ISRAEL JOURNAL OF MATHEMATICS **130** (2002), 249–258

PRODUCTS OF CONJUGACY CLASSES IN CHEVALLEY GROUPS II. COVERING AND GENERATION

BY

NIKOLAI GORDEEV*

Department of Mathematics, Russian State Pedagogical University
Moijka 48, Sankt Petersburg 191-186, Russia
e-mail: gordeev@pdmi.ras.ru

AND

JAN SAXL

Department of Pure Mathematics and Mathematical Statistics
University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, England
e-mail: saxl@dpmms.cam.ac.uk

ABSTRACT

In this paper we establish a relationship between generating numbers and covering numbers of conjugacy classes in Chevalley groups over algebraically closed fields.

1. Introduction

Let G be a simple algebraic group over a field K and let $C_1, \ldots, C_k$ be non-central conjugacy classes of G. For the case when the characteristic of K is zero it was proved in [G] that if $\overline{C_1 \cdots C_k} = G$ (so that the product of the classes C_i is dense in G) then for every non-central $g \in G$ there exist elements $g_1 \in C_1, \ldots, g_k \in C_k$ such that $\overline{\langle g, g_1, \ldots, g_k \rangle} = G$. In general, the condition

* The authors gratefully acknowledge EPSRC grant GR58542. The first author acknowledges further a grant SFB 343 "Diskrete Strukturen in der Mathematik". The second author thanks the Institute for Advanced Studies at The Hebrew University for its hospitality.
Received August 7, 2000

$\overline{C_1 \cdots C_k} = G$ does not guarantee the existence of sequences of representatives from these conjugacy classes which generate a dense subgroup, as we see from the simple example $G = SL_2$ with $C_1 = C_2$ the conjugacy class of elements of order 4. However, in [G] it was shown that the condition on products implies the existence of a dense subset in $C_1 \cdots C_k$ such that every sequence from this subset will generate a dense subgroup in some closed reductive subgroup D of G such that $Z(D) = Z(G)$ (again assuming that the characteristic of K is zero). The inverse problem is also considered in [G] in the case of characteristic zero: if $\overline{\langle g_1, \ldots, g_k \rangle} = G$ for some $g_1 \in C_1, \ldots, g_k \in C_k$, does it follow that $\overline{C_1 \cdots C_k} = G$? This is true not only for sequences which generate a dense subgroup in G but also for those which generate a dense subgroup in some closed reductive subgroup $D \leq G$ with $Z(D) = Z(G)$. In the case when $C_1 = C_2 = \ldots, C_k = C$ one can define

$$\overline{cn}(C, G) = min\{m | \ \overline{C^m} = G\},$$

and

$$\overline{gen}(C) = min\{m | \text{there exists a sequence} g_1, \ldots, g_m \in C \text{ with} \overline{\langle g_1, \ldots, g_m \rangle} = G\}.$$

The above results imply

$$(\star) \qquad \overline{cn}(C) \leq \overline{gen}(C) \leq \overline{cn}(C) + 1$$

in the characteristic zero case. Here we prove such results for every characteristic (for the second inequality to hold, one needs to assume that the field is not $\overline{F_p}$). We also obtain some additional information about connections of these two properties of "covering" and "generation". We may omit the bar over cn and define

$$cn(C, G) = min\{m | C^m = G\}.$$

Since the product of conjugacy classes is a constructible set, we have $cn(G) \leq 2\overline{cn}(C)$ and therefore

$$(\star\star) \qquad \frac{1}{2} cn(C) \leq \overline{gen}(C) \leq cn(C) + 1.$$

Let now G be a Chevalley group over K, with K any infinite field not contained in $\overline{F_p}$ (so G is the subgroup of $\tilde{G}(K)$ generated by unipotent elements, where $\tilde{G}$ is a simple algebraic group defined and split over K). Considering G as a subgroup of $\tilde{G}(\overline{K})$ we can define the notion $\overline{gen}(C)$ as above. In section 5 we prove the inequality

$$(\star\star\star) \qquad \frac{1}{8} cn(C) \leq \overline{gen}(C) \leq cn(C) + 1.$$

Note that the condition that K is not contained in the closure of the field of p elements is clearly necessary.

A related result for the finite Chevalley groups G has also been obtained recently: there exists a general positive constant c (independent of G and C) such that

$$c.cn(C) \leq gen(C) \leq cn(C) + 1$$

for every non-trivial conjugacy class C of any finite simple group G of Lie type. The right hand inequality here follows from a result of Guralnick and Kantor [GK]. The left hand inequality follows from a recent paper of Liebeck and Shalev [LS] (note, however, that c is not given explicitly there).

2. Notation and terminology

2.1. Here R is an irreducible root system generated by a simple root system $\{\alpha_1, \dots, \alpha_r\}$. We also write $R = \langle \alpha_1, \dots, \alpha_r \rangle$. Further, R^+ and R^- are the sets of positive and negative roots respectively, $W = W(R)$ is the Weyl group for R. Our notation for root systems is that of Bourbaki [B, Tables I–X].

2.2. Let G be a simple algebraic group corresponding to a root system R which is defined and split over a field K. Let $\alpha \in R$. We use the notation of Steinberg [St1] for unipotent and semisimple root elements $x_\alpha(t), t \in K, h_\alpha(t), t \in K^*$. Further, $X_\alpha = \langle x_\alpha(t) | t \in K^* \rangle$ is the corresponding root subgroup of $G(K)$. The subgroup of $G(K)$ generated by all root subgroups is the Chevalley group over the field K corresponding to G, and is also denoted by G (where this does not lead to any confusion).

2.3. There is another type of Chevalley groups (or twisted Chevalley groups). Namely, in the case where K is a finite field and G is simply connected we consider groups of the form $G(\overline{K})^F$ where F is a Frobenius map (see [C1], [C2]). We also denote such a group by G. The automorphism F can be written in the form $F = \theta\rho$, where θ is the corresponding field automorphism and ρ is the corresponding graph automorphism. The field K^θ of θ-invariants we denote by k, except in the case of Suzuki–Ree groups ${}^2B_2(q^2), {}^2G_2(q^2), {}^2F_4(q^2)$. For these groups we put $k = K$. The Chevalley groups (untwisted or finite twisted) are quasisimple except for a few cases ([St1], [C1]). For a twisted group there exists also the root system which is obtained from R by glueing roots. We will denote this system by R^F (when we speak only of the corresponding twisted group we will omit the superscript ^{F}). The notation for root systems in the twisted cases corresponds to [C1]. The notation for root subgroups (which can be one, two, or three parameter subgroups) is the same as in the untwisted case. The $rank(G)$ is the number of simple roots in R (or in R^F).

2.4. Let G be a Chevalley group (untwisted or twisted) over a field K corresponding to a root system R. Then

$$H = \langle h_\alpha(t) | \alpha \in R, t \in K^* (\text{or}, t \in k^*, \text{ if } \rho(\alpha) = \alpha) \rangle,$$
$$U = \langle X_\alpha | \alpha \in R^+ \rangle, \quad U^- = \langle X_\alpha | \alpha \in R^- \rangle, \quad B = HU, B^- = HU^-.$$

The subgroup N (see [St1], [C1,2]) contains the group H as a normal subgroup and $N/H \cong W$. By $\dot{w}$ we denote any preimage of an element $w \in W$ in N.

2.5. Let $u \in U$. Then u can be written as a product of elements of the form $x_\alpha \in X_\alpha, \alpha > 0$. This expression depends on the order in which we take this product, but if we fix the order of roots the expression becomes unique.

2.6. The general group notation and terminology we use is standard. When we consider algebraic groups the bar over a set means the Zariski closure. The bar over a field means the algebraic closure.

3. From covering to generation

THEOREM 1: *Let G be a simple algebraic group defined over an algebraically closed field K and let $C_1, \ldots, C_k$ be conjugacy classes of $G(K)$ such that $\overline{C_1 \cdots C_k} = G$.*

If $K \neq \overline{F_p}$ for any prime p, then for every non-central element $g \in G(K)$ there exists a sequence $g_1 \in C_1, \ldots, g_k \in C_k$ such that

$$\overline{\langle g, g_1, \ldots, g_k \rangle} = G(K).$$

Moreover, the set of such sequences $(g_1, \ldots, g_k)$ is dense in $C_1 \times C_2 \times \cdots \times C_k$.

In all cases there exists a non-empty open subset $X \subset C_1 \times C_2 \times \cdots \times C_k$ such that for every sequence $x = (g_1, \ldots, g_k) \in X$ the group $D_x = \overline{\langle g_1, \ldots, g_k \rangle}$ is reductive and has a finite centraliser $C_G(D_x)$. If, in addition, $K \neq \overline{F_p}$, then for points x of some dense subset of X the corresponding group D_x contains a maximal torus of G.

Proof: If $K \neq \overline{F_p}$ then there exists an element $t \in T(K)$ such that $\overline{\langle t \rangle} = T(K)$ ([Bo], ch. 18). Moreover, the set of such t is dense in $T(K)$. Hence there exists a dense subset $Y \subset C_1 \times \cdots \times C_k$ satisfying the following condition: if $(g_1, \ldots, g_k) \in Y$ then $\overline{\langle g_1 g_2 \cdots g_k \rangle} = T'(K)$ for some maximal torus T'. Note that there exists only a finite number of maximal proper closed subgroups of $G(K)$ containing a fixed torus $T'(K)$. Thus there exists an open subset $M \subset G(K)$ such that for every $\sigma \in M$ the element $\sigma g \sigma^{-1}$ does not belong to any closed subgroup of G containing the torus T'. Hence the group $\overline{\langle \sigma g \sigma^{-1}, g_1, \ldots, g_k \rangle}$ equals $G(K)$ for every $\sigma \in M$, since it is not contained in any proper closed subgroup of $G(K)$. Thus, for a non-central element g we find an appropriate sequence $\langle \sigma^{-1} g_1 \sigma, \ldots, \sigma^{-1} g_k \sigma \rangle$. The density of the set of such sequences follows from the fact that Y is dense and M is open.

Now we prove the second assertion. Let $\Gamma < G$ be a closed subgroup which has a non-trivial algebraic character $\phi\colon \Gamma \longrightarrow K^*$ such that $\phi(\Gamma) = K^*$. Then the set of semisimple parts in the Jordan decomposition (up to conjugation) of all elements of the set $(C_1 \cap \Gamma)(C_2 \cap \Gamma) \cdots (C_k \cap \Gamma)$ is contained in a proper closed subset of T (see [G], II, Lemma 8). Note that the number of orbits (with respect to conjugation) of maximal closed subgroups of G which have a non-trivial character is finite. Hence there exists an open set $M \subset T$ such that if $t \in M$, then for any such subgroup Γ we have $t \notin (C_1 \cap \Gamma)(C_2 \cap \Gamma) \cdots (C_k \cap \Gamma)$. The set of all conjugates of elements of M contains a subset X' which is open in G. There exists an open subset $X \in C_1 \times \cdots \times C_k$ such that $g_1 g_2 \cdots g_k \in X'$ for every $(g_1, g_2, \ldots, g_k) \in X$. Now the group $D_x = \overline{\langle g_1, \ldots, g_k \rangle}$ for $x = (g_1, \ldots, g_k) \in X$ cannot be contained in any parabolic subgroup (since the parabolics have a non-trivial character) and cannot have any torus in its centraliser. Thus D_x is reductive and has a finite centraliser. If, in addition, $K \neq \overline{F_p}$, then we can choose as above those sequences in X whose products generate a dense subgroup in a maximal torus. ∎

4. From generation to covering

We use the notion of augmentative modules.

Definition 1: Let Γ be a group, A be a commutative ring. Let $A[\Gamma]$ be the corresponding group ring and $I_A[\Gamma]$ be its augmentation ideal. We say that the $A[\Gamma]$-module M is *augmentative* if $I_A[\Gamma]M = M$.

In [GS] it is shown that if M is an augmentative $A[\Gamma]$-module and $\Gamma = \langle \gamma_1 \cdots \gamma_k \rangle$, then the map

$$\Phi\colon M \oplus M \oplus \cdots \oplus M \longrightarrow M$$

given by the formula

$$\Phi((m_1, \ldots, m_k)) = (1-\gamma_1)(m_1) + \gamma_1(1-\gamma_2)(m_2) + \cdots + \gamma_1\gamma_2 \cdots \gamma_{k-1}(1-\gamma_k)(m_k)$$

is surjective.

Definition 2: Let G be an algebraic group defined over a field K and let L be the Lie algebra of G. We say that a subgroup $D \leq G(K)$ is *augmentative* if L is an augmentative D-module with respect to the adjoint action of G on L.

THEOREM 2: *Let $D = \langle f_1, \ldots, f_k \rangle \leq G(K)$ be an augmentative subgroup and let $C_1, \ldots, C_k$ be the conjugacy classes in $G(\overline{K})$ of elements $f_1, \ldots, f_k$. Then*

$$\overline{C_1 C_2 \cdots C_k} = G(\overline{K}).$$

Proof: We may assume that the point $f = f_1 f_2 \cdots f_k$ is not singular in $C_1 C_2 \cdots C_k$ (otherwise we replace the elements $f_1, \ldots, f_k$ by suitable conjugates). Consider the map

$$\phi\colon G \times G \times \cdots \times G \longrightarrow G$$

given by the formula

$$\phi((x_1, \ldots, x_k)) = (x_1 f_1 x_1^{-1})(x_2 f_2 x_2^{-1}) \cdots (x_k f_k x_k^{-1}) f^{-1}.$$

Using the formulas for differentials we see that the differential

$$d\phi\colon \mathsf{L} \oplus \mathsf{L} \oplus \cdots \oplus \mathsf{L} \longrightarrow \mathsf{L}$$

at the point $(1, \ldots, 1)$ is the map

$$d\phi((l_1, \ldots, l_k)) = (1 - f_1)(l_1) + f_1(1 - f_2)(l_2) + \cdots + f_1 f_2 \cdots f_{k-1}(1 - f_k)(l_k)$$

(here we identify the operators $\mathrm{ad}(f_i)$ with f_i). Since L is an augmentative D-module we have $\mathrm{Im} d\phi = \mathsf{L}$. But $\mathrm{Im}\phi = C_1 C_2 \cdots C_k f^{-1}$ and the point 1 is non-singular in $C_1 C_2 \cdots C_k f^{-1}$. Thus $\dim \mathrm{Im}\phi = \dim G = \dim C_1 C_2 \cdots C_k$. ∎

To apply Theorem 2 we need a supply of augmentative subgroups. Some examples are given by the following Theorem.

THEOREM 3: *Let G be a simple simply connected algebraic group defined over a field K. In each of the following cases the subgroup $D \leq G(K)$ is augmentative:*

A. *$\mathrm{char} K = 0$ and $\overline{D}$ is a reductive subgroup of G with the same centre.*

B. *G is split over K and $D = G(K)$, except possibly the cases when D is not a quasi-simple group.*

C. *G is a group over $K = \overline{F_p}$ and $D = G^F(K)$, except possibly the cases when D is not a quasi-simple group (here F is a Frobenius map).*

Proof: Case A is easier than the others, so we give the proof only in the cases B and C. If $|K| > 2$, then the Lie algebra $sl_2(K)$ is an augmentative $SL_2(K)$-module. Further, the Lie algebra L of G is the sum of algebras of the form $\mathsf{L}_\alpha = Ku_{-\alpha} + Kh_\alpha + Ku_\alpha$ where $u_{\pm\alpha}, h_\alpha$ are corresponding elements of the Chevalley basis ([St1]), and each of these is isomorphic to $sl_2(K)$ (recall that G is simply connected). If we are in the untwisted case then the group $\langle X_{\pm\alpha}\rangle$ is isomorphic to $SL_2(K)$. Thus if $|K| > 2$, then L_α is an augmentative $\langle X_{\pm\alpha}\rangle$-module and therefore the whole algebra L is an augmentative module with respect to the group generated by root subgroups. Assume now that $|K| = 2$; then the algebra $sl_3(K)$ is an augmentative $SL_3(K)$-module (this follows from a direct calculation with transvections). It follows that in the untwisted case, if all the roots in R have the same length and rank ≥ 2, the algebra L is also an augmentative D-module. (Indeed, if $I[D]\mathsf{L}$ contains a subalgebra of L corresponding to the root subsystem of rank 2, then it contains the whole algebra L because we can spread root elements of a Chevalley basis by the Weyl group.) Next consider the untwisted cases B_r, C_r when $r \geq 3$. If α, β are the simple roots of different length which generate the root subsystem B_2, then $(x_\alpha(1) - 1)u_\beta = s_\gamma u_\gamma + s_\delta u_\delta$ where $\gamma = \alpha + \beta, \delta = \alpha + 2\beta$, $s_\gamma, s_\delta \neq 0$. Since $r \geq 3$, either γ or δ is an element of a root subsystem of type A_2. Hence, as we have seen above, $u_\gamma \in I[D]\mathsf{L}$ or $u_\delta \in I[D]\mathsf{L}$. It follows that both $u_\gamma, u_\delta \in I[D]\mathsf{L}$. Further, for every root ϵ we have $(x_\epsilon(1) - 1)u_{-\epsilon} = \pm h_\epsilon \pm u_\epsilon$. Hence $h_\epsilon \in I[D]\mathsf{L}$. Thus every element of the Chevalley basis is in $I[D]\mathsf{L}$ and therefore L is an augmentative D-module. The case F_4 is handled similarly, using the root subsystem B_3. We do not consider the cases $A_1(2), B_2(2), G_2(2)$ since these groups are not quasi-simple.

Now consider the twisted cases.

Let D be of type ${}^2A_2, {}^2B_2, {}^2G_2$ acting on the corresponding Lie algebra of type A_2, B_2, G_2. The first of these is handled by a direct computation with $SU_3(q^2)$ on $sl_3(K)$. In the second and third cases we assume $q^2 \neq 2$, $q^2 \neq 3$ respectively. Then in both cases we have an element in the group H which is regular in $G(\overline{K})$. It follows that $u_\alpha \in I[D]L$ for every root $\alpha \in R$. Let α, β be the simple roots of R and let $x = x_\alpha(1)x_\beta(1)x'$ be an element of D, where x' is a product of positive root elements from $G(K)$ corresponding to roots of the form $i\alpha + j\beta$, $i, j \geq 0$ (see [St1]). Then $(x - 1)u_{-\alpha} = t_\alpha h_\alpha + u$, where $t_\alpha \neq 0$ and u belongs to the subspace of L generated by $u_\gamma, \gamma > 0$. Thus we have $h_\alpha \in I[D]\mathsf{L}$. Similarly we get h_β included. Thus L is contained in $I[D]\mathsf{L}$.

Now consider the general twisted case. Note that the Chevalley basis in L splits into F-orbits and every such orbit generates a subalgebra of type $A_1, A_1 \times A_1$,

$A_1 \times A_1 \times A_1, A_2, B_2, G_2$ with a subgroup of D of type $A_1, A_1, A_1, {}^2A_2, {}^2B_2, {}^2G_2$ acting on this subalgebra. For the last three of these we have seen that this action is augmentative. The first case was also considered above and we have seen that if $|K| = q > 2$ this action is augmentative. Next, $SL_2(q^2)$ acts by conjugation on $sl_2(K) \times sl_2(K)$ in the following way: $g((l_1, l_2)) = (g(l_1), g^\theta(l_2))$ (recall that θ is the corresponding field automorphism). It is easy to check that this action is augmentative. The same holds for the action of $SL_2(q^3)$ on $sl_2(K) \times sl_2(K) \times sl_2(K)$. It remains to consider the cases where there is an orbit consisting of one root and where $q = 2$. These are the cases when D is of type ${}^2A_{2l+1}(4), {}^2D_r(4), {}^3D_4(8), {}^2E_6(4)$ (note that in the case ${}^2F_4$ we assume $q^2 \neq 2$). In all of these, except for ${}^3D_4(8)$, we have a subalgebra L_3 in L of type A_3 which is F-stable and a subgroup of D of type ${}^2A_3(4)$ which acts on it. Let $\alpha_1, \alpha_2, \alpha_3$ be a simple root system for A_3 such that $\{\alpha_1, \alpha_3\}, \{\alpha_2\}$ are F-orbits. Since $q^2 > 2$ we have $u_{\pm\alpha_1}, u_{\pm\alpha_3}, h_{\alpha_1}, h_{\alpha_3} \in I[D]L$ because we have here the action of $SL_2(q^2)$ on the Lie algebra of the type $A_1 \times A_1$. Let $x = x_{\alpha_1}(1)x_{\alpha_3}(1)$. Then $(x-1)u_{\alpha_2} = s_1 u_{\alpha_1+\alpha_2} + s_2 u_{\alpha_2+\alpha_3} + s_3 u_{\alpha_1+\alpha_2+\alpha_3}$ for some $s_1, s_2, s_3 \neq 0$. Moreover, the first and second roots in this sum are in the same F-orbit and correspond in R^F to the root which is in the same W^F-orbit as the root corresponding to α_1, α_3. Therefore they are in $I[D]\mathsf{L}$. Hence the last member of this sum which corresponds to an F-stable root is also in $I[D]\mathsf{L}$. Thus we can get all elements of the form u_α from L_3 in $I[D]\mathsf{L}$. The same consideration as for B_2 above gives us also inclusions $h_\alpha \in I[D]\mathsf{L}$. Thus $\mathsf{L}_3 \subset I[D]\mathsf{L}$. Since every element of a Chevalley basis can be embedded in such an L_3 we have our statement. Similar argument deals with the case ${}^3D_4(8)$. ∎

COROLLARY 1: *Let G be a simple simply connected algebraic group defined and split over a field K (or quasisplit over $K = F_q$). Let $g_1, \dots, g_k \in G(K)$ and let $C_1, \dots, C_k$ be the conjugacy classes of $g_1, \dots, g_k$ in $G(\overline{K})$. If $G(K)$ is quasisimple and $\langle g_1, \dots, g_k \rangle = G(K)$ or $\overline{\langle g_1, \dots, g_k \rangle} = G(\overline{K})$ then*

$$\overline{C_1 C_2 \cdots C_k} = G(\overline{K}).$$

Proof: Since the adjoint action of G on its Lie algebra L is regular the $\langle g_1, \dots, g_k \rangle$-module L is augmentative if and only if the $\overline{\langle g_1, \dots, g_k \rangle}$-module L is augmentative. Now, the result follows from Theorems 2 and 3. ∎

5. Proofs of the inequalities

Let $\tilde{G}$ be a simple algebraic group which is defined and split over a field K and let $G \leq \tilde{G}(K)$ be the corresponding Chevalley subgroup (i.e., the subgroup generated by the unipotent elements). There exists a simple simply connected algebraic group $\hat{G}$ which is defined and split over K and an isogeny

$$\phi: \hat{G} \longrightarrow \tilde{G}$$

such that $\phi(\hat{G}(K)) = G$ ([St1]). Let $g \in G$ and let $\hat{g} \in \hat{G}(K)$ be a fixed preimage of g with respect to ϕ. Further, let $C \subset G, \tilde{C} \subset \tilde{G}(K), \hat{C} \subset \hat{G}(K)$ be conjugacy classes of g in G, $\tilde{G}(K)$ and the conjugacy class of $\hat{g}$ in $\hat{G}(K)$ respectively.

Now let K be an algebraically closed field. Then $G = \tilde{G}(K), C = \tilde{C}$. Since ϕ is an isogeny we have $\overline{cn}(\tilde{C}) = \overline{cn}(\hat{C})$. Moreover, $\overline{gen}(\tilde{C}) = \overline{gen}(\hat{C})$. Thus, to prove ($\star$) we may assume that $\tilde{G}$ is simply connected. Now Theorems 1, 2 and 3 imply inequalities ($\star$) and therefore ($\star\star$).

Now let K be an infinite field which is not a subfield of $\overline{F_p}$. Let Q be the conjugacy class of $g \in C$ in $\tilde{G}(\overline{K})$. The group $\tilde{G}(K)$ is dense in $\tilde{G}(\overline{K})$ ([Bo], 18.3). This implies the density of G in $\tilde{G}(\overline{K})$ and therefore of C^k in Q^k for every k. The condition $C^k = G$ imples $\overline{Q^k} = \tilde{G}(\overline{K})$. From part two of Theorem 1 it follows that there exists a sequence $g_1, \ldots, g_k \in C$ such that the group $\overline{\langle g_1, \ldots, g_k \rangle}$ contains a maximal torus of $\tilde{G}$ (recall that the set X in Theorem 1 is open in $Q \times Q \times \cdots \times Q$ and the class C is dense in Q). Hence if we add an appropriate element from C to this sequence we get a dense subgroup of $\tilde{G}$ (see the proof of Theorem 1) and therefore we have the right-hand inequality in ($\star\star\star$). Let $\overline{\langle g_1, \ldots, g_k \rangle} = \tilde{G}(\overline{K})$ for some $g_1, \ldots, g_k \in C$. Further, let $\hat{g}_1 \in \hat{G}(\overline{K})$ be a fixed preimage of g_1 with respect to ϕ and let $\hat{Q}$ be the conjugacy class of $\hat{g}_1$ in $\hat{G}(\overline{K})$. Let $\hat{g}_2, \ldots, \hat{g}_k \in \hat{Q}$ be a sequence of fixed preimages of $g_2, \ldots, g_k$ with respect to ϕ. Obviously, $\overline{\langle \hat{g}_1, \ldots, \hat{g}_k \rangle} = \hat{G}(\overline{K})$. Thus, the set $\hat{Q}^k$ is dense in $\hat{G}(\overline{K})$ by Corollary 1 and therefore Q^k is dense in $\tilde{G}(\overline{K})$. Let $\tilde{B}\dot{w}_0\tilde{B}$ is the big Bruhat cell of $\tilde{G}$, where $\tilde{B}$ is a Borel subgroup of $\tilde{G}$ and $\dot{w}_0$ is a fixed preimage of the longest element from the Weyl group. We may assume $\dot{w}_0 \in G$. Since the big Bruhat cell is an open subset of $\tilde{G}$ and C^k is dense in $\overline{Q^k}$, we can find an element $g \in (\tilde{B}\dot{w}_0\tilde{B}) \cap C^k$. The uniqueness of the Bruhat decomposition shows that $g \in B\dot{w}_0 B$ where B is a Borel subgroup of G. The eighth power of every conjugacy class which has a non-trivial intersection with the big Bruhat cell covers the whole Chevalley group if the ground field is infinite — this is proved in greater generality in ([GS, Proposition 4]). Hence $C^{8k} = G$ and we get the left-hand inequality of ($\star\star\star$).

References

[Bo] A. Borel, *Linear Algebraic Groups*, Springer-Verlag, Berlin, 1991.

[B] N. Bourbaki, *Groupes et algèbres de Lie IV, V, VI,* Hermann, Paris, 1968.

[C1] R. W. Carter, *Simple Groups of Lie Type,* John Wiley & Sons, London, 1989.

[C2] R. W. Carter, *Finite Groups of Lie Type,* John Wiley & Sons, Chichester, 1993.

[G] N. Gordeev, *Products of conjugacy classes in algebraic groups I, II,* Journal of Algebra **173** (1995), 715–744, 745–779.

[GS] N. Gordeev and J. Saxl, *Products of conjugacy classes in Chevalley groups I. Extended covering numbers,* Israel Journal of Mathematics, this volume.

[Gu] R. M. Guralnick, *Some applications of subgroup structure to probabilistic generation and covers of curves,* in *Algebraic groups and their representations* (R. W. Carter and J. Saxl, eds.), Kluwer Academic Publishers, Dodrecht, Boston, London, 1998, pp. 301–320.

[GK] R. M. Guralnick and W. M. Kantor, *Probabilistic generation of finite simple groups,* Journal of Algebra **234** (2000), 743–792.

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

[St1] R. Steinberg, *Lectures on Chevalley Groups,* Yale University, 1967.