ISRAEL JOURNAL OF MATHEMATICS 111 (1999), 339–372

COVERING NUMBERS FOR CHEVALLEY GROUPS

BY

ERICH W. ELLERS*

Department of Mathematics, University of Toronto
100 St. George Street, Toronto, Ontario, Canada M5S 3G3
e-mail: ellers@math.toronto.edu

AND

NIKOLAI GORDEEV*

Department of Mathematics, Russian State Pedagogical University
Moyka 48, St. Petersburg, Russia 191-186
e-mail: algebra@ivt.rgpu.spb.ru

AND

MARCEL HERZOG**

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv 69978, Israel
e-mail: herzog@math.tau.ac.il

ABSTRACT

Let G be a quasisimple Chevalley group. We give an upper bound for the covering number $cn(G)$ which is linear in the rank of G, i.e. we give a constant d such that for every noncentral conjugacy class C of G we have $C^{rd} = G$, where $r = \mathrm{rank}G$.

* Research supported in part by NSERC Canada Grant A7251.

** Research supported in part by the Hermann Minkowski-Minerva Center for Geometry at Tel Aviv University.

Received November 30, 1997

1. Introduction

We are dealing with the following problem: Let G be a group and let $\mathfrak{A}$ be a set of subsets of G. Suppose $X^n = G$ for every $X \in \mathfrak{A}$ and for some positive integer n depending on X (here $X^n = \{x_1x_2\cdots x_n | x_i \in X\}$); determine the smallest positive integer n_o (if it exists) such that $X^{n_o} = G$ for all $X \in \mathfrak{A}$. In particular, we are concerned with the case where G is a simple or quasisimple (i.e. G is perfect and G modulo its center is simple [GLS, Definition 4.6]) group and $\mathfrak{A}$ is the set of all nonidentity or noncentral conjugacy classes of G. Here the integer n_o is called the covering number of G. We write $n_o = \mathrm{cn}(G)$.

The covering number is known in the following cases: $\mathrm{cn}(A_n) = \lceil \frac{n}{2} \rceil$ if $n \geq 6$, and $\mathrm{cn}(A_5) = 3$ ([Dv]); $\mathrm{cn}(\mathrm{PSL}_2(K)) = 3$ if K is a finite field and $|K| \geq 4$, and $\mathrm{cn}(\mathrm{PSL}_2(K)) = 2$ if K is an algebraically closed field ([ACM]); $\mathrm{cn}(\mathrm{Sz}(2^{2n+1})) = 3$ ([ACM]); $\mathrm{cn}(\mathrm{PSL}_n(K)) = n$ if $|K| \geq 4$ and $n \geq 4$, and $\mathrm{cn}(\mathrm{PSL}_3(K)) = 3$ if K is a finite field, $|K| \geq 4$, or K is an algebraically closed field ([Lev]). Also, the covering numbers are known for all finite simple groups with order less than 10^6 ([Kar]) and for all sporadic simple groups ([Z]).

In addition to the exact calculation of covering numbers for some classes of simple groups there are estimates of such numbers which also can be useful. In particular, $\mathrm{cn}(G) \leq \min(k(k-1)/2, 4k^2/9)$, where G is a finite simple group and k is the number of its conjugacy classes ([AHS]). In [Go1] it has been proved that for every simple algebraic group G over an algebraically closed field of characteristic 0 and for every noncentral conjugacy class C of G we have $\overline{C^{2r}} = G$, where r is the rank of G and $\overline{C^{2r}}$ is the closure of C^{2r} with respect to the Zariski topology. Thus $C^{4r} = G$ and therefore $\mathrm{cn}(G) \leq 4 \cdot \mathrm{rank}\, G$. Recently Arad, Fisman and Muzychuk ([AFM]) proved that if C is a nonidentity conjugacy class of a finite simple group G and if $n = |C_G(g)|$, where $g \in C$, then $C^n = G$.

The purpose of this paper is to show that there is a constant d such that for every quasisimple Chevalley group G (proper or twisted) the inequality $\mathrm{cn}(G) \leq d \cdot \mathrm{rank}\, G$ holds (here d is general and does not depend on the type, rank, or field of G). By Chevalley group here we mean a group generated by root subgroups corresponding to an irreducible root system in the sense of R. Steinberg ([St]). Thus such groups are always quasisimple except for a few groups over small fields. In the case of twisted groups we consider only groups over finite fields. Thus we consider all proper quasisimple Chevalley groups over arbitrary fields and all twisted quasisimple Chevalley groups over finite fields. It should be noted that all finite simple groups of Lie type belong to the set considered. In general the constant d emerging from our calculations is large. However, we believe that this

constant should be small. In some cases we get better estimates for d than in the general case, e.g. if G is a classical group of rank at least 3 and over a field K with $|K| \geq 4$, or $|k| \geq 4$ in case ${}^2D_{r+1}$. Here we can say $d \leq 2^8 \cdot 3$. However, our proof yields an estimate for d which is valid for all cases.

For more information on covering numbers we refer the reader to the Lecture Notes by Arad and Herzog [AH] which contain results, motivation and applications. There one finds also a discussion on lower and upper bounds.

As mentioned above, the covering number for the projective special linear groups has been determined by Lev [Lev]: $\mathrm{cn}(\mathrm{PSL}_n(K)) = n$ ($|K| \geq 4$, $n \geq 4$). Thus $\mathrm{cn}(G) = \mathrm{rank}G + 1$ in this case, so $\mathrm{cn}(G) \leq 2 \cdot \mathrm{rank}G$. Gordeev showed (see [Go1], [Go2]) that $\mathrm{cn}\, B_r \leq 2r = 2 \cdot \mathrm{rank}B_r$. Examples confirm that this bound cannot be improved. For a large class of groups Gordeev established $\mathrm{cn}(G) \leq 4 \cdot \mathrm{rank}G$. We expect similar results to be true for all Chevalley groups.

The referee informed us that there is a preprint by Lawther and Liebeck [LL] dealing with related topics and using entirely different methods. They provide an upper bound for the conjugacy diameter $\mathrm{cd}(G)$ for a finite simple group G of Lie type, which is linear in the rank of G. They also discuss lower bounds for $\mathrm{cd}(G)$. It follows immediately from the definitions that $\mathrm{cd}(G) \leq \mathrm{cn}(G)$.

2. Notation and terminology

2.1 GROUP THEORY. Let G be a group. Let 1 denote the identity of G and let $[x, y] = xyx^{-1}y^{-1}$ be the commutator of the elements x, y in G. If $X \subset G$, then $X^m = \{x_1 x_2 \cdots x_m | x_i \in X\}$. A conjugacy class C is said to be real if $C^{-1} = C$. Let $I(G)$ denote the augmentation ideal of the group ring $K[G]$, i.e. $I(G) = \ker\epsilon$, where $\epsilon : K[G] \to K$ with $\epsilon|_K = 1_K$ and $\epsilon(G) = 1$.

Let $N_1 \trianglelefteq N \trianglelefteq G$ and $N_1 \trianglelefteq G$. Then the group G acts on the factor group N/N_1 by conjugation. If the group $U = N/N_1$ is abelian, we shall say that U is a G-module and we write the action on the group U in additive form. Also, we let an element $g \in G$ act on U. Thus $g(u)$ means gng^{-1} mod N_1, where u is the image of $n \in N$ in $U = N/N_1$. Note that in the additive language the element $(g-1)(u)$ corresponds to $[g, n]$ mod N_1. We say that an element $g \in G$ acts on U without fixed points if the operator $g - 1$ on U is invertible.

2.2. CHEVALLEY GROUPS (see [St], [Car1, 2]). Here R is an irreducible root system. We shall use the notation of N. Bourbaki ([Bou, Tables I–IX]) for R and for roots. Thus $R = A_r$, B_r, C_r, D_r, E_6, E_7, E_8, F_4, or G_2. The simple root system $\Delta = \{\alpha_1, \ldots, \alpha_r\}$ which generates R is numerated according to [Bou, Tables I–IX].

In the case of twisted groups we attach the root system B_r to the groups of type ${}^2A_{2r}$ and ${}^2D_r$; C_r to ${}^2A_{2r-1}$; F_4 to ${}^2E_6$; G_2 to ${}^3D_4$ (see [Car 1, 2]). If $\beta_1, \ldots, \beta_s \in R$, then $\langle \beta_1, \ldots, \beta_s \rangle := \{\gamma = m_1\beta_1 + \cdots + m_s\beta_s | \gamma \in R,\ m_i \in \mathbb{Z}\}$. Further, $R = R^+ \cup R^-$ where R^+ is the set of positive roots and R^- is the set of negative roots.

Let K be a field. For $\alpha \in R$ let U_α be a root subgroup. Then

$$U_\alpha = \langle x_\alpha(t) | \ t \in K \rangle,$$

or $U_\alpha = \langle x_\alpha(t,s) | \ t,\ s \in K \rangle$ or $U_\alpha = \langle x_\alpha(t,s,q) \mid t,s,q \in K \rangle$ for twisted groups (see [St], [Car1]). Here U_α acts as a group of unipotent matrices on some vector space over the field K. The linear group $G = \langle U_\alpha | \ \alpha \in R \rangle$ acting on the same vector space will be called a Chevalley group defined over K ([St]). As in [St] we define $w_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$ and $w_\alpha = w_\alpha(1)$. Then $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the matrix corresponding to w_α in $\mathrm{SL}_2(K)$. For the twisted group ${}^2A_{2r}$ the matrix corresponding to w_α is $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ in $\mathrm{SU}_3(K)$.

The automorphisms of the field K which correspond to twisted groups will be denoted by Θ and we will write t^Θ instead of $\Theta(t)$ for $t \in K$. The subfield of Θ-invariant elements will be denoted by k. Note that for twisted groups we shall always assume that K is a finite field.

Let $B = HU$ be the Borel subgroup corresponding to the decomposition $R = R^+ \cup R^-$. Here H is a maximal split torus of G and $U = \langle U_\alpha | \ \alpha \in R^+ \rangle$. Also $U^- = \langle U_\alpha | \ \alpha \in R^- \rangle$. Let W be the Weyl group of R and $N \leq G$ be a subgroup such that $H \trianglelefteq N$ and $W \simeq N/H$. An element $n \in N$ will be denoted by $\dot{w}$, where w is the image of n in W. We also use the notation $h_\alpha(t)$ for $t \in K^*$ (see [St]) for semisimple elements of $\langle U_\alpha,\ U_{-\alpha} \rangle$ and $H_\alpha = \langle h_\alpha(t) | \ t \in K^* \rangle$.

2.3. ALGEBRAIC GROUPS (see [Bo]). Let G be an algebraic group defined over a field F, let L/F be an extension field of F. Let $G(L)$ denote a group of L-points. If $X \subset G(L)$, then $\overline{X}$ denotes the Zariski closure of X in $G(L)$.

3. The main result and outline of the proof

THEOREM M: *There is a positive integer d such that $\mathrm{cn}(G) \leq d \cdot \mathrm{rank}\, G$ for every quasisimple proper Chevalley group or quasisimple finite twisted Chevalley group G.*

The statement of this theorem can be split into the following two results. The first, which we shall call M1, is exactly Theorem M, but for the cases where G is

a classical group, i.e. a group of type A_r, B_r, C_r, D_r, ${}^2A_{2r-1}$, ${}^2A_{2r}$, ${}^2D_{r+1}$, of rank ≥ 3. The second, which we call M2, says that for every positive integer r there is a positive integer $d_0 = d_0(r)$ such that $\mathrm{cn}(G) \leq d_0$ if $\mathrm{rank}\, G \leq r$ (here G is, of course, a quasisimple proper Chevalley group or a quasisimple finite twisted Chevalley group). The last statement is much easier to prove than M1 and will be established at the end of the paper. Thus we first concentrate on M1. Let G here be a classical group of rank ≥ 3, but not of type A_r. The case A_r will be considered separately in Section 5.

We choose a parabolic subgroup $P \subset G$ corresponding to $\Delta \backslash \{\alpha_r\}$ (here G is a classical group of rank r). Then $P = LV$ where L is a Levi factor and $V = R_u(P)$ is the unipotent radical of P ([Car2]). The group L in turn can be presented in the form $L = HG_1$, where $G_1 = \langle U_\alpha | \alpha \in \langle \alpha_1, \ldots, \alpha_{r-1} \rangle \rangle$. Note that

$$G_1 \simeq \mathrm{SL}_r(K)/Z \quad \text{or} \quad G_1 \simeq \mathrm{SL}_r(k)/Z \tag{1}$$

for some subgroup $Z \leq Z(\mathrm{SL}_r(K))$ or $Z \leq Z(\mathrm{SL}_r(k))$ (because we remove the last root α_r from the Dynkin diagram). Further, put $\tilde{P} = G_1 V$.

The first and most difficult step to prove M1 is

PROPOSITION 1: *Let C be a noncentral conjugacy class of G. Then C^{32} contains an element $g = zg_1v$ where $z \in Z(G)$, $g_1 \in G_1$, $g_1 \notin Z(G_1)$ and $v \in V$.*

The next step is based on (1), the results of A. Lev on covering numbers for $\mathrm{SL}_n(K)$ ([Lev]), and some estimates of covering numbers for $\mathrm{SL}_n(K)$ where $|K| = 2, 3$. We shall prove

PROPOSITION 2: *If C is a conjugacy class of G containing an element of the form $g = zg_1v$ where $z \in Z(G)$, $g_1 \in G_1$, $g_1 \notin Z(G_1)$, and $v \in V$, then $z_1\tilde{P} \subset C^{64r}$ for some $z_1 \in Z(G)$. If in addition $|K| \geq 4$, or $|k| \geq 4$ if G is of type ${}^2D_{r+1}$, then $z_1\tilde{P} \subset C^{6r}$.*

From Propositions 1 and 2 we obtain

$$\begin{aligned} &z_1\tilde{P} \subset C^{2^5 \cdot 64r}; \\ &z_1\tilde{P} \subset C^{2^5 \cdot 6r} \quad (\text{if } |K| \geq 4, \text{ or } |k| \geq 4 \text{ in case } {}^2D_{r+1}) \end{aligned} \tag{2}$$

for some $z_1 \in Z(G)$. Since $U \subset \tilde{P}$ the inclusion (2) implies

$$\begin{aligned} &z_1U \subset C^{2^5 \cdot 64r}, \quad z_1U^- \subset C^{2^5 \cdot 64r}; \\ &z_1U \subset C^{2^5 \cdot 6r}, \quad z_1U^- \subset C^{2^5 \cdot 6r} \quad (\text{if } |K| \geq 4, \text{ or } |k| \geq 4 \text{ in case } {}^2D_{r+1}). \end{aligned} \tag{3}$$

Further, we use the following result.

THEOREM H ([EGI, II, III]): *Let G be a proper Chevalley group or a finite twisted Chevalley group, and let Q be a noncentral conjugacy class of G. Then for every $h \in H$ there is an element $x \in Q$ such that $x = u_1 h u_2$ where $u_1 \in U^-$ and $u_2 \in U$.*

Note that this is a generalization of a theorem of Sourour ([So]).

According to Theorem H we can find an element $x = u_1 z_1^2 u_2$, where $u_1 \in U^-$, $u_2 \in U$, and z_1 is from (3). Using (3) we get

$$\begin{aligned} &x \in C^{2^6 \cdot 64r}; \\ &x \in C^{2^6 \cdot 6r} \quad (\text{if } |K| \geq 4, \text{ or } |k| \geq 4 \text{ in case } {}^2D_{r+1}). \end{aligned} \tag{4}$$

Since the set C is invariant under conjugation, (4) yields

$$\begin{aligned} &Q \subset C^{2^6 \cdot 64r}; \\ &Q \subset C^{2^6 \cdot 6r} \quad (\text{if } |K| \geq 4, \text{ or } |k| \geq 4 \text{ in case } {}^2D_{r+1}) \end{aligned} \tag{5}$$

for all noncentral conjugacy classes Q and C of the group G. Since every element in G can be presented as a product of two noncentral elements, we obtain from (5):

$$\begin{aligned} &G = C^{2^7 \cdot 64r}; \\ &G = C^{2^7 \cdot 6r} \quad (\text{if } |K| \geq 4, \text{ or } |k| \geq 4 \text{ in case } {}^2D_{r+1}). \end{aligned}$$

This will complete the proof of M1.

4. Auxiliary results

4.1 GROUP THEORY. Let Γ be a group, $V \trianglelefteq \Gamma$, and $F = \Gamma/V$. We assume that the group V has a central filtration $1 = V_m \trianglelefteq V_{m-1} \trianglelefteq \cdots \trianglelefteq V_0 = V$ such that $V_i \trianglelefteq \Gamma$ for every i, every factor V_i/V_{i+1} is a finite-dimensional vector space over some field L, and the natural Γ-action on V_i/V_{i+1} (see 2.1) is L-linear.

PROPOSITION A: *Let $\gamma \in \Gamma$, $u \in V_i$. If γ acts without fixed points on V_i/V_{i+1} (see 2.1), then there is some $v \in V_i$ such that*

$$v\gamma v^{-1} \equiv \gamma u \bmod V_{i+1}.$$

Proof: The operator γ^{-1} acts also without fixed points on V_i/V_{i+1}. Hence $(\gamma^{-1} - 1)v \equiv u \bmod V_{i+1}$ for some $v \in V_i$. This congruence in the multiplicative form gives us $[\gamma^{-1}, v] \equiv u \bmod V_{i+1}$. Thus $v\gamma v^{-1} = \gamma[\gamma^{-1}, v] \equiv \gamma u \bmod V_{i+1}$. ∎

PROPOSITION B: *Let $\gamma \in \Gamma$. Suppose γ acts without fixed points on each factor V_i/V_{i+1}. Then for every $u \in V$ there is some $v \in V$ such that $v\gamma v^{-1} = \gamma u$.*

Proof: This follows immediately from Proposition A by induction. ∎

PROPOSITION C: *Let C be a conjugacy class of Γ and let $\overline{C}$ be its image in $F = \Gamma/V$. Suppose*

(a) *$\overline{C}^k = F$ for some positive integer k,*

(b) *there exists a sequence $g_1, \ldots, g_k \in C$ (where k is the same in (a) as in (b)) such that the group $D = \langle g_1, \ldots, g_k \rangle$ satisfies $I(D)V_i/V_{i+1} = V_i/V_{i+1}$ for every i (here $I(D)$ is the augmentation ideal of $L[D]$). Then*

$$V \subset C^{2k} \quad \text{and} \quad \Gamma = C^{3k}.$$

For the proof of Proposition C we need a few lemmas.

LEMMA 1: *Let Δ be a group and let $g_1, \ldots, g_s, v_1, \ldots, v_s \in \Delta$. Then*

$$(v_1 g_1 v_1^{-1})(v_2 g_2 v_2^{-1}) \cdots (v_s g_s v_s^{-1})\ g_s^{-1} \cdots g_1^{-1} =$$
$$[v_1,\ g_1](g_1\ [v_2,\ g_2]\ g_1^{-1}) \cdots (g_1\ g_2 \cdots g_{s-1}\ [v_s,\ g_s]\ g_{s-1}^{-1} \cdots g_2^{-1} g_1^{-1}).$$

Lemma 1 can be proved by simple calculation.

LEMMA 2: *Let $g_1, \ldots, g_s \in \Gamma$, $v_1, \ldots, v_s \in V_i$, $u_1, \ldots, u_s \in V_{i+1}$ (here Γ, V_i and V_{i+1} are as above). Then the elements*

$$x = (v_1 g_1 v_1^{-1})(v_2 g_2 v_2^{-1}) \cdots (v_s g_s v_s^{-1}) g_s^{-1} \cdots g_1^{-1}$$

and

$$y = (u_1 v_1 g_1 v_1^{-1} u_1^{-1})(u_2 v_2 g_2 v_2^{-1} u_2^{-1}) \cdots (u_s v_s g_s v_s^{-1} u_s^{-1}) g_s^{-1} \cdots g_1^{-1}$$

belong to the group V_i. Moreover, $yx^{-1} \in V_{i+1}$ and

$$x \equiv (1 - g_1)v_1 + g_1(1 - g_2)v_2 + \ldots + g_1 g_2 \cdots g_{s-1}(1 - g_s)v_s \bmod V_{i+1},$$
$$yx^{-1} \equiv (1 - g_1)u_1 + g_1(1 - g_2)u_2 + \ldots + g_1 g_2 \cdots g_{s-1}(1 - g_s)u_s \bmod V_{i+2}$$

(here we use the additive form; see 2.1).

Proof: The inclusion $x, y \in V_i$ and the congruence for x follow directly from Lemma 1. Consider

$$yx^{-1} = (u_1 v_1 g_1 v_1^{-1} u_1^{-1}) \cdots (u_s v_s g_s v_s^{-1} u_s^{-1})(v_s g_s^{-1} v_s^{-1}) \cdots (v_1 g_1^{-1} v_1^{-1}).$$

Put $\tilde{g}_i = v_i g_i v_i^{-1}$. From Lemma 1 we get $yx^{-1} \in V_{i+1}$ and

$$(6) \quad yx^{-1} \equiv (1-\tilde{g}_1)u_1 + \tilde{g}_1(1-\tilde{g}_2)u_2 + \cdots + \tilde{g}_1 \cdots \tilde{g}_{s-1}(1-\tilde{g}_s)u_s \bmod V_{i+2}.$$

Since $1 = V_m \trianglelefteq \cdots \trianglelefteq V_0 = V$ is a central filtration, the operator v_i acts trivially on every factor V_j/V_{j+1}. Hence the operators g and $\tilde{g}$ coincide on V_i/V_{i+1}. Thus in (6) we can change $\tilde{g}_j$ to g_j. ∎

LEMMA 3: *Let $\Delta = \langle g_1, \ldots, g_s \rangle$ be a group and let L be a field. Further, let M be an $L[\Delta]$-module with $\dim_L M < \infty$, and let T: $M \oplus M \oplus \cdots \oplus M \to M$ be a map given by the formula $T((m_1, \ldots, m_s)) = (1-g_1)\, m_1 + g_1\, (1-g_2)\, m_2 + \cdots + g_1\, g_2 \cdots g_{s-1}\, (1-g_s)\, m_s$. If $I(\Delta)M = M$, then $\operatorname{im} T = M$ (where $\operatorname{im} T$ is the image of T).*

Proof: Put $m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_s = 0$. Then

$$(7) \qquad g_1 g_2 \cdots g_{i-1}(1-g_i)M \subset \operatorname{im} T$$

for every i. In particular, $(1-g_1)M \subset \operatorname{im} T$. Hence $(1-g_1)\ \operatorname{im} T \subset \operatorname{im} T$, which in turn implies $g_1\ \operatorname{im} T \subset \operatorname{im} T$ (note that $\operatorname{im} T$ is a subspace of M). Since g_1 is a linear operator on the finite-dimensional vector space M, we also have $g_1^{-1}\ \operatorname{im} T \subset \operatorname{im} T$. Suppose $(1-g_l)M \subset \operatorname{im} T$ and

$$(8) \qquad g_l^{\pm 1}\ \operatorname{im} T \subset \operatorname{im} T$$

for every $l < i$. Then from (7) and (8) we have

$$(9) \qquad (1-g_i)M \subset \operatorname{im} T,$$

which in turn implies (as for g_1)

$$(10) \qquad g_i^{\pm 1}\ \operatorname{im} T \subset \operatorname{im} T.$$

Thus (9) and (10) hold for every i. Now (10) implies that $\operatorname{im} T$ is Δ-invariant (recall $\Delta = \langle g_1, \ldots, g_s \rangle$) and (9) that Δ acts trivially on $M/\operatorname{im} T$. Hence $I(\Delta)M \subset \operatorname{im} T$. But $I(\Delta)M = M$ according to the last assumption in our lemma. Thus $M = \operatorname{im} T$. ∎

Now we return to the proof of Proposition C: First we will show

$$(11) \qquad V \subset C^{2k}.$$

Let $g_1, \ldots, g_k$ be elements satisfying (b). Put $g_0 = g_k^{-1} g_{k-1}^{-1} \cdots g_1^{-1}$. Since $\overline{C}^k = F$, we can present the element g_0 in the form $g_0 = f_0 v_0$, where $f_0 \in C^k$, $v_0 \in V$. Let $v \in V = V_0$. The factor V_0/V_1 is a D-module satisfying the conditions of Lemma 3. Therefore

$$v \equiv (1 - g_1)v_1' + g_1(1 - g_2)v_2' + \cdots + g_1\, g_2 \cdots g_{k-1}(1 - g_k)v_k' \bmod V_1$$

for some $v_1', \ldots, v_k' \in V$. According to Lemma 2,

$$x_0 = (v_1' g_1 v_1'^{-1}) \cdots (v_k'\, g_k v_k'^{-1})\, g_0 \equiv v \bmod V_1.$$

Suppose

$$x_i \equiv (\tilde{v}_1\, g_1 \tilde{v}_1^{-1}) \cdots (\tilde{v}_k\, g_k \tilde{v}_k^{-1}) g_0 \equiv v \bmod V_{i+1} \tag{12}$$

for some $\tilde{v}_1, \ldots, \tilde{v}_k \in V$. Then $v \equiv u x_i \bmod V_{i+2}$ for some $u \in V_{i+1}$. The factor V_{i+1}/V_{i+2} also satisfies the conditions in Lemma 3. Thus

$$u \equiv (1 - g_1)u_1 + g_1(1 - g_2)u_2 + \cdots + g_1 g_2 \cdots g_{k-1}(1 - g_k)u_k \bmod V_{i+2}$$

for some $u_1, \ldots, u_k \in V_{i+1}$. Using Lemma 2 we obtain

$$(u_1 \tilde{v}_1 g_1 \tilde{v}_1^{-1} u_1^{-1}) \cdots (u_k \tilde{v}_k g_k \tilde{v}_k^{-1} u_k^{-1}) g_0 x_i^{-1} \equiv u \bmod V_{i+2}.$$

Put $x_{i+1} = (u_1 \tilde{v}_1 g_1 \tilde{v}_1^{-1} u_1^{-1}) \cdots (u_k \tilde{v}_k g_k \tilde{v}_k^{-1} u_k^{-1}) g_0$. Now we have

$$v \equiv x_{i+1} \bmod V_{i+2}. \tag{13}$$

Since from the assumption (12) we can get (13), we can present every element in V in the form $(v_1 g_1 v_1^{-1}) \cdots (v_k g_k v_k^{-1}) g_0$ for some $v_1, \ldots, v_k \in V$ (recall that V is a nilpotent group). Since $g_0 = f_0 v_0$, $f_0 \in C^k$, we can obtain any element of $V v_0^{-1}$ in C^{2k}. But $V v_0^{-1} = V$ because $v_0 \in V$, and we obtain (11).

Now let $\gamma \in \Gamma$. Since $\overline{C}^k = F$, we have $\gamma = fv$, where $f \in C^k$, $v \in V$. Thus the equality $C^{3k} = \Gamma$ follows from (11). ∎

4.2. CHEVALLEY GROUPS.

PROPOSITION D: *Let G be a Chevalley group (proper or twisted) of rank ≥ 3 (if G is of type A_r we allow $r \geq 2$), and let Q be a noncentral conjugacy class of G. If $z' \in Q^m$ for some $z' \in Z(G)$, then the set Q^{2m} contains an element of the form zu, where $z \in Z(G)$, $u \in U$, $u \neq 1$, or G is a group of type C_r and Q^{2m}*

contains a noncentral element of the form $zh_\alpha(-1)x_\alpha(s)$, *where* α *is a long root,* $z \in Z(G)$, $s \in K$.

Proof: Let α be a maximal positive root of R (or $\alpha = \epsilon_1$ in case G is of type ${}^2A_{2r}$), and let $t \in U_\alpha$ (or $t \in Z(U_{\epsilon_1})$ in the case of ${}^2A_{2r}$). We take $t \neq 1$. Since α is a maximal root (or $\alpha = \epsilon_1$, $t \in Z(U_{\epsilon_1})$ for ${}^2A_{2r}$), we have $t \in Z(U)$. Further, there exists an element $g' \in Q$ that does not commute with t (indeed, G is quasisimple and hence G is generated by every noncentral conjugacy class, in particular, G is generated by elements in Q). We can write $g' = uwb'$ for some $u \in U$, $w \in N$, $b' \in B$. Since t does not commute with g', it does not commute with $g = u^{-1}g'u = wb$, where $b = b'u$ (recall that $t \in Z(U)$). Put $t_1 = gtg^{-1} = wbtb^{-1}w^{-1}$. Therefore $t_1 \in U_{w(\alpha)}$, $t_1 \neq 1$. Since $z' \in Q^m$, we get $g^{-1}z' \in Q^{m-1}$ and therefore $(t^{-1}gt)g^{-1}z' = t^{-1}t_1z' \in Q^m$. We have $t^{-1} \in U_\alpha$, $t_1 \in U_{w(\alpha)}$, $t^{-1}t_1 \neq 1$ (by choice of g). Put $\bar{t} = t^{-1}t_1$. If $\bar{t}$ is a unipotent element, one can easily get a nontrivial unipotent element of the form $\sigma\bar{t}\sigma^{-1}\bar{t}$ for some $\sigma \in G$, and therefore one can get a desired element $zu \in Q^{2m}$. If $\bar{t}^2 \neq 1$ and $\bar{t}^2$ is unipotent, then $\bar{t}^2z'^2 \in Q^{2m}$ is an appropriate element.

Assume that $\bar{t}$ is not unipotent, and that $\bar{t}^2$ is also not unipotent or $\bar{t}^2 = 1$. This can happen only if $w(\alpha) = -\alpha$ (recall, $\bar{t} \in \langle U_\alpha, U_{w(\alpha)}\rangle$). Put $G_\alpha = \langle U_{\pm\alpha}\rangle$ if G is not of type ${}^2A_{2r}$ and put $G_\alpha = \langle Z(U_{\pm\alpha})\rangle$ if G is of type ${}^2A_{2r}$. Thus $\bar{t}$ is a semisimple element of $G_\alpha \simeq \mathrm{SL}_2(K)$ or $\mathrm{SL}_2(k)$ or $\mathrm{PSL}_2(K)$ or $\mathrm{PSL}_2(k)$. If G is not of type C_r and $\operatorname{rank} G \geq 3$, one can easily check that the image of the homomorphism $\varphi : HG_\alpha \to \operatorname{Aut} G_\alpha$ given by the formula $\varphi(x)(y) = xyx^{-1}$, is isomorphic to $\mathrm{PGL}_2(K)$ (or $\mathrm{PGL}_2(k)$). Hence the elements $\bar{t}$, $\bar{t}^{-1}$ belonging to G_α are HG_α-conjugate (recall that α is a long root). Now let γ be a root such that $\{\alpha, \gamma\}$ is a simple root system for an irreducible root system of rank 2. Put $M_\alpha = \langle U_{i\alpha+j\gamma} \mid i \geq 0,\ j \geq 1\rangle$. Then G_α normalizes M_α and for every $x \in G_\alpha$, $x \neq 1$, there exists an element $m_x \in M_\alpha$ such that $xm_xx^{-1} \neq m_x$ (we omit here the simple arguments concerning classical groups of rank 2 which imply these statements). Thus $u = [\bar{t}, y] \neq 1$ for some $y \in M_\alpha$. Since $\bar{t}z' \in Q^m$ and $\bar{t}, \bar{t}^{-1}$ are HG_α- conjugate, we have $\bar{t}^{-1}z' \in Q^m$ and $\bar{t}z'y\bar{t}^{-1}z'y^{-1} = uz'^2 \in Q^{2m}$. Thus we obtain our statement.

Consider now the case where G is a group of type C_r. We have $G_\alpha \simeq \mathrm{SL}_2(K)$ (α is a long root by our choice) and $\bar{t} \in G_\alpha$. Since $\bar{t} = t^{-1}t_1$, where $t^{-1} \in U_\alpha$, $t_1 \in U_{-\alpha}$, the element $\bar{t}$ does not belong to $Z(G_\alpha)$. Hence $\bar{t}$ is conjugate (in G_α) to an element $w_\alpha h_\alpha(\ell)x_\alpha$ for some $\ell \in K^*$ and $x_\alpha \in U_\alpha$ (see [EG I, Lemma 2]) and therefore to $x_\alpha w_\alpha h_\alpha(\ell)$. But

$$(x_\alpha w_\alpha h_\alpha(\ell))(w_\alpha h_\alpha(\ell)x_\alpha) = x_\alpha h_\alpha(-1)x_\alpha = h_\alpha(-1)x'_\alpha \tag{14}$$

for some $x'_\alpha \in U_\alpha$. If $h_\alpha(-1)x'_\alpha \in Z(G)$, then char $K = 2$, $h_\alpha(-1)x'_\alpha = 1$. This means that $\bar{t}$ is a real element. Then we can repeat our previous considerations with M_α and obtain an appropriate element. If char $K \neq 2$, then $h_\alpha(-1)x'_\alpha \notin Z(G)$. Thus we obtain from (14) a noncentral element $h_\alpha(-1)x'_\alpha z'^2 \in Q^{2m}$. ∎

Remark: The trick with conjugate long root elements t, t_1 used at the beginning of the proof of Proposition D is from [Va].

PROPOSITION E: *Let G, G_1, V be as in Section 3. Let $v \in V$, $v \neq 1$. Suppose*

$$v = \prod_{i,j} x_{\epsilon_i+\epsilon_j}, \tag{15}$$

where $x_{\epsilon_i+\epsilon_j} \in U_{\epsilon_i+\epsilon_j}$ (recall that we use the numeration of roots of [Bou] *here). Then the element v is G_1-conjugate to an element*

$$\begin{aligned} &v' = x_{\epsilon_1+\epsilon_2} \cdot x_{\epsilon_3+\epsilon_4} \cdots, \text{ or} \\ &v' = x_{2\epsilon_1} \cdot x_{2\epsilon_2} \cdots x_{2\epsilon_r} \prod_{i,j} x_{\epsilon_i+\epsilon_j} \text{ and the root system } R = C_r, \end{aligned} \tag{16}$$

where $x_{\epsilon_i+\epsilon_j} \in U_{\epsilon_i+\epsilon_j}$, $x_{2\epsilon_i} \in U_{2\epsilon_i}$, and $x_{2\epsilon_k} \neq 1$ for some k, or

$$v' = x_{\epsilon_1}(0,b_1)\cdots x_{\epsilon_r}(0,b_r)\prod_{i,j} x_{\epsilon_i+\epsilon_j} \text{ and } G \text{ is a group of type } {}^2A_{2r},$$

where $x_{\epsilon_i}(0,b_i) \in U_{\epsilon_i}$, $x_{\epsilon_i+\epsilon_j} \in U_{\epsilon_i+\epsilon_j}$, and $b_k \neq 0$ for some k.

Proof: We may assume $x_{\epsilon_1+\epsilon_2} \neq 1$ in the expression (15). Otherwise we can conjugate v by some $\dot{w}$, where $w \in W(G_1)$. Further, assume i, j, k are distinct, then, according to Chevalley's commutator formula [Car1, Theorem 5.2.2],

$$\begin{aligned} &[x_{\epsilon_i+\epsilon_j}(a),\ x_{\epsilon_k-\epsilon_j}(b)] = x_{\epsilon_i+\epsilon_k}(\pm ab), \\ &[x_{\epsilon_i+\epsilon_j}(a),\ x_{\epsilon_k-\epsilon_l}(b)] = 1 \text{ if } l \neq i,j,k; \\ &[x_{\epsilon_i+\epsilon_j}(a),\ x_{\epsilon_i-\epsilon_j}(b)] = 1 \text{ if } R \neq C_r \text{ or } G \text{ is not of type } {}^2A_{2r}; \\ &[x_{\epsilon_i+\epsilon_j}(a),\ x_{\epsilon_i-\epsilon_j}(b)] \in U_{2\epsilon_i} \text{ if } R = C_r \text{ and } [x_{\epsilon_i+\epsilon_j}(a), x_{\epsilon_i-\epsilon_j}(b)] \\ &\qquad\qquad = x_{\epsilon_i}(0,b_i) \text{ for some } b_i \in K \text{ if } G \text{ is of type } {}^2A_{2r}. \end{aligned} \tag{17}$$

Conjugating v by an appropriate $x_{\epsilon_k-\epsilon_2}(b)$, $k > 2$, we can eliminate factors of the form $x_{\epsilon_1+\epsilon_k}$, $k > 2$, in (15) or we obtain a factor of the form $x_{2\epsilon_k} \neq 1$ (in the case $R = C_r$) or a factor $x_{\epsilon_k}(0,b_k)$, $b_k \neq 0$ (in the case ${}^2A_{2r}$). If

we obtain $x_{2\epsilon_k} \neq 1$ or $x_{\epsilon_k}(0, b_k) \neq 1$, we quit, otherwise we continue. Then, conjugating v by an appropriate $x_{\epsilon_k - \epsilon_1}(b)$ we can eliminate factors of the form $x_{\epsilon_2+\epsilon_k}$, $k > 2$, or we obtain factors $x_{2\epsilon_k} \neq 1$ or $x_{\epsilon_k}(0, b_k) \neq 1$. After such procedures we shall have an element v' that is G_1-conjugate to v and has the form $v' = x_{\epsilon_1+\epsilon_2} \prod_{i,j>2} x'_{\epsilon_i+\epsilon_j}$ or v' has factors $x_{2\epsilon_k} \neq 1$ or $x_{\epsilon_k}(0, b_k) \neq 1$. Repeating this process with $x'_{\epsilon_3+\epsilon_4}$, $x'_{\epsilon_5+\epsilon_6}$, etc. we shall obtain an appropriate element. ∎

4.3 ALGEBRAIC GROUPS.

PROPOSITION F: *Let G be a Chevalley group over a field K, char $K = 0$. Consider G as a subset of $\Delta(K)$, where Δ is the corresponding simple algebraic group. Then $\overline{\langle a, b\rangle} = \Delta$ for some $a, b \in G$.*

Proof: There is an element $a \in H$ such that $\overline{\langle a\rangle} = T$, where T is a maximal torus of Δ (here $H \subset T(K)$) ([Bo, Proposition 8.8]). Further, there is only a finite number of closed connected subgroups of Δ containing T ([Bo, Proposition 13.20]). Let $\mathfrak{A}$ be the set of all such subgroups except the group Δ. Then every closed proper subgroup of Δ containing T is contained in $N_G(F)$ for some $F \in \mathfrak{A}$. Thus we have the open subset $M = \Delta \backslash (\bigcup_{F\in\mathfrak{A}} N_G(F))$ of Δ, satisfying the following condition: $\overline{\langle m, a\rangle} = \Delta$ for every $m \in M$. Since char $K = 0$, we have $\overline{G} = \Delta$ and therefore $M \cap G \neq \phi$. ∎

5. Covering numbers for the groups of type A_r

5.1. ESTIMATES FOR COVERING NUMBERS FOR A_1. In [ACM] it has been shown that $\mathrm{cn}(\mathrm{PSL}_2(K)) = 2$ if K is an algebraically closed field, or $= 3$ if K is a finite field. Here we will derive weaker results which hold for any field.

PROPOSITION G: *Let Q be a noncentral conjugacy class of $\mathrm{SL}_2(K)$, $|K| > 5$. Then*

$$Q^4 \supset \mathrm{SL}_2(K) \backslash Z(\mathrm{SL}_2(K)) \tag{18}$$

and

$$Q^8 = \mathrm{SL}_2(K). \tag{19}$$

Proof: We can take an element x in Q that has the form

$$x = \begin{pmatrix} 0 & \alpha \\ -\alpha^{-1} & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{for some } \alpha \in K^*, \quad a \in K.$$

Let $\beta \in K^*$, $\beta^2 \neq \pm 1$, and let

$$d = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}.$$

Then

$$y = d\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} d^{-1} d \begin{pmatrix} 0 & \alpha \\ -\alpha^{-1} & 0 \end{pmatrix} d^{-1} = \begin{pmatrix} 1 & \beta^2 a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \alpha\beta^2 \\ -\alpha^{-1}\beta^{-2} & 0 \end{pmatrix} \in Q.$$

Thus

$$z = yx = \begin{pmatrix} -\beta^2 & 0 \\ 0 & -\beta^{-2} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in Q^2, \quad \text{where } b = a + a\beta^{-2}.$$

Since $\beta^2 \neq \pm 1$, we get that z is a semisimple regular element. Hence $Q^4 \supset \mathrm{SL}_2(K)\backslash Z(\mathrm{SL}_2(K))$ ([EGI]).

(Note that $1 \in Q^4$.) Thus if $|K| > 5$, then we can find $\beta \in K^*$, $\beta^2 \neq \pm 1$, and we get (18). Note that (19) follows automatically from (18). ∎

Remark: We omit the group $\mathrm{SL}_2(\mathrm{GF}(5))$ in our considerations, as we can do with any finite set of finite groups. However, $\mathrm{cn}(\mathrm{PSL}_2(\mathrm{GF}(5))) = 3$ ([ACM]). That means that the third power of any noncentral conjugacy class of $\mathrm{SL}_2(\mathrm{GF}(5))$ contains a semisimple regular element of order 4. The square of the conjugacy class of this element of order 4 gives the whole group $\mathrm{SL}_2(\mathrm{GF}(5))$. Hence $\mathrm{cn}(\mathrm{SL}_2(\mathrm{GF}(5))) \leq 6$.

5.2 THE ESTIMATES OF COVERING NUMBERS FOR A_r, $r > 1, |K| \geq 4$. Here we have the principal result of A. Lev [Lev, Theorem 2]: If Q is a noncentral conjugacy class of $\mathrm{SL}_n(K)$, $n \geq 3$, $|K| \geq 4$, then

$$Q^n \supset \mathrm{SL}_n(K)\backslash Z(\mathrm{SL}_n(K)). \tag{20}$$

The inclusion (20) implies immediately

$$Q^{2n} = \mathrm{SL}_n(K). \tag{21}$$

Remark: If we are concerned with the covering number for $\mathrm{PSL}_n(K)$ only, there is a result of A. Lev [Lev] that is much stronger than (21); namely, $\mathrm{cn}(\mathrm{PSL}_n(K)) = n$ if $|K| \geq 4$, $n \geq 3$, and in the case $n = 3$ the field K is supposed to be finite or algebraically closed.

5.3 ESTIMATES FOR COVERING NUMBERS FOR A_r, $r \geq 2, |K| = 2, 3$.

PROPOSITION H: *Let $K = \mathrm{GF}(2)$ or $\mathrm{GF}(3)$ and let Q be a noncentral conjugacy class of $\mathrm{SL}_n(K)$, $n \geq 3$. Then $Q^{8(n+1)} = \mathrm{SL}_n(K)$.*

Proof of Proposition H:

LEMMA 4: *Let E_{ij} be matrix units. Let $F_n \in \mathrm{GL}_n(K)$ be a cyclic matrix, i.e. a matrix in rational canonical form: $F_n = \sum_{k=2}^{n} E_{k,k-1} + \sum_{i=1}^{n} a_i E_{in}$, $a_i \in K$. Then F_n is $\mathrm{SL}_n(K)$-conjugate to a matrix of the form*

$$\sum_{i+j \geq n+1} a_{ij} E_{ij}, \quad 1 \leq i, j \leq n, \quad a_{ij} \in K \tag{22}$$

i.e. to wb, where

$$w = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$$

and b is upper triangular.

Proof: Clearly $E_{ij}E_{kl} = \delta_{jk}E_{il}$, and $t_{ij} = 1 + E_{ij}$ is a transvection if $i \neq j$. Then for $n \geq 3$,

$$\begin{aligned} &(1 + E_{2n})\,(1 + E_{n-1,1})\,F_n\,(1 - E_{n-1,1})\,(1 - E_{2n}) \\ =&(\sum_{k=3}^{n-1} E_{k,k-1} + \sum_{l=2}^{n-1} b_l\, E_{l,n-1}) + (\sum_{i=1}^{n} a_i'\, E_{in} + \sum_{j=1}^{n-1} a_j''\, E_{nj}) \\ =&F_{n-1} + M_{n-1}, \end{aligned}$$

where F_{n-1} is a cyclic matrix and b_l, a_i', $a_j'' \in K$. The proof is now completed by induction. Observe that our contention is trivial for $n = 1$ and $n = 2$. Also observe that all entries in M_{n-1} are zero except for entries in the last row and the last column and that these zeros remain zeros in the next induction step. ∎

LEMMA 5: *Let Q be a noncentral conjugacy class of $\mathrm{SL}_n(L)$, where L is an arbitrary field and $n \geq 3$. Then Q^4 contains a noncentral upper triangular matrix.*

Proof: We can take a matrix $q \in Q$ of the form $q = q_{n_1} \oplus q_{n_2} \oplus \cdots \oplus q_{n_s}$, where q_{n_i} is an n_i-cyclic matrix and $n_1 + n_2 + \cdots + n_s = n$. By Lemma 4 we may assume that all cyclic components of q are in the form (22), i.e. $q_{n_i} = w_i b_i$. Put

$w = w_1 \oplus \cdots \oplus w_s$ and $b = b_1 \oplus \cdots \oplus b_s$. Then $q = wb$ and $wqw = bw \in Q$, hence $bwwb = b^2 \in Q^2$. If b^2 is a noncentral upper triangular matrix, then $b^2\sigma b^2\sigma^{-1}$ is also a noncentral upper triangular matrix for some $\sigma \in \mathrm{SL}_n(L)$. Thus we will have a noncentral upper triangular matrix in Q^4. If b^2 is a central matrix, we can apply Proposition D. ∎

LEMMA 6: *Let Q be a conjugacy class of a noncentral upper triangular matrix in $\mathrm{SL}_n(K)$, where $K = \mathrm{GF}(2)$ or $\mathrm{GF}(3)$. Then Q^2 contains a transvection.*

Proof: Let $K = \mathrm{GF}(2)$. Then we can take $u \in Q$ in the form

$$u = J_{k_1} \oplus J_{k_2} \oplus \ldots \oplus J_{k_l},$$

where J_{k_j} is the Jordan block of the size k_j. We may assume $k_1 > 1$. Then $t = u^{-1}t_{2n}(1)ut_{2n}(1)$ is a transvection. Since every unipotent element in $\mathrm{SL}_n(\mathrm{GF}(2))$ is real, we have $t \in Q^2$.

Let $K = \mathrm{GF}(3)$. Suppose Q is not semisimple. Then we may take $u \in Q$ in the form $u = J'_{k_1} \oplus J_{k_2} \oplus \cdots \oplus J_{k_l}$, where $J'_{k_1} = J_{k_1}$ or $\sigma J_{k_1}\sigma^{-1}$, where $\sigma = \mathrm{diag}(-1, 1, \ldots, 1)$. Suppose $k_j \geq 3$ for some j, then we may assume $k_1 \geq 3$. Put $u_1 = J'_{k_1}$, $u_2 = J_{k_2+\cdots+k_l}$, $m = k_2+\cdots+k_l$. There exists $\delta \in \mathrm{GL}_m(K)$ such that $\delta u_2\delta^{-1} = u_2^{-1}$. Let $\delta_1 = \mathrm{diag}(\alpha, 1, \ldots, 1) \in \mathrm{GL}_{k_1}(K)$, where $\alpha = \det \delta = \pm 1$. Put $\gamma = \delta_1 \oplus \delta$. We have

$$\gamma u\gamma^{-1} = \delta_1 u_1 \delta_1^{-1} \oplus \delta u_2 \delta^{-1} = \delta_1 u_1 \delta_1^{-1} \oplus u_2^{-1} \in Q^2. \tag{23}$$

Further, we have two possibilities,

$$x\delta_1 u_1 \delta_1^{-1} x^{-1} = u_1^{-1} \quad \text{for some } x \in \mathrm{SL}_{k_1}(K), \tag{24}$$

or

$$x\delta_1 u_1 \delta_1^{-1} x^{-1} = \delta_0 u_1^{-1} \delta_0^{-1}, \tag{25}$$

where $x \in \mathrm{SL}_{k_1}(K)$, $\delta_0 = \mathrm{diag}(-1, 1, \ldots, 1) \in \mathrm{SL}_{k_1}(K)$.

In case (24) we have from (23) that $(x \oplus E_m)\gamma u\gamma^{-1}(x^{-1} \oplus E_m) = u_1^{-1} \oplus u_2^{-1} = u^{-1} \in Q^2$. Hence $t = t_{2k_1}(1)ut_{2k_1}(-1)u^{-1} \in Q^4$. But one easily checks that t is a transvection.

Now let us have (25). Then$(x \oplus E_m)\gamma u\gamma^{-1}(x^{-1} \oplus E_m) = \delta_0 u_1^{-1}\delta_0^{-1} \oplus u_2^{-1} = t_{12}(1)(u_1^{-1} \oplus u_2^{-1}) = t_{12}(1)u^{-1} \in Q^2$, and we obtain $t_{12}(1) \in Q^2$.

Let $k_j \leq 2$ for every j. We may assume $k_1 = 2$. If l is odd, then the element u_2 consists of an even number of Jordan blocks of size ≤ 2. Hence u_2 is real in $\mathrm{SL}_n(K)$ and therefore $u' = u_1 \oplus u_2^{-1} \in Q$. Thus we have a transvection $uu' = u_1^2 \oplus E_m \in Q^2$. If l is even, we put $u_1 = J'_{k_1} \oplus J_{k_2}$, $u_2 = J_{k_3} \oplus \cdots \oplus J_{k_l}$, $m = k_3 + \cdots + k_l$. Thus u_2 is real in $\mathrm{SL}_m(K)$. Hence $u' = u_1 \oplus u_2^{-1} \in Q$. Now we only need to obtain a transvection in $\mathrm{SL}_{k_1+k_2}(K)$ in the form $u_1 z u_1 z^{-1}$, where $z \in \mathrm{SL}_{k_1+k_2}(K)$. If $k_1 + k_2 = 3$, then u_1^2 is a transvection. Let $k_1 + k_2 = 4$, then u_1 is real in $\mathrm{SL}_4(K)$ and the element $t_{24}(1)u_1 t_{24}(-1)u_1^{-1} \in Q^2$ is a transvection. ∎

Now we return to the proof of Proposition H: Let S be the set of all transvections in $\mathrm{SL}_n(K)$. Then

$$S \cup S^2 \cup \cdots \cup S^{n+1} = \mathrm{SL}_n(K) \tag{26}$$

([El]). Since every transvection is a product of two transvections (here $n \geq 3$), (26) implies

$$S^{n+1} = \mathrm{SL}_n(K). \tag{27}$$

Our statement follows from (27) and Lemmas 5 and 6. ∎

6. Proof of Proposition 1

Recall that we consider here only classical groups G of rank ≥ 3 other than of type A_r.

PROPOSITION I: *Let $g = z'u' \in C$ for some $z' \in Z(G)$ and $u' \in U, u' \neq 1$. Then C^4 contains an element of the form zg_1u, where $z \in Z(G)$, $g_1 \in G_1$, $g_1 \notin Z(G_1)$, $u \in V$.*

Proof: The element u' can be presented in the form σv, where $\sigma \in G_1$, $v \in V$ (recall that $u' \in U \leq \tilde{P} = G_1 V$). If $\sigma \neq 1$, then obviously every power of C contains a desired element. Thus we may assume $\sigma = 1$ and $g = z'v$.

Now we consider different cases.

B_r, $r \geq 3$. Here

$$v = \prod_{i=1}^{r} x_{\epsilon_i} \prod_{i,j} x_{\epsilon_i+\epsilon_j}, \tag{28}$$

where $x_{\epsilon_i} \in U_{\epsilon_i}$, $x_{\epsilon_i+\epsilon_j} \in U_{\epsilon_i+\epsilon_j}$, because $V = \langle U_{\epsilon_i},\ U_{\epsilon_i+\epsilon_j} | 1 \leq i, j \leq r \rangle$. (We use the notation of [Bou].)

Note that here $G_1 \simeq \mathrm{SL}_r(K)$. Put $V_1 = \langle U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$, then V_1 is G_1-invariant. Moreover, if we consider the factor group V/V_1 as G_1-module, we obtain the natural action of the group $G_1 \simeq \mathrm{SL}_r(K)$ on the r-dimensional vector space V/V_1. Thus, conjugating v by appropriate elements in G_1, we can get $x_{\epsilon_2} = x_{\epsilon_3} = \cdots = x_{\epsilon_r} = 1$ in (28). If $x_{\epsilon_k+\epsilon_l} \neq 1$ in (28), then we may assume $l = r$ (we can get this by conjugation by an appropriate element $\dot{w}$, where $w \in W(\alpha_2,\ldots,\alpha_{r-1})$). Put $u_1 = \prod_{i=1}^{r-1} x_{\epsilon_i+\epsilon_r}$, $u_2 = \prod_{i,j<r} x_{\epsilon_i+\epsilon_j}$. Then $g = z'v = z'x_{\epsilon_1}u_1u_2 = z'u_1x_{\epsilon_1}u_2$ and $w_{\epsilon_r}gw_{\epsilon_r}^{-1} = z'\bar{u}_1x_{\epsilon_1}u_2$, where $1 \neq \bar{u}_1 = \prod_{i=1}^{r-1} x'_{\epsilon_i-\epsilon_r} \in G_1$ (here $x'_{\epsilon_i-\epsilon_r} = w_{\epsilon_r}x_{\epsilon_i+\epsilon_r}w_{\epsilon_r}^{-1}$). Thus we can get here an appropriate element just in C and therefore in every power of C. (Indeed, the image of such an element in $Z(G)\tilde{P}/V$ is not in the centre and therefore every power of its conjugacy class in $Z(G)\tilde{P}/V$ contains a noncentral element.) Let $x_{\epsilon_i+\epsilon_j} = 1$ for all i, j. Then $v = x_{\epsilon_1}$. If $\mathrm{char}K \neq 2$, then $x_{-\epsilon_2}x_{\epsilon_1}x_{-\epsilon_2}^{-1} = x'_{\epsilon_1-\epsilon_2}x_{\epsilon_1}$ for some $x_{-\epsilon_2} \in U_{-\epsilon_2}$, $x_{-\epsilon_2} \neq 1$, and $x'_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x'_{\epsilon_1-\epsilon_2} \neq 1$. Thus again we have an appropriate element in C and therefore in C^4. Let $\mathrm{char}K = 2$. Then $x_{\epsilon_2-\epsilon_1}x_{\epsilon_2}x_{\epsilon_2-\epsilon_1}^{-1} = x_{\epsilon_1}x'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2}$, where $x_{\epsilon_2-\epsilon_1} \in U_{\epsilon_2-\epsilon_1}$, $x_{\epsilon_2-\epsilon_1} \neq 1$, $x'_{\epsilon_2} \in U_{\epsilon_2}$, $x'_{\epsilon_2} \neq 1$, $x'_{\epsilon_1+\epsilon_2} \in U_{\epsilon_1+\epsilon_2}$, $x'_{\epsilon_1+\epsilon_2} \neq 1$ ([St, Lemma 33], [Car1, Theorem 5.2]). Hence

$$x_{\epsilon_1}x_{\epsilon_2-\epsilon_1}x_{\epsilon_1}x_{\epsilon_2-\epsilon_1}^{-1} = x_{\epsilon_1}^2x'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2} = x'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2} \in Z(G)C^2.$$

Further, $w_{\epsilon_1}x'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2}w_{\epsilon_1}^{-1} = x''_{\epsilon_2-\epsilon_1}x'_{\epsilon_2} \in Z(G)C^2$ for $x''_{\epsilon_2-\epsilon_1} = w_{\epsilon_1}x'_{\epsilon_1+\epsilon_2}w_{\epsilon_1}^{-1} \neq 1$. Thus we have an appropriate element in C^2 and therefore in C^4 (note that here we don't consider the central factor z' of g because it does not influence these calculations).

C_r, $r \ge 3$. Here

$$v = \prod_{i=1}^{r} x_{2\epsilon_i} \prod_{i,j} x_{\epsilon_i+\epsilon_j}, \tag{29}$$

where $x_{2\epsilon_i} \in U_{2\epsilon_i}$, $x_{\epsilon_i+\epsilon_j} \in U_{\epsilon_i+\epsilon_j}$. We may assume $x_{2\epsilon_i} \neq 1$ for some i or we can get an element v' which is conjugate to v, in the form $v' = x_{\epsilon_1+\epsilon_2}x_{\epsilon_3+\epsilon_4}\cdots x_{\epsilon_k+\epsilon_{k+1}} \in Z(G)C$ (it follows from Proposition E). In the last case the element $w_{\epsilon_1}z'v'w_{\epsilon_1}^{-1}$ will be an appropriate element in C. Suppose $x_{2\epsilon_i} \neq 1$; we may assume $i = 1$, so $x_{2\epsilon_1} \neq 1$. Further,

$$[x_{2\epsilon_1}(a), x_{\epsilon_k-\epsilon_1}(b)] = x_{2\epsilon_k}(\pm ab^2)x_{\epsilon_1+\epsilon_k}(\pm ab) \tag{30}$$

([St, Lemma 33], [Car1, Theorem 5.2]). By conjugating v by appropriate elements in groups $\{U_{\epsilon_k-\epsilon_1}\}$ we can eliminate all factors of the form $x_{\epsilon_1+\epsilon_k}$ in (29) (this

follows from (30)). Thus we can suppose

$$v = x_{2\epsilon_1} \prod_{i=2}^{r} x_{2\epsilon_i} \prod_{i,j\neq 1} x_{\epsilon_i+\epsilon_j}. \tag{31}$$

Further, there exists $\sigma \in \langle U_{\pm 2\epsilon_1} \rangle$ such that

$$\sigma x_{2\epsilon_1} \sigma^{-1} = w_{2\epsilon_1} h_{2\epsilon_1} u_{2\epsilon_1}, \tag{32}$$

where $h_{2\epsilon_1} \in H_{2\epsilon_1}$, $u_{2\epsilon_1} \in U_{2\epsilon_1}$. Note that $\sigma x_{2\epsilon_i} \sigma^{-1} = x_{2\epsilon_i}$ for every $i \neq 1$ and $\sigma x_{\epsilon_i+\epsilon_j} \sigma^{-1} = x_{\epsilon_i+\epsilon_j}$ if $i, j \neq 1$. From (31) and (32) we obtain

$$\begin{aligned} v_1 = \sigma v \sigma^{-1} &= \sigma x_{2\epsilon_1} \prod_{i=2}^{r} x_{2\epsilon_i} \prod_{i,j\neq 1} x_{\epsilon_i+\epsilon_j} \sigma^{-1} \\ &= w_{2\epsilon_1} h_{2\epsilon_1} u_{2\epsilon_1} u_1 \in Z(G)C \end{aligned} \tag{33}$$

for some $u_1 \in V$. Also, we have

$$v_2 = (w_{2\epsilon_1} h_{2\epsilon_1})^{-1} v_1 (w_{2\epsilon_1} h_{2\epsilon_1}) = u_{2\epsilon_1} u_1 w_{2\epsilon_1} h_{2\epsilon_1} \in Z(G)C. \tag{34}$$

Note that

$$(w_{2\epsilon_1} h_{2\epsilon_1})^2 = h_{2\epsilon_1}(-1). \tag{35}$$

Now from (33), (34), (35) we have

$$v_3 = v_2 v_1 = u_{2\epsilon_1} u_1 h_{2\epsilon_1}(-1) u_{2\epsilon_1} u_1 = h_{2\epsilon_1}(-1) u_2 \in Z(G)C^2 \tag{36}$$

for some $u_2 \in V$. From (36), $v_4 = x_{\epsilon_1-\epsilon_2} v_3 x_{\epsilon_1-\epsilon_2}^{-1} = h_{2\epsilon_1}(-1) x'_{\epsilon_1-\epsilon_2} u_3 \in Z(G)C^2$, where $x_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x_{\epsilon_1-\epsilon_2} \neq 1$, $u_3 \in V$. If $\operatorname{char} k \neq 2$, then $x'_{\epsilon_1-\epsilon_2} \neq 1$. In this case, put $v_5 = h_{2\epsilon_1}(-1) v_4 h_{2\epsilon_1}(-1) \in Z(G)C^2$. Now $v_6 = v_5 v_4 = (x'_{\epsilon_1-\epsilon_2} u_3)^2 = x''_{\epsilon_1-\epsilon_2} u_4 \in Z(G)C^2$ for some $x''_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x''_{\epsilon_1-\epsilon_2} \neq 1$, $u_4 \in V$. Thus we get an appropriate element in C^4. Suppose $\operatorname{char} K = 2$. From (31) and (30) we obtain $\tilde{v} = x_{\epsilon_2-\epsilon_1} v x_{\epsilon_2-\epsilon_1}^{-1} = v x_{2\epsilon_2} x_{\epsilon_1+\epsilon_2}$, where $x_{\epsilon_2-\epsilon_1} \neq 1$, $x_{\epsilon_1+\epsilon_2} \neq 1$. Thus $v\tilde{v} = x_{\epsilon_1+\epsilon_2} x_{2\epsilon_2} \in Z(G)C^2$. (Note that in the case $\operatorname{char} K = 2$, $v^2 = 1$.) Then $w_{2\epsilon_1} v \tilde{v} w_{2\epsilon_1}^{-1} = x'_{\epsilon_2-\epsilon_1} x_{2\epsilon_2} \in Z(G)C^2$ for some $x'_{\epsilon_2-\epsilon_1} \in U_{\epsilon_2-\epsilon_1}$, $x'_{\epsilon_2-\epsilon_1} \neq 1$ and hence we obtain an appropriate element in C^2.

D_r, $r \geq 4$. According to Proposition E we may assume

$$v = x_{\epsilon_1+\epsilon_2} x_{\epsilon_3+\epsilon_4} x_{\epsilon_5+\epsilon_6} \cdots.$$

Also, we may assume $x_{\epsilon_1+\epsilon_2} \neq 1$. Thus $w_{\epsilon_2+\epsilon_4} z' v w_{\epsilon_2+\epsilon_4}^{-1} = z' x'_{\epsilon_1-\epsilon_4} x'_{\epsilon_3-\epsilon_2} u \in C$ (for some $u \in V$) is an appropriate element in C.

${}^2A_{2r-1}$, $r \geq 3$. Here the root system is C_r and the proof in this case is the same as that for C_r. The only difference is that here we use the commutator formula $[x_{2\epsilon_1}(a),\ x_{\epsilon_k-\epsilon_1}(b)] = x_{2\epsilon_1}(\pm abb^{\Theta}) x_{\epsilon_1+\epsilon_k}(\pm ab)$ instead of (30) ([St, Section 11], [Car 1, 14.4, p. 265]).

${}^2A_{2r}$, $r \geq 3$. Here $R = B_r$ and therefore the element v can be written in the form (28). As in the case B_r we may assume

$$v = x_{\epsilon_1} v_1, \tag{37}$$

where $v_1 \in V_1 = \langle U_{\epsilon_i+\epsilon_j},\ x_{\epsilon_i}(0, b_l) \big| 1 \leq i < j \leq r,\ b_l \in K \rangle$. If among the factors of v_1 there is $x_{\epsilon_k+\epsilon_l} \neq 1$ for some k, l, then

$$v_1 = x_{\epsilon_k+\epsilon_l} x_{\epsilon_k}(0, b_k) x_{\epsilon_l}(0, b_l) v_2, \tag{38}$$

where $v_2 \in V_1$, and among the factors of v_2 there is no element from the root subgroups U_{ϵ_k}, U_{ϵ_l}, $U_{\epsilon_k+\epsilon_l}$. Let $s \in K^*$, $ss^{\Theta} = -1$, $s(s^{\Theta})^{-1} \neq -1$. One can easily check

$$\begin{aligned} &h_{\epsilon_k-\epsilon_l}(s) x_{\epsilon_k+\epsilon_l}(a) h_{\epsilon_k-\epsilon_l}(s^{-1}) = x_{\epsilon_k+\epsilon_l}(s(s^{\Theta})^{-1} a), \\ &h_{\epsilon_k-\epsilon_l}(s) x_{\epsilon_k}(0, b_k) h_{\epsilon_k-\epsilon_l}(s^{-1}) = x_{\epsilon_k}(0, ss^{\Theta} b_k) = x_{\epsilon_k}(0, -b_k), \\ &h_{\epsilon_k-\epsilon_l}(s) x_{\epsilon_l}(0, b_l) h_{\epsilon_k-\epsilon_l}(s^{-1}) = x_{\epsilon_l}(0, (ss^{\Theta})^{-1} b_l) = x_{\epsilon_l}(0, -b_l). \end{aligned} \tag{39}$$

Now from (37), (38), (39) we get $v' = v h_{\epsilon_k-\epsilon_l}(s) v h_{\epsilon_k-\epsilon_l}(s^{-1}) = x'_{\epsilon_1} x'_{\epsilon_k+\epsilon_l} v'_2 \in Z(G)C^2$, where $x'_{\epsilon_k+\epsilon_l} \neq 1, v'_2 \in V_1$ and among factors of v'_2 there is no element from the root subgroups U_{ϵ_k}, U_{ϵ_l}, $U_{\epsilon_k+\epsilon_l}$. We may assume $l \neq 1$. Then $\dot{w}_{\epsilon_l} v' \dot{w}_{\epsilon_l}^{-1} = x'_{\epsilon_1} x'_{\epsilon_k-\epsilon_l} v'_2 \in Z(G)C^2$, $x'_{\epsilon_k-\epsilon_l} \neq 1$. Thus we can find an appropriate element in C^2 and therefore in C^4. Let

$$v = x_{\epsilon_1} \prod_{i=2}^{r} x_{\epsilon_i}(0, b_i). \tag{40}$$

Here $x_{\epsilon_1} = x_{\epsilon_1}(a_1, b_1)$. Further, let δ be the image of the matrix

$$\operatorname{diag}(s, \ldots, s,\ s^{-r}(s^{\Theta})^r, (s^{\Theta})^{-1}, \ldots, (s^{\Theta})^{-1}) \in \mathrm{SU}_{2r+1}(K),$$

$s \in K^*$, $ss^{\Theta} = -1$. One can check

$$\begin{aligned} \delta x_{\epsilon_1}(a_1,\ b_1) \delta^{-1} &= x_{\epsilon_1}(s^{r+1}(s^{\Theta})^{-r} a_1,\ -b_1), \\ \delta x_{\epsilon_i}(0,\ b_i) \delta^{-1} &= x_{\epsilon_i}(0, -b_i). \end{aligned} \tag{41}$$

If $\operatorname{char} K \neq 2$, then

$$s^{r+1}(s^\Theta)^{-r} \neq -1 \tag{42}$$

(indeed, $s^{r+1}(s^\Theta)^{-r} = -1$ implies $(s^\Theta)^{r+1}s^{-r} = -1^\Theta = -1$ and therefore $ss^\Theta = 1$ which contradicts our choice of s). Thus, if $a_1 \neq 0$ and $\operatorname{char} K \neq 2$, then (41), (42) imply

$$v' = v\delta v\delta^{-1} = x_{\epsilon_1}(a_1',\ b_1') \in Z(G)C^2,$$

where $a_1' \neq 0$. Hence

$$x_{-\epsilon_2}v'x_{-\epsilon_2}^{-1} = v'x_{\epsilon_1-\epsilon_2} \in Z(G)C^2$$

for some $x_{-\epsilon_2} \in U_{-\epsilon_2}$, $x_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x_{\epsilon_1-\epsilon_2} \neq 1$. Thus we have an appropriate element in C^2 and hence in C^4. If $a_1 \neq 0$ and $\operatorname{char} K = 2$, then

$$v^2 = x_{\epsilon_1}(0, a_1a_1^\Theta) \in Z(G)C^2. \tag{43}$$

Further,

$$[x_{\epsilon_1}(a,b),\ x_{\epsilon_2-\epsilon_1}(c)] = x_{\epsilon_1+\epsilon_2}(\pm cb^\Theta)x_{\epsilon_2}(\pm ac,\ \pm cc^\Theta b^\Theta) \tag{44}$$

([Car1, p. 265]). From (43) and (44) we obtain

$$v' = v^2x_{\epsilon_2-\epsilon_1}v^2x_{\epsilon_2-\epsilon_1}^{-1} = x_{\epsilon_2}x_{\epsilon_1+\epsilon_2} \in Z(G)C^4,$$

where $x_{\epsilon_2-\epsilon_1} \in U_{\epsilon_2-\epsilon_1}$, $x_{\epsilon_2} \in U_{\epsilon_2}$, $x_{\epsilon_1+\epsilon_2} \in U_{\epsilon_1+\epsilon_2}$, $x_{\epsilon_1+\epsilon_2} \neq 1$. Now $\dot{w}_{\epsilon_1}v'\dot{w}_{\epsilon_1}^{-1} = x_{\epsilon_2}x'_{\epsilon_2-\epsilon_1} \in Z(G)C^4$. Thus we have an appropriate element in C^4. If $a_1 = 0$ we may assume $b_1 \neq 0$. Then by (44) the element $x_{\epsilon_2-\epsilon_1}v\,x_{\epsilon_2-\epsilon_1}^{-1}$ has the factor $x_{\epsilon_1+\epsilon_2} \neq 1$ and we obtain the case considered above.

${}^2D_{r+1}$, $r \geq 3$. Here $R = B_r$ and therefore v has the form (28). If $x_{\epsilon_i} = 1$ for every i, then we can apply Proposition E to obtain an appropriate element in C. If $x_{\epsilon_i} \neq 1$ for some i, we may assume $i = 1$. Further, if $\operatorname{char} K = 2$, then $v_1 = x_{\epsilon_2-\epsilon_1}vx_{\epsilon_2-\epsilon_1}^{-1} = vx'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2}\prod_{k=3}^r x_{\epsilon_2+\epsilon_k}$, where $x'_{\epsilon_1+\epsilon_2} \neq 1$. Hence $v_2 = vv_1 = x'_{\epsilon_2}x'_{\epsilon_1+\epsilon_2}\prod_{k=3}^r x_{\epsilon_2+\epsilon_k} \in Z(G)C^2$ (note that $v^2 = 1$ if $\operatorname{char} K = 2$). Then $w_{\epsilon_1}v_2w_{\epsilon_1}^{-1}$ is an appropriate element. Let $\operatorname{char} K \neq 2$. Put $h = h_{\epsilon_{r-1}-\epsilon_r}(-1)h_{\epsilon_{r-2}-\epsilon_{r-1}}(1)\cdots h_{\epsilon_2-\epsilon_1}((-1)^{r-1})$. One can verify that $hx_{\epsilon_i}h^{-1} = x_{\epsilon_i}^{-1}$ for every $i > 2$. We have

$$v_3 = vhvh^{-1} = x'_{\epsilon_1}\prod\prod x'_{\epsilon_i+\epsilon_j} \in Z(G)C^2. \tag{45}$$

We may assume $v_3 \neq 1$. Indeed, if $v_3 = 1$, we consider the element $v_4 = x_{\epsilon_2}vx_{\epsilon_2}^{-1}hvh^{-1}$ instead of v_3. The element v_4 has also the form (45). Now our proof can be completed in the same way as for B_r. ∎

PROPOSITION J: *Assume G is not of type ${}^2A_{2r}$. Then the set C^2 contains an element of the form $h_{\alpha_r}(\pm 1)g_1 v$, $g_1 \in G_1$, $v \in V$.*

Proof: Here $R = B_r$, C_r, or D_r; $W(G) \simeq AW(G_1)$; $W(G_1) \simeq S_r$, $A \trianglelefteq W(G)$, and A is an abelian group of exponent 2. Further, as the set of representatives of double cosets $W(G) = \bigcup_i W(G_1)\omega_i W(G_1)$ we can take the set $\{\omega_k\}$, where $\omega_0 = 1$ and for $k \geq 1$:

(46)
$$\omega_k = \begin{cases} w_{\epsilon_k} w_{\epsilon_{k+1}} \cdots w_{\epsilon_r} & \text{if } R = B_r, \\ w_{2\epsilon_k} w_{2\epsilon_{k+1}} \cdots w_{2\epsilon_r} & \text{if } R = C_r, \\ w_{\epsilon_k - \epsilon_{k+1}} w_{\epsilon_k + \epsilon_{k+1}} w_{\epsilon_{k+2} - \epsilon_{k+3}} w_{\epsilon_{k+2} + \epsilon_{k+3}} \cdots w_{\epsilon_{r-1} - \epsilon_r} w_{\epsilon_{r-1} + \epsilon_r} & \text{if } R = D_r. \end{cases}$$

(Note that in the cases B_r and C_r the number k can be arbitrary, while in the case D_r the number of integers in the interval $[k, r]$ must be even.) Hence $G = \bigcup_i P\dot{\omega}_i P$ [Car2, Proposition 2.8.1]). Since $C \not\subset P$, one can find an element $x \in C$ of the form $x = \dot{\omega}_i p$, $i \neq 0$. The element p can be written in turn as $p = h_{\alpha_r}(s) g_1' u$ for some $g_1' \in G_1$, $u \in V$. Thus

$$x = \dot{\omega}_i h_{\alpha_r}(s) g_1' u, \quad i \neq 0. \tag{47}$$

By (46) we can express $\dot{\omega}_i$ in the form

$$\dot{\omega}_i = \dot{w}_{\beta_1} \dot{w}_{\beta_2} \cdots \dot{w}_{\beta_s} \dot{w}_{\alpha_r} \tag{48}$$

for some roots $\beta_1, \ldots, \beta_s$ (note that the last root in the expression (46) coincides with α_r). The elements w_{β_i} commute with each other and with w_{α_r}. Moreover, $\dot{w}_{\beta_i}^2 = h_{\beta_i}(-1)$ and $(w_{\alpha_r} h_{\alpha_r}(s))^2 = h_{\alpha_r}(-1)$. Thus

$$(\dot{\omega}_i h_{\alpha_r}(s))^2 = h_{\beta_1}(-1) h_{\beta_2}(-1) \cdots h_{\beta_s}(-1) h_{\alpha_r}(-1). \tag{49}$$

Further, every element in the group H can be written in the form $h_{\alpha_r}(t)h_1$ for some $t \in K^*$ and some $h_1 \in H \cap G_1$. Therefore, (49) yields

$$(\dot{\omega}_i h_{\alpha_r}(s))^2 = h_{\alpha_r}(\pm 1) h_1 \tag{50}$$

for some $h_1 \in H \cap G_1$. From (47) and (50) we obtain $(\dot{\omega}_i h_{\alpha_r}(s))^{-1} x (\dot{\omega}_i h_{\alpha_r}(s))\, x = g_1' u h_{\alpha_r}(\pm 1) h_1 g_1' u = h_{\alpha_r}(\pm 1) g_1 v \in C^2$, where $g_1 \in G_1$, $v \in V$. ∎

PROPOSITION K: *Let G be a group of type ${}^2A_{2r}$. Then C^4 contains an element of the form $g_1 v$, $g_1 \in G_1$, $v \in V$.*

Proof: In the same way as in the proof of Proposition J we can take an element $x \in C$ in the form $\dot{w}_{\epsilon_k} \dot{w}_{\epsilon_{k+1}} \cdots \dot{w}_{\epsilon_r} h_{\alpha_r} g_1' u$, where $h_{\alpha_r} = h_{\alpha_r}(s)$ for some $s \in$

K^*, $g_1' \in G_1$, $u \in V$. Note that the elements $\dot{w}_{\epsilon_i}$ commute with each other and with $\dot{w}_{\epsilon_r} h_{\alpha_r}$. Hence

$$x = \dot{w}_{\epsilon_r} h_{\alpha_r} \dot{w}_{\epsilon_k} \cdots \dot{w}_{\epsilon_{r-1}} g_1' u = \dot{w}_{\epsilon_r} h_{\alpha_r} \dot{\omega} g_1' u, \tag{51}$$

where $\dot{\omega} = \dot{w}_{\epsilon_k} \cdots \dot{w}_{\epsilon_{r-1}}$. Further, there exists an element $x_{\epsilon_r} \in U_{\epsilon_r}$ such that

$$x_{\epsilon_r} \dot{w}_{\epsilon_r} h_{\alpha_r} = x_1 x_2, \tag{52}$$

where $x_1 \in U_{-\epsilon_r}$, $x_2 \in U_{\epsilon_r}$ ([EGIII]). From (51), (52) we have

$$\begin{aligned} y_1 &= x_{\epsilon_r} x x_{\epsilon_r}^{-1} = x_1 x_2 \dot{\omega} g_1' u x_{\epsilon_r}^{-1} \\ &= x_1 \dot{\omega} x_2' g_1' u x_{\epsilon_r}^{-1} = x_1 \dot{\omega} g_1' u_1 = \dot{\omega} x_1' g_1' u_1, \end{aligned} \tag{53}$$

where

$$x_2' = \dot{\omega}^{-1} x_2 \dot{\omega} \in U_{\epsilon_r}, \ x_1' = \dot{\omega}^{-1} x_1 \dot{\omega} \in U_{-\epsilon_r}, \tag{54}$$

and $u_1 = (g_1'^{-1} x_2' g_1') u x_{\epsilon_r}^{-1} \in V$.

Since $x_1 \in U_{-\epsilon_r}$, it can be expressed in the form $x_1 = x_{-\epsilon_r}(a, b)$ for some $a, b \in K$. Further,

$$\dot{\omega}^{-1} x_{-\epsilon_r}(a, b) \dot{\omega} = x_{-\epsilon_r}(\pm a, b). \tag{55}$$

(This equality can be checked easily for the corresponding matrices in $\mathrm{SU}_{2r+1}(K)$; therefore it holds for $G \simeq \mathrm{SU}_{2r+1}(K)/Z$, $Z \leq Z(\mathrm{SU}_{2r+1}(K))$.) Also,

$$h_{\epsilon_r}(-1) x_{-\epsilon_r}(a, b) h_{\epsilon_r}(-1) = x_{\epsilon_r}(-a, b) \tag{56}$$

([St, Section 11]). By (55), (56) we have an element $h = h_{\epsilon_r}(\pm 1)$ such that

$$h x_1 h^{-1} x_1' = x_{-\epsilon_r}(0, b_1) \tag{57}$$

for some $b_1 \in K$. Put $\tilde{x} = h x_1 h^{-1} x_1'$, $g_2 = h g_1' h^{-1}$, $u_2 = h u_1 h^{-1}$, $y_2 = g_2 u_2 h x_1 h^{-1} \dot{\omega}$ (note, $h \dot{\omega} h^{-1} = \dot{\omega}$ because $h = h_{\alpha_r}(\pm 1)$ and among the factors of $\dot{\omega}$ there is no $\dot{w}_{\epsilon_r}$). Obviously $y_2 \in C$. Put $y_3 = y_2 y_1$. By (53) and (54), $y_3 = g_2 u_2 \tilde{x} g_1' u_1 \in C^2$ (note $\dot{\omega}^2 = 1$). Put $y_4 = \tilde{x} g_1' u_1 g_2 u_2 = \tilde{x} g_3 u_3$, where $g_3 = g_1' g_2$, $u_3 = g_2^{-1} u_1 g_2 u_2 \in V$. Obviously $y_4 \in C^2$. Further, let $s \in K^*$ such that $s\bar{s} = -1$. Then from (57), $h_{\alpha_r}(s) \tilde{x} h_{\alpha_r}(s^{-1}) = x_{-\epsilon_r}(0, s\bar{s} b_1) = \tilde{x}^{-1}$. Put $y_5 = h_{\alpha_r}(s) y_4 h_{\alpha_r}(s^{-1}) = \tilde{x}^{-1} g_4 u_4$, where $g_4 = h_{\alpha_r}(s) g_3 h_{\alpha_r}(s^{-1})$, $u_4 = h_{\alpha_r}(s) u_3 h_{\alpha_r}(s^{-1})$, and put $y_6 = g_4 u_4 \tilde{x}^{-1}$. Then $y_6 \in C^2$ and $y_6 y_4 = g_4 u_4 g_3 u_3 = g_1 v \in C^4$, where $g_1 = g_4 g_3 \in G_1$, $v = g_3^{-1} u_4 g_3 u_3 \in V$. ∎

PROPOSITION L: *If $x = h_{\alpha_r}(\pm 1)g_1'v' \in C$ for some $g_1' \in G_1$, $v' \in V$, and if $h_{\alpha_r}(\pm 1)g_1' \notin Z(G)$ (in the case ${}^2A_{2r}$ we suppose $x = g_1'v'$ and $g_1' \notin Z(G)$), then the set C^4 contains an element $x = g_1 v$, where $g_1 \in G_1$, $g_1 \notin Z(G_1)$, $v \in V$.*

Proof: Put $\Gamma = \langle h_{\alpha_r}(\pm 1),\ G_1\rangle$, $\gamma = h_{\alpha_r}(\pm 1)g_1'$. If $\gamma \notin Z(\Gamma)$, then $g = \gamma\sigma\gamma\sigma^{-1} \notin Z(\Gamma)$ for some $\sigma \in G_1$. But $g \in G_1$, and we have

$$\gamma x\gamma^{-1}\sigma x\sigma^{-1} = \gamma(\gamma v'\gamma^{-1})(\sigma\gamma\sigma^{-1})(\sigma v'\sigma^{-1}) = \gamma^2 v'\gamma^{-2}(\gamma\sigma\gamma\sigma^{-1})(\sigma v'\sigma^{-1})$$
$$= \gamma^2 v'\gamma^{-2}g\sigma v'\sigma^{-1} = gv, \quad \text{where } v = g^{-1}(\gamma^2 v'\gamma^{-2}g)\sigma v'\sigma^{-1} \in V.$$

Thus we have an appropriate element just in C^2 and therefore will have it in C^4.

Let $\gamma \in Z(\Gamma)$. We consider the different types.

B_r, $r \geq 3$.

The inclusion $\gamma \in Z(\Gamma)$ implies here

$$\gamma = h_{\epsilon_1-\epsilon_2}(s)h_{\epsilon_2-\epsilon_3}(s^2)\cdots h_{\epsilon_{r-1}-\epsilon_r}(s^{r-1})h_{\epsilon_r}(t)$$

for some s, $t \in K^*$, $s^r = t^2$. It is easy to verify that

$$\gamma x_{\epsilon_i}(a)\gamma^{-1} = x_{\epsilon_i}(sa), \tag{58}$$
$$\gamma x_{\epsilon_i+\epsilon_j}(a)\gamma^{-1} = x_{\epsilon_i+\epsilon_j}(s^2a)$$

for every i, j. Since $\gamma \notin Z(G)$, we have $s \neq 1$. Suppose $s = -1$ (here char $K \neq 2$). Using Proposition A for $V_0 = V$, $V_1 = [V, V]$, we can get an element x_1 that is conjugate to x and has the form $x_1 = \gamma u$, $u \in [V, V] = \langle U_{\epsilon_i+\epsilon_j} \mid 1 \leq i \neq j \leq r\rangle$. Suppose $u \neq 1$. Then $x_1^2 = \gamma^2 u^2 = u^2 \neq 1$ (note that $\gamma^2 = 1$ because $s = -1$ and $\gamma^2 \in G_1$, and $u^2 \neq 1$ because char $K \neq 2$). Thus we have an element $u^2 \neq 1$ in $C^2 \cap \langle U_{\epsilon_i+\epsilon_j} \mid 1 \leq i \neq j \leq r\rangle$. Applying Proposition E we can get an element $\tilde{u} \in C^2$ in the form $\tilde{u} = x_{\epsilon_1+\epsilon_2}x_{\epsilon_3+\epsilon_4}\cdots$. Thus $\dot{w}_{\epsilon_1}\tilde{u}\dot{w}_{\epsilon_1}^{-1}$ is an appropriate element in C^2. Hence we can get such an element in C^4, too. Now let $u = 1$. Then $\gamma x_{\epsilon_1}\dot{\omega}_0\gamma\dot{\omega}_0^{-1}x_{\epsilon_1}^{-1} = \gamma x_{\epsilon_1}\gamma^{-1}x_{\epsilon_1}^{-1} = x_{\epsilon_1}' \in C^2$ for some x_{ϵ_1}, $x_{\epsilon_1}' \in U_{\epsilon_1}$, x_{ϵ_1}, $x_{\epsilon_1}' \neq 1$. Since char $K \neq 2$, we have $x_{-\epsilon_2}x_{\epsilon_1}'x_{-\epsilon_2}^{-1} = x_{\epsilon_1-\epsilon_2}x_{\epsilon_1}'$ and $x_{\epsilon_1-\epsilon_2} \neq 1$. Thus we obtain our element in C^2. Let $s \neq \pm 1$. We may assume $x = \gamma$ (this follows from (58) and Proposition B). Further, $\dot{\omega}_0\gamma\dot{\omega}_0^{-1}x_{\epsilon_1+\epsilon_2}\gamma x_{\epsilon_1+\epsilon_2}^{-1} = x_{\epsilon_1+\epsilon_2}' \in C^2$ for some $x_{\epsilon_1+\epsilon_2}, x_{\epsilon_1+\epsilon_2}' \in U_{\epsilon_1+\epsilon_2}$, $x_{\epsilon_1+\epsilon_2}, x_{\epsilon_1+\epsilon_2}' \neq 1$. Now $\dot{w}_{\epsilon_1}x_{\epsilon_1+\epsilon_2}'\dot{w}_{\epsilon_1}^{-1}$ is an appropriate element in C^2.

C_r.

The inclusion $\gamma \in Z(\Gamma)$ implies here $\gamma = h_{2\epsilon_1}(s)h_{2\epsilon_2}(s)\cdots h_{2\epsilon_r}(s)$ for some $s \in K^*$. Since $\gamma \notin Z(G)$, we have $s^2 \neq 1$. Further, $\gamma x_{2\epsilon_i}(a)\gamma^{-1} = x_{2\epsilon_i}(s^2a)$ and

$$\gamma x_{\epsilon_i+\epsilon_j}(a)\gamma^{-1} = x_{\epsilon_i+\epsilon_j}(s^2a). \tag{59}$$

Using Proposition A we may assume $x = \gamma$. Thus

$$\dot{w}_{2\epsilon_i}(\dot{\omega}_0\gamma\dot{\omega}_0^{-1})x_{\epsilon_1+\epsilon_2}\gamma x_{\epsilon_1+\epsilon_2}^{-1}\dot{w}_{2\epsilon_1}^{-1}$$

is an appropriate element in C^2 (for some $x_{\epsilon_1+\epsilon_2} \in U_{\epsilon_1+\epsilon_2}$, $x_{\epsilon_1+\epsilon_2} \neq 1$).

D_r.

The inclusion $\gamma \in Z(\Gamma)$ implies here

$$\gamma = h_{\epsilon_1-\epsilon_2}(s)h_{\epsilon_2-\epsilon_3}(s^2)\cdots \\ \cdots h_{\epsilon_{r-2}-\epsilon_{r-1}}(s^{r-2})h_{\epsilon_{r-1}-\epsilon_r}(s^{(r-2)/2})h_{\epsilon_{r-1}+\epsilon_r}(s^{(r-2)/2+1})$$

(if r is odd, then s should be a square in K^*). The formula (59) also holds here and using Proposition A we also may assume $x = \gamma$. If $r = 2k$, then $\dot{\omega}_0\gamma\dot{\omega}_0^{-1} = \gamma^{-1}$ and therefore $\dot{w}_{\epsilon_2+\epsilon_3}(\dot{\omega}_0\gamma\dot{\omega}_0^{-1})x_{\epsilon_1+\epsilon_2}\gamma x_{\epsilon_2+\epsilon_3}^{-1}\dot{w}_{\epsilon_2+\epsilon_3}^{-1} \in C^2$ is an appropriate element. Let $r = 2k+1$. Then $w(\epsilon_i) = -\epsilon_i$ for some $w \in W(G)$ and for every $i > 1$. Thus $\delta = \dot{w}\gamma\dot{w}^{-1}\gamma = h_{\epsilon_1-\epsilon_2}(s)h_{\epsilon_1+\epsilon_2}(s) \in C^2$. Further, there exists $w_1 \in W(G)$ such that $\dot{w}_1\delta\dot{w}_1^{-1} = \delta^{-1}$. Thus we have $\dot{w}_1\delta\dot{w}_1^{-1}x_{\epsilon_1-\epsilon_2}\delta x_{\epsilon_1-\epsilon_2}^{-1} = x'_{\epsilon_1-\epsilon_2} \in C^4$ for some $x_{\epsilon_1-\epsilon_2}, x'_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x_{\epsilon_1-\epsilon_2}, x'_{\epsilon_1-\epsilon_2} \neq 1$.

${}^2A_{2r-1}$.

The inclusion $\gamma \in Z(\Gamma)$ implies here $\gamma x_{2\epsilon_i}(a)\gamma^{-1} = x_{2\epsilon_i}(sa)$, $\gamma\, x_{\epsilon_i+\epsilon_j}(a)\gamma^{-1} = x_{\epsilon_i+\epsilon_j}(sa)$ for some $s \in k$ and $s \neq 1$ because $\gamma \notin Z(G)$. Thus again we may assume $x = \gamma$ (Proposition A). The preimage γ in the group $\mathrm{SU}_{2r}(K)$ can be represented by the matrix $\tilde{\gamma} = \mathrm{diag}(t, \ldots, t, (t^\Theta)^{-1}, \ldots, (t^\Theta)^{-1})$, where $tt^\Theta = s$. One can see that $\tilde{\gamma}\dot{\omega}_0\tilde{\gamma}\dot{\omega}_0^{-1} \in Z(\mathrm{SU}_{2r}(K))$. Hence

$$\gamma\dot{\omega}_0\gamma\dot{\omega}_0^{-1} \in Z(G). \tag{60}$$

Let $x_1 = \gamma x_{\epsilon_1+\epsilon_2}\gamma x_{\epsilon_1+\epsilon_2}^{-1} = \gamma^2 x'_{\epsilon_1+\epsilon_2}$. Then $x_1 \in C^2$. If $\gamma^2 \in Z(G)$, then $\dot{w}_{\epsilon_2}x_1\dot{w}_{\epsilon_2}^{-1} = \gamma^2 x''_{\epsilon_1-\epsilon_2} \in C^2$ is an appropriate element for some $x''_{\epsilon_1-\epsilon_2} \in U_{\epsilon_1-\epsilon_2}$, $x''_{\epsilon_1-\epsilon_2} \neq 1$, because $\gamma^2 = (h_{\alpha_r}(\pm 1)g_1)^2 \in G_1$. If $\gamma^2 \notin Z(G)$, then using (60) we obtain $x_2 = \dot{\omega}_0\gamma^2\dot{\omega}_0^{-1}\gamma^2 x'_{\epsilon_1+\epsilon_2} = \delta x'_{\epsilon_1+\epsilon_2} \in C^4$, where $\delta = \dot{\omega}_0\gamma^2\dot{\omega}_0^{-1}\gamma^2 \in Z(G) \cap G_1$. Thus $\dot{w}_{\epsilon_1}x_2\dot{w}_{\epsilon_1}^{-1}$ is an appropriate element in C^4.

${}^2A_{2r}$.

Let $\tilde{\gamma}$ be the preimage of γ in $\mathrm{SU}_{2r+1}(K)$. Then $\tilde{\gamma} = \mathrm{diag}(t, \ldots, t, t^{-r}(t^\Theta)^r, (t^\Theta)^{-1}, \ldots, (t^\Theta)^{-1})$. Using the form $\tilde{\gamma}$ one can easily see

$$\begin{aligned} &\gamma x_{\epsilon_i}(a,b)\gamma^{-1} = x_{\epsilon_i}(t^{r+1}(t^\Theta)^{-r}a,\ tt^\Theta b), \\ &\gamma x_{\epsilon_i+\epsilon_j}(a)\gamma^{-1} = x_{\epsilon_i+\epsilon_j}(tt^\Theta a) \end{aligned} \tag{61}$$

for every i, j. If $t^{r+1}(t^\Theta)^{-r} = 1$, then $t^{r+1} = (t^\Theta)^r$ and therefore $(t^{r+1})^\Theta = t^r$. Thus $t^\Theta = t^{-1}$ and hence $tt^\Theta = 1$. In this case (61) and the condition $\gamma \in Z(\Gamma)$

imply $\gamma \in Z(G)$, which contradicts the assumption of the proposition. Thus $t^{r+1}(t^\Theta)^{-r} \neq 1$. We may assume $v' \in \langle x_{\epsilon_i}(0, b_i),\ U_{\epsilon_i+\epsilon_j} \,\big|\, 1 \leq i, j \leq r\rangle$ (see Proposition A). Moreover, $v' = 1$ if $tt^\Theta \neq 1$ (see Proposition B) or $tt^\Theta = 1$ and $\gamma v' = v'\gamma$. Suppose $tt^\Theta \neq 1$. Then $x = \gamma$. We have $x_{\epsilon_{r-1}+\epsilon_r}\gamma x_{\epsilon_{r-1}+\epsilon_r}^{-1} = \gamma x'_{\epsilon_{r-1}+\epsilon_r}$ for some $x_{\epsilon_{r-1}+\epsilon_r},\ x'_{\epsilon_{r-1}+\epsilon_r} \neq 1$. Put $\delta = \dot\omega_0\gamma\dot\omega_0^{-1}\gamma$. Using the form $\tilde\gamma$ one can see that $\dot w_{\epsilon_r}\delta\dot w_{\epsilon_r}^{-1} = \delta$. Thus $\omega_r(\dot\omega_0\gamma\dot\omega_0^{-1})(\gamma x'_{\epsilon_{r-1}+\epsilon_r})\dot\omega_r^{-1} = \dot\omega_r\delta x'_{\epsilon_{r-1}+\epsilon_r}\dot\omega_r^{-1} = \delta x''_{\epsilon_{r-1}-\epsilon_r} \in C^2$ is an appropriate element because $\delta \in G_1$ (recall $\gamma \in G_1$ in the case ${}^2A_{2r}$). Suppose $tt^\Theta = 1$ and $x = \gamma v' = v'\gamma$. If $v' \neq 1$, then we may assume

$$v' = x_{\epsilon_1+\epsilon_2}x_{\epsilon_1}(0,\ b_1)x_{\epsilon_2}(0, b_2)v'_1, \tag{62}$$

where $x_{\epsilon_1+\epsilon_2} \in U_{\epsilon_1+\epsilon_2},\ x_{\epsilon_1+\epsilon_2} \neq 1,\ v'_1 \in \langle U_{\epsilon_i+\epsilon_j},\ x_{\epsilon_i}(0, b_i) \big| i, j \neq 1, 2\rangle$. Indeed, if among the factors of v' there is $x_{\epsilon_k+\epsilon_l} \neq 1$, then conjugating x by an appropriate $\dot w,\ w \in W(G_1)$, we obtain $k = 1, l = 2$. If all factors of v' have the form $x_{\epsilon_i}(0, b_i)$ and $x_{\epsilon_k}(0,\ b_k) \neq 1$ for some k, then conjugating x by an element in the group $U_{\epsilon_l-\epsilon_k}$ we can obtain a nontrivial factor $x_{\epsilon_k+\epsilon_l}$ (see (44)). Thus we suppose (62). From (35) we obtain for some $h \in H$

$$v'hv'h^{-1} = x'_{\epsilon_1+\epsilon_2}v''_1, \tag{63}$$

where $x'_{\epsilon_1+\epsilon_2} \neq 1$ and among the factors of v''_1 there are no elements from the groups $U_{\epsilon_1},\ U_{\epsilon_2},\ U_{\epsilon_1+\epsilon_2}$. Since $x = \gamma v' = v'\gamma$, using (62), (63) we obtain

$$x_1 = xhxh^{-1} = \gamma v'hv'h^{-1}\gamma = \gamma^2 x'_{\epsilon_1+\epsilon_2}v''_1 \in C^2. \tag{64}$$

Further, for some $h_1 \in H$

$$h_1v'h_1^{-1} = v'^{-1} \tag{65}$$

(it follows from (61)). From (65)

$$x_2 = xh_1xh_1^{-1} = \gamma^2 \in C^2. \tag{66}$$

Let $\delta = \dot\omega_0\gamma^2\dot\omega_0^{-1}\gamma^2$. Since $\gamma \in G_1$, we have $\delta \in G_1$. From (64), (66)

$$x_3 = \dot\omega_0 x_2\dot\omega_0^{-1}x_1 = \delta x'_{\epsilon_1+\epsilon_2}v''_1 \in C^4. \tag{67}$$

Further, $\dot w_{\epsilon_r}\delta\dot w_{\epsilon_r}^{-1} = \delta$ (this follows as above from the form $\tilde\gamma$). From (67) we have $x_4 = \dot w_{\epsilon_1}x_3\dot w_{\epsilon_1}^{-1} \in C^4$ as an appropriate element. Let $v' = 1$. Then $x = \gamma$. From (61)

$$x_{\epsilon_1}xx_{\epsilon_1}^{-1} = \gamma x'_{\epsilon_1} \in C \tag{68}$$

for some x_{ϵ_1}, $x'_{\epsilon_1} \neq 1$. In the same way

$$x''_{\epsilon_1}\gamma \in C, \tag{69}$$

where $x'_{\epsilon_1}x''_{\epsilon_1} = x_{\epsilon_1}(0, b_1)$, $b_1 \neq 0$. From (68), (69)

$$y = \gamma x'_{\epsilon_1}x''_{\epsilon_1}\gamma = \gamma^2 x_{\epsilon_1}(0, b_1) \in C^2 \tag{70}$$

(recall that γ commutes with $x_{\epsilon_i}(0, b_i)$). From (44) and (70)

$$y_1 = x_{\epsilon_2-\epsilon_1}yx^{-1}_{\epsilon_2-\epsilon_1} = \gamma^2 x_{\epsilon_1}(0, b_1)x_{\epsilon_2}(0, b_2)x_{\epsilon_1+\epsilon_2} \in C^2, \tag{71}$$

where $x_{\epsilon_1+\epsilon_2} \neq 1$. Further, $\dot{\omega}_0\gamma\dot{\omega}_0^{-1} \in C$. Using the same arguments as above we obtain

$$y_2 = \dot{\omega}_0\gamma^2\dot{\omega}_0^{-1}x_{\epsilon_1}(0, -b_1) \in C^2. \tag{72}$$

From (71), (72)

$$y_3 = y_2y_1 = \dot{\omega}_0\gamma^2\dot{\omega}_0^{-1}\gamma^2 x_{\epsilon_2}(0, b_2)x_{\epsilon_1+\epsilon_2} \in C^4.$$

Now $\dot{w}_{\epsilon_1}y_3\dot{w}^{-1}_{\epsilon_1}$ is an appropriate element from C^4.

[2] D_{r+1}.

Since $\gamma = h_{\epsilon_r}(\pm 1)g_1 \in Z(\Gamma)$, we have $g_1 \in H_1 = G_1 \cap H$. Then

$$\gamma = h_{\epsilon_1-\epsilon_2}(s_1)\cdots h_{\epsilon_{r-1}-\epsilon_r}(s_{r-1})h_{\epsilon_r}(\pm 1),$$

where $s_i \in k^*$. All parameters $s_1, \ldots, s_{r-1}, \pm 1$ in the expression for γ belong to k, so $\dot{\omega}_0\gamma\dot{\omega}_0^{-1} = \gamma^{-1}$. Now the proof proceeds as in the case B_r. ∎

Now we can prove Proposition 1: According to Propositions J and K one can find an element $x = g_1v$ in C^4. If $\gamma = g_1 \notin Z(G)$, using Proposition L, we can find an element $x' = z'g'_1v$, $g'_1 \notin Z(G)$, in C^{16}. If $\gamma = g_1 \in Z(G)$ and $v \neq 1$, then we can apply Proposition I and again obtain an appropriate element in C^{16}. Let $x \in Z(G) \cap C^4$. By Proposition D we have an element $x' = zu$, $z \in Z(G)$, $u \in U, u \neq 1$, in C^8 if $R \neq C_r$; or $x' = zh_\alpha(-1)x_\alpha(s) \in C^8, x' \notin Z(G)$, for some long root α, $z \in Z(G)$, if $R = C_r$. Now if $R \neq C_r$, then we apply Proposition I and we obtain an appropriate element in C^{32}. Let $R = C_r$, then by conjugation by an appropriate element $\dot{\omega}$ we can get $\alpha = \alpha_r$. Further, in the case C_r we have $|Z(G)| = 1$ or 2 and $z \in G_1$ or $zh_{\alpha_r}(-1) \in G_1$. Thus we can apply Proposition L and obtain an appropriate element in C^{32}. Note that if we find an element of the form zg_1v, $g_1 \notin Z(G_1)$, $z \in Z(G)$, in C^m for some m, then we can find an element of such form in any power of C^m. Thus in all cases we can find an element $x = zg_1v$, $g_1 \notin Z(G)$, in C^{32} for every noncentral conjugacy class C. ∎

7. Proof of Proposition 2

We shall use here Proposition C. We put $\Gamma = \tilde{P}$, $V = V$, $F = G_1$, and Q is the conjugacy class of the element $g_1 v$ (from Proposition 2) in $\tilde{P}$. Further we put

$$\ell = \begin{cases} 2 \cdot \operatorname{rank} G & \text{if } |K| \geq 4 \text{ (or } |k| \geq 4 \text{ if } G \text{ is of type } {}^2D_{r+1}), \\ 16(\operatorname{rank} G + 1) & \text{if } |K| < 4 \text{ (or } |k| < 4 \text{ if } G \text{ is of type } {}^2D_{r+1}). \end{cases}$$

The group G_1 here is isomorphic to a factor group of $\mathrm{SL}_r(K)$ (or $\mathrm{SL}_r(k)$ if G is of type ${}^2D_{r+1}$), ($r = \operatorname{rank} G$). From (21) (see Section 5.2) and Proposition H we get

$$\overline{Q}^{\ell} = G_1, \tag{73}$$

where $\overline{Q}$ is the image of Q in $G_1 = \tilde{P}/V$.

Now we define a subgroup $D_1 \leq G_1$ in the following way. If char $K = p \neq 0$, then we put $D_1 = \langle x_\alpha(t) | \alpha \in \langle \alpha_1, \ldots, \alpha_{r-1} \rangle, t \in \mathrm{GF}(p) \rangle$. Thus in this case the group D_1 is a factor group of $\mathrm{SL}_r(\mathrm{GF}(p))$. If char $K = 0$, then according to Proposition F we can find $a, b \in G_1$ such that the group $\langle a, b \rangle$ is dense in G_1. Put $D_1 = \langle a, b \rangle$. Since every Chevalley group is generated by two elements, the group D_1 in the first case is also generated by two elements which we also will denote by a and b.

Both generators a and b of the group D_1 are noncentral elements. Using (18) and Proposition H we obtain $a, b \in \overline{Q}^{\ell/2}$. This inclusion implies that $D_1 \leq \langle g_1, \ldots, g_\ell \rangle$, where $g_1, \ldots, g_\ell$ are some elements in C. Put $D = \langle g_1, \ldots, g_\ell \rangle$.

Now we will check the condition (b) of Proposition C. Obviously, we can check the condition (b) for the subgroup D_1 of D instead of for D. Moreover, in the case of char $K = 0$ we can check the condition (b) for any dense subgroup of G_1 (note that the action of G_1 on V_i/V_{i+1} is algebraic). Hence in the case char $K = 0$ we can check the condition (b) for $\langle x_\alpha(t) | \alpha \in \langle \alpha_1, \ldots, \alpha_{r-1} \rangle, t \in \mathbb{Q} \rangle$ (here $\mathbb{Q}$ is the field of rational numbers), i.e. for a factor group of $\mathrm{SL}_r(\mathbb{Q})$.

B_r, $r \geq 3$.

Here $V = \langle U_{\epsilon_i}, U_{\epsilon_i + \epsilon_j} | 1 \leq i, j \leq r \rangle$, $V_0 = V$, $V_1 = \langle U_{\epsilon_i + \epsilon_j} | 1 \leq i, j \leq r \rangle$. We have $G_1 \simeq \mathrm{SL}_r(K)$ and V_0/V_1 is an r-dimensional $K[G_1]$-module, where the group $G_1 \simeq \mathrm{SL}_r(K)$ acts in the natural way. Hence $I(\mathrm{SL}_r(K'))V_0/V_1 = V_0/V_1$ for every subfield $K' \subset K$. Further,

$$[x_{\epsilon_k - \epsilon_j}(1), x_{\epsilon_i + \epsilon_j}(a)] = x_{\epsilon_i + \epsilon_k}(\pm a). \tag{74}$$

Hence every element of the $K[G_1]$-module V_1 can be presented (in additive form) as a sum of elements $(x_{\epsilon_k - \epsilon_j}(1) - 1)x_{\epsilon_1 + \epsilon_j}(a)$. This implies the condition (b).

C_r.

Here $V_0 = V = \langle U_{2\epsilon_i},\ U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$, $V_1 = 1$. We also have (74) and

$$[x_{\epsilon_j-\epsilon_i}(1),\ x_{2\epsilon_i}(a)] = x_{2\epsilon_j}(\pm a)x_{\epsilon_j+\epsilon_i}(\pm a) \tag{75}$$

([St, Lemma 33], [Car1, Section 5.2]). These formulas show that every element in the $K[G_1]$-module V is a sum of elements of the form $(x_{\epsilon_i-\epsilon_j}(1) - 1)v$, where $v \in V$. This gives the condition (b).

D_r.

Here $V_0 = V = \langle U_{\epsilon_i+\epsilon_j} |\ 1 \le i < j \le r\rangle$, $V_1 = 1$. The proof is the same as above.

${}^2A_{2r-1}$, $r \ge 3$.

Here $V_0 = V = \langle U_{2\epsilon_i},\ U_{\epsilon_i+\epsilon_j} | 1 \le i < j \le r\rangle$, $V_1 = 1$. We also have (74), (75) ([St, Section 11], [Car1, p. 265]), and can check the condition (b) as in the case C_r.

${}^2A_{2r}$, $r \ge 3$.

Here $V_0 = V = \langle U_{\epsilon_i}, U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$,

$$V_1 = \langle x_{\epsilon_i}(0,b), U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r,\ b \in K,\ b + b^\Theta = 0\rangle,$$

$V_2 = \langle U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$. We have

$$[x_{\epsilon_i-\epsilon_j}(1),\ x_{\epsilon_j}(a,b)] = x_{\epsilon_i}(\pm a, \pm b^\Theta)x_{\epsilon_i+\epsilon_j}(\pm b^\Theta) \tag{76}$$

([Car1, p. 265]), and also (74). Using (74) and (76), we again obtain the condition (b).

${}^2D_{r+1}$.

Here $V_0 = V = \langle U_{\epsilon_i},\ U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$, $V_1 = \langle U_{\epsilon_i+\epsilon_j} | 1 \le i,j \le r\rangle$. We have

$$[x_{\epsilon_i-\epsilon_j}(1),\ x_{\epsilon_j}(u)] = x_{\epsilon_i}(\pm u)x_{\epsilon_i+\epsilon_j}(\pm u\bar{u}) \tag{77}$$

([St, Section 11], [Car1, p. 265]), and also (74). Using (74) and (77) we obtain the condition (b).

Now we have checked the condition (b) and have the condition (a) from (73). Thus

$$\tilde{P} = Q^{3\ell} \tag{78}$$

and

$$z_1\tilde{P} \subset C^{3\ell}, \tag{79}$$

where $3\ell = 6r$ if $|K| \ge 4$ (or $|k| \ge 4$ in the case ${}^2D_{r+1}$) or $3\ell = 48(r+1)$. Note, instead of (78), (79) we can write $\tilde{P} = Q^{3\ell+m}$, $z_1\tilde{P} \subset C^{3\ell+m}$ for every positive integer m. Thus we have $z_1\tilde{P} \subset C^{64r}$. ∎

8. Proof of M2

We prove here that for every positive integer r there exists a positive integer $d_0 = d_0(r)$ such that

$$\mathrm{cn}(G) \leq d_0 \tag{80}$$

for every proper quasisimple Chevalley group G of rank $\leq r$ and for every finite twisted quasisimple Chevalley group of rank $\leq r$.

First we consider the cases where G is of type A_1, B_2 (char $K \neq 2$), or C_r. For the case A_1 the inequality (80) follows from Proposition G. The case C_r was considered before, in M1. For B_2 (char $K \neq 2$) we prove

PROPOSITION M: *Let G be a group of type B_2,* char $K \neq 2$, $|K| > 5$. *Then* $\mathrm{cn}(G) \leq 448$.

Proof of Proposition M:

LEMMA 7: *Let $g = zu \in G$, $z \in Z(G)$, $u \in U$, $u \neq 1$, and let C be the conjugacy class of g. Then $C^{112} = G$.*

Proof: Put $G_1 = \langle U_{\pm(\epsilon_1 - \epsilon_2)} \rangle$, $V = \langle U_{\epsilon_1}, U_{\epsilon_2}, U_{\epsilon_1+\epsilon_2} \rangle$, $\tilde{P} = G_1 V$. We have $u = \sigma v$, where $\sigma \in U_{\epsilon_1-\epsilon_2}$, $v \in V$. We may assume $\sigma \neq 1$. Indeed, let $\sigma = 1$. We may assume $v = x_{\epsilon_1} x_{\epsilon_1+\epsilon_2}$, where $x_{\epsilon_1+\epsilon_2} \neq 1$ (this is easy to get by conjugation). Then $w_{\epsilon_2} v w_{\epsilon_2}^{-1}$ is an appropriate element. Let Q be a conjugacy class of u in $\tilde{P}$ and $\overline{Q}$ its image in G_1. We have $\overline{Q}^8 = G_1$ (see (19)). The factor $V/U_{\epsilon_1+\epsilon_2}$ satisfies the condition (b) of Propositon C with respect to the group D introduced in the preceding section. (Indeed, $V/U_{\epsilon_1+\epsilon_2}$ is a standard SL_2-module.) Using also (18) we get (as above) from Proposition C that $\tilde{Q}^{24} = \tilde{P}/U_{\epsilon_1+\epsilon_2}$; moreover, $V/U_{\epsilon_1+\epsilon_2} \subset \tilde{Q}^{16}$, where $\tilde{Q}$ is the image of Q in $V/U_{\epsilon_1+\epsilon_2}$. Since char $K \neq 2$, every element of the group $U_{\epsilon_1+\epsilon_2}$ is a commutator $[u_1, u_2]$ for some $u_1, u_2 \in V$. Hence every element of $U_{\epsilon_1+\epsilon_2}$ is contained in Q^{32}. Thus $\tilde{P} = Q^{24+32} = Q^{56}$. Since the order of the element z is 1 or 2, we have $\tilde{P} \subset C^{56}$. Thus $U \subset C^{56}$ and according to Theorem H: $G = C^{112}$. ∎

LEMMA 8: *Let C be a noncentral conjugacy class such that C^2 contains an element from the center of G, then $C^{224} = G$.*

Proof: We proceed as in Proposition D. Namely, if $g \in C$, then $g^{-1}z \in C$ for some $z \in Z(G)$. For some element t in the long root subgroup U_β we have that $tgt^{-1}g^{-1}$ is either a nontrivial unipotent element or a noncentral element in $\langle U_{\pm\alpha} \rangle$ where α is a long root. In the first case we apply Lemma 7. In the second case we may assume that $\alpha = \epsilon_1 - \epsilon_2$. Thus we have an element $x \in C^2$

of the form $x = zg_1$, where $g_1 \in G_1$, $g_1 \notin Z(G_1)$. Then we can repeat the considerations of the proof of Lemma 7. ∎

Now we can prove Proposition M.

Let C be a noncentral conjugacy class of G. Then we can find an element $x \in C^2$ of the form $x = h_{\epsilon_2}(\pm 1)g_1 v$, $g_1 \in G_1$, $v \in V$ (see the proof of Proposition J). If $x \in Z(G)$ or $h_{\epsilon_2}(\pm 1)g_1 \in Z(G)$, then $C^{224} = G$ according to Lemmas 7 and 8. Let $h_{\epsilon_2}(\pm 1)g_1 \notin Z(G)$. If $h_{\epsilon_2}(\pm 1)g_1 \notin Z(\Gamma)$ for $\Gamma = \langle h_{\epsilon_2}(\pm 1),\ G_1\rangle$, then C^4 contains an element of the form $g_1' v'$, where $g_1' \in G_1$, $g_1' \notin Z(G_1), v' \in V$ (see proof of Proposition L). Again as in the proof of Lemma 7 we get $C^{4\cdot 112} = G$. Now let $h = h_{\epsilon_2}(\pm 1)g_1 \in Z(\Gamma)$. Then $g_1 = h_{\epsilon_1 - \epsilon_2}(-1)$. Using Proposition A we can obtain $v = x_{\epsilon_1+\epsilon_2}$. Then $x^2 = h^2 v^2 = v^2$. If $v \neq 1$, then $v^2 \neq 1$, so we have a nontrivial unipotent element in C^4. Thus $C^{4\cdot 112} = G$. If $v = 1$, then C^4 contains 1 and, applying Lemma 8, we obtain $C^{4\cdot 112} = G$. ∎

Now we will prove (80) for all remaining cases. We need the following lemmas.

LEMMA 9: *Assume G is not of type A_1, C_r, B_2 with* char $K \neq 2$, *or ${}^2G_2$. Further, let $\beta \in R$ and let $\{U_\beta^i\}$ be the central series of U_β (i.e. $U_\beta^i = [U_\beta^{i-1}, U_\beta]$). Let $x_\beta \in U_\beta^i$, $x_\beta \notin U_\beta^{i+1}$. Then $hx_\beta h^{-1} \equiv x_\beta^{-1} \bmod U_\beta^{i+1}$ for some $h \in H$.*

Proof: Let G be a proper Chevalley group. Then rank $G \geq 2$. For a group of type B_2, char $K = 2$, we can take $h = 1$. Thus we may assume that G is not of type B_2. Then for every root β there exists a long root α such that $h_\alpha(-1)x_\alpha(a)h_\alpha(-1) = x_\alpha(-a)$ (if char $K = 2$, then $-1 = 1$ and $h = 1$).

Let G be a twisted group. Consider groups of rank 1. If G is of type ${}^2A_2$, then $U_\beta = \langle x_\beta(a,b) \big| a, b \in K,\ b + b^\Theta + aa^\Theta = 0\rangle$. Here $U_\beta^1 = \langle x_\beta(0,b) \big| b \in K,\ b + b^\Theta = 0\rangle$, $U_\beta^2 = 1$, and $h_\beta(-1)x_\beta(a,b)h_\beta(-1) = x_\beta(-a,b)$, $h_\beta(s)x_\beta(0,b)h_\beta(s^{-1}) = x_\beta(0,-b)$ for $s \in K$ such that $ss^\Theta = -1$ ([St, Section 11]).

Let G be a group of type ${}^2B_2$. Then char $K = 2$, $U_\beta = \langle x_\beta(a,b) \big| a,\ b \in K\rangle$, $U_\beta^1 = \langle x_\beta(0,b) \big| b \in K\rangle$, $U_\beta^2 = 1$, and $x_\beta^2(a,b) = x_\beta(0,b')$, $x_\beta^2(0,b) = x_\beta(0,0)$. Thus we can take $h = 1$ here.

Consider groups of rank 2, i.e. ${}^2A_3$, ${}^2A_4$, ${}^3D_4$, ${}^2F_4$. The last is a group over a field of characteristic 2. Hence we can take $h = 1$. Let G be of type ${}^2A_3$, let α_1 be a short root and α_2 a long root. Then $h_{\alpha_1}(s)x_{\alpha_2}(a)h_{\alpha_1}(s^{-1}) = x_{\alpha_2}((ss^\Theta)^{-1}a)$. We can find $s \in K^*$ such that $ss^\Theta = -1$. Put here $h = h_{\alpha_1}(s)$. Further, $h_{\alpha_1}(-1)x_{\alpha_1}(a)h_{\alpha_1}(-1) = x_{\alpha_1}(-a)$. Let G be of type ${}^2A_4$. For short roots we can use the same considerations as for ${}^2A_2$, and if $\beta = \alpha_1$ is a long root, then $h_{\alpha_2}(-1)x_{\alpha_1}(a)h_{\alpha_2}(-1) = x_{\alpha_1}(-a)$.

The case ${}^3D_4$ as well as the cases of rank ≥ 3, all have the same proof as the proof for untwisted groups. ∎

LEMMA 10: *Let G be a finite group of rank ≥ 2, but not of the type ${}^2A_{2r}$, C_r, B_2, (char $K \neq 2$), or ${}^2F_4$. Suppose $|K| > (n|R^+|+1)^3$. Then there exists an element $h \in H$ such that h^n is a regular element.*

Proof: The root subgroups for the groups considered are only one-parameter groups, i.e. $U_\alpha = \langle x_\alpha(a)\rangle$, where $a \in K$ or k. For every root $\alpha \in R$ we have a homomorphism $\alpha : H \to K^*$, defined by the formula $hx_\alpha(a)h^{-1} = x_\alpha(\alpha(h)a)$. It is easy to see that for the groups considered, $\operatorname{im}\alpha \supset k^*$ (if the group is not twisted, we put $k = K$) for every $\alpha \in R^+$. Let $H_n = \{h^n | h \in H\}$. Then $\alpha(H_n) \supset k^{*n}$ for every α (here k^{*n} is the set of the nth powers of all elements in k^*). Put $M = \bigcup_{\alpha\in R^+}(\ker\alpha \cap H_n)$, then

$$|M| < \frac{|H_n||R^+|}{|k^{*n}|}.$$

Therefore, if $|k^{*n}| > |R^+|$, then we have an element $h' \in H_n$, $h' \notin M$. Obviously it is a regular element. Since k^* is a cyclic group, we have

$$|k^{*n}| \geq \frac{|k^*|}{n}.$$

Hence we have an appropriate element if $|k^*| > n|R^+|$ or $|k| > n|R^+|+1$. Since $|K| \leq |k|^3$, we have a desired element if $|K| > (n|R^+|+1)^3$. ∎

LEMMA 11: *Let G be a group of type ${}^2A_{2r}$, $r \geq 1$. Suppose $|K| > (2|R^+|n+1)^2$. Then there exists an element $h \in H$ such that h^n is a regular element.*

Proof: We have here $U_\alpha = \langle x_\alpha(a)\rangle$ if α is a long root, and $U_\alpha = \langle x_\alpha(a,b)\rangle$ if α is a short root. Thus we define $\alpha : H \to K^*$, $\tilde{\alpha} : H \to K^*$ in the following way: $\tilde{\alpha} = \alpha$ if α is a long root, and $hx_\alpha(a,b)h^{-1} = x_\alpha(\alpha(h)a, \tilde{\alpha}(h)b)$ if α is a short root. Thus we have $2|R^+|$ homomorphisms α, $\tilde{\alpha} : H \to K^*$, and one can easily see that $\alpha(H)$, $\tilde{\alpha}(H) \supset k^*$ for every $\alpha \in R^+$. For the rest of the proof simply repeat the proof of Lemma 10 replacing $|R^+|$ by $2|R^+|$. ∎

LEMMA 12: *Let G be a proper Chevalley group over an infinite field K, except A_1, B_2, C_r, then for every n there exists an element $h \in H$ such that h^n is a regular element.*

Proof: If K is an algebraic extension of a finite field, our statement follows from Lemma 10. If not, we can find an element $h \in H$ such that $\langle h\rangle$ is dense in $\overline{H}$ [Bo]. Obviously h is a desired element. ∎

Now we can complete the proof of (80): First we can omit any finite number of groups in our considerations (for those we can take as an estimate of their covering numbers, say, their orders). Hence we may assume that $|K|$ is big enough. Let G be a group not of type A_1, B_2, C_r, ${}^2B_2$, ${}^2G_2$, ${}^2F_4$. Let $h \in H$ be an element such that h^n is regular, where $n = 2^{2|R^+|}$ (such an element exists according to Lemmas 10, 11, 12 if K is big enough). Further, let C be a noncentral conjugacy class of G. Then there exists an element $g \in C$ of the form

$$g = u_1 h u_2, \tag{81}$$

where $u_1 \in U^-$, $u_2 \in U$ (see Theorem H). Further, let $u_2 \in U_i$, $u_2 \notin U_{i+1}$, where U_i is the ith member of the central series of U. Then $u_2 \equiv x_{\beta_1} x_{\beta_2} \cdots x_{\beta_s} \bmod U_{i+1}$ for some $x_{\beta_i} \in U_{\beta_i}$. Since G is not of type ${}^2G_2$, by Lemma 9 we get

$$\tilde{h} x_{\beta_1} \tilde{h}^{-1} \equiv x_{\beta_1}^{-1} \bmod U_{i+1}. \tag{82}$$

We have $g_1 = g(\tilde{h}u_2\tilde{h}^{-1})(\tilde{h}g\tilde{h}^{-1})\tilde{h}u_2^{-1}\tilde{h}^{-1} = u_1 h u_2 \tilde{h} u_2 \tilde{h}^{-1} \tilde{h} u_1 \tilde{h}^{-1} h \in C^2$. Now

$$\begin{aligned} g_2 &= (\tilde{h}u_1\tilde{h}^{-1}h)g_1(\tilde{h}u_1\tilde{h}^{-1}h)^{-1} = \tilde{h}u_1\tilde{h}^{-1}hu_1h(u_2\tilde{h}u_2\tilde{h}^{-1}) \\ &= (\tilde{h}u_1\tilde{h}^{-1}hu_1h^{-1})h^2(u_2\tilde{h}u_2\tilde{h}^{-1}) \in C^2. \end{aligned}$$

According to (82), $u_2\tilde{h}u_2\tilde{h}^{-1} \equiv x'_{\beta_2}x'_{\beta_3}\cdots x'_{\beta_s} \bmod U_{i+1}$ for some $x'_{\beta_i} \in U_{\beta_i}$. Carrying out this procedure $2|R^+|$ times (recall that in the case ${}^2A_{2r}$ we have two-parameter roots) we can obtain an element $\tilde{g} \in C^n$ ($n = 2^{2|R^+|}$) in the form $g = vh^n$, where $v \in U^-$. Since h^n is a regular element, g is also semisimple and regular. Hence $C^{2n} \supset G\backslash Z(G)$ ([EGI, II, III]) and therefore $C^{4n} = G$.

Since ${}^2B_2$ and ${}^2F_4$ are groups over a field of characteristic 2, we may use the same proof because a 2^ℓ-power of a regular element is also regular in this case.

Let G be a group of type ${}^2G_2$. We assume that K is big enough for H to contain a regular element h. Again we present an element in C in the form (81). We have $g_1 = gu_2gu_2^{-1} = u_1hu_2^2u_1h \in C^2$, $g_2 = u_1hg_1(u_1h)^{-1} = u_1'h^2u_2^2 \in C^2$, $g_3 = gu_2^2g_2u_2^{-2} = u_1hu_2^3u_1'h^2 \in C^3$, $g_4 = (u_1'h^2)g_3(u_1'h^2)^{-1} = u_1''h^3u_2^3 \in C^3$. If $u_2 \in U_i$, then $u_2^3 \in U_{i+1}$ because $\operatorname{char} K = 3$. Since we have here $U_3 = 1$, we obtain in C^{27} an element of the form vh^{27}. Since $\operatorname{char} K = 3$, the element h^{27} is also regular and therefore vh^{27} is regular. Thus $C^{54} \supset {}^2G_2\backslash\{1\}$ and $C^{108} = {}^2G_2$. ∎

References

[ACM] Z. Arad, D. Chillag and G. Moran, *Groups with a small covering number*, in [AH, Chapter 4].

[AFM] Z. Arad, E. Fisman and M. Muzychuk, *Order evaluation of products of subsets in finite groups and its applications I*, Journal of Algebra **182** (1996), 577–603.

[AH] Z. Arad and M. Herzog, *Products of Conjugacy Classes in Groups*, Lecture Notes in Mathematics **1112**, Springer-Verlag, New York, 1985.

[AHS] Z. Arad, M. Herzog and J. Stavi, *Powers and products of conjugacy classes*, in [AH, Chapter 1].

[Bo] A. Borel, *Linear Algebraic Groups*, 2nd enlarged edition, Graduate Texts in Mathematics **126**, Springer-Verlag, New York, 1991.

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

[Car1] R. W. Carter, *Simple Groups of Lie Type*, Wiley, London, 1989.

[Car2] R. W. Carter, *Finite Groups of Lie Type*, Wiley, Chichester, 1993.

[Dv] Y. Dvir, *Covering properties of permutation groups*, in [AH, Chapter 3].

[EGI] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in classical Chevalley groups*, Communications in Algebra **22** (1994), 5935–5950.

[EGII] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in Chevalley groups II: exceptional cases*, Communications in Algebra **23** (1995), 3085–3098.

[EGIII] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in classical Chevalley groups III: twisted groups*, Communications in Algebra **24** (1996), 4447–4475.

[El] E. W. Ellers, *Decomposition of equiaffinities into reflections*, Geometriae Dedicata **6** (1977), 297–304.

[GLS] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Math Surveys and Monographs* **40**, Number 1, American Mathematical Society, Providence, R.I., 1994.

[Go1] N. L. Gordeev, *Products of conjugacy classes in algebraic groups I*, Journal of Algebra **173** (1995), 715–744.

[Go2] N. L. Gordeev, *Products of conjugacy classes in algebraic groups II*, Journal of Algebra **173** (1995), 745–779.

[Kar] S. Karni, *Covering numbers of groups of small order and sporadic groups*, in [AH, Chapter 2].

[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, to appear.

[Lev] A. Lev, *The covering number of the group* $\mathrm{PSL}_n(F)$, Journal of Algebra **182** (1996), 60–84.

[So] A. R. Sourour, *A factorization theorem for matrices.*, Linear and Multilinear Algebra **19** (1986), 141–147.

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

[Va] N. A. Vavilov, *The geometry of long root subgroups in Chevalley groups*, Vestnik Leningradskogo Universiteta Matematika Mekhanika Atronomiya (1988), vyp 1, 8–11, 116; translated in Vestnik Leningrad University Mathematics **21** (1988), 5–10.

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