Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 39 (1998), No. 2, 349-358.

$1\frac{1}{2}$-Generation of Finite Simple Groups

Alexander Stein

Institut für Algebra und Geometrie, FB Mathematik und Informatik
Martin-Luther-Universität Halle-Wittenberg
Theodor-Lieser-Straße 5, D-06099 Halle, Germany

In 1962 Robert Steinberg showed in [11], that each finite simple group of Lie-type is generated by two elements, using his generators and relations for this groups. He asked whether or not each finite simple group G can be generated by two elements, one an arbitrary nonidentity element of G. For alternating groups this was already known. Using the classification of finite simple groups we can now state:

Theorem. *Every finite simple group G can be generated by two elements, one an arbitrary nonidentity element, the other one from a fixed conjugacy class only depending on G.*

The theorem holds for large classes of finite simple groups by work of other authors such as alternating groups (Piccard [10](1946)), (Brenner and Wiegold [1](1975), [2](1980)), sporadic groups (Woldar [13](1995)) and some classical groups (Malle, Saxl and Weigel [8](1994)).

After finishing the proof we came across with a preprint due to R. Guralnick and W. Kantor [4]. They proved a much stronger theorem, which uses some hard arguments concerning the number of fixed points in some permutation representations of finite simple groups. Both papers heavily depend on the work of G. Malle, J. Saxl and T. Weigel [8], [12]. But in contrast to [4] our proof just uses elementary arguments beside the use of [8] and [12].

As the theorem obviously is equivalent to the existence of a $y \in G$ such that no whole nontrivial conjugacy class of G lies in the union of all maximal subgroups of G containing y, the argumentation is as follows:

For an element $y \in G$ all maximal subgroups of G containing y are determined. (In fact this was already done in [12] and [8].) Now one has to prove, that no whole conjugacy class of G lies in the union of these maximal subgroups. Now we are done.

The author gratefully acknowledges the support of Prof. G. Stroth.

Remark. If a conjugacy class C of G lies in a union of subgroups, there exists a conjugacy class D, which also lies in the union of these subgroups and elements of D have prime order.

Proposition 1. *Let G be a finite group and C any nontrivial conjugacy class with $< C >= G$. Then C cannot lie in the union of two proper subgroups.*

Proof. Assume false and let U, V be the subgroups with $C \subset U \cup V$. Let $C_V = C - U \subset V$ and $C_U = C - V \subset U$. The sets C_U and C_V are nonempty for otherwise C is contained in one of the proper subgroups U or V but $< C >= G$.

C_U is normalized by V because C_U is the set of all elements of C outside of V. Thus $H :=< C_U > V$ is a subgroup of G. Because C_V is nonempty and $< C_U > \triangleleft H, < C_U > \leq U$ there exist elements $x \in C_U,\ y \in C_V$, which are conjugate in G, but not in H. Thus H is a proper subgroup of G, contradicting $< C >= G$, as $C \subset H$. □

Proposition 2. *Let G be a finite group, $P_1, P_2, N_G(L)$ maximal subgroups of G which satisfy the following conditions: $L := P_1 \cap P_2$, $|N_G(L) : L| = 2$, P_1, P_2 are the only conjugates of P_1 containing L. If $\mathrm{core}_G(L) = 1$ and a conjugacy class C of elements of prime order with $< C >= G$ lies in the union of this three maximal subgroups, then G is a symmetric group and C is a class of transpositions.*

Proof. If the elements of C have odd order and C lies in $P_1 \cup P_2 \cup N_G(L)$, then C already lies in $P_1 \cup P_2$ as $|N_G(L) : L| = 2$ and $L = P_1 \cap P_2$. By Proposition 1 this is impossible. So C is a class of involutions. Let Ω be the set of all conjugates of P_1 and identify this set with natural numbers, s.t. $P_1 = 1$ and $P_2 = 2$. Because of $P_1 = N_G(P_1)$ (P_1 maximal) and $1 = \mathrm{core}_G(L) = \mathrm{core}_G(P_1)$ the operation of G on Ω is transitive and faithful. By assumption every element x of C has one of the following types:

(α): $x = (1a)(2)\ldots,\quad a \neq 1, 2,$

(β): $x = (2b)(1)\ldots,\quad b \neq 1, 2,$

(γ): $x = (12)\ldots,$

(ϵ): $x = (1)(2)\ldots$

Because of Proposition 1 there exist elements of the types $(\alpha), (\beta), (\gamma)$.

Let i be an element of type (γ) and B_1^2, B_2^1 be the orbits of $\mathrm{Stab}_1 = P_1$ resp. $\mathrm{Stab}_2 = P_2$, containing 2 resp. 1. Assume i moves a point $a \in B_1^2 - \{2\}$. By definition there is a $g \in \mathrm{Stab}_1$ with $g(1) = 1$ and $g(a) = 2$, so i^g has type $(1g(2))(2g(i(a)))\ldots$ and has none of the above types, a contradiction. So i is trivial on $B_1^2 - \{2\}$ and symmetrically trivial on $B_2^1 - \{1\}$.

Let $a \in B_1^2 - \{2\}$. Then there is an element h with $h(1) = 1$ and $h(2) = a$. Now $h^i(2) = 2$ and $h(1) = a$, so $B_1^2 \cup \{1\} = B_2^1 \cup \{2\} =: \Omega'$ is invariant under P_1, P_2, i so under $< P_1, P_2, i >= G$ but G is transitive. So $\Omega' = \Omega$ and i is a transposition. Using transitivity and generation by transpositions one gets $G \cong \Sigma_n$ for $n = |G : P_1|$. □

Proposition 3. *Let $y \in G$ and $M_i, i \in I$, be all maximal subgroups of G, containing y. For $J \subset I$ define $D_J = \bigcap_{i \in J} M_i$ and assume $D_J < D_K$ for every proper subset K of J. Let C be a conjugacy class with $C \subset \bigcup_{i \in I} M_i$ and $< C >= G$. Then there is a $x \in C$ with $G =< x, y >$.*

Proof. Assume C lies in the union of the maximal subgroups $M_i, i \in I$. Choose x_1 in C such that $l = |L| = |\{j \in I : x_1 \in M_j\}|$ is minimal. Assume $l < |I|$. Set $K = I - L$ and

$C_1 = C - \bigcup_{k\in K} M_k$. Every element $x_2 \in C_1$ lies in at least l subgroups M_j, but $j \notin K$, so $j \in L$ and $C_1 \subset D_L$. Because of $x_1 \in C_1$, C_1 is nonempty. Let $x_3 \in C_1$ and $v \in D_K$. Because $x_3^v \in C$ there exists a $j \in I$ with $x_3^v \in M_j$. Assume $j \in K$. Because $v \in D_K \leq M_j$ and $x_3 \notin M_j$ this is a contradiction. So $j \in L$ and by minimality of l x_3^v is in C_1. So D_K permutes C_1 and normalizes $N :=< C_1 >\leq D_L < G$. Set $H := ND_K$ and assume $H = G$. Then $< C_1 >= N \triangleleft H = G$, which contradicts $< C >= G$.

Because $y \in D_K < H$, H is contained in M_j for some $j \in I$. Because $x \in M_j$ it follows $j \in L$ but then $D_K \not\leq M_j$ because $D_K > D_{K\cup\{j\}} = D_K \cap M_j$. This contradiction shows, that $l = |I|$, so $C \subset D_I$, which contradicts $G =< C >$. This final contradiction shows the existence of an $x \in C$, such that $< x, y >$ never lies in a maximal subgroup of G containing y, so $< x, y >= G$. □

Alternating and sporadic groups

Lemma 1. *Let G be alternating or sporadic. Then there is a $y \in G$, such that for any $1 \neq x \in G$ a conjugate y^g exists with $G =< x, y^g >$.*

Proof. For alternating groups the theorem is a classical result. An old proof is in [10], a newer one follows for instance from Theorem 3.05 in [1] and Theorem 2.3 in [2] for even/odd degree respectively. The sporadic groups were recently handled by Woldar in [13]. □

Exceptional groups

Lemma 2. *Let G be an exceptional simple group of Lie-type. There exists a maximal abelian p'-subgroup T of order given in Table 1. T is either cyclic and then y is defined as a generator of T or $G = E_7(q)$. Every maximal subgroup of G containing T is either listed in the third column or G is one of the following groups: ${}^2F_4(2)'$, $G_2(3)$, $G_2(4)$, $F_4(2)$. In this list τ means a graph-automorphism of G, which normalizes $< y >$ (if it exists), P_1 in $E_7(q)$ means a parabolic subgroup of type $E_6(q)$ and i is an involution of $N_G(T) - T$ in case of $E_7(q)$.*

Proof. This is exactly the statement in [12] about the maximal subgroups of G containing T. The statement in [12] even holds for the case $G = F_4(3)$, ${}^2E_6(2)$ and ${}^2E_6(3)$, which one can check using the classification (as only the nonlocal case has to be checked). □

Lemma 3. *Let G be an exceptional simple group of Lie-type. There exists a conjugacy class C, such that for any $1 \neq x \in G$ there is a $y \in C$ with $< x, y >= G$.*

Proof. Let $1 \neq x \in G$. First let G be none of the exceptional cases of Lemma 2 and $G \neq E_7(q)$. By Lemma 2 there are at most two maximal subgroups containing y, so by Proposition 1 and simplicity of G there is a conjugate x^g of x with $< y, x^g >= G$, so $G =< y^{g^{-1}}, x >$. Let $G = E_7(q)$. If $q = 3^n$ let y be an element of order $(q-1)/(q-1,2)(q^6+q^3+1)$ for $n > 1$ and of order $2(3^6 - 3^3 + 1)$ if $q = 3$. If $(q-1,3) = 3$ let y be an element of order $(q+1)/(q-1,2)(q^6 - q^3 + 1)$ and if $(q+1,3) = 3$ let y be an element of order $(q-1)/(q-1,2)(q^6+q^3+1)$. By [12] such a y always exists.

G	$\|T\|$	Maximal subgroups containing T
${}^2B_2(2^{2n+1})$	$2^{2n+1}+2^{n+1}+1$	$N_G(T)$
${}^2G_2(3^{2n+1})$	$3^{2n+1}+3^{n+1}+1$	$N_G(T)$
${}^2F_4(2^{2n+1})$	$2^{4n+2}+2^{3n+2}+2^{2n+1}+2^{n+1}+1$	$N_G(T)$
$G_2(q)$	q^2-q+1	$M \cong SU(3,q).2, (M^\tau)$
${}^3D_4(q)$	q^4-q^2+1	$N_G(T)$
$F_4(q)$	q^4-q^2+1	$M \cong {}^3D_4(q).3, (M^\tau)$
$E_6(q)$	$\frac{1}{(3,q-1)}(q^6+q^3+1)$	$PSL(3,q^3).3$
${}^2E_6(q)$	$\frac{1}{(q+1,3)}(q^6-q^3+1)$	$PSU(3,q^3).3$
$E_7(q)$	$\frac{1}{(q-1,2)}(q-1)(q^6+q^3+1)$ $\frac{1}{(q-1,2)}(q+1)(q^6-q^3+1)$	$P_1, P_1^i, N_G(P_1 \cap P_1^i)$ $(\frac{q+1}{(q-1,2)}{}^2E_6(q)).2$
$E_8(q)$	$q^8+q^7+q^5-q^4-q^3+q+1$	$N_G(T)$

Table 1: Maximal subgroups of exceptional groups of Lie-type containing T

If y has order $(q+1)/(q-1,2)(q^6-q^3+1)$ there is by Lemma 2 just one maximal subgroup of G containing y, in the other case the maximal subgroups of G containing y satisfy the conditions of Proposition 2, but $G \neq \Sigma_n$. So in both cases there exists a conjugate $x^g \in G$ with $G =< y, x^g >$ and $G =< x, y^{g^{-1}} >$. So let G be one of ${}^2F_4(2)'$, $G_2(3)$, $G_2(4)$, $F_4(2)$. The first two cases one can check by computer: For a small permutation- or matrix-representation of G a set of representatives for the conjugacy classes of elements of prime order of G is calculated. (In case of $G_2(3)$ was the 7-dimensional representation over GF(3) used given by the Atlas of Modular Representations (http://for.mat.bham.ac.uk/atlas/), in case of ${}^2F_4(2)'$ a permutation representation on 1755 points given in the computer algebra system MAGMA.) The representatives can be chosen, such that any representative and a fixed $y \in G$, here both of order 13, generate G, which one checks also by computer.

In case of $G = G_2(4)$ there are by [3] exactly two subgroups of G containing an element of order 13 and by Proposition 1 the statement holds.

So $G = F_4(2)$. Let y be an element of order 17. By [9] there are two conjugacy classes of maximal subgroups divisible by 17, both isomorphic to $Sp_8(2)$, so $N_G(< y >)$ is contained in any maximal subgroup containing y, so y is contained in exactly 2 maximal subgroups. By Proposition 1 now there is an $x^g \in G$ with $G =< x^g, y >=< x, y^{g^{-1}} >$. □

Classical groups

Definition. *In the following let G be a finite simple classical group of Lie-type and y an element of the order given in Table 2. If $G = P\Omega^+(2n,q)$ and $n \geq 6$ let y be an element of the given order, which acts fixed point freely on its natural projective module. So y is chosen as in* [8].

Lemma 4. *Let M be a maximal subgroup of G containing y. Then either M is contained in Table 3 or G is one of the following groups: $PSL(2,q)$, $PSL(3,4)$, $PSL(4,2)$, $PSU(3,3)$,*

G	Conditions	$o(y)$
$PSL(n+1,q)$	n even	$(q^{n+1}-1)/((q-1)(q-1,n+1))$
	$n \geq 3$ odd	$(q^n-1)/(q-1,n+1)$
$PSU(n+1,q)$	n even,	$(q^{n+1}+1)/((q+1)(q+1,n+1))$
	$n \geq 3$ odd	$(q^n+1)/(q+1,n+1)$
$P\Omega(2n+1,q)$	$n \geq 3, q$ odd	$(q^n+1)/2$
$PSp(2n,q)$	$n \geq 2$	$(q^n+1)/(2,q-1)$
$P\Omega^+(2n,q)$	$n \geq 4$	$(q^{n-1}+1)/(2,q-1)$
$P\Omega^-(2n,q)$	$n \geq 4$	$(q^n+1)/(4,q^n+1)$

Table 2: The order of y in classical simple groups

$PSU(3,5)$, $PSU(4,2) \cong PSp(4,3)$, $PSU(4,3)$, $PSU(5,2)$, $PSU(6,2)$, $PSp(8,2)$, $P\Omega(7,3)$, $P\Omega^+(8,2)$. P_i means a stabilizer of a subspace of dimension i, N_i^ϵ means a stabilizer of a non-degenerate subspace W of dimension i, with $W^\perp$ of ϵ-type in the odd-dimensional orthogonal groups.

Proof. This is Theorem 1.1 in [8]. □

G	type of maximal subgroup	conditions
$PSL(n+1,q)$	$GL(\frac{n+1}{k},q^k).k$	k prime, $k\|n+1$, n even
	P_1, P_n	n odd, $n \geq 3$
$PSU(n+1,q)$	$GU(\frac{n+1}{k},q^k).k$	k prime,$k\|n+1$, n even
	N_1	$n \geq 3$ odd
$P\Omega(2n+1,q)$	N_1^-	$n \geq 3, q$ odd
$PSp(2n,q)$	$Sp(\frac{2n}{k},q^k).k$, $GU(n,q).2$	qn odd,k prime, $k\|n$,$n>2$
	$Sp(\frac{2n}{k},q^k).k$	q odd,k prime, $k\|n$,$n \geq 2$ even
	$Sp(\frac{2n}{k},q^k).k$, $O^-(2n,q)$	q even,k prime, $k\|n$,$n \geq 2$
$P\Omega^+(2n,q)$	N_2^-, $GU(n,q).2$	$n \geq 6$, even
	N_2^-, $O_n(q^2).2$	$n \geq 5$ odd
	$(N_2^-)^{\tau^k}$, $N_1^{\tau^k}$	$n=4$, τ some triality
$P\Omega^-(2n,q)$	$O^-(\frac{2n}{k},q^k)$, $GU(n,q).2$,	k prime, $k\|n$, $n \geq 4$ even,
	$O^-(\frac{2n}{k},q^k)$	k prime, $k\|n$, $n>4$ odd

Table 3: The maximal subgroups of classical simple groups containing y

Lemma 5. *Let G be a finite simple group of type $PSL(n,q)$, $PSU(n,q)$, $P\Omega(2n+1,q)$, $P\Omega^-(2n,q)$ or $P\Omega^+(4m+2,q)$ and y as defined or y of order $(q+1)/(q-1,2)$ in case $PSL(2,q)$. Then for any $1 \neq x \in G$ there is a conjugate y^g, such that $G = <x, y^g>$.*

Proof. First let G be one of $U_5(2)$, $P\Omega(7,3)$, $PSL(3,4)$ or any classical simple group not in the list of exceptions of Lemma 4. By [8], theorems 2.1, 2.2, 2.4, 2.5 and 2.6 there is a $z \in G$, such that $G = \{y^g z^h | g, h \in G\} \cup \{1\}$. So $x = y^g z^h$ for some $g, h \in G$. The order of z is given in Table 4. So one can show, using Lemma 4 or [3] in case of the exceptions of Lemma 4, that $G =< y, z^h >$ for any $h \in G$. Because $z^h \in< x, y^g >$ and $< y^g, z^h >= G$ also $< x, y^g >= G$. So let G one of the exceptions of Lemma 4 not handled above. If G is of type $PSL(2, q)$, the maximal subgroups of G containing y are very well known. In case $q \neq 4, 7, 9$ the only maximal subgroup containing y is a dihedral subgroup of order $(2, q)(q + 1)$. In case $q = 7, 9$ there are at most two maximal subgroups of G containing y, so by Proposition 1 we are done and in case $q = 5$ the conditions of Proposition 2 are satisfied, but G is not symmetric.

In case $PSU(3, 3)$ there is by [3] exactly one maximal subgroup containing y, so we are done. The cases $PSU(3, 5)$, $PSU(4, 2)$, $PSU(4, 3)$ and $PSU(6, 2)$ could be verified using a computer, as in the case of the exceptional groups of Lie-type. (The representations used were the permutation representations on the isotropic points, given by the computer algebra system MAGMA.) The case of $PSL(4, 2) = A_8$ was already handled in Lemma 1. □

G	Conditions	$o(z)$
$PSL(n+1, q)$	n even	$(q^{n/2} + 1)/(2, q - 1)$
	$n \geq 3$ odd	$(q^{(n+1)/2} + 1)$
$PSU(n+1, q)$	n even	$(q^{n/2} + (-1)^{n/2})$
	$n \geq 3$ odd,	$(q^{(n+1)/2} + (-1)^{(n+1)/2})/(2, q - 1)$
$P\Omega(2n+1, q)$	$n \geq 3, q$ odd	$(q^n - 1)/2$
$P\Omega^+(2n, q)$	$n > 4$ odd	$(q^n - 1)/(q^n - 1, 4)$
$P\Omega^-(2n, q)$	$n \geq 4$	$(q^{n-1} + 1)(q - 1)/(q - 1, 2)$

Table 4: The order of z in classical simple groups

Lemma 6. *Let $G = PSp(2n, q)$, $n \geq 2$ and G simple. Then for each $1 \neq x \in G$ there exists a y^g of order given in Table 2 with $G =< x, y^g >$.*

Proof. By Lemma 4 the maximal subgroups of G containing y are given in Table 3 or $G = PSp(8, 2)$ or $G = PSp(4, 3)$. The case of $PSp(4, 3)$ was checked on a computer together with the case $U_4(2)$ (note that the elements y given in Table 2 are different), in case $PSp(8, 2)$ [3] gives the maximal subgroups containing y of order 17. These are of type $O^-(8, 2)$, $PSp(4, 4).4$ and $PSL(2, 17)$.

In all cases from each of these conjugacy classes of maximal subgroups there is exactly one maximal subgroup containing y, because there is a Zsygmondy-prime r dividing $o(y)$ and each maximal subgroup containing y contains $N_G(R)$ for some $R \in \mathrm{Syl}_r(G)$. We show now, that all intersections of the maximal subgroups containing y are known and satisfy the conditions of Proposition 3.

Let $k = \mathrm{GF}(q)$ and $k \leq K = \mathrm{GF}(q^n)$. For any subfield L between k and K define subgroups of type $A(L) := Sp(2|K : L|, |L|).Gal(L/k)$, $B(L) := O^-(2|K : L|, |L|).Gal(L/k)$ in case q even and $B(L) := U(|K : L|, |L|).2Gal(L/k)$ in case qn odd. Let Π denote the set of all primes dividing n, and n_0 their product. For m dividing n denote with $k[m]$ the (unique) subfield of K of degree m over k. So in general the maximal subgroups of G containing y

are of type $A(k[r])$ and $B(k)$, where $r \in \Pi$. For a type T denote with M_T a subgroup of G containing y of type T.
Then the following holds for $\emptyset \neq \Psi \subseteq \Pi$:

(i) $\bigcap_{r\in\Psi} M_{A(k[r])} = M_{A(k[n_0|_\Psi])}$

(ii) $M_{B(k)} \cap \bigcap_{r\in\Psi} M_{A(k[r])} = M_{B(k[n_0|_\Psi])}$

(iii) The conditions of Proposition 3 are satisfied or $G = PSp(8,2)$.

Proof of the claim: Denote with D the intersection of all maximal subgroups of type A or B containing y. For (i) and (ii) we have only the inclusion " $\supseteq$ " to show, as we know by [6] that the intersection of any two overgroups of D is maximal in both of them if the inclusion " $\supseteq$ " in (i) and (ii) holds.

For fields $E \leq F$ denote with T_E^F the tracemap from F to E. Let f be a nondegenerate symplectic form on the F-space V. Then $T_E^F f$ is a nondegenerate symplectic form on the natural E-space V. This shows, that there exist subgroups of type $A(k[r])$ in G and for any $\emptyset \neq \Psi \subseteq \Pi$ there exist an embedding of groups of type $A(k[n_0|_\Psi])$ into subgroups of type $A(k[r])$ for $r \in \Psi$. But all these different embeddings lead to the same embedding into G as the equation $T_E^F T_F^H = T_E^H$ for fields $E \leq F \leq H$ holds. So we got the inclusion " $\supseteq$ " in (i).

Let q even and V be a 2-dimensional K-space with a nondegenerate orthogonal form of minus-type Q. Then $f(u,v) = T_k^K(Q(u+v) + Q(u) + Q(v))$ is a nondegenerate symplectic form on the k-space V. Also if $E \leq F$ are fields and Q is a nondegenerate orthogonal form of minus-type over the F-space V, then $T_E^F f$ is a nondegenerate symplectic form of the E-space V linked to the nondegenerate orthogonal form of minus-type $T_E^F Q$. Arguing like in the proof of (i) we get (ii).

So let qn odd. Denote with K_1 an (up to ismorphisms unique) field of degree 2 over K and k_1 the unique subfield of K_1 of degree 2 over k. Let $\lambda \in k_1$ with $\bar{\lambda} = -\lambda$. For a nondegenerate unitary form f of an F_1-space V the map $T_F^{F_1}(\lambda f)$ is a nondegenerate symplectic form of the natural F-space V. Also for a unitary form f and a subfield E_1 of F_1 the map $T_E^F f$ is a unitary form of an E_1-space. As $|K_1 : k_1| = |K : k| = n$ is odd we can show as in (i), that all probably different embeddings of subgroups of type A and B lead to the same embeddings, which shows (ii). Now by (i), (ii) and Lemma 4 holds (iii) except in case $PSp(4,3)$ and $PSp(8,2)$.

Now Proposition 3 gives us a conjugate x^g with $G =< x^g, y >=< x, y^{g^{-1}} >$.

In case $Sp(8,2)$ we have three maximal subgroups and by (ii) the maximal subgroups of type $O^-(8,2)$ and $Sp(4,4).2$ have a subgroup $O^-(4,4).2 = L_2(16).4$ in common. A small modification of Proposition 3 gives us then a conjugate x^g with $G =< x^g, y >$. (If a conjugacy class C lies in these three subgroups, the $L_2(16).4$ normalizes all elements of C outside of $O^-(8,2)$ and $Sp(4,4).2$, but all these elements lie by assumption inside of the $L_2(17)$. So we can construct a new maximal subgroup containing y, a contradiction.) □

Lemma 7. *Let $G = P\Omega^+(4m,q)$ with $m \geq 2$ and y as defined. Then for any $1 \neq x \in G$ there exists a conjugate y^g, such that $G =< x, y^g >$.*

Proof. First let $n = 2m \geq 6$. By definition y is chosen to fix no nonsingular points. (There exists a subgroup of type $O^-(2,q) \perp O^-(2n-2,q)$ inside of $O^+(2n,q)$. Take an element

y_1 of order $q+1$ inside of the $O^-(2,q)$ and y_2 of order $q^{n-1}+1$ inside of $O^-(2n-2,q)$. Then the image of y_1y_2 in $P\Omega^+(2n,q)$ fixes no point of the projective module, even for $q=3$ where y is a product of an involution acting fixed point freely on the projective points of a 2-space and an element of odd order acting irreducibly on the $2n-2$-dimensional orthogonal complement.) There are three subgroups containing y, one (M_1) of type N_2^- (stabilizer of a $2 \perp 2n-2$ decomposition of the natural projective module V) and two (M_2 and M_3) of type $\mathrm{GU}_n(q)$, conjugate under a graph automorphism. This follows from Lemma 4 together with the observation that all these maximal subgroups contain $N_G(R)$ for $R \in \mathrm{Syl}_r(G)$ for a Zsygmondy-prime r dividing $o(y)$.

Assume a nontrivial conjugacy class C of G is contained in these three subgroups. Let U be the 2-dimensional subspace of V, stabilized by y (and M_1). Let N_2^- be the set of all nondegenerate 2-subspaces of V of minus-type. Then $U^C \subset N_2^-$ is a union of orbits of M_1 on N_2^-: For let $W = U^x$ a 2-dimensional subspace with $x \in C$ and $g \in M_1$. Then $U^{g^{-1}xg} = U^{xg} = W^g$.

Let $f(u,v)$ be a unitary form on an l-dimensional vectorspace over $\mathrm{GF}(q^2)$. Then $Q(u) := f(u,u)$ is an orthogonal form over the field $\mathrm{GF}(q)$. This shows the embedding of $GU_n(q)$ into $O_{2n}^+(q)$ with n even and the following: Let $\hat{V}$ be the unitary space and V the orthogonal space. An isotropic point of $\hat{V}$ is a total singular 2-subspace of V and a nonisotropic point of $\hat{V}$ is a total nonsingular 2-subspace of V. Every orthogonal point lies in a unique unitary point and two different unitary points have no orthogonal point in common. By the action of M_2 on $\hat{V}$, we see that U is a nonisotropic point. Let C be the conjugacy class of G, contained in $M_1 \cup M_2 \cup M_3$ and $x \in C$ with $W := U^x \neq U$. So x is contained in one of the unitary groups and $W \cap U = 0$, because W and U are different unitary points. So the number $|U^C|$ is bounded by twice the number of points of an n-dimensional (unitary) space over $\mathrm{GF}(q^2)$ which is less than $s_0 := 2(q^{2n}-1)/(q^2-1)$. We will show now that no such orbit of M_1 exists: Let $U_1 = U^\perp \cap (W+U) \leq \hat{V}$. Then U_1 is a unitary point, so either a 2-dimensional total nonsingular or total singular space. But U_1 and U are orthogonal also in V. As M_1 is transitive on both the total singular and total nonsingular 2-subspaces of $U^\perp$, the orbit of M_1 containing U_1 has size at least

$$s_1 := \min\left((q^{n-1}+1)(q^{n-3}-1)(q^{2n-4}-1)/((q-1)(q^2-1))\,, 1/2q^{2n-4}(q^{n-1}+1)\right)$$

The orbit of M_1 on W has size at least s_1, because the map $z \in M_1$ mapping U_1 to $U_1^z \neq U_1$ maps W to $W^z \neq W$, as $U \perp U_1 = U+W$. By comparing s_1 and s_0 we get the contradiction, that in praxis $s_1 > s_0$, but it should be $s_1 \leq s_0$, if C is contained in the union of the three subgroups M_1, M_2, M_3.

So let $n=4$. The case $q=2$ was handled using a computer (using a permutation representation on the 135 singular points given in MAGMA), as there are more maximal subgroups containing y.

By [5] every subgroup of G containing y is conjugate (under $\mathrm{Aut}(G)$) to some subgroup of type N_1 (stabilizer of a nonsingular point) or N_2^- (stabilizer of a nonsingular O_2^--space). So let y centralize a 2-dimensional total nonsingular subspace. Let Ω be a set, on which a group G with pointstabilizer $M < G$ acts transitively and faithfully. Then the following equation holds: $|C \cap M|/|C| = |\mathrm{Fix}(x)|/|\Omega|$, where x is an element of the conjugacy class C. By the action of G on the nonsingular points and 2-spaces of minus-type, we can give an upper bound for $|\mathrm{Fix}(x)|$, which gives us an upper bound for $|M \cap C|/|C|$. We can show, that an element fixes at most $q^5 + q^2$ resp. $1/2(q^5 + q^3)$ nonsingular points (all nonsigular points of a 6-dimensional subspace of minus-type resp. all nonsigular points of a 6-dimensional space U with $\mathrm{Rad}U$ 1-dimensional) of one orbit in case q even resp. odd. The total number of nonsingular points in an orbit is $1/(2, q-1)q^3(q^4-1)$. So we get $\frac{|M \cap C|}{|C|} \leq 0.5/(q+1)$ for $q \geq 3$. We can show, that an element fixes at most $n_1 + n_2$ nonsingular 2-dimensional subspaces of minus-type, where $n_1 = (q^6-1)(q^5-1)/((q^2-1)(q-1))$ is the number of 2-spaces of a 6-dimensional space and $n_2 = (q^8-1)/(q-1)$ is the number of points of an 8-dimensional projective space. (The total number of fixed spaces is the number of centralized spaces, which are all inside an at most 6-dimensional space plus the number of fixed, but noncentralized spaces, which one can write as $< P, P^x >$, where P is a point of the 8-dimensional projective space.) The number of all 2-dimensional nonsingular subspaces of minus-type is $1/2q^6(q^4-1)(q^3-1)/(q+1)$, so we get $|M \cap C|/|C| \leq 0.08$ for $q \geq 3$ in this case. By action of a triality τ, which just permutes the conjugacy classes and the maximal subgroups, we get an upper bound of $|C \cap M^\tau|/|C|$ for every maximal subgroup of G containing y.

By the Zsygmondy-prime dividing $o(y)$ we get, that y lies in exactly one maximal subgroup of each of the three conjugacy classes of subgroups isomorphic to N_2^-. As y fixes exactly $q+1$ nonsingular points, there are at least $q+1$ maximal subgroups of type N_1 containing y. Let $y = y_1y_2 = y_2y_1$, where y_1 has order $(q+1)/(2, q+1)$ and y_2 has order $q^2 - q + 1$. There is a triality τ, which fixes y_2, as there is a $G_2(q)$, which is fixed by τ and contains an element of order $q^2 - q + 1$ and all subgroups of this order are conjugate in G by the Zsygmondy-prime. But $y_1^\tau \neq y_1$, as subgroups of order $q^2 - q + 1$ in $G_2(q) = C_G(\tau)$ are selfcentralizing. Assume y is contained in subgroups of type N_1^τ or $N_1^{\tau^2}$. Then there is a $\hat{y} \in C_G(y_2)$ with $< \hat{y} > \neq < y >$ and $\hat{y}$ fixes a nonsingular point. ($\hat{y} = y^{\tau^2}$ resp. y^τ). But this point must lie in the 2-dimensional subspace fixed by y_2. Thus the stabilizer of this point contains y and $\hat{y}$, which is impossible, as $< y >$ is selfcentralizing in this pointstabilizer. This gives us, that there are exactly $q+1$ maximal subgroups of type $N_1^{\tau^i}$. By the upper bound for $|M \cap x^G|/|x^G|$ given above we get a conjugate x^g with $G = < x, y^g > = < x, y^{g^{-1}} >$. □

Proof of the Theorem

By the classification theorem we had only the groups to consider, which were handled in Lemma 1, 3, 5, 6 and 7. □

References

[1] Brenner, J. L.; Wiegold, J.: *Two-Generator Groups I.* Michigan Math. J. **22** (1975), 53–64.

[2] Brenner, J. L.; Wiegold, J.: *Two-Generator Groups II.* Bull. Austral. Math. Soc. **22** (1980), 112–124.

[3] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A.: *Atlas of finite groups.* Oxford University Press 1985.

[4] Guralnick, R. M.; Kantor, W. M.: *Probabilistic generation of finite simple groups.* Preprint.

[5] Kleidman, P. B.: *The maximal subgroups of the finite 8-dimensional orthogonal groups* $\mathrm{P}\Omega_8^+(q)$ *and of their automorphism groups.* J. Algebra **110** (1987), 173–242.

[6] Kleidman, P. B.; Liebeck, M. W.: *The subgroup structure of the finite classical groups.* London Math. Soc. Lecture Notes Series **129**, Cambridge University Press 1990.

[7] Liebeck, M. W.; Saxl, J.: *On the orders of maximal subgroups of the finite exceptional groups of Lie-type.* Proc. London Math. Soc. (3) **55** (1987), 299–330.

[8] Malle, G.; Saxl, J.; Weigel, T.: *Generation of classical groups.* Geom. Dedicata **49** (1994), 85–116.

[9] Norton, S. P; Wilson, R. A.: *The maximal subgroups of* $F_4(2)$ *and its automorphism group.* Comm. Algebra **17** (1989), 2809–2824.

[10] Piccard, S.: *Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier.* Mém. Univ. Neuchâtel **19** (1946).

[11] Steinberg, R.: *Generators for simple groups.* Canad. J. Math. **14** (1962), 277–283.

[12] Weigel, T. S.: *Generation of Exceptional Groups of Lie-type.* Geom. Dedicata **41** (1992), 63–87.

[13] Woldar, A. J.: *3/2-Generation of the sporadic simple groups.* Comm. Algebra **22** (1994), 675–685.

Received July 29, 1997