A very intensively studied question is the existence on an extremal code of length 72. This survey talk reports on recent progress in the study of possible automorphism groups of such a code. I will also give a construction of the extremal even unimodular lattice Γ of dimension 72 I discovered in summer 2010. The existence of such a lattice was a longstanding open problem. The construction that allows to obtain the minimum by computer is similar to the one of the Leech lattice from E_8 and of the Golay code from the Hamming code (Turyn 1967). Γ can also be obtained as a tensor product of the Leech lattice (realised over the ring of integers R in the imaginary quadratic number field of discriminant -7) and the 3-dimensional Hermitian unimodular R-lattice of minimum 2, usually known as the Barnes lattice. This Hermitian tensor product construction shows that the automorphism group of Γ contains the absolutely irreducible rational matrix group $(\mathrm{SL}_2(25)\times\mathrm{PSL}_2(7)) : 2$.

Constructive recognition of classical matrix groups in even characteristic

Heiko Dietrich

(joint work with C. R. Leedham-Green, F. Lübeck, E. A. O'Brien)

Let $G = \langle X \rangle$ be isomorphic to a classical matrix group $H = \langle \mathcal{S} \rangle \leq \mathrm{GL}(d, q)$ in natural representation, where $\mathcal{S}$ is a *nice* generating set. For example, one can efficiently write an arbitrary element of H as a word in $\mathcal{S}$. Informally, a constructive recognition algorithm constructs an *effective* isomorphism from G to H, and vice versa. An approach for doing this is to consider a generating set $\mathcal{S}' \subseteq G$ corresponding to $\mathcal{S}$, and to write the elements of $\mathcal{S}'$ as words in X. If every element of G can efficiently be written as a word in $\mathcal{S}'$, then the isomorphisms $G \leftrightarrow H$ defined by $\mathcal{S}' \leftrightarrow \mathcal{S}$ are *effective* since images can be computed readily. For example, if $g \in G$ is written as a word $w(\mathcal{S}')$ in $\mathcal{S}'$, then the image of g in H is easily determined as $w(\mathcal{S})$. Thus, instead of working in G, this allows us to work in the *nice* group H.

An interesting special case is $G = H$, where the constructive recognition problem is reduced to writing $\mathcal{S}$ as words in the given generators X. In 2009, Leedham-Green & O'Brien [4] presented a solution to this problem for odd q. Their chosen generating set $\mathcal{S}$ contains at most seven elements, and Costi [2] developed an algorithm to write $g \in G$ as a word in $\mathcal{S}$. *Practical* implementations of both algorithms are publicly available in the computer algebra system Magma [1]. The approach of Leedham-Green & O'Brien is to use a reduction to classical groups of smaller degree. These groups are constructed as subgroups of a centraliser of a *strong* involution, which can be found efficiently in G by a random search.

Now let q be even. Guralnick & Lübeck [3] showed that the proportion of elements of even order in a classical group over the field with q elements is at most $5/q$; thus a random search is not efficient to construct an involution. Moreover, the structure of involution centralisers is significantly different from those in odd characteristic. Consequently, the approach of Leedham-Green & O'Brien does not

immediately carry over to even characteristic. (We mention that Costi's algorithm also works for even characteristic.) It is the aim of this talk to describe a constructive recognition algorithm for classical matrix groups in natural representation and even characteristic. Our main result is a Las Vegas algorithm which, subject to the existence of a discrete logarithm oracle, needs $O(d^4 \log q)$ field operations. At present, we try to improve our analysis to obtain $O(d^3 \log d \log q)$. In addition, we also discuss modifications of this algorithm which allow an efficient construction of involutions in G. Implementations of our algorithms are publicly available in Magma. Our results rely on recent work of Bray, Wilson & Parker, and Praeger, Seress & Yalzinkaya.

This work contributes to the *Matrix Group Recognition Project*; its goal is to provide efficient algorithms to investigate matrix groups defined over finite fields. For an overview of this project and references to related significant results of other authors we refer to the survey articles [5, 6].

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265

[2] E. M. Costi. Constructive membership testing in classical groups. PhD thesis, Queen Mary, University of London, 2009.

[3] R. Guralnick and F. Lübeck. On p-singular elements in Chevalley groups in characteristic p. Groups and computation, III (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

[4] C. R. Leedham-Green and E. A. O'Brien. Constructive recognition of classical groups in odd characteristic. *J. Algebra*, **322** (2009), 833–881.

[5] E. A. O'Brien. Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, (Colorado), pp. 163–190. De Gruyter, Berlin, 2006.

[6] E. A. O'Brien. Algorithms for matrix groups. Groups St Andrews 2009 in Bath II, London Math. Soc. Lecture Note Series **388** (2011), 297–323.

Problems I Would Like to Solve in CGT

John Cannon

A substantial body of sophisticated algorithms have been developed in CGT over the past 40 years. With the wide availability of software packages, the techniques of CGT find wide application both within mathematics and in other areas. The growing use of CGT techniques has highlighted areas where there is a current lack of effective algorithms.

Finitely presented groups are commonplace in topology and other areas. A basic question concerns whether a given presentation defines the trivial group, a finite group or an infinite group. A second question asks for an isomorphic group with a soluble word problem. Both problems are known to be insoluble in general. However, I argue that with the current tools we can frequently solve one or both problems in the case of a particular group. I reported on two experiments. In one I constructed a program which is highly successful in proving that a group is infinite. In a second case study I applied Derek Holt's Knuth-Bendix to a large number