Counting Nilpotent Pairs in Finite Groups

Jason E. Fulman Michael D. Galloy
Gary J. Sherman Jeffrey M. VanderKam*

Abstract

Let G be a finite group and let $\nu_i(G)$ denote the proportion of ordered pairs of G that generate a subgroup of nilpotency class i. Various properties of the ν_i's are established. In particular it is shown that $\nu_i = k_i \cdot |G|/|G|^2$ for some non-negative integers k_i and that $\sum_{i=1}^{\infty} \nu_i$ is either 1 or at most 1/2 for solvable groups.

1 Introduction

Let G be a finite group and let

$$\nu_i(G) = \frac{n_i(G)}{|G|^2}$$

where

$$n_i(G) = |\{(x,y) \in G^2 | \langle x,y \rangle \text{ is nilpotent of class } i\}|$$

for $0 \leq i \leq \infty$. We take '$\langle x,y \rangle$ is nilpotent of class 0' to mean that $\langle x,y \rangle$ is non-nilpotent. Clearly,

$$\nu_0(G) = 1 - \sum_{i=1}^{\infty} \nu_i(G).$$

It is well known that $\nu_1(G)$, the proportion of commuting pairs in G, is at most 5/8 for non-abelian groups [5]. There is no analogous lower bound for $\nu_1(G)$. In particular, $\nu_1(S_n) \to 0$ where S_n is the

*All authors' work supported by NSF grant NSF-DMS 9100509

symmetric group on n symbols. Both of these results follow from the fact that $\nu_1(G)$ is the ratio of the number of conjugacy classes in G to the order of G [2].

In this paper we establish the following results concerning nilpotent pairs.

- G is nilpotent if, and only if, $\nu_0(G) = 0$.
- $|G|$ is a divisor of $n_i(G)$.
- If $i \neq 1$, then there exists a sequence of groups for which $\nu_i \to 1$.
- If $i \neq 0$, then there exists a sequence of groups for which $\nu_i \to 0$.
- If G is a solvable non-nilpotent group, then $\nu_0(G) \geq (p_s - 1)/p_s$ where p_s is the smallest prime dividing $|G|$.
- $\nu_0(G) = (p_s - 1)/p_s$ if, and only if, $G/Z_h \cong S_3$ where Z_h is the hypercenter of G (i.e. the largest group in the upper central series of G).

2 A characterization of nilpotent groups

It is clear that a group is abelian if, and only if, $\langle x, y\rangle$ is abelian for each pair of elements in G. An elementary proof of the analogous criterion for nilpotency follows.

Lemma 1 *Let $x, y \in G$. The subgroup $\langle x, y\rangle$ is nilpotent if, and only if, the following two conditions hold.*

1. *For any positive m, n, if x^m and y^n have relatively prime orders, then they commute.*
2. *For any positive m, n, if x^m and y^n have orders which are powers of the same prime p, then $\langle x^m, y^n\rangle$ is a p-group.*

PROOF: The necessity of the conditions follows because G is the direct product of its Sylow subgroups. To prove the converse, we will show that the two conditions imply that $\langle x, y\rangle = H$ is a direct product of its Sylow subgroups. Let $|x| = p_1^{a_1} \cdots p_k^{a_k}$ and $|y| =$

$p_1^{b_1} \cdots p_k^{b_k}$, where some of the a_i's and b_i's may be zero. Then there exist $x_1, \ldots, x_k$ which are powers of x such that $|x_i| = p_i^{a_i}$ (we let $x_i = x^{|x|/p_i^{a_i}}$).

Since $\gcd(|x|/p_1^{a_1}, \ldots, |x|/p_k^{a_k}) = 1$, we know that $\langle x \rangle = \langle x_1, \ldots, x_k \rangle$. Similarly, there exist $y_1, \ldots, y_k$ which are all powers of y such that $|y_i| = p_i^{b_i}$ and $\langle y \rangle = \langle y_1, \ldots, y_k \rangle$, so we may write $H = \langle x_1, \ldots, x_k, y_1, \ldots y_k \rangle$. Since x_i and x_j are both powers of x, they must commute for all i, j. Also, due to the first condition, if $i \neq j$, then x_i and y_j must commute, since they have relatively prime order. The second condition implies that $\langle x_i, y_i \rangle$ is a p_i-group for all i, and since all other generators of H commute with both x_i and y_i, $\langle x_i, y_i \rangle$ is in fact the normal p_i-Sylow subgroup of H; i.e., there are k normal Sylow subgroups in H. But since all Sylow subgroups of H are normal, H must in fact be a direct product of its Sylow subgroups. □

Theorem 1 *G is nilpotent if, and only if, $\nu_0(G) = 0$.*

Proof: If G is nilpotent, then all subgroups of G are nilpotent, so $\nu_0(G) = 0$. If G is non-nilpotent, then it is not the direct product of its Sylow subgroups. Therefore, there exist x and y in G of relatively prime order such that x and y do not commute. By Lemma 1, these generate a non-nilpotent group. □

3 $|G|$ divides $n_i(G)$

We will show more: the number of n-tuples which generate a subgroup of nilpotency class i is a multiple of the order of the group for all n and i.

Lemma 2 *The group $G = \langle x_1, \ldots, x_n \rangle$ is nilpotent of class less than or equal to i if, and only if, all commutators of length $i+1$ with only the x_k's as entries are equal to the identity.*

Proof: (A commutator of the form $[x, y]$ has length 2, while a commutator of length i is of the form $[x, c_{i-1}]$, where c_{i-1} is a commutator of length $i-1$.)

Assume that G is nilpotent of class at most i. By the commutator definition of nilpotency, $G^{(i)} = [G, G^{(i-1)}] = \{e\}$, so in particular the commutators of length $i+1$ with x_k's as entries must equal the identity.

For the converse, we proceed by induction on i. Suppose that all commutators of length $i+1$ with x_k's as entries equal the identity. Then all commutators of length i with x_k's as entries are contained in $Z(G)$. Thus, in $G/Z(G)$ all commutators of length i with $x_k \cdot Z(G)$'s as entries are trivial. By the induction hypothesis, $G/Z(G)$ has nilpotency class less than or equal to $i-1$. The lemma follows because G has nilpotency class exactly one greater than $G/Z(G)$. □

Theorem 2 *The number of n-tuples, $(x_1, \ldots, x_n)$, such that $\langle x_1, \ldots, x_n \rangle$ has nilpotency class i is a multiple of $|G|$ for all $i \geq 1$.*

PROOF: It suffices to show that the number of n-tuples generating a subgroup of nilpotency class less than or equal to i is a multiple of $|G|$.

For each n-tuple $(x_1, \ldots, x_n)$, define a sequence $\mathcal{C} = \{c_j\}$ consisting of commutators of the x_k's of lengths $i, i-1, \ldots, 2$ and the generators $x_1, x_2, \ldots, x_{n-1}$. For example, if $i = 2$ and $n = 2$, then the sequence would be

$$\mathcal{C} = \{[x_1, x_1], [x_1, x_2], [x_2, x_1], [x_2, x_2], x_1\}.$$

We say that x_n 'works' with $\mathcal{C}$ if $(x_1, \ldots, x_n)$ yield $\mathcal{C}$ and if all commutators of the x_k's of length $i+1$ are the identity. Let $\mathrm{w}(\mathcal{C})$ denote the number of x_n working with $\mathcal{C}$. Let K denote the intersection of the centralizers of the components of $\mathcal{C}$.

We claim that $\mathrm{w}(\mathcal{C})$ is either 0 or $|K|$. To prove this it suffices to show that if s works with $\mathcal{C}$, then t works with $\mathcal{C}$ if, and only if, $t^{-1}s$ is in K. First, let t be some other element of the group which works with $\mathcal{C}$. Since $[t, c_j] = [s, c_j]$, $t^{-1}s \in C(c_j)$, the centralizer of c_j in G. This is true for each c_j so $t^{-1}s$ must be in K. The converse is immediate using the same reasoning.

Now let $g^{-1}\mathcal{C}g$ denote the sequence obtained by conjugating each component of $\mathcal{C}$ by g. Observe that $g^{-1}x_n g$ works with $g^{-1}\mathcal{C}g$ if, and only if, x_n works with $\mathcal{C}$. Thus, $\mathrm{w}(\mathcal{C}) = \mathrm{w}(g^{-1}\mathcal{C}g)$ for any $g \in G$. It is easy to see that the number of distinct sequences obtained by conjugating $\mathcal{C}$ by an element in G is $|G|/|K|$.

It follows that

$$\frac{|G|}{|K|}\mathrm{w}(\mathcal{C}) = \sum_{g^{-1}\mathcal{C}g} \mathrm{w}(g^{-1}\mathcal{C}g) = \begin{cases} |G| \\ 0 \end{cases} .$$

Thus, the sum over all possible $\mathcal{C}$ can be expressed as

$$\sum \sum_{g^{-1}\mathcal{C}g} \mathrm{w}(g^{-1}\mathcal{C}g) = \sum |G|$$

which is also a multiple of $|G|$. □

Corollary 1 *The number of n-tuples, $(x_1, x_2, \ldots, x_n)$, that generate a non-nilpotent subgroup is a multiple of $|G|$.*

4 Limiting values of $\nu_i(G)$

Lemma 3 *For all groups G and H and all $m \geq 1$,*

$$\sum_{i=1}^{m} \nu_i(G \times H) = \left(\sum_{i=1}^{m} \nu_i(G)\right)\left(\sum_{i=1}^{m} \nu_i(H)\right).$$

PROOF: It suffices to show that

$$\sum_{i=1}^{m} n_i(G \times H) = \left(\sum_{i=1}^{m} n_i(G)\right)\left(\sum_{i=1}^{m} n_i(H)\right).$$

Let x_G and x_H denote the projection of x onto G and H, respectively. Since the nilpotency class of a direct product is the maximum of the nilpotency classes of its factors and since both $\langle x_G, y_G \rangle$ and $\langle x_H, y_H \rangle$ are quotient groups of $\langle x, y \rangle$, it follows that $\langle x, y \rangle$ has nilpotency class greater than or equal to $\langle x_G, y_G \rangle \times \langle x_H, y_H \rangle$. The opposite inequality follows since $\langle x, y \rangle$ is a subgroup of $\langle x_G, y_G \rangle \times \langle x_H, y_H \rangle$. □

Theorem 3 *For each non-negative integer m other than one, there exists a sequence $\{G_n\}$ of groups such that $\nu_m(G_n) \to 1$.*

PROOF: It is known [5] that ν_1, the probability of two elements commuting, is either 1 or less than or equal to 5/8. For the other values of m, we will define a sequence of groups $\{G_n\}$ in which $G_n = \prod_{i=1}^{n} G$.

Case: $m = 0$. Let $G = S_3$ and note that $\nu_0(G) = 1/2 > 0$, $\nu_1(G) = 1/2$, and $\nu_i(G) = 0$ for $i \geq 2$. By Lemma 3, $\nu_1(G_n) = (1/2)^n \to 0$; i.e. $\nu_0(G_n) \to 1$.

Case: $m \geq 2$. We define G to be the dihedral group on 2^m symbols. G has nilpotency class m and is 2-generated, so $\nu_m(G) > 0$ and $\sum_{i=1}^{m-1} \nu_i(G) < 1$. It follows that from Lemma 3 that

$$\lim_{n\to\infty} \sum_{i=1}^{m-1} \nu_i(G_n) = \lim_{n\to\infty} (\sum_{i=1}^{m-1} \nu_i(G))^n = 0$$

which implies that $\nu_m(G_n) \to 1$. □

Theorem 4 *For each integer $m \geq 1$, there exists a sequence $\{G_n\}$ of groups such that $\nu_m(G_n) > 0$ for all n and $\nu_m(G_n) \to 0$.*

PROOF: Let G be the dihedral group on 2^{m+1} symbols and let $G_n = \prod_{i=1}^{n} G$. Note that G is 2-generated and has nilpotency class m, so $\nu_m(G) > 0$. Since G contains a subgroup isomorphic to the dihedral group on 2^{m-1} symbols, each G_n contains such a subgroup, so $\nu_m(G_n) > 0$ for each n. Theorem 3 implies that $\nu_{m+1}(G_n) \to 1$, which in turn implies $\nu_m(G_n) \to 0$. □

5 A lower bound on $\nu_0(G)$ for solvable non-nilpotent groups

Theorem 5 *If G is a solvable non-nilpotent group, then $\nu_0(G) \geq (p_s - 1)/p_s$, where p_s is the smallest prime dividing $|G|$. Moreover, $\nu_0(G) = (p_s - 1)/p_s$ if, and only if, $G/Z_h \cong S_3$.*

The proof of this theorem is quite long and is best made through a sequence of lemmas.

Lemma 4 *If G is non-nilpotent and p_s is the smallest prime dividing $|G|$, then $\nu_1(G) \leq 1/p_s$.*

PROOF: We note that $\nu_1(G) \leq \nu_1(G/Z(G))$, since if two elements commute in G, their cosets commute in $G/Z(G)$. Thus it suffices to prove the lemma for groups with trivial center. Now by Erdös [2], we know that we may write $\nu_1(G) = k/|G|$, where k is the number of conjugacy classes of G. In order to prove the lemma, we assume that $k/|G| > 1/p_s$ and derive a contradiction. The assumed inequality implies that $k \geq |G|/p_s + 1$, since p_s divides the order of G. But then we may use the class equation as follows ($\overline{x}$ denotes the conjugacy class of x):

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\overline{x}} \frac{|G|}{|C(x)|} \\ &\geq 1 + p_s(k-1) \\ &\geq 1 + |G|, \end{aligned}$$

a contradiction. □

Lemma 5 *If all Sylow subgroups of a group G are abelian, then $\nu_i(G) = 0$ for all $i \geq 2$ and either the group is abelian or $\nu_0(G) \geq (p_s - 1)/p_s$.*

PROOF: We will show that in such a group G, either two elements commute or they generate a non-nilpotent subgroup. Combining this with Lemma 4 gives the desired result, because if $\nu_i(G) = 0$ for all $i \geq 2$, then $\nu_0(G) + \nu_1(G) = 1$.

Consider two elements $x, y \in G$ for which $\langle x, y \rangle$ is nilpotent. This means that $\langle x, y \rangle$ can be written as a direct product of its Sylow subgroups, each of which is a subgroup of a Sylow subgroup of G. Thus $\langle x, y \rangle$ can be written as a direct product of abelian groups. □

Corollary 2 *If $|G|$ is not divisible by the cube of any prime, then $\nu_0(G) \geq (p_s - 1)/p_s$.*

PROOF: If $|G|$ is cube-free, then all Sylow subgroups of G have order p or p^2. $\square$

Lemma 6 *For any group G, $\nu_0(G) = \nu_0(G/Z(G))$.*

PROOF: If $\langle x, y\rangle$ is nilpotent, then so is $\langle z_1x, z_2y\rangle$ for $z_1, z_2 \in Z(G)$. Since cosets of $Z(G)$ all have the same cardinality, it suffices to show that $\langle x, y\rangle$ is nilpotent in G if, and only if, $\langle xZ(G), yZ(G)\rangle$ is nilpotent in $G/Z(G)$.

If $\langle x, y\rangle$ is nilpotent in G, then clearly $\langle xZ(G), yZ(G)\rangle$ is nilpotent in $G/Z(G)$. In fact, it is clear that $\nu_0(G) \geq \nu_0(G/N)$ for any $N \trianglelefteq G$. If $\langle x, y\rangle$ is non-nilpotent in G, then $H = \langle x, y, Z(G)\rangle$ is non-nilpotent in G. Thus $H/Z(H)$ is non-nilpotent. But $H/Z(H)$ is isomorphic to a quotient group of $H/Z(G)$, so $H/Z(G)$ cannot be nilpotent. Thus $\langle xZ(G), yZ(G)\rangle \cong H/Z(G)$ is non-nilpotent. $\square$

Corollary 3 *For any group G, $\nu_0(G) = \nu_0(G/Z(G)) = \nu_0(G/Z^{(2)}(G)) = \cdots = \nu_0(G/Z^{(n)}(G))$.*

PROOF: Let H_i denote $G/Z^{(i-1)}$. It follows from the construction of the upper central series that

$$Z^{(i)}(G)/Z^{(i-1)}(G) \cong Z(H_i).$$

Since $G/Z^{(i)}(G) \cong H_i/Z(H_i)$ and since $\nu_0(H_i) = \nu_0(H_i/Z(H_i))$, we have $\nu_0(G/Z^{(i)}(G)) = \nu_0(G/Z^{(i-1)}(G))$. $\square$

Corollary 4 *If N is a normal subgroup of G and is contained in Z_h, then $\nu_0(G) = \nu_0(G/N)$.*

PROOF: As noted in the proof of Lemma 6, $\nu_0(G) \geq \nu_0(G/N)$. Since N is contained in $Z_h, G/Z_h$ is a quotient group of G/N. Thus $\nu_0(G/N) \geq \nu_0(G/Z_h) = \nu_0(G)$. $\square$

Corollary 5 *If $G/Z_h \cong S_3$ then $\nu_0(G) = \frac{1}{2}$.*

Corollary 6 *$|G||Z_h|$ is a divisor of $n_0(G)$.*

PROOF: By Corollary 1, $|G|/|Z_h|$ is a divisor of $n_0(G/Z_h)$. By Corollary 3, $\nu_0(G) = \nu_0(G/Z_h)$, so $|G|/|Z_h|$ is a divisor of $n_0(G)/|Z_h|^2$. □

Lemma 7 *If G has trivial center, then $\nu_0(G) > \nu_0(G/N)$ for all non-trivial normal subgroups N of G.*

PROOF: Since $\langle x, y\rangle$ nilpotent in G implies $\langle xN, yN\rangle$ nilpotent in G/N, it suffices to show that some subgroup $\langle x, y\rangle$ is non-nilpotent in G while its image $\langle xN, yN\rangle$ is nilpotent in G/N.

If N is non-nilpotent, we are done because by Theorem 1, we have a non-nilpotent subgroup $\langle x, y\rangle$ of N whose image in G/N is necessarily trivial.

Now we consider the case in which N is nilpotent and $\nu_0(G) = \nu_0(G/N)$. First we show that we may assume N to be a p-group. N is the direct product of its Sylow subgroups $P_1 \times P_2 \cdots \times P_n$. Since N is normal in G, P_1 is normal in G. Since ν_0 is non-increasing over quotients, $\nu_0(G) \geq \nu_0(G/P_1) \geq \nu_0((G/P_1)/(N/P_1)) = \nu_0(G/N) = \nu_0(G)$, so $\nu_0(G) = \nu_0(G/P_1)$. If N is not a p-group, we replace N by P_1.

Now it suffices to show that some element in N together with some element of $G - N$ generates a non-nilpotent subgroup of G because the image of the element in N is trivial in G/N. Suppose instead that $\langle x, y\rangle$ is nilpotent for all $x \in N$, $y \in G - N$. In particular, we may take $x \in Z(N)$ and conclude, by Theorem 1, that x must also commute with all elements of order relatively prime to p. Writing G as a product (not necessarily direct) of its Sylow subgroups, we see that x commutes with all of G, contradicting $Z(G) = e$. □

If there is a solvable non-nilpotent group G for which $\nu_0(G) < (p_s - 1)/p_s$, then there is one of minimal order, say M.
Fact *All proper quotients of M are nilpotent.*
PROOF: Suppose that $N \trianglelefteq M$ and M/N is non-nilpotent. Let p_s and p'_s denote the smallest primes dividing $|M|$ and $|M/N|$, respectively. Then

$$\nu_0(M/N) \leq \nu_0(M) < (p_s - 1)/p_s \leq (p'_s - 1)/p'_s,$$

contradicting the minimality of the order of M. □

Solvable non-nilpotent groups with all of their proper quotients nilpotent are referred to as just-non-nilpotent (JNN) groups. Note that all JNN groups must have trivial center (otherwise $G/Z(G)$ is a proper non-nilpotent quotient). Francosi and de Giovanni [3] have characterized finite JNN groups:

Theorem 6 *A finite group G is JNN if, and only if, G is isomorphic to the semi-direct product $L \propto A$ where A is an elementary abelian q-group (q a prime), L is a finite nilpotent group whose order is not divisible by q, and the action of L on A is faithful and irreducible.*

Thus, to prove Theorem 5 it suffices to prove it for JNN groups. To this end let J denote such a group: $J \cong L \propto A$ where L and A are as in the Francosi and de Giovanni result. Since $L \cong P_1 \times \cdots \times P_k$, where the P_i's are the unique p_i-Sylow subgroups of L, we may write

$$J = P_k \propto (P_{k-1} \propto \cdots \propto (P_1 \propto A)). \qquad (*)$$

Due to Lemma 1 and the structure of J, we see that the number of p-Sylow subgroups containing a given element in J will play an important role in our proof . Given a subset $\{x_1, \ldots, x_k\}$ of a group, we define $\#_p(x_1, \ldots, x_k)$ as the number of p-Sylow subgroups containing $\{x_1, \ldots x_k\}$.

Lemmas 9-12 and Corollaries 8 and 9 each concern groups of the form $P \propto N$ where P is a p-group and p does not divide $|N|$.

Lemma 8 *If x and y are in a common p-Sylow subgroup of $P \propto N$, then*

$$\#_p(x, y) = \frac{|C(x) \cap C(y) \cap N|}{|C(P) \cap N|}.$$

PROOF: We may assume that $x, y \in P$ because $P \propto N$ may be written as the semi-direct product of any of its p-Sylow subgroups with N. Since $G = PN$, we may write any other p-Sylow subgroup as

$$P' = (x_P x_N)^{-1} P (x_P x_N) = x_N^{-1}(x_P^{-1} P x_P) x_N = x_N^{-1} P x_N$$

where $x_P \in P$, $x_N \in N$. Thus all p-Sylow subgroups are conjugate to P, and thus to each other, by elements in N. Now each p-Sylow subgroup contains exactly one element from each coset of N and conjugation by an element of N preserves cosets of N, so conjugating P by $z_N \in N$ will yield a p-Sylow containing x and y if, and only if, $z_N \in C(x) \cap C(y) \cap N$. For the same reasons, conjugation by z_N fixes P if, and only if, z_N commutes with all of P. Therefore we must divide $|C(x) \cap C(y) \cap N|$ by $|C(P) \cap N|$. □

Corollary 7 *If $G = P \propto N$, then*

$$\#_p(x) = \frac{|C(x) \cap N|}{|C(P) \cap N|} \text{ and } \#_p(e) = \frac{|N|}{|C(P) \cap N|}.$$

PROOF: This follows by observing that $\#_p(x) = \#_p(x, e)$ and $\#_p(e) = \#_p(e, e)$. □

Note that $\#_p(e)$ is just the number of p-Sylow subgroups in $P \propto N$. Hereafter, we will denote this number by $\#_p$.

Corollary 8 *If x is in a p-Sylow subgroup of $P \propto N$, then $\#_p(x)$ divides $\#_p$.*

PROOF: This follows from the fact that $\#_p/\#_p(x) = |N|/|C(X) \cap N|$. □

Lemma 9 *If x and y are in p-Sylow subgroups of $P \propto N$ and in the same coset of N, then $\#_p(x) = \#_p(y)$.*

PROOF: Since all p-Sylow subgroups are conjugate by an element in N, and conjugation by N preserves cosets of N, there is a group automorphism (conjugation by some element of N) that sends x to y. □

Lemma 10 *If $x \in (P \propto N) - N$, then x has order divisible by p.*

PROOF: If p does not divide the order of x, then $x^{|N|} = e$. Thus the coset xN has order a divisor of $|N|$ in $(P \propto N)/N$. This is impossible since $(P \propto N)/N$ is a p-group and N has order relatively prime to p. □

Lemma 11 *If $\langle x, y\rangle$ is nilpotent in $P \propto N$, then there exists a p-Sylow subgroup, $P_{x,y}$, of $P \propto N$ and unique elements x_p, y_p, x_N, y_N such that*

1. $x = x_p x_N$, $y = y_p y_N$,
2. $\langle x\rangle = \langle x_p, x_N\rangle$, $\langle y\rangle = \langle y_p, y_N\rangle$,
3. $x_p, y_p \in P_{x,y}$,
4. $x_N, y_N \in C(x_p) \cap C(y_p) \cap N$, *and*
5. $\langle x_N, y_N\rangle$ *is nilpotent.*

PROOF: Let $|P| = p^k$. Choose $x_p = x^{h_1|N|}$ and $x_N = x^{h_2 p^k}$ and assign h_1 and h_2 by the equation

$$h_1|N| + h_2 p^k \equiv 1 \pmod{p^k|N|}.$$

By the Chinese Remainder Theorem, this equation has a solution $\pmod{p^k|N|}$, since p^k and $|N|$ are relatively prime. Such a solution is in fact unique in the context of the group, because if

$$h_1'|N| + h_2' p^k \equiv 1 \pmod{p^k|N|},$$

we have that

$$(h_1' - h_1)|N| + (h_2' - h_2)p^k \equiv 0 \pmod{p^k|N|}.$$

But then $(h_1' - h_1)$ must be divisible by p^k, so $x^{h_1|N|} = x^{h_1'|N|}$ (similarly for h_2). Therefore, $x_p x_N = x^{h_1|N| + h_2 p^k} = x$, since $|x|$ is a divisor of $p^k|N|$. We choose y_p and y_N in a similar fashion.

Clearly, $\langle x\rangle = \langle x_p, x_N\rangle$, $\langle y\rangle = \langle y_p, y_N\rangle$, and x_p, y_p, x_N, y_N are unique.

Now since $|x_p|$ and $|y_p|$ are both powers of p and $\langle x, y\rangle$ is nilpotent, Lemma 1 implies that $\langle x_p, y_p\rangle$ is a p-group. Therefore there is some p-Sylow subgroup, $P_{x,y}$, which contains both x_p and y_p.

That $y_N \in C(x_p) \cap C(y_p)$ follows from Lemma 1 because x_p and y_N have relatively prime orders and because y_p and y_N are both powers of y. That $y_N \in N$ follows from Lemma 10 because the order of y_N is relatively prime to p. The argument for x_N is similar.

Finally, since $\langle x_N, y_N\rangle$ is contained in $\langle x_p, y_p, x_N, y_N\rangle = \langle x, y\rangle$, it is nilpotent. $\square$

Recall the structure of J (see $(*)$). We will show that if $N = P_{i-1} \propto \cdots \propto (P_1 \propto A)$ and $\nu_0(N) \geq (p_s - 1)/p_s$, then $p_\nu(P_i \propto N) \geq (p_s - 1)/p_s$. After that, we will show that $\nu_0(P_1 \propto A) \geq (p_s - 1)/p_s$.

Consider $P_i \propto N$. How do we count the number of pairs (x, y) such that x is in one fixed coset of N, y is in another fixed coset of N, and $\langle x, y\rangle$ is nilpotent? (We will refer throughout this part of the proof to p_i as p.) First we fix a p-Sylow subgroup P of $P_i \propto N$ and ask how many ordered pairs (x, y) are in the fixed ordered pair of cosets (x_pN, y_pN), with $x_p, y_p \in P$ such that we may represent $x = x_px_N$ and $y = y_py_N$ with all of the conditions in Lemma 11 holding for x_N, y_N (x_p and y_p are fixed). We denote this number by $c(x_p, y_p)$. An upper bound for $c(x_p, y_p)$ is obtained by noting that x_N and y_N both satisfy condition (4) of Lemma 11; i.e., there are no more than $|C(x_p) \cap C(y_p) \cap N|$ choices for x_N — and likewise for y_N. Thus $c(x_p, y_p) \leq |C(x_p) \cap C(y_p) \cap N|^2$. Note that this is an upper bound because we have not included the condition that $\langle x_N, y_N\rangle$ is nilpotent.

Any other two elements x'_p, y'_p which are in some other p-Sylow subgroup P' and the same cosets of N as x_p, y_p, respectively, satisfy $c(x'_p, y'_p) = c(x_p, y_p)$ because there is an inner automorphism which sends x_p, y_p to x'_p, y'_p. The number of such x'_p, y'_p equals the number of distinct p-Sylow subgroups in the group divided by the number which contain both x_p and y_p; i.e., $\#_p/\#_p(x_p, y_p)$. But every pair of elements (x, y) with $x \in x_pN$ and $y \in y_pN$ and $\langle x, y\rangle$ nilpotent must yield exactly one of the x'_p, y'_p's (Lemma 11), so the total number of nilpotent pairs (x, y) with $x \in x_pN$, $y \in y_pN$ (denoted by $c_T(x_p, y_p)$) can be expressed as follows:

$$\begin{aligned} c_T(x_p, y_p) &= c(x_p, y_p)\left(\frac{\#_p}{\#_p(x_p, y_p)}\right) \\ &\leq |C(x_p) \cap C(y_p) \cap N|^2 \frac{\left(\frac{|N|}{|C(P) \cap N|}\right)}{\left(\frac{|C(x_p) \cap C(y_p) \cap N|}{|C(P) \cap N|)}\right)} \\ &= |C(x_p) \cap C(y_p) \cap N||N|. \end{aligned}$$

But the total number of pairs (x, y) with x and y in the appropriate cosets is just $|N|^2$, so the probability that a pair (x, y) chosen from the coset pair (x_pN, y_pN) generates a nilpotent subgroup is bounded by $|C(x_p) \cap C(y_p) \cap N|/|N|$.

By Theorem 6, the action of P on A (which is a subgroup of N) is faithful, so unless both x_p and y_p are the identity, either x_p or y_p (or both) commutes with no more than $1/q$ of the elements A. This in turn means that at least one of x_p or y_p commutes with no more than $1/q$ of the elements of N. Thus, unless both x_p and y_p are the identity, the probability that a pair of elements (x, y), chosen from the cosets x_pN, y_pN respectively, generates a nilpotent group is bounded by $1/q \leq 1/p_s$, as desired. But if the probability that two elements both chosen from N generate a nilpotent group is also less than or equal to $1/p_s$, then the probability that two elements generate a nilpotent group is less than or equal to $1/p_s$ for any coset pair. Thus given that $\nu_0(N) \geq (p_s - 1)/p_s$, we have shown that $\nu_0(P_i \propto N) \geq (p_s - 1)/p_s$, and the induction step is complete.

Now we proceed with the base case of the induction. We need to show that $\nu_0(P \propto A) \geq (p_s - 1)/p_s$ for $A = (\mathbf{Z}_q)^n$ and P a p-Sylow subgroup, $p \neq q$. Using the argument made in the induction step, we know that if the two elements in a pair are not both in A, then the probability that the pair generates a nilpotent subgroup is less than or equal to $1/q$. The probability that two elements chosen at random from the group generate a non-nilpotent group is at least

$$\left(\frac{p^{2m} - 1}{p^{2m}}\right)\left(\frac{q - 1}{q}\right).$$

We consider two cases, remembering that the choice of which Sylow subgroup of L would serve as P_1 was arbitrary, since L was just the direct product of the P_i's.

Case: q is not the largest prime dividing $|J|$. Choose some Sylow subgroup P of L, where $p > q$, and act first with it. Let $|P| = p^m$. We will first show that not all of the values of $|C(x_p) \cap C(y_p) \cap A|$ that were used in the induction proof are actually equal to q^{n-1}. Suppose instead that they were. This implies that $C(x_p) \cap A$ and $C(y_p) \cap A$ have order q^{n-1} for any choice of $x_p, y_p \in P$ (they cannot have order q^n, because then the action of P on A would not be faithful). But for any x_p not equal to the identity, $|C(x_p) \cap A| \leq q^{n-1}$, since P acts faithfully on A. Thus every element in P must commute with exactly the same q^{n-1} elements in A, so $|C(P) \cap A| = q^{n-1}$. Then the number of p-Sylow subgroups of $P \propto A$ is equal to $|A|/|C(P) \cap A| = q$. Since no non-identity element of P is in all of the p-Sylow subgroups (the action is faithful so no non-identity element commutes with all of A) and since the number of Sylow p-groups an element is in must divide the total number of p-Sylow subgroups (Lemma 8), they must all be in exactly one p-Sylow subgroup, namely P. Thus the total number of elements in p-Sylow subgroups is just $q(p^m - 1) + 1 = qp^m - q + 1$. By Frobenius [4], this number must be divisible by p^m, so $q \equiv 1 \pmod{p^m}$. This is impossible since $q < p$. So, as claimed, not all of the $|C(x_p) \cap C(y_p) \cap A|$ are equal to q^{n-1}.

Now if $|C(x_p) \cap C(y_p) \cap A| \leq q^{n-2}$, then there are at least $p-1$ elements of P, namely $y_p, y_p^2, \ldots, y_p^{p-1}$, all of which are in different cosets of N and whose centralizers intersect $C(x_p) \cap A$ in no more than q^{n-2} elements. We will show that this is in fact enough to make the total probability greater than $(q-1)/q$. Given this set of $2(p-1)$ ordered pairs in P (x_p can be either the first or last element in the pair, so there is a 2 in the expression) with sufficiently small centralizer intersections, the probability that two elements in $P \propto A$ generate a non-nilpotent group can be bounded as follows:

$$\begin{aligned}
\nu_0(P \propto A) &\geq \left(\frac{p^{2m} - 2p + 1}{p^{2m}}\right)\left(\frac{q-1}{q}\right) + \left(\frac{2p-2}{p^{2m}}\right)\left(\frac{q^2-1}{q^2}\right) \\
&= \left(\frac{q-1}{q}\right)\left(\frac{q(p^{2m} - 2p + 1) + (q+1)(2p-2)}{qp^{2m}}\right) \\
&= \left(\frac{q-1}{q}\right)\left(\frac{qp^{2m} - 2pq + q + 2pq - 2q + 2p - 2}{qp^{2m}}\right) \\
&= \left(\frac{q-1}{q}\right)\left(\frac{qp^{2m} - q + 2p - 2}{qp^{2m}}\right) \\
&> \frac{q-1}{q}.
\end{aligned}$$

We note that equality cannot hold for this case, since $p > q \geq 2$ implies that $2p > q + 2$.

Case: q is the largest prime dividing $|J|$. We act first with the Sylow subgroup of L corresponding to the largest prime, say p, which divides L. Note that $p < q$. But then $q \geq p+1$, so $(q-1)/q \geq p/(p+1)$. In this case,

$$\begin{aligned}
\nu_0(P \propto A) &\geq \left(\frac{p^{2m}-1}{p^{2m}}\right)\left(\frac{p}{p+1}\right) \\
&= \frac{p(p^2-1)(p^{2m-2}+\ldots+1)}{p^{2m}(p+1)} \\
&\geq \frac{p^{2m-1}(p^2-1)}{p^{2m}(p+1)} \text{ (equality only if } m=1) \\
&= \frac{p-1}{p} \\
&\geq \frac{p_s-1}{p_s}.
\end{aligned}$$

As a result, we see that we have equality only if $m = 1$ and $q = p+1$, i.e., if $p^m = 2$ and $q = 3$. But since p was the largest prime dividing $|L|$, this means that for equality to occur, $L \cong \mathbf{Z}_2$ and $A \cong (\mathbf{Z}_3)^n$. Thus the base case of our induction is complete, and so is our proof that, for all solvable non-nilpotent groups G, $\nu_0(G) \geq (p_s - 1)/p_s$.

Now we prove the equality condition of Theorem 5. From our analysis of the base case of the induction, we know that the only way that $\nu_0(J)$ can actually equal $(p_s - 1)/p_s$ is if $J \cong \mathbf{Z}_2 \propto (\mathbf{Z}_3)^n$. In this case all Sylow subgroups of J are abelian. Lemma 5 implies that $\nu_0(J) = (p_s - 1)/p_s = \frac{1}{2}$ only if $p_1(J) = \frac{1}{2}$. It is known [7] that the only groups in which the probability of two elements commuting is exactly one half are those groups H such that $H/Z(H) \cong S_3$. Therefore, the only JNN group J for which $\nu_0(J) = (p_s - 1)/p_s$ is $J \cong S_3$. Now if a group G is solvable (but not JNN), $\nu_0(G) = (p_s - 1)/p_s$ only if S_3 is a quotient group of G, and $\nu_0(G) = \nu_0(S_3)$. By Lemma 4 and Corollary 4, this requires that $G/N \cong S_3$, where $N \subseteq Z_h(G)$. If N is not equal to $Z_h(G)$, then $G/Z_h(G)$ must be a proper quotient group of S_3. But all proper quotients of S_3 are abelian, which contradicts the fact that G must be non-nilpotent, so $N \cong Z_h(G)$. Thus $\nu_0(G) = (p_s - 1)/p_s$ for a solvable group G if, and only if, $G/Z_h(G) \cong S_3$.

6 Solvable pairs

For $(x, y) \in G^2$, consider the derived series of $\langle x, y\rangle$:

$$\langle x, y\rangle \geq \langle x, y\rangle^{(1)} \geq \cdots \geq \langle x, y\rangle^{(i)} = R.$$

Here R is the unique maximal perfect subgroup of G and i is the smallest non-negative integer such that $\langle x, y\rangle^{(i)} = R$. If $R = \{e\}$, then $\langle x, y\rangle$ is solvable of class i. If $R \neq \{e\}$, then $\langle x, y\rangle$ is non-solvable and we say it is solvable of class 0. Let

$$\sigma_i(G) = \frac{s_i(G)}{|G|^2}$$

where

$$s_i(G) = |\{(x, y) \in G^2 | \langle x, y\rangle \text{ is solvable of class } i\}|.$$

It is known that $\sigma_i(G) = 1$ if, and only if, G is solvable [8].

Question 1 *Does $|G|$ divide $s_i(G)$?*

We can show the answer is yes for $s_2(G)$.

Question 2 *Is the limiting behavior of $\sigma_i(G)$ predictable?*

Conjecture 1 *If G is non-solvable, then $\sigma_0(G) \geq 19/30$.*

We note that $\sigma_0(\mathrm{PSL}(2, 5)) = \sigma_0(S_5) = \sigma_0(A_5) = 19/30$.

Conjecture 2 *Theorem 5 holds for non-solvable groups.*

Note that Conjecture 2 follows from Conjecture 1:

$$\nu_0(G) \geq \sigma_0(G) \geq 19/30 > 1/2 = (p_s - 1)/p_s$$

because all non-solvable groups have even order.

References

[1] Dubose-Schmidt, R., M. D. Galloy, and D. L. Wilson. *Counting nilpotent pairs in finite groups: some conjectures.* Rose-Hulman Technical Report MS TR 92-05. (1992).

[2] Erdös, P. and P. Turán. *On some problems of a statistical group theory, IV.* Acta. Math. Acad. Science Hung., **19** (1968), pp. 413-435.

[3] Franciosi, Silvana and Francesco de Giovanni. *Soluble groups with many nilpotent quotients.* Proceedings of the Royal Irish Academy. Sect. A. **89** (1989) pp. 43-52.

[4] Frobenius, G. *Verallgemeinerung des Sylowschen Satze.* Berliner Sitz. (1895), pp. 981-993.

[5] Gustafson, W. H. *What is the probability that two group elements commute?* Amer. Math. Monthly. **80** (1973), pp. 1031-1034.

[6] Rose, John S. *A Course on Group Theory.* Cambridge: Cambridge University Press, 1978.

[7] Rusin, David J. *What is the probability that two elements of a finite group commute?* Pacific Journal of Mathematics. **82** (1979), pp. 237-247.

[8] Thompson, John G. *Nonsolvable finite groups all of whose local subgroups are solvable.* Bull. Amer. Math. Soc. **74** (1968), No. 3, pp. 383-437.

Acknowledgements: The calculations (including [1]) which motivated the results appearing in this paper were done with the computer algebra system Cayley. The authors wish to thank Eric Wepsic for suggestions that simplified the proofs appearing in Section 2.

Author's addresses:

Jason E. Fulman, Harvard University, Cambridge MA 02138 (USA)

Michael D. Galloy, University of Kentucky, Lexington KY 40506 (USA)

Gary J. Sherman, Rose-Hulman Institute of Technology, Terre Haute IN 47803 (USA)

Jeffrey M. Vanderkam, Princeton University, Princeton NJ 08544 (USA)