ISRAEL JOURNAL OF MATHEMATICS 130 (2002), 207–248

PRODUCTS OF CONJUGACY CLASSES IN CHEVALLEY GROUPS I. EXTENDED COVERING NUMBERS

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

This paper is concerned with products of conjugacy classes in Chevalley groups. We prove that in any quasisimple Chevalley group G proper or twisted, over any field, the extended covering number is bounded above linearly in terms of the rank of G, that is, for some constant e, for any Chevalley group G, the product of any $e \cdot \mathrm{rank}(G)$ non-central classes covers all of G. We give estimates for the constant e in different cases.

1. Introduction

This paper is concerned with certain properties of products of conjugacy classes in groups. In particular, we consider the covering number and extended covering number in various classes of groups.

* The authors gratefully acknowledge the support of EPSRC through a Visiting Fellowship number GR/M58542 and a Research grant number GR/L92174.
Received May 4, 2000 and in revised form February 23, 2001

Definition: Let G be a group. The *covering number* $cn(G)$ is the smallest integer m such that $C^m = G$ for every conjugacy class C of G which is not contained in any proper normal subgroup of G. The *extended covering number* $ecn(G)$ is the smallest integer e such that the product $C_1C_2\cdots C_e = G$ whenever $C_1, C_2, \ldots, C_e$ are conjugacy classes of G not contained in any proper normal subgroup of G. Here the product X_1X_2 is $\{x_1x_2 \mid x_1 \in X_1, x_2 \in X_2\}$ for $X_\imath \subset G$.

Recent considerations of these concepts start with the collection of papers [AH] of Arad, Herzog and their coworkers. There are references to numerous older papers in [AH].

What is known about these numbers for specific groups? Dvir [D] proved that for the alternating group A_n, $n \geq 5$, $cn(A_n) = [n/2]$, $ecn(A_n) = [n/2]+1$. A. Lev [Lev2] proved that $cn(PSL_n(K)) = n$ under the condition $\mid K \mid\geq 4$ and $n > 2$. Zisser [Z] calculated the covering numbers of the sporadic groups. That seems to be all that is currently known about the precise values of $cn(G), ecn(G)$ for natural classes of groups. The calculations in these cases mentioned are difficult. Even estimates of these numbers are difficult to obtain. In [AH] it is shown that for every finite simple group $ecn(G) \leq k(k-1)/2$, where k is a number of conjugacy classes. The natural classes of groups which could be studied from this point of view are different classes of linear groups, not necessarily finite. In [G] products of conjugacy classes are studied in the case of simple algebraic groups over algebraically closed fields of characteristic zero. In particular, it is proved there that for such a group $cn(G) \leq 4\,\mathrm{rank}(G)$, $ecn(G) \leq 4\,\mathrm{rank}(G) + 2$. In [EGH] it is proved that there exists a constant c such that $cn(G) \leq c \cdot rank(G)$ for every quasisimple Chevalley group G (here $rank(G)$ is the Lie rank of G). The general constant which can be obtained from the proof given there is rather large. It seems that a more careful consideration should give $c \leq 2$, or at least $c \leq 10$. However, to prove even the existence of such a constant is not easy. We also mention a related recent result of Lawther and Liebeck [LL] who proved that every conjugacy class C of a finite simple group G of Lie type has diameter less than $8rank(G) + 5$ (here the diameter of a conjugacy class C of a group G is the smallest integer d such that $G = \bigcup_{m\leq d}(C \cup C^{-1})^m)$. Even more recently, Liebeck and Shalev [LiSh] proved very strong asymptotic results concerning the diameters of simple groups.

In this paper we consider the extended covering numbers for the Chevalley groups.

THEOREM: *There is a constant e such that for any Chevallley group $G = G(F)$ (over any field F), we have the inequality $ecn(G) \leq e \cdot rank(G)$.*

The estimate for the constant e which can be obtained from our proof is rather large in general. In particular, we obtain $ecn(G) \leq 288(r+4)$ for G of rank r greater than 8. Over an algebraically closed field, the bound can be sharpened: here $ecn(G) \leq 4r$ for groups of any r, and there are stronger results also in the case of other infinite fields.

The above results lead us to pose the following question:

QUESTION: *Is there a general constant c such that for every perfect linear group $G \leq GL_n(K)$ over any field K for which the number $ecn(G)$ exists, the inequality $ecn(G) \leq c \cdot n$ holds?*

We are confident that the answer is positive for a number of natural classes of groups G. As a first step, one should look at classes with additional restrictions, and we intend to investigate this further. Natural classes to consider are finite groups and connected algebraic groups. The class of Chevalley groups plays an intermediate role between the two, and our results provide evidence that the answer indeed may be positive.

The lifting procedure which we use to compare "covering" in a parabolic subgroup and its Levi factor allows us in addition to extend the class of groups which satisfy our bound on extended covering numbers by adding some Chevalley groups over complete local rings. We hope that further work on this will enable us to estimate covering numbers for finite perfect groups through covering numbers of their simple factors.

We now outline the contents of the paper. In section 2 we survey the notation used. Section 3 is concerned with lifting information concerning covering numbers from quotient groups, which is then used later. In section 4 we obtain results for Chevalley groups over algebraically closed fields; in fact, more generally, we investigate here products of conjugacy classes which meet a Borel subgroup, under mild assumptions on the field size. In section 5 we obtain the bound for the extended covering numbers in the case where the defining field is infinite. The next short section is concerned with Chevalley groups of small rank. Finally, in section 7 we prove the general bound, by dealing with classical groups. We first analyze the special linear groups and establish the bound $ecn(SL_n(K)) \leq 6n+24$, and then use that to cover all the classical groups. In the process, we obtain the result that in a crystallographic Chevalley group, every non-central conjugacy class has a non-empty intersection with a general Coxeter cell of the Bruhat decomposition — a result which is of independent interest.

We mention one consequence of our results. Given a finite group G, the extended generating number $egen(G)$ is the least number k such that in any k

conjugacy classes we can choose elements, one in each class, generating G. As a consequence of our results, using the.theorem [GK] of Guralnick and Kantor, we obtain an upper bound on the extended generating numbers in the finite Chevalley groups, which is linear in the rank of G.

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^+, R^- are the sets of positive and negative roots respectively, $W(R)$ 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 (if it leads to no confusion). In Section 3 we also consider the case when K is a ring.

2.3. There are other types of groups which are also called 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 expressed 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 cases of Suzuki and Ree groups ${}^2B_2(q^2)$, ${}^2G_2(q^2)$, ${}^2F_4(q^2)$. For these groups we put $k = K$. Chevalley groups (untwisted or finite twisted) are quasisimple except in a few cases ([St1], [C1]). For a twisted group there exists also the root system which is obtained from R by gluing roots. We will denote this system by R^F (when we speak only of a corresponding twisted group we shall omit the superscript ^{F}). The notation for root systems in the twisted cases corresponds to [C1] (note, however, that [C1] assigns root system B_r for the groups of the type ${}^2A_{2r}(q^2)$ instead of BC_r). The notation for root subgroups (which can be one, two, or three parameter subgroups) is the same as for 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]) 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 the group N.

An element $g \in G$ is called regular if it is regular as an element of the corresponding simple algebraic group.

2.5. Let $u \in U$. Then the element u can be written as a product of elements of the form $x_\alpha \in X_\alpha$, $\alpha > 0$. This presentation depends on the order in which we take the product. If we fix the order of roots, such a presentation is defined uniquely ([St1], Lemma 17). Moreover, if α is a simple root and $u_\alpha = x_\alpha$ is the corresponding root factor of u in *some* decomposition of u into a product of root elements, then the condition $u_\alpha = 1$ does not depend on the decomposition (i.e., it holds or does not hold for every possible decomposition). This follows from the Chevalley commutator formula. The Chevalley commutator formula also implies the following fact. If α is a simple root and if $u_\alpha = 1$ for some $u \in U$, then $gug^{-1} \in U$ for every $g \in \langle X_{\pm\alpha}\rangle$.

2.6. We use below the notion of *big field.* This is designed to guarantee the existence of sufficiently many regular elements in H satisfying certain desirable conditions. We say that a Chevalley group G is over a *big field* K if $\mid K \mid > (4(\mid R \mid + 2r) + 1)^2$ for every case except $R = G_2$, in which case $\mid K \mid > 73^3$. (The right sides of inequalities could be decreased for specific families; in particular, the exponents 2, 3 could be deleted in the untwisted cases.)

2.7. The general notation and terminology below are more or less 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. Lifting from factor groups

Definition 1: Let G be a group, A be a ring and let M be an $A[G]$-module. Further, let $I[G]$ be the augmentation ideal of the group ring $A[G]$. We say that M is an *augmentative* $A[G]$-module if $I[G]M = M$.

The following result is an extension of Lemma 3 of [EGH].

PROPOSITION 1: *Let $F = \langle f_1, \dots, f_k \rangle$ be a group and let A be a commutative ring, let $A[F]$ be a group ring and $I[F]$ its augmentation ideal. Further, let M be an $A[F]$-module. Then the image of the homomorphism*

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

of A-modules given by the formula

$$\Phi((m_1, \dots, m_k)) = (1 - f_1)m_1 + f_1(1 - f_2)m_2 + \cdots + f_1 f_2 \cdots f_{k-1}(1 - f_k)m_k$$

contains $I[F]M$. Thus, if M is an augmentative F-module then Φ is surjective.

Proof: Put $m_1 = 0, \dots, m_{i-1} = 0, m_{i+1} = 0, \dots, m_k = 0$. From the definition of Φ we get

$$f_1 f_2 \cdots f_{i-1}(1 - f_i)M \subset Im\Phi \tag{1}$$

for every $i > 1$ and

$$(1 - f_1)M \subset Im\Phi. \tag{2}$$

The inclusion (2) implies the inclusion $(1 - f_1)Im\Phi \subset Im\Phi$, which in turn implies $f_1(Im\Phi) \subset Im\Phi$. Further, $(1 - f_1^{-1})M = (f_1 - 1)f_1^{-1}M \subset (f_1 - 1)M = (1 - f_1)M$ and therefore $(1 - f_1^{-1})Im\Phi \subset Im\Phi$. Thus $f_1^{\pm 1}(Im\Phi) \subset Im\Phi$. Assume now that

$$f_i^{\pm 1}(Im\Phi) \subset Im\Phi \tag{3}$$

for every $i < j$. Then (3) also holds for $i = j$. Indeed, it is enough to multiply both sides of the inclusion (1) (with $i = j$) by $f_{j-1}^{-1} f_{j-2}^{-1} \cdots f_1^{-1}$ and then use the assumption to get

$$(1 - f_j)M \subset Im\Phi, \tag{4}$$

which gives us (3) for $i = j$. Now (3) and (4) imply that $Im\Phi$ is an $A[F]$-submodule of the $A[F]$-module M and the factor module $M/Im\Phi$ is trivial as an F-module (i.e., all elements of this module are F-invariants). Hence $I[F]M \subset Im\Phi$ as claimed. If M is an augmentative $A[F]$-module then Φ is surjective. ∎

The following identity is easily checked by direct computation:

$$\begin{gathered}(x_1 y_1 x_1^{-1})(x_2 y_2 x_2^{-1}) \cdots (x_k y_k x_k^{-1}) y_k^{-1} y_{k-1}^{-1} \cdots y_1^{-1} = \\ [x_1, y_1](y_1 [x_2, y_2] y_1^{-1}) \cdots (y_1 y_2 \cdots y_{k-1} [x_k, y_k] y_{k-1}^{-1} \cdots y_2^{-1} y_1^{-1})\end{gathered} \tag{$*$}$$

(Here $x_1, \dots, x_k$ and $y_1, \dots, y_k$ are elements of a group.)

From Proposition 1 and $(*)$ we get:

PROPOSITION 2: *Let G be a group satisfying the following conditions:*

1. *There exists a sequence of normal subgroups $G \geq N = N_0 \geq N_1 \cdots \geq N_i \cdots$ (infinite or finite) satisfying the following conditions.*

a.
$$G = \lim_{\leftarrow} G/N_i.$$

b. *Every factor N_i/N_{i+1} is a module over a commutative ring A_i.*

c. $[N, N_i] \subset N_{i+1}$ *for every* $i \geq 0$.

2. *There exist elements $g_1, \ldots, g_k \in G$ satisfying the following condition. Let $\overline{g_1}, \ldots, \overline{g_k}$ be the images of the elements $g_1, \ldots, g_k$ in the factor group G/N and let $\Gamma = \langle \overline{g_1}, \ldots, \overline{g_k} \rangle$. Then N_i/N_{i+1} is an augmentative $A_i[\Gamma]$-module for every i.*

Further, let $X_1, X_2 \subset G$ be any two subsets such that $\overline{X_1} = \overline{X_2} = G/N$ where $\overline{X_1}, \overline{X_2}$ are the images in the factor group G/N of the sets X_1, X_2.

Then

$$N \subset (C_1C_2 \cdots C_k)X_1,$$
$$G = (C_1C_2 \cdots C_k)X_1X_2.$$

Proof: We show that every element $n \in N$ can be written in the form

$$n = (n_1g_1n_1^{-1}n_2g_2n_2^{-1} \cdots n_kg_kn_k^{-1})g_k^{-1}g_{k-1}^{-1} \cdots g_1^{-1} \tag{5}$$

for some $n_1, \ldots, n_k \in N$.

Consider the $A_0[\Gamma]$-module N/N_1. According to Proposition 1 and $(*)$ we have the equality (5) modulo N_1. Assume

$$n \equiv (n_1g_1n_1^{-1}n_2g_2n_2^{-1} \cdots n_kg_kn_k^{-1})g_k^{-1}g_{k-1}^{-1} \cdots g_1^{-1}(modN_i) \tag{6}$$

for some i and some $n_1, \ldots, n_k \in N$. We denote the right side of (6) by r_i and put $m_i = nr_i^{-1}$. Hence (6) implies $m_i \in N_i$. Further, the action of the element $n_jg_jn_j^{-1}$ on N_i/N_{i+1} which is induced by conjugation is the same as the action of g_j, by condition 1.c. Thus we can use $(*)$ and Proposition 1, putting in $(*)$ the elements $n_jg_jn_j^{-1}$ instead of the elements y_j and the elements $l_j \in N_i$ instead of the x_j. Therefore we can write m_i in the form

$$\begin{aligned} m_i \equiv &(l_1n_1g_1n_1^{-1}l_1^{-1})(l_2n_2g_2n_2^{-1}l_2^{-1}) \cdots (l_kn_kg_kn_k^{-1}l_k^{-1}) \\ &\times (n_kg_k^{-1}n_k^{-1})(n_{k-1}g_{k-1}^{-1}n_{k-1}^{-1}) \cdots (n_1g_1^{-1}n_1^{-1}) \ (modN_{i+1}) \end{aligned} \tag{7}$$

for some $l_1, \ldots, l_k \in N_i$. Now if we put l_jn_j in instead of n_j, we get the equality (5) modulo N_{i+1}. This follows from (6), (7) and the definition of m_i. Thus, correcting the elements n_j at every step i by multiplying them by elements from

N_{i+1} we construct elements satisfying (5), since G is a direct limit of the G/N_i (by condition 1.a).

Now put $g_0 = g_k^{-1}g_{k-1}^{-1}\cdots g_1^{-1}$. From the definition of X_1 we have $g_0 = f_0n_0$ where $f_0 \in X_1$ and $n_0 \in N$. Then (5) implies

$$N \subset (C_1C_2\cdots C_k)X_1n_0.$$

Since $Nn_0^{-1} = N$ we have our first assertion. From the definition of X_2 we have that every $g \in G$ can be written in the form $g = nf$ where $f \in X_2$ and $n \in N$. Therefore the second assertion follows from the first. ∎

Proposition 3: *Let G, N be as in the previous Proposition and assume that conditions 1 and 2 hold. Then*

$$ecn(G) \leq 3k(ecn(G/N)), \quad cn(G) \leq 3k(cn(G/N)).$$

Proof: Let $m = ecn(G/N)$ (we assume that m exists — otherwise there is nothing to prove) and let $C_1, C_2, \ldots, C_{3km}$ be conjugacy classes of G, where no C_i is contained in any proper normal subgroup of G. Let $\overline{C_\imath}$ be the image of $C_\imath$ in G/N. Since the product of any m classes $\overline{C_i}$ equals the whole group G/N, we can write each element from the set $\{\overline{g_1}, \ldots, \overline{g_k}\}$ (recall, that these elements satisfy condition 2 as a product of m representatives of conjugacy classes $\overline{C_\imath}$). Therefore we can find a system of representatives $f_\imath \in C_\imath$ in any km conjugacy classes, say, $C_1, \ldots, C_{km}$ such that $\langle\overline{g_1}, \ldots, \overline{g_k}\rangle \leq \langle\overline{f_1}, \ldots, \overline{f_{km}}\rangle$. Now condition 2 will hold if we consider instead of elements $g_1, \ldots, g_k$ the elements $f_1, \ldots, f_{km}$. Moreover, the sets $X_1 = C_{km+1}C_{km+2}\cdots C_{2km}$ and $X_2 = C_{2km+1}C_{2km+2}\cdots C_{3km}$ satisfy the conditions of Proposition 2. Thus we have $G = C_1C_2\cdots C_{3km}$ and therefore the first inequality holds. The second is proved in the same way. ∎

One can apply the previous results to a more concrete situation. We announce a theorem, which can be proved using the techniques developed here; a proof will appear in a later paper.

Theorem 1: *Let G be a Chevalley group (untwisted), over a complete local ring A with a maximal ideal M and residue field $K = A/M$. Further, let $\overline{G}$ be the corresponding Chevalley group over the field K. Assume that the group $\overline{G}$ is quasisimple. Then*

$$ecn(G) \leq 6(ecn(\overline{G})), \quad cn(G) \leq 6(cn(\overline{G})).$$

4. Covering and extended covering numbers for simple algebraic groups over algebraically closed fields

This section contains a generalisation and extension of the results [G] to the cases of non-zero characteristic.

Let G be a simple algebraic group defined over a field K and let $\overline{cn}(G)$, $\overline{ecn}(G)$ be topological covering and extended covering numbers of G, i.e.,

$$\overline{cn}(G) = min\{k|\ \overline{C^k} = G\}, \quad \overline{ecn}(G) = min\{m|\ \overline{C_1C_2\cdots C_m} = G\}$$

for all non-central conjugacy classes $C, C_1, \ldots, C_m$ (where $\overline{X}$ is the Zariski closure of X). A product of conjugacy classes is a constructible subset of G and therefore contains a Zariski open subset of its closure. Since the product of any two open subsets of G coincides with G ([Bo], I, 1, Prop. 1.3), we have

$$\frac{1}{2}cn(G) \leq \overline{cn}(G) \leq cn(G), \quad \frac{1}{2}ecn(G) \leq \overline{ecn}(G) \leq ecn(G).$$

Thus estimates for topological covering numbers give estimates for covering numbers. In the case where charK=0 it was proved in [G] that

$$\overline{cn}(G) \leq 2r, \quad \overline{ecn}(G) \leq 2r+1.$$

(Here $r = \operatorname{rank}(G)$.) The proof of such inequalities in [G] partly depends on the characteristic of the ground field K being 0 because the theorem of Morozov–Jacobson was used (which also holds in the case of characteristic $p \neq 0$ with the exception of G_2 in characteristic 3, but only for unipotent elements of order p). Here we give a stronger result which holds in every characteristic.

Let R be the root system corresponding to G. Put $l(R) = r+1$ if all roots in R have the same length and $l(R) = 2r$ if R contains roots of different length.

THEOREM 2: *For K algebraically closed, we have*

$$\overline{cn}(G) \leq \overline{ecn}(G) \leq l(R).$$

Moreover, if G is a group of type A_r, B_r, C_r then the inequalities above are equalities.

The proof of this Theorem can be obtained from a more general fact formulated in the next Theorem. However, a more direct proof of Theorem 2 can be given; namely, using the fact that the semisimple part in the Jordan decomposition of an element g lies in the closure of the conjugacy class of g, and the fact that the closure of the conjugacy class of any non-trivial unipotent element contains a root element, one can simplify the proof below.

THEOREM 3: *Let G be a Chevalley group of rank r over a big field K and let R be the corresponding root system. Further, let $C_1, \ldots, C_k$ be non-central conjugacy classes of G such that each class C_i has a non-trivial intersection with a Borel subgroup of G. If $k \geq l(R)$, then the product $C_1C_2\cdots C_k$ contains a regular semisimple element of G. If K is an infinite field, this product contains a subset of H which is dense in the maximal torus T. Moreover, if all roots in the root system R have the same length, then for every big field K and $r > 1$ this product contains all semisimple regular elements of G.*

Theorem 2 now follows easily from Theorem 3. Indeed, for any algebraic group G the group of points $G(\overline{K})$ is a Chevalley group over $\overline{K}$. Since $C_1C_2\cdots C_k$ contains a dense subset of $T(\overline{K})$ then $T(\overline{K}) \subset \overline{C_1C_2\cdots C_k}$. Hence the set $\overline{C_1C_2\cdots C_k}$ contains all semisimple elements from the group $G(\overline{K})$ and therefore $\overline{C_1C_2\cdots C_k} = G(\overline{K})$ and we have the first assertion of Theorem 2. Consider the case when G is of type A_r, B_r, C_r. Let $g \in G(\overline{K})$ be a long root element if $R = A_r, C_r$ and let $g = h_{\epsilon_1}(i)h_{\epsilon_2}(i)\cdots h_{\epsilon_r}(i)$ if $R = B_r$, where $i = \sqrt{-1}$ (we may assume that $\operatorname{char} K \neq 2$ for the case $R = B_r$). Further, let C be the conjugacy class of g in the group $G(\overline{K})$. If we consider a natural form of G, i.e., SL, SO, Sp, we can see that $\overline{C^m} \neq G(\overline{K})$ if $m < l(R)$ (every element in such C^m will always have fixed vectors in cases $R = A_r, C_r$; in case B_r such an element has two independent eigenvectors with eigenvalues 1 and ±1).

We remark that the result claimed in [Kn] implies that there is equality in Theorem 2 also in the case D_r, provided that the characteristic is not 2.

From Theorem 3 we also have the following result which will be used in the next section.

COROLLARY 1: *Let G be a simple algebraic group defined over an infinite field K. Let $C_1, \ldots, C_k$ be non-central conjugacy classes of $G(K)$. If $k \geq l(R)$ then the product $C_1C_2\cdots C_k$ is Zariski dense in G.*

Proof: Let $c_i \in C_i$ and let Q_i be the conjugacy class of c_i in $G(\overline{K})$. Since K is an infinite field and G is a simple group, the set $G(K)$ is dense in $G(\overline{K})$ ([Bo], 18.3). Now C_i is dense in Q_i and hence $C_1C_2\cdots C_k$ is dense in $Q_1Q_2\cdots Q_k$ but the latter product is dense in $G(\overline{K})$. Thus $C_1C_2\cdots C_k$ is dense in G. ∎

Now we start the proof of Theorem 3.

LEMMA 1: *Let G be a Chevalley group corresponding to a root system R and let $G_0 \leq G$ be a Chevalley group corresponding to a subsystem of R. Let $h_1, h_2 \in H$*

and $g \in G_0$, and assume that h_1 is regular in HG_0 and $h_2g \notin Z(HG_0)$. Let C_1, C_2 be the conjugacy classes of h_1, h_2g in HG_0. Then every regular element of HG_0 of the form h_1h_2h with $h \in H \cap G_0$ is contained in C_1C_2.

Proof: Let $\gamma = h_1h_2h$ be a regular element of HG_0, and write $\gamma_1 = h_1, \gamma_2 = h_2g$. There exists an element $\sigma \in HG_0$ such that $\sigma\gamma_2^{-1}\sigma^{-1} = v\gamma_1\gamma^{-1}u = vh_2^{-1}h^{-1}u$ where $v \in U_0^- = U^- \cap G_0, u \in U_0 = U \cap G_0$ ([EG]). Since γ_1, γ^{-1} are regular in HG_0, one can find elements $v_1 \in U_0^-, u_1 \in U_0$ such that $v = [v_1, \gamma_1], u = [\gamma, u_1]$ (see [EG]). Thus, $\sigma\gamma_2^{-1}\sigma^{-1} = (v_1\gamma_1v_1^{-1})(u_1\gamma^{-1}u_1^{-1})$ and therefore $\gamma \in C_1C_2$. ∎

LEMMA 2: *Let G be a Chevalley group and let $g = hu$ be a non-central element of a Borel subgroup, where $h \in H$ and $u \in U$. Then there exists an element $g' = h'u'$ where $h' \in H$, $u' \in U$ which is conjugate to g and such that the element u' written as a product of positive root elements has a non-trivial factor $u'_\alpha \in X_\alpha$ corresponding to some simple root α.*

Proof: We may assume $u \neq 1$: Otherwise we can conjugate $g = h \notin Z(G)$ by an element from the group U. Further, assume that in a decomposition of u as a product of positive root elements there are no factors corresponding to simple roots. Then for every simple root β we have $w_\beta h w_\beta^{-1} \in H$ and $w_\beta u w_\beta^{-1} \in U$. Thus conjugating g by appropriate elements of N corresponding to simple roots we can get an appropriate element. ∎

LEMMA 3: *Let g' be the element from the previous lemma. Let β be a fixed simple root. If α and β have the same length, then there exists an element $g'' = h''u''$ with $h'' \in H, u'' \in U$ which is conjugate to g' and such that the element u'' written as a product of positive root elements has a non-trivial factor $u''_\beta \in X_\beta$.*

Proof: Assume first that α, β are neighbours in the Dynkin diagram. Let $P_{\alpha,\beta}$ be the parabolic subgroup corresponding to the subset $\{\alpha, \beta\}$ of the simple root system, let $V_{\alpha,\beta} = R_u(P_{\alpha,\beta})$ be its unipotent radical and let $G_{\alpha,\beta}$ be the Chevalley subgroup of G generated by root subgroups of the root system $\langle\alpha, \beta\rangle$. Assume that the element g' does not satisfy the conditions for g'' (otherwise there is nothing to prove). Hence we can write g' in the form

$$g' = h'x_\alpha x_{\alpha+\beta} v \tag{8}$$

where $v \in V_{\alpha,\beta}$ (note that when two neighbours are of the same length they generate a root system of type A_2). If h' does not commute with elements of the root group X_β then $g'' = x_\beta(p)g'x_\beta(-p)$ is an appropriate element for every $p \neq 0$. (This follows immediately from the commutator formulas.) Let h' commute with elements of the group X_β but not with elements of the group $X_{\alpha+\beta}$. Then conjugating g' by an appropriate element of the group $X_{\alpha+\beta}$ we can get $x_{\alpha+\beta} = 0$ in (8). Then the element $g'' = w_\alpha w_\beta g' w_\beta^{-1} w_\alpha^{-1}$ satisfies our condition (note, that $\sigma v \sigma^{-1} \in V_{\alpha,\beta}$ for every $\sigma \in G_{\alpha,\beta}$). Now assume that h' commutes with both subgroups $X_\beta, X_{\alpha+\beta}$. Then it commutes with $X_{-\beta}, X_{-\alpha-\beta}$ and therefore with the whole group $G_{\alpha,\beta}$. But $G_{\alpha,\beta}$ is a factor group of $SL_3(K)$ by a subgroup contained in the centre. This implies that $\sigma x_\alpha x_{\alpha+\beta}\sigma^{-1} = x_\beta$ for some $\sigma \in G_{\alpha,\beta}$. Now $g'' = \sigma g' \sigma^{-1}$ is an appropriate element.

Now consider the general case. Since we can make by conjugation a non-trivial factor corresponding to the neighbour on the Dynkin diagram, we can move along the diagram until we get to our root β (here we use the property of Dynkin diagrams that any two roots of the same length can be connected by a chain where all the edges correspond to roots of the same length). ∎

Lemma 4: *Let G be a Chevalley group over a field K. Assume that $|K| > 3$ (or $|k| > 3$ in the twisted cases) if $R \neq G_2$ and $|K| > 4$ (or $|k| > 4$ in the twisted case) if $R = G_2$. Let C_1, C_2 be any two non-central conjugacy classes which have a non-trivial intersection with a Borel subgroup. Then for every simple root α there exists an element $g = hu \in C_1C_2$ such that $h \in H, u \in U$ and in an expression of u as a product of positive root elements there is a non-trivial factor corresponding to α.*

Proof: According to Lemmas 2 and 3 we may assume that there exist representatives $g_1 = h_1u_1 \in C_1, g_2 = h_2u_2 \in C_2$ where $h_1, h_2 \in H, u_1, u_2 \in U$ satisfying the following conditions. If u_γ is the factor corresponding to the positive root γ in a fixed decomposition of $u \in U$ as a product of positive root elements, then one of the following possibilities holds:

1. $u_{1\alpha} \neq 0$,
2. $u_{1\alpha} = u_{2\alpha} = 0, \quad u_{1\beta}, u_{2\beta} \neq 0$,

where β is a neighbour of α in the Dynkin diagram and the roots α, β have different lengths.

Assume that we are in case 1. Since $|K| > 3$ (or $|k| > 3$) we may assume that $h_2^{-1}u_{1\alpha}h_2 \neq u_{2\alpha}^{-1}$ (otherwise, we can conjugate the element g_1 by an appropriate element from H). Then $g = g_1g_2$ is an appropriate element.

Now consider case 2. Let P_β be the parabolic subgroup corresponding to the simple root subsystem $\{\beta\}$ and let V_β be its unipotent radical. We have $u_1 = v_1u_{1\beta}, u_2 = u_{2\beta}v_2$ where $v_1, v_2 \in V_\beta$. Note, that for every $\tau \in H\langle X_{\pm\beta}\rangle$ we have $\tau V_\beta \tau^{-1} = V_\beta$. Further, there exist elements $\sigma_1, \sigma_2 \in \langle X_{\pm\beta}\rangle$ such that

$$\sigma_1 h_1 u_{1\beta}\sigma_1^{-1} = u'_{1\beta}\dot{w}_{1\beta}, \quad \sigma_2 h_2 u_{2\beta}\sigma_2^{-1} = \dot{w}_{2\beta}u'_{2\beta}$$

where $\dot{w}_{1\beta}, \dot{w}_{2\beta}$ are different preimages in N of w_β (this follows from the fact that non-central conjugacy classes cannot be contained in the Borel subgroup). Now $\dot{w}_{1\beta}\dot{w}_{2\beta} = h \in H$. Moreover, conjugating $\dot{w}_{1\beta}$ by an appropriate element from the group H we can get $[h, x_\alpha] \neq 1$ (here we use the assumption of the lemma about the field K). Now one can see that the element $x_\alpha(\sigma_1 g_1 \sigma_1^{-1})(\sigma_2 g_2 \sigma_2^{-1})x_\alpha^{-1}$ is an appropriate element from C_1C_2. ∎

Lemma 5: *Let G be a Chevalley group of rank $r > 1$ over a big field K. Let $j > 1$, and write*

$$X_j = \{h_{\alpha_1}(x_1)h_{\alpha_2}(x_2)\cdots h_{\alpha_{j-1}}(x_{j-1})h_0 |\, x_1, x_2, \ldots, x_{j-1} \in K^*(\text{or } k^*)\},$$

where h_0 is a fixed element from the group $\langle h_{\alpha_m}(s)|\, s \in K^*(\text{or } k^*), m \geq j\rangle$.

Suppose that there is no root in the root subsystem $R_j = \langle\alpha_1, \ldots, \alpha_j\rangle$ which is orthogonal to each of $\alpha_1, \ldots, \alpha_{j-1}$.

Then the set X_j contains a regular element $h \in H$ of the group HG_j where $G_j = \langle X_{\pm\gamma}|\, \gamma \in \langle\alpha_1, \ldots, \alpha_j\rangle\rangle$.

Proof: Assume G is untwisted. Let $\gamma \in R_j$. The condition of the lemma implies that γ is not orthogonal to some α_i with $i < j$. Thus the image of the group $\langle h_{\alpha_i}(x)|x \in K^*\rangle$ in K^* under the homomorphism γ is equal to K^{*n} where $n =< \alpha_i, \gamma >$. Note that $n = \pm1, \pm2, \pm3$ and the last is possible only for the root system G_2 which does not satisfy the condition of the lemma. Thus

$$K^{*2} \subset \gamma(\langle h_{\alpha_i}(x)|x \in K^*\rangle) \subset K^*. \tag{9}$$

Now put

$$X_{j\gamma} = \{x \in X_j|\gamma(x) = 1\}.$$

Suppose that K is a finite field. Then (9) implies

$$|X_{j\gamma}| \leq \frac{2|X_j|}{|K^*|}. \tag{10}$$

Therefore

$$\left|\bigcup_{\gamma\in R_j^+} X_{j\gamma}\right| \le \frac{2|X_j|}{|K^*|}|R_j^+| = |X_j|\frac{|R_j|}{|K^*|} < |X_j|$$

(the last inequality follows from the assumption that K is a big field for G). Hence the set

$$X_j' = X_j \setminus \bigcup_{\gamma\in R^+} X_{j\gamma}$$

is not empty. The definition of X_j' implies that all its elements are regular in HG_j.

Suppose that K is an infinite field. Then we may consider the group HG_j as a subgroup of $T(K)\tilde{G}_j(K)$ where $\tilde{G}_j$ is the corresponding simple algebraic group. Then the set X_j is a subset of $Y_j(K)$ where Y_j is an algebraically closed subset of $\tilde{G}_j$ which is the translation of a $(j-1)$-dimensional torus by the fixed element h_0. Unirationality of the torus and infiniteness of K imply density of X_j in Y_j (see [Bo], 18.3) and hence X_j has a non-empty intersection with any non-empty open subset of Y_j. On the other hand, (9) implies that the set $X_{j\gamma}$ is contained in a proper closed subset of Y_j and therefore the set of regular elements of the group $T\tilde{G}_j$ is open in Y_j.

Let now G be a finite twisted group. Again we can exclude the case where the root system is G_2 and for the same reason also the case ${}^2F_4(q)$. Now instead of root maps $\gamma\colon H \longrightarrow K^*$ we have to consider either such maps or pairs of maps $\gamma_1, \gamma_2\colon H \longrightarrow K^*$, where $\gamma \in R$ is a root such that the corresponding root subgroup X_γ is a two parameter subgroup $X_\gamma = X_\gamma(u,v)$ and where γ_1, γ_2 are the homomorphisms induced by the action of H on the parameters of X_γ. For every γ_l (where $l=1$ or $l=1,2$) instead of (9) we now have

$$k^{*2} \subset \gamma_l(\langle h_{\alpha_i}(x) |\, x\in K^*(\text{or}, x\in k^*)\rangle) \subset K^*$$

(recall that $k=K$ if G is a Suzuki or a Ree group, and otherwise $k=K^\theta$). Since we exclude the case G_2, i.e., the type ${}^3D_4$, we have

$$|k^{*2}| > \frac{\sqrt{|K^*|}-1}{2}.$$

Now using the same argument as in the untwisted case we show that the set $X_j' = X_j \setminus \bigcup_{\gamma\in R_j^+} X_{j\gamma_l}$ is not empty if $|K^*| > (2|R|+1)^2$. This gives us a semisimple regular element in the set X_j. ∎

LEMMA 6: *Let G be a Chevalley group of rank > 1 over a big field.*

Let $Y = \{\beta_1, \dots, \beta_r\} \subset R$ be a set of linearly independent roots and let $H_Y = \{h_{\beta_1}(t_1^2)h_{\beta_2}(t_2^2)\cdots h_{\beta_r}(t_r^2) |\ t_1, t_2, \dots, t_r \in K^*$(or k^* in the twisted case)$\}$. Further, for every $i \leq r$ fix a set $M_i \subset K^{*2}$(or k^{*2}), $|M_i| \leq 2$ (if $R \neq G_2$) and $|M_1| \leq 3$ (if $R = G_2$). Put

$$H_M = \{h_{\beta_1}(t_1^2)h_{\beta_2}(t_2^2)\cdots h_{\beta_r}(t_r^2) |\ t_i^2 \in M_i \text{ for some } 1 \leq i \leq r\}.$$

Then for every $h \in H$ the set $h(H_Y \setminus H_M)$ contains a regular element. If K is infinite then the set $h(H_Y \setminus H_M)$ is dense in T.

Proof: We use the same arguments as in the previous lemma. Namely, let hH'_Y be the subset of hH_Y consisting of such elements h' which satisfy the condition $\gamma(h') = 1$ for some positive root γ (or $\gamma_i(h') = 1$ for some $i = 1, 2$ in twisted cases). Since the roots in Y are linearly independent, $K^{*n} \subset \gamma(H_Y)$ (or $k^{*n} \subset \gamma_i(H_Y)$) where $n = 2, 4, 6$. If we exclude the groups with $R = G_2$ we have $n \leq 4$ and we get as above

$$|hH'_Y| \leq \frac{|hH_Y| \cdot 4|R|}{|k^*|}.$$

Further, from the definition of hH_M we have

$$|hH_M| \leq \frac{2 \cdot 4 \cdot r|hH_Y|}{|k^*|}.$$

Thus

$$|hH'_Y \cup hH_M| \leq \frac{|hH_Y| \cdot 4(|R| + 2r)}{|k^*|}.$$

Now if $|K| > (4(|R| + 2r) + 1)^2$ then $|k^*| > 4(|R| + 2r)$ and therefore the set $h(H_Y \setminus H_M)$ contains a regular element. Now consider the case $R = G_2$. Here (even in the twisted case ${}^3D_4(q^3)$) we have only one parameter root subgroups. Now we have

$$|hH'_Y| \leq |hH_Y| \cdot 6|R^+|/|k^*| = |hH_Y| \cdot (36/|k^*|),$$
$$|hH_M| \leq 6 \cdot 3 \cdot r \cdot |hH_Y|/|k^*| = |hH_Y| \cdot (36/|k^*|).$$

Thus, if $|K| > (36 + 36 + 1)^3$ then $|k^*| > 36 + 36$ and we have a regular element in $h(H_Y \setminus H_M)$.

The assertion about the density of $h(H_Y \setminus H_M)$ is obvious. ∎

LEMMA 7: *Assume that R is not one of B_2 $(= C_2), G_2, F_4$ or a non-crystallographic system corresponding to ${}^2F_4$. Then there exists a numbering of simple roots $\alpha_1, \ldots, \alpha_r$ such that for every $1 \leq i \leq r-1$ the root system generated by $\alpha_1, \ldots, \alpha_{i+1}$ is irreducible and does not contain a root γ which is orthogonal to all $\alpha_1, \ldots, \alpha_i$.*

Proof: For the cases $R = A_r, B_r (r > 2), C_r (r > 2), D_r (r \geq 4)$ we can take the standard numbering of Bourbaki ([B], Tables I-X). In cases $R = E_6, E_7, E_8$ one can take the numbering where roots $\alpha_1, \ldots, \alpha_{r-1}$ generate the root system D_{r-1} and α_r is the root of the type $\frac{1}{2}(\sum \epsilon_i)$. Note that roots of the latter type cannot be orthogonal simultaneously to a pair of roots $\epsilon_i \pm \epsilon_j$. ∎

Now we give the proof of Theorem 3 for the case where $r > 1$ and all the roots are of the same length.

We assume that the numbering of simple roots in R satisfies the conditions of Lemma 7. Let R_i be the irreducible root system generated by the subset $\{\alpha_1, \ldots, \alpha_i\}$ of the simple root system and let $G_i = \langle X_\gamma | \gamma \in R_i \rangle$. Let P_i be the standard parabolic subgroup of G corresponding to R_i and let V_i be its unipotent radical. Then HG_i is a Levi factor of P_i.

According to Lemmas 2 and 3 we can choose representatives $g_1 = h_1 u_1 \in C_1, \ldots, g_k = h_k u_k \in C_k$ where $h_1, \ldots, h_k \in H, u_1, \ldots, u_k \in U$ such that in an expression of each u_i as a product of positive root elements there is a non-trivial factor corresponding to the root α_1. We can write the elements g_1, g_2 in the form

$$g_1 = h' h_{\alpha_1}(p) u_{1\alpha_1} v_{11}, \quad g_2 = h'' h_{\alpha_1}(q) u_{2\alpha_1} v_{12} \tag{11}$$

where h', h'' are elements from the subgroup of H generated by elements $h_{\alpha_j}(a)$ with $j > 1$, $1 \neq u_{1\alpha_1}, u_{2\alpha_1} \in X_{\alpha_1}$, $v_{11}, v_{12} \in V_1$. Further, we can find elements $\sigma, \tau \in HG_1$ such that

$$(\sigma h' h_{\alpha_1}(p) u_{1\alpha_1} \sigma^{-1})(\tau h'' h_{\alpha_1}(q) u_{2\alpha_2} \tau^{-1}) = h' h'' h_{\alpha_1}(t), \tag{12}$$

where $t \in K^*$ (or $t \in k^*$) is any prescribed element except maybe one for which $h'h''h_{\alpha_1}(t) \in Z(HG_1)$ (this follows from [EG] and the fact that all non-trivial unipotent elements in G_1 are HG_1-conjugate).

From (11) and (12) we have elements $h'h''h_{\alpha_1}(t)v \in C_1C_2$, where $v \in V_1$ and where t can be any prescribed element from K^* (or k^*) except maybe one for which $h'h''h_{\alpha_1}(t) \in Z(HG_1)$. By Lemma 5 we can choose the value of the parameter t such that the element $h'h''h_{\alpha_1}(t)$ is a regular element in HG_2 (note that the possible exclusion of elements $h'h''h_{\alpha_1}(t) \in Z(HG_1)$ from the set X_2

defined in Lemma 5 does not influence the claim because the elements excluded cannot be regular for HG_2). Put $\tilde{h}_2 = h'h''h_{\alpha_1}(t)$. Thus, $\tilde{h}_2 v \in C_1C_2$ where $\tilde{h}_2$ is a regular element of HG_2. Since $\tilde{h}_2 \in H$ is a regular element of the group HG_2 there exists a unipotent element u from the group $U_2 = G_2 \cap U$ such that $u\tilde{h}_2vu^{-1} = \tilde{h}_2\tilde{v}_2$ where $\tilde{v}_2 \in V_2$. Indeed, the element $v \in V_1$ can be written in the form $v = \tilde{v}_1\tilde{v}_2'$ where $\tilde{v}_1 \in U_2$ and $\tilde{v}_2' \in V_2$. Since $\tilde{h}_2$ is a regular element of HG_2, every element of U_2 can be written in the form $[\tilde{h}_2^{-1}, \tilde{u}]$ for some $\tilde{u} \in U_2$ (this is a simple and well-known fact — see, for instance, [EG]). Thus, we have $\tilde{v}_1^{-1} = [\tilde{h}_2^{-1}, \tilde{u}]$ for some $\tilde{u} \in U_2$. Hence $\tilde{u}\tilde{h}_2v\tilde{u}^{-1} = \tilde{h}_2[\tilde{v}_1^{-1}, \tilde{u}](\tilde{u}\tilde{v}_2'\tilde{u}^{-1})$ where $\tilde{u}\tilde{v}_2'\tilde{u}^{-1} \in V_2$, $[\tilde{v}_1^{-1}, \tilde{u}] \in U_2$. Moreover, the element $[\tilde{v}_1^{-1}, \tilde{u}]$ lies in the next member of the central series of the group U_2, compared with the element $\tilde{v}_1$. Thus acting in this way we can eliminate the $\tilde{v_1}$-part of v.

Now we have an element of the form $\tilde{h}_2\tilde{v}_2 \in C_1C_2$ and $g_3 = h_3u_3 \in C_3$, where $\tilde{h}_2$ is a regular element of $HG_2, \tilde{v}_2 \in V_2, h_3 \in H, u_3 \in U$ is an element which has a non-trivial u_{α_1}-factor. Let Q be the conjugacy class of $\tilde{h}_2\tilde{v}_2$. Note that $\tilde{h}_2\tilde{v}_2, g_3 \in P_2$. Moreover, the image of $\tilde{h}_2\tilde{v}_2$ in the factor group $P_2/V_2 \cong HG_2$ is a regular semisimple element of HG_2 and the image of g_3 in P_2/V_2 is a non-trivial element (because the u_{α_1}-factor of u_3 is non-trivial). Thus we can apply Lemma 1 to the conjugacy classes of images of elements $\tilde{h}_2\tilde{v}_2, g_3$ in $P_2/V_2 \cong HG_2$. This implies that the product QC_3 contains elements of the form

$$\tilde{h}_2h_3h_{\alpha_1}(t_1)h_{\alpha_2}(t_2)v_2 \tag{13}$$

where $v_2 \in V_2$ and where parameters t_1, t_2 take all possible values for which the element $\tilde{h}_2h_3h_{\alpha_1}(t_1)h_{\alpha_2}(t_2)$ is regular in HG_2. Lemma 5 guarantees that among such elements one can find a regular element of the group HG_3. Thus, $\tilde{h}_3v_2 \in QC_3 \subset C_1C_2C_3$ where $\tilde{h}_3$ is a regular element of the group HG_3 and $v_2 \in V_2$. Since the element $\tilde{h}_3$ is regular in HG_3 we can conjugate the element $\tilde{h}_3v_2$ by an appropriate element from $U_3 = HG_3 \cap U$ (as we did above) to get an element of the form $\tilde{h}_3\tilde{v}_3 \in C_1C_2C_3$, where $\tilde{v}_3 \in V_3$. Continuing this process we obtain in the product of $r + 1$ conjugacy classes all regular elements of H. The further multiplication cannot eliminate any such element, again by Lemma 1.

Consider now the case $r = 1$.

Here G is of type A_1, ${}^2A_2(q^2)$, ${}^2B_2(q^2)$, ${}^2G_2(q^2)$. We take representatives of conjugacy classes $g_1 \in C_1, g_2 \in C_2$ in the form $g_1 = b_1\dot{w}, g_2 = \dot{w}b_2$ where w is a generator of W and $b_1, b_2 \in B$. Then $g_1g_2 = hu$ for some $h \in H$ and $u \in U$. Here $H = \langle h_\alpha(t) | t \in K^* \rangle$. Conjugating now the element g_1 by elements $h_\alpha(t)$ we can get in the product C_1C_2 elements of the form $h[h_\alpha(t), \dot{w}]u'$ for every

t. One can check $[h_\alpha(t), \dot{w}] = h_\alpha(t^2)$ if G is of type A_1, ${}^2B_2(q^2)$, ${}^2G_2(q^2)$ or $[h_\alpha(t), \dot{w}] = h_\alpha(t\bar{t})$ if G is of type ${}^2A_2(q^2)$. In all cases we have in C_1C_2 all regular elements from the set $\{hh_\alpha(t^2)\}$ (or $\{hh_\alpha(t\bar{t})\}$). This set is dense in T if K is infinite.

Cases B_r, C_r with $r \geq 2$.

We may assume that $k = 2r$ (because of Lemma 1). Suppose that among the classes $C_1, \ldots, C_{2r}$ there exists a class, C_1 say, which has a representative $g_1 = h_1u_1$, $h_1 \in H$, $u_1 \in U$ such that $u_{1\alpha_1} \neq 1$ where $u_{1\alpha_1}$ is the corresponding root-factor in the decomposition of u_1 as a product of positive root elements. Then we consider

$$C_1(C_2C_3)(C_4C_5)\cdots(C_{2r-2}C_{2r-1})C_{2r}.$$

In every product C_iC_{i+1} one can find a representative like in C_1 (this follows from Lemma 4). Following the same procedure as in the first case we can get an element $h \in H \cap C_1(C_2C_3)\cdots(C_{2r-2}C_{2r-1})$ which is regular in G. Then we have from Lemma 1 that the product of such $2r$ conjugacy classes contains all regular semisimple elements from the group H.

Suppose that there is no such representative in all classes considered. Then for every $i = 1, \ldots, 2r$ there exists a representative $g_i \in C_i$ of the form

$$g_i = h_ix_\alpha v \tag{14}$$

where $h_i \in H, \alpha \in \Pi, 1 \neq x_\alpha \in X_\alpha, v \in U$ and among root factors of any decomposition of v as a product of root elements there is no non-trivial factor from X_α (note that this property does not depend on the decomposition because α is a simple root). Since we have no representatives with $\alpha = \alpha_1$ we may assume that $\alpha = \alpha_r$ (Lemma 3) and among factors of v in every decomposition into a product of positive root elements there are no factors corresponding to α_r and to roots of the form $\epsilon_k - \epsilon_l$. Otherwise we can get a representative as in the previous case conjugating g_i by an appropriate element from the Weyl group W_1 corresponding to the root subsystem $\langle\alpha_1, \ldots, \alpha_{r-1}\rangle$ (see the proof of Lemma 2). Now we take two conjugacy classes C_p, C_q and take their representatives of the form (14). We can get in C_pC_q elements of the form

$$g_{pq} = h_{pq}h_{\alpha_r}(t^2)u \tag{15}$$

for every $t \in K^*$ (or $t \in k^*$ in twisted cases; note that in the case ${}^2A_{2r}(q^2)$ we can even take t instead of t^2 in (15)), where $h_{pq} \in H$ is a fixed element depending on the classes C_p, C_q, and $u \in U$. Indeed, let P be the parabolic subgroup of G corresponding to the root α_r, i.e., the parabolic subgroup where the group $L = H\langle X_{\pm\alpha_r}\rangle$ is a Levi factor. Further, let $V = R_u(P)$ be the unipotent radical. Take two elements $g_p \in C_p$, $g_q \in C_q$ of the form (14). Then $g_p, g_q \in P$ and the images of such elements in L with respect to the natural homomorphism $P \longrightarrow L$ do not belong to the center of L (this follows from (14)). Now conjugating these elements by appropriate elements from the group L we can obtain elements of the form $b_1\dot{w}_{\alpha_r}v_1$, $\dot{w}_{\alpha_r}b_2v_2$ where $b_1, b_2 \in HX_\alpha, v_1, v_2 \in V$. Then we can apply the same procedure that we used in the case $r = 1$.

Since the elements v in (14) have no root factors from the groups $X_{\epsilon_k - \epsilon_l}$, the elements v_1, v_2 and therefore also the elements u from (15) have no such factors except perhaps factors from $X_{\epsilon_k-\epsilon_r}$ which can appear after conjugation by elements from L. Further, let $h_{pq}x_{\epsilon_k-\epsilon_r}(a)h_{pq}^{-1} = x_{\epsilon_k-\epsilon_r}(t_ka)$, where $t_k \in K^*$ is a fixed element. Since all elements h in (14) commute with elements from the groups $X_{\epsilon_k-\epsilon_r}$ we have $t_1 = t_2 = \cdots = t_{r-1}$. (Indeed, $h_{pq} = h'h_{\alpha_r}(t_0)$ for some element $h' \in H$ which commutes with elements from subgroups $X_{\epsilon_k-\epsilon_r}$ and $t_0 \in K^*$ is a fixed element. This follows from the procedure which gives (15) from (14) as described above.) Thus the elements $h_{pq}h_{\alpha_r}(t^2)$ do not commute with the elements from $X_{\epsilon_k-\epsilon_r}$ except at most two such. Let M_{pq} be the set of parameters t^2 for such elements. We have $|M_{pq}| \leq 2$ and if $t^2 \notin M_{pq}$ then the element $h_{pq}h_{\alpha_r}(t^2)$ does not commute with the elements from $X_{\epsilon_k-\epsilon_r}$. Thus, if $t^2 \notin M_{pq}$ we can eliminate factors of u from $X_{\epsilon_k-\epsilon_r}$ by conjugation of g_{pq} by appropriate elements of the group $X_{\epsilon_k-\epsilon_r}$. Therefore, if $t^2 \notin M_{pq}$ in (15) we may assume $\dot{w}u\dot{w}^{-1} \in U$ for every $w \in W_1$.

Distribute now our conjugacy classes into pairs corresponding to each root β_j which is conjugate to α_r (here $\beta_j = \epsilon_j$ or $2\epsilon_j$). Taking elements of the form (15) belonging to the product of each such pair C_p, C_q and conjugating by an appropriate element $\dot{w}$ with $w \in W_1$, we can get elements of the form $h'_{pq}h_{\beta_j}(t^2)u'$ for every $t^2 \notin M_{pq}$. Thus in the product of $2r$ conjugacy classes we can get elements of the form

$$hh_{\beta_1}(t_1^2)h_{\beta_2}(t_2^2)\cdots h_{\beta_r}(t_r^2)u \tag{16}$$

where $u \in U$, $h \in H$ is a fixed element and the parameters $t_1, \ldots, t_r$ run through K^* (or k^*) except maybe the cases where $t_i^2 \in M_{pq}$ for some p, q. If the H-part in (16) is a regular element then the element of the form (16) is also regular and conjugate to its H-part. Further, all the H-parts of elements of the form (16) constitute a set of the form $h(H_Y \setminus H_M)$ which is defined in Lemma 6. Thus we can apply Lemma 6.

Case r =2 with different root lengths. Here $\Pi = \{\beta, \gamma\}$ is a simple root system (we do not identify here roots β and γ).

We may assume as above $k = 2r = 4$. Assume that among these four conjugacy classes we have two which have representatives in the form (14) with $\alpha = \beta$ and two classes which have representatives in the form (14) but with $\alpha = \gamma$. Then using the same arguments as above we can get all elements of the form $hh_\beta(t_1^2)h_\gamma(t_2^2)$ for a fixed $h \in H$ and all $t_1, t_2 \in K^*$ (or k^*). Now we apply Lemma 6.

Now let all four conjugacy classes have representatives in the form (14) corresponding to only one simple root, so $\alpha = \beta$. The case $R = B_2 = C_2$ was already treated above. Let $R = G_2$. Using the same arguments as above we get in the product of any two classes a representative in the form

$$hh_\beta(t^2)v \tag{17}$$

where the element h is fixed and $v \in U$. Further, $h_\beta(s)x_\gamma(a)h_\beta^{-1}(s) = x_\gamma(s^n a)$ where $n = -1$ or $n = -3$ (in the twisted case ${}^3D_4(q^3)$ we assume $t \in k^*$). Hence for all parameters t^2 in (17) except possibly at most three, the element $hh_\beta(t^2)$ does not commute with elements from X_γ and, therefore, for such parameters t^2 we may assume that among root factors of v there are no non-trivial factors from X_γ. Hence $\dot{w}_\gamma v \dot{w}_\gamma^{-1} \in U$. Put $\delta = w_\gamma(\beta)$. Conjugating the elements of the form (17) by $\dot{w}_\gamma$ and multiplying them for such conjugates, we get in the product of our four classes elements of the form

$$hh_\beta(t^2)h_\delta(s^2)u \tag{18}$$

where h is a fixed element, $u \in U$ and the parameters t, s can have all possible values except possibly sets containing not more than six elements. Hence the set of H-parts of elements of the form (18) which we can find in the product of four conjugacy classes is a set of the form $h(H_Y \setminus H_M)$ and again we can apply Lemma 6.

Let G be a group of type ${}^2F_4(q^2)$ and let β be the root corresponding to the ρ-orbit $\{\alpha_1.\alpha_4\}$ and γ to $\{\alpha_2, \alpha_3\}$ (see Notation 2.3). Then

$$X_\beta = \langle x_\beta(a) | a \in K \rangle, \quad X_\gamma = \langle x_\gamma(a, b) | a, b \in K \rangle.$$

Further, $h_\beta(s)x_\gamma(a,b)h_\beta^{-1}(s) = x_\gamma(s^{-1}a, s^{-1-2\theta}b)$, $h_\gamma(s)x_\beta(a)h_\gamma^{-1}(s) = x_\gamma(s^{-1}a)$ (this follows from the definition of root subgroups, [St1, §11]). It is easy to check $s^{-1-2\theta} \neq 1$ if $s \neq 1$ — recall that $2\theta^2 = 1$ (see [St1, §11], [C1, Ch. 13]). Assume that all four classes contain elements in the form (14). Then in the same way as above, we can get in the product of any two conjugacy classes elements of the form $hh_\beta(t^2)u$ where $h \in H$ is a fixed element, $t \in K^*, t \neq 1$, $u \in U$ and among root factors of u there are no non-trivial elements from X_γ. Put $\delta = w_\gamma(\beta)$. Since $charK = 2$ we have $K^{*2} = K^*$ and therefore we can find in the product of our four classes all elements of the form $hh_\beta(t)h_\delta(s)u$ where $h \in H$ is a fixed element, $t, s \in K^*, t \neq 1, s \neq 1$, $u \in U$. Now we can apply Lemma 6. The case when all four classes have representatives of the form (14) but with γ instead of β is handled in the same way.

Now consider the case when 3 classes (say C_1, C_2, C_3) have representatives in the form (14) only for $\alpha = \beta$ and one class (say C_4) has such a representative only for $\alpha = \gamma$. We can find in C_1C_2 representatives of the form

$$h_\beta(t_0t^2)h_\gamma(s_0)u \tag{19}$$

where t_0, s_0 are fixed, $u \in U$ and t runs through K^* (or k^*). Also we have a representative from C_4 in the form

$$h_\beta(t')h_\gamma(s')x_\gamma u' \tag{20}$$

where t', s' are fixed, $1 \neq x_\gamma \in X_\gamma$ and the element $u' \in U$ has no factors of the form x_β, x_γ.

We can find a value of the parameter t in (19) satisfying the following conditions:

1) $h_\beta(t_0t^2)h_\gamma(s_0)$ does not commute with all non-trivial elements of the group X_γ;

2) $h_\beta(t't_0t^2)$ does not commute with all non-trivial elements of the group X_ω where ω is a positive root which is orthogonal to γ.

Condition 1) implies that in (19) we can get u without non-trivial factors from X_γ (by conjugation by an appropriate x_γ). Then (as in Lemma 5) one can see that for every fixed $d \in K^*$ there exists $s \in K^*$ such that $h_\beta(t't_0t^2)h_\gamma(ds^2)$ is a regular element of G. But the elements of this type can be obtained as above by multiplying elements which are conjugate to (19) and (20) by appropriate elements from the group $\langle X_{\pm\gamma}\rangle$. Now we have a regular element in $H \cap C_1C_2C_4$. Thus applying Lemma 1 we have our statement.

Case F_4:

We can take representatives of classes $C_1, \ldots, C_8$ in the form (14). Moreover, we may assume that at least four classes, C_1, C_2, C_3, C_4 say, have the same α in (14), namely, $\alpha = \alpha_1$ or $\alpha = \alpha_4$ (recall that $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is the simple root system in the notation of Bourbaki). Indeed, we may have as α a long or a short simple root and can always change it for the neighbour of the same length in the Dynkin diagram. Let G_1 be the Chevalley subgroup of G generated by the root subsystem $R_1 = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ if $\alpha = \alpha_1$, or $R_1 = \langle \alpha_2, \alpha_3, \alpha_4 \rangle$ if $\alpha = \alpha_4$. Then G_1 is a group of type B_3 or C_3. If $\alpha = \alpha_4$ we renumber roots in the opposite order. Thus we will assume $\alpha = \alpha_1$. Since in representatives of C_1, C_2, C_3, C_4 which are in the form (14) we have a non-trivial factor x_α for the same $\alpha = \alpha_1$, the same arguments as in the first case show that the product $C_1C_2C_3C_4$ contains elements of the form h_1hv where $h_1 \in H$ is a fixed element depending on the classes C_1, C_2, C_3, C_4, $v \in U$, $h \in H_1 = H \cap G_1$ and h_1h is a regular element of HG_1. Moreover, for every regular element of HG_1 of the form h_1h (where $h \in H_1$) we can find in this product an element of the form h_1hv for some $v \in U$. (Indeed, in the first case we used the fact that all roots have the same length only to get representatives in the form (14) with a non-trivial root factor corresponding to the root at the beginning of the Dynkin diagram and to have the condition of Lemma 7 which in fact also holds for B_3 and C_3.)

Further, in the products C_5C_6 and C_7C_8 we can find representatives in the form (14) with $\alpha = \alpha_4$ (Lemma 4). Put $\gamma = \alpha_4$ (recall that after renumbering we assume that the root system R_1 is generated by $\alpha_1, \alpha_2, \alpha_3$). Using the same arguments as in the case $r = 1$ we can find in the product $C_5C_6C_7C_8$ elements of the form $h_2h_\gamma(t^2)u$ where $h_2 \in H$ is a fixed element depending on classes C_5, C_6, C_7, C_8, $u \in U$ and the parameter t runs through K^* (or k^*).

Let M_γ be the set of positive roots in R which are orthogonal to γ. Put

$$\tilde{H}_1 = \{h \in H_1 |\, \beta(h) \neq \beta(h_1^{-1}), \beta(h) \neq \beta(h_1^{-1}h_2^{-1}) \text{for all} \beta \in R^+ \\ \text{and } \delta(h) \neq 1 \text{ for all } \delta \in M_\gamma\}.$$

Let $H_\gamma = \{h_\gamma(t) | t \in K^* (\text{or } t \in k^*)\}$. Then $H = H_1H_\gamma$. Thus, $K^{*2} \subset \delta(H_1)$ (or $k^{*2} \subset \delta(H_1)$) for every $\delta \in M_\gamma$. Hence, if K is a finite field then the set $\tilde{H}_1$ is obtained from the group H_1 by the exclusion of $2|R^+|+|M_\gamma|$ subsets and each such set has no more than $2(|H_1|/|K^*|)$ (or $2(|H_1|/|k^*|)$) elements. If K is an infinite field then the set $\tilde{H}_1$ is obtained from H_1 by the exclusion of $2|R^+|+|M_\gamma|$ subsets contained in proper closed subsets of the torus corresponding to H_1. Using the definition of a big field it is easy to check that $\tilde{H}_1 \neq \emptyset$ and, moreover, in the case of an infinite field the set $\tilde{H}_1$ is dense in the torus

$$\{h_{\alpha_1}(t_1)h_{\alpha_2}(t_2)h_{\alpha_3}(t_3) | t_1, t_2, t_3 \in \overline{K}^*\}.$$

Now fix $h \in \tilde{H}_1$. The definition of $\tilde{H}_1$ implies that the element h_1h is regular in HG_1. Thus $h_1hv \in C_1C_2C_3C_4$ for some $v \in U$.

Put

$$\tilde{H}_{\gamma,h} = \{h_\gamma(t^2)|t \in K^*(\text{or } t \in k^*), \beta(h_\gamma(t^2)) \neq \beta(h_1^{-1}h_2^{-1}h^{-1})\text{for every}\beta \in R^+\}.$$

If $\beta \in M_\gamma$ (i.e., β is orthogonal to γ), then the condition $\beta(h_\gamma(t^2))(= 1) \neq \beta(h_1^{-1}h_2^{-1}h^{-1})$ holds for every t because of the definition of the element $h \in \tilde{H}_1$. If $\beta \notin M_\gamma$ then $K^{*2}(\text{or } k^{*2}) \subset \beta(H_\gamma)$. Thus in this case we exclude from the set of parameters t^2 at most two elements to get the condition $\beta(h_\gamma(t^2)) \neq \beta(h_1^{-1}h_2^{-1}h^{-1})$. Since $|k^*| > 4|R^+|$ (recall that our field is big) we have $\tilde{H}_{\gamma,h} \neq \emptyset$. Moreover, in the case of an infinite field the set $\tilde{H}_{\gamma,h}$ is dense in the torus $\{h_\gamma(t)|t \in \overline{K}^*\}$.

Let $t \in K^*(\text{or } t \in k^*)$ be an element such that $h_\gamma(t^2) \in \tilde{H}_{\gamma,h}$. We know that we can find an element of the form $h_1hv \in C_1C_2C_3C_4$ where $h \in \tilde{H}_1, v \in U$, and an element $h_2h_\gamma(t^2)u \in C_5C_6C_7C_8$ such that $h_\gamma(t^2) \in \tilde{H}_{\gamma,h}$ for some $u \in U$. According to the definition of $\tilde{H}_{\gamma,h}$ the element $h_1h_2hh_\gamma(t^2)$ is a regular element of G. Since we can find an element in $C_1C_2C_3C_4C_5C_6C_7C_8$ of the form $h_1h_2hh_\gamma(t^2)u'$ for some $u' \in U$, we can also get in this product the regular element $h_1h_2hh_\gamma(t^2)$ (conjugating by an appropriate element of the group U).

If K is an infinite field the definitions imply that the set of elements of the form $h_1h_2hh_\gamma(t^2)$ is dense in $\{h_1h_2h_{\alpha_1}(t_1)h_{\alpha_2}(t_2)h_{\alpha_3}(t_3)h_{\alpha_4}(t_4)|t_1,t_2,t_3,t_4 \in \overline{K}^*\} = \{h_{\alpha_1}(t_1)h_{\alpha_2}(t_2)h_{\alpha_3}(t_3)h_{\alpha_4}(t_4)|t_1,t_2,t_3,t_4 \in \overline{K}^*\}$. Thus, in this case we have a dense subset of semisimple regular elements in $C_1C_2C_3C_4C_5C_6C_7C_8$.

Thus the proof in case F_4 is complete.

Theorem 3 is now proved. ∎

5. Covering numbers for Chevalley groups over infinite fields

THEOREM 4: *Let G be a Chevalley group over an infinite field K. Then*

$$cn(G) \leq ecn(G) \leq 8l(R).$$

Moreover, every non-central element of G is contained in the product of any $4l(R)$ non-central conjugacy classes of G.

Proof: We may assume that G is simply connected. Consider G as the group $\tilde{G}(K)$ where $\tilde{G}$ is the corresponding simple group which is split over K. Moreover, we may assume $B \leq \tilde{B}, H \leq \tilde{H}, N \leq \tilde{N}$ where $\tilde{B}, \tilde{H}, \tilde{N}$ are the corresponding subgroups of $\tilde{G}(\overline{K})$. We have $\tilde{G}(\overline{K}) = \tilde{B}N\tilde{B}$.

Put $X = \tilde{B}\dot{w}_0\tilde{B}$ where $\dot{w}_0 \in N$ is an element corresponding to the longest element in the Weyl group. Then X is an open subset of $\tilde{G}(\overline{K})$. By Corollary 1, a product of any $l(R)$ non-central conjugacy classes of the group $G = \tilde{G}(K)$ is dense in $\tilde{G}(\overline{K})$. Hence one can find an element $g \in G$ in such a product which also belongs to X. Thus, $g = \tilde{b}_1\dot{w}_0\tilde{b}_2$ for some $\tilde{b}_1, \tilde{b}_2 \in \tilde{B}$. On the other hand, g belongs to some Bruhat cell in the group G, so $g = b_1\dot{w}b_2$ for some $b_1, b_2, \in B, \dot{w} \in N$. But $b_1\dot{w}b_2 \in \tilde{B}\dot{w}_0\tilde{B}$ and, since different Bruhat cells have trivial intersections, we have $w = w_0$. Thus in a product of any $l(R)$ non-central conjugacy classes we can find an element from the big Bruhat cell $B\dot{w}_0B$.

Now our statement follows from

PROPOSITION 4: *Let G be a Chevalley group over a big field K. Further, let Bw_0B be the big Bruhat cell (i.e., w_0 is the element of the group W of maximal length). If C_1, C_2, C_3, C_4 are any four conjugacy classes of G such that $C_i \cap Bw_0B \neq \emptyset$ for $i = 1, 2, 3, 4$ then*

$$G \setminus Z(G) \subset C_1C_2C_3C_4.$$

Proof: We need the following lemma.

LEMMA 8: *Let S be the image of the homomorphism*

$$\theta\colon H \longrightarrow H$$

where $\theta(h) = w_0(h)h^{-1}$. Assume K is a big fiel^d. Then for every $h \in H$ there exists an element $s \in S$ such that sh is a regular element.

Proof: Let G be an untwisted Chevalley g.oup. Let α be a positive root. Then $\beta = w_0(\alpha)$ is a negative root. Moreover, β has the same length as α. It implies

$$\alpha(h_\alpha(t^{-1})h_\beta(t)) = t^{-n} \tag{21}$$

where $n = 1, 2, 3$, or 4. From (21) we have

$$K^{*n} \subset \alpha(S) \subset K^*. \tag{22}$$

Therefore $\alpha(S) \not\subset Ker\alpha$ for every root α.

Suppose K is an infinite field. We may consider the map $\theta\colon T \longrightarrow T$ which is defined as above, where T is the maximal torus of the corresponding algebraic group such that $H = T(K)$. Let $\tilde{S} = \theta(T)$. The inclusions (22) imply

$$\tilde{S}_h = h\tilde{S} \setminus \bigcup_{\alpha \in R^+} Ker\alpha$$

is a Zariski open subset of $h\tilde{S}$. Since $H = T(K)$ is dense in T ([Bo], Ch. 18) the set $S = \theta(H)$ is dense in $\tilde{S}$. Hence hS is dense in $h\tilde{S}$ and therefore we can find such a point in the open subset $\tilde{S}_h$ of $h\tilde{S}$. This element satisfies the required condition of the lemma.

Now consider the case when K is a finite field and G is an untwisted Chevalley group.

Obviously,

$$|hS \cap \operatorname{Ker}\alpha| \leq |S \cap \operatorname{Ker}\alpha|$$

for every $h \in H$ and every root α. Thus we have from (22)

$$|hS \cap \operatorname{Ker}\alpha| \leq \frac{n|S|}{|K^*|} \tag{23}$$

and (23) in its turn implies

$$|\bigcup_{\alpha \in R^+} (hS \cap \operatorname{Ker}\alpha)| \leq \frac{n|S||R^+|}{|K^*|}. \tag{24}$$

Thus if $|K^*| > 4|R^+| \geq n|R^+|$ then we have a regular element in hS.

Let now G be a finite twisted group. This case differs from the untwisted case in that for every root $\alpha \in R^+$ we possibly have to consider not one homomorphism α: $H \longrightarrow K^*$ as in the untwisted case but two or three homomorphisms α_i: $H \longrightarrow K^*$ or α_i: $H \longrightarrow k^*$ where $i = 1$ or $1, 2$ or $1, 2, 3$. Such homomorphisms are induced by the conjugation with H of the corresponding one, two or three parameter root subgroup X_α ([C1], [St1]). Moreover, instead of (22) we will have

$$k^{*n} \subset \alpha_i(S) \subset K^*$$

(except for the cases of Suzuki and Ree groups where we have the same as in (22)). This can be easily checked using formulas for conjugations of root subgroups by H ([St1]). Now exclude from our consideration the groups of type ${}^2G_2$ and ${}^3D_4$. Omitting the first type means that we have only two parameter root subgroups. Hence we can simply put in the previous inequality $2|R^+|$ instead of $|R^+|$. Omitting the second type of excluded groups means that we have $(|k^*| + 1)^2 = |K|$ (again except for the cases of Suzuki and Ree groups). Thus, if $|K| > (4|R| + 1)^2$ then $|k^*| > 4 \cdot 2|R^+| = 4|R|$ and we have the required inequality as above for all finite twisted groups except groups of type ${}^2G_2$ and ${}^3D_4$. Now let G be a group of the type ${}^2G_2(q^2)$. Then $\Pi = \{\gamma\}$ and $h_\gamma(t)x_\gamma(a, b, c)h_\gamma^{-1}(s) = x_\gamma(t^{2-3\theta}a, t^{-1+3\theta}b, tc)$ ([St1], §11). Further, let γ_i: $S \longrightarrow K^*$ be the corresponding maps (here $i = 1, 2, 3$). Since $w_0 = -1$

here we have $S = H^2$. Using the fact that 4 does not divide $|K^*|$ ([C1], 13.7) we get $K^{*2} \subset \gamma_i(S)$ for every i and therefore, if $|K| > 2 \cdot 3 + 1$, we have a regular element of the form sh. Let G be a group of type ${}^3D_4(q^3)$. Here we have only one parameter root subgroups. Thus if $|k^*| > 4|R^+| = 24$ we have our regular element of the form hs. Thus we have such an element if $|K| > (24+1)^3$. ∎

Now we can easily get the statement of the Proposition. Indeed, take representatives $x_1 = u_1 h_1 \dot{w}_0 \in C_1, x_2 = \dot{w}_0 h_2 u_2$ where $h_1, h_2 \in H$ and $u_1, u_2 \in U$. Hence $x_1 x_2 = hu$ where $h = h_1 \dot{w}_0^2 h_2 \in H$ and $u = h^{-1} u_1 h u_2 \in U$. Let $s = w_0(t) t^{-1}$, $t \in H$ be the element given by Lemma 8 such that sh is a regular element of G. Put $x_2' = t x_2 t^{-1} = \dot{w}_0 (\dot{w}_0^{-1} t \dot{w}_0 t^{-1}) h_2 (t u_2 t^{-1}) = \dot{w}_0 s h_2 u'$ where $u' \in U$ (note, that $w_0(t) = \dot{w}_0 t \dot{w}_0^{-1}$ and since $\dot{w}_0^2 \in H$ we have $\dot{w}_0 t \dot{w}_0^{-1} = \dot{w}_0^{-1} t \dot{w}_0$). Thus we have $x = x_1 x_2' = shv \in C_1 C_2$ for some $v \in U$. Since sh is a regular element from H, the element x is conjugate to sh. In the same way we can get a regular element from H in $C_3 C_4$. Now the result follows from ([EG]). ∎

6. Covering numbers for groups of restricted rank

THEOREM 5: *Let G be a Chevalley group over a big field. Then*

$$ecn(G) \leq 4l(R)|W|.$$

Proof: Note that among subproducts of any $\mid W \mid$ non-central conjugacy classes we meet an element from B. Indeed, $(b_2(b_1 \dot{w}_1 b_2) b_2^{-1})(\tilde{b}_1^{-1}(\tilde{b}_1 \dot{w}_2 \tilde{b}_2)\tilde{b}_1) = b_2 b_1 \dot{w}_1 \dot{w}_2 \tilde{b}_2 \tilde{b}_1$ and in a product of any $\mid W \mid$ elements from the group W there is some non-empty subproduct equal to the identity. Moreover, we can ensure that we get a non-central element from B. Indeed, if $(b_1 \dot{w})(\dot{w}^{-1} b_2)$ is in the centre of G then we consider the element $(b_1 \dot{w}) h \dot{w}^{-1} b_2 h^{-1}$ for an appropriate $h \in H$. Thus by Theorem 2, in a subproduct of a product of $l(R) \mid W \mid$ non-central conjugacy classes one can find a regular element from H and therefore in a subproduct of a product of $4l(R) \mid W \mid$ non-central conjugacy classes one can find every element of G. ∎

COROLLARY 2: *There exists a constant $e = e(r)$ depending on the natural number r such that the extended covering numbers of all Chevalley groups of rank $\leq r$ are less than e.*

7. The linearity of extended covering numbers for Chevalley groups. General case

The purpose of this section is to prove the following

THEOREM 6: *There exists a positive integer d such that $ecn(G) \leq d\, rank(G)$ for every Chevalley group.*

Moreover, if $\mathrm{rank}(G) > 8$ *then* $ecn(G) \leq 288(rank(G) + 4)$.

ESTIMATES FOR EXTENDED COVERING NUMBERS OF $SL_n(K)$.

Here we follow the general terminology of Chevalley groups for the group $SL_n(K)$ with the natural identification of H with the group of diagonal matrices, B with the group of upper triangular matrices and N with the group of monomial matrices. Some of the intermediate results here are formulated for general Chevalley groups.

PROPOSITION 5: *If $n > 5$, then $ecn(SL_n(K)) \leq 6n + 8$ if n is odd and $ecn(SL_n(K)) \leq 6n + 24$ if n is even.*

In the following lemmas, the term "Coxeter element" is taken to mean an element of the Weyl group which is a product of all simple reflections $w_{\alpha_1}, \ldots, w_{\alpha_r}$ of a *fixed* simple root system which are taken in any order. Note that in this definition an element which is conjugate to a Coxeter element need not be a Coxeter element in general.

LEMMA 9: *Let G be a Chevalley group or $G = GL_n(K)$ and let $g = \dot{w}u$ be an element where $w \in W$ is a Coxeter element and $u \in U$. Then for every Coxeter element w' there exists a preimage $\dot{w}'$ of w' and an element $u' \in U$ such that the element $g' = \dot{w}'u'$ is conjugate to g.*

Proof: For every Coxeter element w there exists a sequence of simple roots $\beta_1 = \alpha_{i_1}, \ldots, \beta_k = \alpha_{i_k}$ (possibly not all distinct) such that all elements in the sequence $w_1 = w_{\beta_1} w w_{\beta_1}^{-1}, w_2 = w_{\beta_2} w_1 w_{\beta_2}^{-1}, \ldots, w_k = w_{\beta_k} w_{k-1} w_{\beta_k}^{-1}$ are Coxeter elements and w_k is the product of simple reflections in the standard order (one can check this using the Dynkin diagrams). Thus we may assume that $w' = w_\alpha w w_\alpha^{-1}$ for some simple root α.

Let u_α be a root factor of u corresponding to α in some decomposition $u = u_\alpha v$ where the element $v \in U$ has no root factors corresponding to α. If $u_\alpha = 1$, then $\dot{w}_\alpha u \dot{w}_\alpha^{-1} \in U$ and therefore the element $\dot{w}_\alpha g \dot{w}_\alpha^{-1}$ has the same form as g, so is a product of a preimage of a Coxeter element and an element from the group U. Suppose $u_\alpha \neq 1$. If $\beta = w(\alpha) > 0$, then $u_\beta = \dot{w} u_\alpha \dot{w}^{-1} \in U$ and the element

$$u_\beta^{-1} g u_\beta = u_\beta^{-1} \dot{w} u_\alpha v u_\beta = u_\beta^{-1} \dot{w} u_\alpha \dot{w}^{-1} \dot{w} v u_\beta = \dot{w} v u_\beta$$

is a product of a preimage $\dot{w}$ of the Coxeter element w and an element of the group U which does not have a non-trivial factor from the root group X_α (note that $\beta \neq \alpha$ because w is a Coxeter element). Hence we return to the previous case.

Let $w(\alpha) < 0$. Assume $w^{-1}(\alpha) < 0$. Then $w = w_\alpha w_1$ for some w_1 which has length $r-1$ ([C2], [St1]). Note that in the case $r = 1$ there is nothing to prove. We may assume $r > 1$ and therefore $w_1 \neq 1$. Since w_1 is a product of $r-1$ different basic reflections we have $w_1(\alpha) \neq \alpha$ and therefore $w_1 = w_2 w_\alpha$ for some w_2 which has length $r-2$ ([C2], [St1]). Thus $w = w_\alpha w_2 w_\alpha$. But in a reduced expression of w_2 there are only $r-2$ simple reflections. Hence w belongs to a subgroup of W generated by $r-1$ simple reflections and cannot be a Coxeter element. This is a contradiction. Thus $\gamma = w^{-1}(\alpha) > 0$. We have now an element

$$u_\alpha g u_\alpha^{-1} = u_\alpha \dot{w} u_\alpha v u_\alpha^{-1} = \dot{w}(\dot{w}^{-1} u_\alpha \dot{w})(u_\alpha v u_\alpha^{-1})$$

which is a product of a preimage $\dot{w}$ of the Coxeter element w and an element from the group U which has no root factors from X_α and we are again in the case considered first. ∎

Lemma 10: *Let $G = GL_n(K)$ or $SL_n(K)$ and let $C \subset G$ be a conjugacy class of regular elements. Then C intersects all Bruhat cells BwB where w is any element conjugate to a Coxeter element.*

Proof: Let $W_r = W$ and let W_{r-1} be the subgroup of W_r generated by $w_{\alpha_2}, \ldots, w_{\alpha_r}$. Then we have the following decomposition into double cosets, $W_r = W_{r-1} \cup W_{r-1} w_{\alpha_1} W_{r-1}$. Since w is conjugate to a Coxeter element it is an $(r+1)$-cycle as an element of the group $S_{r+1} = W_r$. Thus, $w \in W_{r-1} w_{\alpha_1} W_{r-1}$ and therefore w is conjugate by an element of the group W_{r-1} to an element of the form $w_1 w_{\alpha_1}$, where $w_1 \in W_{r-1}$. Then w_1 must be an r-cycle and it is also conjugate by an element of the group $W_{r-2} = \langle w_{\alpha_3}, \ldots, w_{\alpha_r} \rangle$ to an element of the form $w_2 w_{\alpha_2}$, where $w_2 \in W_{r-2}$. Since the elements of W_{r-2} commute with w_{α_1}, we have an element of the form $w_2 w_{\alpha_2} w_{\alpha_1}$, where $w_2 \in W_{r-2}$ which is conjugate to w by an element of W_{r-1}. Acting in the same way we get $w = \sigma w_{\alpha_r} w_{\alpha_{r-1}} \cdots w_{\alpha_1} \sigma^{-1}$ for some $\sigma \in W_{r-1}$. Now we consider a rational form of the class C; we can take a representative $g \in C$ of the form $g = \dot{w}' u$ where $w' = w_{\alpha_r} w_{\alpha_{r-1}} \cdots w_{\alpha_1}$ and $u = u_1 u_2 \cdots u_r$ for $u_i \in X_{\alpha_1 + \alpha_2 + \cdots + \alpha_i}$. Now let $P = BW_{r-1}B$ be the parabolic subgroup corresponding to the set $\{\alpha_2, \ldots, \alpha_r\}$. Then $u \in R_u(P)$ and every preimage $\dot{\sigma}$ of the element $\sigma \in W_{r-1}$ is in a Levi subgroup of P. Thus, $\dot{\sigma} g \dot{\sigma}^{-1} = \dot{w}(\dot{\sigma} u \dot{\sigma}^{-1}) \in \dot{w}B$. ∎

LEMMA 11: *Let G be a Chevalley group of type other than ${}^2A_{2n}(q^2)$ or a Suzuki–Ree group. Let $g \in BwB$ where $w \in W$ is a Coxeter element. Then g is regular.*

Proof: See [St2], Remark 8.8. ∎

LEMMA 12: *Let $g \in SL_n(K)$ be a non-central element. Suppose that g is in rational form:*

$$g = \dot{w}u = \dot{w}_1\dot{w}_2\cdots\dot{w}_m u$$

where $\dot{w}_1, \ldots, \dot{w}_m$ are monomial elements from N corresponding to elements $w_1, \ldots, w_m \in W$ such that

$$w_1 = w_{\alpha_1}w_{\alpha_2}\cdots w_{\alpha_{k_1}}, w_2 = w_{\alpha_{k_1+1}}w_{\alpha_{k_1+2}}\cdots w_{\alpha_{k_2}}, \ldots, w_m = w_{\alpha_{k_{m-1}+1}}\cdots w_{\alpha_{k_m}}$$

and $w_1, \ldots, w_m$ correspond to cycles of lengths $k_1 + 1 \geq (k_2 - k_1 + 1) \geq \cdots \geq (k_m - k_{m-1} + 1)$, and $u = u_1u_2\cdots u_m \in U$ where u_i is an element belonging to the subgroup generated by the $X_\gamma, \gamma \in \langle \alpha_{k_{i-1}+1}, \ldots, \alpha_{k_i}\rangle$.

Let w' be an element of W which is conjugate to w. Then there exist an element $u' \in U$ and a preimage $\dot{w}' \in N$ of w' such that g is conjugate in $SL_n(K)$ to $\dot{w}'u'$.

Proof: The element w' is the product of independent cycles $w'_1\cdots w'_m$ which are conjugate respectively to $w_1, \ldots, w_m$. Let $\Sigma_1, \Sigma_2, \ldots, \Sigma_m$ be disjoint subsets of $[1, n]$ corresponding to those cycles. We may assume $\bigcup \Sigma_i = [1, n]$ (we can always add trivial cycles with $|\Sigma_i| = 1$).

Consider the set

$$\Sigma_i = \{l_{i1}, l_{i2}, \ldots, l_{i(k_i - k_{i-1}+1)}\}.$$

Assume $l_{i1} < l_{i2}\cdots < l_{i(k_i-k_{i-1}+1)}$. Put $n_i = k_i - k_{i-1} + {}^1$. Let $G_i \cong SL_{n_i}(K)$ be the group generated by the root subgroups of the form $X_{\pm\delta}$ where δ is a positive root of the root system generated by $\epsilon_{l_{i1}} - \epsilon_{l_{i2}}, \ldots, \epsilon_{l_{i(k_i-k_{i-1}-1)}} - \epsilon_{l_{i(k_i-k_{i-1})}}$. The assumption implies that a positive root δ with respect to this new root system is also positive with respect to our fixed root system for the whole group $SL_n(K)$. Let V be the linear space of the natural representation of $G = SL_n(K)$ with a fixed basis labelled by $\epsilon_1, \ldots, \epsilon_n$ and let V_i be the subspace spanned by the subsets of this basis corresponding to $\epsilon_s, s \in \Sigma_i$. Then we have

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_m.$$

Now we can construct elements $\tilde{g}_i \in GL(V_i)$ of the form $\dot{w}''_i u''_i$ which have the same rational form as $\dot{w}_i u_i$, where the element w''_i is the cycle

$$(l_{i1}l_{i2})(l_{i2}l_{i3})\cdots(l_{i(k_i-k_{i-1})}l_{i(k_i-k_{i-1}+1)})$$

and u_i'' is a product of positive root elements (transvections) of $SL_{n_i}(K)$. As we see above, such elements are also positive root elements in the group $SL_n(K)$ with respect to our fixed simple root system. By Lemma 9 we can get by conjugation in $GL(V_{n_i})$ an element g_i' of the form $\dot{w}_i' u_i'$ for some element u_i' which is also a product of positive root elements of SL_{n_i}. Now we have the element

$$g' = g_1' \oplus g_2' \oplus \cdots \oplus g_m' = \dot{w}_1' \dot{w}_2' \cdots \dot{w}_m' u_1' u_2' \cdots u_m' = \dot{w}' u'$$

which is conjugate in $GL_n(K)$ to g. Hence $\sigma a g' a^{-1} \sigma^{-1} = g$ for some $\sigma \in SL_n(K), a = diag(t, 1, \ldots, 1)$. Now the element $ag'a^{-1}$ belongs to the same Bruhat cell as g' and is conjugate to g in $SL_n(K)$. ∎

LEMMA 13: *Let $g \in SL_n(K)$ be as in the previous lemma. Assume $k_1 > 1$. Then g is conjugate to an element $\dot{w}'u'$ where $u' \in U$ and $l(w') = l(w) + 1$ (here $l(x)$ is the length of x in W).*

Proof: We can write $u = vx_{\alpha_1}$, where $x_{\alpha_1} \in X_{\alpha_1}$ and the element $v \in U$ has no factors from X_{α_1}.

We may assume $x_{\alpha_1} \neq 1$. Indeed, otherwise put $\beta = w(\alpha_1)$ and consider the element $x_\beta g x_\beta^{-1} = \dot{w}(\dot{w}^{-1} x_\beta \dot{w}) v x_\beta^{-1} = \dot{w} x'_{\alpha_1} v x_\beta^{-1}$ for some $1 \neq x_\beta \in X_\beta$. Since $k_1 > 1$ we have $0 < \beta \neq \alpha_1$. Thus we have the form required (since α_1 is a simple root and interchanging the corresponding component with others we can get the non-trivial α_1-factor to be on the right).

There exists $x_{-\alpha_1} \in X_{-\alpha_1}$ such that $x_{\alpha_1} x_{-\alpha_1} = \dot{w}_{\alpha_1} x'_{\alpha_1}$ for some preimage $\dot{w}_{\alpha_1} \in N$ of a basic reflection $w_{\alpha_1} \in W$ and some $x'_{\alpha_1} \in X_{\alpha_1}$. Conjugating g by $x_{-\alpha_1}^{-1}$, we get an element

$$x_{-\alpha_1}^{-1} \dot{w} v \dot{w}_{\alpha_1} x'_{\alpha_1} = x_{-\alpha_1}^{-1} \dot{w} \dot{w}_{\alpha_1} \dot{w}_{\alpha_1}^{-1} v \dot{w}_{\alpha_1} x'_{\alpha_1}. \tag{25}$$

Since v has no factors from the group X_{α_1}, we have $w_{\alpha_1}^{-1} v w_{\alpha_1} \in U$. Further, the root $\beta = w^{-1}(-\alpha_1)$ is positive and different from α_1. This follows from the construction of w and the assumption $k_1 > 1$. Thus $\gamma = w_{\alpha_1}(\beta) > 0$. Now we have

$$x_{-\alpha_1}^{-1} \dot{w} \dot{w}_{\alpha_1} = \dot{w} \dot{w}_{\alpha_1} x_\gamma \tag{26}$$

for some $x_\gamma \in X_\gamma$. Comparing (25) and (26) we get an element conjugate to g in the form $\dot{w}\dot{w}_{\alpha_1} u'$ for some $u' \in U$. From the definition of w we get $l(ww_{\alpha_1}) = l(w) + 1$. ∎

LEMMA 14: *Let $g' = \dot{w}'u' \in SL_n(K)$ where $\dot{w}' \in N$, $u' \in U$. Suppose that w' is a product of basic reflections w_{α_i} where each such reflection occurs not more than once and w' contains an independent cycle of length > 2. Then g' is conjugate to an element g which has the form as in Lemma 12 with $k_1 > 1$.*

Proof: Let $w' = w'_1 w'_2 \cdots w'_m$ where w'_i are independent cycles which are products of basic reflections, where such reflections occur at most once in the decompositions of all the w'_i. This means that g' is contained in some standard parabolic subgroup of $SL_n(K)$. Moreover, since w' contains a cycle of length > 2 a Levi factor of this parabolic subgroup contains a simple component of rank > 1 and the natural projection on this component of the element g' gives a regular element (Lemma 11). This implies that the minimal polynomial of g' has degree not less than the length of the corresponding cycle, which implies our statement. ∎

LEMMA 15: *Let $g_1 = \dot{w}_1 u_1, g_2 = \dot{w}_2 u_2 \in SL_n(K), n \geq 6$, be two rational forms where $w_1 = (12)(34)\cdots((2s_1-1)2s_1), w_2 = (12)(34)\cdots((2s_2-1)2s_2), s_1 \leq s_2$ and let C_1, C_2 be the conjugacy classes in $SL_n(K)$ of g_1, g_2. Then there exists an element in C_1C_2 in the form as in Lemma 12 and with $k_1 > 1$.*

Proof: Let $s_1 < s_2$ or $2s_2 < n$. There exists an element g'_1 of the form $u'\dot{w}' \in SL_n(K)$ which is conjugate to g_1 and where $w' = (23)(45)\cdots(2s_1 2s_1+1)$. Then the element $g'_1 g_2$ is conjugate to an element of the form $\dot{w}u$, where w is a product of basic reflections with each such reflection occurring at most once and having a cycle of length > 2. Thus we can apply the previous lemma.

Now let $2s_1 = 2s_2 = n$. Then

(27)
$$((23)(45)\cdots(n1))((12)(34)\cdots((n-1)n)) = (1357\cdots(n-1))(n(n-2)\cdots 42).$$

Since g_1, g_2 are in rational form, we can write

$$g_1 = \dot{w}_1 x_{\epsilon_1-\epsilon_2} x_{\epsilon_3-\epsilon_4} \cdots x_{\epsilon_{n-1}-\epsilon_n}, \quad g_2 = \dot{w}_2 y_{\epsilon_1-\epsilon_2} y_{\epsilon_3-\epsilon_4} \cdots y_{\epsilon_{n-1}-\epsilon_n} \tag{28}$$

where $x_\alpha, y_\alpha \in X_\alpha$. Now instead of g_1 we take an element g'_1 which is conjugate to g_1 and has the form

$$g'_1 = \dot{w}'_1 x'_{\epsilon_3-\epsilon_2} x'_{\epsilon_5-\epsilon_4} \cdots x'_{\epsilon_{n-1}-\epsilon_{n-2}} x'_{\epsilon_1-\epsilon_n} \tag{29}$$

where $w'_1 = (23)(45)\cdots((n-2)(n-1))(n1)$ and $x'_\alpha \in X_\alpha$. Now take a different ordering of the basis $\epsilon_1, \ldots, \epsilon_n$ of the vector space of the natural representation of $SL_n(K)$. We put vectors with odd indices in the first $s_1 = n/2$ positions, $\epsilon_1, \epsilon_3, \epsilon_5, \ldots$, and then the vectors with even indices in the next $n/2$ positions, $\epsilon_2, \epsilon_4, \ldots$. Note that the elements y_α in (28) are represented by upper triangular matrices with respect to the new basis. The same is true for the elements x'_α in (29). Thus the element $g'_1 g_2$ is conjugate to an element which is represented with respect to the new basis by a matrix of the form $\dot{w}u$, where w is a product of two independent cycles corresponding to first and second $n/2$ elements of the new basis (see (27)) and u is an upper triangular matrix. Note that these cycles are products of basic reflections corresponding to the new order of the basis and each such reflection may occur at most once. Now we can apply the previous lemma. ∎

We now prove Proposition 5.

Let C_1, C_2 be noncentral conjugacy classes of $SL_n(K)$. We can take representatives of these classes in the form $g_1 = u_1\dot{w}_1, g_2 = \dot{w}_2 u_2$ where $\dot{w}_1, \dot{w}_2 \in N$, $u_1, u_2 \in U$. Moreover, we may take w_1, w_2 to be elements which are conjugate to the permutations which appear in the rational forms of corresponding elements. Thus by Lemma 12 we may assume in the positions of w_1, w_2 every pair from given conjugacy classes of W. Therefore we may assume that $w = w_1 w_2 \neq 1$ and for appropriate choice of w_1, w_2 we can get in this product every element in the conjugacy class of w. Now in the product of any two noncentral conjugacy classes we can get a representative in the form $\dot{w}u$ where $1 \neq w \in W$ and $u \in U$. Moreover, if we fix the conjugacy class Q_w of w in W we can get a representative of our product of the form $\dot{w}'u'$ for every element $w' \in Q_w$.

Now let $n = 2l + 1 > 5$. Then every n-cycle is in the alternating group A_n. Since $ecn(A_n) = [n/2] + 1$ ([D]), multiplying $l + 1$ appropriate elements from given nontrivial conjugacy classes of A_n we can get every element of A_n. Now take any $12(l+1)+2$ non-central conjugacy classes of $SL_n(K)$. We say that the class is odd (resp. even) if the rational form of a representative has the form $\dot{w}u$ for $w \notin A_n$ (resp. $w \in A_n$). Then we distribute this set into pairs in which both classes are odd or even. Only two classes may have no such pair. If the product of the other $12(l + 1)$ classes gives the whole of $SL_n(K)$, the multiplication by these two classes does not change the result. Thus we need to consider only $6(l + 1)$ pairs. In the product of such a pair we can find a representative $\dot{w}u$ where $w \in A_n$, $w \neq 1$. From the above it follows that in the product of any $l + 1$ noncentral conjugacy classes obtained in the product of such pairs we can find an element of the form $\dot{w}u$ where $w \in W$ is a Coxeter element of W and $u \in U$. Such an element is regular (Lemma 11). Further, every noncentral element of $SL_n(K)$ is contained in the product of any three regular conjugacy classes ([Levl]). Therefore every element of $SL_n(K)$ is contained in the product of any six regular conjugacy classes. Hence $ecn(SL_n(K)) \leq 12(l+1)+2 = 6n+8$.

Now let $n = 2l \geq 6$. Consider $12(l+1)+12$ non-central conjugacy classes. Distribute these classes into pairs as above. We divide these pairs into two sets: in the first we take $6(l+1)$ and in the second 6, where there can be one pair which consists of odd and even elements. For every pair from the first set we fix an even nontrivial class contained in the product of this pair. In the product of any $(l+1)$ such classes we can get elements of the form $\dot{w}u$ for every $w \in A_n$ (since $ecn(A_n) = l+1$ by [D]). Now take any pair from the second set. There are two possibilities. The first possibility is that we have a representative in at least one class which is odd or which satisfies the condition of Lemma 13. In the latter case Lemma 13 implies that we can find a representative of the class of the form $\dot{w}u$ where $l(w)$ is odd. In the second case rational forms of representatives of both classes have forms $\dot{w}u$,where w is a product of an even number of independent transpositions. Now use Lemmas 13 and 15, and get in the product of our two conjugacy classes of $SL_n(K)$ an odd class. Now we fix an element of the form $\dot{w}u$ where $l(w)$ is odd which is contained in one of the pairs of the second class or in the product of such a pair. Now every element of the group $S_n \setminus A_n$ can be written in the form $w\omega$ for some $\omega \in A_n$. Thus, if we consider a product of $(l+1)$ pairs from the first set and a pair from the second set, we can find in this product or in a subproduct (with one class removed) an element of the form $\dot{w}u$, where w is a Coxeter element of W, which is a regular element in $SL_n(K)$ by Lemma 11.

Now every non-central element can be found in a subproduct of $3(l+1)$ pairs from the first set and 3 pairs from the second ([Levl]), and therefore in the subproduct of $6(l+1)$ pairs from the first set and 6 pairs from the second set. Note that we take the subproduct of a fixed subset of our $12(l+1)+12$ classes. Thus the product of this subset gives us the whole group and therefore the whole product also coincides with $SL_n(K)$. Hence $ecn(SL_n(K)) \leq 12(l+1)+12 = 6n+24$.

General Coxeter cells.

Definition: Let R be a root system (possibly reducible) and Π be its fixed simple root system. Further, let $R' \subset R$ be a root subsystem (possibly empty) generated by a simple root system $\Pi' \subset \Pi$. Then every Coxeter element of $W(R')$ (i.e., a product of all basic reflections $w_\alpha, \alpha \in \Pi'$ in any order, or, the identity if $R' = \emptyset$) will be called a *general Coxeter element* of the Weyl group $W(R)$.

Definition: Let $G = BNB$ be a group with (B, N)-pair. The cell $B\dot{w}B$ will be called a *general Coxeter cell* if w is a general Coxeter element.

PROPOSITION 6: *Let G be a finite crystallographic Chevalley group (untwisted or twisted). Then every non-central conjugacy class of G has a non-empty intersection with a general Coxeter cell of the Bruhat decomposition of G.*

For the purpose of the proof of Proposition 6 we need to recall some notions and to introduce some notation.

1. Recall that R is the irreducible root system corresponding to G ([St1], [C1]) generated by a simple root system Π. The group G is generated by root subgroups $X_\alpha, \alpha \in R$. Further, $G = BNB, B = HU, N/H \cong W = W(R), rank(G) = rank(R)$.

2. If the statement is true for all simply connected Chevalley groups it will be also true for all groups. Thus we will assume that G is simply connected.

3. We can exclude the cases of Suzuki–Ree groups. Indeed, since G is crystallographic, it is not of type $^2F_4$. The other cases are groups of rank one. There is nothing to prove for such groups since both Bruhat cells are general Coxeter.

4. Thus we may assume $G = {}^mX_l(q^m)$ where $m = 1, 2, 3$ and $X_l = A_l, \ldots, G_2$. Put $K = F_{q^m}, k = F_q$. There exists a simple and simply connected algebraic group $\tilde{G}$ defined and split (if $m = 1$) or quasi-split (if $m > 1$) over k such that $G = \tilde{G}(k) = \tilde{G}(\bar{k})^F$ where F is a Frobenius map ([C2]). Further, there exists a maximal torus T of the group $\tilde{G}$ which is defined over k and stable under F and such that $H = T(k)$. Then we have an irreducible root system $\tilde{R}$ with respect to T such that $R = \tilde{R}/F$ (here we take a root from R to correspond to an F-orbit in $\tilde{R}$). Also, $\Pi = \tilde{\Pi}/F$ for the simple root system.

5. Now let $X \subset \Pi$, $G_X = \langle X_\alpha | \ \alpha \in \langle X \rangle \rangle$. Then there exists a subset $\tilde{X} \subset \tilde{\Pi}$ such that $X = \tilde{X}/F$. Further, there exists a simply connected semisimple algebraic group $\tilde{G}_{\tilde{X}}$ which is defined and split or quasi-split over the field k such that $G_X = \tilde{G}_{\tilde{X}}(k)$.

6. *Cross-section of regular conjugacy classes for $\tilde{G}_{\tilde{X}}$.* In [St2] it is shown that for a semisimple algebraic group defined over a field L there exists a cross-section of conjugacy classes of regular elements. Moreover, if such a group is simply connected and quasi-split over L, then this cross-section can be defined over L under the condition that this group has no simple component of type $^2A_{2s}$. If such a component does exist, we can construct over L a closed subset of our group which intersects every *semisimple regular conjugacy class* in exactly one point. Thus in our case we have a closed subset $N_{\tilde{X}}$ of the group $\tilde{G}_{\tilde{X}}$ defined over the field k satisfying the following condition:

($\star$) Every regular semisimple conjugacy class of $G_{\tilde{X}}$ intersects $N_{\tilde{X}}$ in exactly one point.

7. *Description of* $N_{\tilde{X}}$. We follow [St2, 9.8, 9.11]. If G_X does not contain any components of type ${}^2A_{2s}$ then

$$N_{\tilde{X}} = \prod_{\beta\in\tilde{X}} \dot{w}_\beta \tilde{X}_\beta. \tag{30}$$

Here the $\tilde{X}_\beta$ are root subgroups defined over K. However, the whole product is F-stable and can be defined over k with an appropriate choice of preimages $\dot{w}_\beta$ of basic reflections. Moreover, we can get such a set $N_{\tilde{X}}$ for every order in the product (30) and every such product satisfies ($\star$). (Note that compared to [St2] we change the position of $w_\beta, \tilde{X}_\beta$, but that is not essential.) We can rewrite (30) in the form

$$N_{\tilde{X}} = \prod_{\beta\in\tilde{X}} \dot{w}_\beta \prod_{\theta(\beta)} \tilde{X}_{\theta(\beta)} = \dot{w}_{\tilde{X}} V_{\tilde{X}}, \tag{31}$$

where $\dot{w}_{\tilde{X}}$ is an element belonging to G_X and $V_{\tilde{X}}$ is a closed subgroup of $\tilde{U}_{\tilde{X}}$ defined over k. Indeed, we can move $\dot{w}_\beta$ in (30) to the left side by interchanging it with various terms $\tilde{X}_{\beta'}$. Then $\tilde{X}_\beta$ in (30) gets replaced by the root subgroup $\tilde{X}_{\theta(\beta)}$, where $\theta(\beta) = w(\beta)$ for w which is the product of all reflections corresponding to roots which appear in (30) to the right of β. Such a root $\theta(\beta)$ is positive (see [St2]). Further,

$$\dot{w}_{\tilde{X}} = \prod_{\alpha\in X} \dot{w}_\alpha \tag{32}$$

for appropriate choice of preimages $\dot{w}_\alpha$. This follows from the definition of $w_{\tilde{X}}$. Now from (31) and (32) one can see that every F-stable element from the set $N_{\tilde{X}}$ is in a general Coxeter cell of G.

Now we consider the case when the group G_X contains a component of type ${}^2A_{2s}$. This occurs only if the whole group G is of the same type and in this case there exists at most one such component in G_X. Thus we have $X = Y \cup Z$ (respectively, $\tilde{X} = \tilde{Y} \cup \tilde{Z}$) where the group G_Y has no components of type ${}^2A_{2s}$ and G_Z is the group ${}^2A_{2s}(q^2)$. We define $N_{\tilde{Y}}$ in the same way as above. Let $\tilde{Z} = \{\gamma_1, \dots, \gamma_{2s}\}$ be the numbering where $F(\gamma_i) = \gamma_{2s+1-i}$. Put $\delta = \gamma_s + \gamma_{s+1}$. Let $\tilde{B}_\delta = T_\delta \tilde{X}_\delta$ be a Borel subgroup of $\langle \tilde{X}_{\pm\delta}\rangle$. Put

$$N_{\tilde{Z}} = (\dot{w}_\delta \tilde{X}_\delta \cup \dot{w}_\delta x_1 x_2 \tilde{B}_\delta) \prod_{i\neq s,s+1} \dot{w}_{\gamma_i} \tilde{X}_{\gamma_i} \tag{33}$$

where $x_1 \in \tilde{X}_{\gamma_s}, x_2 \in \tilde{X}_{\gamma_{s+1}}$ are some fixed non-trivial elements. Put

$$N_{\tilde{X}} = N_{\tilde{Y}} N_{\tilde{Z}}. \tag{34}$$

Then the set $N_{\tilde{X}}$ satisfies condition $(\star)$, is F-stable and can be defined over k with an appropriate choice of preimages of elements from the Weyl group and elements x_1, x_2. The definitions (33) and (34) also imply that the F-stable elements from $N_{\tilde{X}}$ are in general Coxeter cells of the Bruhat decomposition of G (by the same argument as above).

8. *The group HG_X.* Let $h \in H = T(k)$. Then the set $hN_{\tilde{X}}$ is a closed subset of $\tilde{G}_{\tilde{X}}$. Moreover, if $N_{\tilde{X}}$ is defined over k then $hN_{\tilde{X}}$ is also defined over k.

LEMMA 16: *Let $hg \in HG_X$ where $g \in G_X$, and let C be the conjugacy class of hg in the group $T\tilde{G}_{\tilde{X}}$. Suppose that hg is a semisimple regular element of $T\tilde{G}_{\tilde{X}}$. Then C intersects the set $hN_{\tilde{X}}$ just in one point.*

Proof: We can write $h = th_1$ for some t which lies in the centre of $T\tilde{G}_{\tilde{X}}$ and for some $h_1 \in \tilde{G}_{\tilde{X}}$. Note that these two elements need not be defined over k. However, the closed subset $h_1 N_{\tilde{X}}$ satisfies the condition $(\star)$ (but need not be defined over k). This follows from the constructions of $N_{\tilde{X}}$ (the multiplication by h_1 changes only the preimages of the same reflections in (29), (33)). Further, the multiplication by the central element of a semisimple regular element changes neither the semisimplicity nor the regularity. Hence the conjugacy class of $h_1 g$ intersects the set $h_1 N_{\tilde{X}}$ in just one point. The same is true for C and $th_1 N_{\tilde{X}} = hN_{\tilde{X}}$. ∎

LEMMA 17: *Every regular semisimple element of the group HG_X is conjugate to one from a general Coxeter cell of the Bruhat decomposition of G.*

Proof: Let $\sigma \in HG_X$ be a regular semisimple element of the group $T\tilde{G}_{\tilde{X}}$ and let C be the conjugacy class of this element in this group. The previous lemma implies that $C \cap hN_{\tilde{X}}$ consists of one point for some $h \in H$. Since C and $hN_{\tilde{X}}$ are both defined over k the element in the intersection is in HG_X. Since $\tilde{G}_{\tilde{X}}$ is simply connected, the elements in HG_X which are conjugate in $T\tilde{G}_{\tilde{X}}$ are also conjugate in HG_X ([C2, Proposition 3.7.3]. But the elements from the set $N_{\tilde{X}}$ which are also in G_X lie in a general Coxeter cell, as we have seen above in 7. The same is true for the elements from $hN_{\tilde{X}}$. ∎

Proof of Proposition 6: The groups of the form HG_X also possess a (B, N)-pair and therefore we can formulate the statement as in the Proposition for groups of this form. We prove the statement for groups of the form HG_X (it is clear that G is also such a group, with $X = \Pi$). Let C be a non-central conjugacy class of HG_X. If C is a semisimple regular class then we have our statement from Lemma 17. If not, then there exists an element $g \in C$ which belongs to a proper standard parabolic subgroup P of HG_X. This follows from the fact that $p = \operatorname{char} k$ divides $|C_{HG_X}(g)|$ for such an element g, as we see from the properties of the Frobenius map and well known facts about centralisers of semisimple elements, and from ([C2, Proposition 6.4.5]). Let L be the Levi factor of P of the form HG_Y where $Y \subset X$ and let ϕ: $P \longrightarrow L$ be the natural homomorphism. Assume that P is a minimal parabolic subgroup containing elements from C. Then $\phi(g)$ is a regular semisimple element of the group L. Thus $g = su$, where s is a semisimple regular element of L and $u \in R_u(P)$. Again by Lemma 17, $\sigma s \sigma^{-1}$ is in a general Coxeter cell for some $\sigma \in L$. Since $\sigma R_u(P)\sigma^{-1} = R_u(P)$ then $\sigma g \sigma^{-1}$ is in the same cell.

The Proposition is now proved. ∎

Proof of the Theorem. Now we are able to prove the Theorem. We may restrict our attention to the case of finite fields, because of Theorem 3. Also we need to consider only groups of rank > 8, and hence only classical groups, other than type A_r already considered above. Thus G here is a finite Chevalley group of type $B_r(q), C_r(q), D_r(q), {}^2A_n(q^2), {}^2D_n(q^2)$.

Let $R_1 = \langle \alpha_1, \ldots, \alpha_{r-1} \rangle$ (with the standard numbering of simple roots) , $G_1 = \langle X_{\pm\alpha} | \alpha \in R_1 \rangle$ (note that $G_1 \cong SL_r(K)/Z$ for some $Z \leq Z(G)$), $W_1 = W(R_1)$, N_1 is the corresponding subgroup of G_1, $H_1 = H \cap G_1$. Further, let $P = BN_1B$ be the corresponding parabolic subgroup, $L = HG_1$ its Levi factor, $V = R_u(P)$ and ϕ: $P \longrightarrow L$ be the natural homomorphism.

Lemma 18: *Let C_1, C_2 be two non-central conjugacy classes of G. Then at least one of the sets $C_1 \cap P$, $C_2 \cap P$ and $C_1C_2 \cap P$ is not empty and is not contained in the center of the group G.*

Proof: We can choose $g_1 = u_1\dot{w}_1 \in C_1$, $g_2 = \dot{w}_2u_2 \in C_2$ where $u_1, u_2 \in U$ and w_1, w_2 are general Coxeter elements (Proposition 6). If both classes have trivial intersection with P, then among basic reflection factors of w_1, w_2 there is w_{α_r}. Moreover, we may assume $w_1 = w_1'w_{\alpha_r}$, $w_2 = w_{\alpha_r}w_2'$ (by the same argument as in the proof of Lemma 9). Hence $g = u_1^{-1}(g_1g_2)u_1 \in P$. Suppose $g \in Z(G)$. Then $g_1g_2 \in Z(G)$. This implies $\dot{w}_1\dot{w}_2 \in Z(G), u_1 = u_2^{-1}$. Since w_1 is a general Coxeter element, there exists a positive root α such that $\alpha \neq w_1(\alpha) > 0$. Now take a root element $x_\alpha \neq 1$ and consider $g_1' = x_\alpha^{-1}g_1x_\alpha = x_\alpha^{-1}u_1(\dot{w}_1x_\alpha\dot{w}_1^{-1})\dot{w}_1$ instead of g_1. Now $g_1'g_2 \in P \setminus Z(G)$. ∎

LEMMA 19: *Let C_1, C_2 be two non-central conjugacy classes of G such that $(C_1 \cap P), (C_2 \cap P)$ are non-empty sets. Then $\phi(g) \notin Z(L)$ for some element $g \in (C_1 \cup C_2 \cup C_1C_2) \cap P$ (recall that ϕ is the natural surjection $P \longrightarrow L$).*

Proof: Let $g \in P$ and $\phi(g) = h \in Z(L)$. Then $h \in H$ and $g = hu$ for some $u \in V$. According to Lemma 2, we may assume that the root factor u_{α_r} of u is not trivial. Also, by Lemma 4 we may assume $|K| \leq 3$ or $|k| \leq 3$: otherwise we can find in C_1C_2 an element of the form $g = hu$ (also in P) such that u has non-trivial α-factor for any chosen simple root α; taking $\alpha \in \{\alpha_1, \ldots, \alpha_{r-1}\}$ we can make sure that $\phi(g) \notin Z(L)$. Similarly, the case $D_r(q)$ can be excluded because of Lemma 3. Put $\alpha = \alpha_r = \epsilon_r$, or $2\epsilon_r$ and $\beta = \epsilon_r + \epsilon_{r-1}$ (we take the standard numbering for root systems B_r and C_r).

Now we assume that for every element g from the sets $C_1 \cap P, C_2 \cap P$ we have $\phi(g) \in Z(L)$. Thus, representatives g_1, g_2 of the sets $C_1 \cap P, C_2 \cap P$ have the form described above. Below, using this form we show that either a conjugate $g \in P$ of g_1, g_2 has the property $\phi(g) \notin Z(L)$ (and this is a contradiction with our assumption) or a product $g \in P$ of conjugates g_2, g_2 has the property $\phi(g) \notin Z(L)$.

Let G be of type $C_r(q)$ or ${}^2A_{2r-1}(q^2)$.

We can take representatives g_1, g_2 of C_1, C_2 in the form

$$g_1 = h_1 x_\alpha x_\beta v_1, \quad g_2 = h_2 x'_\alpha v_2$$

where $h_1, h_2 \in Z(L)$ and the elements $v_1, v_2 \in V$ have no factors from the groups X_α, X_β and $x_\alpha, x'_\alpha, x_\beta \neq 1$. (This can be obtained by conjugation by appropriate elements from the group $X_{\alpha_{r-1}}$; see [St1], Lemma 33.)

We may assume $h_1, h_2 \in Z(G)$. Indeed, otherwise the element h_1 (or h_2) does not commute with elements of the group X_{α_r} because it commutes with all X_{α_i}, $i < r$, but $h_1 \notin Z(G)$ (or $h_2 \notin Z(G)$). Thus conjugating g_1 (or g_2) by an appropriate element from the groups X_α, $X_{\alpha_{r-1}}$ we can get an element in one of these conjugacy classes of the same form as g_1 but with $x_\alpha = 1$. Now we have $g' = \dot{w}_\alpha g_1 \dot{w}_\alpha^{-1} \in P$ and $\phi(g') \notin Z(L)$.

If $x'_\alpha = x_\alpha^{-1}$ then $g = \dot{w}_\alpha (g_1 g_2) \dot{w}_\alpha^{-1} \in P$ and $\phi(g) \notin Z(L)$. If $x'_\alpha \neq x_\alpha^{-1}$ then $|K| = 3$ (or $|k| = 3$) and $x'_\alpha = x_\alpha$. Conjugating the elements g_1, g_2 by appropriate elements $\tau_1, \tau_2 \in \langle X_{\pm\alpha} \rangle$ we can get elements

$$g'_1 = h_1 y_\alpha \dot{w}_\alpha v'_1, \quad g'_2 = h_2 \dot{w}_\alpha y_\alpha v'_2$$

where $y_\alpha \in X_\alpha, v'_1, v'_2 \in V$. Note that in both expressions $\dot{w}_\alpha$ is the same preimage of w_α because of the assumption $x'_\alpha = x_\alpha$. Since $(\dot{w}_\alpha)^2 = h_\alpha(-1)$

we have $g' = g_1'g_2' = h'v'$ where $h' \in H$, $v' \in V$ and $[h', x_{\alpha_{r-1}}] \neq 1$. Thus $x_{\alpha_{r-1}} g' x_{\alpha_{r-1}}^{-1}$ is an appropriate element.

Let G be of type $B_r(q)$ with $q \neq 2^m$ (the case $q = 2^m$ is included in $C_r(q)$).

Let $g = hu$ be a representative of one of these classes. Assume $h \notin Z(G)$; then $[h, x_\alpha] \neq 1$. Now conjugating g by appropriate elements from X_{ϵ_i} we get an element g' of the form hu' where all root factors of u' of the form x_{ϵ_i} are trivial. If u' has a factor of the form $x_{\epsilon_i+\epsilon_j}$ then $\dot{w}_{\epsilon_i} g' \dot{w}_{\epsilon_i}^{-1}$ is an appropriate element. If all such factors are trivial then $u' = 1$ and $g' = h$. If h does not commute with all long root elements we can return to the previous case. We assume now that $h_1 \in C_1, h_2 \in C_2$ where the elements $h_1, h_2 \in H$ commute with all long root elements. By conjugation we can get elements in C_2, C_1 of the form $x_{\alpha_r} h_2 x_{\alpha_{r-1}+\alpha_r} x_{\alpha_{r-1}+2\alpha_r}$, $h_1 x_{\alpha_r}^{-1}$ where $x_{\alpha_{r-1}+2\alpha_r} \neq 1$. If g is the product of such elements then $\dot{w}_{\alpha_r} g \dot{w}_{\alpha_r}^{-1}$ is an appropriate element from the product C_1C_2.

Suppose $h \in Z(G)$. Then conjugating the element g by an appropriate element $x_{\alpha_{r-1}} \in X_{\alpha_{r-1}}$ we can get an element of the form $g' = hu'$, where $u' \in V$ has non-trivial factor u'_{α_r} and trivial factor $u'_{\alpha_{r-1}+\alpha_r}$ (here $\alpha_{r-1} + \alpha_r = \epsilon_{r-1}$) in some decomposition into product of root elements. We may also assume that u' has no non-trivial factors from the group $X_{\epsilon_r+\epsilon_{r-1}}$. (Otherwise $\dot{w}_{\epsilon_{r-1}} g \dot{w}_{\epsilon_{r-1}}^{-1}$ is an appropriate element.) Then conjugating g' by some non-trivial $x_{-(\alpha_{r-1}+\alpha_r)} \in X_{-(\alpha_{r-1}+\alpha_r)}$ we get an element g'' such that $\phi(g'') \notin Z(L)$ (this follows from the Chevalley commutator formula).

Let G be of the type ${}^2D_{r+1}(q^2)$.

Put $\gamma = \epsilon_{r-1}$. We can take representatives $g_1 \in C_1$, $g_2 \in C_2$ in the form

$$g_1 = h_1 x_\gamma(s_1) x_\beta(m_1) u_1 x_\alpha(t_1), \quad g_2 = h_2 x_\alpha(t_2) x_\gamma(s_2) x_\beta(m_2) u_2$$

where $h_1, h_2 \in Z(L)$ and the elements $u_1, u_2 \in V$ have no root factors corresponding to α, β, γ and $t_1, t_2 \neq 0$. If h_1 or $h_2 \notin Z(G)$ then the proof is the same as in the case $B_r(q)$. Assume $h_1, h_2 \in Z(G)$. We can always make m_1 or $m_2 = 0$. Thus, if $t_2 = -t_1$ we have the same situation as in the case $C_r(q)$. If $|k| = 2$ we can always get $t_2 = -t_1 = t_1$ by conjugation of g_1 by an appropriate element $h_\alpha(t)$.

Now $|K^*| = 8$. Thus $-1 \in K^{*2}$. We may assume $t_1 \notin t_2K^{*2}$ (otherwise we can make $t_1 = -t_2$ by conjugation of g_1 by an appropriate element $h_\alpha(t)$). We also assume $m_1 \neq 0, m_2 = 0$ (this can be done by conjugation with elements from the group $X_{\alpha_{r-1}}$). Let $s_1 = 0$. Then $\dot{w}_\gamma g_1 \dot{w}_\gamma^{-1}$ is an appropriate element. Thus we assume $s_1 \neq 0$. Let $s_2 = 0$. Then $x_{-\gamma} g_2 x_{-\gamma}^{-1}$ is an appropriate element for some $x_{-\gamma} \in X_{-\gamma}$. Thus we assume $s_2 \neq 0$. The same arguments as above give us the assumption $s_1 \notin s_2K^{*2}$. Now we have $t_1 \notin t_2K^{*2}, s_1 \notin s_2K^{*2}$. Since we can change $x_\alpha(t_1)$ to $x_\gamma(\pm t_1)$ by conjugating g_1 by $\dot{w}_{\alpha_{r-1}}$ we can also add the assumption $t_1 \notin s_2K^{*2}$. Again by an appropriate conjugation we can get $t_1 = s_1$ and $t_2 = s_2$. Conjugating g_2 by an appropriate element from $X_{\alpha_{r-1}}$ we can get $s_2 = 0$. Then conjugating g_2 by $x_{-\gamma}(1)$ we get an element which has a non-trivial root factor corresponding to α_{r-1}. Thus we get the required element.

Let G be ${}^2A_{2r}(q^2)$.

Recall that here $R = B_r$ ([C1]), $\alpha = \alpha_r = \epsilon_r$ and $X_{\epsilon_r} = \langle x_{\epsilon_r}(a,b)\rangle$ is a two parameter subgroup. Let $\dot{w}_\alpha$ be a preimage of $w_\alpha \in W$; then $[\dot{w}_\alpha, h_\alpha(t)] = h_\alpha(tt^\theta)$ (recall that θ is a field automorphism corresponding to the Frobenius map F). Thus, if $|k| = 3$ we can find an element $t \in K^*$ such that $tt^\theta = -1$ and obtain $[\dot{w}_\alpha, h_\alpha(t)] = h_\alpha(-1)$. Now using the same representation of elements in C_1, C_2 as in the proof of Lemma 4 we can obtain an element $g = hu \in C_1C_2$ such that $[h, x_{\alpha_{r-1}}] \neq 1$. Now $x_{\alpha_{r-1}}gx^{-1}_{\alpha_{r-1}}$ is an element as required. Thus we can exclude the case $|k| = 3$ and we assume $|k| = 2$. Now take representatives of $g_1 \in C_1, g_2 \in C_2$ as in the previous case

$$g_1 = h_1x_\gamma(s_1, s_1')x_\beta(m_1)v_1x_\alpha(t_1, t'), \quad g_2 = h_2x_\alpha(t_2, t_2')x_\gamma(s_2, s_2')x_\beta(m_2)v_2$$

where in the first expression $t_1 \neq 0$ or $t_1' \neq 0$ and $t_2 \neq 0$ or $t_2' \neq 0$ in the second one. We may also assume that $m_1 \neq 0$ and $m_2 = 0$, or $m_1 = 0$ and $m_2 \neq 0$. If $t_1 = t_2 = 0$ then $t_1' = t_2' = 1$ and then $\dot{w}_\alpha g_1g_2\dot{w}_\alpha^{-1}$ is an appropriate element. We assume $t_1 \neq 0$. Let $t_2 \neq 0$. Then conjugating g_2 by an appropriate element from the group HX_α we can get $x_\alpha(t_2, t_2') = h_2x_\alpha^{-1}(t_1, t_1')h_2^{-1}$. Also, we may assume $m_1 \neq 0, m_2 = 0$ (by conjugating with $x_{\alpha_{r-1}}$). Thus $\dot{w}_\alpha(g_1g_2)$ is an appropriate element. Now we may assume $t_2 = 0, t_2' \neq 0$. Also, we can make $s_1 = 0$. If in addition $s_1' \neq 0$, we are in the situation described above. Let $s_1 = s_1' = 0$. If $m_1 \neq 0$ then $\dot{w}_\gamma g_1\dot{w}_\gamma^{-1}$ is an appropriate element. Assume $s_1 = s_1' = m_1 = 0$. Then $x_{-\beta}g_1x_\beta^{-1}$ is an appropriate element for some $x_{-\beta} \in X_{-\beta}$. ∎

Lemma 20: *If* rank$(G) > 8$, *then the action of* G_1 *on each factor* V_i/V_{i+1} *of the central series of* V *is augmentative.*

Proof: This follows from the Chevalley commutator formula. ∎

Now we can prove our estimate. We use the same trick with subproducts as we used in the case $SL_n(K)$. Assume that we have $2\cdot 2\cdot(6r+24)\cdot 3\cdot 2\cdot 2$ noncentral conjugacy clases; if we identify a subset of this set the product of which covers the whole group, then the product of all classes also covers the whole group. By

Lemma 18 the subproduct of any two classes contains a noncentral element from P. Then by Lemma 19 the subproduct of two classes which have noncentral intersection with P has a nontrivial Levi component. From the estimates for $SL_r(K)$, Lemma 20 and Proposition 3 (with $k = 2$ because every finite Chevalley group is generated by two elements) we see that the subproduct of $2\cdot 2(6r+24)\cdot 3\cdot 2$ classes contains the whole group G_1V and therefore the group U. But every element of G is conjugate to an element from U^-U ([EG]). Thus the product of $48(6r + 24)$ noncentral conjugacy classes covers the whole group G.

References

[AH] Z. Arad and M. Herzog, *Products of conjugacy classes in groups,* Lecture Notes in Mathematics **1112**, Springer-Verlag, Berlin/New York, 1985.

[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.

[D] Y. Dvir, *Covering properties in permutation groups,* in [AH], ch. 3.

[EG] E. W. Ellers and N. Gordeev, *Gauss decomposition with prescribed semisimple part in Chevalley groups,* Communications in Algebra **22** (1994), 5935–5950; **23** (1995), 3085–3098; **24** (1996), 4447–4475.

[EGH] E. W. Ellers, N. Gordeev and M. Herzog, *Covering numbers for Chevalley groups,* Israel Journal of Mathematics **111** (1999), 339–372.

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

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

[Kn] F. Knüppel, *The length-problem for Eichler-transformations,* Forum Mathematicum **10** (1998), 59–74.

[Lev1] A. Lev, *Products of cyclic similarity classes in the groups $GL_n(F)$,* Linear Algebra and its Applications **202** (1994), 235–266.

[Lev2] A. Lev, *The covering number of the group $PSL_n(F)$,* Journal of Algebra **182** (1996), 60–84.

[LL] R. Lawther and M. W. Liebeck, *On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class,* Journal of Combinatorial Theory, Series A **83** (1998), 118–137.

[LiSh] M. W. 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.

[St2] R. Steinberg, *Regular elements of semisimple algebraic groups*, in *Collected Papers*, American Mathematical Society, Providence, RI, 1997, pp. 183–214.

[Z] I. Zisser, *The covering numbers of the sporadic simple groups*, Israel Journal of Mathematics **67** (1989), 217–224.