Commuting conjugacy classes: An application of Hall's Marriage Theorem to Group Theory

John R. Britnell and Mark Wildon

25 October 2008

Abstract

Let G be a finite group. Define a relation $\sim$ on the conjugacy classes of G by setting $C \sim D$ if there are representatives $c \in C$ and $d \in D$ such that $cd = dc$. In the case where G has a normal subgroup H such that G/H is cyclic, two theorems are proved concerning the distribution, between cosets of H, of pairs of conjugacy classes of G related by $\sim$. One of the proofs involves an interesting application of the famous Marriage Theorem of Philip Hall.

The paper concludes by discussing some aspects of these theorems and of the relation $\sim$ in the particular cases of symmetric and general linear groups, and by mentioning an open question related to Frobenius groups.

1   Introduction

Let G be a finite group. Given two conjugacy classes C and D of G, we shall say that C *commutes* with D, and write $C \sim D$, if there exist elements $c \in C$ and $d \in D$ such that c and d commute.

In this paper we are particularly concerned with the case where G has a normal subgroup H such that G/H is cyclic; in this case, since G/H is abelian, each conjugacy class of G is entirely contained within a particular

coset of H. Our main results concern the distribution between the cosets of H of pairs of conjugacy classes of G related by $\sim$.

In order to state our theorems, we make the following definition: a conjugacy class g^G of G is *non-split* if $g^G = g^H$, and *split* otherwise. Observe that g^G is non-split if and only if its centralizer $\mathrm{Cent}_G(g)$ meets every coset of H in G, or equivalently, if and only if g commutes with an element in a generating coset of G/H. In particular, if a coset Ht generates the quotient group G/H, then all of the conjugacy classes in Ht are non-split.

Theorem 1. *Let G be a finite group containing a normal subgroup H such that G/H is cyclic. Let Ht be a generating coset for G/H, and let Hx be any coset. There is a matching between the non-split conjugacy classes in Hx and the conjugacy classes in Ht, such that if C is matched with D, then $C \sim D$.*

Our proof of this theorem, given in §2 below, involves an interesting application of Philip Hall's famous Marriage Theorem.

In the special case where G/H has prime order, Theorem 1 can be strengthened in the following manner.

Theorem 2. *Let G be a finite group containing a normal subgroup H such that G/H is cyclic of prime order p. Let Ht be a generating coset for G/H. The non-split conjugacy classes of G may be partitioned into sets of the form*

$$\{g_0^G, g_1^G, \ldots, g_{p-1}^G\}$$

where $g_m^G \subseteq Ht^m$ and $g_0^G, g_1^G, \ldots, g_{p-1}^G$ all commute with one another.

Theorem 1 implies the purely numerical result that the number of non-split classes in Hx is equal to the number of classes in Ht. Indeed, it can be shown that the number of non-split classes in *any* two cosets are equal; this is a special case of [6, Proposition 9.4][1]. This fact has recently been used by the authors [1], to establish a more general result about the distribution of conjugacy classes of G.

It is not clear whether the assumption in Theorem 1, that Ht is a generating coset, is necessary. The numerical result mentioned in the preceding

---

[1] We thank Tom Wilde for drawing our attention to Isaac's article.

paragraph guarantees that for any two cosets Hx and Hy, there exists a bijection between the non-split classes of Hx and the non-split classes of Hy. We conjecture that a bijection with the matching property of Theorem 1 is always available, but this remains an open question.

It will be apparent to the reader that we believe the commuting relation $\sim$ on conjugacy classes to be of some interest in its own right. In §3 of this paper we look at properties of the relation when G is a symmetric group or a finite general linear group. We also observe that if $|G : H|$ is prime and all of the non-identity classes in H are split, then G is a Frobenius group with kernel H.

2   Proof of Theorems 1 and 2

We first recall Hall's Marriage Theorem in a form suitable for our purposes. Hall's original formulation, and his proof, may be found in [5].

Theorem (Hall's Marriage Theorem). *Suppose that X and Y are finite sets each with k elements, and that a relation $\sim$ is defined between X and Y. It is possible to order the elements of X and Y so that*

$$X = \{x_1, x_2, \ldots, x_k\}$$
$$Y = \{y_1, y_2, \ldots, y_k\}$$

and

$$x_i \sim y_i \quad for\ 1 \leq i \leq k$$

if and only if for every set of r distinct elements of X, the total number of elements of Y which relate to one of these elements is at least r.

In order to apply Hall's Marriage Theorem to prove Theorem 1 we must show (a) that the number of non-split conjugacy classes in Hx is equal to the number of conjugacy classes in Ht, and (b) that given any r distinct non-split classes from Hx, there are at least r conjugacy classes in Ht which commute with one of these given classes. The following double counting argument will establish both of these facts. We shall use the following notation: if X is any subset of G and $g \in G$, then we let $\mathrm{Cent}_X(g) = \mathrm{Cent}_G(g) \cap X$.

Let $C_{i_1}, \ldots, C_{i_r}$ be distinct non-split conjugacy classes in Hx and let $R = C_{i_1} \cup \ldots \cup C_{i_r}$. The total number of conjugacy classes in Ht which commute with one of the classes making up R is

$$s = \sum_{\substack{g \in Ht \\ \mathrm{Cent}_R(g) \neq \varnothing}} \frac{1}{|g^G|} = \frac{1}{|G|} \sum_{\substack{g \in Ht \\ \mathrm{Cent}_R(g) \neq \varnothing}} |\mathrm{Cent}_G(g)|.$$

If $g \in Ht$ then g^G is non-split and $\mathrm{Cent}_G(g)$ meets every coset of H in G. In particular, it meets Hx. Using this to rewrite the second sum gives

$$s = \frac{1}{|H|} \sum_{\substack{g \in Ht \\ \mathrm{Cent}_R(g) \neq \varnothing}} |\mathrm{Cent}_{Hx}(g)|.$$

Now, it is clear that $|\mathrm{Cent}_{Hx}(g)| \geq |\mathrm{Cent}_R(g)|$, and so we can establish a lower bound for s by replacing the condition that $g \in Ht$ with the condition that $g \in R$ in the sum above. This change makes redundant the second condition, that $\mathrm{Cent}_R(g) \neq \varnothing$; so we have

$$s \geq \frac{1}{|H|} \sum_{g \in Ht} |\mathrm{Cent}_R(g)|.$$

The quantity on the right-hand side of the above may instead be found by summing over elements of R. This gives

$$s \geq \frac{1}{|H|} \sum_{k \in R} |\mathrm{Cent}_{Ht}(k)|$$

$$= \frac{1}{|G|} \sum_{k \in R} |\mathrm{Cent}_G(k)| = \sum_{k \in R} \frac{1}{|k^G|} = r,$$

where to pass from the first line to the second, we use the fact that if $k \in R$ then k^G is non-split, and so $\mathrm{Cent}_G(k)$ meets every coset of H. We have shown that $s \geq r$, which establishes (b). Moreover, if R contains every non-split class in Hx, then $\mathrm{Cent}_{Hx}(g) = \mathrm{Cent}_R(g)$ for every $g \in Ht$; hence we have equality at every stage, and (a) follows. This completes the proof of Theorem 1. $\qquad\square$

Remark. It is well known that Hall's Marriage Theorem may be used to

4

prove that if H is a subgroup (not necessarily normal) of a finite group G, then there exists a set of representatives for the left cosets of H which serves also as a set of representatives for the right cosets. This fact can be proved without Hall's Marriage Theorem, or any close equivalent; an elementary proof using double cosets was given by Miller [7] in 1910.[2] It seems likely, by contrast, that the use of the Marriage Theorem in the proof of Theorem 1 is essential.

We now turn to the proof of Theorem 2. To establish the existence of a partition of the collection of non-split conjugacy classes of G, with the properties stated in the theorem, we invoke the following lemma.

Lemma 3. *Let G be a finite group containing a normal subgroup H, and Hx a coset of H. Let c be an integer coprime with $|G|$. The function on G given by $g \mapsto g^c$ induces a bijection between the conjugacy classes in Hx and the conjugacy classes in Hx^c.*

Proof. Since c is coprime with $|G|$, there exists an integer d such that $cd \equiv 1 \bmod |G|$. It follows that the function $g \mapsto g^c$ is invertible, with inverse $g \mapsto g^d$. Moreover, if y and z lie in Hx and y^c and z^c are conjugate, then $y^{cd} = y$ and $z^{cd} = z$ are also conjugate. Hence the function induced on conjugacy classes is bijective. $\qquad\square$

Now suppose that in the matching given by Theorem 1 between the non-split conjugacy classes in H and the conjugacy classes in Ht, the class $h^G \subseteq H$ is paired with $g^G \subseteq Ht$ where h and g commute. For $i = 2, \ldots, p-1$, let c_i be an integer coprime with $|G|$ such that $c_i \equiv i \bmod p$.

The conjugacy classes in the set

$$\left\{ h^G, g^G, (g^{c_2})^G, \ldots, (g^{c_{p-1}})^G \right\}$$

---

[2]Contrary to a folklore belief, it seems improbable that Hall was motivated in [5] by the coset representatives problem, to which we have been unable to find reference in any of his published work. It is likely that Hall was aware of Miller's paper and also of Van der Waerden's paper [11] of 1927. Indeed it is possible that Hall has been confused at some time with Van der Waerden, who establishes a theorem similar to Hall's, and explicitly mentions the problem of coset representatives as his motivation.

lie in distinct cosets of H since the integers c_i together with 0 and 1 form a complete set of residues modulo p. Moreover, the elements h, g and g^{c_i} for $i = 2, \ldots, p-1$ certainly commute with one another. Consider the collection of sets which are obtained in this way. Lemma 3 ensures that distinct sets are disjoint, and it follows easily that they partition the set of non-split classes of G. This completes the proof of Theorem 2. $\qquad\square$

3 Examples

3.1 Symmetric groups

We recall that conjugacy classes of $\mathrm{Sym}(n)$ are parametrized, via their cycle structure, by partitions of n. The classes which lie in $\mathrm{Alt}(n)$ correspond to those partitions for which the number of parts of even size is even. It is a standard result (see, for example, [2, page 65]) that the class C^λ corresponding to the partition λ splits when the conjugacy action is restricted to $\mathrm{Alt}(n)$, if and only if the sizes of the parts of λ are odd and distinct.

Let $\mathcal{P}(n)$ denote the set of all partitions of n. Let $\mathcal{P}_{\mathrm{even}}(n)$ be the subset of partitions with an even number of even parts, $\mathcal{P}_{\mathrm{odd}}(n)$ the subset of partitions with an odd number of even parts, and $\mathcal{D}_{\mathrm{o}}(n)$ the subset of partitions with distinct odd parts. Theorem 1 asserts that there exists an bijection

$$f : \mathcal{P}_{\mathrm{even}}(n) \setminus \mathcal{D}_{\mathrm{o}}(n) \longrightarrow \mathcal{P}_{\mathrm{odd}}(n)$$

such that $C^\lambda \sim C^{f(\lambda)}$ for all $\lambda \in \mathcal{P}_{\mathrm{even}}(n) \setminus \mathcal{D}_{\mathrm{o}}(n)$.

The numerical implication that $|\mathcal{P}_{\mathrm{even}}(n)| = |\mathcal{P}_{\mathrm{odd}}(n)| - |\mathcal{D}_{\mathrm{o}}(n)|$ is well known, but constructing an explicit bijection is by no means trivial. An elegant one is given by Gupta [4], which happens to possess the commuting property in which we are interested.

It is straightforward to describe the commuting relation $\sim$ in terms of the partitions which parametrize the classes of $\mathrm{Sym}(n)$. Given two partitions μ and ν in $\mathcal{P}(n)$, we say that ν is a *coarsening* of μ if ν can be obtained from μ by adding together parts of μ of the same size. For example, $(4, 3^4, 1^2)$ has both $(12, 4, 2)$ and $(6, 4, 3^2, 1^2)$ as coarsenings. The following proposition completely describes $\sim$ for $\mathrm{Sym}(n)$.

Proposition 4. *Let $\lambda, \mu \in \mathcal{P}(n)$. The conjugacy classes C^λ and C^μ commute if and only if there is a partition $\nu \in \mathcal{P}(n)$ which is a coarsening of both λ and μ.* □

Proof. The action of a permutation in C^ν decomposes into orbits whose lengths are the parts of ν; a class C_μ contains an element which acts regularly on each of these orbits if and only if ν is a coarsening of μ.

Suppose that $x \in C^\lambda$ and $y \in C^\mu$ are commuting permutations. For $i, j \leq n$, let w_{ij} be the subset of $\{1, \ldots, n\}$ consisting of elements lying in i-cycles of x and j-cycles of y. We note that w_{ij} is a union of cycles both of x and y. If ν is the partition whose parts are the sizes of the sets w_{ij}, then ν is a coarsening of both λ and μ as required.

Conversely, suppose that ν is a coarsening of λ and μ. Each part k of ν is an amalgamation of parts of λ with size i, say. If $z \in C^\nu$, then $z^{k/i}$ acts regularly on a k-orbit of z, with cycles of length i. Thus we may construct an element x of C^λ which acts as a power of z on each orbit of z. Similarly, we can find an element y of C^μ which acts as a power of z on each orbit of z, and clearly x and y commute. □

It is worth remarking that Proposition 4 is essentially about conjugacy classes, rather than individual permutations. In general it is not the case that if $x, y \in \mathrm{Sym}(n)$ commute then there exists a permutation z, such that x and y act as powers of z on each orbit of z. The double transpositions in $\mathrm{Sym}(4)$ provide a simple counterexample.

3.2 Finite general linear groups[3]

A natural description of conjugacy classes in general linear groups is provided by the theory of rational canonical form; this yields the following combinatorial parametrization: for each conjugacy class of $\mathrm{GL}_d(q)$, a partition λ_f is assigned to each monic irreducible polynomial f over $\mathrm{GF}(q)$ other than $f(t) = t$; the only constraint is that $\sum_f |\lambda_f| \cdot \deg f = d$. If the conjugacy class of an element $M \in \mathrm{GL}_d(q)$ is parametrized with the assignment $\{\lambda_f\}$ then each part a of λ_f corresponds to an elementary divisor f^a

---

[3]Certain facts concerning commuting elements in linear groups are stated here without proof. A paper is in preparation, in which these and other results will be established.

of M. The determinant of M is equal to the product

$$(-1)^d \prod_f f(0)^{|\lambda|},$$

from which it is possible to determine, from the parametrization, in which coset of $\mathrm{SL}_d(q)$ a conjugacy class lies.

The commuting relation $\sim$ on conjugacy classes appears to be very much harder to analyse for linear groups than it is for permutation groups. Working by analogy with Proposition 4, it might be tempting to conjecture that if two classes C_1 and C_2 of $\mathrm{GL}_d(q)$ commute, then there exist elements $Z \in \mathrm{GL}_d(q)$, $X \in C_1$, and $Y \in C_2$, which preserve a common direct sum decomposition, such that X and Y act as polynomials in Z on each summand. However this conjecture would be false; the classes of unipotent elements of $\mathrm{GL}_4(q)$ corresponding to the partitions $(3,1)$ and (2^2) commute, but they have no common proper decomposition, and no cyclic subalgebra of $\mathrm{Mat}_4(q)$ contains elements of both classes.

A conjugacy class with parametrization $\{\lambda_f\}$ splits when the conjugacy action is restricted to $\mathrm{SL}_d(q)$, if and only if it satisfies the condition that some prime divisor of $q-1$ divides all of the parts in all of the partitions λ_f.

Let ξ be a non-zero element of $\mathrm{GF}(q)$ with multiplicative order $q-1$. Theorem 1 establishes that there exists a bijection between the non-split classes in $\mathrm{SL}_d(q)$, and the classes in the coset of $\mathrm{SL}_d(q)$ whose elements have determinant ξ. It is difficult to exhibit such a bijection in general, though it is simple enough to do so in small dimensional cases; we present here the elementary case $d = 2$, in order to give an indication of how such bijections can be constructed. When q is even, the presence of scalar matrices in every coset of $\mathrm{SL}_2(q)$ means that the problem is trivial, and so we assume that q is odd.

In this case there are four distinct types of conjugacy class: (A) scalars; (B) non-semisimple classes of elements with a single eigenvalue; (C) classes of elements with two distinct eigenvalues; (D) eigenvalue-free classes. The parameters for (A) and (B) involve only a single linear polynomial, with the associated partitions being (1^2) and (2) respectively. Classes of type (C) involves two linear polynomials, each with associated partition (1). Classes

of type (D) involve a quadratic polynomial, with the associated partition (1). The split classes, over fields of odd characteristic, are those of type (B).

Let C_ξ be the set of elements of $\mathrm{GL}_2(q)$ with determinant ξ. It is not hard to calculate the number of classes of each of the types (A), (B), (C) and (D) in $\mathrm{SL}_2(q)$ and in C_ξ; the results are presented in the following table.

	(A)	(B)	(C)	(D)
$\mathrm{SL}_2(q)$	2	2	$(q-3)/2$	$(q-1)/2$
C_ξ	0	0	$(q-1)/2$	$(q+1)/2$

A useful fact, which we shall not prove here, is that two classes of the same type contain elements which are polynomial in each other, and hence commute. With this observation, it is easy to present a scheme for a matching between the classes of types (A), (C) and (D) in the two cosets. We simply match up classes within the types (C) and (D) as far as possible; this leaves just one remaining class of each type in the coset C_ξ. Since the two remaining classes in $\mathrm{SL}_2(q)$ contain scalars, the matching can certainly now be completed.

3.3 Groups of prime index with many split classes

In the case that $|G : H|$ is prime, there is an interesting characterization of groups with the property that all of the classes in H, other than the identity class, are split.

Proposition 5. *Let G be a finite group containing a normal subgroup H of prime index p. Every non-identity class of H is split if and only if G is a Frobenius group with kernel H and complement C_p.*

Proof. Suppose that every non-identity class of H is split. If $t \in G \backslash H$ then t does not commute with any non-identity element of H. Since $t^p \in H$, we must have $t^p = 1$, and moreover t must act on H as a fixed-point-free automorphism of order p. It follows that G is a Frobenius group with kernel H and complement $\langle t \rangle$. The converse follows from standard results on Frobenius groups: see for example [3, Ch. 2, Theorem 7.6]. $\square$

A famous theorem of Thompson (see [10, Theorem 1] or [3, Ch. 10, Theorem 2.1]) states that the Frobenius kernel H is nilpotent. It is natural to ask what happens when we weaken the hypothesis of Proposition 5 to require only that every *non-central* class of G is split. At least when $p = 2$, it remains the case that H must be nilpotent (though not necessarily abelian), but we have no general answer to this question at present.

We conclude with the remark that the centre of G can be recognized by means of the commuting relation $\sim$ on conjugacy classes. Suppose that g^G is a conjugacy class which commutes with every other conjugacy class of G. Then clearly the conjugates of $\mathrm{Cent}_G(g)$ cover G. It is a well-known fact (see for example [8, Exercise 237]) that the conjugates of a proper subgroup of G cannot cover G. Hence $\mathrm{Cent}_G(g) = G$, and so the element g is central.

References

[1] J. R. Britnell and M. Wildon. On the distribution of conjugacy classes between the cosets of a finite group in a cyclic extension. *Bull. London Math. Soc.* **40** (2008), 897–906.

[2] W. Fulton and J. Harris. *Representation Theory: A First Course* (Springer, New York, 1991).

[3] D. Gorenstein. *Finite Groups, second edition* (Chelsea Publishing Company, New York, 1980).

[4] H. Gupta. Combinatorial proof of a theorem on partitions into an even or odd number of parts. *J. Combin. Theory Ser. A.* **21** (1976), 100–103.

[5] P. Hall. On representatives of subsets. *J. London Math. Soc.* **10** (1935), 26–30.

[6] I. M. Isaacs. Characters of π-separable groups. *J. Algebra.* **86** (1984), 98–128.

[7] G. A. Miller. On a method due to Galois. *Quart. J. Math.* **41** (1910), 382–384.

[8] J. S. Rose. A Course on Group Theory (Cambridge University Press, Cambridge, 1978).

[9] J. E. Roseblade, Obituary: Philip Hall. *Bull. London Math. Soc.* **16** (1984), 603–626. With contributions by J. G. Thompson and J. A. Green.

[10] J. Thompson. Finite groups with fixed-point-free automorphisms of prime order. *Proc. Nat. Acad. Sci. U.S.A.* **45** (1959), 578–581.

[11] B. L. V. Van der Waerden. Ein Satz über Klasseneinteilungen von endlichen Mengen. *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 185–188.