Oberwolfach
Preprints

OWP 2012 - 05

JEROEN SCHILLEWAERT AND KOEN THAS

Categoric Aspects of Authentication

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

Oberwolfach Preprints (OWP)

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.

Categoric Aspects of Authentication

Jeroen Schillewaert and Koen Thas

FREE UNIVERSITY OF BRUSSELS (ULB), DEPARTMENT OF MATHEMATICS,
CP 216, BOULEVARD DU TRIOMPHE, B-1050 BRUSSELS, BELGIUM
E-mail address: jschille@ulb.ac.be
URL: http://www.jeroenschillewaert.com

GHENT UNIVERSITY, DEPARTMENT OF MATHEMATICS, KRIJGSLAAN 281, S25,
B-9000 GHENT, BELGIUM
E-mail address: kthas@cage.UGent.be
URL: http://cage.ugent.be/∼kthas

2000 *Mathematics Subject Classification.* 18B99 68P30 94A62 20B25 51E12 51E15 51E20

Key words and phrases. Authentication code, category, morphism, construction

Contents

CHAPTER 1

Foreword

One of the main problems we want to address is the fact that in the construction theory of authentication codes, the expression “new code” is used all the time, while almost never it is shown that the obtained codes indeed *are* new, or even what the notion “new” means to begin with. In this text, we introduce an entirely new viewpoint on the theory of authentication codes, in which we are able to compare these code systems (having such notions as “isomorphisms” and “automorphisms” at hand), shedding as such new lights on the theory. One of the features is that authentication codes can now be studied using the invariant of automorphism groups. In our approach, we then define operations which enable us to “multiply” and “add” arbitrary authentication codes, regardless of how they are initially constructed, so as to obtain other (nonisomorphic) codes with easily calculated parameters. The number of newly constructed codes is huge.

The present text differs in some ways from the versions [**10**]-[**11**] which are submitted for publication as papers. For one, we added an informal discussion on codes with arbitration (besides mixing both manuscripts into one coherent file), and inserted a number of “blackboard drawings” to illustrate some of the features. Also, we aimed at providing an introduction to the synthetic side of authentication, and included more introductory definitions and examples than in [**10, 11**].

Very likely, some mistakes and typos are still creeping through the manuscipt, but we hope the reader will not be bothered by this.

Acknowledgement. This research was supported through the programme “Research in Pairs” by the Mathematisches Forschungsinstitut Oberwolfach (MFO) in 2010.
A big part of the manuscript was written in the MFO, while the authors enjoyed the tremendous atmosphere of the institute, being hosted as true chosen Kings.

Jeroen Schillewaert and Koen Thas
November 2010—December 2011

CHAPTER 2

Introduction

Ever since Simmons introduced the concept of authentication code (scheme) in [**12**], a vast amount of literature has appeared, especially through the construction theory of examples, and especially with direct application in mind. An important feature in this construction theory is that not only an abundance of examples, and hence of their associated parameters, are known, but also that almost as many "different" constructions are known, for instance through the use of elliptic curves, projective planes and other combinatorial designs, elementary arithmetic, Galois geometries, etc. In fact, the prototypical example *avant la lettre* by Gilbert-McWilliams-Sloane uses projective planes defined over the finite field $\mathbb{F}_q$ with q elements. (Other constructions of geometrical nature can be found in the recent work [**4**].)

In the published literature, a rather big problem has arisen.

Often, authentication code schemes look totally different, for instance because one is constructed with the use of combinatorial designs, and the other with the use of elliptic curves, while they easily could be exactly the same; they could have not only the *same* parameters (number of keys, number of messages, attack probability parameters, etc.), but also be *isomorphic* in a precise sense of the word. That is, from the point of view of the coding scheme, no distinction can be made between the constructions while *a priori* they could *seem* different. So in order to claim that a "new" construction is *really* new — a claim which unfortunately appears to be a stubborn inhabitant of the literature — we need a good comparison theory. The latter seems to be totally missing.

The solution of this problem is one of the main features of the present text: we propose a universal approach to authentication codes, in which we can *compare* authentication codes in a precise sense, that is, which makes us able to decide when a given construction of authentication schemes is really new. In other words, we want to study authentication codes as a *category*.

A pleasant byproduct of our approach is that we can also measure the "strength" of a construction: often, when an authentication code scheme is constructed through the use of some mathematical structure, only a modest number of features of the structure is really used, that is, not the whole mathematical structure is used to define the scheme. In examples where this is the case, often much more simple constructions exist in more general mathematical structures (with less structure); our invariant measures how intimately the authentication code is connected (or, is dependent) with/on the mathematical structure in which it is constructed. The farther the code is from the structure in this sense, the worse the construction is (and the easier it unfortunately is to claim that the code is “new”, because it is completely hidden behind the redundant mathematical structure). Simply said: much too often, constructions are too complicated, while the exact same scheme can be produced in a much more transparent way. (And then it appears it is not new at all.)

We introduce authentication code schemes as abstract data (of some sets and some maps between these sets), which allow us to study all authentication codes in a unified way. Not only are we then easily capable of comparing (and hence distinguishing) codes — two natural operations “addition” ($\oplus$) and “multiplication” ($\otimes$) arise which make it possible to combine any two (and hence any finite number of) authentication codes to give new ones via these operations. We then obtain precise formulas which relate the parameters of the new codes to the parameters of the given codes. It then becomes very easy to construct a true mass of new (in the real sense, i.e., nonisomorphic) authentication codes, with new parameters, without having to go through a physical construction process.

The great strength of this feature is that we can start with any two codes, for example one constructed in a Galois geometry and one constructed by elementary Number Theory, and then just obtain infinitely many other authentication codes by combining the two operations, while we have complete control over the parameters of the newly constructed codes! In fact, we will prove a theorem in this context which essentially states that if given is a set of parameters which do not violate the necessary arithmetical existence conditions for authentication codes, it is also sufficient for such a code to exist. So our operations describe an easily implemented algorithm which can combine any finite number of given codes to produce new ones with easy-to-calculate parameters.

We will illustrate the theoretical considerations (abstract definition, the operations “$\oplus$” and “$\otimes$”, isomorphisms, etc.) we make by means of several concrete examples. As a very general illustration of our theory, we introduce what we call “group schemes”, and show that many of the known constructions (which are at first sight completely unrelated!) are special cases of this type of code. Again this underlines our point: exactly the same coding schemes often appear through very different guises. We then apply several features of our theory to this kind of code.

CHAPTER 3

Authentication

This chapter is strongly based on the reference work [**9**], and a lot more can be found there.

Authentication is very important in information security, when e.g. Alice and Bob try to exchange messages. It provides protection against malicious persons trying to change messages or to impersonate the sender of these messages. There are two main models:

- one where Alice and Bob trust each other, called *A-codes*;
- one where they do not, called A^2*-codes*.

In the latter case, an *arbiter* is needed.

We denote the set of all source states by $\mathscr{S}$, the set of keys by $\mathscr{K}$, the set of encoding rules by $\mathscr{E}$ and the set of all possible encoded messages by $\mathscr{M}$.

1. A-Model

In the A-model, sender Alice and receiver Bob agree upon a secret private key k. With each key there is associated a unique encoding rule e. Alice selects a source state s and encodes s into a message m using the encoding rule e corresponding to the chosen key k. After having received the message Bob checks whether it lies in the range $e(\mathscr{S})$. If it does, then the message is accepted as authentic. Bob can recover the possible source states as the preimage of the message under e. If this preimage is always unique, then we say the code is *Cartesian*. So once the message is observed, one can retrack the corresponding source state. Whence there is no secrecy involved here.

An opponent can try to construct a message lying in $e(\mathscr{S})$ after observing r valid messages. The probability of success of such a spoofing attack will be denoted by P_r.

2. A^2-Model

In the A^2-model, we assume that Alice and Bob do not trust each other. In this case, they do not agree upon an encoding rule. Instead, a trusted person, the *arbiter*, is also involved in the scheme. Now Alice has a set of encoding rules $\mathscr{E}_T$, and Bob a set of decoding rules $\mathscr{E}_R$. If Alice and Bob want to communicate, Bob chooses a decoding rule $f \in \mathscr{E}_R$ and sends it to the arbiter. For every given f and given source state s there is a set of *valid* messages $\mathscr{M}(s, f)$. On receipt of f the arbiter selects

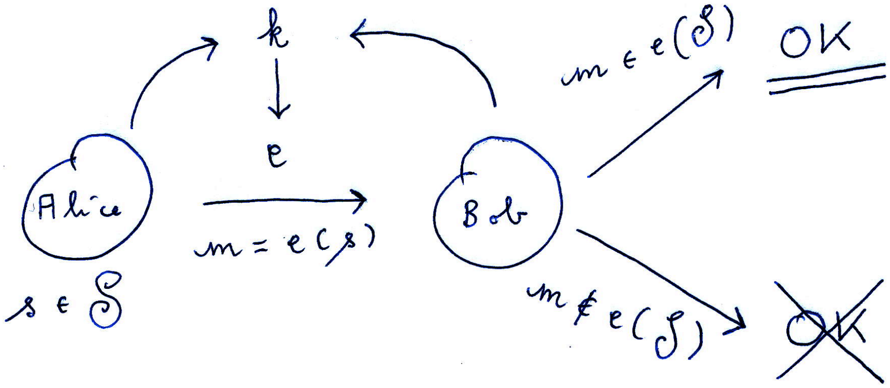

FIGURE 3.1. A-scheme.

one message $m(s,f)$ out of $\mathscr{M}(s,f)$, hereby forming an encoding rule $e \in \mathscr{E}_T$ defined as $e : \mathscr{S} \longrightarrow \mathscr{M}(s,f) : s \longrightarrow m(s,f)$, which he secretly sends to Alice. In this case, the encoding rule e is valid for the decoding rule f. When Bob receives a message he checks whether it is in some subset $\mathscr{M}(s,f)$. If so he accepts it as a valid one and he can retreive the corresponding source state. If there is a dispute between Alice and Bob about a message m, the arbiter checks if m is valid for the encoding rule given to the transmitter. (We also refer to the appendix for more details.)

3. Attack probability

Below, we define this attack probability more formally. As in [**9**] we will use the "worst case definition". Denote a set of r observed messages as m^r. Let $P(m^r)$ be the probability that one has observed m^r after r messages. Furthermore, let $P(m|m^r)$ be the probability that the message m is valid given that m^r has been observed. Then we define the *attack probability* of the opponent P_{O_r}, or also P_r, as

$$P_r = P_{O_r} = \sum_{m^r \in \mathscr{M}_r} P(m^r) \max_{m \in \mathscr{M}} P(m|m^r). \tag{1}$$

If we assume a uniform probability distribution for the messages, then we get

$$P_r = P_{O_r} = \max_{m \in \mathscr{M}} P(m|m^r). \tag{2}$$

Introduce the following notation:

$$\mathscr{E}(m^r) = \{e \in \mathscr{E} | m_i \in e(\mathscr{S}), 1 \le i \le r\}. \tag{3}$$

Denote by m'^r the set of $r+1$ messages m^r and m' (where m' is a message not contained in m^r). Then

$$P_r = P_{O_r} = \frac{|\mathscr{E}(m'^r)|}{|\mathscr{E}(m^r)|}. \tag{4}$$

THEOREM 3.1 (see [**9**]). *Let v be the total number of messages and ℓ the number of keys; r is defined as above. We have that*

$$P_r = P_{O_r} \ge \frac{\ell - r}{v - r}. \tag{5}$$

Equality holds if and only if

$$P(m|m^r) = \frac{\ell - r}{v - r}. \tag{6}$$

is satisfied for any $m^r = (m_1, \ldots, m_r)$ and $m \in \mathscr{M}$ with $m \in m_i$ for $i = 1, 2, \ldots, r$.

The following theorem is important. It assumes that the attack probabilities are uniformly distributed.

THEOREM 3.2 (see [**9**]). *If an authentication code in the A-setting has attack probabilities $P_r = P_{O_r} = 1/n_r$ for $r \in \{0, 1, \ldots, l\}$, then*

$$|\mathscr{E}| \ge \prod_{i=0}^{l} n_i. \tag{7}$$

If equality holds, the code is called *perfect*.

In the A^2-model, three types of attacks have to be considered. The first one is the spoofing attack by the opponent such as in the A-model. The other two attacks are the spoofing attack T by Alice, sending a message and then claiming not to have sent it, and the spoofing attack by Bob, claiming to have received a message from Alice while this is not the case. One denotes the corresponding probabilities by P_{O_r}, P_{R_r} and P_T respectively. The opponent's *attack probability* P_{O_r} is defined as in the A-model.

Let $P(f)$ denote the probability of a decoding rule f, and let $P(m|f, m^r)$ denote the probability of the event that the message m could be valid for the encoding rule used by the transmitter, given the decoding rule f and the first r messages $m^r = (m_1, \ldots, m_r)$. The *spoofing attack probability* of the receiver is then defined as

$$P_{R_r} = \sum_{f \in \mathscr{E}_R} P(f) \sum_{m^r \in \mathscr{M}^r} P(m^r|f) \max_{m \in \mathscr{M}} P(m|f, m^r). \tag{8}$$

Let $P(e)$ denote the probability of an encoding rule e, and let $P(m'|e)$ denote the probability of the event that the message $m' \in \mathscr{M}'(e)$ is acceptable by the receiver, given the encoding rule e. The *spoofing attack probability* of the transmitter is then defined as

$$P_T = \sum_{e \in \mathscr{E}_T} P(e) \max_{m' \in \mathscr{M}'(e)} P(m'|e). \tag{9}$$

If we assume a uniform probability distribution on the messages, the formulas reduce in the same way as for the A-codes.

CHAPTER 4

A bit of background

In this chapter a concise description of the geometrical and group theoretical background needed to read this paper is provided. Details are omitted, since the main scope is not the geometries nor the groups themselves, but the use of them to construct (and understand) our viewpoint of authentication codes.

1. Projective space

Starting from a vector space V of dimension $n+1$, $n \in \mathbb{N}$, over a skew field $\mathbb{D}$ one forms a *projective space* $\mathbf{PG}(n, \mathbb{D})$ by defining the objects "points", "lines", …, "hyperplanes" as the vector spaces of dimension $1, 2, \ldots, n$ contained in V. Incidence is defined naturally in terms of containment of vector subspaces. In other words, passing from $V = V(n+1, \mathbb{D})$ to $\mathbf{PG}(n, \mathbb{D})$ can be done by putting the equivalence relation "proportionality" $\sim$ on $V \setminus \{\text{zero vector}\}$.

Affine space $\mathbf{AG}(n, \mathbb{D})$ is defined by considering a vector space V of dimension n, $n \in \mathbb{N} \setminus \{0\}$, over a skew field $\mathbb{D}$. The objects "points", "lines", …, "hyperplanes" are defined as the cosets in $V, +$ of the subspaces (seen as additive abelian subgroups of V) of dimension $0, 1, \ldots, n-1$. Again, incidence is defined naturally. If the skew field $\mathbb{D}$ is a finite field $\mathbb{F}_q$ we also use the notations $\mathbf{PG}(n, q)$ and $\mathbf{AG}(n, q)$, respectively.

One can also define projective spaces axiomatically. However if the dimension is at least 3, it can be shown that they are always of the form above. In the case of dimension 2, this is not true. A *projective plane* consists of a set of lines, a set of points, and a symmetric relation between points and lines called incidence, having the following properties.

(1) Given any two distinct points, there is exactly one line incident with both of them.
(2) Given any two distinct lines, there is exactly one point incident with both of them.
(3) There are four points such that no line is incident with more than two of them.

2. Generalized dual arcs

A *generalized dual arc* $\mathscr{F}$ of degree d with dimensions $n = n_0 > n_1 > n_2 > \cdots > n_{d+1} > -1$ of $\mathbf{PG}(n,q)$ is a set of n_1-dimensional subspaces of $\mathbf{PG}(n,q)$ such that:

- any j of these subspaces intersect in a subspace of dimension n_j, $1 \leq j \leq d+1$,
- any $d+2$ of these subspaces have no common intersection.

We call $(n = n_0, n_1, \ldots, n_{d+1})$ the *type* of the generalized dual arc.

Example. Consider the tangent lines to a conic in $\mathbf{PG}(2,q)$, q odd. Then clearly every two tangent lines intersect in a point and any three such lines have an empty intersection.
There exist generalized dual arcs for any degree, see [**6**].

3. Generalized quadrangles

A *generalized quadrangle* GQ of *order* (s,t) is an incidence structure $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathtt{I})$ in which $\mathscr{P}$ and $\mathscr{B}$ are disjoint non-empty sets of objects called *points* and *lines* respectively, and for which $\mathtt{I}$ is a symmetric point-line incidence relation satisfying the following axioms.

(GQ1) Each point is incident with $t+1$ lines ($t \geq 1$) and two distinct points are incident with at most one common line.
(GQ2) Each line is incident with $s+1$ points ($s \geq 1$) and two distinct lines are incident with at most one common point.
(GQ3) If x is a point and L is a line not incident with x, then there is a unique point-line pair (y, M) such that $x \mathtt{I} M \mathtt{I} y \mathtt{I} L$.

A generalized quadrangle of order (s,t) contains $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines. If $s = t$, then $\mathscr{S}$ is also said to be of *order* s.
A *subquadrangle* or *subGQ* $\mathscr{S}' = (\mathscr{P}', \mathscr{B}', \mathtt{I}')$ of a generalized quadrangle $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathtt{I})$ is a GQ such that $\mathscr{P}' \subseteq \mathscr{P}$, $\mathscr{B}' \subseteq \mathscr{B}$, and $\mathtt{I}'$ is the induced incidence relation of $\mathtt{I}$.
A pair $(\mathscr{S}, x)$, with $\mathscr{S}$ a generalized quadrangle and x a distinguished point in $\mathscr{S}$, will be called a *pointed* generalized quadrangle.

REMARK 4.1. (1) If both s and t are finite, we speak of a *finite* generalized quadrangle.
(2) A generalized quadrangle is an example of a rank 2 geometry, i.e., a geometry with only two types of objects, points and lines.

3.1. The classical generalized quadrangles.

Consider a non-singular quadric of Witt index 2, that is of projective index 1, in $\mathbf{PG}(3,q)$, $\mathbf{PG}(4,q)$ and $\mathbf{PG}(5,q)$. The points and lines of these quadrics form generalized quadrangles which are denoted by $\mathbf{Q}(3,q)$, $\mathbf{Q}(4,q)$ and $\mathbf{Q}(5,q)$, and of order $(q,1)$, (q,q) and (q,q^2) respectively.

Next, let $\mathbf{H}$ be a non-singular hermitian variety in $\mathbf{PG}(3,q^2)$ or $\mathbf{PG}(4,q^2)$. The points and lines of $\mathbf{H}$ form a generalized quadrangle $\mathbf{H}(3,q^2)$ or $\mathbf{H}(4,q^2)$, which has order (q^2,q) or (q^2,q^3) respectively.
The points of $\mathbf{PG}(3,q)$ together with the totally isotropic lines with respect to a symplectic polarity form a GQ, denoted by $\mathbf{W}(q)$, of order q.
The generalized quadrangles so-defined here are the *classical generalized quadrangles*.

3.2. Collinearity/Concurrency/Regularity. Let x and y be (not necessarily distinct) points of the GQ $\mathscr{S} = (\mathscr{P},\mathscr{B},\mathtt{I})$; we write $x \sim y$ and call these points *collinear*, provided that there is some line L such that $x\mathtt{I}L\mathtt{I}y$. Dually, for $L, M \in \mathscr{B}$, we write $L \sim M$ when L and M are *concurrent*.
For $x \in \mathscr{P}$, put

$$x^{\perp} = \{y \in \mathscr{P} | y \sim x\} \tag{10}$$

Note that $x \in x^{\perp}$. For a set C of distinct points, we denote $\bigcap_{y\in C} y^{\perp}$ also by $C^{\perp}$, and $\left(C^{\perp}\right)^{\perp}$ by $C^{\perp\perp}$.

Example. For a pair of distinct points $\{x,y\}$, we have $|\{x,y\}^{\perp}| = s+1$ or $t+1$, according as $x \sim y$ or $x \not\sim y$, respectively. If $x \sim y$, $x \neq y$, or if $x \not\sim y$, and $|x,y^{\perp\perp}| = t+1$, we say that the pair (x,y) is *regular*. The point x is *regular* provided (x,y) is regular for all $y \in \mathscr{P}$, $y \neq x$.

3.3. Automorphisms. An *automorphism* of a GQ $\mathscr{S} = (\mathscr{P},\mathscr{B},\mathtt{I})$ is a permutation of $\mathscr{P} \cup \mathscr{B}$ which preserves $\mathscr{P}$, $\mathscr{B}$ and $\mathtt{I}$. The set of automorphisms of a GQ $\mathscr{S}$ is a group, called the *automorphism group* of $\mathscr{S}$, which is denoted by $\mathrm{Aut}(\mathscr{S})$.

4. Basic group theory

We review some basic notions. For more information we refer to one of the many online sources.
If G is a group with identity element $\mathbf{1}$ and X is a set, then a *group action* of G on X is a binary function $G \times X \longrightarrow X$ denoted

$$(g,x) \longrightarrow g \cdot x \tag{11}$$

such that

- $(gh) \cdot x = g \cdot (h \cdot x)$;
- $e \cdot x = x \ \ \forall x \in X$.

Usually, instead of denoting the action by $g \cdot x$, we write x^g.
If Y is a subset of the set X, then G_Y denotes the *stabilizer* of Y in G; we have that

$$G_Y = \{g \in G | Y^g = Y\}, \tag{12}$$

where $Y^g = \{y^g | y \in Y\}$.
In particular, if $Y = \{y\}$ consists of a single point, we also write G_y instead of $G_{\{y\}}$.
The action is called *n-transitive* if the size of X is at least n, and if for every two n-tuples $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ with $x_i \neq x_j$ for $i \neq j$ and the same for the y_ks, there exists a $g \in G$ such that

$$x_k^g = y_k, \;\; 1 \leq k \leq n. \tag{13}$$

In this case G is said to act *n-transitively* on X, and if $|G|$ is finite, it is easy to show that $n!$ divides $|G|$.
A subset H of G which forms a group itself by induction is called a *subgroup* of G. Associated to such a subgroup H are its left and right cosets; for every $g \in G$ we respectively have the corresponding left and right coset

$$gH = \{gh | h \in H\} \;\text{ and }\; Hg = \{hg | h \in H\}. \tag{14}$$

A subgroup N of a group G is a *normal subgroup*, denoted $N \trianglelefteq G$, if

$$\forall g \in G, \forall n \in N : \;\; g^{-1} n g \in N. \tag{15}$$

In this case we can define the *quotient group* with as elements the cosets and the normal operation of G defined on them. (Note that left and right cosets coincide now.)
The *direct product* of two groups A and B, is the Cartesian product set $A \times B$ endowed with the natural binary operation

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b'). \tag{16}$$

A group C is isomorphic to the direct product of its subgroups A and B if both A and B are normal subgroups for which $AB = C$, and if A and B only intersect in the identity. In that case, we identify C with $A \times B$. If C is a group and A a normal subgroup of C, B a subgroup of C and $A \cap B = \mathrm{id}$, then we say that C is the *semi-direct product* of A and B, provided that $AB = C$. We denote this by

$$C = A \rtimes B. \tag{17}$$

A group is called an *elementary abelian p-group* if it is a finite abelian group where every element has prime order p.

5. Categories

A *category* $\mathscr{C}$ consists of

(1) A collection $\{X, Y, Z, \cdots\}$ whose members are the *objects*. We write $X \in \mathscr{C}$.
(2) For every pair of objects $X, Y \in \mathscr{C}$, a set of $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ of *morphisms* from X to Y. We write $f : X \longrightarrow Y$ when $f \in \mathrm{Hom}_{\mathscr{C}}(X, Y)$.
(3) For every object $X \in \mathscr{C}$, an *identity morphism* $\mathrm{id}_X \in \mathrm{Hom}_{\mathscr{C}}(X, X)$.
(4) For every triple of objects $X, Y, Z \in \mathscr{C}$, a composition map

$$\mathrm{Hom}_{\mathscr{C}}(X, Y) \times \mathrm{Hom}_{\mathscr{C}}(Y, Z) \longrightarrow \mathrm{Hom}_{\mathscr{C}}(X, Z). \tag{18}$$

Moreover these data have to satisfy the following conditions.

(5) For every morphism $f : X \longrightarrow Y$ we have $\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X$ in $\mathrm{Hom}_{\mathscr{C}}(X, Y)$.
(6) For every triple of composable morphisms $f : W \longrightarrow X; g : X \longrightarrow Y; h : Y \longrightarrow Z$, we have an equality $h \circ (g \circ f) = (h \circ g) \circ f$ in $\mathrm{Hom}_{\mathscr{C}}(W, Z)$.

Below we list a few examples:

5.1. Sets. The category **Set** whose objects are sets and whose morphisms are maps of sets.

5.2. Groups. The category **Grp** whose objects are groups and whose morphisms are group homomorphisms.

5.3. Topologies. The category **Top** whose objects are topological spaces and whose morphisms are continuous maps.

5.4. Projective spaces. Let V and W be vector spaces over the skew fields $\mathbb{F}$ and $\mathbb{K}$ respectively. A pair of maps

$$(g, g') : (V, \mathbb{F}) \longrightarrow (W, \mathbb{K}) \tag{19}$$

is called a *semi-linear map* if $g : V, + \longrightarrow W, +$ is a group homomorphism and $g' : \mathbb{F} \longrightarrow \mathbb{K}$ a homomorphism of skew fields such that

$$g(\alpha v) = g'(\alpha) g(v) \; \forall \alpha \in \mathbb{F}, \; \forall v \in V. \tag{20}$$

Given such a semi-linear map, define an induced map

$$\bar{g} : \mathbf{PG}(V) \longrightarrow \mathbf{PG}(W) : \bar{g}(\langle v \rangle) = \langle g(v) \rangle. \tag{21}$$

Hence we obtain the category of projective spaces **Proj** having projective spaces as objects and the above defined maps as morphisms.

5.5. Incidence geometries. We now look at a more general category of geometries than $\mathbf{Proj}$. An *incidence geometry* $(G, \mathtt{I}, c, T)$ of rank k is a graph with a proper vertex coloring c (with k colors), i.e., two adjacent vertices are colored differently. Here $c : V(G) \longrightarrow T$ is the coloring, where T is the set of types. We take c to be surjective, and $|T| = k \in \mathbb{N}_0$. The relation $\mathtt{I}$ is the adjacency, or "incidence", relation. (In fact, we present the *incidence graph* of an incidence geometry — cf. the remark below.)

A *morphism* between two incidence geometries $(G, \mathtt{I}, c, T)$ and $(G', \mathtt{I}', c', T')$ consists of a pair (f, g) of mappings where $f : G \longrightarrow G'$ and $g : T \longrightarrow T'$ such that

(1) $\forall v \in V(G)$, we have $c'(f(v)) = g(c(v))$,

(2) $\forall u, v \in V(G)$ we have that $u\mathtt{I}v$ implies $f(u)\mathtt{I}'f(v)$.

One can form a category $\mathbf{Inc}$ with as objects incidence geometries and as morphisms the morphisms between them.

REMARK 4.2. Let $T = \{t_1, \ldots, t_k\}$, and let $(G, \mathtt{I}, c, T)$ be an incidence graph. To depict the corresponding geometry Γ, let, for each $i \in \{1, \ldots, k\}$, $T_i := c^{-1}(t_i)$ be the elements "of type *i*". Then the elements of Γ are those of $V(G)$ provided with this type function, and incidence is defined by adjacency. (As such, different elements of the same type cannot be incident.) The size of T is the *rank* of the geometry. If $|T| = 2$, we call Γ a *point-line geometry*.

CHAPTER 5

Definitions and basic properties

In this chapter, we first define an abstract category **A**, called the "category of authentication codes". After having introduced a comparison theory (through the notion of *(iso)morphisms*), we re-define the classic authentication codes in the category **CA**, and show that **A** and **CA** are in $1-1$ correspondence. Then we illustrate the new notions via a series of concrete examples.

1. Definition

Let $\mathtt{I}$ be an arbitrary index set and let A and E be non-empty sets, $\iota : \mathbf{A} \to E$ a bijection, and $\{\phi_i\}_{i\in\mathtt{I}} : E \to X$ a collection of mappings.
Then **A** has as its objects o tuples

$$(A,\ E,\ \iota, \mathtt{I}, \{\phi_i\}_{i\in\mathtt{I}}, X). \tag{22}$$

For two objects $o = (A,\ E,\ \iota, \mathtt{I}, \{\phi_i\}_{i\in\mathtt{I}}, X)$ and $o' = (A',\ E',\ \iota', \mathtt{I}', \{\phi'_i\}_{i\in\mathtt{I}'}, X')$ we define a *morphism* from o to o' as a tuple $(\nu, \overline{a}, \overline{e}, \overline{x})$, where ν is a bijection from $\mathtt{I} \to \mathtt{I}'$, and $\overline{a} : A \to A'$, $\overline{e} : E \to E'$ and $\overline{x} : X \to X'$ are mappings making the following diagrams commute

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[d, "\overline{a}"'] & E \arrow[d, "\overline{e}"'] \\ A' \arrow[r, "\iota'"] & E' \end{tikzcd} \tag{23}$$

and for all $i \in \mathtt{I}$

$$\begin{tikzcd} E \arrow[r, "\phi_i"] \arrow[d, "\overline{e}"'] & X \arrow[d, "\overline{x}"'] \\ E' \arrow[r, "\phi'_{\nu(i)}"] & X' \end{tikzcd} \tag{24}$$

REMARK 5.1. Note that for a given morphism everything is determined by the maps $\overline{e}$ and ν. Indeed, for $a \in A$, we have

$$\overline{a}(a) = \iota'^{-1}(\overline{e}(\iota(a))), \tag{25}$$

so $\overline{a} = \iota'^{-1} \circ \overline{e} \circ \iota$.

Denote the identity mapping on a set S by $\mathbf{1}_S$. The identity morphism $\mathbf{1}_o$ of an object $o = (A, E, \iota, \mathtt{I}, \{\phi_i\}_{i \in \mathtt{I}}, X)$ is $(\mathbf{1}_{\mathtt{I}}, \mathbf{1}_A, \mathbf{1}_E, \mathbf{1}_X)$. If for two objects o_1 and o_2 there exist morphisms $\alpha : o_1 \longrightarrow o_2$ and $\beta : o_2 \longrightarrow o_1$ such that $\beta \circ \alpha = \mathbf{1}_{o_1}$ and $\alpha \circ \beta = \mathbf{1}_{o_2}$, then we call α and β *isomorphisms* and we say that o_1 and o_2 are *isomorphic*. If $o_1 = o_2$, we speak of *automorphisms* and *automorphic objects*.
This leads to the notion of *isomorphism classes of codes*.

THEOREM 5.2. *Isomorphic objects have the same attack probability parameters P_i.*

Proof. As we will see later, the parameters P_i are completely determined by the sizes of the fibres of ϕ_i and $\phi_{i'}$ respectively. Since there is a bijection between E and E' compatible with these functions, the result follows immediately. ■

To a given object o, one can attach its automorphism group $\mathrm{Aut}(o)$. This is another tool to distinguish codes as clearly

THEOREM 5.3. *Two isomorphic objects have isomorphic automorphism groups.*

Proof. Indeed if α is an isomorphism from o_1 to o_2 and β is an automorphism of o_2 then $\alpha^{-1} \circ \beta \circ \alpha$ is an automorphism of o_1. This implies $\mathrm{Aut}(o_1) \cong \mathrm{Aut}(o_2)$. ■

2. Subcodes

If $\alpha : o_1 \longrightarrow o_2$ is a morphism $(\nu, \overline{a}, \overline{e}, \overline{x})$ where $\nu, \overline{a}, \overline{e}$ and $\overline{x}$ are injections then we say that o_1 is a *subcode* of o_2. Note that if o_1 is a subcode of o_2 and o_2 is a subcode of o_1 then o_1 and o_2 are isomorphic.

3. "Concrete" authentication codes

The category of "concrete authentication codes" **CA** has as objects 5-tuples

$$(\mathscr{K}, \mathscr{E}, f, \mathscr{S}, \mathscr{M}) \tag{26}$$

where $\mathscr{K}$ is a set of *keys*, $\mathscr{E}$ a set of *encoding rules*, $f : \mathscr{K} \longrightarrow \mathscr{E}$ is a bijection, $\mathscr{S}$ a set of *source states*, and $\mathscr{M}$ a set of *(encoded) messages*. They are equipped with the following scheme.
One picks a key $k \in \mathscr{K}$, and associates with it an encoding rule $e = f(k) \in \mathscr{E}$, which is a mapping from $\mathscr{S}$ to $\mathscr{M}$. For a given source state $s \in \mathscr{S}$, we obtain the encoded message $m = e(s) \in \mathscr{M}$.
A *morphism* $\alpha : c_1 \longrightarrow c_2$ between two objects $c_1 = (\mathscr{K}, \mathscr{E}, f, \mathscr{S}, \mathscr{M})$ and $c_2 = (\mathscr{K}', \mathscr{E}', f', \mathscr{S}', \mathscr{M}')$ of **CA** is a 4-tuple $(\sigma, \kappa, \eta, \mu)$ of maps making the following diagrams commute.

(27)
$$\begin{tikzcd}
\mathscr{K} \arrow[r, "f"] \arrow[d, "\kappa"'] & \mathscr{E} \arrow[d, "\eta"'] \\
\mathscr{K}' \arrow[r, "f'"] & \mathscr{E}'
\end{tikzcd}$$

and also

$$\begin{tikzcd}
\mathscr{S} \arrow[r, "e"] \arrow[d, "\sigma"'] & \mathscr{M} \arrow[d, "\mu"'] \\
\mathscr{S}' \arrow[r, "\eta(e')"] & \mathscr{M}'
\end{tikzcd} \tag{28}$$

4. Functoriality

We now define the functor F between the abstract and the concrete category mapping the object $(A,\ E,\iota,\mathtt{I},\{\phi_i\}_{i\in\mathtt{I}},X)$ to the authentication code $(A,\widetilde{E},\iota,\mathtt{I},X)$, where $\widetilde{E}$ is a set of mappings $\{\widetilde{e} \mid e \in E\}$ from $\mathtt{I}$ to X with

$$\widetilde{e}(i) = \phi_i(e). \tag{29}$$

Moreover F maps a morphism $(\nu,\bar{a},\bar{e},\bar{x})$ between objects $(A,\ E,\ \iota,\mathtt{I},\{\phi_i\}_{i\in\mathtt{I}},X)$ and $(A',\ E',\ \iota',\mathtt{I}',\{\phi_i\}_{i\in\mathtt{I}'},X')$ of the abstract code to the morphism $(\nu,\bar{a},\eta,\bar{x})$ between the concrete objects $(A,\widetilde{E},\iota,\mathtt{I},X)$ and $(A',\widetilde{E}',\iota',\mathtt{I}',X')$. Here η is the unique map making the following diagram commute:

$$\begin{tikzcd}
\mathtt{I} \arrow[r, "\widetilde{e}"] \arrow[d, "\nu"'] & \mathscr{M} \arrow[d, "\bar{x}"'] \\
\mathtt{I}' \arrow[r, "\eta(\widetilde{e'})"] & \mathscr{M}'
\end{tikzcd} \tag{30}$$

Next we define a functor G from the concrete category to the abstract category. It will map an object $(\mathscr{K},\mathscr{E},f,\mathscr{S},\mathscr{M})$ to $(\mathscr{K},\mathscr{E},f,\mathscr{S},\{\psi_s\}_{s\in\mathscr{S}},\mathscr{M})$, where

$$\psi_s(e) = e(s). \tag{31}$$

Moreover it maps a morphism (σ,κ,η,μ) between objects $(\mathscr{K},\mathscr{E},f,\mathscr{S},\mathscr{M})$ and $(\mathscr{K}',\mathscr{E}',f',\mathscr{S}',\mathscr{M}')$ to a morphism (σ,κ,η,μ) between the objects $(\mathscr{K},\mathscr{E},f,\mathscr{S},\{\psi_s\}_{s\in\mathscr{S}},\mathscr{M})$ and $(\mathscr{K}',\mathscr{E}',f',\mathscr{S}',\{\psi'_s\}_{s\in\mathscr{S}},\mathscr{M}')$.

5. Connection between the categories

In the theorem below we formalize the intuitive feeling that these categories are ”the same”. We will not further investigate the properties of our categories in the present set of notes.

THEOREM 5.4. *The functors F and G defined above have the following properties.*

(1) *F and G are covariant.*
(2) *$G \circ F = \mathbf{1_A}$ and $F \circ G = \mathbf{1_{CA}}$.*
(3) *F and G are fully faithful.*

So F and G are isomorphic categories.

Proof. Only (2) requires a small proof, since (3) is an immediate corollary of (2). To prove (2) the only thing which needs verification is that we end up with the same maps in the respective categories. But F maps a function $\phi_i : E \to x$ to $\widetilde{e} = \phi_i(e)$ and G finds functions ψ_s as $\psi_s(e) = \widetilde{e}(s) = \phi_s(e)$. For the other direction start with a function $e : S \to M$. Then G maps e to e and defines functions $\phi_i(e) = e(s)$ and after returning we find $\widetilde{e}(i) = \phi_i(e) = e(i)$. ■

CHAPTER 6

Examples

Below we describe several examples of authentication code schemes as examples of **A**. They also illustrate how wide the possibilities are for construction of authentication schemes.

1. Gilbert-McWilliams-Sloane and its dual

The following construction is taken from [**3**].
Let L be a line in the projective plane $\mathbf{PG}(2,q)$ defined over the finite field $\mathbb{F}_q$. Then the points on L are the source states, the points not on L are the encoding rules, and the lines different from L are the encoded message. Given a source state s and an encoding rule e, we obtain the encoded message $\langle s,\ e\rangle$.
Abstractly (in **A**) this corresponds to:

- $A = E$ is the set of points not on L and $\iota = \mathbf{1}_A$;
- $\mathtt{I}$ is an index set of the points on L;
- X is the set of lines different from L, and
- the ϕ_i transform a point r into line $\langle r, i\rangle$.

Dually we could consider the code where abstractly $A' = E'$ is the lines not through a given point p', the index set $\mathtt{I}'$ comes from the lines through p, X is the set of points different from p and the ϕ_i are the projections onto line i through p.
Intuitively, it is clear the two above codes are ”the same”, and using our above terminology, it is easy to check that a duality of the projective plane yields an isomorphism between these two codes. (A *duality* of a projective plane with point set $\mathscr{P}$ and line set $\mathscr{B}$ is a permutation of $\mathscr{P} \cup \mathscr{B}$ which preserves incidence and switches $\mathscr{P}$ and $\mathscr{B}$.)
Moreover, if in any of the two schemes above we don’t use all the source states, we clearly obtain subcodes of the given codes.

Automorphism group. An automorphism of the code is nothing else than an automorphism of the projective plane fixing the line L. So the automorphism group is isomorphic to $\mathbf{P\Gamma L}_3(q)_L$.

2. De Soete’s scheme

The scheme below based on generalized quadrangles is due to De Soete [**1**].

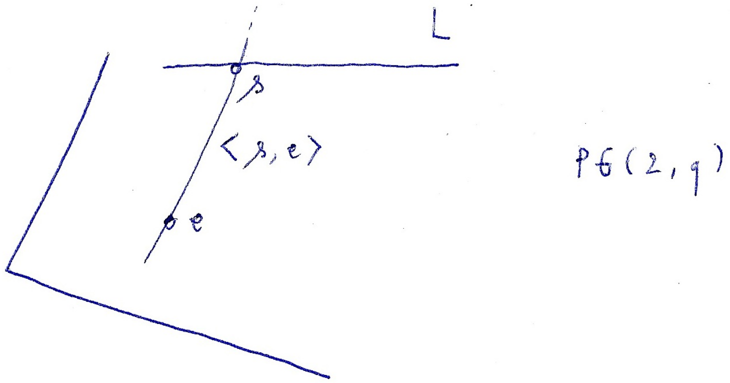

FIGURE 6.1. Gilbert-McWilliams-Sloane scheme.

Let x be a fixed point of a GQ $\Gamma = (\mathscr{P}, \mathscr{B}, \mathtt{I})$ of order (s,t), $s \neq 1 \neq t$. The $t+1$ lines of the GQ through x are the source states, the points not collinear with x are the keys, and the points collinear with, but different from x are the messages. If Alice wants to send a message to Bob, she chooses one of the lines l of the GQ through x. If the key is the point k, then by (GQ3) there is a unique point r on l collinear with k. Alice sends the pair (l,r) to Bob. When receiving a (line, point)-pair, Bob checks if the point r is collinear with k. If this is the case, he decides Alice has sent the message.

In the category **A** this example is easily described as follows.

- $A = E = \mathscr{P} \setminus x^{\perp}$ and $\iota = \mathbf{1}_A$;
- $X = x^{\perp} \setminus x$;
- $\mathtt{I}$ is the index set of the lines through x, and
- ϕ_i is the projection on line L_i through x.

THEOREM 6.1 ([**1**]). *The De Soete scheme yields a Cartesian authentication code with*

$$|\mathscr{S}| = t+1,\ |\mathscr{M}| = (t+1)s,\ |\mathscr{E}| = ts^2. \tag{32}$$

Furthermore, $P_0 = P_1 = \frac{1}{s}$.

Automorphism group. This is much more tricky than for the previous scheme. We defer its calculation to a later section.

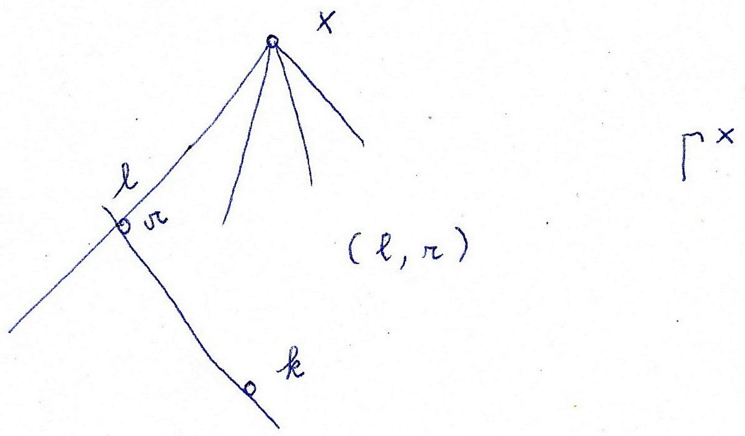

FIGURE 6.2. De Soete's scheme.

3. A perfect scheme using generalized dual arcs

Let Π be a hyperplane of $\mathbf{PG}(n+1,q)$ and let $\mathscr{D}$ be a *generalized dual arc* of degree d in Π of type $(n,n_1,\ldots,n_{d+1})$.
The elements of $\mathscr{D}$ are the messages and the points of $\mathbf{PG}(n+1,q)$ not in Π are the keys. The authentication tag that belongs to a message and a key is the generated (n_1+1)-dimensional subspace.
This defines a perfect MAC of order $r = d+1$ with attack probabilities

$$P_i = q^{n_{i+1}-n_i}. \tag{33}$$

This example considered as an object in $\mathbf{A}$ has the following description:

- $A = E$ is the set of points not contained in the hyperplane, and $\iota = \mathbf{1}_A$;
- X is the collection of (n_1+1) dimensional spaces intersecting Π in an arc element,
- $\mathtt{I} = \{1,2,\ldots,|\mathscr{D}|\}$, and
- the ϕ_i are the maps which send an element e of E to the space spanned by e and the arc element with index i.

Automorphism group. Calculating the automorphism group will heavily depend on the type of arc. We do not go into any details on this matter.

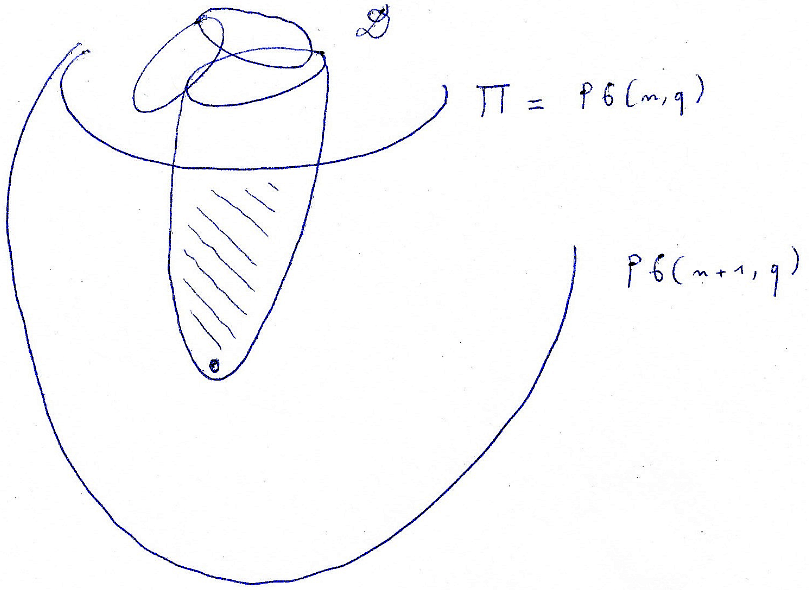

FIGURE 6.3. A-scheme from generalized dual arc.

4. An example using elementary number theory

As a third example we use the Chinese remainder theorem.
Let $n_1, \ldots, n_k$ be integers which are relatively prime, let $N = n_1 \cdots n_k$ and let $a_1, \ldots, a_k$ be arbitrary integers. Then there is a unique integer x, $0 \leq x \leq N-1$ such that

$$x \equiv a_i \mod n_i. \tag{34}$$

We make the following element o of $\mathbf{A}$ (and thus $\mathbf{CA}$!):

- $A = E$ is the set of integers from 0 to $N-1$ and $\iota = \mathbf{1}_A$;
- X is the set of integers from 0 to $N-1$
- $\mathtt{I} = \{1, 2, \ldots, k\}$, and
- the ϕ_i are the maps modulo n_i.

Automorphism group. An automorphism of o is a permutation α of $\mathbb{Z}/N\mathbb{Z}$ such that

$$a \equiv b \mod n_i \implies \alpha(a) \equiv \alpha(b) \mod n_i \ \forall i. \tag{35}$$

To such an automorphism of the code corresponds a unique permutation of $\mathbb{Z}/n_i\mathbb{Z}$ by the above rule, since the above equation tells us that equivalence classes are mapped onto equivalence classes.

Conversely given automorphisms α_i of $\mathbb{Z}/n_i\mathbb{Z}$ we can construct an automorphism α of $\mathbb{Z}/N\mathbb{Z}$ as follows. Given $y \in \mathbb{Z}/N\mathbb{Z}$, calculate $y_i \equiv y \mod n_i$. Then by the Chinese remainder theorem we can define $\alpha(y)$ as being the unique integer z with $0 \leq z \leq N-1$ such that $z \equiv \alpha_i(y_i) \mod n_i \ \forall i$. We need to check that α is a permutation. This follows immediately from the fact that the α_i are permutations. For the readers sake we check this here explicitly. First injectivity, so suppose $\alpha(y) = \alpha(z)$. Then we have

$$\alpha(y)_i \equiv \alpha(y) \mod n_i \equiv \alpha(z)_i \equiv \alpha(z) \mod n_i. \tag{36}$$

By definition this means $y_i \equiv y \mod n_i \equiv z_i \equiv z \mod n_i$. By the Chinese remainder theorem this implies $y = z$. Bijectivity follows immediately since there are only a finite number of equivalence classes.

Clearly the permutation groups of $\mathbb{Z}/n_i\mathbb{Z}$ are symmetric groups $\mathbf{S}_{n_i}$. The copies of them inside our automorphism group are the ones corresponding with taking all $\alpha_j = \mathbf{1}_{\mathbb{Z}/n_j\mathbb{Z}}$ for all $j \neq i$. These yield normal subgroups. So our automorphism group is isomorphic to

$$\mathbf{S}_{n_1} \times \cdots \times \mathbf{S}_{n_k}. \tag{37}$$

REMARK 6.2. As an algebraic structure the automorphism group of $\mathbb{Z}/N\mathbb{Z}$ is equal to

$$(\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^\times.$$

Every such automorphism automatically fulfills

$$a \equiv b \mod n_i \implies \alpha(a) \equiv \alpha(b) \mod n_i \ \forall i.$$

Indeed, if α is an automorphism of $\mathbb{Z}/N\mathbb{Z}$ we need to have $\alpha(x+y) = \alpha(x) + \alpha(y)$. Hence if $a = b + kn_i$ we obtain $\alpha(a) = \alpha(b) + \alpha(k)n_i$. We will describe this example in a more abstract setting later on.

CHAPTER 7

Other examples coming from GQs

Below, we describe further examples of authentication schemes coming from generalized quadrangles, taken from [**11**]. The reader is invited to translate the examples in the more abstract theory described in the previous two chapters.

1. Construction

Suppose $\mathscr{S}$ is a GQ of order (s,t). Suppose $\mathscr{S}'$ is a subGQ of $\mathscr{S}$ of order $(s,t/s)$; then an easy counting exercise shows that each line of $\mathscr{S}$ meets $\mathscr{S}'$ in either 1 or $s+1$ points. Let x be a point of $\mathscr{S} \setminus \mathscr{S}'$; then the $t+1$ points of $\mathscr{S}'$ which are collinear with x (and which respectively correspond to the lines incident with x by the previous property) are two by two non-collinear; since $t+1 = s \cdot t/s + 1$, this means that these points form an "ovoid", $\mathscr{O}_x$, of $\mathscr{S}'$. (An *ovoid* is a point set meeting each line precisely once.) This ovoid is *subtended* by x.

Now suppose $\{\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_r\}$ is a set of $r > 0$ distinct subGQs of order $(s,t/s)$ of the GQ $\mathscr{S}$ of order (s,t), where $s \neq 1 \neq t$ but we allow $t/s = 1$. Let Σ be the number of points in

$$\bigcup_{i=1}^{r} \mathscr{S}_i, \tag{38}$$

so that the number of points outside this union is

$$(s+1)(st+1) - \Sigma. \tag{39}$$

The $\mathscr{S}_j$s are the source states. The keys are the points of $\mathscr{S} \setminus \bigcup_{i=1}^{r} \mathscr{S}_i$, and the messages are the ovoids in the GQs $\mathscr{S}_j$ which are subtended by a point outside their union.

Let k be the maximal number of points outside $\bigcup_{i=1}^{r} \mathscr{S}_i$ that subtend the same ovoid of some $\mathscr{S}_j$. Then

$$P_0 \leq \frac{|\mathscr{E}(m)|}{|\mathscr{E}|} = \frac{k}{(s+1)(st+1) - \Sigma}. \tag{40}$$

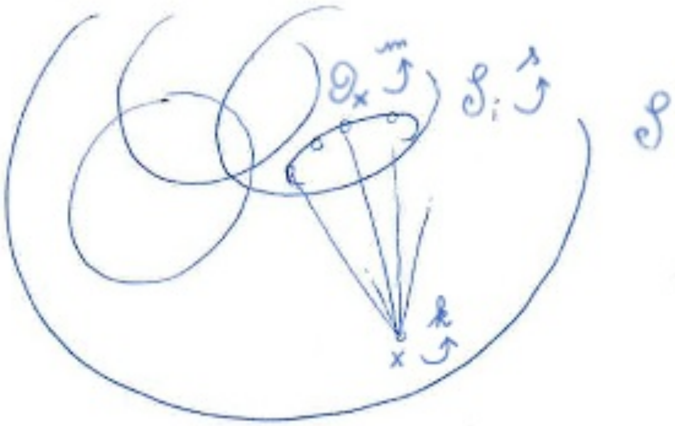

FIGURE 7.1. Construction.

By [**8**, 1.4.1], we have

$$k \leq \frac{s^2}{t} + 1 \tag{41}$$

so that

$$P_0 \leq \frac{s^2/t+1}{(s+1)(st+1)-\Sigma}. \tag{42}$$

We want to focus on two particular situations that appear to yield satisfying results.

(1) Let $t = s^2$ so that $t/s = s$. Then

$$P_0 \leq \frac{2}{(s+1)(s^3+1)-\Sigma}. \tag{43}$$

Suppose now that in $\mathscr{S}$ we have the following situation: Γ is an $(s+1) \times (s+1)$-grid (that is, a subGQ of order $(s,1)$), and all the $\mathscr{S}_j$s contain Γ — it then follows easily that Γ is precisely the pairwise intersection of any two distinct $\mathscr{S}_j$s. Moreover, if z is a point outside the subGQ union, and $\mathscr{S}_g, \mathscr{S}_h \neq \mathscr{S}_g$ are elements of $\{\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_r\}$, then z obviously subtends different ovoids in $\mathscr{S}_g$ and $\mathscr{S}_h$.

In order to avoid a trivial situation, we assume $r < s+1$ (if $r = s+1$, then $\cup_i \mathscr{S}_i = \mathscr{S}$). Whence

$$P_0 \leq \frac{2}{(s+1)(s^3+1)-(s+1)^2-r(s^3-s)} = \frac{2}{(s+1)(s^2-s)(s+1-r)}. \tag{44}$$

Note that we can choose the subGQs in such a way that the inequality becomes strict.

(2) Let $t = s$, so that $t/s = 1$ and

$$P_0 \leq \frac{s+1}{(s+1)(s^2+1)-\Sigma}. \tag{45}$$

Also, let Γ be two distinct intersecting lines, and let all the $\mathscr{S}_j$s contain Γ — it follows (again) that Γ is precisely the pairwise intersection of any two distinct $\mathscr{S}_j$s. If z is a point outside the union, and $\mathscr{S}_g, \mathscr{S}_h \neq \mathscr{S}_g$ are elements of $\{\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_r\}$, then z subtends different ovoids in $\mathscr{S}_g$ and $\mathscr{S}_h$. Whence

$$P_0 \leq \frac{s+1}{s(s^2+(1-r)s-1)}. \tag{46}$$

REMARK 7.1. The schemes described in this section are *Cartesian*. Furthermore, the scheme is *perfect* if every ovoid is subtended by the same number of points. Examples of this situation are given below.

2. Authentication with arbitration: H-schemes

Consider the following situation. $\{\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_r\}$ is a set of distinct $\mathbf{Q}(4,q)$-subGQs in a $\mathbf{Q}(5,q)$ (which, as above, can be chosen in a suitable position), and let those subGQs be source states. Let x be a point of $\mathbf{Q}(5,q)$ outside the union of the subGQs, which is chosen by Bob. For such a point x and for each source state $\mathscr{S}_j$, let $\mathscr{O}_x$ be the ovoid of $\mathscr{S}_j$ which is subtended by x. The arbiter chooses a point c_j of $\mathscr{S}_j$ on $\mathscr{O}_x$.

We can now make a scheme with arbitration as follows. For the system we choose a list $\mathbf{H}$ of subgroups of $\mathrm{Aut}(\mathbf{Q}(5,q))$, being $\mathbf{O}^-(6,q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ (q is a power of the prime p). Bob chooses a fixed subgroup H in $\mathbf{H}$. Bob hands H and his chosen point x to the arbiter. The subgroup H has different orbits on $\mathbf{Q}(5,q)$. The arbiter hands c_j and the H-orbit c_j, denoted by c_j^H, as encoding rule to Alice for a given source state $\mathscr{S}_j$. If Alice transmits a message to Bob, then she picks a source state $\mathscr{S}_j$ and sends the triple $(\mathscr{S}_j, c_j, c_j^H)$ to Bob. When receiving a triple (a,b,c) Bob accepts it as valid if b is on the ovoid of a and c is the H-orbit of b. In case of a dispute concerning a triple (a,b,c), the arbiter checks if b is the point he handed to Alice for the subGQ a and if c is the orbit under H of b. If this is the case, then he decides Alice sent the message, otherwise that she has not. If Bob wants to cheat (that is, to imitate Alice), he has to make a guess about the point c_j. If Alice wants to cheat (that is, to imitate Bob), she has to make sure she gets the right group. It is almost impossible for Alice to guess H from the orbits she sees, except possibly by exhaustive search through all subgroups of $\mathrm{Aut}(\mathbf{Q}(5,q))$ if there are only very few groups producing an orbit she observes. But the arbiter can avoid this by choosing the appropriate points. Besides that, Alice has to find x, which is essentially not possible since c_j is contained in at least $(q^3 - q\Sigma')/2$ subtended ovoids in $\mathscr{S}_j$, Σ' being the number of distinct lines on c_j which are completely contained in $\cup_i \mathscr{S}_i$. An opponent has to guess both c_j and the group H, an even harder task.

We do not make calculations in detail, but once one has chosen the list of allowed subgroups one can adapt the scheme to one's own needs. This scheme depends largely on the list $\mathbf{H}$ of subgroups we allow. By choosing them appropriately, one can control the length of the orbits.
For the abstract side of the story, we refer to the appendix to this text.

REMARK 7.2. (i) Similar schemes can be built from other incidence geometries, such as the natural embedding of Hermitian quadrangles $\mathbf{H}(3,q^2) \subset \mathbf{H}(4,q^2)$, or from nonclassical situations.
(ii) We always assume that the points outside the union of subGQs are chosen with equal probability. One could define a natural probability

$$P : \mathscr{S} \setminus \cup_i \mathscr{S}_i \mapsto (0,1) \tag{47}$$

on this set by comparing, for a pre-chosen subgroup G of $\mathrm{Aut}(\mathscr{S})_{\cup_i \mathscr{S}_i}$, the size of the G-orbit $G(x)$ that contains x, to $|\mathscr{S} \setminus \cup_i \mathscr{S}_i|$.

CHAPTER 8

Addition and multiplication

In this chapter, we will call an object $o = (\mathscr{A}, \mathscr{E}, \iota, \mathtt{I}, \{\phi_i\}_{\mathtt{I}}, X) \in \mathbf{A}$ *Cartesian* if for $i \neq j$ in $\mathtt{I}$, we have that

$$\phi_i(\mathscr{E}) \cap \phi_j(\mathscr{E}) = \emptyset. \tag{48}$$

Notation. If $o = (\mathscr{A}, \mathscr{E}, \iota, \mathtt{I}, \{\phi_i\}_{\mathtt{I}}, X) \in \mathbf{A}$, then we define functions $\mathscr{A}(.)$ and $\mathscr{S}(.)$ by $\mathscr{A}(o) = \mathscr{A} = \mathscr{E}(o)$ and, $\mathscr{S}(o) = \{1, 2, \ldots, k\}$.
Let $A = \{a_i | i \in I\}$ and $B = \{b_j | j \in J\}$ be sets; then by $(f(a_i, b_j))_{ij}$, with $f : A \times B \longrightarrow C$ any map to some set C, we mean the (unordered) row consisting of all elements of $\{f(a, b) | (a, b) \in A \times B\}$.
By slight abuse of notation, we index the functions with $1, 2, \ldots, k$, although the index set $\mathtt{I}$ is allowed to have any (and so also uncountable) cardinality. Below, finiteness of the objects is nowhere required (although in applications, some things will only make sense when they are finite).

1. Addition

Let $o = (\mathscr{A}, \mathscr{E}, \iota, \mathtt{I}, \{\phi_i\}_{\mathtt{I}}, X)$ and $o' = (\mathscr{A}', \mathscr{E}', \iota', \mathtt{I}', \{\phi'_j\}_{\mathtt{I}'}, X')$ be objects of $\mathbf{A}$. We define an addition $\oplus$ as follows:

$$o \oplus o' = (\mathscr{A} \coprod \mathscr{A}', \mathscr{E} \coprod \mathscr{E}', \iota \coprod \iota', \mathtt{I} \times \mathtt{I}', X \coprod X', (\phi_i \coprod \phi'_j)_{ij}). \tag{49}$$

Here, for sets C and D, $C \coprod D$ means the disjoint union between C and D (that is, $C \coprod D = C \times \{0\} \cup D \times \{1\}$). Also, $\phi_i \coprod \phi'_j(c)$ $(= (\phi_i \coprod \phi'_j)(c))$, with $c \in X \coprod X'$ is $\phi_i(c)$ when $c \in X \times \{0\}$ and $\phi'_j(c)$ otherwise.
In the next observation (the last part), we implicitly assume that index sets of objects in $\mathbf{A}$ do not have size 1.

OBSERVATION 8.1. *$o \oplus o'$ is an object of $\mathbf{A}$ with $|\mathscr{A}(o \oplus o')| = |\mathscr{A}(o)| + |\mathscr{A}(o')|$ and $|\mathscr{S}(o \oplus o')| = |\mathscr{S}(o)| \times |\mathscr{S}(o')|$. Also, $o \oplus o' \cong o' \oplus o$, and $o \oplus o'$ is never Cartesian.*

Proof. Only the last assertion needs a small proof. Let m be an element of $\cup_{i,j}(\phi_i(\mathscr{E}) \coprod \phi'_j(\mathscr{E}'))$, and suppose without loss of generality that $m \in \phi_i(\mathscr{E}) \times \{0\}$ for some $i \in \mathtt{I}$. (This i need not be unique since we do not demand o to be Cartesian.) Then $m \in \phi_i(\mathscr{E}) \coprod \phi'_j(\mathscr{E}')$ for all $j \in \mathtt{I}'$. ■

Note that $|\mathscr{A} \coprod \mathscr{A}'| = |\mathscr{A}| + |\mathscr{A}'|$.

REMARK 8.2. Note that the fact that we require disjoint unions instead of ordinary set theoretic unions is a necessity: for $o \oplus o'$ to be well-defined, one needs the property that for each i and j, ϕ_i and ϕ'_j have the same action on the elements of $\mathscr{E} \cap \mathscr{E}'$ (in order that when combined, they still define a map on $\mathscr{E} \cup \mathscr{E}'$).

2. Multiplication

We consider o and o' as above, and define $o \otimes o'$ as follows:

$$o \otimes o' = (\mathscr{A} \times \mathscr{A}', \mathscr{E} \times \mathscr{E}', \iota \times \iota', \mathtt{I} \times \mathtt{I}', (\phi_i \times \phi'_j)_{ij}, X \times X'). \tag{50}$$

Here, $\phi_i \times \phi'_j(e,e') = (\phi_i(e), \phi'_j(e'))$.

OBSERVATION 8.3. *$o \otimes o'$ is an object of* $\mathbf{A}$ *with $|\mathscr{A}(o \otimes o')| = |\mathscr{A}(o)| \times |\mathscr{A}(o')|$ and $|\mathscr{S}(o \otimes o')| = |\mathscr{S}(o)| \times |\mathscr{S}(o')|$. Also, in general $o \otimes o' \not\cong o' \otimes o$, and $o \otimes o'$ is Cartesian if and only if both o and o' are.*

Proof. Again, only the last part will be indicated. Let (m,m') be an element of $\cup_{i,j}(\phi_i(\mathscr{E}) \times \phi'_j(\mathscr{E}'))$; if o and o' are Cartesian, then clearly there is only one element $\phi_i(\mathscr{E}) \times \phi'_j(\mathscr{E}')$ containing (m,m'). The converse is also clear. ■

Here, $|\mathscr{A} \times \mathscr{A}'| = |\mathscr{A}| \times |\mathscr{A}'|$.
In a later section, we will obtain the precise connections between the probability parameters of authentication codes and those of their sums/products. As a direct corollary, we will find the relation between perfectness of authentication codes and perfectness of sums/products.

3. Matrix representation

Consider $o = (\mathscr{A}, \mathscr{E}, \iota, \mathtt{I}, \{\phi_i\}_{\mathtt{I}}, X) \in \mathbf{A}$. Then o can also be represented by a matrix $M(o)$, for which the rows are indexed by $\mathscr{E}$ and the columns by $\mathtt{I}$, such that the er-entry of $M(o)$ is $\phi_r(e)$.

OBSERVATION 8.4. *Consider two objects o and o'.*

SUM *We have that $M(o \oplus o')$ is an $(|\mathscr{E}| + |\mathscr{E}'|) \times k \cdot k'$-matrix.*

PRODUCT *Moreover, $M(o \otimes o')$ is precisely a tensor-like product "$M(o) \otimes M(o')$", with as entries all possible products $(\phi_i(e), \phi'_j(e'))$.*

■

CHAPTER 9

Example of sum and product

We now consider the Gilbert-MacWilliams-Sloane scheme constructed from the smallest plane, and the De Soete scheme constructed from an easy generalized quadrangle. We then make sum and product, presented in the matrix form.

1. Gilbert-MacWilliams-Sloane

Consider the Fano plane with points $s_0, s_1, s_2, e_0, e_1, e_2, e_3$ and with as lines

$$L_0 = \{s_0, s_1, s_2\}, L_1 = \{s_0, e_0, e_1\}, L_2 = \{s_0, e_2, e_3\}, L_3 = \{s_1, e_0, e_2\},\\ L_4 = \{s_1, e_1, e_3\}, L_5 = \{s_2, e_0, e_3\}, L_6 = \{s_2, e_1, e_2\}. \tag{51}$$

We construct the affine plane of order 2 by deleting the line L_0, and keeping the same notation for the other lines.

The Gilbert-MacWilliams-Sloane scheme is then encoded in the following matrix.

GMWS	s_0	s_1	s_2
e_0	L_1	L_3	L_5
e_1	L_1	L_4	L_6
e_2	L_2	L_3	L_6
e_3	L_2	L_4	L_5

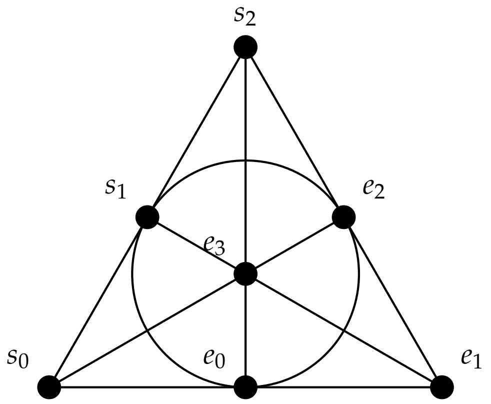

FIGURE 9.1. The unique projective plane of order 2 (“Fano plane”).

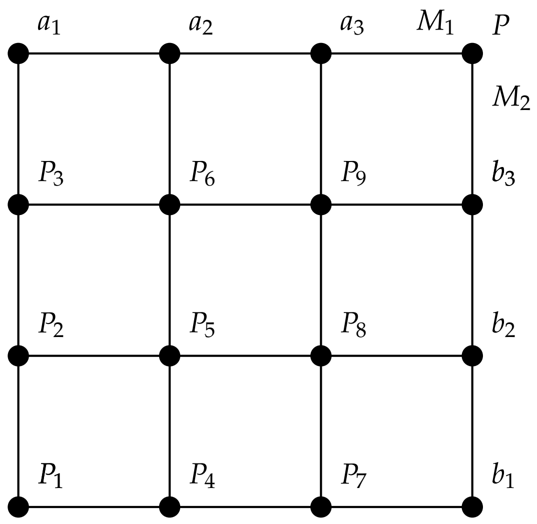

FIGURE 9.2. A grid of order $(3,1)$.

2. De Soete

Consider a GQ of order $(3,1)$ with special point P and denote the two lines through P by $M_1 = \{P, a_1, a_2, a_3\}$ and $M_2 = \{P, b_1, b_2, b_3\}$ respectively. The other lines are

$$\begin{aligned}&\{a_1, P_1, P_2, P_3\}, \{a_2, P_4, P_5, P_6\}, \{a_3, P_7, P_8, P_9\},\\ &\{b_1, P_1, P_4, P_7\}, \{b_2, P_2, P_5, P_8\}, \{b_3, P_3, P_6, P_9\}.\end{aligned} \tag{52}$$

The corresponding authentication scheme is then given by:

DS	M_1	M_2
P_1	a_1	b_1
P_2	a_1	b_2
P_3	a_1	b_3
P_4	a_2	b_1
P_5	a_2	b_2
P_6	a_2	b_3
P_7	a_3	b_1
P_8	a_3	b_2
P_9	a_3	b_3

3. Sum

The sum of the above schemes is depicted below. The source states are point-line pairs consisting of one of the three points of the GMWS-scheme and one of the two lines of the De Soete scheme. The encoding rules consist of the (disjoint) union of the encoding rules of both schemes. The encoded messages belong to either the GMWS-scheme or the De Soete scheme according to where the encoding rule comes from.

SUM	(s_0, M_1)	(s_0, M_2)	(s_1, M_1)	(s_1, M_2)	(s_2, M_1)	(s_2, M_2)
e_0	L_1	L_1	L_3	L_3	L_5	L_5
e_1	L_1	L_1	L_4	L_4	L_6	L_6
e_2	L_2	L_2	L_3	L_3	L_6	L_6
e_3	L_2	L_2	L_4	L_4	L_5	L_5
P_1	a_1	b_1	a_1	b_1	a_1	b_1
P_2	a_1	b_2	a_1	b_2	a_1	b_2
P_3	a_1	b_3	a_1	b_3	a_1	b_3
P_4	a_2	b_1	a_2	b_1	a_1	b_1
P_5	a_2	b_2	a_2	b_2	a_2	b_2
P_6	a_2	b_3	a_2	b_3	a_2	b_3
P_7	a_3	b_1	a_3	b_1	a_3	b_1
P_8	a_3	b_2	a_3	b_2	a_3	b_2
P_9	a_3	b_3	a_3	b_3	a_3	b_3

4. Product

As an illustration of our product we combine the above two schemes. Source states are couples (s_i, M_j) with s_i a source state of the Fano plane, and M_j a source state from the De Soete scheme of above. Encoding rules are couples (e_r, P_s), with e_r an encoding rule of the Fano plane and P_s one from the De Soete scheme. Message encoding is componentwise. Since this is a 36x6 matrix we have only listed some of the rows.

PROD	(s_0, M_1)	(s_0, M_2)	(s_1, M_1)	(s_1, M_2)	(s_2, M_1)	(s_2, M_2)
(e_0, P_1)	(L_1, a_1)	(L_1, b_1)	(L_3, a_1)	(L_3, b_1)	(L_5, a_1)	(L_5, b_1)
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
(e_2, P_4)	(L_2, a_2)	(L_2, b_1)	(L_3, a_2)	(L_3, b_1)	(L_6, a_2)	(L_6, b_1)
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
(e_3, P_9)	(L_2, a_3)	(L_2, b_3)	(L_4, a_3)	(L_4, b_3)	(L_3, a_3)	(L_5, b_3)

CHAPTER 10

Automorphism groups and operations

In this chapter we investigate what happens with automorphism groups when applying the standard operations. A warning: one has to be very careful when reasoning with automorphism groups. Sometimes, it might be tempting to think that automorphisms will be induced "by the operations". In general this is completely false.
We will use the obvious notations below.

1. Automorphism of a sum

THEOREM 10.1. *Isomorphic copies of* $\mathrm{Aut}(o)$ *and* $\mathrm{Aut}(o')$ *are contained in* $\mathrm{Aut}(o \oplus o')$. *Moreover, an isomorphic copy of their direct product is also in* $\mathrm{Aut}(o \oplus o')$.

Proof. With $\alpha \in \mathrm{Aut}(o)$ one can associate $\widetilde{\alpha}$, which acts as α on o and as the identity on o'. The isomorphic copy of $\mathrm{Aut}(o)$ thus obtained is clearly a subgroup of $\mathrm{Aut}(o \oplus o')$. Clearly, the copies normalize each other, so their direct product is contained in $\mathrm{Aut}(o \oplus o')$. ∎

2. Automorphism of a product

A slightly stronger statement can be obtained for the product.

THEOREM 10.2. *Isomorphic copies of* $\mathrm{Aut}(o)$ *and* $\mathrm{Aut}(o')$ *are contained in* $\mathrm{Aut}(o \otimes o')$. *Moreover, an isomorphic copy of their direct product is also in* $\mathrm{Aut}(o \otimes o')$. *In fact,* $\mathrm{Aut}(o)$ *and* $\mathrm{Aut}(o')$ *can be seen as normal subgroups of* $\mathrm{Aut}(o \otimes o')$.

Proof. If $\alpha = (v, \overline{a}, \overline{e}, \overline{x}) \in \mathrm{Aut}(o)$ and $\alpha' = (v', \overline{a'}, \overline{e'}, \overline{x'}) \in \mathrm{Aut}(o')$ then $(v \times v', \overline{a} \times \overline{a'}, \overline{e} \times \overline{e'}, \overline{x} \times \overline{x'}) \in \mathrm{Aut}(o \otimes o')$. Indeed, since everything works componentwise, we obtain bijections and the diagrams will still commute.
If in the above construction one takes $\alpha' = \mathbf{1}_{o'}$ we obtain an isomorphic copy G of $\mathrm{Aut}(o)$ contained in $\mathrm{Aut}(o \times o')$. Then G is a normal subgroup of $\mathrm{Aut}(o \times o')$. (Indeed take an arbitrary element $s \in \mathrm{Aut}(o \times o')$. Then for all $g \in G$ it follows that $s^{-1}gs \in G$.) Similarly an isomorphic copy of $\mathrm{Aut}(o')$ is contained as a normal subgroup in $\mathrm{Aut}(o \times o')$. Hence the product is a direct product. ∎

CHAPTER 11

Calculation of parameters

We keep using the standard notation.

1. P_i-Formulas

Consider an object o of $\mathbf{A}$. We want to find an expression for the probability parameters of o, so we have to determine, for a given natural number n,

$$\mathscr{E}(\overline{m}) = \{e \in \mathscr{E} | m_i \in \cup_j \phi_j(e) \ \forall i \in \{1,\ldots,n\}\}, \tag{53}$$

with $\overline{m} = (m_1, m_2, \ldots, m_n)$ any element of $\mathscr{M}^n$, where $\mathscr{M} = \cup_i \phi_i(\mathscr{E})$. We will keep using the “bar notation” in this sense throughout.
It is obvious that

$$\mathscr{E}(\overline{m}) = \bigcap_{i=1}^{n}(\bigcup_{j=1}^{k} \phi_j^{-1}(m_i)), \tag{54}$$

again remarking that similar formulas hold for infinite n and k. The probability formulas can now easily be computed. (Below, uniform probability distributions are assumed, although one easily adapts the formulas to general distributions using the expression (54).)

THEOREM 11.1 (P_0-Formula). *For $o \in \mathbf{A}$, we have that*

$$P_0 = \frac{|\bigcup_{j=1}^{k} \phi_j^{-1}(m)|}{|\mathscr{E}|}, \tag{55}$$

for any $m \in \cup_i \phi_i(\mathscr{E})$ ■

THEOREM 11.2 (P_j-Formula, $j > 0$). *For $o \in \mathbf{A}$ and $j > 0$, we have that*

$$P_j = \frac{|\bigcap_{i=1}^{n+1}(\bigcup_{j=1}^{k} \phi_j^{-1}(m_i))|}{|\bigcap_{i=1}^{n}(\bigcup_{j=1}^{k} \phi_j^{-1}(m_i))|}, \tag{56}$$

for any $\overline{m} = (m_1, m_2, \ldots, m_n)$ and $\overline{m}' = (m_1, m_2, \ldots, m_n, m_{n+1})$. ■

For Cartesian codes, these formulas get a lot simpler. (In the theorems stated below, $\ell(m)$ denotes the unique element of $\mathtt{I}$ determined by m.)

THEOREM 11.3 (Cartesian P_0-Formula). *For $o \in \mathbf{A}$ Cartesian, we have that*

$$P_0 = \frac{|\phi_{\ell(m)}^{-1}(m)|}{|\mathscr{E}|}, \tag{57}$$

for any $m \in \cup_i \phi_i(\mathscr{E})$ ■

THEOREM 11.4 (Cartesian P_j-Formula, $j > 0$). *For $o \in \mathbf{A}$ Cartesian and $j > 0$, we have that*

$$P_j = \frac{|\bigcap_{i=1}^{n+1} \phi_{\ell(m_i)}^{-1}(m_i)|}{|\bigcap_{i=1}^{n} \phi_{\ell(m_i)}^{-1}(m_i)|}, \tag{58}$$

for any $\overline{m} = (m_1, m_2, \ldots, m_n)$ and $\overline{m}' = (m_1, m_2, \ldots, m_n, m_{n+1})$. ■

2. P_i-Formulas for addition and product

We now start with objects o and o' (using the notation of above), and consider the P_i-values of $o \oplus o'$.

2.1. Addition.

We have that

$$P_0 = \frac{|\bigcup_{i,j} \phi_i^{-1} \coprod \phi_j^{-1}(m)|}{|\mathscr{E}| + |\mathscr{E}'|}, \tag{59}$$

for any $m \in \cup_{i,j} \phi_i \coprod \phi_j'(\mathscr{E} \coprod \mathscr{E}')$. Suppose without loss of generality that $m \in (\cup_i \phi_i(\mathscr{E})) \times \{0\} \subseteq X \times \{0\}$. We have

$$|\bigcup_{i,j} \phi_i^{-1} \coprod \phi_j^{-1}(m)| = |(\bigcup_i \phi_i^{-1}(m)) \times \{0\}|. \tag{60}$$

Let o and o' be objects in $\mathbf{A}$ with P-vectors $\overline{P(o)} = (P_0(o), P_1(o), \ldots, P_r(o))$ and $\overline{P(o')} = (P_0(o'), P_1(o'), \ldots, P_{r'}(o'))$. (The *$P$-vector* of o is the element $(x_0, \ldots, x_r)$ of $[0,1[^{r+1}$ for some $r \in \mathbb{N}$ for which $x_i = P_i(o)$ if $i \leq r$, and such that $P_{r+1}(o) = 1$.) We need to calculate, for any feasible natural n, and $(m_1, m_2, \ldots, m_n) \in (\mathscr{M} \coprod \mathscr{M}')^n$:

$$P_j = \frac{|\bigcap_{i=1}^{n+1} (\bigcup_{u,v} (\phi_u^{-1} \coprod {\phi'}_v^{-1})(m_i))|}{|\bigcap_{i=1}^{n} (\bigcup_{u,v} (\phi_u^{-1} \coprod {\phi'}_v^{-1})(m_i))|}. \tag{61}$$

Of course, the problem here is that we don't know whether, for given i, m_i is in $\mathscr{M} \times \{0\}$ or $\mathscr{M}' \times \{1\}$. (This problem will luckily not occur for the product formulas.) So suppose, for now, that $m_1, m_2, \ldots, m_k \in \mathscr{M} \times \{0\}$ with $k \leq n$ and the other entries of $\overline{m}'$ are in $\mathscr{M}' \times \{1\}$. The formula for $\mathscr{E}(\overline{m})$ becomes

$$\bigcap_{i=1}^{k} (\bigcup_{u} (\phi_u^{-1}(m_i) \times \{0\}) \cap \bigcap_{i=k+1}^{n} (\bigcup_{v} (\phi'^{-1}_{v}(m_i) \times \{1\}). \tag{62}$$

So $\mathscr{E}(\overline{m}) = \emptyset$ as soon as $\overline{m} \notin \mathscr{M}^n \cup \mathscr{M}'^n$. It is clear that in general, even when one has assumed uniform distributions for the messages in $\mathscr{M}$ and $\mathscr{M}'$, the same property will not be true for $\mathscr{M} \coprod \mathscr{M}'$, so we want to calculate P_j using the formula

$$P_j(o \oplus o') = \sum_{\overline{m} \in (\mathscr{M} \coprod \mathscr{M}')^j} P(\overline{m}) \max_{m \in \mathscr{M} \coprod \mathscr{M}'} P(m|\overline{m}), \tag{63}$$

where $\overline{m}$ is as usual. By the above observation, (63) simplifies to

$$\begin{aligned} P_j(o \oplus o') &= \textstyle\sum_{\overline{m} \in (\mathscr{M} \times \{0\})^j} P(\overline{m}) \max_{m \in \mathscr{M} \times \{0\}} P(m|\overline{m}) \\ &+ \textstyle\sum_{\overline{m} \in (\mathscr{M}' \times \{1\})^j} P(\overline{m}) \max_{m \in \mathscr{M}' \times \{1\}} P(m|\overline{m}). \end{aligned} \tag{64}$$

Of course, in the latter expression $P(\overline{m})$ (in the first, respectively second, summation) is not the $P(\overline{m})$ in the calculation of $P_j(o)$, respectively $P_j(o')$; the probability is measured in $(\mathscr{M} \coprod \mathscr{M}')^j$ and $(\mathscr{M} \coprod \mathscr{M}')^{j+1}$. On the other hand, one notes that for $\overline{m} \in (\mathscr{M} \times \{0\})^j$, we have

$$\max_{m \in \mathscr{M} \coprod \mathscr{M}'} P(m|\overline{m}) = \max_{m \in \mathscr{M} \times \{0\}} P(m|\overline{m}), \tag{65}$$

and the same remark holds for $\overline{m} \in (\mathscr{M}' \times \{1\})^j$.

Finally, assuming uniform distribution for the total message space, we obtain the very pleasant expression

$$P_j(o \oplus o') = \frac{C^j_{|\mathscr{M}|}}{C^j_{|\mathscr{M}|+|\mathscr{M}'|}} P_j(o) + \frac{C^j_{|\mathscr{M}'|}}{C^j_{|\mathscr{M}|+|\mathscr{M}'|}} P_j(o'). \tag{66}$$

Here, C^n_m denotes the number of n-subsets in an m-set.

$|\mathscr{M}| = |\mathscr{M}'|$, one obtains the natural formula

$$P_j(o \oplus o') = \frac{C^j_{|\mathscr{M}|}}{C^j_{2|\mathscr{M}|}} (P_j(o) + P_j(o')). \tag{67}$$

The reader notes that for $j = 0$, exactly the same can be done as for the case $j > 0$.

2.2. Multiplication. In this section, we suppose a uniform distribution for the messages in o and o'.

Let (m, m') be in $\bigcup_{i,j} \phi_i(\mathscr{E}) \times \phi'_j(\mathscr{E}')$. Then

$$P_0 = \frac{|\bigcup_{i,j} \phi_i^{-1} \times \phi_j^{-1}(m, m')|}{|\mathscr{E}| \times |\mathscr{E}'|}. \tag{68}$$

Note that

$$|\bigcup_{i,j} \phi_i^{-1} \times \phi_j^{-1}(m, m')| = |(\bigcup_i \phi_i^{-1}(m)) \times (\bigcup_j {\phi'}_j^{-1}(m'))|. \tag{69}$$

It follows that we have the following satisfying formula:

$$P_0(o \otimes o') = P_0(o) \times P_0(o'). \tag{70}$$

Now let o and o' be objects in $\mathbf{A}$ with P-vectors $\overline{P(o)} = (P_0(o), P_1(o), \ldots, P_r(o))$ and $\overline{P(o')} = (P_0(o'), P_1(o'), \ldots, P_{r'}(o'))$. Then we need to calculate, for any feasible natural n (which we will easily make explicit below), and $((m_1, m'_1), (m_2, m'_2), \ldots, (m_n, m'_n)) \in (\mathscr{M} \times \mathscr{M}')^n$:

(71)

$$\bigcap_{i=1}^{n} (\bigcup_j \phi_j^{-1}(m_i) \times \bigcup_r \phi_r'^{-1}(m'_i)) = (\bigcap_{i=1}^{n} (\bigcup_j \phi_j^{-1}(m_i))) \times (\bigcap_{i=1}^{n} (\bigcup_r \phi_r'^{-1}(m'_i))).$$

Whence we have the following formula for the general case:

$$P_j(o \otimes o') = P_j(o) \times P_j(o'). \tag{72}$$

Notice that for Cartesian objects o and o', the latter expression again can be greatly simplified.

COROLLARY 11.5. *Let o and o' be perfect objects in* $\mathbf{A}$ *with P-vectors of lengths ℓ and ℓ' respectively. Then $o \otimes o'$ is again a perfect object with a P-vector of length* $\max(\ell, \ell')$.

Proof. Follows directly from the product formula (72) and the equalities in $|\mathscr{E}| = \prod_{i=1}^{\ell} \frac{1}{P_i(o)}$ and $|\mathscr{E}'| = \prod_{i=1}^{\ell'} \frac{1}{P_i(o')}$. ■

CHAPTER 12

Automorphisms of the De Soete example

In this chapter we will compute the automorphism group of the scheme of De Soete which was explained earlier. As the reader will notice, this is not trivial. (A reader not familiar with quadrangles might want to skip this chapter at first reading.) In general, the automorphism group of the scheme will be bigger than the automorphism group of the quadrangle fixing x (see also the observation below), and it will appear that the former can be identified with the automorphism group of a geometry which completely encodes the properties of the authentication code. That geometry strips off the geometrical structure of the generalized quadrangle which cannot be seen from the point of view of the code.

1. $\Gamma(o)$ and $\Pi(o)$

We denote the GQ by $\mathcal{S}$, and we choose a fixed point x of $\mathcal{S}$. Its point set is $\mathcal{P}$. We do not suppose *a priori* that the quadrangle is finite (in the infinite case, one also obtains interesting geometrical results).
First one notices the following, the proof of which we will leave to the reader.

OBSERVATION 12.1. *Let $o \in \mathbf{A}$ correspond to the scheme by De Soete with the above data. Then $\mathrm{Aut}(\mathcal{S})_x$ induces a subgroup of $\mathrm{Aut}(o)$.* ■

Let $\alpha \in \mathrm{Aut}(o)$. Then clearly α has the property that $y\mathtt{I}L$ if and only if $y^\alpha\mathtt{I}L^\alpha$, when $y \in x^\perp \setminus \{x\}$, and $L\mathtt{I}x$. So locally it induces an automorphism of $\mathcal{S}$. (We assume without loss of generality that x is also fixed.) Since the fibers (inverse images) of ϕ_i, where $i \in \mathtt{I}$ is arbitrary, must be mapped to the fibers of $\phi_{\alpha(i)}$, it follows that if U is any subset of $x^\perp \setminus \{x\}$, then

$$(\bigcap_{u\in U} u^\perp)^\alpha = \bigcap_{u\in U} u^{\alpha\perp}. \tag{73}$$

In particular, if $v \in \mathcal{P} \setminus x^\perp$, then $\cap_{w\in\{x,v\}^\perp} w^\perp =: \{x,v\}^{\perp\perp}$ is bijectively sent to $\{x,v^\alpha\}^{\perp\perp} = (\{x,v\}^{\perp\perp})^\alpha$. Moreover, if $r \in \{a,x\}^{\perp\perp}$, then $r^\alpha \in \{a^\alpha,x\}^{\perp\perp}$. We have proved the next theorem.

THEOREM 12.2. *The automorphism group of o is isomorphic to the stabilizer of the point x in the automorphism group of the rank 2 geometry $\Gamma(o)$, of which*

- *the* POINTS *are the points of $\mathcal{S}$, and*

- *the* LINES *are of two types: lines incident with x, and sets $\{x,u\}^{\perp\perp} \setminus \{x\}$, with $u \not\sim x$.*

(Incidence is the natural one.) ■

(Notice that finiteness is not used.) In general, it follows that $\mathrm{Aut}(o)$ is bigger than $\mathrm{Aut}(\mathscr{S})_x$. The following theorem explicitly describes this phenomenon.

THEOREM 12.3. *$\mathrm{Aut}(\mathscr{S})_x$ is strictly contained in $\mathrm{Aut}(o)$ if at least one span $\{x,v\}^{\perp\perp}$ with $v \not\sim x$ has size at least 3.*

Proof. Suppose some span $S = \{x,w\}^{\perp\perp}$ with $w \notin x^{\perp}$ contains a point a different from x and w. Define the following element β of $\mathrm{Aut}(\Gamma(o))$: β fixes all points of $\mathscr{S}$ not in S, and induces an arbitrary nontrivial permutation of $S \setminus \{x\}$. Then β clearly is not in $\mathrm{Aut}(\mathscr{S})_x$. ■

Conversely, one might wonder whether $\mathrm{Aut}(\mathscr{S})_x = \mathrm{Aut}(o)$ if all spans of the form $\{x,v\}^{\perp\perp}$ have size 2; this can be shown to be so, for instance, when the order of the GQ is (s,s^2) [**19**]. (We refer the reader to [**19**] for much more considerations on this matter.)

More generally, if $\{T_j | j \in J\}$ is the set of all such spans (with the point x already left out), and by $\mathbf{S}(\Omega)$ we denote the symmetric group on a given set Ω, then Theorem 12.2 "generates" an automorphism group of $\Gamma(o)$ isomorphic to the direct product

$$\Pi_{j\in J}\mathbf{S}(T_j) \tag{74}$$

which fixes all points of $x^{\perp}$. In a generalized quadrangle, the only such group must act freely on $\mathscr{P} \setminus x^{\perp}$ (by [**8**, 8.1.1]).

There is another transparent way to calculate $\mathrm{Aut}(o)$. Define the rank 2 geometry $\Pi(o)$ as follows:

- POINTS are the points of $x^{\perp}$;
- LINES are the lines incident with x and perps $\{u,x\}^{\perp}$, $u \not\sim x$;
- INCIDENCE is (symmetrized) containment.

Clearly,

$$\mathrm{Aut}(\Gamma(o))_x = T \rtimes \mathrm{Aut}(\Pi(o))_x, \tag{75}$$

where T is the subgroup of $\mathrm{Aut}(\Gamma(o))_x$ which fixes $x^{\perp}$ pointwise (that is, the kernel of the action of $\mathrm{Aut}(\Gamma(o))_x$ on $\Pi(o)$). Note that we already met T as

$$T = \Pi_{j\in J}\mathbf{S}(T_j). \tag{76}$$

2. Example

Now suppose that $\mathscr{S}$ is finite, $s = t$, and x a regular point. Then it is easy to see that $\Pi(o)$ is a projective plane of order s. Putting for instance $\mathscr{S}$ equal to the symplectic quadrangle $\mathbf{W}(q)$, which has as point set the points of projective 3-space $\mathbf{PG}(3,q)$ over the finite field $\mathbb{F}_q$, and as lines the totally isotropic lines of a given symplectic polarity of that space, this observation holds true (since any point of $\mathbf{W}(q)$ is regular [**8**, Chapter 5], and $s = t = q$). In that case, $\Pi(o)$ is isomorphic to the Desarguesian plane $\mathbf{PG}(2,q)$, and

$$\mathrm{Aut}(\Pi(o))_x \cong \mathbf{P\Gamma L}_3(q)_x. \tag{77}$$

The set $\mathscr{P} \setminus x^{\perp}$ is partitioned in precisely q^2 sets T_i, each of size q, since x is a regular point, so that

$$T = \Pi_{i=1}^{q^2}\mathbf{S}_q. \tag{78}$$

Together with (75), we obtain a precise description of $\mathrm{Aut}(o)$ for the De Soete scheme with $\mathscr{S} = \mathbf{W}(q)$ and x arbitrary.

CHAPTER 13

Group schemes

In this chapter, by using our abstract setting, we introduce a general type of authentication scheme using groups, and note that many known examples are particular instances of this scheme.

Let G be a finite group, and $\{G_i | i = 1, \ldots, n\}$ a set of nontrivial subgroups of G. Then these data define the following object in **A**:

$$(G, G, \mathrm{id}, \mathtt{I}, (\phi_i)_{i \in \mathtt{I}}, \cup_{i \in \mathtt{I}} G/G_i), \tag{79}$$

where $\mathtt{I} = \{1, 2, \ldots, n\}$ and $\phi_i : G \longrightarrow G/G_i$ sends any g to gG_i. (Here G/G_i denotes the left coset space of G_i in G.) Often we will abbreviate the data by $(G, \{G_i\}_i)$.
Note that the object is Cartesian since $gG_i = hG_j$ implies $i = j$.
The P-values are given by the following expressions (below we assume the typical uniform probability distributions, although again all formulas are easily adapted to the general case):

$$\begin{cases} P_0 = \dfrac{|G_i|}{|G|} \\ \\ P_j = \dfrac{|G_1 \cap G_2 \cap \cdots \cap G_{j+1}|}{|G_1 \cap G_2 \cap \cdots \cap G_j|} \quad \text{for } j > 0, \end{cases} \tag{80}$$

where in the first formula, the size of G_i is independent of i by assumption (and similar remarks hold for the second formula). Note that for any $l \in G$, we have $|lG_i| = |G_i|$, and for any set $S \subseteq G$, and any set of subgroups $\{G_s | s \in S, G_s \leq G\}$, we have that

$$| \cap_{s \in S} sG_s | = | \cap_{s \in S} G_s | \tag{81}$$

if $\cap_{s \in S} sG_s$ is not empty.

1. Normal subgroups

An interesting example is when each G_i is a normal subgroup of G (which we then denote by N_i). So in that case we have, for each i, exact sequences

$$0 \longrightarrow G_i \longrightarrow G \longrightarrow G/G_i \longrightarrow 0. \tag{82}$$

2. Geometrical examples

We call the scheme *geometrical* if G is an elementary abelian p-group for some prime p. In that case, G can be seen as a u-dimensional vector space over $\mathbb{F}_p$ (where $|G| = p^u$), and the G_i can be seen as subspaces. (Note that the geometrical examples are special cases of the normal ones.) The whole situation can equally be represented in $\mathbf{PG}(u, p)$ by projectively completing G, that is, by adding the hyperplane at infinity so as to obtain a projective space.

The scheme of Klein, Schillewaert and Storme (using generalized dual arcs) [**6**] is an example of this geometrical scheme. For, if $\mathscr{D}$ is a generalized dual arc in $\mathbf{PG}(n, q)$, the elements of $\mathscr{D}$ having dimension n_1, one embeds $\mathbf{PG}(n, q)$ as a hyperplane in $\mathbf{PG}(n+1, q)$. Defining $\mathbf{AG}(n+1, q)$ to be $\mathbf{PG}(n+1, q)$ without $\mathbf{PG}(n, q)$, and choosing an affine point z, the spaces $z\beta_i$ with $\beta_i \in \mathscr{D}$ can be seen as subgroups of T of size q^{n_1+1}, where T is the translation group of $\mathbf{AG}(n+1, q)$. Since T is an elementary abelian p-group, putting $G = T$, $G_i = z\beta_i$ and interpreting everything over $\mathbb{F}_p$, we obtain that the scheme indeed is geometrical. (Note that in the generalized dual arc scheme, one chooses an affine point e as encoding rule, and the encoded message, after choosing the source state i, is the space $e\beta_i$; this space corresponds precisely with the coset eG_i.)

3. Multiple transitivity

Let G be a finite group acting n-transitively on the set S, and identify $\mathtt{I}$ with S. Put $\{G_i\} = \{G_s | s \in S\}$. Then for $j \leq n-1$, the P-values are easily computed as:

$$P_j = \frac{1}{|S| - j}. \tag{83}$$

Particularly, with $|S| = n \in \mathbb{N}$ and G isomorphic to the symmetric group $\mathbf{S}_n$ acting naturally on S, we obtain that

$$|G| = \Pi_{i=0}^{n-1}(n-i), \tag{84}$$

so that the obtained schemes are perfect and Cartesian. (We have no doubt that the multiply transitive examples were already known in one way or another.)

4. Arithmetical example

For retaining the aforementioned arithmetic example, just put $G = \mathbb{Z}/N\mathbb{Z}$, $G_i = \mathbb{Z}/n_i\mathbb{Z}$ (where $N = n_1 n_2 \ldots n_k$ and the n_i have no common nontrivial divisors); the ϕ_i are projections

$$\phi_i : G \longrightarrow G/G_i : x + N\mathbb{Z} \longrightarrow x + n_i\mathbb{Z}(+N\mathbb{Z}). \tag{85}$$

5. The Gilbert-McWilliams-Sloane example as a group scheme

Consider group scheme data $(G, \{G_i\}_{\mathtt{I}})$, and suppose that for all $i \in \mathtt{I}$ we have that $|G| = |G_i|^2 = c^2$, $c \in \mathbb{N}_{0,1} = \mathbb{N} \setminus \{0, 1\}$, $|\mathtt{I}| = c + 1$, and suppose that $G_i \cap G_j = \{\mathbf{1}\}$ when i and j are different. It follows that $G_iG_j = G$ for any such i, j. Define a rank 2 geometry $\Gamma \equiv \Gamma(G, \{G_i\}_{\mathtt{I}})$ as follows:

- POINTS are elements of G;
- LINES are the left cosets gG_i;
- INCIDENCE is (symmetrized) containment.

Then it is easy to see that Γ is an affine plane of order c. Moreover, G acts sharply transitively on Γ by left multiplication, while fixing all parallel classes. So, by definition, Γ is a *translation plane* with translation group G. As a corollary, G is an elementary abelian p-group for some prime p.
Consider the corresponding scheme $o = (G, G, \mathrm{id}, \mathtt{I}, (\phi_i)_{i\in\mathtt{I}}, \cup_{i\in\mathtt{I}} G/G_i)$. Then the reader notices the next theorem:

THEOREM 13.1. *o is isomorphic to the Gilbert-McWilliams-Sloane scheme for the projective completion $\overline{\Gamma}$ of Γ.* ■

As before, it is easy to prove that the automorphism group of o coincides with $\mathrm{Aut}(\Gamma)$. On the other hand, note that the subgroup of $\mathrm{Aut}(G)$ which stabilizes the set $\mathscr{G} = \{G/G_i | i \in \mathtt{I}\}$ (the "stabilizer of the scheme" in $\mathrm{Aut}(G)$) does *not* coincide with $\mathrm{Aut}(o)$. (The left action of G is not contained in $\mathrm{Aut}(G)$.) Still, the following is easily seen to be true:

OBSERVATION 13.2. $\mathrm{Aut}(G)_{\mathscr{G}} \leq \mathrm{Aut}(o)$. *Moreover, for any point $g \in \Gamma$, we have that* $\mathrm{Aut}(\Gamma)_g \cong \mathrm{Aut}(G)_{\mathscr{G}}$. ■

6. De Soete schemes as group schemes

We can easily imitate the previous example so as to obtain a similar viewpoint for the De Soete schemes. For consider a GQ $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathtt{I})$ of order (s, t) with $s \neq 1 \neq t$. Suppose that for some point x of $\mathscr{S}$, there is a subgroup E of $\mathrm{Aut}(\mathscr{S})_x$ which fixes every line through x, and acts sharply transitively on $\mathscr{P} \setminus x^\perp$ (so that $|E| = s^2t$). Let $L_0, L_1, \ldots, L_t$ be the lines incident with x. Choose any point z not collinear with x, and let $x_i = \mathrm{proj}_{L_i} z$ for all i. Define for such i, E_i to be E_{x_i}.

THEOREM 13.3. *In this setting, $o = (E, E, \mathrm{id}, \mathtt{I}, (\phi_i)_{i\in\mathtt{I}}, \cup_{i\in\mathtt{I}} E/E_i)$ is isomorphic to the De Soete scheme constructed from the pointed GQ $(\mathscr{S}, x)$.*

Proof. The isomorphism is natural: send a point v of $\mathscr{P} \setminus x^\perp$ to the $\alpha \in E$ for which $z^\alpha = v$, let the permutation of $\mathtt{I}$ be the identity, and let a point $y \in x^\perp \setminus \{x\}$

correspond to lE_i if $y\mathtt{I}L_i$, with l any element of E which sends x_i to y. ■

Later, we will see that in some situations, the De Soete scheme “covers” the Gilbert-McWilliams-Sloane scheme.

7. Automorphism groups

In general, it is not possible to give a unifying formula for the automorphism groups of group schemes — the automorphism groups depend heavily on the structure of G and the given subgroups G_i (for instance, in the Gilbert-McWilliams-Sloane group scheme determination of $\mathrm{Aut}(o)$ boils down to determination of the automorphism group of the plane). But still, in some situations it is possible to say slightly more (thinking especially of variations on the arithmetic example).

THEOREM 13.4. *Consider group scheme data* $(G, \{G_i\}_{\mathtt{I}})$*, and suppose that for* $i \neq j$*,* $(|G_i|, |G_j|) = 1$ *and* $G_iG_j = G_jG_i$*. Also assume that* $|G| = \Pi_{i=1}^{|\mathtt{I}|}|G_i|$*. Write* $|G_i| = n_i$ *for* $i \in \mathtt{I}$*. Then*

$$\mathrm{Aut}(o) \cong G \rtimes (\Pi_{i=1}^{|\mathtt{I}|}\mathbf{S}_{n_i-1}). \tag{86}$$

Proof. It is clear that G acts by left multiplication on o, and sharply transitively on the encoding rules, so that we can fix any point in G, say $\mathbf{1}$, and look at the point stabilizer. Clearly, since $(n_i, n_j) = 1$ for $i \neq j$, an element α in $\mathrm{Aut}(o)_{\mathbf{1}}$ must fix all subgroups G_i. So α induces a permutation in each of the G_is which fixes $\mathbf{1}$. (Note at this point that $G_i \cap G_j = \{\mathbf{1}\}$ for all $i \neq j$.) Vice versa, let $\alpha_i \in \mathbf{S}(G_i^{\times})$ be arbitrary. Note that since $G_iG_j = G_jG_i$ for all i, j, we have that

$$G = G_1G_2 \cdots G_k, \tag{87}$$

with $k = |\mathtt{I}|$, and each element of G can be uniquely be written in the form $g_1g_2 \cdots g_k$, with $g_j \in G_j$. It follows now that $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ naturally induces an element of $\mathrm{Aut}(o)_{\mathbf{1}}$ which induces in each G_i the element α_i. ■

COROLLARY 13.5. *Consider group scheme data* $(G, \{G_i\}_{\mathtt{I}})$*, and suppose that for* $i \neq j$*,* $(|G_i|, |G_j|) = 1$*. Assume that* $|G| = \Pi_{i=1}^{|\mathtt{I}|}|G_i|$*, and that the* G_i *are all normal subgroups of* G*. Write* $|G_i| = n_i$ *for* $i \in \mathtt{I}$*. Then*

$$\mathrm{Aut}(o) \cong G \rtimes (\Pi_{i=1}^{|\mathtt{I}|}\mathbf{S}_{n_i-1}). \tag{88}$$

In particular, the theorem holds when G *is abelian.* ■

Putting $G = \mathbb{Z}/N\mathbb{Z}$ and $G_i = \mathbb{Z}/n_i\mathbb{Z}$ for natural numbers N and n_i such that $N = n_1n_2 \ldots n_k$, and $(n_i, n_j) = 1$ for $i \neq j$, we obtain again the automorphism group of the numerical scheme!

CHAPTER 14

Construction of examples — Algorithms

In this chapter, we show, using the multiplication in $\mathbf{A}/\mathbf{CA}$, that there are transparent algorithms to produce authentication codes *à la minute*. In fact, what the algorithms essentially say is that given a set of parameters of a hypothetical "very good" authentication code (so which does not violate the necessary standard arithmetic inequalities), such codes actually exist.

1. Practical — short length

From the practical point of view, the most important probability parameters for authentication codes are the P_0 (= P_I) and the P_1 (= P_S) values. In that case, one wants to have codes at hand where the P_i, $i = 0, 1$, are as small as possible with respect to the number of encoding rules. A natural additional assumption for having a strong code is demanding minimal decay for P_1, that is, demanding that P_1 is close to P_0. So an important class of authentication codes consists of the perfect codes with

$$(89) \qquad |\mathscr{E}| = \frac{1}{P_0} \cdot \frac{1}{P_1} = \frac{1}{P_0^2}.$$

The only such codes known seem to be the GMWS-schemes from projective planes; there, if n is the order of the plane, $|\mathscr{E}| = n^2$ and $P_0 = P_1 = 1/n$. It is important to note that it is conjectured that the order of a finite projective plane is always a prime power — see [**17**] for more details.
The following theorem presents a broad generalization of this construction.

THEOREM 14.1. *Let $k \in \mathbb{N}$ be any natural number different from $0, 1$. Then there exists a perfect authentication A-scheme with*

$$(90) \qquad |\mathscr{E}| = k^2 \text{ and } \frac{1}{P_I} = \frac{1}{P_S} = k.$$

Proof. We will give a constructive proof.

STEP 1 Write down the prime power decomposition for k:

$$(91) \qquad k = \prod_{i=1}^{r} p_i^{n_i},$$

where the p_i are distinct primes and the n_i nonzero natural numbers.

STEP 2 For each $i \in \{1,2,\ldots,r\}$, put o_i equal to the GMWS-scheme constructed from the Desarguesian projective plane $\mathbf{PG}(2,{p_i}^{n_i})$ over the field with ${p_i}^{n_i}$ elements. For each i, this is a perfect scheme with probability parameters $P_I^i = 1/({p_i}^{n_i}) = P_S^i$.

STEP 3 Apply Corollary 11.5 to construct the perfect scheme

$$o = \bigotimes_{i=1}^{r} o_i \tag{92}$$

which is the desired code.

■

Note that for any i, one is allowed to construct a GMWS-scheme from *any* projective plane of order ${p_i}^{n_i}$, so that Theorem 14.1 truly gives an algorithm for construction a great deal of such schemes (which can easily be computed in function of the prime power decomposition, and the number $\chi(\ell)$ of nonisomorphic projective planes of a given prime power order ℓ).

If one wants to concentrate on P_S and P_I, and for instance aims to construct schemes where equality $P_I = P_S$ holds, but not necessarily perfect schemes, one can consider, e.g., a set S of De Soete schemes and GMWS-schemes, and apply the previous algorithm to obtain products of elements in S.

REMARK 14.2. Let o be an A-code (without splitting), such that $P_0 = P_1 = 1/c$ for some $c \in]0,1[$. It is well-known that

$$|\mathscr{E}| \geq |\mathtt{I}|(c-1)+1, \tag{93}$$

and equality holds if and only if the incidence matrix of $\mathscr{E}$ is an orthogonal array $\mathrm{OA}(c,|\mathtt{I}|,\lambda)$ with $\lambda = (|\mathtt{I}|(c-1)+1)/c^2$ and each $e \in \mathscr{E}$ is used with equal probability. (And of course, in general, $|\mathscr{E}| \geq c^2$.) Although the codes from which we start in Theorem 14.1 indeed come from orthogonal arrays, one must note that the eventually constructed codes do not; it is easily verified that equality cannot hold because the cardinalities of the source sets are multiplied. Still, all the constructed codes "are" very close to equality.

The following theorem presents a variation on the algorithm of Theorem 14.1. It constructs perfect codes with $|\mathscr{E}| = \frac{1}{P_I P_S}$, P_I and P_S still being very close to each other, but not equal. It generalizes the shorth length schemes based on sharply 2-transitive groups.

THEOREM 14.3. *Let $k \in \mathbb{N}$ be any natural number different from* $0, 1$. *Then there exists a perfect authentication A-scheme with*

$$|\mathscr{E}| = k\prod_{i=1}^{r}({p_i}^{n_i} - 1) \ \textit{and}\ \frac{1}{P_I} = k,\ \frac{1}{P_S} = \prod_{i=1}^{r}({p_i}^{n_i} - 1), \tag{94}$$

where $\prod_{i=1}^{r} {p_i}^{n_i}$ is the prime number decomposition of k.

Proof. Again we provide a constructive proof.

STEP 1 As in Theorem 14.1, write down the prime power decomposition for k:

$$k = \prod_{i=1}^{r} p_i^{n_i}, \tag{95}$$

where the p_i are distinct primes and the n_i nonzero natural numbers.

STEP 2 For each $i \in \{1, 2, \dots, r\}$, put o_i equal to the group scheme constructed from a sharply 2-transitive group K acting on a set of ${p_i}^{n_i}$ letters. For each such i, this is a perfect scheme with probability parameters $P_I^i = 1/({p_i}^{n_i})$ and $P_S^i = 1/({p_i}^{n_i} - 1)$.

STEP 3 Apply Corollary 11.5 again to construct the perfect scheme

$$o = \bigotimes_{i=1}^{r} o_i \tag{96}$$

which is the desired code.

■

Theorem 14.1 and Theorem 14.3 can now be combined to construct still other large classes of perfect schemes with similar properties as those constructed in Theorem 14.3.

The reader can of course substitute “sharply 2-transitive” by “sharply 3-transitive” (for instance by considering the groups $\mathbf{PGL}_2(q)$ in their natural action on the projective line over $\mathbb{F}_q$) in the above approach to generate similar examples with probability length 3, etc.

2. Theoretical — any length

Now we construct some perfect group schemes of any length. Both algorithms below are based on the symmetric group schemes considered earlier.

2.1. Power algorithm. First construct the group scheme o from the symmetric group $\mathbf{S}_{r+1}$, with $r \in \mathbb{N}_0$; it is perfect and for $j \in \{0, 1, \ldots, r-1\}$, we have that

$$\frac{1}{P_j} = \frac{1}{r+1-j}. \tag{97}$$

For any $w \in \mathbb{N}_0$, now consider

$$\bigotimes_{i=1}^{w} o, \tag{98}$$

which is a perfect scheme with $|\mathscr{E}| = ((r+1)!)^w$ and probability parameters

$$\frac{1}{P_j} = \frac{1}{(r+1-j)^w}. \tag{99}$$

The advantage of this construction is the fact that we fix the probability length of the scheme, which remains perfect throughout the process, while getting the worst parameter (P_{r-1}) as small as we want. (The cost being the fact that $|\mathscr{E}|$ grows exponentially.)

2.2. Breakdown algorithm. A second code we propose is the following. Let $k \in \mathbb{N}_{0,1}$ be any natural number, and write

$$k = \prod_{i=1}^{n} k_i, \tag{100}$$

where $k_i \in \mathbb{N}_{0,1}$ is not necessarily a prime power.
For each k_j, $j \in \{1, \ldots, n\}$, construct the group scheme o_j from the symmetric group $\mathbf{S}_{k_j}$; it is a perfect scheme with probability parameters

$$\frac{1}{P_m^j} = \frac{1}{k_j - m} \tag{101}$$

for $m = 0, 1, \ldots, k_j - 2$.
Now multiply all schemes to obtain

$$o := \bigotimes_{i=1}^{n} o_i. \tag{102}$$

It is a perfect A-scheme with $\mathbf{I} = \prod_{i=1}^{n} k_j$,

$$|\mathscr{E}| = \prod_{i=1}^{n} (k_i)! \leq k!, \tag{103}$$

and parameters

$$\frac{1}{P_u} = \prod_{i=1}^{n} \frac{1}{k_i - u}, \tag{104}$$

where in the latter, we put $1/(k_v - v) = 1$ if $v \geq k_v$. The probability length of o is $\max_j(k_j)$.

2.3. Combining short and arbitrary length. It is now easy to construct perfect codes of arbitrary probability length ℓ, with strong P_I and P_S paramaters, as follows.

Take any of the above perfect code schemes of probability length ℓ (or any other such code), and multiply it with any short length scheme. By Corollary 11.5, we still have a perfect scheme (with the same probability length of the "longest factor"), which is concentrated in P_I and P_S.
The latter two can be chosen as small (and as close together) as we want by taking the appropriate short length code, and all parameters can be easily controlled.

2.4. Generation of algorithms. Combining both addition and multiplication, one can describe a universe of algorithms by starting from some initial set of good authentication codes, in the spirit of the previous sections.

CHAPTER 15

Covers

Suppose $(\mathscr{S},x)$ is a pointed generalized quadrangle of order (s,s), $s \neq 1$ and $s < \infty$, and let x be a regular point. Moreover, suppose E is a subgroup of $\mathrm{Aut}(\mathscr{S})_x$ fixing each line on x and acting sharply transitively on the points not collinear with x. As before, with respect to some fixed point z not collinear with x, we introduce the subgroups E_i for $i = 0,1,\ldots,s$. Each of these subgroups has size s^2 (and E itself has size s^3). It can be proved (cf. [**18**]) that E has a subgroup $\mathbb{E}$ of order s, of which each of the elements fixes every point of $x^{\perp}$. (Essentially, this expresses group theoretically that x is a regular point.) We note that s is the maximal possible size for a subgroup with this property. Let $o \in \mathbf{A}$ be the group theoretical De Soete code defined by the data $(E,\{E_i\}_{\mathtt{I}})$, with $\mathtt{I} = \{0,1,\ldots,s\}$ (cf. §6).

As $\mathbb{E}$ is a normal subgroup of E, we can now consider the data

$$(E/\mathbb{E},\{E_i/\mathbb{E}\}_{\mathtt{I}}), \tag{105}$$

and construct the code o' out of it. Note that $E/\mathbb{E}$ has size s^2, each $E_i/\mathbb{E}$ has size s, and for $i \neq j$, $(E_i/\mathbb{E}) \cap (E_j/\mathbb{E})$ is trivial. Whence we have a group theoretical Gilbert-McWilliams-Sloane scheme (which corresponds with the scheme constructed from the projective plane $\Pi(x)$).

So the first code o "covers" the second one o' (through the group $\mathbb{E}$) — in other words, o is an "extension" of o' and o' a "quotient" of o. This observation opens an interesting setting to pass from one code to another.

1. Covers and quotients

In general, we say that a group scheme determined by data $(G,\{G_i\}_{\mathtt{I}})$ *covers* the scheme with data $(H,\{H_i\}_{\mathtt{I}})$, if there is a normal subgroup $\mathbb{G}$ of G contained in $\bigcap_{i\in\mathtt{I}} G_i$ such that

$$\begin{cases} G/\mathbb{G} = H \\ G_i/\mathbb{G} = H_i \quad \text{for all } i \in \mathtt{I}, \end{cases} \tag{106}$$

possibly up to a permutation of $\mathtt{I}$. We also use the terms "quotient" and "extension" as above. The cover is *maximal* if $\mathbb{G} = \bigcap_{i\in\mathtt{I}} G_i$. We require that $\mathbb{G}$ does not coincide with any of the G_is for obvious reasons. (So both codes indeed have the same index sets $\mathtt{I}$.)

2. Automorphisms of covers

Suppose a code o determined by data $(G, \{G_i\}_{i \in \mathtt{I}})$ is a maximal cover of the code o' through the normal subgroup $\mathbb{G}$. Without loss of generality we may suppose that o' is given by data

$$(G/\mathbb{G}, \{G_i/\mathbb{G}\}_{i \in \mathtt{I}}). \tag{107}$$

Let $\alpha \in \mathrm{Aut}(o)$ fix the element $\mathbf{1}$ of G. Then α must fix $\mathbb{G}$. Still, there is no reason to conclude that α induces an element of $\mathrm{Aut}(o')$, since α is not necessarily a group morphism (so that one does not know *a priori* what happens with the left cosets). But if α *would be* an automorphism of G, it is clear that it would induce an element of $\mathrm{Aut}(o')$.

On the other hand, if we start from an automorphism β of o' it is always possible to lift β in a maximal sense (i.e., by a theoretical maximal number of ways) to automorphisms of o. For suppose β is as such. Let

$$\mathscr{F} = \{g\mathbb{G} | g \in G\} \tag{108}$$

be the set of fibers of the projection morphism defined by $\mathbb{G}$; its size is $|G|/|\mathbb{G}| = r$. For the sake of convenience, we write $\mathscr{F} = \{F_j | j \in \mathbf{J}\}$ with $\mathbf{J}$ a set of size r, and see each F_j as a copy of some set F. Let $\gamma = (\gamma_1, \ldots, \gamma_r)$ be any element of $\Pi_{i=1}^{r}\mathbf{S}(F_i)$. Then (β, γ) determines an automorphism of o in the following way: the action on $\mathscr{F}$ is determined by β and, for $F_i \in \mathbf{F}$, the action on the points of F_i is given by the action of γ_i on F (with images lying in the copy F_i^{β}).

We have proved that

$$(\Pi_{i=1}^{r}\mathbf{S}(F_i)) \rtimes \mathrm{Aut}(o') \leq \mathrm{Aut}(o), \tag{109}$$

a formula which we already observed in the special case of the De Soete scheme (with some additional assumptions). Here, $\Pi_{i=1}^{r}\mathbf{S}(F_i)$ can be seen as a group fixing $\mathbf{F}$ elementwise.

REMARK 15.1 (Combinatorial covers). One could also introduce the concept of "combinatorial covering", so that one does not need the group theoretical setting, while the formula (109) still holds. The group theoretical notion then becomes a particular instance of the combinatorial one. We leave the details to the reader, who can use the combinatorial connection between the general De Soete scheme (with x a regular point and $s = t$) and the general Gilbert-McWilliams-Sloane scheme as a model.

CHAPTER 16

Cohomology

Consider the De Soete scheme $o(\mathscr{S},x)$ arising from a pointed generalized quadrangle $(\mathscr{S},x)$, and let $o \in \mathbf{A}$ correspond to $o(\mathscr{S},x)$. We have seen that the automorphism group $\mathrm{Aut}(o)$ of o is in general *much* bigger than $\mathrm{Aut}(\mathscr{S})_x$, although the latter is a subgroup of $\mathrm{Aut}(o)$ in a natural way. On the other hand, the geometry $\Gamma(o)$ has the same automorphism group (stabilizing x) as o. The factor

$$\frac{|\mathrm{Aut}(o)|}{|\mathrm{Aut}(\mathscr{S})_x|} \tag{110}$$

expresses the fact that a big part of the geometric structure of the quadrangle is not used (and not necessary) in the scheme o. And on the contrary, we have

$$\frac{|\mathrm{Aut}(o)|}{|\mathrm{Aut}(\Gamma(o))_x|} = 1. \tag{111}$$

So the two latter fractions measures in a sense the cohomological property how essential the geometry is for the scheme.

We want to formalize this idea.

1. Cohomology principle

Let $o \in \mathbf{A}$. We say that a mathematical structure $\Gamma(o)$ is a *module* for o if a (concrete) model of o can be defined "as a substructure" of $\Gamma(o)$. (This model is just an element of $\mathbf{CA}$.) (Think of the De Soete scheme which is defined on a substructure of $\mathscr{S}$.) We say $\Gamma(o)$ is *natural* if

$$\mathrm{Aut}(\Gamma(o))_o/K \leq \mathrm{Aut}(o), \tag{112}$$

where $\mathrm{Aut}(\Gamma(o))_o$ denotes the stabilizer of the defining substructure for o in $\mathrm{Aut}(\Gamma(o))$, and K the kernel of the induced action on the substructure. (In the De Soete scheme, $\mathrm{Aut}(\Gamma(o)) = \mathrm{Aut}(\mathscr{S})_x$ and K is trivial — note that here $\Gamma(o)$ has a different meaning than in the De Soete section.) Then to o we associate the set $\mathbf{S}(o)$, which we call the *moduli space* of o, which consists of all natural modules of o. The *cohomology* of o with respect to $\Gamma(o)$ is

$$H(o,\Gamma(o)) = \mathrm{Aut}(o)/(\mathrm{Aut}(\Gamma(o))_o/K), \tag{113}$$

where the latter denotes the left coset space of $\mathrm{Aut}(\Gamma(o))_o/K$ in $\mathrm{Aut}(o)$. The *cohomology* $H(o)$ of o is the set of all $H(o,\Gamma(o))$ where $\Gamma(o)$ varies over $\mathbf{S}(o)$. The size of an element $H(o,\Gamma(o))$ of $H(o)$ expresses how "close" the structure of the module $\Gamma(o)$ is to the structure of the scheme o, that is, how much of the structure of the module is used in the construction of the scheme. So of special interest are the modules with trivial cohomology spaces.

If a cohomology space $H(o,\Gamma(o))$ is large, it means that the scheme o can be constructed in modules with much less structure, and in particular in modules which might look completely different in nature than $\Gamma(o)$ (while the scheme still is the same one!). It might therefore be a good idea to calculate the cohomology once a construction of an authentication code is given, in order to check the strength of the construction. Of course, usually this is a hard problem.

OBSERVATION 16.1 (Cohomology principle). *If $H(o,\Gamma(o))$ is "large", the probability is "large" that the scheme can be/has been constructed in another setting.*

This principle can easily be explained with an example. In the scheme of De Soete, applied to the symplectic quadrangle $\mathbf{W}(q)$, we have that

$$|H(o,\mathbf{W}(q))| = \frac{(q!)^{q^2}}{q}, \tag{114}$$

while $|H(o,\Gamma(o))| = 1$, meaning that one can construct many geometries (the many being some function of q) in between $\Gamma(o)$ and $\mathbf{W}(q)$ which are all natural modules for o, with cohomology "in between" the one point space and $H(o,\mathbf{W}(q))$. Note that now we use the $\Gamma(o)$-notation of §12 (both $\mathbf{W}(q)$ and $\Gamma(o)$ are o-modules). Another good example we already met is the Gilbert-McWilliams-Sloane example where the cohomology is trivial (which makes the planar module a very good one).

2. Cohomology of covers

Suppose that o is a maximal cover of o' (in the group theoretical setting); we use the notation of §2. Then

$$(\Pi_{i=1}^{r}\mathbf{S}(F_i)) \rtimes \mathrm{Aut}(o') \leq \mathrm{Aut}(o). \tag{115}$$

Remark that the translations by elements of G form a subgroup of $\mathrm{Aut}(G)_o$ which intersects trivially with $(\Pi_{i=1}^{r}\mathbf{S}(F_i)) \rtimes \mathrm{Aut}(o')$.

Elements of $\mathrm{Aut}(G)_o$ induce elements of $\mathrm{Aut}(G/\mathbb{G})_{o'}$. Conversely, there is no general way to lift elements of $\mathrm{Aut}(G/\mathbb{G})_{o'}$ to elements of $\mathrm{Aut}(G)_o$. It follows that

$$\left\{\begin{array}{l} \dfrac{|\mathrm{Aut}(o)|}{|\mathrm{Aut}(o')|} \geq |\mathbb{G}| \cdot (|\mathbb{G}|!)^r; \\ \dfrac{|\mathrm{Aut}(G)_o|}{|\mathbb{G}|} \leq |\mathrm{Aut}(G/\mathbb{G})_{o'}|. \end{array}\right. \tag{116}$$

We have obtained the following, noting that the cohomology for both o and o' (with respect to $\Gamma(o) = (G, \{G_i\}_{\mathtt{I}})$ and $\Gamma(o') = (G/\mathbb{G}, \{G_i/\mathbb{G}\}_{\mathtt{I}})$) is well-defined, since both modules are natural.

THEOREM 16.2 (Cohomology of covers). *The cohomology of a maximal cover* o *of* o' *(with respect to the group data* $(G, \{G_i\}_{\mathtt{I}})$*) is bigger than the cohomology of* o' *(with respect to* $(G/\mathbb{G}, \{G/\mathbb{G}_i\}_{\mathtt{I}})$*). More precisely, we have that*

$$|H(o, \Gamma(o))| \geq |H(o', \Gamma(o'))| \cdot (|\mathbb{G}|!)^r. \tag{117}$$

■

The theorem expresses the fact that once an authentication code (maximally) covers another one (by a nontrivial normal subgroup), it always uses the structure of the group data by which it is defined *in a less essential way* than the code it covers.

The reader might see this result (relative the comparison of sizes) in the light of the Lyndon-Hochschild-Serre five-term exact sequence which states that, when A is an abelian H-module and K a normal subgroup of G, we have

$$\begin{aligned} 0 \longrightarrow H^1(H/K, A^K) \longrightarrow H^1(H, A) \longrightarrow H^1(K, A)^{H/K} \longrightarrow \\ H^2(H/K, A^K) \longrightarrow H^2(H, A). \end{aligned} \tag{118}$$

REMARK 16.3. The general cohomology we defined (of an object $o \in \mathbf{A}$ with respect to a natural module $\Gamma(o)$) seems to be the first cohomology of some appropriately defined "complex" $(C_i, \partial_i)_{i \in \mathbb{N}}$ of objects related to group modules. We expect that the 0-th cohomology might be something like K (the kernel of the action of $\mathrm{Aut}(\Gamma(o))_o$ on o). We suspect that $\partial_0(C_0) = \mathrm{Aut}(\Gamma(o))_o$ and $\ker(\partial_1) = \mathrm{Aut}(o)$.

APPENDIX A

Authentication codes with arbitration

Below we briefly describe how one can also view authentication codes with arbitration in a formal categorical setting. We will however not explore this in full depth, and let the reader fill in the details.

1. Abstract category

Let $\mathtt{I}$ be an arbitrary index set and let A_R, E_R, A_T, E_T and X be nonempty sets, $\iota_t : A_T \to E_T$ and $\iota_r : A_R \to E_R$ bijections, and $\alpha : A_R \to A_T$ and $\tau_i : E_T \to X$ mappings, $i \in \mathtt{I}$. Finally the ρ_is are mappings of the form $E_R \to \mathscr{P}(X)$ (the latter is the power set of X), $i \in \mathtt{I}$. Then the *category of authentication codes with arbitration* $\mathbf{A}_{arb}$ has as its objects tuples

$$(A_R,\ E_R, \iota_r, A_T, E_T,\ \iota_t, \alpha, \mathtt{I}, \{\tau_i\}_{i\in\mathtt{I}}, \{\rho_i\}_{i\in\mathtt{I}}, X). \tag{119}$$

For tuples

$$(A_R,\ E_R, \iota_r, A_T, E_T,\ \iota_t, \alpha, \mathtt{I}, \{\tau_i\}_{i\in\mathtt{I}}, \{\rho_i\}_{i\in\mathtt{I}}, X) \tag{120}$$

and

$$(A'_R,\ E'_R, \iota'_r, A'_T, E'_T,\ \iota'_t, \alpha', \mathtt{I}', \{\tau'_i\}_{i\in\mathtt{I}'}, \{\rho'_i\}_{i\in\mathtt{I}'}, X') \tag{121}$$

defined over index sets $\mathtt{I}$ and $\mathtt{I}'$ with $|\mathtt{I}| = |\mathtt{I}'|$, and for a bijective mapping $\nu : \mathtt{I} \to \mathtt{I}'$, one can define morphisms as tuples $(\nu, \overline{a_r}, \overline{a_t}, \overline{e_r}, \overline{e_t}, \overline{x})$, which are mappings making the following diagrams commute

$$\begin{tikzcd} A_R \arrow[r, "\iota_r"] \arrow[d, "\overline{a_r}"'] & E_R \arrow[d, "\overline{e_r}"'] \\ A'_R \arrow[r, "\iota'_r"] & E'_R \end{tikzcd} \tag{122}$$

$$\begin{tikzcd} A_T \arrow[r, "\iota_t"] \arrow[d, "\overline{a_t}"'] & E_T \arrow[d, "\overline{e_t}"'] \\ A'_T \arrow[r, "\iota'_t"] & E'_T \end{tikzcd} \tag{123}$$

and

(124)
$$\begin{tikzcd} A_R \arrow[r, "\alpha"] \arrow[d, "\overline{a_r}"'] & A_T \arrow[d, "\overline{a_t}"'] \\ A'_R \arrow[r, "\alpha'"] & A'_T \end{tikzcd}$$

For all $i \in \mathtt{I}$ we want

(125)
$$\begin{tikzcd} E_T \arrow[r, "\tau_i"] \arrow[d, "\bar{e}_t"'] & X \arrow[d, "\overline{x}"'] \\ E'_T \arrow[r, "\tau'_{\nu(i)}"] & X' \end{tikzcd}$$

and finally we want the following commutative diagram, where $\overline{x} : \mathscr{P}(X) \to \mathscr{P}(X')$ is naturally induced by $\overline{x} : X \to X'$:

(126)
$$\begin{tikzcd} E_R \arrow[r, "\rho_i"] \arrow[d, "\bar{e}_r"'] & \mathscr{P}(X) \arrow[d, "\overline{x}"'] \\ E'_R \arrow[r, "\rho'_{\nu(i)}"] & \mathscr{P}(X') \end{tikzcd}$$

2. Concrete authentication codes with arbitration

An object in the category of concrete authentication codes with arbitration $\mathbf{CA}_{arb}$ is a tuple

$$(\mathscr{K}_R, \mathscr{E}_R, f_r, \mathscr{K}_T, \mathscr{E}_T, f_t, \alpha, \mathscr{S}, \mathscr{M}). \tag{127}$$

Here $f_r : \mathscr{K}_R \to \mathscr{E}_R$ and $f_t : \mathscr{K}_T \to \mathscr{E}_T$ are bijections and $\alpha : \mathscr{K}_R \to \mathscr{K}_T$ is a mapping. The set $\mathscr{E}_T$ consists of mappings $e_t : \mathscr{S} \to \mathscr{M}$. The set $\mathscr{E}_R$ consists of mappings $e_r : \mathscr{S} \to \mathscr{P}(\mathscr{M})$. A *morphism* between two objects is a tuple $(\kappa_r, \eta_r, \kappa_t, \eta_t, \sigma, \mu)$ making the necessary diagrams commute.

In the A^2-model, we assume that Alice and Bob do not trust each other. In this case, they do not agree upon an encoding rule. Instead, a trusted person, the *arbiter*, is also involved in the scheme. Now Alice has a set of encoding rules $\mathscr{E}_T$, and Bob a set of decoding rules $\mathscr{E}_R$. If Alice and Bob want to communicate, Bob chooses a key k_r in $\mathscr{K}_R$ and calculates his encoding rule $e_r = f_r(k_r)$. He then sends k_r to the arbiter. Upon receipt of the key k_r the arbiter forms $k_t = \alpha(k_r)$ and sends it to Alice. With k_t corresponds an encoding rule $e_t = f_t(k_t) \in \mathscr{E}_t$. When Alice wants to communicate, she picks a source state $s \in \mathscr{S}$ and she sends the pair $(s, e_t(s))$ to Bob. When Bob receives a pair (s, m), he checks whether $m \in e_r(s)$. If so, he accepts it as a valid one. If there is a dispute between Alice and Bob about a pair (s, m), the arbiter checks if $m = e_t(s)$. If so he decides that Alice has sent the message, otherwise that she has not.

We define a functor F_{arb} from the abstract to the concrete category as follows. It maps an object $(A_R, E_R, \iota_r, A_T, E_T, \iota_t, \alpha, \mathtt{I}, \{\tau_i\}_{i\in\mathtt{I}}, \{\rho_i\}_{i\in\mathtt{I}}, X)$ of $\mathbf{A}_{arb}$ to an object $(\mathscr{A}_R, \widetilde{\mathscr{E}}_R, \widetilde{f}_r, \mathscr{A}_T, \widetilde{\mathscr{E}}_T, \widetilde{f}_t, \alpha, \mathtt{I}, \mathscr{X})$. Here $\widetilde{\mathscr{E}}_R = \psi(E_R)$ is a set of mappings $\psi_r(e_r) = \widetilde{e_r} : \mathtt{I} \longrightarrow \mathscr{P}(X)$ corresponding to elements $e_r \in E_R$ such that for all $i \in \mathtt{I} : \widetilde{e}_r(i) = \rho_i(e_r)$. Moreover $\widetilde{\mathscr{E}}_T = \psi(E_T)$ is a set of mappings $\psi_t(e_t) = \widetilde{e}_t : \mathtt{I} \longrightarrow X$ corresponding to elements $e_t \in E_T$ such that for all $i \in \mathtt{I}$: $\widetilde{e}_t(i) = \tau_i(e_t)$. The maps $\widetilde{f}_r$ and $\widetilde{f}_t$ make the following diagrams commute:

(128)
$$\begin{tikzcd}
A_R \arrow[r, "\iota_r"] \arrow[d, "\mathrm{id}"'] & E_R \arrow[d, "\psi_r"] \\
\mathscr{A}_R \arrow[r, "\widetilde{f}_r"] & \widetilde{\mathscr{E}}_R
\end{tikzcd}$$

(129)
$$\begin{tikzcd}
A_T \arrow[r, "\iota_t"] \arrow[d, "\mathrm{id}"'] & E_T \arrow[d, "\psi_t"] \\
\mathscr{A}_T \arrow[r, "\widetilde{f}_t"] & \widetilde{\mathscr{E}}_T
\end{tikzcd}$$

The notion of *morphisms* is left to the reader to introduce.

3. Examples

As for codes without arbitration we illustrate our general concept with some examples. We first describe the “practical code” and then give its abstract form.

3.1. Johansson’s example. The scheme below is due to Johansson [**5**]. Take a fixed line L in $\mathbf{PG}(3,q)$. The points on L are regarded as the source states. The decoding rules are the points not on L, and the encoding rules are the lines not intersecting L. The messages are planes spanned by a source state and an encoding rule. When Alice and Bob want to communicate, Bob chooses a decoding rule F and hands it to the arbiter. The arbiter chooses an encoding rule e which contains F and hands e to Alice. If Alice wants to transmit a message, she chooses a source state s and sends s and the plane $\langle s, e\rangle$ to Bob. In case of a dispute, the arbiter checks if the encoding rule he gave to Alice is contained in the transmitted plane. If this is the case, he decides Alice has sent the message, otherwise he decides it was someone else. This defines a 2-fold perfect Cartesian code with $P_0 = P_1 = \frac{1}{q}$.

The abstract code

- $A_R = E_R$ consists of the points not on L;

- $\mathtt{I}$ is indexed by the points on L;
- the map α is determined by the line which the arbiter picks for a given choice of a point;
- $A_T = E_T$ consists of the lines not intersecting L;
- the τ_i take a line M of E_T to the plane spanned by point i of L and M, i.e. $\langle i, M\rangle$;
- the ρ_i associate to a given point y of E_R the set of planes intersecting L in a point i and containing y;
- X is the set of all planes not containing L.

3.2. The use of generalized dual arcs. The scheme below is due to A. Klein, J. Schillewaert and L. Storme [**6**]. We work over a finite field $\mathbb{F}_q$.

Consider the space Π_n spanned by a generalized dual arc of type $(n = n_0, \ldots, n_{l+1})$ and embed Π_n in an $(n+2)$-dimensional space Π_{n+2}. The source states are the n_1-dimensional spaces which are the elements of the generalized dual arc, the decoding rules are the points in $\Pi_{n+2}\backslash\Pi_n$, the encoding rules are the lines in Π_{n+2} which are skew to Π_n, and the encoded messages are the (n_1+2)-dimensional spaces generated by a source state and an encoding rule. We assume that Alice and Bob do not trust each other. When Alice and Bob want to communicate, Bob chooses a point x in $\Pi_{n+2}\backslash\Pi_n$ as decoding rule and sends it to the trusted arbiter. The arbiter picks one of the lines L through x skew to Π_n as encoding rule and sends it to Alice. When receiving an (n_1+2)-dimensional space Π_{n_1+2}, Bob checks if $x \in \Pi_{n_1+2}$. If this is the case he accepts the message, else he does not. The goal for an opponent Eve is thus to produce a pair (Π_{n_1}, Π_{n_1+2}) such that $x \in \Pi_{n_1+2}$.
If there is a dispute between Alice and Bob about a valid message, then the arbiter checks if the encoding rule which he handed to Alice is contained in Π_{n_1+2}. If this is the case, then he decides that Alice has sent the message, else that she has not.
If Alice wants to fool Bob, she has to produce an (n_1+2)-dimensional space containing x but not L. If Bob wants to fool Alice, he has to produce an (n_1+2)-dimensional space which contains the line L.

The number of encoding rules for the transmitter is the number of lines skew to Π_n; this is equal to $|\mathscr{E}_T| = q^{2n_0+2}$. The number of decoding rules is the number of points in $\Pi_{n+2}\backslash\Pi_n$; this is $|\mathscr{E}_R| = (q+1)q^{n_0+1}$.

If an opponent wants to cheat, he has to produce an (n_1+2)-space containing the point x. His chance to do so after having seen i pairs is $P_{O_i} = q^{n_i - n_{i-1}}$. If Alice wants to fool Bob, she has to guess which point x on L is Bob's decoding rule. Hence, she has a chance $P_T = \frac{1}{q+1}$. If Bob wants to fool Alice, he has to produce an (n_1+2)-space containing L. After seeing i pairs, this chance is equal to $q^{n_i - n_{i-1}}$.

Comparing with the lower bounds above, this scheme is perfect.

The abstract authentication code

- $A_R = E_R$ consists of the points not in Π_n;
- $\mathtt{I}$ is indexed by the elements of the arc;
- the map α is determined by the line which an arbiter picks for a given choice of a point;
- $A_T = E_T$ consists of the lines skew to Π_n;
- the maps τ_i take a line M of E to the space spanned by arc element i and M;
- the ρ_i associate to a given point y of E_R the set of (n_1+2)-dimensional spaces containing y and intersecting Π_n in the arc element i;
- X is the set of the (n_1+2)-dimensional spaces spanned by an arc element and a line skew to Π_n.

Bibliography

[1] M. De Soete. Some construction for authentication-secrecy codes, in: *Advances in Cryptology—EUROCRYPT '88* (Davos, 1988), 57–75.

[2] R. Feng and Z. Wan. A construction of Cartesian authentication codes from geometry of classical groups, *J. Combin. Inform. Syst. Sciences* **20** (1995), 197–270.

[3] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception, *Bell Syst. Techn. J.* **53** (1974), 405–424.

[4] Michael Huber. Combinatorial designs for authentication and secrecy codes, *Found. Trends Commun. Inform. Theory* **5** (2008), 581–675.

[5] T. Johansson. Contributions to unconditionally secure authentication, *Ph. D. Thesis*, Lund University, Sweden, 1994.

[6] A. Klein, J. Schillewaert and L. Storme. Generalized dual arcs and Veronesean surfaces, with applications to cryptography, *J. Combin. Theory Ser. A* **116** (2009), 684–698.

[7] A. Klein, J. Schillewaert and L. Storme. Generalized Veroneseans, submitted.

[8] S. E. Payne and J. A. Thas. *Finite Generalized Quadrangles*, Research Notes in Math. **110**, Pitman Advanced Publishing Program, Boston/London/Melbourne, 1984.

[9] D. Pei. *Authentication Codes and Combinatorial Designs*, Discrete Math. Appl., Chapman & Hall/CRC, Boca Raton, FL, 2006.

[10] J. Schillewaert and K. Thas. Authentication codes from generalized quadrangles, 12 pp., submitted.

[11] J. Schillewaert and K. Thas. *Categoric authentication*, 52 pp., submitted.

[12] G. L. Simmons. Authentication theory/coding theory, in: *Advances in Cryptology-Crypto '84*, Lecture Notes in Computer Science **196** (1985), pp. 411–431.

[13] J.A. Thas, K. Thas and H. Van Maldeghem. *Translation Generalized Quadrangles*, Series in Pure Math. **26**, World Scientific, Singapore, 2006.

[14] K. Thas. Translation generalized quadrangles for which the translation dual arises from a flock, *Glasgow Math. J.* **45** (2003), 457–474.

[15] K. Thas. *Symmetry in Finite Generalized Quadrangles*, Frontiers Math. **1**, Birkhäuser, 2004.

[16] K. Thas. A stabilizer lemma for translation generalized quadrangles, *European J. Combin.* **28** (2007), 1–16.

[17] K. Thas. Order in building theory, in: *Surveys in Combinatorics 2011*, Cambridge Univ. Press, 2011, pp. 235–331.

[18] K. Thas. *A Course on Elation Quadrangles*, Monograph, European Math. Soc., 135 pp., to appear.

[19] K. Thas. Automorphisms and cohomology of local geometries in generalized quadrangles, preprint.

[20] Z. Wan, B. Smeets and P. Vanroose. On the construction of Cartesian authentication codes over symplectic spaces, *IEEE Trans. Inform. Theory* **40** (1994), 920–929.

Index