GROUPS EQUAL TO A PRODUCT OF THREE CONJUGATE SUBGROUPS

JOHN CANNON, MARTINO GARONZI, DAN LEVY, ATTILA MARÓTI,
AND IULIAN I. SIMION

Abstract. Let G be a finite non-solvable group. We prove that there exists a proper subgroup A of G such that G is the product of three conjugates of A, thus replacing an earlier upper bound of 36 with the smallest possible value. The proof relies on an equivalent formulation in terms of double cosets, and uses the following theorem which is of independent interest and wider scope: Any group G with a BN-pair and a finite Weyl group W satisfies $G = (Bn_0B)^2 = BB^{n_0}B$ where n_0 is any preimage of the longest element of W. The proof of the last theorem is formulated in the dioid consisting of all unions of double cosets of B in G. Other results on minimal length product covers of a group by conjugates of a proper subgroup are given.

1. Introduction

This paper continues and expands the study, initiated in [15], of minimal length factorizations of groups in terms of conjugates of a proper subgroup. Here we do not limit the discussion to finite groups and therefore we define $\gamma_{\mathrm{cp}}(G)$, for any group G, to be the minimal integer k such that G is a product of k conjugates of a proper subgroup of G, and $\gamma_{\mathrm{cp}}(G) = \infty$ if no such k exists. Note that any G such that every maximal subgroup of G is normal, has $\gamma_{\mathrm{cp}}(G) = \infty$, so in particular, if G is finite, $\gamma_{\mathrm{cp}}(G) = \infty$ if and only if G is nilpotent. In [15] it was shown that $\gamma_{\mathrm{cp}}(G)$ cannot be bounded by a universal constant in the class of finite solvable non-nilpotent groups while $\gamma_{\mathrm{cp}}(G) \leq 36$ for any finite non-solvable G. In the present paper we prove that $\gamma_{\mathrm{cp}}(G) = 3$ for any finite non-solvable G (Theorem 2 below). Note that for any non-trivial G we have $\gamma_{\mathrm{cp}}(G) \geq 3$.

Once the problem is reduced to the almost simple case, the proof of $\gamma_{\mathrm{cp}}(G) \leq 36$ uses two related ingredients which we would like to recall. The first one is the interpretation of the condition $G = A_1 \cdots A_k$, where A_i is a conjugate of $A < G$ for any $1 \leq i \leq k$, in terms of the right multiplication action of G on $\Omega_A := \{Ax | x \in G\}$ (which induces a right multiplication action of any subgroup of G on Ω_A). The second one is a relation between products of conjugates of A and products of double cosets of A. Our first result can be viewed as an extension of these observations.

Date: January 6, 2015.

2000 *Mathematics Subject Classification.* 20D40, 20E42, 20D05, 20B40.

Key words and phrases. double cosets, triple factorization, BN-pairs, dioid.

A.M. acknowledges the support of an Alexander von Humboldt Fellowship for Experienced Researchers and the support of OTKA K84233.

I.S. acknowledges the support of the Swiss National Science Foundation (project number P2ELP2_148913) as well as the support of the University of Padova by grants CPDR131579/13 and CPDA125818/12 .

We denote $x^{-1}Ax$ by A^x for any $A \leq G$ and $x \in G$, and for any two sets A and B, "A intersects B" is equivalent to $A \cap B \neq \phi$.

Theorem 1. *Let G be a group and $A \leq G$.*

1. Let $x, y \in G$. Then $G = AA^xA^y$ implies $y \in AA^x$. Moreover, assuming that $y \in AA^x$, the following three conditions are equivalent:

(a) $G = AA^xA^y$.

(b) $G = (AzA)(AwA)$ where $z = x^{-1}$ and $w = xy^{-1}$.

(c) $G = AA^xA = \left(Ax^{-1}A\right)(AxA)$.

2. Let $x \in G$ then:

(i) $G = AA^xA$ if and only if Ox intersects every orbit of the action of A on Ω_A, where O is the unique A-orbit satisfying $Ax^{-1} \in O$. Furthermore, Ox intersects every orbit of the action of A on Ω_A if and only if Oz intersects every orbit of the action of A on Ω_A, where $z \in AxA$ is arbitrary.

(ii) $G = (AxA)^2 \Longleftrightarrow G = AA^xA^{x^2}$.

Theorem 2. *Let G be a finite non-solvable group. Then there exists $A < G$ and $x \in G$ such that $G = (AxA)^2$. In particular $\gamma_{cp}(G) = 3$.*

Remark 1. *We do not know if for a general group G the existence of $z, w \in G$ such that $G = (AzA)(AwA)$ implies the existence of $x \in G$ such that $G = (AxA)^2$, or even if the seemingly weaker implication which states that $\gamma_{cp}(G) = 3$ implies the existence of $A < G$ and $x \in G$ such that $G = (AxA)^2$, is true.*

Corollary 1. *Any finite group which is not a cyclic p-group has a factorization of the form $G = ABA$, where A and B are proper subgroups of G.*

A major part of the proof of Theorem 2 relies on the next theorem, which is, however, of wider scope and interest. We recall that a group G is said to be a group with a BN-pair ([11], Section 2.1) if there exist subgroups B and N of G such that: (i) $G = \langle B, N\rangle$; (ii) $H := B \cap N \trianglelefteq N$; (iii) $W := N/H$ (the Weyl group of the BN-pair) is generated by a set of elements s_i, $i \in I$, where I is some indexing set, and $s_i^2 = 1$ for all $i \in I$; (iv) For any $n_i \in N$ such that $s_i = n_iH$, it holds that $n_iBn_i \neq B$; (v) $n_iBn \subseteq Bn_inB \cup BnB$ for all $n \in N$ and $n_i \in N$ such that $s_i = n_iH$. By assumption, any element of W can be written as a product of some of the s_i. We define the length function $l : W \to \mathbb{N}_0$ ([11], Section 2.1), by the conditions $l(1_W) = 0$ and for any $1_W \neq w \in W$, the positive integer $l(w)$ is the minimal length of an expression for w as a product of the s_i. If W is finite there exists a (unique) element $w_0 \in W$ such that $l(w_0) > l(w)$ for all $w \in W$, $w \neq w_0$ ([11], Proposition 2.2.11).

Theorem 3. *Let G be a group with a BN-pair and a finite Weyl group. Let $n_0 \in N$ be such that $n_0H = w_0$. Then $G = (Bn_0B)^2 = BB^{n_0}B$.*

Remark 2. *If W is infinite then G is not equal to any (finite) product of double cosets of B.*

Corollary 2. *Let G be a group with a BN-pair and a finite Weyl group W. Let $U \leq B$ satisfy $B = UH$. Then $G = HUU^{n_0}U$.*

Note that in particular, Corollary 2 applies to any group with a split BN-pair ([11], Section 2.5). For the origin, applications and discussion of necessary and sufficient conditions for the identity $G = HUU^{n_0}U$ in the context of Chevalley groups, we refer the reader to [30].

In the case of simple groups of Lie type, the proof of Theorem 3 can be obtained from [20] where the structure constants of Iwahori-Hecke algebras are described. The starting point for the characterization of these constants is [4], which describes the product of double cosets for Borel subgroups in the context of connected reductive linear algebraic groups. Although in proving Theorem 2 we do make use of the Hecke algebra approach which represents double cosets by group algebra sums, and then computes the structure constants, the proof of Theorem 3 takes advantage of the fact that one only needs to distinguish between zero and non-zero structure constants. This leads us to consider another algebraic structure, which we call the DC dioid, to handle double cosets. Both approaches are introduced and discussed in Section 2.

A special case of Theorem 3 is the case where G is a connected reductive linear algebraic group (see for example [[25], Theorem 11.16]). In this case one can offer a different proof which is based on a topological argument. This argument is applicable to any group G such that G is a topological space, and right and left multiplications by fixed elements of G are continuous maps (such a group is customarily called a semi-topological group). The core of the argument relies on standard topological considerations, and it is clear and easy to grasp, so we hope it can be applied for other groups as well.

Proposition 1. *Let G be a semi-topological group. If A is an open dense subset of G then $G = AA^{-1}$. In particular, if $A = A^{-1}$ then $G = A^2$.*

Corollary 3. *Let G be a connected reductive linear algebraic group, B a Borel subgroup of G, and n_0 as in Theorem 3. Then, since Bn_0B is open and dense in G, $G = (Bn_0B)^2$.*

Returning to the setting of Theorem 3, let G be a group with BN-pair and finite Weyl group W. For any subset $I' \subseteq I$, the standard parabolic subgroup $W_{I'}$ of W is defined by $W_{I'} := \langle s_i | i \in I' \rangle$. There is a bijection ([10], Section 8.3) between overgroups of B (the standard parabolic subgroups of G w.r.t B and N) and standard parabolic subgroups of W given by $W_{I'} \longleftrightarrow BW_{I'}B$ (here $W_{I'}$ is regarded as a union of left cosets of H in N). Furthermore, since any standard parabolic subgroup P of G contains B, it is immediate from Theorem 3 that $G = PP^{n_0}P$. Since W is a finite Coxeter group (see [11] Chapter 2) it is natural to consider the question of which irreducible finite Coxeter groups (the terminology is explained in Section 6) are equal to a product of three conjugate parabolic subgroups. This is answered by Theorem 4. Note that by the above mentioned bijection between the standard parabolics of W and those of G, to any factorization of W by three conjugates of some $W_{I'}$ there is a naturally corresponding factorization of G (see Remark 3 below).

Theorem 4. *Let C be a finite irreducible Coxeter group. Then C is the product of three conjugates of at least one of its proper parabolic subgroups if C is of one of the following types: A_n, $n \geq 2$, B_n, $n \geq 3$, D_n, $n \geq 4$, H_4, E_6, E_7, E_8. Otherwise, for the remaining types A_1, B_2, F_4, H_3, $I_2\,(m > 4)$, C is not a product of three conjugates of a proper parabolic subgroup.*

Remark 3. *Let G be a group with BN-pair and a finite Weyl group W whose generators are indexed by I. Suppose that W is the product of three conjugates of* *the standard parabolic subgroup $W_{I'}$ where $I' \subseteq I$. Then G is the product of the corresponding three conjugates of the standard parabolic subgroup $P_{I'} = BW_{I'}B$.*

Finally, we mention other recent papers which discuss similar problems to those addressed in the present paper. Liebeck, Nikolov and Shalev ([21]) consider products of conjugate subgroups in finite simple groups. They conjecture that there exists a universal constant c such that for every non-trivial subgroup A of a simple group G, the minimal number of conjugates of A such that the setwise product of these conjugates is G, is bounded above by $c \log |G| / \log |A|$. Later, in [22], they extend this conjecture to subsets of G of size at least 2. For a discussion of triple factorizations of the form $G = ABA$ for $A, B < G$, see [1] and [2] and the references therein. Liebeck and Pyber have proved ([24] Theorem D) that every finite simple group of Lie type is a product of no more than 25 Sylow p-subgroups, where p is the defining characteristic. In [3] it is claimed, without proof, that the 25 can be replaced by 5, while a sketch of a proof of this claim for exceptional Lie type groups appears in a survey by Pyber and Szabó ([28] Theorem 15). For (non-twisted) Chevalley groups the best possible bound of 4 is shown to hold by Smolensky, Sury and Vavilov in [29].

2. Products of Double Cosets

In this section we prove Theorem 1 and describe two algebraic frameworks for discussing products of double cosets.

Let G be any group and $A \leq G$. Recall that the set of all double cosets of A in G forms a partition of G and $AxA = Ax'A$ if and only if $x' \in AxA$. By a product of two double cosets of A we mean their setwise product, and $(AzA)(AwA)$ is equal to a disjoint union of some double cosets of A.

The following lemma is needed for the proof of Theorem 1 and, in fact, gives a more general version of part of its claims.

Lemma 1. *Let G be a group, $A \leq G$ and $A_1, A_2, \ldots, A_k$ are $k \geq 3$ conjugates of A in G. Then $G = A_1 A_2 \cdots A_k$ if and only if $G = (Ax_1A)(Ax_2A) \cdots (Ax_{k-1}A)$ for some $x_1, \ldots, x_{k-1} \in G$.*

Proof. 1. Suppose that $G = (Ax_1A)(Ax_2A) \cdots (Ax_{k-1}A)$ for some $x_1, \ldots, x_{k-1} \in G$. Then

$$\begin{aligned} G &= (Ax_1A)(Ax_2A) \cdots (Ax_{k-1}A) = Ax_1Ax_2A \cdots Ax_{k-1}A = \\ &= AA^{x_1^{-1}} A^{(x_1x_2)^{-1}} \cdots A^{(x_1x_2\cdots x_{k-2})^{-1}} A^{(x_1x_2\cdots x_{k-1})^{-1}} x_1x_2 \cdots x_{k-1}, \end{aligned}$$

and multiplying both sides on the right by $(x_1x_2 \cdots x_{k-1})^{-1}$, gives

$$G = AA^{x_1^{-1}} A^{(x_1x_2)^{-1}} \cdots A^{(x_1x_2\cdots x_{k-2})^{-1}} A^{(x_1x_2\cdots x_{k-1})^{-1}}.$$

2. Suppose that $G = A_1 A_2 \cdots A_k$ where each A_i is a conjugate of A in G and $k \geq 3$. Let $g_i \in G$, $1 \leq i \leq k$ be such that $A_i = A^{g_i}$. Then:

$$G = A_1 A_2 \cdots A_k = \left(g_1^{-1} A g_1\right)\left(g_2^{-1} A g_2\right) g_3^{-1} A \cdots g_{k-1}\left(g_k^{-1} A g_k\right).$$

Multiplying by g_1 on the left and g_k^{-1} on the right, gives:

$$\begin{aligned} G &= Ag_1g_2^{-1}Ag_2g_3^{-1}A \cdots g_{k-1}g_k^{-1}A = Ag_1g_2^{-1}AAg_2g_3^{-1}AA \cdots AAg_{k-1}g_k^{-1}A = \\ &= \left(Ag_1g_2^{-1}A\right)\left(Ag_2g_3^{-1}A\right) \cdots \left(Ag_{k-1}g_k^{-1}A\right). \end{aligned}$$

□

Proof of Theorem 1. 1. First we show that (a) $\Longrightarrow$ (b) independent of the assumption $y \in AA^x$: Take $k = 3$ in Lemma 1, and in part (2) of its proof, $A_1 = A$, $g_1 = 1$, $g_2 = x$ and $g_3 = y$. We get (b) for $z = x^{-1}$ and $w = xy^{-1}$. Now let z, w be any two elements of G such that $G = (AzA)(AwA)$. Then, in particular, $1_G \in (AzA)(AwA)$, from which it follows that there exist $a_1, a_2 \in A$ such that $(a_1wa_2)^{-1} = a_2^{-1}w^{-1}a_1^{-1} \in AzA$. It follows that $w^{-1} \in AzA$, and so there exist $a_3, a_4 \in A$ such that $w^{-1} = a_3za_4$. Therefore, since (a) $\Longrightarrow$ (b), we get that (a) implies $yx^{-1} = a_3x^{-1}a_4$ which is equivalent to $y = a_3x^{-1}a_4x \in AA^x$. Moreover, since (b) implies $w^{-1} \in AzA$ and hence $AwA = Az^{-1}A$, substituting $z = x^{-1}$ in (b) gives (c), so (b) implies (c). Finally we prove (c) $\Longrightarrow$ (a) for any $y \in AA^x$. Assume $G = AA^xA$, and let $y = a_3x^{-1}a_4x$, where $a_3, a_4 \in A$ are arbitrary. Then

$$\begin{aligned} AA^xA^y &= AA^xA^{a_3x^{-1}a_4x} = Ax^{-1}Ax\left(x^{-1}a_4x\right)^{-1}Ax^{-1}a_4x = \\ &= Ax^{-1}AxAx^{-1}a_4x = AA^xA\left(x^{-1}a_4x\right) = G. \end{aligned}$$

2. (i) We have $O = \left(Ax^{-1}\right)A$ and therefore $AA^x = Ox$, and hence, since G is the union of all right cosets of A, the condition $G = (AA^x)A$ is equivalent to $(Ox)A = \Omega_A$. The last equality is equivalent to the statement that Ox intersects every orbit of the action of A on Ω_A, since Ω_A is the union of all of the orbits of A on Ω_A. Finally, if $z \in AxA$ then $z = a_1xa_2$, with $a_1, a_2 \in A$. So $Oz = \left(Ax^{-1}\right)Aa_1xa_2 = \left(Ax^{-1}\right)Axa_2 = (Ox)a_2$, and Ox intersects every orbit of the action of A on Ω_A if and only if $(Ox)a_2$ does.

(ii) First note (by taking inverses) that $G = (AxA)^2 \Longleftrightarrow G = \left(Ax^{-1}A\right)^2$. Now take $k = 3$ and $x_1 = x_2 = x^{-1}$ in the proof of Lemma 1 part 1. Thus $G = (AxA)^2$ implies $G = AA^xA^{x^2}$. Conversely, if $G = AA^xA^{x^2}$, we take $k = 3$, $g_1 = 1$, $g_2 = x$ and $g_3 = x^2$ in the proof part 2 of Lemma 1 and use the above mentioned equivalence to get $G = (AxA)^2$. □

Let G be a group and $A < G$. We discuss two possible algebraic frameworks to deal with products of double cosets of A. Fix a set $J \subseteq G$ of representatives of distinct double cosets of A in G.

2.1. **The Hecke algebra of double cosets.** For the first algebraic framework, it is sufficient, for our purpose, to assume that G is finite. Let $\mathbb{Q}$ be the field of rational numbers and $\mathbb{Q}[G]$ the group algebra of G over $\mathbb{Q}$. For any subset $S \subseteq G$ define $\underline{S} \in \mathbb{Q}[G]$ by $\underline{S} := \sum_{g \in S} g$. The set $\left\{e_j := \frac{1}{|A|}\underline{AjA} | j \in J\right\}$ is linearly independent in $\mathbb{Q}[G]$, and its elements satisfy the product rule $e_xe_y = \sum_{j \in J} a_{xyj}e_j$, where the structure constants a_{xyj} (also called *intersection numbers*) are nonnegative integers. The span of the set $\left\{e_j := \frac{1}{|A|}\underline{AjA} | j \in J\right\}$ in $\mathbb{Q}[G]$ is the Hecke algebra of the double cosets of A - see [18] Chapter 1, Section 11D. The advantage in representing the double cosets as group algebra sums lies in its relation to the action of G on Ω_A. This relation gives a highly non-trivial algorithm to compute the a_{xyj} from the permutation character 1_A^G associated with the action of G on Ω_A, viewed as a complex character - see [9] Chapters 2 and 3 for some general background and [8], [26] for the details of the specific algorithm we later use in Section 5. This algorithm requires the additional assumption that the character 1_A^G is multiplicity free. Since we are assuming that G is finite, the number $r := |J|$ of distinct double cosets of A

is a natural number that is equal to the rank of the permutation representation of G on Ω_A (see Exercise 3.2.27 of [13]). It is customary to view the a_{xyj} as defining r square nonnegative integer $r \times r$ matrices called the *collapsed adjacency matrices*, via $(P_y)_{xj} = a_{xyj}$. Typically, the rank of the given permutation representation is much smaller than its degree $|G : A|$, and this explains why the above mentioned algorithm is capable of computing the collapsed adjacency matrices even for the larger sporadic groups and some of their subgroups. Note that for a given G and A and $x, y \in J$, the condition $G = (AxA)(AyA)$ is equivalent to the condition $(P_y)_{xj} \neq 0$ for all $j \in J$, namely, that the row labeled by x in the matrix labeled by y consists entirely of non-zero entries.

2.2. **The dioid of double cosets.** Our second approach to products of double cosets of A in G (here G can be any group, not necessarily finite) utilizes the following algebraic structure.

Definition 1. *A quintuple $(R, +, \cdot, 0, 1)$ where R is a set and $+$ and $\cdot$ are two binary operations over R, called respectively addition and multiplication, is a* semiring *if the following axioms are satisfied:*

(a) $(R, +, 0)$ is a commutative monoid with an identity element 0.

(b) $(R, \cdot, 1)$ is a monoid with an identity element 1.

(c) Multiplication is right and left distributive over addition.

(d) Multiplication by 0 annihilates R, that is $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

A starred semiring *is a semiring equipped with an additional unary operation denoted by $*$ (no axioms are imposed in the general case). A semiring in which addition is idempotent, namely, $a + a = a$ for all $a \in R$, is called an* idempotent semiring *or a* dioid *([17]). Note that every dioid is equipped with a "ready made" partial order relation defined by $a \leq b$ if and only if $a + b = b$. A* complete semiring *is a semiring with an infinitary sum operation, namely, $\sum_{i \in I} a_i$ is defined for any indexing set I with $a_i \in R$ for every $i \in I$. An infinitary sum reduces to an ordinary finite sum when I is finite and behaves in a natural way with respect to partitions of I. Moreover, it is required to satisfy the left and right distributive laws: $a \cdot \left(\sum_{i \in I} a_i \right) = \sum_{i \in I} (a \cdot a_i)$ and $\left(\sum_{i \in I} a_i \right) \cdot a = \sum_{i \in I} (a_i \cdot a)$ for any $a \in R$.*

One can easily check that the set D of all unions of double cosets of A in G together with the empty set is a starred, idempotent, complete semiring under the following: addition is the operation of set union, multiplication is the setwise product, 0 is the empty set (we define the product of the empty set with any subset of G to be the empty set), 1 is the trivial double coset $A1_GA = A$ and the star operation maps each non-empty $S \in D$ to its inverse $S^{-1} := \left\{ s^{-1} | s \in S \right\}$ and $\emptyset$ to $\emptyset$. We shall call this structure the *DC dioid* associated with G and A. Note that the natural partial order relation defined above for a general dioid amounts in the case of the DC dioid to set inclusion. Also note that the star operation is involutive, that it is an isomorphism of the additive substructure and an anti-isomorphism of the multiplicative substructure, and that $aa^* = 1 + \ldots$ for all $\emptyset \neq a \in D$. In Section 3, when computing in the DC dioid, we will use $\cup$, $\subseteq$ and $^{-1}$ for, respectively, $+$, $\leq$ and *.

We set $d_j := AjA$, for any $j \in J$. Any element of the DC dioid can then be written as an infinitary sum $\sum_{j \in J} c_j d_j$, where for each $j \in J$, c_j is either 0 or 1

$(0, 1 \in D)$. In particular $G = \sum_{j \in J} d_j$, and the product of any two double cosets defines the structure constants $c_{xyj} \in \{0, 1\} \subseteq D$ via $d_x d_y = \sum_{j \in J} c_{xyj} d_j$. Hence, in this framework, the existence of two double cosets of G whose product equals G is equivalent to the existence of $x, y \in J$ such that $d_x d_y = G$, which is equivalent to $c_{xyj} = 1$ for all $j \in J$.

Finally observe the easy connection between the two approaches (in case of G finite): $c_{xyj} = 1$ if and only if $a_{xyj} \neq 0$.

3. Groups with a BN-pair

Throughout this section G is a fixed group with a fixed BN-pair and the associated Weyl group W. Recall that W is generated by a set of involutions $\{s_i | i \in I\}$. We work in the DC dioid defined by the double cosets of B in G (see Section 2). By Proposition 2.1.2 of [11] there is a bijective map between the set of all double cosets of B in G and the set of all elements of W. Thus we can choose the set J (see Section 2) of distinct B-double cosets representatives as a subset of N, in the form $J = \{n_w \in N | n_w H = w, w \in W\}$, where $H = B \cap N$ and $|J| = |W|$. The specific choices of the n_w do not matter since the double cosets of B are uniquely labeled by the Weyl group elements. Hence, to simplify the notation, we write d_w for the double coset $d_{n_w} := B n_w B$. Observe that $d_w^{-1} = d_{w^{-1}}$ for every $w \in W$ since $(B n_w B)^{-1} = B n_w^{-1} B = B n_{w^{-1}} B$. The following lemma is a basic tool for computing products in the DC dioid, given these settings.

Lemma 2. *For all $w \in W$, and $i \in I$ we have:*

$$d_w d_{s_i} = \begin{cases} d_{ws_i} & \text{if } l(ws_i) = l(w) + 1 \\ d_{ws_i} \cup d_w & \text{if } l(ws_i) = l(w) - 1, \end{cases} \tag{3.1}$$

$$d_{s_i} d_w = \begin{cases} d_{s_i w} & \text{if } l(s_i w) = l(w) + 1 \\ d_{s_i w} \cup d_w & \text{if } l(s_i w) = l(w) - 1. \end{cases} \tag{3.2}$$

Proof. Note that (3.1) is obtained from (3.2) by taking the inverse of both sides of (3.2), and vice versa. Hence it suffices to prove (3.2). If $l(s_i w) = l(w) + 1$ the claim follows from [11], Proposition 2.1.3 (ii).

Now suppose that $l(s_i w) = l(w) - 1$. First we prove the claim for the case $w = s_i$. Denote n_{s_i} by n_i. We have $d_{s_i}^2 = B n_i B n_i B$, and so we have to show that $B n_i B n_i B = B \cup B n_i B$. The l.h.s is contained in the r.h.s, by axiom (v) of the definition of a group with a BN-pair (see Section 1). To prove the reverse inclusion, observe that since $n_i^2 \in B$ we get $B \subseteq B n_i B n_i B$. On the other hand, by the definition of a group with a BN-pair, $n_i B n_i \neq B$ so $B n_i B n_i B \neq B$. Since $B n_i B n_i B \subseteq B \cup B n_i B$, this implies $B n_i B \subseteq B n_i B n_i B$, and altogether $B n_i B n_i B = B \cup B n_i B$, which is equivalent to $d_{s_i} d_{s_i} = d_1 \cup d_{s_i}$.

Now consider a general $w \in W$ of positive length. Using $s_i^2 = 1$ and $l(s_i w) = l(w) - 1$, we get $l(w) = l(s_i(s_i w)) = l(s_i w) + 1$ and by the upper branch of the identity, which is already accounted for, $d_{s_i} d_{s_i w} = d_{s_i^2 w} = d_w$. Multiply the last relation by d_{s_i} on the left. We get:

$$d_{s_i} d_w = (d_{s_i})^2 d_{s_i w} = (d_1 \cup d_{s_i}) d_{s_i w} = d_{s_i w} \cup d_{s_i} d_{s_i w} = d_{s_i w} \cup d_w.$$

□

An expression for $w \in W$ as a product of $l(w)$ generators s_i is called a reduced word for w. Since reduced words are, in general, not unique, we introduce the following formalism in order to make our arguments precise. Let $\mathcal{E}_I$ be the free monoid generated by the letters $\{\varepsilon_i | i \in I\}$. Let ε_0 be the identity of $\mathcal{E}_I$, and define a length function $l : \mathcal{E}_I \to \mathbb{N}_0$ by $l(\varepsilon_0) = 0$, $l(\varepsilon_i) = 1$ for all $i \in I$, and recursively $l(\varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_m}) = l\left(\varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_{m-1}}\right) + l(\varepsilon_{i_m})$ for all $m \geq 2$, where $i_1, \ldots, i_m \in I \cup \{0\}$ (assume $0 \notin I$). We denote both length functions on $\mathcal{E}_I$ and on W by the same letter l. Let $\tau : \mathcal{E}_I \to W$ be the monoid homomorphism defined by $\tau(\varepsilon_0) = 1_W$ and $\tau(\varepsilon_i) = s_i$ for all $i \in I$. We will call $a = \varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_m} \in \mathcal{E}_I$ reduced if $l(a) = l(\tau(a))$. For each $w \in W$ define:

$$Red(w) := \left\{a \in \tau^{-1}(w) \, | a \text{ is reduced}\right\},$$

namely, $Red(w)$ is the set of all reduced expressions for w. Clearly $Red(w) \neq \emptyset$ for any $w \in W$. Finally, recall that if W is finite then w_0 denotes the unique element of maximal length in W.

Lemma 3. *Let $x, y \in \mathcal{E}_I$ be such that x, y and xy are reduced. Then $d_{\tau(xy)} = d_{\tau(x)}d_{\tau(y)}$.*

Proof. By induction on $l(y)$. For $l(y) = 0$ we have $y = \varepsilon_0$ so $xy = x\varepsilon_0 = x$ and $\tau(y) = \tau(\varepsilon_0) = 1_W$. In this case $d_{\tau(xy)} = d_{\tau(x)}$ and $d_{\tau(x)}d_{\tau(y)} = d_{\tau(x)}B = d_{\tau(x)}$ so the claim holds. If $l(y) = 1$ then $y = \varepsilon_i$ with $i \in I$. We have $d_{\tau(x)}d_{\tau(y)} = d_{\tau(x)}d_{s_i}$ and since xy is reduced, $l(xy) = l(\tau(xy)) = l(\tau(x)s_i)$. Since x is reduced, $l(xy) = l(x\varepsilon_i) = l(x) + 1 = l(\tau(x)) + 1$, and so we proved $l(\tau(x)s_i) = l(\tau(x)) + 1$. By Lemma 2 we get $d_{\tau(x)}d_{s_i} = d_{\tau(x)s_i} = d_{\tau(xy)}$.

Now suppose that $l(y) = m > 1$. Thus $y = \varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_m}$ for some $i_1, \ldots, i_m \in I$. Since y is reduced, $l(y) = l(\tau(y))$, and hence $y = \varepsilon_{i_1}y'$, and $l(y') = l(\tau(y')) = m - 1$, so $y' \in \mathcal{E}_I - \{\varepsilon_0\}$ is reduced of length $l(y') = l(y) - 1$. By Lemma 2 we have $d_{\tau(y)} = d_{s_{i_1}}d_{\tau(y')}$. By assumption, $xy = x\varepsilon_{i_1}y'$ is also reduced. Therefore $l(\tau(x\varepsilon_{i_1})) = l(x) + 1$, because, otherwise, $l(\tau(x\varepsilon_{i_1})) < l(x) + 1$ and so $l(\tau(xy)) = l(\tau(x\varepsilon_{i_1})\tau(y')) < l(x) + 1 + l(y) - 1 = l(x) + l(y) = l(xy)$ contradicting the fact the xy is reduced. Now we can use the induction assumption with $x\varepsilon_{i_1}$ in the role of x and y' in the role of y. We get $d_{\tau(xy)} = d_{\tau\left(x\varepsilon_{i_1}y'\right)} = d_{\tau\left(x\varepsilon_{i_1}\right)}d_{\tau(y')}$. Using twice the length 1 case (it works for both orderings) gives $d_{\tau\left(x\varepsilon_{i_1}\right)}d_{\tau(y')} = d_{\tau(x)}d_{s_{i_1}}d_{\tau(y')} = d_{\tau(x)}d_{\tau\left(\varepsilon_{i_1}y'\right)} = d_{\tau(x)}d_{\tau(y)}$. □

Lemma 4. *Assume that W is finite. Let $b \in \mathcal{E}_I$. Then $d_{w_0} \subseteq d_{\tau(b)}d_{w_0}$.*

Proof. By induction on $l(\tau(b))$. If $l(\tau(b)) = 0$ then $d_{\tau(b)}$ is the multiplicative identity of the DC dioid and the claim is clear. If $l(\tau(b)) > 0$ choose a reduced expression $\varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_m} \in Red(b)$, and set $b' = \varepsilon_{i_1}\varepsilon_{i_2}\cdots\varepsilon_{i_{m-1}}$. By Lemma 3 we have $d_{\tau(b)} = d_{\tau(b')}d_{\tau(\varepsilon_{i_m})} = d_{\tau(b')}d_{s_{i_m}}$. Hence $d_{\tau(b)}d_{w_0} = d_{\tau(b')}d_{s_{i_m}}d_{w_0}$. By maximality of $l(w_0)$, we have $l(s_{i_m}w_0) < l(w_0)$, hence, by Lemma 2 (3.2), $d_{w_0} \subseteq d_{s_{i_m}}d_{w_0}$ and so $d_{\tau(b')}d_{w_0} \subseteq d_{\tau(b')}d_{s_{i_m}}d_{w_0} = d_{\tau(b)}d_{w_0}$. Since $l(\tau(b')) = m - 1 < m = l(\tau(b))$ we have by induction $d_{w_0} \subseteq d_{\tau(b')}d_{w_0}$ and the claim follows. □

Lemma 5. *Let $a, b \in \mathcal{E}_I$. Then $d_{\tau(ab)} \subseteq d_{\tau(a)}d_{\tau(b)}$.*

Proof. We have $d_{\tau(a)}d_{\tau(b)} = \left(Bn_{\tau(a)}B\right)\left(Bn_{\tau(b)}B\right) = Bn_{\tau(a)}Bn_{\tau(b)}B$. Since $1_G \in B$ we get $n_{\tau(a)}n_{\tau(b)} \in n_{\tau(a)}Bn_{\tau(b)}$. Hence $n_{\tau(a)}n_{\tau(b)} \in d_{\tau(a)}d_{\tau(b)}$ and $Bn_{\tau(a)}n_{\tau(b)}B \subseteq d_{\tau(a)}d_{\tau(b)}$. Now, τ is a homomorphism, so $\tau(ab) = \tau(a)\tau(b)$, and hence $d_{\tau(ab)} =$

$Bn_{\tau(ab)}B = Bn_{\tau(a)\tau(b)}B$. Now $\left(n_{\tau(a)}H\right)\left(n_{\tau(b)}H\right) = n_{\tau(a)\tau(b)}H$, and since $H \subseteq B$ this implies $Bn_{\tau(a)\tau(b)}B = Bn_{\tau(a)}n_{\tau(b)}B$. Thus $d_{\tau(ab)} = Bn_{\tau(a)}n_{\tau(b)}B$ and the claim follows. □

Note that one can also prove Lemma 4, using Lemma 3 and Lemma 2 (3.2), without explicitly invoking the definition of the d_w.

Proof of Theorem 3. Let $w \in W$ be arbitrary. We will show that $d_w \subseteq d_{w_0}^2$. If $w = 1_W$ we get $d_w = B$ and $d_{w_0}^2 = BB^{n_0}B$ since $w_0^2 = 1$. Since $B \subseteq BB^{n_0}B$ our claim holds for this case and hence we can assume that $l(w) > 0$.

Fix $a \in \mathit{Red}(ww_0)$. Since $w \neq 1$, we have $ww_0 \neq w_0$ and hence $l(ww_0) < l(w_0)$. Hence there exists $b \in \mathcal{E}_I$ such that b is reduced, $l(b) > 0$ and $ab \in \mathit{Red}(w_0)$ (see the first paragraph of the proof of Proposition 2.5.5 of [11] and note that it relies on properties of W that apply for the general case of a group with a BN-pair and a finite Weyl group W). We have $\tau(a) = ww_0$ and hence $\tau(ab) = \tau(a)\tau(b) = ww_0\tau(b)$. On the other hand $ab \in \mathit{Red}(w_0)$ implies that $\tau(ab) = w_0$, so, substituting this in the previous relation, we obtain $w_0 = ww_0\tau(b)$ and hence $\tau(b) = w_0w^{-1}w_0$. Furthermore, $d_{w_0}^2 = d_{w_0}d_{w_0} = d_{\tau(ab)}d_{w_0}$. By Lemma 3, $d_{\tau(ab)} = d_{\tau(a)}d_{\tau(b)}$ and hence we proved $d_{w_0}^2 = d_{\tau(a)}d_{\tau(b)}d_{w_0}$.

By Lemma 4 we have $d_{w_0} \subseteq d_{\tau(b)}d_{w_0}$. Hence $d_{\tau(a)}d_{w_0} \subseteq d_{\tau(a)}d_{\tau(b)}d_{w_0} = d_{w_0}^2$. Now we get from Lemma 5 (taking, in that lemma, $b \in \mathcal{E}_k$ such that $\tau(b) = w_0$) $d_{\tau(a)w_0} \subseteq d_{\tau(a)}d_{w_0}$. However, $a \in \mathit{Red}(ww_0)$, so $\tau(a) = ww_0$, giving $w = \tau(a)w_0$, and so $d_w \subseteq d_{\tau(a)}d_{w_0}$. Combining this with $d_{\tau(a)}d_{w_0} \subseteq d_{w_0}^2$ we obtain $d_w \subseteq d_{w_0}^2$ as desired. □

Proof of Remark 2. An arbitrary product of double cosets of B in G takes the form, in the associated DC dioid, $d_{w_1}\cdots d_{w_m}$ for some $w_1, \ldots, w_m \in W$. For each $1 \leq j \leq m$, choose a reduced expression $w_j = s_{j_1}\cdots s_{j_{l(w_j)}}$. Applying Lemma 3, we get $d_{w_j} = d_{s_{j_1}}\cdots d_{s_{j_{l(w_j)}}}$. Thus, any product of double cosets of B in G, is a finite length product of some d_{s_i} for some $i \in I$ (with possible repetitions). Now, employing Lemma 2, it follows by induction on the number of the d_{s_i} factors in the product, that such a product is a union of a finite number of various d_w with $w \in W$. Since G is equal to the union of the infinite set $\{d_w | w \in W\}$, no product of double cosets of B in G is equal to G. □

Proof of Corollary 2. The claim follows immediately from Theorem 3 upon substituting $B = UH$ in $G = BB^{n_0}B$ and noting that H commutes with both U and n_0. □

4. The topological approach

This section illustrates the topological approach to products of double cosets.

Proof of Proposition 1. Let $g \in G$. We have to prove that $g \in AA^{-1}$. Consider gA. This is an open subset of G, and hence, since A is dense in G, it intersects A, that is $gA \cap A \neq \emptyset$. It follows that there exist $a, a' \in A$ such that $ga' = a$. This is equivalent to $g = a\left(a'\right)^{-1} \in AA^{-1}$. □

Proof of Corollary 3. Observe that a linear algebraic group is a semi-topological group and hence we can apply Proposition 1 with $A = Bn_0B$, provided that we show that $\left(Bn_0B\right)^{-1} = Bn_0B$ and that Bn_0B is an open dense subset of G. The first claim is an immediate consequence of $w_0^2 = 1$ and the second is well known (see [25], proof of Theorem 11.20). □

5. $\gamma_{\text{cp}}(G) = 3$ for a non-solvable finite G

In this section we prove Theorem 2. For any group G we define $\beta_{\text{cp}}(G)$ as the smallest natural number k such that there exist $A < G$ and $x \in G$ for which $G = (AxA)^k$ ($\Longleftrightarrow G = AA^x \cdots A^{x^k}$), and $\beta_{\text{cp}}(G) = \infty$ if no such k exists. Then $\beta_{\text{cp}}(G)$ satisfies the lifting property, namely, for every $N \trianglelefteq G$ we have $\beta_{\text{cp}}(G) \leq \beta_{\text{cp}}(G/N)$ (see Proposition 8 of [15] and note that $(xN)^i = x^i N$). Assume, henceforth, that G is a finite non-solvable group. Following the proof of Theorem 3 of [15], using the same arguments, we reduce to the case where G has a unique minimal normal subgroup N, and N is non-abelian. Thus we can assume the minimal non-solvable setting (see the beginning of Section 3 of [15]). Now one checks that the analysis carried in Section 3 of [15] goes through also for $\beta_{\text{cp}}(G)$ since the restriction that the conjugating elements are successive powers of a given x lifts from subgroups to direct products of subgroups and to normalizers of subgroups. Thus, relying on an analogue of Lemma 14 of [15] for $\beta_{\text{cp}}(G)$, we have the following reduction of the statement $\beta_{\text{cp}}(G) = 2$ for every finite non-solvable group G to almost simple groups.

Claim 1. *$\beta_{cp}(G) = 2$ for every finite non-solvable group G if for any almost simple group X with $S = soc(X)$, there exist $A < S$ and $x \in S$ such that:*
(a) $S = (AxA)^2$ and (b) $N_X(A)S = X$.

Proof. By the discussion preceding the claim we can assume that G satisfies the minimal non-solvable setting of Section 3 of [15]. Hence it is sufficient to show that the existence of $A < S$ with the properties specified in the claim, ensures the existence of $U \leq X$ satisfying all of the assumptions of (the $\beta_{\text{cp}}(G)$ analogue of) Lemma 14 of [15]. Indeed, we set $U := N_X(A)$. Then $US = X$ is just (b). In order to prove that $S = ((U \cap S)\, x\, (U \cap S))^2$ we note that $U \cap S = N_S(A) \geq A$. Using this, the fact that for any $s \in S$ we have $(N_S(A))^s = N_S(A^s)$, and Theorem 1(2)(ii) we get that $S = (AxA)^2 = AA^xA^{x^2}$ implies $S = N_S(A)(N_S(A))^x(N_S(A))^{x^2} = ((N_S(A))\, x\, (N_S(A)))^2 = ((U \cap S)\, x\, (U \cap S))^2$. Finally, $N_S(A) \geq A > 1$ and $N_S(A) < S$ since S is simple and A is proper in S and non-trivial. □

Thus it remains to use the classification of simple non-abelian groups in order to find an appropriate choice of A for any almost simple group X. As a matter of fact, in all cases we find $A < S$, for each simple non-abelian group S, such that this A satisfies (a) and (b) for all almost simple X with $S = soc(X)$.

1. $S \cong Alt(n)$, the alternating group of degree n, and $n \geq 5$. Here we use Corollary 15 of [15]. Note that in all cases there, $A < S$ is a point stabilizer of a 2-transitive action of S on some set. In this case $S = A \cup AxA$ for any $x \in S - A$. Furthermore, one can choose x to be an involution so clearly $A \subseteq (AxA)^2$. On the other hand $(AxA)^2 \neq A$ since $A^x \subseteq (AxA)^2$ and $A \neq A^x$ since A is self normalizing. Thus $S = (AxA)^2$ so condition (a) of Claim 1 holds, while condition (b) is checked in the proof of Corollary 15 of [15].

2. S is a simple group of Lie type. Here we use the fact that all finite simple groups of Lie type are groups with a BN-pair (See [16] Definition 2.2.8, Theorem 2.2.10 and Theorem 2.3.4. The Tits group is not counted in this category). Hence,

by Theorem 3, $S = (Bn_0B)^2$ where B is a Borel subgroup of S and $n_0 \in S$ is any preimage of the longest element of the Weyl group. Thus we take $A = B$ in Claim 1, and this choice satisfies condition (a). It is clear that $B < S$ (see axiom (iv) for groups with a BN-pair). It remains to check that condition (b) of Claim 1 is satisfied, that is, that $N_X(B)S = X$. Let p be the defining characteristic of S. Then, by [16], Theorem 2.6.5 (d) (taking there $J = \emptyset$) we have $B = N_S(P)$ where P is a Sylow p-subgroup of S. Let $x \in X$. Then

$$B^x = N_S(P)^x = N_S(P^x).$$

But P^x is a Sylow p-subgroup of S so by Sylow's theorem there exist $s \in S$ such that $P^x = P^s$ for some $s \in S$. Hence $B^x = N_S(P^s) = N_S(P)^s = B^s$. Thus we have proved that for each $x \in X$ there exists $s \in S$ such that $B^x = B^s$. The last equality is equivalent to $B^{xs^{-1}} = B$ which is equivalent to $xs^{-1} \in N_X(B)$. From here we get $x \in N_X(B)s \subseteq N_X(B)S$ and $N_X(B)S = X$ follows.

3. S is one of the 26 sporadic simple groups or S is the Tits group ${}^2F_4(2)'$. First note that for all of the 27 groups under discussion $|Aut(S) : S| \in \{1, 2\}$. Therefore, for a fixed S, we have two possibilities: (i) $Aut(S) = S$ and then it suffices to find $A < S$ satisfying (a) of Claim 1 or (ii) $|Aut(S) : S| = 2$ in which case it suffices to find a maximal $A < S$ satisfying (a) of Claim 1 and $N_{Aut(S)}(A) \neq A$. Note that $N_{Aut(S)}(A) \neq A$ for A maximal in S ensures that $N_{Aut(S)}(A)$ contains an element of $Aut(S) - S$ and hence $N_{Aut(S)}(A)S = Aut(S)$. Information about maximal subgroups A of the simple groups S in question, satisfying $N_{Aut(S)}(A) \neq A$ is readily available in the ATLAS [12]. The verification of condition (a) for the candidate subgroup was done using GAP [14] and MAGMA [5]. For twenty six out of the twenty seven simple groups under discussion, we have used the GAP package `mfer` ([6], [7]). This package, written by T. Breuer, I. Höhler and J. Müller, contains a database which enables one to compute the collapsed adjacency matrices associated with various multiplicity-free permutation modules arising from actions of the simple sporadic groups. Given these matrices we can use the method explained in the second part of Section 2 in order to look for an appropriate double coset of A where A is a point stabilizer of the action. More precisely, let $A < S$ be a subgroup such that the permutation character 1_A^S is multiplicity-free, and let $P_1, \ldots, P_r$ be the r collapsed adjacency matrices computed by `mfer`. We had run a simple GAP program which loops over $1 \leq i \leq r$, and for each i checks whether all of the entries of the i-th row of P_i are non-zero. As explained in Section 2, the double coset labeled by i squares to G if and only if P_i satisfies this condition. Note that the `mfer` package also allows the computation of collapsed adjacency matrices associated with multiplicity-free permutation modules of groups which appear in GAP's table of marks library (TOM, see [27]). We have used this feature for the Tits group ${}^2F_4(2)'$.

For $S = O'N$ we have $|Aut(S) : S| = 2$, and the `mfer` database does not contain a subgroup A satisfying $N_{Aut(S)}(A) \neq A$. Thus, for $S = O'N$, we cannot use the collapsed adjacency matrices method. Instead, we have verified condition (a) of Claim 1 for $A = J_1$ using a different algorithm, which we implemented in MAGMA. Note that $N_{Aut(S)}(A) \neq A$ (see [12]). This algorithm relies on the possibility to construct representatives $x_1, \ldots, x_r$ of the r distinct A double cosets (a built-in MAGMA function) and on the ability to test, for each $1 \leq i \leq r$, if a given $s \in S$ belongs to the Ax_iA (without computing the full set Ax_iA). This function is not provided by MAGMA and had to be written separately. The main steps of the algorithm are:

1. Calculate a set $\{x_1 = 1, x_2, \dots, x_r\}$ of distinct A-double cosets representatives.

2. For each $2 \leq i \leq r$ check if $x_i^{-1} \in Ax_iA$ - this guarantees $A \subseteq (Ax_iA)^2$ which is necessary for $S = (Ax_iA)^2$.

3. For each double coset AxA, $x \in \{x_2, \dots, x_r\}$, satisfying the necessary condition in 2, check whether $(AxA)^2 = S$ by checking $(AxA)^2 \cap (Ax_jA) \neq \emptyset$ for all $2 \leq j \leq r$ using the following probabilistic function (TRIALS is a predefined positive integer constant): Choose $a \in A$ at random TRIALS times. For each a find the unique $2 \leq j \leq r$ such that $xax \in Ax_jA$ and mark it (clearly $(AxA)^2 \cap (Ax_jA) \neq \emptyset$ if and only if $xax \in Ax_jA$ for some $a \in A$). If all $j \in \{2, \dots, r\}$ are marked after TRIALS trials, then $(AxA)^2 = S$ with certainty. Otherwise, we can only estimate the probability that $(AxA)^2 \neq S$, but this is not needed for our purpose. One should choose TRIALS big enough compared to r, taking into consideration the relative sizes of the non-trivial double cosets.

Table 1 in the appendix summarizes the results of the computations described above by listing pairs (S, A) such that S varies over all of the 26 sporadic simple groups and the Tits group. For each S it displays one choice of $A < S$ that satisfies Claim 1.

Proof of Corollary 1. If G is non-solvable then Theorem 1 and Theorem 2 imply the existence of $A < G$ and $x \in G$ such that $G = AA^xA$. Suppose now that G is a finite solvable group which is not a cyclic p-group. Then $G = NH = NHN$ where N is a maximal normal subgroup and H is any proper subgroup which is not contained in N. For if $H < G$, $H \not\leq N$ then $HN/N \leq G/N$ is non-trivial. But G/N is cyclic of order p by the solvability of G so $HN/N = G/N$ and $G = HN$. If there is no $H < G$, $H \not\leq N$, then any $g \in G - N$ generates G and so G is cyclic. Since G/N is of order p, we can choose g to be a p-element and hence G is a cyclic p-group - a contradiction. □

6. Finite Coxeter Groups and products of conjugate parabolics

Recall that the Weyl group of a finite simple group of Lie type is in particular a finite Coxeter group. A finite Coxeter group C is a finite group with presentation $\langle s_1, \dots, s_n | \, (s_is_j)^{m_{ij}} = 1, \forall 1 \leq i, j \leq n\rangle$ where the positive integers m_{ij} satisfy: (i) $m_{ij} = m_{ji}$, $\forall 1 \leq i, j \leq n$ (ii) $m_{ii} = 1$ for all $1 \leq i \leq n$ (equivalently, each s_i is an involution) (iii) For any $1 \leq i \neq j \leq n$, $m_{ij} \geq 2$ (note that $m_{ij} = 2$ if and only if s_i and s_j commute). The values of the m_{ij} can be encoded in a finite, undirected, simple, edge-labeled graph (the Coxeter graph) on n vertices. The set of vertices is $\{s_1, \dots, s_n\}$. For any $1 \leq i \neq j \leq n$, s_i and s_j are connected by an edge if and only if $m_{ij} \geq 3$. If $m_{ij} = 3$ the edge is left unlabeled, and otherwise it is labeled by m_{ij} (≥ 4). If the Coxeter graph is connected then the corresponding Coxeter group is irreducible (i.e., it is not the direct product of two Coxeter groups). The irreducible finite Coxeter groups were classified by Coxeter (see [19], Section 2.4, Fig. 2.1 which lists all connected Coxeter graphs). If C is a finite Coxeter group with a Coxeter graph Γ then the Coxeter graph of a standard parabolic subgroup of C is obtained from Γ by deleting the vertices (and the edges adjacent to them) corresponding to the s_i that do not belong to the subgroup. The maximal standard parabolic subgroups of C are obtained by deleting just a single s_i. It is clear that for the purpose of proving Theorem 4, it is sufficient to consider only the maximal standard parabolic subgroups of C.

Proof of Theorem 4. 1. C is of type A_n, $n \geq 2$. Then $C \cong S_{n+1}$, is a product of three conjugates of a parabolic subgroup which is isomorphic to S_n - see Section 5, the discussion following the proof of Claim 1. Note that the 2-transitivity argument applies for S_{n+1} with $n \geq 2$.

2. C is of type B_n, $n \geq 3$. In this case $C = V \rtimes S_n$ where

$$V = \{(v_1, \ldots, v_n) \,|v_i \in \{0,1\}\,,\, 1 \leq i \leq n\} \cong Z_2^n$$

is an elementary abelian 2-group of rank n. We realize S_n as S_Ω acting naturally (on the right) on the set $\Omega := \{1, \ldots, n\}$. Then, for any $\pi \in S_\Omega$ and any $v = (v_1, \ldots, v_n) \in V$ we have $\pi^{-1} v \pi = \big(v_{(1)\pi}, \ldots, v_{(n)\pi}\big)$. For each $1 \leq i \leq n$ set $C_i := V_i \rtimes S_{\Omega_i}$, where $\Omega_i := \Omega - \{i\}$ and V_i is the subgroup of V consisting of all n-tuples $(v_1, \ldots, v_n)$ satisfying $v_i = 0$. Note that C_i is a maximal parabolic subgroup of C. Moreover, it is straightforward to check that if $g \in S_\Omega$ satisfies $(1)\,g^{-1} = i$ then $C_1^g = C_i$. Fix $i \in \{2, \ldots, n\}$. We prove that $C = C_1 C_i C_1$. We have $C_1 C_i C_1 = V_1 S_{\Omega_1} V_i S_{\Omega_i} V_1 S_{\Omega_1}$. Let $\pi \in S_{\Omega_1}$ be arbitrary. Then $V_1 \pi V_i = V_1 V_i^{\pi^{-1}} \pi$. Since 1 is fixed by π, we have $V_1 \neq V_i^{\pi^{-1}}$. Hence V_1,$V_i^{\pi^{-1}}$ are two distinct subgroups of V (recall that $V \trianglelefteq C$) of index 2 in V, hence $\left|V_1 V_i^{\pi^{-1}}\right| \geq \frac{|V|^2}{4\frac{|V|}{4}} = |V|$. Therefore $V_1 V_i^{\pi^{-1}} = V$. Since this holds for any $\pi \in S_{\Omega_1}$ we can conclude that $V_1 S_{\Omega_1} V_i S_{\Omega_i} V_1 S_{\Omega_1} = V S_{\Omega_1} S_{\Omega_i} S_{\Omega_1}$. Finally, $S_{\Omega_1} S_{\Omega_i} S_{\Omega_1} = S_\Omega$, by the same argument used for the case $C \cong S_{n+1}$ above.

3. C is of type D_n, $n \geq 4$. In this case $C = U \rtimes S_n$ where U is the subgroup of V consisting of all n-tuples $(v_1, \ldots, v_n)$ satisfying $\sum\limits_{i=1}^{n} v_i \equiv 0 \,(\mathrm{mod}\, 2)$. All the arguments of the previous section carry through if we replace V_i by $U_i := U \cap V_i$. Note that the parabolic subgroup C_1 obtained in this way is isomorphic to the Coxeter group of type D_{n-1} (if $n = 4$ set $D_3 := A_3$).

4. C is of type $I_2\,(m)$, that is, C is a dihedral group Dih_{2m}, $m \geq 3$ an integer (see [19], Section 2.4, Fig. 2.1). Note that $I_2\,(3) = A_2$ is dealt with in part 1. For C of type $I_2\,(4) = B_2$ we get $|C| = 8$ so C is nilpotent and $\gamma_{\mathrm{cp}}\,(C) = \infty$. Finally, consider $C \cong Dih_{2m}$, $m \geq 5$. A maximal parabolic subgroup is generated by a single involution and hence it is of order 2. Since $|C| \geq 10$, we get that C is not a product of three conjugates of a maximal parabolic subgroup.

5. We have checked the remaining Coxeter groups by implementing criterion 2(i) of Theorem 1 in GAP. The functions provided by GAP allow one to compute faithful permutation representations for each C in question, with explicit representations of the s_i. Thus it is possible to compute the maximal parabolic subgroups, and, for each maximal parabolic subgroup to compute its coset space and the orbits of its right multiplication action on its own right cosets. □

Proof of Remark 3. By part 1 of Theorem 1, $W = (W_{I'} z W_{I'})\,(W_{I'} w W_{I'})$ for some $z, w \in W$, where elements of W stand for left cosets of H. Now, $G = BWB$ ([11], Proposition 2.1.1). Hence, substituting the expression for W gives $G = B\,(W_{I'} n_z W_{I'})\,(W_{I'} n_w W_{I'})\,B$, where n_z and n_w are some fixed preimages in N of respectively z and w. In particular we have

$$G \subseteq ((BW_{I'}B)\,n_z\,(BW_{I'}B))\,((BW_{I'}B)\,n_w\,(BW_{I'}B))\,.$$

Applying part 1 of Theorem 1 again, it follows that G is the product of three parabolic subgroups conjugate to $P_{I'} = BW_{I'}B$. □

Appendix

Table 1 lists, for each sporadic simple group S including the Tits group ${}^2F_4\,(2)'$, one choice of a subgroup $A < S$ satisfying the conditions of Claim 1. Note that the subgroups are specified by their isomorphism type, and there may be more than one conjugacy class of subgroups belonging to the same isomorphism type.

S	A	S	A
M_{11}	$A_6.2_3$	$O'N$	J_1
M_{12}	M_{11}	Co_3	$M^cL.2$
J_1	$L_2(11)$	Co_2	$U_6(2).2$
M_{22}	$L_3(4)$	Fi_{22}	$2.U_6(2)$
J_2	$U_3(3)$	HN	A_{12}
M_{23}	M_{22}	Ly	$G_2\,(5)$
${}^2F_4\,(2)'$	$L_2(25)$	Th	${}^3D_4(2).3$
HS	M_{22}	Fi_{23}	$2.Fi_{22}$
J_3	$L_2(16).2$	Co_1	Co_2
M_{24}	M_{23}	J_4	$2^{11} : M_{24}$
M^cL	$U_4\,(3)$	Fi_{24}'	Fi_{23}
He	$S_4(4).2$	B	$2.{}^2E_6(2).2$
Ru	${}^2F_4\,(2)$	M	$2.B$
Suz	$G_2(4)$		

Table 1. Subgroups of simple sporadic groups and the Tits group with a double coset which squares to the group

References

[1] S. H. Alavi and T.C. Burness, "Large subgroups of simple groups", (2014), arXiv:1311.6733.

[2] S. H. Alavi and C. E. Praeger, "On triple factorizations of finite groups", J. Group Theory 14 (2011) (3), 341-360.

[3] L. Babai, N. Nikolov and L. Pyber, "Product Growth and Mixing in Finite Groups", Proceeding SODA '08 Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms p. 248-257.

[4] A. Borel and J. Tits, "Compléments à l'article *Groupes réductifs*" ,Publications Mathématiques de l'Institut des Hautes Études Scientifiques, December 1972, vol 41, Issue 1, pp 253-276.

[5] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system I, the user language", J. Symbolic Comput., 24(3-4):235–265, 1997.

[6] T. Breuer, CTblLib, - GAP's Character Table Library package, version 1.2.1, (2012), http://www.math.rwth-aachen.de/ ˜Thomas.Breuer/ctbllib

[7] T. Breuer and J. Müller, GAP file tst/mferctbl.gap, a compiled database of character tables of endomorphism rings of multplicity-free permutation modules of the sporadic simple groups and their cyclic and bicyclic extensions.

[8] T. Breuer, K. Lux, ”The multiplicity-free permutation characters of the sporadic simple groups and their automorphism groups”, Communications in Algebra, vol 24, number 7, (1996), 2293-2316

[9] P. J. Cameron, Permutation Groups, London Mathematical Society Student Texts 45, Cambridge University Press, (1999).

[10] R. W. Carter, Simple Groups of Lie Type, John Wiley & Sons, (1989).

[11] R. W. Carter, Finite Groups of Lie Type: Conjugacy classes and Complex Characters, John Wiley & Sons, (1985).

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford (1985) (Reprinted with corrections 2003).

[13] J. D. Dixon and B. Mortimer, Permutation Groups, Graduate Texts in Mathematics, Springer (1996).

[14] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.5; 2013. (http://www.gap-system.org)

[15] M. Garonzi and D. Levy, ”Factorizing a finite group into conjugates of a subgroup”, J. Algebra 418 (2014), 129-141.

[16] D. Gorenstein, R. Lyons, and R. Solomon, “The classification of the finite simple groups, Number 3” vol. 40, pp. xvi+419, 1998.

[17] J. Gunawardena, ”An introduction to idempotency”, In Gunawardena, Jeremy. Idempotency. Based on a workshop, Bristol, UK, October 3–7, 1994. Cambridge: Cambridge University Press. pp. 1–49.

[18] C.W.Curtis and I.Reiner, Methods of Representation Theory: With Applications to Finite Groups and Orders, Vol. 1, (Wiley Classics Library) Wiley-Interscience (1990).

[19] J. E. Humphreys, Reflection Groups and Coxeter Groups, Cambridge Studies in Advanced Mathematics (29), Cambridge University Press (1990).

[20] N. Kawanaka, ”Unipotent elements and characters of finite Chevalley groups”, Osaka Journal of Mathematics, vol 12, Number 2 (1975), 523-554.

[21] M.W. Liebeck, N. Nikolov and A. Shalev, ”A conjecture on product decompositions in simple groups”, Groups Geom. Dyn. 4 (2010), 799–812.

[22] M.W. Liebeck, N. Nikolov and A. Shalev, ”Product decompositions in finite simple groups”, Bull. London Math. Soc. (2012) 44 (3): 469-472.

[23] M.W. Liebeck , C.E. Praeger, J. Saxl, ”The maximal factorizations of the finite simple groups and their automorphism groups”, Memoirs of the American Mathematical Society, (1990), vol 86, 1-151.

[24] M.W. Liebeck, L. Pyber: ”Finite linear groups and bounded generation”, Duke Math. J. 107, (2001), 159-171.

[25] G. Malle and D. Testerman, Linear Algebraic Groups and Finite Groups of Lie Type, Cambridge studies in advanced mathematics 133, Cambridge university press, second edition (2012).

[26] J. Müller, ”On the multiplicity-free actions of the sporadic simple groups”, Journal of Algebra 320 (2008) 910–926.

[27] L. Naughton and G. Pfeiffer, GAP Package TomLib 1.2.2, The Library of Tables of Marks.

[28] L. Pyber, E. Szabó, ”Growth in Linear Groups”, (2012), http://arxiv.org/pdf/1208.2538v1.pdf

[29] N. A. Vavilov, A. V. Smolensky, B. Sury, ”Unitriangular Factorizations of Chevalley Groups”, (2011), http://arxiv.org/pdf/1107.5414v1.pdf

[30] N. A. Vavilov, A. V. Smolensky, B. Sury, ”Gauss decomposition for Chevalley groups, revisited”, http://arxiv.org/pdf/arXiv:1109.5254v2.pdf

(John Cannon) Computational Algebra Group, School of Mathematics and Statistics, The University of Sydney, Sydney, NSW 2006, Australia
E-mail address: john@maths.usyd.edu.au

(Martino Garonzi) Department of Mathematics, University of Padova, Via Trieste 63, 35121 Padova, Italy
E-mail address: mgaronzi@gmail.com

(Dan Levy) The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel
E-mail address: danlevy@mta.ac.il

(Attila Maróti) Fachbereich Mathematik, Technische Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany, and Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
E-mail address: maroti@mathematik.uni-kl.de and maroti.attila@renyi.mta.hu

(Iulian I. Simion) Department of Mathematics, University of Padova, Via Trieste 63, 35121 Padova, Italy
E-mail address: iulian.simion@math.unipd.it