Maximal non-commuting subsets of groups

Umut Işık

March 29, 2005

Abstract

Given a finite group G, we consider the problem of finding the maximal size $\mathrm{nc}(G)$ of subsets of G that have the property that no two of their elements of commute. After constructing a large non-commuting subset of S_n, we consider the definition and classification of extraspecial p-groups and focus on such a group: $S(p.n)$. We show that $\mathrm{nc}(S(2,n)) = 2n + 1$ and that $S(p,n) \geq pn + 1$.

1 Introduction

There are several ways to consider how abelian a non-abelian finite group G is. One of them is the derived subgroup $[G, G]$, another is the minimal number $\mathrm{a}(G)$ of abelian subgroups required to cover the whole group. Another is the size $\mathrm{nc}(G)$ of the non-commuting subset of G having the largest cardinality. A non-commuting subset of a group has the property that no two of its elements commute under the group operation.

The non-commuting graph $\Gamma(G)$ of a group G is an undirected graph the vertices of which are the elements of G and the edges of which are the ones connecting two non-commuting elements. The problem of finding a maximal non-commuting subset of a group G is the clique problem for $\Gamma(G)$.

$\mathrm{nc}(G)$ and $\mathrm{a}(G)$ are related in the sense that $\mathrm{nc}(G) \leq \mathrm{a}(G)$ since two elements that do not commute cannot be in the same abelian subgroup.

Mason [3] has shown that any finite group G can be covered with at most $\lfloor \frac{|G|}{2} \rfloor + 1$ abelian subgroups, so we also have $nc(G) \leq \lfloor \frac{|G|}{2} \rfloor + 1$, which he also shows separately.

$\mathrm{nc}(G)$ is also related to the index of the center of a group, as Pyber [5] has shown, there is some constant c such that $|G : Z(G)| \leq c^{\mathrm{nc}(G)}$. Which gives that $\mathrm{a}(G) \leq c^{\mathrm{nc}(G)}$. Our argument about an extraspecial 2-group shows that these results are optimal.

In [2] Erdos studies maximal commuting k-tuples of groups. For tuples, the following result is easily established.

Theorem 1 *(Erdos) The number of commuting pairs in a group G is*

$$|G|c(G)$$

where c(g) is the number of conjugacy classes of G.

Proof: Consider the action of G on itself by conjugation, each element $g \in G$ commutes with all the elements in its stabilizer under this action, namely its centralizer $Z_G(g)$. So for each $g \in G$ there are $|Z_G(g)|$ pairs that contain g in the first place. $|Z_G(g')| = |Z_G(g)|$ for all $g' \in Orb(g)$, namely the conjugacy class of g, so there are $|Orb(g)||Z_G(g)| = |G|$ commuting pairs for each conjugacy class. Summing over all conjugacy classes, there are $|G|c(G)$ commuting pairs. □

From this, we obtain the number of non-commuting pairs in a group G to be $|G|(|G| - c(G))$.

2 Maximal non-commuting subsets of the symmetric group

We shall frequently use the fact that every element of S_n can be uniquely decomposed into disjoint cycles. We shall also use the following lemma when dealing with permutations.

Lemma 2 *If $\sigma, \tau \in S_n$, and and σ decomposes into disjoint cycles as:*

$$\sigma = (k_{1,1}\, k_{1,2} \ldots k_{1,s}) \ldots (k_{r,1}\, k_{r,2} \ldots k_{r,s})$$

then

$$\tau\sigma\tau^{-1} = (\tau(k_{1,1})\, \tau(k_{1,2}) \ldots \tau(k_{1,s})) \ldots (\tau(k_{r,1})\, \tau(k_{r,2}) \ldots \tau(k_{r,s})) \qquad (1)$$

Lemma 3 *If $\sigma \in S_n$ contains m_i i-cycles in its disjoint cycle decomposition, then there are*

$$\prod_i m_i! i^{m_i}$$

elements of S_n that commute with σ.

Proof: By Lemma 2, $\tau \in S_n$ commutes with σ if and only if it permutes cycles of the same length in the disjoint cycle decomposition of σ when it acts on σ under conjugation. This gives us the above number of elements that commute with σ because when permuting those cycles, τ can write an i-cycle in i different ways. □

Lemma 4 *Two cycles, $c_1, c_2 \in S_n$ commute if and only if they are disjoint cycles or $c_1 = c_2^r$ for some integer r.*

Proof: If those cycles do not derange the same set of elements in $\{1, 2, \ldots n\}$, they cannot commute unless they are disjoint. If they do derange the same set of elements, then since c_1 and c_2 commute, we have $c_1 c_2 c_1^{-1} = c_2$. By

Lemma 2, c_1 is completely determined by which element $k \in \{1, 2, ..., n\}$ satisfies $c_2(k) = l$ for some l deranged by c_1. $\square$

So, in the set of n-cycles in S_n, each element commutes with exactly $\phi(n)$ elements and in general where ϕ is Euler's function because for an n-cycle c, if $(r, n) \neq 1$, then c^r is not an n-cycle. In general, each k-cycle in S_n commutes with exactly ϕk elements. Let, for $2 \leq k \leq n$, N_k be a subset of the set of k-cycles in S_n that derange 1, such that if $c \in N_k$, then $c_r \notin N_k$ for any $r \neq 1 \, (mod \, k)$.

Consider the union

$$N = \bigcup_{k=2}^{n} N_k$$

Then by Lemma 4 and the above argument, N is a non-commuting subset of S_n. Observe that each N_k contains $\binom{n-1}{k-1}\frac{(k-1)!}{\phi(k)}$ elements. Hence:

Theorem 5 *There exists a non-commuting subset of S_n of size*

$$\sum_{k=2}^{n} \binom{n-1}{k-1} \frac{(k-1)!}{\phi(k)} \tag{2}$$

This gives us a lower bound for the maximal non-commuting subset in S_n. We have

$$\begin{aligned}
\sum_{k=2}^{n} \binom{n-1}{k-1} \frac{(k-1)!}{\phi(k)} &\geq \sum_{k=2}^{n} \frac{(n-1)!}{(n-k)!} \frac{1}{\phi(k)} \\
&\geq (n-1)! \sum_{k=2}^{n} \frac{1}{(n-k)!k} \\
&\geq (n-2)!
\end{aligned}$$

So $\mathrm{nc}(S_n) \geq (n-2)!$. Observe that this number is quite close to the order of S_n, but it is D_{2n} is the group that has the largest maximal non-commuting subset with respect to the order of the group.

3 The extraspecial p-group

We start with the result leading to the basic definition.

Proposition 6 *If P is a p-group, then the following are equivalent:*

(i) The center, the derived subgroup and the Frattini subgroup of P coincide and have order p.

(ii) P is non-abelian and P contains a normal subgroup Z such that $|Z| = p$ and P/Z is elementary abelian.

Proof: Recall that the Frattini subgroup of a group G, denoted $\Phi(G)$, is the intersection of all the maximal subgroups of G and that the derived subgroup of G, denoted $[G, G]$ is the subgroup generated by the commutators (elements of the form $x^{-1}y^{-1}xy$ for $x, y \in G$). Assume a p-group P satisfies (i). Let Z be the coinciding center, derived subgroup and the Frattini subgroup of order p. Then since Z is the center, it is a normal subgroup of P. Let $H_1, ..., H_k$ be the maximal subgroups of P. Consider the homomorphism $\phi : P \to P/H_1 \times ... \times P/H_k$ such that $\phi(g) = (gH_1, ..., gH_k)$. Then we have $ker\phi = Z$ so $P/Z \equiv H_1 \times ... \times P/H_k$. Since P is a p-group, each H_i has index p, so for each i, $|P/H_i| = p$ so $H_1 \times ... \times P/H_k$ is elementary abelian. Conversely, let Z be as in (ii). Then since P/Z is abelian, we have for $a, b \in Z$, $abZ = baZ$, so $a^{-1}b^{-1}ab \in Z$ so Z contains the derived subgroup of P, since $|Z| = p$ and P is not abelian, $Z = [P, P]$. We shall now show that $Z \supseteq \Phi(P)$. Let $H_1, ..., H_r$, $r < k$, be the maximal subgroups of P containing Z. Let $N = \cap_1^r H_i$.Then, since there is a one to one correspondence between the maximal subgroups of P/Z and the maximal subgroups of P that contain Z, we have that $P/N \equiv C_p \times ...C_p \equiv P/Z$. In particular $N = Z$. So Z contains an intersection of some of the maximal subgroups, hence $\Phi(P) \subset Z$. Thus, since $|Z| = p$ and the Frattini subgroup is non-trivial because then by the above homomorphism, we would have P to be abelian; $Z = \Phi(P)$. It remains to show that Z is the center of P. Since P has non-trivial center, it suffices to show that $Z(G) \subset Z$. Assume that $Z \subset Z(P)$ with $Z \neq Z(P)$. Then clearly, $G/Z(P)$ is elementary abelian since Z is the Frattini subgroup. Then we have that there is a normal series $\{1\} \lhd Z \lhd Z(P) \lhd P$. So we have that the center of P/Z is equal to $Z(P)/Z$. But P/Z is abelian. Hence $Z(P) = P$, a contradiction. □

A group satisfying the conditions of the proposition above is called an *extraspecial p-group.*

Let P be an extraspecial p-group with center Z. Z is isomorphic to the finite field F_p and P/Z is isomorphic to a finite dimensional vector space V over F_p because it is elementary abelian. Define maps $B : P/Z \times P/Z \to F_p$ and $Q : P/Z \to F_p$ by

$$\begin{aligned} B(xZ, yZ) =& [x, y] \\ Q(xZ) =& x^p \end{aligned} \tag{3}$$

Observe that these maps are well-defined because Z is the center of P and $|Z| = p$.

On the other hand, the maps B and Q above (given on a finite dimensional vector space over a finite field) uniquely determine the group operation on P. Indeed, if we are given an n-dimensional vector space over the field F with p elements and maps B and Q as above, we can express each element $x \in P$ as $x_1x_2...x_kt$, where each x_i is a fixed representative of its coset in P/Z and $t \in F$. Then we have that the multiplication $(x_1^{\alpha_1}...x_k^{\alpha_k}t_1).(x_1^{\beta_1}...x_k^{\beta_k}t_2)$ $= x_1^{\alpha_1+\beta_1}...x_{k_1}^{\alpha_k+\beta_k}t$ for some $t \in F$ because we can interchange elements with the cost of adding an element from the center (because the center is the derived subgroup and B gives us those elements). Also, we can reduce powers using Q, which will give us uniqueness, so we have that two exraspecial p-groups are isomorphic if and only if they have the same B and Q.

A symplectic form on a vector space V over a finite field F is a bilinear form that is skew-symmetric and definite. For a bilinear form B over a vector space V, we define $\ker B = \{\, x \in V \mid \forall y \in V,\, B(x,y) = 0\}$.

Lemma 7 *B is a symplectic form.*

Proof: Since Z is the center of P and P/Z is abelian, we have that P is nilpotent of class 2. For nilpotent groups of class 2, we have $[xy,z] = [x,z][y,z]$. Which shows that B is a bilinear form. Also, it is clear that B is skew-symmetric since $[x,y] = [y,x]^{-1}$ and that B is definite since $[x,x] = 1_P$. Moreover, B is non-degenerate since $[x,y] = 1_P$ for all $y \in P$ if and only if $x \in Z(P) = Z$. Hence B is a symplectic form. □

Lemma 8 *If V is a finite dimensional vector space over a finite field and there is a symplectic form on V, then $\dim V$ is even.*

Proof: Fix a basis of V. A bilinear form B is skew-symmetric if and only if a corresponding matrix $\mathtt{B}$ is skew-symmetric, that is $\mathtt{B} = -\mathtt{B}^{\mathrm{T}}$. But we have $\det(-\mathtt{B}^{\mathrm{T}}) = (-1)^m det(\mathtt{B})$ where m is the dimension of V. Hence, if m is odd, then $det(\mathtt{B}) = 0$, hence B is degenerate.

Corollary 9 *An extraspecial p-group has order p^{2n+1}, where p is prime and $n \geq 1$.*

The following lemma will be useful. We accept it without proof.

Lemma 10 *If x and y are elements of a nilpotent group of class 2, then*

$$(xy)^n = x^n y^n [y,x]^{n(n-1)/2}$$

Here is the final step for the classification of extraspecial p-groups.

Theorem 11 *For each $n \geq 1$, there exist, up to isomorphism, two extraspecial p-groups.*

Proof: Since we know that B and Q determine the whole group, we can argue by determining the possible maps B and Q.
If $p = 2$, then $Z \cong F_2$, and by Lemma 10 we have, in the vector space notation:

$$Q(x+y) = Q(x) + Q(y) + B(x,y)$$

So,

$$(Q(x+y) - Q(x) - Q(y)) = B(x,y)$$

Since $-1 \equiv 1\,(mod\,2)$, we have that B is a symmetric bilinear form, so Q is a quadratic form. There are exactly two distinct possible quadratic form ranks in F_2, so there are two quadratic forms in this setting. Hence there exist only two extraspecial 2-groups of order 2^{2n+1} for $n \geq 1$.
For the case $p > 2$, consider Lemma 10 again. This time, since $\frac{p(p-1)}{2} \equiv 0\,(mod\,p)$, we have: $Q(x+y) = Q(x) + Q(y)$. So Q is a linear functional on the vector space $V \cong P/Z$. So, there is a unique $a \in V$ such that $Q(x) = B(x,a)$ for all $x \in V$. But since the symplectic group contains the elements that preserve B, and for any two non-zero vectors a_1 and a_2, there exists an element S of the symplectic group such that $Sa_1 = a_2$, there are only two distinct linear functionals. Namely the one with $a = 0$ and the one with $a \neq 0$.

Let F be a finite field of order p. Consider the set $F^{2n} \times F$ with the operation

$$(x,t)(y,u) = (x+y, z+t+w(x,y)) \tag{4}$$

where $+$ is the addition in the $2n$-dimensional vector space over F and $w(x,y)$, for vectors $x = (x_1, x_2, ..., x_{2n-1}, x_{2n})$ and $y = (y_1, y_2, ..., y_{2n-1}, y_{2n})$ is given by

$$w(x,y) = \sum_{i=0}^{n-1} (x_{2i+1}y_{2i+2} - x_{2i+2}y_{2i+1}) \tag{5}$$

Observe that the subgroup $\{0\} \times F$ satisfies the conditions of Proposition 6. So it is an extraspecial p-group under the above operation. We shall denote this group by $S(p,n)$. Observe that when we are considering the non-commuting subsets of this group, we only need to consider maximal *non-orthogonal* subsets of F^{2n} because two elements (x,t) and (y,u) commute in $S(p,n)$ if and only if $w(x,y) = 0$, and $w(x,x) = 0$ for all $x \in F^{2n}$. We shall also refer to these subsets as non-commuting subsets.

Theorem 12 *The maximal non-commuting subset of $S(2,n)$ has $2n+1$ elements.*

Proof: Let $\{x_1, x_2, ..., x_{2n+2}\} \subset S(2,n)$ be a non-commuting subset of G. Consider the set $K = \{x_i + x_{i+1} \,|\, 1 \leq i \leq 2n+1\}$. Assume K was linearly dependent in $\mathbf{F}_2^{2n}$, then we would have for some l and some odd r that $x_l = x_{i_1} + ... + x_{i_r}$ but then, since we have that $w(x_i, x_j) = 1$ for $i \neq j$ and that w is a bilinear form, we would have $w(x_l, x_l) = w(x_{i_1}, x_l) + ... + w(x_{i_r}, x_l) = 1$ since r is odd. Which would imply that x_l does not commute with itself. So K is linearly independent. But K has 2n+1 elements, a contradiction. So it suffices to find a non-commuting subset of $S(2,n)$ with $2n+1$ elements, which can be constructed as in the following lemma.

Lemma 13 *If $A \subset F^{2n_1}$ and $B \subset F^{2n_2}$ are non-commuting subsets, then there is a non-commuting subset of $F^{2n_1+2n_2}$ of order $|A| + |B| - 1$.*

Proof: Denote the concatenation of two elements $a \in A$ and $b \in B$, by $\mathrm{concat}(a, b)$. We shall regard this element in $F^{2n_1+2n_2}$. Fix an element $b_0 \in B$ and Let $0^{(k)}$ be the zero vector in F^k. Consider the subset

$$\{\mathrm{concat}(a, b_0) \,|\, a \in A\} \cup \{\mathrm{concat}(0^{(2n_1)}, b) \,|\, b \in B \, and \, b \neq b_0\}$$

which has $|A| + |B| - 1$ elements. □

Since, the subset

01, 10, 11, 12, 13, ..., 1(p-1)

is a non-commuting subset, and by the above lemma, we have that for each prime p and integer n, one can construct a non-commuting subset of $pn + 1$ elements. Which a the maximal non-commuting subset for the case $p = 2$, as shown in Theorem 12.

However, it is not true in general that $S(p, n)$ has a maximal non-commuting subset of $pn + 1$ elements as can be seen with the elements presented in Table 1.

02 11 11	11 12 00	20 12 20
02 11 12	00 20 01	02 20 12
21 21 00	12 22 00	20 00 21
20 12 01	21 02 22	02 12 00
20 00 11		

Table 1: 13 elements of F^4 that do not commute with each other.

Proposition 14 *The number of conjugacy classes of $S(p, n)$ is*

$$p^{2n+1} + p - 1$$

Proof: Observe that any conjugate of an element $(x, t) \in S(p, n)$ has is of the form (x, u). And it is clear that for any non-zero $x \in F_p^{2n}$ and $k \in F_p$, there is some $y \in F_p^{2n}$ such that $w(x, y) = k$. Hence each element not in the center has a conjugacy class of p elements. Since each element of the center has its singleton as its conjugacy class, we have $p^{2n} + p - 1$ conjugacy classes. □

This proposition and Theorem 1 imply that the number of non-commuting pairs in $S(p, n)$ is

$$p^{4n+2} - p^{4n+1} - p^{2n+2} + p^{2n+1} \tag{6}$$

4 Conclusions

The study of non-commuting subsets of finite groups is an algebraic problem which has many combinatorial and geometric aspects. Unfortunately, very little is known about maximal non-commuting subsets in general. More connections could be made by considering some other finite groups.

We could not find an exact maximal non-commuting subset of the groups we have considered except for the extraspecial 2-group. We hope that some better upper bounds on $\mathrm{nc}(S(p,n))$ and $\mathrm{nc}(S_n)$ will be discovered.

The extraspecial p-groups are also useful in some classification results for other finite groups (see [1]).

The set of non-commuting subsets of a group G forms a partially ordered set (poset, with). One can also consider some properties of the simplicial complex associated with this poset and obtain some general results (see [4]).

The problem could be extended to infinite groups as the problem of finding the non-commuting subset with maximal cardinality. But since most of the interesting groups are countable, do not have many subgroups with different infinite cardinalities, it may be better, keeping Zorn's Lemma in mind to simply consider locally maximal subsets of infinite groups.

On the other hand, one can consider the decision problem of finding whether a finite group, given by its Cayley table or generating relations, has a non-commuting subset consisting of k elements. It is complicated for complexity matters to consider generating relations since some groups having simple generating relations can be very complicated. So we may state

Definition 15 *(NCSUBSET)*
Instance: The Cayley table of a group G and an integer k.
Question: Does there exist a non-commuting subset of G with k elemants.

Clearly, this problem is in NP. And it reduces very easily to the CLIQUE problem. It may be NP-complete, but one tends to think that there is too much structure on a group for NP-complete problems that are based on quite arbitrary structures to be reducible to this problem. One can also consider the same problem for semigroups and monoids and try to obtain NP-completeness results.

References

[1] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, second edition, 2000.

[2] P. Erdős and E. G. Straus. How abelian is a finite group? *Linear and Multilinear Algebra*, 3(4):307–312, 1975/76.

[3] David R. Mason. On coverings of a finite group by abelian subgroups. *Math. Proc. Cambridge Philos. Soc.*, 83(2):205–209, 1978.

[4] Jonathan Pakianathan and Ergün Yalçı n. On commuting and noncommuting complexes. *J. Algebra*, 236(1):396–418, 2001.

[5] L. Pyber. The number of pairwise noncommuting elements and the index of the centre in a finite group. *J. London Math. Soc. (2)*, 35(2):287–295, 1987.