Mathematisches Forschungsinstitut Oberwolfach

Report No. 12/2005

# Groups and Geometries

Organised by
Martin Liebeck (London)
Bernhard Mühlherr (Bruxelles)
Gernot Stroth (Halle-Wittenberg)

March 6th – March 12th, 2005

Abstract. The workshop *Groups and Geometries* was one of a series of Oberwolfach workshops which takes place every 3 years. It focused on finite simple groups, Lie-type groups and their interactions with geometry.

*Mathematics Subject Classification (2000):* 20D06, 20D08, 20G15, 20G40, 51N30, 51E12, 51E24.

## Introduction by the Organisers

The workshop *Groups and Geometries* was one of a series of Oberwolfach workshops which takes place every 3 years. It focused on finite simple groups, Lie-type groups and their interactions with geometry.

There were 47 participants and 25 talks. The themes of the latter centered around the classification of the finite simple groups and its applications, simple algebraic groups and group-theoretic applications of Moufang buildings. There were several 1-hour talks describing recent major results concerning these topics. For instance, D. Segal gave a talk about a proof of a long standing conjecture on finitely generated pro-finite groups which uses the classification. The topic of B. Martin's was the answer to a question of Serre about the notion of complete reducibility for algebraic groups. R. Weiss determined the Whitehead group for certain algebraic groups of type $E_6$ and $E_7$ as an application of his new approach to exceptional Moufang quadrangles. There had been also important contributions by young participants. For instance, by D. Bundy on the $C(G,T)$-theorem, by P.-E. Caprace on the solution of the isomorphism problem for Kac-Moody groups, by T. De Medts on rank-1 groups and by R. Gramlich on local recognition.

The conference showed that the theory of simple groups and their geometries is a very active area and that there is a lot of interaction with an increasing number of other areas. There is in particular growing impact of algebraic groups on the theory of finite groups. One of the aims of the conference was, to bring together people from these different areas, so that they can speak with each other and possibly work together on common problems. This interaction was indeed very lively and thus the meeting stands in the tradition of very successful meetings on *Groups and Geometries* at Oberwolfach.

## Workshop: Groups and Geometries

## Table of Contents

# Abstracts

## Weak Moufang conditions

Katrin Tent

Spherical buildings were invented by Tits to give a geometric interpretation of all simple algebraic groups over arbitrary fields including the exceptional ones. The canonical building associated to such a group is the simplicial complex obtained from all parabolic subgroups with reversed inclusion. The rank of the building is the same as the relative rank of the group. All spherical buildings of rank is at least 3 arise in this way. However, in the rank 2 case many other examples are known. Buildings of rank 2 are also called generalized polygons.

A generalized $n$-gon $\Gamma$ is a bipartite graph with valencies at least 3, diameter $n$ and girth $2n$. The vertices of this graph are called the *elements* of $\Gamma$. We call $(x_0, \dots x_k)$ a simple path if the $x_i$ are pairwise distinct and $x_i$ is adjacent to $x_{i+1}$ for $i = 0, \dots k-1$.

If $G \leq \mathrm{Aut}\,(\Gamma)$, we denote by $G^{[1]}_{x_0,x_1,\dots,x_k}$ the subgroup of $G$ fixing all neighbours of $x_i,\ i = 0, \dots k$ For $2 \leq k \leq n$, the generalized $n$-gon $\Gamma$ is said to be $k$-Moufang with respect to $G \leq \mathrm{Aut}\,(\Gamma)$ if for each simple $k$-path $(x_0, \dots x_k)$ the group $G^{[1]}_{x_1,\dots,x_{k-1}}$ acts transitively on the set of $2n$-cycles through $(x_0, \dots x_k)$. If $\Gamma$ is $n$-Moufang with respect to some group $G$, then we say that $\Gamma$ is a Moufang polygon. It is well-known that finite or Moufang generalized $n$-gons exist only for $n = 3, 4, 6, 8$.

The generalized $n$-gon $\Gamma$ is said to be half-Moufang with respect to $G \leq \mathrm{Aut}\,(\Gamma)$ if for each simple $n$-path $(x_0, \dots x_n)$ *of fixed type*, the group $G^{[1]}_{x_1,\dots,x_{n-1}}$ acts transitively on the set of $2n$-cycles through $(x_0, \dots x_n)$. If $G_{x_0,x_1}$ acts transitively on the set of $2n$-cycles through $(x_0, x_1)$ for all paths $(x_0, x_1)$ (sometimes referred to as the 1-Moufang condition), then $G$ acts transitively on the set of ordered $2n$-cycles. This is equivalent to $G$ having a BN-pair of rank 2, which is in general too weak to allow a classification, see examples in [13, 5]. The BN-pair is called *split* if there is a nilpotent normal subgroup $U$ in $B$ such that $B = U(B \cap N)$.

A *root elation* of $\Gamma$ is a member of $G^{[1]}_{x_1,\dots,x_{n-1}}$ for some simple path $(x_1, x_2, \dots, x_{n-1})$ of $\Gamma$. The group generated by all root elations of a Moufang polygon is called its *little projective group.* The classification of the Moufang polygons by Tits and Weiss [14] shows that Moufang polygons and higher rank buildings all arise from classical or algebraic groups. Background on the Moufang condition for generalized $n$-gons can be found in [16] and [14].

For finite simple groups, the existence of a BN-pair is sufficient to identify the group as a finite group of Lie type. For infinite groups it turns out that the assumption that the BN-pair is split is necessary for the analogous statement:

**Theorem.** [11, 12, 7] *Let $G$ be a group with a split BN-pair of rank 2 and let $\Gamma$ be the associated polygon. Then $\Gamma$ is a Moufang with respect to $G \leq Aut(\Gamma)$, and $G$ contains its little projective group.*

This result then extends to higher rank once we show that the splitting is unique [3], and we thus see that the following three concepts are equivalent:

(1) an algebraic group of relative rank $n \geq 2$,
(2) a split BN-pair of rank $n \geq 2$,
(3) a Moufang building of rank $n \geq 2$

The implication $(i) \Rightarrow (ii)$ is classical, $(ii) \Rightarrow (iii)$ is in [3], $(iii) \Rightarrow (i)$ is contained in [14], and $(iii) \Rightarrow (ii)$ is contained in [6].

However, for identifying a group as one of these groups through its action on the associated geometry, often only an apparently weaker form of the Moufang condition can be verified and hence it is very useful to know that this form is already sufficient for the classification. By [15, 17] *finite* 2-Moufang polygons are Moufang, and *finite* half-Moufang *quadrangles* are Moufang by [4]. These result do generalize to the infinite setting:

**Theorem.** [8, 9, 10] *Let $\Gamma$ be a generalized $n$-gon with $n \leq 6$. If $\Gamma$ is either 2-Moufang or half-Moufang with respect to $G$, then $n = 3, 4$ or $6$, $\Gamma$ is Moufang and $G$ contains its little projective group.*

This shows that a much weaker form of the Moufang condition is sufficient in order to identify the group.

We conjecture that any 2-Moufang generalized $n$-gon or half-Moufang polygon should in fact be a Moufang polygon. Note, however, that so far not even a bound on the possible $n$ has been established.

Examples in [1] however give a lower bound as to how much the condition might be weakened: call a generalized $n$-gon *almost 2-Moufang* with respect to $G$ if for every path $(x_0, x_1, x_2)$ and every finite subset $A \subset \Gamma_1(x_1)$ the group $G_A$ acts transitively on the $2n$-cycles containing $(x_0, x_1, x_2)$.

**Theorem.** [1] *For all $n \geq 3$, there exist almost 2-Moufang generalized $n$-gons.*

It would be nice to show that the automorphism groups of these examples are in fact simple.

## References


[1] M. Bhattacharjee, K. Tent, Amalgams of free polygons, preprint 2004.

[2] P. Fong and G. Seitz, Groups with a $(B, N)$-pair of rank 2. I, II. *Invent. Math.* **21** (1973), 1 – 57; ibid. **24** (1974), 191 – 239.

[3] F. Haot, T. de Medts, K. Tent, H. Van Maldeghem, Split BN-pairs of rank at least 2 and the uniqueness of splittings, J. Group Theory 8, No. 1, 1–10 (2005).

[4] S. Payne, J.A. Thas, H. Van Maldeghem, Half Moufang implies Moufang for finite generalized quadrangles, *Invent. Math.* **105** (1991), no. 1, 153–156.

[5] K. Tent, Very homogeneous generalized $n$-gons of finite Morley rank. *J. London Math. Soc.* (2) 62 (2000), no. 1, 1–15.

[6] K. Tent, A short proof that root groups are nilpotent, *J. Algebra* 277, No.2, 765–768 (2004).

[7] K: Tent, Split BN-pairs of rank 2: the octagons, Adv. Math. 181, No.2, 308–320 (2004).

[8] K. Tent, Half-Moufang implies Moufang for generalized quadrangles, J. Reine Angew. Math. 566, 231–236 (2004).

[9] K. Tent, Half-Moufang generalized hexagons, *Israel Journal of Mathematics* 141, 83–92 (2004).
[10] K: Tent, A weak-Moufang condition suffices, European J. Combinatorics, (2005)
[11] K. Tent, H. Van Maldeghem, On irreducible split (B,N)-pairs of rank 2, *Forum Math.* **13** (2001), 853–862.
[12] K. Tent, H. Van Maldeghem, Moufang polygons and irreducible spherical (B,N)-pairs of rank 2, I, *Adv. in Math* 174, No. 2, 254–265 (2003).
[13] J. Tits, Endliche Spiegelungsgruppen, die als Weylgruppen auftreten, *Invent. Math.* **43** (1977), 283 – 295.
[14] J. Tits and R. Weiss, *Moufang Polygons*, Springer *Monographs in Mathematics*, 2002.
[15] H. Van Maldeghem, Some consequences of a result of Brouwer, *Ars Combin.* 48 (1998), 185–190.
[16] H. Van Maldeghem, *Generalized polygons*, Birkhäuser (1998)
[17] H. Van Maldeghem, R. Weiss, On finite Moufang polygons. *Israel J. Math.* 79 (1992), no. 2-3, 321–330.

## 2F-modules, abelian sets of roots and 2-ranks

Ross Lawther

Let $G$ be a finite group, and $V$ be an absolutely irreducible faithful $\mathbb{F}G$-module over a finite field $\mathbb{F}$ of characteristic $\ell$. For a subgroup $A$ of $G$, set

$$f_1(A) = |A|.|C_V(A)|, \qquad f_2(A) = |A|^2.|C_V(A)|.$$

**Definition.** *$V$ is an* F-module *(respectively a* 2F-module*) if there exists a non-trivial elementary abelian $\ell$-subgroup $A$ such that*

$$f_1(A) \geq |V| \qquad \textit{(respectively } f_2(A) \geq |V|\textit{).}$$

F-modules arose in work of Thompson in the 1960s in the context of factorizations of groups, where they act as obstructions; it was Glauberman who subsequently gave them the name 'failure of factorization modules' (abbreviated to F-modules). 2F-modules were a later development; in particular they arose in the recent work of Aschbacher and Smith [1, 2] on quasithin groups, which finally completed the classification of finite simple groups. This required a list of possible 2F-modules for quasi-simple groups in the case $\ell = 2$; in [4, 5] Guralnick and Malle produced a list (for arbitrary $\ell$) with a small number of undecided cases. This talk described the methods by which these cases were settled.

In two of the cases the group $G$ was of Lie type with the module $V$ being over the field of definition of $G$. In each case it was possible to take a larger group $J$ over the same field with parabolic subgroup $P$ such that $G$ and $V$ could be found in the Levi subgroup and unipotent radical of $P$ respectively. Variations of a technique due to Mal'cev (described in [3]) could then be employed to convert the problem into one about the root system of $G$, which was then solved. As a consequence the following results were obtained.

**Theorem 1.** *Let $G = E_7(q)$; then the irreducible $\mathbb{F}_qG$-module of dimension 56 is not a 2F-module.*

**Theorem 2.** *Let $G = F_4(q)$ and $\ell \geq 3$; then the irreducible $\mathbb{F}_q G$-module of dimension $26 - \delta_{\ell,3}$ is a 2F-module if $\ell = 3$ and is not a 2F-module if $\ell > 3$.*

In the remaining outstanding cases, the group $G$ was sporadic; somewhat unexpectedly, it was found that a similar approach could be applied. In the first of these, $G$ was $Co_1$ and $V$ the irreducible $\mathbb{F}_2 G$-module of dimension 24 (the Leech lattice modulo 2). We took a Sylow 2-subgroup $S_1$ of $G$ with central involution $\zeta$, and found that $S_1/\langle\zeta\rangle$ and $C_V(\zeta)$ closely resembled the Sylow 2-subgroup of $D_5(2)$ and the unipotent radical of the $D_5$-parabolic subgroup of $E_6(2)$; we defined explicit 'root elements' in $S_1$ and 'root vectors' in $C_V(\zeta)$ in such a way that commutation was for the most part as predicted by the $E_6$ root system. This enabled the Mal'cev technique to be employed again; although the situation presented complications not found in the Lie type cases, we nevertheless succeeded in proving the following.

**Theorem 3.** *Let $G = Co_1$; then the irreducible $\mathbb{F}_2 G$-module of dimension 24 is not a 2F-module.*

The remaining case was similar, although the details were more involved; the result was the following.

**Theorem 4.** *Let $G = Co_2$; then the irreducible $\mathbb{F}_2 G$-module of dimension 22 is not a 2F-module.*

Finally it was observed that the insight gained in these calculations could be used to settle the last cases of unknown $p$-ranks of sporadic groups. The role of the group $J$ in the Lie type cases was played by the Monster $M$ in the $Co_1$ case, and by the Baby Monster $B$ in the $Co_2$ case; we were able to prove the following.

**Theorem 5.** *The 2-ranks of $M$, $2.B$ and $B$ are 15, 15 and 14 respectively.*

## References


[1] M. Aschbacher and S. Smith, *The Classification of Quasithin Groups: I. Structure of Strongly Quasithin $\mathcal{K}$-groups*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 2004.

[2] M. Aschbacher and S. Smith, *The Classification of Quasithin Groups: II. Main Theorems: The Classification of Simple QTKE-groups*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 2004.

[3] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Number 3*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 1994.

[4] R.M. Guralnick and G. Malle, Classification of 2F-modules, I, *J. Algebra* **257** (2002), 348–372.

[5] R.M. Guralnick and G. Malle, Classification of 2F-modules, II, in Finite Groups 2003, Proceedings of the Gainesville Conference on Finite Groups, March 6 - 12, 2003, ed. by C. Ho, P. Sin, P. Tiep, and A. Turull, de Gruyter, Berlin, New York, 2004, 117–183.

**Isomorphisms of Kac-Moody groups**

Pierre-Emmanuel Caprace
(joint work with Bernhard Mühlherr)

Kac-Moody groups are Lie-type groups attached to the Kac-Moody algebras. The latter are (infinite-dimensional) complex Lie algebras which generalize the semi-simple complex Lie algebras. Kac-Moody groups can be defined of arbitrary fields [14]; they admit both a split and a relative theory [9]. Therefore, they may be viewed as a natural (infinite-dimensional) generalization of algebraic groups. We are interested in the isomorphism problem for Kac-Moody groups. This is a classical problem for algebraic groups, and we start by recalling some historical facts.

## 1. History

One of the first results related to the isomorphism problem for algebraic groups is the following.

**Theorem 1.1.** [11] *Let $V, V'$ be finite-dimensional vector spaces over infinite fields $\mathbb{K}, \mathbb{K}'$ respectively. Let $\varphi : \mathrm{PSL}(V) \to \mathrm{PSL}(V')$ be an isomorphism. Then there exists an isomorphism $\pi : \mathbb{K} \to \mathbb{K}'$ and a $\pi$-linear isomorphism $\phi : V \to V'$ (resp. $\phi^* : V \to (V')^*$) such that $\phi \circ g = \varphi(g) \circ \phi$ or $\phi^* \circ g = \varphi(g)^\top \circ \phi^*$ holds for all $g \in \mathrm{PSL}(V)$.*

This theorem is the first of a long list of results of similar nature. Let us quote for example the work of E. Cartan and H. Freudenthal for Lie groups, J. Dieudonné for classical groups and R. Steinberg for Chevalley groups. All of these results found a definitive form in the advanced theory of A. Borel and J. Tits [1] on abstract homomorphisms between algebraic groups. In all cases, the global statement is, roughly speaking, that, up to a few exceptions for very small finite groups, two groups are isomorphic only if they are of the same type and defined over the same ground field. It is natural to ask if an analogous result holds for Kac-Moody groups.

## 2. An example

It turns out that such an analogue does hold for Kac-Moody groups, as we will see in the next section. We illustrate this here by discussing an elementary example. The easiest example of a Kac-Moody group which is attached to an infinite-dimensional Lie algebra is the group $G := \mathrm{SL}_2(\mathbb{K}[t, t^{-1}])$, where $\mathbb{K}$ is any field. This group has the special feature that is splits as an amalgamated product $G = P_1 *_B P_2$, where $P_1 := \mathrm{SL}_2(\mathbb{K}[t])$, $P_2 := \left\{ \begin{pmatrix} \mathbb{K}[t] & t\mathbb{K}[t] \\ t^{-1}\mathbb{K}[t] & \mathbb{K}[t] \end{pmatrix} \right\} \cap G$ and $B := P_1 \cap P_2$. Let $T$ be the Bass-Serre tree corresponding to that amalgam. The tree $T$ is thus equipped with an edge-transitive action of the Kac-Moody group $G$.

Let now $\mathbb{K}'$ be another field and let $G' := \mathrm{SL}_2(\mathbb{K}'[u, u^{-1}])$. Any isomorphism $\varphi : G \to G'$ induces an action of $G'$ and all of its subgroups on $T$. In particular, such an isomorphism yields an action of $\mathrm{SL}_2(\mathbb{K}')$ on the tree $T$. At this point, we appeal to the following result of Tits.

**Theorem 2.1.** [13] *Let $T$ be a simplicial tree, let $\mathbb{F}$ be a field and let $H := \mathrm{SL}_2(\mathbb{F})$ act on $T$. If $H$ fixes no vertex, no edge and no end of $T$, then the field $\mathbb{F}$ admits a discrete valuation and the associated Bruhat-Tits tree is $H$-equivariantly embedded in $T$.*

It is not difficult to compute that the stabilizer in $G$ of an end of $T$ is solvable, from which it follows that $\mathrm{SL}_2(\mathbb{K}')$ fixes no end of $T$ if $|\mathbb{K}'| \geq 4$. One can also show that $\mathrm{SL}_2(\mathbb{K})$ fixes no edge of $T$. Under the additional assumption that $\mathbb{K}$ does not admit any discrete valuation, Theorem 2.1 implies that $\mathrm{SL}_2(\mathbb{K}')$ fixes a vertex of $T$. Thus, we may assume w.l.o.g. that, up to conjugation, the isomorphism $\varphi^{-1}$ maps $\mathrm{SL}_2(\mathbb{K}')$ to a subgroup of $P_1 = \mathrm{SL}_2(\mathbb{K}[t])$. Let us now consider the evaluation morphism $\mathrm{ev}_{t=0} : \mathrm{SL}_2(\mathbb{K}[t]) \to \mathrm{SL}_2(\mathbb{K})$. An easy computation shows that the kernel of this morphism coincides with the kernel of the action of $P_1$ on the quotient $P_1/B$. Since $\mathrm{SL}_2(\mathbb{K}')$ stabilizes no edge of $T$, the restriction of the morphism $\mathrm{ev}_{t=0}$ to $\mathrm{SL}_2(\mathbb{K}')$ is nontrivial, and, moding out the centers, we obtain a monomorphism $\mathrm{PSL}_2(\mathbb{K}') \hookrightarrow \mathrm{PSL}_2(\mathbb{K})$. Finally, assuming also that $\mathbb{K}'$ does not admit a discrete valuation, we use a symmetry argument to deduce that the isomorphism $\varphi$ induces an isomorphism $\mathrm{PSL}_2(\mathbb{K}) \simeq \mathrm{PSL}_2(\mathbb{K}')$. By Theorem 1.1, this implies $\mathbb{K} \simeq \mathbb{K}'$. Thus we have established the following.

**Theorem 2.2.** *Let $\mathbb{K} \not\simeq \mathbb{K}'$ be two non-isomorphic fields which do not admit any discrete valuation. Then the groups $\mathrm{SL}_2(\mathbb{K}[t, t^{-1}])$ and $\mathrm{SL}_2(\mathbb{K}'[u, u^{-1}])$ are non-isomorphic.*

Note that finite fields, real closed, quadratically closed and algebraic closed fields do not admit any discrete valuation.

## 3. Kac-Moody groups

Following Tits [14], a (split) Kac-Moody group is defined by generators and relations, and the presentation is parametrized by a Coxeter diagram $\mathcal{D}$ with labels in $\{3, 4, 6, \infty\}$ (more accurately: a generalized Cartan matrix) and a field $\mathbb{K}$. Thus, to the ordered pair $(\mathcal{D}, \mathbb{K})$, a group $\mathcal{G}(\mathcal{D}, \mathbb{K})$ is associated. It is called the *Kac-Moody group* of type $\mathcal{D}$ over the field $\mathbb{K}$. Note that $\mathcal{G}(\mathcal{D}, \mathbb{K})$ depends functorially on the field $\mathbb{K}$. Our main result is the following.

**Theorem 3.1.** [4, 5] *Let $\mathbb{K}, \mathbb{K}'$ be algebraically closed or finite fields of cardinality at least 4. An isomorphism $\varphi : \mathcal{G}(\mathcal{D}, \mathbb{K}) \to \mathcal{G}(\mathcal{D}', \mathbb{K}')$ between Kac-Moody groups of type $\mathcal{D}$ and $\mathcal{D}'$ induces an isomorphism $(\mathcal{D}, \mathbb{K}) \simeq (\mathcal{D}', \mathbb{K}')$ of the parameter sets.*

The corresponding result for Kac-Moody algebras of symmetrizable type is a theorem of Kac and Peterson [8]. The statement above was conjectured for complex Kac-Moody groups in [7], and a few special cases were known [6, 10].

The proof of Theorem 3.1 appeals to the same kind of arguments we used in the preceding section. The key is that a Kac-Moody group $\mathcal{G}(\mathcal{D}, \mathbb{K})$ acts strongly transitively on a (twin) building $\Delta(\mathcal{D},\mathbb{K})$ of type $\mathcal{D}$. For the Kac-Moody group $\mathcal{G}(\tilde{A}_1,\mathbb{K}) = \mathrm{SL}_2(\mathbb{K}[t,t^{-1}])$, (a half of) this building is the Bass-Serre tree we considered above.

Let us now give a rough sketch of the proof of Theorem 3.1 in the case of algebraically closed fields $\mathbb{K}$ and $\mathbb{K}'$. Tits' presentation of the Kac-Moody group $G := \mathcal{G}(\mathcal{D},\mathbb{K})$ highlights a distinguished subgroup $H < G$ such that $H \simeq (\mathbb{K}^\times)^n$ for some $n \in \mathbb{N}$. The group $W := N_G(H)/H$ is a Coxeter group of type $\mathcal{D}$. It is called the *Weyl group* of $G$. By analogy with the classical theory, it is natural to call $H$ a *maximal torus* of $G$. However, this definition of a torus is not intrinsic and depends of the definition of $G$ by a certain presentation. For our purposes, it is useful to consider also the following subgroup. Let $p > 3$ be a prime distinct from $\mathrm{char}(\mathbb{K})$ and let $H_p$ be the $p$-torsion subgroup of $H$. The following result says that $H_p$ is a good substitute for a maximal torus in $G$: it shares important properties of $H$, and its definition is intrinsic.

**Proposition 3.2.** *The group $H_p$ is a maximal elementary abelian $p$-subgroup of $G$. Any two such subgroups are conjugate in $G$.*

One of the key ingredients in the proof of that proposition is the fixed point theorem for finite groups acting on buildings. Since $N_G(H) = N_G(H_p)$ and (in the generic case) $Z(C_G(H_p)) = H$, we deduce from Proposition 3.2 that an isomorphism between two Kac-Moody groups over algebraically closed fields induces an isomorphism between their Weyl groups.

The next step in the proof consists in considering the corank one subgroups of $H_p$. Given a well chosen corank one subgroup $H_p^1 < H_p$, one shows that $Fix_{\Delta(\mathcal{D},\mathbb{K})}(H_p^1)$ has a canonical structure of a simplicial tree, on which the group $C_G(H_p^1)$ acts. The latter is a group of Kac-Moody type, and the arguments of the preceding section can be applied in this context. A typical situation is that $C_G(H_p^1) = \mathrm{SL}_2(\mathbb{K}[t,t^{-1}])$, which allows to appeal directly to Theorem 2.2.

We remark that our arguments also show that unipotents elements of $\mathcal{G}(\mathcal{D},\mathbb{K})$ are mapped by $\varphi$ to unipotent elements of $\mathcal{G}(\mathcal{D}',\mathbb{K}')$. From this, one deduces a splitting result for automorphisms of a Kac-Moody group [4, 5], which is an analogue of Steinberg's theorem on automorphisms of Chevalley groups [12].

## 4. Compact forms of Kac-Moody groups

We end by mentioning another result related to the isomorphism problem of Kac-Moody groups. It concerns the so-called *compact forms* (or *unitary forms*) of the complex split Kac-Moody groups (see [7] for the precise definition). Any split Kac-Moody group $G := \mathcal{G}(\mathcal{D},\mathbb{C})$ over $\mathbb{C}$ admits an anistropic involution $\omega$ and the *compact form* of $G$ is $K(\mathcal{D}) := G^\omega$. If $\mathcal{D}$ is a diagram of finite type, the group $K(\mathcal{D})$ is just a compact semi-simple Lie group, and any compact semi-simple Lie group arises in this way. The solution of the isomorphism problem for compact Lie groups is well known and similar to the results of Section 1. However, the situation is slightly different in the Kac-Moody case.

**Theorem 4.1.** [3] *An isomorphism $\varphi : K(\mathcal{D}) \to K(\mathcal{D}')$ between compact forms induces a reflection-preserving isomorphism between their Weyl groups. Furthermore, if the diagrams $\mathcal{D}$ and $\mathcal{D}'$ are twist-equivalent, then there exists a (discontinuous) isomorphism $K(\mathcal{D}) \to K(\mathcal{D}')$.*

The notion of *twist-equivalence* was introduced in [2] in the context of the isomorphism problem for Coxeter and Artin groups. It is proved in [2] that two twist-equivalent diagrams yield isomorphic Coxeter and Artin groups. This is also true for compact forms of Kac-Moody groups, and the preceding theorem shows that the rigidity of $K(\mathcal{D})$ is controlled by the (reflection-)rigidity of its Weyl group.

## References

[1] A. Borel and J. Tits. Homomorphismes "abstraits" de groupes algébriques simples. *Ann. Math.* **97**, pages 499–571, 1973.
[2] N. Brady, J. McCammond, B. Mühlherr, and W. Neumann. Rigidity of Coxeter groups and Artin groups. In *Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part I (Haifa, 2000)*, pages 91–109. Geom. Dedicata **94**, 2002.
[3] P.-E. Caprace. PhD Thesis. In preparation.
[4] P.-E. Caprace and B. Mühlherr. Isomorphisms of Kac-Moody groups. *Invent. Math.* (to appear).
[5] P.-E. Caprace and B. Mühlherr. On isomorphisms between Kac-Moody groups which preserve bounded subgroups. Preprint (submitted).
[6] R. W. Carter and Y. Chen. Automorphisms of affine Kac-Moody groups and related Chevalley groups over rings. *J. Algebra* **155**, pages 44–94, 1993.
[7] V. G. Kac and D. H. Peterson. On geometric invariant theory for infinite-dimensional groups. *Springer Lecture Notes in Mathematics* **1271**, pages 109–142, 1987.
[8] D. Peterson and V. Kac. Infinite flag varieties and conjugacy theorems. *Proc. Nat. Acad. Sci. U.S.A.* **80**, pages 1778–1782, 1983.
[9] B. Rémy. Groupes de Kac-Moody déployés et presque déployés. *Astérisque* **277**, 2002.
[10] B. Rémy. Immeubles de Kac-Moody hyperboliques, groupes non isomorphes de même immeuble. *Geom. Dedicata* **90**, pages 29–44, 2002.
[11] O. Schreier and B.L. van der Waerden. Die Automorphismen der projektiven Gruppen. *Abh. Math. Sem. Hamburg* **6**, (303–322), 1928.
[12] R. Steinberg. Lectures on Chevalley groups. Yale University, 1968.
[13] J. Tits. A "theorem of Lie-Kolchin" for trees. *Contributions to Algebra*, pages 377–388, 1977. A collection of papers dedicated to Ellis Kolchin.
[14] J. Tits. Uniqueness and presentation of Kac-Moody groups over fields. *J. Algebra* **105**, pages 542–573, 1987.

# Identifications of Lie-type groups

Franz G. Timmesfeld

Let $\mathcal{B}$ be an irreducible spherical Moufang building of rank $\ell \geq 2$, $\mathcal{A}$ an apartment of $\mathcal{B}$ and $\Phi$ the 'extended' root-system corresponding to $\mathcal{A}$ (i.e. $\Phi$ might be of type $BC_\ell$, when $\mathcal{B}$ is of type $C_\ell$). Let $A_r, r \in \Phi$, be the root-subgroup corresponding to $r$. Then we call the following subgroup of Aut$(\mathcal{B})$:

$$G := \langle A_r \mid r \in \Phi\rangle\text{-the Lie-type group of } \mathcal{B}.$$

We fix the following notation:

(a) $X_r := \langle A_r, A_{-r}\rangle$ is a 'rank one group', i.e. satisfies: If $a \in A_r^{\#}$ then there exists a $b \in A_{-r}$ with $A_r^b = A_{-r}^a$ (and vice versa).
(b) $U := \langle A_r \mid r \in \Phi^+\rangle$ is the unipotent subgroup corresponding to $\Phi^+$.
(c) $B := N_G(U) = G_c$, $c \in \mathcal{A}$ where $c$ is the chamber fixed by $U$.

Suppose $\mathcal{B}$ is no octogon. Then, if $r, s \in \Phi$ with $s \neq -r, -2r$ and $r \neq -2s$ we have:

(d) $[A_r, A_s] \leq \langle A_{\lambda r+\mu s} \mid \lambda, \mu \in \mathbb{N} \text{ with } \lambda r + \mu s \in \Phi\rangle$.

If now $\pi = \widehat{G} \to G$ is a perfect central extension of $G$, then we say $\widehat{G}$ is of type $\mathcal{B}$ (resp. $\Phi$) if there exist coimages $\widehat{A}_r$ of the $A_r$, satisfying (a) and (d). Then:

**Theorem 1.** *(Steinberg-type-presentation) Suppose the group $\overline{G}$ is generated by subgroups $\overline{A}_r, r \in \Phi$ satisfying (a) and (d). Let*

$$\Psi = \{r \in \Phi \mid 2r \notin \Phi\} \cup \{s \in \Phi \mid 2s \in \Phi \text{ and } \overline{A}_s \neq \overline{A}_{2s}\}.$$

*Then $\Psi = \dot\cup \Psi_i$ such that the following hold:*

(i) *Either $\Psi_i$ 'carries' the structure of an irreducible spherical root system or $\Psi_i = \{\pm r\}$ resp. $\Psi_i = \{\pm r, \pm 2r\}$.*
(ii) *$\overline{G}$ is the central product of subgroups*

$$\overline{G}(\Psi_i) := \langle \overline{A}_r \mid r \in \Psi_i\rangle,$$

*which are either of type $\Psi_i$, or $\overline{G}(\Psi_i) = \overline{X}_r = \langle \overline{A}_r, \overline{A}_{-r}\rangle$.*

The proof of this theorem is over a series of papers [M], [O], [Ti1], $\cdots$, [Ti5], where the $\Phi = G_2$ case is done in [M] and [O], while in [Ti2] it is shown that $\overline{G}$ is already of type $\mathcal{B}$, if in addition:

(e) $\overline{A}_r^{\overline{n}_s} = \overline{A}_{r^{w_s}}$ for all $r, s \in \Phi$, where $w_s$ is the reflection along $s$ on $\Phi$ and $\overline{n}_s \in \overline{X}_s$ interchanging $\overline{A}_s$ and $\overline{A}_{-s}$.

holds. This identification theorem is used to identify the $\overline{G}(\Psi_i)$.

Let in the following $G \leq \widetilde{G} \leq \mathrm{Aut}\,(\mathcal{B})$, $\widetilde{B} = \widetilde{G}_c$, $\widetilde{H}$ the pointwise stabilizer of $\mathcal{A}$ in $\widetilde{G}$, and $\Pi = \{r_1, \cdots, r_\ell\}$ a fundamental system and $\widetilde{P}_i, i = 1, \cdots, \ell$ the minimal parabolic subgroups of $\widetilde{G}$ containing $\widetilde{B}$. Then $\widetilde{P}_i = \langle \widetilde{B}, n_i\rangle$, where $n_i \in X_{r_i}$ interchanging $A_{r_i}$ and $A_{-r_i}$. We want to discuss, what can be said about a group $\overline{G}$ generated by subgroups $\overline{P}_i, i = 1, \cdots, r$ satisfying:

(i) There exist surjective homomorphisms $\sigma_i : \overline{P}_i, \to \widetilde{P}_i$ that $\sigma_i^{-1}(\widetilde{B}) = \sigma_j^{-1}(\widetilde{B}) =: \overline{B}$ for $1 \leq i, j \leq \ell$ and $\sigma_i|_{\overline{B}} = \sigma_j|_{\overline{B}} =: \sigma$.
(ii) There exists a normal subgroup $\overline{U}$ of $\overline{B}$, such that $\sigma|_{\overline{U}} : \overline{U} \to U$ is an isomorphism.

**Theorem 2.** *Suppose $\overline{G}$ satisfies (i), (ii) and*

(iii) *$o(\overline{n}_i\overline{n}_j) \mod \overline{H} \leq o(n_i n_j) \mod \widetilde{H}$ for $1 \leq i \neq j \leq \ell$, where $\overline{H} = \sigma^{-1}(\widetilde{H})$ and $\overline{n}_i \in \sigma_i^{-1}(n_i)$.*

*Then $\langle \overline{U}^{\overline{G}}\rangle$ is of type $\mathcal{B}$. ($\mathcal{B}$ the building we started with).*

Theorem 2 is a consequence of the identification theorem [Ti2]. It generalizes a Theorem of Tits [Se, Ch. II, Th. 8], which was slightly generalized by Bennett and Shpectorov [B.S], which in case $\ell = 2$ determines $G$ as universal closure of the amalgam of $P_1, P_2$ and $N$. ($N$ the global stabilizer of $\mathcal{A}$ in $G$.)

## References


[B.S.] C. D. Bennett and S. Shpectorov. A remark on a theorem of Tits. *Proc. of the AMS* **129** (2001), 2571–2579.

[M] C. Müller. *Gruppen mit Wurzelsystem vom Typ $G_2$*. Dissertation, Univ. Bielefeld, 2004.

[O] H. Oueslati, *Gruppen vom Typ $G_2$ und ${}^2F_4$*. Dissertation, Univ. Gießen. In Preparation.

[S] J.-P. Serre. *Trees*. Springer-Verlag, 1980.

[Ti1] F. G. Timmesfeld. A remark on presentations of certain Chevalley groups. *Arch. Math.* **79**, (2002), 404–407.

[Ti2] F. G. Timmesfeld. On the Steinberg-Presentation for Lie-type groups. *Forum Math.* **15**, (2003), 645–663.

[Ti3] F. G. Timmesfeld. A classification of Weyl groups as finite $\{3,4\}$-transposition groups. *Proc. of the conference on finite groups*, Gainsville (2003).

[Ti4] F. G. Timmesfeld. Groups with root system of type $B_\ell$, $C_\ell$ and $F_4$. *J. Algebra* **284** (2005), 737–754.

[Ti5] F. G. Timmesfeld. The Steinberg-Type Presentation for Lie-Type Groups. Preprint.


## Finite groups with small automorphism groups

Robert A. Wilson
(joint work with John Bray)

If $G$ is a group of order $n$, what can we say about the order of its automorphism group $\mathrm{Aut}\,(G)$? The largest values of $|\mathrm{Aut}\,(G)|$ relative to $|G|$ are obtained when $G$ is an elementary abelian 2-group, but the smallest values are not so obvious. In the case when $G$ is abelian it is easy to see that $|\mathrm{Aut}\,(G)| \geq \phi(n)$ with equality if and only if $G$ is cyclic. It is therefore tempting to suggest, as was done in Problem 15.43 of the Kourovka Notebook [2], that this should hold for arbitrary finite groups $G$.

In joint work with John Bray, we have shown that neither part of the statement holds for arbitrary finite groups [1]. Specifically, we have constructed examples of finite groups $G$ with $|\mathrm{Aut}\,(G)| < \phi(|G|)$, and examples of non-cyclic finite groups $G$ with $|\mathrm{Aut}\,(G)| = \phi(|G|)$. Indeed, given any $\varepsilon > 0$ we showed how to find a finite group $G$ with $|\mathrm{Aut}\,(G)| < \varepsilon.\phi(|G|)$.

We have now extended and simplified these results, in particular showing that the two parts of the statement are false even for soluble groups. The smallest counterexample we have found for the second part is now $G = 3 \times 7_+^{1+2}{:}2{\cdot}S_4^-$, of order $n = 2^4.3^2.7^3$. For then $\mathrm{Aut}\,(G) = 2 \times 7^2{:}(3 \times 2{\cdot}S_4^-)$, of order $2^5.3^2.7^2 = \phi(n)$. For the first part we take a direct product of groups of shape $p^{1+2}{:}2S_4^-$ as $p$ ranges over a set of primes congruent to $\pm 1$ modulo 8. Since each of these factors is characteristic, with centre of order $p$ and outer automorphism group cyclic of order $(p-1)/2$, it follows that $|\mathrm{Aut}\,(G)|/\phi(|G|)$ is $3/2^k$, where $k$ is the number of factors.

A similar argument using factors of the form $p^{1+2}{:}2A_5$, for primes $p$ congruent to $\pm 1$ modulo 10, shows that the second part of the statement fails to hold for perfect groups. For the first part, we can take a group of shape

$$3^6{:}M_{11} \times 5^{1+2}{:}SL_2(5) \times 11^{1+2}{:}SL_2(11) \times 19^{1+2}{:}SL_2(5),$$

which has centre of order 3.5.11.19 and outer automorphism group of order 2.4.10.9. Then $|\mathrm{Aut}\,(G)|/|G| = 2^4.3/11.19$ while $\phi(|G|)/|G| = \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{10}{11}\cdot\frac{18}{19} = 2^4.3/11.19$ also.

A long-standing conjecture for $p$-groups, that if $G$ is non-cyclic of order at least $p^3$ then $|G|$ is a divisor of $|\mathrm{Aut}\,(G)|$ (see [3]), would however imply that the statement holds for nilpotent groups. This seems to be a hard problem. The statement may even hold for supersoluble groups: so far, we have been unable to find a counterexample.

## References


[1] J. N. Bray and R. A. Wilson. On the orders of automorphism groups of finite groups. *Bull. London Math. Soc.*, to appear.

[2] E. I. Khukhro and V. D. Mazurov (Eds). Unsolved problems in group theory. The Kourovka Notebook, no. 15. Novosibirsk, 2002.

[3] E. Schenkman. The existence of outer automorphisms of some nilpotent groups of class 2. *Proc. Amer. Math. Soc.* **6** (1955), 6–11.


# Buildings of rank one according to Tits

Hendrik Van Maldeghem

## Abstract

In 1997, Jacques Tits explained in his lectures at the Collège de France an approach to buildings of rank one. In the present note, we slightly generalize his ideas. We will then treat the rank one buildings of Suzuki-Tits type.

## 1. Introduction

Technically, a building of rank one is just a set, endowed with all pairs of elements (which form the set of apartments). However, the buildings of rank one arising from higher rank (spherical or Moufang) buildings have a richer structure, induced by the larger rank building they are sitting in. As a standard example we mention the projective line over a field $k$, where every ordered quadruple gives a unique field elements (the cross-ratio), uniquely determined by the action of the group $\mathrm{PSL}_2(k)$ on the line. The presence and action of the unipotent subgroups allows one to speak here about a *Moufang line*. More generally, we will define a Moufang line as a split BN-pair of rank one. Every algebraic group of relative rank one gives rise to a Moufang line, but those with root groups of nilpotency class two also give rise to an additional geometric structure on that Moufang line, according to Tits [2]. Tits then asked whether this additional structure is enough to recover the algebraic group. More precisely, is the automorphism group of this geometric structure inside the automorphism group of the corresponding algebraic group? Tits himself answered positively to that question for some classes of algebraic groups (${}^2\mathrm{A}_2$, $\mathrm{E}_8$). In the present paper we introduce a slightly more general notion of Moufang building of rank one, and we answer Tits' question in the case of general Suzuki groups.

## 2. Definitions

Let $X$ be a set, and let, for each $x \in X$, there be a group $U_x$ acting on $X$, fixing $x$. Then we say that $(X, (U_x)_{x\in X})$ is a *Moufang line* (for terminology, see Buekenhout [1]), if

(ML1) for every $x \in X$, $U_x$ acts sharply transitively on $X \setminus \{x\}$, and
(ML2) the set $\{U_x \mid x \in X\}$ is normalized by the group $G^\dagger := \langle U_x \mid x \in X\rangle$.

The group $G^\dagger$ is usually referred to as the *little projective group.* If $G^\dagger$ is sharply 2-transitive, then we say that the Moufang line is *improper*; otherwise it is *proper.*

Now, for some $x \in X$, let $V_x \neq U_x$ be a nontrivial subgroup of $U_x$ such that $V_x$ is a normal subgroup of $G^\dagger_x$. We can then define $V_y$, $y \in X$ as the conjugate of $V_x$ by an arbitrary element $g \in G^\dagger$ with $x^g = y$. Since $V_x \trianglelefteq G^\dagger_x$, this is well defined. The *Moufang building of rank one defined on $X$ by $(U_x)_{x\in X}$ relative to $(V_x)_{x\in X}$* is the geometry $(X, \Lambda)$, where $\Lambda$ is a distinguished set of subsets of $X$ obtained as follows: for each pair $x, y \in X$, the set $\{x\} \cup \{y^v \mid v \in V_x\}$ belongs to $\Lambda$.

We are especially interested in Moufang buildings of rank one defined on proper Moufang lines. Defining an automorphism of $(X, \Lambda)$ as a permutation of $X$ inducing a permutation of $\Lambda$, a fundamental question now is

(★) Is $\mathrm{Aut}(X, \Lambda) \leq \mathrm{Aut}(G^\dagger)$ ?

A positive answer means that the study of the rank one Moufang building is equivalent with the study of the corresponding group.

## 3. Suzuki-Tits buildings of rank one and the Main Result

The following description is based on Section 7.6 of [3]. Let $k$ be a field with characteristic 2, and suppose that $k$ admits a *Tits endomorphism* $\theta : x \mapsto x^\theta$; hence $(x^\theta)^\theta = x^2$ (but we do not necessarily have that $x^2$ is surjective). Let $k^\theta$ denote the image of $k$ under $\theta$. Let $L$ be a vector space over $k^\theta$ contained in $k$, such that $k^\theta \subseteq L$ and such that $L \setminus \{0\}$ is closed under taking multiplicative inverses. We also assume that $L$ generates $k$ as a ring. We now define the *Suzuki-Tits Moufang line* as follows.

Let $X$ be the following set of points of $\mathrm{PG}(3, k)$, given with coordinates with respect to some given basis:

$$\begin{aligned} X &= \{k(1,0,0,0)\} \cup \{k(a^{2+\theta} + aa' + a'^\theta, 1, a', a) \mid a, a' \in L\}, \\ &= \{k(0,1,0,0)\} \cup \{k(1, a^{2+\theta} + aa' + a'^\theta, a, a') \mid a, a' \in L\}. \end{aligned}$$

We set $\infty = k(1,0,0,0)$ and $O = k(0,1,0,0)$. Let $(x,x')_\infty$ be the collineation of $\mathrm{PG}(3,k)$ determined by

$$k(x_0\ x_1\ x_2\ x_3) \mapsto k(x_0\ x_1\ x_2\ x_3)\begin{pmatrix} 1 & 0 & 0 & 0 \\ x^{2+\theta}+xx'+x'^{\theta} & 1 & x' & x \\ x & 0 & 1 & 0 \\ x^{1+\theta}+x' & 0 & x^{\theta} & 1 \end{pmatrix},$$

and let $(x,x')_O$ be the collineation of $\mathrm{PG}(3,k)$ determined by

$$k(x_0\ x_1\ x_2\ x_3) \mapsto k(x_0\ x_1\ x_2\ x_3)\begin{pmatrix} 1 & x^{2+\theta}+xx'+x'^{\theta} & x & x' \\ 0 & 1 & 0 & 0 \\ 0 & x^{1+\theta}+x' & 1 & x^{\theta} \\ 0 & x & 0 & 1 \end{pmatrix}.$$

Define the groups

$$U_\infty = \{(x,x')_\infty \mid x,x' \in L\} \text{ and } U_O = \{(x,x')_O \mid x,x' \in L\}.$$

Both groups $U_\infty$ and $U_O$ act on $X$, as an easy computation shows (for $U_0$ use the second description of $X$ above), and they act sharply transitively on $X \setminus \{k(1,0,0,0)\}$ and $X \setminus \{k(0,1,0,0)\}$, respectively. Moreover, one can check that $(U_O)^{(x,x')_\infty} = (U_\infty)^{(y,y')_O}$, with

$$y = \frac{x'}{x^{2+\theta}+xx'+x'^{\theta}} \text{ and } y' = \frac{x}{x^{2+\theta}+xx'+x'^{\theta}}.$$

It follows easily that we obtain a Moufang line, which we call a *Suzuki-Tits Moufang line.* The group $\mathrm{Sz}(k,L,\theta)$ is the (simple) *Suzuki group* generated by $U_\infty$ and $U_O$.

Now define $V_\infty = \{(0,x')_\infty \mid x' \in L\}$, then $V_\infty = [U_\infty, U_\infty] = Z(U_\infty)$. Hence $V_\infty$ is normal in $\mathrm{Sz}(k,L,\theta)_\infty$ and we obtain a Moufang building $(X,\Lambda)$ of rank one, which we call a *Suzuki-Tits Moufang building of rank one.*

In the finite case $k = L$, $|k| = 2^{2e+1}$, and $(X,\Lambda)$ is the inversive plane corresponding to the Suzuki group $\mathrm{Sz}(2^{2e+1})$.

**Main result.** *Let* $(X,\Lambda)$ *be the Suzuki-Tits Moufang building of rank one corresponding to* $\mathrm{Sz}(k,L,\theta)$*, with* $|k| > 2$*. Then* $\mathrm{Aut}(X,\Lambda)$ *is generated by* $\mathrm{Sz}(k,L,\theta)$*, by the permutations* $m_\ell$*,* $\ell \in L$ *with the property that* $\ell L = L$*, with*

$$m_\ell : X \to X : k(x_0,x_1,x_2,x_3) \mapsto k(\ell^{2+\theta}x_0, x_1, \ell^{1+\theta}x_2, \ell x_3),$$

*and by the permutations* $m_\sigma$*,* $\sigma \in \mathrm{Aut}(k)$ *with* $\sigma\theta = \theta\sigma$ *and*

$$m_\sigma : X \to X : k(x_0,x_1,x_2,x_3) \mapsto k(x_0^\sigma, x_1^\sigma, x_2^\sigma, x_3^\sigma).$$

## References


[1] F. Buekenhout, Foundations of one dimensional projective geometry based on perspectivities, *Abhandlungen Math. Sem. Univ. Hamburg* **43** (1975), 21 – 29.

[2] J. Tits, *Résumé de cours (Annuaire du Collège de France,* $97^e$ année, 1996-1997, pp. 89 – 102.

[3] H. Van Maldeghem, *Generalized Polygons*, Birkhauser Verlag, Basel, Boston, Berlin, *Monographs in Mathematics* **93**, 1998.

## A link between Moufang sets and Jordan division algebras

Tom De Medts
(joint work with Richard M. Weiss)

In his famous Lecture Notes [11], Jacques Tits showed that the only (irreducible) spherical buildings of rank $\ell \geq 3$ are those arising (via the notion of a BN-pair) from simple algebraic groups, classical groups and groups of "mixed type." Spherical buildings of rank 2 (a.k.a. generalized polygons) are too numerous to classify, but if the Moufang condition is imposed, it is again possible to show that the only examples are those arising from simple algebraic groups, classical groups and groups of mixed type [12]. Buildings of rank 1 are merely sets with no additional structure at all. The buildings of rank 1 which are associated with simple algebraic groups, classical groups and (the known) groups of mixed type, however, do come equipped with the additional structure of a split BN-pair. Some of this additional structure is captured in the notion of Moufang set (due to Tits). An essentially (but not completely) equivalent notion is the notion of an (abstract) rank one group, as introduced by Franz Timmesfeld [10].

Our results grew out of an effort to find a simple existence criterion for Moufang sets, in the same spirit of the one which exists for Moufang polygons [12, (8.13)]. The solution we have found seems to be quite natural and should serve, we hope, as a basis for future work on Moufang sets.

On the other hand, it was already clear from the known examples of Moufang sets that there is a connection between Jordan (division) algebras and Moufang sets, but the deeper reason for this was not understood. The question to make this link more explicit was, to our knowledge, first posed by Bernhard Mühlherr (see also [8]), and recently, such a connection was made visible by Rafael Knop [5], but in a very indirect way, using the Tits-Kantor-Koecher graded Lie-algebra. The method that we have found is, we believe, much more elementary, and illustrates the naturalness of our criterion.

A *Moufang set* is a set $X$ together with a set of subgroups $\{U_x \mid x \in X\}$ of $\mathrm{Sym}(X)$ such that for all $x \in X$, the subgroup $U_x$ acts regularly on $X \backslash \{x\}$ (and therefore fixes $x$) and $(U_x)^\varphi = U_{\varphi(x)}$ for all $\varphi \in G^\dagger$, where $G^\dagger$ denotes the subgroup of $\mathrm{Sym}(X)$ generated by all the subgroups $U_x$; the subgroups $U_x$ are called the *root groups* of the Moufang set, and the group $G^\dagger$ is called its *little projective group.*

Let $U$ be a group with composition $\boxplus$ and identity 0. (The operation $\boxplus$ is not necessarily commutative.) The inverse of an element $a$ will be denoted by $\boxminus a$. Let $X := U \cup \{\infty\}$, where $\infty$ is a new symbol. For each $a \in U$, we denote by $\alpha_a$ the permutation of $X$ which fixes $\infty$ and maps $x$ to $x \boxplus a$ for all $x \in U$. We extend the operation $\boxplus$ by setting $x \boxplus \infty = \infty \boxplus x = \infty$ for all $x \in U$; $\infty \boxplus \infty$ is undefined. Let $U_\infty = \{\alpha_a \mid a \in U\} \cong U$.

Now suppose that $\tau$ is a permutation of $U^*$. We extend $\tau$ to an element of $\mathrm{Sym}(X)$ (which we also denote by $\tau$) by setting $0^\tau = \infty$ and $\infty^\tau = 0$. Next we set $U_0 = U_\infty^\tau$ and $U_a = U_0^{\alpha_a}$ for all $a \in U$. Let $\mathbb{M}(U, \tau) = (X, (U_x)_{x \in X})$ and let

$G^\dagger = \langle U_\infty, U_0 \rangle$. Our first goal is to give a criterion which determines when $\mathbb{M}(U,\tau)$ is a Moufang set. (It is clear that every Moufang set arises in this way.)

**Theorem 1.** *$\mathbb{M}(U,\tau)$ is a Moufang set if and only if the "Hua maps"*

$$h_a : x \mapsto \tau\Big(\tau^{-1}\big(\tau(x)\boxplus a\big)\boxminus\tau^{-1}(a)\Big)\boxminus\tau\big(\boxminus\tau^{-1}(a)\big)$$

*are additive (w.r.t. $\boxplus$) for each $a \in U^*$.*

The group $H := \langle h_a \mid a \in U^* \rangle$ will be called the Hua group of the Moufang set. It turns out that this group coincides with the diagonal subgroup [10, (1.1)]:

**Theorem 2.** *$H = \mathrm{Stab}_{G^\dagger}\{0,\infty\}$.*

**Example 1.** *Let $K$ be an arbitrary field or skew field, let $U := (K,+)$, and let $\tau : K^* \to K^* : x \mapsto -x^{-1}$. Then $\mathbb{M}(U,\tau)$ is a Moufang set; its Hua maps are given by $h_a : x \mapsto axa$ for all $a, x \in U$. This Moufang set is denoted by $\mathbb{M}(K)$. (Geometrically, this is the projective line over $K$; the group $G^\dagger$ is isomorphic to $\mathsf{PSL}_2(K)$.)*

**Example 2.** *Let $G$ be a group acting sharply two-transitively on a set $X$. Then $(X, (\mathrm{Stab}_G\{x\})_{x\in X})$ is a Moufang set (with $G = G^\dagger$). All its Hua maps are trivial. In fact, for a given Moufang set, $H = 1$ if and only if $G^\dagger$ is sharply two-transitive.*

The following example shows that every Jordan division algebra gives rise to a Moufang set, in a very natural way:

**Example 3.** *Let $(J, U, 1)$ be a quadratic Jordan division algebra over some commutative field $k$ (of arbitrary characteristic), as introduced by McCrimmon [6] —see also [7]— and let $\tau : J^* \to J^* : x \mapsto -x^{-1} = -U_x^{-1}(x)$. Then $\mathbb{M}((J,+),\tau)$ is a Moufang set; its Hua maps are given by $h_a : x \mapsto U_a(x)$ for all $a, x \in J$. This Moufang set is denoted by $\mathbb{M}(J, U, 1)$.*

**Example 4.** *Let $\mathcal{O}$ be an octonion division algebra over some commutative field $k$ (of arbitrary characteristic), let $U := \{(x,y) \in \mathcal{O}\times\mathcal{O} \mid \mathrm{Nrd}(x) + \mathrm{Trd}(y) = 0\}$ be the (non-abelian) group with composition $(a,b)\boxplus(c,d) = (a+c, b+d-\overline{c}a)$. Let $\tau : U^* \to U^* : (x,y) \mapsto (-xy^{-1}, y^{-1})$. Then $\mathbb{M}(U,\tau)$ is a Moufang set corresponding to an algebraic group of type $F_4$ of $k$-rank one; see [1].*

Franz Timmesfeld introduced the important notion of *special* rank one groups [10, (1.1)]. In our setting, a Moufang set $\mathbb{M}(U,\tau)$ is special if and only if $\tau(\boxminus x) = \boxminus\tau(x)$ for all $x \in U$.

**Conjecture 1.** *Let $\mathbb{M} = \mathbb{M}(U,\tau)$ be a Moufang set such that $G^\dagger$ does* not *act sharply two-transitively on $X$. Then $\mathbb{M}$ is special if and only if $U$ is abelian.*

(This is a double conjecture: both the "if" part and the "only if" part are not known to be true, but to our knowledge, no counterexamples are known.)

**Conjecture 2.** *Let $\mathbb{M} = \mathbb{M}(U,\tau)$ be a special Moufang set with $U$ abelian. Then there exists a quadratic Jordan division algebra $(J, U, 1)$ over some commutative field $k$ such that $\mathbb{M} \cong \mathbb{M}(J, U, 1)$.*

A positive answer to both conjectures would imply a classification of all Moufang sets with abelian root groups, since the sharply two-transitive groups with abelian stabilizers are classified by Kerby and Wefelscheid [4]; see also [3].

We cannot answer this question in its full generality, but under some additional natural "degree" assumptions, we could obtain the required result:

**Theorem 3.** *Let $\mathbb{M} = \mathbb{M}(U, \tau)$ be a special Moufang set with identity element $e$, such that*

- *$U$ is a finite-dimensional vector space over a (commutative) field $k$ with $|k| > 3$ ;*
- *the Hua maps $h_a$ are $k$-linear for all $a \in U^*$ ;*
- *the map $h : x \mapsto h_x$ from $U$ to $\mathrm{End}_k(U)$ is $k$-quadratic (i.e. $h_{tx} = t^2 h_x$ for all $t \in K$ and $x \in U$, and $h_{x,y} := h_{x+y} - h_x - h_y$ is $k$-bilinear for all $x, y \in U$) .*

*Then $(U, h, e)$ is a quadratic Jordan division algebra over $k$, and $\tau(x) = -x^{-1}$ for all $x \in U^*$ .*

Finally, we have applied our criterion to give a characterization of the Moufang sets associated with the groups $\mathsf{PSL}_2(k)$ over commutative fields $k$ of characteristic different from 2.

**Theorem 4.** *Suppose that $\mathbb{M} = \mathbb{M}(U, \tau)$ is a special Moufang set, where $U$ is an abelian group, but not an elementary abelian 2-group. Assume, moreover, that the Hua group $H$ is abelian. Then there exists a commutative field $k$ with $\mathrm{char}(k) \neq 2$ such that $\mathbb{M} \cong \mathbb{M}(k)$.*

## References


[1] T. De Medts and H. Van Maldeghem, *Moufang sets of type $F_4$*, in preparation.

[2] T. De Medts and Richard M. Weiss, *Moufang sets and Jordan division algebras*, submitted.

[3] Gy. Károlyi, S.J. Kovács and P.P. Pálfy, *Doubly transitive permutation groups with abelian stabilizers*, Aequationes Math. **39** (1990), no. 2-3, 161–166.

[4] W. Kerby and H. Wefelscheid, *Conditions of finiteness on sharply 2-transitive groups*, Aequationes Math. **8** (1972), 287–290.

[5] R. Knop, *Die Geometrie der Moufang-Mengen*, Ph.D. Thesis, to appear in 2005.

[6] K. McCrimmon, *A general theory of Jordan rings*, Proc. Nat. Acad. Sci. U.S.A. **56** (1966), 1072–1079.

[7] K. McCrimmon, *A Taste of Jordan Algebras*, Springer-Verlag, Berlin, Heidelberg, New York, 2004.

[8] B. Mühlherr and H. Van Maldeghem, *Moufang sets from groups of mixed type*, submitted.

[9] T.A. Springer, *Jordan algebras and algebraic groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete **75**, Springer-Verlag, Berlin, Heidelberg, New York, 1973.

[10] F. Timmesfeld, *Abstract Root Subgroups and Simple Groups of Lie-Type*, Birkhäuser-Verlag, Monographs in Mathematics **95**, Basel, Berlin, Boston, 2001.

[11] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Lecture Notes in Mathematics **386**, Springer-Verlag, New York, Heidelberg, Berlin, 1974.

[12] J. Tits and R. M. Weiss, *Moufang Polygons*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York, 2002.

## A Geometric Approach to Complete Reducibility

Ben Martin

(joint work with Michael Bate, Gerhard Röhrle, Martin Liebeck and Aner Shalev)

### 1. $G$-completely reducible subgroups

Let $G$ be a connected reductive algebraic group over an algebraically closed field $k$. Most of the results discussed below are true but uninteresting in characteristic zero, so we assume that $\mathrm{char}(k) = p > 0$. By a subgroup of $G$ we mean a closed subgroup.

Consider the problem of studying conjugacy classes of maximal subgroups of $G$. It is often useful to look at subgroups satisfying extra conditions: for example, it is a classical result from representation theory that if $F$ is a finite group then the number of conjugacy classes of completely reducible subgroups of $GL_n(k)$ that are isomorphic to $F$ is finite. Serre generalised the notion of complete reducibility to arbitrary $G$ [11], [12].

**Definition.** *A subgroup $H$ of $G$ is $G$-*completely reducible *if whenever $H$ lies in a parabolic subgroup of $G$, $H$ lies in some Levi subgroup of that parabolic subgroup.*

A subgroup of $GL_n(k)$ is $GL_n(k)$-completely reducible if and only it is completely reducible in the usual sense of representation theory.

Many people have studied $G$-cr subgroups of a reductive group $G$ [4], [5], [9], [10], [11], [12], and [13]. In this talk I describe a new approach to $G$-complete reducibility using geometric invariant theory and ideas from the theory of character varieties. A key part is played by the notion of a *canonical destabilising parabolic subgroup*. In the last part of the talk, I discuss some applications of these methods to finite groups of Lie type.

We begin with a generalisation of the representation-theoretic result given above. Let $r$ denote the rank of $G$.

**Theorem 1.1.** *Let $F$ be a finite group. There exist only a finite number — call this $n(F,G)$ — of conjugacy classes of $G$-cr subgroups of $G$ that are isomorphic to $F$. Moreover, for any positive integer $B$, the sum $\sum_{|F|\leq B} n(G,F)$ is bounded by a function $f(B,r)$ which depends only on $B$ and $r$, not on $k$.*

The final assertion is proved in [3, Prop. 2.1]. The speaker proved the first part [6, Thm. 2], replacing $G$-cr subgroups with "strongly reductive" subgroups of $G$ (as defined below), building on ideas of Vinberg, who proved the result in characteristic zero [15]. The result for $G$-cr subgroups now follows from Theorem 2.1 below.

### 2. Strongly reductive subgroups of $G$

Our geometric approach is inspired by work of R.W. Richardson. He studied the action of $G$ by simultaneous conjugation on the Cartesian product $G^m$, where

$m$ is a positive integer:

$$g \cdot (g_1, \ldots, g_m) := (gg_1g^{-1}, \ldots, gg_mg^{-1}).$$

**Definition.** *Let $H \leq G$ and suppose that $H$ is topologically generated by elements $h_1, \ldots, h_m \in G$ for some $m$. We say $H$ is* strongly reductive *in $G$ if the orbit $G \cdot (h_1, \ldots, h_m)$ is a closed subset of $G^m$.*

This is not Richardson's original definition [8, Def. 16.1] but it is equivalent to it [8, Thm. 16.4]; as a corollary of this, the definition above does not depend on the choice of topological generators $h_i$. For simplicity, we assume below that all subgroups of $G$ under consideration are topologically finitely generated.

Here is the main result Theorem 3.1 of [1], which allows us to apply geometric methods to the problem of studying $G$-cr subgroups.

**Theorem 2.1.** *A subgroup of $G$ is $G$-completely reducible if and only if it is strongly reductive in $G$.*

## 3. Canonical destabilising parabolic subgroups

If $H = \overline{\langle h_1, \ldots, h_m \rangle}$ is a non-$G$-cr subgroup of $G$ then $H$ is not strongly reductive by Theorem 2.1, so $G \cdot (h_1, \ldots, h_m)$ is not closed. The Hilbert-Mumford-Kempf Theorem [2, Thm. 3.4] from geometric invariant theory asserts the existence of a canonical one-parameter subgroup $\lambda$ of $G$ such that $(h_1', \ldots, h_m') := \lim_{x \to 0} \lambda(x) \cdot (h_1, \ldots, h_m)$ exists and $G \cdot (h_1', \ldots, h_m')$ is closed. This leads to the following result (cf. [7] and the proofs of [3, Prop. 2.2] and [1, Thm. 5.8]).

**Principle 3.1.** *If $H$ is a non-$G$-cr subgroup of $G$ then there exists a canonical parabolic subgroup $P$ of $G$ such that $P \supseteq H$ but no Levi subgroup of $P$ contains $H$.*

Since $H$ is not $G$-cr, we know by definition that there exists at least one parabolic subgroup $P$ with $H$ contained in $P$ but not in any Levi subgroup of $P$; the point of the principle is that there is a choice of $P$ that is canonical in an appropriate sense (which we do not define here). Now we give two applications of this principle. The first, which answers a question of Serre [11, p. 24], is the starting point of Gerhard Röhrle's talk in this meeting.

**Theorem 3.2.** *(*[1, Thm. 3.10]*) Let $N \trianglelefteq H \leq G$. If $H$ is $G$-cr then $N$ is $G$-cr.*

*Proof.* If $N$ is not $G$-cr then there exists a canonical $P$ as in Principle 3.1 which contains $N$. As $H$ normalises $N$ and $P$ is canonical, $H$ normalises $P$. Parabolic subgroups of $G$ are self-normalising, so $H \leq P$, and $H$ does not lie in any Levi subgroup of $P$ because $N$ does not. Thus $H$ is not $G$-cr. □

Now assume $G$ is simple and adjoint and $\sigma \colon G \to G$ is a Frobenius map. The fixed point subgroup $G_\sigma$ is a finite group of Lie type.

**Theorem 3.3.** *(Cf.* [3, Prop. 2.2]*) Let $M \leq G_\sigma$. Then $M$ is $G$-cr or $M$ lies in a proper $\sigma$-stable parabolic subgroup of $G$.*

*Proof.* If $M$ is not $G$-cr then there exists a canonical $P$ as in Principle 3.1 which contains $M$. As $M$ is $\sigma$-stable and $P$ is canonical, $P$ is $\sigma$-stable; moreover, $P$ is proper because no Levi subgroup of $P$ contains $M$. □

## 4. Finite groups of Lie type

Let $\mathcal{M}(F)$ denote the set of conjugacy classes of a finite group $F$. The following result has applications to probabilistic generation. For example, if $x, y \in F$ fail to generate $F$ then $x, y$ lie in a common maximal subgroup of $F$. To show that the probability that a randomly chosen pair of elements generates $F$ is large, one needs to control the number of maximal subgroups.

**Theorem 4.1.** *(*[3, Thm. 1.3]*) There exists a function $c(r)$ and a constant $d$ such that if $F$ is an almost simple finite group with socle of Lie type of rank $r$ over the finite field $\mathbb{F}_q$ then*

$$|\mathcal{M}(F)| < c(r) + dr \log\log q.$$

The proof uses information about maximal subgroups of finite simple groups which has been built up over the years. Our geometric methods deal with the following case. Take $F = G_\sigma$ for simplicity and assume $G$ is of exceptional type. Known results dispose of a large class of maximal subgroups, including subgroups contained in a proper $\sigma$-stable parabolic; their contribution to $|\mathcal{M}(F)|$ is bounded by the $dr \log\log q$ term. The remaining subgroups are $G$-cr, by Theorem 3.3, and their orders are bounded by an absolute constant $B$. Theorem 1.1, together with Lang's Theorem, shows that the number of conjugacy classes of such subgroups does not exceed $f(B, r)$, and the required bound follows.

## References


[1] M. Bate, B.M.S. Martin, G. Röhrle, *A geometric approach to complete reducibility*, Invent. Math., to appear.

[2] G.R. Kempf, *Instability in invariant theory*, Ann. Math. **108** (1978), 299–316.

[3] M.W. Liebeck, B.M.S. Martin, A. Shalev, *On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function*, Duke Math. J., to appear.

[4] M.W. Liebeck, G.M. Seitz, *Variations on a theme of Steinberg*, Special issue celebrating the 80th birthday of Robert Steinberg. J. Algebra **260** (2003), no. 1, 261–297.

[5] M.W. Liebeck, D.M. Testerman, *Irreducible subgroups of algebraic groups*, Q. J. Math. **55** (2004), 47–55.

[6] B.M.S. Martin, *Reductive subgroups of reductive groups in nonzero characteristic*, J. Algebra **262**, (2003), no. 2, 265–286.

[7] B.M.S. Martin, *A normal subgroup of a strongly reductive subgroup is strongly reductive*, J. Algebra **265**, (2003), no. 2, 669–674.

[8] R.W. Richardson *Conjugacy classes of $n$-tuples in Lie algebras and algebraic groups*, Duke Math. J. **57**, (1988), no. 1, 1–35.

[9] G.M. Seitz, *Abstract homomorphisms of algebraic groups*, J. London Math. Soc. (2) **56** (1997), no. 1, 104–124.

[10] J.-P. Serre, *La notion de complète réductibilité dans les immeubles sphériques et les groupes réductifs*, Séminaire au Collège de France, résumé dans [14, pp. 93–98], (1997).

[11] J.-P. Serre, *The notion of complete reducibility in group theory*, Moursund Lectures, Part II, University of Oregon, 1998, `http://darkwing.uoregon.edu/~math/serre/index.html`

[12] J.-P. Serre, *Complète réductibilité*, Séminaire Bourbaki, 56ème année, 2003-2004, n° 932.

[13] P. Slodowy, *Two notes on a finiteness problem in the representation theory of finite groups*, Austral. Math. Soc. Lect. Ser., **9**, Algebraic groups and Lie groups, 331–348, Cambridge Univ. Press, Cambridge, 1997.
[14] J. Tits, *Théorie des groupes*, Résumé des Cours et Travaux, Annuaire du Collège de France, 97e année, (1996–1997), 89–102.
[15] E.B. Vinberg, *On invariants of a set of matrices*, J. Lie Theory **6** (1996), 249–269.

## Permutation groups and Quantum Computing

Aner Shalev
(joint work with J. Kempe and L. Pyber)

### 1. Introduction

In the framework of Quantum Computing, combining computer science with the principles of quantum mechanics, one can solve problems not known to be efficiently solvable classicaly (see [8] for general backgound). The most celebrated examples include factoring large numbers [9], and carried out by solving the so called Hidden Subgroup Problem (HSP) for abelian groups via Quantum Fourier Sampling (QFS). A main challenge in Quantum Computing is solving the Hidden Subgroup Problem for nonabelian groups, and most importantly for the symmetric group $S_n$, as this would (quantumly) solve the prominent graph isomorphism problem and related questions. See [4, 3] for partial results.

In the works [6] with Kempe, and [7] with Kempe and Pyber, we employ concepts and tools from the theory of finite permutation groups in order to analyse the Hidden Subgroup Problem via Quantum Fourier Sampling for the symmetric group. Our results are negative, showing that both the so called weak and the random-strong form of QFS have no advantage whatsoever over classical exhaustive search.

It is intriguing that the classical concept of *minimal degree* of a permutation group, studied since the days of Jordan 130 years ago [5], plays a key role in our proof. However, we also employ various modern tools, including the Classification of Finite Simple Groups.

### 2. Preliminaries and notation

We first describe the Hidden Subgroup Problem. Fix a finite group $G$ and let $H \leq G$ be an unknown subgroup. Given a function $f : G \to S$ that is constant on (left)-cosets $gH$ of $H$ and takes different values for different cosets, we have to find the subgroup $H$. The decision version of this problem is to determine whether the hidden subgroup $H$ is the identity subgroup or not. Enumerating over all elements $g \in G$ and checking whether $f(g) = f(1)$ (namely whether $g \in H$) would result in listing all the elements of $H$. However, we are interested in polynomial time algorithms, which give the answer (or a highly probable answer) in $(\log |G|)^c$ steps.

The standard quantum solution of this problem (for abelian groups $G$ and certain other groups) involves performing the Quantum Fourier Transform (QFT) over $G$, resulting in the so called Fourier basis of the complex group algebra $\mathbb{C}[G]$.

Let $Irr(G)$ denote all irreducible complex characters of $G$. Each subgroup $H \leq G$ induces a probability measure $P_H$ on $Irr(G)$ given by $P_H(\chi) = \frac{\chi(1)}{|G|} \sum_{h \in H} \chi(h)$. To solve HSP this way we need to infer $H$ from the resulting distribution. Distinguishing the trivial subgroup $\{1\}$ from a larger subgroup $H$ efficiently using the so called weak (or random-strong) standard method is possible if and only if the $L_1$ distance $D_H$ between $P_{\{1\}}$ and $P_H$ is larger than some inverse polynomial in $\log |G|$. Here

$$D_H = \frac{1}{|G|} \sum_{\chi} \chi(1) \Big| \sum_{h \in H, h \neq e} \chi(h) \Big|.$$

We therefore say that $H$ is *distinguishable* if $D_H \geq (\log |G|)^{-c}$ for some constant $c$, and is *indistinguishable* otherwise.

The *minimal degree* $m(H)$ of a permutation group $H \leq S_n$ is defined to be the minimal number of points moved by a non-identity element of $H$.

## 3. Main Results

Our first result (from [6]) provides character-free bounds on the distance $D_H$, and serves as a basic tool for our investigations.

**Theorem 3.1.** *Let $C_1, \ldots, C_k$ denote the non-identity conjugacy classes of $G$. Then*

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H \leq \sum_{i=1}^{k} |C_i \cap H| |C_i|^{-\frac{1}{2}}.$$

Applying this we show in [6] that for $H \leq S_n$ of polynomial size ($\leq n^c$), $H$ is distinguishable if and only if its minimal degree $m(H)$ is bounded. Thus we cannot distinguish a group generated by a cycle of unbounded length, or an involution with non-constant number of transpositions, implying negative results from [4, 3] in the case $|H| = 2$.

Our next result concerns primitive permutation groups, which are the building blocks of finite permutation groups in general. Let $H \leq S_n$ be primitive and $H \neq A_n, S_n$. Then we have $m(H) \geq (\sqrt{n} - 1)/2$ by [1], and $|H| \leq 2n^{\sqrt{n}}$ by [2] (and CFSG). Using this and other ingredients, we obtain the following somewhat surprising result [6]:

**Theorem 3.2.** *Let $H \neq A_n, S_n$ be a primitive subgroup of $S_n$. Then $H$ is indistinguishable.*

Our most general result, from [7], deals with arbitrary permutation groups. By a painstaking enumeration of elements of given support in a permutation group of given minimal degree we are able to deduce the following.

**Theorem 3.3.** *Let $H \leq S_n$ be any permutation group. Suppose $H$ is distinguishable. Then its minimal degree $m(H)$ is bounded.*

Thus every distinguishable subgroup must contain a non-identity element of bounded support. Since there are only polynomially many such elements in $S_n$ we can just exhaustively query them, thereby distingushing $H$ from $\{1\}$.

**Corollary 3.4.** *Any subgroup $H \leq S_n$ which can be distinguished from $\{1\}$ using the above quantum method can already be distinquished from $\{1\}$ using classical exhaustive search.*

## References

[1] L. Babai, On the order of uniprimitive permutation groups, *Annals of Math.* **113**, pp. 553-568, 1981
[2] P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13**, pp. 1-22, 1981.
[3] M. Grigni, L. Schulman, M. Vazirani and U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, *Proc. 33th STOC*, pp. 68-74, 2001.
[4] S. Hallgren, A. Russell and A. Ta-Shma, Normal subgroup reconstruction and quantum computation using group representations, *Proc. 32nd STOC*, pp. 627-635, 2000.
[5] C. Jordan, Sur la limite de degré des groupes primitifs qui contiennent une substitution donnée, *J. reine angew Math.* **79**, pp. 248-258, 1875.
[6] J. Kempe and A. Shalev, The hidden subgroup problem and permutation group theory, *Proc. 16th ACM SODA*, ACM, 2005.
[7] J. Kempe, L. Pyber and A. Shalev, Permutation groups, minimal degrees and Quantum Computing, in preparation.
[8] A.Y. Kitaev, A.H. Shen and M.N. Vyalyi, *Classical and Quantum Computation*, AMS Graduate Series in Mathematics **47**, Providence, RI, 2002.
[9] P.W. Shor, Algorithms for Quantum Computation: Discrete Log and Factoring, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, ed: S. Goldwasser, 1994.

# Pure quaternions, ultra-products and valuations

Yoav Segev
(joint work with A. Rapinchuk and L. Rowen)

## Introduction

We give here a short account of the joint work [4] together with A. Rapinchuk and L. Rowen. The work in [4], as well as the earlier work [3], are related to the analysis of the Whitehead group $W(G, k)$ of an absolutely simple simply connected algebraic $k$-group $G$ of type ${}^{3,6}D_4$ having $k$-rank 1 (see Tits's Bourbaki talk [5] for the relevant terminology). We divide our account into the following short parts:

(1) Motivation.
(2) An explicit description of the Whitehead group.
(3) Outline of the construction of $\mathcal{D}$: using ultarproducts.
(4) Constructing valuations on non-commutative algebras of rational functions.

## 1. Motivation

Let us recall the definition of the Whitehead group: let $G$ be an absolutely almost simple simply connected algebraic group defined over an infinite field $k$. The subgroup $G(k)^+$ of $G(k)$ is the subgroup generated by the $k$-rational points of the unipotent radicals of $k$-defined parabolic subgroups of $G$. The quotient $W(G,k) = G(k)/G(k)^+$ was termed the Whitehead group by J. Tits in [5]. The *Kneser-Tits problem* (or conjecture) is to determine whether or not $W(G,k) = 1$, and more generally to determine the structure of $W(G,k)$.

Let $G$ be of type ${}^{3,6}D_4$ defined over $k$ and of $k$-rank 1. We are interested in the structure of $W(G,k)$ in this case. In [3] it was shown that when $\mathrm{char}(k)$ is odd, $W(G,k)$ is abelian-by-nilpotent-by-abelian. This was achieved by obtaining results on normal subgroups of the multiplicative group of a quaternion division algebra generated by a pure quaternion (see below). Here we show that this approach may not work in characteristic zero by giving an example of a quaternion division algebra $\mathcal{D}$ and a pure quaternion $\mathfrak{e} \in \mathcal{D}$ such that $\mathcal{D}^\times/\langle \mathfrak{e}^{\mathcal{D}^\times}\rangle$ is not solvable.

## 2. An explicit description of the Whitehead group

¿From now on the letter $D$ (and also $\mathcal{D}$) will always denote a quaternion division algebra of characteristic $\neq 2$. The letter $K$ will denote the center of $D$.

Given $G$ as above of $k$-rank 1 and of type ${}^{3,6}D_4$, the following is an explicit description of $W(G,k)$. There exists $D$ with center $K$ such that $K/k$ is a separable cubic extension and such that the corestriction of $D$ to $k$ is trivial. Let

$$V = \{d \in D^\times \mid \mathrm{Nrd}(d) \in k\} \ \text{ and } \ U = \{d \in D^\times \mid \mathrm{Nrd}(d), \mathrm{Trd}(d) \in k\}.$$

(Here Nrd and Trd are the reduced norm and trace.) Then

$$W(G,k) = V/\langle U\rangle.$$

Since the corestriction of $D$ to $k$ is trivial, there is a basis $1, e, f, ef$ of $D$ over $K$ such that $e^2 \in k$, $f^2 \in K$, $N_{K/k}(f^2) = 1$ and $ef = -fe$ (cf. (43.9) in [2]). Notice that the element $e$ is in $U$, because $\mathrm{Nrd}(e) = -e^2 \in k$ and $\mathrm{Trd}(e) = 0$. We will return to this fact in the next section. We call any non-central element $v \in D$ such that $v^2 \in K$ a *pure quaternion.*

## 3. The subgroup $S$ and outline of the construction of $\mathcal{D}$.

Both in the odd characteristic case (i.e. when $\mathrm{char}(D)$ is odd) and in the zero characteristic case ($\mathrm{char}(D) = 0$) a crucial role is played by the subgroup

$$S = K^\times\langle 1 + 2\mathrm{SL}_1(D)\rangle.$$

(recall what $\mathrm{SL}_1(D)$ is the subgroup of $D^\times$ consisting of elements having reduced norm 1.)

In the odd characteristic case ([3]) we showed that $D^\times/S$ is nilpotent-by-abelian, then we showed that this implies that for *any* pure quaternion $e \in D$, $D^\times/\langle e^{D^\times}\rangle$ is abelian-by-nilpotent-by-abelian. Since, as noted above, $U$ above contains a pure quaternion, this enabled us to prove that the Whitehead group is abelian-by-nilpotent-by-abelian, in the odd characteristic case.

Here we construct $D$ of characteristic zero such that $D^\times/S$ is not solvable and we show:

(i) If $D^\times/S$ is not solvable, then for all $\mathbb{Z} \ni i \geq 0$, there exists a pure quaternion $e(i) \in D$ such that $D/\langle e(i)^{D^\times}\rangle$ is not solvable of derived length $\leq i$.

(ii) We let $\mathcal{F}$ be an ultrafilter on $I = \mathbb{Z}^{>0}$ containing the cofinite filter and we show that the ultraproduct

$$\mathcal{D} = (\prod_{i\in I} D_i)/\mathcal{F} \quad D_i = D \;\forall i,$$

is a quaternion division algebra such that the element $\mathfrak{e} := (e(i))$ is pure and satisfies $\mathcal{D}^\times/\langle \mathfrak{e}^{\mathcal{D}^\times}\rangle$ is not solvable.

For the proof of (i) we let $D^\bullet := D^\times/S$ and $\bullet\colon D^\times \to D^\bullet$ be the canonical homomorphism. We first show that $[\langle e^{D^\times}\rangle^\bullet, \mathrm{SL}_1(K(e))^\bullet] = 1^\bullet$, *for any pure quaternion* $e \in D$. This fact together with a short argument yields (i).

## 4. Constructing valuations on non-commutative algebras of rational functions

We construct $D$ of characteristic zero having a non-archimedean valuation $\tilde{w}$ such that the residue algebra $\bar{D}_{\tilde{w}}$ has characteristic two and is not commutative. A short argument then shows that $D^\times/S$ is not solvable (notation as in §3 ) completing the construction of $\mathcal{D}$.

Let $v$ be the 2-adic valuation on $\mathbb{Q}$ and extend $v$ to the field of rational functions $F := Q(y)$ by setting $w(a/b) = w(a) - w(b)$, where for a polynomial $a[y] = a_0 + a_1 y + \cdots + a_n y^n$ we let

$$w(a) = \min_{a_i\neq 0} v(a_i).$$

This is a standard construction, cf. [1, Section 10.1, Proposition 2]. Let $\sigma \in \mathrm{Aut}\,(F)$ be the unique automorphism taking $y$ to $y^{-1}$ and let $R := F[x,\sigma]$ be the ring of skew-polynomials. Then the center of $R$ is $R_0 = F^\sigma[x^2]$, where $F^\sigma$ is the fixed subfield of $\sigma$. Let $D := F(x,\sigma)$ be the localization of $R$ at $R_0 \setminus \{0\}$. Then $D$ is a quaternion division algebra whose center is the field of fractions of $R_0$. We define a map $\tilde{w}\colon D^\times \to \mathbb{Z}$ by $\tilde{w}(ab^{-1}) = \tilde{w}(a) - \tilde{w}(b)$ ($a \in R$ and $b \in R_0 \setminus \{0\}$) where for a polynomial $a \in R$, we define as above $\tilde{w}(a) = \min_{a_i\neq 0} w(a_i)$. It turns out that $\tilde{w}$ is a valuation on $D$ such that $\bar{D}_{\tilde{w}}$ is of characteristic 2 and is not commutative.

### References


[1] N. Bourbaki, *Commutative algebra, chapters 1–7,* translated from French. Herman, Paris; Addison-Wesley Publishing Co. 1972.

[2] M-A. Knus, A.S. Merkurev, M. Rost, J-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.

[3] G. Prasad, L. Rowen, Y. Segev, *Normal subgroups of quaternion algebras and the Whitehead group of algebraic groups of type* ${}^{3,6}D_4$, preprint 2004.
[4] A. Rapinchuk, L. Rowen, Y. Segev, *A quaternion division algebra having a nonsolvable quotient group modulo a pure quaternion*, preprint 2005.
[5] J. Tits, *Groupes de Whitehead de groupes algébriques simples sur un corps (d'aprés V. P. Platonov at al.), Séminaire Bourbaki, 29e année (1976/7), Exp. No. 505, pp. 218-236.*

## Meager finite simple groups

Ron Solomon
(joint work with Daniel Gorenstein, Richard Lyons and Kay Magaard)

This is a progress report on a certain portion of the second generation proof of the Classification of the Finite Simple Groups: Theorem $\mathcal{C}_6^+$, the classification of meager finite simple groups. This is collaborative research with Daniel Gorenstein, Richard Lyons and Kay Magaard. I shall also take this opportunity to describe the post-QT modifications to the GLS (Gorenstein, Lyons, Solomon) classification strategy laid out in [3]. In order to do this, quite a few definitions will be necessary.

For each prime $p$, let $\mathcal{K}_p$ denote the set of all isomorphism classes of (known) quasisimple groups $K$ with $Z(K)$ a $p$-group (possibly trivial). The GLS strategy relies fundamentally on the partitions

$$\mathcal{K}_p = \mathcal{C}_p \cup \mathcal{T}_p \cup \mathcal{G}_p.$$

Here $\mathcal{C}_p$ contains all simple groups of Lie type in characteristic $p$ and all simple alternating groups of degree $p$, $2p$, and $3p$. Other members of $\mathcal{C}_p$ are "small" and/or sporadic.

**Definition.** *A finite simple group $G$ is said to be of* **even type** *if the following conditions hold:*

- $m_2(G) \geq 3$;
- $O_{2'}(C_G(t)) = 1$ *for all* $t \in G$ *with* $t^2 = 1$; *and*
- *If $t$ is an involution of $G$ and $L$ is a component of $C_G(t)$, then $L$ is isomorphic to a member of $\mathcal{C}_2$.*

Typically, a group of even type is a simple group of Lie type defined over a field of even order. However, also many of the sporadic simple groups are of even type. Meager groups are by definition of even type, and so we shall henceforth assume that $p$ is odd.

Now

$$\mathcal{T}_p \geq \{K \in \mathcal{K}_p - \mathcal{C}_p : m_p(K) = 1\},$$

with equality if $p > 5$. If $p = 5$, we add $Fi_{22}$, while if $p = 3$ we add $L_3(q)$ and $U_3(q)$ for $q$ not a power of 3, as well as

$$\{A_7, 3A_7, M_{12}, M_{22}, 3M_{22}, J_2\}.$$

For groups of even type, an important role is played by the parameter $e(G)$ introduced by Thompson in [6].

**Definition.** *For $p$ an odd prime, the 2-local $p$-rank of $G$, $m_{2,p}(G)$, is the maximum $p$-rank of a 2-local subgroup of $G$; and $e(G)$ is the maximum value achieved by $m_{2.p}(G)$.*

**Definition.** *A finite simple group $G$ is of* **quasithin even type** *if $G$ is of even type and $e(G) \leq 2$.*

Groups of quasithin even type have recently been classified by Aschbacher and Smith [2].

**Definition.** *A finite simple group $G$ is of* **sporadic even type** *if $G$ is of even type with $e(G) \geq 3$, and there exists an odd prime $p$ such that $m_{2,p}(G) \geq max\{e(G), 4\}$ and for every $x \in G$ of order $p$, every component $K$ of $C_G(x)/O_{p'}(C_G(x))$ lies in $\mathcal{C}_p$.*

We remark that most sporadic simple groups are of quasithin or sporadic even type. Moreover only finitely many simple groups $G$ are of sporadic even type.

**Definition.** *A finite simple group $G$ is of* **generic even type** *if $G$ is of even type and there exists an odd prime $p$ such that $m_p(G) \geq 4$ and for some $x \in G$ of order $p$ with $m_p(C_G(x)) \geq 4$, there exists a component $K$ of $C_G(x)/O_{p'}(C_G(x))$ with $K \in \mathcal{G}_p$.*

We remark that if $G$ is a simple group of Lie type defined over a field of even order and having a torus of $p$-rank at least 4 for some odd prime $p$, then, with a small number of exceptions, $G$ is of generic even type. A first major step towards the classification of groups of generic even (and odd) type was taken in [4].

Finally we reach our goal.

**Definition.** *A finite simple group $G$ is of* **meager even type** *if $G$ is of even type, but $G$ is neither of quasithin even type nor of sporadic even type nor of generic even type.*

**Theorem $\mathcal{C}_6^+$.** *Let $G$ be a finite simple group all of whose proper simple sections are known. Suppose that $G$ is of meager even type. Then $G \cong L_4(2^n)$ ($n > 1$), $Sp_6(2^n)$ ($n > 1$), $\Omega_8^-(2^n)$, $L_6(2)$, or $L_7(2)$.*

In [3], the corresponding Theorem $\mathcal{C}_6$ had an empty set of conclusions. The reason for this is that GLS expected a stronger Quasithin Theorem (Theorem $\mathcal{C}_4$) to be proved, classifying all finite simple groups of even type with $e(G) \leq 3$. However GLS now intend to quote the Quasithin Theorem (for groups of even type) of Aschbacher and Smith [2] as the key Theorem $\mathcal{C}_4^-$. This necessitates that both Theorem $\mathcal{C}_5$ and Theorem $\mathcal{C}_6$ must be replaced by stronger Theorems $\mathcal{C}_5^+$ and $\mathcal{C}_6^+$ to cover the case $e(G) = 3$.

The new Theorem $\mathcal{C}_5^+$ is the following statement.

**Theorem $\mathcal{C}_5^+$.** *Let $G$ be a finite simple group all of whose proper simple sections are of known type. Suppose that $G$ is of sporadic even type. Then either $G$ is isomorphic to a member of the set:*

$$\{A_{12}, P\Omega_7(3), P\Omega_8^{\pm}(3), Sp_8(2), \Omega_8^+(2), \Omega_{10}^-(2), U_5(2), U_6(2), U_7(2), F_4(2), {}^2E_6(2)\}$$

*or $G$ has the same centralizer of involution pattern as some member of the set:*

$$\{Suz, Co_1, Co_2, Co_3, Fi_{22}, Fi_{23}, Fi'_{24}, F_5, F_3, F_2, F_1\}.$$

This theorem is a work-in-progress with Gorenstein, Korchagina, and Lyons. See Lyons' article [5] in this volume for further details.

We conclude with a brief discussion of the proof of Theorem $\mathcal{C}_6^+$. The strategy for the proof of this theorem is to study the centralizers of non-identity elements in a maximal elementary abelian $p$-subgroup $A$ of $G$ for a suitable odd prime $p$. The goal is to prove that these centralizers are of reductive type, i.e. that the components of $C_G(x)/O_{p'}(C_G(x))$ pull back to quasisimple components of $C_G(x)$ for all $x \in A$. With this information together with a bit of information about $p$-fusion in $A$, we can arrive at a presentation for $G$ of Curtis-Tits-Phan type.

The principal methodology for proving that the centralizers are of reductive type is the Signalizer Functor Method. In view of the Glauberman-McBride Signalizer Functor Theorem and Strong $p$-Uniqueness Theorems provided by Stroth, it will suffice to establish the existence of suitable $A$-signalizer functors. Our first line of attack is to attempt to use one of the $k+\frac{1}{2}$-balanced signalizer functors introduced by Aschbacher, Gorenstein and Lyons. One consequence of the meager hypothesis is that there is no local obstruction to $\frac{5}{2}$-balance. Hence we are done if $m_p(G) \geq 4$.

The remaining case is when $m_p(G) = 3$ and there is a local obstruction to $\frac{3}{2}$-balance. The principal example of such a local obstruction is afforded by an element $x \in A$ such that $C_G(x)$ has a $p$-component $L$ with $L/O_{p'}(L) \in \mathcal{T}_p$ and $m_p(L) = 2$. Hence $p \in \{3, 5\}$. Using other signalizer functors and related methods, we hope to reduce to the case where $p = 3$, $O_{3'}(L)$ is a 2-group and

$$L/Z_3^*(L) \in \{L_3(q), U_3(q), A_7, M_{12}, M_{22}, J_2\}.$$

At this point we expect to use pushing up arguments combined with a version of the Thompson Transitivity Theorem to complete the proof.

We remark that a large portion of this problem was treated earlier by Aschbacher under the hypotheses that $G$ is of characteristic 2-type and $e(G) = 3$ [1]. We draw inspiration for our work from his papers.

## References


[1] M. Aschbacher, *Finite groups of rank* 3. *I,II*, Invent. Math. **63** (1981), 357–402; Invent. Math. **71** (1983), 51–163.

[2] M. Aschbacher and S. D. Smith, The Classification of Quasithin Groups. I,II, A. M. S. Surveys and Monographs **111,112**, 2004.

[3] D. Gorenstein, R. Lyons and R. Solomon, The Classification of the Finite Simple Groups, A. M. S. Surveys and Monographs **40** #1, 1995.

[4] D. Gorenstein, R. Lyons and R. Solomon, The Classification of the Finite Simple Groups, A. M. S. Surveys and Monographs **40** #5, 2002.
[5] R. Lyons, *Bicharacteristic finite simple groups*, Oberwolfach Reports (this conference).
[6] J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable. I*, Bull. A. M. S. **74** (1968), 383–437.

## Which profinite groups are generated by finitely many random elements with positive probability?

László Pyber
(joint work with A. Jaikin-Zapirain)

By a classical result of Dixon [Di] two randomly chosen elements generate $\mathrm{Alt}(n)$ with probability $\to 1$ as $n \to \infty$.

Results of similar flavour were obtained for various classes of profinite groups. Recall that a profinite group $G$ is called positively finitely generated (PFG) if for some $r$ a random $r$-tuple generates $G$ with positive probability.

There are various examples of PFG groups related to Dixon's theorem, such as inverse limits of iterated wreath products of alternating groups [Bh] and infinite products of pairwise non-isomorphic finite simple groups [KL], [LSh].

On the other hand, finitely generated prosoluble groups were shown to have this property and more generally finitely generated profinite groups which do not have arbitrarily large alternating sections [BPSh].

Denote by $m_n(G)$ the number of index $n$ maximal subgroups of $G$. A group $G$ is said to have polynomial maximal subgroup growth (PMSG) if $m_n(G) \leq n^c$ for all $n$ (for some constant $c$).

A one-line argument shows that PMSG groups are positively finitely generated. By a very surprising result of Mann and Shalev the converse also holds.

**Theorem** ([MSh])**.** *A profinite group is PFG exactly if it has polynomial maximal subgroup growth.*

This result gives a characterisation of PFG groups. However, it does not make it any easier to prove that the above mentioned examples of profinite groups are PFG.

We give a characterisation which achieves this i.e. one which really describes which groups are PFG.

Let $L$ be a finite group with a non-abelian unique minimal normal subgroup $M$. A crown-based power $L_k$ of $L$ is defined as the subdirect product subgroup of the direct power $L^k$ containing $M^k$ such that $L_k/M^k$ is isomorphic to $L/M$ (here $L/M$ is the diagonal subgroup of $(L/M)^k$). Denote by $t(L)$ the minimal degree of $L$ as a transitive permutation group.

**Theorem.** *Let $G$ be a finitely generated profinite group. Then $G$ is PFG exactly if for any $L$ as above if $L_k$ is a quotient of $G$ then $k \leq t(M)^c$ for some constant $c$.*

This theorem can be used to answer various questions of Lubotzky, Mann and Segal (see [LS]). For example answering an innocent looking but challenging question of Mann [Ma] we show that an open subgroup of a PFG group is also PFG.

Our main technical result is the following

**Theorem.** *The number of conjugacy classes of d-generated primitive subgroups of* $\mathrm{Sym}\,(n)$ *is at most* $n^{cd}$ *for some constant c.*

This estimate unifies and improves several earlier ones.

## References

[Bh] M. Bhattacharjee, The probability of generating certain profinite groups by two elements, Israel J. Math. 86 (1994), 311–329.

[BPSh] A. Borovik, L. Pyber, A. Shalev, Maximal subgroups in finite and profinite groups, Trans. Amer. Math. Soc. 348 (1996), 3745–3761.

[Di] J. D. Dixon, The probability of generating the symmetric group, Math. Zeit. 110 (1969), 199–205.

[KL] W. M. Kantor, A. Lubotzky, The probability of generating a finite classical group, Geom. Ded. 36 (1996), 67–87.

[LSh] M. W. Liebeck, A. Shalev, The probability of generating a finite simple group, Geom. Ded. 56 (1995), 103–113.

[LS] A. Lubotzky, D. Segal, Subgroup Growth, Progress in Mathematics, Birkhäuser, 2003.

[Ma] A. Mann, Positively finitely generated groups, Forum Math. 8 (1996), 429–459.

[MSh] A. Mann, A. Shalev, Simple groups, maximal subgroups and probabilistic aspects of profinite groups, Israel J. Math. 96 (1996), 449–468.

# Coprime Action on Finite Groups

Paul Flavell

## 1. Introduction

We wish to develop further the theory of automorphisms of finite groups, without recourse to the Classification of Finite Simple Groups. But naturally, the techniques used to prove the Classification are very relevant to this programme. Henceforth we assume:

**Hypothesis.**

- *$r$ is a prime,*
- *$R$ is an $r$-group and*
- *$G$ is an $r'$-group on which $R$ acts as a group of automorphisms.*

We outline three areas on which progress has been made:

(1) Thompson's Thesis asserts

*if $|R| = r$ and $C_G(R) = 1$ then $G$ is nilpotent.*

We shall present a generalization of this result.

(2) Known results on soluble groups will be extended to insoluble groups.

(3) The following is a consequence of the Classification and a theorem of Steinberg:

*if $G$ is simple and $R$ acts faithfully on $G$ then $R$ is cyclic.*

We shall present progress towards proving this result independently of the Classification.

## 2. Modules

The following result on modules is an essential tool.

**Theorem A.** [6] *Suppose that*

(a) $|R| = r$,
(b) *$V$ is a faithful irreducible $RG$-module over a field of characteristic $p$, and*
(c) $C_V(R) = 0$.

*Then either*

- $[G, R] = 1$ *or*
- *$r$ is a Fermat prime and $[G, R]$ is a nonabelian special 2-group.*

Shult [10] proved Theorem A in the case that $G$ is nilpotent. He used his result to study automorphisms of soluble groups. Shult's work is a nonmodular analogue of the work of Hall and Higman on representations of $p$-soluble groups. In the first edition of his book *Finite Group Theory*, Aschbacher extended Shult's results, essentially proving Theorem A when $G$ is soluble [1, (36.4), p.194]. Aschbacher's motivation was a new proof of the Soluble Signalizer Functor Theorem. If it is ever possible to prove the General Signalizer Functor Theorem outside of the inductive framework of the Classification, then Theorem A may have a role to play.

**Corollary B.** *Assume* (a), (b) *and that $G$ contains a cyclic $p'$-subgroup $X \neq 1$ that acts transitively on $[V, X]^{\#}$. Then $C_V(R) \neq 0$.*

## 3. Fusion

**Theorem C.** [7] *Suppose $|R| = r$. Let $p$ be an odd prime and suppose that $C_G(R)$ is a $p'$-group. Let $S \in Syl_p(G)$. Then $N_G(S)$ controls strong fusion in $S$.*

Theorem C and Frobenius' Normal $p$-Complement Theorem imply Thompson's Thesis. Theorem C follows from Theorem A, Corollary B and Theorem D below, which in turn is a slight extension of previous work of Collins [2, 3] and Glauberman [5].

**Theorem D.** [7] *Let $G$ be a group, $p$ an odd prime, $S \in Syl_p(G)$ and $T \leq Z(S)$. Suppose that $T \trianglelefteq N_G(J(S))$. Then at least one of the following holds:*

(a) *$T$ is weakly closed in $S$ with respect to $G$.*
(b) *There exists a cyclic $p'$-subgroup $X \leq N_G(T)$ such that $X$ acts nontrivially on $T$ and transitively on $[T, X]^{\#}$.*

## 4. $R$-Components

The following result on soluble groups is an easy consequence of Shult's work and has many applications in local analysis. For simplicity, we state it fully only in the case that $r$ is not a Fermat prime.

**Theorem.** *Suppose $G$ is soluble, $|R| = r$ and $D$ is an $RC_G(R)$-invariant nilpotent subgroup of $G$. Then $[D, R] \leq F(G)$, unless $r$ is a Fermat prime in which case .......*

The idea is to say something global about a subgroup that is specified locally in terms of the automorphism. Using Theorem A it is possible to extend this result to insoluble groups provided one replaces '$\leq F(G)$' with 'acts nilpotently on $F(G)$'. In the transition from soluble to insoluble, the Fitting subgroup is replaced by the Generalized Fitting subgroup, $F^*(G) = F(G)E(G)$, where $E(G)$, the layer of $G$, is the subgroup generated by the components of $G$. Consequently we wish to consider component like subgroups that are defined locally in terms of the automorphism.

**Definition.** *$K$ is an $R$-*component *of $G$ if $K$ is quasisimple and commutes with its $RC_G(R)$-conjugates; equivalently, $K$ is a component of an $RC_G(R)$-invariant subgroup of $G$.*

Note that we do not require $K$ to be $R$-invariant.

**Theorem E.** [8] *Suppose $|R| = r$ and $K$ is an $R$-component of $G$. Then at least one of the following holds:*

(a) *$K$ is a component of $C_G(R)$.*
(b) *$K$ is a component of $G$.*
(c) *$K$ is contained in an $R$-invariant component of $G$.*

In proving this result, we inevitably have to consider the action of a simple group on another simple group. We avoid appealing to the Schreier Conjecture by using a beautiful result of Dade [4].

**Corollary F.** *Suppose $|R| = r$ and $H$ is an $RC_G(R)$-invariant subgroup of $G$ with $H = [H, R]$. Then $E(H) \leq E(G)$.*

## 5. Pushing Up

Let $p$ be a prime. Define

$$\begin{aligned} P &= O_p(G; R) \\ &= \text{the unique maximal } RC_G(R)\text{-invariant } p\text{-subgroup of } G \\ &= \text{the intersection of all } R\text{-invariant Sylow } p\text{-subgroups.} \end{aligned}$$

**Theorem G.** [8] *Suppose $F^*(G) = O_p(G)$ and $p > 3$ then $P$ contains a nontrivial characteristic subgroup that is normal in $G$.*

This result is an analogue of Glauberman's $ZJ$-Theorem, but note there is no hypothesis on the noninvolvement of $SL_2(p)$.

## 6. Automorphisms of Simple Groups

Suppose that $R$ is abelian and noncyclic. Then

$$G = \left\langle C_G(\alpha) \mid \alpha \in R^{\#} \right\rangle .$$

Now $R$ is abelian so it acts on the fixed point subgroups. Thus we expect the action of $R$ on these subgroups to have considerable influence over the action of $R$ on $G$. Using many of the previous results, we are able to prove the following:

**Theorem H.** [8] *Suppose $R$ is noncyclic and abelian, $p > 3$ and*

$$[O^p F^* C_G(\alpha), R] = 1 \quad \textit{for all } \alpha \in R^{\#}.$$

*Then*

$$[O^p F^*(G), R] = 1.$$

Note that the principal hypothesis is satisfied if $F^* C_G(\alpha)$ is a $p$-group for all $\alpha \in R^{\#}$. Thus we have the following result about the automorphism group of a simple group.

**Corollary I.** [8] *Suppose $G$ is simple, that $R$ is abelian and faithful on $G$, that $p > 3$ and*

$$F^* C_G(\alpha) \ \textit{ is a } p\textit{-group for all } \alpha \in R^{\#}.$$

*Then $R$ is cyclic.*

## References

[1] M. Aschbacher, *Finite Group Theory, first edition* (Cambridge University Press, 1986).
[2] M.J. Collins, *Some Problems in the Theory of Finite Insoluble Groups*, D.Phil thesis, University of Oxford, 1969.
[3] M.J. Collins, 'Finite groups admitting almost fixed point free automorphisms', *Proc. symposia in Pure Math.* **21** 25-27 Amer. Math. Soc., Providence, R.I. 1971.
[4] E.C. Dade, 'Automorphismes extérieurs centralisant tout sous-groupes de Sylow', Math. Z. **117** (1970) 35-40.
[5] G. Glauberman, 'Weakly closed elements of Sylow subgroups', Math. Z. **107** (1968) 1-20.
[6] P. Flavell, 'A Hall-Higman-Shult type theorem for arbitrary finite groups', *Preprint*, 2004.
[7] P. Flavell, 'Automorphisms and fusion in finite groups', *Preprint*, 2004.
[8] P. Flavell, '$RC_G(R)$-signalizers in finite groups', *Preprint*, 2004.
[9] P. Flavell, 'An equivariant analogue of Glauberman's $ZJ$-Theorem', J. Algebra **257** (2002) 249-264.
[10] E. Shult, 'On groups admitting fixed point free operator groups', Illinois J. Math. **9** (1965) 701-720.

## Uniform bounds for finitely generated groups

Dan Segal
(joint work with Nikolay Nikolov)

An announcement of the results presented here has appeared in [NS1], and full proofs will appear in [NS2].

Our main result is

**Theorem 1.** *In a finitely generated profinite group, every subgroup of finite index is open.*

This answers Question 7.37 of the 1980 Kourovka Notebook [K], restated as Open Question 4.2.14 in [RZ]. It implies that the topology of a finitely generated profinite group is completely determined by its underlying abstract group structure, and that the category of finitely generated profinite groups is a full subcategory of the category of (abstract) groups.

The proof depends on properties of certain *verbal subgroups*. A group word $w$ is called *$d$-locally finite* if $F_d/w(F_d)$ is finite (where $F_d$ is the $d$-generator free group). Now let $G$ be a $d$-generator profinite group and $N$ a normal subgroup of finite index. It is easy to cook up a $d$-locally finite word $w$ such that $w(G) \subseteq N$ (by considering the finitely many homomorphisms from $F_d$ into $G/N$), so Theorem 1 follows from

**Theorem 2.** *Let $G$ be a $d$-generator profinite group and let $w$ be a $d$-locally finite group word. Then the verbal subgroup $w(G)$ is open in $G$.*

(By $w(G)$ we mean the subgroup generated *algebraically*, not topologically, by the values of $w$ in $G$). Though not necessary for Theorem 1, the following variation is also of interest:

**Theorem 3.** *Let $G$ be a finitely generated profinite group and $H$ a closed normal subgroup of $G$. Then the subgroup $[H, G]$ generated (algebraically) by all commutators $[h, g]$ ($h \in H$, $g \in G$) is closed in $G$.*

This implies in particular that *the (algebraic) derived group $G'$ is closed*, and (by an obvious induction) that *every term of the (algebraic) lower central series of $G$ is also closed.*

Thus $w(G)$ is closed if (a) $w$ is a locally finite word or (b) $w$ is one of the words $[x_1, \ldots, x_n]$ with $n \geq 2$. This does *not* hold for arbitrary words, however: Romankov [Ro] has shown that it fails (even in pro-$p$ groups) for the "2nd derived word" $w = [[x_1, x_2], [x_3, x_4]]$. On the other hand, it seems likely that it does hold for the "Burnside words" $w = x^q$; indeed, we can prove that the verbal subgroup $G^q$ is closed in a finitely generated profinite group $G$ provided $G$ does not involve all finite groups as open sections.

If the word $w$ is $d$-locally finite and $G$ is a $d$-generator profinite group, then $w(G)$ is open if and only if it is closed. A simple compactness argument then shows that Theorem 2 is equivalent to the following result about finite groups:

**Theorem 4.** *Let $d$ be a natural number and let $w$ be a $d$-locally finite group word. Then there exists $f = f_w(d)$ such that if $G$ is any $d$-generator finite group, then every element of $w(G)$ is equal to a product of $f$ $w$-values.*

(By *$w$-values* here we mean elements of the form $w(g_1, \dots, g_k)^{\pm 1}$.)

Similarly, Theorem 3 follows from

**Theorem 5.** *Let $d$ be a natural number. Then there exists $g = g(d)$ such that if $G$ is any $d$-generator finite group and $H$ is any normal subgroup of $G$, then every element of $[H, G]$ is equal to a product of $g$ commutators $[u, v]$ with $u \in H$ and $v \in G$.*

These theorems are applications of our main technical result, which is as follows. Before stating it let us introduce some notation. For any subset $S$ of a group $G$ and natural number $n$, $S^{*n} = \{s_1 s_2 \dots s_n \mid s_1, \dots, s_n \in S\}$. For $g \in G$ and $S, T \subseteq G$, $[S, g] = \{[s, g] \mid s \in S\}$, $\mathfrak{c}(S, T) = \{[s, t] \mid s \in S, t \in T\}$. For an integer $q$ we write $G^{\{q\}} = \{g^q \mid g \in G\}$.

**Key Theorem** *There exist numerical functions $h_1$, $h_2$ and $z$ and an absolute constant $D$ with the following property. Let $G = \langle g_1, \dots, g_d \rangle$ be a finite group and $H$ a subgroup such that* (i) *$H = [H, G]$,* (ii) *if $H \geq N > Z$, where $N$ and $Z$ are normal subgroups of $G$ and $N/Z$ is non-abelian, then $N/Z$ is neither simple nor the direct product of two isomorphic simple groups. Then*

$$\text{(A)}: \qquad H = ([H, g_1] \cdot \ldots \cdot [H, g_d])^{*h_1(d,q)} \cdot (H^{\{q\}})^{*z(q)}$$

for each $q \in \mathbb{N}$, and

$$\text{(B)}: \qquad H = ([H, g_1] \cdot \ldots \cdot [H, g_d])^{*h_2(d)} \cdot \mathfrak{c}(H, H)^{*D}.$$

The deduction of Theorem 4 is not quite direct. One applies the Key Theorem not to $G$ itself but to the group $w(G)$, which is generated by a bounded number of $w$-values $g_1, \dots, g_{d'}$. We take $q = |C_\infty / w(C_\infty)|$, and find a characteristic subgroup $H$ of $w(G)$ such that (a) the pair $(w(G), H)$ satisfies the hypotheses of the Key Theorem and (b) Theorem 4 is already known for the quotient group $G/H$. The result then follows from (A) on noting that each element $[h, g_i]$ is a product of two $w$-values and each element $h^q$ is a $w$-value. Theorem 5 is deduced in a similar way from Key Theorem (B).

The proof of the Key Theorem is long and elaborate; it is modelled in principle on Hensel's Lemma. Given an arbitrary element $h \in H$ we have to solve an equation of the form $h = \Phi(u_1, \dots, u_m)$ where $\Phi$ is a group word involving the 'unknowns' $u_i$, to be found in $H$, and some 'constants' $g_1, \dots, g_m \in G$. We assume inductively that this can be done modulo $K$, where $K$ is some small normal subgroup of $G$ inside $H$, and then have to kill the error term by adjusting the unknowns. This comes down to solving a new system of equations in $K$ (or perhaps a slightly larger normal subgroup), considered as a $G$-operator group.

The possibility of doing this depends ultimately on properties of the finite simple groups. Let $\alpha$, $\beta$ be automorphisms of a group $G$. For $x$, $y \in G$, we define the "twisted commutator"

$$T_{\alpha,\beta}(x,y) = x^{-1}y^{-1}x^{\alpha}y^{\beta}.$$

**Theorem 6.** *There is an absolute constant $D$ such that if $S$ is a finite quasisimple group and $\alpha_i$, $\beta_i$ $(i = 1,\ldots,D)$ are any automorphisms of $S$ then*

$$S = T_{\alpha_1,\beta_1}(S,S)\cdot\ldots\cdot T_{\alpha_D,\beta_D}(S,S).$$

**Theorem 7.** *Let $q$ be a natural number. There exist natural numbers $C = C(q)$ and $M = M(q)$ such that if $S$ is a finite quasisimple group with $|S| > C$, $\beta_i$ $(i = 1,\ldots,M)$ are any automorphisms of $S$, and $q_i$ $(i = 1,\ldots,M)$ are any divisors of $q$, then there exist inner automorphisms $\alpha_i$ of $S$ such that*

$$S = [S,(\alpha_1\beta_1)^{q_1}]\cdot\ldots\cdot[S,(\alpha_M\beta_M)^{q_M}].$$

These generalize several known results about products of commutators and products of powers in simple groups. They are proved by a delicate analysis of the internal structure of the groups, known from the Classification, together with recent results of Liebeck, Pyber and Shalev [LP], [LS].

## References


[K] *Kourovka Notebook*, 7th ed., Novosibirsk, 1980.

[LP] M. W. Liebeck and L. Pyber, Finite linear groups and bounded generation, *Duke Math. J.* **107** (2001), 159-171.

[LS] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383-406.

[RZ] L. Ribes and P. A. Zalesskii, *Profinite groups*. Ergebnisse der Math. **40**, Springer, Berlin – Heidelberg , 2000.

[NS1] N. Nikolov and D. Segal, Finite index subgroups in profinite groups, *C. R. Acad. Sci. Paris I* **337** (2003), 303-308.

[NS2] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds; II: products in quasimple groups, *Annals of Math.*, to appear

[Ro] V. A. Roman'kov, Width of verbal subgroups in solvable groups, *Algebra i Logika* **21** (1982), 60-72 (*Russian*); Algebra and Logic **21** (1982), 41-49 (*English*).


## "All" geometries for the smallest sporadic groups

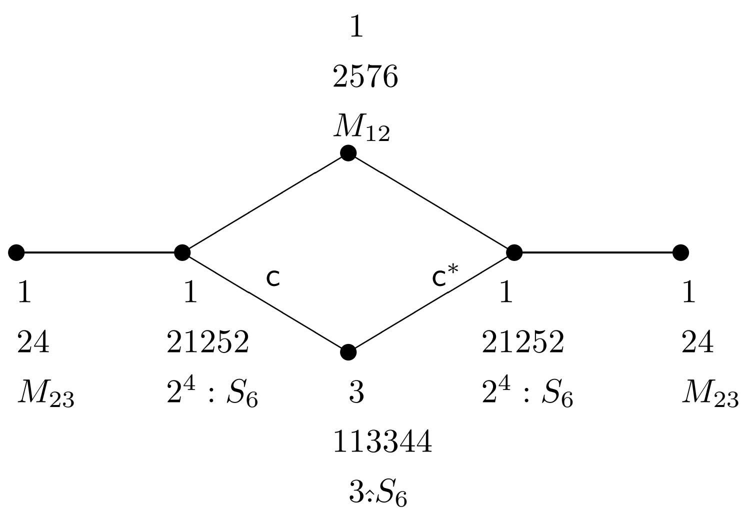

Francis Buekenhout

(joint work with Dimitri Leemans)


This is a report prepared jointly with Dimitri Leemans on the present status of a project going back to 1985. The project was progressing with a series of persons including mainly Dimitri Leemans, Philippe Cara and Michel Dehon. The purpose is to find "all" geometries of all sporadic groups under conditions that are both reasonably general to justify the term "all" and reasonably restricted in order to allow for a classification. We rely essentially but not exclusively on computations within MAGMA [1]. Our conditions are mainly to require (FT) flag-transitivity, (RC) residual connectedness, (RWPRI) residual weak primitivity ( at least one of the maximal parabolic subgroups is a maximal subgroup and residually), $(2T)_1$

doubly transitive rank one residues (rank one residues are BN-pairs of rank one) and $(IP)_2$ intersection property for rank two residues (two distinct points are incident to at most one line and dually). A basic rule is that all conditions must be satisfied by a building and the corresponding group of Lie type. A detailed synthesis of our work as of 2000 is provided in [2]. At that time, four sporadic groups had been dealt with. By now, thanks to extensive work due to Dimitri Leemans[1], the classification is complete for the nine smallest sporadic groups and it is close to completion for McL. In the latter case, the group has 373 conjugacy classes of subgroups. Each of these is chosen at its turn to provide a Borel subgroup for an exploration of geometries. At this time, only 6 of the 373 possibilities remain to be explored. Among the geometries obtained, the highest rank that is achieved is six. For each of these cases, a computer-free existence proof has been provided in rather surprising geometric terms by Dimitri Leemans (see for instance [4, 5]). An additional intersection property (IP) from Tits' heritage going back to 1956, has been studied by Dimitri Leemans and his student Pascale Jacobs [3]. It reduces our collection of geometries to about 40% of its initial size.

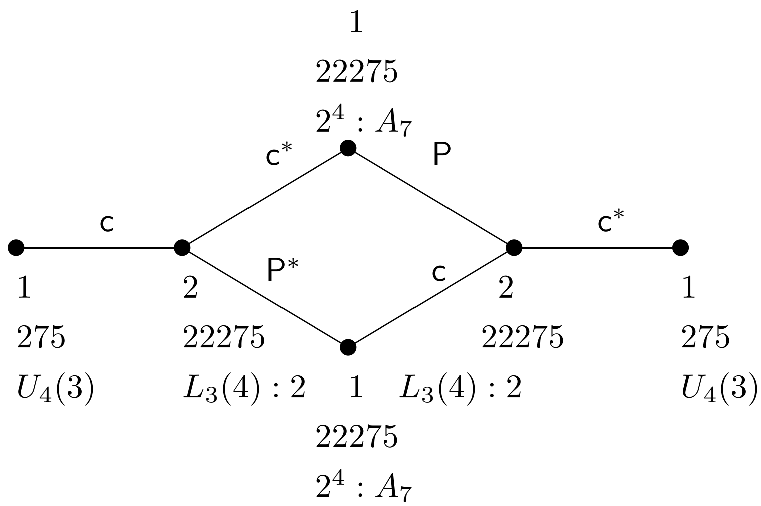
A gem among others due to Dimitri Leemans is for the Mathieu group $\mathsf{M}_{24}$. It looks as follows.




The $\mathsf{M}_{12}$-residue was observed long ago by Meixner. The $\mathsf{M}_{24}$-geometry could be constructed geometrically from the classical Steiner system $S(5, 8, 24)$.

Another one due to Leemans for McL has the following diagram.

[1]See Leemans Website at (http://cso.ulb.ac.be/∼dleemans/) for recent papers on the subject.




An attack on a group $G$ requires, as a first step, to get a complete control over the subgroup lattice of $G$, more exactly, the poset of conjugacy classes of subgroups. A new programme due to Dimitri Leemans has allowed to get this computation in less than 3 seconds for $\mathsf{M}_{12}$ and less than 30 seconds for $\mathsf{McL}$.

## References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: the user language. *J. Symbolic Comput.*, (3/4):235–265, 1997.

[2] F. Buekenhout, P. Cara, M. Dehon, and D. Leemans. Residually weakly primitive geometries of small almost simple groups : a synthesis. In A. Pasini, editor, *Topics in Diagram Geometry*, volume 12 of *Quaderni Mat.*, pages 1–27. 2003.

[3] P. Jacobs and D. Leemans. An algorithmic analysis of the intersection property. *LMS J. Comput. Math.*, 7:284–299, 2004.

[4] D. Leemans. A family of geometries related to the Suzuki tower. *Comm. Algebra*, to appear.

[5] D. Leemans. Two rank six geometries for the Higman-Sims sporadic group. *Discrete Math.*, to appear.

## Bicharacteristic Finite Simple Groups

Richard Lyons
(joint work with Inna Korchagina and Ron Solomon)

Only a handful of general types of $p$-local structures are to be found in the simple groups[1]. The groups of Lie type show uniform behavior (of two types, according as $p$ is or is not the characteristic of the underlying field), as do the alternating groups. Unsurprisingly the sporadic groups show more variation. In the "GLS" project [3] for a second generation proof of the classification of the simple groups,

[1] Throughout, "group" means "finite group".

the basic strategy yields the twenty-six sporadic groups in four cohorts[2]

$$\begin{aligned} Spor_U &= \{J_1\} \\ Spor_{SO} &= \{M_{11}, M_{12}, Mc, Ly, ON\} \\ Spor_{QT} &= \{M_{22}, M_{23}, M_{24}, J_2, J_3, J_4, HS, He, Ru\} \\ Spor_{bi\text{-}\chi} &= \{Co_1, Co_2, Co_3, Suz, F_1, F_2, F_3, F_5, Fi'_{24}, Fi_{23}, Fi_{22}\}. \end{aligned}$$

The first arises from a uniqueness theorem ($J_1$ has a proper 2-generated 2-core), the second from the special odd case [5], and the third from the Quasithin Theorem of Aschbacher and Smith [1]. We comment here on the local axioms and methods leading to the set $Spor_{bi\text{-}\chi}$ of "bicharacteristic" groups (in the sense of the hypothesis of Theorem 2 below).

Recall that if $p$ is a prime, then a simple group $G$ is said to be of characteristic $p$-type if and only if $F^*(N) = O_p(N)$ for every $p$-local subgroup $N$ of $G$ (or equivalently for all $N = C_G(x)$, $x \in G$ of order $p$.) Let us say also that $G$ is of $p'$-type[3] if and only if there exists $x \in G$ such that $x$ has order $p$ and $C_G(x)$ has a component $L$ such that $L$ is not a group of Lie type in characteristic $p$, but is a group of Lie type. For the purposes of this talk, let us add the condition $m_p(G) > 1$ to both definitions. Here is the tally of the sporadic groups.

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | $> 13$ |
|---|---|---|---|---|---|---|---|
| # of spor. gps. of char. $p$-type | 8 | 2 | 6 | 1 | 1 | 0 | 0 |
| # of spor. gps. of char. $p'$-type | 0 | 3 | 1 | 1 | 0 | 1 | 0 |

Thirteen of the sporadic groups are not of characteristic $p$ type for any prime $p$. The low numbers for $p'$-type confirm the efficacy of the "semisimple" approach to the characterization of simple groups of Lie type (moreover, $m_p(G) = 2$ for each sporadic group of characteristic $p'$-type.) It is clear in any case that the notions of $p$-type and $p'$-type, combined, still miss a significant number of sporadic groups. In particular the rich 3-structure of many sporadic groups is not captured by either definition, although one feels for example that the Fischer groups, even $F_1$, $F_2$, $F_3$ and $F_5$, tend strongly toward characteristic 3-type.

Which simple groups $G$ are of both characteristic $p$-type and characteristic $q$-type for some distinct primes $p$ and $q$? Among the sporadic groups we find only $(G, p, q) = (M_{12}, 2, 3)$, $(Mc, 3, 5)$, $(F_3, 2, 5)$, $(Co_2, 2, 5)$, and $(J_4, 2, 11)$. There are (in)famous examples of Lie type, for instance $(A_5, 2, 5)$, $(A_6, 2, 3)$, $(PSp_4(3), 2, 3)$, $(L_3(4), 2, 3)$, $(U_4(3), 2, 3)$ and $(G_2(3), 2, 3)$. But the complete list is not long. Moreover, many of the sporadic groups *nearly* qualify as being of characteristic 2-type

[2]In this partition, the unusual placement of $J_1$, $M_{11}$ and $M_{12}$, which are conclusions of the Aschbacher-Smith theorem, is an artifact of the GLS strategy. Groups of 2-rank at most 3 are considered to be of special odd type and so are characterized before the quasithin groups. Moreover the proper 2-generated core theorem, to which $J_1$ is an exceptional conclusion, necessarily precedes the treatment of special odd type groups.

[3]This notion has only been devised for the expository purpose of this talk.

and characteristic 3-type. This is particularly so for the larger ones, from which one expects the most regular behavior.

We define below a weaker notion than characteristic $p$-type so that the simple groups which are bicharacteristic in this weaker sense (a) include these sporadic groups, and (b) can still be classified by existing techniques or extensions of them.

In the $N$-group paper [11, 12] Thompson introduced most of the techniques (including the "Thompson Dihedral Lemma") for studying simple groups of characteristic $p$-type and characteristic $q$-type such that $m_p(G)$ and $m_q(G)$ are both at least 3. Though there are no $N$-groups satisfying these conditions, Thompson [12] gave independent characterizations of the (non-$N$-)groups $G_2(3)$ and $PSp_4(3)$ by axioms with a characteristic 2 and characteristic 3 flavor. Pursuing his ideas, Klinger and Mason, with a later boost from Korchagina, proved the following theorem. Here $m_{2,p}(G)$ is the largest $p$-rank of all 2-local subgroups of $G$.

**Theorem 1.** [6, 7] *If $p$ is an odd prime and $G$ is a group of characteristic $p$-type and characteristic 2-type, then $m_{2,p}(G) \le 2$.*

Our broader notions are as follows. We say that a $K$-proper simple group $G$ is of **even type** if and only if for every involution $x \in G$ and every 2-component $L$ of $C_G(x)$, $O_{2'}(C_G(x)) = 1$ and $L \in C_2$. Likewise for an odd prime $p$, $G$ is of **weak $p$-type** if and only if for every element $x \in G$ of order $p$ such that $m_p(G) \ge \min(e(G), 4)$, $O_{p'}(C_G(x))$ has odd order and $L/O_{p'}(L) \in C_p$ for every $p$-component $L$ of $C_G(x)$. Here $C_2$ and $C_p$ are certain sets of quasisimple $K$-groups [3], rather close to the sets $Chev(2)$ and $Chev(p)$, respectively. (See also Ron Solomon's report from this conference [10].)

Volume 8 of GLS is now planned to treat what Solomon calls the "sporadic" case, and in particular to do much of the analysis for the following theorem, which explains the terminology $Spor_{bi\text{-}\chi}$.

**Theorem 2.** (In progress) *Let $G$ be a $K$-proper simple group and $p$ an odd prime such that $m_{2,p}(G) \ge 3$. Assume that $G$ is of even type and of weak $p$-type. Then $p = 3$ and one of the following holds:*

(1) *$G$ has the same centralizer of involution pattern as some $G^* \in Spor_{bi\text{-}\chi}$.*
(2) *$G \cong U_5(2)$, $U_6(2)$, $U_7(2)$, $C_4(2)$, $D_4(2)$, ${}^2D_5(2)$, ${}^2E_6(2)$, $F_4(2)$, $B_3(3)$, $D_4(3)$, ${}^2D_4(3)$ or $A_{12}$.*
(3) *$G$ possesses a maximal subgroup $M$ which is a $p$-uniqueness subgroup.*

Most of the groups in (2) are sizable composition factors of local or maximal subgroups of groups in $Spor_{bi\text{-}\chi}$.

Alternative (1) of Theorem 2 means that there is an isomorphism between a Sylow 2-subgroup of $G$ and one of $G^*$, preserving the fusion pattern of involutions and the isomorphism types of centralizers of involutions. Alternative (3) is rather technical; roughly it means that $M$ contains $\Gamma^o_{P,2}(G)$ for some $P \in \mathrm{Syl}_p(G)$, and either $N \le M$ or $m_p(N \cap M) \le 1$ for any 2-local subgroup $N$ of $G$. In fact, Volume 8 will only establish a weaker version of this alternative, from which the full version will be deduced in a later volume devoted to odd uniqueness theorems.

In 1992, Gorenstein and the author [2] proved a test version of Theorem 2 under somewhat stronger hypotheses on components, and the considerably stronger hypothesis $m_{2,p}(G) \geq 4$, so that the only target groups were the six sporadic groups $F_1$, $F_2$, $Fi'_{24}$, $Fi_{23}$, $Fi_{22}$ and $Co_1$. We took or extended the techniques from [6]; some basic techniques are discussed in Section 24 of [4]. One technical challenge was the lack of a "cross-characteristic" version of $L_{p'}$-balance governing the relationships between the layers of $C_G(x)$ and $C_G(y)$, where $x$ and $y$ are commuting elements of respective orders 2, $p$. At the moment the author is working to drop the special hypotheses in [2]. One resulting change in the assumptions on elements $x \in G$ of order $p$ – from $O_{p'}(C_G(x)) = 1$ to $|O_{p'}(C_G(x))|$ being odd – is absorbed almost trivially. The case $e(G) = 3$, which in our original plan was to have been treated in a quasithin vein (again cf. [10]), is now the subject of several papers by Inna Korchagina and collaborators, with more papers in preparation at the time of this report [7, 8, 9].

## References


[1] M. Aschbacher and S. D. Smith, The Classification of Quasithin Groups I,II. A. M. S. Surveys and Monographs **111**, **112** (2004).

[2] D. Gorenstein and R. Lyons, *A local characterization of large sporadic groups*, preprint (1992).

[3] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups: Overview and Outline*, A. M. S. Surveys and Monographs **40.1** (1995).

[4] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups: General Group Theory*, A. M. S. Surveys and Monographs **40.2** (1996).

[5] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups: The Special Odd Case*, A. M. S. Surveys and Monographs **40.6** (2004).

[6] K. Klinger and G. Mason, *Centralizers of p-subgroups in groups of characteristic* $2, p$ *type*, J. Algebra **37** (1975), 362–375.

[7] I. Korchagina, *Ph.D. Thesis*, The Ohio State University (2001).

[8] I. Korchagina and R. Lyons, *A* $\{2,3\}$*-local characterization of the simple groups* $A_{12}$*,* $Sp_8(2)$*,* $F_4(2)$ *and* $F_5$, in preparation.

[9] I. Korchagina, R. Lyons and R. Solomon, *Toward a characterization of the sporadic groups of Suzuki and Thompson*, J. Algebra **257** (2002), 414–451.

[10] R. Solomon, *Meager finite simple groups*, Oberwolfach Reports (this conference).

[11] J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable I*, Bull. A. M. S. **74** (1968), 383–437.

[12] J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable II*, Pacific J. Math. **33** (1970), 451–536.


# On minimal subdegrees of finite primitive permutation groups

Cheryl E. Praeger, Ákos Seress

We study the minimal non-trivial subdegrees of finite primitive permutation groups that admit an embedding into a wreath product in product action, giving a connection with the same quantity for the primitive component. We discover that the primitive groups of twisted wreath type exhibit different (but interesting) behaviour from the other primitive types. This is joint work also with Michael Giudici, Cai Heng Li, and Vladimir Trofimov, and the full version will be published in [2].

For a transitive permutation group $G$ on a set $\Omega$, a *suborbit of $G$ relative to a point $\alpha \in \Omega$* is a $G_\alpha$-orbit $\Gamma$, and its size $|\Gamma|$ is the corresponding *subdegree* of $G$. A suborbit $\Gamma$, and the corresponding subdegree, are said to be non-trivial provided $\Gamma \neq \{\alpha\}$. In general, a non-trivial subdegree may be equal to 1. However, if $G$ is primitive and not cyclic of prime order, then $\alpha$ is the unique fixed point of $G_\alpha$, and consequently all non-trivial subdegrees of a non-cyclic primitive permutation group are greater than 1. Let $\mathrm{MinSubDeg}(G)$ denote the minimum of the non-trivial subdegrees of $G$, and note that the transitivity of $G$ implies that the value of $\mathrm{MinSubDeg}(G)$ is independent of the choice of $\alpha$.

The O'Nan–Scott Theorem partitions the finite primitive permutation groups into a number of disjoint types. For several of these types, each group $G$ of the type admits a natural embedding into a wreath product $H \wr S_k$ in its product action on a Cartesian power $\Delta^k$, where $k \geq 2$, $H$ is a primitive permutation group on the smaller set $\Delta$, and $H$ is induced by $G$. The group $H$ is called the *primitive component of $G$ relative to the Cartesian decomposition $\Delta^k$*. We study the relationship between $\mathrm{MinSubDeg}(G)$ and $\mathrm{MinSubDeg}(H)$ for these types of primitive groups.

The *socle* of a finite group is the product of its minimal normal subgroups. Our first theorem treats the case where $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k) = \mathrm{Soc}(H)^k$.

**Theorem 1.** [2, Theorem 1.1] *Let $G$ be a finite primitive permutation group such that $G \leq H \wr S_k$ acting in product action on $\Delta^k$, with primitive component $H$ and $k \geq 2$. Suppose further that $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k)$ and is non-abelian. Then $\mathrm{MinSubDeg}(G) = k \cdot \mathrm{MinSubDeg}(H)$. Moreover, let $\delta \in \Delta$ and $\alpha = (\delta, \ldots, \delta) \in \Delta^k$, and let $\Gamma$ be a $G_\alpha$-orbit in $\Delta^k \setminus \{\alpha\}$ of minimum length. Then there exists a minimum length $H_\delta$-orbit $\Gamma_0$ in $\Delta \setminus \{\delta\}$ such that either*

(a) $\Gamma = \bigcup_{1 \leq i \leq k} \Gamma_i$ *where $\Gamma_i$ consists of all $k$-tuples $(\delta_1, \ldots, \delta_k)$ such that $\delta_j = \delta$ for $j \neq i$, and $\delta_i \in \Gamma_0$, or*

(b) *each $k$-tuple in $\Gamma$ has exactly two entries in $\Gamma_0$, with the remaining entries all equal to $\delta$. Moreover, $H \leq H_0 \wr S_\ell$ in product action on $\Delta = \Delta_0^\ell$ with primitive component $H_0$, $\mathrm{Soc}(H) = \mathrm{Soc}(H_0 \wr S_\ell)$ (where possibly $\ell = 1$ in which case $H_0 = H$), $|\Gamma_0| = 4\ell$, and $(H_0, |\Delta_0|)$ is one of* $(\mathrm{PGL}(2,7), 21)$, $(\mathrm{PGL}(2,9), 45)$, $(\mathrm{M}_{10}, 45)$, *or* $(\mathrm{P\Gamma L}(2,9), 45)$.

**Remark 2.** (a) This theorem applies to all finite primitive groups of product action type and compound diagonal type, and those with two regular, non-abelian, non-simple minimal normal subgroups.

(b) In Theorem 1 (b), $G \leq H_0 \wr S_{\ell k}$ in product action with primitive component $H_0$ relative to the decomposition $\Omega = \Delta_0^{\ell k}$. Moreover, for each possibility for $(H_0, |\Delta_0|)$, the stabiliser $(H_0)_{\delta_0}$ (where $\delta_0 \in \Delta_0$) has a unique orbit in $\Delta_0$ of length $\mathrm{MinSubDeg}(H_0) = 4$ (see [1, Lemma 3.1]), and we show in [2, Proposition 3.2] that there are examples of groups $G$ as in (b), corresponding to each group $H_0$, for each even integer $k$.

(b) The study of $\mathrm{MinSubDeg}(G)$ for finite primitive groups $G \leq \mathrm{Sym}(\Omega)$ was motivated by problems concerning edge-transitive graphs, since the smallest non-trivial $G$-suborbit determines a directed graph with smallest possible valency among the $G$-invariant directed graphs on $\Omega$. Such minimum-valency graphs arose in [3] in the investigation of limits of convergent sequences of finite vertex-primitive graphs with respect to a certain metric on the space of locally finite, vertex-transitive graphs. The minimum-valency graphs for the primitive groups $G$ occuring in Theorem 1 were characterised in [2, Theorem 1.4] by extending the arguments used in the proof of Theorem 1.

There is one O'Nan–Scott type that admits natural embeddings into a wreath product in product action to which Theorem 1 does not apply, namely the twisted wreath type TW. As with the types covered by Theorem 1, for every primitive group $G$ of type TW we have $G \leq H \wr S_k$ acting on $\Delta^k$, where $H$ is the primitive component of $G$ and $k \geq 2$. However, $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$, while $\mathrm{Soc}(H) \cong T \times T$, so that $\mathrm{Soc}(G)$ is not equal to $\mathrm{Soc}(H \wr S_k)$.

The socle of $G$ acts regularly on $\Delta^k$ and $G$ is a semidirect product $\mathrm{Soc}(G) \rtimes P$, for some transitive subgroup $P$ of $S_k$. In fact, for these groups the relationship between $\mathrm{MinSubDeg}(G)$ and $\mathrm{MinSubDeg}(H)$ given in Theorem 1 fails spectacularly. For a group $P$, we denote by $\mathrm{MinDeg}(P)$, called the *minimal degree of* $P$, the least positive integer $n$ such that $P$ acts faithfully and transitively on a set of size $n$.

**Theorem 3.** *Let $G$ be a finite primitive permutation group of O'Nan–Scott type* TW *and suppose that $G = \mathrm{Soc}(G) \rtimes P \leq H \wr S_k$ acting on a set $\Delta^k$ (where $k \geq 2$) with primitive component $H \leq \mathrm{Sym}(\Delta)$. Then*

$$\max\{\mathrm{MinSubDeg}(H), \mathrm{MinDeg}(P)\} \leq \mathrm{MinSubDeg}(G) \leq k \cdot \mathrm{MinSubDeg}(H).$$

*Moreover there are infinitely many examples with* $\mathrm{MinSubDeg}(G) = \mathrm{MinDeg}(P) = \mathrm{MinSubDeg}(H)$*, and with* $\mathrm{MinSubDeg}(G) = \mathrm{MinDeg}(P) > \mathrm{MinSubDeg}(H)$*, and there are examples with* $\mathrm{MinSubDeg}(G) = \mathrm{MinSubDeg}(H) > \mathrm{MinDeg}(P)$*.*

In analogy with Theorem 1(a), we define a certain collection $\mathcal{R}$ of points in the permutation domain (see [2, Construction 4.1]) and prove that $\mathrm{MinSubDeg}(G)$ is always attained by a $G_\alpha$–orbit containing one of these special points. Further, there is a partial analogy to Theorem 1(b), in that we show that there can be additional minimal length suborbits in certain situations.

Thus although there are certain similarities, the behaviour of primitive groups of type TW is different from that of primitive groups considered in Theorem 1. Moreover, we wonder whether it is perhaps never possible for $\mathrm{MinSubDeg}(G)$ with $G$ of type TW, to achieve the bound of Theorem 1.

**Question 4.** *Is it true that, for all finite primitive permutation groups $G = \mathrm{Soc}(G) \rtimes P \leq H \wr S_k$ of type* TW*, with $P, H$ as in Theorem* 3*, the strict inequality* $\mathrm{MinSubDeg}(G) < k \cdot \mathrm{MinSubDeg}(H)$ *holds?*

References

[1] Anton Betten, Anne Delandtsheer, Alice C. Niemeyer and Cheryl E. Praeger, On a theorem of Wielandt for finite primitive permutation groups, *J. Group Theory* **6** (2003), 415–420.

[2] Michael Giudici, Cai Heng Li, Cheryl E. Praeger, Ákos Seress and Vladimir Trofimov, On minimal subdegrees of finite primitive permutation groups, to appear in: *Finite Geometries, Groups, and Computation*, A. Hulpke, R. Liebler, T. Penttila, Á. Seress eds, deGruyter.

[3] Michael Giudici, Cai Heng Li, Cheryl E. Praeger, Ákos Seress and Vladimir Trofimov, On limit graphs of finite vertex-primitive graphs, preprint, 2004.


## The Local $C(G, T)$ Theorem


David Bundy

(joint work with Bernd Stellmacher and Nils Hebbinghaus)


Throughout we fix $G$ to be a finite group, $p$ a prime dividing the order of $G$ and $T \in Syl_p(G)$. We also define $\mathcal{A}(G)$ to be the set of elementary abelian $p$-subgroups of $G$ of maximal order and $\Omega(G)$ to be the subgroup generated by the elements of order $p$ of $G$. Then

$$J(G) := \langle A \mid A \in \mathcal{A}(G) \rangle$$

is the **Thompson subgroup** of $G$ (with respect to $p$), and

$$B(G) := \langle C_T(\Omega(Z(J(T)))) \mid T \in Syl_p G \rangle$$

is the **Baumann subgroup** of $G$ (with respect to $p$).

**Definition.** *Let $S \leq T$. Then*

$$C(G, S) := \langle N_G(C) \mid 1 \neq C \text{ char } S \rangle,$$

$$C^*(G, T) := \langle C_G(\Omega(Z(T))), C(G, B(T)) \rangle,$$

$$C^{**}(G, T) := \langle C_G(\Omega(Z(T))), N_G(J(T)) \rangle.$$

*Notice that every characteristic subgroup of $B(T)$ is characteristic in $T$ and $J(T)$ is characteristic in $B(T)$. In particular*

$$C^{**}(G, T) \leq C^*(G, T) \leq C(G, T).$$

**Definition.** *A group $G$ is of characteristic $p$ if*

$$C_G(O_p(G)) \leq O_p(G).$$

We will classify those groups of characteristic $p$ that are not equal to $C(G, T)$ with respect to some Sylow $p$-subgroup $T$, a result called the **Local $\boldsymbol{C(G, T)}$-Theorem**. This result is of interest to a project initiated by Meierfrankenfeld, see [2], which aims to revise parts of the classification of the finite simple groups.

The Local $C(G, T)$-Theorem for the case when $p = 2$ was already proven by Aschbacher in [1] and is a crucial part of the original classification of the finite simple groups. An alternative proof for $p = 2$ was also given by Gorenstein and Lyons [3]. Their proof avoids the use of some deep results needed in Aschbacher's proof. Instead it requires the $K$-group hypothesis (that any simple section of $G$ is one of the known finite simple groups), which is sufficient for the purposes of the classification of the finite simple groups.

Our proof uses a different approach to either of the above; in particular it does not need a $K$-group assumption and works for all primes $p$. To state the main result we need one further technical definition.

**Definition.** *A subgroup $E \leq G$ is a* $\boldsymbol{B(T)}$**-block** *of $G$ if for $W := \Omega(Z(O_p(E)))$:*

- (*i*) $E = O^p(E) = [E, B(T)]$, $[O_p(E), E] = O_p(E)$, *and* $[E, \Omega(Z(T))] \neq 1$.
- (*ii*) $E/O_p(E) \cong SL_2(p^n)'$ *or* $p = 2$ *and* $E/O_2(E) \cong A_{2m+1}$, *and* $W/C_W(E)$ *is a natural* $SL_2(p^n)'$*- resp.* $A_{2m+1}$*-module for* $E/O_p(E)$.
- (*iii*) $O_p(E) = W$, *or*
  - (1) $p = 3$, *and* $O_3(E)/W$ *is a natural* $SL_2(3^n)'$*-module,*
  - (2) $O_3(E)' = \Phi(O_3(E)) = Z(E) = C_W(E)$ *and* $|Z(E)| = 3^n$, *and*
  - (3) *no element of* $B(T) \setminus C_{B(T)}(W)$ *acts quadratically on* $O_3(E)/Z(E)$.

*If* $E/O_p(E) \cong SL_2(p^n)'$, *then $E$ is a* **linear** *block, and in the other case $E$ is a* **symmetric** *block. Moreover, if* (1) – (3) *in* (*iii*) *hold, then $E$ is an* **exceptional** *block.*

Notice that in [1] (for $p = 2$) such blocks are called *short* subgroups, while a *block* is defined to be a subnormal short subgroup. We also remark that exceptional blocks do exist, for example as a subgroup of $G_2(3^n)$.

We will prove the following theorem.

**Theorem 1.** (**Local** $\boldsymbol{C^*(G,T)}$**-Theorem**) *Let $G$ be of characteristic $p$ such that $G \neq C^*(G,T)$. Then there exist $B(T)$-blocks $G_1, \ldots, G_r$ of $G$ such that the following hold:*

- (*a*) $\{G_1, \ldots, G_r\}^G = \{G_1, \ldots, G_r\}$.
- (*b*) $G = C^*(G,T) \prod_{i=1}^r G_i$.
- (*c*) $[G_i, G_j] = 1$ *for* $i \neq j$.
- (*d*) *Every $B(T)$-block of $G$ that is not in $C^*(G,T)$ is contained in one of the $B(T)$-blocks $G_1, \ldots, G_r$.*

**Corollary 2.** (**Local** $\boldsymbol{C(G,T)}$**-Theorem**) *Let $G$ be of characteristic $p$ such that $G \neq C(G,T)$. Then $G$ has the same structure as given in Theorem 1 with the additional restriction that if $G_i$ is a symmetric block, then* $G_i/O_2(G_i) \cong A_{2^n+1}$.

It is easy to see that under the assumption of Theorem 1 every proper subgroup $L$ with $B(T) \leq L$ and $L \not\leq C^*(G,T)$ satisfies the hypothesis of Theorem 1. Hence, those groups $G$, where $C^*(G,T)$ is the unique maximal subgroup containing $B(T)$, are the basis for an induction on the order of $G$. This leads to a class of groups that plays the same role for groups of local characteristic $p$ as the class of minimal parabolic groups for groups of Lie type in characteristic $p$ (see [2]).

**Definition.** *Let $T \in Syl_p(G)$. Then $G$ is a* **minimal parabolic** *group (with respect to $p$), if $T$ is not normal in $G$ and there is a unique maximal subgroup of $G$ containing $T$.*

The restricted structure of minimal parabolic groups allows us to prove a Local $C^{**}(G,T)$-Theorem that is of interest on its own:

**Theorem 3. (Local $C^{**}(G,T)$-Theorem for Minimal Parabolic Groups)** *Let $G$ be a minimal parabolic group of characteristic $p$ such that $G \neq C^{**}(G,T)$, and let $V := \Omega(Z(O_p(G)))$ and $\overline{G} := G/C_G(V)$. Then there exist subgroups $E_1,\dots,E_r$ of $G$ such that*

(a) $\overline{G} = \overline{J(G)T}$ *and* $\overline{J(G)} = \overline{E}_1 \times \cdots \times \overline{E}_r$,
(b) $\overline{T}$ *acts transitively on* $\{\overline{E}_1,\dots,\overline{E}_r\}$,
(c) $V = C_V(\overline{E}_1 \times \ldots \times \overline{E}_r)\prod_{i=1}^{r}[V,E_i]$, *with* $[V,E_i,E_j]=1$,
(d) $\overline{E}_i \cong SL_2(p^n)$ *or* $p=2$ *and* $\overline{E}_i \cong S_{2^n+1}$, *for some* $n\in\mathbb{N}$, *and*
(e) $[V,E_i]/C_{[V,E_i]}(E_i)$ *is a natural module for* $E_i$.

## References


[1] M. Aschbacher, A Factorization Theorem for 2-constrained Groups, Proc. LMS(3) 43 (1981), 450–477.

[2] U. Meierfrankenfeld, B. Stellmacher, G. Stroth, Finite groups of local characteristic $p$: an overview, Groups, combinatorics and geometry, Durham 2001, 155–192, World Sci. Publishing, River Edge, NJ, 2003.

[3] D. Gorenstein, R. Lyons, On Aschbacher's local $C(G;T)$ theorem. Israel J. Math. 82 (1993), no. 1-3, 227–279.


## Cohomology decompositions and sporadic geometries


Stephen D. Smith

(joint work with David J. Benson)


**Introduction.** Our main result in [BS] can be roughly stated as follows:

**Theorem 1** (Benson–Smith). *Each sporadic simple group $G$ admits a "small, simplex" decomposition of its mod-2 cohomology, over its 2-local geometry $\Delta$.*

We survey some of the history of decompositions, up to some comparatively recent technology, which make it possible to complete the proof of the result.

**Cohomology decompositions for general finite groups.** Let $G$ be *any* finite group. Let $p$ be a prime $p$ dividing the order $|G|$ of $G$; from now on *by $H^*$ we mean cohomology taken with coefficients in $\mathbf{F}_p$.*

The existence of what we are calling a cohomology decomposition (without necessarily having the "small, simplex" conditions) is not surprising:

Brown in [Bro75] introduced the complex $|\mathcal{S}_p(G)|$ of chains of nontrivial $p$-subgroups of $G$. Work of Quillen [Qui78] and then Webb [Web87, Thm. A] gives a decomposition over the cohomology of subgroups $G_\sigma$ stabilizing simplices $\sigma$:

$$(1) \qquad H^*(G) = \oplus_{\sigma\in|\mathcal{S}_p(G)|/G}\, H^*(G_\sigma)$$

We mention some potential difficulties for computing with this formula in practice:

- The poset $\mathcal{S}_p(G)$ can be very *large*, when $p$ divides $|G|$ to a high power.
- The quotient structure $|\mathcal{S}_p(G)|/G$ can be a very complicated CW-complex.

The first difficulty can often be alleviated by passing to some suitable subposet, for which the inclusion in $\mathcal{S}_p(G)$ can be shown to be a homotopy equivalence: for example the poset $\mathcal{A}_p(G)$ of nontrivial elementary abelian $p$-subgroups in Quillen [Qui78, 2.1], or the poset $\mathcal{B}_p(G)$ of nontrivial *p-radical* $p$-subgroups—$P$ satisfying $P = O_p\big(N_G(P)\big)$—in Bouc [Bou84, Cor., p. 50].

But we might also hope to further remedy both difficulties if we pass to a more specific class of groups $G$—for example, *simple* groups. We recall that the (nonabelian) simple groups are customarily described via three types:

- alternating groups $A_n (n \geq 5)$;
- groups of Lie type (defined over a finite field, of some characteristic $p$); and
- 26 sporadic groups (not fitting into any infinite family such as the above).

Among these, the groups of Lie type are regarded as the "generic" simple groups; they are suitable analogues of the real and complex matrix groups of the Lie theory.

**The model case: Lie type groups and buildings.** Tits in [Tit74] showed that each group $G$ of Lie type has a natural geometry $\Delta$, namely the simplicial complex called its *building*.

Let $p$ denote the characteristic of the field over which $G$ is defined. Quillen in [Qui78, 3.1] showed that the building $\Delta$ of $G$ is homotopy equivalent to $\mathcal{S}_p(G)$. Hence the decomposition (1) can instead be taken over $\sigma \in \Delta/G$. And this new decomposition has two very special properties: It is "small", in the sense that $\Delta$ has dimension given by one less than the Lie rank of $G$, where this dimension turns out to be minimal for the purpose of decompositions. And it is a "simplex" decomposition, in the sense that the action of $G$ on its building $\Delta$ is *flag-transitive*, so that the quotient $\Delta/G$ is just a single simplex of the indicated dimension.

These two aspects of the decomposition for Lie type groups provided specific motivation for our search for analogous decompositions for sporadic groups in Theorem 1. We will focus in particular on the 2-*local geometries* $\Delta$ for sporadic groups $G$, introduced by Ronan and Smith in [RS80], since they seem to be especially well suited for consideration of cohomology. They exhibit "simplex" decompositions, in that $G$ is flag-transitive on $\Delta$; and they are also "small"—indeed in some cases, $\Delta$ has dimension strictly less than standard general posets such as $\mathcal{A}_2(G)$ or $\mathcal{B}_2(G)$.

**Sporadics leading to the homotopy type of $\mathcal{S}_p(G)$.** The proof of Theorem 1 for 11 of the 26 sporadic groups in fact follows easily from work done during the 1980s, in a different context of the research area of groups and geometries.

To describe that deduction, we begin by recalling a particular aspect of Webb's original proof of Theorem A of [Web87]. That result gave a sufficient condition for a general $G$-complex $\Delta$ in place of $\mathcal{S}_p(G)$ to afford the decomposition of (1):

**Hypothesis 1.** *Assume for all nontrivial p-subgroups $P$ of $G$ that the fixed subcomplex $\Delta^P$ is contractible.*

In fact Webb obtained Theorem A by generalizing to $\Delta$ the Brown–Quillen result [Qui78, 4.3] showing projectivity of the *reduced Lefschetz (virtual) module* $\tilde{L}(\Delta)$ of $\Delta$, and then applying Ext-functors. We summarize this in the form:

(2) Under Hypothesis 1, $\tilde{L}(\Delta)$ is projective; and then (1) holds over $\Delta$.

When $G$ is of Lie type in characteristic $p$ and $\Delta$ is the building, the projective $\tilde{L}(\Delta)$ is the celebrated Steinberg module for $G$.

This result motivated Ryba, Smith, and Yoshiara in [RSY90] to determine which of the then-known sporadic geometries satisfied Hypothesis 1. For $p = 2$, that condition turned out to hold for the 2-local geometries $\Delta$ for 10 of the sporadic groups. The appropriate geometry for an 11th case, namely the group $Ly$ of Lyons, was not discovered until later; and the condition for it is in fact verified in the present Benson–Smith work. Thus one obtains from (2) the cohomology decompositions desired for Theorem 1 for those particular $\Delta$. This observation by Benson in some sense began our present work.

However it is probably more appropriate to mention a later approach to those cases: Smith and Yoshiara observed in [SY97] that for most $p$-local geometries, Hypothesis 1 leads to a homotopy equivalence of $\Delta$ with $\mathcal{S}_2(G)$. Thus these 11 sporadic groups are the ones whose 2-local geometry $\Delta$ lies in the homotopy type of $\mathcal{S}_2(G)$; so that the decomposition over $\Delta$ can also be deduced from that in (1).

But notice that this view also indicates the difficulty that remained in order to establish Theorem 1 for the remaining 15 sporadics: it was clearly necessary to have further methods for decompositions which apply to homotopy types *other* than the standard one for $\mathcal{S}_2(G)$.

**More general decompositions from homotopy theory.** Decompositions have also been studied by homotopy theorists, at the underlying topological level of the classifying space $BG$ of $G$. Much of this work has been analyzed in a unified setting by Dwyer; see e.g. [Dwy01].

We first sketch Dwyer's viewpoint on Webb's formula (1) for general $\Delta$, the type of decomposition used in the statement of Theorem 1. The Borel construction on $\Delta$ appearing in Webb's approach to decompositions in [Web91] is instead regarded as $\underrightarrow{\mathrm{Hocolim}}_{\sigma \in \Delta/G} BG_\sigma$, using the *homotopy colimit* construction of Bousfield and Kan [BK72]. Since the stabilizer $G_\sigma$ is the normalizer $N_G(\sigma)$, this colimit is called the *normalizer decompsition*. When it gives an isomorphism in cohomology with that of $BG$, the decomposition is called *ample*. When in addition the spectral sequence associated to the homotopy colimit collapses, the decomposition is called *sharp*—and Webb's formula (1) holds over $\Delta$.

We go a step beyond Dwyer's analysis: the *p-completion* of a space is another construction of Bousfield and Kan in [BK72], which takes a mod-$p$ cohomology isomorphism, and produces a homotopy equivalence at the level of completions. So using this language, we can now add to our earlier statement of Theorem 1 some further content at the level of the underlying topological spaces:

- The normalizer decomposition for those sporadic $\Delta$ is ample and sharp.
- The 2-completion of that homotopy colimit is homotopy equivalent to $BG^{\wedge}_2$.

The latter provides an explicit construction of the 2-completed classifying space $BG^{\wedge}_2$—and it is standard that $BG^{\wedge}_p$ affords exactly the mod-$p$ cohomology of $G$.

We move on to the work on other decompositions from homotopy theory:

The work of Jackowski and McClure in [JM92] is based on $\mathcal{A}_p(G)$—but they use a more complicated category than just the poset, involving among the morphisms also the $G$-conjugations. In this viewpoint the relevant stabilizers are not normalizers but centralizers, and so they use the *centralizer decomposition* $\underrightarrow{\text{Hocolim}}_{E\in\mathcal{A}_p(G)/G} BC_G(E)$—which they show is ample and sharp. They also showed that the same holds for a subposet which we call $\mathcal{E}_p(G)$; this poset may be proper and determine a homotopy type distinct from that of $\mathcal{A}_p(G)$. Because of the more complicated category, the sharpness of the centralizer decomposition does not give a formula as simple as Webb's alternating sum for the normalizer decomposition. However, the latter is still available, in view of the following piece of recent technology; among the results of Grodal and Smith in [GS] is:

(3) The normalizer decomposition for $\mathcal{E}_p(G)$ is ample and sharp.

Benson in [Ben94] observed that the relevant condition for a proper subposet $\mathcal{E}_2(G)$ holds for the Conway sporadic group $Co_3$. This observation was in effect the beginning of our work in establishing Theorem 1 for the remaining 15 sporadic groups which do not lead to the homotopy type of $\mathcal{S}_2(G)$.

The work of Jackowski, McClure, and Oliver in [JMO92a, JMO92b] is instead based on $\mathcal{B}_p(G)$. They also consider a more complicated category, with objects given by $G$-orbits of form $G/H$ for $H \in \mathcal{B}_p(G)$, and further morphisms corresponding to coset translations. The stabilizers here are not normalizers but just subgroups, such as $H$ for the orbit $G/H$; and so they use the *subgroup decomposition* $\underrightarrow{\text{Hocolim}}_{H\in\mathcal{B}_p(G)/G} BH$—which they show is ample and sharp. Later Dwyer in [Dwy97, 8.10] established the same for the subposet $\mathcal{B}^{cen}_p(G)$ of members $P$ which are *p-centric*; that is, $P$ contains all $p$-elements of $C_G(P)$. Often this subposet is proper, and determines a different homotopy type than that of $\mathcal{B}_p(G)$. Again the sharpness of the subgroup decomposition does not give a simple alternating sum as in the normalizer decomposition. But again, the latter is still available by virtue of more recent technology; among the results of Grodal in [Gro02] is:

(4) The normalizer decomposition for $\mathcal{B}^{cen}_p(G)$ is ample and sharp.

**Sporadics leading to other homotopy types.** We now summarize the process of establishing Theorem 1 for the remaining 15 sporadic groups: we show that the 2-local geometry $\Delta$ is homotopy equivalent either to $\mathcal{E}_2(G)$ or to $\mathcal{B}^{cen}_2(G)$.

The necessary background information about the posets $\mathcal{A}_2(G)$ and $\mathcal{B}_2(G)$, at least for the larger sporadic groups $G$, had not been available until rather recently: The work of Meierfrankenfeld and Shpectorov [MS] completed the description of the local subgroups on the Monster and Baby Monster; this was used by Yoshiara in [Yos] to determine $\mathcal{B}_p(G)$ for several remaining sporadics.

We show that for 6 of the sporadics, the 2-local geometry $\Delta$ is homotopy equivalent to $\mathcal{E}_2(G)$; for them we obtain Theorem 1 by (3).

Similarly for 11 of the sporadics, we show that the 2-local geometry is homotopy equivalent to $\mathcal{B}_2^{cen}(G)$; for them we obtain Theorem 1 by (4).

(Our numbers add up to 11 + 6 + 11 = 28 rather than 26—since two of the sporadic groups fall into the intersection of the two above categories: that is, for them the homotopy types of $\mathcal{E}_2(G)$ and $\mathcal{B}_2^{cen}(G)$ agree.)

## References


[AMM91] A. Adem, J. Maginnis, and R. J. Milgram, *The geometry and cohomology of the Mathieu group $M_{12}$*, J. Algebra **139** (1991), 90–133.

[Ben94] D. J. Benson, *Conway's group $Co_3$ and the Dickson invariants*, Manuscripta Math. **85** (1994), 177–193.

[BK72] A. K. Bousfield and D. M. Kan, *Homotopy limits, completions and localizations*, Lec. Notes in Math., vol. 304, Springer-Verlag, Berlin/New York, 1972.

[Bou84] S. Bouc, *Homologie de certains ensembles ordonnés*, Comptes Rendus Acad. Sci. Paris, Série I **299** (1984), 49–52.

[Bro75] K. S. Brown, *Euler characteristics of groups: the p-fractional part*, Inv. Math. **29** (1975), 1–5.

[BS] David J. Benson and Stephen D. Smith, *Homotopy decompositions and 2-completed classifying spaces for sporadic simple groups*, In preparation, March 2003; expect soon to post web preprint...

[Bue79] F. Buekenhout, *Diagrams for geometries and groups*, J. Combin. Theory Ser. A **27** (1979), no. 2, 121–151.

[Dwy97] W. G. Dwyer, *Homology decompositions for classifying spaces of finite groups*, Topology **36** (1997), 783–804.

[Dwy01] ———, *Classifying spaces and homology decompositions*, Homotopy theoretic methods in group cohomology (W. G. Dwyer and H.-W. Henn, eds.), Advanced Courses in Mathematics—CRM Barcelona, Birkhäuser Verlag, Basel, 2001, pp. 3–53.

[Gro02] J. Grodal, *Higher limits via subgroup complexes*, Ann. of Math. **155** (2002), 405–457.

[GS] J. Grodal and S. D. Smith, *Propagating sharpness of group homology decompositions*, to appear 2005? in *Adv. in Math.*; posted at arXiv as math.AT/0402270.

[JM92] S. Jackowski and J. E. McClure, *Homotopy decomposition of classifying spaces via elementary abelian subgroups*, Topology **31** (1992), 113–132.

[JMO92a] S. Jackowski, J. E. McClure, and R. Oliver, *Homotopy classification of self-maps of BG via G-actions, I*, Annals of Math. **135** (1992), 183–226.

[JMO92b] ———, *Homotopy classification of self-maps of BG via G-actions, II*, Annals of Math. **135** (1992), 227–270.

[MS] U. Meierfrankenfeld and S. Shpectorov, *Maximal 2-local subgroups of the Monster and Baby Monster*, submitted; preprint available from author.

[Qui78] D. G. Quillen, *Homotopy properties of the poset of nontrivial p-subgroups of a finite group*, Adv. in Math. **28** (1978), 101–128.

[RS80] M. A. Ronan and S. D. Smith, *2-local geometries for some sporadic groups*, The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)

(Providence, R.I.), Proc. Symp. Pure Math., vol. 37, Amer. Math. Soc., 1980, pp. 283–289.

[RSY90] A. J. E. Ryba, S. D. Smith, and S. Yoshiara, *Some projective modules determined by sporadic geometries*, J. Algebra **129** (1990), 279–311.

[SY97] S. D. Smith and S. Yoshiara, *Some homotopy equivalences for sporadic geometries*, J. Algebra **192** (1997), 326–379.

[Tit74] J. Tits, *Buildings of Spherical Type and Finite BN-Pairs*, Lec. Notes in Math., vol. 386, Springer-Verlag, Berlin/New York, 1974.

[TW91] J. Thévenaz and P. Webb, *Homotopy equivalence of posets with a group action*, J. Combin. Th. A **56** (1991), 173–181.

[Web87] P. J. Webb, *A local method in group cohomology*, Comment. Math. Helv. **62** (1987), 135–167.

[Web91] ———, *A split exact sequence of Mackey functors*, Comment. Math. Helv. **66** (1991), 34–69.

[Yos] S. Yoshiara, *Radical 2-subgroups of the monster and baby monster*, submitted; preprint available from author.

## Property $\tau$ for $\mathrm{SL}_d(\mathbb{Z}[x])$, $d \geq 3$

Nikolay Nikolov

(joint work with Martin Kassabov)

Let $G$ be a discrete group generated by a finite set $S$. Let $\rho : G \to U(\mathcal{H})$ be a unitary representation of the group $G$. A vector $v \in \mathcal{H}$ is called an $\epsilon$-invariant vector (for $S$) iff $||\rho(s)v - v|| < \epsilon ||v||$ for all $s \in S$.

**Definition.** *The group $G$ has the Kazhdan property* T *if there is $\epsilon > 0$ such that every irreducible unitary representation $\rho : G \to U(\mathcal{H})$ on a Hilbert space $\mathcal{H}$, which contains an $\epsilon$-invariant vector for $S$ is isomorphic to the trivial representation. The largest $\epsilon$ with this property is called the* Kazhdan constant *for $S$ and is denoted by $\mathcal{K}(G; S)$.*

Property $T$ depends only on the group $G$ and does not depend on the choice of the generating set $S$, however the Kazhdan constant depends also on $S$.

Property $T$ implies certain group theoretic conditions on $G$ (finite generation, FP, FAB etc) and can be used for construction of *expanders* from the finite images of $G$. For this last application the following weaker property $\tau$ (introduced by A. Lubotzky in [5]) is sufficient:

**Definition.** *Let $G$ be an discrete group generated by a set $S$. Then $G$ has the property $\tau$ if there is $\epsilon > 0$ such that for every nontrivial **finite** irreducible unitary representation $\rho :\ G \to U(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ and every vector $v \neq 0$ there is some $s \in S$ such that $||\rho(s)v - v|| > \epsilon ||v||$. The largest $\epsilon$ with this property is called the* $\tau$-constant *and is denoted by $\tau(G; S)$.*

Property $\tau$ is not interesting for groups which do not have many finite quotients. All the groups we are going to work with are residually finite.

Our approach to property $\tau$ is inspired by a paper by Shalom [6] which relates property $T$ to *bounded generation*. In this paper we will work only with the groups $\mathrm{SL}_d(R)$, where $d > 2$ and $R$ is a finitely generated commutative ring. The arguments can be easily generalized to any high rank Chevalley group over f.g. commutative ring $R$. It is also possible to extend some parts of the argument to 'Chevalley' groups over noncommutative rings [3].

Let $R$ be a commutative (unital) ring, and for $i \neq j \in \{1, 2, \ldots, d\}$ let $E_{i,j}$ denote the set of elementary $d \times d$ matrices $\{\mathrm{Id} + r \cdot e_{i,j} \mid r \in R\}$. Also set $E = E(R) = \bigcup_{i \neq j} E_{i,j}$ and let $\mathrm{EL}(d; R)$ be the subgroup in $\mathrm{GL}_n(R)$ generated by $E(R)$. By a result of Suslin we have that $\mathrm{SL}_d(R) = \mathrm{EL}(d; R)$ in the case of $d \geq 3$ and $R = \mathbb{Z}[x_1, \ldots, x_k]$.

**Definition.** *The group $G = \mathrm{EL}(d; R)$ is said to have bounded elementary generation property if there is a number $N = BE_d(R)$ such that every element of $G$ can be written as a product of at most $N$ elements from $E(R)$.*

Examples of $R$ satisfying the above definition are rings of integers $\mathcal{O}$ in number fields $K$ (for $d \geq 3$), see [1]. In this classical case this property is known as *bounded generation* because each group $E_{i,j} \simeq (\mathcal{O}, +)$ is a product of finitely many cyclic groups.

The following theorem was proved in [6] and the method of its proof forms the basis of our results.

**Theorem 1.** *Suppose that $d \geq 3$, $R$ is a $k$-generated commutative ring such that $\mathrm{SL}_d(R) = \mathrm{EL}(d; R)$ has bounded elementary generation property. Then $\mathrm{SL}_d(R)$ has property* T *(as a discrete group). Moreover the Kazhdan constant $\mathcal{K}(G, S)$ is bounded from bellow by*

$$\mathcal{K}(G, S) \geq \frac{1}{BE_d(R) 22^{k+1}},$$

*for a specific generating set $S$ (defined below).*

The generating set $S$ in Theorem 1 is defined as follows: Suppose that the ring $R$ is generated by 1 and $\alpha_1, \ldots, \alpha_k \in R$. Then $S = S_{d,k} := F_1 \cup F_2$, where $F_1 = \{\mathrm{Id} \pm e_{i,j}\}$ is the set of $2(d^2 - d)$ unit elementary matrices, and

$$F_2 = \{\mathrm{Id} \pm \alpha_l \cdot e_{i,j} \mid |i - j| = 1, 1 \leq l \leq k\},$$

is the set of $4(d-1)k$ elementary matrices with generators of the ring $R$ next to the main diagonal.

A very interesting conjecture is whether the group $G_{d,1} := \mathrm{SL}_d(\mathbb{Z}[x])$ has bounded elementary generation property. In view of Theorem 1 this would imply that $G_{d,1}$ (and therefore all of its images which include $\mathrm{SL}_d(\mathcal{O})$ for many rings of algebraic integers $\mathcal{O}$[1]) has property $T$.

[1]Property $T$ for each of the groups $\mathrm{SL}_d(\mathcal{O})$ is known, but the Kazhdan constants depend on the discriminant of the ring $\mathcal{O}$. Property $T$ of $\mathrm{SL}_d(\mathbb{Z}[x])$ would give a uniform property $T$ and universal Kazhdan constant for many $\mathrm{SL}_d(\mathcal{O})$.

We are unable to say anything about property $T$, but we shall prove that $G_{d,1}$ at least has $\tau$. More generally:

**Theorem 2.** *Let $d \geq 3$, $k \geq 0$ and denote the ring $\mathbb{Z}[x_1, \ldots, x_k]$ by $R_k$. Then the group $G_{d,k} := \mathrm{SL}_d(R_k)$ has property $\tau$.*

*Moreover we have the following explicit bound for the $\tau$-constant $\tau(G_{d,k}; S)$ with respect to the generating set $S_{d,k}$ as above:*

$$\tau(G_{d,k}; S) > \frac{1}{(2d^2 + 18k + 30)\, 22^{k+1}}$$

It is a deep theorem proved by Suslin that the group $G_{d,k}$ is generated by the set $S_{d,k}$.

Let $\widehat{G}_{d,k}$ be the profinite completion of $G_{d,k}$ and define the *pro-elementary subgroup* $\widehat{E}_{i,j}$ to be the closure of $E_{i,j}$ in $\widehat{G}_{d,k}$. Each $\widehat{E}_{i,j}$ is isomorphic to the additive group of the profinite completion $\widehat{R}$ of the ring $R$.

We prove

**Theorem 3.** *The profinite completion $\widehat{G}_{d,k}$ is 'boundedly pro-elementary' generated: it is a finite product of the groups $\widehat{E}_{i,j}$.*

*In fact $\widehat{G}$ can be written as a product of at most $(3d^2 - d - 2)/2 + 18(k + 2)$ pro-elementary subgroups $\widehat{E}_{i,j}$ in some fixed order.*

In order to prove this Theorem we use the bounded elementary generation property of $\mathrm{SL}_d$ over a finite ring, and the following result which may be of independent interest:

**Theorem 4.** *Let $\bar{R}$ be a finite commutative ring generated by $k$ elements. Then every element of $K_2(\bar{R})$ is a product of at most $k + 2$ Steinberg symbols $\{a, b\}$.*

Once Theorem 3 has been proved, the general techniques from [6] are applied to prove that $\widehat{G}$ has property $T$. As noted above this gives that $G$ has property $\tau$.

Most of the known examples of discrete finitely generated groups $G$ with property $\tau$ arise as lattices in higher rank semi-simple Lie groups. In particular they have property $T$ and 'rigidity' (even super-rigidity): their representation theory is controlled by the representations of the ambient Lie group. There are also many examples of 'randomly presented' hyperbolic groups with property $T$, e.g. [2, 7], but it is not known if their profinite completion is infinite.

The groups $G_{d,k}$ seem to be the first residually finite 'non-arithmetic' groups with property $\tau$ discovered so far. They have infinitely (even continuously) many irreducible representations of fixed finite degree. In this light the question whether they have property $T$ is even more interesting.

Finally we remark that Theorem 2 gives a lower bound for the $\tau$-constant which is asymptotically $d^{-2}22^{-k}$ in $d$ and $k$. However it is possible to improve this estimate to $\lambda d^{-1/2}(1 + (k/d)^{3/2})^{-1}$ for some absolute constant $\lambda > 0$, see [3].

## References

[1] D. Carter, G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$. *Amer. J. Math 105 (1983), no.3, 673–687.*

[2] M. Gromov, Random walks in random groups, *GAFA, Geom. funct. anal. 13:1 (2003), 73–148.*

[3] M. Kassabov, Universal lattices and unbounded rank expanders, `arXiv:math.GR/0502237`.

[4] D. A. Kazhdan, On the connection of the dual space of a group with the structure of its closed subgroups, *Funkcional. Anal. i Priloz. 1 (1967), 71-74.*

[5] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progr. Math. 125, Birkhäuser, Boston, 1994.

[6] Y. Shalom, Bounded generation and Kazhdan's property (T), *Publ. Math. IHES, 90 (1999), 145-168.*

[7] A. $\widehat{\text{Z}}$uk, Property T and Kazhdan constants for discrete groups, *Geom. Funct. Anal. 13, no.3, 643-670*

## A combinatorial characterization of the groups $E_6$, $F_4$, and ${}^2E_6$

Ralf Gramlich
(joint work with Kristina Altmann)

The characterization of graphs and geometries using certain configurations is a central problem in synthetic geometry. One class of such characterizations are the so-called local recognition theorems of locally homogeneous graphs. A graph $\Gamma$ is called **locally homogeneous** if $\Gamma(x) \cong \Gamma(y)$ for each pair of vertices $x, y \in \Gamma$, where $\Gamma(x)$ denotes the induced subgraph on the neighbors of $x$ in $\Gamma$. A locally homogeneous graph $\Gamma$ with $\Gamma(x) \cong \Delta$ is called **locally** $\Delta$. For some fixed graph $\Delta$ it is a natural question to ask for a classification of all graphs $\Gamma$ that are locally $\Delta$. This classification problem is called local recognition. Usually in local recognition one only studies connected graphs, because a graph is locally $\Delta$ if and only if each of its connected components is locally $\Delta$. Local recognition of graphs can be found in the literature in abundance. By way of example we refer to the local recognition of the Kneser graphs by Jonathan Hall [4] and to the classification of locally cotriangular graphs by Jonathan Hall and Ernest Shult [5].

The present paper focuses on graphs with the local structure of line-hyperline graphs of projective spaces. More precisely, as in [3], let $\mathbf{L}_n(\mathbb{F})$ denote the graph on the non-intersecting line-hyperline pairs of the projective space $\mathbb{P}_n(\mathbb{F})$, where $n$ is a, possibly infinite, cardinal number and $\mathbb{F}$ a division ring, in which two vertices are adjacent if the line of one vertex is contained in the hyperline of the other vertex and vice versa.

The graph $\mathbf{L}_n(\mathbb{F})$ can also be described group-theoretically. Let us recall that a **fundamental** $\mathrm{SL}_2(\mathbb{F})$ of $\mathrm{SL}_{n+1}(\mathbb{F})$ is defined to be a subgroup $F$ of $\mathrm{SL}_{n+1}(\mathbb{F})$ isomorphic to $\mathrm{SL}_2(\mathbb{F})$ whose action on the natural module $V$ of $\mathrm{SL}_{n+1}(\mathbb{F})$ has a two-dimensional commutator

$$[V, F] = \{vf - v \in V \mid f \in F, v \in V\}$$

and a centralizer

$$C_V(F) = \{v \in V \mid vf = v \text{ for all } f \in F\}$$

of codimension two. There is a one-to-one correspondence between the non-intersecting line-hyperline pairs of $\mathbb{P}_n(\mathbb{F})$ and the fundamental $\mathrm{SL}_2(\mathbb{F})$'s of the group $\mathrm{SL}_{n+1}(\mathbb{F})$ by assigning a fundamental $\mathrm{SL}_2(\mathbb{F})$, say $F$, to the pair consisting of the commutator $[V, F]$ and the centralizer $C_V(F)$ of its action on the natural module $V$ of $\mathrm{SL}_{n+1}(\mathbb{F})$. Since two fundamental $\mathrm{SL}_2(\mathbb{F})$'s commute if and only if the commutator of one is contained in the centralizer of the other and vice versa, the graph $\mathbf{L}_n(\mathbb{F})$ is isomorphic to the graph on the fundamental $\mathrm{SL}_2(\mathbb{F})$'s of $\mathrm{SL}_{n+1}(\mathbb{F})$ with the commutation relation as adjacency.

It has been shown in [3] that the graph $\mathbf{L}_n(\mathbb{F})$ is locally $\mathbf{L}_{n-2}(\mathbb{F})$ (cf. Proposition 2.2 of [3]) and that, for $n \geq 8$, a connected locally $\mathbf{L}_{n-2}(\mathbb{F})$ graph is isomorphic to $\mathbf{L}_n(\mathbb{F})$, with the exception of the case $(\mathbb{F}, n) = (\mathbb{F}_2, 8)$ (cf. Theorem 1 of [3]). Up to this exception, the bound on $n$ in this result in [3] is optimal, because besides the graph $\mathbf{L}_7(\mathbb{F})$ also the graph on the fundamental $\mathrm{SL}_2(\mathbb{F})$'s of the Chevalley group $E_6(\mathbb{F})$ with the commutation relation as adjacency is connected and locally $\mathbf{L}_5(\mathbb{F})$, as can be read off the extended Dynkin diagram of type $E_6$, see also [2] or [8]. We denote this graph on the fundamental $\mathrm{SL}_2(\mathbb{F})$'s of $E_6(\mathbb{F})$ by $\mathbf{E}_6(\mathbb{F})$.

Our main result is the following generalization of Theorem 1 of [3]:

**Main Theorem**
*Let $n \geq 5$ be a, possibly infinite, cardinal number and let $\mathbb{F}$ be a division ring. If $\Gamma$ is a connected, locally $\mathbf{L}_n(\mathbb{F})$ graph, then $\Gamma$ is isomorphic to $\mathbf{L}_{n+2}(\mathbb{F})$ or to $\mathbf{E}_6(\mathbb{F})$.*

The proof of the Main Theorem is based on the reconstruction of the projective space $\mathbb{P}_n(\mathbb{F})$ from an arbitrary graph $\Gamma$ isomorphic to $\mathbf{L}_n(\mathbb{F})$, cf. Section 3 of [3], and on Timmesfeld's classification [8] of groups generated by abstract root subgroups, see also [6] and [7].

(The authors realized that the reconstruction method for automorphisms that has been presented at the workshop contains a gap, so strictly speaking the Main Theorem is only proved for graphs $\Gamma$ with a sufficiently transitive group of automorphisms. Nevertheless, the authors believe the Main Theorem to be true and are currently working on a slightly different approach.)

We would like to point out that, by results by Francis Buekenhout and Xavier Hubaut [1], Jonathan Hall [4], and Jonathan Hall and Ernest Shult [5], in the thin case, where one studies graphs that are locally graphs on commuting transpositions of the symmetric group, not only graphs related to the Coxeter group of type $A_n$ or $E_6$ occur, but also a graph related to the group $\mathrm{Sp}_6(\mathbb{F}_2)$. This example occurs because of the exceptional isomorphism $\mathrm{Sym}_6 \cong \mathrm{Sp}_4(\mathbb{F}_2)$. For details the reader is referred to the literature.

Similar results for the groups of type $F_4(\mathbb{F})$ and ${}^2E_6(\mathbb{F})$ are in reach, however, one needs to work around the problem that there exist pairs of root subgroups that do not occur in a common centralizer of a fundamental $SL_2(\mathbb{F})$.

## References


[1] Francis Buekenhout, Xavier Hubaut, Locally polar spaces and related rank-3-groups, *J. Algebra* **45** (1977), 391–434.
[2] Bruce Cooperstein, Subgroups of the group $E_6(q)$ which are generated by root subgroups, *J. Algebra* **46** (1977), 355–388.
[3] Ralf Gramlich, Line-hyperline pairs of projective spaces and fundamental subgroups of linear groups, *Adv. Geom.* **4** (2004), 83–103.
[4] Jonathan Hall, A local characterization of the Johnson scheme, *Combinatorica* **7** (1987), pp. 77–85.
[5] Jonathan Hall, Ernest Shult, Locally cotriangular graphs, *Geom. Dedicata* **18** (1985), 113–159.
[6] Franz Georg Timmesfeld, Groups generated by $k$-root subgroups, *Invent. math.* **106** (1991), 575–666.
[7] Franz Georg Timmesfeld, Abstract root subgroups and quadratic action, *Adv. Math.* **142** (1999), 1–150.
[8] Franz Georg Timmesfeld, *Abstract root subgroups and simple groups of Lie type*, Birkhäuser, Basel 2001.


## Lang in Las Vegas

Arjeh M. Cohen
(joint work with Scott Murray)

An expanded version of the title reads: An effective version of Lang's theorem in Las Vegas time. It concerns joint work with Scott Murray [1].

A Las Vegas algorithm is a probabilistic algorithm that is not guaranteed to return an answer but, if it does, its answer is guaranteed to be correct. The probability that an answer is returned can approximate 1 at the cost of more computation time. Usually, the time given for a Las Vegas algorithm is the amount of computation needed for a probability of success that is at least 1/2.

Let $G$ be a connected linear algebraic group defined over $\mathbb{F}_q$, the finite field of order $q$, and denote by $F$ the corresponding Frobenius endomorphism. Lang's theorem states that the map $G \to G$, $a \mapsto a^{-F}a$ is surjective. The effective version we have in mind is: given $c \in G(q)$, find $a \in G$ such that Lang's equation $c = a^{-F}a$ is satisfied.

As a first estimate of the complexity, we establish that if $c$ has order $s$, then $a \in G(q^s)$, and this is best possible. Consequently, the algorithm will necessarily involve computations in $\mathbb{F}_{q^s}$ and, as $s = q - 1$ is conceivable, its running time cannot be expected to be polynomial in $\log(q)$. Therefore, we take $s$ to be a parameter in our running time estimates.

The reason for studying this problem is that it is crucial for many other effective problems for groups of Lie type. For instance, representatives of the conjugacy classes of maximal tori of $G(q)$, for $G$ reductive, are usually described as follows: let $T$ be a fixed split maximal torus of $G$. Then the usual representatives are $T_{F\dot{w}}(q)$, the fixed points in $T(q^s)$ of the abstract group automorphism $g \mapsto \dot{w}^{-1}g^F\dot{w}$ of $G(q^s)$, where $w$ runs over the conjugacy class representatives of $W = N_G(T)/T$ and $\dot{w}$ denotes a fixed choice of element in the inverse image of $w$ in $N_G(T)$. But

$T_{F\dot{w}}(q)$ is a subgroup of $G_{F\dot{w}}(q)$ rather than $G(q)$. Usually, this is not considered a problem as $G_{F\dot{w}}(q)$ is conjugate to $G(q)$ by Lang's theorem. But for computer implementations this is not precise enough. If $a \in G(q^s)$ satisfies $\dot{w} = a^{-F}a$, then $T_{F\dot{w}}(q)^{a^{-1}}$ is a subgroup of $G(q)$. So, solving Lang's equation leads to an explicit representative of the class of maximal tori of type $w$.

We think of $G$ as being split reductive and given by means of the Steinberg presentation, as implemented in Magma. Due to earlier work [2], we are able to go back and forth between this presentation and the standard (if any) or adjoint representation of $G$ in polynomial time. We shall use these linear representations for our algorithms.

For $G = \mathrm{GL}_n$, we have a deterministic algorithm: consider the natural representation of $G$ on $n$-dimensional space $V$. Compute $s$, the order of $c$ and determine a basis $B$ over $\mathbb{F}_q$ of the $F$-eigenspace $E := \{x \in V \otimes \mathbb{F}_{q^s} \mid x^F = xc\}$. Then the inverse $a$ of the matrix whose rows are the elements of $B$ belongs to $G(q^s)$ and satisfies Lang's equation. This algorithm is polynomial in $n, s, \log q$.

This principle also works for $G$ a classical group and use of the natural representation. Here, a canonical basis $B$ of $E$ (for instance one with respect to which the Gram matrix has a fixed form in case $G = \mathrm{Sp}$) is needed to guarantee that the matrix $a$ belongs to $G$. A complication is that $a$ may turn out to be an outer automorphism of $G$—however this obstacle is easily overcome. The algorithm is nondeterministic where the choice of $B$ is concerned; its Las Vegas time is polynomial in $s$, the Lie rank $n$ of $G$ and $\log q$.

A more unified approach (although not more efficient for the classical groups) of the principle of utilizing the $F$-eigenspace $E$ of $c$ can be achieved by considering the adjoint representation of $G$. Then canonical bases of $E$ are obtained by requiring that we have a standard Chevalley basis (where standard refers to the fact that the usual sign problem has been resolved in a unique manner). To this end, an algorithm is needed for finding a split Cartan subalgebra in $L = \mathrm{Lie}(G)(q)$. If $G = \mathrm{SL}_2$, the probability that an element $x \in L$ is such that $C_L(x)$ is a split Cartan subalgebra is $(1 - q^{-2})/2$, which leads to a simple but sound nondeterministic algorithm of Las Vegas time polynomial in $\log q$. In the general case, elements $x \in L$ are chosen at random until $H = C_L(x)$ is a Cartan subalgebra. For the algorithm to work, we need the characteristic to be odd, and sometimes even bigger than 3. By computing rational normal forms of elements from a basis of $H$, a split fundamental subalgebra $M$ of $L$, normalized by $H$ is found with high probability. This is done without extending the field. By recursion, a split Cartan subalgebra $A$ of $M$ is found, and we continue with $C_L(A)$ instead of $L$. This algorithm is Las Vegas polynomial time in the Lie rank $n$ and $\log q$. Once the split Cartan subalgebra $H$ has been found, an algorithm by Willem de Graaf can be used for finding a standard Chevalley basis.

All Las Vegas timings are polynomial in the order $s$ of $c$, the Lie rank of $G$, and $\log q$. For the asymptotic analysis we needed estimates of the proportion of elements of the Weyl group $W$ that fix a reflection in the conjugation action. We found this fraction to be at least $1/3$ for $W$ irreducible. It leads to a lower bound on the proportion of regular semisimple elements of $L$ whose centralizer normalizes a (split) fundamental subalgebra isomorphic to $\mathrm{Lie}(\mathrm{SL}_2)(q)$.

## References


[1] A.M. Cohen and S. Murray, Algorithm for Lang's Theorem, preprint, Eindhoven, 2005.

[2] A.M. Cohen, S. Murray and D. E. Taylor, Computing in groups of Lie type. Math. Comp. **73** (2004) 1477–1498.


## Finiteness properties of BN-pairs and the Curtis-Tits theorem

Peter Abramenko

### 1. Finiteness properties of twin BN–pairs

In the following, we investigate groups with a twin BN-pair, which can be considered as generalizations of spherical BN-pairs. For a definition of a twin BN-pair, see [6], Subsection 3.2.

**Examples.** Typical examples of twin BN-pairs arise from Kac–Moody groups over a field $k$ (see [6], Subsection 3.3 or [1], Example 5). As a special case, one obtains in a canonical way a twin BN-pair of rank $m+1$ of affine type in $G = \mathcal{G}(k[t,t^{-1}])$ if $\mathcal{G}$ is a simple and simply connected Chevalley group (scheme) of rank $m$. (The twin BN–pair in $G$ can also be described without any Kac–Moody theory, see [2], Section 3.) Note that $\mathcal{G}(k[t])$ is a parabolic subgroup of $\mathcal{G}(k[t,t^{-1}])$. This example generalizes to (absolutely almost) simple and simply connected isotropic $k$–groups $\mathcal{G}$ of $k$–rank $m$ and $G = \mathcal{G}(k[t,t^{-1}])$, see [6], Subsection 3.2 and [1], Section 3.1, for the explicit description of the twin BN–pair in $\mathcal{G}(k[t,t^{-1}])$ for some classical groups $\mathcal{G}$.

Having the above examples in mind, we are going to discuss some results about finiteness properties of groups with twin BN–pairs, respectively of their parabolic subgroups. By finiteness properties we here mean finite generation, finite presentation and the higher (homological) finiteness properties $FP_l$, respectively $F_l$ (which is $FP_l$ plus finite presentability in case $l \geq 2$). In the examples it's clear that one even cannot expect finite generation if the field $k$ is infinite. So one would deal with finite fields $k = \mathbb{F}_q$ in these examples, and we need to introduce the parameter $q$ in the general context of twin BN–pairs in some appropriate way.

For a group $G$ with twin BN–pair $(B_+, B_-, N)$, Weyl group $W$, distinguished set of generators $S$ of $W$ and rank–1 parabolic subgroups $P_{\epsilon,\{s\}}$, we define the parameters $q_{\min}, q_{\max} \in \mathbb{N} \cup \{\infty\}$ as follows.

$$q_{\min} = \min_{\epsilon\in\{+,-\},s\in S}[P_{\epsilon,\{s\}} : B_\epsilon] - 1, \; q_{\max} = \max_{\epsilon\in\{+,-\},s\in S}[P_{\epsilon,\{s\}} : B_\epsilon] - 1$$

**Assumption.** $q_{\max}$ is finite, and also the intersections

$$\bigcap_{g\in G} gB_+g^{-1} \text{ and } \bigcap_{g\in G} gB_-g^{-1}$$

are finite.

Under this assumption, the finiteness properties of $G$ and its parabolic subgroups are now determined by the *sphericity* of the twin BN-pair.

The twin BN–pair $(B_+, B_-, N)$ is called $n$*–spherical* (with $n \in \mathbb{N}$) if each of its parabolic subgroups of rank $\leq n$ is spherical, i. e. if an only if $W_J$ is finite for any $J \subseteq S$ of cardinality $|J| \leq n$.

**Theorem 1.** *Assume that the twin BN–pair $(B_+, B_-, N)$ is $n$–spherical and that $2^{2n-1} \leq q_{\min}$. Assume further that the Coxeter diagram of the the Coxeter system $(W, S)$ associated to the twin BN–pair does not contain any subdiagrams of type $F_4, E_6, E_7$ or $E_8$. Then any parabolic subgroup of $G$ is of type $F_{n-1}$.*
*If additionally the twin BN–pair is not $(n+1)$–spherical then any spherical parabolic subgroup of $G$ is not of type $FP_n$.*

Theorem 1 has the following corollary, which is also stated as Theorem C in Chapter III of [1]. (The special case $\mathcal{G} = SL_{n+1}$ was already treated before independently by Abels and the author.)

**Application.** Let $\mathcal{G}$ be an absolutely almost simple classical group, defined over $\mathbb{F}_q$ and of $\mathbb{F}_q$–rank $n > 0$. Assume that $2^{2n-1} \leq q$. Then $\mathcal{G}(\mathbb{F}_q[t, t^{-1}])$ and $\mathcal{G}(\mathbb{F}_q[t])$ are of type $F_{n-1}$, and $\mathcal{G}(\mathbb{F}_q[t])$ is not of type $FP_n$.

Since finite generation and finite presentation are of interest in their own right and since the corresponding proofs work under less technical assumptions in these cases, I will restate what can be proved here.

**Theorem 2.** *If the twin BN–pair $(B_+, B_-, N)$ is 2-spherical and $4 \leq q_{\min}$ then any parabolic subgroup of $G$ is finitely generated.*
*If additionally the twin BN–pair is not 3–spherical then any spherical parabolic subgroup of $G$ is not of type $FP_2$ (and so in particular not finitely presented).*

**Counter–Example 1.** It is somewhat surprising that the parameter $q_{\min}$ does matter in this context. In fact, one can prove that certain Kac–Moody groups of compact hyperbolic type of rank 3 over the fields $\mathbb{F}_2$ and $\mathbb{F}_3$ have proper parabolic subgroups which are **not** finitely generated.

**Theorem 3.** *If the twin BN–pair $(B_+, B_-, N)$ is 3-spherical and $7 \leq q_{\min}$ then any parabolic subgroup of $G$ is finitely presented.*
*If additionally the twin BN–pair is not 4–spherical then any spherical parabolic subgroup of $G$ is not of type $FP_3$.*

## 2. A generalization of the Curtis-Tits theorem

For the full group $G$, one can derive finite presentability under less restrictive assumptions. This follows directly from the main result proved in [4]. This result is an amalgam presentation of 2–spherical BN-pairs, which does not make use of the assumption stated in Section 1, and generalizes the classical Curtis-Tits theorem for spherical BN-pairs.

**Theorem 4.** *Let $G$ be a group with a 2–spherical twin BN-pair such that none of its rank–2 parabolic subgroups is of type $B_2(2)$, $G_2(2)$, $G_2(3)$ or ${}^2F_4(2)$. Then $G$ is the amalgam of all intersections $P_{+,\{s,t\}} \cap P_{-,\{s,t\}}$ $(s, t \in S)$ of all pairs of opposite rank–2 parabolic subgroups of $G$.*

**Corollary 5.** *If the twin BN–pair $(B_+, B_-, N)$ is 2-spherical, satisfies the assumption of Section 1 and $4 \leq q_{\min}$, then $G$ is finitely presented.*

**Counter-Example 2.** It is again surprising that the exclusion of certain "small" residues in Theorem 4 and its corollary is indeed necessary. Recent joint work of Mühlherr and the author shows that there exist Kac–Moody groups of compact hyperbolic type of rank 3 over $\mathbb{F}_2$ (and maybe also over $\mathbb{F}_3$) which are **not** finitely presented. This result emerges from the construction of non-algebraic Moufang twin buildings with root groups of order 2.

## References


[1] P. Abramenko: *Twin Buildings and Applications to S-Arithmethic Groups.* Springer LNM 1641, 1996.

[2] P. Abramenko: *Group actions on twin buildings.* Bull. Belg. Math. Soc. **3** (1996), 391 – 406.

[3] P.Abramenko: *Finiteness properties of groups acting on twin buildings* L.M.S. Lecture Notes 311 (Proceedings of a conference on Groups: Topological, combinatorial and arithmetic aspects, Bielefeld 1999), Cambridge University Press (2004), 21 – 26.

[4] P. Abramenko und B. Mühlherr: *Présentations de certaines BN-paires jumelées comme sommes amalgamées.* C. R. Acad. Sci. Paris **325**, Série I (1997), 701 – 706.

[5] J. Tits: *Uniqueness and presentation of Kac–Moody groups over fields.* J. Algebra **105** (1987), 542 – 573.

[6] *Twin buildings and groups of Kac–Moody type.* L.M.S. Lecture Notes 165 (Proceedings of a conference on groups, combinatorics and geometry, Durham 1990), Cambridge University Press (1992), 249 – 286.


# On Tits' Center Conjecture

Gerhard Röhrle


### abstract

We give a short proof of a special case of Tits' Center Conjecture using a theorem of J.-P. Serre [10] and a recent result from [1]. Precisely, we show that this conjecture holds for fixed point subcomplexes $X^H$ of the building $X = X(G)$ of a connected reductive algebraic group $G$ for $H$ a subgroup of $G$. This in turn can be viewed as a partial converse to a result by Serre, [10, Prop. 2.11].

## 1. Introduction

Let $G$ be a connected reductive linear algebraic group defined over an algebraically closed field $k$. Let $X = X(G)$ be the spherical Tits building of $G$, cf. [12]. Recall that the simplices in $X$ correspond to the parabolic subgroups of $G$ and the vertices of $X$ correspond to the maximal proper parabolic subgroups, see [10, §3.1]. The topological notions that follow all relate to the geometric realization of $X$. A subset $Y$ of $X$ is *convex* if whenever two simplices of $Y$ are not opposite in $X$, then $Y$ contains the unique geodesic joining these points, [10, §2.1]. A convex subcomplex $Y$ of $X$ is *strictly convex*, if does not contain any two opposite points of $X$, [10, §2.1]. A subcomplex $Y$ of $X$ is *contractible* if it has the homotopy type of a point, [10, §2.2]. The following is a strengthened version due to J.-P. Serre of the so-called "Center Conjecture" by J. Tits, cf. [11, Lem. 1.2], [8, §4], [10, §2.4], [13].

**Conjecture 1.1.** *Let $Y$ be a convex and contractible subcomplex of $X$. Then there is a point in $Y$ which is fixed by any automorphism of $X$ which stabilizes $Y$.*

A point whose existence is asserted in Conjecture 1.1 is sometimes referred to in the literature as a "center" of $Y$. The original formulation of the conjecture is stated for strictly convex subcomplexes $Y$ of $X$.

For an overview of special cases of Conjecture 1.1 in this original form that have been established, frequently relying on a case-by-case analysis, see [3, p. 64], [7], [8, §4], [10, §2.4], [13]; see also [4, §3.6] and [5] for related results. For instance, in [10, Prop. 2.10] Serre shows that Conjecture 1.1 holds in case $\dim Y \leq 1$ and also in case the group of automorphisms under consideration is finite and solvable.

For a subgroup $H$ of $G$ let $X^H$ be the fixed point subcomplex of the action of $H$, i.e., the subcomplex of all $H$-stable (thus $H$-fixed) simplices in $X$; the simplices in $X^H$ correspond to the parabolic subgroups of $G$ containing $H$. Thus, if $H \subseteq K \subseteq G$ are subgroups of $G$, then we have $X^K \subseteq X^H$. Observe that the subcomplex $X^H$ of $X$ is always convex, cf. [10, Prop. 3.1]. Our main result, Theorem 3.1, gives a short, conceptual proof of Conjecture 1.1 for subcomplexes of the form $Y = X^H$ for $H$ a subgroup of $G$ and the group of automorphisms of $X$ stabilizing $Y$ considered lies in $G$.

The initial motivation for Tits' Conjecture 1.1 was a question about the existence of a canonical parabolic subgroup associated with a unipotent subgroup of a Borel subgroup of $G$ (cf. [8, §4.1], [10, §2.4]). This existence theorem was ultimately proved by other means, [2, §3]. In Example 3.4 below we show that this result is a special case of Theorem 3.1.

## 2. Serre's notion of complete reducibility

Following Serre [10], we say that a (closed) subgroup $H$ of $G$ is *$G$-completely reducible* ($G$-cr) provided that whenever $H$ is contained in a parabolic subgroup $P$ of $G$, it is contained in a Levi subgroup of $P$; for an overview of this concept see for instance [9] and [10].

In the case $G = \mathrm{GL}(V)$ ($V$ a finite-dimensional $k$-vector space) a subgroup $H$ is $G$-cr exactly when $V$ is a semisimple $H$-module, so this faithfully generalizes the notion of complete reducibility from representation theory.

Following Serre [10, Def. 2.2.1], a convex subset $Y$ of $X$ is *$X$-completely reducible* ($X$-cr) if for every $y \in Y$ there exists a point $y' \in Y$ opposite to $y$ in $X$. Thanks to [10, Prop. 3.1], $X^H$ is a convex subcomplex of $X$ for any subgroup $H$ of $G$.

The following is part of a more general theorem due to Serre, [8, Thm. 2]; see also [10, §2] and [13].

**Theorem 2.1.** *Let $H$ be a (closed) subgroup of $G$ and set $Y = X^H$. Then the following are equivalent:*

(i) *$H$ is $G$-completely reducible;*
(ii) *$Y$ is $X$-completely reducible;*
(iii) *$Y$ is not contractible;*
(iv) *$Y$ has the homotopy type of a bouquet of spheres.*

*Remark* 2.2. By convention, the empty subcomplex of $X$ is not contractible.

Our next result [1, Thm. 3.10] gives an affirmative answer to a question by Serre, [9, p. 24]. The special case when $G = \mathrm{GL}(V)$ is just a particular instance of Clifford Theory. See also the abstract of Ben Martin's talk above.

**Theorem 2.3.** *Let $N \subseteq H \subseteq G$ be (closed) subgroups of $G$ with $N$ normal in $H$. If $H$ is $G$-completely reducible, then so is $N$.*

## 3. Tits' Center Conjecture for fixed point subcomplexes

Here is the main result of this note.

**Theorem 3.1.** *Let $N \subseteq H \subseteq G$ be (closed) subgroups of $G$ with $N$ normal in $H$. Suppose that $X^N$ is contractible. Then $H$ has a fixed point in $X^N$.*

*Proof.* Since $N$ is normal in $H$, the latter acts on $X^N$ (by conjugation on the set of parabolic subgroups in $X^N$). Clearly, we have $X^H \subseteq X^N$. Thus, it suffices to show that $X^H \neq \varnothing$.

Since $X^N$ is contractible, Theorem 2.1 implies that $N$ is not $G$-cr. Thus by Theorem 2.3 it follows that $H$ is not $G$-cr and again by Theorem 2.1 that $X^H$ is contractible. In particular, $X^H$ is non-empty, by Remark 2.2. Thus $H$ has a fixed point in $X^N$, as claimed. □

*Remark* 3.2. In [10, Prop. 2.11] Serre showed that Theorem 2.3 is a consequence of Tits' Center Conjecture 1.1. So, Theorem 3.1 is just the reverse implication of Serre's result 0,0cite[Prop. 2.11]serre2B in the special case when Theorem 2.3 applies, namely when the subcomplex $Y$ is of the form $Y = X^N$ for some subgroup $N$ of $G$ and the group of automorphisms of $X$ stabilizing $Y$ considered lies in $G$. Our proof of Theorem 3.1 relies on Serre's Theorem 2.1.

Observing that $Y \subseteq X^{C_G(Y)}$ for any subcomplex $Y$ of $X$ and that $C_G(Y)$ is normal in $N_G(Y)$, the following is immediate by Theorem 3.1.

**Corollary 3.3.** *Let $Y$ be a convex and contractible subcomplex of $X$. Suppose that $Y = X^{C_G(Y)}$. Then $N_G(Y)$ has a fixed point in $Y$.*

It is easy to see that every fixed point subcomplex $Y = X^H$ satisfies the condition $X^H = X^{C_G(Y)}$ of Corollary 3.3.

As indicated in the Introduction, a fundamental theorem of Borel and Tits on unipotent subgroups of Borel subgroups of $G$ [2, §3] yields a key example for Theorem 3.1.

**Example 3.4.** Let $U$ be a non-trivial unipotent subgroup of $G$ contained in a Borel subgroup $B$ of $G$. Let $Y = X^U$; so $Y$ is the subcomplex of $X$ consisting of all parabolic subgroups of $G$ containing $U$. By [10, Prop. 3.1], $Y$ is convex.

Note that $U$ is not $G$-cr; for if $U$ is contained in a Borel subgroup $B^-$ opposite to $B$, then $U$ is contained in the maximal torus $B^- \cap B$ of $G$, which is absurd. So $Y$ is contractible, by Theorem 2.1.

Thus, by Theorem 3.1, $N_G(U)$ has a fixed point in $Y$, i.e., there is a parabolic subgroup $P$ of $G$ containing $N_G(U)$, thus the simplex $s_P$ corresponding to $P$ is a "center" of $Y$.

Indeed, by a construction, due to Borel and Tits [2, §3], there exists a canonical parabolic subgroup $P$ of $G$ (depending only on $U$) such that $U \subseteq R_u(P)$ and $N_G(U) \subseteq P$.

*Remark* 3.5. Since the identity component $H^0$ of a $G$-cr subgroup $H$ of $G$ is reductive ([9, Property 4]), in view of Theorem 2.1, Theorem 3.1 applies to any non-reductive subgroup $N$ of $G$. An example due to M. Liebeck, [1, Ex. 3.45], gives an instance of Theorem 3.1 when the subgroup in $N$ question is simple.

## References


[1] M. Bate, B. Martin, G. Röhrle, *A geometric approach to complete reducibility*, Inventiones math. (to appear).

[2] A. Borel, J. Tits, *Éléments unipotents et sous-groupes paraboliques des groupes réductifs, I,* Invent. Math. **12** (1971), 95–104.

[3] D. Mumford, *Geometric Invariant Theory*, Springer Verlag 1965.

[4] B. Mühlherr, *Some contributions to the Theory of Buildings based on the Gate Property*, Dissertation Tübingen 1994.

[5] ———, *Complete reducibility in projective spaces and polar spaces*, Preprint 2004.

[6] B. Mühlherr, P. Schmid, *The extended Steinberg character*, J. Algebra **175** (1995), no. 1, 373–384.

[7] G. Rousseau, *Immeubles sphériques et théorie des invariants*, C.R.A.S. **286** (1987), 247–250.

[8] J.-P. Serre, *La notion de complète réductibilité dans les immeubles sphériques et les groupes réductifs*, Séminaire au Collège de France, résumé dans [14, pp. 93–98], (1997).

[9] ———, *The notion of complete reducibility in group theory*, Moursund Lectures, Part II, University of Oregon, 1998, `http://darkwing.uoregon.edu/~math/serre/index.html`

[10] ———, *Complète Réductibilité*, Séminaire Bourbaki, 56ème année, 2003-2004, n° 932.

[11] J. Tits, *Groupes semi-simples isotropes*, Colloq. Théorie des Groupes Algébriques, Bruxelles, 1962.

[12] ———, *Buildings of spherical type and finite BN-pairs*, Lecture Notes in Math. **386**, Springer-Verlag (1974).

[13] ______, *Quelques cas d'existence d'un centre pour des ensembles de chambres qui sont convexes, non vides et ne contiennent pas de paires de chambres opposées*, Séminaire au Collège de France, résumé dans [14, pp. 98–101], (1997).

[14] ______, *Théorie des groupes*, Résumé des Cours et Travaux, Annuaire du Collège de France, 97$^{\text{e}}$ année, (1996–1997), 89–102.

## The Exceptional Moufang Quadrangles

Richard M. Weiss

The spherical buildings of rank at least two associated to classical simple algebraic groups are classified by one of three classes of algebraic structures: anisotropic quadratic spaces, skew-fields with involution and anisotropic pseudo-quadratic spaces.

An anisotropic (skew-hermitian) pseudo-quadratic space is a set

$$(L, \sigma, X, h, \pi),$$

where $L$ is a skew-field, $\sigma$ is an involution of $L$ (i.e. $\sigma$ is an anti-automorphism whose square is the identity), $X$ is a right vector space over $L$, $h$ is a skew-hermitian form on $X$ with respect to $\sigma$ (that is:

(i) $h$ is a bi-additive map from $X \times X$ to $L$;
(ii) $h(a, bv) = h(a, b)v$;
(iii) $h(a, b)^\sigma = h(b, a)$

for all $a, b \in X$ and all $v \in L$); and $\pi$ is a map from $X$ to $L$ such that

(iv) $\pi(a + b) \equiv \pi(a) + \pi(b) + h(a, b) \pmod{L_\sigma}$;
(v) $\pi(av) \equiv v^\sigma \pi(a) v \pmod{L_\sigma}$; and
(vi) $\pi(a) \equiv 0 \pmod{L_\sigma}$ if and only if $a = 0$

for all $a, b \in X$ and all $v \in L$. Here $L_\sigma$ denotes the set

$$\{a + a^\sigma \mid a \in L\}$$

of traces with respect to $\sigma$.

A classical theorem of Dieudonné and Herstein says that if $(L, \sigma)$ is an arbitrary skew-field with non-trivial involution, then either $L_\sigma$ generates $L$ as a ring or one of two exceptional cases occurs:

(A) $L$ is a commutative field, $K := L_\sigma$ is a subfield and $L/K$ is a separable quadratic extension.
(B) $L$ is a quaternion division algebra, $\sigma$ is its standard involution and $K := L_\sigma$ is its center.

Let $(L, \sigma)$ and $K$ be as in (A) or (B), let $q(u) = u^\sigma u$ for all $u \in L$ and let

$$f(u, v) = u^\sigma v + v^\sigma u$$

for all $u, v \in L$. Then $q$ is an anisotropic quadratic form on $L$ as a vector space over $K$, $f$ is the corresponding bilinear form and $\sigma$ can be recovered from $f$ and the distinguished element 1 of $L$ by the formula

$$u^\sigma = f(u, 1) \cdot 1 - u$$

for all $u \in L$. The dual nature of these structures as both skew-fields with involution and as anisotropic quadratic spaces plays a central role in the structure of many of the exceptional groups.

Let $K$ be an arbitrary commutative field. We say that a quadratic form over $K$ is *of type* $E_\ell$ for $\ell = 6$, 7 or 8 if it is anistropic and (up to isomorphism) of the form

$$\alpha_1 N \perp \alpha_2 N \perp \cdots \perp \alpha_d N,$$

where $N$ is the norm of a separable quadratic extension $E/K$ and $d = 3$ if $\ell = 6$; $d = 4$ and $\alpha_1 \cdots \alpha_4 \notin N(E)$ if $\ell = 7$; and $d = 6$ and $-\alpha_1 \cdots \alpha_6 \in N(E)$ if $\ell = 8$. We say that a quadratic form over $K$ is *of type* $F_4$ it is is anisotropic and (up to isomorphism) of the form

$$\alpha_1 N \perp \alpha_2 N \perp q_F,$$

where $\mathrm{char}(K) = 2$ and $F$ is a subfield of $K$ containing $K^2$ regarded as a vector space over $K$ with respect to the scalar multiplication $*$ given by $t * u = t^2 u$ for all $t \in K$ and all $u \in F$; where $q_F$ is the quadratic form on $F$ over $K$ given by $q_F(u) = u$ for all $u \in F$; where $N$ is the norm of a separable quadratic extension $E/F$; and where $\alpha_1$ and $\alpha_2$ are non-zero elements of $K$ whose product lies in $F$.

The spherical buildings of rank at least two associated to exceptional simple algebraic groups are classified by one of three families of algebraic structures: alternative division algebras, quadratic Jordan division algebras of degree three (also called, more succinctly, hexagonal systems) and quadrangular algebras. Alternative division algebras arose already in the work of Ruth Moufang on projective planes, i.e. on buildings with Coxeter diagram $A_2$. They are classified as follows: Suppose that $L$ is an alternative division algebra with center $K$. In the first stage, one shows that if $L$ is not associative, then $L$ is quadratic over $K$. In the second stage, one assumes that $L$ is quadratic over some subfield $F$ of $K$ and shows that one of the following holds:

(i) $L = K$ and $x^2 \in F$ for all $x \in L$;
(ii) $L = K$ and $L/F$ is a separable quadratic extension;
(iii) $L$ is quaternion and $K = F = Z(L)$; or
(iv) $L$ is octonion and $K = F = Z(L)$.

These same four classes of algebras are those which classify buildings of type $F_4$.

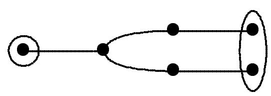
Moufang hexagons are classified by hexagonal systems. An hexagonal system is a vector space $L$ over a commutative field $K$ together with maps $T$ and $N$ from $L$ to $K$ and $u \mapsto u^\#$ from $L$ to itself which are assumed to satisfy twelve axioms. (See [2] for details.) These axioms are all satisfied in the special case that $L/K$ is a separable cubic extension, $N$ and $T$ are the norm and trace of this extension and $u^\# = N(u)/u$ for all $u \in L^*$. Like the notion of an alternative division algebra, the definition of an hexagonal system can thus be seen as a list of identities left over after basic aspects – the associative law for multiplication in the first case, the multiplication itself in the second – of a suitable classical algebraic structure are deleted. In both cases, it is geometry which guides us in the choice of identities to keep and structures to discard.

The notion of a quadrangular algebra (introduced in [3]) has an analogous relationship to the notion of an anisotropic pseudo-quadratic space over a pair $(L, \sigma)$ as in A or B above. The structure which is discarded is the multiplication on $L$. The structure of $L$ and $X$ as vector spaces over a field $K$, a $K$-bilinear map from $X \times L$ to $X$, a distinguished element 1 in $L$ and an anisotropic quadratic form $q$ on $L$ such that $q(1) = 1$ (and hence also the "involution" $\sigma$ given by $u^\sigma = f(u,1) \cdot 1 - u$ for all $u \in L$) are, however, all retained as are a number of identities.

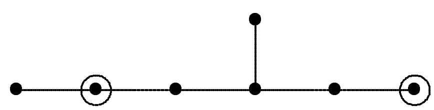
Moufang quadrangles which are not classical are classified by quadrangular algebras. The classification of quadrangular algebras is carried out in [3]. It turns out that every quadrangular algebra $\Xi$ is of one of the following four types:

(i) $\dim L = 2$ or 4 and $\Xi$ is an anistropic pseudo-quadratic space after all.

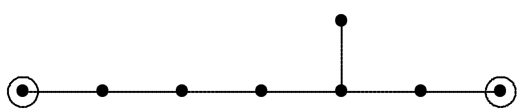
(ii) $q$ is a quadratic form of type $E_\ell$ for $\ell = 6$, 7 or 8 (as defined above) and $\Xi$ is uniquely determined by the similarity class of $q$. These are the quadrangular algebras associated with the simple algebraic groups whose indices are



,



and



.

(iii) $q$ is a quadratic form of type $F_4$ and again $\Xi$ is uniquely determined by the similarity class of $q$.

(iv) The bilinear form $f$ associated with $q$ is trivial. Also in this case we have an exact description of $\Xi$, but we omit the details here.

Now let $\Delta$ be an arbitrary Moufang building (of rank at least two). In each case $\Delta$ is defined over some field $K$ and there is a canonical notion of a $K$-*linear* element of $\mathrm{Aut}(\Delta)$. Let $G$ denote the subgroup consisting of these $K$-linear automorphisms and let $G^\dagger$ denote the subgroup of $G$ generated by all the root groups. Then $G^\dagger$ is a normal subgroup of $G$ and, except in three cases where $K$ has only two elements, $G^\dagger$ is simple. Now suppose that $\Delta$ is the Moufang quadrangle associated with a quadrangular algebra $\Xi$ of type (ii) or (iii). Tom De Medts showed in [1] that $G = G^\dagger$ if $\Xi$ is of type (iii). Suppose that $\Xi$ is of type (ii). In [4], we show that if $q$ is of type $E_6$, then there is an invariant quadratic separable extension $E/K$ and

$$G/G^\dagger \cong \mathrm{Gal}(E/K) \cdot E^*/(E^*)^3$$

and if $q$ is of type $E_7$, then there is an invariant quaternion division algebra $D$ with center $K$ and

$$G/G^\dagger \cong D^*/(D^*)^2 K^*.$$

We conjecture that $G = G^\dagger$ if $q$ is of type $E_8$, but we have only partial results pointing in this direction. If this conjecture is true, it would imply the Kneser-Tits conjecture for the corresponding form of $E_8$.

## References

[1] T. De Medts, Automorphisms of $F_4$ quadrangles, *Math. Ann.* **328** (2004), 399-418.
[2] J. Tits and R. M. Weiss, *Moufang Polygons*, Springer, 2002.
[3] R. M. Weiss, *Quadrangular Algebras*, Princeton University Press, to appear.
[4] R. M. Weiss, *Moufang quadrangles of type $E_6$ and $E_7$*, Crelle's Journal, to appear.

*Reporter: Pierre-Emmanuel Caprace*

# Participants

**Prof. Dr. Peter Abramenko**

Dept. of Mathematics
University of Virginia
Kerchof Hall
P.O.Box 400137
Charlottesville, VA 22904-4137
USA

**Prof. Dr. Michael Aschbacher**

Dept. of Mathematics
California Institute of Technology
Pasadena, CA 91125
USA

**Dr. Barbara Baumeister**

Institut für Mathematik I
Freie Universität Berlin
Arnimallee 2-6
14195 Berlin

**Prof. Dr. Francis Buekenhout**

Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

**Dr. David Bundy**

Mathematisches Seminar
Christian-Albrechts-Universität
Kiel
Ludewig-Meyn-Str. 4
24118 Kiel

**Pierre-Emmanuel Caprace**

Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

**Prof. Dr. Andrew L. Chermak**

Department of Mathematics
Kansas State University
Manhattan, KS 66506-2602
USA

**Prof. Dr. Arjeh M. Cohen**

Department of Mathematics and
Computer Science
Eindhoven University of Technology
Postbus 513
NL-5600 MB Eindhoven

**Dr. Hans Cuypers**

Department of Mathematics and
Computer Science
Eindhoven University of Technology
Postbus 513
NL-5600 MB Eindhoven

**Dr. Tom De Medts**

Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

**Prof. Dr. Bernd Fischer**

Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

**Prof. Dr. Paul Flavell**

School of Maths and Statistics
The University of Birmingham
Edgbaston
GB-Birmingham, B15 2TT

**Dr. Ralf Gramlich**

Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

**Prof. Dr. Jonathan I. Hall**

Department of Mathematics
Michigan State University
Wells Hall
East Lansing, MI 48824-1027
USA

**Dipl.-Math. Andreas Hirn**

Institut für Algebra und Geometrie
Fachbereich Mathematik u.Informatik
Universität Halle-Wittenberg
Theodor-Lieser-Str. 5
06120 Halle

**Prof. Dr. Alexander A. Ivanov**

Department of Mathematics
Imperial College London
Huxley Building
180, Queen's Gate
GB-London SW7 2BZ

**Prof. William M. Kantor**

Department of Mathematics
University of Oregon
Eugene, OR 97403-1222
USA

**Dr. Ross Lawther**

Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

**Prof. Dr. Martin W. Liebeck**

Dept. of Mathematics
Imperial College of Science
and Technology
180 Queen's Gate, Huxley Bldg
GB-London, SW7 2BZ

**Prof. Dr. Richard N. Lyons**

Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center
New Brunswick, NJ 08903
USA

**Prof. Dr. Kay Magaard**

Department of Mathematics
Wayne State University
656 West Kirby Avenue
Detroit, MI 48202
USA

**Prof. Dr. Hendrik Van Maldeghem**

Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

**Dr. Ben Martin**

Department of Mathematics
University of Canterbury
Private Bag 4800
8020 Christchurch
NEW ZEALAND

**Prof. Dr. Bernhard Mühlherr**

Universite Libre de Bruxelles
Service Geometrie,
C.P. 216
Bd du Triomphe
B-1050 Bruxelles

**Dr. Nikolay Nikolov**

New College
University of Oxford
GB-Oxford OX1 3BN

**Prof. Dr. Christopher W. Parker**

School of Maths and Statistics
The University of Birmingham
Edgbaston
GB-Birmingham, B15 2TT

**Dr. Gemma Parmeggiani**

Dipartimento di Matematica Pura
ed Applicata
Universita di Padova
Via Belzoni, 7
I-35131 Padova

**Prof. Dr. Cheryl E. Praeger**

School of Mathematics & Statistics
The University of Western Australia
35 Stirling Highway
Crawley 6009 WA
Australia

**Prof. Dr. Laszlo Pyber**

Alfred Renyi Institute of
Mathematics
Hungarian Academy of Sciences
P.O.Box 127
H-1364 Budapest

**Prof. Dr. Gerhard Röhrle**

School of Maths and Statistics
The University of Birmingham
Edgbaston
GB-Birmingham, B15 2TT

**Prof. Dr. Peter J. Rowley**

Dept. of Mathematics
UMIST (University of Manchester
Institute of Science a. Technology)
P. O. Box 88
GB-Manchester, M60 1QD

**Prof. Jan Saxl**

Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

**Prof. Dr. Dan Segal**

All Souls College
GB-Oxford OX1 4AL

**Prof. Dr. Yoav Segev**

Dept. of Mathematics
Ben-Gurion University of the Negev
Beer Sheva 84 105
ISRAEL

**Prof. Akos Seress**

Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus, OH 43210-1174
USA

**Prof. Dr. Aner Shalev**

Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

**Prof. Dr. Sergey V. Shpectorov**

Dept. of Mathematics and Statistics
Bowling Green State University
Bowling Green, OH 43403-0221
USA

**Prof. Dr. Stephen D. Smith**

Dept. of Mathematics, Statistics
and Computer Science, M/C 249
University of Illinois at Chicago
851 South Morgan
Chicago, IL 60607-7045
USA

**Prof. Dr. Ronald M. Solomon**

Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus, OH 43210-1174
USA

**Dr. Alexander Stein**

Mathematisches Seminar
Christian-Albrechts-Universität
Kiel
Ludewig-Meyn-Str. 4
24118 Kiel

**Prof. Dr. Bernd Stellmacher**

Mathematisches Seminar
Christian-Albrechts-Universität
Kiel
24098 Kiel

**Prof. Dr. Gernot Stroth**

Institut für Algebra und Geometrie
Fachbereich Mathematik u.Informatik
Universität Halle-Wittenberg
06099 Halle

**Prof. Dr. Katrin Tent**

Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

**Prof. Dr. Donna M. Testerman**

Ecole Polytechnique Federale de
Lausanne
SMA - IGAT
MA-Ecublens
CH-1015 Lausanne

**Prof. Dr. Franz-Georg Timmesfeld**

Mathematisches Institut
Universität Gießen
Arndtstr. 2
35392 Gießen

**Prof. Dr. Richard M. Weiss**

Dept. of Mathematics
Tufts University
503 Boston Ave.
Medford, MA 02155
USA

**Prof. Dr. Robert A. Wilson**

School of Mathematical Sciences
Queen Mary College
University of London
Mile End Road
GB-London, E1 4NS