www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 4 No. 2 (2015), pp. 69-78.

www.ui.ac.ir

CONJUGATE FACTORIZATIONS OF FINITE GROUPS

MARTINO GARONZI

Communicated by Patrizia Longobardi

Abstract. In this paper we illustrate recent results about factorizations of finite groups into conjugate subgroups. The illustrated results are joint works with John Cannon, Dan Levy, Attila Maróti and Iulian I. Simion.

1. **Introduction**

In this paper we illustrate recent results [4, 5] about factorizations of finite groups into conjugate subgroups. For a group G and $A \leq G$, a conjugate product factorization, or *cp*-factorization, is a factorization $G = A_1, \dots, A_k$ where $A_1, \dots, A_k$ are all conjugate to A and the product is the setwise product.

We define $\gamma_{cp}^A(G)$ to be the smallest number k such that G equals a product $A_1, \cdots, A_k$ of conjugates of A or ∞ if no such k exists. We also set

$$\gamma_{cp}(G) := \min\{\gamma_{cp}^A(G) \ : \ A < G\},$$

where $\min\{\infty\} = \infty$. Observe that $\gamma_{cp}(G)$ is also the minimum of the $\gamma_{cp}^A(G)$ where A ranges in the family of maximal subgroups of G.

We have $\gamma_{cp}^A(G) \geq 3$ if $A < G$ (see Proposition 2.3 (1) below). For finite, non-nilpotent, solvable groups $\gamma_{cp}(G) \leq 4 \log_2 |G|$ ([4, Theorem 5]). Moreover, if p is an odd prime and D_p denotes the dihedral group of degree p (and order $2p$) then $\gamma_{cp}(D_p) = 1 + \lceil \log_2 p \rceil$ ([4, Proposition 23]); this

MSC(2010): Primary: 20F05; Secondary: 05C05.
Keywords: Subgroup Factorizations, Double Cosets, Simple Groups.
Received: 25 February 2015, Accepted: 22 June 2015.
∗ Martino Garonzi.

implies that for solvable groups there is no constant upper bound for $\gamma_{cp}(G)$. In [4] we proved that $\gamma_{cp}(G) \leq 36$ for G any non-solvable group. This was improved in [5] where we proved that $\gamma_{cp}(G) = 3$ whenever G is non-solvable. Actually we proved more: if G is any finite non-solvable group there exist $A < G$ and $x \in G$ such that $G = (AxA)^2$. This has the following consequence: if G is any finite group there exist subgroups A, B of G, conjugated if G is non-solvable, such that $G = ABA$.

These results will be discussed in this paper.

We also mention one result to appear soon in a paper in preparation [6]. Let G be a finite group. There exists a nilpotent subgroup H of G such that G is the product of at most $1 + c(\log_2 |G : H|)(\log_2 \log_2 |G|)^2$ conjugates of H, where $0 < c < 6.721$ is a universal constant.

2. Some properties of conjugate factorizations

Let us state a nice folklore (as far as we know) lemma. The proof is taken from [10], by Ilya Bogdanov.

Lemma 2.1. *Let G be a finite group and let X be a non-empty subset of G. Then $X^{|G|} \leq G$ (here X^n denotes the setwise power $X \cdot X \cdots X$, n times).*

Proof. Consider the powers X, X^2, X^3,... We prove that $|X^i| \leq |X^{i+1}|$ with equality if and only if $|X^i| = |X^{i+1}| = |X^{i+2}| = \cdots$

For $x \in X$ we have $X^i x \subseteq X^{i+1}$ and $|X^i x| = |X^i|$ hence $|X^i| = |X^i x| \leq |X^{i+1}|$. Now suppose $|X^i| = |X^{i+1}|$, and let us prove that $|X^{i+1}| = |X^{i+2}|$. For $x \in X$ we have $X^i x \subseteq X^{i+1}$ and $|X^i x| = |X^i| = |X^{i+1}|$, hence by finiteness $X^i x = X^{i+1}$. Therefore, for any $x, y \in X$ we have $X^i x = X^{i+1} = X^i y$. Now $X^{i+1} x = X X^i x = X X^i y = X^{i+1} y$ for all $x, y \in X$, hence for a fixed $x \in X$ we have $X^{i+2} = X^{i+1} X = \bigcup_{y \in X} X^{i+1} y = \bigcup_{y \in X} X^{i+1} x = X^{i+1} x$ hence $|X^{i+2}| = |X^{i+1} x| = |X^{i+1}|$.

This means that what happens if the following:

$$|X| < |X^2| < |X^3| < \cdots < |X^n| = |X^{n+1}| = |X^{n+2}| = \ldots$$

Observe that $n \leq |X| + (|X^2| - |X|) + \ldots + (|X^n| - |X^{n-1}|) = |X^n| \leq |G|$ hence $|X^{|G|}| = |X^n|$. Since $1 \in X^{|G|}$, $X^{|G|} \subseteq X^{2|G|}$ and from $|X^{|G|}| = |X^n| = |X^{2|G|}|$ we deduce $X^{|G|} = X^{2|G|}$ thus $X^{|G|} \leq G$. □

For $A \leq G$ denote by A^G the normal closure of A in G, i.e. the intersection of the normal subgroups of G containing A. In the following for $g \in G$ the symbol A^g will denote the conjugate $g^{-1} A g$.

Corollary 2.2. *Let A be a subgroup of a finite group G and assume $A^G = G$. Then G is a product of conjugates of A.*

Actually G is the product of the distinct conjugates of A in some order (cf. [7]).

Proof. Define a sequence X_i of subsets of G by $X_1 := A$ and for X_i defined, if there exists $g \in G$ such that $X_i A^g \neq X_i$ set $X_{i+1} = X_i A^g$ otherwise set $X_{i+1} = X_i$. Since $1 \in X_i$ for all i we have $X_i \subseteq X_{i+1}$ for all i. By finiteness of G, the increasing sequence $X_1 \subset X_2 \subset X_3 \subset \ldots$ stabilizes, i.e. there exists n such that $X_n = X_{n+1} = X_{n+2} = \ldots$. Set $X := X_n$. Then X is a normal subset of G because if

$g \in G$ then $XX^g = X$ hence $X^g \subseteq X$ (since $1 \in X$) which implies $X^g = X$ by finiteness. Therefore $\langle X \rangle \trianglelefteq G$. By Lemma 2.1 we have $X^n \leq G$ where $n = |G|$. Since $1 \in X$ we have $X \subseteq X^n$, so also $\langle X \rangle \subseteq X^n$ being $X^n \leq G$. On the other hand clearly $X^n \subseteq \langle X \rangle$ hence $\langle X \rangle = X^n$. But since $A \subseteq X$, $A^G = G$ and $\langle X \rangle \trianglelefteq G$ we obtain $X^n = \langle X \rangle = G$. Since X is a product of conjugates of A so is G. $\square$

Let us list some properties of conjugate factorizations.

Proposition 2.3. *Let G be a group and $H \leq G$.*

1. *G is not the product of two conjugates of H, unless $H = G$.*
2. *Let $N \trianglelefteq G$ and suppose there are elements $x_1, \ldots, x_k \in G$ such that $H^{x_1} \cdots H^{x_k} \supseteq N$. If $HN = G$ then $H^{x_1} \cdots H^{x_k} = G$.*
3. *(Frattini-type argument). Let $N \trianglelefteq G$ and suppose N is a product $A_1 \cdots A_k$ of subgroups $A_i \leq N$, conjugated in N, with the following property: $(*)$ if $g \in G$ and $i \in \{1, \ldots, k\}$ then A_i and A_i^g are conjugated in N. Then $G = N_G(A_1) \cdots N_G(A_k)$.*

Note that property $(*)$ happens for example when the A_i's are Sylow subgroups of N or normalizers in N of Sylow subgroups of N.

Proof.

We prove 1. Suppose G is a product $H^x H^y$ for $x, y \in G$. Then $G = G^{x^{-1}} = (H^x H^y)^{x^{-1}} = HH^{yx^{-1}}$, hence we may assume $x = 1$ and $G = HH^y = Hy^{-1}Hy$. Thus $G = Gy^{-1} = Hy^{-1}Hyy^{-1} = Hy^{-1}H$ and since $1 \in G$ there are $h, k \in H$ with $1 = hy^{-1}k$, so that $y = kh \in H$. This implies that $G = HH^y = HH = H$.

We prove 2. We have $H^{x_k}H^{x_k} = H^{x_k}$ hence

$$H^{x_1} \cdots H^{x_k} = H^{x_1} \cdots H^{x_k} H^{x_k} \supseteq NH^{x_k} = (NH)^{x_k} = G^{x_k} = G.$$

We prove 3. Write $A_i = A_1^{x_i}$ for $x_i \in G$. Let $H := N_G(A_1)$. Then $N_G(A_i) = H^{x_i}$ for all $i = 1, \ldots, k$. Now the result follows from (2) if we show $HN = G$. Let $g \in G$. We prove that $g \in HN$. By assumption there is $n \in N$ with $A_1^g = A_1^n$, i.e. $A_1^{gn^{-1}} = A_1$, in other words $gn^{-1} \in N_G(A_1) = H$. Thus $g \in Hn \subseteq HN$. $\square$

3. **Double cosets**

A double coset of a subgroup A of a group G is a set of the form $AgA = \{agb \ : \ a, b \in A\}$ where $g \in G$. Some easy observations follow.

1. The double cosets of A form a partition of G.
2. If $g, h \in G$ then $AgA = AhA$ if and only if $g \in AhA$, if and only if $h \in AgA$.
3. If A is finite, $|AgA| = |A|^2/|A^g \cap A|$.
4. Any product of double cosets of A is a union of double cosets of A: indeed, $AxA \cdot AyA = AxAyA = \bigcup_{a \in A} AxayA$.

The reason we introduced double cosets is the following:

Proposition 3.1. *Let $A \leq G$. Writing G as product of k conjugates of A is equivalent to writing G as product of $k-1$ double cosets of A.*

Proof. Suppose G is a product $A^{x_1} \cdots A^{x_k}$ with $x_1, \dots, x_k \in G$. Then

$$G = x_1^{-1}Ax_1x_2^{-1}Ax_2 \cdots x_k^{-1}Ax_k = x_1^{-1}(Ax_1x_2^{-1}A)(Ax_2x_3^{-1}A)\cdots(Ax_{k-1}x_k^{-1}A)x_k$$

hence multiplying both sides by x_1 on the left and x_k^{-1} on the right we find

$$G = (Ax_1x_2^{-1}A)(Ax_2x_3^{-1}A)\cdots(Ax_{k-1}x_k^{-1}A).$$

Suppose G is a product $(Ax_1A)\cdots(Ax_{k-1}A)$. Then

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

hence multiplying both sides by $(x_1 \cdots x_{k-1})^{-1}$ on the right we find

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

□

3.1. **Group actions.** Now we give an interesting well-known interpretation of double cosets in terms of group actions. Let G be a permutation group of degree n, i.e. a subgroup of the symmetric group S_n on n letters. G is equipped with the action on $\Omega = \{1, \dots, n\}$ induced by the natural action of S_n. Suppose this action of G is transitive, and let A be a point stabilizer. It is well-known that the given action of G is equivalent to the action of G on $\{Ax \ : \ x \in G\}$ given by $(Ax)g := Axg$ for $g \in G$. This is the way we will think of the action of G from now on.

Since the action of G is transitive there is only one G-orbit, namely Ω. But we now focus our interest on A-orbits. The shape of an A-orbit is as follows:

$$(Ax)A = \{(Ax)a \ : \ a \in A\}.$$

It is visible that it looks like a double coset of A. The formal connection is the following. Let DC be the set of double cosets of A in G and let AO be the set of A-orbits in $\{Ax \ : \ x \in G\}$. Then the following map is a bijection:

$$AO \to DC, \qquad (Ax)A \mapsto AxA.$$

The number of A-orbits is customarily called the rank of the transitive permutation group G and denoted by r.

Recall that groups of rank 2 are also called 2-transitive groups. Examples of 2-transitive groups are the alternating and the symmetric group.

Proposition 3.2. *Let G be a 2-transitive permutation group of degree $n \geq 3$. Then G is the square of a double coset of a point stabilizer. In particular G is a product of three conjugates of a point stabilizer.*

Proof. Since G has rank 2 by the above discussion a point stabilizer A has exactly two double cosets. One of them is the trivial double coset $A1A = A$. We will denote the other by AxA. Since any product of double cosets is a union of double cosets, the square $(AxA)^2$ is a union of double cosets of A. Since A has only two double cosets and they form a partition of G the only possible non-empty unions of double cosets of A are A, AxA and $A \cup AxA = G$. So in order to show that $(AxA)^2 = G$ it is enough to show that $(AxA)^2 \neq A$ and $(AxA)^2 \neq AxA$. Note that the multiplication by x on the right (or on the left) gives an injective map $AxA \to (AxA)^2$ hence $|AxA| \leq |(AxA)^2|$.

If $(AxA)^2 = A$ then $|A| = |(AxA)^2| \geq |AxA| = |A|^2/|A^x \cap A|$ hence $|A| = |A^x \cap A|$, in other words $A^x = A$. But since $AxA = AyA$ for all $y \in G - A$ (because A has only two double cosets) this shows that $A^y = A$ for all $y \in G$, i.e. $A \trianglelefteq G$. But this is false for $n \geq 3$.

If $(AxA)^2 = AxA$ then by induction $(AxA)^k = AxA$ for all $k \geq 1$. Now choose k to be the order of the element x. Then $AxA = (AxA)^k \ni x^k = 1$, thus $AxA = A$, a contradiction. □

4. A connection with conjugacy class factorizations

The main open problem about factorizing with conjugacy classes is Thompson's conjecture stating that any non-abelian finite simple group is the square of one of its conjugacy classes. There is a natural connection between factorizing a group with conjugate subgroups and factorizing a group with conjugacy classes. Specifically, writing a group S as product of conjugacy classes amounts to writing $G := S \times S$ as product of conjugates of $\Delta := \{(s,s) \ : \ s \in S\}$. We explicit this in the language of double cosets (cf. Section 3).

Proposition 4.1. *Let S be a group. Let $G := S \times S$ and $\Delta := \{(s,s) \ : \ s \in S\}$. Let $b_1, \ldots, b_k \in S$. Then in the group $S \times S$ we have*

$$\left(\prod_{i=1}^{k} \Delta(1,b_i)\Delta \right) \cap (\{1\} \times S) = \{1\} \times \left(\prod_{i=1}^{k} {b_i}^S \right)$$

where for $x \in S$, x^S denotes the conjugacy class of x in S.

Proof. We prove $\subseteq$. Let $h \in S$ and assume that $(1,h) \in \prod_{i=1}^{k} \Delta(1,b_i)\Delta$. Then there exist $t_0, t_1, \ldots, t_k \in S$ such that $t_0 \cdots t_k = 1$ and $t_0 b_1 t_1 \cdots b_k t_k = h$.

$$\begin{aligned} h &= t_0 b_1 t_1 \cdots b_k t_k = t_k^{-1} \cdots t_1^{-1} b_1 t_1 \cdots b_k t_k \\ &= t_k^{-1} \cdots t_2^{-1} {b_1}^{t_1} b_2 t_2 \cdots b_k t_k \\ &= t_k^{-1} \cdots t_3^{-1} {b_1}^{t_1 t_2} {b_2}^{t_2} b_3 t_3 \cdots b_k t_k \\ &= \ldots = {b_1}^{t_1 \cdots t_k} {b_2}^{t_2 \cdots t_k} \cdots {b_k}^{t_k}. \end{aligned}$$

We now prove $\supseteq$. Let $h \in \prod_{i=1}^{k} {b_i}^S$. We want to prove that $(1,h) \in \prod_{i=1}^{k} \Delta(1,b_i)\Delta$. There exist $r_1, \ldots, r_k \in S$ such that $h = {b_1}^{r_1} \cdots {b_k}^{r_k}$. We want to find $t_0, \ldots, t_k \in S$ such that

$$(1,h) = (t_0,t_0)(1,b_1)(t_1,t_1)(1,b_2)(t_2,t_2) \cdots (1,b_k)(t_k,t_k),$$

that is, by the reasoning above made,

$$h = {b_1}^{t_1 \cdots t_k} {b_2}^{t_2 \cdots t_k} \cdots {b_k}^{t_k}.$$

Hence it is enough to choose $t_k = r_k$ and $t_i = r_i r_{i+1}^{-1}$ for $i = k-1, \dots, 1$ and $t_0 = t_k^{-1} \cdots t_1^{-1}$. □

Corollary 4.2. *$\prod_{i=1}^k {b_i}^S = S$ if and only if $\prod_{i=1}^k \Delta(1, b_i)\Delta = G$.*

Proof. The implication $\Leftarrow$ follows immediately from the proposition.

Now assume that $\prod_{i=1}^k {b_i}^S = S$. Then by the proposition

$$\left(\prod_{i=1}^k \Delta(1, b_i)\Delta \right) = \Delta \left(\prod_{i=1}^k \Delta(1, b_i)\Delta \right) \supseteq \Delta\left(\{1\} \times S\right) = G.$$

This is actually an application of Proposition 2.3 (2) with $H = \Delta$, $N = \{1\} \times S$. □

In particular if S is a non-abelian simple group then saying that S is a square of one conjugacy class (Thompson's conjecture) is equivalent to saying that $S \times S$ is the square of a double coset of the diagonal subgroup $\Delta = \{(s, s) \ : \ s \in S\}$.

5. Factorizing with few conjugate subgroups

In this section we discuss the invariant $\gamma_{cp}(G)$ and some results about its value.

Proposition 5.1. *Let G be a finite group. Then $\gamma_{cp}(G)$ is finite if and only if G is not nilpotent.*

Proof. Easy consequence of Corollary 2.2 and the fact that a finite group is nilpotent if and only if all of its maximal subgroups are normal. □

5.1. **The dihedral group.** Let us immediately show an example where we can actually compute $\gamma_{cp}(G)$: the dihedral groups.

Let n be a positive integer and let $G = D_n$ be the dihedral group of degree n and order $2n$. It has the following presentation:

$$D_n = \langle a, b \ : \ a^n = 1, \ b^2 = 1, \ bab = a^{-1} \rangle.$$

Proposition 5.2. *$\gamma_{cp}(D_n) = 1 + \lceil \log_2 p \rceil$ where p is the smallest odd prime divisor of n if such prime exists, otherwise $\gamma_{cp}(D_n) = \infty$.*

Proof. D_n is nilpotent if and only if n is a power of 2, so in this case $\gamma_{cp}(D_n) = \infty$. Now assume n is not a power of 2. To compute γ_{cp} of any finite group we can clearly work with maximal subgroups, i.e. we can restrict our interest to conjugate factorizations $A_1 \cdots A_k$ where the A_i's are maximal (i.e. one of them is maximal). Let M be a maximal subgroup of $G = D_n$ and let M_G be its normal core. Then M_G is contained in all the conjugates of M hence we may assume that $M_G = \{1\}$. But then G is a primitive group (in the sense that it has a faithful primitive action, namely the right multiplication action on $\{Mx \ : \ x \in G\}$). It is well-known that the quotients of D_n are dihedral groups. The only primitive non-nilpotent dihedral groups are the dihedral groups of prime degree. Hence we may assume that $n = p$ is an odd prime. In other words, $\gamma_{cp}(D_n)$ equals $\gamma_{cp}(D_p)$ where p is some odd prime divisor of n. Now the conclusion follows from [4, Proposition 23]. $\square$

5.2. **Non-solvable groups.** For the following result (due to Frobenius) see (for a modern treatment) [1] Section 5. Here if H, K are two groups and $K \leq S_n$, $H \wr K$ denotes the wreath product between H and K, i.e. the semidirect product $H^n \rtimes K$ where K acts on H^n permuting the coordinates.

Theorem 5.3 (Embedding Theorem)**.** *Let H be a subgroup of the finite group G, let $x_1, \ldots, x_n$ be a right transversal for H in G and let ξ be any homomorphism with domain H. Then the map $G \to \xi(H) \wr S_n$ given by*

$$x \mapsto (\xi(x_1 x x_{1^\pi}^{-1}), \ldots, \xi(x_n x x_{n^\pi}^{-1}))\pi$$

where $\pi \in S_n$ satisfies $x_i x x_{i^\pi}^{-1} \in H$ for all $i = 1, \ldots, n$ is a well-defined homomorphism with kernel equal to $(\ker \xi)_G$.

Let $\beta(G)$ be the smallest positive integer k such that there exists a proper subgroup A of G and $x \in G$ such that $(AxA)^k = G$ if such k exists, otherwise set $\beta(G) = \infty$. The following is the main result of [5].

Theorem 5.4. *If G is any non-solvable group then G is the square of a double coset of a proper subgroup. In other words $\beta(G) = 2$. In particular $\gamma_{cp}(G) = 3$.*

Proof. (Sketch).
We proceed by induction on $|G|$. By the lifting property $\beta(G) \leq \beta(G/N)$ for all $N \trianglelefteq G$, we may assume that G/N is solvable whenever N is a non-trivial normal subgroup of G. Let N be a minimal normal subgroup of G. Then since G/N is solvable by assumption, N is non-solvable, i.e. N is a non-abelian minimal normal subgroup of G. The centralizer $C_G(N)$ is a normal subgroup of G and $G/C_G(N)$ contains $NC_G(N)/C_G(N) \cong N$ hence $G/C_G(N)$ is non-solvable. By assumption we have then $C_G(N) = \{1\}$. Therefore N is the unique minimal normal subgroup of G (any two distinct minimal normal subgroups centralize each other). It is well-known that N has the form $T^n = T_1 \times \cdots \times T_n$ where $T_1 \cong \ldots \cong T_n \cong T$ and T is a non-abelian simple group.

We apply Theorem 5.3 with $H := N_G(T_1)$ and $\xi : H \to \mathrm{Aut}(T_1)$ the homomorphism given by the conjugation action of H on T_1. We have $\ker \xi = C_G(T_1)$ and

$$(\ker \xi)_G = C_G(T_1) \cap \ldots \cap C_G(T_n) = C_G(N) = \{1\}.$$

Basically this means that we can think of G as embedded in $X \wr S_n$ where $X = N_G(T_1)/C_G(T_1)$ is an almost-simple group with socle $T_1 C_G(T_1)/C_G(T_1) \cong T_1 \cong T$. More precisely, G embeds in $X \wr K$ where $K \leq S_n$ is the image of the composition $G \to X \wr S_n \to S_n$.

The idea is now the following. Suppose for the almost-simple group X with socle T we can find $A < T$ and $x \in T$ such that $(AxA)^2 = T$ and $N_X(A)T = X$. Then a computation shows that the normalizer $N_G(A^n)$ (where $A^n = A \times \cdots \times A \leq T^n$) will play the role of A, in the sense that $(N_G(A^n) \cdot (x,\dots,x) \cdot N_G(A^n))^2 = G$. Indeed using $N_X(A)T = X$ it is easy to show (and well-known) that $N_G(A^n)N = G$ (see [4, Lemma 13]), so by the analogous of Proposition 2.3 (2) it is enough to show that $(N_G(A^n) \cdot (x,\dots,x) \cdot N_G(A^n))^2$ contains N. This is clear because such double coset squared contains $(A^n(x,\dots,x)A^n)^2$ which equals $((AxA)^2)^n = T^n = N$.

The problem is successfully reduced to simple groups. For S a non-abelian simple group we need to find $A < S$ and $x \in S$ with the following two properties:

(1) $(AxA)^2 = S$;
(2) $N_{\mathrm{Aut}(S)}(A)S = \mathrm{Aut}(S)$.

We have already solved the case S an alternating group when we discussed 2-transitive groups (Proposition 3.2). Let us briefly describe the techniques we used for groups of Lie type and sporadic groups.

Let S be a simple group of Lie type. We used the BN-pair structure of S (cf. [2, Chapter 2]), where B is the normalizer of a Sylow p-subgroup of S, p being the defining characteristic. The Weyl group $W = N/B \cap N$ admits a length function and a unique element w_0 of maximal length. Let n_0 be a representative of w_0 in N. In [5] we show that $(Bn_0B)^2 = S$ by using only the BN-pair structure of S. The fact that $N_{\mathrm{Aut}(S)}(B)S = \mathrm{Aut}(S)$ is based on a Frattini-like argument.

To treat sporadic groups let us first introduce some concepts. Let G be a finite group, $A \leq G$, and let J be a fixed set of double coset representatives for A. For any subset S of G define $\underline{S} := \sum_{s \in S} s \subseteq \mathbb{Q}[G]$. The set $\{e_j := \frac{1}{|A|}\underline{AjA} \ : \ j \in J\}$ is linearly independent in $\mathbb{Q}[G]$ and its elements satisfy the product rule

$$e_x e_y = \sum_{j \in J} a_{xyj} e_j$$

where the structure constants a_{xyj} (also called intersection numbers) are non-negative integers. Here is a formula for the structure constants:

$$a_{xyj} = \frac{|AyA \cap Ax^{-1}Aj|}{|A|}.$$

Observe that for $x, y \in J$ saying $(AxA)(AyA) = G$ is equivalent to saying that $a_{xyj} \neq 0$ for all $j \in J$.

The $\mathbb{Q}$-span of $\{e_j \ : \ j \in J\}$ is an example of Hecke algebra.

Let $r = |J|$ be the number of double cosets of A in G. For $y \in J$ define a matrix P_y by setting $(P_y)_{xj} := a_{xyj}$. This gives r matrices, all $r \times r$, called "collapsed adjacency matrices".

Suppose G is a simple sporadic group and A is a maximal subgroup such that the permutation character of G associated to its right multiplication action on $\{Ag \ : \ g \in G\}$ is multiplicity free (i.e. each irreducible complex character of G appears in the decomposition at most once). Müller, Breuer and Höhler [8, 9] have computed the collapsed adjacency matrices of some of these actions and included them in the GAP package mfer. We have used it to find such subgroup A and $x \in J$ such that $G = (AxA)^2$, $N_{\mathrm{Aut}(G)}(A)G = \mathrm{Aut}(G)$.

Only for $G = O'N$, the sporadic O'Nan group, this was not enough. Indeed, all the subgroups A included in the package mfer verify $N_{\mathrm{Aut}(S)}(A) = A$. So we treated this group differently, as follows.

Let $S := O'N$, $X := \mathrm{Aut}(S)$. For this case we needed a MAGMA algorithm. Here is how the algorithm works. Fix a maximal subgroup A of S and let r be the number of double cosets of A.

(1) Calculate a set $\{x_1 = 1, x_2, \dots, x_r\}$ of A-double coset representatives.
(2) For $i = 2, \dots, r$ check if $x_i^{-1} \in Ax_iA$ (so that $A \subseteq (Ax_iA)^2$) (necessary condition).
(3) For each AxA, $x \in \{x_2, \dots, x_r\}$ satisfying (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 (T = TRIALS is a constant).
    - Choose $a \in A$ at random T times and find the unique $2 \leq j \leq r$ such that $xax \in Ax_jA$ (so that $(AxA)^2 \cap Ax_jA \neq \emptyset$) and mark it.
    - If all $j \in \{2, \dots, r\}$ are marked after T trials then $(AxA)^2 = S$ with certainty.

□

Corollary 5.5. *Let G be a finite group which is not a cyclic p-group. There exist proper subgroups A, B of G, conjugated if G is non-solvable, such that $G = ABA$.*

Proof. Suppose first that G is non-solvable. By Theorem 5.4 there exist a proper subgroup A of G and $x \in G$ such that $G = (AxA)^2$. Now since $1 \in G$ there exist $a, b, c, d \in A$ with $axb \cdot cxd = 1$. This implies that $x^{-1} = bcxda$ hence $x^{-1} \in AxA$, in other words $Ax^{-1}A = AxA$. It follows that

$$G = (AxA)^2 = AxA \cdot AxA = Ax^{-1}A \cdot AxA = Ax^{-1}AxA = AA^xA.$$

So we choose $B = A^x$.

Now assume G is solvable. If $|G|$ has only one prime divisor then by hypothesis G is not cyclic, hence it has at least two maximal subgroups A, B. Since G is nilpotent A, B are normal in G hence AB is a subgroup of G containing A and B properly; by maximality of A, B we deduce $G = AB = ABA$. So now assume $|G|$ has more than one prime divisor. Let p be a prime divisor of $|G|$, let A be a Sylow p-subgroup of G and let B be a p'-Hall subgroup of G, where p' denotes the set of all primes different from p. Then clearly $G = AB = ABA$ and A, B are proper subgroups of G because G has more than one prime divisor. □

Acknowledgements

I am grateful to the anonymous referee for his/her very helpful comments on a previous version of this paper.

References

[1] J. Cossey, O. H. Kegel and L. G. Kovács, Maximal Frattini extensions, *Arch. Math. (Basel)*, **35** no. 3 (1980) 210–217.

[2] R. Carter, *Finite Groups of Lie Type*, Conjugacy Classes and Complex Characters, Reprint of the 1985 original, Wiley Classics Library, A Wiley-Interscience Publication, John Wiley Sons, Ltd., Chichester, 1993.

[3] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts 45, Cambridge University Press, Cambridge, 1999.

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

[5] J. Cannon, M. Garonzi, D. Levy, A. Maróti and I. Simion, *Groups equal to a product of three conjugates subgroups*, Preprint.

[6] M. Garonzi, D. Levy, A. Maróti and I. Simion, *Factorizations of finite groups by conjugate subgroups which are solvable or nilpotent*, In preparation.

[7] G. Kaplan and D. Levy, Products of subgroups which are subgroups, *Comm. Algebra*, **35** no. 5 (2007) 1517–1523.

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

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

[10] http://mathoverflow.net/questions/109590/the-powers-of-non-empty-subset-of-a-group-that-generate-a-subgroup

Martino Garonzi

Department of Mathematics, University of Brasília, Brasília, Brazil

Email: `mgaronzi@gmail.com`