ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 469–479

PRODUCTS OF POWERS IN FINITE SIMPLE GROUPS

BY

C. MARTINEZ*

Departamento de Matemáticas, Universidad de Oviedo
33.007 Oviedo, Spain
e-mail: chelo@pinon.ccu.uniovi.es

AND

E. ZELMANOV**

Department of Mathematics, University of Chicago
Chicago, IL 60637, USA
e-mail: zelmanov@math.yale.edu

ABSTRACT

Let G be a group. For a natural number $d \geq 1$ let G^d denote the subgroup of G generated by all powers a^d, $a \in G$.

A. Shalev raised the question if there exists a function $N = N(m,d)$ such that for an m-generated finite group G an arbitrary element from G^d can be represented as $a_1^d \cdots a_N^d$, $a_i \in G$. The positive answer to this question would imply that in a finitely generated profinite group G all power subgroups G^d are closed and that an arbitrary subgroup of finite index in G is closed. In [5,6] the first author proved the existence of such a function for nilpotent groups and for finite solvable groups of bounded Fitting height.

Another interpretation of the existence of $N(m,d)$ is definability of power subgroups G^d (see [10]).

In this paper we address the question for finite simple groups. All finite simple groups are known to be 2-generated. Thus, we prove the following:

THEOREM: *There exists a function $N = N(d)$ such that for an arbitrary finite simple group G either $G^d = 1$ or $G = \{a_1^d \cdots a_N^d | a_i \in G\}$.*

The proof is based on the Classification of finite simple groups and sometimes resorts to a case-by-case analysis.

* Partially supported by DGICYT.
** Partially supported by the NSF Grant DMS-9400466.
Received June 15, 1995 and in revised form November 1, 1995

1. Alternating groups

E. Bertram [1] proved that for any numbers n,l such that $n \geq 5$, $[3n/4] \leq l \leq n$, an arbitrary even permutation on n symbols can be expressed as a product of two cycles each of length l.

Without loss of generality we will assume that the number d is even. If $n \geq 4d$, then there exists an odd number l such that $[3n/4] \leq l \leq n$ and l is relatively prime with d.

Since an element of order l, $(l, d) = 1$, is a d-th power, it follows from the result of Bertram that every even permutation on n symbols $(n \geq 4d)$ is a product of two d-th powers.

There exists a number $M(d)$ such that for any $n < 4d$ an arbitrary element from $A(n)$ is a product of $M(d)$ d-th powers or $A(n)^d = (1)$. Now it remains to let $N(d) = \max(M(d), 2)$.

This proves the theorem for alternating groups.

2. Chevalley groups

Let Σ be a reduced irreducible root system, F a field, and let $G = G(\Sigma, F)$ be the universal Chevalley group, that corresponds to Σ and F (for definitions and notation see [9]). If we want to consider untwisted and twisted Chevalley groups simultaneously we will use the notation $G({}^{\epsilon}\Sigma, F)$.

Let Z be the center of the group $G({}^{\epsilon}\Sigma, F)$. It is known that $G({}^{\epsilon}\Sigma, F)$ is a perfect group and the quotient group $G({}^{\epsilon}\Sigma, F)/Z$ is simple unless both the field F and the rank of Σ are very small. This implies that an arbitrary normal subgroup of $G({}^{\epsilon}\Sigma, F)$ is either the whole group or is contained in Z. If $G({}^{\epsilon}\Sigma, F)^d \subseteq Z$ then the simple group $G({}^{\epsilon}\Sigma, F)/Z$ has exponent dividing d. There are finitely many finite simple groups of a given exponent (see [2]). Hence there exists $r_0 \geq 1$ such that if the rank of Σ is greater than or equal to r_0, then for any field F we have $G({}^{\epsilon}\Sigma, F) = G({}^{\epsilon}\Sigma, F)^d$.

Let Σ be a root system of rank greater than or equal to r_0. Just as it was shown in [10] for products of commutators, we will show that there exists a number $M = M(\Sigma)$ such that for an arbitrary field F we have

$$G({}^{\epsilon}\Sigma, F) = \{a_1^d \cdots a_M^d | a_i \in G({}^{\epsilon}\Sigma, F)\}.$$

Otherwise, for an arbitrary $n \geq 1$ there exists a field F_n and an element $x_n \in G({}^{\epsilon}\Sigma, F_n)$ which is not a product of less than n d-th powers of elements of

$G({}^\epsilon\Sigma, F_n)$. Let $\mathcal{U}$ be an ultrafilter in the set of natural numbers and let F be the ultraproduct $F = \prod_{n\in N} F_n/\mathcal{U}$ of fields F_n. M. Point [7] proved that $G({}^\epsilon\Sigma, F) = \prod_{n\in N} G({}^\epsilon\Sigma, F_n)/\mathcal{U}$. Then the element $x = (x_1, x_2, \ldots)/\mathcal{U}$ does not lie in $G({}^\epsilon\Sigma, F)^d$, which contradicts our earlier assertion.

Since there are finitely many root systems of given rank and in view of the remark above, we will always assume that Σ is one of the root systems A_n, B_n, C_n, D_n, $n \geq r_0$. Let F be a finite field of characteristic $p > 0$.

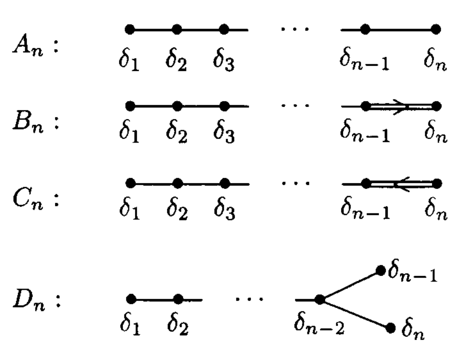
Let $\Delta = \{\delta_1, \ldots, \delta_n\}$ be a system of simple roots of Σ and let Σ^+ be the set of all positive roots with respect to Δ. The subgroup U generated by all root subgroups $X_\alpha = \{x_\alpha(k), k \in F\}$, where $\alpha \in \Sigma^+$, is a Sylow p-subgroup of G. Let U_i be the subgroup of G generated by all root subgroups X_α where $\mathrm{ht}(\alpha) \geq i$. The series $U = U_1 > U_2 > \cdots$ is a central p-series of U, that is, $[U_i, U_j] \subseteq U_{i+j}$ and $U_i^p \subseteq U_{ip}$.

Let $g = x_{\delta_1}(1) \cdots x_{\delta_n}(1) \in U \backslash U_2$. Each factor U_i/U_{i+1} is an elementary abelian p-group. The commutation with the element g induces the linear mapping

$$U_i/U_{i+1} \longrightarrow U_{i+1}/U_{i+2}, \quad \text{where } aU_{i+1} \longrightarrow [a,g]U_{i+2}, \quad a \in U_i.$$

LEMMA 2.1: $[U_m/U_{m+1}, g] = U_{m+1}/U_{m+2}$, $m \geq 1$.

Proof: The Dynkin diagram of Σ is one of the following diagrams:



If $\alpha = \sum_{i=1}^n k_i\delta_i$ is a positive root, $k_i \geq 0$, then k_1 is equal either to 0 or to 1. If $k_1 = 1$, then there is at most one simple root δ such that $\alpha + \delta \in \Sigma$.

We will prove the lemma by induction on n. For $n = 1$ the assertion is trivial. Let α be a root of height $m+1$. There exists a simple root δ_k such that $\alpha - \delta_k$ is a root of height m (see [3] or [4]). If the only simple root δ such that $\alpha - \delta \in \Sigma$ is δ_k, then $[X_{\alpha-\delta_k}, g] = [X_{\alpha-\delta_k}, x_{\delta_k}(1)] = X_\alpha \bmod U_{m+2}$.

That's why we will suppose that at least two differences of α with simple roots lie in Σ.

Let us consider the case when the decomposition of α as a linear combination of simple roots nontrivially involves δ_1. Then there exists a root δ_k, $k \geq 2$, such that $\alpha - \delta_k \in \Sigma$. The decomposition of $\alpha - \delta_k$ still involves δ_1. Hence, $[X_{\alpha-\delta_k}, g] = [X_{\alpha-\delta_k}, x_{\delta_k}(1)] = X_\alpha \bmod U_{m+2}$.

Now suppose that the decomposition of α does not involve δ_1. Let Σ' be the (root) subsystem of Σ generated by $\pm\delta_2, \ldots, \pm\delta_n$. Let $\alpha_1, \ldots, \alpha_t$ be all positive roots of Σ' of height m (with respect to $\delta_2, \ldots, \delta_n$). Let $g' = x_{\delta_2}(1) \cdots x_{\delta_n}(1)$. By the induction assumption the root subgroup X_α lies in $[X_{\alpha_1} \cdots X_{\alpha_t}, g']U_{m+2}$. Hence $X_\alpha \subseteq [X_{\alpha_1} \cdots X_{\alpha_t}, g][X_{\alpha_1} \cdots X_{\alpha_t}, x_{\delta_1}(-1)]U_{m+2}$.

But $[X_{\alpha_1} \cdots X_{\alpha_t}; x_{\delta_1}(-1)] \subseteq X_{\alpha_1+\delta_1} \cdots X_{\alpha_t+\delta_1} U_{m+2} \subseteq [U_m, g]U_{m+2}$ by what we proved above. Lemma 2.1 is proved. ∎

LEMMA 2.2: *Let P be a finite p-group with a central p-series $P = P_1 > P_2 > \cdots$. Suppose that there exists an element $g \in P \backslash P_2$ such that $[P_m/P_{m+1}, g] = P_{m+1}/P_{m+2}$ for any $m \geq 1$. Then for any $k \geq 1$ an arbitrary element from $g^{p^k} P_{p^k+1}$ is a p^k-th power.*

Proof: Let a be an element from $g^{p^k} P_{p^k+1}$. Suppose that we have found an element $b_s = gc$, $c \in P_2$, such that $b_s^{p^k} = a \bmod P_s$, $s \geq p^k + 1$. To start the process we let $b_{p^k+1} = g$. Let $b_s^{p^k} = a.d$, $d \in P_s$.

There exists an element $u \in P_{s-p^k+1}$ such that

$$[\cdots[u, \underbrace{g], g], \cdots, g]}_{p^k-1} = d^{-1} \bmod P_{s+1}.$$

Then

$$(gcu)^{p^k} = (gc)^{p^k} [\cdots [u, \underbrace{g], g], \cdots, g]}_{p^k-1} = add^{-1} = a \bmod P_{s+1}.$$

Now it remains to let $b_{s+1} = gcu$. If $P_s = (1)$ then $b_s^{p^k} = a$. Lemma 2.2 is proved. ∎

Let $d = p^k m$, where p and m are coprime. An element of U is a d-th power if and only if it is a p^k-th power.

From Lemmas 2.1 and 2.2 it follows that an arbitrary element from the coset $g^{p^k} U_{p^k+1}$ is a p^k-th power.

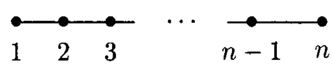
COROLLARY 2.1: *An arbitrary element from $U_{p^k+1} = g^{-p^k}(g^{p^k}U_{p^k+1})$ is a product of two p^k-th powers.*

LEMMA 2.3: *A system of simple roots Δ is a union of subsets*

$$\Delta = \Delta_1 \bigcup \cdots \bigcup \Delta_{q+1} \bigcup \Delta'_1 \bigcup \cdots \bigcup \Delta'_q,$$

where each Δ'_i, Δ'_j corresponds to a connected part of the Dynkin diagram; $|\Delta_1| = \cdots = |\Delta_q| = |\Delta'_1| = \cdots = |\Delta'_q| = r_0$, $r_0 \leq |\Delta_{q+1}| \leq 2r_0 + 2$; for any $\alpha \in \Delta_i$, $\beta \in \Delta_j$, where $i \neq j$, the $\alpha + \beta$ is not a root; for any $\alpha \in \Delta'_i$, $\beta \in \Delta'_j$, where $i \neq j$, the $\alpha + \beta$ is not a root.

Proof: If $n \leq 2r_0 + 2$ then $q = 0$ and $\Delta_{q+1} = \Delta$. Suppose, therefore, that $n \geq 2r_0 + 3$. Let $\Sigma = A_n$, the Dynkin diagram is:



where natural numbers represent simple roots. We have $n = (r_0 + 1)(q + 1) + r$, $0 \leq r \leq r_0$, $q \geq 1$.

Let

$$\begin{aligned} &\Delta_1 = \{1, 2, \ldots, r_0\}, \quad \Delta_2 = \{r_0 + 2, \ldots, 2r_0 + 1\}, \ldots, \\ &\Delta_q = \{(q-1)r_0 + q, \ldots, qr_0 + q - 1\}, \quad \Delta_{q+1} = \{q(r_0 + 1) + 1, \ldots, n\}, \\ &|\Delta_{q+1}| = r_0 + 1 + r \leq 2r_0 + 1; \quad \Delta'_1 = \{2, \ldots, r_0 + 1\}, \\ &\Delta'_2 = \{r_0 + 3, \ldots, 2r_0 + 2\}, \ldots, \quad \Delta'_q = \{(q-1)r_0 + q + 1, \ldots, q(r_0 + 1)\}. \end{aligned}$$

If Σ is a root system of one of the types B_n, C_n, D_n then we add the n-th root to the subset Δ_{q+1}, thus possibly increasing its size to $2r_0 + 2$. Lemma 2.3 is proved. ∎

Recall, that for an arbitrary $r \geq 1$ there exists a number $N = N(r)$ such that if Σ is a reduced irreducible root system of rank $\leq r$, F is a field, and $G = G(\Sigma, F)$, then either $G^d = (1)$ or $G = \{g_1^d \cdots g_N^d | g_i \in G\}$.

LEMMA 2.4: *Let $t = N(2r_0 + 2) + N(r_0)$. An arbitrary element from U can be represented as $g_1^d \cdots g_t^d u$, where $u \in U_2$.*

Proof: Let G_i be the subgroup generated by root subgroups $X_{\pm\alpha}$, $\alpha \in \Delta_i$, $1 \leq i \leq q + 1$ and let G'_j be the subgroup generated by root subgroups $X_{\pm\alpha}$,

$\alpha \in \Delta'_j$, $1 \leq j \leq q$. Then any two elements from distinct subgroups G_i, G_j (resp. G'_i, G'_j) commute.

We have $U \subseteq G_1 \cdots G_{q+1} G'_1 \cdots G'_q U_2$. An arbitrary element from G_i can be represented as a product of $N(2r_0+2)$ d-th powers of elements of G_i. Hence, an arbitrary element from $G_1 \cdots G_{q+1}$ also can be represented as a product of $N(2r_0+2)$ d-th powers. Similarly, an arbitrary element from $G'_1 \cdots G'_q$ is a product of $N(r_0)$ d-th powers. This finishes the proof of the lemma. ∎

LEMMA 2.5: *An arbitrary element from U_k, $k \geq 2$, can be represented as $g_1^d \cdots g_{2t}^d u$, where $g_i \in G$, $1 \leq i \leq 2t$, $u \in U_{k+1}$.*

Proof: Let $u_k \in U_k$. By Lemma 2.1 we have $u_k = [u_{k-1}, g].u_{k+1}$, where $u_{k-1} \in U_{k-1}$, $u_{k+1} \in U_{k+1}$.

Furthemore, Lemma 2.4 implies that $g = g'u_2$, where g' is a product of t d-th powers of elements of G, $u_2 \in U_2$. Now,

$$u_k = [u_{k-1}, g'.u_2]u_{k+1} = [u_{k-1}, u_2][u_{k-1}, g'][[u_{k-1}, g'], u_2]u_{k+1}.$$

The element $[u_{k-1}, g']$ is a product of $2t$ d-th powers. The elements $[[u_{k-1}, g'], u_2]$ and $[u_{k-1}, u_2]$ lie in U_{k+1}.

Hence,

$$\begin{aligned} u_k &= ([u_{k-1}, u_2][u_{k-1}, g'][u_{k-1}, u_2]^{-1}) \cdot ([u_{k-1}, u_2][[u_{k-1}, g+], u_2]u_{k+1}) \\ &= g_1^d \cdots g_{2t}^d u, \end{aligned}$$

where $u = [u_{k-1}, u_2][[u_{k-1}, g'], u_2]u_{k+1} \in U_{k+1}$. Lemma 2.5 is proved. ∎

From Lemmas 2.4 and 2.5 and the Corollary of Lemma 2.2 it follows that an arbitrary element from U is a product of $N_U = t + 2t(p^k - 1) + 2$ d-th powers of elements of G.

Now let us consider elements $\omega_\alpha(k) = x_\alpha(k)x_{-\alpha}(-k^{-1})x_\alpha(k)$ and $h_\alpha(k) = \omega_\alpha(k)\omega_\alpha(1)^{-1}$, $\alpha \in \Sigma$, $0 \neq k \in F$.

The subgroup H is generated by elements $h_\alpha(k)$, $\alpha \in \Delta$, $0 \neq k \in F$. Following the notation of Lemma 2.3, let $H(\Delta_i)$ and $H(\Delta'_j)$ denote the subgroups generated by elements $h_\alpha(k)$, $\alpha \in \Delta_i$ and by $h_\alpha(k)$, $\alpha \in \Delta'_j$ respectively. We have

$$H = H(\Delta_1) \cdots H(\Delta_{q+1}) H(\Delta'_1) \cdots H(\Delta'_q) \leq G_1 \cdots G_{q+1} G'_1 \cdots G'_q.$$

Hence, an arbitrary element from H can be represented as a product of $N_H = N(2r_0+2) + N(r_0)$ d-th powers.

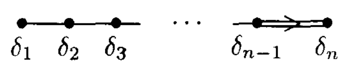
Let N be the subgroup of G generated by all elements $\omega_\alpha(k)$, $\alpha \in \Sigma$, $0 \neq k \in F$. Let W be the Weyl group of Σ, that is the group generated by reflections ω_α, $\alpha \in \Sigma$. It is known (see [9]) that H is a normal subgroup of N and there is an isomorphism $\varphi\colon W \longrightarrow N/H$ such that $\varphi(\omega_\alpha) = H\omega_\alpha(k)$ for any α.

CASE A: Let $\Sigma = A_n$. Then W is isomorphic to the symmetric group $S_{n+1} = (12)A_{n+1}$. Thus, $W = \omega_{\delta_1} W_0$, where $W_0 \cong A_{n+1}$.

Let N_0 be the subgroup of N generated by all cosets lying in $\varphi(W_0)$. Clearly, $N = \omega_{\delta_1}(1)N_0$. The element $\omega_{\delta_1}(1)$ lies in the subgroup of G generated by $X_{\pm\delta_i}$, $1 \le i \le r_0$.

Hence, $\omega_{\delta_1}(1)$ is a product of $N(r_0)$ d-th powers. An arbitrary element of N_0 is a product of N_A d-th powers modulo H. Finally, an arbitrary element from N is a product of $N(r_0) + N_A + NH$ d-th powers.

CASE B: If $\Sigma = B_n$, then the Dynkin diagram is:



and the Weyl group is isomorphic to $S_n \propto Z_2^n$. An element $a = (a_1, \dots, a_n) \in Z_2^n$ can be represented as a commutator (g, b), $g \in S_n$, $b \in Z_2^n$, if and only if $a_1 + \cdots + a_n = 0$. Hence, $W = \omega_{\delta_1} W_0(\omega_1 W_0, Z_2^n)\omega_{\delta_n}$, $W_0 \cong A(n)$. Each of the elements $\omega_{\delta_1}(1)$, $\omega_{\delta_n}(1)$ is a product of $N(r_0)$ d-th powers. As above we conclude that an arbitrary element from N is a product of $N(r_0) + N_A + 2(N(r_0) + N_A) + N(r_0) + N_H = 4N(r_0) + 3N_A + N_H$ d-th powers.

CASE C: This case is similar to the case B.

CASE D: If $\Sigma = D_n$, then the Weyl group is $W \cong S_n \propto Z_2^n(0)$, where $Z_2^n(0) = \{(a_1, \dots, a_n) \in Z_2^n | a_1 + \cdots + a_n = 0\}$. Hence, $W = \omega_{\delta_1} W_0(\omega_{\delta_1} W_0, Z_2^n(0))$. An arbitrary element from N is a product of $3(N(r_0) + N_A) + N_H$ d-th powers.

Now we can finish the proof of the Theorem for Chevalley groups. Let $B = UH$ be the Borel subgroup of G. From the Bruhat decomposition it follows that an arbitrary element of G is a product of $2(N_H + N_U) + 4N(r_0) + 3N_A + N_H$ d-th powers.

Remark: If G is a Chevalley group over an infinite field F, then every element of G is a product of a bounded number of d-th powers, as it follows from the proofs of the above results.

3. Twisted groups

Since we are interested only in groups of sufficiently big rank we will consider only groups of type ${}^2\Sigma$, where $\Sigma = A_n$ or $\Sigma = D_n$. Such a group is the subgroup of the Chevalley group $G(\Sigma, F)$ which is fixed by a certain automorphism σ of order 2 (see [9]).

For any root subgroup X_α, $\alpha \in \Sigma$ we have $\sigma(X_\alpha) = X_{\rho(\alpha)}$, where ρ is the automorphism of Σ induced by the symmetry of the Dynkin diagram. The subgroups U, H, N, B are fixed by σ and $G({}^2\Sigma, F) = B_\sigma N_\sigma B_\sigma$, $B_\sigma = H_\sigma U_\sigma$. That's why we'll apply the same scheme as before.

CASE ${}^2D_n$: Consider the lattice $\bigoplus_{i=1}^n Z\omega_i \subseteq R^n$. Then

$$\Sigma = \{\pm\omega_i \pm \omega_j, 1 \leq i \neq j \leq n\},$$
$$\Delta = \{\delta_1 = \omega_1 - \omega_2, \delta_2 = \omega_2 - \omega_3, \ldots, \delta_{n-1} = \omega_{n-1} - \omega_n, \delta_n = \omega_{n-1} + \omega_n\}.$$

The symmetry ρ is induced by the linear mapping $\omega_i \to \omega_i$ for $1 \leq i \leq n-1$, $\omega_n \to -\omega_n$. For a ρ-orbit a of Σ let $\mathcal{X}_a = X_\alpha$ if $a = \{\alpha\}$, $\alpha \in \Sigma \bigcap (\bigoplus_{i=1}^{n-1} Z\omega_i)$ and $\mathcal{X}_a = \{x_\alpha \sigma(x_\alpha), x_\alpha \in X_\alpha\}$ if $a = \{\alpha, \rho(\alpha)\}$, $\alpha = \pm\omega_i \pm \omega_n$. Since ρ permutes positive roots it makes sense to speak about the set of positive orbits Σ^+/ρ. Since $\mathrm{ht}(\alpha) = \mathrm{ht}(\rho(\alpha))$ for any $\alpha \in \Sigma^+$ it makes sense to speak about the height of an orbit $a \in \Sigma^+/\rho$.

The subgroup $U_{\sigma,}$ is generated by all x_α's, where $a \in \Sigma^+/\rho$, $\mathrm{ht}(a) \geq i$. Then $U_\sigma = U_{\sigma,1} \geq U_{\sigma,2} \geq \cdots$ is a central p-series. Let $g' = x_{\delta_1}(1) \cdots x_{\delta_{n-2}}(1)$.

LEMMA 3.1: *For any $m \geq 1$ we have $[U_{\sigma,m}/U_{\sigma,m+1}, g'] = U_{\sigma,m+1}/U_{\sigma,m+2}$.*

Proof: Let a be a ρ-orbit of Σ^+ of height $m+1$. If $a \in \sum_{i=1}^{n-1} Z\omega_i$, then the assertion follows from Lemma 2.1.

For $a = \{\omega_i + \omega_n, \omega_i - \omega_n\}$, $\mathrm{ht}(a) = n - i = m+1$, we have $\mathcal{X}_a = [\mathcal{X}_b, x_{\delta_i}(1)] = [\mathcal{X}_b, g'] \bmod U_{\sigma,m+2}$, where $b = \{\omega_{i+1} + \omega_n, \omega_{i+1} - \omega_n\}$. Lemma 3.1 is proved. ∎

In view of Lemma 2.2 an arbitrary element from U_{σ,p^k+1} is a product of two d-th powers.

For every subset Δ_i, Δ'_j of Lemma 2.3 we have $\rho(\Delta_i) = \Delta_i$, $\rho(\Delta'_j) = \Delta'_j$ and $\Delta/\rho = \Delta_1 \bigcup \cdots \bigcup \Delta_q \bigcup (\Delta_{q+1}/\rho) \bigcup \Delta'_1 \bigcup \cdots \bigcup \Delta'_q$. We can assume that the number r_0 is big enough so that for any field F the groups $G({}^2D_{r_0}, F)$ and $G({}^2A_{r_0}, F)$ do not satisfy the law $x^d = 1$. The number $N(k)$, $k \geq r_0$, can also be adjusted to make sure that an arbitrary element from $G(^2D_k, F)$ or $G(^2A_k, F)$ is a product of $N(k)$ d-th powers. Repeating the arguments from Lemmas 2.4, 2.5, we get that an arbitrary element from U_σ is a product of $N_{U,\sigma} = t + 2t(p^k - 1) + 2$ d-th powers, where $t = N(2r_0 + 2) + N(r_0)$.

Again repeating the arguments from the second section we conclude that $H_\sigma \subseteq G_1 \cdots G_{q+1} G'_1 \cdots G'_q$ and, thus, an arbitrary element from H_σ is a product of $N_{H,\sigma} = t$ d-th powers.

The group $W_\sigma = N_\sigma / H_\sigma$ is isomorphic to the Weyl group of type B_{n-1}, that is $W_\sigma \cong S(n-1) \propto Z_2^{n-1}$. As in the second section, it implies that an arbitrary element from N_σ is a product of $4N(r_0) + 3N_A + t$ d-th powers. From Bruhat decomposition $G = G(^2D_n, F) = B_\sigma N_\sigma B_\sigma$ it follows that an arbitrary element of G is a product of $2(N_{U,\sigma} + t) + (4N(r_0) + 3N_A + t)$ d-th powers.

CASE ^2A_n: Consider the lattice $\bigoplus_{i=1}^{n+1} Z\omega_i \subseteq R^n$. Then

$$\Sigma = \{\omega_i - \omega_j, 1 \le i \ne j \le n+1\},$$
$$\Delta = \{\delta_1 = \omega_1 - \omega_2, \delta_2 = \omega_2 - \omega_3, \ldots, \delta_n = \omega_n - \omega_{n+1}, \}.$$

The symmetry ρ is induced by the linear mapping $\omega_i \to -\omega_{n+2-i}$ for $1 \le i \le n+1$.

Let $\tau(i) = n + 2 - i$.

Let $k = \frac{1}{2}(r_0 + 1)$ if r_0 is odd and $k = \frac{1}{2} r_0 + 1$ if r_0 is even. In both cases $2k \ge r_0 + 1$ and $4k \le 2r_0 + 4$.

Let $n + 1 = 2k(q+1) + r$, $r < 2k$. Consider the sets

$$\begin{aligned} S_1 &= \{1, 2, \ldots, k, \tau(1), \ldots, \tau(k)\}, \\ S_2 &= \{k+1, \ldots, 2k, \tau(k+1), \ldots, \tau(2k)\}, \\ \ldots, S_q &= \{(q-1)k + 1, \quad \ldots, \quad qk, \tau((q-1)k+1), \ldots, \tau(qk)\}, \\ S_{q+1} &= \{i, qk < i < n + 2 - qk\}. \end{aligned}$$

It is easy to see that $\{1, 2, \ldots, n+1\}$ is the disjoint union of $S_1, \ldots, S_{q+1}$; $|S_i| = 2k$ for $1 \le i \le q$ and $|S_{q+1}| = 2k + r < 4k$. For

$$S_i = \{i_1, \ldots, i_k, \tau(i_1), \ldots, \tau(i_k)\}$$

consider also the subset $S'_i = \{i_1 + 1, \ldots, i_k + 1, \tau(i_1 + 1), \ldots, \tau(i_k + 1)\}$. Then $|S'_i| = 2k$ and $S'_i \bigcap S'_j = \emptyset$ for $i \ne j$.

Let G_l (resp. G'_l) be the subgroup of $G(A_n, F)$ generated by root subgroups $X_{\omega_i-\omega_j}$ where $i, j \in S_l$ (resp. S'_l). Each subgroup G_l, G'_l is σ-invariant. Let $G_{l,\sigma}$ (resp. $G'_{l,\sigma}$) be the subgroups of σ-fixed elements. We have

$$H_\sigma \subseteq G_{1\sigma} \cdots G_{q+1,\sigma} G'_{1\sigma} \cdots G'_{q\sigma}.$$

Hence an arbitrary element from H is a product of $t = N(2r_0 + 4) + N(r_0)$ d-th powers.

Furthemore,

$$U_\sigma \subseteq G_{1\sigma} \cdots G_{q+1,\sigma} G'_{1\sigma} \cdots G'_{q\sigma} U_{\sigma,2}.$$

Let $\delta_{i_1}, \ldots, \delta_{i_m}$ be all simple roots lying in $\bigoplus_{\mu \in S_i} Z\omega_\mu$. Since S_i is symmetric we can put them in such an order that the element $g_i = x_{\delta_{i_1}}(1) \cdots x_{\delta_{i_m}}(1)$ lies in $G_{i,\sigma}$. And similarly we get elements $g'_i \in G'_i$. Let $g = g_1 \cdots g_{q+1} g'_1 \cdots g'_q$. The element g is a product of t d-th powers of elements of G_σ.

One-element orbits of ρ in Σ look like $\{\omega_i - \omega_{\tau(i)}\}$. Let C be the subgroup generated by all root subgroups $X_{\omega_i - \omega_{\tau(i)}}$, where $i < \tau(i)$.

LEMMA 3.2: *An arbitrary element x from $U_{\sigma,2}$ can be represented as $x = c[u, g]$, where $c \in C$, $u \in U_\sigma$.*

Proof: Let $a = \{\alpha, \rho(\alpha)\}$ be a two-element orbit from Σ^+/ρ of height m. Then $\mathcal{X}_a = \{x_\alpha \sigma(x_\alpha), x_\alpha \in X_\alpha\}$. By Lemma 2.1, for an arbitrary element $x_\alpha \in X_\alpha$ we have $x_\alpha = [x_{\alpha_1} \cdots x_{\alpha_r}, g] \bmod U_{m+1}$, where $x_{\alpha_i} \in X_{\alpha_i}$, $\mathrm{ht}(\alpha_i) = m - 1$. Then,

$$x_\alpha \sigma(x_\alpha) = [x_{\alpha_1} \sigma(x_{\alpha_1}) \cdots x_{\alpha_r} \sigma(x_{\alpha_r}), g] \quad \bmod U_{\sigma,m+1}.$$

Suppose that we have found elements $c_m \in C$, $u_m \in U_\sigma$ such that $x = c_m[u_m, g]$ mod $U_{\sigma,m}$.

For a two-element orbit $a \in \Sigma^+/\rho$ of height m, and for an arbitrary element $x_a \in \mathcal{X}_a$, we have $x_a = [y, g] \bmod U_{\sigma,m+1}$, where $y \in U_{\sigma,m}$. Hence, $c_m[u_m, g]x_a = c_m[u_m y, g] \bmod U_{\sigma,m+1}$.

If a is a one-element orbit of height m, then $\mathcal{X}_a \subseteq C$ and $c_m[u_m, g]x_a = (c_m x_a)[u_m, g] \bmod U_{\sigma,m+1}$. This proves Lemma 3.2. ∎

The set $\{1, 2, \ldots, n+1\}$ can be divided into a disjoint union of τ-symmetric subsets $T_1, T_2, \ldots$ each of size k, $r_0 \leq k \leq 2r_0$. Let $G(T_k)$ be the subgroup generated by all root subgroups $X_{\omega_i - \omega_j}$; $i, j \in T_k$ and let $G(T_k)_\sigma$ be the subgroup of σ-fixed elements of $G(T_k)$. Elements from distinct subgroups $G(T_i)$, $G(T_j)$

commute, and $C \subseteq \prod_k G(T_k)_\sigma$. Hence, an arbitrary element from C is a product of $N(2r_0)$ d-th powers.

Now it follows that an arbitrary element from U_σ is a product of $N(2r_0) + 3t$ d-th powers.

The quotient group N_σ/H_σ is isomorphic to the Weyl group of type B_n. Thus, like in the second section, we conclude that an arbitrary element of $G({}^2A_n, F)$ is a product of $2(N(2r_0) + 4t) + (4N(r_0) + 3N_A + t)$ d-th powers. The Theorem is proved.

The authors are grateful to A. Mann and the referee for helpful remarks.

Remark: After this work was finished the first author learned from J. S. Wilson that I. Saxl and J. S. Wilson have independently proved the Theorem.

References

[1] E. Bertram, *Even permutations as a product of two conjugate cycles,* Journal of Combinatorial Theory (A) **12** (1972), 368–380.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. P. Parker and R. A. Wilson, *Atlas of Finite Groups,* Clarendon Press, Oxford, 1985.

[3] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory,* Springer-Verlag, Berlin, 1975.

[4] N. Jacobson, *Lie Algebras,* Wiley-Interscience, New York, 1962.

[5] C. Martinez, *On power subgroups of pro-finite groups,* Transactions of the American Mathematical Society **345** (1994), 865–869.

[6] C. Martinez, *Power subgroups of pro-(finite soluble) groups,* Journal of the London Mathematical Society, to appear.

[7] M. Point, *Ultraproducts of Chevalley groups,* submitted.

[8] A. Shalev, *Finite p-groups,* Proceedings of the NATO Conference in Group Theory, Istanbul, 1994.

[9] R. Steinberg, *Lectures on Chevalley groups,* Lecture Notes, Yale University, 1968.

[10] J. S. Wilson, *First-order group theory,* School of Mathematics and Statistics preprints, The University of Birmingham, 1994.