GENERATING SYSTEMS FOR QUASISIMPLE GROUPS WITH AN APPLICATION TO BEAUVILLE SURFACES

KAY MAGAARD

1. Generation of Quasisimple Groups

Let G be a finite group. How can we tell whether or not $\{x_1, \dots, x_{r-1}\}$ is a generating set for G?
Example: $\{(1,2),(1,2,3,4,5)\}$ is a generating set for S_5.

This example is needed to show that there exists $f(x) \in \mathbb{Q}[x]$ with Galois group S_5 and is a special case of the following

Theorem. 1. *A primitive subgroup of S_n containing a 2-cycle resp. a 3-cycle contains S_n resp. A_n.*

We remark that stronger versions of this theorem exist. The main point of the theorem is to guarantee generation of the primitive subgroup provided it contains elements from a certain conjugacy class of S_n.

Another other well known results is this type are

Theorem. 2. *If $G = \mathrm{SL}_2(q)$, then every pair of elements (x, y), with $|x| = q-1$ and $|y| = q+1$, is a generating set for G.*

Theorem. 3. *If $G = \mathrm{SL}_n(q)$, then every pair of elements (x, y), with x a transvection and y an element of order $(q^n-1)/(q-1)$ (the norm 1 part of a Singer cycle), is a generating set for G.*

Along the same lines as the theorem above is the result by McLaughlin on linear groups of characteristic two containing transvections.

Using the classification of the finite simple groups and the O'Nan Scott Theorem from Jürgen Müller's lectures, the theorem above generalizes considerably. For example

Theorem. 4. *(Guralnick-Magaard, 1995) Let G be a primitive permutation group acting on a set Ω of size n. If $x \in G$ has the property that $f(x,\Omega)_G \geq \frac{1}{2}$ then one of the following holds:*

1. *G is an affine group with regular normal subgroup N. N is elementary abelian of order 2^k and x acts as a transvection on N. In this case $f(x,\Omega)_G = \frac{1}{2}$.*

Date: September 12, 2010.

(2) $F^*(G) = A_m^r$ *and* $G \leq S_m \wr S_r$, *(*$m \geq 5$*), where the wreath product acts on* $\Omega = \Delta^r$ *and* S_m *acts on* Δ*; either* Δ *is the set of* k*-subsets of* $\{1, \dots, m\}$, *(*$k < \frac{m}{2}$*) and* $n = \binom{m}{k}^r$, *or* $m = |\Delta| = 6$ *and* $n = 6^r$.

(3) $F^*(G) = L^r$ *and* $G \leq L_1 \wr S_r$, *where* L_1 *is an almost simple group of type* $O_m(2)$ *with* $m \geq 7$ *or* $m = 4, 6$ *and we have* $O_4^-(2)$ *respectively* $O_6^-(2), L = soc(L_1)$, *and* $\Omega = \Delta^r$ *where* Δ *and* $x \in L_1$ *are one of the following:*

(a) $L_1 = O_{2k+1}(2)$, $k \geq 3$, Δ *is the right cosets of* $O_{2k}^-(2)$, *and* x *is a transvection. In this case* $|\Delta| = 2^{k-1}(2^k - 1)$ *and*

$$f(x, \Delta)_{L_1} = \frac{1}{2} + \frac{1}{2(2^k - 1)}.$$

(b) $L_1 = O_{2k}^+(2)$, $k/geq4$, Δ *is the set of nonsingular points in the natural module and* x *is a transvection. In this case* $|\Delta| = 2^{k-1}(2^k - 1)$ *and*

$$f(x, \Delta)_{L_1} = \frac{1}{2} + \frac{1}{2(2^k - 1)}.$$

(c) $L_1 = O_{2k}^-(2)$, $k \geq 2$, Δ *is the set of right cosets of the stabilizer of a singular point of the natural module* V *of* L_1, *and* x *is a transvection. In this case* $|\Delta| = (2^k + 1)(2^{k-1} - 1)$ *and*

$$f(x, \Delta)_{L_1} = \frac{1}{2} + \frac{1}{2(2^k + 1)}.$$

(d) $L_1 = O_8^+(2)$, Δ *is the set of right cosets of a conjugate of* $Spin_7(2) = Sp_6(2)$ *acting irreducibly on the natural module of* L_1, *and* x *is conjugate via an outer automorphism of order* 3 *to a transvection. In this case* $|\Delta| = 2^3(16 - 1) = 120$ *and*

$$f(x, \Delta)_{L_1} = \frac{1}{2} + \frac{1}{2(2^4 - 1)} = \frac{16}{30} = \frac{8}{15}.$$

Modern versions of theorems concerning the generation of classical groups, which generalize the results on $\mathrm{SL}_n(q)$ stated above, are based on the Aschbacher's characterization of the maximal subgroups of classical groups as we well as the classification of the finite simple groups. We mention here that Aschbacher's characterization of maximal subgroups and the classification of the finite simple groups form the basis for the constructive recognition algorithms that were mentioned to during the conference. The following is an example. For a linear group G acting on a vector space $V = \mathbb{F}_q^d$ define $\nu_G(V)$ to be the minimum over all for $g \in G \setminus Z(G)$ and $\lambda \in \mathbb{F}_q$ of $\dim([\lambda g, V])$.

Theorem. 5. *If* G *is a linear group acting primitively and tensor indecomposably on a vector space* $V = \mathbb{F}_q^d$, *then either* $\nu_G(V) > \max\{2, \sqrt{d}/2\}$ *or*

(1) G *is classical,*

(2) G *is an alternating or symmetric group and* V *is the reduced permutation module,*

(3) $F^*(G) = U_5(2)$, $\dim(V) = 10$ *and* $(q, 2) = 1$.

Another example is a the theorem of Guralnick, Penttila, Praeger and Saxl, on linear groups with orders having certain large prime divisors, [14]. If $V = \mathbb{F}_q^d$, then $\mathrm{GL}(V)$ contains a unique conjugacy class of elements σ_e^G of order $q^e - 1$ and $\dim(C_V(\sigma_e)) = d - e$. By Zsigmondy's theorem there exist a prime divisor of $q^e - 1$ which does not divide q^{e-i} for any $0 < i < e$ (unless $q = 2$ and $e = 6$). In their main theorem they classify the maximal subgroups of classical groups containing elements of Zsigmondy prime order $q^e - 1$ and $\dim(C_V(\sigma_e)) = d - e$ and $e > d/2$.. Their theorem was later strengthened by Bereczky [6], however the statement of both theorems is too long to be presented here. The main point of the theorems is that the set of overgroups of elements with large prime divisors is limited and can be described.

2. Riemann Surfaces, Automorphisms and Triangle Groups

In his lecture series Prof. Jones explained how equivalence classes of homomorphic images of Fuchsian groups are in one to one correspondence with covers on Riemann surfaces. In this section we adopt a slightly different, perhaps a more topological point of view.

Let X is a compact Riemann surface of genus $g(X)$. A meromorphic map $\phi : X \to \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ is called a *cover* of the Riemann sphere. The *degree* of ϕ is the number of preimages of a general point $p_0 \in \mathbb{P}^1$ The branch points of ϕ are $p_1, \ldots, p_r \in \mathbb{P}^1$ are points $p \in \mathbb{P}^1$ such that $|\phi^{-1}(p)| < \deg(\phi)$.

As p_0 moves around p_i, the pre-images of p_0 are permuted via some $x_i \in S_n$. This yields the following *branching data* $x_1, \ldots, x_r \in S_n$ satisfying

(1) $\prod_{i=1}^r x_i = 1$.
(2) $G = \langle x_1, \ldots, x_r \rangle$ is a transitive subgroup of S_n, the *monodromy group* of ϕ.
(3) **Riemann-Hurwitz formula**

$$2(n + g(X) - 1) = \sum_{i=1}^{r} ind(x_i),$$

where $ind(x_i) = n-$ # cycles x_i.

Conversely whenever we encounter branching data as above then we have

Theorem. 6 (Riemann's Existence Theorem)**.** *If $\sigma_1, \ldots, \sigma_r \in S_n$ satisfy*

(1) $\prod_{i=1}^r \sigma_i = 1$.
(2) *$G = \langle \sigma_1, \ldots, \sigma_r \rangle$ is a transitive subgroup of S_n.*
(3)

$$2(n + g - 1) = \sum_{i=1}^{r} ind(\sigma_i),$$

then there exists a Riemann surface Y of genus g and a covering map $\Sigma :\ Y \to \mathbb{P}^1$ whose branching data is given by $\sigma_1, \ldots, \sigma_r$.

If in the setup above $r = 3$ then the resulting monodromy group is a homomorphic image of a triangle group.

We note that Riemann's existence theorem does not imply the uniqueness of Y or the covering map. In fact the moduli space of equivalence classes of G-covers $Y \to \mathbb{P}^1$ with branching data $(\sigma_1, \ldots, \sigma_r)$, usually called a Hurwitz space and denoted by $\mathcal{H}((\sigma_1, \ldots, \sigma_r))$, is a quasi-projective variety of dimension $r - 3$. Fried and Völklein showed that G occurs as a Galois group over $\mathbb{Q}$ with branching data $(\sigma_1, \ldots, \sigma_r)$ if and only if the corresponding Hurwitz space has a rational point. See for example Völklein's book [16] and the references therein. While it is generally not known how to find rational points in Hurwitz spaces we note that when $r = 3$ then $\mathcal{H}((\sigma_1, \ldots, \sigma_3))$ is a finite set. So when $|\mathcal{H}((\sigma_1, \ldots, \sigma_3))| = 1$ then the corresponding cover $Y \to \mathbb{P}^1$ is defined over $\mathbb{Q}$ and if also the tuple $(\sigma_1, \ldots, \sigma_3)$ is *rational* in the sense that $\chi(s_i) \in \mathbb{Q}$ for all $\chi \in \mathrm{Irr}(G)$, then there exists an extension field of $\mathbb{Q}$ with Galois group isomorphic to G. This a special case of Thompson's celebrated rigidity criterion.

Theorem. 7 (Thompson)**.** *If G is a finite group with $Z(G) = 1$ and there exists rational elements $g_1, \ldots, g_r \in G$ which generate G such that $g_1 g_2 \ldots g_r = 1$ and that whenever $h_1 \ldots h_r \in G$ generate G, $h_1 h_2 \ldots h_r = 1$ and for all i we have $h_i \in g_i^G$, then there exists an extension field of $\mathbb{Q}$ with Galois group isomorphic to G.*

To check the product one condition in Riemann's Existence Theorem the following result of Gow is extremely valuable. For G a finite simple group of Lie type of characteristic p, an element is *semisimple* if its order is relatively prime to p and is *regular semisimple element* if its centralizer in G has order relatively prime to p.

Theorem. 8 (Gow)**.** *Let G be a finite simple group of Lie type of characteristic p, and let s be a non-central semisimple element in G. Assume that R_1 and R_2 are conjugacy classes of G consisting of regular semisimple elements of G. Then there exist $x \in R_1$ and $y \in R_2$ such that $s = xy$.*

In [FMP] we extend Gow's result to quasisimple groups. The proof is almost identical to that presented by Gow in [12].This yields:

Corollary. 9. *For every finite quasisimple group of Lie type and and every integer $r \geq 3$ we have: For every $r - 1$-tuple of conjugacy classes $C_1, \ldots C_{r-1}$ of regular semisimple elements and every semisimple class C_r, there exist $x_i \in C_i$, such that $\prod_i x_i = 1$.*

3. Beauville Surfaces

Bauer, Catanese and Grunewald [1, 2, 4] have recently initiated the study of Beauville surfaces. Such surfaces are 2-dimensional complex algebraic varieties which are rigid, in the sense of admitting no deformations. These surfaces are defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers, and provide a geometric action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. By generalizing Beauville's original example [3, p.159], such surfaces can be constructed from finite groups acting on suitable pairs of algebraic curves.

Definition. 10. *Suppose that a finite group G acts by holomorphic transformations on two algebraic curves $\mathcal{C}_1$ and $\mathcal{C}_2$ of genus at least 2. Let G act diagonally on $\mathcal{C}_1 \times \mathcal{C}_2$ and assume that*

(a) *G acts effectively on $\mathcal{C}_1$ and $\mathcal{C}_2$ so that both $\mathcal{C}_1/G$ and $\mathcal{C}_2/G$ are isomorphic to the projective line and the coverings $\mathcal{C}_i \to \mathcal{C}_i/G$. $i = 1, 2$, are ramified over at most three points; and*

(b) *G acts freely on $\mathcal{C}_1 \times \mathcal{C}_2$.*

Then the surface $(\mathcal{C}_1 \times \mathcal{C}_2)/G$ is a Beauville surface of unmixed type.

Definition. 11. *Let G be a group. An* unmixed Beauville structure*, or simply a* Beauville structure *of G is a pair triples $(x_1, y_1, z_1), (x_2, y_2, z_2) \in G \times G \times G$ such that for $i = 1, 2$ the following hold.*

(1) *$G = \langle x_i, y_i, z_i\rangle$ and $x_i y_i z_i = 1$;*

(2) *$1/o(x_i) + 1/o(y_i) + 1/o(z_i) < 1$; and*

(3) *no non-identity power of x_1, y_1 or z_1 is conjugate in G to a power of x_2, y_2 or z_2.*

The Beauville structure then has type $((o(x_1), o(y_1), o(z_1)), (o(x_2), o(y_2), o(z_2)))$. *We call a group possessing a Beauville structure a* Beauville group.

Property (i) is equivalent to condition (a), with x_i, y_i and z_i representing the ramification over the three points, property (ii) is equivalent to each of the curves $\mathcal{C}_i$ having genus at least 2 (arising as a smooth quotient of the hyperbolic plane), and property (iii) is equivalent to G acting freely on the product $\mathcal{C}_1 \times \mathcal{C}_2$. Note that this last condition is always satisfied if $l_1 m_1 n_1$ is coprime to $l_2 m_2 n_2$.

A number of special cases of the conjecture were verified in [2]. Since then there have been a number of contributions towards a proof of the conjecture. The primary contributions are as follows.

- The alternating groups $\mathrm{Alt}(n)$ for $n \geq 6$ (and the symmetric groups $\mathrm{Sym}(n)$ for $n \geq 5$) were shown to be Beauville groups by Fuertes and González-Diez in [7].
- The groups $\mathrm{PSL}_2(q)$ were shown to be Beauville groups by Fuertes and Jones in [8, Section 2] (who also considered the groups $\mathrm{SL}_2(q)$) and using very different methods by Garion and Penegini in [11, Section 3.3].
- The Suzuki groups ${}^2\mathrm{B}_2(2^{2n+1})$ as well as the small Ree groups ${}^2\mathrm{G}_2(3^{2n+1})$ were shown to be Beauville groups by Fuertes and Jones in [8, Section 6].
- The groups $\mathrm{G}_2(q)$, ${}^3\mathrm{D}_4(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ were shown to be Beauville groups when q is sufficiently large by Garion and Penegini in [11, Section 3.4].

We also mention a recent article by Garion, Larsen and Lubotzky [10] in which they prove the conjecture for sufficiently large groups and a preprint by Guralnick and Malle, dated September 30, 2010, which gives an alternative proof that every non-abelian finite simple group other than A_5 is a Beauville group. We prove

Theorem. 12. *(Fairbairn, M. , Parker) With the exception of* $\mathrm{SL}_2(5)$ *and* A_5 *every finite quasisimple finite group is a Beauville group.*

We conclude with some examples of generating systems for some classes of simple groups.

The group $E_8(q)$ possesses hyperbolic triples (x_1, x_2, x_3) and (y_1, y_2, y_3) such that the order of all x_i is $\phi_{30}(q)$ and the order of all y_i is $\phi_{15}(q)$. To see this one checks that elements of orders $\phi_{15}(q)$ and $\phi_{30}(q)$ lie in a unique maximal subgroup. Next we verify the hypothesis of the lemma below to show that $E_8(q)$ has generating systems (x_1, x_2, x_3) and (y_1, y_2, y_3). These generating systems are easily seen to be a Beauville structure as $(\phi_{30}(q), \phi_{15}(q)) = 1$.

Lemma. 13. *Suppose that G is a group, $x \in G$, $Z = \langle x \rangle$ and $N = N_G(Z)$. Assume that*

(1) *N is the unique maximal subgroup of G containing Z;*
(2) *$|N/C_G(Z)| = k$, $|Z \setminus Z(G)| > \binom{k+1}{2}$;*
(3) *$x^G \cap N \subset Z$; and*
(4) *for all non-trivial $z \in Z \setminus Z(G)$, the (x^G, x^G, z^G) structure constant is non-zero.*

Then there exists $z \in Z$, such that there is a hyperbolic triple for G in $x^G \times x^G \times z^G$.

To find Beauville structures for $\mathrm{SL}_d(q)$ we recall that if $V = \mathbb{F}_q^d$, then $\mathrm{GL}(V)$ contains a unique conjugacy class of elements σ_e^G of order $q^e - 1$ and $\dim(C_V(\sigma_e)) = d - e$. Now define τ_e to be the generator of $\langle \sigma_e^g \rangle \cap SL_e(q)$. Let x_e be the element $t_e t_{d-e}$ where $[t_e, V] = C_V(t_{d-e})$ and $[t_{d-e}, V] = C_V(t_e)$. Using [14], [15] and our generalization of Gows theorem we prove a version of the following

Lemma. 14. *The triple x_a, x_b, τ_c is a hyperbolic generating system for* $\mathrm{SL}_d(q)$, *$d > 8$, provided $a, b > d/2$ and $c < \sqrt{d}/2$.*

Thus we produce roughly $d^{5/2}/8$ classes of hyperbolic generating systems. In fact we actually produce more as we can replace τ_e by elements of orders divisible by a Zsigmondy prime for $q^e - 1$. It is now easy to select two triples which form a Beauville structure. For example $(x_d, x_{d-2}^2, \tau_2^2)$ and (x_{d-1}, x_{d-3}, y^2) where y is an element of order $q - 1$ such that $\dim([y, V]) = 2$ will do and there are many others. For classical groups not equal to $\mathrm{SL}_d(q)$ we prove similar results.

Complications arise however when d is small. One such case is $\mathrm{Sp}_4(q)$ where one triple consists of semisimple elements whereas the second triple consists of a semisimple and regular unipotent elements.

References

[1] I.C Bauer, F. Catanese and F. Grunewald, Beauville surfaces without real structures, in *Geometric Methods in Algebra and Number Theory*, Progr. Math. 235, Birkhäuser Boston, Boston, 2005, 1–42.

[2] I. C. Bauer, F. Catanese and F. Grunewald, Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory, Mediterr. J. Math. 3 (2006), 121–146.

[3] A. Beauville, Surfaces algébriques complexes, *Astérisque* 54, Soc. Math. France, Paris, 1978.

[4] F. Catanese, Fibered surfaces, varieties isogenous to a product and related moduli spaces, Am. J. Math. 122 (2000), 1–44.

[5] I.C. Bauer, F. Catanese and R. Pignatelli, Complex surfaces of general type: some recent progress", in *Global Aspects of Complex Geometry*,(eds. F.Catanese et al.), 1–58 Springer (Berlin, Heidelberg) (2006).

[6] A. Bereczky, Maximal overgroups of Singer elements in classical groups, J. Algebra 234 (2000), no. 1, 187–206.

[7] Y. Fuertes and G. González-Diez, On Beauville structures on the groups S_n and A_n, Math. Z. V. 264, No. 4, 2010, 959-968.

[8] Y. Fuertes and G. Jones, Beauville surfaces and finite groups, preprint 2009, available at the time of writing from `http://arxiv.org/abs/0910.5489`.

[9] Ben Fairbairn, Kay Magaard, Christopher Parker, Generation of finite simple groups with an application to groups acting on Beauville surfaces (2010) `http://arxiv.org/abs/1010.3500`

[10] S. Garion, M. Larsen and A. Lubotzky, Beauville surfaces and finite simple groups. `http://arxiv.org/abs/1005.2316v1`.

[11] S. Garion and M. Penegini, New Beauville surfaces, moduli spaces and finite groups, preprint 2009, available at the time of writing from `http://arxiv.org/abs/0910.5402`

[12] R. Gow, Commutators in finite simple groups of Lie type. Bull. London Math. Soc. 32 (2000), no. 3, 311–315.

[13] R. Guralnick, Gunter Malle, Simple groups admit Beauville structures `http://arxiv.org/abs/1009.6183`

[14] R. Guralnick, T. Penttila, C. Praeger and J. Saxl, Linear groups with orders having certain large prime divisors, Proc. London Math. Soc. (3) 78 (1999), no. 1, 167–214.

[15] R. Guralnick and J. Saxl, Generation of finite almost simple groups by conjugates, J. Algebra 268 (2003), no. 2, 519–571.

[16] H. Völklein, Groups as Galois Groups. An Introduction. Cambridge Studies in Advanced Mathematics, 53. Cambridge University Press, Cambridge, 1996.

K.M.: School of Mathematics, University of Birmingham, Edgbaston, Birmingham B15 2TT, U.K.

E-mail address: `K.M.: k.magaard@bham.ac.uk`