Electronic Colloquium on Computational Complexity, Report No. 183 (2026)

Nilpotency determines multiparty communication complexity

Emanuele Viola*

June 12, 2026

We consider the problem of computing *iterated multiplication* (IM) of nk elements from a finite group in the number-on-forehead model [CFL83] with k parties. The input is a $k \times n$ matrix X and the output is the product $\prod_j \prod_i X_{i,j}$ of the elements in column-major order. Party i has row i on the forehead. This problem has been studied in a number of recent works [MV13, GV15, GV19, GV22, Sha16, Vio19, DV23, DLV24], focusing on *quasirandom groups* [Gow08]. It is conjectured in [GV19] that for quasirandom groups this problem requires large communication even for $k \geq \log n$. Proving such bound is a notorious open problem, and I am not aware of any non-trivial upper bounds.

In this paper we show that IM has constant-communication protocols *if and only if* the group is *nilpotent*, thus giving a new characterization of nilpotency based on communication complexity. In fact, for non-nilpotent groups we essentially recover the state-of-the-art lower bound from [BNS92]. These results suggest a refinement of the conjecture in [GV19]: Does IM require large communication even for $k \geq \log n$ for every non-nilpotent group?

Definition 1. A finite group is nilpotent if it is the direct product of groups of prime-power order.

Theorem 2. *If G is nilpotent then IM can be computed with communication $\leq c_G$ by c_G parties, for every partition.*

If G is not nilpotent then for any k, for some partition, IM requires communication $\geq n/(c_G)^k$ for k parties.

Each occurrence of the notation c_x indicates a possibly different real > 0 depending only on x.

In circuit complexity, Barrington famously proved [Mix89] a similar dichotomy with respect to the *solvability* of the group : IM over solvable groups is in ACC^0, but over non-solvable groups is complete for NC^1. However it is open whether $\mathrm{NC}^1 = \mathrm{ACC}^0$. By contrast the present results characterize nilpotency unconditionally.

To prove the upper bound in Theorem 2 we use that IM on nilpotent groups can be computed by a suitable polynomial of degree c_G [PT01], and then communication protocols for polynomials [HG91]. However the result in [PT01] can't be used as stated, and its proof is somewhat indirect, so let us repeat the argument once again. Essentially the same proof

*Supported by NSF grant CCF-2430026.

ISSN 1433-8092

appears in [LV25], except for a minor issue that is corrected here. It suffices to give a protocol when G is of order p^r for a prime p and $r \in \mathbb{N}$. The claim is that we can identify the group with the vector space $\mathbb{F}_p^r$ and that there are r polynomials of degree c_G which compute IM. We prove this by induction. For base case we can take the trivial case $r = 0$. For the inductive step, G has a normal subgroup H of size p^{r-1} (see e.g. [DF04], Chapter 6, Theorem 1.(3)). The quotient group has size p and so is cyclic. So any $g \in G$ can be written as $a^i h$ for $i \in \mathbb{Z}_p$. So a product $\prod_{i \le n} g_i$ can be written as

$$\prod_i a^{f(i)} h_i = \left(a^{f(1)} h_1 a^{-f(1)}\right) \left(a^{+f(1)+f(2)} h_2 a^{-f(1)-f(2)}\right) \cdots = \prod_i (b_i h_i b_i^{-1}) b_n$$

where $b_i := a^{\sum_{j \le i} f(j)}$. We claim that each b_i is computable by a constant-degree polynomial. Note that although the quotient is cyclic the order of a may not be p, so this last claim is not immediate. However, we can compute the base-p representation of the exponent by constant-degree polynomials. This is a relatively standard step, relying on Lucas' theorem, which has been carried out before, for example in Theorem 2.8 in [BGL06]. From this representation we can compute b_i via a polynomial generically, via a polynomial of degree c_G. A similar argument shows that multiplication of two elements and inverses are computable. Finally, the elements inside the brackets are in H, and so we can apply induction.

In the rest of this paper we prove the lower bound. The following lemma shows that any non-nilpotent group has as a subquotient a certain type of semi-direct product group. Then we show that the lower bound in [BNS92] can be applied to such semi-direct products.

Lemma 3. *Any finite non-nilpotent group G has a subquotient H/N (where H is a subgroup of G and N is a normal subgroup of H) which is a semidirect product $\mathbb{F}_p^d \rtimes Q$ between a vector space $\mathbb{F}_p^d$ and a cyclic q-group Q generated by $g \in Q$ and such that the action of g on $\mathbb{F}_p^d$ is a $d \times d$ matrix M s.t. $Mv \neq v$ for every non-zero vector $v \in \mathbb{F}_p^d$. I.e., elements of H/N can be written as vg^i where $v \in \mathbb{F}_p^d$ with multiplication rule*

$$vg^i \cdot v'g^j := (v + (M^i v'))g^{i+j}.$$

Here p and q are distinct primes.

For example, for the dihedral group on 6 elements we have $p = 3$, $d = 1, M = -1$.

Lemma 3 seems a folklore consequence of known results. I am unable to find a reference. So I include a proof below, relying on a number of facts from group theory.

Note that from a communication protocol for IM in G we can obtain a protocol for Iin M in any subquotient of G. Indeed, given elements in the subquotient we can pick representatives, multiply in the mother group G, and then compute cosets. Except for computing IM in G, all these operations can be done without communication. Hence by Lemma 3 it suffices to prove a lower bound for groups $\mathbb{F}_p^d \rtimes Q$ given by Lemma 3. We consider inputs in whose product the Q coordinates cancel out and we obtain a vector $\in \mathbb{F}_p^d$. Define the distribution D over input matrices as follows. We divide the columns in adjacent blocks of 2. The blocks

are i.i.d., so it suffices to describe one block:

$$\begin{array}{cc} g^{x_1} & g^{-x_1} \\ g^{x_2} & g^{-x_2} \\ \cdots & \cdots \\ g^{x_{k-1}} & g^{-x_{k-1}} \\ x_k \cdot v & 1 \end{array}$$

where $x_i \in [2]$ are uniform. Letting $s := \sum_{i<k} x_i \in \mathbb{N}$ the IM of this block is

$$M^s(x_k \cdot v) \cdot g^s \cdot g^{-s} = M^s(x_k \cdot v) \in \mathbb{F}_p^d.$$

We will show that for any efficient protocol π

$$|\mathbb{E}_D e[\pi(D) - \mathrm{IM}(D)]| < 1$$

where $e(v)$ is a character of $\mathbb{F}_p^d$ to be determined. In fact, it suffices that e is a character of a single coordinate, i.e., $e(v_1, v_2, \ldots, v_d) := e^{2\pi\sqrt{-1}v_i/p}$ for $i = c_{G,k}$.

As in [VW08], for a protocol π with communication $\leq b$ we can bound

$$|\mathbb{E}_D e[\pi(D) - \mathrm{IM}(D)]| \leq 2^b \cdot |e(\mathrm{IM})|_\square$$

where for $f : ([2]^n)^k \to \mathbb{C}$ the *box norm* $|f|_\square$ of f is defined as

$$|f|_\square := \left| \mathbb{E}_{\substack{x_1^0, x_1^1 \in [2]^n \\ \vdots \\ x_k^0, x_k^1 \in [2]^n}} \left[\prod_{\epsilon_1, \epsilon_2, \ldots, \epsilon_k \in [2]} f\left(x_1^{\epsilon_1}, \ldots, x_k^{\epsilon_k}\right)^{(-1)^{\epsilon_1 + \cdots + \epsilon_k}} \right] \right|^{1/2^k}.$$

If f can be written as a product

$$f(y_1 z_1, \cdots, y_k z_k) = f(y_1, \cdots, y_k) \cdot f(z_1, \cdots, z_k)$$

then the box norm multiplies (cf [VW08]). So it suffices to prove that the box norm of a block is < 1. We have

$$|M^s(x_k \cdot v)|_\square^{2^k} = \left| \mathbb{E}_{\substack{x_1^0, x_1^1 \in [2]^n \\ \vdots \\ x_k^0, x_k^1 \in [2]^n}} \left[\prod_{\epsilon_1, \epsilon_2, \ldots, \epsilon_k \in [2]} e(M^{\sum_{i<k} x_i^{\epsilon_i}} x_k^{\epsilon_k} v)^{(-1)^{\epsilon_1 + \cdots + \epsilon_k}} \right] \right| = \left| \mathbb{E} e \left(\sum_{\epsilon_1, \epsilon_2, \ldots, \epsilon_k \in [2]} (-1)^{\epsilon_1 + \cdots + \epsilon_k} M^{\sum_{i<k} x} \right. \right.$$

Let $S \in \mathbb{F}_p^d$ be the sum over $\epsilon_1, \epsilon_2, \ldots, \epsilon_k \in [2]$. When $x_k^0 = x_k^1 = 0$ we have $S = 0 \in \mathbb{F}_p^d$, and so the expectation is 1. Now suppose $x_i^b = b$ for every $i = 1..k$ and $b \in [2]$. Then $\sum_{i<k} x_i^{\epsilon_i} = \sum_{i<k} \epsilon_i$ and

$$S = \left(\sum_{\epsilon_1, \epsilon_2, \ldots, \epsilon_{k-1} \in [2]} (-M)^{\sum_{i<k} \epsilon_i} \right) (-v) = -(I - M)^{k-1} v.$$

Let v be any non-zero vector. Then $(I-M)v \neq 0$ as well, for else $Mv = v$, contradicting Lemma 3. Iterating, it follows that $S = -(I-M)^{k-1}v \neq 0$. Hence there is a coordinate i such that $S_i \neq 0$. We pick the corresponding character $e(v) := e^{2\pi\sqrt{-1}v_i/p}$. In this case the expectation is a non-trivial root of unity. It follows that $|M^s(x_k \cdot v)|_{\square}^{2^k} \leq 1 - 1/c^k$.

Proof of Lemma 3. Let H be a smallest non-nilpotent subgroup of G. Schmidt's theorem [Sch24], Theorem 9.1.9 in [Rob96], shows that H is the (internal) semi-direct product of a normal p-group P and a cyclic q-group Q, for different primes p and q. Recall that the action of $q \in Q$ on $p \in P$ is via conjugation qpq^{-1}. This is true in every internal semi-direct product, because $qp = qpq^{-1}q$.

Let $N := \Phi(P)$ be the Frattini subgroup [Fra85] of P, i.e., the intersection of all maximal subgroups of P. We recall that $\Phi(P)$ is preserved under every automorphism of P. This is because automorphisms permute maximal subgroups, so the intersection does not change. It follows that $\Phi(P)$ is normal in P, because conjugation by any $x \in P$ is an automorphism. Moreover, N is also normal in H. To verify this, let $x \in P$ and $y \in Q$ and note

$$xy\Phi(P)y^{-1}x^{-1} = x\left(y\Phi(P)y^{-1}\right)x^{-1} = x\Phi(P)x^{-1} = \Phi(P).$$

Because N is normal in H we can consider the group H/N.

We have $P/\Phi(P) = \mathbb{F}_p^d$, for some d. This appears in [Rob96], proof of Theorem 5.3.2, or [DF04], Exercise 25 of Section 6.1. Hence $H/N = \mathbb{F}_p^d \rtimes Q$. The actions on $\mathbb{F}_p^d$ are linear. Let M be the matrix corresponding to a generator g of Q. Finally, we have to verify that the action of g on $\mathbb{F}_p^d$ has no fixed points. Suppose g maps a coset $v = p\Phi(P)$ on itself. The coset has size $|\Phi(P)|$, which is a power of p. Consider the orbit of $x \in p\Phi(P)$ under Q. Because Q is a q-group, by the orbit-stabilizer theorem the size of each orbit is a power of q. Because p and q and different primes, some orbit must have size 1. So there is $x \in p\Phi(P)$ such that $gxg^{-1} = x$. This means x is an element that commutes with Q. We prove next that this implies $x \in \Phi(P)$. But then the coset is the trivial coset $\Phi(P)$ and so v is zero, as desired.

There remains to prove that if x commutes with Q then $x \in \Phi(P)$. Suppose not. Consider the set S of maximal subgroups of P which do not contain x. There is at least one such subgroup R since $x \notin \Phi(P)$. Note that since x commutes with Q, the action by Q preserves the set of maximal subgroups not containing x. Indeed, if R does not contain x and gRg^{-1} contained x, then R would contain $g^{-1}xg = x$, contradiction. So we can view Q as acting on S. We apply again the orbit-stabilizer theorem, obtaining that the size of the orbits is a power of q. We claim below that $|S| = p^{d-1}$. Because p and q are different primes, like before there must be an orbit of size 1. This means there is a maximal subgroup R of P not containing x s.t. $gRg^{-1} = R$. From this it follows that RQ is a subgroup of PQ. It is proper because it doesn't contain x. Since H is a smallest non-nilpotent group, RQ is nilpotent. But then R commutes with Q. But recall x also commutes with Q by assumption. Since R is maximal and x is not in R, P is generated by R and x. (If not, the generated group lies strictly between R and P, contradicting maximality.) But then P and Q commute, so H is nilpotent, contradiction.

Finally, we prove that $|S| = p^{d-1}$. Because by definition maximal subgroups of P contain $\Phi(P)$, by the fourth isomorphism theorem, a.k.a. the lattice isomorphism theorem, the maximal subgroups of P are in bijective correspondence with maximal subgroups of $V = P/\Phi(P)$

via the natural map $x \to x\Phi(P)$, see [DF04], Exercise 26, Section 6.1. The maximal subgroups of V are hyperplanes, i.e., sets of vectors v with inner product $\langle v, a\rangle = 0$ for some non-zero a. Similarly, the maximal subgroups of P that do not contain x are hyperplanes that avoid the vector $x\Phi(P)$, i.e., $\langle x\Phi(P), a\rangle \neq 0$. There are p^d total choices of a, and p^{d-1} choices of a s.t. $\langle x\Phi(P), a\rangle = 0$. Vectors a which are multiple of each other give the same hyperplane, so

$$|S| = \frac{p^d - p^{d-1}}{p-1} = p^{d-1},$$

as claimed. □

References

[BGL06] Nayantara Bhatnagar, Parikshit Gopalan, and Richard J. Lipton. Symmetric polynomials over Z_m and simultaneous communication protocols. *J. of Computer and System Sciences*, 72(2):252–285, 2006.

[BNS92] László Babai, Noam Nisan, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. of Computer and System Sciences*, 45(2):204–232, 1992.

[CFL83] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *15th ACM Symp. on the Theory of Computing (STOC)*, pages 94–99, 1983.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, 3rd edition, 2004.

[DLV24] Harm Derksen, Chin Ho Lee, and Emanuele Viola. Boosting uniformity in quasirandom groups: fast and simple. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2024.

[DV23] Harm Derksen and Emanuele Viola. Quasirandom groups enjoy interleaved mixing. *Discrete Analysis*, 2023.

[Fra85] Giovanni Frattini. Intorno alla generazione dei gruppi di operazioni. *Rendiconti della Reale Accademia dei Lincei*, 1:281–285, 1885.

[Gow08] W. T. Gowers. Quasirandom groups. *Combinatorics, Probability & Computing*, 17(3):363–387, 2008.

[GV15] W. T. Gowers and Emanuele Viola. The communication complexity of interleaved group products. In *ACM Symp. on the Theory of Computing (STOC)*, 2015.

[GV19] W. T. Gowers and Emanuele Viola. Interleaved group products. *SIAM J. on Computing*, 48(3):554–580, 2019. Special issue of FOCS 2016.

[GV22] W. T. Gowers and Emanuele Viola. Mixing in non-quasirandom groups. In *ACM Innovations in Theoretical Computer Science conf. (ITCS)*, 2022.

[HG91] Johan Håstad and Mikael Goldmann. On the power of small-depth threshold circuits. *Computational Complexity*, 1(2):113–129, 1991.

[LV25] Chin Ho Lee and Emanuele Viola. Pseudorandom bits for non-commutative programs. In *Conf. on Computational Complexity (CCC)*, 2025.

[Mix89] David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *J. of Computer and System Sciences*, 38(1):150–164, 1989.

[MV13] Eric Miles and Emanuele Viola. Shielding circuits with groups. In *ACM Symp. on the Theory of Computing (STOC)*, 2013.

[PT01] Pierre Péladeau and Denis Thérien. On the languages recognized by nilpotent groups (a translation of "sur les langages reconnus par des groupes nilpotents"). *Electron. Colloquium Comput. Complex.*, TR01-040, 2001.

[Rob96] Derek J. S. Robinson. *A Course in the Theory of Groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2 edition, 1996.

[Sch24] O. Yu. Schmidt. Groups all of whose subgroups are nilpotent. *Mat. Sbornik*, 31:366–372, 1924.

[Sha16] Aner Shalev. Mixing, communication complexity and conjectures of Gowers and Viola. *Combinatorics, Probability and Computing*, pages 1–13, 6 2016. arXiv:1601.00795.

[Vio19] Emanuele Viola. Non-abelian combinatorics and communication complexity. *SIGACT News, Complexity Theory Column*, 50(3), 2019.

[VW08] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for polynomials and protocols. *Theory of Computing*, 4:137–168, 2008.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il