Before we step to the actual proof, we need to make some preparation. First of all, $(I_1, I_2, \ldots, I_{p+q})$ is the interval system corresponding to the composition $\alpha\beta$. In other words,

$$(I_1, I_2, \ldots, I_{p+q}) = \operatorname{intsys}(\alpha\beta). \tag{6.2.2}$$

But since $\alpha = (\ell(a_1), \ell(a_2), \ldots, \ell(a_p))$ and $\beta = (\ell(b_1), \ell(b_2), \ldots, \ell(b_q))$, we have

$$\alpha\beta = (\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q)).$$

Thus, (6.2.2) rewrites as

$$(I_1, I_2, \ldots, I_{p+q}) = \operatorname{intsys}(\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q)).$$

By the definition of $\operatorname{intsys}(\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q))$, we thus have

$$I_i = \left[\sum_{k=1}^{i-1} \ell(a_k) : \sum_{k=1}^{i} \ell(a_k)\right]^+ \qquad \text{for every } i \in \{1, 2, \ldots, p\},$$

and besides

$$I_{p+j} = \left[n + \sum_{k=1}^{j-1} \ell(b_k) : n + \sum_{k=1}^{j} \ell(b_k)\right]^+ \qquad \text{for every } j \in \{1, 2, \ldots, q\}$$

(since $\sum_{k=1}^{p} \ell(a_k) = n$). Moreover, Remark 6.2.6(c) shows that $(I_1, I_2, \ldots, I_{p+q})$ is a $(p+q)$-tuple of nonempty intervals of $\mathbb{Z}$ and satisfies the following three properties:

- The intervals $I_1$, $I_2$, …, $I_{p+q}$ form a set partition of the set $[0 : n+m]^+$.
- We have $I_1 < I_2 < \cdots < I_{p+q}$.
- We have $|I_i| = \ell(a_i)$ for every $i \in \{1, 2, \ldots, p\}$ and $|I_{p+j}| = \ell(b_j)$ for every $j \in \{1, 2, \ldots, q\}$.

Of course, every $i \in \{1, 2, \ldots, p\}$ satisfies

$$I_i \subset [0 : n]^+ \text{ and } (uv)[I_i] = u[I_i] = a_i. \tag{6.2.3}$$

Meanwhile, every $i \in \{p+1, p+2, \ldots, p+q\}$ satisfies

$$I_i \subset [n : n+m]^+ \text{ and } (uv)[I_i] = v[I_i - n] = b_{i-p} \tag{6.2.4}$$

(where $I_i - n$ denotes the interval $\{k - n \mid k \in I_i\}$). We thus see that

$$(uv)[I_i] \text{ is a Lyndon word for every } i \in \{1, 2, \ldots, p+q\} \tag{6.2.5}$$

[306].

By the definition of a CFL factorization, we have $a_1 \geq a_2 \geq \cdots \geq a_p$ and $b_1 \geq b_2 \geq \cdots \geq b_q$.

[306] Indeed, when $i \leq p$, this follows from (6.2.3) and the fact that $a_i$ is Lyndon; whereas in the other case, this follows from (6.2.4) and the fact that $b_{i-p}$ is Lyndon.

We have $\sigma \in \operatorname{Sh}_{n,m}$, so that $\sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n)$ and $\sigma^{-1}(n+1) < \sigma^{-1}(n+2) < \cdots < \sigma^{-1}(n+m)$. In other words, the restriction of the map $\sigma^{-1}$ to the interval $[0:n]^+$ is strictly increasing, and so is the restriction of the map $\sigma^{-1}$ to the interval $[n:n+m]^+$.

(b) We will first show that

$$\begin{array}{l} \text{if } J \subset [0:n]^+ \text{ is an interval} \\ \text{such that the word } (uv)[J] \text{ is Lyndon,} \\ \text{then } \sigma^{-1}(J) \text{ is an interval.} \end{array} \tag{6.2.6}$$

*Proof of (6.2.6):* We will prove (6.2.6) by strong induction over $|J|$.

So, fix some $N \in \mathbb{N}$. Assume (as the induction hypothesis) that (6.2.6) has been proven whenever $|J| < N$. We now need to prove (6.2.6) when $|J| = N$.

Let $J \subset [0:n]^+$ be an interval such that the word $(uv)[J]$ is Lyndon and such that $|J| = N$. We have to prove that $\sigma^{-1}(J)$ is an interval. This is obvious if $|J| = 1$ (because in this case, $\sigma^{-1}(J)$ is a one-element set, thus trivially an interval). Hence, we WLOG assume that we don't have $|J| = 1$. We also don't have $|J| = 0$, because $(uv)[J]$ has to be Lyndon (and the empty word is not). So we have $|J| > 1$. Now, $\ell((uv)[J]) = |J| > 1$, and thus $(uv)[J]$ is a Lyndon word of length $> 1$. Let $v'$ be the (lexicographically) smallest nonempty **proper** suffix of $(uv)[J]$. Since $v'$ is a proper suffix of $w$, there exists a nonempty $u' \in \mathfrak{A}^*$ such that $(uv)[J] = u'v'$. Consider this $u'$.

Now, Theorem 6.1.30(a) (applied to $(uv)[J]$, $u'$ and $v'$ instead of $w$, $u$ and $v$) yields that the words $u'$ and $v'$ are Lyndon. Also, Theorem 6.1.30(b) (applied to $(uv)[J]$, $u'$ and $v'$ instead of $w$, $u$ and $v$) yields that $u' < (uv)[J] < v'$.

But from the fact that $(uv)[J] = u'v'$ with $u'$ and $v'$ both being nonempty, it becomes immediately clear that we can write $J$ as a union of two disjoint nonempty intervals $K$ and $L$ such that $K < L$, $u' = (uv)[K]$ and $v' = (uv)[L]$. Consider these $K$ and $L$. The intervals $K$ and $L$ are nonempty and have their sizes add up to $|J|$ (since they are disjoint and their union is $J$), and hence both must have size smaller than $|J| = N$. So $K \subset [0:n]^+$ is an interval of size $|K| < N$ having the property that $(uv)[K]$ is Lyndon (since $(uv)[K] = u'$ is Lyndon). Thus, we can apply (6.2.6) to $K$ instead of $J$ (because of the induction hypothesis). As a result, we conclude that $\sigma^{-1}(K)$ is an interval. Similarly, we can apply (6.2.6) to $L$ instead of $J$ (we know that $(uv)[L]$ is Lyndon since $(uv)[L] = v'$), and learn that $\sigma^{-1}(L)$ is an interval. The intervals $\sigma^{-1}(K)$ and $\sigma^{-1}(L)$ are both nonempty (since $K$ and $L$ are nonempty), and their union is $\sigma^{-1}(J)$ (because the union of $K$ and $L$ is $J$). The nonempty intervals $K$ and $L$ both are subsets of $[0:n]^+$ (since their union is $J \subset [0:n]^+$), and their union $K \cup L$ is an interval (since their union $K \cup L$ is $J$, and we know that $J$ is an interval).

Now, assume (for the sake of contradiction) that $\sigma^{-1}(J)$ is not an interval. Since $J$ is the union of $K$ and $L$, we have $J = K \cup L$ and thus $\sigma^{-1}(J) = \sigma^{-1}(K \cup L) = \sigma^{-1}(K) \cup \sigma^{-1}(L)$ (since $\sigma$ is a bijection). Therefore, $\sigma^{-1}(K) \cup \sigma^{-1}(L)$ is not an interval (since $\sigma^{-1}(J)$ is not an interval). Thus, Lemma 6.2.8(b) yields that there exists a nonempty interval

$P \subset [n : n+m]^+$ such that $\sigma^{-1}(P)$, $\sigma^{-1}(K) \cup \sigma^{-1}(P)$ and $\sigma^{-1}(P) \cup \sigma^{-1}(L)$ are intervals and such that $\sigma^{-1}(K) < \sigma^{-1}(P) < \sigma^{-1}(L)$. Consider this $P$. Since $P$ is nonempty, we have $|P| \neq 0$.

Lemma 6.2.10(b) (applied to $K$ and $P$ instead of $I$ and $J$) yields

$$(uv)[K] \cdot (uv)[P] \geq (uv)[P] \cdot (uv)[K]. \tag{6.2.7}$$

Since $(uv)[K] = u'$, this rewrites as

$$u' \cdot (uv)[P] \geq (uv)[P] \cdot u'. \tag{6.2.8}$$

But Lemma 6.2.10(c) (applied to $P$ and $L$ instead of $I$ and $J$) yields

$$(uv)[P] \cdot (uv)[L] \geq (uv)[L] \cdot (uv)[P]. \tag{6.2.9}$$

Since $(uv)[L] = v'$, this rewrites as

$$(uv)[P] \cdot v' \geq v' \cdot (uv)[P]. \tag{6.2.10}$$

Recall also that $u' < v'$, and that both words $u'$ and $v'$ are Lyndon. Now, Corollary 6.1.17 (applied to $u'$, $v'$ and $(uv)[P]$ instead of $u$, $v$ and $z$) yields that $(uv)[P]$ is the empty word (because of (6.2.8) and (6.2.10)), so that $\ell((uv)[P]) = 0$. This contradicts $\ell((uv)[P]) = |P| \neq 0$. This contradiction shows that our assumption (that $\sigma^{-1}(J)$ is not an interval) was wrong. Hence, $\sigma^{-1}(J)$ is an interval. This completes the induction step, and thus (6.2.6) is proven.

Similarly to (6.2.6), we can show that

$$\begin{aligned} &\text{if } J \subset [n : n+m]^+ \text{ is an interval} \\ &\text{such that the word } (uv)[J] \text{ is Lyndon,} \\ &\text{then } \sigma^{-1}(J) \text{ is an interval.} \end{aligned} \tag{6.2.11}$$

Now, let $i \in \{1, 2, \ldots, p+q\}$ be arbitrary. We are going to prove that

$$\sigma^{-1}(I_i) \text{ is an interval.} \tag{6.2.12}$$

*Proof of (6.2.12):* We must be in one of the following two cases:

*Case 1:* We have $i \in \{1, 2, \ldots, p\}$.

*Case 2:* We have $i \in \{p+1, p+2, \ldots, p+q\}$.

Let us first consider Case 1. In this case, we have $i \in \{1, 2, \ldots, p\}$. Thus, $I_i \subset [0 : n]^+$ (by (6.2.3)). Also, (6.2.3) yields that $(uv)[I_i] = a_i$ is a Lyndon word. Hence, (6.2.6) (applied to $J = I_i$) yields that $\sigma^{-1}(I_i)$ is an interval. Thus, (6.2.12) is proven in Case 1.

Similarly, we can prove (6.2.12) in Case 2, using (6.2.4) and (6.2.11) instead of (6.2.3) and (6.2.6), respectively. Hence, (6.2.12) is proven.

So we know that $\sigma^{-1}(I_i)$ is an interval. But we also know that either $I_i \subset [0 : n]^+$ or $I_i \subset [n : n+m]^+$ (depending on whether $i \leq p$ or $i > p$). As a consequence, the restriction of the map $\sigma^{-1}$ to the interval $I_i$ is increasing (because the restriction of the map $\sigma^{-1}$ to the interval $[0 : n]^+$ is strictly increasing, and so is the restriction of the map $\sigma^{-1}$ to the interval $[n : n+m]^+$).

Now, let us forget that we fixed $i$. We thus have shown that every $i \in \{1, 2, \ldots, p+q\}$ has the two properties that:

- the set $\sigma^{-1}(I_i)$ is an interval;
- the restriction of the map $\sigma^{-1}$ to the interval $I_i$ is increasing.

In other words, the permutation $\sigma$ is $(\alpha\beta)$-clumping (since $(I_1, I_2, \ldots, I_{p+q})$ is the interval system corresponding to the composition $\alpha\beta$). Hence, Proposition 6.2.16(b) (applied to $n+m$, $\alpha\beta$ and $p+q$ instead of $n$, $\alpha$ and $\ell$) shows that there exists a unique $\tau \in \mathfrak{S}_{p+q}$ satisfying $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Thus, the uniqueness part of Theorem 6.2.22(b) (i.e., the claim that the $\tau$ in Theorem 6.2.22(b) is unique if it exists) is proven.

It now remains to prove the existence part of Theorem 6.2.22(b), i.e., to prove that there exists at least one permutation $\tau \in \mathrm{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. We already know that there exists a unique $\tau \in \mathfrak{S}_{p+q}$ satisfying $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Consider this $\tau$. We will now prove that $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\tau \in \mathrm{Sh}_{p,q}$. Once this is done, the existence part of Theorem 6.2.22(b) will be proven, and thus the proof of Theorem 6.2.22(b) will be complete.

Proposition 6.2.18 yields that $\tau \in \mathrm{Sh}_{p,q}$ if and only if $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$. Since we know that $\operatorname{iper}(\alpha\beta, \tau) = \sigma \in \mathrm{Sh}_{n,m}$, we thus conclude that $\tau \in \mathrm{Sh}_{p,q}$. The only thing that remains to be proven now is that

$$(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.13}$$

*Proof of (6.2.13):* We have $\tau \in \mathrm{Sh}_{p,q}$. In other words, $\tau^{-1}(1) < \tau^{-1}(2) < \cdots < \tau^{-1}(p)$ and $\tau^{-1}(p+1) < \tau^{-1}(p+2) < \cdots < \tau^{-1}(p+q)$. In other words, the restriction of the map $\tau^{-1}$ to the interval $[0:p]^+$ is strictly increasing, and so is the restriction of the map $\tau^{-1}$ to the interval $[p:p+q]^+$.

Let $i \in \{1, 2, \ldots, p+q-1\}$. We will show that

$$(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]. \tag{6.2.14}$$

Clearly, both $\tau(i)$ and $\tau(i+1)$ belong to $\{1, 2, \ldots, p+q\} = \{1, 2, \ldots, p\} \cup \{p+1, p+2, \ldots, p+q\}$. Thus, we must be in one of the following four cases:

*Case 1:* We have

$$\tau(i) \in \{1, 2, \ldots, p\} \text{ and } \tau(i+1) \in \{1, 2, \ldots, p\}.$$

*Case 2:* We have

$$\tau(i) \in \{1, 2, \ldots, p\} \text{ and } \tau(i+1) \in \{p+1, p+2, \ldots, p+q\}.$$

*Case 3:* We have

$$\tau(i) \in \{p+1, p+2, \ldots, p+q\} \text{ and } \tau(i+1) \in \{1, 2, \ldots, p\}.$$

*Case 4:* We have

$$\tau(i) \in \{p+1, p+2, \ldots, p+q\} \text{ and } \tau(i+1) \in \{p+1, p+2, \ldots, p+q\}.$$

Let us consider Case 1 first. In this case, we have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{1, 2, \ldots, p\}$. From the fact that the restriction of the map $\tau^{-1}$ to the interval $[0:p]^+$ is strictly increasing, we can easily deduce $\tau(i) < \tau(i+1)$ [307]. Therefore, $a_{\tau(i)} \geq a_{\tau(i+1)}$ (since $a_1 \geq a_2 \geq \cdots \geq a_p$).

[307] *Proof.* Assume the contrary. Then, $\tau(i) \geq \tau(i+1)$. Since both $\tau(i)$ and $\tau(i+1)$ belong to $\{1, 2, \ldots, p\} = [0:p]^+$, this yields $\tau^{-1}(\tau(i)) \geq \tau^{-1}(\tau(i+1))$ (since the restriction of the map $\tau^{-1}$ to the interval $[0:p]^+$ is strictly increasing), which contradicts $\tau^{-1}(\tau(i)) = i < i+1 = \tau^{-1}(\tau(i+1))$. This contradiction proves the assumption wrong, qed.

But $(uv)\left[I_{\tau(i)}\right] = a_{\tau(i)}$ (by (6.2.3), applied to $\tau(i)$ instead of $i$) and $(uv)\left[I_{\tau(i+1)}\right] = a_{\tau(i+1)}$ (similarly). In view of these equalities, the inequality $a_{\tau(i)} \geq a_{\tau(i+1)}$ rewrites as $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$. Thus, (6.2.14) is proven in Case 1.

Similarly, we can show (6.2.14) in Case 4 (observing that $(uv)\left[I_{\tau(i)}\right] = b_{\tau(i)-p}$ and $(uv)\left[I_{\tau(i+1)}\right] = b_{\tau(i+1)-p}$ in this case).

Let us now consider Case 2. In this case, we have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$. From $\tau(i) \in \{1, 2, \ldots, p\}$, we conclude that $I_{\tau(i)} \subset [0:n]^{+}$. From $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$, we conclude that $I_{\tau(i+1)} \subset [n:n+m]^{+}$. The intervals $I_{\tau(i)}$ and $I_{\tau(i+1)}$ are clearly nonempty.

Proposition 6.2.14(d) (applied to $n+m$, $\alpha\beta$, $p+q$ and $(I_1, I_2, \ldots, I_{p+q})$ instead of $n$, $\alpha$, $\ell$ and $(I_1, I_2, \ldots, I_\ell)$) yields that the sets $\sigma^{-1}\left(I_{\tau(i)}\right)$, $\sigma^{-1}\left(I_{\tau(i+1)}\right)$ and $\sigma^{-1}\left(I_{\tau(i)}\right) \cup \sigma^{-1}\left(I_{\tau(i+1)}\right)$ are nonempty intervals, and that we have $\sigma^{-1}\left(I_{\tau(i)}\right) < \sigma^{-1}\left(I_{\tau(i+1)}\right)$. Hence, Lemma 6.2.10(b) (applied to $I = I_{\tau(i)}$ and $J = I_{\tau(i+1)}$) yields

$$(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right].$$

But $(uv)\left[I_{\tau(i)}\right]$ and $(uv)\left[I_{\tau(i+1)}\right]$ are Lyndon words (as a consequence of (6.2.5)). Thus, Proposition 6.1.18 (applied to $(uv)\left[I_{\tau(i)}\right]$ and $(uv)\left[I_{\tau(i+1)}\right]$ instead of $u$ and $v$) shows that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$ if and only if $(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right]$. Since we know that $(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right]$ holds, we thus conclude that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$. Thus, (6.2.14) is proven in Case 2.

The proof of (6.2.14) in Case 3 is analogous to that in Case 2 (the main difference being that Lemma 6.2.10(c) is used in lieu of Lemma 6.2.10(b)).

Thus, (6.2.14) is proven in all possible cases. So we always have (6.2.14). In other words, $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$.

Now, forget that we fixed $i$. We hence have shown that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$ for all $i \in \{1, 2, \ldots, p+q-1\}$. This proves (6.2.13), and thus completes our proof of Theorem 6.2.22(b).

(a) Let $\tau \in \mathrm{Sh}_{p,q}$ be such that

$$(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.15}$$

Set $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Then, Proposition 6.2.18 yields that $\tau \in \mathrm{Sh}_{p,q}$ if and only if $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$. Since we know that $\tau \in \mathrm{Sh}_{p,q}$, we can deduce from this that $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$, so that $\sigma = \operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$.

It remains to prove that the word $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$.

It is clear that the multiset $u \sqcup\!\sqcup v$ has **some** lexicographically highest element. This element has the form $u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v$ for some $\widetilde{\sigma} \in \mathrm{Sh}_{n,m}$ (because any element of this multiset has such a form). Consider this $\widetilde{\sigma}$. Theorem 6.2.22(b) (applied to $\widetilde{\sigma}$ instead of $\sigma$) yields that there exists a unique permutation $\widetilde{\tau} \in \mathrm{Sh}_{p,q}$ satisfying $(uv)\left[I_{\widetilde{\tau}(1)}\right] \geq (uv)\left[I_{\widetilde{\tau}(2)}\right] \geq \cdots \geq (uv)\left[I_{\widetilde{\tau}(p+q)}\right]$ and $\widetilde{\sigma} = \operatorname{iper}(\alpha\beta, \widetilde{\tau})$. (What we call $\widetilde{\tau}$ here is what has been called $\tau$ in Theorem 6.2.22(b).)

Now, the chain of inequalities

$$(uv)\left[I_{\widetilde{\tau}(1)}\right] \geq (uv)\left[I_{\widetilde{\tau}(2)}\right] \geq \cdots \geq (uv)\left[I_{\widetilde{\tau}(p+q)}\right]$$

shows that the list $\left((uv)\left[I_{\widetilde{\tau}(1)}\right],(uv)\left[I_{\widetilde{\tau}(2)}\right],\ldots,(uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right)$ is the result of sorting the list $((uv)[I_1],(uv)[I_2],\ldots,(uv)[I_{p+q}])$ in decreasing order. But the chain of inequalities (6.2.15) shows that the list $\left((uv)\left[I_{\tau(1)}\right],(uv)\left[I_{\tau(2)}\right],\ldots,(uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting the same list $((uv)[I_1],(uv)[I_2],\ldots,(uv)[I_{p+q}])$ in decreasing order. So each of the two lists $\left((uv)\left[I_{\widetilde{\tau}(1)}\right],(uv)\left[I_{\widetilde{\tau}(2)}\right],\ldots,(uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right)$ and $\left((uv)\left[I_{\tau(1)}\right],(uv)\left[I_{\tau(2)}\right],\ldots,(uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting one and the same list $((uv)[I_1],(uv)[I_2],\ldots,(uv)[I_{p+q}])$ in decreasing order. Since the result of sorting a given list in decreasing order is unique, this yields

$$\begin{aligned}&\left((uv)\left[I_{\widetilde{\tau}(1)}\right],(uv)\left[I_{\widetilde{\tau}(2)}\right],\ldots,(uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right)\\&=\left((uv)\left[I_{\tau(1)}\right],(uv)\left[I_{\tau(2)}\right],\ldots,(uv)\left[I_{\tau(p+q)}\right]\right).\end{aligned}$$

Hence,

$$\begin{aligned}&(uv)\left[I_{\widetilde{\tau}(1)}\right]\cdot(uv)\left[I_{\widetilde{\tau}(2)}\right]\cdot\cdots\cdot(uv)\left[I_{\widetilde{\tau}(p+q)}\right]\\&=(uv)\left[I_{\tau(1)}\right]\cdot(uv)\left[I_{\tau(2)}\right]\cdot\cdots\cdot(uv)\left[I_{\tau(p+q)}\right].\end{aligned}\tag{6.2.16}$$

But Lemma 6.2.20 yields

$$u \underset{\sigma}{\sqcup\!\sqcup} v=(uv)\left[I_{\tau(1)}\right]\cdot(uv)\left[I_{\tau(2)}\right]\cdot\cdots\cdot(uv)\left[I_{\tau(p+q)}\right].\tag{6.2.17}$$

Meanwhile, Lemma 6.2.20 (applied to $\widetilde{\tau}$ and $\widetilde{\sigma}$ instead of $\tau$ and $\sigma$) yields

$$\begin{aligned}u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v&=(uv)\left[I_{\widetilde{\tau}(1)}\right]\cdot(uv)\left[I_{\widetilde{\tau}(2)}\right]\cdot\cdots\cdot(uv)\left[I_{\widetilde{\tau}(p+q)}\right]\\&=(uv)\left[I_{\tau(1)}\right]\cdot(uv)\left[I_{\tau(2)}\right]\cdot\cdots\cdot(uv)\left[I_{\tau(p+q)}\right]\qquad(\text{by }(6.2.16))\\&=u \underset{\sigma}{\sqcup\!\sqcup} v\qquad(\text{by }(6.2.17)).\end{aligned}$$

Thus, $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ (since we know that $u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$). This proves Theorem 6.2.22(a). □

Now, in order to prove Theorem 6.2.2, we record a very simple fact about counting shuffles:

**Proposition 6.2.23.** *Let $p \in \mathbb{N}$ and $q \in \mathbb{N}$. Let $\mathfrak{W}$ be a totally ordered set, and let $h : \{1,2,\ldots,p+q\} \to \mathfrak{W}$ be a map. Assume that $h(1) \geq h(2) \geq \cdots \geq h(p)$ and $h(p+1) \geq h(p+2) \geq \cdots \geq h(p+q)$.*

*For every $w \in \mathfrak{W}$, let $\mathfrak{a}(w)$ denote the number of all $i \in \{1,2,\ldots,p\}$ satisfying $h(i)=w$, and let $\mathfrak{b}(w)$ denote the number of all $i \in \{p+1,p+2,\ldots,p+q\}$ satisfying $h(i)=w$.*

*Then, the number of $\tau \in \operatorname{Sh}_{p,q}$ satisfying $h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))$ is $\prod_{w\in\mathfrak{W}}\dbinom{\mathfrak{a}(w)+\mathfrak{b}(w)}{\mathfrak{a}(w)}$. (Of course, all but finitely many factors of this product are 1.)*

**Exercise 6.2.24.** Prove Proposition 6.2.23.

*Proof of Theorem 6.2.2.* Let $n=\ell(u)$ and $m=\ell(v)$. Define $\alpha$, $\beta$ and $(I_1,I_2,\ldots,I_{p+q})$ as in Theorem 6.2.22.

Since $(a_1,a_2,\ldots,a_p)$ is the CFL factorization of $u$, we have $a_1 \geq a_2 \geq \cdots \geq a_p$ and $a_1a_2\cdots a_p=u$. Similarly, $b_1 \geq b_2 \geq \cdots \geq b_q$ and $b_1b_2\cdots b_q=v$.

From (6.2.3), we see that $(uv)[I_i] = a_i$ for every $i \in \{1, 2, \ldots, p\}$. From (6.2.4), we see that $(uv)[I_i] = b_{i-p}$ for every $i \in \{p+1, p+2, \ldots, p+q\}$. Combining these two equalities, we obtain

$$(uv)[I_i] = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} \tag{6.2.18}$$

for every $i \in \{1, 2, \ldots, p+q\}$. In other words,

$$\begin{aligned} &((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}]) \\ &= (a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q). \end{aligned} \tag{6.2.19}$$

(a) Let $z$ be the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. We must prove that $z = c_1 c_2 \cdots c_{p+q}$.

Since $z \in u \sqcup\!\sqcup v$, we can write $z$ in the form $u \underset{\sigma}{\sqcup\!\sqcup} v$ for some $\sigma \in \operatorname{Sh}_{n,m}$ (since we can write any element of $u \sqcup\!\sqcup v$ in this form). Consider this $\sigma$. Then, $u \underset{\sigma}{\sqcup\!\sqcup} v = z$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Hence, Theorem 6.2.22(b) yields that there exists a unique permutation $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Consider this $\tau$.

Now, $\tau \in \operatorname{Sh}_{p,q} \subset \mathfrak{S}_{p+q}$ is a permutation, and thus the list $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is a rearrangement of the list $((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}])$. Due to (6.2.19), this rewrites as follows: The list $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is a rearrangement of the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$. Hence, $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order (since $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$). But since the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order is $(c_1, c_2, \ldots, c_{p+q})$, this becomes

$$\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right) = (c_1, c_2, \ldots, c_{p+q}).$$

Hence,

$$(uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right] = c_1 \cdot c_2 \cdot \cdots \cdot c_{p+q}.$$

But Lemma 6.2.20 yields

$$u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right].$$

Altogether, we have

$$\begin{aligned} z = u \underset{\sigma}{\sqcup\!\sqcup} v &= (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right] \\ &= c_1 \cdot c_2 \cdot \cdots \cdot c_{p+q} = c_1 c_2 \cdots c_{p+q}. \end{aligned}$$

This proves Theorem 6.2.2(a).

(b) Recall that $u \sqcup\!\sqcup v = \left\{ u \underset{\sigma}{\sqcup\!\sqcup} v \ : \ \sigma \in \operatorname{Sh}_{n,m} \right\}_{\text{multiset}}$. Hence,

$$\begin{aligned} &(\text{the multiplicity with which the lexicographically highest element} \\ &\qquad \text{of the multiset } u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v) \\ &= \Big(\text{the number of all } \sigma \in \operatorname{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the} \\ &\qquad \text{lexicographically highest element of the multiset } u \sqcup\!\sqcup v\Big). \end{aligned}$$

However, for a given $\sigma \in \operatorname{Sh}_{n,m}$, we know that $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ if and only if $\sigma$ can be written in the form $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ for some $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$. [308] Hence,

$$\begin{aligned}
&\Big(\text{the number of all } \sigma \in \operatorname{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the} \\
&\qquad \text{lexicographically highest element of the multiset } u \sqcup\!\sqcup v) \\
&= (\text{the number of all } \sigma \in \operatorname{Sh}_{n,m} \text{ which can be written in} \\
&\qquad \text{the form } \sigma = \operatorname{iper}(\alpha\beta, \tau) \text{ for some } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]\big) \\
&= (\text{the number of all } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]\big)
\end{aligned}$$

(because if a $\sigma \in \operatorname{Sh}_{n,m}$ can be written in the form $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ for some $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$, then $\sigma$ can be written **uniquely** in this form[309]). Thus,

$$\begin{aligned}
&(\text{the multiplicity with which the lexicographically highest element} \\
&\qquad \text{of the multiset } u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v) \\
&= \Big(\text{the number of all } \sigma \in \operatorname{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the} \\
&\qquad \text{lexicographically highest element of the multiset } u \sqcup\!\sqcup v) \\
&= (\text{the number of all } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]\big). \qquad (6.2.20)
\end{aligned}$$

Now, define a map $h : \{1, 2, \ldots, p+q\} \to \mathfrak{L}$ by

$$h(i) = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} \qquad \text{for every } i \in \{1, 2, \ldots, p+q\}.$$

Then, $h(1) \geq h(2) \geq \cdots \geq h(p)$ (because this is just a rewriting of $a_1 \geq a_2 \geq \cdots \geq a_p$) and $h(p+1) \geq h(p+2) \geq \cdots \geq h(p+q)$ (since this is just a rewriting of $b_1 \geq b_2 \geq \cdots \geq b_q$). For every $w \in \mathfrak{L}$, the number of

[308] In fact, the "if" part of this assertion follows from Theorem 6.2.22(a), whereas its "only if" part follows from Theorem 6.2.22(b).

[309] *Proof.* Let $\sigma \in \operatorname{Sh}_{n,m}$ be such that $\sigma$ can be written in the form $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ for some $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$. Then, the word $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ (according to Theorem 6.2.22(a)). Hence, there exists a unique permutation $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ (according to Theorem 6.2.22(b)). In other words, $\sigma$ can be written **uniquely** in the form $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ for some $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$, qed.

all $i \in \{1, 2, \ldots, p\}$ satisfying $h(i) = w$ is

$$\begin{aligned}
&\left|\left\{ i \in \{1, 2, \ldots, p\} \mid \underbrace{h(i)}_{=a_i} = w \right\}\right| \\
&= |\{i \in \{1, 2, \ldots, p\} \mid a_i = w\}| \\
&= (\text{the number of terms in the list } (a_1, a_2, \ldots, a_p) \text{ which are equal to } w) \\
&= (\text{the number of terms in the CFL factorization of } u \text{ which are equal to } w) \\
&\qquad (\text{since the list } (a_1, a_2, \ldots, a_p) \text{ is the CFL factorization of } u) \\
&= \operatorname{mult}_w u
\end{aligned}$$

(because $\operatorname{mult}_w u$ is defined as the number of terms in the CFL factorization of $u$ which are equal to $w$). Similarly, for every $w \in \mathfrak{L}$, the number of all $i \in \{p+1, p+2, \ldots, p+q\}$ satisfying $h(i) = w$ equals $\operatorname{mult}_w v$. Thus, we can apply Proposition 6.2.23 to $\mathfrak{W} = \mathfrak{L}$, $\mathfrak{a}(w) = \operatorname{mult}_w u$ and $\mathfrak{b}(w) = \operatorname{mult}_w v$. As a result, we see that the number of $\tau \in \operatorname{Sh}_{p,q}$ satisfying $h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))$ is $\prod_{w \in \mathfrak{L}} \dbinom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$. In other words,

$$\begin{aligned}
&(\text{the number of all } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))) \\
&= \prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}. \qquad (6.2.21)
\end{aligned}$$

However, for every $i \in \{1, 2, \ldots, p+q\}$, we have

$$h(i) = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} = (uv)[I_i] \qquad (\text{by } (6.2.18)).$$

Hence, for any $\tau \in \operatorname{Sh}_{p,q}$, the condition $h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))$ is equivalent to $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$. Thus,

$$\begin{aligned}
&(\text{the number of all } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))) \\
&= (\text{the number of all } \tau \in \operatorname{Sh}_{p,q} \\
&\qquad \text{satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]) \\
&= (\text{the multiplicity with which the lexicographically highest element of} \\
&\qquad \text{the multiset } u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v)
\end{aligned}$$

(by (6.2.20)). Compared with (6.2.21), this yields

$$\begin{aligned}
&(\text{the multiplicity with which the lexicographically highest element of} \\
&\qquad \text{the multiset } u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v) \\
&= \prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}.
\end{aligned}$$

This proves Theorem 6.2.2(b).

(c) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Assume that $a_i \geq b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$. This, combined with $a_1 \geq a_2 \geq \cdots \geq a_p$ and $b_1 \geq b_2 \geq \cdots \geq b_q$, yields that $a_1 \geq a_2 \geq \cdots \geq a_p \geq b_1 \geq b_2 \geq \cdots \geq b_q$. Thus, the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ is weakly decreasing. Thus, the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order is the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ itself. But since this result is $(c_1, c_2, \ldots, c_{p+q})$, this shows that $(c_1, c_2, \ldots, c_{p+q}) = (a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$. Hence, $c_1 c_2 \cdots c_{p+q} = \underbrace{a_1 a_2 \cdots a_p}_{=u} \underbrace{b_1 b_2 \cdots b_q}_{=v} = uv$. Now, Theorem 6.2.2(a) yields that the lexicographically highest element of the multiset $u ⧢ v$ is $c_1 c_2 \cdots c_{p+q} = uv$. This proves Theorem 6.2.2(c).

(d) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Assume that $a_i > b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$. Thus, $a_i \geq b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$. Hence, Theorem 6.2.2(c) yields that the lexicographically highest element of the multiset $u ⧢ v$ is $uv$. Therefore, Theorem 6.2.2(b) shows that the multiplicity with which this word $uv$ appears in the multiset $u ⧢ v$ is $\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$.

Now, every $w \in \mathfrak{L}$ satisfies $\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} = 1$ [310]. Thus, as we know, the multiplicity with which this word $uv$ appears in the multiset $u ⧢ v$ is $\prod_{w \in \mathfrak{L}} \underbrace{\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}}_{=1} = \prod_{w \in \mathfrak{L}} 1 = 1$. This proves Theorem 6.2.2(d).

(e) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Since $u$ is a Lyndon word, the 1-tuple $(u)$ is the CFL factorization of $u$. Hence, we can apply Theorem 6.2.2(c) to 1 and $(u)$ instead of $p$ and $(a_1, a_2, \ldots, a_p)$. As a result, we conclude that the lexicographically highest element of the multiset $u ⧢ v$ is $uv$. It remains to prove that the multiplicity with which this word $uv$ appears in the multiset $u ⧢ v$ is $\operatorname{mult}_u v + 1$.

For every $w \in \mathfrak{L}$ satisfying $w \neq u$, we have

$$\operatorname{mult}_w u = 0 \tag{6.2.22}$$

[311]. Also, $\operatorname{mult}_u u = 1$ (for a similar reason). But $uv$ is the lexicographically highest element of the multiset $u ⧢ v$. Hence, the multiplicity with which

[310] *Proof.* Assume the contrary. Then, there exists at least one $w \in \mathfrak{L}$ such that $\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} \neq 1$. Consider this $w$. Both $\operatorname{mult}_w u$ and $\operatorname{mult}_w v$ must be positive (since $\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} \neq 1$). Since $\operatorname{mult}_w u$ is positive, there must be at least one term in the CFL factorization of $u$ which is equal to $w$. In other words, there is at least one $i \in \{1, 2, \ldots, p\}$ satisfying $a_i = w$ (since $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of $u$). Similarly, there is at least one $j \in \{1, 2, \ldots, q\}$ satisfying $b_j = w$. These $i$ and $j$ satisfy $a_i = w = b_j$, which contradicts $a_i > b_j$. This contradiction shows that our assumption was false, qed.

[311] *Proof of (6.2.22):* Let $w \in \mathfrak{L}$ be such that $w \neq u$. Then, the number of terms in the list $(u)$ which are equal to $w$ is 0. Since $(u)$ is the CFL factorization of $u$, this rewrites as follows: The number of terms in the CFL factorization of $u$ which are equal to $w$ is 0. In other words, $\operatorname{mult}_w u = 0$. This proves (6.2.22).

the word $uv$ appears in the multiset $u \sqcup\!\sqcup v$ is the multiplicity with which the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ appears in the multiset $u \sqcup\!\sqcup v$. According to Theorem 6.2.2(b), the latter multiplicity is

$$\begin{aligned}
&\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} \\
&= \underbrace{\binom{\operatorname{mult}_u u + \operatorname{mult}_u v}{\operatorname{mult}_u u}}_{\substack{= \binom{1 + \operatorname{mult}_u v}{1} \\ (\text{since } \operatorname{mult}_u u = 1)}} \cdot \prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} \underbrace{\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}}_{\substack{= \binom{0 + \operatorname{mult}_w v}{0} \\ (\text{since } \operatorname{mult}_w u = 0 \text{ (by (6.2.22)))}}} \qquad (\text{since } u \in \mathfrak{L}) \\
&= \underbrace{\binom{1 + \operatorname{mult}_u v}{1}}_{= 1 + \operatorname{mult}_u v = \operatorname{mult}_u v + 1} \cdot \prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} \underbrace{\binom{0 + \operatorname{mult}_w v}{0}}_{=1} = (\operatorname{mult}_u v + 1) \cdot \underbrace{\prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} 1}_{=1} \\
&= \operatorname{mult}_u v + 1.
\end{aligned}$$

This proves Theorem 6.2.2(e). □

As an application of our preceding results, we can prove a further necessary and sufficient criterion for a word to be Lyndon; this criterion is due to Chen/Fox/Lyndon [38, $\mathfrak{A}'' = \mathfrak{A}''''$]:

**Exercise 6.2.25.** Let $w \in \mathfrak{A}^*$ be a nonempty word. Prove that $w$ is Lyndon if and only if for any two nonempty words $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ satisfying $w = uv$, there exists at least one $s \in u \sqcup\!\sqcup v$ satisfying $s > w$.

### 6.3. Radford's theorem on the shuffle algebra.

We recall that our goal in Chapter 6 is to exhibit an algebraically independent generating set of the **k**-algebra QSym. Having the notion of Lyndon words – which will, to some extent, but not literally, parametrize this generating set – in place, we could start the construction of this generating set immediately. However, it might come off as rather unmotivated this way, and so we begin with some warmups. First, we shall prove Radford's theorem on the shuffle algebra.

**Definition 6.3.1.** A *polynomial algebra* will mean a **k**-algebra which is isomorphic to the polynomial ring $\mathbf{k}[x_i \mid i \in I]$ as a **k**-algebra (for some indexing set $I$). Note that $I$ need not be finite.

Equivalently, a polynomial algebra can be defined as a **k**-algebra which has an algebraically independent (over **k**) generating set. Yet equivalently, a polynomial algebra can be defined as a **k**-algebra which is isomorphic to the symmetric algebra of a free **k**-module.

Keep in mind that when we say that a certain bialgebra $A$ is a polynomial algebra, we are making no statement about the coalgebra structure on $A$. The isomorphism from $A$ to the symmetric algebra of a free **k**-module need not be a coalgebra isomorphism, and the algebraically independent generating set of $A$ need not consist of primitives. Thus, showing that a bialgebra $A$ is a polynomial algebra does not trivialize the study of its bialgebraic structure.

*Remark* 6.3.2. Let $V$ be a $\mathbf{k}$-module, and let $\mathfrak{A}$ be a totally ordered set. Let $b_a$ be an element of $V$ for every $a \in \mathfrak{A}$. Consider the shuffle algebra $\operatorname{Sh}(V)$ (defined in Definition 1.6.7).

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element $b_w$ of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where $\ell$ is the length of $w$. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\underline{\sqcup\!\sqcup}$.)

Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words over the alphabet $\mathfrak{A}$. Let $n = \ell(u)$ and $m = \ell(v)$. Then,

$$b_u \underline{\sqcup\!\sqcup} b_v = \sum_{\sigma \in \operatorname{Sh}_{n,m}} b_{u \underset{\sigma}{\sqcup\!\sqcup} v}.$$

**Exercise 6.3.3.** Prove Remark 6.3.2.

[**Hint:** This follows from the definition of $\underline{\sqcup\!\sqcup}$.]

We can now state Radford's theorem [177, Theorem 3.1.1(e)]:

**Theorem 6.3.4.** *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $V$ be a free $\mathbf{k}$-module with a basis $(b_a)_{a \in \mathfrak{A}}$, where $\mathfrak{A}$ is a totally ordered set. Then, the shuffle algebra $\operatorname{Sh}(V)$ (defined in Definition 1.6.7) is a polynomial $\mathbf{k}$-algebra. An algebraically independent generating set of $\operatorname{Sh}(V)$ can be constructed as follows:*

*For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element $b_w$ of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where $\ell$ is the length of $w$. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\underline{\sqcup\!\sqcup}$.) Let $\mathfrak{L}$ denote the set of all Lyndon words over the alphabet $\mathfrak{A}$. Then, $(b_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$.*

**Example 6.3.5.** For this example, let $\mathfrak{A}$ be the alphabet $\{1, 2, 3, \ldots\}$ with total order given by $1 < 2 < 3 < \cdots$, and assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $V$ be the free $\mathbf{k}$-module with basis $(b_a)_{a \in \mathfrak{A}}$. We use the notations of Theorem 6.3.4. Then, Theorem 6.3.4 yields that $(b_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$. Here are some examples of elements of $\operatorname{Sh}(V)$ written as polynomials in this generating set:

$$\begin{aligned}
b_{12} &= b_{12} \qquad \text{(the word 12 itself is Lyndon)};\\
b_{21} &= b_1 \shuffle b_2 - b_{12};\\
b_{11} &= \frac{1}{2} b_1 \shuffle b_1;\\
b_{123} &= b_{123} \qquad \text{(the word 123 itself is Lyndon)};\\
b_{132} &= b_{132} \qquad \text{(the word 132 itself is Lyndon)};\\
b_{213} &= b_2 \shuffle b_{13} - b_{123} - b_{132};\\
b_{231} &= b_{23} \shuffle b_1 - b_2 \shuffle b_{13} + b_{132};\\
b_{312} &= b_3 \shuffle b_{12} - b_{123} - b_{132};\\
b_{321} &= b_1 \shuffle b_2 \shuffle b_3 - b_{23} \shuffle b_1 - b_3 \shuffle b_{12} + b_{123};\\
b_{112} &= b_{112} \qquad \text{(the word 112 itself is Lyndon)};\\
b_{121} &= b_{12} \shuffle b_1 - 2 b_{112};\\
b_{1212} &= \frac{1}{2} b_{12} \shuffle b_{12} - 2 b_{1122};\\
b_{4321} &= b_1 \shuffle b_2 \shuffle b_3 \shuffle b_4 - b_1 \shuffle b_2 \shuffle b_{34} - b_1 \shuffle b_{23} \shuffle b_4 - b_{12} \shuffle b_3 \shuffle b_4\\
&\qquad + b_1 \shuffle b_{234} + b_{12} \shuffle b_{34} + b_{123} \shuffle b_4 - b_{1234}.
\end{aligned}$$

[312]

Note that Theorem 6.3.4 cannot survive without the condition that $\mathbb{Q}$ be a subring of $\mathbf{k}$. For instance, for any $v \in V$, we have $v \shuffle v = 2vv$ in $\operatorname{Sh}(V)$, which vanishes if $2 = 0$ in $\mathbf{k}$; this stands in contrast to the fact that polynomial $\mathbf{k}$-algebras are integral domains when $\mathbf{k}$ itself is one. We will see that QSym is less sensitive towards the base ring in this regard (although proving that QSym is a polynomial algebra is much easier when $\mathbb{Q}$ is a subring of $\mathbf{k}$).

*Remark* 6.3.6. Theorem 6.3.4 can be contrasted with the following fact: If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the shuffle algebra $\operatorname{Sh}(V)$ of **any** $\mathbf{k}$-module $V$ (not necessarily free!) is isomorphic (as a $\mathbf{k}$-algebra) to the symmetric algebra $\operatorname{Sym}\left((\ker \epsilon) / (\ker \epsilon)^2\right)$ (by Theorem 1.7.29(e), applied to $A = \operatorname{Sh}(V)$). This fact is closely related to Theorem 6.3.4, but neither follows from it

[312] A pattern emerges in the formulas for $b_{21}$, $b_{321}$ and $b_{4321}$: for every $n \in \mathbb{N}$, we have

$$b_{(n,n-1,\ldots,1)} = \sum_{\alpha \in \operatorname{Comp}_n} (-1)^{n-\ell(\alpha)} b_{\mathbf{d}_1(\alpha)} \shuffle b_{\mathbf{d}_2(\alpha)} \shuffle \cdots \shuffle b_{\mathbf{d}_{\ell(\alpha)}(\alpha)},$$

where $(\mathbf{d}_1(\alpha)) \cdot (\mathbf{d}_2(\alpha)) \cdot \cdots \cdot \left(\mathbf{d}_{\ell(\alpha)}(\alpha)\right)$ is the factorization of the word $(1, 2, \ldots, n)$ into factors of length $\alpha_1$, $\alpha_2$, $\ldots$, $\alpha_\ell$ (where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$). This can be proved by an application of Lemma 5.2.7(a) (as it is easy to see that for any composition $\alpha$ of $n$, we have

$$\begin{aligned}
&b_{\mathbf{d}_1(\alpha)} \shuffle b_{\mathbf{d}_2(\alpha)} \shuffle \cdots \shuffle b_{\mathbf{d}_{\ell(\alpha)}(\alpha)}\\
&= \left(\text{the sum of } b_\pi \text{ for all words } \pi \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}\left(\pi^{-1}\right) \subset D(\alpha)\right)\\
&= \sum_{\substack{\beta \in \operatorname{Comp}_n;\\ \beta \text{ coarsens } \alpha}} \sum_{\substack{\pi \in \mathfrak{S}_n;\\ \gamma\left(\pi^{-1}\right) = \beta}} b_\pi,
\end{aligned}$$

where $\gamma\left(\pi^{-1}\right)$ denotes the composition $\tau$ of $n$ satisfying $D(\tau) = \operatorname{Des}\left(\pi^{-1}\right)$).

(since Theorem 6.3.4 only considers the case of free $\mathbf{k}$-modules $V$) nor yields it (since this fact does not provide explicit generators for the $\mathbf{k}$-module $(\ker \epsilon) / (\ker \epsilon)^2$ and thus for the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$).

In our proof of Theorem 6.3.4 (but not only there), we will use part (a) of the following lemma[313], which makes proving that certain families indexed by Lyndon words generate certain $\mathbf{k}$-algebras more comfortable:

**Lemma 6.3.7.** *Let $A$ be a commutative $\mathbf{k}$-algebra. Let $\mathfrak{A}$ be a totally ordered set. Let $\mathfrak{L}$ be the set of all Lyndon words over the alphabet $\mathfrak{A}$. Let $b_w$ be an element of $A$ for every $w \in \mathfrak{L}$. For every word $u \in \mathfrak{A}^*$, define an element $\mathbf{b}_u$ of $A$ by $\mathbf{b}_u = b_{a_1} b_{a_2} \cdots b_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of $u$.*

(a) *The family $(b_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $A$ if and only if the family $(\mathbf{b}_u)_{u \in \mathfrak{A}^*}$ is a basis of the $\mathbf{k}$-module $A$.*

(b) *The family $(b_w)_{w \in \mathfrak{L}}$ generates the $\mathbf{k}$-algebra $A$ if and only if the family $(\mathbf{b}_u)_{u \in \mathfrak{A}^*}$ spans the $\mathbf{k}$-module $A$.*

(c) *Assume that the $\mathbf{k}$-algebra $A$ is graded. Let $\operatorname{wt} : \mathfrak{A} \to \{1, 2, 3, \ldots\}$ be any map such that for every $N \in \{1, 2, 3, \ldots\}$, the set $\operatorname{wt}^{-1}(N)$ is finite.*

*For every word $w \in \mathfrak{A}^*$, define an element $\operatorname{Wt}(w) \in \mathbb{N}$ by $\operatorname{Wt}(w) = \operatorname{wt}(w_1) + \operatorname{wt}(w_2) + \cdots + \operatorname{wt}(w_k)$, where $k$ is the length of $w$.*

*Assume that for every $w \in \mathfrak{L}$, the element $b_w$ of $A$ is homogeneous of degree $\operatorname{Wt}(w)$.*

*Assume further that the $\mathbf{k}$-module $A$ has a basis $(g_u)_{u \in \mathfrak{A}^*}$ having the property that for every $u \in \mathfrak{A}^*$, the element $g_u$ of $A$ is homogeneous of degree $\operatorname{Wt}(u)$.*

*Assume also that the family $(b_w)_{w \in \mathfrak{L}}$ generates the $\mathbf{k}$-algebra $A$.*

*Then, this family $(b_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $A$.*

**Exercise 6.3.8.** Prove Lemma 6.3.7.

[**Hint:** For (a) and (b), notice that the $\mathbf{b}_u$ are the "monomials" in the $b_w$. For (c), use Exercise 2.5.18(b) in every homogeneous component of $A$.]

The main workhorse of our proof of Theorem 6.3.4 will be the following consequence of Theorem 6.2.2(c):

**Proposition 6.3.9.** *Let $V$ be a free $\mathbf{k}$-module with a basis $(b_a)_{a \in \mathfrak{A}}$, where $\mathfrak{A}$ is a totally ordered set.*

*For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element $b_w$ of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where $\ell$ is the length of $w$. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.)*

*For every word $u \in \mathfrak{A}^*$, define an element $\mathbf{b}_u$ by $\mathbf{b}_u = b_{a_1} \sqcup\!\sqcup b_{a_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup b_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of $u$.*

[313] And in a later proof, we will also use its part (c) (which is tailored for application to QSym).

*If $\ell \in \mathbb{N}$ and if $x \in \mathfrak{A}^\ell$ is a word, then there is a family $\left(\eta_{x,y}\right)_{y\in\mathfrak{A}^\ell} \in \mathbb{N}^{\mathfrak{A}^\ell}$ of elements of $\mathbb{N}$ satisfying*

$$\mathbf{b}_x = \sum_{\substack{y\in\mathfrak{A}^\ell;\\ y\leq x}} \eta_{x,y} b_y$$

*and $\eta_{x,x} \neq 0$ (in $\mathbb{N}$).*

Before we prove this, let us show a very simple lemma:

**Lemma 6.3.10.** *Let $\mathfrak{A}$ be a totally ordered set. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\sigma \in \operatorname{Sh}_{n,m}$.*

*(a) If $u$, $v$ and $v'$ are three words satisfying $\ell(u) = n$, $\ell(v) = m$, $\ell(v') = m$ and $v' < v$, then $u \underset{\sigma}{\sqcup\!\sqcup} v' < u \underset{\sigma}{\sqcup\!\sqcup} v$.*

*(b) If $u$, $u'$ and $v$ are three words satisfying $\ell(u) = n$, $\ell(u') = n$, $\ell(v) = m$ and $u' < u$, then $u' \underset{\sigma}{\sqcup\!\sqcup} v < u \underset{\sigma}{\sqcup\!\sqcup} v$.*

*(c) If $u$, $v$ and $v'$ are three words satisfying $\ell(u) = n$, $\ell(v) = m$, $\ell(v') = m$ and $v' \leq v$, then $u \underset{\sigma}{\sqcup\!\sqcup} v' \leq u \underset{\sigma}{\sqcup\!\sqcup} v$.*

**Exercise 6.3.11.** Prove Lemma 6.3.10.

**Exercise 6.3.12.** Prove Proposition 6.3.9.

[**Hint:** Proceed by induction over $\ell$. In the induction step, apply Theorem 6.2.2(c)[314] to $u = a_1$ and $v = a_2 a_3 \cdots a_p$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of $x$. Use Lemma 6.3.10 to get rid of smaller terms.]

**Exercise 6.3.13.** Prove Theorem 6.3.4.

[**Hint:** According to Lemma 6.3.7(a), it suffices to show that the family $(\mathbf{b}_u)_{u\in\mathfrak{A}^*}$ defined in Proposition 6.3.9 is a basis of the $\mathbf{k}$-module $\operatorname{Sh}(V)$. When $\mathfrak{A}$ is finite, the latter can be proven by triangularity using Proposition 6.3.9. Reduce the general case to that of finite $\mathfrak{A}$.]

## 6.4. **Polynomial freeness of** QSym**: statement and easy parts.**

**Definition 6.4.1.** For the rest of Section 6.4 and for Section 6.5, we introduce the following notations: We let $\mathfrak{A}$ be the totally ordered set $\{1, 2, 3, \ldots\}$ with its natural order (that is, $1 < 2 < 3 < \cdots$.) Thus, the words over $\mathfrak{A}$ are precisely the compositions. That is, $\mathfrak{A}^* = \operatorname{Comp}$. We let $\mathfrak{L}$ denote the set of all Lyndon words over $\mathfrak{A}$. These Lyndon words are also called *Lyndon compositions*.

A natural question is how many Lyndon compositions of a given size exist. While we will not use the answer, we nevertheless record it:

**Exercise 6.4.2.** Show that the number of Lyndon compositions of size $n$ equals

$$\frac{1}{n}\sum_{d|n} \mu(d)\left(2^{n/d} - 1\right) = \frac{1}{n}\sum_{d|n} \mu(d)\, 2^{n/d} - \delta_{n,1}$$

for every positive integer $n$ (where "$\sum_{d|n}$" means a sum over all positive divisors of $n$, and where $\mu$ is the number-theoretic Möbius function).

[314] Or Theorem 6.2.2(e), if you prefer.

[**Hint:** One solution is similar to the solution of Exercise 6.1.29 using CFL factorization. Another proceeds by defining a bijection between Lyndon compositions and Lyndon words over a two-letter alphabet $\{\mathbf{0}, \mathbf{1}\}$ (with $\mathbf{0} < \mathbf{1}$) which are $\neq \mathbf{1}$. [315]]

Let us now state Hazewinkel's result ([89, Theorem 8.1], [93, §6.7]) which is the main goal of Chapter 6:

**Theorem 6.4.3.** *The* $\mathbf{k}$*-algebra* QSym *is a polynomial algebra. It is isomorphic, as a graded* $\mathbf{k}$*-algebra, to the* $\mathbf{k}$*-algebra* $\mathbf{k}\left[x_w \mid w \in \mathfrak{L}\right]$*. Here, the grading on* $\mathbf{k}\left[x_w \mid w \in \mathfrak{L}\right]$ *is defined by setting* $\deg\left(x_w\right) = \sum_{i=1}^{\ell(w)} w_i$ *for every* $w \in \mathfrak{L}$*.*

We shall prove Theorem 6.4.3 in the next section (Section 6.5). But the particular case of Theorem 6.4.3 when $\mathbb{Q}$ is a subring of $\mathbf{k}$ can be proven more easily; we state it as a proposition:

**Proposition 6.4.4.** *Assume that* $\mathbb{Q}$ *is a subring of* $\mathbf{k}$*. Then, Theorem 6.4.3 holds.*

We will give two proofs of Proposition 6.4.4 in this Section 6.4; a third proof of Proposition 6.4.4 will immediately result from the proof of Theorem 6.4.3 in Section 6.5. (There **is** virtue in giving three different proofs, as they all construct different isomorphisms $\mathbf{k}\left[x_w \mid w \in \mathfrak{L}\right] \to \mathrm{QSym}$.)

Our first proof – originating in Malvenuto's [145, Corollaire 4.20] – can be given right away; it relies on Exercise 5.4.12:

*First proof of Proposition 6.4.4.* Let $V$ be the free $\mathbf{k}$-module with basis $\left(\mathfrak{b}_n\right)_{n \in \{1,2,3,\ldots\}}$. Endow the $\mathbf{k}$-module $V$ with a grading by assigning to each basis vector $\mathfrak{b}_n$ the degree $n$. Exercise 5.4.12(k) shows that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ (defined as in Proposition 1.6.7) as Hopf algebras. By being a bit more careful, we can obtain the slightly stronger result that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ as **graded** Hopf algebras[316]. In particular, $\mathrm{QSym} \cong \mathrm{Sh}(V)$ as graded $\mathbf{k}$-algebras.

Theorem 6.3.4 (applied to $b_a = \mathfrak{b}_a$) yields that the shuffle algebra $\mathrm{Sh}(V)$ is a polynomial $\mathbf{k}$-algebra, and that an algebraically independent generating set of $\mathrm{Sh}(V)$ can be constructed as follows:

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element $\mathfrak{b}_w$ of $\mathrm{Sh}(V)$ by $\mathfrak{b}_w = \mathfrak{b}_{w_1}\mathfrak{b}_{w_2}\cdots\mathfrak{b}_{w_\ell}$, where $\ell$ is the length of $w$. (The

[315] This bijection is obtained by restricting the bijection

$$\mathrm{Comp} \to \left\{w \in \{\mathbf{0},\mathbf{1}\}^* \mid w \text{ does not start with } \mathbf{1}\right\},$$
$$(\alpha_1, \alpha_2, \ldots, \alpha_\ell) \mapsto \mathbf{0}\mathbf{1}^{\alpha_1 - 1}\mathbf{0}\mathbf{1}^{\alpha_2 - 1}\cdots\mathbf{0}\mathbf{1}^{\alpha_\ell - 1}$$

(where $\mathbf{0}\mathbf{1}^k$ is to be read as $\mathbf{0}\left(\mathbf{1}^k\right)$, not as $\left(\mathbf{0}\mathbf{1}\right)^k$) to the set of Lyndon compositions. The idea behind this bijection is well-known in the Grothendieck-Teichmüller community: see, e.g., [94, §3.1] (and see [77, Note 5.16] for a different appearance of this idea).

[316] *Proof.* In the solution of Exercise 5.4.12(k), we have shown that $\mathrm{QSym} \cong T(V)^o$ as graded Hopf algebras. But Remark 1.6.9(b) shows that the Hopf algebra $T(V)^o$ is naturally isomorphic to the shuffle algebra $\mathrm{Sh}(V^o)$ as Hopf algebras; it is easy to see that the natural isomorphism $T(V)^o \to \mathrm{Sh}(V^o)$ is graded (because it is the direct sum of the isomorphisms $\left(V^{\otimes n}\right)^o \to \left(V^o\right)^{\otimes n}$ over all $n \in \mathbb{N}$, and each of these isomorphisms is graded). Hence, $T(V)^o \cong \mathrm{Sh}(V^o)$ as graded Hopf algebras. But $V^o \cong V$ as graded $\mathbf{k}$-modules (since $V$ is of finite type), and thus $\mathrm{Sh}(V^o) \cong \mathrm{Sh}(V)$ as graded Hopf algebras. Altogether, we obtain $\mathrm{QSym} \cong T(V)^o \cong \mathrm{Sh}(V^o) \cong \mathrm{Sh}(V)$ as graded Hopf algebras, qed.

multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.) Then, $(\mathfrak{b}_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the **k**-algebra $\operatorname{Sh}(V)$.

For every $w \in \mathfrak{A}^*$, we have $\mathfrak{b}_w = \mathfrak{b}_{w_1}\mathfrak{b}_{w_2}\cdots\mathfrak{b}_{w_{\ell(w)}}$ (by the definition of $\mathfrak{b}_w$). For every $w \in \mathfrak{A}^*$, the element $\mathfrak{b}_w = \mathfrak{b}_{w_1}\mathfrak{b}_{w_2}\cdots\mathfrak{b}_{w_{\ell(w)}}$ of $\operatorname{Sh}(V)$ is homogeneous of degree $\sum_{i=1}^{\ell(w)} \underbrace{\deg(\mathfrak{b}_{w_i})}_{=w_i} = \sum_{i=1}^{\ell(w)} w_i$.

Now, define a grading on the **k**-algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$ by setting

$$\deg(x_w) = \sum_{i=1}^{\ell(w)} w_i \qquad \text{for every } w \in \mathfrak{L}.$$

By the universal property of the polynomial algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$, we can define a **k**-algebra homomorphism $\Phi : \mathbf{k}[x_w \mid w \in \mathfrak{L}] \to \operatorname{Sh}(V)$ by setting

$$\Phi(x_w) = \mathfrak{b}_w \qquad \text{for every } w \in \mathfrak{L}.$$

This homomorphism $\Phi$ is a **k**-algebra isomorphism (since $(\mathfrak{b}_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the **k**-algebra $\operatorname{Sh}(V)$) and is graded (because for every $w \in \mathfrak{L}$, the element $\mathfrak{b}_w$ of $\operatorname{Sh}(V)$ is homogeneous of degree $\sum_{i=1}^{\ell(w)} w_i = \deg(x_w)$). Thus, $\Phi$ is an isomorphism of graded **k**-algebras. Hence, $\operatorname{Sh}(V) \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded **k**-algebras. Altogether, $\operatorname{QSym} \cong \operatorname{Sh}(V) \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded **k**-algebras. Thus, QSym is a polynomial algebra. This proves Theorem 6.4.3 under the assumption that $\mathbb{Q}$ be a subring of **k**. In other words, this proves Proposition 6.4.4. □

Our second proof of Proposition 6.4.4 comes from [93] (where Proposition 6.4.4 appears as [93, Theorem 6.5.13]). This proof will construct an explicit algebraically independent family generating the **k**-algebra QSym. [317] The generating set will be very unsophisticated: it will be $(M_\alpha)_{\alpha\in\mathfrak{L}}$, where $\mathfrak{A}$ and $\mathfrak{L}$ are as in Theorem 6.4.3. Here, we are using the fact that words over the alphabet $\{1, 2, 3, \ldots\}$ are the same thing as compositions, so, in particular, a monomial quasisymmetric function $M_\alpha$ is defined for every such word $\alpha$.

It takes a bit of work to show that this family indeed fits the bill. We begin with a corollary of Proposition 5.1.3 that is essentially obtained by throwing away all non-bijective maps $f$:

**Proposition 6.4.5.** *Let $\alpha \in \mathfrak{A}^*$ and $\beta \in \mathfrak{A}^*$. Then,*

$$\begin{aligned} & M_\alpha M_\beta \\ & = \sum_{\gamma\in\alpha\sqcup\!\sqcup\beta} M_\gamma + (\text{a sum of terms of the form } M_\delta \text{ with } \delta \in \mathfrak{A}^* \\ & \qquad\qquad \text{satisfying } \ell(\delta) < \ell(\alpha) + \ell(\beta)). \end{aligned}$$

[318]

[317] We could, of course, obtain such a family from our above proof as well (this is done by Malvenuto in [145, Corollaire 4.20]), but it won't be a very simple one.

[318] The sum $\sum_{\gamma\in\alpha\sqcup\!\sqcup\beta} M_\gamma$ ranges over the **multiset** $\alpha \sqcup\!\sqcup \beta$; if an element appears several times in $\alpha \sqcup\!\sqcup \beta$, then it has accordingly many addends corresponding to it.

**Exercise 6.4.6.** Prove Proposition 6.4.5.

[**Hint:** Recall what was said about the $p = \ell + m$ case in Example 5.1.4.]

**Corollary 6.4.7.** *Let $\alpha \in \mathfrak{A}^*$ and $\beta \in \mathfrak{A}^*$. Then, $M_\alpha M_\beta$ is a sum of terms of the form $M_\delta$ with $\delta \in \mathfrak{A}^*$ satisfying $\ell(\delta) \leq \ell(\alpha) + \ell(\beta)$.*

**Exercise 6.4.8.** Prove Corollary 6.4.7.

We now define a partial order on the compositions of a given nonnegative integer:

**Definition 6.4.9.** Let $n \in \mathbb{N}$. We define a binary relation $\underset{\text{wll}}{\leq}$ on the set $\operatorname{Comp}_n$ as follows: For two compositions $\alpha$ and $\beta$ in $\operatorname{Comp}_n$, we set $\alpha \underset{\text{wll}}{\leq} \beta$ if and only if

$$\text{either } \ell(\alpha) < \ell(\beta) \text{ or } (\ell(\alpha) = \ell(\beta) \text{ and } \alpha \leq \beta \text{ in lexicographic order}).$$

This binary relation $\underset{\text{wll}}{\leq}$ is the smaller-or-equal relation of a total order on $\operatorname{Comp}_n$; we refer to said total order as the *wll-order* on $\operatorname{Comp}_n$, and we denote by $\underset{\text{wll}}{<}$ the smaller relation of this total order.

Notice that if $\alpha$ and $\beta$ are two compositions satisfying $\ell(\alpha) = \ell(\beta)$, then $\alpha \leq \beta$ in lexicographic order if and only if $\alpha \leq \beta$ with respect to the relation $\leq$ defined in Definition 6.1.1.

A remark about the name "wll-order" is in order. We have taken this notation from [89, Definition 6.7.14], where it is used for an extension of this order to the whole set Comp. We will never use this extension, as we will only ever compare two compositions of the same integer.[319]

We now state a fact which is similar (and plays a similar role) to Proposition 6.3.9:

**Proposition 6.4.10.** *For every composition $u \in \operatorname{Comp} = \mathfrak{A}^*$, define an element $\mathbf{M}_u \in \operatorname{QSym}$ by $\mathbf{M}_u = M_{a_1} M_{a_2} \cdots M_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of the word $u$.*

*If $n \in \mathbb{N}$ and if $x \in \operatorname{Comp}_n$, then there is a family $(\eta_{x,y})_{y \in \operatorname{Comp}_n} \in \mathbb{N}^{\operatorname{Comp}_n}$ of elements of $\mathbb{N}$ satisfying*

$$\mathbf{M}_x = \sum_{\substack{y \in \operatorname{Comp}_n; \\ y \underset{\text{wll}}{\leq} x}} \eta_{x,y} M_y$$

*and $\eta_{x,x} \neq 0$ (in $\mathbb{N}$).*

Before we prove it, let us show the following lemma:

**Lemma 6.4.11.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \operatorname{Comp}_n$ and $v \in \operatorname{Comp}_m$. Let $z$ be the lexicographically highest element of the multiset $u \sqcup\!\sqcup\, v$.*

*(a) We have $z \in \operatorname{Comp}_{n+m}$.*

[319] In [89, Definition 6.7.14], the name "wll-order" is introduced as an abbreviation for "**w**eight first, then **l**ength, then **l**exicographic" (in the sense that two compositions are first compared by their weights, then, if the weights are equal, by their lengths, and finally, if the lengths are also equal, by the lexicographic order). For us, the alternative explanation "**w**ord **l**ength, then **l**exicographic" serves just as well.

*(b) There exists a positive integer $h$ such that*

$$M_u M_v = h M_z + \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \\ \text{satisfying } w \underset{\text{wll}}{<} z\Big).$$

*(c) Let $v' \in \operatorname{Comp}_m$ be such that $v' \underset{\text{wll}}{<} v$. Then,*

$$M_u M_{v'} = \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \\ \text{satisfying } w \underset{\text{wll}}{<} z\Big).$$

**Exercise 6.4.12.** Prove Lemma 6.4.11.

[**Hint:** For (b), set $h$ to be the multiplicity with which the word $z$ appears in the multiset $u \sqcup\!\sqcup v$, then use Proposition 6.4.5 and notice that $M_u M_v$ is homogeneous of degree $n+m$. For (c), use (b) for $v'$ instead of $v$ and notice that Lemma 6.3.10(a) shows that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v'$ is $\underset{\text{wll}}{<} z$.]

**Exercise 6.4.13.** Prove Proposition 6.4.10.

[**Hint:** Proceed by strong induction over $n$. In the induction step, let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of $x$, and set $u = a_1$ and $v = a_2 a_3 \cdots a_p$; then apply Proposition 6.4.10 to $v$ instead of $x$, and multiply the resulting equality $\mathbf{M}_v = \sum_{\substack{y \in \operatorname{Comp}_{|v|}; \\ y \underset{\text{wll}}{\leq} v}} \eta_{v,y} M_y$ with $M_u$ to obtain an expression for $M_u \mathbf{M}_v = \mathbf{M}_x$. Use Lemma 6.4.11 to show that this expression has the form $\sum_{\substack{y \in \operatorname{Comp}_n; \\ y \underset{\text{wll}}{\leq} x}} \eta_{x,y} M_y$ with $\eta_{x,x} \neq 0$; here it helps to remember that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $uv = x$ (by Theorem 6.2.2(c)).]

We are almost ready to give our second proof of Proposition 6.4.4; our last step is the following proposition:

**Proposition 6.4.14.** *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Then, $(M_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra* QSym.

**Exercise 6.4.15.** Prove Proposition 6.4.14.

[**Hint:** Define $\mathbf{M}_u$ for every $u \in \operatorname{Comp}$ as in Proposition 6.4.10. Conclude from Proposition 6.4.10 that, for every $n \in \mathbb{N}$, the family $(\mathbf{M}_u)_{u \in \operatorname{Comp}_n}$ expands invertibly triangularly[320] (with respect to the total order $\underset{\text{wll}}{\leq}$ on $\operatorname{Comp}_n$) with respect to the basis $(M_u)_{u \in \operatorname{Comp}_n}$ of $\operatorname{QSym}_n$. Conclude that this family $(\mathbf{M}_u)_{u \in \operatorname{Comp}_n}$ is a basis of $\operatorname{QSym}_n$ itself, and so the whole family $(\mathbf{M}_u)_{u \in \operatorname{Comp}}$ is a basis of QSym. Conclude using Lemma 6.3.7(a).]

*Second proof of Proposition 6.4.4.* Proposition 6.4.14 yields that $(M_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym.

Define a grading on the $\mathbf{k}$-algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$ by setting $\deg(x_w) = \sum_{i=1}^{\ell(w)} w_i$ for every $w \in \mathfrak{L}$. By the universal property of the polynomial algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$, we can define a $\mathbf{k}$-algebra homomorphism

[320] See Definition 11.1.16(b) for the meaning of this.

$\Phi : \mathbf{k}[x_w \mid w \in \mathfrak{L}] \to \operatorname{QSym}$ by setting

$$\Phi(x_w) = M_w \qquad \text{for every } w \in \mathfrak{L}.$$

This homomorphism $\Phi$ is a $\mathbf{k}$-algebra isomorphism (since $(M_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym) and is graded (because for every $w \in \mathfrak{L}$, the element $M_w$ of QSym is homogeneous of degree $|w| = \sum_{i=1}^{\ell(w)} w_i = \deg(x_w)$). Thus, $\Phi$ is an isomorphism of graded $\mathbf{k}$-algebras. Hence, $\operatorname{QSym} \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded $\mathbf{k}$-algebras. In particular, this shows that QSym is a polynomial algebra. This proves Theorem 6.4.3 under the assumption that $\mathbb{Q}$ be a subring of $\mathbf{k}$. Proposition 6.4.4 is thus proven again. □

6.5. **Polynomial freeness of** QSym**: the general case.** We now will prepare for proving Theorem 6.4.3 without any assumptions on $\mathbf{k}$. In our proof, we follow [89] and [93, §6.7], but without using the language of plethysm and Frobenius maps. We start with the following definition:

**Definition 6.5.1.** Let $\alpha$ be a composition. Write $\alpha$ in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$.

(a) Let $\operatorname{SIS}(\ell)$ denote the set of all strictly increasing $\ell$-tuples $(i_1, i_2, \ldots, i_\ell)$ of positive integers.[321] For every $\ell$-tuple $\mathbf{i} = (i_1, i_2, \ldots, i_\ell) \in \operatorname{SIS}(\ell)$, we denote the monomial $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell}$ by $\mathbf{x}_{\mathbf{i}}^{\alpha}$. This $\mathbf{x}_{\mathbf{i}}^{\alpha}$ is a monomial of degree $\alpha_1 + \alpha_2 + \cdots + \alpha_\ell = |\alpha|$. Then,

$$M_\alpha = \sum_{\mathbf{i}\in\operatorname{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha}. \tag{6.5.1}$$

[322]

(b) Consider the ring $\mathbf{k}[[\mathbf{x}]]$ endowed with the coefficientwise topology[323]. The family $(\mathbf{x}_{\mathbf{i}}^{\alpha})_{\mathbf{i}\in\operatorname{SIS}(\ell)}$ of elements of $\mathbf{k}[[\mathbf{x}]]$ is power-summable[324]. Hence,

[321] "Strictly increasing" means that $i_1 < i_2 < \cdots < i_\ell$ here. Of course, the elements of $\operatorname{SIS}(\ell)$ are in 1-to-1 correspondence with $\ell$-element subsets of $\{1, 2, 3, \ldots\}$.

[322] *Proof of (6.5.1):* By the definition of $M_\alpha$, we have

$$M_\alpha = \underbrace{\sum_{i_1<i_2<\cdots<i_\ell \text{ in } \{1,2,3,\ldots\}}}_{=\sum_{(i_1,i_2,\ldots,i_\ell)\in\operatorname{SIS}(\ell)}} x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell} = \sum_{(i_1,i_2,\ldots,i_\ell)\in\operatorname{SIS}(\ell)} x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell}$$
$$= \sum_{\mathbf{i}=(i_1,i_2,\ldots,i_\ell)\in\operatorname{SIS}(\ell)} \underbrace{x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell}}_{\substack{=\mathbf{x}_{\mathbf{i}}^{\alpha} \\ \text{(by the definition of } \mathbf{x}_{\mathbf{i}}^{\alpha})}} = \sum_{\mathbf{i}=(i_1,i_2,\ldots,i_\ell)\in\operatorname{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha} = \sum_{\mathbf{i}\in\operatorname{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha},$$

qed.

[323] This topology is defined as follows:

We endow the ring $\mathbf{k}$ with the discrete topology. Then, we can regard the $\mathbf{k}$-module $\mathbf{k}[[\mathbf{x}]]$ as a direct product of infinitely many copies of $\mathbf{k}$ (by identifying every power series in $\mathbf{k}[[\mathbf{x}]]$ with the family of its coefficients). Hence, the product topology is a well-defined topology on $\mathbf{k}[[\mathbf{x}]]$; this topology is denoted as the *coefficientwise topology*. A sequence $(a_n)_{n\in\mathbb{N}}$ of power series converges to a power series $a$ with respect to this topology if and only if for every monomial $\mathfrak{m}$, all sufficiently high $n \in \mathbb{N}$ satisfy

$$(\text{the coefficient of } \mathfrak{m} \text{ in } a_n) = (\text{the coefficient of } \mathfrak{m} \text{ in } a).$$

Note that this is **not** the topology obtained by taking the completion of $\mathbf{k}[x_1, x_2, x_3, \ldots]$ with respect to the standard grading (in which all $x_i$ have degree 1). (The latter completion is actually a smaller ring than $\mathbf{k}[[\mathbf{x}]]$.)

[324] Let us define what "power-summable" means for us:

for every $f \in \Lambda$, there is a well-defined power series $f\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) \in \mathbf{k}\left[\left[\mathbf{x}\right]\right]$ obtained by "evaluating" $f$ at $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}$ [325]. In particular, for every $s \in \mathbb{Z}$, we can evaluate the symmetric function $e_s \in \Lambda$ [326] at $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}$. The resulting power series $e_s\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) \in \mathbf{k}\left[\left[\mathbf{x}\right]\right]$ will be denoted $M_{\alpha}^{\langle s\rangle}$. Thus,

$$M_{\alpha}^{\langle s\rangle} = e_s\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right).$$

A family $\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in \mathbb{N}^{\mathbf{I}}$ (where $\mathbf{I}$ is some set) is said to be *finitely supported* if all but finitely many $\mathbf{i} \in \mathbf{I}$ satisfy $n_{\mathbf{i}} = 0$.

If $\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in \mathbb{N}^{\mathbf{I}}$ is a finitely supported family, then $\sum_{\mathbf{i}\in\mathbf{I}} n_{\mathbf{i}}$ is a well-defined element of $\mathbb{N}$. If $N \in \mathbb{N}$, then a family $\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in \mathbb{N}^{\mathbf{I}}$ will be called $(\leq N)$*-supported* if it is finitely supported and satisfies $\sum_{\mathbf{i}\in\mathbf{I}} n_{\mathbf{i}} \leq N$.

We say that a family $\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in R^{\mathbf{I}}$ of elements of a topological commutative $\mathbf{k}$-algebra $R$ is *power-summable* if it satisfies the following property: For every $N \in \mathbb{N}$, the sum

$$\sum_{\substack{\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}};\\ \left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \text{ is } (\leq N)\text{-supported}}} \alpha_{\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}} \prod_{\mathbf{i}\in\mathbf{I}} s_{\mathbf{i}}^{n_{\mathbf{i}}}$$

converges in the topology on $R$ for every choice of scalars $\alpha_{\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}} \in \mathbf{k}$ corresponding to all $(\leq N)$-supported $\left(n_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in \mathbb{N}^{\mathbf{I}}$. In our specific case, we consider $\mathbf{k}\left[\left[\mathbf{x}\right]\right]$ as a topological commutative $\mathbf{k}$-algebra, where the topology is the coefficientwise topology. The fact that the family $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}$ is power-summable then can be proven as follows:

- If $\alpha \neq \varnothing$, then this fact follows from the (easily-verified) observation that every given monomial in the variables $x_1, x_2, x_3, \ldots$ can be written as a product of monomials of the form $\mathbf{x}_{\mathbf{i}}^{\alpha}$ (with $\mathbf{i} \in \operatorname{SIS}(\ell)$) in only finitely many ways.
- If $\alpha = \varnothing$, then this fact follows by noticing that $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}$ is a finite family (indeed, $\operatorname{SIS}(\ell) = \operatorname{SIS}(0) = \{()\}$), and every finite family is power-summable.

[325] Here is how this power series $f\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right)$ is formally defined:

Let $R$ be any topological commutative $\mathbf{k}$-algebra, and let $\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in R^{\mathbf{I}}$ be any power-summable family of elements of $R$. Assume that the indexing set $\mathbf{I}$ is countably infinite, and fix a bijection $\mathfrak{j} : \{1, 2, 3, \ldots\} \to \mathbf{I}$. Let $g \in R(\mathbf{x})$ be arbitrary. Then, we can substitute $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, $s_{\mathfrak{j}(3)}$, $\ldots$ for the variables $x_1$, $x_2$, $x_3$, $\ldots$ in $g$, thus obtaining an infinite sum which converges in $R$ (in fact, its convergence follows from the fact that the family $\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in R^{\mathbf{I}}$ is power-summable). The value of this sum will be denoted by $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$. In general, this value depends on the choice of the bijection $\mathfrak{j}$, so the notation $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$ is unambiguous only if this bijection $\mathfrak{j}$ is chosen once and for all. However, when $g \in \Lambda$, one can easily see that the choice of $\mathfrak{j}$ has no effect on $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$.

We can still define $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$ when the set $\mathbf{I}$ is finite instead of being countably infinite. In this case, we only need to modify our above definition as follows: Instead of fixing a bijection $\mathfrak{j} : \{1, 2, 3, \ldots\} \to \mathbf{I}$, we now fix a bijection $\mathfrak{j} : \{1, 2, \ldots, |\mathbf{I}|\} \to \mathbf{I}$, and instead of substituting $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, $s_{\mathfrak{j}(3)}$, $\ldots$ for the variables $x_1$, $x_2$, $x_3$, $\ldots$ in $g$, we now substitute $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, $\ldots$, $s_{\mathfrak{j}(|\mathbf{I}|)}$, $0$, $0$, $0$, $\ldots$ for the variables $x_1$, $x_2$, $x_3$, $\ldots$ in $g$. Again, the same observations hold as before: $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$ is independent on $\mathfrak{j}$ if $g \in \Lambda$.

Hence, $g\left(\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}}\right)$ is well-defined for every $g \in R(\mathbf{x})$, every countable (i.e., finite or countably infinite) set $\mathbf{I}$, every topological commutative $\mathbf{k}$-algebra $R$ and every power-summable family $\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} \in R^{\mathbf{I}}$ of elements of $R$, as long as a bijection $\mathfrak{j}$ is chosen. In particular, we can apply this to $g = f$, $\mathbf{I} = \operatorname{SIS}(\ell)$, $R = \mathbf{k}\left[\left[\mathbf{x}\right]\right]$ and $\left(s_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbf{I}} = \left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}$, choosing $\mathfrak{j}$ to be the bijection which sends every positive integer $k$ to the $k$-th smallest element of $\operatorname{SIS}(\ell)$ in the lexicographic order. (Of course, since $f \in \Lambda$, the choice of $\mathfrak{j}$ is irrelevant.)

[326] Recall that $e_0 = 1$, and that $e_s = 0$ for $s < 0$.

The power series $M_\alpha^{\langle s\rangle}$ are the power series $e_s(\alpha)$ in [93]. We will shortly (in Corollary 6.5.8(a)) see that $M_\alpha^{\langle s\rangle} \in \operatorname{QSym}$ (although this is also easy to prove by inspection). Here are some examples of $M_\alpha^{\langle s\rangle}$:

**Example 6.5.2.** If $\alpha$ is a composition and $\ell$ denotes its length $\ell(\alpha)$, then

$$M_\alpha^{\langle 0\rangle} = \underbrace{e_0}_{=1}\left(\left(\mathbf{x}_{\mathbf{i}}^\alpha\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) = 1\left(\left(\mathbf{x}_{\mathbf{i}}^\alpha\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) = 1$$

and

$$M_\alpha^{\langle 1\rangle} = e_1\left(\left(\mathbf{x}_{\mathbf{i}}^\alpha\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) = \sum_{\mathbf{i}\in\operatorname{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^\alpha = M_\alpha \qquad \text{(by (6.5.1))}$$

and[327]

$$M_\alpha^{\langle 2\rangle} = e_2\left(\left(\mathbf{x}_{\mathbf{i}}^\alpha\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) = \sum_{\substack{\mathbf{i}\in\operatorname{SIS}(\ell),\ \mathbf{j}\in\operatorname{SIS}(\ell);\\ \mathbf{i}<\mathbf{j}}} \mathbf{x}_{\mathbf{i}}^\alpha \mathbf{x}_{\mathbf{j}}^\alpha$$

(where the notation "$\mathbf{i} < \mathbf{j}$" should be interpreted with respect to an arbitrary but fixed total order on the set $\operatorname{SIS}(\ell)$ – for example, the lexicographic order). Applying the last of these three equalities to $\alpha = (2,1)$, we obtain

$$\begin{aligned}
M_{(2,1)}^{\langle 2\rangle} &= \sum_{\substack{\mathbf{i}\in\operatorname{SIS}(2),\ \mathbf{j}\in\operatorname{SIS}(2),\\ \mathbf{i}<\mathbf{j}}} \mathbf{x}_{\mathbf{i}}^{(2,1)}\mathbf{x}_{\mathbf{j}}^{(2,1)} = \sum_{\substack{(i_1,i_2)\in\operatorname{SIS}(2),\ (j_1,j_2)\in\operatorname{SIS}(2);\\ (i_1,i_2)<(j_1,j_2)}} \underbrace{\mathbf{x}_{(i_1,i_2)}^{(2,1)}}_{=x_{i_1}^2 x_{i_2}^1} \underbrace{\mathbf{x}_{(j_1,j_2)}^{(2,1)}}_{=x_{j_1}^2 x_{j_2}^1} \\
&= \sum_{\substack{(i_1,i_2)\in\operatorname{SIS}(2),\ (j_1,j_2)\in\operatorname{SIS}(2);\\ (i_1,i_2)<(j_1,j_2)}} x_{i_1}^2 x_{i_2}^1 x_{j_1}^2 x_{j_2}^1 \\
&= \underbrace{\sum_{\substack{i_1<i_2;\ j_1<j_2;\\ i_1<j_1}} x_{i_1}^2 x_{i_2}^1 x_{j_1}^2 x_{j_2}^1}_{=M_{(2,1,2,1)}+M_{(2,3,1)}+2M_{(2,2,1,1)}+M_{(2,2,2)}} + \underbrace{\sum_{\substack{i_1<i_2;\ j_1<j_2;\\ i_1=j_1;\ i_2<j_2}} x_{i_1}^2 x_{i_2}^1 x_{j_1}^2 x_{j_2}^1}_{=M_{(4,1,1)}} \\
&\qquad \left(\begin{array}{c}\text{here, we have WLOG assumed that the}\\ \text{order on } \operatorname{SIS}(2) \text{ is lexicographic}\end{array}\right) \\
&= M_{(2,1,2,1)} + M_{(2,3,1)} + 2M_{(2,2,1,1)} + M_{(2,2,2)} + M_{(4,1,1)}.
\end{aligned}$$

Of course, every negative integer $s$ satisfies $M_\alpha^{\langle s\rangle} = \underbrace{e_s}_{=0}\left(\left(\mathbf{x}_{\mathbf{i}}^\alpha\right)_{\mathbf{i}\in\operatorname{SIS}(\ell)}\right) = 0$.

There is a determinantal formula for the $s!M_\alpha^{\langle s\rangle}$ (and thus also for $M_\alpha^{\langle s\rangle}$ when $s!$ is invertible in $\mathbf{k}$), but in order to state it, we need to introduce one more notation:

**Definition 6.5.3.** Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ be a composition, and let $k$ be a positive integer. Then, $\alpha\{k\}$ will denote the composition $(k\alpha_1, k\alpha_2, \ldots, k\alpha_\ell)$. Clearly, $\ell(\alpha\{k\}) = \ell(\alpha)$ and $|\alpha\{k\}| = k|\alpha|$.

**Exercise 6.5.4.** Let $\alpha$ be a composition. Write the composition $\alpha$ in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$.

[327] This is not completely obvious, but easy to check (see Exercise 6.5.4(b)).

(a) Show that the $s$-th power-sum symmetric function $p_s \in \Lambda$ satisfies

$$p_s \left( \left( \mathbf{x}_{\mathbf{i}}^{\alpha} \right)_{\mathbf{i} \in \operatorname{SIS}(\ell)} \right) = M_{\alpha\{s\}}$$

for every positive integer $s$.

(b) Let us fix a total order on the set $\operatorname{SIS}(\ell)$ (for example, the lexicographic order). Show that the $s$-th elementary symmetric function $e_s \in \Lambda$ satisfies

$$M_{\alpha}^{\langle s \rangle} = e_s \left( \left( \mathbf{x}_{\mathbf{i}}^{\alpha} \right)_{\mathbf{i} \in \operatorname{SIS}(\ell)} \right) = \sum_{\substack{(\mathbf{i}_1, \mathbf{i}_2, \ldots, \mathbf{i}_s) \in (\operatorname{SIS}(\ell))^s; \\ \mathbf{i}_1 < \mathbf{i}_2 < \cdots < \mathbf{i}_s}} \mathbf{x}_{\mathbf{i}_1}^{\alpha} \mathbf{x}_{\mathbf{i}_2}^{\alpha} \cdots \mathbf{x}_{\mathbf{i}_s}^{\alpha}$$

for every $s \in \mathbb{N}$.

(c) Let $s \in \mathbb{N}$, and let $n$ be a positive integer. Let $e_s^{\langle n \rangle}$ be the symmetric function $\sum_{i_1 < i_2 < \cdots < i_s} x_{i_1}^n x_{i_2}^n \cdots x_{i_s}^n \in \Lambda$. Then, show that

$$M_{\alpha\{n\}}^{\langle s \rangle} = e_s^{\langle n \rangle} \left( \left( \mathbf{x}_{\mathbf{i}}^{\alpha} \right)_{\mathbf{i} \in \operatorname{SIS}(\ell)} \right).$$

(d) Let $s \in \mathbb{N}$, and let $n$ be a positive integer. Prove that there exists a polynomial $P \in \mathbf{k}[z_1, z_2, z_3, \ldots]$ such that

$$M_{\alpha\{n\}}^{\langle s \rangle} = P \left( M_{\alpha}^{\langle 1 \rangle}, M_{\alpha}^{\langle 2 \rangle}, M_{\alpha}^{\langle 3 \rangle}, \ldots \right).$$

[**Hint:** For (a), (b) and (c), apply the definition of $f \left( \left( \mathbf{x}_{\mathbf{i}}^{\alpha} \right)_{\mathbf{i} \in \operatorname{SIS}(\ell)} \right)$ with $f$ a symmetric function[328]. For (d), recall that $\Lambda$ is generated by $e_1, e_2, e_3, \ldots$.]

**Exercise 6.5.5.** Let $s \in \mathbb{N}$. Show that the composition $(1)$ satisfies $M_{(1)}^{\langle s \rangle} = e_s$.

**Proposition 6.5.6.** *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ be a composition.*

*(a) Let $n \in \mathbb{N}$. Define a matrix $A_n^{\langle \alpha \rangle} = \left( a_{i,j}^{\langle \alpha \rangle} \right)_{i,j=1,2,\ldots,n}$ by*

$$a_{i,j}^{\langle \alpha \rangle} = \begin{cases} M_{\alpha\{i-j+1\}}, & \text{if } i \geq j; \\ i, & \text{if } i = j - 1; \\ 0, & \text{if } i < j - 1 \end{cases} \qquad \text{for all } (i,j) \in \{1, 2, \ldots, n\}^2.$$

[328] There are two subtleties that need to be addressed:

- the fact that the definition of $f \left( \left( \mathbf{x}_{\mathbf{i}}^{\alpha} \right)_{\mathbf{i} \in \operatorname{SIS}(\ell)} \right)$ distinguishes between two cases depending on whether or not $\operatorname{SIS}(\ell)$ is finite;
- the fact that the total order on the set $\{1, 2, 3, \ldots\}$ (which appears in the summation subscript in the equality $e_s = \sum_{\substack{(i_1, i_2, \ldots, i_s) \in \{1,2,3,\ldots\}^s; \\ i_1 < i_2 < \cdots < i_s}} x_{i_1} x_{i_2} \cdots x_{i_s}$) has nothing to do with the total order on the set $\operatorname{SIS}(\ell)$ (which appears in the summation subscript in $\sum_{\substack{(\mathbf{i}_1, \mathbf{i}_2, \ldots, \mathbf{i}_s) \in (\operatorname{SIS}(\ell))^s; \\ \mathbf{i}_1 < \mathbf{i}_2 < \cdots < \mathbf{i}_s}} \mathbf{x}_{\mathbf{i}_1}^{\alpha} \mathbf{x}_{\mathbf{i}_2}^{\alpha} \cdots \mathbf{x}_{\mathbf{i}_s}^{\alpha}$). For instance, the former total order is well-founded, whereas the latter may and may not be. So there is (generally) no bijection between $\{1, 2, 3, \ldots\}$ and $\operatorname{SIS}(\ell)$ preserving these orders (even if $\operatorname{SIS}(\ell)$ is infinite). Fortunately, this does not matter much, because the total order is only being used to ensure that every product of $s$ distinct elements appears exactly once in the sum.

*This matrix* $A_n^{\langle\alpha\rangle}$ *looks as follows:*

$$A_n^{\langle\alpha\rangle} = \begin{pmatrix} M_{\alpha\{1\}} & 1 & 0 & \cdots & 0 & 0 \\ M_{\alpha\{2\}} & M_{\alpha\{1\}} & 2 & \cdots & 0 & 0 \\ M_{\alpha\{3\}} & M_{\alpha\{2\}} & M_{\alpha\{1\}} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ M_{\alpha\{n-1\}} & M_{\alpha\{n-2\}} & M_{\alpha\{n-3\}} & \cdots & M_{\alpha\{1\}} & n-1 \\ M_{\alpha\{n\}} & M_{\alpha\{n-1\}} & M_{\alpha\{n-2\}} & \cdots & M_{\alpha\{2\}} & M_{\alpha\{1\}} \end{pmatrix}.$$

*Then,* $\det\left(A_n^{\langle\alpha\rangle}\right) = n! M_\alpha^{\langle n\rangle}$.

*(b) Let* $n$ *be a positive integer. Define a matrix* $B_n^{\langle\alpha\rangle} = \left(b_{i,j}^{\langle\alpha\rangle}\right)_{i,j=1,2,\ldots,n}$ *by*

$$b_{i,j}^{\langle\alpha\rangle} = \begin{cases} iM_\alpha^{\langle i\rangle}, & \text{if } j=1; \\ M_\alpha^{\langle i-j+1\rangle}, & \text{if } j>1 \end{cases} \qquad \text{for all } (i,j)\in\{1,2,\ldots,n\}^2.$$

*The matrix* $B_n^{\langle\alpha\rangle}$ *looks as follows:*

$$B_n^{\langle\alpha\rangle} = \begin{pmatrix} M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} & M_\alpha^{\langle -1\rangle} & \cdots & M_\alpha^{\langle -n+3\rangle} & M_\alpha^{\langle -n+2\rangle} \\ 2M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} & \cdots & M_\alpha^{\langle -n+4\rangle} & M_\alpha^{\langle -n+3\rangle} \\ 3M_\alpha^{\langle 3\rangle} & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & \cdots & M_\alpha^{\langle -n+5\rangle} & M_\alpha^{\langle -n+4\rangle} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & M_\alpha^{\langle n-3\rangle} & \cdots & M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} \\ nM_\alpha^{\langle n\rangle} & M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & \cdots & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} \end{pmatrix}$$

$$= \begin{pmatrix} M_\alpha^{\langle 1\rangle} & 1 & 0 & \cdots & 0 & 0 \\ 2M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & 1 & \cdots & 0 & 0 \\ 3M_\alpha^{\langle 3\rangle} & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & M_\alpha^{\langle n-3\rangle} & \cdots & M_\alpha^{\langle 1\rangle} & 1 \\ nM_\alpha^{\langle n\rangle} & M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & \cdots & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} \end{pmatrix}.$$

*Then,* $\det\left(B_n^{\langle\alpha\rangle}\right) = M_{\alpha\{n\}}$.

**Exercise 6.5.7.** Prove Proposition 6.5.6.

[**Hint:** Substitute $(\mathbf{x}_\mathbf{i}^\alpha)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$ for the variable set in Exercise 2.9.13, and recall Exercise 6.5.4(a).]

**Corollary 6.5.8.** *Let* $\alpha$ *be a composition. Let* $s\in\mathbb{Z}$.

(a) *We have* $M_\alpha^{\langle s\rangle}\in\mathrm{QSym}$.

(b) *We have* $M_\alpha^{\langle s\rangle}\in\mathrm{QSym}_{s|\alpha|}$.

**Exercise 6.5.9.** Prove Corollary 6.5.8.

We make one further definition:

**Definition 6.5.10.** Let $\alpha$ be a nonempty composition. Then, we denote by $\gcd\alpha$ the greatest common divisor of the parts of $\alpha$. (For instance, $\gcd(8,6,4)=2$.) We also define $\operatorname{red}\alpha$ to be the composition $\left(\frac{\alpha_1}{\gcd\alpha}, \frac{\alpha_2}{\gcd\alpha}, \ldots, \frac{\alpha_\ell}{\gcd\alpha}\right)$, where $\alpha$ is written in the form $(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$.

We say that a nonempty composition $\alpha$ is *reduced* if $\gcd \alpha = 1$.

We define $\mathfrak{RL}$ to be the set of all reduced Lyndon compositions. In other words, $\mathfrak{RL} = \{w \in \mathfrak{L} \mid w \text{ is reduced}\}$ (since $\mathfrak{L}$ is the set of all Lyndon compositions).

Hazewinkel, in [93, proof of Thm. 6.7.5], denotes $\mathfrak{RL}$ by $eLYN$, calling reduced Lyndon compositions "elementary Lyndon words".

*Remark* 6.5.11. Let $\alpha$ be a nonempty composition.

(a) We have $\alpha = (\operatorname{red} \alpha) \{\gcd \alpha\}$.

(b) The composition $\alpha$ is Lyndon if and only if the composition $\operatorname{red} \alpha$ is Lyndon.

(c) The composition $\operatorname{red} \alpha$ is reduced.

(d) If $\alpha$ is reduced, then $\operatorname{red} \alpha = \alpha$.

(e) If $s \in \{1, 2, 3, \ldots\}$, then the composition $\alpha \{s\}$ is nonempty and satisfies $\operatorname{red}(\alpha \{s\}) = \operatorname{red} \alpha$ and $\gcd(\alpha \{s\}) = s \gcd \alpha$.

(f) We have $(\gcd \alpha) |\operatorname{red} \alpha| = |\alpha|$.

**Exercise 6.5.12.** Prove Remark 6.5.11.

Our goal in this section is now to prove the following result of Hazewinkel:

**Theorem 6.5.13.** *The family* $\left(M_w^{\langle s \rangle}\right)_{(w,s) \in \mathfrak{RL} \times \{1,2,3,\ldots\}}$ *is an algebraically independent generating set of the* $\mathbf{k}$*-algebra* QSym.

This will (almost) immediately yield Theorem 6.4.3.

Our first step towards proving Theorem 6.5.13 is the following observation:

**Lemma 6.5.14.** *The family* $\left(M_w^{\langle s \rangle}\right)_{(w,s) \in \mathfrak{RL} \times \{1,2,3,\ldots\}}$ *is a reindexing of the family* $\left(M_{\operatorname{red} \alpha}^{\langle \gcd \alpha \rangle}\right)_{\alpha \in \mathfrak{L}}$.

**Exercise 6.5.15.** Prove Lemma 6.5.14.

Next, we show a lemma:

**Lemma 6.5.16.** *Let $\alpha$ be a nonempty composition. Let $s \in \mathbb{N}$. Then,*

$$s! M_\alpha^{\langle s \rangle} - M_\alpha^s \in \sum_{\substack{\beta \in \mathrm{Comp}_{s|\alpha|}; \\ \ell(\beta) \leq (s-1)\ell(\alpha)}} \mathbf{k} M_\beta. \tag{6.5.2}$$

*(That is, $s! M_\alpha^{\langle s \rangle} - M_\alpha^s$ is a $\mathbf{k}$-linear combination of terms of the form $M_\beta$ with $\beta$ ranging over the compositions of $s|\alpha|$ satisfying $\ell(\beta) \leq (s-1)\ell(\alpha)$.)*

**Exercise 6.5.17.** Prove Lemma 6.5.16.

[**Hint:** There are two approaches: One is to apply Proposition 6.5.6(a) and expand the determinant; the other is to argue which monomials can appear in $s! M_\alpha^{\langle s \rangle} - M_\alpha^s$.]

We now return to studying products of monomial quasisymmetric functions:

**Lemma 6.5.18.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \mathrm{Comp}_n$ and $v \in \mathrm{Comp}_m$. Let $z$ be the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Let*

*$h$ be the multiplicity with which the word $z$ appears in the multiset $u \sqcup\!\sqcup v$. Then,*[329]

$$M_u M_v = h M_z + \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} z\Big).$$

*Proof of Lemma 6.5.18.* Lemma 6.5.18 was shown during the proof of Lemma 6.4.11(b). □

**Corollary 6.5.19.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \operatorname{Comp}_n$ and $v \in \operatorname{Comp}_m$. Regard $u$ and $v$ as words in $\mathfrak{A}^*$. Assume that $u$ is a Lyndon word. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of the word $v$.*

*Assume that $u \geq b_j$ for every $j \in \{1, 2, \ldots, q\}$. Let*

$$h = 1 + |\{j \in \{1, 2, \ldots, q\} \mid b_j = u\}|.$$

*Then,*

$$M_u M_v = h M_{uv} + \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} uv\Big).$$

**Exercise 6.5.20.** Prove Corollary 6.5.19.

[**Hint:** Apply Lemma 6.5.18, and notice that $uv$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ (by Theorem 6.2.2(e)), and that $h$ is the multiplicity with which this word $uv$ appears in the multiset $u \sqcup\!\sqcup v$ (this is a rewriting of Theorem 6.2.2(e)).]

**Corollary 6.5.21.** *Let $k \in \mathbb{N}$ and $s \in \mathbb{N}$. Let $x \in \operatorname{Comp}_k$ be such that $x$ is a Lyndon word. Then:*

(a) *The lexicographically highest element of the multiset $x \sqcup\!\sqcup x^s$ is $x^{s+1}$.*

(b) *We have*

$$M_x M_{x^s} = (s+1) M_{x^{s+1}} + \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{(s+1)k} \text{ satisfying } w \underset{\text{wll}}{<} x^{s+1}\Big).$$

(c) *Let $t \in \operatorname{Comp}_{sk}$ be such that $t \underset{\text{wll}}{<} x^s$. Then,*

$$M_x M_t = \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{(s+1)k} \text{ satisfying } w \underset{\text{wll}}{<} x^{s+1}\Big).$$

**Exercise 6.5.22.** Prove Corollary 6.5.21.

[**Hint:** Notice that $\Big(\underbrace{x, x, \ldots, x}_{s \text{ times}}\Big)$ is the CFL factorization of the word $x^s$. Now, part (a) of Corollary 6.5.21 follows from Theorem 6.2.2(c), part (b) follows from Corollary 6.5.19, and part (c) from Lemma 6.4.11(c) (using part (a)).]

[329] The following equality makes sense because we have $z \in \operatorname{Comp}_{n+m}$ (by Lemma 6.4.11(a)).

**Corollary 6.5.23.** *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \operatorname{Comp}_n$ and $v \in \operatorname{Comp}_m$. Regard $u$ and $v$ as words in $\mathfrak{A}^*$. Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of $u$. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of the word $v$. Assume that $a_i > b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$. Then,*

$$M_u M_v = M_{uv} + \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\mathrm{wll}}{<} uv\Big).$$

**Exercise 6.5.24.** Prove Corollary 6.5.23.

[**Hint:** Combine Lemma 6.5.18 with the parts (c) and (d) of Theorem 6.2.2.]

**Corollary 6.5.25.** *Let $n \in \mathbb{N}$. Let $u \in \operatorname{Comp}_n$ be a nonempty composition. Regard $u$ as a word in $\mathfrak{A}^*$. Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of $u$. Let $k \in \{1, 2, \ldots, p-1\}$ be such that $a_k > a_{k+1}$. Let $x$ be the word $a_1 a_2 \cdots a_k$, and let $y$ be the word $a_{k+1} a_{k+2} \cdots a_p$. Then,*

$$M_u = M_x M_y - \Big(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_n \text{ satisfying } w \underset{\mathrm{wll}}{<} u\Big).$$

**Exercise 6.5.26.** Prove Corollary 6.5.25.

[**Hint:** Apply Corollary 6.5.23 to $x$, $y$, $|x|$, $|y|$, $k$, $p-k$, $(a_1, a_2, \ldots, a_k)$ and $(a_{k+1}, a_{k+2}, \ldots, a_p)$ instead of $u$, $v$, $n$, $m$, $p$, $q$, $(a_1, a_2, \ldots, a_p)$ and $(b_1, b_2, \ldots, b_q)$; then, notice that $xy = u$ and $|x| + |y| = n$.]

**Corollary 6.5.27.** *Let $k \in \mathbb{N}$. Let $x \in \operatorname{Comp}_k$ be a composition. Assume that $x$ is a Lyndon word. Let $s \in \mathbb{N}$. Then,*

$$M_x^s - s! M_{x^s} \in \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\mathrm{wll}}{<} x^s}} \mathbf{k} M_w.$$

*(Recall that $x^s$ is defined to be the word $\underbrace{xx \cdots x}_{s \text{ times}}$.)*

**Exercise 6.5.28.** Prove Corollary 6.5.27.

[**Hint:** Rewrite the claim of Corollary 6.5.27 in the form $M_x^s \in s! M_{x^s} + \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\mathrm{wll}}{<} x^s}} \mathbf{k} M_w$. This can be proven by induction over $s$, where in the induction step we need the following two observations:

(1) We have $M_x M_{x^s} \in (s+1) M_{x^{s+1}} + \sum_{\substack{w \in \operatorname{Comp}_{(s+1)k}; \\ w \underset{\mathrm{wll}}{<} x^{s+1}}} \mathbf{k} M_w$.

(2) For every $t \in \operatorname{Comp}_{sk}$ satisfying $t \underset{\mathrm{wll}}{<} x^s$, we have $M_x M_t \in \sum_{\substack{w \in \operatorname{Comp}_{(s+1)k}; \\ w \underset{\mathrm{wll}}{<} x^{s+1}}} \mathbf{k} M_w$.

These two observations follow from parts (b) and (c) of Corollary 6.5.21.]

**Corollary 6.5.29.** *Let $k \in \mathbb{N}$. Let $x \in \operatorname{Comp}_k$ be a composition. Assume that $x$ is a Lyndon word. Let $s \in \mathbb{N}$. Then,*

$$M_x^{\langle s \rangle} - M_{x^s} \in \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w .$$

*(Recall that $x^s$ is defined to be the word $\underbrace{xx \cdots x}_{s \text{ times}}$.)*

**Exercise 6.5.30.** Prove Corollary 6.5.29.

[**Hint:** Lemma 6.5.16 (applied to $\alpha = x$) yields

$$s! M_x^{\langle s \rangle} - M_x^s \in \sum_{\substack{\beta \in \operatorname{Comp}_{sk}; \\ \ell(\beta) \leq (s-1)\ell(x)}} M_\beta = \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ \ell(w) \leq (s-1)\ell(x)}} \mathbf{k} M_w \subset \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$$

[330]. Adding this to the claim of Corollary 6.5.27, obtain $s! M_x^{\langle s \rangle} - s! M_{x^s} \in \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$, that is, $s! \left( M_x^{\langle s \rangle} - M_{x^s} \right) \in \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$. It remains to get rid of the $s!$ on the left hand side. Assume WLOG that $\mathbf{k} = \mathbb{Z}$, and argue that every $f \in \operatorname{QSym}$ satisfying $s! \cdot f \in \sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$ must itself lie in $\sum_{\substack{w \in \operatorname{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$.]

We are now ready to prove Theorem 6.5.13:

**Exercise 6.5.31.** Prove Theorem 6.5.13.

[**Hint:** Lemma 6.5.14 yields that the family $\left( M_w^{\langle s \rangle} \right)_{(w,s) \in \mathfrak{RL} \times \{1,2,3,\ldots\}}$ is a reindexing of the family $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$. Hence, it is enough to prove that the family $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym. The latter claim, in turn, will follow from Lemma 6.3.7(c)[331] once it is proven that the family $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$ generates the $\mathbf{k}$-algebra QSym. So it remains to show that the family $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$ generates the $\mathbf{k}$-algebra QSym.

Let $U$ denote the $\mathbf{k}$-subalgebra of QSym generated by $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$. It then suffices to prove that $U = \operatorname{QSym}$. To this purpose, it is enough to prove that

$$M_\beta \in U \qquad \text{for every composition } \beta. \tag{6.5.3}$$

For every reduced Lyndon composition $\alpha$ and every $j \in \{1,2,3,\ldots\}$, the quasisymmetric function $M_\alpha^{\langle j \rangle}$ is an element of the family $\left( M_{\operatorname{red} w}^{\langle \gcd w \rangle} \right)_{w \in \mathfrak{L}}$

[330] since every $w \in \operatorname{Comp}_{sk}$ with the property that $\ell(w) \leq (s-1)\ell(x)$ must satisfy $w \underset{\text{wll}}{<} x^s$

[331] applied to $A = \operatorname{QSym}$, $b_w = M_{\operatorname{red} w}^{\langle \gcd w \rangle}$, $\operatorname{wt}(N) = N$ and $g_u = M_u$

and thus belongs to $U$. Combine this with Exercise 6.5.4(d) to see that

(6.5.4)
$$M_\beta^{\langle s\rangle} \in U \qquad \text{for every Lyndon composition } \beta \text{ and every } s \in \{1,2,3,\ldots\}$$

(because every Lyndon composition $\beta$ can be written as $\alpha\{n\}$ for a reduced Lyndon composition $\alpha$ and an $n \in \{1,2,3,\ldots\}$). Now, prove (6.5.3) by strong induction: first, induct on $|\beta|$, and then, for fixed $|\beta|$, induct on $\beta$ in the wll-order. The induction step looks as follows: Fix some composition $\alpha$, and assume (as induction hypothesis) that:

- (6.5.3) holds for every composition $\beta$ satisfying $|\beta| < |\alpha|$;
- (6.5.3) holds for every composition $\beta$ satisfying $|\beta| = |\alpha|$ and $\beta \underset{\text{wll}}{<} \alpha$.

It remains to prove that (6.5.3) holds for $\beta = \alpha$. In other words, it remains to prove that $M_\alpha \in U$.

Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of the word $\alpha$. Assume WLOG that $p \neq 0$ (else, all is trivial). We are in one of the following two cases:

*Case 1:* All of the words $a_1$, $a_2$, …, $a_p$ are equal.

*Case 2:* Not all of the words $a_1$, $a_2$, …, $a_p$ are equal.

In Case 2, there exists a $k \in \{1, 2, \ldots, p-1\}$ satisfying $a_k > a_{k+1}$ (since $a_1 \geq a_2 \geq \cdots \geq a_p$), and thus Corollary 6.5.25 (applied to $u = \alpha$, $n = |\alpha|$, $x = a_1 a_2 \cdots a_k$ and $y = a_{k+1} a_{k+2} \cdots a_p$) shows that

$$M_\alpha = \underbrace{M_{a_1 a_2 \cdots a_k}}_{\substack{\in U \\ \text{(by the induction} \\ \text{hypothesis)}}} \underbrace{M_{a_{k+1} a_{k+2} \cdots a_p}}_{\substack{\in U \\ \text{(by the induction} \\ \text{hypothesis)}}} - \left( \text{a sum of terms of the form } \underbrace{M_w}_{\substack{\in U \\ \text{(by the induction} \\ \text{hypothesis)}}} \text{ with } w \in \operatorname{Comp}_{|\alpha|} \text{ satisfying } w \underset{\text{wll}}{<} \alpha \right)$$
$$\in UU - (\text{a sum of terms in } U) \subset U.$$

Hence, it only remains to deal with Case 1. In this case, set $x = a_1 = a_2 = \cdots = a_p$. Thus, $\alpha = a_1 a_2 \cdots a_p = x^p$, whence $|\alpha| = p\,|x|$. But

Corollary 6.5.29 (applied to $s = p$ and $k = |x|$) yields

$$M_x^{\langle p \rangle} - M_{x^p} \in \sum_{\substack{w \in \operatorname{Comp}_{p|x|};\\ w \underset{\text{wll}}{<} x^p}} \mathbf{k} M_w = \sum_{\substack{w \in \operatorname{Comp}_{|\alpha|};\\ w \underset{\text{wll}}{<} \alpha}} \mathbf{k} \underbrace{M_w}_{\substack{\in U \\ \text{(by the induction} \\ \text{hypothesis)}}}$$

$$\left(\text{since } p\,|x| = |\alpha| \text{ and } x^p = \alpha\right)$$

$$\subset \sum_{\substack{w \in \operatorname{Comp}_N;\\ w \underset{\text{wll}}{<} \alpha}} \mathbf{k} U \subset U,$$

so that $M_{x^p} \in \underbrace{M_x^{\langle p \rangle}}_{\substack{\in U \\ \text{(by (6.5.4))}}} - U \subset U - U \subset U$. This rewrites as $M_\alpha \in U$ (since $\alpha = x^p$). So $M_\alpha \in U$ is proven in both Cases 1 and 2, and thus the induction proof of (6.5.3) is finished.]

**Exercise 6.5.32.** Prove Theorem 6.4.3.

Of course, this proof of Theorem 6.4.3 yields a new (third) proof for Proposition 6.4.4.

We notice the following corollary of our approach to Theorem 6.4.3:

**Corollary 6.5.33.** *The* $\Lambda$*-algebra* QSym *is a polynomial algebra (over* $\Lambda$*).*

**Exercise 6.5.34.** Prove Corollary 6.5.33.

[**Hint:** The algebraically independent generating set $\left(M_w^{\langle s \rangle}\right)_{(w,s) \in \mathfrak{RL} \times \{1,2,3,\ldots\}}$ of QSym contains the elements $M_{(1)}^{\langle s \rangle} = e_s \in \Lambda$ for all $s \in \{1, 2, 3, \ldots\}$.]

## 6.6. The Gessel-Reutenauer bijection and symmetric functions.

In this section, we shall discuss the Gessel-Reutenauer bijection between words and multisets of aperiodic necklaces, and use it to study another family of symmetric functions.

The Gessel-Reutenauer bijection was studied in [82], where it was applied to various enumeration problems (e.g., counting permutations in $\mathfrak{S}_n$ with given descent set and given cycle type); it is also closely related to the Burrows-Wheeler bijection used in data compression ([45]), and to the structure of free Lie algebras ([81], [182]). We shall first introduce the Gessel-Reutenauer bijection and study it combinatorially in Subsection 6.6.1; then, in the following Subsection 6.6.2, we shall apply it to symmetric functions.

### 6.6.1. *Necklaces and the Gessel-Reutenauer bijection.*

We begin with definitions, some of which have already been made in Exercise 6.1.34:

**Definition 6.6.1.** Throughout Section 6.6, we shall freely use Definition 6.1.1 and Definition 6.1.13. We fix a totally ordered alphabet $\mathfrak{A}$. (This alphabet can be arbitrary, although most examples will use $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$.)

Let $C$ denote the infinite cyclic group, written multiplicatively. Fix a generator $c$ of $C$. [332]

[332] So $C$ is a group isomorphic to $(\mathbb{Z}, +)$, and the isomorphism $(\mathbb{Z}, +) \to C$ sends every $n \in \mathbb{Z}$ to $c^n$. (Recall that we write the binary operation of $C$ as $\cdot$ instead of $+$.)

For any positive integer $n$, the group $C$ acts on $\mathfrak{A}^n$ from the left according to the rule

$$c \cdot (a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_n, a_1) \qquad \text{for all } (a_1, a_2, \ldots, a_n) \in \mathfrak{A}^n.$$

[333] The orbits of this $C$-action will be called *$n$-necklaces*[334]; they form a set partition of the set $\mathfrak{A}^n$.

The $n$-necklace containing a given $n$-tuple $w \in \mathfrak{A}^n$ will be denoted by $[w]$.

A *necklace* shall mean an $n$-necklace for some positive integer $n$. Thus, for each nonempty word $w$, there is a well-defined necklace $[w]$ (namely, $[w]$ is an $n$-necklace, where $n = \ell(w)$).

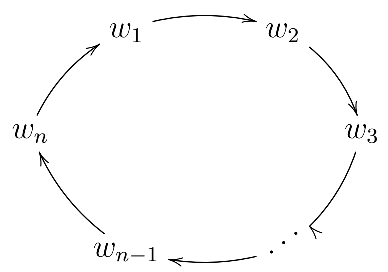
The *period* of a necklace $N$ is defined as the positive integer $|N|$. (This $|N|$ is indeed a positive integer, since $N$ is a finite nonempty set[335].)

An $n$-necklace is said to be *aperiodic* if its period is $n$.

**Example 6.6.2.** Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$. The orbit of the word 223 under the $C$-action is the 3-necklace $\{223, 232, 322\}$; it is an aperiodic 3-necklace. The orbit of the word 223223 under the $C$-action is the 6-necklace $\{223223, 232232, 322322\}$; it is not aperiodic (since it has period 3). The orbit of any nonempty word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ is the $n$-necklace

$$\{(w_i, w_{i+1}, \ldots, w_n, w_1, w_2, \ldots, w_{i-1}) \mid i \in \{1, 2, \ldots, n\}\}.$$

We can draw this $n$-necklace on the plane as follows:



It is easy to see that the notion of an "aperiodic necklace" we just defined is equivalent to the notion of a "primitive necklace" used in Exercise 4.6.4(b).

Exercise 6.1.34(a) shows that any $n$-necklace for any positive integer $n$ is a finite nonempty set. In other words, any necklace is a finite nonempty set.

Let us next introduce some notations regarding words and permutations. We recall that a cycle of a permutation $\tau \in \mathfrak{S}_n$ is an orbit under the action of $\tau$ on $\{1, 2, \ldots, n\}$. (This orbit can be a 1-element set, when $\tau$ has fixed points.) We begin with a basic definition:

**Definition 6.6.3.** Let $\tau \in \mathfrak{S}_n$ be a permutation. Let $h \in \{1, 2, \ldots, n\}$.

[333] In other words, $c$ rotates any $n$-tuple of elements of $\mathfrak{A}$ cyclically to the left. Thus, $c^n \in C$ acts trivially on $\mathfrak{A}^n$, and so this action of $C$ on $\mathfrak{A}^n$ factors through $C / \langle c^n \rangle$ (a cyclic group of order $n$).

[334] See Exercise 6.1.34 for the motivation behind this word.

Notice that there are no 0-necklaces, because we required $n$ to be positive in the definition of a necklace. This is intentional.

[335] by Exercise 6.1.34(a), because $N$ is an $n$-necklace for some positive integer $n$

(a) We let $\operatorname{ord}_\tau(h)$ denote the smallest positive integer $i$ such that $\tau^i(h) = h$. (Basic properties of permutations show that this $i$ exists.)

(b) Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Then, $w_{\tau,h}$ shall denote the word $w_{\tau^1(h)} w_{\tau^2(h)} \cdots w_{\tau^k(h)}$, where $k = \operatorname{ord}_\tau(h)$.

**Example 6.6.4.** Let $\tau$ be the permutation $3142765 \in \mathfrak{S}_7$ (in one-line notation). Then, $\operatorname{ord}_\tau(1) = 4$ (since $\tau^4(1) = 1$, but $\tau^i(1) \neq 1$ for every positive integer $i < 4$). Likewise, $\operatorname{ord}_\tau(2) = 4$ and $\operatorname{ord}_\tau(3) = 4$ and $\operatorname{ord}_\tau(4) = 4$ and $\operatorname{ord}_\tau(5) = 2$ and $\operatorname{ord}_\tau(6) = 1$ and $\operatorname{ord}_\tau(7) = 2$.

Now, let $w$ be the word $4112524 \in \mathfrak{A}^7$. Then,

$$\begin{aligned} w_{\tau,3} &= w_{\tau^1(3)} w_{\tau^2(3)} w_{\tau^3(3)} w_{\tau^4(3)} \qquad \left(\text{since } \operatorname{ord}_\tau(3) = 4\right) \\ &= w_4 w_2 w_1 w_3 \\ &\qquad \left(\begin{array}{c} \text{since } \tau^1(3) = 4 \text{ and } \tau^2(3) = \tau(4) = 2 \\ \text{and } \tau^3(3) = \tau(2) = 1 \text{ and } \tau^4(3) = \tau(1) = 3 \end{array}\right) \\ &= 2141. \end{aligned}$$

Likewise, we can check that $w_{\tau,1} = w_3 w_4 w_2 w_1 = 1214$ and $w_{\tau,5} = w_7 w_5 = 45$ and $w_{\tau,6} = w_6 = 2$.

We begin the study of the words $w_{\tau,h}$ by stating some of their simplest properties:[336]

**Proposition 6.6.5.** *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Let $\tau \in \mathfrak{S}_n$. Let $h \in \{1, 2, \ldots, n\}$. Then:*

(a) *The word $w_{\tau,h}$ is nonempty and has length* $\operatorname{ord}_\tau(h)$.

(b) *The first letter of the word $w_{\tau,h}$ is $w_{\tau(h)}$.*

(c) *The last letter of the word $w_{\tau,h}$ is $w_h$.*

(d) *We have $w_{\tau,\tau(h)} = c \cdot w_{\tau,h}$.*

(e) *We have $w_{\tau,\tau^i(h)} = c^i \cdot w_{\tau,h}$ for each $i \in \mathbb{Z}$.*

Recall that if $n \in \mathbb{N}$ and if $w \in \mathfrak{A}^n$ is a word, then a permutation $\operatorname{std} w \in \mathfrak{S}_n$ was defined in Definition 5.3.3. The words $w_{\tau,h}$ have particularly nice properties when $\tau = (\operatorname{std} w)^{-1}$:

**Lemma 6.6.6.** *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let $\alpha$ and $\beta$ be two elements of $\{1, 2, \ldots, n\}$ such that $\alpha < \beta$. Then:*

(a) *If $\tau^{-1}(\alpha) < \tau^{-1}(\beta)$, then $w_\alpha \leq w_\beta$.*

(b) *If $\tau^{-1}(\alpha) \geq \tau^{-1}(\beta)$, then $w_\alpha > w_\beta$.*

(c) *We have $w_{\tau(\alpha)} \leq w_{\tau(\beta)}$.*

(d) *If $\tau(\alpha) \geq \tau(\beta)$, then $w_{\tau(\alpha)} < w_{\tau(\beta)}$.*

(e) *If $w_{\tau(\alpha)} = w_{\tau(\beta)}$, then $\tau(\alpha) < \tau(\beta)$.*

(f) *If $w_{\tau,\alpha} = w_{\tau,\beta}$, then $\tau(\alpha) < \tau(\beta)$ and $w_{\tau,\tau(\alpha)} = w_{\tau,\tau(\beta)}$.*

(g) *If $w_{\tau,\alpha} = w_{\tau,\beta}$, then $\tau^i(\alpha) < \tau^i(\beta)$ for each $i \in \mathbb{N}$.*

(h) *Let $j \in \mathbb{N}$ be such that every $i \in \{0, 1, \ldots, j-1\}$ satisfies $w_{\tau^{i+1}(\alpha)} = w_{\tau^{i+1}(\beta)}$. Then, $w_{\tau^{j+1}(\alpha)} \leq w_{\tau^{j+1}(\beta)}$.*

**Proposition 6.6.7.** *Let $w \in \mathfrak{A}^n$ be a word. Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let $z$ be a cycle of $\tau$. Then:*

[336] See Exercise 6.6.8 below for the proof of Proposition 6.6.5, as well as for the proofs of all other propositions stated before Exercise 6.6.8.

(a) *For each $h \in z$, we have $[w_{\tau,h}] = \{w_{\tau,i} \mid i \in z\}$.*
(b) *If $\alpha$ and $\beta$ are two distinct elements of $z$, then $w_{\tau,\alpha} \neq w_{\tau,\beta}$.*
(c) *We have $|\{w_{\tau,i} \mid i \in z\}| = |z|$.*
(d) *The set $\{w_{\tau,i} \mid i \in z\}$ is an aperiodic necklace.*

**Exercise 6.6.8.** Prove Proposition 6.6.5, Lemma 6.6.6 and Proposition 6.6.7.

**Definition 6.6.9.** Let $w \in \mathfrak{A}^n$ be a word. Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let $z$ be a cycle of $\tau$. Then, we define an aperiodic necklace $[w]_z$ by $[w]_z = \{w_{\tau,i} \mid i \in z\}$. (This is indeed an aperiodic necklace, according to Proposition 6.6.7(d).)

**Example 6.6.10.** Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let $w$ be the word $2511321 \in \mathfrak{A}^7$. Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_7$; this is the permutation 3471652 (in one-line notation). One cycle of $\tau$ is $z = \{1, 3, 7, 2, 4\}$. The corresponding aperiodic necklace $[w]_z$ is

$$\begin{aligned}
[w]_z &= \{w_{\tau,i} \mid i \in z\} \\
&= \{w_{\tau,1}, w_{\tau,3}, w_{\tau,7}, w_{\tau,2}, w_{\tau,4}\} \qquad (\text{since } z = \{1,3,7,2,4\}) \\
&= \{11512, 15121, 51211, 12115, 21151\} = [11512] .
\end{aligned}$$

**Definition 6.6.11.** We let $\mathfrak{N}$ be the set of all necklaces. We let $\mathfrak{N}^{\mathfrak{a}}$ be the set of all aperiodic necklaces. We let $\mathfrak{M}\mathfrak{N}^{\mathfrak{a}}$ be the set of all finite multisets of aperiodic necklaces.

**Definition 6.6.12.** We define a map $\operatorname{GR} : \mathfrak{A}^* \to \mathfrak{M}\mathfrak{N}^{\mathfrak{a}}$ as follows:

Let $w \in \mathfrak{A}^*$. Let $n = \ell(w)$ (so that $w \in \mathfrak{A}^n$). Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Then, we define the multiset $\operatorname{GR} w \in \mathfrak{M}\mathfrak{N}^{\mathfrak{a}}$ by setting

$$\operatorname{GR} w = \{[w]_z \mid z \text{ is a cycle of } \tau\}_{\text{multiset}} .$$

(This multiset $\operatorname{GR} w$ is indeed a finite multiset of aperiodic necklaces[337], and thus belongs to $\mathfrak{M}\mathfrak{N}^{\mathfrak{a}}$.)

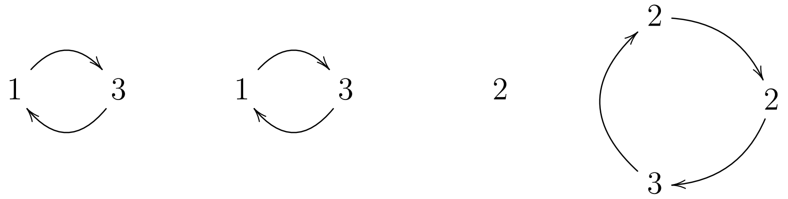
**Example 6.6.13.** Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let $w = 33232112 \in \mathfrak{A}^8$.

To compute $\operatorname{GR} w$, we first notice that $\operatorname{std} w = 67384125$ (in one-line notation). Hence, the permutation $\tau$ from Definition 6.6.12 satisfies $\tau = (\operatorname{std} w)^{-1} = 67358124$. The cycles of $\tau$ are $\{1, 6\}$, $\{2, 7\}$, $\{3\}$ and $\{4, 5, 8\}$. Thus,

$$\begin{aligned}
\operatorname{GR} w &= \{[w]_z \mid z \text{ is a cycle of } \tau\}_{\text{multiset}} \\
&= \left\{[w]_{\{1,6\}}, [w]_{\{2,7\}}, [w]_{\{3\}}, [w]_{\{4,5,8\}}\right\}_{\text{multiset}} \\
&= \{[31], [31], [2], [322]\}_{\text{multiset}} = \{[13], [13], [2], [223]\}_{\text{multiset}}
\end{aligned}$$

[337] Indeed, this multiset $\operatorname{GR} w$ is finite (since $\tau$ has only finitely many cycles), and its elements $[w]_z$ are aperiodic necklaces (as we have seen in the definition of $[w]_z$).

(since $[31] = [13]$ and $[322] = [223]$ as necklaces). Drawn on the plane, the necklaces in $\operatorname{GR} w$ look as follows:



The map GR is called the *Gessel-Reutenauer bijection*. In order to show that it indeed is a bijection, we shall construct its inverse. First, we introduce some further objects.

**Definition 6.6.14.** A nonempty word $w$ is said to be *aperiodic* if there exist no $m \geq 2$ and $u \in \mathfrak{A}^*$ satisfying $w = u^m$.

Let $\mathfrak{A}^{\mathfrak{a}}$ be the set of all aperiodic words in $\mathfrak{A}^*$.

For example, the word 132231 is aperiodic, but the word 132132 is not (since $132132 = u^m$ for $u = 132$ and $m = 2$).

Aperiodic words are directly connected to aperiodic necklaces, as the following facts show:[338]

**Proposition 6.6.15.** *Let $w \in \mathfrak{A}^*$ be a nonempty word. Then, the word $w$ is aperiodic if and only if the necklace $[w]$ is aperiodic.*

**Corollary 6.6.16.** *Let $w \in \mathfrak{A}^*$ be an aperiodic word. Then, the word $c \cdot w$ is aperiodic.*[339]

**Corollary 6.6.17.** *Each aperiodic necklace is a set of aperiodic words.*

Let us now introduce a new total order on the set $\mathfrak{A}^{\mathfrak{a}}$ of all aperiodic words:

**Definition 6.6.18.** Let $u$ and $v$ be two aperiodic words. Then, we write $u \leq_\omega v$ if and only if $uv \leq vu$. Thus, we have defined a binary relation $\leq_\omega$ on the set $\mathfrak{A}^{\mathfrak{a}}$ of all aperiodic words.

**Proposition 6.6.19.** *The relation $\leq_\omega$ on the set $\mathfrak{A}^{\mathfrak{a}}$ is the smaller-or-equal relation of a total order.*

For the next proposition, we should recall Definition 6.6.1 (and, in particular, the meaning of $c$ and its action on words).

**Proposition 6.6.20.** *Let $u$ and $v$ be two aperiodic words.*

(a) *We have $u \leq_\omega v$ if and only if*

$$\textit{either } u_1 < v_1 \textit{ or } \left(u_1 = v_1 \textit{ and } c \cdot u \leq_\omega c \cdot v\right).$$

[340]

(b) *If $u \neq v$, then there exists some $i \in \mathbb{N}$ satisfying $\left(c^i \cdot u\right)_1 \neq \left(c^i \cdot v\right)_1$.*

(c) *We have $u \leq_\omega v$ if and only if the smallest $i \in \mathbb{N}$ satisfying $\left(c^i \cdot u\right)_1 \neq \left(c^i \cdot v\right)_1$* ***either*** *does not exist* ***or*** *satisfies $\left(c^i \cdot u\right)_1 < \left(c^i \cdot v\right)_1$.*

[338] See Exercise 6.6.23 for the proofs of all unproved statements made until Exercise 6.6.23.

[339] See Definition 6.6.1 for the definition of $c$ and its action on words.

[340] The relation "$c \cdot u \leq_\omega c \cdot v$" here makes sense because the words $c \cdot u$ and $c \cdot v$ are aperiodic (by Corollary 6.6.16).

(d) *Let $n$ and $m$ be positive integers such that $n\ell(u) = m\ell(v)$. We have $u \leq_\omega v$ if and only if $u^n \leq v^m$.*

*Remark* 6.6.21. We are avoiding the use of infinite words here; if we didn't, we could restate the relation $\leq_\omega$ in a simpler way (which is easily seen to be equivalent to Proposition 6.6.20(c)): Two aperiodic words $u$ and $v$ satisfy $u \leq_\omega v$ if and only if $u^\infty \leq v^\infty$. Here, for any nonempty word $w$, we are letting $w^\infty$ denote the infinite word

$$\left(w_1, w_2, \ldots, w_{\ell(w)}, w_1, w_2, \ldots, w_{\ell(w)}, w_1, w_2, \ldots, w_{\ell(w)}, \ldots\right)$$

(that is, the word $w$ repeated endlessly), and the symbol "$\leq$" in "$u^\infty \leq v^\infty$" refers to the lexicographic order on $\mathfrak{A}^\infty$.

Other equivalent descriptions of the relation $\leq_\omega$ (or, more precisely, of the "strictly less" relation corresponding to it) can be found in [54, Corollary 11].

**Proposition 6.6.22.** *Let $w \in \mathfrak{A}^n$ be a word. Let $\tau$ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Then:*

(a) *The words $w_{\tau,1}, w_{\tau,2}, \ldots, w_{\tau,n}$ are aperiodic.*

(b) *We have $w_{\tau,1} \leq_\omega w_{\tau,2} \leq_\omega \cdots \leq_\omega w_{\tau,n}$.*

**Exercise 6.6.23.** Prove Proposition 6.6.15, Corollary 6.6.16, Corollary 6.6.17, Proposition 6.6.19, Proposition 6.6.20 and Proposition 6.6.22.

We need two more notations about multisets:

**Definition 6.6.24.** Let $T$ be a totally ordered set, and let $\leq_T$ be the smaller-or-equal relation of $T$. Let $M$ be a finite multiset of elements of $T$. Then, there is a unique list $(m_1, m_2, \ldots, m_n)$ such that

$$\{m_1, m_2, \ldots, m_n\}_{\text{multiset}} = M \qquad \text{and} \qquad m_1 \leq_T m_2 \leq_T \cdots \leq_T m_n.$$

This list $(m_1, m_2, \ldots, m_n)$ is obtained by listing all elements of $M$ (with their multiplicities) in increasing order (increasing with respect to $\leq_T$). We shall refer to this list $(m_1, m_2, \ldots, m_n)$ as the *$\leq_T$-increasing list* of $M$.

(For example, the $\leq_\mathbb{Z}$-increasing list of $\{1, 2, 3, 2, 1\}_{\text{multiset}}$ is $(1, 1, 2, 2, 3)$.)

**Definition 6.6.25.** Let $S$ be a finite multiset.

(a) The *support* $\operatorname{Supp} S$ is defined to be the set of all elements of $S$. Thus, if $S = \{m_1, m_2, \ldots, m_n\}_{\text{multiset}}$, then $\operatorname{Supp} S = \{m_1, m_2, \ldots, m_n\}$.

(b) For each $s \in S$, let $M_s$ be a finite multiset. Then, we define the *multiset union* $\biguplus_{s \in S} M_s$ to be the finite multiset $M$ with the following property: For any object $x$, we have

$$\begin{aligned}&(\text{multiplicity of } x \text{ in } M) \\ &= \sum_{s \in \operatorname{Supp} S} (\text{multiplicity of } s \text{ in } S) \cdot (\text{multiplicity of } x \text{ in } M_s).\end{aligned}$$

For example:

- If $S = \{1, 2, 3\}_{\text{multiset}}$ and $M_s = \{s, s+1\}_{\text{multiset}}$ for each $s \in \operatorname{Supp} S$, then $\biguplus_{s \in S} M_s = \{1, 2, 2, 3, 3, 4\}_{\text{multiset}}$.
- If $S = \{1, 1, 2\}_{\text{multiset}}$ and $M_s = \{s, s+1\}_{\text{multiset}}$ for each $s \in \operatorname{Supp} S$, then $\biguplus_{s \in S} M_s = \{1, 1, 2, 2, 2, 3\}_{\text{multiset}}$.

We regard each set as a multiset; thus, the multiset union $\biguplus_{s \in S} M_s$ is also defined when the $M_s$ are sets.

Now, we can construct the inverse of the Gessel-Reutenauer bijection:

**Definition 6.6.26.** We define a map $\operatorname{RG} : \mathfrak{MN}^{\mathfrak{a}} \to \mathfrak{A}^*$ as follows:

Let $M \in \mathfrak{MN}^{\mathfrak{a}}$ be a finite multiset of aperiodic necklaces. Let $M' = \biguplus_{N \in M} N$. (We are here using the fact that each necklace $N \in M$ is a finite set, thus a finite multiset.) Notice that $M'$ is a finite multiset of aperiodic words[341]. Let $(m_1, m_2, \ldots, m_n)$ be the $\leq_\omega$-increasing list of $M'$. For each $i \in \{1, 2, \ldots, n\}$, let $\ell_i$ be the last letter of the nonempty word $m_i$. Then, $\operatorname{RG}(M)$ is defined to be the word $(\ell_1, \ell_2, \ldots, \ell_n) \in \mathfrak{A}^*$.

**Example 6.6.27.** Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let $M = \{[13], [13], [2], [223]\}_{\text{multiset}}$. Clearly, $M \in \mathfrak{MN}^{\mathfrak{a}}$ (since $M$ is a finite multiset of aperiodic necklaces). (Actually, $M$ is the multiset of aperiodic necklaces drawn in Example 6.6.13.) In order to compute the word $\operatorname{RG}(M)$, let us first compute the multiset $M'$ from Definition 6.6.26. Indeed, the definition of $M'$ yields

$$\begin{aligned}
M' = \biguplus_{N \in M} N &= \underbrace{[13]}_{=\{13,31\}} \uplus \underbrace{[13]}_{=\{13,31\}} \uplus \underbrace{[2]}_{=\{2\}} \uplus \underbrace{[223]}_{=\{223,232,322\}} \\
&\qquad \left( \begin{array}{c} \text{where we are using the notation } M_1 \uplus M_2 \uplus \cdots \uplus M_k \\ \text{for a multiset union } \biguplus_{s \in \{1,2,\ldots,k\}} M_s \end{array} \right) \\
&= \{13, 31\} \uplus \{13, 31\} \uplus \{2\} \uplus \{223, 232, 322\} \\
&= \{13, 31, 13, 31, 2, 223, 232, 322\}_{\text{multiset}} .
\end{aligned}$$

Hence, the $\leq_\omega$-increasing list of $M'$ is $(13, 13, 2, 223, 232, 31, 31, 322)$ (since $13 \leq_\omega 13 \leq_\omega 2 \leq_\omega 223 \leq_\omega 232 \leq_\omega 31 \leq_\omega 31 \leq_\omega 322$). The last letters of the words in this list are $3, 3, 2, 3, 2, 1, 1, 2$ (in this order). Hence, Definition 6.6.26 shows that

$$\operatorname{RG}(M) = (3, 3, 2, 3, 2, 1, 1, 2) = 33232112.$$

*Remark* 6.6.28. The $\leq_\omega$-increasing list of a multiset $M'$ of aperiodic words is not always the same as its $\leq$-increasing list. For example, the $\leq_\omega$-increasing list of $\{2, 21\}$ is $(21, 2)$ (since $21 \leq_\omega 2$), whereas its $\leq$-increasing list is $(2, 21)$ (since $2 \leq 21$).

A comparison of Examples 6.6.13 and 6.6.27 suggests that the maps GR and RG undo one another. This is indeed true, as the following theorem (due to Gessel and Reutenauer [82, Lemma 3.4 and Example 3.5]; also proved in [182, Theorem 7.20], [51, Theorem 3.1 and Proposition 3.1] and [81, §2]) shows:

**Theorem 6.6.29.** *The maps* $\operatorname{GR} : \mathfrak{A}^* \to \mathfrak{MN}^{\mathfrak{a}}$ *and* $\operatorname{RG} : \mathfrak{MN}^{\mathfrak{a}} \to \mathfrak{A}^*$ *are mutually inverse bijections.*

[341] Indeed:

- Each $N \in M$ is an aperiodic necklace (since $M$ is a multiset of aperiodic necklaces), and thus (by Corollary 6.6.17) a set of aperiodic words. Therefore, $\biguplus_{N \in M} N$ is a multiset of aperiodic words.
- Each $N \in M$ is a necklace, and thus is a finite set (since any necklace is a finite set). Since the multiset $M$ is also finite, this shows that $\biguplus_{N \in M} N$ is finite.

Thus, $\biguplus_{N \in M} N$ is a finite multiset of aperiodic words. In other words, $M'$ is a finite multiset of aperiodic words (since $M' = \biguplus_{N \in M} N$).

**Exercise 6.6.30.** Prove Theorem 6.6.29.

[**Hint:** First, use Proposition 6.6.22 to show that $\mathrm{RG} \circ \mathrm{GR} = \mathrm{id}$. Then recall the fact that any injective map between two finite sets of the same sizes is a bijection. This does not directly apply here, since the sets $\mathfrak{A}^*$ and $\mathfrak{MN}^{\mathfrak{a}}$ are usually not finite. However, GR can be restricted to a map between two appropriate finite subsets, obtained by focussing on a finite sub-alphabet of $\mathfrak{A}$ and fixing the length of the words; these subsets can be shown to have equal size using the Chen-Fox-Lyndon factorization (see the following paragraph for the connection).[342]]

Theorem 6.6.29 shows that the sets $\mathfrak{A}^*$ and $\mathfrak{MN}^{\mathfrak{a}}$ are in bijection. This bijection is in some sense similar to the Chen-Fox-Lyndon factorization[343], and preserves various quantities (for example, the number of times a given letter $a$ appears in a word $w \in \mathfrak{A}^*$ equals the number of times this letter $a$ appears in the words in the corresponding multiset $\mathrm{GR}\, w \in \mathfrak{MN}^{\mathfrak{a}}$, provided that we pick one representative of each necklace in $\mathrm{GR}\, w$), and predictably affects other quantities (for example, the cycles of the standardization $\operatorname{std} w$ of a word $w \in \mathfrak{A}^*$ have the same lengths as the aperiodic necklaces in the corresponding multiset $\mathrm{GR}\, w \in \mathfrak{MN}^{\mathfrak{a}}$); these properties have ample applications to enumerative questions (discussed in [82]).

*Remark* 6.6.31. The Gessel-Reutenauer bijection relates to the *Burrows-Wheeler transformation* (e.g., [45, §2]). Indeed, the latter sends an aperiodic word $w \in \mathfrak{A}^{\mathfrak{a}}$ to the word $\mathrm{RG}\left(\{[w]\}_{\text{multiset}}\right)$ obtained by applying RG to the multiset consisting of the single aperiodic necklace $[w]$. This transformation is occasionally applied in (lossless) data compression, as the word $\mathrm{RG}\left(\{[w]\}_{\text{multiset}}\right)$ tends to have many strings of consecutive equal letters when $w$ has substrings occurring multiple times (for example, if $\mathfrak{A} = \{a < b < c < d < \cdots\}$ and $w = bananaban$, then $\mathrm{RG}\left(\{[w]\}_{\text{multiset}}\right) = nnbbnaaaa$), and strings of consecutive equal letters can easily be compressed. (In order to guarantee that $w$ can be recovered from the result, one can add a new letter $\zeta$ – called a "sentinel symbol" – to the alphabet $\mathfrak{A}$, and apply the Burrows-Wheeler transformation to the word $w\zeta$ instead of $w$. This also ensures that $w\zeta$ is an aperiodic word, so the Burrows-Wheeler transformation can be applied to $w\zeta$ even if it cannot be applied to $w$.)

Kufleitner, in [116, §4], suggests a bijective variant of the Burrows-Wheeler transformation. In our notations, it sends a word $w \in \mathfrak{A}^*$ to the word $\mathrm{RG}\left(\{[a_1], [a_2], \ldots, [a_k]\}_{\text{multiset}}\right)$, where $(a_1, a_2, \ldots, a_k)$ is the CFL factorization of $w$.

For variants and generalizations of the Gessel-Reutenauer bijection, see [116], [209], [200], [56] and [179].

6.6.2. *The Gessel-Reutenauer symmetric functions.* In this subsection, we shall study a certain family of symmetric functions. First, we recall that

[342] This argument roughly follows [81].

[343] The Chen-Fox-Lyndon factorization (Theorem 6.1.27) provides a bijection between words in $\mathfrak{A}^*$ and multisets of Lyndon words (because the factors in the CFL factorization of a word $w \in \mathfrak{A}^*$ can be stored in a multiset), whereas the Gessel-Reutenauer bijection $\mathrm{GR} : \mathfrak{A}^* \to \mathfrak{MN}^{\mathfrak{a}}$ is a bijection between words in $\mathfrak{A}^*$ and multisets of aperiodic necklaces. Since the Lyndon words are in bijection with the aperiodic necklaces (by Exercise 6.1.34(e)), we can thus view the two bijections as having the same targets (and the same domains). That said, they are not the same bijection.

every word $w \in \mathfrak{A}^*$ has a unique CFL factorization (see Theorem 6.1.27). Based on this fact, we can make the following definition:

**Definition 6.6.32.** For the rest of Subsection 6.6.2, we let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$.

Let $w \in \mathfrak{A}^*$ be a word. The *CFL type* of $w$ is defined to be the partition whose parts are the positive integers $\ell(a_1), \ell(a_2), \ldots, \ell(a_k)$ (listed in decreasing order), where $(a_1, a_2, \ldots, a_k)$ is the CFL factorization of $w$. This CFL type is denoted by $\operatorname{CFLtype} w$.

**Example 6.6.33.** Let $w$ be the word 213212412112. Then, the tuple $(2, 132, 124, 12, 112)$ is the CFL factorization of $w$. Hence, the CFL type of $w$ is the partition whose parts are the positive integers $\ell(2), \ell(132), \ell(124), \ell(12), \ell(112)$ (listed in decreasing order). In other words, the CFL type of $w$ is the partition $(3, 3, 3, 2, 1)$ (since the positive integers $\ell(2), \ell(132), \ell(124), \ell(12), \ell(112)$ are $1, 3, 3, 2, 3$).

**Definition 6.6.34.** For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^*$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$. (For example, $\mathbf{x}_{(1,3,2,1)} = x_1 x_3 x_2 x_1 = x_1^2 x_2 x_3$.)

For any partition $\lambda$, we define a power series $\mathbf{GR}_\lambda \in \mathbf{k}[[\mathbf{x}]]$ by

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{CFLtype} w = \lambda}} \mathbf{x}_w .$$

**Example 6.6.35.** Let us compute $\mathbf{GR}_{(2,1)}$. Indeed, the words $w \in \mathfrak{A}^*$ satisfying $\operatorname{CFLtype} w = (2, 1)$ are the words whose CFL factorization consists of two words, one of which has length 1 and the other has length 2. In other words, these words $w \in \mathfrak{A}^*$ must have the form $w = a_1 a_2$ for two Lyndon words $a_1$ and $a_2$ satisfying $a_1 \geq a_2$ and $(\ell(a_1), \ell(a_2)) \in \{(1, 2), (2, 1)\}$. A straightforward analysis of possibilities reveals that these are precisely the 3-letter words $w = (w_1, w_2, w_3)$ satisfying either ($w_1 < w_2$ and $w_1 \geq w_3$) or ($w_1 > w_2$ and $w_2 < w_3$). Hence,

$$\begin{aligned}
\mathbf{GR}_{(2,1)} &= \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{CFLtype} w = (2,1)}} \mathbf{x}_w = \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 < w_2 \text{ and } w_1 \geq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3}} \mathbf{x}_w \\
&= \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 < w_2 \text{ and } w_1 \geq w_3}} \mathbf{x}_w \\
&\qquad + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3 \text{ and } w_1 \leq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3 \text{ and } w_1 > w_3}} \mathbf{x}_w \\
&\qquad \left(\begin{array}{c} \text{here, we have split the second sum} \\ \text{according to the relation between } w_1 \text{ and } w_3 \end{array}\right) \\
&= \sum_{\substack{w \in \mathfrak{A}^*; \\ w_3 \leq w_1 < w_2}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_2 < w_1 \leq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_2 < w_3 < w_1}} \mathbf{x}_w
\end{aligned}$$

(here, we rewrote the conditions under the summation signs). The three sums on the right hand side are clearly quasisymmetric functions. Using (5.2.3), we can rewrite them as $L_{(2,1)}$, $L_{(1,2)}$ and $L_{(1,1,1)}$, respectively. Thus, we obtain

$$\begin{aligned}\mathbf{GR}_{(2,1)} &= L_{(2,1)} + L_{(1,2)} + L_{(1,1,1)} = 3M_{(1,1,1)} + M_{(1,2)} + M_{(2,1)} \\ &= 3m_{(1,1,1)} + m_{(2,1)}.\end{aligned}$$

Thus, $\mathbf{GR}_{(2,1)}$ is actually a symmetric function! We shall soon (in Proposition 6.6.37) see that this is not a coincidence.

We shall now state various properties of the power series $\mathbf{GR}_\lambda$; their proofs are all part of Exercise 6.6.51.

**Proposition 6.6.36.** *Let $n$ be a positive integer. Then:*

(a) *The partition $(n)$ satisfies*

$$\mathbf{GR}_{(n)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ w \text{ is Lyndon}}} \mathbf{x}_w .$$

(b) *Assume that $\mathbf{k}$ is a $\mathbb{Q}$-algebra. Then,*

$$\mathbf{GR}_{(n)} = \frac{1}{n} \sum_{d \mid n} \mu(d) \, p_d^{n/d} .$$

*Here, $\mu$ denotes the number-theoretical Möbius function (defined as in Exercise 2.9.6), and the summation sign "$\sum_{d|n}$" is understood to range over all **positive** divisors $d$ of $n$.*

**Proposition 6.6.37.** *Let $\lambda$ be a partition. Then, the power series $\mathbf{GR}_\lambda$ belongs to $\Lambda$.*

Thus, $(\mathbf{GR}_\lambda)_{\lambda \in \mathrm{Par}}$ is a family of symmetric functions.[344] Unlike many other such families we have studied, it is not a basis of $\Lambda$; it is not linearly independent (e.g., it satisfies $\mathbf{GR}_{(2,1,1)} = \mathbf{GR}_{(4)}$). Nevertheless, it satisfies a Cauchy-kernel-like identity[345]:

**Proposition 6.6.38.** *Consider two countable sets of indeterminates $\mathbf{x} = (x_1, x_2, x_3, \ldots)$ and $\mathbf{y} = (y_1, y_2, y_3, \ldots)$.*

(a) *In the power series ring $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$, we have*

$$\sum_{\lambda \in \mathrm{Par}} \mathbf{GR}_\lambda(\mathbf{x}) \, p_\lambda(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} p_\lambda(\mathbf{x}) \, \mathbf{GR}_\lambda(\mathbf{y}) .$$

(b) *For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^*$, we define a monomial $\mathbf{y}_w$ in $\mathbf{k}[[\mathbf{y}]]$ by setting $\mathbf{y}_w = y_{w_1} y_{w_2} \cdots y_{w_n}$. Then,*

$$\begin{aligned}\sum_{\lambda \in \mathrm{Par}} \mathbf{GR}_\lambda(\mathbf{x}) \, p_\lambda(\mathbf{y}) &= \sum_{w \in \mathfrak{A}^*} \mathbf{x}_w p_{\mathrm{CFLtype}\, w}(\mathbf{y}) = \prod_{w \in \mathfrak{L}} \prod_{u \in \mathfrak{L}} \frac{1}{1 - \mathbf{x}_w^{\ell(u)} \mathbf{y}_u^{\ell(w)}} \\ &= \sum_{\lambda \in \mathrm{Par}} p_\lambda(\mathbf{x}) \, \mathbf{GR}_\lambda(\mathbf{y}) .\end{aligned}$$

The proof of this proposition rests upon the following simple equality[346]:

[344] Several sources, including [82], [206, Exercise 7.89] and [66], write $L_\lambda$ for what we call $\mathbf{GR}_\lambda$. (So would we if $L_\alpha$ didn't already have another meaning here.)

[345] Recall that $\mathfrak{L}$ denotes the set of Lyndon words in $\mathfrak{A}^*$.

[346] Recall that $\mathfrak{L}$ denotes the set of Lyndon words in $\mathfrak{A}^*$. Also, recall that $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$. Thus, $p_1 = \sum_{i \geq 1} x_i = \sum_{a \in \mathfrak{A}} x_a$.

**Proposition 6.6.39.** *In the power series ring* $(\mathbf{k}[[\mathbf{x}]])[[t]]$, *we have*

$$\frac{1}{1-p_1 t} = \prod_{w\in\mathfrak{L}} \frac{1}{1-\mathbf{x}_w t^{\ell(w)}}.$$

We can furthermore represent the symmetric functions $\mathbf{GR}_\lambda$ in terms of the fundamental basis $(L_\alpha)_{\alpha\in\operatorname{Comp}}$ of QSym; here, the Gessel-Reutenauer bijection from Theorem 6.6.29 reveals its usefulness. We will use Definition 5.3.5.

**Proposition 6.6.40.** *Let* $\lambda$ *be a partition. Let* $n = |\lambda|$. *Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{\sigma\in\mathfrak{S}_n;\\ \sigma \text{ has cycle type } \lambda}} L_{\gamma(\sigma)}.$$

The proof of this relies on Lemma 5.3.6 (see Exercise 6.6.51 below for the details).

**Definition 6.6.41.** Let $\mathfrak{S} = \bigsqcup_{n\in\mathbb{N}} \mathfrak{S}_n$ (an external disjoint union). For each $\sigma\in\mathfrak{S}$, we let $\operatorname{type}\sigma$ denote the cycle type of $\sigma$.

**Proposition 6.6.42.** *Consider two countable sets of indeterminates* $\mathbf{x} = (x_1, x_2, x_3, \ldots)$ *and* $\mathbf{y} = (y_1, y_2, y_3, \ldots)$.

*In the power series ring* $\mathbf{k}[[\mathbf{x},\mathbf{y}]]$, *we have*

$$\sum_{\lambda\in\operatorname{Par}} \mathbf{GR}_\lambda(\mathbf{x})\, p_\lambda(\mathbf{y}) = \sum_{\lambda\in\operatorname{Par}} p_\lambda(\mathbf{x})\, \mathbf{GR}_\lambda(\mathbf{y}) = \sum_{\sigma\in\mathfrak{S}} L_{\gamma(\sigma)}(\mathbf{x})\, p_{\operatorname{type}\sigma}(\mathbf{y}).$$

Let us finally give two alternative descriptions of the $\mathbf{GR}_\lambda$ that do not rely on the notion of CFL factorization. First, we state a fact that is essentially trivial:

**Proposition 6.6.43.** *Let* $N$ *be a necklace. Let* $w$ *and* $w'$ *be two elements of* $N$. *Then:*

(a) *There exist words* $u$ *and* $v$ *such that* $w = uv$ *and* $w' = vu$.
(b) *We have* $\mathbf{x}_w = \mathbf{x}_{w'}$.

**Definition 6.6.44.** Let $N\in\mathfrak{N}$ be a necklace. Then, we define a monomial $\mathbf{x}_N$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_N = \mathbf{x}_w$, where $w$ is any element of $N$. (This is well-defined, because Proposition 6.6.43(b) shows that $\mathbf{x}_w$ does not depend on the choice of $w$.)

**Definition 6.6.45.** Let $M$ be a finite multiset of necklaces. Then, we define a monomial $\mathbf{x}_M$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_M = \mathbf{x}_{N_1}\mathbf{x}_{N_2}\cdots\mathbf{x}_{N_k}$, where $M$ is written in the form $M = \{N_1, N_2, \ldots, N_k\}_{\text{multiset}}$.

**Definition 6.6.46.** Let $M$ be a finite multiset of necklaces. Then, we can obtain a partition by listing the sizes of the necklaces in $M$ in decreasing order. This partition will be called the *type* of $M$, and will be denoted by $\operatorname{type} M$.

**Example 6.6.47.** If $M = \{[13], [13], [2], [223]\}_{\text{multiset}}$, then the type of $M$ is $(3, 2, 2, 1)$ (because the sizes of the necklaces in $M$ are $2, 2, 1, 3$).

**Proposition 6.6.48.** *Let* $\lambda$ *be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{M\in\mathfrak{M}\mathfrak{N}^{\mathfrak{a}};\\ \operatorname{type} M = \lambda}} \mathbf{x}_M.$$

This was our first alternative description of $\mathbf{GR}_\lambda$. Note that it is used as a definition of $\mathbf{GR}_\lambda$ in [82, (2.1)] (where $\mathbf{GR}_\lambda$ is denoted by $L_\lambda$). Using the Gessel-Reutenauer bijection, we can restate it as follows:

**Proposition 6.6.49.** *Let $\lambda$ be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{type}(\mathrm{GR}\, w) = \lambda}} \mathbf{x}_w .$$

Let us finally give a second alternative description of $\mathbf{GR}_\lambda$:

**Proposition 6.6.50.** *Let $\lambda$ be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{type}(\operatorname{std} w) = \lambda}} \mathbf{x}_w .$$

**Exercise 6.6.51.** Prove all statements made in Subsection 6.6.2.

[**Hint:** Here is one way to proceed:

- First prove Proposition 6.6.39, by using the CFL factorization to argue that both sides equal $\sum_{w \in \mathfrak{A}^*} \mathbf{x}_w t^{\ell(w)}$.
- Use a similar argument to derive Proposition 6.6.38 (starting with part (b)).
- Proposition 6.6.43 is almost trivial.
- Derive Proposition 6.6.48 from the definition of $\mathbf{GR}_\lambda$ using the uniqueness of the CFL factorization.
- Derive Proposition 6.6.49 from Proposition 6.6.48 using the bijectivity of GR.
- Derive Proposition 6.6.50 from Proposition 6.6.49.
- Obtain Proposition 6.6.40 by combining Proposition 6.6.50 with Lemma 5.3.6.
- Derive Proposition 6.6.42 from Propositions 6.6.40 and 6.6.38.
- Derive Proposition 6.6.37 either from Proposition 6.6.48 or from Proposition 6.6.38. (In the latter case, make sure to work with $\mathbf{k} = \mathbb{Q}$ first, and then extend to all other $\mathbf{k}$, as the proof will rely on the $\mathbf{k}$-linear independence of $(p_\lambda)_{\lambda \in \mathrm{Par}}$, which doesn't hold for all $\mathbf{k}$.)
- Prove Proposition 6.6.36(a) directly using the definition of $\mathbf{GR}_{(n)}$.
- Show that each positive integer $n$ satisfies

$$p_1^n = \sum_{d \mid n} d \cdot \mathbf{GR}_{(d)} \left( x_1^{n/d}, x_2^{n/d}, x_3^{n/d}, \ldots \right)$$

  by taking logarithms in Proposition 6.6.39. Use this and (2.9.7) to prove Proposition 6.6.36(b) recursively.

Other approaches are, of course, possible.]

*Remark* 6.6.52. Let $n$ be a positive integer. The symmetric function $\mathbf{GR}_{(n)}$ has a few more properties:

(a) It is an $\mathbb{N}$-linear combination of Schur functions. To state the precise rule, we need a few more notations: A *standard tableau* can be defined as a column-strict tableau $T$ with $\operatorname{cont}(T) = (1^m)$, where $m$ is the number of boxes of $T$. (That is, each of the numbers

$1, 2, \ldots, m$ appears exactly once in $T$, and no other numbers appear.) If $T$ is a standard tableau with $m$ boxes, then a *descent* of $T$ means an $i \in \{1, 2, \ldots, m-1\}$ such that the entry $i+1$ appears in $T$ in a row further down than $i$ does. The *major index* $\operatorname{maj} T$ of a standard tableau $T$ is defined to be the sum of its descents.[347] Now,

$$\mathbf{GR}_{(n)} = \sum_{\lambda \in \operatorname{Par}_n} a_{\lambda,1} s_\lambda,$$

where $a_{\lambda,1}$ is the number of standard tableaux $T$ of shape $\lambda$ satisfying $\operatorname{maj} T \equiv 1 \operatorname{mod} n$. (See [206, Exercise 7.89 (c)].)

(b) Assume that $\mathbf{k} = \mathbb{C}$. Recall the map $\operatorname{ch} : A(\mathfrak{S}) \to \Lambda$ from Theorem 4.4.1. Embed the cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ as a subgroup in the symmetric group $\mathfrak{S}_n$ by identifying some generator $g$ of $C_n$ with some $n$-cycle in $\mathfrak{S}_n$. Let $\omega$ be a primitive $n$-th root of unity in $\mathbb{C}$ (for instance, $\exp(2\pi i/n)$). Let $\gamma : C_n \to \mathbb{C}$ be the character of $C_n$ that sends each $g^i \in C_n$ to $\omega^i$. Then,

$$\mathbf{GR}_{(n)} = \operatorname{ch}\left(\operatorname{Ind}_{C_n}^{\mathfrak{S}_n} \gamma\right).$$

(See [206, Exercise 7.89 (b)].)

(c) The character $\operatorname{Ind}_{C_n}^{\mathfrak{S}_n} \gamma$ of $\mathfrak{S}_n$ is actually the character of a representation. To construct it, set $\mathbf{k} = \mathbb{C}$, and recall the notations from Exercise 6.1.41 (while keeping $\mathfrak{A} = \{1, 2, 3, \ldots\}$). Let $\mathfrak{m}_n$ be the $\mathbb{C}$-vector subspace of $T(V)$ spanned by the products $x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ with $\sigma \in \mathfrak{S}_n$. The symmetric group $\mathfrak{S}_n$ acts on $T(V)$ by algebra homomorphisms, with $\sigma \in \mathfrak{S}_n$ sending each $x_i$ to $x_{\sigma(i)}$ when $i \leq n$ and to $x_i$ otherwise. Both $\mathfrak{g}_n$ and $\mathfrak{m}_n$ are $\mathbb{C}\mathfrak{S}_n$-submodules of $T(V)$. Thus, so is the intersection $\mathfrak{g}_n \cap \mathfrak{m}_n$. It is not hard to see that this intersection is spanned by all "nested commutators" $\left[x_{\sigma(1)}, \left[x_{\sigma(2)}, \left[x_{\sigma(3)}, \ldots\right]\right]\right]$ (in $T(V)$) with $\sigma \in \mathfrak{S}_n$. The character of this $\mathbb{C}\mathfrak{S}_n$-module $\mathfrak{g}_n \cap \mathfrak{m}_n$ is precisely the $\operatorname{Ind}_{C_n}^{\mathfrak{S}_n} \gamma$ from Remark 6.6.52(b), so applying the Frobenius characteristic map ch to it yields the symmetric function $\mathbf{GR}_{(n)}$. (See [182, Theorem 9.41(i)]. There are similar ways to obtain $\mathbf{GR}_\lambda$ for all $\lambda \in \operatorname{Par}$.)

**Exercise 6.6.53.** Prove the claim of Remark 6.6.52(b).

[**Hint:** It helps to recall (or prove) that for any positive integer $m$, the sum of all primitive $m$-th roots of unity in $\mathbb{C}$ is $\mu(m)$.]

The symmetric functions $\mathbf{GR}_\lambda$ for more general partitions $\lambda$ can be expressed in terms of the symmetric functions $\mathbf{GR}_{(n)}$ (which, as we recall from Proposition 6.6.36(b), have a simple expression in terms of the $p_m$) using the concept of *plethysm*; see [82, Theorem 3.6].

In [82], Gessel and Reutenauer apply the symmetric functions $\mathbf{GR}_\lambda$ to questions of permutation enumeration via the following result[348]:

[347] For example, the tableau

$$\begin{array}{cccc} 1 & 3 & 4 & 8 \\ 2 & 5 & 6 & 9 \\ 7 & & & \end{array}$$

is standard and has descents $1, 4, 6, 8$ and major index $1 + 4 + 6 + 8 = 19$.

[348] Proposition 6.6.54(a) is [82, Corollary 2.2]; Proposition 6.6.54(b) is [82, Theorem 2.1].

**Proposition 6.6.54.** *Let $n \in \mathbb{N}$. Let $\lambda \in \operatorname{Par}_n$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in \operatorname{Comp}_n$. We shall use the notations introduced in Definition 5.1.10. Definition 5.3.5 and Definition 6.6.41.*

(a) *Let $\mu \in \operatorname{Par}_n$ be the partition obtained by sorting the entries of $\beta$ into decreasing order. Then,*

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \\
&\qquad\qquad \text{such that } \beta \text{ refines } \gamma(\sigma)) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \\
&\qquad\qquad \text{and } \operatorname{Des}\sigma \subset D(\beta)) \\
&= \left(\text{the coefficient of } x_1^{\beta_1} x_2^{\beta_2} \cdots x_k^{\beta_k} \text{ in } \mathbf{GR}_\lambda\right) \\
&= (\text{the coefficient of } \mathbf{x}^\mu \text{ in } \mathbf{GR}_\lambda) \\
&= (\mathbf{GR}_\lambda, h_\mu) \\
&\qquad (\text{this is the Hall inner product of } \mathbf{GR}_\lambda \in \Lambda \text{ and } h_\mu \in \Lambda).
\end{aligned}$$

(b) *Recall the ribbon diagram $\operatorname{Rib}(\beta)$ corresponding to the composition $\beta$ (defined as in Definition 5.1.10). Then,*

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \\
&\qquad\qquad \text{and } \beta = \gamma(\sigma)) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \\
&\qquad\qquad \text{and } \operatorname{Des}\sigma = D(\beta)) \\
&= \left(\mathbf{GR}_\lambda, s_{\operatorname{Rib}(\beta)}\right) \\
&\qquad \left(\text{this is the Hall inner product of } \mathbf{GR}_\lambda \in \Lambda \text{ and } s_{\operatorname{Rib}(\beta)} \in \Lambda\right).
\end{aligned}$$

**Exercise 6.6.55.** Prove Proposition 6.6.54.

[**Hint:** Use Proposition 6.6.40, Theorem 5.4.10, the equality (5.4.3) and the adjointness between $\pi$ and $i$ in Corollary 5.4.3.]

By strategic application of Proposition 6.6.54, Gessel and Reutenauer arrive at several enumerative consequences, such as the following:

- ([82, Theorem 8.3]) If $A$ is a proper subset of $\{1, 2, \ldots, n-1\}$, then

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \\
&\qquad\qquad \text{satisfying } |\operatorname{Fix}\sigma| = 0 \text{ and } \operatorname{Des}\sigma = A) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \\
&\qquad\qquad \text{satisfying } |\operatorname{Fix}\sigma| = 1 \text{ and } \operatorname{Des}\sigma = A),
\end{aligned}$$

  where $\operatorname{Fix}\sigma$ denotes the set of all fixed points of a permutation $\sigma$. This can also be proved bijectively; such a bijective proof can be obtained by combining [50, Theorems 5.1 and 6.1].

- ([82, Theorem 9.4]) If $i \in \{1, 2, \ldots, n-1\}$, then

$$\begin{aligned}
&(\text{the number of } n\text{-cycles } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}\sigma = \{i\}) \\
&= \sum_{d \mid \gcd(n,i)} \mu(d) \binom{n/d}{i/d}.
\end{aligned}$$

  Note that this also equals the number of necklaces $[(w_1, w_2, \ldots, w_n)]$ (or, equivalently, Lyndon words $(w_1, w_2, \ldots, w_n)$) with $w_1, w_2, \ldots, w_n \in$

$\{0,1\}$ and $w_1+w_2+\cdots+w_n = i$. This suggests that there should be a bijection between $\{n\text{-cycles } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}\sigma = \{i\}\}$ and the set of such necklaces; and indeed, such a bijection can be found in [45, Theorem 1].

See [82] and [66] for more such applications.

## 7. Aguiar-Bergeron-Sottile character theory Part I: QSym as a terminal object

It turns out that the universal mapping property of NSym as a free associative algebra leads via duality to a universal property for its dual QSym, elegantly explaining several combinatorial invariants that take the form of quasisymmetric or symmetric functions:

- Ehrenborg's quasisymmetric function of a *ranked poset* [64],
- Stanley's *chromatic* symmetric function of a *graph* [205],
- the quasisymmetric function of a *matroid* considered in [21].

### 7.1. Characters and the universal property.

**Definition 7.1.1.** Given a Hopf algebra $A$ over $\mathbf{k}$, a *character* is an algebra morphism $A \xrightarrow{\zeta} \mathbf{k}$, that is,

- $\zeta(1_A) = 1_{\mathbf{k}}$,
- $\zeta$ is $\mathbf{k}$-linear, and
- $\zeta(ab) = \zeta(a)\zeta(b)$ for $a, b$ in $A$.

**Example 7.1.2.** A particularly important character for $A = \mathrm{QSym}$ is defined as follows:[349]

$$\begin{array}{rcl} \mathrm{QSym} & \xrightarrow{\zeta_Q} & \mathbf{k}, \\ f(\mathbf{x}) & \longmapsto & f(1,0,0,\ldots) = [f(\mathbf{x})]_{x_1=1, x_2=x_3=\cdots=0}\,. \end{array}$$

Hence,

$$\zeta_Q(M_\alpha) = \zeta_Q(L_\alpha) = \begin{cases} 1, & \text{if } \alpha = (n) \text{ for some } n; \\ 0, & \text{otherwise.} \end{cases}$$

In other words, the restriction $\zeta_Q|_{\mathrm{QSym}_n}$ coincides with the functional $H_n$ in $\mathrm{NSym}_n = \mathrm{Hom}_{\mathbf{k}}(\mathrm{QSym}_n, \mathbf{k})$: one has for $f$ in $\mathrm{QSym}_n$ that

$$\zeta_Q(f) = (H_n, f). \tag{7.1.1}$$

It is worth remarking that there is nothing special about setting $x_1 = 1$ and $x_2 = x_3 = \cdots = 0$: for quasisymmetric $f$, we could have defined the same character $\zeta_Q$ by picking any variable, say $x_n$, and sending

$$f(\mathbf{x}) \longmapsto [f(\mathbf{x})]_{\substack{x_n=1, \text{ and} \\ x_m=0 \text{ for } m \neq n}}\,.$$

This character $\mathrm{QSym} \xrightarrow{\zeta_Q} \mathbf{k}$ has a certain universal property, known as the *Aguiar-Bergeron-Sottile universality theorem* (part of [4, Theorem 4.1]):

**Theorem 7.1.3.** *Let $A$ be a connected graded Hopf algebra, and let $A \xrightarrow{\zeta} \mathbf{k}$ be a character. Then, there is a unique graded Hopf morphism $A \xrightarrow{\Psi}$ QSym making the following diagram commute:*

$$\begin{tikzcd} A \arrow[rr, "\Psi"] \arrow[dr, "\zeta"'] & & \mathrm{QSym} \arrow[dl, "\zeta_Q"] \\ & \mathbf{k} & \end{tikzcd} \tag{7.1.2}$$

[349] We are using the notation of Proposition 5.1.9 here, and we are still identifying QSym with QSym $(\mathbf{x})$, where $\mathbf{x}$ denotes the infinite chain $(x_1 < x_2 < \cdots)$.

*Furthermore,* $\Psi$ *is given by the following formula on homogeneous elements:*

$$\Psi(a) = \sum_{\alpha \in \mathrm{Comp}_n} \zeta_\alpha(a) M_\alpha \qquad \text{for all } n \in \mathbb{N} \text{ and } a \in A_n, \tag{7.1.3}$$

*where for* $\alpha = (\alpha_1, \ldots, \alpha_\ell)$*, the map* $\zeta_\alpha$ *is the composite*

$$A_n \xrightarrow{\Delta^{(\ell-1)}} A^{\otimes \ell} \xrightarrow{\pi_\alpha} A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_\ell} \xrightarrow{\zeta^{\otimes \ell}} \mathbf{k}$$

*in which* $A^{\otimes \ell} \xrightarrow{\pi_\alpha} A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_\ell}$ *is the canonical projection.*

*Proof.* One argues that $\Psi$ is unique, and has formula (7.1.3), using only that $\zeta$ is $\mathbf{k}$-linear and sends 1 to 1 and that $\Psi$ is a graded $\mathbf{k}$-*coalgebra* map making (7.1.2) commute. Equivalently, consider the adjoint $\mathbf{k}$-*algebra* map[350]

$$\mathrm{NSym} = \mathrm{QSym}^o \xrightarrow{\Psi^*} A^o.$$

Commutativity of (7.1.2) implies that for $a$ in $A_n$,

$$(\Psi^*(H_n), a) = (H_n, \Psi(a)) \overset{(7.1.1)}{=} \zeta_Q(\Psi(a)) = \zeta(a),$$

whereas gradedness of $\Psi^*$ yields that $(\Psi^*(H_m), a) = 0$ whenever $a \in A_n$ and $m \neq n$. In other words, $\Psi^*(H_n)$ is the element of $A^o$ defined as the following functional on $A$:

$$\Psi^*(H_n)(a) = \begin{cases} \zeta(a), & \text{if } a \in A_n; \\ 0, & \text{if } a \in A_m \text{ for some } m \neq n. \end{cases} \tag{7.1.4}$$

By the universal property for $\mathrm{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots \rangle$ as free associative $\mathbf{k}$-algebra, we see that any choice of a $\mathbf{k}$-linear map $A \xrightarrow{\zeta} \mathbf{k}$ uniquely produces a $\mathbf{k}$-algebra morphism $\Psi^* : \mathrm{QSym}^o \to A^o$ which satisfies (7.1.4) for all $n \geq 1$. It is easy to see that this $\Psi^*$ then automatically satisfies (7.1.4) for $n = 0$ as well if $\zeta$ sends 1 to 1 (it is here that we use $\zeta(1) = 1$ and the connectedness of $A$). Hence, any given $\mathbf{k}$-linear map $A \xrightarrow{\zeta} \mathbf{k}$ sending 1 to 1 uniquely produces a $\mathbf{k}$-algebra morphism $\Psi^* : \mathrm{QSym}^o \to A^o$ which satisfies (7.1.4) for all $n \geq 0$. Formula (7.1.3) follows as

$$\Psi(a) = \sum_{\alpha \in \mathrm{Comp}} (H_\alpha, \Psi(a)) \, M_\alpha$$

and for a composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, one has

$$\begin{aligned} (H_\alpha, \Psi(a)) = (\Psi^*(H_\alpha), a) &= (\Psi^*(H_{\alpha_1}) \cdots \Psi^*(H_{\alpha_\ell}), a) \\ &= \left(\Psi^*(H_{\alpha_1}) \otimes \cdots \otimes \Psi^*(H_{\alpha_\ell}), \Delta^{(\ell-1)}(a)\right) \\ &\overset{(7.1.4)}{=} \left(\zeta^{\otimes \ell} \circ \pi_\alpha\right) \left(\Delta^{(\ell-1)}(a)\right) = \zeta_\alpha(a), \end{aligned}$$

where the definition of $\zeta_\alpha$ was used in the last equality.

We wish to show that if, in addition, $A$ is a Hopf algebra and $A \xrightarrow{\zeta} \mathbf{k}$ is a character (i.e., an algebra morphism), then $A \xrightarrow{\Psi} \mathrm{QSym}$ will be an algebra morphism, that is, the two maps $A \otimes A \longrightarrow \mathrm{QSym}$ given by $\Psi \circ m$

[350] Here we are using the fact that there is a 1-to-1 correspondence between graded $\mathbf{k}$-linear maps $A \to \mathrm{QSym}$ and graded $\mathbf{k}$-linear maps $\mathrm{QSym}^o \to A^o$ given by $f \mapsto f^*$, and this correspondence has the property that a given graded map $f : A \to \mathrm{QSym}$ is a $\mathbf{k}$-coalgebra morphism if and only if $f^*$ is a $\mathbf{k}$-algebra morphism. This is a particular case of Exercise 1.6.1(f).

and $m \circ (\Psi \otimes \Psi)$ coincide. To see this, consider these two diagrams having the two maps in question as the composites of their top rows:

$$\begin{tikzcd}
A \otimes A \arrow[r, "m"] \arrow[dr, "\zeta\otimes\zeta"'] & A \arrow[r, "\Psi"] \arrow[d, "\zeta"'] & \mathrm{QSym} \arrow[dl, "\zeta_Q"] \\
& \mathbf{k} &
\end{tikzcd}$$

(7.1.5)

$$\begin{tikzcd}
A \otimes A \arrow[r, "\Psi\otimes\Psi"] \arrow[dr, "\zeta\otimes\zeta"'] & \mathrm{QSym}^{\otimes 2} \arrow[r, "m"] \arrow[d, "\zeta_Q\otimes\zeta_Q"'] & \mathrm{QSym} \arrow[dl, "\zeta_Q"] \\
& \mathbf{k} &
\end{tikzcd}$$

The fact that $\zeta, \zeta_Q$ are algebra morphisms makes the above diagrams commute, so that applying the uniqueness in the first part of the proof to the character $A \otimes A \xrightarrow{\zeta\otimes\zeta} \mathbf{k}$ proves the desired equality $\Psi \circ m = m \circ (\Psi \otimes \Psi)$. □

*Remark* 7.1.4. When one assumes in addition that $A$ is cocommutative, it follows that the image of $\Psi$ will lie in the subalgebra $\Lambda \subset \mathrm{QSym}$, e.g. from the explicit formula (7.1.3) and the fact that one will have $\zeta_\alpha = \zeta_\beta$ whenever $\beta$ is a rearrangement of $\alpha$. In other words, the character $\Lambda \xrightarrow{\zeta_\Lambda} \mathbf{k}$ defined by restricting $\zeta_Q$ to $\Lambda$, or by

$$\zeta_\Lambda(m_\lambda) = \begin{cases} 1, & \text{if } \lambda = (n) \text{ for some } n; \\ 0, & \text{otherwise,} \end{cases}$$

has a universal property as terminal object with respect to characters on cocommutative Hopf algebras.

The graded Hopf morphism $\Psi$ in Theorem 7.1.3 will be called the *map* $A \to \mathrm{QSym}$ *induced by the character* $\zeta$.

We close this section by discussing a well-known polynomiality and reciprocity phenomenon; see, e.g., Humpert and Martin [103, Prop. 2.2], Stanley [205, §4].

**Definition 7.1.5.** The *binomial Hopf algebra* (over the commutative ring $\mathbf{k}$) is the polynomial algebra $\mathbf{k}[m]$ in a single variable $m$, with a Hopf algebra structure transported from the symmetric algebra $\mathrm{Sym}(\mathbf{k}^1)$ (which is a Hopf algebra by virtue of Example 1.3.14, applied to $V = \mathbf{k}^1$) along the isomorphism $\mathrm{Sym}(\mathbf{k}^1) \to \mathbf{k}[m]$ which sends the standard basis element of $\mathbf{k}^1$ to $m$. Thus the element $m$ is primitive; that is, $\Delta m = 1 \otimes m + m \otimes 1$ and $S(m) = -m$. As $S$ is an algebra anti-endomorphism by Proposition 1.4.10 and $\mathbf{k}[m]$ is commutative, one has $S(g)(m) = g(-m)$ for all polynomials $g(m)$ in $\mathbf{k}[m]$.

**Definition 7.1.6.** For an element $f(\mathbf{x})$ in QSym and a nonnegative integer $m$, let $\mathrm{ps}^1(f)(m)$ denote the element of $\mathbf{k}$ obtained by *principal specialization at* $q = 1$

$$\begin{aligned}\mathrm{ps}^1(f)(m) &= [f(\mathbf{x})]_{\substack{x_1=x_2=\cdots=x_m=1,\\ x_{m+1}=x_{m+2}=\cdots=0}} \\ &= f(\underbrace{1, 1, \ldots, 1}_{m \text{ ones}}, 0, 0, \ldots).\end{aligned}$$

**Proposition 7.1.7.** *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. The map $\mathrm{ps}^1$ has the following properties.*

(i) *Let $f \in \mathrm{QSym}$. There is a unique polynomial in $\mathbf{k}[m]$ which agrees for each nonnegative integer $m$ with $\mathrm{ps}^1(f)(m)$, and which, by abuse of notation, we will also denote $\mathrm{ps}^1(f)(m)$. If $f$ lies in $\mathrm{QSym}_n$, then $\mathrm{ps}^1(f)(m)$ is a polynomial of degree at most $n$, taking these values on $M_\alpha, L_\alpha$ for $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ in $\mathrm{Comp}_n$:*

$$\mathrm{ps}^1(M_\alpha)(m) = \binom{m}{\ell},$$
$$\mathrm{ps}^1(L_\alpha)(m) = \binom{m-\ell+n}{n}.$$

(ii) *The map $\mathrm{QSym} \xrightarrow{\mathrm{ps}^1} \mathbf{k}[m]$ is a Hopf morphism into the binomial Hopf algebra.*

(iii) *For all $m$ in $\mathbb{Z}$ and $f$ in $\mathrm{QSym}$ one has*

$$\zeta_Q^{\star m}(f) = \mathrm{ps}^1(f)(m).$$

*In particular, one also has*

$$\zeta_Q^{\star(-m)}(f) = \mathrm{ps}^1(S(f))(m) = \mathrm{ps}^1(f)(-m).$$

(iv) *For a graded Hopf algebra $A$ with a character $A \xrightarrow{\zeta} \mathbf{k}$, and any element $a$ in $A_n$, the polynomial $\mathrm{ps}^1(\Psi(a))(m)$ in $\mathbf{k}[m]$ has degree at most $n$, and when specialized to $m$ in $\mathbb{Z}$ satisfies*

$$\zeta^{\star m}(a) = \mathrm{ps}^1(\Psi(a))(m).$$

*Proof.* To prove assertion (i), note that one has

$$\begin{aligned}
\mathrm{ps}^1(M_\alpha)(m) &= M_\alpha(1,1,\ldots,1,0,0,\ldots) = \sum_{1 \le i_1 < \cdots < i_\ell \le m} \left[x_{i_1}^{\alpha_1} \cdots x_{i_\ell}^{\alpha_\ell}\right]_{x_j=1} \\
&= \binom{m}{\ell}, \\
\mathrm{ps}^1(L_\alpha)(m) &= L_\alpha(1,1,\ldots,1,0,0,\ldots) = \sum_{\substack{1 \le i_1 \le \cdots \le i_n \le m: \\ i_k < i_{k+1} \text{ if } k \in D(\alpha)}} \left[x_{i_1} \cdots x_{i_n}\right]_{x_j=1} \\
&= |\{1 \le j_1 \le j_2 \le \cdots \le j_n \le m-\ell+1\}| = \binom{m-\ell+n}{n}.
\end{aligned}$$

As $\{M_\alpha\}_{\alpha \in \mathrm{Comp}_n}$ form a basis for $\mathrm{QSym}_n$, and $\binom{m}{\ell}$ is a polynomial function in $m$ of degree $\ell (\le n)$, one concludes that for $f$ in $\mathrm{QSym}_n$ one has that $\mathrm{ps}^1(f)(m)$ is a polynomial function in $m$ of degree at most $n$. The polynomial giving rise to this function is unique, since infinitely many of its values are fixed.

To prove assertion (ii), note that $\mathrm{ps}^1$ is an algebra morphism because it is an evaluation homomorphism. To check that it is a coalgebra morphism, it suffices to check $\Delta \circ \mathrm{ps}^1 = (\mathrm{ps}^1 \otimes \mathrm{ps}^1) \circ \Delta$ on each $M_\alpha$ for $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ in $\mathrm{Comp}_n$. Using the Vandermonde summation $\binom{A+B}{\ell} = \sum_k \binom{A}{k}\binom{B}{\ell-k}$, one has

$$\begin{aligned}(\Delta \circ \mathrm{ps}^1)(M_\alpha) &= \Delta \binom{m}{\ell} = \binom{m \otimes 1 + 1 \otimes m}{\ell} = \sum_{k=0}^{\ell} \binom{m \otimes 1}{k} \binom{1 \otimes m}{\ell - k} \\ &= \sum_{k=0}^{\ell} \binom{m}{k} \otimes \binom{m}{\ell - k}\end{aligned}$$

while at the same time

$$\begin{aligned}\left((\mathrm{ps}^1 \otimes \mathrm{ps}^1) \circ \Delta\right)(M_\alpha) &= \sum_{k=0}^{\ell} \mathrm{ps}^1(M_{(\alpha_1,\ldots,\alpha_k)}) \otimes \mathrm{ps}^1(M_{(\alpha_{k+1},\ldots,\alpha_\ell)}) \\ &= \sum_{k=0}^{\ell} \binom{m}{k} \otimes \binom{m}{\ell - k}.\end{aligned}$$

Thus $\mathrm{ps}^1$ is a bialgebra morphism, and hence also a Hopf morphism, by Corollary 1.4.27.

For assertion (iii), first assume $m$ lies in $\{0, 1, 2, \ldots\}$. Since $\zeta_Q(f) = f(1, 0, 0, \ldots)$, one has

$$\begin{aligned}\zeta_Q^{\star m}(f) &= \zeta_Q^{\otimes m} \circ \Delta^{(m-1)} f(\mathbf{x}) = \zeta_Q^{\otimes m}\left(f(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)})\right) \\ &= \left[f(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)})\right]_{\substack{x_1^{(1)}=x_1^{(2)}=\cdots=x_1^{(m)}=1, \\ x_2^{(j)}=x_3^{(j)}=\cdots=0 \text{ for all } j}} \\ &= f(1, 0, 0, \ldots, 1, 0, 0, \ldots, \cdots, 1, 0, 0, \ldots) = f(\underbrace{1, 1, \ldots, 1}_{m \text{ ones}}, 0, 0, \ldots) \\ &= \mathrm{ps}^1(f)(m).\end{aligned}$$

[351] But then Proposition 1.4.26(a) also implies

$$\begin{aligned}\zeta_Q^{\star(-m)}(f) &= \left(\zeta_Q^{\star(-1)}\right)^{\star m}(f) = (\zeta_Q \circ S)^{\star m}(f) = \zeta_Q^{\star m}(S(f)) \\ &= \mathrm{ps}^1(S(f))(m) = S(\mathrm{ps}^1(f))(m) = \mathrm{ps}^1(f)(-m).\end{aligned}$$

For assertion (iv), note that

$$\zeta^{\star m}(a) = (\zeta_Q \circ \Psi)^{\star m}(a) = (\zeta_Q^{\star m})(\Psi(a)) = \mathrm{ps}^1(\Psi(a))(m),$$

where the three equalities come from (7.1.2), Proposition 1.4.26(a), and assertion (iii) above, respectively. □

*Remark* 7.1.8. Aguiar, Bergeron and Sottile give a very cute (third) proof of the QSym antipode formula Theorem 5.1.11, via Theorem 7.1.3, in [4, Example 4.8]. They apply Theorem 7.1.3 to the *coopposite coalgebra* $\mathrm{QSym}^{cop}$ and its character $\zeta_Q^{\star(-1)}$. One can show that the map $\mathrm{QSym}^{cop} \xrightarrow{\Psi} \mathrm{QSym}$ induced by $\zeta_Q^{\star(-1)}$ is $\Psi = S$, the antipode of QSym, because $S : \mathrm{QSym} \to \mathrm{QSym}$ is a coalgebra anti-endomorphism (by Exercise 1.4.28) satisfying $\zeta_Q^{\star(-1)} = \zeta_Q \circ S$. They then use the formula (7.1.3) for $\Psi = S$ (together with the polynomiality Proposition 7.1.7) to derive Theorem 5.1.11.

[351] See Exercise 7.1.9 for an alternative way to prove this, requiring less thought to verify its soundness.

**Exercise 7.1.9.** Show that $\zeta_Q^{\star m}(f) = \operatorname{ps}^1(f)(m)$ for all $f \in \operatorname{QSym}$ and $m \in \{0, 1, 2, \ldots\}$. (This was already proven in Proposition 7.1.7(iii); give an alternative proof using Proposition 5.1.7.)

## 7.2. **Example: Ehrenborg's quasisymmetric function of a ranked poset.**

Here we consider incidence algebras, coalgebras and Hopf algebras generally, and then particularize to the case of graded posets, to recover Ehrenborg's interesting quasisymmetric function invariant via Theorem 7.1.3.

### 7.2.1. *Incidence algebras, coalgebras, Hopf algebras.*

**Definition 7.2.1.** Given a family $\mathcal{P}$ of finite partially ordered sets $P$, let $\mathbf{k}[\mathcal{P}]$ denote the free $\mathbf{k}$-module whose basis consists of symbols $[P]$ corresponding to isomorphism classes of posets $P$ in $\mathcal{P}$.

We will assume throughout that each $P$ in $\mathcal{P}$ is *bounded*, that is, it has a unique minimal element $\hat{0} := \hat{0}_P$ and a unique maximal element $\hat{1} := \hat{1}_P$. In particular, $P \neq \varnothing$, although it is allowed that $|P| = 1$, so that $\hat{0} = \hat{1}$; denote this isomorphism class of posets with one element by $[o]$.

If $\mathcal{P}$ is closed under taking intervals

$$[x, y] := [x, y]_P := \{z \in P : x \leq_P z \leq_P y\},$$

then one can easily see that the following coproduct and counit endow $\mathbf{k}[\mathcal{P}]$ with the structure of a coalgebra, called the *(reduced) incidence coalgebra*:

$$\Delta[P] := \sum_{x \in P} [\hat{0}, x] \otimes [x, \hat{1}],$$

$$\epsilon[P] := \begin{cases} 1, & \text{if } |P| = 1; \\ 0, & \text{otherwise.} \end{cases}$$

The dual algebra $\mathbf{k}[\mathcal{P}]^*$ is generally called the *reduced incidence algebra (modulo isomorphism)* for the family $\mathcal{P}$ (see, e.g., [192]). It contains the important element $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$, called the *$\zeta$-function* that takes the value $\zeta[P] = 1$ for all $P$.

If $\mathcal{P}$ (is not empty and) satisfies the further property of being *hereditary* in the sense that for every $P_1, P_2$ in $\mathcal{P}$, the *Cartesian product poset* $P_1 \times P_2$ with componentwise partial order is also in $\mathcal{P}$, then one can check that the following product and unit endow $\mathbf{k}[\mathcal{P}]$ with the structure of a (commutative) algebra:

$$\begin{aligned} [P_1] \cdot [P_2] &:= m([P_1] \otimes [P_2]) := [P_1 \times P_2], \\ 1_{\mathbf{k}[\mathcal{P}]} &:= [o]. \end{aligned}$$

**Proposition 7.2.2.** *For any hereditary family $\mathcal{P}$ of finite posets, $\mathbf{k}[\mathcal{P}]$ is a bialgebra, and even a Hopf algebra with antipode $S$ given as in* (1.4.7) *(Takeuchi's formula):*

$$S[P] = \sum_{k \geq 0} (-1)^k \sum_{\hat{0} = x_0 < \cdots < x_k = \hat{1}} [x_0, x_1] \cdots [x_{k-1}, x_k].$$

*Proof.* Checking the commutativity of the pentagonal diagram in (1.3.4) amounts to the fact that, for any $(x_1, x_2) <_{P_1 \times P_2} (y_1, y_2)$, one has a poset isomorphism

$$[(x_1, x_2)\ ,\ (y_1, y_2)]_{P_1 \times P_2} \cong [x_1, y_1]_{P_1} \times [x_2, y_2]_{P_2}.$$

Commutativity of the remaining diagrams in (1.3.4) is straightforward, and so $\mathbf{k}[\mathcal{P}]$ is a bialgebra. But then Remark 1.4.25 implies that it is a Hopf algebra, with antipode $S$ as in (1.4.7), because the map $f := \mathrm{id}_{\mathbf{k}[\mathcal{P}]} - u\epsilon$ (sending the class $[o]$ to 0, and fixing all other $[P]$) is locally $\star$-nilpotent:

$$f^{\star k}[P] = \sum_{\hat{0}=x_0<\cdots<x_k=\hat{1}} [x_0, x_1] \cdots [x_{k-1}, x_k]$$

will vanish due to an empty sum whenever $k$ exceeds the maximum length of a chain in the finite poset $P$. □

It is perhaps worth remarking how this generalizes the Möbius function formula of P. Hall. Note that the zeta function $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$ is a *character*, that is, an algebra morphism. Proposition 1.4.26(a) then tells us that $\zeta$ should have a convolutional inverse $\mathbf{k}[\mathcal{P}] \xrightarrow{\mu=\zeta^{\star-1}} \mathbf{k}$, traditionally called the *Möbius function*, with the formula $\mu = \zeta^{\star-1} = \zeta \circ S$. Rewriting this via the antipode formula for $S$ given in Proposition 7.2.2 yields P. Hall's formula.

**Corollary 7.2.3.** *For a finite bounded poset $P$, one has*

$$\mu[P] = \sum_{k \geq 0} (-1)^k |\{\textit{chains } \hat{0} = x_0 < \cdots < x_k = \hat{1} \textit{ in } P\}|.$$

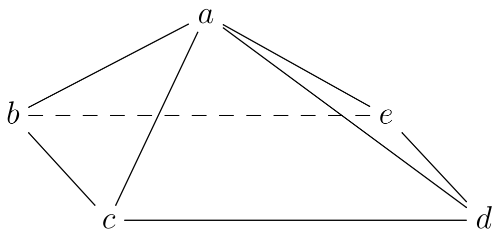
We can also notice that $S$ is an algebra anti-endomorphism (by Proposition 1.4.10), thus an algebra endomorphism (since $\mathbf{k}[\mathcal{P}]$ is commutative, so Exercise 1.5.8(a) shows that the algebra anti-endomorphisms of $\mathbf{k}[\mathcal{P}]$ are the same as the algebra endomorphisms of $\mathbf{k}[\mathcal{P}]$). Hence, $\mu = \zeta \circ S$ is a composition of two algebra homomorphisms, thus an algebra homomorphism itself. We therefore obtain the following classical fact:

**Corollary 7.2.4.** *For two finite bounded posets $P$ and $Q$, we have $\mu[P \times Q] = \mu[P] \cdot \mu[Q]$.*

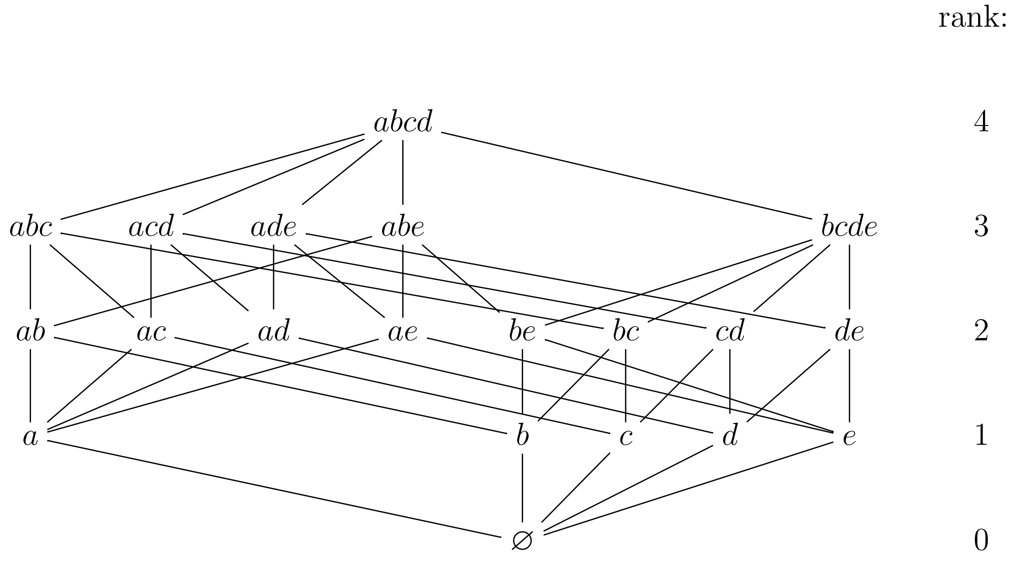
7.2.2. *The incidence Hopf algebras for ranked posets and Ehrenborg's function.*

**Definition 7.2.5.** Take $\mathcal{P}$ to be the class of bounded *ranked* finite posets $P$, that is, those for which all maximal chains from $\hat{0}$ to $\hat{1}$ have the same length $r(P)$. This is a hereditary class, as it implies that any interval is $[x, y]_P$ is also ranked, and the product of two bounded ranked posets is also bounded and ranked. It also uniquely defines a *rank function* $P \xrightarrow{r} \mathbb{N}$ in which $r(\hat{0}) = 0$ and $r(x)$ is the length of any maximal chain from $\hat{0}$ to $x$.

**Example 7.2.6.** Consider a pyramid with apex vertex $a$ over a square base with vertices $b, c, d, e$:



Ordering its faces by inclusion gives a bounded ranked poset $P$, where the rank of an element is one more than the dimension of the face it represents:



**Definition 7.2.7.** *Ehrenborg's quasisymmetric function* $\Psi[P]$ for a bounded ranked poset $P$ is the image of $[P]$ under the map $\mathbf{k}[\mathcal{P}] \xrightarrow{\Psi} \mathrm{QSym}$ induced by the zeta function $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$ as a character, via Theorem 7.1.3.

The quasisymmetric function $\Psi[P]$ captures several interesting combinatorial invariants of $P$; see Stanley [206, Chap. 3] for more background on these notions.

**Definition 7.2.8.** Let $P$ be a bounded ranked poset $P$ of rank $r(P) := r(\hat{1})$. Define its *rank-generating function*

$$RGF(P,q) := \sum_{p \in P} q^{r(p)} \in \mathbb{Z}[q],$$

its *characteristic polynomial*

$$\chi(P,q) := \sum_{p \in P} \mu(\hat{0},p) q^{r(p)} \in \mathbb{Z}[q]$$

(where $\mu(u,v)$ is shorthand for $\mu([u,v])$), and its *zeta polynomial*

$$\begin{aligned} & Z(P,m) \\ (7.2.1) \qquad & = |\{\text{multichains } \hat{0} \leq_P p_1 \leq_P \cdots \leq_P p_{m-1} \leq_P \hat{1}\}| \\ (7.2.2) \qquad & = \sum_{s=0}^{r(P)-1} \binom{m}{s+1} |\{\text{chains } \hat{0} < p_1 < \cdots < p_s < \hat{1}\}| \\ & \in \mathbb{Q}[m] \end{aligned}$$

[352]. Also, for each subset $S \subset \{1, 2, \ldots, r(P) - 1\}$, define the *flag number* $f_S$ of $P$ by

$$f_S = |\{\text{chains } \hat{0} <_P p_1 <_P \cdots <_P p_s <_P \hat{1} \text{ with } \{r(p_1), \ldots, r(p_s)\} = S\}|.$$

[352] Actually, (7.2.2) is false if $|P| = 1$ (but only then). We use (7.2.1) to define $Z(P,m)$ in this case.

These flag numbers are the components of the *flag $f$-vector* $(f_S)_{S\subset[r-1]}$ of $P$. Further define the *flag $h$-vector* $(h_T)_{T\subset[r-1]}$ of $P$, whose entries $h_T$ are given by $f_S = \sum_{T\subset S} h_T$, or, equivalently[353], by $h_S = \sum_{T\subset S}(-1)^{|S\setminus T|} f_T$.

**Example 7.2.9.** For the poset $P$ in Example 7.2.6, one has $RGF(P,q) = 1+5q+8q^2+5q^3+q^4$. Since $P$ is the poset of faces of a polytope, the Möbius function values for its intervals are easily predicted: $\mu(x,y) = (-1)^{r[x,y]}$, that is, $P$ is an *Eulerian ranked poset*; see Stanley [206, §3.16]. Hence its characteristic polynomial is trivially related to the rank generating function, sending $q \mapsto -q$, that is,

$$\chi(P,q) = RGF(P,-q) = 1 - 5q + 8q^2 - 5q^3 + q^4.$$

Its flag $f$-vector and $h$-vector entries are given in the following table.

| $S$ | $f_S$ | | $h_S$ |
|---|---|---|---|
| $\varnothing$ | 1 | | 1 |
| $\{1\}$ | 5 | $5-1=$ | 4 |
| $\{2\}$ | 8 | $8-1=$ | 7 |
| $\{3\}$ | 5 | $5-1=$ | 4 |
| $\{1,2\}$ | 16 | $16-(5+8)+1=$ | 4 |
| $\{1,3\}$ | 16 | $16-(5+5)+1=$ | 7 |
| $\{2,3\}$ | 16 | $16-(5+8)+1=$ | 4 |
| $\{1,2,3\}$ | 32 | $32-(16+16+16)+(5+8+5)-1=$ | 1 |

and using (7.2.2), its zeta polynomial is

$$\begin{aligned} Z(P,m) &= 1\binom{m}{1} + (5+8+5)\binom{m}{2} + (16+16+16)\binom{m}{3} + 32\binom{m}{4} \\ &= \frac{m^2(2m-1)(2m+1)}{3}. \end{aligned}$$

**Theorem 7.2.10.** *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Ehrenborg's quasisymmetric function $\Psi[P]$ for a bounded ranked poset $P$ encodes*

(i) *the flag $f$-vector entries $f_S$ and flag $h$-vector entries $h_S$ as its $M_\alpha$ and $L_\alpha$ expansion coefficients*[354] *:*

$$\Psi[P] = \sum_\alpha f_{D(\alpha)}(P)\ M_\alpha = \sum_\alpha h_{D(\alpha)}(P)\ L_\alpha,$$

(ii) *the zeta polynomial as the specialization from Definition 7.1.6*

$$Z(P,m) = \mathrm{ps}^1(\Psi[P])(m) = [\Psi[P]]_{\substack{x_1=x_2=\cdots=x_m=1,\\ x_{m+1}=x_{m+2}=\cdots=0}},$$

(iii) *the rank-generating function as the specialization*

$$RGF(P,q) = [\Psi[P]]_{\substack{x_1=q,x_2=1,\\ x_3=x_4=\cdots=0}},$$

(iv) *the characteristic polynomial as the convolution*

$$\chi(P,q) = ((\psi_q \circ S) \star \zeta_Q) \circ \Psi[P],$$

*where* $\mathrm{QSym} \xrightarrow{\psi_q} \mathbf{k}[q]$ *maps* $f(\mathbf{x}) \longmapsto f(q,0,0,\ldots)$.

[353] The equivalence follows from inclusion-exclusion (more specifically, from the converse of Lemma 5.2.6(a)).

[354] In fact, Ehrenborg *defined* $\Psi[P]$ in [64, Defn. 4.1] via this $M_\alpha$ expansion, and then showed that it gave a Hopf morphism.

*Proof.* In assertion (i), the expansion $\Psi[P] = \sum_\alpha f_{D(\alpha)}(P)\, M_\alpha$ is (7.1.3), since $\zeta_\alpha[P] = f_{D(\alpha)}(P)$. The $L_\alpha$ expansion follows from this, as $L_\alpha = \sum_{\beta: D(\beta)\supset D(\alpha)} M_\beta$ and $f_S(P) = \sum_{T\subset S} h_T$.

Assertion (ii) is immediate from Proposition 7.1.7(iv), since $Z(P,m) = \zeta^{\star m}[P]$.

Assertion (iii) can be deduced from assertion (i), but it is perhaps more fun and in the spirit of things to proceed as follows. Note that $\psi_q(M_\alpha) = q^n$ for $\alpha = (n)$, and $\psi_q(M_\alpha)$ vanishes for all other $\alpha \neq (n)$ in $\mathrm{Comp}_n$. Hence for a bounded ranked poset $P$ one has

$$(\psi_q \circ \Psi)[P] = q^{r(P)}. \tag{7.2.3}$$

But if we treat $\zeta_Q : \mathrm{QSym} \to \mathbf{k}$ as a map $\mathrm{QSym} \to \mathbf{k}[q]$, then (1.4.2) (applied to $\mathbf{k}[\mathcal{P}]$, QSym, $\mathbf{k}[q]$, $\mathbf{k}[q]$, $\Psi$, $\mathrm{id}_{\mathbf{k}[q]}$, $\psi_q$ and $\zeta_Q$ instead of $C$, $C'$, $A$, $A'$, $\gamma$, $\alpha$, $f$ and $g$) shows that

$$(\psi_q \star \zeta_Q) \circ \Psi = (\psi_q \circ \Psi) \star (\zeta_Q \circ \Psi), \tag{7.2.4}$$

since $\Psi : \mathbf{k}[\mathcal{P}] \to \mathrm{QSym}$ is a $\mathbf{k}$-coalgebra homomorphism. Consequently, one can compute

$$\begin{aligned} RGF(P,q) &= \sum_{p\in P} q^{r(p)} \cdot 1 = \sum_{p\in P} q^{r([\hat{0},p])} \cdot \zeta[p,\hat{1}] \\ &\overset{\substack{(7.2.3),\\(7.1.2)}}{=} \sum_{p\in P} (\psi_q \circ \Psi)[\hat{0},p] \cdot (\zeta_Q \circ \Psi)[p,\hat{1}] \\ &= ((\psi_q \circ \Psi) \star (\zeta_Q \circ \Psi))\,[P] \overset{(7.2.4)}{=} (\psi_q \star \zeta_Q)(\Psi[P]) \\ &= (\psi_q \otimes \zeta_Q)\,(\Delta\Psi[P]) \\ &= [\Psi[P](\mathbf{x},\mathbf{y})]_{\substack{x_1=q,x_2=x_3=\cdots=0\\ y_1=1,y_2=y_3=\cdots=0}} = [\Psi[P](\mathbf{x})]_{\substack{x_1=q,x_2=1,\\ x_3=x_4=\cdots=0}}. \end{aligned}$$

Similarly, for assertion (iv) first note that

$$((\psi_q \circ S) \star \zeta_Q) \circ \Psi = (\psi_q \circ S \circ \Psi) \star (\zeta_Q \circ \Psi), \tag{7.2.5}$$

(this is proven similarly to (7.2.4), but now using the map $\psi_q \circ S$ instead of $\psi_q$). Now, Proposition 7.2.2 and Corollary 7.2.3 let one calculate that

$$\begin{aligned} &(\psi_q \circ \Psi \circ S)[P] \\ &= \sum_k (-1)^k \sum_{\hat{0}=x_0<\cdots<x_k=\hat{1}} (\psi_q \circ \Psi)([x_0,x_1]) \cdots (\psi_q \circ \Psi)([x_{k-1},x_k]) \\ &\overset{(7.2.3)}{=} \sum_k (-1)^k \sum_{\hat{0}=x_0<\cdots<x_k=\hat{1}} q^{r(P)} = \mu(\hat{0},\hat{1}) q^{r(P)}. \end{aligned}$$

This is used in the penultimate equality here:

$$\begin{aligned} ((\psi_q \circ S) \star \zeta_Q) \circ \Psi[P] &\overset{(7.2.5)}{=} ((\psi_q \circ S \circ \Psi) \star (\zeta_Q \circ \Psi))[P] \\ &= ((\psi_q \circ \Psi \circ S) \star \zeta)[P] = \sum_{p\in P} (\psi_q \circ \Psi \circ S)[\hat{0},p] \cdot \zeta[p,\hat{1}] \\ &= \sum_{p\in P} \mu[\hat{0},p] q^{r(p)} = \chi(P,q). \qquad \square \end{aligned}$$

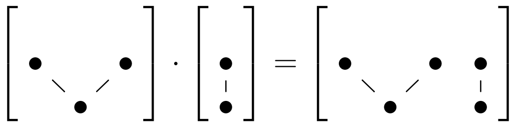
7.3. **Example: Stanley's chromatic symmetric function of a graph.** We introduce the *chromatic Hopf algebra of graphs* and an associated character $\zeta$ so that the map $\Psi$ from Theorem 7.1.3 sends a graph $G$ to Stanley's *chromatic symmetric function* of $G$. Then principal specialization $\mathrm{ps}^1$ sends this to the *chromatic polynomial* of the graph.

7.3.1. *The chromatic Hopf algebra of graphs.*

**Definition 7.3.1.** The *chromatic Hopf algebra* (see Schmitt [194, §3.2]) $\mathcal{G}$ is a free $\mathbf{k}$-module whose $\mathbf{k}$-basis elements $[G]$ are indexed by isomorphism classes of (finite) simple graphs $G = (V, E)$. Define for $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ the multiplication

$$[G_1] \cdot [G_2] := [G_1 \sqcup G_2]$$

where $[G_1 \sqcup G_2]$ denote the isomorphism class of the disjoint union, on vertex set $V = V_1 \sqcup V_2$ which is a disjoint union of copies of their vertex sets $V_1, V_2$, with edge set $E = E_1 \sqcup E_2$. For example,



Thus the class $[\varnothing]$ of the empty graph $\varnothing$ having $V = \varnothing, E = \varnothing$ is a unit element.

Given a graph $G = (V, E)$ and a subset $V' \subset V$, the *subgraph induced on vertex set* $V'$ is defined as the graph $G|_{V'} := (V', E')$ with edge set $E' = \{e \in E : e = \{v_1, v_2\} \subset V'\}$. This lets one define a comultiplication $\Delta : \mathcal{G} \to \mathcal{G} \otimes \mathcal{G}$ by setting

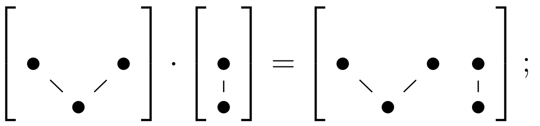
$$\Delta[G] := \sum_{(V_1,V_2):V_1 \sqcup V_2 = V} [G|_{V_1}] \otimes [G|_{V_2}].$$

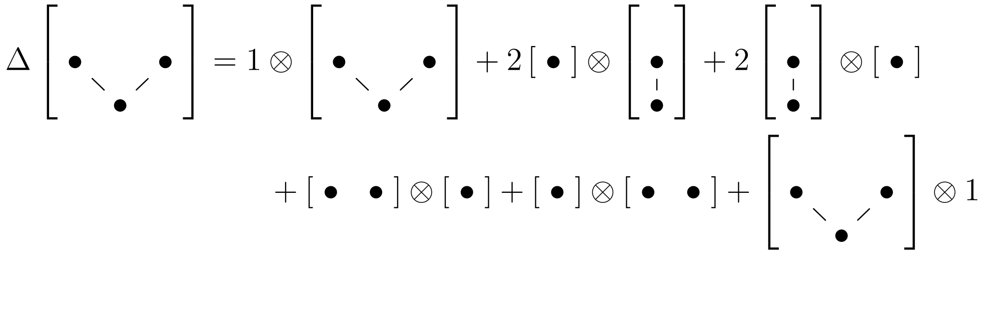
Define a counit $\epsilon : \mathcal{G} \to \mathbf{k}$ by

$$\epsilon[G] := \begin{cases} 1, & \text{if } G = \varnothing; \\ 0, & \text{otherwise.} \end{cases}$$

**Proposition 7.3.2.** *The above maps endow $\mathcal{G}$ with the structure of a connected graded finite type Hopf algebra over* $\mathbf{k}$, *which is both commutative and cocommutative.*

**Example 7.3.3.** Here are some examples of these structure maps:





*Proof of Proposition 7.3.2.* The associativity of the multiplication and comultiplication should be clear as

$$m^{(2)}([G_1] \otimes [G_2] \otimes [G_3]) = [G_1 \sqcup G_2 \sqcup G_3],$$
$$\Delta^{(2)}[G] = \sum_{\substack{(V_1,V_2,V_3): \\ V=V_1 \sqcup V_2 \sqcup V_3}} [G|_{V_1}] \otimes [G|_{V_2}] \otimes [G|_{V_3}].$$

Checking the unit and counit conditions are straightforward. Commutativity of the pentagonal bialgebra diagram in (1.3.4) comes down to check that, given graphs $G_1, G_2$ on disjoint vertex sets $V_1, V_2$ , when one applies to $[G_1] \otimes [G_2]$ either the composite $\Delta \circ m$ or the composite $(m \otimes m) \circ (\mathrm{id} \otimes T \otimes \mathrm{id}) \circ (\Delta \otimes \Delta)$, the result is the same:

$$\sum_{\substack{(V_{11},V_{12},V_{21},V_{22}): \\ V_1=V_{11} \sqcup V_{12} \\ V_2=V_{21} \sqcup V_{22}}} [G_1|_{V_{11}} \sqcup G_2|_{V_{21}}] \otimes [G_1|_{V_{12}} \sqcup G_2|_{V_{22}}].$$

Letting $\mathcal{G}_n$ be the $\mathbf{k}$-span of $[G]$ having $n$ vertices makes $\mathcal{G}$ a bialgebra which is graded and connected, and hence also a Hopf algebra by Proposition 1.4.16. Cocommutativity should be clear, and commutativity follows from the graph isomorphism $G_1 \sqcup G_2 \cong G_2 \sqcup G_1$. Finally, $\mathcal{G}$ is of finite type since there are only finitely many isomorphism classes of simple graphs on $n$ vertices for every given $n$. □

*Remark* 7.3.4. Humpert and Martin [103, Theorem 3.1] gave the following expansion for the antipode in the chromatic Hopf algebra, containing fewer terms than Takeuchi's general formula (1.4.7): given a graph $G = (V, E)$, one has

$$S[G] = \sum_F (-1)^{|V|-\mathrm{rank}(F)} \operatorname{acyc}(G/F)[G_{V,F}]. \tag{7.3.1}$$

Here $F$ runs over all subsets of edges that form *flats* in the graphic matroid for $G$, meaning that if $e = \{v, v'\}$ is an edge in $E$ for which one has a path of edges in $F$ connecting $v$ to $v'$, then $e$ also lies in $F$. Here $G/F$ denotes the quotient graph in which all of the edges of $F$ have been *contracted*, while $\operatorname{acyc}(G/F)$ denotes its number of *acyclic orientations*, and $G_{V,F} := (V, F)$ as a simple graph.[355]

*Remark* 7.3.5. In [14], Benedetti, Hallam and Machacek define a Hopf algebra of simplicial complexes, which contains $\mathcal{G}$ as a Hopf subalgebra (and also has $\mathcal{G}$ as a quotient Hopf algebra). They compute a formula for its antipode similar to (and generalizing) (7.3.1).

*Remark* 7.3.6. The chromatic Hopf algebra $\mathcal{G}$ is used in [122] and [39, §14.4] to study *Vassiliev invariants of knots.* In fact, a certain quotient of $\mathcal{G}$ (named $\mathcal{F}$ in [122] and $\mathcal{L}$ in [39, §14.4]) is shown to naturally host invariants of *chord diagrams* and therefore Vassiliev invariants of knots.

[355] The notation $\mathrm{rank}(F)$ denotes the *rank* of $F$ in the graphic matroid of $G$. We can define it without reference to matroid theory as the maximum cardinality of a subset $F'$ of $F$ such that the graph $G_{V,F'}$ is acyclic. Equivalently, $\mathrm{rank}(F)$ is $|V| - c(F)$, where $c(F)$ denotes the number of connected components of the graph $G_{V,F}$. Thus, the equality (7.3.1) can be rewritten as $S[G] = \sum_F (-1)^{c(F)} \operatorname{acyc}(G/F)[G_{V,F}]$. In this form, this equality is also proven in [15, Thm. 7.1].

*Remark* 7.3.7. The $\mathbf{k}$-algebra $\mathcal{G}$ is isomorphic to a polynomial algebra (in infinitely many indeterminates) over $\mathbf{k}$. Indeed, every finite graph can be uniquely written as a disjoint union of finitely many connected finite graphs (up to order). Therefore, the basis elements $[G]$ of $\mathcal{G}$ corresponding to connected finite graphs $G$ are algebraically independent in $\mathcal{G}$ and generate the whole $\mathbf{k}$-algebra $\mathcal{G}$ (indeed, the disjoint unions of connected finite graphs are precisely the monomials in these elements). Thus, $\mathcal{G}$ is isomorphic to a polynomial $\mathbf{k}$-algebra with countably many generators (one for each isomorphism class of connected finite graphs). As a consequence, for example, we see that $\mathcal{G}$ is an integral domain if $\mathbf{k}$ is an integral domain.

7.3.2. *A "ribbon basis" for $\mathcal{G}$ and self-duality.* In this subsection, we shall explore a second basis of $\mathcal{G}$ and a bilinear form on $\mathcal{G}$. This material will not be used in the rest of these notes (except in Exercise 7.3.25), but it is of some interest and provides an example of how a commutative cocommutative Hopf algebra can be studied.

First, let us define a second basis of $\mathcal{G}$, which is obtained by Möbius inversion (in an appropriate sense) from the standard basis $([G])_{[G] \text{ is an isomorphism class of finite graphs}}$:

**Definition 7.3.8.** For every finite graph $G = (V, E)$, set

$$[G]^\sharp = \sum_{\substack{H=(V,E'); \\ E' \supset E^c}} (-1)^{|E' \setminus E^c|} [H] \in \mathcal{G},$$

where $E^c$ denotes the complement of the subset $E$ in the set of all two-element subsets of $V$. Clearly, $[G]^\sharp$ depends only on the isomorphism class $[G]$ of $G$, not on $G$ itself.

**Proposition 7.3.9.** (a) *Every finite graph $G = (V, E)$ satisfies*

$$[G] = \sum_{\substack{H=(V,E'); \\ E' \cap E = \varnothing}} [H]^\sharp .$$

(b) *The elements $[G]^\sharp$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$.*

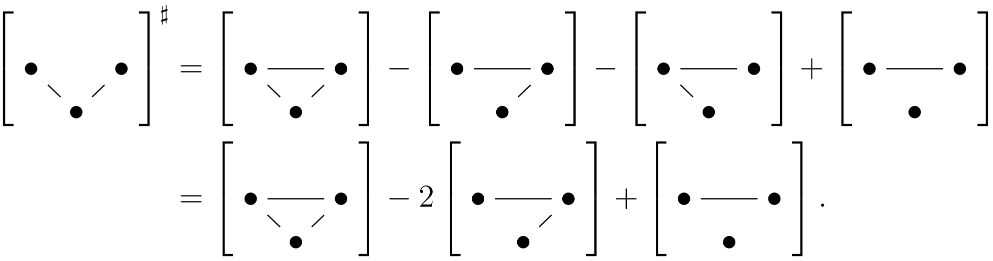
(c) *For any graph $H = (V, E)$, we have*

$$\Delta [H]^\sharp = \sum_{\substack{(V_1,V_2); \\ V=V_1 \sqcup V_2; \\ H=H|_{V_1} \sqcup H|_{V_2}}} [H|_{V_1}]^\sharp \otimes [H|_{V_2}]^\sharp . \tag{7.3.2}$$

(d) *For any two graphs $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$, we have*

$$[H_1]^\sharp [H_2]^\sharp = \sum_{\substack{H=(V_1 \sqcup V_2,E); \\ H|_{V_1}=H_1; \\ H|_{V_2}=H_2}} [H]^\sharp . \tag{7.3.3}$$

For example,



Proving Proposition 7.3.9 is part of Exercise 7.3.14 further below.

The equalities that express the elements $[G]^\sharp$ in terms of the elements $[H]$ (as in Definition 7.3.8), and vice versa (Proposition 7.3.9(a)), are reminiscent of the relations (5.4.10) and (5.4.9) between the bases $(R_\alpha)$ and $(H_\alpha)$ of NSym. In this sense, we can call the basis of $\mathcal{G}$ formed by the $[G]^\sharp$ a "ribbon basis" of $\mathcal{G}$.

We now define a $\mathbf{k}$-bilinear form on $\mathcal{G}$:

**Definition 7.3.10.** For any two graphs $G$ and $H$, let $\operatorname{Iso}(G, H)$ denote the set of all isomorphisms from $G$ to $H$ [356]. Let us now define a $\mathbf{k}$-bilinear form $(\cdot, \cdot) : \mathcal{G} \times \mathcal{G} \to \mathbf{k}$ on $\mathcal{G}$ by setting

$$\left([G]^\sharp, [H]\right) = |\operatorname{Iso}(G, H)| .$$

[357]

**Proposition 7.3.11.** *The form $(\cdot, \cdot) : \mathcal{G} \times \mathcal{G} \to \mathbf{k}$ is symmetric.*

Again, we refer to Exercise 7.3.14 for a proof of Proposition 7.3.11.

The basis of $\mathcal{G}$ constructed in Proposition 7.3.9(b) and the bilinear form $(\cdot, \cdot)$ defined in Definition 7.3.10 can be used to construct a Hopf algebra homomorphism from $\mathcal{G}$ to its graded dual $\mathcal{G}^o$:

**Definition 7.3.12.** For any finite graph $G$, let $\operatorname{aut}(G)$ denote the number $|\operatorname{Iso}(G, G)|$. Notice that this is a positive integer, since the set $\operatorname{Iso}(G, G)$ is nonempty (it contains $\operatorname{id}_G$).

Now, recall that the Hopf algebra $\mathcal{G}$ is a connected graded Hopf algebra of finite type. The $n$-th homogeneous component is spanned by the $[G]$ where $G$ ranges over the graphs with $n$ vertices. Since $\mathcal{G}$ is of finite type, its graded dual $\mathcal{G}^o$ is defined. Let $([G]^*)_{[G] \text{ is an isomorphism class of finite graphs}}$ be the basis of $\mathcal{G}^o$ dual to the basis $([G])_{[G] \text{ is an isomorphism class of finite graphs}}$ of $\mathcal{G}$. Define a $\mathbf{k}$-linear map $\psi : \mathcal{G} \to \mathcal{G}^o$ by

$$\psi\left([G]^\sharp\right) = \operatorname{aut}(G) \cdot [G]^* \qquad \text{for every finite graph } G.$$

[356] We recall that if $G = (V, E)$ and $H = (W, F)$ are two graphs, then an *isomorphism* from $G$ to $H$ means a bijection $\varphi : V \to W$ such that $\varphi_*(E) = F$. Here, $\varphi_*$ denotes the map from the powerset of $V$ to the powerset of $W$ which sends every $T \subset V$ to $\varphi(T) \subset W$.

[357] This is well-defined, because:

- the number $|\operatorname{Iso}(G, H)|$ depends only on the isomorphism classes $[G]$ and $[H]$ of $G$ and $H$, but not on $G$ and $H$ themselves;
- the elements $[G]^\sharp$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$ (because of Proposition 7.3.9(b));
- the elements $[G]$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$.

[358]

**Proposition 7.3.13.** *Consider the map $\psi : \mathcal{G} \to \mathcal{G}^o$ defined in Definition 7.3.12.*

(a) *This map $\psi$ satisfies $(\psi(a))(b) = (a, b)$ for all $a \in \mathcal{G}$ and $b \in \mathcal{G}$.*
(b) *The map $\psi : \mathcal{G} \to \mathcal{G}^o$ is a Hopf algebra homomorphism.*
(c) *If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the map $\psi$ is a Hopf algebra isomorphism $\mathcal{G} \to \mathcal{G}^o$.*

**Exercise 7.3.14.** Prove Proposition 7.3.9, Proposition 7.3.11 and Proposition 7.3.13.

*Remark* 7.3.15. Proposition 7.3.13(c) shows that the Hopf algebra $\mathcal{G}$ is self-dual when $\mathbb{Q}$ is a subring of $\mathbf{k}$. On the other hand, if $\mathbf{k}$ is a field of positive characteristic, then $\mathcal{G}$ is never self-dual. Here is a quick way to see this: The elements $[G]^*$ of $\mathcal{G}^o$ defined in Definition 7.3.12 have the property that

$$\left([\circ]^*\right)^n = n! \cdot \sum_{\substack{[G] \text{ is an isomorphism} \\ \text{class of finite graphs on} \\ n \text{ vertices}}} [G]^*$$

for every $n \in \mathbb{N}$, where $\circ$ denotes the graph with one vertex.[359] Thus, if $p$ is a prime and $\mathbf{k}$ is a field of characteristic $p$, then $\left([\circ]^*\right)^p = 0$. Hence, the $\mathbf{k}$-algebra $\mathcal{G}^o$ has nilpotents in this situation. However, the $\mathbf{k}$-algebra $\mathcal{G}$ does not (indeed, Remark 7.3.7 shows that it is an integral domain whenever $\mathbf{k}$ is an integral domain). Thus, when $\mathbf{k}$ is a field of characteristic $p$, then $\mathcal{G}$ and $\mathcal{G}^o$ are not isomorphic as $\mathbf{k}$-algebras (let alone as Hopf algebras).

7.3.3. *Stanley's chromatic symmetric function of a graph.*

**Definition 7.3.16.** *Stanley's chromatic symmetric function* $\Psi[G]$ for a simple graph $G = (V, E)$ is the image of $[G]$ under the map $\mathcal{G} \xrightarrow{\Psi} \mathrm{QSym}$ induced via Theorem 7.1.3 from the *edge-free character* $\mathcal{G} \xrightarrow{\zeta} \mathbf{k}$ defined by

(7.3.4)
$$\zeta[G] = \begin{cases} 1, & \text{if } G \text{ has no edges, that is, } G \text{ is an independent/stable} \\ & \qquad\qquad \text{set of vertices;} \\ 0, & \text{otherwise.} \end{cases}$$

Note that, because $\mathcal{G}$ is cocommutative, $\Psi[G]$ is symmetric and not just quasisymmetric; see Remark 7.1.4.

Recall that for a graph $G = (V, E)$, a (vertex-)coloring $f : V \to \{1, 2, \ldots\}$ is called *proper* if no edge $e = \{v, v'\}$ in $E$ has $f(v) = f(v')$.

[358] This is well-defined, since $\left([G]^\sharp\right)_{[G] \text{ is an isomorphism class of finite graphs}}$ is a basis of the $\mathbf{k}$-module $\mathcal{G}$ (because of Proposition 7.3.9(b)).

[359] To see this, observe that the tensor $[\circ]^{\otimes n}$ appears in the iterated coproduct $\Delta^{(n-1)}([G])$ exactly $n!$ times whenever $G$ is a graph on $n$ vertices.

**Proposition 7.3.17.** *For a graph $G = (V, E)$, the symmetric function $\Psi[G]$ has the expansion* [360]

$$\Psi[G] = \sum_{\substack{\text{proper colorings} \\ f:V\to\{1,2,\ldots\}}} \mathbf{x}_f$$

*where $\mathbf{x}_f := \prod_{v\in V} x_{f(v)}$. In particular, its specialization from Proposition 7.1.6 gives the chromatic polynomial of $G$:*

$$\mathrm{ps}^1\Psi[G](m) = \chi_G(m) = |\{\text{proper colorings } f : V \to \{1, 2, \ldots, m\}\}| .$$

*Proof.* The iterated coproduct $\mathcal{G} \xrightarrow{\Delta^{(\ell-1)}} \mathcal{G}^{\otimes\ell}$ sends

$$[G] \longmapsto \sum_{\substack{(V_1,\ldots,V_\ell): \\ V=V_1\sqcup\cdots\sqcup V_\ell}} [G|_{V_1}] \otimes \cdots \otimes [G|_{V_\ell}]$$

and the map $\zeta^{\otimes\ell}$ sends each addend on the right to 1 or 0, depending upon whether each $V_i \subset V$ is a stable set or not, that is, whether the assignment of color $i$ to the vertices in $V_i$ gives a proper coloring of $G$. Thus formula (7.1.3) shows that the coefficient $\zeta_\alpha$ of $x_1^{\alpha_1} \cdots x_\ell^{\alpha_\ell}$ in $\Psi[G]$ counts the proper colorings $f$ in which $|f^{-1}(i)| = \alpha_i$ for each $i$. □

**Example 7.3.18.** For the complete graph $K_n$ on $n$ vertices, one has

$$\Psi[K_n] = n!e_n, \qquad \text{thus}$$

$$\mathrm{ps}^1(\Psi[K_n])(m) = n!e_n(\underbrace{1, 1, \ldots, 1}_{m \text{ ones}}) = n!\binom{m}{n}$$
$$= m(m-1)\cdots(m-(n-1)) = \chi_{K_n}(m).$$

In particular, the single vertex graph $K_1$ has $\Psi[K_1] = e_1$, and since the Hopf morphism $\Psi$ is in particular an algebra morphism, a graph $K_1^{\sqcup n}$ having $n$ isolated vertices and no edges will have $\Psi[K_1^{\sqcup n}] = e_1^n$.

As a slightly more interesting example, the graph $P_3$ which is a path having three vertices and two edges will have

$$\Psi[P_3] = m_{(2,1)} + 6m_{(1,1,1)} = e_2e_1 + 3e_3.$$

One might wonder, based on the previous examples, when $\Psi[G]$ is *e-positive*, that is, when does its unique expansion in the $\{e_\lambda\}$ basis for $\Lambda$ have nonnegative coefficients? This is an even stronger assertion than *s-positivity*, that is, having nonnegative coefficients for the expansion in terms of Schur functions $\{s_\lambda\}$, since each $e_\lambda$ is $s$-positive. This weaker property fails, starting with the *claw graph* $K_{3,1}$, which has

$$\Psi[K_{3,1}] = s_{(3,1)} - s_{(2,2)} + 5s_{(2,1,1)} + 8s_{(1,1,1,1)}.$$

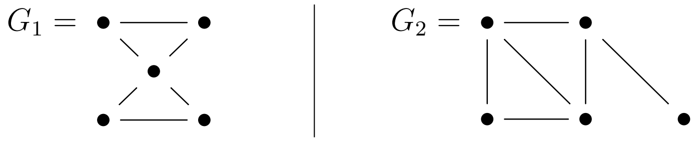
On the other hand, a result of Gasharov [75, Theorem 2] shows that one at least has $s$-positivity for $\Psi[\mathrm{inc}(P)]$ where $\mathrm{inc}(P)$ is the *incomparability graph* of a poset which is $(\mathbf{3} + \mathbf{1})$-free; we refer the reader to Stanley [205, §5] for a discussion of the following conjecture, which remains open[361]:

[360] In fact, Stanley *defined* $\Psi[G]$ in [205, Defn. 2.1] via this expansion.

[361] A recent refinement for incomparability graphs of posets which are both $(\mathbf{3} + \mathbf{1})$- and $(\mathbf{2}+\mathbf{2})$-free, also known as *unit interval orders* is discussed by Shareshian and Wachs [198].

**Conjecture 7.3.19.** *For any* $(\mathbf{3}+\mathbf{1})$*-free poset* $P$*, the incomparability graph* $\operatorname{inc}(P)$ *has* $\Psi[\operatorname{inc}(P)]$ *an e-positive symmetric function.*

Here is another question about $\Psi[G]$: how well does it distinguish non-isomorphic graphs? Stanley gave this example of two graphs $G_1, G_2$ having $\Psi[G_1] = \Psi[G_2]$:



At least $\Psi[G]$ appears to do better at distinguishing *trees*, much better than its specialization, the chromatic polynomial $\chi_G(m)$, which takes the same value $m(m-1)^{n-1}$ on all trees with $n$ vertices.

**Question 7.3.20.** Does the chromatic symmetric function (for $\mathbf{k} = \mathbb{Z}$) distinguish trees?

It has been checked that the answer is affirmative for trees on 23 vertices or less. There are also interesting partial results on this question by Martin, Morin and Wagner [161].

We close this section with a few other properties of $\Psi[G]$ proven by Stanley which follow easily from the theory we have developed. For example, his work makes no explicit mention of the chromatic Hopf algebra $\mathcal{G}$, and the fact that $\Psi$ is a Hopf morphism (although he certainly notes the trivial algebra morphism property $\Psi[G_1 \sqcup G_2] = \Psi[G_1]\Psi[G_2]$). One property he proves is implicitly related to $\Psi$ as a coalgebra morphism: he considers (in the case when $\mathbb{Q}$ is a subring of $\mathbf{k}$) the effect on $\Psi$ of the operator $\frac{\partial}{\partial p_1} : \Lambda_{\mathbb{Q}} \longrightarrow \Lambda_{\mathbb{Q}}$ which acts by first expressing a symmetric function $f \in \Lambda_{\mathbb{Q}}$ as a polynomial in the power sums $\{p_n\}$, and then applies the partial derivative operator $\frac{\partial}{\partial p_1}$ of the polynomial ring $\mathbb{Q}[p_1, p_2, p_3, \ldots]$. It is not hard to see that $\frac{\partial}{\partial p_1}$ is the same as the skewing operator $s_{(1)}^{\perp} = p_1^{\perp}$: both act as derivations on $\Lambda_{\mathbb{Q}} = \mathbb{Q}[p_1, p_2, \ldots]$ (since $p_1 \in \Lambda_{\mathbb{Q}}$ is primitive), and agree in their effect on each $p_n$, in that both send $p_1 \mapsto 1$, and both annihilate $p_2, p_3, \ldots$.

**Proposition 7.3.21.** *(Stanley* [205, Cor. 2.12(a)]*) For any graph* $G = (V, E)$*, one has*

$$\frac{\partial}{\partial p_1}\Psi[G] = \sum_{v \in V} \Psi[G|_{V \setminus v}].$$

*Proof.* Since $\Psi$ is a coalgebra homomorphism, we have

$$\Delta\Psi[G] = (\Psi \otimes \Psi)\Delta[G] = \sum_{\substack{(V_1,V_2):\\ V = V_1 \sqcup V_2}} \Psi[G|_{V_1}] \otimes \Psi[G|_{V_2}].$$

Using this expansion (and the equality $\frac{\partial}{\partial p_1} = s_{(1)}^{\perp}$), we now compute

$$\frac{\partial}{\partial p_1}\Psi[G] = s_{(1)}^{\perp}\Psi[G] = \sum_{\substack{(V_1,V_2):\\ V = V_1 \sqcup V_2}} (s_{(1)}, \Psi[G|_{V_1}]) \cdot \Psi[G|_{V_2}] = \sum_{v \in V} \Psi[G|_{V \setminus v}]$$

(since degree considerations force $(s_{(1)}, \Psi[G|_{V_1}]) = 0$ unless $|V_1| = 1$, in which case $\Psi[G|_{V_1}] = s_{(1)}$). □

**Definition 7.3.22.** Given a graph $G = (V, E)$, an acyclic orientation $\Omega$ of the edges $E$ (that is, an orientation of each edge such that the resulting directed graph has no cycles), and a vertex-coloring $f : V \to \{1, 2, \ldots\}$, say that the pair $(\Omega, f)$ are *weakly compatible* if whenever $\Omega$ orients an edge $\{v, v'\}$ in $E$ as $v \to v'$, one has $f(v) \leq f(v')$. Note that a *proper* vertex-coloring $f$ of a graph $G = (V, E)$ is weakly compatible with a unique acyclic orientation $\Omega$.

**Proposition 7.3.23.** *(Stanley* [205, Prop. 4.1, Thm. 4.2]*) The involution $\omega$ of $\Lambda$ sends $\Psi[G]$ to $\omega(\Psi[G]) = \sum_{(\Omega,f)} \mathbf{x}_f$ in which the sum runs over weakly compatible pairs $(\Omega, f)$ of an acyclic orientation $\Omega$ and vertex-coloring $f$.*

*Furthermore, the chromatic polynomial $\chi_G(m)$ has the property that $(-1)^{|V|}\chi_G(-m)$ counts all such weakly compatible pairs $(\Omega, f)$ in which $f : V \to \{1, 2, \ldots, m\}$ is a vertex-$m$-coloring.*

*Proof.* As observed above, a proper coloring $f$ is weakly compatible with a unique acyclic orientation $\Omega$ of $G$. Denote by $P_\Omega$ the poset on $V$ which is the transitive closure of $\Omega$, endowed with a *strict labelling* by integers, that is, every $i \in P_\Omega$ and $j \in P_\Omega$ satisfying $i <_{P_\Omega} j$ must satisfy $i >_{\mathbb{Z}} j$. Then proper colorings $f$ that induce $\Omega$ are the same as $P_\Omega$-partitions, so that

$$\Psi[G] = \sum_{\Omega} F_{P_\Omega}(\mathbf{x}). \tag{7.3.5}$$

Applying the antipode $S$ and using Corollary 5.2.20 gives

$$\omega(\Psi[G]) = (-1)^{|V|} S(\Psi[G]) = \sum_{\Omega} F_{P_\Omega^{\mathrm{opp}}}(\mathbf{x}) = \sum_{(\Omega,f)} \mathbf{x}_f$$

where in the last line one sums over weakly compatible pairs as in the proposition. The last equality comes from the fact that since each $P_\Omega$ has been given a strict labelling, $P_\Omega^{\mathrm{opp}}$ acquires a *weak (or natural) labelling*, that is, every $i \in P_\Omega$ and $j \in P_\omega$ satisfying $i <_{P_\Omega^{\mathrm{opp}}} j$ must satisfy $i <_{\mathbb{Z}} j$.

The last assertion follows from Proposition 7.1.7(iii). □

*Remark* 7.3.24. The interpretation of $\chi_G(-m)$ in Proposition 7.3.23 is a much older result of Stanley [204]. The special case interpreting $\chi_G(-1)$ as $(-1)^{|V|}$ times the number of acyclic orientations of $G$ has sometimes been called Stanley's *(-1)-color theorem.* It also follows (via Proposition 7.1.7) from Humpert and Martin's antipode formula for $\mathcal{G}$ discussed in Remark 7.3.4: taking $\zeta$ to be the character of $\mathcal{G}$ given in (7.3.4),

$$\begin{aligned}\chi_G(-1) = \zeta^{\star(-1)}[G] = \zeta(S[G]) &= \sum_F (-1)^{|V|-\mathrm{rank}(F)} \operatorname{acyc}(G/F)\zeta[G_{V,F}] \\ &= (-1)^{|V|} \operatorname{acyc}(G)\end{aligned}$$

where the last equality uses the vanishing of $\zeta$ on graphs that have edges, so only the $F = \varnothing$ term survives.

**Exercise 7.3.25.** If $V$ and $X$ are two sets, and if $f : V \to X$ is any map, then $\operatorname{eqs} f$ will denote the set

$$\{\{u, u'\} \mid u \in V,\ u' \in V,\ u \neq u' \text{ and } f(u) = f(u')\}.$$

This is a subset of the set of all two-element subsets of $V$.

If $G = (V, E)$ is a finite graph, then show that the map $\Psi$ introduced in Definition 7.3.16 satisfies

$$\Psi\left([G]^\sharp\right) = \sum_{\substack{f:V\to\{1,2,3,\ldots\};\\ \text{eqs}\, f=E}} \mathbf{x}_f,$$

where $\mathbf{x}_f := \prod_{v\in V} x_{f(v)}$. Here, $[G]^\sharp$ is defined as in Definition 7.3.8.

7.4. **Example: The quasisymmetric function of a matroid.** We introduce the *matroid-minor Hopf algebra* of Schmitt [191], and studied extensively by Crapo and Schmitt [41, 42, 43]. A very simple character $\zeta$ on this Hopf algebra will then give rise, via the map $\Psi$ from Theorem 7.1.3, to the quasisymmetric function invariant of matroids from the work of Billera, Jia and the second author [21].

7.4.1. *The matroid-minor Hopf algebra.* We begin by reviewing some notions from matroid theory; see Oxley [164] for background, undefined terms and unproven facts.

**Definition 7.4.1.** A *matroid* $M$ of rank $r$ on a (finite) ground set $E$ is specified by a nonempty collection $\mathcal{B}(M)$ of $r$-element subsets of $E$ with the following *exchange property*:

For any $B, B'$ in $\mathcal{B}(M)$ and $b$ in $B$, there exists $b'$ in $B'$ with
$(B \setminus \{b\}) \cup \{b'\}$ in $\mathcal{B}(M)$.

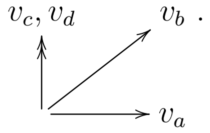
The elements of $\mathcal{B}(M)$ are called the *bases* of the matroid $M$.

**Example 7.4.2.** A matroid $M$ with ground set $E$ is *represented* by a family of vectors $S = (v_e)_{e\in E}$ in a vector space if $\mathcal{B}(M)$ is the collection of subsets $B \subset E$ having the property that the subfamily $(v_e)_{e\in B}$ is a basis for the span of all of the vectors in $S$.

For example, if $M$ is the matroid with

$$\mathcal{B}(M) = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}\}$$

on the ground set $E = \{a, b, c, d\}$, then $M$ is represented by the family $S = (v_a, v_b, v_c, v_d)$ of the four vectors $v_a = (1, 0), v_b = (1, 1), v_c = (0, 1) = v_d$ in $\mathbb{R}^2$ depicted here



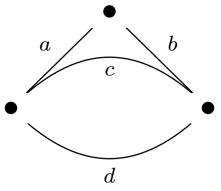
Conversely, whenever $E$ is a finite set and $S = (v_e)_{e\in E}$ is a family of vectors in a vector space, then the set

$$\left\{B \subset E : \text{the subfamily } (v_e)_{e\in B} \text{ is a basis for the span} \right.$$
$$\left. \text{of all of the vectors in } S\right\}$$

is a matroid on the ground set $E$.

A matroid is said to be *linear* if there exists a family of vectors in a vector space representing it. Not all matroids are linear, but many important ones are.

**Example 7.4.3.** A special case of matroids $M$ represented by vectors are *graphic matroids*, coming from a graph $G = (V, E)$, with parallel edges and self-loops allowed. One represents these by vectors in $\mathbb{R}^V$ with standard basis $\{\epsilon_v\}_{v \in V}$ by associating the vector $\epsilon_v - \epsilon_{v'}$ to any edge connecting a vertex $v$ with a vertex $v'$. One can check (or see [164, §1.2]) that the bases $B$ in $\mathcal{B}(M)$ correspond to the edge sets of *spanning forests* for $G$, that is, edge sets which are acyclic and contain one spanning tree for each connected component of $G$. For example, the matroid $\mathcal{B}(M)$ corresponding to the graph $G = (V, E)$ shown below:



is exactly the matroid represented by the vectors in Example 7.4.2; indeed, the spanning forests of this graph $G$ are the edge sets $\{a, b\}, \{a, c\}, \{a, d\}$, $\{b, c\}, \{b, d\}$. (In this example, spanning forests are the same as spanning trees, since $G$ is connected.)

To define the matroid-minor Hopf algebra one needs the basic matroid operations of *deletion* and *contraction*. These model the operations of deleting or contracting an edge in a graph. For configurations of vectors they model the deletion of a vector, or the passage to images in the quotient space modulo the span of a vector.

**Definition 7.4.4.** Given a matroid $M$ of rank $r$ and an element $e$ of its ground set $E$, say that $e$ is *loop* (resp. *coloop*) of $M$ if $e$ lies in no basis (resp. every basis) $B$ in $\mathcal{B}(M)$. If $e$ is not a coloop, the *deletion* $M \setminus e$ is a matroid of rank $r$ on ground set $E \setminus \{e\}$ having bases

$$\mathcal{B}(M \setminus e) := \{B \in \mathcal{B}(M) : e \notin B\}. \tag{7.4.1}$$

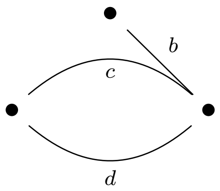
If $e$ is not a loop, the *contraction* $M/e$ is a matroid of rank $r - 1$ on ground set $E \setminus \{e\}$ having bases

$$\mathcal{B}(M/e) := \{B \setminus \{e\} : e \in B \in \mathcal{B}(M)\}. \tag{7.4.2}$$

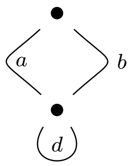
When $e$ is a loop of $M$, then $M/e$ has rank $r$ instead of $r - 1$ and one defines its bases as in (7.4.1) rather than (7.4.2); similarly, if $e$ is a coloop of $M$ then $M \setminus e$ has rank $r - 1$ instead of $r$ and one defines its bases as in (7.4.2) rather than (7.4.1).

**Example 7.4.5.** Starting with the graph $G$ and its graphic matroid $M$ from Example 7.4.3, the deletion $M \setminus a$ and contraction $M/c$ correspond to the graphs $G \setminus a$ and $G/c$ shown here:

$G \setminus a =$



$G/c =$



One has

- $\mathcal{B}(M \setminus a) = \{\{b, c\}, \{b, d\}\}$, so that $b$ has become a coloop in $M \setminus a$, and
- $\mathcal{B}(M/c) = \{\{a\}, \{b\}\}$, so that $d$ has become a loop in $M/c$.

**Definition 7.4.6.** Deletions and contractions commute with each other. Thus, given a matroid $M$ with ground set $E$, and a subset $A \subset E$, two well-defined matroids can be constructed:

- the *restriction* $M|_A$, which is a matroid on ground set $A$, obtained from $M$ by deleting all $e \in E \setminus A$ in any order, and
- the *quotient/contraction* $M/A$, which is a matroid on ground set $E \setminus A$, obtained from $M$ by contracting all $e \in A$ in any order.

We will also need the *direct sum* $M_1 \oplus M_2$ of two matroids $M_1$ and $M_2$. This is the matroid whose ground set $E = E_1 \sqcup E_2$ is the disjoint union of a copy of the ground sets $E_1, E_2$ for $M_1, M_2$, and whose bases are

$$\mathcal{B}(M_1 \oplus M_2) := \{B_1 \sqcup B_2 : B_i \in \mathcal{B}(M_i) \text{ for } i = 1, 2\}.$$

Lastly, say that two matroids $M_1, M_2$ are *isomorphic* if there is a bijection of their ground sets $E_1 \xrightarrow{\varphi} E_2$ having the property that $\varphi\mathcal{B}(M_1) = \mathcal{B}(M_2)$.

Now one can define the matroid-minor Hopf algebra, originally introduced by Schmitt [191, §15], and studied further by Crapo and Schmitt [41, 42, 43].

**Definition 7.4.7.** Let $\mathcal{M}$ have $\mathbf{k}$-basis elements $[M]$ indexed by isomorphism classes of matroids. Define the multiplication via

$$[M_1] \cdot [M_2] := [M_1 \oplus M_2],$$

so that the class $[\varnothing]$ of the *empty matroid* $\varnothing$ having empty ground set gives a unit. Define the comultiplication for $M$ a matroid on ground set $E$ via

$$\Delta[M] := \sum_{A \subset E} [M|_A] \otimes [M/A],$$

and a counit

$$\epsilon[M] := \begin{cases} 1, & \text{if } M = \varnothing; \\ 0, & \text{otherwise.} \end{cases}$$

**Proposition 7.4.8.** *The above maps endow $\mathcal{M}$ with the structure of a connected graded finite type Hopf algebra over $\mathbf{k}$, which is commutative.*

*Proof.* Checking the unit and counit conditions are straightforward. Associativity and commutativity of the multiplication follow because the direct sum operation $\oplus$ for matroids is associative and commutative up to isomorphism. Coassociativity follows because for a matroid $M$ on ground set $E$, one has the following equality between the two candidates for $\Delta^{(2)}[M]$:

$$\begin{aligned} &\sum_{\varnothing \subset A_1 \subset A_2 \subset E} [M|_{A_1}] \otimes [(M|_{A_2})/A_1] \otimes [M/A_2] \\ &= \sum_{\varnothing \subset A_1 \subset A_2 \subset E} [M|_{A_1}] \otimes [(M/A_1)|_{A_2 \setminus A_1}] \otimes [M/A_2] \end{aligned}$$

due to the matroid isomorphism $(M|_{A_2})/A_1 \cong (M/A_1)|_{A_2 \setminus A_1}$. Commutativity of the bialgebra diagram in (1.3.4) amounts to the fact that for a pair of matroids $M_1, M_2$ and subsets $A_1, A_2$ of their (disjoint) ground sets

$E_1, E_2$, one has isomorphisms

$$M_1|_{A_1} \oplus M_2|_{A_2} \cong (M_1 \oplus M_2)\,|_{A_1 \sqcup A_2},$$
$$M_1/A_1 \oplus M_2/A_2 \cong (M_1 \oplus M_2)\,/(A_1 \sqcup A_2).$$

Letting $\mathcal{M}_n$ be the $\mathbf{k}$-span of $[M]$ for matroids whose ground set $E$ has cardinality $|E| = n$, one can then easily check that $\mathcal{M}$ becomes a bialgebra which is graded, connected, and of finite type, hence also a Hopf algebra by Proposition 1.4.16. □

See [59] for an application of $\mathcal{M}$ (and the operator $\exp^\star$ from Section 1.7) to proving the *Tutte recipe theorem*, a "universal" property of the Tutte polynomial of a matroid.

7.4.2. *A quasisymmetric function for matroids.*

**Definition 7.4.9.** Define a character $\mathcal{M} \xrightarrow{\zeta} \mathbf{k}$ by

$$\zeta[M] = \begin{cases} 1, & \text{if } M \text{ has only one basis;} \\ 0, & \text{otherwise.} \end{cases}$$

It is easily checked that this is a character, that is, an algebra morphism $\mathcal{M} \xrightarrow{\zeta} \mathbf{k}$. Note that if $M$ has only one basis, say $\mathcal{B}(M) = \{B\}$, then $B := \operatorname{coloops}(M)$ is the set of coloops of $M$, and $E \setminus B = \operatorname{loops}(M)$ is the set of loops of $M$. Equivalently, $M = \bigoplus_{e \in E} M|_{\{e\}}$ is the direct sum of matroids each having one element, each a coloop or loop.

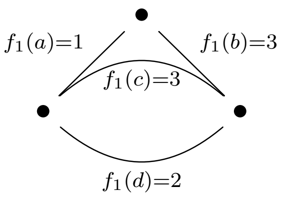
Define $\Psi[M]$ for a matroid $M$ to be the image of $[M]$ under the map $\mathcal{M} \xrightarrow{\Psi} \mathrm{QSym}$ induced via Theorem 7.1.3 from the above character $\zeta$.

It turns out that $\Psi[M]$ is intimately related with greedy algorithms and finding minimum cost bases. A fundamental property of matroids (and one that characterizes them, in fact; see [164, §1.8]) is that no matter how one assigns costs $f : E \to \mathbb{R}$ to the elements of $E$, the following *greedy algorithm* (generalizing *Kruskal's algorithm* for finding minimum cost spanning trees) always succeeds in finding one basis $B$ in $\mathcal{B}(M)$ achieving the minimum *total cost* $f(B) := \sum_{b \in B} f(b)$:

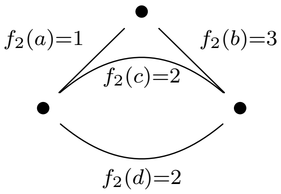
**Algorithm 7.4.10.** Start with the empty subset $I_0 = \varnothing$ of $E$. For $j = 1, 2, \ldots, r$, having already defined the set $I_{j-1}$, let $e$ be the element of $E \setminus I_{j-1}$ having the lowest cost $f(e)$ among all those for which $I_{j-1} \cup \{e\}$ is *independent*, that is, still a subset of at least one basis $B$ in $\mathcal{B}(M)$. Then define $I_j := I_{j-1} \cup \{e\}$. Repeat this until $j = r$, and $B = I_r$ will be among the bases that achieve the minimum cost.

**Definition 7.4.11.** Say that a cost function $f : E \to \{1, 2, \ldots\}$ is $M$-*generic* if there is a *unique* basis $B$ in $\mathcal{B}(M)$ achieving the minimum cost $f(B)$.

**Example 7.4.12.** For the graphic matroid $M$ of Example 7.4.3, this cost function $f_1 : E \to \{1, 2, \ldots\}$



is $M$-generic, as it minimizes uniquely on the basis $\{a, d\}$, whereas this cost function $f_2 : E \to \{1, 2, \ldots\}$



is *not* $M$-generic, as it achieves its minimum value on the two bases $\{a, c\}$, $\{a, d\}$.

**Proposition 7.4.13.** *For a matroid $M$ on ground set $E$, one has this expansion*[362]

$$\Psi[M] = \sum_{\substack{M\text{-generic} \\ f:E\to\{1,2,\ldots\}}} \mathbf{x}_f$$

*where* $\mathbf{x}_f := \prod_{e\in E} x_{f(e)}$. *In particular, for $m \geq 0$, its specialization* $\mathrm{ps}^1$ *from Definition 7.1.6 has this interpretation:*

$$\mathrm{ps}^1\Psi[M](m) = |\{M\text{-generic } f : E \to \{1, 2, \ldots, m\}\}|.$$

*Proof.* The iterated coproduct $\mathcal{M} \overset{\Delta^{(\ell-1)}}{\longrightarrow} \mathcal{M}^{\otimes\ell}$ sends

$$[M] \longmapsto \sum [M|_{A_1}] \otimes [(M|_{A_2})/A_1] \otimes \cdots \otimes [(M|_{A_\ell})/A_{\ell-1}]$$

where the sum is over flags of nested subsets

$$\varnothing = A_0 \subset A_1 \subset \cdots \subset A_{\ell-1} \subset A_\ell = E. \tag{7.4.3}$$

The map $\zeta^{\otimes\ell}$ sends each summand to 1 or 0, depending upon whether each $(M|_{A_j})/A_{j-1}$ has a unique basis or not. Thus formula (7.1.3) shows that the coefficient $\zeta_\alpha$ of $x_{i_1}^{\alpha_1} \cdots x_{i_\ell}^{\alpha_\ell}$ in $\Psi[M]$ counts the flags of subsets in (7.4.3) for which $|A_j \setminus A_{j-1}| = \alpha_j$ and $(M|_{A_j})/A_{j-1}$ has a unique basis, for each $j$.

Given a flag as in (7.4.3), associate the cost function $f : E \to \{1, 2, \ldots\}$ whose value on each element of $A_j \setminus A_{j-1}$ is $i_j$; conversely, given any cost function $f$, say whose distinct values are $i_1 < \cdots < i_\ell$, one associates the flag having $A_j \setminus A_{j-1} = f^{-1}(i_j)$ for each $j$.

Now, apply the greedy algorithm (Algorithm 7.4.10) to find a minimum-cost basis of $M$ for such a cost function $f$. At each step of the greedy algorithm, one new element is added to the independent set; these elements

[362] In fact, this expansion was the original definition of $\Psi[M]$ in [21, Defn. 1.1].

weakly increase in cost as the algorithm progresses[363]. Thus, the algorithm first adds some elements of cost $i_1$, then adds some elements of cost $i_2$, then adds some elements of cost $i_3$, and so on. We can therefore subdivide the execution of the algorithm into phases $1, 2, \ldots, \ell$, where each phase consists of some finite number of steps, such that all elements added in phase $k$ have cost $i_k$. (A phase may be empty.) For each $k \in \{1, 2, \ldots, \ell\}$, we let $\beta_k$ be the number of steps in phase $k$; in other words, $\beta_k$ is the number of elements of elements of cost $i_k$ added during the algorithm.

We will prove below, using induction on $s = 0, 1, 2, \ldots, \ell$ the following **claim**: After having completed phases $1, 2, \ldots, s$ in the greedy algorithm (Algorithm 7.4.10), there is *a unique choice* for the independent set produced thus far, namely

$$I_{\beta_1+\beta_2+\cdots+\beta_s} = \bigsqcup_{j=1}^{s} \operatorname{coloops}((M|_{A_j})/A_{j-1}), \tag{7.4.4}$$

if and only if each of the matroids $(M|_{A_j})/A_{j-1}$ for $j = 1, 2, \ldots, s$ *has a unique basis.*

The case $s = \ell$ in this claim would show what we want, namely that $f$ is $M$-generic, minimizing uniquely on the basis shown in (7.4.4) with $s = \ell$, if and only if each $(M|_{A_j})/A_{j-1}$ has a unique basis.

The assertion of the claim is trivially true for $s = 0$. In the inductive step, one may assume that

- the independent set $I_{\beta_1+\beta_2+\cdots+\beta_{s-1}}$ takes the form in (7.4.4), replacing $s$ by $s - 1$,
- it is the unique $f$-minimizing basis for $M|_{A_{s-1}}$, and
- $(M|_{A_j})/A_{j-1}$ has a unique basis for $j = 1, 2, \ldots, s - 1$.

Since $A_{s-1}$ exactly consists of all of the elements $e$ of $E$ whose costs $f(e)$ lie in the range $\{i_1, i_2, \ldots, i_{s-1}\}$, in phase $s$ the algorithm will work in the quotient matroid $M/A_{s-1}$ and attempt to augment $I_{\beta_1+\beta_2+\cdots+\beta_{s-1}}$ using the next-cheapest elements, namely the elements of $A_s \setminus A_{s-1}$, which all have cost $f$ equal to $i_s$. Thus the algorithm will have no choices about how to do this augmentation if and only if $(M|_{A_s})/A_{s-1}$ has a unique basis, namely its set of coloops, in which case the algorithm will choose to add all of these coloops, giving $I_{\beta_1+\beta_2+\cdots+\beta_s}$ as described in (7.4.4). This completes the induction.

The last assertion follows from Proposition 7.1.7. □

**Example 7.4.14.** If $M$ has one basis then every function $f : E \to \{1, 2, \ldots\}$ is $M$-generic, and

$$\Psi[M] = \sum_{f:E\to\{1,2,\ldots\}} \mathbf{x}_f = (x_1 + x_2 + \cdots)^{|E|} = M_{(1)}^{|E|}.$$

**Example 7.4.15.** Let $U_{r,n}$ denote the *uniform matroid* of rank $r$ on $n$ elements $E$, having $\mathcal{B}(U_{r,n})$ equal to all of the $r$-element subsets of $E$.

[363] *Proof.* Let $e$ be the element added at step $i$, and let $e'$ be the element added at step $i+1$. We want to show that $f(e) \leq f(e')$. But the element $e'$ could already have been added at step $i$. Since it wasn't, we thus conclude that the element $e$ that was added instead must have been cheaper or equally expensive. In other words, $f(e) \leq f(e')$, qed.

As $U_{1,2}$ has $E = \{1, 2\}$ and $\mathcal{B} = \{\{1\}, \{2\}\}$, genericity means $f(1) \neq f(2)$, so

$$\Psi[U_{1,2}] = \sum_{\substack{(f(1),f(2)):\\ f(1)\neq f(2)}} x_{f(1)}x_{f(2)} = x_1x_2 + x_2x_1 + x_1x_3 + x_3x_1 + \cdots = 2M_{(1,1)}.$$

Similarly $U_{1,3}$ has $E = \{1, 2, 3\}$ with $\mathcal{B} = \{\{1\}, \{2\}, \{3\}\}$, and genericity means either that $f(1), f(2), f(3)$ are all distinct, or that two of them are the same and the third is smaller. This shows

$$\begin{aligned}\Psi[U_{1,3}] &= 3\sum_{i<j} x_ix_j^2 + 6\sum_{i<j<k} x_ix_jx_k\\ &= 3M_{(1,2)} + 6M_{(1,1,1)};\\ \mathrm{ps}^1\Psi[U_{1,3}](m) &= 3\binom{m}{2} + 6\binom{m}{3} = \frac{m(m-1)(2m-1)}{2}.\end{aligned}$$

One can similarly analyze $U_{2,3}$ and check that

$$\begin{aligned}\Psi[U_{2,3}] &= 3M_{(2,1)} + 6M_{(1,1,1)};\\ \mathrm{ps}^1\Psi[U_{2,3}](m) &= 3\binom{m}{2} + 6\binom{m}{3} = \frac{m(m-1)(2m-1)}{2}.\end{aligned}$$

These last examples illustrate the behavior of $\Psi$ under the duality operation on matroids.

**Definition 7.4.16.** Given a matroid $M$ of rank $r$ on ground set $E$, its *dual* or *orthogonal matroid* $M^\perp$ is a matroid of rank $|E|-r$ on the same ground set $E$, having

$$\mathcal{B}(M^\perp) := \{E \setminus B\}_{B\in\mathcal{B}(M)}.$$

See [164, Theorem 2.1.1] or [34, Section 4] for a proof of the fact that this is well-defined (i.e., that the collection $\{E \setminus B\}_{B\in\mathcal{B}(M)}$ really satisfies the exchange property). Here are a few examples of dual matroids.

**Example 7.4.17.** The dual of a uniform matroid is another uniform matroid:

$$U_{r,n}^\perp = U_{n-r,n}.$$

**Example 7.4.18.** If $M$ is matroid of rank $r$ represented by family of vectors $\{e_1, \ldots, e_n\}$ in a vector space over some field $\mathbf{k}$, one can find a family of vectors $\{e_1^\perp, \ldots, e_n^\perp\}$ that represent $M^\perp$ in the following way. Pick a basis for the span of the vectors $\{e_i\}_{i=1}^n$, and create a matrix $A$ in $\mathbf{k}^{r\times n}$ whose columns express the $e_i$ in terms of this basis. Then pick any matrix $A^\perp$ whose row space is the null space of $A$, and one finds that the columns $\{e_i^\perp\}_{i=1}^n$ of $A^\perp$ represent $M^\perp$. See Oxley [164, §2.2].

**Example 7.4.19.** Let $G = (V, E)$ be a graph embedded in the plane with edge set $E$, giving rise to a graphic matroid $M$ on ground set $E$. Let $G^\perp$ be a planar dual of $G$, so that, in particular, for each edge $e$ in $E$, the graph $G^\perp$ has one edge $e^\perp$, crossing $e$ transversely. Then the graphic matroid of $G^\perp$ is $M^\perp$. See Oxley [164, §2.3].

**Proposition 7.4.20.** *If* $\Psi[M] = \sum_\alpha c_\alpha M_\alpha$ *then* $\Psi[M^\perp] = \sum_\alpha c_\alpha M_{\mathrm{rev}(\alpha)}$. *Consequently,* $\mathrm{ps}^1\Psi[M](m) = \mathrm{ps}^1\Psi[M^\perp](m)$.

*Proof.* First, let us prove that

$$\text{if } \Psi[M] = \sum_{\alpha} c_\alpha M_\alpha \text{ then } \Psi[M^\perp] = \sum_{\alpha} c_\alpha M_{\operatorname{rev}(\alpha)}.$$

In other words, let us show that for any given composition $\alpha$, the coefficient of $M_\alpha$ in $\Psi[M]$ (when $\Psi[M]$ is expanded in the basis $(M_\beta)_{\beta\in\mathrm{Comp}}$ of QSym) equals the coefficient of $M_{\operatorname{rev}(\alpha)}$ in $\Psi[M^\perp]$. This amounts to showing that for any composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, the cardinality of the set of $M$-generic $f$ having $\mathbf{x}_f = \mathbf{x}^\alpha$ is the same as the cardinality of the set of $M^\perp$-generic $f^\perp$ having $\mathbf{x}_{f^\perp} = \mathbf{x}^{\operatorname{rev}(\alpha)}$. We claim that the map $f \longmapsto f^\perp$ in which $f^\perp(e) = \ell + 1 - f(e)$ gives a bijection between these sets. To see this, note that any basis $B$ of $M$ satisfies

$$f(B) + f(E \setminus B) = \sum_{e\in E} f(e), \tag{7.4.5}$$

$$f(E \setminus B) + f^\perp(E \setminus B) = (\ell + 1)(|E| - r), \tag{7.4.6}$$

where $r$ denotes the rank of $M$. Thus $B$ is $f$-minimizing if and only if $E \setminus B$ is $f$-maximizing (by (7.4.5)) if and only if $E \setminus B$ is $f^\perp$-minimizing (by (7.4.6)). Consequently $f$ is $M$-generic if and only if $f^\perp$ is $M^\perp$-generic.

The last assertion follows, for example, from the calculation in Proposition 7.1.7(i) that $\mathrm{ps}^1(M_\alpha)(m) = \binom{m}{\ell(\alpha)}$ together with the fact that $\ell(\operatorname{rev}(\alpha)) = \ell(\alpha)$. □

Just as (7.3.5) showed that Stanley's chromatic symmetric function of a graph has an expansion as a sum of $P$-partition enumerators for certain strictly labelled posets[364] $P$, the same holds for $\Psi[M]$.

**Definition 7.4.21.** Given a matroid $M$ on ground set $E$, and a basis $B$ in $\mathcal{B}(M)$, define the *base-cobase poset* $P_B$ to have $b < b'$ whenever $b$ lies in $B$ and $b'$ lies in $E \setminus B$ and $(B \setminus \{b\}) \cup \{b'\}$ is in $\mathcal{B}(M)$.

**Proposition 7.4.22.** *For any matroid $M$, one has*

$$\Psi[M] = \sum_{B\in\mathcal{B}(M)} F_{(P_B,\mathrm{strict})}(\mathbf{x})$$

*where $F_{(P,\,\mathrm{strict})}(\mathbf{x})$ for a poset $P$ means the $P$-partition enumerator for any strict labelling of $P$, i.e. a labelling such that the $P$-partitions satisfy $f(i) < f(j)$ whenever $i <_P j$.*

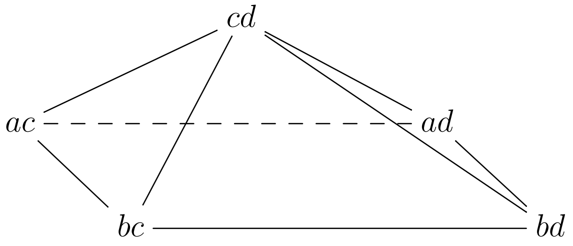
*In particular, $\Psi[M]$ expands nonnegatively in the $\{L_\alpha\}$ basis.*

*Proof.* A basic result about matroids, due to Edmonds [62], describes the *edges* in the *matroid base polytope* which is the convex hull of all vectors $\{\sum_{b\in B} \epsilon_b\}_{B\in\mathcal{B}(M)}$ inside $\mathbb{R}^E$ with standard basis $\{\epsilon_e\}_{e\in E}$. He shows that all such edges connect two bases $B, B'$ that differ by a single *basis exchange*, that is, $B' = (B \setminus \{b\}) \cup \{b'\}$ for some $b$ in $B$ and $b'$ in $E \setminus B$.

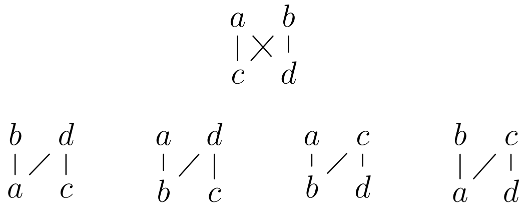
Polyhedral theory then says that a cost function $f$ on $E$ will minimize uniquely at $B$ if and only if one has a strict increase $f(B) < f(B')$ along each such edge $B \to B'$ emanating from $B$, that is, if and only if $f(b) < f(b')$ whenever $b <_{P_B} b'$ in the base-cobase poset $P_B$, that is, $f$ lies in $\mathcal{A}(P_B, \mathrm{strict})$. □

[364] A labelled poset $P$ is said to be *strictly labelled* if every two elements $i$ and $j$ of $P$ satisfying $i <_P j$ satisfy $i >_{\mathbb{Z}} j$.

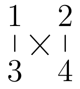
**Example 7.4.23.** The graphic matroid from Example 7.4.3 has this matroid base polytope, with the bases $B$ in $\mathcal{B}(M)$ labelling the vertices:



The base-cobase posets $P_B$ for its five vertices $B$ are as follows:



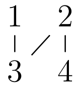
One can label the first of these five strictly as



and compute its strict $P$-partition enumerator from the linear extensions $\{3412, 3421, 4312, 4321\}$ as

$$L_{(2,2)} + L_{(2,1,1)} + L_{(1,1,2)} + L_{(1,1,1,1)},$$

while any of the last four can be labelled strictly as



and they each have an extra linear extension 3142 giving their strict $P$-partition enumerators as

$$L_{(2,2)} + L_{(2,1,1)} + L_{(1,1,2)} + L_{(1,1,1,1)} + L_{(1,2,1)}.$$

Hence one has

$$\Psi[M] = 5L_{(2,2)} + 5L_{(1,1,2)} + 4L_{(1,2,1)} + 5L_{(2,1,1)} + 5L_{(1,1,1,1)}.$$

As $M$ is a graphic matroid for a self-dual planar graph, one has a matroid isomorphism $M \cong M^{\perp}$ (see Example 7.4.19), reflected in the fact that $\Psi[M]$ is invariant under the symmetry swapping $M_\alpha \leftrightarrow M_{\mathrm{rev}(\alpha)}$ (and simultaneously swapping $L_\alpha \leftrightarrow L_{\mathrm{rev}(\alpha)}$).

This $P$-partition expansion for $\Psi[M]$ also allows us to identify its image under the antipode of QSym.

**Proposition 7.4.24.** *For a matroid $M$ on ground set $E$, one has*

$$S(\Psi[M]) = (-1)^{|E|} \sum_{f: E \to \{1,2,\ldots\}} |\{f\text{-maximizing bases } B\}| \cdot \mathbf{x}_f$$

*and*

$$\mathrm{ps}^1 \Psi[M](-m) = (-1)^{|E|} \sum_{f: E \to \{1,2,\ldots,m\}} |\{f\text{-maximizing bases } B\}|.$$

*In particular, the expected number of $f$-maximizing bases among all cost functions $f : E \to \{1, 2, \ldots, m\}$ is $(-m)^{-|E|}\mathrm{ps}^1\Psi[M](-m)$.*

*Proof.* Corollary 5.2.20 implies

$$S(\Psi[M]) = \sum_{B\in\mathcal{B}(M)} S(F_{(P_B,\mathrm{strict})}(\mathbf{x})) = (-1)^{|E|} \sum_{B\in\mathcal{B}(M)} F_{(P_B^{\mathrm{opp}},\mathrm{natural})}(\mathbf{x}),$$

where $F_{(P,\mathrm{natural})}(\mathbf{x})$ is the enumerator for $P$-partitions in which $P$ has been *naturally* labelled, so that they satisfy $f(i) \leq f(j)$ whenever $i <_P j$. When $P = P_B^{\mathrm{opp}}$, this is exactly the condition for $f$ to achieve its maximum value at $f(B)$ (possibly not uniquely), that is, for $f$ to lie in the *closed* normal cone to the vertex indexed by $B$ in the matroid base polytope; compare this with the discussion in the proof of Proposition 7.4.22. Thus one has

$$S(\Psi[M]) = (-1)^{|E|} \sum_{\substack{(B,f):\\ B\in\mathcal{B}(M)\\ f \text{ maximizing at } B}} \mathbf{x}_f,$$

which agrees with the statement of the proposition, after reversing the order of the summation.

The rest follows from Proposition 7.1.7. □

**Example 7.4.25.** We saw in Example 7.4.23 that the matroid $M$ from Example 7.4.3 has

$$\Psi[M] = 5L_{(2,2)} + 5L_{(1,1,2)} + 4L_{(1,2,1)} + 5L_{(2,1,1)} + 5L_{(1,1,1,1)},$$

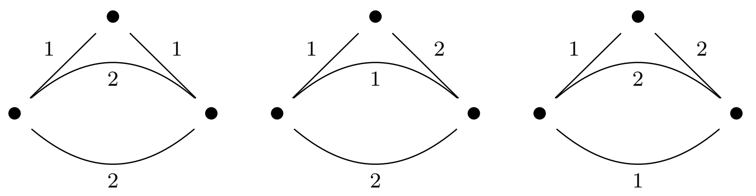
and therefore will have

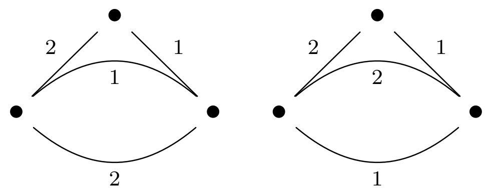
$$\begin{aligned}\mathrm{ps}^1\Psi[M](m) &= 5\binom{m-2+4}{4} + (5+4+5)\binom{m-3+4}{4} + 5\binom{m-4+4}{4}\\ &= \frac{m(m-1)(2m^2-2m+1)}{2}\end{aligned}$$

using $\mathrm{ps}^1(L_\alpha)(m) = \binom{m-\ell+|\alpha|}{|\alpha|}$ from Proposition 7.1.7 (i). Let us first do a reality-check on a few of its values with $m \geq 0$ using Proposition 7.4.13, and for negative $m$ using Proposition 7.4.24:

| $m$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|
| $\mathrm{ps}^1\Psi[M](m)$ | 5 | 0 | 0 | 5 |

When $m = 0$, interpreting the set of cost functions $f : E \to \{1, 2, \ldots, m\}$ as being empty explains why the value shown is 0. When $m = 1$, there is only one function $f : E \to \{1\}$, and it is not $M$-generic; any of the 5 bases in $\mathcal{B}(M)$ will minimize $f(B)$, explaining both why the value for $m = 1$ is 0, but also explaining the value of 5 for $m = -1$. The value of 5 for $m = 2$ counts these $M$-generic cost functions $f : E \to \{1, 2\}$:





Lastly, Proposition 7.4.24 predicts the expected number of $f$-minimizing bases for $f : E \to \{1, 2, \ldots, m\}$ as

$$\begin{aligned}(-m)^{-|E|}\mathrm{ps}^1\Psi[M](-m) &= (-m)^{-4}\frac{m(m+1)(2m^2+2m+1)}{2} \\ &= \frac{(m+1)(2m^2+2m+1)}{2m^3},\end{aligned}$$

whose limit as $m \to \infty$ is 1, consistent with the notion that "most" cost functions should be generic with respect to the bases of $M$, and maximize/minimize on a unique basis.

*Remark* 7.4.26. It is not coincidental that there is a similarity of results for Stanley's chromatic symmetric function of a graph $\Psi[G]$ and for the matroid quasisymmetric function $\Psi[M]$, such as the $P$-partition expansions (7.3.5) versus Proposition 7.4.22, and the reciprocity results Proposition 7.3.23 versus Proposition 7.4.24. It was noted in [21, §9] that one can associate a similar quasisymmetric function invariant to any *generalized permutohedra* in the sense of Postnikov [173]. Furthermore, recent work of Ardila and Aguiar [3] has shown that there is a Hopf algebra of such generalized permutohedra, arising from a *Hopf monoid* in the sense of Aguiar and Mahajan [6]. This Hopf algebra generalizes the chromatic Hopf algebra of graphs[365] and the matroid-minor Hopf algebra, and its quasisymmetric function invariant derives as usual from Theorem 7.1.3. Their work [3] also provides a generalization of the chromatic Hopf algebra antipode formula of Humpert and Martin [103] discussed in Remark 7.3.4 above.

[365] Aguiar and Ardila actually work with a larger Hopf algebra of graphs. Namely, their concept of graphs allows parallel edges, and it also allows "half-edges", which have only one endpoint. If $G = (V, E)$ is such a graph (where $E$ is the set of its edges and its half-edges), and if $V'$ is a subset of $V$, then they define $G/_{V'}$ to be the graph on vertex set $V'$ obtained from $G$ by

- removing all vertices that are not in $V'$,
- removing all edges that have no endpoint in $V'$, and all half-edges that have no endpoint in $V'$, and
- replacing all edges that have only one endpoint in $V'$ by half-edges.

(This is to be contrasted with the induced subgraph $G\mid_{V'}$, which is constructed in the same way but with the edges that have only one endpoint in $V'$ getting removed as well.) The comultiplication they define on the Hopf algebra of such graphs sends the isomorphism class $[G]$ of a graph $G = (V, E)$ to $\sum_{(V_1,V_2): V_1 \sqcup V_2 = V} [G\mid_{V_1}] \otimes [G/_{V_2}]$. This is no longer a cocommutative Hopf algebra; our Hopf algebra $\mathcal{G}$ is a quotient of it. In [3, Corollary 13.10], Ardila and Aguiar compute the antipode of the Hopf monoid of such graphs; this immediately leads to a formula for the antipode of the corresponding Hopf algebra, because what they call the Fock functor $\overline{\mathcal{K}}$ preserves antipodes [3, Theorem 2.18].

## 8. The Malvenuto-Reutenauer Hopf algebra of permutations

Like so many Hopf algebras we have seen, the *Malvenuto-Reutenauer Hopf algebra* FQSym can be thought of fruitfully in more than one way. One is that it gives a natural noncommutative lift of the quasisymmetric $P$-partition enumerators and the fundamental basis $\{L_\alpha\}$ of QSym, rendering their product and coproduct formulas even more natural.

### 8.1. Definition and Hopf structure.

**Definition 8.1.1.** We shall regard permutations as words (over the alphabet $\{1,2,3,\ldots\}$) by identifying every permutation $\pi \in \mathfrak{S}_n$ with the word $(\pi(1), \pi(2), \ldots, \pi(n))$.

Define $\mathrm{FQSym} = \bigoplus_{n\geq 0} \mathrm{FQSym}_n$ to be a graded $\mathbf{k}$-module in which $\mathrm{FQSym}_n$ has $\mathbf{k}$-basis $\{F_w\}_{w\in\mathfrak{S}_n}$ indexed by the permutations $w = (w_1, \ldots, w_n)$ in $\mathfrak{S}_n$.

We first attempt to lift the product and coproduct formulas (5.2.6), (5.2.5) in the $\{L_\alpha\}$ basis of QSym. We attempt to define a product for $u \in \mathfrak{S}_k$ and $v \in \mathfrak{S}_\ell$ as follows[366]:

$$F_u F_v := \sum_{w \in u \sqcup\!\sqcup v[k]} F_w, \tag{8.1.1}$$

where for any word $v = (v_1, \ldots, v_\ell)$ we set $v[k] := (k+v_1, \ldots, k+v_\ell)$. Note that the multiset $u \sqcup\!\sqcup v[k]$ is an actual set in this situation (i.e., has each element appear only once) and is a subset of $\mathfrak{S}_{k+\ell}$.

The coproduct will be defined using the notation of standardization of $\mathrm{std}(w)$ a word $w$ in some linearly ordered alphabet (see Definition 5.3.3).

**Example 8.1.2.** Considering words in the Roman alphabet $a < b < c < \cdots$, we have

$$\begin{array}{l} \mathrm{std}(b \quad a \quad c \quad c \quad b \quad a \quad a \quad b \quad a \quad c \quad b) \\ = (5 \quad 1 \quad 9 \quad 10 \quad 6 \quad 2 \quad 3 \quad 7 \quad 4 \quad 11 \quad 8). \end{array}$$

Using this, define for $w = (w_1, \ldots, w_n)$ in $\mathfrak{S}_n$ the element $\Delta F_w \in \mathrm{FQSym} \otimes \mathrm{FQSym}$ by

$$\Delta F_w := \sum_{k=0}^{n} F_{\mathrm{std}(w_1, w_2, \ldots, w_k)} \otimes F_{\mathrm{std}(w_{k+1}, w_{k+2}, \ldots, w_n)}. \tag{8.1.2}$$

It is possible to check directly that the maps defined in (8.1.1) and (8.1.2) endow FQSym with the structure of a connected graded finite type Hopf algebra; see Hazewinkel, Gubareni, Kirichenko [93, Thm. 7.1.8]. However in justifying this here, we will follow the approach of Duchamp, Hivert and Thibon [58, §3], which exhibits FQSym as a subalgebra of a larger ring of (noncommutative) power series of bounded degree in a totally ordered alphabet.

**Definition 8.1.3.** Given a totally ordered set $I$, create a totally ordered variable set $\{X_i\}_{i\in I}$, and the ring $R\langle\{X_i\}_{i\in I}\rangle$ of *noncommutative power series of bounded degree* in this alphabet[367]. Many times, we will use a variable set $\mathbf{X} := (X_1 < X_2 < \cdots)$, and call the ring $R\langle\mathbf{X}\rangle$.

[366] Recall that we regard permutations as words.

[367] Let us recall the definition of $R\langle\{X_i\}_{i\in I}\rangle$.

We first identify the algebra structure for FQSym as the subalgebra of finite type within $R\langle\{X_i\}_{i\in I}\rangle$ spanned by the elements

$$F_w = F_w(\{X_i\}_{i\in I}) := \sum_{\substack{\mathbf{i}=(i_1,\ldots,i_n):\\ \operatorname{std}(\mathbf{i})=w^{-1}}} \mathbf{X}_{\mathbf{i}}, \tag{8.1.3}$$

where $\mathbf{X}_{\mathbf{i}} := X_{i_1}\cdots X_{i_n}$, as $w$ ranges over $\bigcup_{n\geq 0}\mathfrak{S}_n$ .

**Example 8.1.4.** For the alphabet $\mathbf{X} = (X_1 < X_2 < \cdots)$, in $R\langle\mathbf{X}\rangle$ one has

$$\begin{aligned}
F_1 &= \sum_{1\leq i} X_i = X_1 + X_2 + \cdots ,\\
F_{12} &= \sum_{1\leq i\leq j} X_iX_j = X_1^2 + X_2^2 + \cdots + X_1X_2 + X_1X_3 + X_2X_3 + X_1X_4 + \cdots ,\\
F_{21} &= \sum_{1\leq i<j} X_jX_i = X_2X_1 + X_3X_1 + X_3X_2 + X_4X_1 + \cdots ,\\
F_{312} &= \sum_{\mathbf{i}:\operatorname{std}(\mathbf{i})=231} \mathbf{X}_{\mathbf{i}} = \sum_{1\leq i<j\leq k} X_jX_kX_i\\
&= X_2^2X_1 + X_3^2X_1 + X_3^2X_2 + \cdots + X_2X_3X_1 + X_2X_4X_1 + \cdots .
\end{aligned}$$

**Proposition 8.1.5.** *For any totally ordered infinite set $I$, the elements $\{F_w\}$ as $w$ ranges over $\bigcup_{n\geq 0}\mathfrak{S}_n$ form a $\mathbf{k}$-basis for a subalgebra* FQSym$(\{X_i\}_{i\in I})$ *of $R\langle\mathbf{X}\rangle$, which is connected graded and of finite type, having multiplication defined $\mathbf{k}$-linearly by* (8.1.1).

*Consequently all such algebras are isomorphic to a single algebra* FQSym, *having basis $\{F_w\}$ and multiplication given by the rule* (8.1.1), *with the isomorphism mapping $F_w \longmapsto F_w(\{X_i\}_{i\in I})$.*

Let $N$ denote the free monoid on the alphabet $\{X_i\}_{i\in I}$; it consists of words $X_{i_1}X_{i_2}\cdots X_{i_k}$. We define a topological $\mathbf{k}$-module $\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ to be the Cartesian product $\mathbf{k}^N$ (equipped with the product topology), but we identify its element $(\delta_{w,u})_{u\in N}$ with the word $w$ for every $w\in N$. Thus, every element $(\lambda_w)_{w\in N}\in\mathbf{k}^N = \mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ can be rewritten as the convergent sum $\sum_{w\in N}\lambda_w w$. We call $\lambda_w$ the *coefficient of* $w$ in this element (or the *coefficient of this element before* $w$). The elements of $\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ will be referred to as *noncommutative power series*. We define a multiplication on $\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ by the formula

$$\left(\sum_{w\in N}\lambda_w w\right)\left(\sum_{w\in N}\mu_w w\right) = \sum_{w\in N}\left(\sum_{(u,v)\in N^2;\ w=uv}\lambda_u\mu_v\right)w.$$

(This is well-defined thanks to the fact that, for each $w\in N$, there are only finitely many $(u,v)\in N^2$ satisfying $w=uv$.) Thus, $\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ becomes a $\mathbf{k}$-algebra with unity 1 (the empty word). (It is similar to the monoid algebra $\mathbf{k}N$ of $N$ over $\mathbf{k}$, with the only difference that infinite sums are allowed.)

Now, we define $R\langle\{X_i\}_{i\in I}\rangle$ to be the $\mathbf{k}$-subalgebra of $\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ consisting of all noncommutative power series $\sum_{w\in N}\lambda_w w\in\mathbf{k}\langle\langle\{X_i\}_{i\in I}\rangle\rangle$ *of bounded degree* (i.e., such that all words $w\in N$ of sufficiently high length satisfy $\lambda_w = 0$).

For example,

$$\begin{aligned}
F_1F_{21} &= (X_1+X_2+X_3+\cdots)(X_2X_1+X_3X_1+X_3X_2+X_4X_1+\cdots)\\
&= X_1\cdot X_3X_2 + X_1\cdot X_4X_2+\cdots\\
&\qquad + X_1\cdot X_2X_1 + X_2\cdot X_3X_2 + X_2\cdot X_4X_2+\cdots\\
&\qquad + X_2\cdot X_3X_1 + X_2\cdot X_4X_1+\cdots\\
&\qquad + X_2\cdot X_2X_1 + X_3\cdot X_3X_1 + X_3\cdot X_3X_2+\cdots\\
&\qquad + X_3\cdot X_2X_1 + X_4\cdot X_2X_1+\cdots\\
&= \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=132}\mathbf{X_i} + \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=231}\mathbf{X_i} + \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=321}\mathbf{X_i} = F_{132}+F_{312}+F_{321}\\
&= \sum_{w\in 1\,\sqcup\!\sqcup\,32} F_w.
\end{aligned}$$

*Proof of Proposition 8.1.5.* The elements $\{F_w(\{X_i\}_{i\in I})\}$ are linearly independent as they are supported on disjoint monomials, and so form a $\mathbf{k}$-basis for their span. The fact that they multiply via rule (8.1.1) is the equivalence of conditions (i) and (iii) in the following Lemma 8.1.6, from which all the remaining assertions follow. □

**Lemma 8.1.6.** *For a triple of permutations*

$$\begin{aligned}
u &= (u_1,\ldots,u_k) \text{ in } \mathfrak{S}_k,\\
v &= (v_1,\ldots,v_{n-k}) \text{ in } \mathfrak{S}_{n-k},\\
w &= (w_1,\ldots,w_n) \text{ in } \mathfrak{S}_n,
\end{aligned}$$

*the following conditions are equivalent:*

(i) $w^{-1}$ *lies in the set* $u^{-1}\,\sqcup\!\sqcup\, v^{-1}[k]$.

(ii) $u=\mathrm{std}(w_1,\ldots,w_k)$ *and* $v=\mathrm{std}(w_{k+1},\ldots,w_n)$,

(iii) *for some word* $\mathbf{i}=(i_1,\ldots,i_n)$ *with* $\mathrm{std}(\mathbf{i})=w$ *one has* $u=\mathrm{std}(i_1,\ldots,i_k)$ *and* $v=\mathrm{std}(i_{k+1},\ldots,i_n)$.

*Proof.* The implication (ii) ⇒ (iii) is clear since $\mathrm{std}(w)=w$. The reverse implication (iii) ⇒ (ii) is best illustrated by example, e.g. considering Example 8.1.2 as concatenated, with $n=11$ and $k=6$ and $n-k=5$:

$$\begin{array}{rcccccccccccc}
w=\mathrm{std} & (b & a & c & c & b & a & | & a & b & a & c & b)\\
= & (5 & 1 & 9 & 10 & 6 & 2 & | & 3 & 7 & 4 & 11 & 8)
\end{array}$$

$$\begin{array}{rcccccc||rcccccc}
\hline
u=\mathrm{std} & (5 & 1 & 9 & 10 & 6 & 2) & v=\mathrm{std} & (3 & 7 & 4 & 11 & 8)\\
= & (3 & 1 & 5 & 6 & 4 & 2) & = & (1 & 3 & 2 & 5 & 4)\\
=\mathrm{std} & (b & a & c & c & b & a) & =\mathrm{std} & (a & b & a & c & b)
\end{array}$$

The equivalence of (i) and (ii) is a fairly standard consequence of unique parabolic factorization $W=W^JW_J$ where $W=\mathfrak{S}_n$ and $W_J=\mathfrak{S}_k\times\mathfrak{S}_{n-k}$, so that $W^J$ are the minimum-length coset representatives for cosets $xW_J$ (that is, the permutations $x\in\mathfrak{S}_n$ satisfying $x_1<\cdots<x_k$ and $x_{k+1}<\cdots<x_n$). One can uniquely express any $w$ in $W$ as $w=xy$ with $x$ in $W^J$ and $y$ in $W_J$, which here means that $y=u\cdot v[k]=v[k]\cdot u$ for some $u$ in $\mathfrak{S}_k$ and $v$ in $\mathfrak{S}_{n-k}$. Therefore $w=xuv[k]$, if and only if $w^{-1}=u^{-1}v^{-1}[k]x^{-1}$, which means that $w^{-1}$ is the shuffle of the sequences $u^{-1}$ in positions $\{x_1,\ldots,x_k\}$ and $v^{-1}[k]$ in positions $\{x_{k+1},\ldots,x_n\}$. □

**Example 8.1.7.** To illustrate the equivalence of (i) and (ii) and the parabolic factorization in the preceding proof, let $n = 9$ and $k = 5$ with

$$\begin{aligned} w &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \mid & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 1 & 5 & \mid & 8 & 2 & 3 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \mid & 6 & 7 & 8 & 9 \\ 1 & 4 & 5 & 6 & 9 & \mid & 2 & 3 & 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \\ 9 & 6 & 7 & 8 \end{pmatrix} \\ &= x \cdot u \cdot v[k]; \end{aligned}$$

then

$$\begin{aligned} w^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 1 & 5 & 8 & 2 & 3 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \underline{1} & \underline{\underline{6}} & \underline{\underline{7}} & \underline{2} & \underline{3} & \underline{4} & \underline{\underline{8}} & \underline{\underline{9}} & \underline{5} \end{pmatrix} \\ &= u^{-1} \cdot v^{-1}[k] \cdot x^{-1}. \end{aligned}$$

Proposition 8.1.5 yields that FQSym is isomorphic to the $\mathbf{k}$-subalgebra $\operatorname{FQSym}(\mathbf{X})$ of the $\mathbf{k}$-algebra $R\langle \mathbf{X} \rangle$ when $\mathbf{X}$ is the variable set $(X_1 < X_2 < \cdots)$. We identify FQSym with $\operatorname{FQSym}(\mathbf{X})$ along this isomorphism. For any infinite alphabet $\{X_i\}_{i \in I}$ and any $f \in \operatorname{FQSym}$, we denote by $f\left(\{X_i\}_{i \in I}\right)$ the image of $f$ under the algebra isomorphism $\operatorname{FQSym} \to \operatorname{FQSym}\left(\{X_i\}_{i \in I}\right)$ defined in Proposition 8.1.5.

One can now use this to define a coalgebra structure on FQSym. Roughly speaking, one wants to first evaluate an element $f$ in $\operatorname{FQSym} \cong \operatorname{FQSym}(\mathbf{X}) \cong \operatorname{FQSym}(\mathbf{X}, \mathbf{Y})$ as $f(\mathbf{X}, \mathbf{Y})$, using the linearly ordered variable set $(\mathbf{X}, \mathbf{Y}) := (X_1 < X_2 < \cdots < Y_1 < Y_2 < \cdots)$. Then one should take the image of $f(\mathbf{X}, \mathbf{Y})$ after imposing the partial commutativity relations

$$X_i Y_j = Y_j X_i \text{ for every pair } (X_i, Y_j) \in \mathbf{X} \times \mathbf{Y}, \tag{8.1.4}$$

and hope that this image lies in a subalgebra isomorphic to

$$\operatorname{FQSym}(\mathbf{X}) \otimes \operatorname{FQSym}(\mathbf{Y}) \cong \operatorname{FQSym} \otimes \operatorname{FQSym}.$$

We argue this somewhat carefully. Start by considering the canonical monoid epimorphism

$$F\langle \mathbf{X}, \mathbf{Y} \rangle \overset{\rho}{\twoheadrightarrow} M, \tag{8.1.5}$$

where $F\langle \mathbf{X}, \mathbf{Y} \rangle$ denotes the *free monoid* on the alphabet $(\mathbf{X}, \mathbf{Y})$ and $M$ denotes its quotient monoid imposing the partial commutativity relations (8.1.4). Let $\mathbf{k}^M$ denote the $\mathbf{k}$-module of all functions $f : M \to \mathbf{k}$, with pointwise addition and scalar multiplication; similarly define $\mathbf{k}^{F\langle \mathbf{X}, \mathbf{Y} \rangle}$. As both monoids $F\langle \mathbf{X}, \mathbf{Y} \rangle$ and $M$ enjoy the property that an element $m$ has only finitely many factorizations as $m = m_1 m_2$, one can define a convolution algebra structure on both $\mathbf{k}^{F\langle \mathbf{X}, \mathbf{Y} \rangle}$ and $\mathbf{k}^M$ via

$$(f_1 \star f_2)(m) = \sum_{\substack{(m_1, m_2) \in N \times N: \\ m = m_1 m_2}} f_1(m_1) f_2(m_2),$$

where $N$ is respectively $F\langle \mathbf{X}, \mathbf{Y} \rangle$ or $M$. As fibers of the map $\rho$ in (8.1.5) are finite, it induces a map of convolution algebras, which we also call $\rho$:

$$\mathbf{k}^{F\langle \mathbf{X}, \mathbf{Y} \rangle} \overset{\rho}{\twoheadrightarrow} \mathbf{k}^M. \tag{8.1.6}$$

Now recall that $R\langle \mathbf{X}\rangle$ denotes the algebra of noncommutative formal power series in the variable set $\mathbf{X}$, of bounded degree, with coefficients in $\mathbf{k}$. One similarly has the ring $R\langle \mathbf{X},\mathbf{Y}\rangle$, which can be identified with the subalgebra of $\mathbf{k}^{F\langle \mathbf{X},\mathbf{Y}\rangle}$ consisting of the functions $f : F\langle \mathbf{X},\mathbf{Y}\rangle \to \mathbf{k}$ having a bound on the length of the words in their support (the value of $f$ on a word in $(\mathbf{X},\mathbf{Y})$ gives its power series coefficient corresponding to said word). We let $R\langle M\rangle$ denote the analogous subalgebra of $\mathbf{k}^M$; this can be thought of as the algebra of bounded degree "partially commutative power series" in the variable sets $\mathbf{X}$ and $\mathbf{Y}$. Note that $\rho$ restricts to a map

$$R\langle \mathbf{X},\mathbf{Y}\rangle \overset{\rho}{\to} R\langle M\rangle. \tag{8.1.7}$$

Finally, we claim (and see Proposition 8.1.9 below for a proof) that this further restricts to a map

$$\mathrm{FQSym}\left(\mathbf{X},\mathbf{Y}\right) \overset{\rho}{\to} \mathrm{FQSym}\left(\mathbf{X}\right) \otimes \mathrm{FQSym}\left(\mathbf{Y}\right) \tag{8.1.8}$$

in which the target is identified with its image under the (injective[368]) multiplication map

$$\begin{array}{rcl} \mathrm{FQSym}\left(\mathbf{X}\right) \otimes \mathrm{FQSym}\left(\mathbf{Y}\right) & \hookrightarrow & R\langle M\rangle, \\ f(\mathbf{X}) \otimes g(\mathbf{Y}) & \mapsto & f(\mathbf{X})g(\mathbf{Y}). \end{array}$$

Using the identification of FQSym with all three of $\mathrm{FQSym}\left(\mathbf{X}\right), \mathrm{FQSym}\left(\mathbf{Y}\right),$ $\mathrm{FQSym}\left(\mathbf{X},\mathbf{Y}\right)$, the map $\rho$ in (8.1.8) will then define a coproduct structure on FQSym. Abusing notation, for $f$ in FQSym, we will simply write $\Delta(f) = f(\mathbf{X},\mathbf{Y})$ instead of $\rho(f(\mathbf{X},\mathbf{Y}))$.

**Example 8.1.8.** Recall from Example 8.1.4 that one has

$$F_{312} = \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=231} \mathbf{X}_{\mathbf{i}} = \sum_{1\le i<j\le k} X_j X_k X_i,$$

and therefore its coproduct is

$$\begin{aligned}
\Delta F_{312} &= F_{312}(X_1, X_2, \ldots, Y_1, Y_2, \ldots) \qquad \text{(by our abuse of notation)} \\
&= \sum_{i<j\le k} X_j X_k X_i + \sum_{\substack{i<j, \\ k}} X_j Y_k X_i + \sum_{\substack{i, \\ j\le k}} Y_j Y_k X_i + \sum_{i<j\le k} Y_j Y_k Y_i \\
&= \sum_{i<j\le k} X_j X_k X_i \cdot 1 + \sum_{\substack{i<j, \\ k}} X_j X_i \cdot Y_k + \sum_{\substack{i, \\ j\le k}} X_i \cdot Y_j Y_k + \sum_{i<j\le k} 1 \cdot Y_j Y_k Y_i \\
&= F_{312}(\mathbf{X}) \cdot 1 + F_{21}(\mathbf{X}) \cdot F_1(\mathbf{Y}) + F_1(\mathbf{X}) \cdot F_{12}(\mathbf{Y}) + 1 \cdot F_{312}(\mathbf{Y}) \\
&= F_{312} \otimes 1 + F_{21} \otimes F_1 + F_1 \otimes F_{12} + 1 \otimes F_{312}.
\end{aligned}$$

**Proposition 8.1.9.** *The map $\rho$ in* (8.1.7) *does restrict as claimed to a map as in* (8.1.8)*, and hence defines a coproduct on* FQSym*, acting on the $\{F_w\}$ basis by the rule* (8.1.2)*. This endows* FQSym *with the structure of a connected graded finite type Hopf algebra.*

*Proof.* Let $I$ be the totally ordered set $\{1 < 2 < 3 < \cdots\}$. Let $J$ be the totally ordered set
$\left\{1 < 2 < 3 < \cdots < \widetilde{1} < \widetilde{2} < \widetilde{3} < \cdots\right\}$. We set $X_{\widetilde{i}} = Y_i$ for every positive integer $i$. Then, the alphabet $(\mathbf{X},\mathbf{Y})$ can be written as $\{X_i\}_{i\in J}$.

[368] as images of the basis $F_u(\mathbf{X}) \otimes F_v(\mathbf{Y})$ of $\mathrm{FQSym}(\mathbf{X}) \otimes \mathrm{FQSym}(\mathbf{Y})$ are supported on disjoint monomials in $R\langle M\rangle$, so linearly independent.

If $\mathbf{i}$ is a word over the alphabet $I = \{1 < 2 < 3 < \cdots\}$, then we denote by $\widetilde{\mathbf{i}}$ the word over $J$ obtained from $\mathbf{i}$ by replacing every letter $i$ by $\widetilde{i}$.

For the first assertion of Proposition 8.1.9, it suffices to check that $F_w$ indeed has the image under $\Delta$ claimed in (8.1.2). Let $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$. Then,

$$\begin{aligned}
\Delta F_w &= F_w(\mathbf{X}, \mathbf{Y}) \qquad \text{(by our abuse of notation)} \\
&= \sum_{\mathbf{i} \in J^n : \operatorname{std}(\mathbf{i}) = w^{-1}} (\mathbf{X}, \mathbf{Y})_{\mathbf{i}} = \sum_{\mathbf{t} \in J^n : \operatorname{std}(\mathbf{t}) = w^{-1}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}} \\
&= \sum_{k=0}^{n} \sum_{(\mathbf{i},\mathbf{j}) \in I^k \times I^{n-k}} \sum_{\substack{\mathbf{t} \in J^n : \\ \operatorname{std}(\mathbf{t}) = w^{-1}; \\ \mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}} \qquad (8.1.9)
\end{aligned}$$

(since for every $\mathbf{t} \in J^n$, there exists exactly one choice of $k \in \{0, 1, \ldots, n\}$ and $(\mathbf{i}, \mathbf{j}) \in I^k \times I^{n-k}$ satisfying $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$; namely, $\mathbf{i}$ is the restriction of $\mathbf{t}$ to the subalphabet $I$ of $J$, whereas $\mathbf{j}$ is the restriction of $\mathbf{t}$ to $J \setminus I$, and $k$ is the length of $\mathbf{i}$).

We now fix $k$ and $(\mathbf{i}, \mathbf{j})$, and try to simplify the inner sum $\sum_{\substack{\mathbf{t} \in J^n : \\ \operatorname{std}(\mathbf{t}) = w^{-1}; \\ \mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}}$ on the right hand side of (8.1.9). First we notice that this sum is nonempty if and only if there exists some $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ satisfying $\operatorname{std}(\mathbf{t}) = w^{-1}$. This existence is easily seen to be equivalent to $w^{-1} \in \operatorname{std}(\mathbf{i}) \sqcup\!\sqcup \operatorname{std}(\mathbf{j})[k]$ (since the standardization of any shuffle in $\mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ is the corresponding shuffle in $\operatorname{std}(\mathbf{i}) \sqcup\!\sqcup \operatorname{std}(\mathbf{j})[k]$). This, in turn, is equivalent to $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$ (according to the equivalence (i) $\Longleftrightarrow$ (ii) in Lemma 8.1.6). Hence, the inner sum on the right hand side of (8.1.9) is nonempty if and only if $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$. When it is nonempty, it has only one addend[369], and this addend is $(\mathbf{X}, \mathbf{Y})_{\mathbf{t}} = \mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}}$ (since $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$). Summarizing, we see that the inner sum on the right hand side of (8.1.9) equals $\mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}}$ when $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$, and is empty otherwise. Thus, (8.1.9) simplifies to

$$\begin{aligned}
\Delta F_w &= \sum_{k=0}^{n} \sum_{\substack{(\mathbf{i},\mathbf{j}) \in I^k \times I^{n-k} : \\ \operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1} \\ \operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}}} \mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}} \\
&= \sum_{k=0}^{n} F_{\operatorname{std}(w_1, \ldots, w_k)}(\mathbf{X}) F_{\operatorname{std}(w_{k+1}, \ldots, w_n)}(\mathbf{Y}) \\
&= \sum_{k=0}^{n} F_{\operatorname{std}(w_1, \ldots, w_k)} \otimes F_{\operatorname{std}(w_{k+1}, \ldots, w_n)} \in \operatorname{FQSym} \otimes \operatorname{FQSym}.
\end{aligned}$$

This proves (8.1.2), and thus the first assertion of Proposition 8.1.9.

From this, it is easy to derive that $\Delta$ satisfies coassociativity (i.e., the diagram (1.2.1) holds for $C = \operatorname{FQSym}$). (Alternatively, one can obtain

[369] In fact, the elements $\operatorname{std}(\mathbf{t})$ for $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ are distinct, and thus only one of them can equal $w^{-1}$.

this from the associativity of multiplication using Corollary 8.1.11.) We have already verified the rule (8.1.2). The connected graded structure on FQSym gives a counit and an antipode for free. □

**Exercise 8.1.10.** We say that a permutation $w \in \mathfrak{S}_n$ is *connected* if $n$ is a positive integer and if there exists no $i \in \{1, 2, \ldots, n-1\}$ satisfying $f(\{1, 2, \ldots, i\}) = \{1, 2, \ldots, i\}$. Let $\mathfrak{CS}$ denote the set of all connected permutations of all $n \in \mathbb{N}$. Show that FQSym is a free (noncommutative) $\mathbf{k}$-algebra with generators $(F_w)_{w \in \mathfrak{CS}}$. (This statement means that $(F_{w_1} F_{w_2} \cdots F_{w_k})_{k \in \mathbb{N};\ (w_1, w_2, \ldots, w_k) \in \mathfrak{CS}^k}$ is a basis of the $\mathbf{k}$-module FQSym.)

[**Hint:** This is a result of Poirier and Reutenauer [172, Theorem 2.1]; it is much easier than the similar Theorem 6.4.3.]

**Corollary 8.1.11.** *The Hopf algebra* FQSym *is self-dual: Let* $\{G_w\}$ *be the dual* $\mathbf{k}$*-basis to the* $\mathbf{k}$*-basis* $\{F_w\}$ *for* FQSym. *Then, the* $\mathbf{k}$*-linear map sending* $G_w \longmapsto F_{w^{-1}}$ *is a Hopf algebra isomorphism* $\mathrm{FQSym}^o \longrightarrow \mathrm{FQSym}$.

*Proof.* For any $0 \leq k \leq n$, any $u \in \mathfrak{S}_k$ and any $v \in \mathfrak{S}_{n-k}$, one has

$$F_{u^{-1}} F_{v^{-1}} = \sum_{w^{-1} \in u^{-1} \sqcup\!\sqcup\, v^{-1}[k]} F_{w^{-1}} = \sum_{\substack{w \in \mathfrak{S}_n: \\ \mathrm{std}(w_1, \ldots, w_k) = u \\ \mathrm{std}(w_{k+1}, \ldots, w_n) = v}} F_{w^{-1}}$$

via the equivalence of (i) and (ii) in Lemma 8.1.6. On the other hand, in $\mathrm{FQSym}^o$, the dual $\mathbf{k}$-basis $\{G_w\}$ to the $\mathbf{k}$-basis $\{F_w\}$ for FQSym should have product formula

$$G_u G_v = \sum_{\substack{w \in \mathfrak{S}_n: \\ \mathrm{std}(w_1, \ldots, w_k) = u \\ \mathrm{std}(w_{k+1}, \ldots, w_n) = v}} G_w$$

coming from the coproduct formula (8.1.2) for FQSym in the $\{F_w\}$-basis. Comparing these equalities, we see that the $\mathbf{k}$-linear map $\tau$ sending $G_w \longmapsto F_{w^{-1}}$ is an isomorphism $\mathrm{FQSym}^o \longrightarrow \mathrm{FQSym}$ of $\mathbf{k}$-algebras. Hence, the adjoint $\tau^* : \mathrm{FQSym}^o \to (\mathrm{FQSym}^o)^o$ of this map is an isomorphism of $\mathbf{k}$-coalgebras. But identifying $(\mathrm{FQSym}^o)^o$ with FQSym in the natural way (since FQSym is of finite type), we easily see that $\tau^* = \tau$, whence $\tau$ itself is an isomorphism of both $\mathbf{k}$-algebras and $\mathbf{k}$-coalgebras, hence of $\mathbf{k}$-bialgebras, hence of Hopf algebras. □

We can now be a bit more precise about the relations between the various algebras

$$\Lambda, \mathrm{QSym}, \mathrm{NSym}, \mathrm{FQSym}, R\langle \mathbf{X} \rangle, R(\mathbf{x}).$$

Not only does FQSym allow one to *lift* the Hopf structure of QSym, it dually allows one to *extend* the Hopf structure of NSym. To set up this duality, note that Corollary 8.1.11 motivates the choice of an inner product on FQSym in which

$$(F_u, F_v) := \delta_{u^{-1}, v}.$$

We wish to identify the images of the ribbon basis $\{R_\alpha\}$ of NSym when included in FQSym.

**Definition 8.1.12.** For any composition $\alpha$, define an element $\mathbf{R}_\alpha$ of FQSym by

$$\mathbf{R}_\alpha := \sum_{\substack{w \in \mathfrak{S}_{|\alpha|}: \\ \operatorname{Des}(w)=D(\alpha)}} F_{w^{-1}} = \sum_{\substack{(w,\mathbf{i}): \\ w \in \mathfrak{S}_{|\alpha|}; \\ \operatorname{Des}(w)=D(\alpha); \\ \operatorname{std}(\mathbf{i})=w}} \mathbf{X}_{\mathbf{i}} = \sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha)} \mathbf{X}_{\mathbf{i}},$$

where the *descent set* of a sequence $\mathbf{i} = (i_1, \ldots, i_n)$ is defined by

$$\operatorname{Des}(\mathbf{i}) := \{j \in \{1,2,\ldots,n-1\} : i_j > i_{j+1}\} = \operatorname{Des}(\operatorname{std}(\mathbf{i})).$$

Alternatively,

$$\mathbf{R}_\alpha = \sum_T \mathbf{X}_T \tag{8.1.10}$$

in which the sum is over column-strict tableaux of the ribbon skew shape $\operatorname{Rib}(\alpha)$, and $\mathbf{X}_T = \mathbf{X}_{\mathbf{i}}$ in which $\mathbf{i}$ is the sequence of entries of $T$ read in order from the southwest toward the northeast.

**Example 8.1.13.** Taking $\alpha = (1,3,2)$, with ribbon shape and column-strict fillings $T$ as shown:

$$\operatorname{Rib}(\alpha) = \begin{array}{cccc} & & \square & \square \\ \square & \square & \square & \\ \square & & & \end{array} \qquad \text{and} \qquad T = \begin{array}{ccccccc} & & & & i_5 & \leq & i_6 \\ & & & & \wedge & & \\ i_2 & \leq & i_3 & \leq & i_4 & & \\ \wedge & & & & & & \\ i_1 & & & & & & \end{array}$$

one has that

$$\mathbf{R}_{(1,3,2)} = \sum_{\substack{\mathbf{i}=(i_1,i_2,i_3,i_4,i_5,i_6): \\ \operatorname{Des}(\mathbf{i})=D(\alpha)=\{1,4\}}} \mathbf{X}_{\mathbf{i}} = \sum_{i_1 > i_2 \leq i_3 \leq i_4 > i_5 \leq i_6} X_{i_1} X_{i_2} X_{i_3} X_{i_4} X_{i_5} X_{i_6} = \sum_T \mathbf{X}_T.$$

**Corollary 8.1.14.** *For every $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$, we let $\gamma(w)$ denote the unique composition $\alpha$ of $n$ satisfying $D(\alpha) = \operatorname{Des}(w)$.*

(a) *The* $\mathbf{k}$*-linear map*

$$\begin{array}{ccc} \text{FQSym} & \overset{\pi}{\twoheadrightarrow} & \text{QSym}, \\ F_w & \longmapsto & L_{\gamma(w)} \end{array}$$

*is a surjective Hopf algebra homomorphism.*

(b) *The* $\mathbf{k}$*-linear map*

$$\begin{array}{ccc} \text{NSym} & \overset{\iota}{\hookrightarrow} & \text{FQSym}, \\ R_\alpha & \longmapsto & \mathbf{R}_\alpha \end{array}$$

*is an injective Hopf algebra homomorphism.*

(c) *The linear maps $\pi$ and $\iota$ are adjoint maps with respect to the above choice of inner product on* FQSym *and the usual dual pairing between* NSym *and* QSym.

*Now, consider the abelianization map* ab : $R\langle\mathbf{X}\rangle \twoheadrightarrow R(\mathbf{x})$ *defined as the continuous* $\mathbf{k}$*-algebra homomorphism sending the noncommutative variable $X_i$ to the commutative $x_i$.*

(d) *The map $\pi$ is a restriction of* ab.

(e) *The map $\iota$ lets one factor the surjection* $\operatorname{NSym} \twoheadrightarrow \Lambda$ *as follows:*

$$\begin{array}{ccccc} \operatorname{NSym} & \to & \operatorname{FQSym} \hookrightarrow R\langle \mathbf{X} \rangle & \overset{\text{ab}}{\to} & R(\mathbf{x}), \\ R_\alpha & \longmapsto & \mathbf{R}_\alpha & \longmapsto & s_{\operatorname{Rib}(\alpha)}(\mathbf{x}). \end{array}$$

*Proof.* Given $n \in \mathbb{N}$, each composition $\alpha$ of $n$ can be written in the form $\gamma(w)$ for some $w \in \mathfrak{S}_n$. [370] Hence, each fundamental quasisymmetric function $L_\alpha$ lies in the image of $\pi$. Thus, $\pi$ is surjective.

Also, for each $n \in \mathbb{N}$ and $\alpha \in \operatorname{Comp}_n$, the element $\mathbf{R}_\alpha$ is a nonempty sum of noncommutative monomials (nonempty because $\alpha$ can be written in the form $\gamma(w)$ for some $w \in \mathfrak{S}_n$). Moreover, the elements $\mathbf{R}_\alpha$ for varying $n$ and $\alpha$ are supported on disjoint monomials. Thus, these elements are linearly independent. Hence, the map $\iota$ is injective.

(d) Let $\mathfrak{A}$ denote the totally ordered set $\{1 < 2 < 3 < \cdots\}$ of positive integers. For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$.

Let $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Then,

$$L_{\gamma(\sigma)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w$$

(by Lemma 5.3.6). But (8.1.3) (applied to $w = \sigma$) yields

$$F_\sigma = \sum_{\substack{\mathbf{i} = (i_1, \ldots, i_n): \\ \operatorname{std}(\mathbf{i}) = \sigma^{-1}}} \mathbf{X}_{\mathbf{i}} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{X}_w$$

and thus

$$\operatorname{ab}(F_\sigma) = \operatorname{ab}\left( \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{X}_w \right) = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \underbrace{\operatorname{ab}(\mathbf{X}_w)}_{= \mathbf{x}_w} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w = L_{\gamma(\sigma)}$$
$$= \pi(F_\sigma).$$

We have shown this for all $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Thus, $\pi$ is a restriction of ab. This proves Corollary 8.1.14(d).

(a) Let $n \in \mathbb{N}$ and $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{S}_n$. Let $\alpha$ be the composition $\gamma(w)$ of $n$. Thus, the definition of $\pi$ yields $\pi(F_w) = L_\alpha$. But applying the map $\pi \otimes \pi$ to the equality (8.1.2), we obtain

$$\begin{aligned} (\pi \otimes \pi)(\Delta F_w) &= (\pi \otimes \pi)\left( \sum_{k=0}^{n} F_{\operatorname{std}(w_1, w_2, \ldots, w_k)} \otimes F_{\operatorname{std}(w_{k+1}, w_{k+2}, \ldots, w_n)} \right) \\ &= \sum_{k=0}^{n} \pi\left(F_{\operatorname{std}(w_1, w_2, \ldots, w_k)}\right) \otimes \pi\left(F_{\operatorname{std}(w_{k+1}, w_{k+2}, \ldots, w_n)}\right) \\ &= \sum_{k=0}^{n} L_{\gamma(\operatorname{std}(w_1, w_2, \ldots, w_k))} \otimes L_{\gamma(\operatorname{std}(w_{k+1}, w_{k+2}, \ldots, w_n))} \qquad (8.1.11) \end{aligned}$$

[370] Indeed, write our composition $\alpha$ as $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Then, we can pick $w$ to be the permutation whose first $\alpha_1$ entries are the largest $\alpha_1$ elements of $\{1, 2, \ldots, n\}$ in increasing order; whose next $\alpha_2$ entries are the next-largest $\alpha_2$ elements of $\{1, 2, \ldots, n\}$ in increasing order; and so on. This permutation $w$ will satisfy $\operatorname{Des}(w) = \{\alpha_1, \alpha_1 + \alpha_2, \ldots, \alpha_1 + \alpha_2 + \cdots + \alpha_{k-1}\} = D(\alpha)$ and thus $\gamma(w) = \alpha$.

(by the definition of $\pi$). Now, for each $k \in \{0, 1, \ldots, n\}$, the two compositions $\gamma\left(\operatorname{std}(w_1, w_2, \ldots, w_k)\right)\ \gamma\left(\operatorname{std}(w_{k+1}, w_{k+2}, \ldots, w_n)\right)$ form a pair $(\beta, \gamma)$ of compositions satisfying[371] either $\beta \cdot \gamma = \alpha$ or $\beta \odot \gamma = \alpha$, and in fact they form the only such pair satisfying $|\beta| = k$ and $|\gamma| = n - k$. Thus, the right hand side of (8.1.11) can be rewritten as

$$\sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha \text{ or } \beta\odot\gamma=\alpha}} L_\beta \otimes L_\gamma.$$

But this sum is $\Delta L_\alpha$, as we know from (5.2.5). Hence, (8.1.11) becomes

$$(\pi \otimes \pi)(\Delta F_w) = \Delta L_\alpha = \Delta(\pi(F_w)) \qquad (\text{since } L_\alpha = \pi(F_w)).$$

We have proven this for each $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$. Thus, we have proven that $(\pi \otimes \pi) \circ \Delta_{\mathrm{FQSym}} = \Delta_{\mathrm{QSym}} \circ \pi$. Combined with $\epsilon_{\mathrm{FQSym}} = \epsilon_{\mathrm{QSym}} \circ \pi$ (which is easy to check), this shows that $\pi$ is a coalgebra homomorphism.

We can similarly see that $\pi$ is an algebra homomorphism by checking that it respects the product (compare (5.2.6) and (8.1.1)). However, this also follows trivially from Corollary 8.1.14(d).

Thus, $\pi$ is a bialgebra morphism, and therefore a Hopf algebra morphism (by Corollary 1.4.27). This proves Corollary 8.1.14(a).

(c) For any composition $\alpha$ and any $w \in \mathfrak{S}$, we have

$$(\iota(R_\alpha), F_w) = (\mathbf{R}_\alpha, F_w) = \sum_{u:\operatorname{Des}(u)=D(\alpha)} (F_{u^{-1}}, F_w) = \begin{cases} 1, & \text{if } \operatorname{Des}(w) = D(\alpha); \\ 0, & \text{otherwise} \end{cases}$$
$$= \begin{cases} 1, & \text{if } \gamma(w) = \alpha; \\ 0, & \text{otherwise} \end{cases} = (R_\alpha, L_{\gamma(w)}) = (R_\alpha, \pi(F_w)).$$

Thus, the maps $\pi$ and $\iota$ are adjoint. This proves Corollary 8.1.14(c).

(b) Again, there are several ways to prove this. Here is one:

First, note that $\iota(1) = 1$ (because $R_\varnothing = 1$ and $\mathbf{R}_\varnothing = 1$). Next, let $\alpha$ and $\beta$ be two nonempty compositions. Let $m = |\alpha|$ and $n = |\beta|$. Then, $R_\alpha R_\beta = R_{\alpha\cdot\beta} + R_{\alpha\odot\beta}$ (by (5.4.11)) and thus

$$\begin{aligned}
\iota(R_\alpha R_\beta) &= \iota(R_{\alpha\cdot\beta} + R_{\alpha\odot\beta}) \\
&= \underbrace{\iota(R_{\alpha\cdot\beta})}_{=\mathbf{R}_{\alpha\cdot\beta}=\sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha\cdot\beta)} \mathbf{X}_\mathbf{i}} + \underbrace{\iota(R_{\alpha\odot\beta})}_{=\mathbf{R}_{\alpha\odot\beta}=\sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha\odot\beta)} \mathbf{X}_\mathbf{i}} \\
&= \sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha\cdot\beta)} \mathbf{X}_\mathbf{i} + \sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha\odot\beta)} \mathbf{X}_\mathbf{i} \\
&= \sum_{\mathbf{i}:\operatorname{Des}(\mathbf{i})=D(\alpha\cdot\beta) \text{ or } \operatorname{Des}(\mathbf{i})=D(\alpha\odot\beta)} \mathbf{X}_\mathbf{i} \\
&= \sum_{\substack{\mathbf{i}=(i_1,i_2,\ldots,i_{m+n}):\\ \operatorname{Des}(i_1,i_2,\ldots,i_m)=D(\alpha) \text{ and}\\ \operatorname{Des}(i_{m+1},i_{m+2},\ldots,i_{m+n})=D(\beta)}} \mathbf{X}_\mathbf{i} \qquad (8.1.12)
\end{aligned}$$

(since the words $\mathbf{i}$ of length $m + n$ satisfying $\operatorname{Des}(\mathbf{i}) = D(\alpha \cdot \beta)$ or $\operatorname{Des}(\mathbf{i}) = D(\alpha \odot \beta)$ are precisely the words $\mathbf{i} = (i_1, i_2, \ldots, i_{m+n})$ satisfying $\operatorname{Des}(i_1, i_2, \ldots, i_m) = D(\alpha)$ and $\operatorname{Des}(i_{m+1}, i_{m+2}, \ldots, i_{m+n}) = D(\beta)$). But choosing a word $\mathbf{i} = (i_1, i_2, \ldots, i_{m+n})$ satisfying $\operatorname{Des}(i_1, i_2, \ldots, i_m) = D(\alpha)$

[371] See Definition 5.2.14 for the notation we are using.

and $\operatorname{Des}(i_{m+1}, i_{m+2}, \ldots, i_{m+n}) = D(\beta)$ is tantamount to choosing a pair $(\mathbf{u}, \mathbf{v})$ of a word $\mathbf{u} = (i_1, i_2, \ldots, i_m)$ satisfying $\operatorname{Des} \mathbf{u} = D(\alpha)$ and a word $\mathbf{v} = (i_{m+1}, i_{m+2}, \ldots, i_{m+n})$ satisfying $\operatorname{Des} \mathbf{v} = D(\beta)$. Thus, (8.1.12) becomes

$$\begin{aligned}\iota(R_\alpha R_\beta) &= \sum_{\substack{\mathbf{i}=(i_1,i_2,\ldots,i_{m+n}): \\ \operatorname{Des}(i_1,i_2,\ldots,i_m)=D(\alpha) \text{ and} \\ \operatorname{Des}(i_{m+1},i_{m+2},\ldots,i_{m+n})=D(\beta)}} \mathbf{X}_\mathbf{i} = \sum_{\mathbf{u}:\operatorname{Des}\mathbf{u}=D(\alpha)} \sum_{\mathbf{v}:\operatorname{Des}\mathbf{v}=D(\beta)} \mathbf{X}_\mathbf{u}\mathbf{X}_\mathbf{v} \\ &= \underbrace{\left(\sum_{\mathbf{u}:\operatorname{Des}\mathbf{u}=D(\alpha)} \mathbf{X}_\mathbf{u}\right)}_{=\mathbf{R}_\alpha=\iota(R_\alpha)} \underbrace{\left(\sum_{\mathbf{v}:\operatorname{Des}\mathbf{v}=D(\beta)} \mathbf{X}_\mathbf{v}\right)}_{=\mathbf{R}_\beta=\iota\left(R_\beta\right)} = \iota(R_\alpha)\,\iota(R_\beta).\end{aligned}$$

Thus, we have proven the equality $\iota(R_\alpha R_\beta) = \iota(R_\alpha)\,\iota(R_\beta)$ whenever $\alpha$ and $\beta$ are two nonempty compositions. It also holds if we drop the "nonempty" requirement (since $R_\varnothing = 1$ and $\iota(1) = 1$). Thus, the $\mathbf{k}$-linear map $\iota$ respects the multiplication. Since $\iota(1) = 1$, this shows that $\iota$ is a $\mathbf{k}$-algebra homomorphism.

For each $n \in \mathbb{N}$, we let $\operatorname{id}_n$ be the identity permutation in $\mathfrak{S}_n$. Next, we observe that each $n \in \mathbb{N}$ satisfies $H_n = R_{(n)}$ (this follows, e.g., from (5.4.9), because the composition $(n)$ is coarsened only by itself). Hence, each $n \in \mathbb{N}$ satisfies

$$\begin{aligned}\iota(H_n) = \iota\left(R_{(n)}\right) = \mathbf{R}_{(n)} &= \sum_{\substack{w\in\mathfrak{S}_n: \\ \operatorname{Des}(w)=D((n))}} F_{w^{-1}} \\ &= F_{\operatorname{id}_n^{-1}} \qquad \left(\begin{array}{c}\text{since the only } w \in \mathfrak{S}_n \\ \text{satisfying } \operatorname{Des}(w) = D((n)) \\ \text{is } \operatorname{id}_n\end{array}\right) \\ &= F_{\operatorname{id}_n}. \qquad (8.1.13)\end{aligned}$$

In order to show that $\iota$ is a $\mathbf{k}$-coalgebra homomorphism, it suffices to check the equalities $(\iota \otimes \iota) \circ \Delta_{\mathrm{NSym}} = \Delta_{\mathrm{FQSym}} \circ \iota$ and $\epsilon_{\mathrm{NSym}} = \epsilon_{\mathrm{FQSym}} \circ \iota$. We shall only prove the first one, since the second is easy. Since $\iota$, $\Delta_{\mathrm{NSym}}$ and $\Delta_{\mathrm{FQSym}}$ are $\mathbf{k}$-algebra homomorphisms, it suffices to check it on the generators $H_1, H_2, H_3, \ldots$ of NSym. But on these generators, it follows from comparing

$$\begin{aligned}((\iota \otimes \iota) \circ \Delta_{\mathrm{NSym}})(H_n) &= (\iota \otimes \iota)(\Delta_{\mathrm{NSym}} H_n) \\ &= (\iota \otimes \iota)\left(\sum_{i+j=n} H_i \otimes H_j\right) \qquad (\text{by } (5.4.2)) \\ &= \sum_{i+j=n} \underbrace{\iota(H_i)}_{\substack{=F_{\operatorname{id}_i} \\ (\text{by } (8.1.13))}} \otimes \underbrace{\iota(H_j)}_{\substack{=F_{\operatorname{id}_j} \\ (\text{by } (8.1.13))}} = \sum_{i+j=n} F_{\operatorname{id}_i} \otimes F_{\operatorname{id}_j} \\ &= \sum_{k=0}^{n} F_{\operatorname{id}_k} \otimes F_{\operatorname{id}_{n-k}}\end{aligned}$$

with

$$\begin{aligned}(\Delta_{\mathrm{FQSym}} \circ \iota)(H_n) = \Delta_{\mathrm{FQSym}}(\iota(H_n)) &= \Delta_{\mathrm{FQSym}}(F_{\mathrm{id}_n}) \qquad (\text{by } (8.1.13)) \\ &= \sum_{k=0}^{n} F_{\mathrm{id}_k} \otimes F_{\mathrm{id}_{n-k}} \qquad (\text{by } (8.1.2)).\end{aligned}$$

Thus, we know that $\iota$ is a $\mathbf{k}$-algebra homomorphism and a $\mathbf{k}$-coalgebra homomorphism. Hence, $\iota$ is a bialgebra morphism, and therefore a Hopf algebra morphism (by Corollary 1.4.27). This proves Corollary 8.1.14(b).

An alternative proof of Corollary 8.1.14(b) can be obtained by adjointness from Corollary 8.1.14(a). Both the inner product on FQSym and the dual pairing $(\cdot, \cdot) : \mathrm{NSym} \otimes \mathrm{QSym} \to \mathbf{k}$ respect the Hopf structures (i.e., the maps $\Delta_{\mathrm{NSym}}$ and $m_{\mathrm{QSym}}$ are mutually adjoint with respect to these forms, and so are the maps $m_{\mathrm{NSym}}$ and $\Delta_{\mathrm{QSym}}$, and the maps $\Delta_{\mathrm{FQSym}}$ and $m_{\mathrm{FQSym}}$, and so on). Corollary 8.1.14(c) shows that the map $\iota$ is adjoint to the map $\pi$ with respect to these two bilinear forms. Hence, we have a commutative diagram

$$\begin{tikzcd}
\mathrm{NSym} \arrow[r, hook, "\iota"] \arrow[d, "\cong"] & \mathrm{FQSym} \arrow[d, "\cong"] \\
\mathrm{QSym}^o \arrow[r, "\pi^*"'] & \mathrm{FQSym}^o
\end{tikzcd}$$

of Hopf algebras (where the two vertical arrows are the isomorphisms induced by the two bilinear forms). Thus, Corollary 8.1.14(b) follows from Corollary 8.1.14(a) by duality.

(e) For each composition $\alpha$, the abelianization map ab sends the noncommutative tableau monomial $\mathbf{X}_T$ to the commutative tableau monomial $\mathbf{x}_T$ whenever $T$ is a tableau of ribbon shape $\mathrm{Rib}(\alpha)$. Thus, ab sends $\mathbf{R}_\alpha$ to $s_{\mathrm{Rib}(\alpha)}(\mathbf{x})$ (because of the formula (8.1.10)). Hence, the composition $\mathrm{NSym} \to \mathrm{FQSym} \hookrightarrow R\langle \mathbf{X} \rangle \overset{\mathrm{ab}}{\to} R(\mathbf{x})$ does indeed send $R_\alpha$ to $s_{\mathrm{Rib}(\alpha)}(\mathbf{x})$. But so does the projection $\pi : \mathrm{NSym} \to \Lambda$, according to Theorem 5.4.10(b). Hence, the composition factors the projection. This proves Corollary 8.1.14(e). □

We summarize some of this picture as follows:

$$\begin{tikzcd}
\mathrm{FQSym} \arrow[r, dotted, no head, "\text{dual}"] \arrow[d, phantom] & \mathrm{FQSym} \arrow[d, "\pi"] \\
\mathrm{NSym} \arrow[u, hook, "\iota"] \arrow[r, dotted, no head, "\text{dual}"] \arrow[d, "\pi"] & \mathrm{QSym} \\
\Lambda \arrow[r, dotted, no head, "\text{dual}"] & \Lambda \arrow[u, hook]
\end{tikzcd}$$

Furthermore, if we denote by $\iota$ the canonical inclusion $\Lambda \to \mathrm{QSym}$ as well, then the diagram

$$\begin{tikzcd}
 & \mathrm{FQSym} \arrow[dr, two heads, "\pi"] & \\
\mathrm{NSym} \arrow[ur, hook, "\iota"'] \arrow[dr, two heads, "\pi"] & & \mathrm{QSym} \\
 & \Lambda \arrow[ur, hook, "\iota"'] &
\end{tikzcd}$$

is commutative (according to Corollary 8.1.14(e)).

*Remark* 8.1.15. Different notations for FQSym appear in the literature. In the book [24] (which presents an unusual approach to the character theory of the symmetric group using FQSym), the Hopf algebra FQSym is called $\mathcal{P}$, and its basis that we call $\{G_w\}_{w\in\mathfrak{S}_n}$ is denoted $\{w\}_{w\in\mathfrak{S}_n}$. In [93, Chapter 7], the Hopf algebra FQSym and its basis $\{F_w\}_{w\in\mathfrak{S}_n}$ are denoted $MPR$ and $\{w\}_{w\in\mathfrak{S}_n}$, respectively.

## 11. Appendix: Some basics

In this appendix, we briefly discuss some basic notions from linear algebra and elementary combinatorics that are used in these notes.

### 11.1. **Linear expansions and triangularity.**

In this Section, we shall recall some fundamental results from linear algebra (most importantly, the notions of a change-of-basis matrix and of a unitriangular matrix), but in greater generality than how it is usually done in textbooks. We shall use these results later when studying bases of combinatorial Hopf algebras; but per se, this section has nothing to do with Hopf algebras.

11.1.1. *Matrices.* Let us first define the notion of a matrix whose rows and columns are indexed by arbitrary objects (as opposed to numbers):[372]

**Definition 11.1.1.** Let $S$ and $T$ be two sets. An *$S\times T$-matrix over* $\mathbf{k}$ shall mean a family $(a_{s,t})_{(s,t)\in S\times T} \in \mathbf{k}^{S\times T}$ of elements of $\mathbf{k}$ indexed by elements of $S\times T$. Thus, the set of all $S\times T$-matrices over $\mathbf{k}$ is $\mathbf{k}^{S\times T}$.

We shall abbreviate "$S\times T$-matrix over $\mathbf{k}$" by "$S\times T$-matrix" when the value of $\mathbf{k}$ is clear from the context.

This definition of $S\times T$-matrices generalizes the usual notion of matrices (i.e., the notion of $n\times m$-matrices): Namely, if $n\in\mathbb{N}$ and $m\in\mathbb{N}$, then the $\{1,2,\ldots,n\}\times\{1,2,\ldots,m\}$-matrices are precisely the $n\times m$-matrices (in the usual meaning of this word). We shall often use the word "*matrix*" for both the usual notion of matrices and for the more general notion of $S\times T$-matrices.

Various concepts defined for $n\times m$-matrices (such as addition and multiplication of matrices, or the notion of a row) can be generalized to $S\times T$-matrices in a straightforward way. The following four definitions are examples of such generalizations:

**Definition 11.1.2.** Let $S$ and $T$ be two sets.

[372] As before, $\mathbf{k}$ denotes a commutative ring.

(a) The sum of two $S \times T$-matrices is defined by $\left(a_{s,t}\right)_{(s,t)\in S\times T} + \left(b_{s,t}\right)_{(s,t)\in S\times T} = \left(a_{s,t} + b_{s,t}\right)_{(s,t)\in S\times T}$.

(b) If $u \in \mathbf{k}$ and if $\left(a_{s,t}\right)_{(s,t)\in S\times T} \in \mathbf{k}^{S\times T}$, then we define $u\left(a_{s,t}\right)_{(s,t)\in S\times T}$ to be the $S \times T$-matrix $\left(u a_{s,t}\right)_{(s,t)\in S\times T}$.

(c) Let $A = \left(a_{s,t}\right)_{(s,t)\in S\times T}$ be an $S \times T$-matrix. For every $s \in S$, we define the *$s$-th row of $A$* to be the $\{1\} \times T$-matrix $\left(a_{s,t}\right)_{(i,t)\in\{1\}\times T}$. (Notice that $\{1\} \times T$-matrices are a generalization of row vectors.) Similarly, for every $t \in T$, we define the *$t$-th column of $A$* to be the $S \times \{1\}$-matrix $\left(a_{s,t}\right)_{(s,i)\in S\times\{1\}}$.

**Definition 11.1.3.** Let $S$ be a set.

(a) The *$S \times S$ identity matrix* is defined to be the $S \times S$-matrix $\left(\delta_{s,t}\right)_{(s,t)\in S\times S}$. This $S \times S$-matrix is denoted by $I_S$. (Notice that the $n \times n$ identity matrix $I_n$ is $I_{\{1,2,\ldots,n\}}$ for each $n \in \mathbb{N}$.)

(b) An $S \times S$-matrix $\left(a_{s,t}\right)_{(s,t)\in S\times S}$ is said to be *diagonal* if every $(s,t) \in S \times T$ satisfying $s \neq t$ satisfies $a_{s,t} = 0$.

(c) Let $A = \left(a_{s,t}\right)_{(s,t)\in S\times S}$ be an $S \times S$-matrix. The *diagonal* of $A$ means the family $\left(a_{s,s}\right)_{s\in S}$. The *diagonal entries* of $A$ are the entries of this diagonal $\left(a_{s,s}\right)_{s\in S}$.

**Definition 11.1.4.** Let $S$, $T$ and $U$ be three sets. Let $A = \left(a_{s,t}\right)_{(s,t)\in S\times T}$ be an $S \times T$-matrix, and let $B = \left(b_{t,u}\right)_{(t,u)\in T\times U}$ be a $T \times U$-matrix. Assume that the sum $\sum_{t\in T} a_{s,t} b_{t,u}$ is well-defined for every $(s,u) \in S \times U$. (For example, this is guaranteed to hold if the set $T$ is finite. For infinite $T$, it may and may not hold.) Then, the $S \times U$-matrix $AB$ is defined by

$$AB = \left(\sum_{t\in T} a_{s,t} b_{t,u}\right)_{(s,u)\in S\times U}.$$

**Definition 11.1.5.** Let $S$ and $T$ be two finite sets. We say that an $S \times T$-matrix $A$ is *invertible* if and only if there exists a $T \times S$-matrix $B$ satisfying $AB = I_S$ and $BA = I_T$. In this case, this matrix $B$ is unique; it is denoted by $A^{-1}$ and is called the *inverse* of $A$.

The definitions that we have just given are straightforward generalizations of the analogous definitions for $n \times m$-matrices; thus, unsurprisingly, many properties of $n \times m$-matrices still hold for $S \times T$-matrices. For example:

**Proposition 11.1.6.** (a) *Let $S$ and $T$ be two sets. Let $A$ be an $S \times T$-matrix. Then, $I_S A = A$ and $A I_T = A$.*

(b) *Let $S$, $T$ and $U$ be three sets such that $T$ is finite. Let $A$ and $B$ be two $S \times T$-matrices. Let $C$ be a $T \times U$-matrix. Then, $(A + B)C = AC + BC$.*

(c) *Let $S$, $T$, $U$ and $V$ be four sets such that $T$ and $U$ are finite. Let $A$ be an $S \times T$-matrix. Let $B$ be a $T \times U$-matrix. Let $C$ be a $U \times V$-matrix. Then, $(AB)C = A(BC)$.*

The proof of Proposition 11.1.6 (and of similar properties that will be left unstated) is analogous to the proofs of the corresponding properties of

$n \times m$-matrices.[373] As a consequence of these properties, it is easy to see that if $S$ is any finite set, then $\mathbf{k}^{S \times S}$ is a $\mathbf{k}$-algebra.

In general, $S \times T$-matrices (unlike $n \times m$-matrices) do not have a predefined order on their rows and their columns. Thus, the classical notion of a triangular $n \times n$-matrix cannot be generalized to a notion of a "triangular $S \times S$-matrix" when $S$ is just a set with no additional structure. However, when $S$ is a poset, such a generalization can be made:

**Definition 11.1.7.** Let $S$ be a poset. Let $A = (a_{s,t})_{(s,t) \in S \times S}$ be an $S \times S$-matrix.

(a) The matrix $A$ is said to be *triangular* if and only if every $(s,t) \in S \times S$ which does not satisfy $t \leq s$ must satisfy $a_{s,t} = 0$. (Here, $\leq$ denotes the smaller-or-equal relation of the poset $S$.)
(b) The matrix $A$ is said to be *unitriangular* if and only if $A$ is triangular and has the further property that, for every $s \in S$, we have $a_{s,s} = 1$.
(c) The matrix $A$ is said to be *invertibly triangular* if and only if $A$ is triangular and has the further property that, for every $s \in S$, the element $a_{s,s}$ of $\mathbf{k}$ is invertible.

Of course, all three notions of "triangular", "unitriangular" and "invertibly triangular" depend on the partial order on $S$.

Clearly, every invertibly triangular $S \times S$-matrix is triangular. Also, every unitriangular $S \times S$-matrix is invertibly triangular (because the element 1 of $\mathbf{k}$ is invertible).

We can restate the definition of "invertibly triangular" as follows: The matrix $A$ is said to be *invertibly triangular* if and only if it is triangular and its diagonal entries are invertible. Similarly, we can restate the definition of "unitriangular" as follows: The matrix $A$ is said to be *unitriangular* if and only if it is triangular and all its diagonal entries equal 1.

Definition 11.1.7(a) generalizes both the notion of upper-triangular matrices and the notion of lower-triangular matrices. To wit:

**Example 11.1.8.** Let $n \in \mathbb{N}$. Let $N_1$ be the poset whose ground set is $\{1, 2, \ldots, n\}$ and whose smaller-or-equal relation $\leq_1$ is given by

$$s \leq_1 t \iff s \leq t \text{ (as integers)}.$$

[373] A little **warning**: In Proposition 11.1.6(c), the condition that $T$ and $U$ be finite can be loosened (we leave this to the interested reader), but cannot be completely disposed of. It can happen that both $(AB)\,C$ and $A\,(BC)$ are defined, but $(AB)\,C = A\,(BC)$ does not hold (if we remove this condition). For example, this happens if $S = \mathbb{Z}$, $T = \mathbb{Z}$, $U = \mathbb{Z}$, $V = \mathbb{Z}$, $A = \left( \begin{cases} 1, & \text{if } i \geq j; \\ 0, & \text{if } i < j \end{cases} \right)_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$, $B = (\delta_{i,j} - \delta_{i,j+1})_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$ and $C = \left( \begin{cases} 0, & \text{if } i \geq j; \\ 1, & \text{if } i < j \end{cases} \right)_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$. (Indeed, in this example, it is easy to check that $AB = I_{\mathbb{Z}}$ and $BC = -I_{\mathbb{Z}}$ and thus $\underbrace{(AB)}_{=I_{\mathbb{Z}}} C = I_{\mathbb{Z}} C = C \neq -A = A \underbrace{(-I_{\mathbb{Z}})}_{=BC} = A\,(BC)$.)

This seeming paradox is due to the subtleties of rearranging infinite sums (similarly to how a conditionally convergent series of real numbers can change its value when its entries are rearranged).

(This is the usual order relation on this set.) Let $N_2$ be the poset whose ground set is $\{1, 2, \ldots, n\}$ and whose order relation $\leq_2$ is given by

$$s \leq_2 t \iff s \geq t \text{ (as integers).}$$

Let $A \in \mathbf{k}^{n \times n}$.

(a) The matrix $A$ is upper-triangular if and only if $A$ is triangular when regarded as an $N_1 \times N_1$-matrix.

(b) The matrix $A$ is lower-triangular if and only if $A$ is triangular when regarded as an $N_2 \times N_2$-matrix.

More interesting examples of triangular matrices are obtained when the order on $S$ is not a total order:

**Example 11.1.9.** Let $S$ be the poset whose ground set is $\{1, 2, 3\}$ and whose smaller relation $<_S$ is given by $1 <_S 2$ and $3 <_S 2$. Then, the triangular $S \times S$-matrices are precisely the $3 \times 3$-matrices of the form $\begin{pmatrix} a_{1,1} & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & 0 & a_{3,3} \end{pmatrix}$ with $a_{1,1}, a_{2,1}, a_{2,2}, a_{2,3}, a_{3,3} \in \mathbf{k}$.

We shall now state some basic properties of triangular matrices:

**Proposition 11.1.10.** *Let $S$ be a finite poset.*

(a) *The triangular $S \times S$-matrices form a subalgebra of the $\mathbf{k}$-algebra $\mathbf{k}^{S \times S}$.*

(b) *The invertibly triangular $S \times S$-matrices form a group with respect to multiplication.*

(c) *The unitriangular $S \times S$-matrices form a group with respect to multiplication.*

(d) *Any invertibly triangular $S \times S$-matrix is invertible, and its inverse is again invertibly triangular.*

(e) *Any unitriangular $S \times S$-matrix is invertible, and its inverse is again unitriangular.*

**Exercise 11.1.11.** Prove Proposition 11.1.10.

11.1.2. *Expansion of a family in another.* We will often study situations where two families $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ of vectors in a $\mathbf{k}$-module $M$ are given, and the vectors $e_s$ can be written as linear combinations of the vectors $f_t$. In such situations, we can form an $S \times T$-matrix out of the coefficients of these linear combinations; this is one of the ways how matrices arise in the theory of modules. Let us define the notations we are going to use in such situations:

**Definition 11.1.12.** Let $M$ be a $\mathbf{k}$-module. Let $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ be two families of elements of $M$. (The sets $S$ and $T$ may and may not be finite.)

Let $A = (a_{s,t})_{(s,t) \in S \times T}$ be an $S \times T$-matrix. Assume that, for every $s \in S$, all but finitely many $t \in T$ satisfy $a_{s,t} = 0$. (This assumption is automatically satisfied if $T$ is finite.)

We say that the family $(e_s)_{s \in S}$ *expands in the family $(f_t)_{t \in T}$ through the matrix $A$* if

$$\text{every } s \in S \text{ satisfies } e_s = \sum_{t \in T} a_{s,t} f_t. \tag{11.1.1}$$

In this case, we furthermore say that the matrix $A$ is a *change-of-basis matrix* (or *transition matrix*) from the family $(e_s)_{s\in S}$ to the family $(f_t)_{t\in T}$.

*Remark* 11.1.13. The notation in Definition 11.1.12 is not really standard; even we ourselves will occasionally deviate in its use. In the formulation "the family $(e_s)_{s\in S}$ expands in the family $(f_t)_{t\in T}$ through the matrix $A$", the word "in" can be replaced by "with respect to", and the word "through" can be replaced by "using".

The notion of a "change-of-basis matrix" is slightly misleading, because neither of the families $(e_s)_{s\in S}$ and $(f_t)_{t\in T}$ has to be a basis. Our use of the words "transition matrix" should not be confused with the different meaning that these words have in the theory of Markov chains. The indefinite article in "a change-of-basis matrix" is due to the fact that, for given families $(e_s)_{s\in S}$ and $(f_t)_{t\in T}$, there might be more than one change-of-basis matrix from $(e_s)_{s\in S}$ to $(f_t)_{t\in T}$. (There also might be no such matrix.) When $(e_s)_{s\in S}$ and $(f_t)_{t\in T}$ are bases of the $\mathbf{k}$-module $M$, there exists precisely one change-of-basis matrix from $(e_s)_{s\in S}$ to $(f_t)_{t\in T}$.

So a change-of-basis matrix $A = (a_{s,t})_{(s,t)\in S\times T}$ from one family $(e_s)_{s\in S}$ to another family $(f_t)_{t\in T}$ allows us to write the elements of the former family as linear combinations of the elements of the latter (using (11.1.1)). When such a matrix $A$ is invertible (and the sets $S$ and $T$ are finite[374]), it also (indirectly) allows us to do the opposite: i.e., to write the elements of the latter family as linear combinations of the elements of the former. This is because if $A$ is an invertible change-of-basis matrix from $(e_s)_{s\in S}$ to $(f_t)_{t\in T}$, then $A^{-1}$ is a change-of-basis matrix from $(f_t)_{t\in T}$ to $(e_s)_{s\in S}$. This is part (a) of the following theorem:

**Theorem 11.1.14.** *Let $M$ be a $\mathbf{k}$-module. Let $S$ and $T$ be two finite sets. Let $(e_s)_{s\in S}$ and $(f_t)_{t\in T}$ be two families of elements of $M$.*

*Let $A$ be an invertible $S\times T$-matrix. Thus, $A^{-1}$ is a $T\times S$-matrix.*

*Assume that the family $(e_s)_{s\in S}$ expands in the family $(f_t)_{t\in T}$ through the matrix $A$. Then:*

(a) *The family $(f_t)_{t\in T}$ expands in the family $(e_s)_{s\in S}$ through the matrix $A^{-1}$.*
(b) *The $\mathbf{k}$-submodule of $M$ spanned by the family $(e_s)_{s\in S}$ is the $\mathbf{k}$-submodule of $M$ spanned by the family $(f_t)_{t\in T}$.*
(c) *The family $(e_s)_{s\in S}$ spans the $\mathbf{k}$-module $M$ if and only if the family $(f_t)_{t\in T}$ spans the $\mathbf{k}$-module $M$.*
(d) *The family $(e_s)_{s\in S}$ is $\mathbf{k}$-linearly independent if and only if the family $(f_t)_{t\in T}$ is $\mathbf{k}$-linearly independent.*
(e) *The family $(e_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module $M$ if and only if the family $(f_t)_{t\in T}$ is a basis of the $\mathbf{k}$-module $M$.*

**Exercise 11.1.15.** Prove Theorem 11.1.14.

**Definition 11.1.16.** Let $M$ be a $\mathbf{k}$-module. Let $S$ be a finite poset. Let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of $M$.

[374] We are requiring the finiteness of $S$ and $T$ mainly for the sake of simplicity. We could allow $S$ and $T$ to be infinite, but then we would have to make some finiteness requirements on $A$ and $A^{-1}$.

(a) We say that the family $\left(e_s\right)_{s\in S}$ *expands triangularly in the family* $\left(f_s\right)_{s\in S}$ if and only if there exists a triangular $S \times S$-matrix $A$ such that the family $\left(e_s\right)_{s\in S}$ expands in the family $\left(f_s\right)_{s\in S}$ through the matrix $A$.

(b) We say that the family $\left(e_s\right)_{s\in S}$ *expands invertibly triangularly in the family* $\left(f_s\right)_{s\in S}$ if and only if there exists an invertibly triangular $S \times S$-matrix $A$ such that the family $\left(e_s\right)_{s\in S}$ expands in the family $\left(f_s\right)_{s\in S}$ through the matrix $A$.

(c) We say that the family $\left(e_s\right)_{s\in S}$ *expands unitriangularly in the family* $\left(f_s\right)_{s\in S}$ if and only if there exists a unitriangular $S \times S$-matrix $A$ such that the family $\left(e_s\right)_{s\in S}$ expands in the family $\left(f_s\right)_{s\in S}$ through the matrix $A$.

Clearly, if the family $\left(e_s\right)_{s\in S}$ expands unitriangularly in the family $\left(f_s\right)_{s\in S}$, then it also expands invertibly triangularly in the family $\left(f_s\right)_{s\in S}$ (because any unitriangular matrix is an invertibly triangular matrix).

We notice that in Definition 11.1.16, the two families $\left(e_s\right)_{s\in S}$ and $\left(f_s\right)_{s\in S}$ must be indexed by one and the same set $S$.

The concepts of "expanding triangularly", "expanding invertibly triangularly" and "expanding unitriangularly" can also be characterized without referring to matrices, as follows:

*Remark* 11.1.17. Let $M$ be a $\mathbf{k}$-module. Let $S$ be a finite poset. Let $\left(e_s\right)_{s\in S}$ and $\left(f_s\right)_{s\in S}$ be two families of elements of $M$. Let $<$ denote the smaller relation of the poset $S$, and let $\leq$ denote the smaller-or-equal relation of the poset $S$. Then:

(a) The family $\left(e_s\right)_{s\in S}$ expands triangularly in the family $\left(f_s\right)_{s\in S}$ if and only if every $s \in S$ satisfies

$$e_s = (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \\ \text{for } t \in S \text{ satisfying } t \leq s) .$$

(b) The family $\left(e_s\right)_{s\in S}$ expands invertibly triangularly in the family $\left(f_s\right)_{s\in S}$ if and only if every $s \in S$ satisfies

$$e_s = \alpha_s f_s + (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \\ \text{for } t \in S \text{ satisfying } t < s)$$

for some invertible $\alpha_s \in \mathbf{k}$.

(c) The family $\left(e_s\right)_{s\in S}$ expands unitriangularly in the family $\left(f_s\right)_{s\in S}$ if and only if every $s \in S$ satisfies

$$e_s = f_s + (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \\ \text{for } t \in S \text{ satisfying } t < s) .$$

All three parts of Remark 11.1.17 follow easily from the definitions.

**Example 11.1.18.** Let $n \in \mathbb{N}$. For this example, let $S$ be the poset $\{1, 2, \ldots, n\}$ (with its usual order). Let $M$ be a $\mathbf{k}$-module, and let $\left(e_s\right)_{s\in S}$ and $\left(f_s\right)_{s\in S}$ be two families of elements of $M$. We shall identify these families $\left(e_s\right)_{s\in S}$ and $\left(f_s\right)_{s\in S}$ with the $n$-tuples $(e_1, e_2, \ldots, e_n)$ and $(f_1, f_2, \ldots, f_n)$. Then, the family $\left(e_s\right)_{s\in S} = (e_1, e_2, \ldots, e_n)$ expands triangularly in the family $\left(f_s\right)_{s\in S} = (f_1, f_2, \ldots, f_n)$ if and only if, for every $s \in \{1, 2, \ldots, n\}$, the vector $e_s$ is a $\mathbf{k}$-linear combination of $f_1, f_2, \ldots, f_s$. Moreover, the family

$(e_s)_{s\in S} = (e_1, e_2, \ldots, e_n)$ expands unitriangularly in the family $(f_s)_{s\in S} = (f_1, f_2, \ldots, f_n)$ if and only if, for every $s \in \{1, 2, \ldots, n\}$, the vector $e_s$ is a sum of $f_s$ with a $\mathbf{k}$-linear combination of $f_1, f_2, \ldots, f_{s-1}$.

**Corollary 11.1.19.** *Let $M$ be a $\mathbf{k}$-module. Let $S$ be a finite poset. Let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of $M$. Assume that the family $(e_s)_{s\in S}$ expands invertibly triangularly in the family $(f_s)_{s\in S}$. Then:*

(a) *The family $(f_s)_{s\in S}$ expands invertibly triangularly in the family $(e_s)_{s\in S}$.*

(b) *The $\mathbf{k}$-submodule of $M$ spanned by the family $(e_s)_{s\in S}$ is the $\mathbf{k}$-submodule of $M$ spanned by the family $(f_s)_{s\in S}$.*

(c) *The family $(e_s)_{s\in S}$ spans the $\mathbf{k}$-module $M$ if and only if the family $(f_s)_{s\in S}$ spans the $\mathbf{k}$-module $M$.*

(d) *The family $(e_s)_{s\in S}$ is $\mathbf{k}$-linearly independent if and only if the family $(f_s)_{s\in S}$ is $\mathbf{k}$-linearly independent.*

(e) *The family $(e_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module $M$ if and only if the family $(f_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module $M$.*

**Exercise 11.1.20.** Prove Remark 11.1.17 and Corollary 11.1.19.

An analogue of Corollary 11.1.19 can be stated for unitriangular expansions, but we leave this to the reader.

## 12. Further hints to the exercises (work in progress)

The following pages contain hints to (some of[375]) the exercises in the text (beyond the hints occasionally included in the exercises themselves). Some of the hints rise to the level of outlined solutions.

Note that there is also a version of this text that contains detailed solutions for all the exercises; this version can be downloaded from `http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf` (or compiled from the sourcecode of the text).

**Warning:** The hints below are new and have never been proofread. Typos (or worse) are likely. In case of doubt, consult the detailed solutions.

### 12.1. Hints for Chapter 1.

*Hint to Exercise 1.2.3.* The claim of the exercise is dual to the classical fact that if $A$ is a $\mathbf{k}$-module and $m : A\otimes A \to A$ is a $\mathbf{k}$-linear map, then there exists *at most one* $\mathbf{k}$-linear map $u : \mathbf{k} \to A$ such that the diagram (1.1.2) commutes[376]. Take any proof of this latter fact, rewrite it in an "element-free" fashion[377], and "reverse all arrows". This will yield a solution to Exercise 1.2.3.

For an alternative solution, use Sweedler notation (as in (1.2.3)) as follows: The commutativity of the diagram (1.2.2) says that

$$c = \sum_{(c)} \epsilon(c_1)\, c_2 = \sum_{(c)} \epsilon(c_2)\, c_1 \qquad \text{for each } c \in C.$$

[375] Currently only the ones from Chapter 1.

[376] This fact is just the linearization of the known fact that any binary operation has at most one neutral element.

[377] This means rewriting it completely in terms of linear maps rather than elements. For example, instead of talking about $m(m(a\otimes b)\otimes c)$ for three elements $a, b, c \in A$, you should talk about the map $m\circ(m\otimes \mathrm{id}_A) : A\otimes A\otimes A \to A$ (which is, of course, the map that sends each $a\otimes b\otimes c$ to $m(m(a\otimes b)\otimes c)$). Instead of computing with elements, you should compute with maps (and commutative diagrams).

Thus, if $\epsilon_1$ and $\epsilon_2$ are two $\mathbf{k}$-linear maps $\epsilon : C \to \mathbf{k}$ such that the diagram (1.2.2) commutes, then each $c \in C$ satisfies

$$c = \sum_{(c)} \epsilon_1(c_1) c_2 = \sum_{(c)} \epsilon_1(c_2) c_1$$

and

$$c = \sum_{(c)} \epsilon_2(c_1) c_2 = \sum_{(c)} \epsilon_2(c_2) c_1 .$$

Apply $\epsilon_2$ to both sides of the equality $c = \sum_{(c)} \epsilon_1(c_2) c_1$, and apply $\epsilon_1$ to both sides of the equality $c = \sum_{(c)} \epsilon_2(c_1) c_2$. Compare the results, and conclude that $\epsilon_1 = \epsilon_2$.

*Hint to Exercise 1.3.4.* Part (a) is well-known, and part (b) is dual to part (a). So the trick is (again) to rewrite the classical proof of part (a) in an "element-free" way, and then "reversing all arrows". Alternatively, part (b) can be solved using Sweedler notation.

*Hint to Exercise 1.3.6.* Same method as for Exercise 1.3.4 above.

*Hint to Exercise 1.3.13.* (a) Use the following fact from linear algebra: If $U$, $V$, $U'$ and $V'$ are four $\mathbf{k}$-modules, and $\phi : U \to U'$ and $\psi : V \to V'$ are two surjective $\mathbf{k}$-linear maps, then the kernel of $\phi \otimes \psi : U \otimes V \to U' \otimes V'$ is

$$\ker(\phi \otimes \psi) = (\ker \phi) \otimes V + U \otimes (\ker \psi) .$$

(b) The fact just mentioned also holds if we no longer require $\phi$ and $\psi$ to be surjective, but instead require $\mathbf{k}$ to be a field.

*Hint to Exercise 1.3.18.* Let $f : V \to W$ be an invertible graded $\mathbf{k}$-linear map. Let $n \in \mathbb{N}$ and $w \in W_n$. Show that the $n$-th homogeneous component of $f^{-1}(w)$ is also a preimage of $w$ under $f$, and thus must equal $f^{-1}(w)$. Therefore, $f^{-1}(w) \in W_n$.

*Hint to Exercise 1.3.19.* (a) Define the $\mathbf{k}$-linear map $\widetilde{\Delta} : A \to A \otimes A$ by $\widetilde{\Delta}(x) = \Delta(x) - (x \otimes 1 + 1 \otimes x)$. Argue that $\widetilde{\Delta}$ is graded, so its kernel $\ker \widetilde{\Delta}$ is a graded $\mathbf{k}$-submodule of $A$. But this kernel is precisely $\mathfrak{p}$.

(b) The hard part is to show that $\epsilon(\mathfrak{p}) = 0$. To do so, consider any $x \in \mathfrak{p}$, and apply the map $\epsilon \otimes \mathrm{id}$ to both sides of the equality $\Delta(x) = x \otimes 1 + 1 \otimes x$. The result simplifies to $x = \epsilon(x) \cdot 1_A + x$. Thus, $\epsilon(x) \cdot 1_A = 0$. Now apply $\epsilon$ to this, thus obtaining $\epsilon(x) = 0$.

*Hint to Exercise 1.3.20.* (a) This follows from $1_A \in A_0$, which is part of what it means for $A$ to be a graded $\mathbf{k}$-algebra.

(b) Let $\epsilon' : A_0 \to \mathbf{k}$ be the restriction of the map $\epsilon$ to $A_0$. We know that $\epsilon'$ is surjective (since $\epsilon'(1_A) = 1_{\mathbf{k}}$), and that both $A_0$ and $\mathbf{k}$ are free $\mathbf{k}$-modules of rank 1 (since connectedness of $A$ means $A_0 \cong \mathbf{k}$ as $\mathbf{k}$-modules). It is an an easy exercise in linear algebra to conclude from these facts that $\epsilon'$ is an isomorphism. Since $\epsilon' \circ u = \mathrm{id}_{\mathbf{k}}$, we thus conclude that $u : \mathbf{k} \to A_0$ is an isomorphism as well (from $\mathbf{k}$ to $A_0$).

(c) This follows from part (b).

(e) This follows from how we solved part (b).

(d) Since the bialgebra $A$ is graded, the map $\epsilon$ must be graded. Thus, for each positive integer $n$, we have $\epsilon\left(A_n\right) \subset \mathbf{k}_n = 0$. This quickly yields $\epsilon\left(I\right) = 0$ (where $I = \bigoplus_{n>0} A_n$), hence $I \subset \ker \epsilon$. On the other hand, $\ker \epsilon \subset I$ can be shown as follows: Let $a \in \ker \epsilon$; write $a$ in the form $a = a' + a''$ for some $a' \in A_0$ and some $a'' \in I$, and then argue that $0 = \epsilon\left(a\right) = \epsilon\left(a' + a''\right) = \epsilon\left(a'\right) + \underbrace{\epsilon\left(a''\right)}_{\substack{=0 \\ (\text{since } a'' \in I \subset \ker \epsilon)}} = \epsilon\left(a'\right)$, so that $a' = 0$ by part (e) and therefore $a \in I$.

(f) This is most intuitive with Sweedler notation: Let $x \in A$. Then, $\Delta\left(x\right) = \sum_{(x)} x_1 \otimes x_2$. Applying $\operatorname{id} \otimes \epsilon$ and recalling the commutativity of (1.2.2), we thus get $x = \sum_{(x)} \epsilon\left(x_2\right) x_1$. Thus,

$$\underbrace{\Delta\left(x\right)}_{=\sum_{(x)} x_1 \otimes x_2} - \underbrace{x}_{=\sum_{(x)} \epsilon(x_2) x_1} \otimes 1 = \sum_{(x)} x_1 \otimes x_2 - \sum_{(x)} \epsilon\left(x_2\right) x_1 \otimes 1$$
$$= \sum_{(x)} \underbrace{x_1}_{\in A} \otimes \underbrace{\left(x_2 - \epsilon\left(x_2\right) \cdot 1\right)}_{\substack{\in \ker \epsilon = I \\ (\text{by part (d)})}} \in A \otimes I.$$

(g) Let $x \in I$. Proceeding similarly to part (f), show that

$$\Delta\left(x\right) - 1 \otimes x - x \otimes 1 + \epsilon\left(x\right) 1 \otimes 1 = \sum_{(x)} \underbrace{\left(x_1 - \epsilon\left(x_1\right) \cdot 1\right)}_{\substack{\in \ker \epsilon = I \\ (\text{by part (d)})}} \otimes \underbrace{\left(x_2 - \epsilon\left(x_2\right) \cdot 1\right)}_{\substack{\in \ker \epsilon = I \\ (\text{by part (d)})}} \in I \otimes I.$$

Since $x \in I = \ker \epsilon$, the $\epsilon\left(x\right) 1 \otimes 1$ term on the left hand side vanishes.

(h) This follows from part (g), since a simple homogeneity argument shows that $\left(I \otimes I\right)_n = \sum_{k=1}^{n-1} A_k \otimes A_{n-k}$.

*Hint to Exercise 1.3.24.* We need to check the four equalities $D_q \circ m = m \circ \left(D_q \otimes D_q\right)$ and $D_q \circ u = u$ and $\left(D_q \otimes D_q\right) \circ \Delta = \Delta \circ D_q$ and $\epsilon \circ D_q = \epsilon$. This can easily be done by hand (just check everything on homogeneous elements); a more erudite proof proceeds as follows: Generalize the map $D_q$ to a map $D_{q,V} : V \to V$ defined (in the same way as $D_q$) for every graded $\mathbf{k}$-module $V$, and show that these maps $D_{q,V}$ are functorial (i.e., if $f : V \to W$ is a graded $\mathbf{k}$-linear map between two graded $\mathbf{k}$-modules $V$ and $W$, then $D_{q,W} \circ f = f \circ D_{q,V}$) and "respect tensor products" (i.e., we have $D_{q,V\otimes W} = D_{q,V} \otimes D_{q,W}$ for any two graded $\mathbf{k}$-modules $V$ and $W$). The four equalities are then easily obtained from these two facts, without having to introduce elements.

*Hint to Exercise 1.3.26.* (a) Our definition of the $\mathbf{k}$-coalgebra $A \otimes B$ yields

$$\Delta_{A\otimes B} = \left(\operatorname{id}_A \otimes T_{A,B} \otimes \operatorname{id}_B\right) \circ \left(\Delta_A \otimes \Delta_B\right) \qquad \text{and} \qquad \epsilon_{A\otimes B} = \theta \circ \left(\epsilon_A \otimes \epsilon_B\right),$$

where $\theta$ is the canonical $\mathbf{k}$-module isomorphism $\mathbf{k} \otimes \mathbf{k} \to \mathbf{k}$. All maps on the right hand sides are $\mathbf{k}$-algebra homomorphisms (see Exercise 1.3.6(a)); thus, so are $\Delta_{A\otimes B}$ and $\epsilon_{A\otimes B}$.

(b) Straightforward.

*Hint to Exercise 1.4.2.* Simple computation (either element-free or with Sweedler notation).

*Hint to Exercise 1.4.4.* Simple computation (either element-free or with Sweedler notation).

*Hint to Exercise 1.4.5.* Straightforward computation, best done using Sweedler notation.

*Hint to Exercise 1.4.15.* Use Exercise 1.4.2.

*Hint to Exercise 1.4.19.* The following is more context than hint (see the last paragraph for an actual hint).

It is easiest to prove this by calculating with elements. To wit, in order to prove that two **k**-linear maps from $A^{\otimes(k+1)}$ are identical, it suffices to show that they agree on all pure tensors $a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1} \in A^{\otimes(k+1)}$. But the recursive definition of $m^{(k)}$ shows that

$$m^{(k)}\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right) = a_1\left(a_2\left(a_3\left(\cdots\left(a_k a_{k+1}\right)\cdots\right)\right)\right) \tag{12.1.1}$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$. Now, the "general associativity" law (a fundamental result in abstract algebra, commonly used without mention) says that, because the multiplication of $A$ is associative, the parentheses in the product $a_1\left(a_2\left(a_3\left(\cdots\left(a_k a_{k+1}\right)\cdots\right)\right)\right)$ can be omitted without making it ambiguous – i.e., any two ways of parenthesizing the product $a_1 a_2 \cdots a_{k+1}$ evaluate to the same result. (For example, for $k = 4$, this says that

$$a_1\left(a_2\left(a_3 a_4\right)\right) = a_1\left(\left(a_2 a_3\right) a_4\right) = \left(a_1 a_2\right)\left(a_3 a_4\right) = \left(a_1\left(a_2 a_3\right)\right) a_4 = \left(\left(a_1 a_2\right) a_3\right) a_4$$

for all $a_1, a_2, a_3, a_4 \in A$.) Thus, we can rewrite (12.1.1) as

$$m^{(k)}\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right) = a_1 a_2 \cdots a_{k+1}.$$

Using this formula, all four parts of the exercise become trivial: For example, part (a) simply says that

$$a_1 a_2 \cdots a_{k+1} = \left(a_1 a_2 \cdots a_{i+1}\right)\left(a_{i+2} a_{i+3} \cdots a_{k+1}\right)$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$, because we have

$$\begin{aligned}&\left(m \circ \left(m^{(i)} \otimes m^{(k-1-i)}\right)\right)\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right)\\ &= \left(a_1 a_2 \cdots a_{i+1}\right)\left(a_{i+2} a_{i+3} \cdots a_{k+1}\right).\end{aligned}$$

Likewise, part (c) simply says that

$$a_1 a_2 \cdots a_{k+1} = a_1 a_2 \cdots a_i\left(a_{i+1} a_{i+2}\right) a_{i+3} a_{i+4} \cdots a_{k+1}$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$. Parts (b) and (d) are particular cases of parts (a) and (c), respectively.

Of course, in order for this to be a complete solution, you have to prove the "general associativity" law used above. It turns out that doing so is not much easier than solving the exercise from scratch (in fact, part (a) of the exercise is an equivalent form of the "general associativity" law). So we can just as well start from scratch and solve part (a) directly by induction on $k$, then derive part (b) as its particular case, then solve part (c) by induction on $k$ using the result of part (b), then derive part (d) as a particular case of (c).

*Hint to Exercise 1.4.20.* If you have solved Exercise 1.4.19 in an "element-free" way, then you can reverse all arrows in said solution and thus obtain a solution to Exercise 1.4.20.

*Hint to Exercise 1.4.22.* (a) Induction on $k$, using Exercise 1.3.6(b).

(b) This is dual to (a).

(d) For every $\mathbf{k}$-coalgebra $C$, consider the map $\Delta_C^{(k)} : C \to C^{\otimes(k+1)}$ (this is the map $\Delta^{(k)}$ defined in Exercise 1.4.20). This map $\Delta_C^{(k)}$ is clearly functorial in $C$. By this we mean that if $C$ and $D$ are any two $\mathbf{k}$-coalgebras, and $f : C \to D$ is any $\mathbf{k}$-coalgebra homomorphism, then the diagram

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C^{(k)}"] & D \arrow[d, "\Delta_D^{(k)}"] \\ C^{\otimes(k+1)} \arrow[r, "f^{\otimes(k+1)}"'] & D^{\otimes(k+1)} \end{tikzcd}$$

commutes. Now, apply this to $C = H^{\otimes(\ell+1)}$, $D = H$ and $f = m_H^{(\ell)}$ (using part (a)).

(c) This is dual to (d).

*Hint to Exercise 1.4.23.* Induction on $k$.

*Hint to Exercise 1.4.28.* This is dual to Proposition 1.4.10, so the usual strategy (viz., rewriting element-free and reversing all arrows) applies.

*Hint to Exercise 1.4.29.* (a) A straightforward generalization of the proof of Proposition 1.4.10 (which corresponds to the particular case when $C = A$ and $r = \mathrm{id}$) does the trick.

(b) This is dual to (a).

(c) Easy.

(d) Apply Exercise 1.4.29(a) to $C = A$ and $r = \mathrm{id}_A$; then, apply Proposition 1.4.26(a) to $H = A$ and $\alpha = S$.

(e) Let $s : C \to A$ be the $\mathbf{k}$-linear map that sends every homogeneous element $c \in C_n$ (for every $n \in \mathbb{N}$) to the $n$-th homogeneous component of $r^{\star(-1)}(c)$. Then, $s$ is graded, and (this takes some work) is also a $\star$-inverse to $r$. But $r$ has only one $\star$-inverse.

*Hint to Exercise 1.4.30.* (a) Rewrite the assumption as $m \circ (P \otimes \mathrm{id}) \circ T \circ \Delta = u \circ \epsilon$, where $T$ is the twist map $T_{A,A}$. Proposition 1.4.10 leads to $m \circ (S \otimes S) = S \circ m \circ T$ and $u = S \circ u$. Exercise 1.4.28 leads to $(S \otimes S) \circ \Delta = T \circ \Delta \circ S$ and $\epsilon \circ S = \epsilon$. Use these to show that $(P \circ S) \star S = u \circ \epsilon$, so that $P \circ S = \mathrm{id}$. Also, show that $S \star (S \circ P) = u \circ \epsilon$, so that $S \circ P = \mathrm{id}$.

(b) Similar to (a).

(c) Let $A$ be a connected graded Hopf algebra. Just as a left $\star$-inverse $S$ to $\mathrm{id}_A$ has been constructed in the proof of Proposition 1.4.16, we could construct a $\mathbf{k}$-linear map $P : A \to A$ such that every $a \in A$ satisfies $\sum_{(a)} P(a_2) \cdot a_1 = u(\epsilon(a))$. Now apply part (a).

*Hint to Exercise 1.4.32.* Since $D$ is a direct summand of $C$, we can identify the tensor products $D \otimes C$, $C \otimes D$ and $D \otimes D$ with their canonical images inside $C \otimes C$. Now, we can show that $\Delta(D) \subset D \otimes D$ as follows: Let $p : C \to D$ be the canonical projection from $C$ onto its direct summand

$D$; then, $\Delta(D) \subset D \otimes C$ shows that $(p \otimes \operatorname{id}) \circ \Delta = \Delta$, and $\Delta(D) \subset C \otimes D$ shows that $(\operatorname{id} \otimes p) \circ \Delta = \Delta$. Hence,

$$\underbrace{(p \otimes p)}_{=(p\otimes \operatorname{id})\circ(\operatorname{id}\otimes p)} \circ \Delta = (p \otimes \operatorname{id}) \circ \underbrace{(\operatorname{id} \otimes p) \circ \Delta}_{=\Delta} = (p \otimes \operatorname{id}) \circ \Delta = \Delta.$$

This yields $\Delta(D) \subset D \otimes D$. Hence, we get a map $\Delta_D : D \to D \otimes D$ by restricting $\Delta$. Obviously, the map $\epsilon : C \to \mathbf{k}$ restricts to a map $\epsilon_D : D \to \mathbf{k}$ as well. It remains to check the commutativity of the diagrams (1.2.1) and (1.2.2) for $D$ instead of $C$; but this is inherited from $C$.

*Hint to Exercise 1.4.33.* (a) Let $\widetilde{f} = (\operatorname{id}_C \otimes f \otimes \operatorname{id}_C) \circ \Delta^{(2)} : C \to C \otimes U \otimes C$; then, $K = \ker \widetilde{f}$. Show (by manipulation of maps, using Exercise 1.4.20(b)) that $(\operatorname{id}_C \otimes \operatorname{id}_U \otimes \Delta) \circ \widetilde{f} = \left(\widetilde{f} \otimes \operatorname{id}_C\right) \circ \Delta$. Now,

$$K = \ker \widetilde{f} \subset \ker \left( \underbrace{(\operatorname{id}_C \otimes \operatorname{id}_U \otimes \Delta) \circ \widetilde{f}}_{=\left(\widetilde{f}\otimes \operatorname{id}_C\right)\circ\Delta} \right) = \ker\left(\left(\widetilde{f} \otimes \operatorname{id}_C\right) \circ \Delta\right)$$
$$= \Delta^{-1}\left(\ker\left(\widetilde{f} \otimes \operatorname{id}_C\right)\right)$$

and therefore

$$\Delta(K) \subset \ker\left(\widetilde{f} \otimes \operatorname{id}_C\right) = \underbrace{\left(\ker \widetilde{f}\right)}_{=K} \otimes C$$
$$\text{(since tensoring over a field is left-exact)}$$
$$= K \otimes C.$$

Similarly, $\Delta(K) \subset C \otimes K$. Now, apply Exercise 1.4.32 to $D = K$.

(b) Let $E$ be a $\mathbf{k}$-subcoalgebra of $C$ which is a subset of $\ker f$. Then, $\Delta^{(2)}(E) \subset E \otimes E \otimes E$ (since $E$ is a subcoalgebra) and $f(E) = 0$ (since $E \subset \ker f$). Now,

$$\left((\operatorname{id}_C \otimes f \otimes \operatorname{id}_C) \circ \Delta^{(2)}\right)(E) = (\operatorname{id}_C \otimes f \otimes \operatorname{id}_C) \left( \underbrace{\Delta^{(2)}(E)}_{\subset E\otimes E\otimes E} \right)$$
$$\subset (\operatorname{id}_C \otimes f \otimes \operatorname{id}_C)(E \otimes E \otimes E)$$
$$= \operatorname{id}_C(E) \otimes \underbrace{f(E)}_{=0} \otimes \operatorname{id}_C(E) = 0.$$

Hence, $E \subset \ker\left((\operatorname{id}_C \otimes f \otimes \operatorname{id}_C) \circ \Delta^{(2)}\right) = K$.

[*Remark:* Exercise 1.4.33(a) would not hold if we allowed $\mathbf{k}$ to be an arbitrary commutative ring rather than a field.]

*Hint to Exercise 1.4.34.* (a) Here is Takeuchi's argument: We know that the map $h\mid_{C_0} \in \operatorname{Hom}(C_0, A)$ is $\star$-invertible; let $\widetilde{g}$ be its $\star$-inverse. Extend $\widetilde{g}$ to a $\mathbf{k}$-linear map $g : C \to A$ by defining it as 0 on every $C_n$ for $n > 0$. It is then easy to see that $(h \star g)\mid_{C_0} = (g \star h)\mid_{C_0} = (u\epsilon)\mid_{C_0}$. This allows us to assume WLOG that $h\mid_{C_0} = (u\epsilon)\mid_{C_0}$ (because once we know that $h \star g$ and $g \star h$ are $\star$-invertible, it follows that so is $h$). Assuming this, we conclude that $h - u\epsilon$ annihilates $C_0$. Define $f$ as $h - u\epsilon$. Now, we can proceed as in the proof of Proposition 1.4.24 to show that $\sum_{k\geq 0}(-1)^k f^{\star k}$ is a well-defined linear map $C \to A$ and a two-sided $\star$-inverse for $h$. Thus, $h$ is $\star$-invertible, and part (a) of the exercise is proven. (An alternative proof proceeds by mimicking the proof of Proposition 1.4.16, again by first assuming WLOG that $h\mid_{C_0} = (u\epsilon)\mid_{C_0}$.)

(b) Apply part (a) to $C = A$ and the map $\mathrm{id}_A : A \to A$.

(c) Applying part (b), we see that $A$ is a Hopf algebra (since $A_0 = \mathbf{k}$ is a Hopf algebra) in the setting of Proposition 1.4.16. This yields the existence of the antipode. Its uniqueness is trivial, and its gradedness follows from Exercise 1.4.29(e).

*Hint to Exercise 1.4.35.* (a) Let $I$ be a two-sided coideal of $A$ such that $I \cap \mathfrak{p} = 0$ and such that $I = \bigoplus_{n\geq 0}(I \cap A_n)$. Let $I_n = I \cap A_n$ for every $n \in \mathbb{N}$. Then, $I = \bigoplus_{n\geq 0} I_n$. Since $I$ is a two-sided coideal, we have $\epsilon(I) = 0$.

We want to prove that $I = 0$. It clearly suffices to show that every $n \in \mathbb{N}$ satisfies $I_n = 0$ (since $I = \bigoplus_{n\geq 0} I_n$). We shall show this by strong induction: We fix an $N \in \mathbb{N}$, and we assume (as induction hypothesis) that $I_n = 0$ for all $n < N$. We must prove that $I_N = 0$.

Fix $i \in I_N$; we aim to show that $i = 0$. We have $i \in I_N \subset A_N$ and thus $\Delta(i) \in (A \otimes A)_N$ (since $\Delta$ is a graded map). On the other hand, from $i \in I_N \subset I$, we obtain

$$\begin{aligned}\Delta(i) \in \Delta(I) &\subset \underbrace{I}_{=\bigoplus_{n\geq 0} I_n} \otimes \underbrace{A}_{=\bigoplus_{m\geq 0} A_m} + \underbrace{A}_{=\bigoplus_{m\geq 0} A_m} \otimes \underbrace{I}_{=\bigoplus_{n\geq 0} I_n} \\ &\qquad \text{(since } I \text{ is a two-sided coideal)} \\ &= \sum_{(m,n)\in\mathbb{N}^2} I_n \otimes A_m + \sum_{(m,n)\in\mathbb{N}^2} A_m \otimes I_n.\end{aligned}$$

Combining this with $\Delta(i) \in (A \otimes A)_N$, we obtain

$$\begin{aligned}\Delta(i) &\in \sum_{\substack{(m,n)\in\mathbb{N}^2;\\ m+n=N}} I_n \otimes A_m + \sum_{\substack{(m,n)\in\mathbb{N}^2;\\ m+n=N}} A_m \otimes I_n \\ &\qquad \left(\text{since } I_n \otimes A_m \text{ and } A_m \otimes I_n \text{ are subsets of } (A\otimes A)_{n+m}\right) \\ &= \sum_{n=0}^{N} I_n \otimes A_{N-n} + \sum_{n=0}^{N} A_{N-n} \otimes I_n \\ &= I_N \otimes \underbrace{A_0}_{=\mathbf{k}\cdot 1_A} + \sum_{n=0}^{N-1} \underbrace{I_n}_{\substack{=0\\ \text{(by the induction}\\ \text{hypothesis)}}} \otimes A_{N-n} \\ &\qquad + \underbrace{A_0}_{=\mathbf{k}\cdot 1_A} \otimes I_N + \sum_{n=0}^{N-1} A_{N-n} \otimes \underbrace{I_n}_{\substack{=0\\ \text{(by the induction}\\ \text{hypothesis)}}} \\ &= I_N \otimes (\mathbf{k}\cdot 1_A) + (\mathbf{k}\cdot 1_A) \otimes I_N.\end{aligned}$$

In other words,

$$\Delta(i) = j \otimes 1_A + 1_A \otimes k \qquad (12.1.2)$$

for some $j, k \in I_N$. By applying $\epsilon \otimes \mathrm{id}$ to both sides of this equality, and recalling the commutativity of (1.2.2), we obtain $i = \epsilon(j) 1_A + k$. But $\epsilon(j) = 0$ (since $j \in I_N \subset I$, so $\epsilon(j) \in \epsilon(I) = 0$), so this simplifies to $i = k$. Similarly, $i = j$. Hence, (12.1.2) rewrites as $\Delta(i) = i \otimes 1_A + 1_A \otimes i$, which shows that $i \in \mathfrak{p}$, hence $i \in I \cap \mathfrak{p} = 0$ and thus $i = 0$. This was for proved for each $i \in I_N$, so we obtain $I_N = 0$. This completes the induction step, and so part (a) is solved.

(b) Exercise 1.3.13(a) shows that $\ker f$ is a two-sided coideal of $C$. If $f\mid_{\mathfrak{p}}$ is injective, then $(\ker f) \cap \mathfrak{p} = 0$. Now, apply part (a) of the current exercise to $I = \ker f$.

(c) Proceed as in part (b), but use Exercise 1.3.13(b) instead of Exercise 1.3.13(a).

*Hint to Exercise 1.5.4.* (a) Straightforward (if slightly laborious) computations.

(b) Direct verification (the hard part of which has been done in (1.3.7) already).

(c) For every subset $S$ of a $\mathbf{k}$-module $U$, we let $\langle S\rangle$ denote the $\mathbf{k}$-submodule of $U$ spanned by $S$. Our definition of $J$ thus becomes

$$J = T(\mathfrak{p}) \cdot C \cdot T(\mathfrak{p}), \tag{12.1.3}$$

where $C = \langle xy - yx - [x, y] \mid x, y \in \mathfrak{p}\rangle$. A simple computation shows that each element of $C$ is primitive. Hence,

$$\Delta(C) \subset C \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes C.$$

Applying $\Delta$ to both sides of (12.1.3), and recalling that $\Delta$ is a $\mathbf{k}$-algebra homomorphism, we find

$$\begin{aligned}
\Delta(J) &= \underbrace{\Delta(T(\mathfrak{p}))}_{\subset T(\mathfrak{p})\otimes T(\mathfrak{p})} \cdot \underbrace{\Delta(C)}_{\subset C\otimes T(\mathfrak{p})+T(\mathfrak{p})\otimes C} \cdot \underbrace{\Delta(T(\mathfrak{p}))}_{\subset T(\mathfrak{p})\otimes T(\mathfrak{p})} \\
&\subset (T(\mathfrak{p}) \otimes T(\mathfrak{p})) \cdot (C \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes C) \cdot (T(\mathfrak{p}) \otimes T(\mathfrak{p})) \\
&= J \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes J.
\end{aligned}$$

A similar (but simpler) argument shows $\epsilon(J) = 0$. Thus, $J$ is a two-sided coideal of $T(\mathfrak{p})$. This yields that $T(\mathfrak{p})/J$ is a $\mathbf{k}$-bialgebra.

(d) We need to show that $S(J) \subset J$. This can be done in a similar way as we proved $\Delta(J) \subset J \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes J$ in part (c), once you know (from Proposition 1.4.10) that the antipode $S$ of $T(\mathfrak{p})$ is a $\mathbf{k}$-algebra anti-homomorphism.

*Hint to Exercise 1.5.5.* Straightforward and easy verification.

*Hint to Exercise 1.5.6.* Straightforward and easy verification. Parts (a) and (b) are dual, of course.

*Hint to Exercise 1.5.8.* (a) Straightforward and easy verification.

(b) The dual says the following: Let $A$ and $B$ be two $\mathbf{k}$-coalgebras, at least one of which is cocommutative. Prove that the $\mathbf{k}$-coalgebra anti-homomorphisms from $A$ to $B$ are the same as the $\mathbf{k}$-coalgebra homomorphisms from $A$ to $B$.

*Hint to Exercise 1.5.9.* For every $1 \leq i < j \leq k$, let $t_{i,j}$ be the transposition in $\mathfrak{S}_k$ which transposes $i$ with $j$. It is well-known that the symmetric group $\mathfrak{S}_k$ is generated by the transpositions $t_{i,i+1}$ with $i$ ranging over $\{1, 2, \ldots, k-1\}$. However, we have $(\rho(\pi)) \circ (\rho(\psi)) = \rho(\pi\psi)$ for any two elements $\pi$ and $\psi$ of $\mathfrak{S}_k$. Thus, it suffices to check that

$$m^{(k-1)} \circ (\rho(t_{i,i+1})) = m^{(k-1)} \qquad \text{for all } i \in \{1, 2, \ldots, k-1\}.$$

But this is not hard to check using $m^{(k-1)} = m^{(k-2)} \circ (\mathrm{id}_{A^{\otimes(i-1)}} \otimes m \otimes \mathrm{id}_{A^{\otimes(k-1-i)}})$ (a consequence of Exercise 1.4.19(c)) and $m \circ T = m$.

*Hint to Exercise 1.5.10.* Here is the dual statement: Let $C$ be a cocommutative $\mathbf{k}$-coalgebra, and let $k \in \mathbb{N}$. The symmetric group $\mathfrak{S}_k$ acts on the $k$-fold tensor power $C^{\otimes k}$ by permuting the tensor factors: $\sigma(v_1 \otimes v_2 \otimes \cdots \otimes v_k) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(k)}$ for all $v_1, v_2, \ldots, v_k \in C$ and $\sigma \in \mathfrak{S}_k$. For every $\pi \in \mathfrak{S}_k$, denote by $\rho(\pi)$ the action of $\pi$ on $C^{\otimes k}$ (this is an endomorphism of $C^{\otimes k}$). Show that every $\pi \in \mathfrak{S}_k$ satisfies $(\rho(\pi)) \circ \Delta^{(k-1)} = \Delta^{(k-1)}$. (Recall that $\Delta^{(k-1)} : C \to C^{\otimes k}$ is defined as in Exercise 1.4.20 for $k \geq 1$, and by $\Delta^{(-1)} = \epsilon : C \to \mathbf{k}$ for $k = 0$.)

*Hint to Exercise 1.5.11.* (a) Use Exercise 1.5.6(b) and Exercise 1.3.6(a) to represent $f \star g$ as a composition of three $\mathbf{k}$-algebra homomorphisms.

(b) Induction on $k$, using part (a).

(c) Use Proposition 1.4.10, Proposition 1.4.26(a) and the easy fact that a composition of a $\mathbf{k}$-algebra homomorphism with a $\mathbf{k}$-algebra anti-homomorphism (in either order) always is a $\mathbf{k}$-algebra anti-homomorphism.

(d) Use Exercise 1.5.6(b). Then, proceed by induction on $k$ as in the solution of Exercise 1.4.22(a).

(e) Use Proposition 1.4.3.

(f) Let $H$ be a commutative $\mathbf{k}$-bialgebra. Let $k$ and $\ell$ be two nonnegative integers. Then, Exercise 1.5.11(b) (applied to $A = H$ and $f_i = \mathrm{id}_H$) yields that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism $H \to H$. Now, apply Exercise 1.5.11(e) to $H$, $H$, $H$, $H$, $\ell$, $\mathrm{id}_H$, $\mathrm{id}_H^{\star k}$ and $\mathrm{id}_H$ instead of $C$, $C'$, $A$, $A'$, $k$, $f_i$, $\alpha$ and $\gamma$.

(g) This is an exercise in bootstrapping. First, let $k \in \mathbb{N}$. Then, part (b) of this exercise shows that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism. Use this together with part (c) to conclude that $\mathrm{id}_H^{\star k} \circ S$ is again a $\mathbf{k}$-algebra homomorphism and a $\star$-inverse to $\mathrm{id}_H^{\star k}$; thus, $\mathrm{id}_H^{\star k} \circ S = \left(\mathrm{id}_H^{\star k}\right)^{\star(-1)} = \mathrm{id}_H^{\star(-k)}$, and this map $\mathrm{id}_H^{\star(-k)}$ is a $\mathbf{k}$-algebra homomorphism.

Now forget that we fixed $k$. We thus have shown that $\mathrm{id}_H^{\star k}$ and $\mathrm{id}_H^{\star(-k)}$ are $\mathbf{k}$-algebra homomorphisms for each $k \in \mathbb{N}$. In other words,

$$\mathrm{id}_H^{\star k} \text{ is a } \mathbf{k}\text{-algebra homomorphism for every } k \in \mathbb{Z}. \tag{12.1.4}$$

Furthermore, we have proved the equality $\mathrm{id}_H^{\star k} \circ S = \mathrm{id}_H^{\star(-k)}$ for each $k \in \mathbb{N}$. Repeating the proof of this, but now taking $k \in \mathbb{Z}$ instead of $k \in \mathbb{N}$, we conclude that it also holds for each $k \in \mathbb{Z}$ (since we already have proved (12.1.4)). In other words,

$$\mathrm{id}_H^{\star(-k)} = \mathrm{id}_H^{\star k} \circ S \qquad \text{for every } k \in \mathbb{Z}. \tag{12.1.5}$$

Now, fix two integers $k$ and $\ell$. From (12.1.4), we know that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism. Hence, if $\ell$ is nonnegative, then we can prove $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star (k\ell)}$ just as we did in the solution to Exercise 1.5.11(f). But the case when $\ell$ is negative can be reduced to the previous case by applying (12.1.5) (once to $-\ell$ instead of $k$, and once again to $-k\ell$ instead of $k$). Thus, in each case, we obtain $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star (k\ell)}$.

(h) The dual of Exercise 1.5.11(a) is the following exercise:

> If $H$ is a $\mathbf{k}$-bialgebra and $C$ is a cocommutative $\mathbf{k}$-coalgebra, and if $f$ and $g$ are two $\mathbf{k}$-coalgebra homomorphisms $C \to H$, then prove that $f \star g$ also is a $\mathbf{k}$-coalgebra homomorphism $C \to H$.

The dual of Exercise 1.5.11(b) is the following exercise:

> If $H$ is a $\mathbf{k}$-bialgebra and $C$ is a cocommutative $\mathbf{k}$-coalgebra, and if $f_1, f_2, \ldots, f_k$ are several $\mathbf{k}$-coalgebra homomorphisms $C \to H$, then prove that $f_1 \star f_2 \star \cdots \star f_k$ also is a $\mathbf{k}$-coalgebra homomorphism $C \to H$.

The dual of Exercise 1.5.11(c) is the following exercise:

> If $H$ is a Hopf algebra and $C$ is a cocommutative $\mathbf{k}$-coalgebra, and if $f : C \to H$ is a $\mathbf{k}$-coalgebra homomorphism, then prove that $S \circ f : C \to H$ (where $S$ is the antipode of $H$) is again a $\mathbf{k}$-coalgebra homomorphism, and is a $\star$-inverse to $f$.

The dual of Exercise 1.5.11(d) is the following exercise:

> If $C$ is a cocommutative $\mathbf{k}$-coalgebra, then show that $\Delta^{(k)}$ is a $\mathbf{k}$-coalgebra homomorphism for every $k \in \mathbb{N}$. (The map $\Delta^{(k)} : C \to C^{\otimes (k+1)}$ is defined as in Exercise 1.4.20.)

The dual of Exercise 1.5.11(e) is Exercise 1.5.11(e) itself (up to renaming objects and maps).

The dual of Exercise 1.5.11(f) is the following exercise:

> If $H$ is a cocommutative $\mathbf{k}$-bialgebra, and $k$ and $\ell$ are two nonnegative integers, then prove that $\mathrm{id}_H^{\star \ell} \circ \mathrm{id}_H^{\star k} = \mathrm{id}_H^{\star (\ell k)}$.

The dual of Exercise 1.5.11(g) is the following exercise:

> If $H$ is a cocommutative $\mathbf{k}$-Hopf algebra, and $k$ and $\ell$ are two integers, then prove that $\mathrm{id}_H^{\star \ell} \circ \mathrm{id}_H^{\star k} = \mathrm{id}_H^{\star (\ell k)}$.

*Hint to Exercise 1.5.13.* This is dual to Corollary 1.4.12 (but can also easily be shown using Exercise 1.4.29(b), Exercise 1.5.8(b) and Proposition 1.4.26(b)).

*Hint to Exercise 1.5.14.* (a) This can be proved computationally (using Sweedler notation), but there is a nicer argument as well:

A *coderivation* of a $\mathbf{k}$-coalgebra $(C, \Delta, \epsilon)$ is defined as a $\mathbf{k}$-linear map $F : C \to C$ such that $\Delta \circ F = (F \otimes \mathrm{id} + \mathrm{id} \otimes F) \circ \Delta$. (The reader can check that this axiom is the result of writing the axiom for a derivation in element-free terms and reversing all arrows. Nothing less should be expected.) It is easy to see that $E$ is a coderivation. Hence, it will be enough to check that $(S \star f)(a)$ and $(f \star S)(a)$ are primitive whenever $f : A \to A$ is a coderivation and $a \in A$. So fix a coderivation $f : A \to A$. Notice that the antipode $S$ of $A$ is a coalgebra anti-endomorphism (by

Exercise 1.4.28), thus a coalgebra endomorphism (by Exercise 1.5.8(b)). Thus, $\Delta \circ S = (S \otimes S) \circ \Delta$. Moreover, $\Delta : A \to A \otimes A$ is a coalgebra homomorphism (by Exercise 1.5.6(a)) and an algebra homomorphism (since $A$ is a bialgebra). Applying (1.4.2) to $A \otimes A$, $A$, $A$, $\Delta$, $\operatorname{id}_A$, $S$ and $f$ instead of $A'$, $C$, $C'$, $\alpha$, $\gamma$, $f$ and $g$, we obtain

$$\begin{aligned}
\Delta \circ (S \star f) &= \underbrace{(\Delta \circ S)}_{=(S \otimes S)\circ\Delta} \star \underbrace{(\Delta \circ f)}_{\substack{=(f \otimes \operatorname{id} + \operatorname{id} \otimes f)\circ\Delta \\ \text{(since } f \text{ is a coderivation)}}} \\
&= ((S \otimes S) \circ \Delta) \star ((f \otimes \operatorname{id} + \operatorname{id} \otimes f) \circ \Delta) \\
&= ((S \otimes S) \star (f \otimes \operatorname{id} + \operatorname{id} \otimes f)) \circ \Delta \\
&= \underbrace{((S \otimes S) \star (f \otimes \operatorname{id}))}_{\substack{=(S \star f)\otimes(S \star \operatorname{id}) \\ \text{(by Exercise 1.4.4(a))}}} \circ \Delta + \underbrace{((S \otimes S) \star (\operatorname{id} \otimes f))}_{\substack{=(S \star \operatorname{id})\otimes(S \star f) \\ \text{(by Exercise 1.4.4(a))}}} \circ \Delta \\
&= \left( (S \star f) \otimes \underbrace{(S \star \operatorname{id})}_{=u\epsilon} \right) \circ \Delta + \left( \underbrace{(S \star \operatorname{id})}_{=u\epsilon} \otimes (S \star f) \right) \circ \Delta \\
&= ((S \star f) \otimes u\epsilon) \circ \Delta + (u\epsilon \otimes (S \star f)) \circ \Delta.
\end{aligned}$$

Hence, every $a \in A$ satisfies

$$\begin{aligned}
(\Delta \circ (S \star f))(a) &= (((S \star f) \otimes u\epsilon) \circ \Delta + (u\epsilon \otimes (S \star f)) \circ \Delta)(a) \\
&= (S \star f)(a) \otimes 1 + 1 \otimes (S \star f)(a)
\end{aligned}$$

(after some brief computations using (1.2.2)). In other words, for every $a \in A$, the element $(S \star f)(a)$ is primitive. Similarly the same can be shown for $(f \star S)(a)$, and so we are done.

(b) is a very simple computation. (Alternatively, the $(S \star E)(p) = E(p)$ part follows from applying part (c) to $a = 1$, and similarly one can show $(E \star S)(p) = E(p)$.)

(c) This is another computation, using Proposition 1.4.17 and the (easy) observation that $E$ is a derivation of the algebra $A$.

(d) Assume that the graded algebra $A = \bigoplus_{n \geq 0} A_n$ is connected and that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let $B$ be the $\mathbf{k}$-subalgebra of $A$ generated by $\mathfrak{p}$. In order to prove part (d), we need to show that $A \subset B$. Clearly, it suffices to show that $A_n \subset B$ for every $n \in \mathbb{N}$. We prove this by strong induction on $n$; thus, we fix some $n \in \mathbb{N}$, and assume as induction hypothesis that $A_m \subset B$ for every $m < n$. Our goal is then to show that $A_n \subset B$. This being trivial for $n = 0$ (since $A$ is connected), we WLOG assume that $n > 0$. Let $a \in A_n$. Part (a) of this exercise yields $(S \star E)(a) \in \mathfrak{p} \subset B$. On the other hand, Exercise 1.3.20(h) (applied to $x = a$) yields

$$\Delta(a) \in 1 \otimes a + a \otimes 1 + \sum_{k=1}^{n-1} A_k \otimes A_{n-k}.$$

Hence, from the definition of convolution, we obtain

$$\begin{aligned}(S\star E)(a) &\in \underbrace{S(1)}_{=1}E(a)+S(a)\underbrace{E(1)}_{=0}+\underbrace{(m\circ(S\otimes E))\left(\sum_{k=1}^{n-1}A_k\otimes A_{n-k}\right)}_{=\sum_{k=1}^{n-1}S(A_k)E(A_{n-k})}\\ &= E(a)+\sum_{k=1}^{n-1}\underbrace{S(A_k)}_{\substack{\subset A_k\\ \text{(since } S \text{ is graded)}}}\underbrace{E(A_{n-k})}_{\substack{\subset A_{n-k}\subset B\\ \text{(by the induction}\\ \text{hypothesis)}}}\\ &\subset E(a)+\sum_{k=1}^{n-1}\underbrace{A_k}_{\substack{\subset B\\ \text{(by the induction}\\ \text{hypothesis)}}}B\subset E(a)+B\end{aligned}$$

(since $B$ is a subalgebra). Hence, $E(a)\in(S\star E)(a)+B=B$ (since $(S\star E)(a)\in B$). Since $E(a)=na$, this becomes $na\in B$, thus $a\in B$ (since $\mathbb{Q}$ is a subring of $\mathbf{k}$). Since we have shown this for each $a\in A_n$, we thus obtain $A_n\subset B$, and our induction is complete.

This solution of part (d) is not the most generalizable one – for instance, (d) also holds if $A$ is connected filtered instead of connected graded, and then a different argument is necessary. This is a part of the Cartier-Milnor-Moore theorem, and appears e.g. in [60, §3.2].

(e) If $a\in T(V)$ is homogeneous of positive degree and $p\in V$, then part (c) quickly yields $(S\star E)(ap)=[(S\star E)(a),p]$. This allows proving (e) by induction over $n$, with the induction base $n=1$ being a consequence of part (b).

*Hint to Exercise 1.6.1.* (a) This can be done by diagram chasing. For example, if $\mathfrak{m}$ denotes the map $\Delta_C^*\circ\rho_{C,C}:C^*\otimes C^*\to C^*$, then the diagram

$$\begin{tikzcd}
 & & & C^*\otimes C^*\otimes C^* \arrow[dll, "\rho_{C,C}\otimes\mathrm{id}"'] \arrow[drr, "\mathrm{id}\otimes\rho_{C,C}"] \arrow[ddlll, bend right, "\mathfrak{m}\otimes\mathrm{id}"'] \arrow[ddrrr, bend left, "\mathrm{id}\otimes\mathfrak{m}"] & & & \\
 & (C\otimes C)^*\otimes C^* \arrow[dl, "\Delta_C^*\otimes\mathrm{id}"'] \arrow[drr, "\rho_{C\otimes C,C}"] & & & & C^*\otimes(C\otimes C)^* \arrow[dll, "\rho_{C,C\otimes C}"'] \arrow[dr, "\mathrm{id}\otimes\Delta_C^*"] & \\
C^*\otimes C^* \arrow[dr, "\rho_{C,C}"] \arrow[ddrrr, bend right, "\mathfrak{m}"'] & & & (C\otimes C\otimes C)^* \arrow[dll, "(\Delta_C\otimes\mathrm{id})^*"'] \arrow[drr, "(\mathrm{id}\otimes\Delta_C)^*"] & & & C^*\otimes C^* \arrow[dl, "\rho_{C,C}"'] \arrow[ddlll, bend left, "\mathfrak{m}"] \\
 & (C\otimes C)^* \arrow[drr, "\Delta_C^*"] & & & & (C\otimes C)^* \arrow[dll, "\Delta_C^*"'] & \\
 & & & C^* & & &
\end{tikzcd}$$

is commutative (since each of its little triangles and squares is); thus, $\mathfrak{m}\circ(\mathfrak{m}\otimes\mathrm{id})=\mathfrak{m}\circ(\mathrm{id}\otimes\mathfrak{m})$ for $\mathfrak{m}$. This proves that the diagram (1.1.1) commutes for our algebra $C^*$. The commutativity of (1.1.2) is obtained similarly.

Alternatively, we could also solve part (a) trivially by first solving part (b) and then recalling Exercise 1.4.2.

(b) Straightforward verification on pure tensors.

(c) Let $C = \bigoplus_{n \geq 0} C_n$ be a graded $\mathbf{k}$-coalgebra. For every $n \in \mathbb{N}$, we identify $(C_n)^*$ with a $\mathbf{k}$-submodule of $C^*$, namely with the $\mathbf{k}$-submodule $\{f \in C^* \mid f(C_p) = 0 \text{ for all } p \in \mathbb{N} \text{ satisfying } p \neq n\}$. By the definition of $C^o$, we have $C^o = \bigoplus_{n \geq 0} (C_n)^*$. Hence, it remains to show that $(C_a)^* (C_b)^* \subset (C_{a+b})^*$ for all $a, b \in \mathbb{N}$, and that $1_{C^*} \in (C_0)^*$. But this is straightforward using the gradedness of $\Delta$ and $\epsilon$.

(d) Diagram chasing or simple element-wise verification.

(e) Simple linear algebra (no Hopf algebras involved here).

(f) The "only if" direction is proved in the same way as part (d) (or as a corollary of part (d), since $D^\circ$ and $C^\circ$ are subalgebras of $D^*$ and $C^*$). It remains to prove the "if" direction.

Assume that $f^* : D^o \to C^o$ is a $\mathbf{k}$-algebra morphism. We want to show that $f : C \to D$ is a $\mathbf{k}$-coalgebra morphism. In other words, we want to show that the two diagrams

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes C \arrow[r, "f \otimes f"] & D \otimes D \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} C \arrow[rr, "f"] \arrow[rd, "\epsilon_C"'] & & D \arrow[ld, "\epsilon_D"] \\ & \mathbf{k} & \end{tikzcd} \tag{12.1.6}$$

commute. Let us start with the left one of these diagrams. The graded $\mathbf{k}$-module $D$ is of finite type, and therefore the map $\rho_{D,D} : D^o \otimes D^o \to (D \otimes D)^o$ (a restriction of the map $\rho_{D,D} : D^* \otimes D^* \to (D \otimes D)^*$) is an isomorphism. Its inverse $\rho_{D,D}^{-1} : (D \otimes D)^o \to D^o \otimes D^o$ is therefore well-defined[378]. We can thus form the (asymmetric!) diagram

(12.1.7)

$$\begin{tikzcd} D^o \arrow[rrr, "f^*"] & & & C^o \\ & D^o \otimes D^o \arrow[lu, "m_{D^*}"'] \arrow[r, "f^* \otimes f^*"] & C^o \otimes C^o \arrow[ru, "m_{C^*}"] \arrow[rd, "\rho_{C,C}"] & \\ (D \otimes D)^o \arrow[uu, "\Delta_D^*"] \arrow[ru, "\rho_{D,D}^{-1}"] \arrow[rrr, "(f \otimes f)^*"'] & & & (C \otimes C)^o \arrow[uu, "\Delta_C^*"'] \end{tikzcd} .$$

(The arrows labelled $m_{C^*}$ and $m_{D^*}$ could just as well have been labelled $m_{C^o}$ and $m_{D^o}$, since the multiplication maps $m_{C^o}$ and $m_{D^o}$ are restrictions of $m_{C^*}$ and $m_{D^*}$.) Argue that the diagram (12.1.7) commutes. Thus, $f^* \circ \Delta_D^* = \Delta_C^* \circ (f \otimes f)^*$ as maps from $(D \otimes D)^o$ to $C^o$. In other words, $(\Delta_D \circ f)^* = ((f \otimes f) \circ \Delta_C)^*$ as maps from $(D \otimes D)^o$ to $C^o$. But a general linear-algebraic fact states that if $U$ and $V$ are two graded $\mathbf{k}$-modules such that $V$ is of finite type, and if $\alpha$ and $\beta$ are two graded $\mathbf{k}$-linear maps $U \to V$ such that $\alpha^* = \beta^*$ as maps from $V^o$ to $U^o$, then $\alpha = \beta$ [379]. Hence, $(\Delta_D \circ f)^* = ((f \otimes f) \circ \Delta_C)^*$ leads to $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$. In other words, the first diagram in (12.1.6) commutes. The second is similar

[378] Beware: we don't have an inverse of the non-restricted map $\rho_{D,D} : D^* \otimes D^* \to (D \otimes D)^*$.

[379] This follows immediately from Exercise 1.6.1 (e).

but easier. Thus, $f$ is a $\mathbf{k}$-coalgebra morphism, and the "if" direction is proved.

*Hint to Exercise 1.6.4.* Straightforward computations. For part (d), first show (independently of whether $\mathbf{k}$ is a field and its characteristic) that $\left(f^{(1)}\right)^m = m! f^{(m)}$ for every $m \in \mathbb{N}$.

*Hint to Exercise 1.6.5.* It is best to solve parts (c) and (d) before approaching (b).

(a) Both maps $\Delta_{\operatorname{Sym} V}$ and

$$\begin{array}{ccc} \mathbf{k}[\mathbf{x}] & \xrightarrow{\Delta} & \mathbf{k}[\mathbf{x}, \mathbf{y}], \\ f(x_1, \ldots, x_n) & \longmapsto & f(x_1 + y_1, \ldots, x_n + y_n) \end{array}$$

are $\mathbf{k}$-algebra homomorphisms. Thus, in order to check that they are equal, it suffices to verify that they agree on $V$ (since $V$ generates $\operatorname{Sym} V$).

(c) This is a straightforward computation unless you get confused with the topologist's sign convention. The latter convention affects the twist map $T = T_{T(V),T(V)} : T(V) \otimes T(V) \to T(V) \otimes T(V)$ (in particular, we now have $T(x \otimes x) = -x \otimes x$ instead of $T(x \otimes x) = x \otimes x$), and thus also affects the multiplication in the $\mathbf{k}$-algebra $T(V) \otimes T(V)$, because this multiplication is given by

$$m_{T(V) \otimes T(V)} = \left(m_{T(V)} \otimes m_{T(V)}\right) \circ (\operatorname{id} \otimes T \otimes \operatorname{id}).$$

Make sure you understand why this leads to $(1 \otimes x) \cdot (x \otimes 1) = -x \otimes x$ (whereas $(x \otimes 1) \cdot (1 \otimes x) = x \otimes x$).

(d) The trickiest part is showing that $J$ is a graded $\mathbf{k}$-submodule of $T(V)$. It suffices to check that $J$ is generated (as a two-sided ideal) by homogeneous elements[380]; however, this is not completely trivial, as the designated generators $x^2$ for $x \in V$ need not be homogeneous. However, it helps to observe that $J$ is also the two-sided ideal generated by the set

$$\{x \otimes x\}_{x \in V \text{ is homogeneous}} \cup \{x \otimes y + y \otimes x\}_{x,y \in V \text{ are homogeneous}}$$

(why?), which set does consist of homogeneous elements. Thus, $J$ is a graded $\mathbf{k}$-submodule of $T(V)$. From part (c), it is easy to observe that $J$ is a two-sided coideal of $T(V)$ as well. Hence, $T(V)/J$ inherits a graded $\mathbf{k}$-bialgebra structure from $T(V)$. The rest is easy.

(b) is now a consequence of what has been done in (d).

*Hint to Exercise 1.6.6.* Easy and straightforward.

*Hint to Exercise 1.6.8.* The hint after the exercise shows the way; here are a few more pointers. The solution proceeds in two steps:

- *Step 1:* Show that Proposition 1.6.7 holds when $V$ is a finite free $\mathbf{k}$-module.
- *Step 2:* Use this to conclude that Proposition 1.6.7 always holds.

The trick to Step 1 is to reduce the proof to Example 1.6.3. In a bit more detail: If $V$ is a finite free $\mathbf{k}$-module with basis $(v_1, v_2, \ldots, v_n)$, then we know from Example 1.6.3 that the graded dual $A^o$ of its tensor algebra $A := T(V)$ is a Hopf algebra whose basis $\left\{y_{(i_1,i_2,\ldots,i_\ell)}\right\}$ is indexed by words

[380] Make sure you understand why.

in the alphabet $I := \{1, 2, \ldots, n\}$. This allows us to define a $\mathbf{k}$-linear map $\phi : A^o \to T(V)$ by setting

$$\phi\left(y_{(i_1, i_2, \ldots, i_\ell)}\right) = v_{i_1} v_{i_2} \cdots v_{i_\ell} \qquad \text{for every } \ell \in \mathbb{N} \text{ and } (i_1, i_2, \ldots, i_\ell) \in I^\ell.$$

This $\mathbf{k}$-linear map $\phi$ then is an isomorphism from the Hopf algebra $A^o$ to the putative Hopf algebra $\left(\operatorname{Sh}(V), \underline{\sqcup\!\sqcup}, 1_{T(V)}, \Delta_{\sqcup\!\sqcup}, \epsilon, S\right)$, in the sense that it is invertible (since it sends a basis to a basis) and satisfies the five equalities

$$\begin{aligned} \phi \circ m_{A^o} &= m_{\sqcup\!\sqcup} \circ (\phi \otimes \phi), \\ \phi \circ u_{A^o} &= u, \\ (\phi \otimes \phi) \circ \Delta_{A^o} &= \Delta_{\sqcup\!\sqcup} \circ \phi, \\ \epsilon_{A^o} &= \epsilon \circ \phi, \\ \phi \circ S_{A^o} &= S \circ \phi \end{aligned}$$

(check all these – for instance, the first of these equalities follows by comparing (1.6.4) with the definition of $\underline{\sqcup\!\sqcup}$). Thus, the latter putative Hopf algebra is an actual Hopf algebra (since the former is). This proves Proposition 1.6.7 for our finite free $V$, and thus completes Step 1.

Step 2 demonstrates the power of functoriality. We want to prove Proposition 1.6.7 in the general case, knowing that it holds when $V$ is finite free. So let $V$ be an arbitrary $\mathbf{k}$-module. For the sake of brevity, we shall write $\mathbf{V}$ for $T(V)$. Let $m_{\sqcup\!\sqcup}$ denote the $\mathbf{k}$-linear map $\mathbf{V} \otimes \mathbf{V} \to \mathbf{V}$ which sends every $a \otimes b$ to $a \underline{\sqcup\!\sqcup} b$. One of the things that need to be shown is the commutativity of the diagram

(12.1.8)
$$\begin{tikzcd}
 & & \mathbf{V} \otimes \mathbf{V} \arrow[dll, "\Delta_{\sqcup\!\sqcup} \otimes \Delta_{\sqcup\!\sqcup}"'] \arrow[ddr, "m_{\sqcup\!\sqcup}"] & \\
\mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \arrow[dd, "\operatorname{id} \otimes T \otimes \operatorname{id}"'] & & & \\
 & & & \mathbf{V} \arrow[ddl, "\Delta_{\sqcup\!\sqcup}"] \\
\mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \arrow[drr, "m_{\sqcup\!\sqcup} \otimes m_{\sqcup\!\sqcup}"'] & & & \\
 & & \mathbf{V} \otimes \mathbf{V} &
\end{tikzcd},$$

where $T$ is the twist map $T_{\mathbf{V},\mathbf{V}}$. By linearity, it is clearly enough to verify this only on the pure tensors; that is, it is enough to check that every $a \in \mathbf{V}$ and $b \in \mathbf{V}$ satisfy

(12.1.9)
$$\left((m_{\sqcup\!\sqcup} \otimes m_{\sqcup\!\sqcup}) \circ (\operatorname{id} \otimes T \otimes \operatorname{id}) \circ (\Delta_{\sqcup\!\sqcup} \otimes \Delta_{\sqcup\!\sqcup})\right)(a \otimes b) = (\Delta_{\sqcup\!\sqcup} \circ m_{\sqcup\!\sqcup})(a \otimes b).$$

So let $a, b \in \mathbf{V}$ be arbitrary. WLOG assume that $a = v_1 v_2 \cdots v_p$ and $b = v_{p+1} v_{p+2} \cdots v_{p+q}$ for some $p, q \in \mathbb{N}$ and $v_1, v_2, \ldots, v_{p+q} \in V$. Define $W$ to be the free $\mathbf{k}$-module with basis $(x_1, x_2, \ldots, x_{p+q})$, and let $\mathbf{W}$ be its tensor algebra $T(W)$. Then, $W$ is a finite free $\mathbf{k}$-module, and so we know from Step 1 that Proposition 1.6.7 holds for $W$ instead of $V$. But we can define a $\mathbf{k}$-linear map $f : W \to V$ that sends $x_1, x_2, \ldots, x_{p+q}$ to $v_1, v_2, \ldots, v_{p+q}$, respectively. This map $f : W \to V$ clearly induces a $\mathbf{k}$-algebra homomorphism $\mathbf{f} := T(f) : \mathbf{W} \to \mathbf{V}$ that respects all relevant shuffle-algebraic structure (i.e., it satisfies $\mathbf{f} \circ m_{\sqcup\!\sqcup} = m_{\sqcup\!\sqcup} \circ (\mathbf{f} \otimes \mathbf{f})$ and $(\mathbf{f} \otimes \mathbf{f}) \circ \Delta_{\sqcup\!\sqcup} = \Delta_{\sqcup\!\sqcup} \circ \mathbf{f}$ and so on), simply because this structure has been defined canonically in terms of each of $V$ and $W$. Thus, in the diagram

$$\begin{tikzcd}
 & & \mathbf{W} \otimes \mathbf{W} \arrow[d, "\mathbf{f} \otimes \mathbf{f}"'] \arrow[ddll, "\Delta_{\sqcup\!\sqcup} \otimes \Delta_{\sqcup\!\sqcup}"'] \arrow[dddrr, "m_{\sqcup\!\sqcup}"] & & \\
 & & \mathbf{V} \otimes \mathbf{V} \arrow[dl, "\Delta_{\sqcup\!\sqcup} \otimes \Delta_{\sqcup\!\sqcup}"'] \arrow[ddr, "m_{\sqcup\!\sqcup}"'] & & \\
\mathbf{W} \otimes \mathbf{W} \otimes \mathbf{W} \otimes \mathbf{W} \arrow[r, "\mathbf{f} \otimes \mathbf{f} \otimes \mathbf{f} \otimes \mathbf{f}"'] \arrow[dd, "\mathrm{id} \otimes T \otimes \mathrm{id}"'] & \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \arrow[dd, "\mathrm{id} \otimes T \otimes \mathrm{id}"'] & & & \\
 & & & \mathbf{V} \arrow[ddl, "\Delta_{\sqcup\!\sqcup}"'] & \mathbf{W} \arrow[l, "\mathbf{f}"] \arrow[dddll, "\Delta_{\sqcup\!\sqcup}"] \\
\mathbf{W} \otimes \mathbf{W} \otimes \mathbf{W} \otimes \mathbf{W} \arrow[r, "\mathbf{f} \otimes \mathbf{f} \otimes \mathbf{f} \otimes \mathbf{f}"] \arrow[ddrr, "m_{\sqcup\!\sqcup} \otimes m_{\sqcup\!\sqcup}"'] & \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \otimes \mathbf{V} \arrow[dr, "m_{\sqcup\!\sqcup} \otimes m_{\sqcup\!\sqcup}"'] & & & \\
 & & \mathbf{V} \otimes \mathbf{V} & & \\
 & & \mathbf{W} \otimes \mathbf{W} \arrow[u, "\mathbf{f} \otimes \mathbf{f}"] & &
\end{tikzcd},$$

all the little quadrilaterals commute. The outer pentagon also commutes, since Proposition 1.6.7 holds for $W$ instead of $V$. If $\mathbf{f}$ was surjective, then we would be able to conclude that the inner pentagon also commutes, so we would immediately get the commutativity of (12.1.8). But even if $\mathbf{f}$ is not surjective, we are almost there: The inner pentagon commutes on the image of the map $\mathbf{f} \otimes \mathbf{f} : \mathbf{W} \otimes \mathbf{W} \to \mathbf{V} \otimes \mathbf{V}$ (because when we start at $\mathbf{W} \otimes \mathbf{W}$, we can walk around the outer pentagon instead, which is known to commute), but this image contains $a \otimes b$ (since $a = v_1 v_2 \cdots v_p = \mathbf{f}(x_1 x_2 \cdots x_p)$ and similarly $b = \mathbf{f}(x_{p+1} x_{p+2} \cdots x_{p+q})$), so we conclude that (12.1.9) holds, as we wanted to show.

This is only one of the diagrams we need to prove in order to prove Proposition 1.6.7, but the other diagrams are done in the exact same way.

*Hint to Exercise 1.7.9.* Straightforward reasoning using facts like "a union of finitely many finite sets is finite" and "a tensor is a sum of finitely many pure tensors".

*Hint to Exercise 1.7.13.* Parts (a), (b), (d) and (e) of Proposition 1.7.11 are easy. (In proving (1.7.3) and later, it helps to first establish an extension of (1.7.2) to infinite sums[381].) For part (c), recall that the binomial formula $(a+b)^n = \sum_{k=0}^n \dbinom{n}{k} a^k b^{n-k}$ holds for any two commuting elements $a$ and $b$ of any ring (such as $f$ and $g$ in the convolution algebra $\operatorname{Hom}(C, A)$). Part (f) follows from (e) using (1.7.3). Part (g) is best proved in two steps: First, use induction to prove part (g) in the case when $u = T^k$ for some $k \in \mathbb{N}$ (this relies on (1.7.3)); then, notice that both sides of (1.7.7) depend $\mathbf{k}$-linearly on $u$, whence the general case follows (up to some mudfighting

[381] Namely: Let $(r_q)_{q \in Q} \in (\mathbf{k}[[T]])^Q$ be a family of power series such that the (possibly infinite) sum $\sum_{q \in Q} r_q$ converges in $\mathbf{k}[[T]]$. Let $f \in \mathfrak{n}(C, A)$. Then, the family $\left((r_q)^\star (f)\right)_{q \in Q} \in (\operatorname{Hom}(C, A))^Q$ is pointwise finitely supported and satisfies $\left(\sum_{q \in Q} r_q\right)^\star (f) = \sum_{q \in Q} (r_q)^\star (f)$.

with infinite sums). Part (h) is an instance of the "local $\star$-nilpotence" already observed in the proof of Proposition 1.4.7. Part (j) follows from (h). Part (i) follows from Proposition 1.4.3 (applied to $C' = C$, $A' = B$, $\gamma = \operatorname{id}_C$ and $\alpha = s$) in a similar way as part (g) followed from (1.7.3).

*Hint to Exercise 1.7.20.* Proposition 1.7.15 is a classical result, often proved by a lazy reference to the mythical complex analysis class the reader has surely seen it in. Here is a do-it-yourself purely algebraic proof:

- *Step 1:* If $u, v \in \mathbf{k}[[T]]$ are two power series having the same constant term and satisfying $\dfrac{d}{dT}u = \dfrac{d}{dT}v$, then $u = v$. This simple lemma (whose analogue for differentiable functions is a fundamental fact of real analysis) is easily proved by comparing coefficients in $\dfrac{d}{dT}u = \dfrac{d}{dT}v$ and recalling that $\mathbf{k}$ is a $\mathbb{Q}$-algebra (so $1, 2, 3, \ldots$ are invertible in $\mathbf{k}$).
- *Step 2:* If $u, v \in \mathbf{k}[[T]]$ are two power series having constant term 1 and satisfying $\left(\dfrac{d}{dT}u\right) \cdot v = \left(\dfrac{d}{dT}v\right) \cdot u$, then $u = v$. This can be proved by applying Step 1 to $uv^{-1}$ and 1 instead of $u$ and $v$.
- *Step 3:* The power series $\overline{\log}\left[\overline{\exp}\right]$ and $\overline{\exp}\left[\overline{\log}\right]$ are well-defined and have constant term 0. (Easy.)
- *Step 4:* If $w \in \mathbf{k}[[T]]$ is a power series having constant term 0, then
$$\frac{d}{dT}\left(\overline{\exp}[w]\right) = \left(\frac{d}{dT}w\right) \cdot \exp[w] \qquad \text{and}$$
$$\frac{d}{dT}\left(\overline{\log}[w]\right) = \left(\frac{d}{dT}w\right) \cdot \frac{1}{1+w}.$$
These formulas can be derived from the chain rule, or more directly from $\overline{\exp}[w] = \sum_{n\geq 1} \dfrac{1}{n!}w^n$ and $\overline{\log}[w] = \sum_{n\geq 1} \dfrac{(-1)^{n-1}}{n}w^n$.
- *Step 5:* Show $\overline{\exp}\left[\overline{\log}\right] = T$ by applying Step 2 to $u = \exp\left[\overline{\log}\right]$ and $v = 1 + T$.
- *Step 6:* Show $\overline{\log}\left[\overline{\exp}\right] = T$ by applying Step 1 to $u = \overline{\log}\left[\overline{\exp}\right]$ and $v = T$.

Lemma 1.7.16 easily follows from Proposition 1.7.11(f).

Remains to prove Proposition 1.7.18. It is easy to see that $\log^\star(\exp^\star f) = \overline{\log}^\star(\overline{\exp}^\star f)$ for each $f \in \mathfrak{n}(C, A)$; thus, Proposition 1.7.18(a) follows from (1.7.7) using Proposition 1.7.15 and Proposition 1.7.11(f) (since $T^\star(f) = f$). A similar argument yields Proposition 1.7.18(b) (this time, we need to observe that $\exp^\star(\log^\star g) = \overline{\exp}^\star\left(\overline{\log}^\star(g - u_A\epsilon_C)\right) + u_A\epsilon_C$ first). To prove Proposition 1.7.18(c), first use Proposition 1.7.11(c) to show that $\exp^\star(f + g)$ is well-defined; then, apply the well-known fact that $\exp(x + y) = \exp x \cdot \exp y$ for any two commuting elements $x$ and $y$ of a ring (provided the exponentials are well-defined; some yak-shaving is required here to convince oneself that the infinite sums behave well)[382]. Part (d) is

[382] If you have not seen this well-known fact, prove it by a quick computation using the binomial formula.

trivial. Part (e) is an induction on $n$. Part (f) is a rehash of the definition of $\log^\star(f + u_A\epsilon_C) = \overline{\log}^\star f$.

*Hint to Exercise 1.7.28.* Proposition 1.7.21(a) is easily proved by unpacking the definition of convolution (just like Proposition 1.4.3). Part (b) follows from (a) by induction.

The trick to Proposition 1.7.22 is to realize that if $f \in \operatorname{Hom}(C, A)$ is as in Proposition 1.7.22, then every $x, y \in C$ satisfy

$$f(xy) = \epsilon(y) f(x) + \epsilon(x) f(y), \tag{12.1.10}$$

because $xy - \epsilon(x) y - \epsilon(y) x = \epsilon(x)\epsilon(y)\cdot 1 + \underbrace{(x - \epsilon(x))}_{\in \ker \epsilon}\underbrace{(y - \epsilon(y))}_{\in \ker \epsilon}$ is annihilated by $f$. Once this equality is known, it is not hard to prove Proposition 1.7.22 "by hand" by induction on $n$ (using Sweedler notation). Alternatively, for a cleaner proof, the equality (12.1.10) can be restated in an element-free way as

$$f \circ m_C = m_A \circ (f \otimes \mathfrak{i} + \mathfrak{i} \otimes f),$$

where $\mathfrak{i} = u_A \circ \epsilon_C$ is the unity of the $\mathbf{k}$-algebra $(\operatorname{Hom}(C, A), \star)$; then, an application of Proposition 1.7.21(b) shows that every $n \in \mathbb{N}$ satisfies

$$\begin{aligned} f^{\star n} \circ m_C &= m_A \circ \underbrace{(f \otimes \mathfrak{i} + \mathfrak{i} \otimes f)^{\star n}}_{\substack{= \sum_{i=0}^{n} \binom{n}{i} (f \otimes \mathrm{i})^{\star i} \star (\mathrm{i} \otimes f)^{\star (n-i)} \\ \text{(by the binomial formula,} \\ \text{since } f \otimes \mathrm{i} \text{ and } \mathrm{i} \otimes f \text{ commute in} \\ \text{the convolution algebra } \operatorname{Hom}(C \otimes C, A \otimes A))}} \\ &= m_A \circ \left( \sum_{i=0}^{n} \binom{n}{i} \underbrace{(f \otimes \mathfrak{i})^{\star i} \star (\mathfrak{i} \otimes f)^{\star (n-i)}}_{\substack{= f^{\star i} \otimes f^{\star (n-i)} \\ \text{(by repeated application of Exercise 1.4.4(a))}}} \right) \\ &= m_A \circ \left( \sum_{i=0}^{n} \binom{n}{i} f^{\star i} \otimes f^{\star (n-i)} \right), \end{aligned}$$

which is precisely Proposition 1.7.22 (restated in an element-free way).

Proposition 1.7.23 is an easy consequence of Proposition 1.7.22, since $(\exp^\star f)(xy) = \sum_{n \in \mathbb{N}} \dfrac{1}{n!} f^{\star n}(xy)$. (Again, fighting infinite sums is probably the most laborious part of the proof.)

Lemma 1.7.24 can be reduced to the fact that the matrix $\left(i^{N+1-j}\right)_{i,j=1,2,\ldots,N+1} \in \mathbb{Q}^{(N+1)\times(N+1)}$ is invertible (since its determinant is the Vandermonde determinant $\prod_{1 \leq i < j \leq N+1} \underbrace{(i - j)}_{\neq 0} \neq 0$) and thus has trivial kernel (not just over $\mathbb{Q}$, but on any torsionfree abelian group).

Lemma 1.7.25 follows from Lemma 1.7.24, because a finitely supported family indexed by nonnegative integers must become all zeroes from some point on.

The proof of Proposition 1.7.26 is rather surprising: It suffices to show that $f(xy) = 0$ for all $x, y \in \ker \epsilon$. So let us fix $x, y \in \ker \epsilon$. Proposition 1.7.11(h) yields $f \in \mathfrak{n}(C, A)$. Let $t \in \mathbb{N}$ be arbitrary. Then, Proposition 1.7.18(e) (applied to $n = t$) shows that $tf \in \mathfrak{n}(C, A)$ and $\exp^\star(tf) = (\exp^\star f)^{\star t}$. But Exercise 1.5.11(b) shows that $(\exp^\star f)^{\star t}$ is a $\mathbf{k}$-algebra homomorphism $C \to A$. Hence, $(\exp^\star f)^{\star t}(xy) = (\exp^\star f)^{\star t}(x) \cdot (\exp^\star f)^{\star t}(y)$. Rewriting $(\exp^\star f)^{\star t}$ as $\exp^\star(tf) = \sum_{n\in\mathbb{N}} \dfrac{1}{n!} f^{\star n} t^n$ on both sides, and multiplying out the right hand side, we can rewrite this as

$$\sum_{k\in\mathbb{N}} \frac{1}{k!} f^{\star k}(xy)\, t^k = \sum_{k\in\mathbb{N}} \left( \sum_{i=0}^{k} \frac{f^{\star i}(x)}{i!} \cdot \frac{f^{\star(k-i)}(y)}{(k-i)!} \right) t^k .$$

In other words,

$$\sum_{k\in\mathbb{N}} w_k t^k = 0, \qquad \text{where we set } w_k = \frac{1}{k!} f^{\star k}(xy) - \sum_{i=0}^{k} \frac{f^{\star i}(x)}{i!} \cdot \frac{f^{\star(k-i)}(y)}{(k-i)!} .$$

But we have proved this for all $t \in \mathbb{N}$. Thus, Lemma 1.7.25 shows that

$$w_k = 0 \qquad \text{for every } k \in \mathbb{N}.$$

Applying this to $k = 1$ and simplifying, we obtain $f(xy) - \epsilon(x) f(y) - f(x)\epsilon(y) = 0$. Since $x, y \in \ker \epsilon$, this simplifies even further to $f(xy) = 0$, which proves Proposition 1.7.26.

Finally, we need to prove Proposition 1.7.27. Set $F = \exp^\star f$ and $\widetilde{F} = F - u_A \epsilon_C$, so that $\widetilde{F} \in \mathfrak{n}(C, A)$. Then, Proposition 1.7.23 shows that $F : C \to A$ is a $\mathbf{k}$-algebra homomorphism, so it remains to show that $F$ is surjective. But it is easy to see using Proposition 1.7.18(a) that $f = \overline{\log}^\star \widetilde{F}$.

Define $\widetilde{\mathrm{id}} \in \mathfrak{n}(C, C)$ by $\widetilde{\mathrm{id}} = \mathrm{id}_C - u_C \epsilon_C$. Then, it is not hard to see that $F \circ \widetilde{\mathrm{id}} = \widetilde{F}$. Hence, $f = \overline{\log}^\star \underbrace{\widetilde{F}}_{= F \circ \widetilde{\mathrm{id}}} = \overline{\log}^\star \left( F \circ \widetilde{\mathrm{id}} \right) = F \circ \left( \overline{\log}^\star \left( \widetilde{\mathrm{id}} \right) \right)$ (by Proposition 1.7.11(i), since $F$ is a $\mathbf{k}$-algebra homomorphism). Therefore, $f(C) \subset F(C)$. Since $F$ is a $\mathbf{k}$-algebra homomorphism, this entails that $F(C)$ is a $\mathbf{k}$-subalgebra of $A$ that contains $f(C)$ as a subset. But this causes $F(C)$ to be the whole $A$ (since $f(C)$ generates $A$). Thus, $F$ is surjective, so Proposition 1.7.27 is proven.

*Hint to Exercise 1.7.33.* We must prove Theorem 1.7.29. Part (a) is easy. For the remainder of the proof, we set $\widetilde{\mathrm{id}} = \mathrm{id}_A - u_A \epsilon_A \in \operatorname{End} A$, and equip ourselves with some simple lemmas:

- The kernel $\ker \epsilon$ is an ideal of $A$.
- We have $\widetilde{\mathrm{id}} \in \mathfrak{n}(A, A)$ and $\ker \widetilde{\mathrm{id}} = \mathbf{k} \cdot 1_A$ and $\widetilde{\mathrm{id}}(A) = \ker \epsilon$.
- We have $A / \left( \mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \right) \cong (\ker \epsilon) / (\ker \epsilon)^2$ as $\mathbf{k}$-modules.

Now, to the proof of Theorem 1.7.29(b). Using $\mathfrak{e} = \log^\star(\mathrm{id}_A) = \overline{\log}^\star \widetilde{\mathrm{id}}$ and $\widetilde{\mathrm{id}}(1_A) = 0$, it is easy to see that $\mathfrak{e}(1_A) = 0$. Hence, $\mathfrak{e}(A_0) = 0$ since $A$ is connected. Thus, Proposition 1.7.26 shows that $\mathfrak{e}\left( (\ker \epsilon)^2 \right) = 0$ (since $\exp^\star \mathfrak{e} = \mathrm{id}_A$ is a $\mathbf{k}$-algebra homomorphism). Combined with $\mathfrak{e}(1_A) = 0$, this yields $\mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \subset \ker \mathfrak{e}$. But this inclusion is actually an equality, as we can show by the following computation: We have $\mathfrak{e} = \overline{\log}^\star \widetilde{\mathrm{id}} =$

$\sum_{n\geq 1} \dfrac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}$, and therefore each $x \in A$ satisfies

$$\begin{aligned}\mathfrak{e}(x) &= \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}(x) = \underbrace{\widetilde{\mathrm{id}}(x)}_{\substack{=x-\epsilon(x)1_A \\ \text{(by the definition of } \widetilde{\mathrm{id}})}} + \sum_{n\geq 2}\frac{(-1)^{n-1}}{n} \underbrace{\widetilde{\mathrm{id}}^{\star n}(x)}_{\substack{\in \left(\widetilde{\mathrm{id}}(A)\right)^n \\ \text{(by induction on } n, \\ \text{using the definition} \\ \text{of convolution)}}} \\ &\in x - \epsilon(x) 1_A + \sum_{n\geq 2}\frac{(-1)^{n-1}}{n} \Bigg( \underbrace{\widetilde{\mathrm{id}}(A)}_{=\ker \epsilon} \Bigg)^n \\ &= x - \underbrace{\epsilon(x)}_{\in \mathbf{k}} 1_A + \underbrace{\sum_{n\geq 2}\frac{(-1)^{n-1}}{n} (\ker \epsilon)^n}_{\subset (\ker\epsilon)^2} \subset x - \mathbf{k}\cdot 1_A + (\ker\epsilon)^2 ,\end{aligned}$$

so that

$$x - \mathfrak{e}(x) \in \mathbf{k}\cdot 1_A + (\ker\epsilon)^2 . \tag{12.1.11}$$

If $x \in \ker \mathfrak{e}$, then this simplifies to $x \in \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. Thus, $\ker\mathfrak{e} \subset \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. Combining this with $\mathbf{k}\cdot 1_A + (\ker\epsilon)^2 \subset \ker\mathfrak{e}$, we obtain $\ker\mathfrak{e} = \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. But the homomorphism theorem yields

$$\mathfrak{e}(A) \cong A / \underbrace{\ker\mathfrak{e}}_{\substack{=\mathbf{k}\cdot 1_A + (\ker\epsilon)^2 \\ \text{(as seen above)}}} = A / \left(\mathbf{k}\cdot 1_A + (\ker\epsilon)^2\right) \cong (\ker\epsilon) / (\ker\epsilon)^2$$

as $\mathbf{k}$-modules. This completes the proof of Theorem 1.7.29(b).

Theorem 1.7.29(c) just requires showing that $\mathfrak{q}(A_0) = 0$, which is a consequence of $\mathfrak{e}(A_0) = 0$.

Next, we shall prove Theorem 1.7.29(d). We have $\mathfrak{q} \in \mathfrak{n}(A, \mathrm{Sym}(\mathfrak{e}(A)))$. Furthermore, $\mathfrak{q}(A)$ generates the $\mathbf{k}$-algebra $\mathrm{Sym}(\mathfrak{e}(A))$ (since $\mathfrak{q}(A) = \mathrm{Sym}^1(\mathfrak{e}(A))$). From Theorem 1.7.29(b), we get $\ker\mathfrak{e} = \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$, from which we easily obtain $\mathfrak{q}(1_A) = 0$ and $\mathfrak{q}\left((\ker\epsilon)^2\right) = 0$. Thus, Proposition 1.7.27 (applied to $A$, $\mathrm{Sym}(\mathfrak{e}(A))$ and $\mathfrak{q}$ instead of $C$, $A$ and $f$) shows that $\exp^\star \mathfrak{q} : A \to \mathrm{Sym}(\mathfrak{e}(A))$ is a surjective $\mathbf{k}$-algebra homomorphism. But $\mathfrak{s}$ is a $\mathbf{k}$-algebra homomorphism $\mathrm{Sym}(\mathfrak{e}(A)) \to A$ and satisfies $\mathbf{i} = \mathfrak{s} \circ \iota_{\mathfrak{e}(A)}$ (by its definition). Thus, Proposition 1.7.11(i) (applied to $A$, $\mathrm{Sym}(\mathfrak{e}(A))$, $A$, $\mathfrak{s}$, exp and $\mathfrak{q}$ instead of $C$, $A$, $B$, $s$, $u$ and $f$) shows that $\mathfrak{s} \circ \mathfrak{q} \in \mathfrak{n}(A, A)$ and $\exp^\star(\mathfrak{s}\circ\mathfrak{q}) = \mathfrak{s} \circ (\exp^\star \mathfrak{q})$. However, it is easy to see that $\mathfrak{s}\circ\mathfrak{q} = \mathfrak{e}$ (since $\mathbf{i} = \mathfrak{s}\circ\iota_{\mathfrak{e}(A)}$); this lets us rewrite the equality $\exp^\star(\mathfrak{s}\circ\mathfrak{q}) = \mathfrak{s}\circ(\exp^\star\mathfrak{q})$ as $\exp^\star\mathfrak{e} = \mathfrak{s}\circ(\exp^\star\mathfrak{q})$. Comparing this with $\exp^\star\mathfrak{e} = \mathrm{id}_A$, we obtain $\mathfrak{s}\circ(\exp^\star\mathfrak{q}) = \mathrm{id}_A$. Since $\exp^\star\mathfrak{q}$ is surjective, this entails that the maps $\exp^\star\mathfrak{q}$ and $\mathfrak{s}$ are mutually inverse. This proves Theorem 1.7.29(d).

Theorem 1.7.29(d) shows that $A \cong \mathrm{Sym}(\mathfrak{e}(A))$ as $\mathbf{k}$-algebras, but Theorem 1.7.29(b) shows that $\mathfrak{e}(A) \cong (\ker\epsilon) / (\ker\epsilon)^2$ as $\mathbf{k}$-modules. Combining these, we obtain Theorem 1.7.29(e).

Finally, to prove Theorem 1.7.29(f), we notice that each $x \in A$ satisfies

$$\begin{aligned} x - \mathfrak{e}(x) &\in \mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \qquad \text{(by (12.1.11))} \\ &= \ker \mathfrak{e} \qquad \text{(by Theorem 1.7.29(b))} \end{aligned}$$

and thus $0 = \mathfrak{e}(x - \mathfrak{e}(x)) = \mathfrak{e}(x) - (\mathfrak{e} \circ \mathfrak{e})(x)$.

## Acknowledgements

The authors thank the following for helpful comments and/or teaching them about Hopf algebras: Marcelo Aguiar, Federico Ardila, Lou Billera, Richard Ehrenborg, Mark Haiman, Florent Hivert, Christophe Hohlweg, Jia Huang, Jang Soo Kim, Aaron Lauve, Dominique Manchon, John Palmieri, Alexander Postnikov, Margie Readdy, Nathan Reading, Christophe Reutenauer, Hans-Jürgen Schneider, Richard Stanley, Josh Swanson, Muge Taskin, Jean-Yves Thibon.

Parts of this text have been written during stays at the Mathematisches Forschungsinstitut Oberwolfach (2019 and 2020)[383] and at the Institut Mittag–Leffler Djursholm (Spring 2020, supported by the Swedish Research Council under grant no. 2016-06596); DG thanks both for their hospitality.

## References

[1] Eiichi Abe. Hopf algebras. *Cambridge Tracts in Mathematics* **74**. Cambridge University Press, Cambridge-New York, 1980.

[2] Marcelo Aguiar, et al. (28 authors). Supercharacters, symmetric functions in noncommuting variables, and related Hopf algebras. *Adv. Math.* **229** (2012), 2310–2337. `https://doi.org/10.1016/j.aim.2011.12.024` . Also available as `arXiv:1009.4134v2`.

[3] Marcelo Aguiar and Federico Ardila. Hopf monoids and generalized permutahedra. `arXiv:1709.07504v1`.

[4] Marcelo Aguiar, Nantel Bergeron, and Frank Sottile. Combinatorial Hopf algebras and generalized Dehn-Sommerville relations. *Compos. Math.* **142** (2006), pp. 1–30. A newer version of this paper appears at `http://pi.math.cornell.edu/~maguiar/CHalgebra.pdf`.

[5] Marcelo Aguiar, Aaron Lauve. The characteristic polynomial of the Adams operators on graded connected Hopf algebras. *Algebra & Number Theory* **9-3** (2015), 547–583. Also available at `http://pi.math.cornell.edu/~maguiar/adams.pdf` and as `arXiv:1403.7584v2`.

[6] Marcelo Aguiar and Swapneel Mahajan. Monoidal functors, species and Hopf algebras. *CRM Monograph Series* **29**. American Mathematical Society, Providence, RI, 2010. Available at `http://pi.math.cornell.edu/~maguiar/a.pdf`

[7] Marcelo Aguiar and Frank Sottile. Structure of the Malvenuto-Reutenauer Hopf algebra of permutations. *Adv. Math.* **191** (2005), 225–275. `https://doi.org/10.1016/j.aim.2004.03.007`.
A preprint is available at `http://pi.math.cornell.edu/~maguiar/MR.pdf`

[8] Nicolas Andruskiewitsch, Walter Ferrer Santos. The beginnings of the theory of Hopf algebras. *Acta Appl Math* **108** (2009), 3–17. See also a corrected postprint published on arXiv as `arXiv:0901.2460v3`.

[9] Sami H. Assaf and Peter R.W. McNamara. A Pieri rule for skew shapes. *J. Combin. Theory, Ser. A* **118** (2011), 277–290. `https://doi.org/10.1016/j.jcta.2010.03.010`

[10] Olga Azenhas. Littlewood-Richardson fillings and their symmetries. *Matrices and group representations* (Coimbra, 1998), 81–92, Textos Mat. Ser. B, 19, Univ. Coimbra, Coimbra, 1999. `http://www.mat.uc.pt/~oazenhas/graciano+.pdf`.

[383] This research was supported through the programme "Oberwolfach Leibniz Fellows" by the Mathematisches Forschungsinstitut Oberwolfach in 2019 and 2020.

[11] Olga Azenhas, Ronald C. King, Itaru Terada. The involutive nature of the Littlewood-Richardson commutativity bijection. `arXiv:1603.05037v1`.

[12] Andrew Baker, and Birgit Richter. Quasisymmetric functions from a topological point of view. *Math. Scand.* **103** (2008), 208–242. `http://dx.doi.org/10.7146/math.scand.a-15078`

[13] Farzin Barekat, Victor Reiner, Stephanie van Willigenburg. Corrigendum to "Coincidences among skew Schur functions" [*Adv. Math.* **216** (2007), 118–152]. *Adv. Math.* **220** (2009), 1655–1656. See also a corrected version of this paper on `arXiv:math/0602634v4`.

[14] Carolina Benedetti, Joshua Hallam, John Machacek. Combinatorial Hopf Algebras of Simplicial Complexes. `arXiv:1505.04458v2`. (Published in: *SIAM J. Discrete Math.* **30** (3), 1737–1757.)

[15] Carolina Benedetti, Bruce Sagan. Antipodes and involutions. `arXiv:1410.5023v4`. (Published in: *Journal of Combinatorial Theory, Series A* **148** (2017), 275–315.)

[16] Georgia Benkart, Frank Sottile, Jeffrey Stroomer. Tableau Switching: Algorithms and Applications. *Journal of Combinatorial Theory, Series A* **76**, 1, October 1996, 11–43. `https://doi.org/10.1006/jcta.1996.0086`
Preprint available at `http://www.math.tamu.edu/~sottile/research/pdf/switching.pdf`

[17] Chris Berg, Nantel Bergeron, Franco Saliola, Luis Serrano, Mike Zabrocki. A lift of the Schur and Hall-Littlewood bases to non-commutative symmetric functions. *Canad. J. Math.* **66** (2014), 525–565. `http://dx.doi.org/10.4153/CJM-2013-013-0`.
A preprint is `arXiv:1208.5191v3`.

[18] Nantel Bergeron, Mike Zabrocki. The Hopf algebras of symmetric functions and quasi-symmetric functions in non-commutative variables are free and co-free. *Journal of Algebra and Its Applications* **08**, Issue 04, August 2009, 581–600. A preprint also appears at `arXiv:math/0509265v3`.

[19] Louis J. Billera. Flag enumeration in polytopes, Eulerian partially ordered sets and Coxeter groups. *Proceedings of the International Congress of Mathematicians* **IV**, 2389–2415, Hindustan Book Agency, New Delhi, 2010. `http://pi.math.cornell.edu/~billera/papers/eulericm.pdf`

[20] Louis J. Billera, Francesco Brenti. Quasisymmetric functions and Kazhdan-Lusztig polynomials. `arXiv:0710.3965v2`. Published in: Israel Journal of Mathematics, August 2011, 184, pp. 317–348. `https://doi.org/10.1007/s11856-011-0070-0`

[21] Louis J. Billera, Ning Jia, and Victor Reiner. A quasisymmetric function for matroids. *European J. Combin.* **30** (2009), pp. 1727–1757. `https://doi.org/10.1016/j.ejc.2008.12.007` . A preprint also appears at `arXiv:math/0606646v3`.

[22] Anders Björner. Some combinatorial and algebraic properties of Coxeter complexes and Tits buildings. *Adv. in Math.* **52** (1984), 173–212. `https://doi.org/10.1016/0001-8708(84)90021-5`

[23] Jonah Blasiak. Kronecker coefficients for one hook shape. *Seminaire Lotharingien de Combinatoire* **77** (2017), B77c. `https://www.emis.de/journals/SLC/wpapers/s77blasiak.html`

[24] D. Blessenohl, H. Laue. Algebraic combinatorics related to the free Lie algebra. *Seminaire Lotharingien de Combinatoire* **29** (1992), B29e. `https://www.emis.de/journals/SLC/opapers/s29laue.html`

[25] Dieter Blessenohl, Manfred Schocker. Noncommutative character theory of the symmetric group. Imperial College Press 2005. `https://www.worldscientific.com/worldscibooks/10.1142/p369`

[26] Ben Blum-Smith, Samuel Coskey. The Fundamental Theorem on Symmetric Polynomials: History's First Whiff of Galois Theory. `arXiv:1301.7116v4`. An updated version was published in: The College Mathematics Journal Vol. 48, No. 1 (January 2017), pp. 18–29. `https://doi.org/10.4169/college.math.j.48.1.18`

[27] N. Bourbaki. Éléments de Mathématique: Groupes et algèbres de Lie, Chapitres 2 et 3. Springer, Heidelberg 2006.

[28] Thomas Britz, Sergey Fomin. Finite posets and Ferrers shapes. *Adv. in Math.* **158**, Issue 1, 1 March 2001, 86–127. Better version to be found on arXiv as `arXiv:math/9912126v1`.

[29] N.G. de Bruijn, D.A. Klarner. Multisets of aperiodic cycles. *SIAM J. Alg. Disc. Math.* **3** (1982), no. 3, 359–368. `https://pure.tue.nl/ws/files/1674487/597568.pdf`

[30] Daniel Bump. Notes on representations of $GL(r)$ over a finite field. Available at `http://math.stanford.edu/~bump/`.

[31] Emily Burgunder. Eulerian idempotent and Kashiwara-Vergne conjecture. *Annales de l'institut Fourier* **58** (2008), Issue 4, 1153–1184. `https://eudml.org/doc/10345`.

[32] Lynne M. Butler, Alfred W. Hales. Nonnegative Hall polynomials. *Journal of Algebraic Combinatorics* **2** (1993), Issue 2, 125–135. `https://www.emis.de/journals/JACO/Volume2_2/l42886q158156k2u.html`

[33] Stefaan Caenepeel, J. Vercruysse. Hopf algebras. *Lecture notes, Vrije Universiteit Brussel* **2013**. `http://homepages.ulb.ac.be/~scaenepe/Hopfalgebra.pdf`

[34] Peter J. Cameron. Notes on matroids and codes. *Lecture notes*, 2000. `http://www.maths.qmul.ac.uk/~pjc/comb/matroid.pdf`

[35] Pierre F. Cartier. A primer of Hopf algebras. Frontiers in number theory, physics, and geometry. II, 537–615, Springer, Berlin, 2007.
A preprint is available at `http://preprints.ihes.fr/2006/M/M-06-40.pdf`

[36] Vyjayanthi Chari, and Andrew N. Pressley. A guide to quantum groups. Cambridge University Press, Cambridge, 1994.

[37] Sunil K. Chebolu, Jan Minac. Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. *Math. Mag.* **84** (2011), 369–371. A preprint is `arXiv:1001.0409v6`.

[38] K.T. Chen, R.H. Fox, R.C. Lyndon. Free Differential Calculus, IV: The Quotient Groups of the Lower Central Series. *Annals of Mathematics* **68** (1), 81–95. `https://doi.org/10.2307/1970044`

[39] Sergei Chmutov, Sergei V. Duzhin, Jacob Mostovoy. Introduction to Vassiliev Knot Invariants. CUP 2012.
Various preprint versions can be found at `https://people.math.osu.edu/chmutov.1/preprints/` , at `http://www.pdmi.ras.ru/~duzhin/papers/cdbook/` and at `arXiv:1103.5628v3`.

[40] Keith Conrad. Expository papers ("Blurbs"), specifically *Tensor Products I*, *Tensor Products II*, *Exterior Powers*. `http://www.math.uconn.edu/~kconrad/blurbs`

[41] Henry Crapo and William Schmitt. Primitive elements in the matroid-minor Hopf algebra. *J. Algebraic Combin.* **28** (2008), 43–64. `https://doi.org/10.1007/s10801-007-0066-3`.
A preprint is `arXiv:math/0511033v1`.

[42] ______. A unique factorization theorem for matroids. *J. Combin. Theory Ser. A* **112** (2005), 222–249. `https://doi.org/10.1016/j.jcta.2005.02.004`

[43] ______. A free subalgebra of the algebra of matroids. *European J. Combin.* **26** (2005), 1066–1085. `https://doi.org/10.1016/j.ejc.2004.05.006`

[44] William Crawley-Boevey. *Lectures on representation theory and invariant theory*, Bielefeld 1989/90. Available from `https://www.math.uni-bielefeld.de/~wcrawley/`.

[45] Maxime Crochemore, Jacques Désarménien, Dominique Perrin. A note on the Burrows–Wheeler transformation. *Theoretical Computer Science* **332** (2005), pp. 567–572. `https://doi.org/10.1016/j.tcs.2004.11.014`
A preprint is `arXiv:cs/0502073`.

[46] Geir Dahl. Network flows and combinatorial matrix theory. Lecture notes, 4 September 2013. `http://www.uio.no/studier/emner/matnat/math/MAT-INF4110/h13/lecturenotes/combmatrix.pdf`

[47] Sorin Dascalescu, Constantin Nastasescu, Serban Raianu. Hopf algebras. An introduction. *Monographs and Textbooks in Pure and Applied Mathematics* **235**. Marcel Dekker, Inc., New York, 2001.

[48] Barry Dayton. Witt vectors, the Grothendieck Burnside ring, and Necklaces. http://orion.neiu.edu/~bhdayton/necksum.htm

[49] Tom Denton, Florent Hivert, Anne Schilling, and Nicolas M. Thiéry. On the representation theory of finite J-trivial monoids. *Sém. Lothar. Combin.* **64** (2010/11), Art. B64d, 44 pp. https://www.emis.de/journals/SLC/wpapers/s64dehiscth.html

[50] Jacques Désarménien, Michelle L. Wachs. Descent classes of permutations with a given number of fixed points. *Journal of Combinatorial Theory, Series A* **64**, Issue 2, pp. 311–328. https://doi.org/10.1016/0097-3165(93)90100-M

[51] Persi Diaconis, Michael Mc Grath, Jim Pitman. Riffle shuffles, cycles, and descents. *Combinatorica* **15**(1), 1995, pp. 11–29. https://doi.org/10.1007/bf01294457

[52] Persi Diaconis, C.Y. Amy Pang and Arun Ram. Hopf algebras and Markov chains: Two examples and a theory. *J. Algebraic Combin.* **39**, Issue 3, May 2014, 527–585. A newer version is available at https://amypang.github.io/papers/hpmc.pdf

[53] Francesco Dolce, Antonio Restivo, Christophe Reutenauer. On generalized Lyndon words. Theoretical Computer Science **777** (2019), 232–242. Also available at arXiv:1812.04515v1.

[54] Francesco Dolce, Antonio Restivo, Christophe Reutenauer. Some variations on Lyndon words. arXiv:1904.00954v1.

[55] William F. Doran IV. A Proof of Reutenauer's $-q_{(n)}$ Conjecture. *J. Combin. Theory, Ser. A* **74** (1996), 342–344. https://doi.org/10.1006/jcta.1996.0056

[56] Andreas W. M. Dress, and Christian Siebeneicher. On the number of solutions of certain linear diophantine equations. *Hokkaido Math. J.* **19** (1990), pp. 385–401. http://www.math.sci.hokudai.ac.jp/hmj/page/19-3/pdf/HMJ_19_3_1990_385-401.pdf

[57] Andreas W. M. Dress, and Christian Siebeneicher. The Burnside Ring of the Infinite Cyclic Group and Its Relations to the Necklace Algebra, $\lambda$-Rings, and the Universal Ring of Witt Vectors. *Advances in Mathematics* **78** (1989), 1–41. https://doi.org/10.1016/0001-8708(89)90027-3

[58] Gérard Duchamp, Florent Hivert, and Jean-Yves Thibon. Noncommutative symmetric functions VI. Free quasi-symmetric functions and related algebras. *Internat. J. Algebra Comput.* **12** (2002), 671–717. A preprint is available at http://monge.univ-mlv.fr/~hivert/PAPER/NCSF6.ps.

[59] Gérard H. E. Duchamp, Nguyen Hoang-Nghia, Thomas Krajewski, Adrian Tanasa. Recipe theorem for the Tutte polynomial for matroids, renormalization group-like approach. *Advances in Applied Mathematics* **51**(3), 345—358. https://doi.org/10.1016/j.aam.2013.04.006

[60] Gérard Henry Edmond Duchamp, Vincel Hoang Ngoc Minh, Christophe Tollu, Bùi Chiên, Nguyen Hoang Nghia. Combinatorics of $\varphi$-deformed stuffle Hopf algebras. arXiv:1302.5391v7.

[61] Tobias Dyckerhoff. Hall Algebras - Bonn, Wintersemester 14/15. Lecture notes, version February 5, 2015. https://web.archive.org/web/20150601115158/http://www.math.uni-bonn.de/people/dyckerho/notes.pdf

[62] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In: Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), Gordon and Breach, New York, 1970, pp. 66–87; reprinted in Combinatorial optimization: Eureka, you shrink!, pp. 11–26, *Lecture Notes in Comput. Sci.* **2570**, Springer, Berlin, 2003. https://doi.org/10.1007/3-540-36478-1_2

[63] Eric S. Egge. *An Introduction to Symmetric Functions and Their Combinatorics.* Student Mathematical Library **91**, American Mathematical Society, 2019. https://bookstore.ams.org/stml-91

[64] Richard Ehrenborg. On posets and Hopf algebras. *Adv. Math.* **119** (1996), 1–25. https://doi.org/10.1006/aima.1996.0026

[65] David Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry. *Graduate Texts in Mathematics* **150**, Springer 1995. https://doi.org/10.1007/978-1-4612-5350-1

[66] Sergi Elizalde, Justin M. Troyka. Exact and asymptotic enumeration of cyclic permutations according to descent set. *J. Combin. Theory, Ser. A* **165** (2019), 360–391. Also available at `arXiv:1710.05103v3`.

[67] Alexander P. Ellis, and Mikhail Khovanov. The Hopf algebra of odd symmetric functions. *Adv. Math.* **231** (2012), 965–999. A newer version is available as `arXiv:1107.5610v2`.

[68] Brittney Ellzey. On Chromatic Quasisymmetric Functions of Directed Graphs. PhD thesis, University of Miami, 2018. `https://scholarlyrepository.miami.edu/oa_dissertations/2091`

[69] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. Introduction to representation theory. *Student Mathematical Library* **59**, Amer. Math. Soc., Providence, RI, 2011. `http://www-math.mit.edu/~etingof/repb.pdf` . (Parts of this book appear in `arXiv:0901.0827v5`.) A newer version is available at `http://www-math.mit.edu/~etingof/reprbook.pdf` .

[70] Loic Foissy. Algèbres de Hopf combinatoires. `http://loic.foissy.free.fr/pageperso/Hopf.pdf`

[71] Loic Foissy. Free and cofree Hopf algebras. *Journal of Pure and Applied Algebra* **216**, Issue 2, February 2012, 480–494. `https://doi.org/10.1016/j.jpaa.2011.07.010` . A preprint is `arXiv:1010.5402v3`.

[72] Harold Fredricksen, James Maiorana. Necklaces of beads in $k$ colors and $k$-ary de Bruijn sequences. *Discrete Mathematics* **23** (1978), 207–210. `https://doi.org/10.1016/0012-365X(78)90002-X`

[73] William Fulton. Young Tableaux. *London Mathematical Society Student Texts* **35**, Cambridge University Press, Cambridge-New York, 1997. `https://doi.org/10.1017/CBO9780511626241`

[74] Adriano M. Garsia. Permutation q-enumeration with the Schur row adder. *PU. M. A. (Pure Mathematics and Applications)* **21** (2010), No. 2, 233–248. `http://puma.dimai.unifi.it/21_2/7_Garsia.pdf` (also mirrored at `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.432.8196&rep=rep1&type=pdf` ).

[75] Vesselin Gasharov. Incomparability graphs of (3+1)-free posets are s-positive. Proceedings of the 6th Conference on Formal Power Series and Algebraic Combinatorics (New Brunswick, NJ, 1994). *Discrete Math.* **157** (1996), 193–197. `https://doi.org/10.1016/S0012-365X(96)83014-7`

[76] Vesselin Gasharov. A Short Proof of the Littlewood-Richardson Rule. *European Journal of Combinatorics*, Volume 19, Issue 4, May 1998, Pages 451–453. `https://doi.org/10.1006/eujc.1998.0212`

[77] Israel M. Gelfand, Daniel Krob, Alain Lascoux, Bernard Leclerc, Vladimir S. Retakh, Jean-Yves Thibon. Noncommutative symmetric functions. *Adv. Math.* **112** (1995), 218–348. `https://doi.org/10.1006/aima.1995.1032`
A preprint is available as `arXiv:hep-th/9407124v1`.

[78] M. Gerstenhaber, S.D. Schack. The shuffle bialgebra and the cohomology of commutative algebras. *Journal of Pure and Applied Algebra* **70** (1991), 263–272. `https://doi.org/10.1016/0022-4049(91)90073-B`

[79] Ira M. Gessel. Multipartite P-partitions and inner products of skew Schur functions. Combinatorics and algebra (Boulder, Colo., 1983), 289–317, *Contemp. Math.* **34**, Amer. Math. Soc., Providence, RI, 1984. `http://people.brandeis.edu/~gessel/homepage/papers/multipartite.pdf`

[80] Ira M. Gessel. A Historical Survey of P-Partitions. 2015, `arXiv:1506.03508v1`. Published in: Patricia Hersh, Thomas Lam, Pavlo Pylyavskyy and Victor Reiner (eds.), *The Mathematical Legacy of Richard P. Stanley*, Amer. Math. Soc., Providence, RI, 2016, pp. 169–188.

[81] Ira M. Gessel, Antonio Restivo, Christophe Reutenauer. A Bijection between Words and Multisets of Necklaces. *European Journal of Combinatorics* **33** (2012), pp. 1537–1546. `https://doi.org/10.1016/j.ejc.2012.03.016`

[82] Ira M. Gessel, Christophe Reutenauer. Counting Permutations with Given Cycle Structure and Descent Set. *Journal of Combinatorial Theory, Series A* **64** (1993), 189–215. `https://doi.org/10.1016/0097-3165(93)90095-P`

[83] Ira M. Gessel, X.G. Viennot. Determinants, Paths, and Plane Partitions. preprint, 1989, `http://people.brandeis.edu/~gessel/homepage/papers/pp.pdf`

[84] Andrew Granville. Number Theory Revealed: A Masterclass. *Number Theory Revealed: The Series* **#1B**, American Mathematical Society 2019.

[85] Darij Grinberg. Double posets and the antipode of QSym. `arXiv:1509.08355v3`.

[86] Darij Grinberg. A constructive proof of Orzech's theorem. Preprint, 20 November 2016.
`https://www.cip.ifi.lmu.de/~grinberg/algebra/orzech.pdf`

[87] Frank D. Grosshans, Gian-Carlo Rota, Joel A. Stein. Invariant Theory and Superalgebras. *CBMS Regional Conference Series in Mathematics* **69**, American Mathematical Society, 1987. `https://bookstore.ams.org/cbms-69`

[88] A.M. Hamel, I.P. Goulden. Planar Decompositions of Tableaux and Schur Function Determinants. *Europ. J. Combinatorics* **16** (1995), 461–477. `https://doi.org/10.1016/0195-6698(95)90002-0`

[89] Michiel Hazewinkel. The algebra of quasi-symmetric functions is free over the integers. *Adv. Math.* **164** (2001), 283–300. `https://doi.org/10.1006/aima.2001.2017`

[90] Michiel Hazewinkel. Witt vectors. Part 1. In: M. Hazewinkel (ed.), *Handbook of Algebra* **6**, Elsevier 2009. Also available at `arXiv:0804.3888v1`.

[91] Michiel Hazewinkel. The Leibniz-Hopf Algebra and Lyndon Words. *Preprint AM CWI* **9612** (1996). `http://oai.cwi.nl/oai/asset/4828/04828D.pdf`

[92] Michiel Hazewinkel. Chen-Fox-Lyndon Factorization for Words over Partially Ordered Sets. *Journal of Mathematical Sciences* **131** (12-2005), Issue 6, 6027–6031. `https://doi.org/10.1007/s10958-005-0458-7`

[93] Michiel Hazewinkel, Nadiya Gubareni, and Vladimir V. Kirichenko. Algebras, rings and modules. Lie algebras and Hopf algebras. *Mathematical Surveys and Monographs* **168**. American Mathematical Society, Providence, RI, 2010.

[94] Robert Henderson. The Algebra Of Multiple Zeta Values. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.227.5432`

[95] Lars Hesselholt. Lecture notes on Witt vectors. `http://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.ps`

[96] Lars Hesselholt. The big de Rham–Witt complex. *Acta Math.* **214** (2015), 135–207. `https://doi.org/10.1007/s11511-015-0124-y`

[97] Florent Hivert. An introduction to combinatorial Hopf algebras: examples and realizations. *Nato Advanced Study Institute School on Physics and Computer Science, 2005, october, 17–29, Cargese, France.* `http://www-igm.univ-mlv.fr/~hivert/PAPER/Cargese.pdf`

[98] Florent Hivert, Jean-Christophe Novelli and Jean-Yves Thibon. Commutative combinatorial Hopf algebras. *J. Algebraic Combin.* **28** (2008), no. 1, 65–95. `https://doi.org/10.1007/s10801-007-0077-0`
Also available as `arXiv:math/0605262v1`.

[99] ______. The algebra of binary search trees. *Theoret. Comput. Sci.* **339** (2005), no. 1, 129–165. `https://doi.org/10.1016/j.tcs.2005.01.012`
A preprint appears as `arXiv:math/0401089v2`.

[100] ______. Trees, functional equations, and combinatorial Hopf algebras. *European J. Combin.* **29** (2008), no. 7, 1682–1695. `https://doi.org/10.1016/j.ejc.2007.09.005`
A preprint appears as `arXiv:math/0701539v1`.

[101] Michael E. Hoffman. Combinatorics of rooted trees and Hopf algebras. *Trans. AMS* **355** (2003), 3795–3811. `https://doi.org/10.1090/S0002-9947-03-03317-8`

[102] ______. A character on the quasi-symmetric functions coming from multiple zeta values. *The Electronic Journal of Combinatorics* **15** (2008), R97. `http://www.combinatorics.org/ojs/index.php/eljc/article/view/v15i1r97`

[103] Brandon Humpert, and Jeremy L. Martin. The incidence Hopf algebra of graphs. *SIAM Journal on Discrete Mathematics* **26**, no. 2 (2012), 555–570. Also available as `arXiv:1012.4786v3`.

[104] Gordon James and Martin Liebeck. Representations and characters of groups. 2nd edition, Cambridge University Press, Cambridge-New York, 2001.

[105] Emma Yu Jin. Outside nested decompositions of skew diagrams and Schur function determinants. *European Journal of Combinatorics* **67** (2018), 239–267. `https://doi.org/10.1016/j.ejc.2017.08.007` . A preprint is available at `http://www.emmayujin.at/Pubs/Jin18.pdf`.

[106] S.A. Joni and Gian-Carlo Rota. Coalgebras and bialgebras in combinatorics. *Studies in Applied Mathematics* **61** (1979), 93–139. `https://doi.org/10.1002/sapm197961293`

[107] Christian Kassel. Quantum groups. *Graduate Texts in Mathematics* **155**. Springer, Berlin, 1995.

[108] Sergei V. Kerov. Asymptotic representation theory of the symmetric group and its applications in analysis. *Translations of Mathematical Monographs* **219**. American Mathematical Society, Providence, RI, 2003.

[109] Anatol N. Kirillov, Arkadiy D. Berenstein. Groups generated by involutions, Gelfand-Tsetlin patterns and the combinatorics of Young tableaux. *Algebra i Analiz* **7** (1995), issue 1, 92–152. A preprint is available at `http://pages.uoregon.edu/arkadiy/bk1.pdf`

[110] T. Klein. The multiplication of Schur-functions and extensions of $p$-modules. *J. London Math. Soc.* **43** (1968), 280–284. `https://doi.org/10.1112/jlms/s1-43.1.280`

[111] Donald E. Knuth. Permutations, matrices, and generalized Young tableaux. *Pacific J. Math.* **34**, Number 3 (1970), 709–727. `https://projecteuclid.org/euclid.pjm/1102971948`

[112] Donald E. Knuth. The Art of Computer Programming, Volume 4A: Combinatorial Algorithms, Part 1. Pearson 2011. See `https://www-cs-faculty.stanford.edu/~knuth/taocp.html` for errata.

[113] Donald Knutson. $\lambda$-Rings and the Representation Theory of the Symmetric Group. *Lecture Notes in Mathematics* **308**, Springer, Berlin-Heidelberg-New York 1973. `https://doi.org/10.1007/BFb0069217`

[114] Manfred Krause. A Simple Proof of the Gale-Ryser Theorem. *The American Mathematical Monthly* **103** (1996), 335–337. `https://doi.org/10.2307/2975191`

[115] Daniel Krob. Eléments de combinatoire. Magistère 1-ère année, Ecole Normale Supérieure, version 1.0, Novembre 1995. `http://krob.cesames.net/IMG/ps/combi.ps`

[116] Manfred Kufleitner. On Bijective Variants of the Burrows-Wheeler Transform. Presented at the Prague Stringology Conference 2009 (PSC 2009). `arXiv:0908.0239v1`.

[117] Andrius Kulikauskas, Jeffrey Remmel. Lyndon words and transition matrices between elementary, homogeneous and monomial symmetric functions. *Electronic Journal of Combinatorics* **13** (2006), Research Paper ♯R18. `http://www.combinatorics.org/ojs/index.php/eljc/article/view/v13i1r18`

[118] Kalle Kytölä. Introduction to Hopf algebras and representations. Lecture notes, Spring 2011. `https://math.aalto.fi/~kkytola/files_KK/lectures_files_KK/Hopf-lecture_notes.pdf`

[119] Dan Laksov, Alain Lascoux, Piotr Pragacz, and Anders Thorup. The LLPT Notes. Edited by A. Thorup, 1995–2018. `http://web.math.ku.dk/noter/filer/sympol.pdf`

[120] Thomas Lam, Aaron Lauve, and Frank Sottile. Skew Littlewood-Richardson rules from Hopf Algebras. *DMTCS Proceedings, 22nd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2010)* **2010**, 355–366. A preprint can also be found at `arXiv:0908.3714v3`.

[121] Thomas Lam, and Pavlo Pylyavskyy. Combinatorial Hopf algebras and K-homology of Grassmanians. *International Mathematics Research Notices*, **2007** (2007), rnm 125, 48 pages. A preprint is `arXiv:0705.2189v1`.

[122] Sergei K. Lando. On a Hopf Algebra in Graph Theory. *Journal of Combinatorial Theory, Series B* **80** (2000), 104–121. `https://doi.org/10.1006/jctb.2000.1973`

[123] Aaron D. Lauda, Heather M. Russell. Oddification of the cohomology of type A Springer varieties. *International Math Research Notices* **2014**, No. 17, 4822–4854. A preprint is `arXiv:1203.0797v1`.

[124] Hartmut Laue. Freie algebraische Strukturen. Lecture notes, Mathematisches Seminar der Universität Kiel 2013, version 16 Sep 2013. `http://www.uni-kiel.de/math/algebra/laue/vorlesungen/frei/freiealgstr.pdf`

[125] Aaron Lauve and Sarah K. Mason. QSym over Sym has a stable basis. FPSAC 2010, San Francisco, USA. *DMTCS proc. AN* **2010**, 367–378. Also available as `arXiv:1003.2124v1`.

[126] Marc van Leeuwen. Schur functions and alternating sums. *Electronic Journal of Combinatorics* **11(2)** A5 (2006). Also available at `http://www-math.univ-poitiers.fr/~maavl/pdf/alt-Schur.pdf`.

[127] Marc van Leeuwen. Flag varieties, and interpretations of Young tableau algorithms. *Journal of Algebra* **224** (2000). Also available at `http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/geometry.pdf`

[128] Marc van Leeuwen. An application of Hopf-Algebra techniques to representations of finite Classical Groups. *Journal of Algebra* **140**, Issue 1, 15 June 1991, pp. 210–246. Also available at `http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/Hopf.pdf`

[129] Marc van Leeuwen. The Littlewood-Richardson rule, and related combinatorics. *Math. Soc. of Japan Memoirs* **11**, Interaction of Combinatorics and Representation Theory. Also available at `http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/lrr.pdf`

[130] Marc van Leeuwen. The Robinson-Schensted and Schützenberger algorithms, an elementary approach. *Electronic Journal of Combinatorics*, Foata Festschrift, **3** (no. 2), R15 (1996). Also available at `http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/foata-fest.pdf`

[131] Ji Li. Prime Graphs and Exponential Composition of Species. *Journal of Combinatorial Theory, Series A* **115**, Issue 8, November 2008, 1374–1401. See `arXiv:0705.0038v4` for a preprint.

[132] Ricky Ini Liu. A simplified Kronecker rule for one hook shape. *Proc. Amer. Math. Soc.* **145** (2017), pp. 3657–3664. `https://doi.org/10.1090/proc/13692` See `arXiv:1412.2180v1` for a preprint.

[133] Arunas Liulevicius. Arrows, symmetries and representation rings. *Journal of Pure and Applied Algebra* **19** (1980), 259–273. `https://doi.org/10.1016/0022-4049(80)90103-6`

[134] Jean-Louis Loday. Cyclic Homology. *Grundlehren der mathematischen Wissenschaften* **301**, 2nd edition, Springer, Berlin-Heidelberg 1998.

[135] Jean-Louis Loday. Série de Hausdorff, idempotents Eulériens et algèbres de Hopf. *Expo. Math.* **12** (1994), 165–178. `http://www-irma.u-strasbg.fr/~loday/PAPERS/94Loday%28Eulerien%29.pdf`

[136] Jean-Louis Loday and María O. Ronco. Combinatorial Hopf algebras. Quanta of maths, *Clay Math. Proc.* **11**, 347–383, Amer. Math. Soc., Providence, RI, 2010. `http://www-irma.u-strasbg.fr/~loday/PAPERS/2011LodayRonco(CHA).pdf`

[137] ———. Hopf algebra of the planar binary trees. *Adv. Math.* **139** (1998), no. 2, 293–309. `https://doi.org/10.1006/aima.1998.1759`

[138] Nicholas A. Loehr. Bijective Combinatorics. CRC Press, 2011. See `http://www.math.vt.edu/people/nloehr/bijbook.html` for errata.

[139] M. Lothaire. *Combinatorics on words.* Corrected printing, Cambridge University Press, 1997.

[140] Kurt Luoto, Stefan Mykytiuk, Stephanie van Willigenburg. An introduction to quasisymmetric Schur functions – Hopf algebras, quasisymmetric functions, and Young composition tableaux. Springer, May 23, 2013. `http://www.math.ubc.ca/~steph/papers/QuasiSchurBook.pdf`

[141] R.C. Lyndon. On Burnside's Problem. *Transactions of the AMS* **77**, 202–215. `https://doi.org/10.1090/S0002-9947-1954-0064049-X`

[142] Ian Grant Macdonald. Symmetric functions and Hall polynomials. 2nd edition, Oxford University Press, Oxford-New York, 1995.

[143] I.G. Macdonald. Schur functions : theme and variations. *Publ. I.R.M.A. Strasbourg*, **1992**, 498/S-27, Actes 28 e Seminaire Lotharingien, 5–39. `https://www.emis.de/journals/SLC/opapers/s28macdonald.html`

[144] Manuel Maia, Miguel Méndez. On the arithmetic product of combinatorial species. *Discrete Mathematics* **308**, Issue 23, 6 December 2008, 5407–5427. `https://doi.org/10.1016/j.disc.2007.09.062` .
See `arXiv:math/0503436v2` for a preprint.

[145] Claudia Malvenuto. Produits et coproduits des fonctions quasi-symétriques et de l'algèbre des descents. PhD dissertation, Univ. du Québéc à Montreal, 1993. `http://lacim.uqam.ca/wp-content/uploads/Publications/16.pdf`

[146] Clauda [sic] Malvenuto and Christophe Reutenauer. Duality between quasi-symmetric functions and the Solomon descent algebra. *J. Algebra* **177** (1995), 967–982. `https://doi.org/10.1006/jabr.1995.1336`

[147] Claudia Malvenuto and Christophe Reutenauer. Plethysm and conjugation of quasi-symmetric functions. *Discrete Mathematics* **193**, Issues 1–3, 28 November 1998, 225–233. `https://doi.org/10.1016/S0012-365X(98)00142-3`

[148] Claudia Malvenuto and Christophe Reutenauer. A self paired Hopf algebra on double posets and a Littlewood-Richardson rule. *Journal of Combinatorial Theory, Series A* **118** (2011), 1322–1333. `https://doi.org/10.1016/j.jcta.2010.10.010`

[149] Dominique Manchon. Hopf algebras, from basics to applications to renormalization. *Comptes Rendus des Rencontres Mathematiques de Glanon* 2001 (published in 2003). `arXiv:math/0408405v2`.

[150] Marco Manetti. A voyage round coalgebras. 27 June 2016. `https://www1.mat.uniroma1.it/people/manetti/dispense/voyage.pdf`

[151] Laurent Manivel. Chern classes of tensor products. `arXiv:1012.0014v1`.

[152] Peter R.W. McNamara, Ryan E. Ward. Equality of $P$-partition generating functions. `arXiv:1210.2412v2`.

[153] Pierre-Loïc Méliot. Representation Theory of Symmetric Groups. *Discrete Mathematics and its Applications*, CRC Press 2017.

[154] Anthony Mendes, Jeffrey Remmel. Counting with Symmetric Functions. *Developments in Mathematics* **43**, Springer 2015.

[155] Miguel Mendez. *MathOverflow answer #139482*. `http://mathoverflow.net/a/139482/`.

[156] John W. Milnor and John C. Moore. On the structure of Hopf algebras. *The Annals of Mathematics, Second Series* **81**, No. 2 (Mar., 1965), 211–264. `https://doi.org/10.2307/1970615`

[157] Susan Montgomery. Hopf algebras and their actions on rings. *Regional Conference Series in Mathematics* **82**, Amer. Math. Soc., Providence, RI, 2010. `https://bookstore.ams.org/cbms-82`

[158] Jack Morava. Homotopy-theoretically enriched categories of noncommutative motives. *Research in the Mathematical Sciences* **2** (2015), no. 8. `https://doi.org/10.1186/s40687-015-0028-7`

[159] Eduardo Moreno. On the theorem of Fredricksen and Maiorana about de Bruijn sequences. *Advances in Applied Mathematics* **33**, Issue 2, August 2004, 413–415. `https://doi.org/10.1016/j.aam.2003.10.002`

[160] Eduardo Moreno, Dominique Perrin. Corrigendum to "On the theorem of Fredricksen and Maiorana about de Bruijn sequences" [Adv. in Appl. Math. 33 (2) (2004) 413–415]. *Advances in Applied Mathematics* **62**, January 2015, Pages 184–187. `http://www.sciencedirect.com/science/article/pii/S0196885814000918`

[161] Jeremy L. Martin, Matthew Morin, Jennifer D. Wagner. On distinguishing trees by their chromatic symmetric functions. *Journal of Combinatorial Theory, Series A* **115**, Issue 2, February 2008, 237–253. `https://doi.org/10.1016/j.jcta.2007.05.008`

[162] Robert Morris. Umbral Calculus and Hopf Algebras. *Contemporary Mathematics* **6**, AMS, Providence 1982. `https://bookstore.ams.org/conm-6`

[163] Jakob Oesinghaus. Quasisymmetric functions and the Chow ring of the stack of expanded pairs. *Res. Math. Sci.* **6** (2019), no. 5. `https://doi.org/10.1007/s40687-018-0168-7` . A preprint is `arXiv:1806.10700v1`.

[164] James Oxley. Matroid theory. Oxford University Press, Oxford-New York, 1992.

[165] Igor Pak, Alexander Postnikov. Oscillating Tableaux, $S_p \times S_q$-modules, and Robinson-Schensted-Knuth Correspondence. Updated (yet unfinished) version of FPSAC 1996 abstract, January 15, 1994. `http://math.mit.edu/~apost/papers/osc.pdf`

[166] Frédéric Patras. La décomposition en poids des algèbres de Hopf. *Annales de l'institut Fourier* **43**, no 4 (1993), 1067–1087. `https://eudml.org/doc/75026`

[167] F. Patras. L'algèbre des descentes d'une bigèbre graduée. *Journal of Algebra* **170** (1994), 547–566. `https://doi.org/10.1006/jabr.1994.1352`

[168] Frédéric Patras, Christophe Reutenauer. On Dynkin and Klyachko idempotents in graded bialgebras. *Advanced in Applied Mathematics* **28**, Issues 3–4, April 2002, 560–579. `https://doi.org/10.1006/aama.2001.0795`

[169] Frédéric Patras, Christophe Reutenauer. Higher Lie idempotents. *J. Algebra* **222** (1999), no. 1, 51–64. `https://doi.org/10.1006/jabr.1999.7887`

[170] Rebecca Patrias. Antipode formulas for combinatorial Hopf algebras. `arXiv:1501.00710v2`. Published in: *The Electronic Journal of Combinatorics* **23**, Issue 4 (2016), P4.30. `http://www.combinatorics.org/ojs/index.php/eljc/article/view/v23i4p30/`

[171] Victor Prasolov. Problems and theorems in linear algebra. *Translations of mathematical monographs* **134**, 1st edition 1994, AMS. `http://www2.math.su.se/~mleites/books/prasolov-1994-problems.pdf`

[172] Stéphane Poirier, Christophe Reutenauer. Algèbres de Hopf de tableaux. *Ann. Sci. Math. Québec* **19** (1995), no. 1, 79–90. `http://www.lacim.uqam.ca/~christo/Publi%C3%A9s/1995/Alg%C3%A8bres%20de%20Hopf%20de%20tableaux.pdf`

[173] Alexander Postnikov. Permutohedra, associahedra, and beyond. *Int. Math. Res. Notices* **2009**, No. 6, pp. 1026–1106. A preprint appears at `https://math.mit.edu/~apost/papers/permutohedron.pdf` and as `arXiv:math/0507163v1`.

[174] Amritanshu Prasad. An Introduction to Schur Polynomials. *Graduate J. Math.* **4** (2019), 62–84. `https://www.gradmath.org/wp-content/uploads/2020/01/Prasad-GJM2019.pdf` . A preprint appears at `arXiv:1802.06073v2`.

[175] Pavlo Pylyavskyy. Comparing products of Schur functions and quasisymmetric functions. PhD dissertation, MIT, 2007. `https://dspace.mit.edu/handle/1721.1/38957`

[176] David E. Radford. Hopf algebras. *Series on Knots and Everything* **49**. World Scientific, 2012. `https://doi.org/10.1142/8055`

[177] David E. Radford. A Natural Ring Basis for the Shuffle Algebra and an Application to Group Schemes. *Journal of Algebra* **58** (1979), 432–454. `https://doi.org/10.1016/0021-8693(79)90171-6`

[178] Nathan Reading. Lattice congruences, fans and Hopf algebras. *Journal of Combinatorial Theory, Series A* **110**, Issue 2, May 2005, pp. 237–273. `https://doi.org/10.1016/j.jcta.2004.11.001` . A preprint is `arXiv:math/0402063v1`.

[179] Victor Reiner. Signed permutation statistics and cycle type. *European J. Combin.* **14** (1993), no. 6, 569–579. `https://doi.org/10.1006/eujc.1993.1059`

[180] Victor Reiner, Kristin M. Shaw, and Stephanie van Willigenburg. Coincidences among skew Schur functions. `arXiv:math/0602634v4`. (Update of a paper published in *Advances in Mathematics*, **216(1)**:118–152, 2007.)

[181] Jeffrey B. Remmel. The combinatorics of $(k, \ell)$-hook Schur functions. In: C. Greene (ed.), *Combinatorics and algebra*, Proceedings of the AMS-IMS-SIAM joint summer research conference in the mathematical sciences on combinatorics and algebra, Colorado, Boulder, 1983, *Contemporary Mathematics* **34**, 1984, 253–287.

[182] Christophe Reutenauer. Free Lie Algebras. *London Mathematical Society Monographs, New Series* **7**. Clarendon Press, Oxford 1993.

[183] Mercedes H. Rosas. The Kronecker Product of Schur Functions Indexed by Two-Row Shapes or Hook Shapes. *Journal of Algebraic Combinatorics* **14** (2001), 153–173. `https://doi.org/10.1023/A:1011942029902`
A preprint is `arXiv:math/0001084v1`.

[184] Mercedes H. Rosas, Bruce E. Sagan. Symmetric functions in noncommuting variables. *Transactions of the American Mathematical Society* **358**, 183–214. https://doi.org/10.1090/S0002-9947-04-03623-2

[185] Joseph P.S. Kung, Gian-Carlo Rota. Gian-Carlo Rota on Combinatorics: Introductory Papers and Commentaries. Birkhäuser 1995.

[186] Bruce E. Sagan. The symmetric group: representations, combinatorial algorithms, and symmetric functions. 2nd edition, Springer, New York-Berlin-Heidelberg 2001. See https://users.math.msu.edu/users/bsagan/Books/Sym/errata.pdf for errata.

[187] Bruce E. Sagan. Combinatorics: The Art of Counting. Draft of a textbook, 2020. https://users.math.msu.edu/users/bsagan/Books/Aoc/aocAMS.pdf

[188] Bruce E. Sagan, Richard P. Stanley. Robinson-Schensted Algorithms for Skew Tableaux. *Journal of Combinatorial Theory, Series A* **55** (1990), 161–193. https://doi.org/10.1016/0097-3165(90)90066-6

[189] Steven V. Sam. Notes for Math 740 (Symmetric Functions), 27 April 2017. https://www.math.wisc.edu/~svs/740/notes.pdf

[190] Olivier Schiffmann. Lectures on Hall algebras. arXiv:math/0611617v2.

[191] William R. Schmitt. Incidence Hopf algebras. *Journal of Pure and Applied Algebra* **96** (1994), 299–330. https://doi.org/10.1016/0022-4049(94)90105-8 . A preprint appears at http://home.gwu.edu/~wschmitt/papers/iha.pdf

[192] William R. Schmitt. Antipodes and Incidence Coalgebras. *Journal of Combinatorial Theory, Series A* **46** (1987), 264–290. https://doi.org/10.1016/0097-3165(87)90006-9

[193] William R. Schmitt. Expository notes, specifically "A concrete introduction to category theory" and "Notes on modules and algebras". http://home.gwu.edu/~wschmitt/

[194] ______. Hopf algebras of combinatorial structures. *Canadian Journal of Mathematics* **45** (1993), 412–428. https://doi.org/10.4153/CJM-1993-021-5 . A preprint appears at http://home.gwu.edu/~wschmitt/papers/hacs.pdf

[195] I. Schur. Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung. *Compositio Mathematica* **4** (1937), 432–444. http://www.numdam.org/item?id=CM_1937__4__432_0

[196] Christoph Schweigert. Hopf algebras, quantum groups and topological field theory. Lecture notes, Winter term 2014/15, Hamburg. Version of 16 May 2015. http://www.math.uni-hamburg.de/home/schweigert/ws12/hskript.pdf

[197] Jean-Pierre Serre. Linear representations of finite groups. Springer, Berlin-Heidelberg-New York, 1977. https://doi.org/10.1007/978-1-4684-9458-7

[198] John Shareshian and Michelle L. Wachs. Chromatic quasisymmetric functions and Hessenberg varieties. In: A. Björner, F. Cohen, C. De Concini, C. Procesi, M. Salvetti (Eds.), Configuration Spaces, *Publications of the Scuola Normale Superiore* **14**, Springer, Berlin-Heidelberg-New York 2013. A preprint is arXiv:1106.4287v3.

[199] John Shareshian and Michelle L. Wachs. Chromatic quasisymmetric functions. *Advances in Mathematics* **295** (2016), pp. 497–551. A preprint is arXiv:1405.4629v2.

[200] John Shareshian and Michelle L. Wachs. Eulerian quasisymmetric functions. *Advances in Mathematics* **225** (2010), pp. 2921–2966. https://doi.org/10.1016/j.aim.2010.05.009 . A preprint is arXiv:0812.0764v2

[201] Seth Shelley-Abrahamson. Hopf Modules and Representations of Finite Groups of Lie Type. Honors thesis, Stanford, May 2013. http://mathematics.stanford.edu/wp-content/uploads/2013/08/Shelley-Abrahamson-Honors-Thesis-2013.pdf

[202] Anatolii I. Shirshov. On Free Lie Rings. *Mat. Sbornik N.S.* **45** (87), (1958), no. 2, 113–122. Original at: http://mi.mathnet.ru/msb4963. Translation in: L.A. Bokut, V. Latyshev, I. Shestakov, E. Zelmanov (eds.), *Selected works of A.I. Shirshov*, Birkhäuser 2009.

[203] Richard P. Stanley. Ordered structures and partitions. *Memoirs of the Amer. Math. Soc.* **119**, American Mathematical Society, Providence, R.I., 1972. http://www-math.mit.edu/~rstan/pubs/pubfiles/9.pdf

[204] ______. Acyclic orientations of graphs. *Discrete Math.* **5** (1973), 171–178. Reprinted in: *Discrete Math.* **306** (2006), 905–909. https://doi.org/10.1016/j.disc.2006.03.010

[205] ______. A symmetric function generalization of the chromatic polynomial of a graph. *Adv. Math.* **111** (1995), 166–194. https://doi.org/10.1006/aima.1995.1020

[206] ______. Enumerative Combinatorics, Volumes 1 and 2. *Cambridge Studies in Advanced Mathematics*, **49** and **62**. Cambridge University Press, Cambridge, 2nd edition 2011 (volume 1) and 1st edition 1999 (volume 2).

[207] Shishuo Fu, Victor Reiner, Dennis Stanton, Nathaniel Thiem. The negative $q$-binomial. *The Electronic Journal of Combinatorics* **19**, Issue 1 (2012), P36. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v19i1p36

[208] R. Steinberg. A geometric approach to the representations of the full linear group over a Galois field. *Trans. Amer. Math. Soc.* **71**, (1951), 274–282. https://doi.org/10.1090/S0002-9947-1951-0043784-0

[209] Jacob Steinhardt. Permutations with Ascending and Descending Blocks. *The Electronic Journal of Combinatorics* **17** (2010), #R14. https://www.combinatorics.org/ojs/index.php/eljc/article/view/v17i1r14

[210] John R. Stembridge. A concise proof of the Littlewood-Richardson rule. *The Electronic Journal of Combinatorics* **9**, 2002, N5. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v9i1n5

[211] John Stembridge. Multiplicity-Free Products of Schur Functions. *Annals of Combinatorics* **5** (2001), 113–121. http://www.math.lsa.umich.edu/~jrs/papers/mfree.ps.gz

[212] Gilbert Strang. The algebra of Elimination. http://www-math.mit.edu/~gs/papers/Paper7_ver8.pdf.

[213] Moss E. Sweedler. Hopf algebras. W.A. Benjamin, New York, 1969.

[214] Mitsuhiro Takeuchi. Free Hopf algebras generated by coalgebras. *J. Math. Soc. Japan* **23** (1971), 561–582. http://projecteuclid.org/euclid.jmsj/1259849779

[215] Harry Tamvakis. The theory of Schur polynomials revisited. *Enseign. Math.* **58** (2012), 147–163. A preprint appears at http://www2.math.umd.edu/~harryt/papers/schurrev.pdf

[216] Jean-Yves Thibon. An Introduction to Noncommutative Symmetric Functions. Cargese lecture, October 2005. J.-P. Gazeau, J. Nesetril, B. Rovan (eds.): From Numbers and Languages to (Quantum) Cryptography, *NATO Security through Science Series: Information and Communication Security* **7**, IOS Press, 2007. Available at http://igm.univ-mlv.fr/~jyt/ARTICLES/cargese_thibon.ps.

[217] Nathaniel Thiem and C. Ryan Vinroot. On the characteristic map of finite unitary groups. *Advances in Mathematics* **210**, Issue 2, 1 April 2007, pp. 707–732. https://doi.org/10.1016/j.aim.2006.07.018 . A preprint is http://www.math.wm.edu/~vinroot/charunitary.pdf

[218] Hugh Thomas, Alexander Yong. An $S_3$-symmetric Littlewood-Richardson rule. *Math. Res. Lett.* **15** (2008), no. 5, 1027–1037. arXiv:0704.0817v1.

[219] Stijn Vermeeren. Sequences and nets in topology. Version of 11 September 2013. http://stijnvermeeren.be/download/mathematics/nets.pdf

[220] Michelle L. Wachs. Flagged Schur Functions, Schubert Polynomials, and Symmetrizing Operators. *Journal of Combinatorial Theory, Series A* **40** (1985), 276–289. https://doi.org/10.1016/0097-3165(85)90091-3

[221] Bartel Leendert van der Waerden. Algebra, Volume I. Translation of the 7th (German) edition. Springer 2003.

[222] Peter Webb. A Course in Finite Group Representation Theory. 23 February 2016. http://www-users.math.umn.edu/~webb/RepBook/

[223] Mark Wildon. Representation theory of the symmetric group. 5 April 2018. http://www.ma.rhul.ac.uk/~uvah099/teaching.html

[224] Mark Wildon. An involutive introduction to symmetric functions. 8 May 2020. http://www.ma.rhul.ac.uk/~uvah099/teaching.html

[225] Robert Wisbauer. Coalgebras and Bialgebras. *The Egyptian Mathematical Society, The Mathematical Sciences Research Centre (MSRC) Technical Reports* **No. 1**, 2004. `http://www.math.uni-duesseldorf.de/~wisbauer/`

[226] Qimh Richey Xantcha. Binomial Rings: Axiomatisation, Transfer, and Classification. `arXiv:1104.1931v4`.

[227] Andrey V. Zelevinsky. Representations of finite classical groups: a Hopf algebra approach. *Lecture Notes in Mathematics* **869**. Springer-Verlag, Berlin-New York, 1981.

[228] Andrey V. Zelevinsky. A Generalization of the Littlewood-Richardson Rule and the Robinson-Schensted-Knuth Correspondence. *Journal of Algebra* **69** (1981), 82–94. `https://doi.org/10.1016/0021-8693(81)90128-9`

[229] G.-S. Zhou, D.-M. Lu. Lyndon words for Artin-Schelter regular algebras. `arXiv:1403.0385v1`.

# Index