

# GROUPS AS SQUARES OF DOUBLE COSETS

Martino Garonzi  
University of Padova

joint work with

John Cannon, Dan Levy, Attila Maróti, Iulian Simion

December 3rd, 2014

Let  $G$  be a group and let  $A \leq G$ . A **double coset** of  $A$  is a set of the form

$$AgA := \{agb : a, b \in A\}$$

where  $g \in G$ .

- 1 Let  $g, h \in G$ .  $AgA = AhA \Leftrightarrow g \in AhA \Leftrightarrow h \in AgA$ .
- 2 The double cosets of  $A$  form a partition of  $G$ .
- 3  $|AgA| = |g^{-1}AgA| = |A^gA| = |A^g||A|/|A^g \cap A| = |A|^2/|A^g \cap A|$ .
- 4 Any product of double cosets of  $A$  is a union of double cosets of  $A$ :  $AgA \cdot AhA = \bigcup_{x \in gAh} AxA$ .
- 5 With the operations of product and union the set of **unions of double cosets** of  $A$  is a ring except for the existence of additive inverses.

We give an interpretation of double cosets in terms of permutation groups.

Let  $G$  be a transitive permutation group of degree  $n$  and let  $A$  be a point stabilizer. We can think of the action of  $G$  as its right multiplication action on  $\Omega = \{Ax : x \in G\}$ . Now consider the induced action of  $A$  on  $\Omega$ . The  $A$ -orbit of  $Ax$  is precisely

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

Let  $\Omega A$  be the set of  $A$ -orbits and let  $DC$  be the set of double cosets of  $A$ . Then we have a bijective correspondence

$$\Omega A \rightarrow DC, (Ax)A \mapsto AxA.$$

In other words, we can identify the double cosets of  $A$  with the  $A$ -orbits of  $\Omega$ . Hence the numbers of double cosets of  $A$  equals the rank of the permutation group  $G$ .

## Rank 2 case.

Assume  $G$  is a permutation group of degree  $n$  and rank 2 (e.g.  $S_n$ ,  $A_n$ ). Let  $A$  be a point stabilizer. Then  $A$  has precisely 2 double cosets,  $A$  and  $AxA$  where  $x$  is any element of  $G - A$ . Since they form a partition,  $G = A \cup AxA$ .

Look at  $(AxA)^2 = (AxA)(AxA)$ . Since it is a union of double cosets, either  $(AxA)^2 = AxA$  or  $(AxA)^2 = G$ . We prove that  $(AxA)^2 = G$ .

If by contradiction  $(AxA)^2 = AxA$  then by induction  $(AxA)^k = AxA$  for all  $k$ . But this is certainly not true for  $k$  the order of  $x$ , since in this case  $(AxA)^k \supseteq A1A = A$ . Here we used that if  $g, h \in G$  then since  $1 \in A$ ,  $(AgA)(AhA) \supseteq AghA$ .

Thus  $(AxA)^2 = G$ .

## The result.

An interesting question arises: is every group the square of a double coset of a proper subgroup?

The answer is no. For instance if  $A$  is normal then  $AxA = Ax$  hence  $(AxA)^k = Ax^k$  and there is no hope that  $(AxA)^2 = G$ . This actually implies that no finite nilpotent group is a product of double cosets of a proper subgroup (in a finite nilpotent group maximal subgroups are normal).

Here is a non-nilpotent example. Consider the dihedral group  $G = D_p$  of degree an odd prime  $p$  and order  $2p$ . Let  $A$  be a proper subgroup of  $G$ .

As we observed to have  $(AxA)^2 = G$  we need  $A$  not to be normal. Hence  $|A| = 2$ , so  $|AxA| = |A^2|/|A^x \cap A| \leq |A|^2 = 4$ , so that  $|(AxA)^2| \leq 4^2 = 16$ . Therefore  $G \neq (AxA)^2$  whenever  $2p > 16$ , i.e.  $p > 8$ .

For  $G$  a group, being a product of double cosets of  $A \leq G$  is equivalent to being a product of conjugates of  $A$ .

- Suppose  $G = (AzA)(AwA)$ . Then  
 $G = AzAAwA = AzAwA = A(zAz^{-1})(zwA(zw)^{-1})zw$  hence  
 $G = A(zAz^{-1})(zwA(zw)^{-1})$ .
- Suppose  $G = A(x^{-1}Ax)(y^{-1}Ay)$ . Then  
 $G = Ax^{-1}Axy^{-1}Ay = (Ax^{-1}A)(Axy^{-1}A)y$  hence  
 $G = (Ax^{-1}A)(Axy^{-1}A)$ .

Write  $A^g$  for  $g^{-1}Ag$ . A remarkable thing to notice is that

$$\text{if } G = AA^xA^y \text{ then } G = AA^xA.$$

Indeed  $G = AA^xA^y = (Ax^{-1}A)(Axy^{-1}A)y$  hence  
 $G = (Ax^{-1}A)(Axy^{-1}A)$  and since  $1 \in G$  this implies  $x \in Axy^{-1}A$  thus  
 $Axy^{-1}A = AxA$  and we conclude that  
 $G = (Ax^{-1}A)(Axy^{-1}A) = (Ax^{-1}A)(AxA) = AA^xA.$

For a group  $G$  let  $\gamma_{cp}(G)$  be the smallest positive integer  $k$  for which there are a proper subgroup  $A$  of  $G$  and  $k$  conjugates of  $A$ ,  $A_1, \dots, A_k$  such that  $G = A_1 \cdots A_k$ . Set  $\gamma_{cp}(G) = \infty$  if this  $k$  does not exist. For the dihedral group  $D_p$  of degree an odd prime  $p$  that we considered above,  $\gamma_{cp}(D_p) = 1 + \lceil \log_2 p \rceil$ .

**THEOREM (J. CANNON, G., D. LEVY, A. MARÓTI, I. SIMION)**

*Any non-solvable group is the square of a double coset of a proper subgroup. In particular if  $G$  is a non-solvable finite group then*

$$\gamma_{cp}(G) = 3.$$

*In particular every finite group  $G$  which is not a cyclic  $p$ -group has a factorization of the form  $ABA$  where  $A, B$  are proper subgroups of  $G$  which can be taken to be conjugated if  $G$  is non-solvable.*

We already proved this (in a previous slide) in case of  $A_n, S_n$  (they are permutation groups of rank 2).

We remark that if  $G$  is any non-nilpotent group and  $A$  is a maximal subgroup of  $G$ ,  $x \in G - A$  then  $(AxA)^k = G$  for some  $k$ . The problem for non-solvable groups is to show that there is some  $A < G$  for which this  $k$  can be taken to be 2.

## Reduction.

As for  $\gamma_{cp}$ , let  $\beta(G)$  be the smallest positive integer  $k$  for which there are a proper subgroup  $A$  of  $G$  and  $x \in G$  with  $(AxA)^k = G$ . Set  $\beta(G) = \infty$  if such  $k$  does not exist. We have the remarkable lifting property

$$\beta(G) \leq \beta(G/N) \text{ for } N \trianglelefteq G.$$

We need to show that  $\beta(G) = 2$  for all non-solvable finite group  $G$ , and for this using the lifting property we may assume that all proper quotients of  $G$  are solvable. In particular,  $G$  admits a minimal normal subgroup  $N$  which is non-abelian.

Consider  $G/C_G(N)$ . Inside here lies  $NC_G(N)/C_G(N) \cong N$  which is minimal normal and non-abelian in  $G/C_G(N)$ , hence using the lifting property we may assume  $C_G(N) = \{1\}$ . Therefore  $N$  is the unique minimal normal subgroup of  $G$ .

We write  $N = T_1 \times \cdots \times T_m$  for  $T_1 \cong \cdots \cong T_n \cong T$  a non-abelian simple group.



For the following result (due to Frobenius) see (for a modern treatment) [2] Section 5.

### THEOREM (EMBEDDING THEOREM)

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

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

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

Recall that in our case  $G$  is a finite group with unique minimal normal subgroup  $N = T_1 \times \dots \times T_m \cong T^m$  for  $T_1 \cong \dots \cong T_m \cong T$  a non-abelian simple group. We take  $H := N_G(T_1)$  and  $\xi : H \rightarrow \text{Aut}(T_1)$  the homomorphism given by the conjugation action. We have  $\ker \xi = C_G(T_1)$  and

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

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  $T_1 \cong T$ . More precisely,  $G$  embeds in  $X \wr K$  where  $K \leq S_n$  is the image of the composition  $G \rightarrow X \wr S_n \rightarrow S_n$ .

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  $N_G(A^n)$  will play the role of  $A$ , in the sense that  $(N_G(A^n) \cdot (x, \dots, x) \cdot N_G(A^n))^2 = G$ .

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  $N_{\text{Aut}(S)}(A)S = \text{Aut}(S)$ .

And we already did this in a previous slide when  $S$  is an alternating group.

## Groups of Lie type.

Let  $G$  be a simple group of Lie type. Then  $G$  admits a BN-pair, that is two subgroups  $B, N$  of  $G$  such that the following hold.

- 1  $G = \langle B, N \rangle$ .
- 2  $H = B \cap N \trianglelefteq N$ .
- 3  $W = N/H$  is generated by  $\{s_i : i \in I\}$  where  $s_i^2 = 1$  for all  $i \in I$ .
- 4 For all  $n_i \in N$  such that  $s_i = n_i H$ ,  $n_i B n_i \neq B$ .
- 5 For all  $n_i \in N$  such that  $s_i = n_i H$ , and for all  $n \in N$ ,  
 $n_i B n \subseteq B n_i n B \cup B n B$ .

$W$  is called the Weyl group of the BN-pair. Its order  $|W|$  equals the number of double cosets of  $B$  in  $G$ . For  $w \in W$  denote  $d_w := BxB$  where  $x \in G$  verifies  $xH = w$ . We will find  $w \in W$  such that  $d_w^2 = d_w d_w = G$ .

Every element  $w \in W$  has the form  $s_{i_1} \cdots s_{i_m}$  for  $i_1, \dots, i_m \in I$ . We define the length of  $w$ ,  $l(w)$ , as the minimal  $m$  for which such an expression exists.

Let  $\mathcal{E}_I$  be the free monoid over  $\{\varepsilon_i : i \in I\}$ . For  $i_1, \dots, i_m \in I$  define  $l(\varepsilon_{i_1} \cdots \varepsilon_{i_m}) := m$ . This defines a length function on  $\mathcal{E}_I$ . Let  $\tau : \mathcal{E}_I \rightarrow W$  be the monoid homomorphism that takes  $\varepsilon_i$  to  $s_i$ . We will say that  $a \in \mathcal{E}_I$  is “a reduced expression for  $\tau(a)$ ” if  $l(a) = l(\tau(a))$ .

We have the following facts (which can be found in Carter’s book [1]).

- 1 (FACT 1) There is a unique element  $w_0 \in W$  of maximal length, and  $w_0^2 = 1$ . (Finiteness of  $W$  needed here).
- 2 (FACT 2) If  $a \in \mathcal{E}_I$  is reduced there exists a reduced  $b \in \mathcal{E}_I$  such that  $ab$  is reduced and  $\tau(ab) = w_0$ .

We argue that

$$d_{w_0} d_{w_0} = G.$$

For  $w \in W$  and  $i \in I$  we have (cf. [1])

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

In particular note that  $d_{w_0} \subseteq d_{w_0} d_{s_i}$  for all  $i \in I$ . This generalizes by induction to show that

(FACT 3) if  $w \in W$  then  $d_{w_0} \subseteq d_{w_0} d_w$ .

Suppose  $a \in \mathcal{E}_I$  is reduced and  $i \in I$ . If  $a\varepsilon_i$  is also reduced then  $l(a) + 1 = l(\tau(a\varepsilon_i)) = l(\tau(a)s_i)$  hence  $d_{\tau(a)} d_{s_i} = d_{\tau(a)s_i}$ . This generalizes by induction to show that

(FACT 4) if  $a, b \in \mathcal{E}_I$  are such that  $a, b$  and  $ab$  are reduced then  $d_{\tau(a)} d_{\tau(b)} = d_{\tau(a)\tau(b)} = d_{\tau(ab)}$ .

- 1 There is a unique element  $w_0 \in W$  of maximal length, and  $w_0^2 = 1$ . (Finiteness of  $W$  needed here).
- 2 If  $a \in \mathcal{E}_I$  is reduced there exists a reduced  $b \in \mathcal{E}_I$  such that  $ab$  is reduced and  $\tau(ab) = w_0$ .
- 3 If  $w \in W$  then  $d_{w_0} \subseteq d_w d_W$ .
- 4 If  $a, b \in \mathcal{E}_I$  are such that  $a, b$  and  $ab$  are reduced then  $d_{\tau(a)} d_{\tau(b)} = d_{\tau(a)\tau(b)} = d_{\tau(ab)}$ .

To show  $d_{w_0} d_{w_0} = G$  we need to show that  $d_w \subseteq d_{w_0} d_{w_0}$  for all  $w \in W$ .

So fix  $w \in W$ . If  $w = 1$  then  $d_w = B$  is contained in  $d_{w_0} d_{w_0}$  because  $w_0^2 = 1$  by (1). Suppose  $w \neq 1$ . Then  $ww_0 \neq w_0$  so  $l(ww_0) < l(w_0)$ . Let  $a \in \mathcal{E}_I$  reduced with  $\tau(a) = ww_0$ . By (2) there is  $b \in \mathcal{E}_I$  reduced with  $\tau(ab) = w_0$  and  $ab$  is reduced. Thus

$$d_{w_0} d_{w_0} = d_{\tau(ab)} d_{w_0} = d_{\tau(a)} d_{\tau(b)} d_{w_0} \supseteq d_{\tau(a)} d_{w_0} \supseteq d_{\tau(a)w_0} = d_w.$$

The first inclusion follows from (3) and the second equality from (4). The second inclusion is simply the fact that  $BxB \cdot ByB$  contains  $BxyB$  being  $1 \in B$ .

## Sporadic groups.

Let  $A \leq G$ , and let  $J$  be a fixed set of double coset representatives for  $A$ . For any subset  $S$  of the group algebra  $\mathbb{Q}[G]$  define  $\underline{S} := \sum_{s \in S} s$ . 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 say that  $a_{xyj} \neq 0$  for all  $j \in J$ .

The  $\mathbb{Q}$ -span of  $\{e_j : j \in J\}$  is a **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. Muller, Breuer and Hohler have computed the collapsed adjacency matrices of some of these actions and included it in the GAP package mfer. We have used it to show that indeed there are such subgroup  $A$  and  $x \in J$  such that  $G = (AxA)^2$ ,  $N_{\text{Aut}(G)}(A)G = \text{Aut}(G)$ .

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  $N_{\text{Aut}(S)}(A) = A$ .



Let  $S := O'N$ ,  $X := \text{Aut}(S)$ . 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 distinct  $A$ -double coset representatives.
- 2 For each  $2 \leq i \leq r$  check if  $x_i^{-1} \in Ax_iA$  (so that  $A \subseteq (Ax_iA)^2$ ) (necessary condition).
- 3 For each  $Ax_iA$ ,  $x \in \{x_2, \dots, x_r\}$  satisfying (2), check whether  $(Ax_iA)^2 = S$  by checking  $(Ax_iA)^2 \cap (Ax_jA) \neq \emptyset$  for all  $2 \leq j \leq r$  using the following probabilistic function ( $T = \text{TRIALS}$  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  $(Ax_iA)^2 \cap Ax_jA \neq \emptyset$ ) and mark it.
  - If all  $j \in \{2, \dots, r\}$  are marked after  $T$  trials then  $(Ax_iA)^2 = S$  with certainty.

-  Carter, Roger; Finite Groups of Lie Type Conjugacy Classes and Complex Characters.
-  Cossey, John; Kegel, O. H.; Kovács, L. G. Maximal Frattini extensions. Arch. Math. (Basel) 35 (1980), no. 3, 210–217.