



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

ARCHIVIO ISTITUZIONALE
DELLA RICERCA

Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

COMMUTING PROBABILITY FOR APPROXIMATE SUBGROUPS OF A FINITE GROUP

This is the final peer-reviewed author's accepted manuscript (postprint) of the following publication:

Published Version:

Detomi, E., Morigi, M., Shumyatsky, P. (2024). COMMUTING PROBABILITY FOR APPROXIMATE SUBGROUPS OF A FINITE GROUP. QUARTERLY JOURNAL OF MATHEMATICS, 75(2), 507-520 [10.1093/qmath/haae021].

Availability:

This version is available at: <https://hdl.handle.net/11585/981020> since: 2024-09-04

Published:

DOI: <http://doi.org/10.1093/qmath/haae021>

Terms of use:

Some rights reserved. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

This item was downloaded from IRIS Università di Bologna (<https://cris.unibo.it/>).
When citing, please refer to the published version.

(Article begins on next page)

Commuting probability for approximate subgroups of a finite group

Eloisa Detomi, Marta Morigi, and Pavel Shumyatsky

ABSTRACT. For subsets X, Y of a finite group G , we write $\Pr(X, Y)$ for the probability that two random elements $x \in X$ and $y \in Y$ commute. This paper addresses the relation between the structure of an approximate subgroup $A \subseteq G$ and the probabilities $\Pr(A, G)$ and $\Pr(A, A)$. The following results are obtained.

Theorem 1.1: Let A be a K -approximate subgroup of a finite group G , and let $\Pr(A, G) \geq \epsilon > 0$. There are two (ϵ, K) -bounded positive numbers γ and K_0 such that G contains a normal subgroup T and a K_0 -approximate subgroup B such that $|A \cap B| \geq \gamma \max\{|A|, |B|\}$ while the index $[G : T]$ and the order of the commutator subgroup $[T, \langle B \rangle]$ are (ϵ, K) -bounded.

Theorem 1.2: Let A be a K -approximate subgroup of a finite group G , and let $\Pr(A, A) \geq \epsilon > 0$. There are two (ϵ, K) -bounded positive numbers γ and s , and a subgroup $C \leq G$ such that $|C \cap A^2| > \gamma|A|$ and $|C'| \leq s$. In particular, A is contained in the union of at most $\gamma^{-1}K^2$ left cosets of the subgroup C .

It is also shown that the above results admit approximate converses.

1. Introduction

If G is a finite group and X, Y are subsets of G , we write $\Pr(X, Y)$ for the probability that two random elements $x \in X$ and $y \in Y$ commute. Thus,

$$\Pr(X, Y) = \frac{|\{(x, y) \in X \times Y \mid xy = yx\}|}{|X||Y|}.$$

2020 *Mathematics Subject Classification.* 20E45; 20P05; 20N99.

Key words and phrases. Commuting probability, approximate subgroups, conjugacy classes, centralizers.

The number $\Pr(G, G)$ is called the commuting probability of G . It is well-known that $\Pr(G, G) \leq 5/8$ for any nonabelian group G . Another important result is the theorem of P. M. Neumann [?] which states that if G is a finite group and ϵ is a positive number such that $\Pr(G, G) \geq \epsilon$, then G has a nilpotent normal subgroup R of nilpotency class at most 2 such that both the index $[G : R]$ and the order of the commutator subgroup $[R, R]$ are ϵ -bounded (see also [?]).

Throughout the article we use the expression “ (a, b, \dots) -bounded” to mean that a quantity is bounded from above by a number depending only on the parameters a, b, \dots .

There are several recent papers studying $\Pr(H, G)$, where H is a subgroup of G (see for example [?, ?, ?]). In particular, it was proved in [?, Proposition 1.2] that if H is a subgroup of a finite group G and $\Pr(H, G) \geq \epsilon > 0$, then there is a normal subgroup $T \leq G$ and a subgroup $B \leq H$ such that the indices $[G : T]$ and $[H : B]$, and the order of the commutator subgroup $[T, B]$ are ϵ -bounded.

Lately there also has been a considerable interest in studying approximate subgroups of finite groups.

Let K be a positive real number. A subset A of a finite group G is said to be a K -approximate subgroup of G , or simply a K -approximate group, if A contains 1 and the inverse of each of its elements, and if there exists $E \subseteq G$ with $|E| \leq K$ such that $A^2 \subseteq EA$.

Here and throughout, given a positive integer j and a subset X of a group G , we write X^j for the set of all products $x_1 \dots x_j$, where $x_i \in X$. The definition of approximate subgroups was introduced by Tao in [?]. Since then many important results on the subject have been established. In particular, Breuillard, Green and Tao essentially described the structure of finite approximate subgroups [?]. The reader is referred to the book [?] for detailed information on these developments.

In the present paper we examine the relation between the structure of an approximate subgroup and the commuting probability. Using the well known analogy between approximate groups and groups, we aim at extending the above mentioned group-theoretical results to approximate subgroups. On the one side, we employ the group-theoretical machinery already available, and, on the other side, ad hoc techniques for approximate subgroups.

Proposition 1.2 in [?] says, roughly speaking, that a subgroup H of a finite group G has many commuting elements with G if and only if H has a large subgroup which almost commutes with a large normal subgroup of G . Replacing H with an approximate subgroup A we obtain that A has many commuting elements with G if and only if it is commensurate with another approximate subgroup B which generates

a subgroup H of G with the same properties as in the aforementioned proposition. More formally, our result is as follows.

Theorem 1.1. *Let A be a K -approximate subgroup of a finite group G , and let $\Pr(A, G) \geq \epsilon > 0$. There are two (ϵ, K) -bounded positive numbers γ and K_0 such that G contains a normal subgroup T and a K_0 -approximate subgroup B such that*

- (i) $|A \cap B| \geq \gamma \max\{|A|, |B|\}$, and
- (ii) the index $[G : T]$ and the order of the subgroup $[T, \langle B \rangle]$ are both (ϵ, K) -bounded.

Throughout, $\langle X \rangle$ denotes the subgroup generated by a subset X of a group.

Next, we study approximate subgroups A such that $\Pr(A, A) \geq \epsilon > 0$. Roughly speaking, Neumann's theorem says that if a finite group has many commuting elements then it has a large subgroup which is almost abelian, in the sense that it has a small commutator subgroup. It turns out that if A is an approximate subgroup with many commuting elements then a big part of A^2 is contained in a subgroup C with small commutator subgroup, and A itself is contained in boundedly many cosets of C .

Theorem 1.2. *Let A be a K -approximate subgroup of a finite group G and assume that $\Pr(A, A) \geq \epsilon > 0$. There are two (ϵ, K) -bounded positive numbers γ and s , and a subgroup $C \leq G$ such that*

- (i) $|C \cap A^2| > \gamma|A|$, and
- (ii) the commutator subgroup of C is of order at most s .

Moreover A is contained in the union of at most $\gamma^{-1}K^2$ left cosets of the group C .

Furthermore, we show that each of the above theorems admits an "approximate" converse.

Proposition 1.3. *Let A, B be subsets and T a subgroup of a finite group G . Set $\gamma = |A \cap B|/|A|$, $n = [G : T]$ and $m = |[T, \langle B \rangle]|$. Then $\Pr(A, G) \geq \frac{\gamma}{nm}$.*

Proposition 1.4. *Let A be a K -approximate subgroup of a finite group G , and let $C \leq G$ be a subgroup. Set $\gamma = |C \cap A^2|/|A|$ and $s = |C'|$. Then*

$$\Pr(A^2, A^2) \geq \frac{\gamma^2}{K^4 s}.$$

Note that some properties of the commuting probability of subgroups cannot be extended verbatim to approximate subgroups but

they do hold when replacing an approximate subgroup A with A^2 (compare Proposition ?? and Example ??). Clearly, A^2 is a K^2 -approximate subgroup, whenever A is a K -approximate subgroup (if $A^2 \subseteq EA$, then $A^4 \subseteq EA^3 \subseteq E^2A^2$).

The next section contains some general comments on the commuting probabilities. In Section 3 we prove Theorems ?? and ?. The last section is devoted to Propositions ?? and ?.

2. General comments on commuting probabilities

Note that if X, Y are subsets of a finite group G , we have

$$\Pr(X, Y) = \frac{1}{|Y|} \sum_{y \in Y} \frac{|C_X(y)|}{|X|} = \frac{1}{|X|} \sum_{x \in X} \frac{|C_Y(x)|}{|Y|}.$$

It was proved in [?, Lemma 2.3] that if K and N are subgroups of a finite group G , with N normal in G , then

$$\Pr(K, G) \leq \Pr(KN/N, G/N) \Pr(N \cap K, N).$$

We are interested in finding an ‘‘approximate’’ variant of this result. We start by looking at symmetric subsets.

Proposition 2.1. *Let G be a finite group, N a normal subgroup of G , and assume that A is a symmetric subset of G . Then*

$$\Pr(A, G) \leq \frac{|A^5|}{|A|} \Pr\left(\frac{AN}{N}, \frac{G}{N}\right) \Pr(A^4 \cap N, N).$$

PROOF. Let $\bar{G} = G/N$ and $\bar{A} = \{hN \mid h \in A\} = \{h_1N, \dots, h_rN\}$. Note that A is contained in the union of the subsets $h_i(N \cap A^2)$, for $i = 1, \dots, r$. Indeed, $A \subseteq \bigcup_i h_iN$ and if $a \in h_iN$, then $h_i^{-1}a = n$ for some $n \in N \cap A^2$ and so $a = h_in \in h_i(N \cap A^2)$. Therefore

$$\begin{aligned} |A| |G| \Pr(A, G) &= \sum_{x \in A} |C_G(x)| \leq \sum_{hN \in \bar{A}} \left(\sum_{x \in h(N \cap A^2)} \frac{|NC_G(x)|}{|N|} |C_N(x)| \right) \\ &\leq \sum_{hN \in \bar{A}} \left(\sum_{x \in h(N \cap A^2)} |C_{\bar{G}}(hN)| |C_N(x)| \right) \\ &= \sum_{hN \in \bar{A}} |C_{\bar{G}}(hN)| \left(\sum_{x \in h(N \cap A^2)} |C_N(x)| \right) \\ &= \sum_{hN \in \bar{A}} |C_{\bar{G}}(hN)| \left(\sum_{y \in N} |C_{h(N \cap A^2)}(y)| \right). \end{aligned}$$

If $C_{h(N \cap A^2)}(y) \neq \emptyset$ take $y_0 \in h(N \cap A^2) \cap C_G(y)$ and observe that $h(N \cap A^2) \subseteq y_0(N \cap A^4)$. Indeed, $y_0 = hu$ with $u \in N \cap A^2$, whence $h = y_0u^{-1}$ and $h(N \cap A^2) \subseteq y_0u^{-1}(N \cap A^2) \subseteq y_0(N \cap A^4)$. Therefore

$$\begin{aligned} C_{h(N \cap A^2)}(y) &= h(N \cap A^2) \cap C_G(y) \\ &\subseteq y_0 C_{N \cap A^4}(y), \end{aligned}$$

whence $|C_{h(N \cap A^2)}(y)| \leq |C_{N \cap A^4}(y)|$. It follows that

$$\begin{aligned} |A| |G| \Pr(A, G) &\leq \left(\sum_{hN \in \bar{A}} |C_{\bar{G}}(hN)| \right) \left(\sum_{y \in N} |C_{N \cap A^4}(y)| \right) \\ &= \left(|\bar{A}| |\bar{G}| \Pr(\bar{A}, \bar{G}) \right) \left(|N| |N \cap A^4| \Pr(N \cap A^4, N) \right). \end{aligned}$$

Thus

$$\Pr(A, G) \leq \frac{|\bar{A}| |N \cap A^4|}{|A|} \Pr(\bar{A}, \bar{G}) \Pr(N \cap A^4, N).$$

As $|\bar{A}| |N \cap A^4| \leq |A|^5$ by [?, Lemma 2.6.3], the result follows. \square

The previous proposition says, in particular, that in a homomorphic image \bar{G} of G the commuting probability of \bar{A} in \bar{G} is controlled in terms of $\Pr(A, G)$. The next lemma deals with the commuting probability $\Pr(\bar{A}, \bar{A})$.

Proposition 2.2. *Let G be a finite group, N a normal subgroup of G , and assume that A is a symmetric subset of G . Then*

$$\Pr(A, A) \leq \frac{|A^3| |A^5|}{|A|^2} \Pr\left(\frac{AN}{N}, \frac{AN}{N}\right) \Pr(A^4 \cap N, A^2 \cap N).$$

PROOF. The proof is very similar to the proof of Proposition ???. Thus we will sketch it, avoiding repetitions. Let $\bar{G} = G/N$ and $\bar{A} = \{hN \mid h \in A\} = \{h_1N, \dots, h_rN\}$. As shown in Proposition ??, A is contained in the union of the subsets $h_i(N \cap A^2)$, for $i = 1, \dots, r$. Moreover, for $x \in A$,

$$C_A(x) \subseteq \bigcup_{hN \in C_{\bar{A}}(xN/N)} h C_{N \cap A^2}(x),$$

since, for $a, h \in C_A(x)$, the equality $aN = hN$ implies $h^{-1}a \in N \cap A^2$. Therefore, as $C_A(x)N/N \subseteq C_{\bar{A}}(xN)$, we have

$$(1) \quad |C_A(x)| \leq |C_{\bar{A}}(xN)| |C_{N \cap A^2}(x)|.$$

It follows that

$$\begin{aligned}
|A| |A| \Pr(A, A) &= \sum_{x \in A} |C_A(x)| \leq \sum_{hN \in \bar{A}} \left(\sum_{x \in h(N \cap A^2)} |C_A(x)| \right) \\
&\leq \sum_{hN \in \bar{A}} \left(\sum_{x \in h(N \cap A^2)} |C_{\bar{A}}(hN)| |C_{N \cap A^2}(x)| \right) \\
&= \sum_{hN \in \bar{A}} |C_{\bar{A}}(hN)| \left(\sum_{x \in h(N \cap A^2)} |C_{N \cap A^2}(x)| \right) \\
&= \sum_{hN \in \bar{A}} |C_{\bar{A}}(hN)| \left(\sum_{y \in N \cap A^2} |C_{h(N \cap A^2)}(y)| \right).
\end{aligned}$$

As in the proof of Proposition ??, the inequality $|C_{h(N \cap A^2)}(y)| \leq |C_{N \cap A^4}(y)|$ holds for every $h \in A$. Therefore

$$\begin{aligned}
|A| |A| \Pr(A, A) &\leq \left(\sum_{hN \in \bar{A}} |C_{\bar{A}}(hN)| \right) \left(\sum_{y \in N \cap A^2} |C_{N \cap A^4}(y)| \right) \\
&= \left(|\bar{A}| |\bar{A}| \Pr(\bar{A}, \bar{A}) \right) \left(|N \cap A^2| |N \cap A^4| \Pr(N \cap A^4, N \cap A^2) \right).
\end{aligned}$$

Thus

$$\Pr(A, A) \leq \frac{|\bar{A}|^2 |N \cap A^4| |N \cap A^2|}{|A|^2} \Pr(\bar{A}, \bar{A}) \Pr(N \cap A^4, N \cap A^2).$$

As $|\bar{A}| |N \cap A^4| \leq |A|^5$ and $|\bar{A}| |N \cap A^2| \leq |A|^3$ by [?, Lemma 2.6.3], the result follows. \square

As $|A^n|/|A| \leq K^{n-1}$ for any K -approximate subgroup A and for every integer $n \geq 2$, the following corollary is a straightforward consequence of the above propositions.

Corollary 2.3. *Let G be a finite group, N a normal subgroup of G , and assume that $A \subseteq G$ is a K -approximate subgroup. Then*

- $\Pr(A, G) \leq K^4 \Pr(AN/N, G/N) \Pr(A^4 \cap N, N)$,
- $\Pr(A, A) \leq K^6 \Pr(AN/N, AN/N) \Pr(A^4 \cap N, A^2 \cap N)$.

In particular,

- $\Pr(AN/N, G/N) \geq (1/K^4) \Pr(A, G)$,
- $\Pr(AN/N, AN/N) \geq (1/K^6) \Pr(A, A)$.

More generally, the above corollary holds in the case where A is a symmetric set containing 1 which has small tripling, i.e. $|A^3| \leq T|A|$. To see this, observe that $|A^5| \leq T^3|A|$ by [?, Proposition 2.5.3].

If $H_1 \leq H_2$ are subgroups of a finite group G , then

$$(2) \quad \Pr(H_1, G) \geq \Pr(H_2, G)$$

(see [?, Theorem 3.7]).

As we will show in Example ??, the above inequality does not hold if H_1, H_2 are K -approximate subgroups. Indeed, if H_1 is a K -approximate subgroup contained in H_2 , then $\Pr(H_1, G)$ might be arbitrarily small compared to $\Pr(H_2, G)$ (even if H_2 is a subgroup). We will show however that $\Pr(H_1^2, G)$ is bounded away from zero (see Proposition ??). In the particular case where H_1 is a subgroup of G and H_2 is a K -approximate subgroup containing H_1 , we get

$$\Pr(H_1, G) \geq \frac{1}{K} \Pr(H_2, G)$$

(see Corollary ??).

To prove these results, we need a preliminary elementary lemma.

Lemma 2.4. *Assume that G is a finite group, $g \in G$ and A is a symmetric subset of G . Then*

- (a) $|C_A(g)| |g^A| \leq |A^2|$.
- (b) $|A| \leq |C_{A^2}(g)| |g^A|$.

PROOF. Note that if $g^A = \{g^{a_1}, \dots, g^{a_r}\}$, then the subsets $C_A(g)a_i$, for $i = 1, \dots, r$, are pairwise disjoint subsets of A^2 , so

$$|C_A(g)| |g^A| = \left| \bigcup_{1 \leq i \leq r} C_A(g)a_i \right| \leq |A^2|,$$

and (a) holds.

To prove (b), observe that whenever $a, b \in A$ are such that $g^a = g^b$, we have $ab^{-1} \in C_G(g) \cap A^2 = C_{A^2}(g)$. \square

The following result holds for approximate subgroups.

Lemma 2.5. *Assume that G is a finite group, $g \in G$ and $A \subseteq G$ is a K -approximate subgroup. Then $|g^{A^n}| \leq K^{n-1}|g^A|$ for every $n \geq 1$.*

PROOF. As $A^2 \subseteq EA$ where $|E| \leq K$, we have $A^n \subseteq E^{n-1}A$. Since A is symmetric, every element $h \in A^n$ can be written as the inverse of an element $ea \in A^n \subseteq E^{n-1}A$, with $e \in E^{n-1}$ and $a \in A$. So

$$g^h = g^{(ea)^{-1}} = (g^{a^{-1}})^{e^{-1}},$$

and since there are at most K^{n-1} elements in E^{n-1} , we deduce that $|g^{A^n}| \leq K^{n-1}|g^A|$. \square

Proposition 2.6. *Let G be a finite group, and let $A_1 \subseteq A_2$ be symmetric subsets of G such that $|A_1^2| \leq K|A_1|$ and $|A_2^2| \leq K'|A_2|$. Then for any subset $B \subseteq G$ we have*

$$\Pr(A_1^2, B) \geq \frac{1}{KK'} \Pr(A_2, B).$$

PROOF. Let $g \in G$. As $|A_1^2| \leq K|A_1|$, it follows from Lemma ?? (b) that

$$\frac{|C_{A_1^2}(g)|}{|A_1^2|} \geq \frac{1}{K|g^{A_1}|}.$$

Clearly, as $A_1 \subseteq A_2$, we have $1/|g^{A_1}| \geq 1/|g^{A_2}|$. Moreover, as $|A_2^2| \leq K'|A_2|$, we deduce from Lemma ?? (a) that

$$\frac{1}{|g^{A_2}|} \geq \frac{|C_{A_2}(g)|}{K'|A_2|}.$$

Therefore

$$\frac{|C_{A_1^2}(g)|}{|A_1^2|} \geq \frac{1}{K|g^{A_1}|} \geq \frac{1}{K|g^{A_2}|} \geq \frac{|C_{A_2}(g)|}{KK'|A_2|}.$$

We conclude that

$$\Pr(A_1^2, B) = \frac{1}{|B|} \sum_{g \in B} \frac{|C_{A_1^2}(g)|}{|A_1^2|} \geq \frac{1}{KK'|B|} \sum_{g \in B} \frac{|C_{A_2}(g)|}{|A_2|} = \frac{1}{KK'} \Pr(A_2, B),$$

as claimed. \square

Corollary 2.7. *Let G be a finite group, and let H be a subgroup contained in a K -approximate subgroup $A \subseteq G$. Then for any subset $B \subseteq G$ we have*

$$\Pr(H, B) \geq \frac{1}{K} \Pr(A, B).$$

PROOF. The result is a straightforward consequence of the previous lemma, taking into account that H is a 1-approximate subgroup and $H^2 = H$. \square

Example 2.8. Here we show that for any positive integer $K \geq 2$ and $\epsilon > 0$ there is a finite group G with a subgroup H and a K -approximate subgroup $A \subseteq H$ of size at least $K|H|/2^K$ such that $\Pr(A, G) \leq \epsilon \Pr(H, G)$. In particular, $\Pr(A, G)/\Pr(H, G)$ cannot be bounded away from zero in terms of $|A|/|H|$ and K .

Let V be an elementary abelian 2-group of rank $n \geq K$, and let g_1, \dots, g_n be a basis of V . Denote by g the automorphism of V which

cyclically permutes g_1, \dots, g_n . Consider the natural semi-direct product $N = V\langle g \rangle$ and let $G = N \times U$, where U is a finite abelian group. Then $Z = Z(G) = \langle g_1 g_2 \cdots g_n \rangle \times U$. Set $z = |Z| = 2|U|$ and note that

$$|G| = n2^n|U| = n2^{n-1}z.$$

Let $k = K - 1$ and set

$$A = \bigcup_{1 \leq i \leq k} g_i Z \cup \{1\} \quad \text{and} \quad H = \langle A \rangle = \langle g_1, \dots, g_k \rangle Z.$$

Note that A is symmetric because the g_i have order 2, moreover $A^2 \subseteq BA$, where $B = \{1, g_1, \dots, g_k\}$ has size $k + 1 = K$, so A is a K -approximate subgroup. Moreover, as $k < n$, we have

$$|A| = kz + 1, \quad |H| = 2^k z, \quad \frac{|A|}{|H|} = \frac{kz + 1}{2^k z} > \frac{k}{2^k}.$$

Since $|a^G| = n$ for every $1 \neq a \in A$, we have

$$\begin{aligned} \Pr(A, G) &= \frac{1}{|A|} \sum_{a \in A} \frac{|C_G(a)|}{|G|} = \frac{1}{|A|} \left(\sum_{1 \neq a \in A} \frac{|C_G(a)|}{|G|} + \frac{|C_G(1)|}{|G|} \right) \\ &= \frac{1}{|A|} \left(\frac{|A| - 1}{n} + 1 \right) = \frac{1}{kz + 1} \left(\frac{kz}{n} + 1 \right) < \frac{kz + n}{kzn}. \end{aligned}$$

As H is contained in VU , which is an abelian subgroup of index n in G , whenever $x \in H$ we have $[G : C_G(x)] \leq n$. So we can estimate $\Pr(H, G)$ as follows:

$$\begin{aligned} \Pr(H, G) &= \frac{1}{|H|} \sum_{x \in H} \frac{|C_G(x)|}{|G|} = \frac{1}{|H|} \left(\sum_{x \in H \setminus Z} \frac{|C_G(x)|}{|G|} + \sum_{x \in Z} \frac{|C_G(x)|}{|G|} \right) \\ &\geq \frac{1}{|H|} \left(\frac{|H| - z}{n} + z \right) = \frac{1}{2^k z} \left(\frac{2^k z - z + nz}{n} \right) \\ &> \frac{1}{2^k z} \left(\frac{nz}{n} \right) = \frac{1}{2^k}. \end{aligned}$$

Therefore

$$\frac{\Pr(A, G)}{\Pr(H, G)} < \frac{kz + n}{kzn} 2^k = \left(\frac{1}{n} + \frac{1}{kz} \right) 2^k.$$

This can be arbitrarily small if n and $|U|$ are chosen large enough.

Example 2.9. In the previous example A was quite small compared to the subgroup $H = \langle A \rangle$, as $|A|/|H| = (kz + 1)/(2^k z) < (k + 1)/2^k$. Now we show that, in the notation of the previous example, we can choose G , A , and a K -approximate subgroup $A_0 \subseteq G$ containing A ,

such that $|A|/|A_0| > k/(k+1)$ and $\Pr(A, G) \leq \Pr(A_0, G)$. Moreover the value of

$$\Pr(A, G)/\Pr(A_0, G)$$

cannot be bounded away from zero in terms of $|A|/|A_0|$ and K .

Let G, A, Z be as in Example ?? and let $A_0 = Z \cup A$. Note that $A^2 \subseteq BA$ and $A_0^2 \subseteq BA_0$, where $B = \{1, g_1, \dots, g_k\}$, so both A and A_0 are K -approximate subgroups.

Note that $|A| = kz + 1$ and $|A_0| = (k+1)z$, where $z = |Z|$, and so $|A|/|A_0| = (kz+1)/(k+1)z > k/(k+1)$. We know from the calculations in Example ?? that

$$\Pr(A, G) < \frac{kz + n}{kzn} = \frac{1}{n} + \frac{1}{kz}.$$

Moreover, as $A_0 = A \cup Z$ and $|C_G(y)|/|G| \geq \frac{1}{n}$ for every $y \in A$ (see Example ??),

$$\begin{aligned} \Pr(A_0, G) &= \frac{1}{|A_0|} \left(\sum_{y \in Z} \frac{|C_G(y)|}{|G|} + \sum_{1 \neq y \in A} \frac{|C_G(y)|}{|G|} \right) \\ &\geq \frac{1}{(k+1)z} \left(z + \frac{kz}{n} \right) \\ &> \frac{1}{k+1}. \end{aligned}$$

Therefore

$$(3) \quad \frac{\Pr(A, G)}{\Pr(A_0, G)} < \left(\frac{1}{n} + \frac{1}{kz} \right) (k+1).$$

If k is fixed and the group G is chosen with n and $|U| = z/2$ arbitrary large, the righthand side of (??) becomes arbitrary small.

3. Proof of the main results

We start with two preliminary results, the first one being purely group theoretical.

Lemma 3.1. *Let $m \geq 1$, and let G be a finite group containing a subgroup B such that $[G : C_G(x)] \leq m$ for all $x \in B$. Then there is a normal subgroup $T \leq G$ such that the index $[G : T]$ and the order of the commutator subgroup $[T, B]$ are m -bounded.*

PROOF. Note that

$$\Pr(B, G) \geq \frac{1}{m}.$$

By Proposition 1.2 of [?] there exists a normal subgroup R of m -bounded index in G and a subgroup U of m -bounded index in B such that $[R, U]$ has m -bounded order. By Remark 2.6 in [?], the normal closure $[R, U]^G$ has m -bounded order.

Passing to the quotient over $[R, U]^G$, we can assume that $R \leq C_G(U)$. Take m -boundedly many elements b_1, \dots, b_r in B such that $B = \langle b_1, \dots, b_r, U \rangle$. Since $[G : C_G(b_i)] \leq m$ for every $i = 1, \dots, r$ and $C_G(U)$ has m -bounded index in G , the intersection C of $C_G(U)$ and all r subgroups $C_G(b_i)$ has m -bounded index in G . So C contains a normal subgroup T of G of m -bounded index with $[T, B] = 1$. This concludes the proof. \square

The following lemma tells us that if A is an approximate subgroup and g_1, \dots, g_s are elements of G having few A -conjugates, then any element of the subgroup $\langle g_1, \dots, g_s \rangle$ has few A -conjugates.

Lemma 3.2. *Let G be a finite group, A a K -approximate subgroup of G , and $g_1, \dots, g_s \in G$ elements such that $|g_i^A| \leq m$ for every $i = 1, \dots, s$. Then there exists a (K, m, s) -bounded integer u such that $|g^A| \leq u$ for every $g \in \langle g_1, \dots, g_s \rangle$.*

PROOF. It is sufficient to show that there exists a (K, m, s) -bounded integer u and elements $d_1, \dots, d_u \in G$ such that

$$(4) \quad A \subseteq \bigcup_{1 \leq i \leq u} C_{A^{2^s}}(g_1, \dots, g_s)d_i.$$

Use induction on s . Let $s = 1$ and $g_1^A = \{g_1^{a_1}, \dots, g_1^{a_m}\}$. If $a \in A$, then there exists k such that $g_1^a = g_1^{a_k}$, thus $aa_k^{-1} \in C_{A^2}(g_1)$ and $a = (aa_k^{-1})a_k$. Hence,

$$A \subseteq \bigcup_{1 \leq i \leq m} C_{A^2}(g_1)a_i,$$

as desired.

Now assume that the result is true for $s - 1$, that is, there are (K, m, s) -boundedly many elements $h_1, \dots, h_v \in G$ such that

$$A \subseteq \bigcup_{1 \leq i \leq v} C_{A^{2^{s-1}}}(g_1, \dots, g_{s-1})h_i.$$

Set $D = C_{A^{2^{s-1}}}(g_1, \dots, g_{s-1})$. Note that by Lemma ?? the size of the class g_s^D is (K, m, s) -bounded. Write

$$g_s^D = \{g_s^{b_1}, \dots, g_s^{b_r}\}$$

for suitable $b_1, \dots, b_r \in D$.

As above, it follows that $D \subseteq \bigcup_{1 \leq i \leq r} C_{D^2}(g_s)b_i$. In particular, we have

$$D \subseteq \bigcup_{1 \leq i \leq r} C_{D^2}(g_s)b_i \subseteq \bigcup_{1 \leq i \leq r} C_{A^{2s}}(g_1, \dots, g_s)b_i.$$

We know that $A \subseteq \bigcup_{1 \leq i \leq v} Dh_i$, whence (??) follows with $u = rv$. This establishes the lemma. \square

Built on the ideas of P. M. Neumann's theorem [?], we get the next proposition, which contains the core of the proofs of Theorem ?? and Theorem ??.

Proposition 3.3. *Let G be a finite group containing a K_1 -approximate subgroup H and a K_2 -approximate subgroup U such that $\Pr(H, U) \geq \epsilon > 0$. Then there exists a symmetric subset X of H , with $1 \in X$, and two positive numbers K_0 and m depending only on K_1, K_2 and ϵ such that*

- $|X| \geq \frac{\epsilon}{2}|H|$,
- X^2 is a K_0 -approximate subgroup of G ,
- $|X^2| \leq K_0|X|$,
- $|y^U| \leq m$ for every $y \in \langle X^2 \rangle$.

PROOF. Set

$$X = \{x \in H \mid |x^U| \leq 2K_2/\epsilon\} = \{x \in H \mid 1/|x^U| \geq \epsilon/(2K_2)\}.$$

As $|U^2| \leq K_2|U|$, from Lemma ?? (a) it follows that, for any $g \in H \setminus X$,

$$|C_U(g)| \leq \frac{K_2|U|}{|g^U|} \leq \frac{\epsilon K_2|U|}{2K_2} = \frac{\epsilon|U|}{2},$$

whence

$$\begin{aligned} \epsilon|H||U| &\leq |\{(x, y) \in H \times U \mid xy = yx\}| = \sum_{x \in H} |C_U(x)| \\ &\leq \sum_{x \in X} |U| + \sum_{x \in H \setminus X} \frac{\epsilon}{2}|U| \\ &\leq |X||U| + (|H| - |X|)\frac{\epsilon}{2}|U| \\ &\leq |X||U| + \frac{\epsilon}{2}|H||U|. \end{aligned}$$

Therefore $(\epsilon/2)|H| \leq |X|$, that is,

$$|X| \geq \alpha|H|$$

for $\alpha = \epsilon/2$. Thus,

$$|X^2| \leq |H^2| \leq K_1|H| \leq (K_1/\alpha)|X|$$

and also

$$|X^3| \leq |H^3| \leq K_1^2 |H| \leq (K_1^2/\alpha) |X|,$$

hence X has tripling K_1^2/α .

It follows that $B = X^2$ is a K_0 -approximate subgroup where K_0 depends on K_1 and α only (see Proposition 2.5.5 in [?]).

Note that $|y^U| \leq (K_2/\alpha)^2$ for every $y \in B$.

Let E be a minimal subset of G such that $B^2 \subseteq EB$ and $|E| \leq K_0$. By minimality of E , for every element $e \in E$ there are $b_1, b_2, b_3 \in B$ such that $b_1 b_2 = e b_3$ and so every element $e \in E$ can be written as a product of at most 3 elements of B . Therefore $|e^U| \leq (K_2/\alpha)^6$ for every $e \in E$.

It follows from Lemma ?? that there exists a (K_0, K_2, α) -bounded integer n such that $|g^U| \leq n$ for every $g \in \langle E \rangle$. Note that $B^i \leq \langle E \rangle B$ for every $i \geq 2$, and so there exists a (K_0, K_2, α) -bounded integer m such that $|y^U| \leq m$ for every $y \in \langle B \rangle$. As K_0 and α depend only on K_1 and ϵ , the proof is complete. \square

Now we are ready to proceed with the proof of our main results. For the reader's convenience we restate Theorem ?? here.

Theorem ??. *Let A be a K -approximate subgroup of a finite group G such that $\Pr(A, G) \geq \epsilon > 0$. There are two (ϵ, K) -bounded positive numbers γ and K_0 such that G contains a normal subgroup T and a K_0 -approximate subgroup B such that*

- (i) $|A \cap B| \geq \gamma \max\{|A|, |B|\}$, and
- (ii) the index $[G : T]$ and the order of the subgroup $[T, \langle B \rangle]$ are both (ϵ, K) -bounded.

PROOF. Apply Proposition ?? with $H = A$, $U = G$, $K_1 = K$ and $K_2 = 1$. Deduce that there exists a subset X of A and two (K, ϵ) -bounded numbers K_0 and m such that $B = X^2$ is a K_0 -approximate subgroup while $|B \cap A| \geq |X| \geq \frac{\epsilon}{2} |A|$ and $|y^G| \leq m$ for every $y \in \langle B \rangle$. Note also that

$$|B \cap A| \geq \frac{\epsilon}{2} |A| \geq \frac{\epsilon}{2K} |A^2| \geq \frac{\epsilon}{2K} |B|,$$

so we can take $\gamma = \epsilon/(2K)$.

It follows from Lemma ?? applied to the subgroup $\langle B \rangle$ that there exists a normal subgroup $T \leq G$ such that the index $[G : T]$ and the order of the commutator subgroup $[T, \langle B \rangle]$ are m -bounded. Since m is (K, ϵ) -bounded, the result follows. \square

We now deal with Theorem ??.

Theorem ??. *If A is a K -approximate subgroup of a finite group G satisfying $\Pr(A, A) \geq \epsilon > 0$, then there are two (ϵ, K) -bounded positive numbers γ and s , and a subgroup $C \leq G$ such that $|C \cap A^2| > \gamma|A|$ and $|C'| \leq s$. Moreover, A is contained in the union of at most $\gamma^{-1}K^2$ left cosets of the group C .*

PROOF. We apply Proposition ?? with $H = U = A$ and $K_1 = K_2 = K$ and deduce that there exists a subset X of A and two positive numbers K_0 and m depending only on K and ϵ such that $|X| \geq \frac{\epsilon}{2}|A|$, the set $B = X^2$ is a K_0 -approximate subgroup, and $|y^A| \leq m$ for every $y \in \langle B \rangle$.

As $|B^2| \leq K_0|B|$, it follows from Lemma ?? (b) that for every $y \in \langle B \rangle$ we have

$$|C_B(y)| \geq \frac{|B|}{K_0|y^X|} \geq \frac{|B|}{K_0|y^A|} \geq \eta|B|,$$

where $\eta = 1/(K_0m)$. Since

$$|C_B(y)| \geq \eta|B|,$$

for every $y \in \langle B \rangle$, we have

$$\Pr(B, \langle B \rangle) = \frac{1}{|\langle B \rangle|} \sum_{y \in \langle B \rangle} \frac{|C_B(y)|}{|B|} \geq \eta.$$

Now we apply Proposition ?? with $H = B$ and $U = \langle B \rangle$, where $K_1 = K_0$ and $K_2 = 1$, to deduce that there exists a symmetric subset Y of B and two positive numbers K_3 and n depending only on K_0 and η such that $|Y| \geq \frac{\eta}{2}|B|$ and Y^2 is a K_3 -approximate subgroup satisfying $|y^{\langle B \rangle}| \leq n$ for every $y \in \langle Y^2 \rangle$.

It follows from Theorem 1.1 in [?] that the commutator subgroup of the subgroup $\langle (Y^2)^{\langle B \rangle} \rangle$ has (K_3, n) -bounded order. As $\langle Y^2 \rangle = \langle Y \rangle$, we deduce that the order of the commutator subgroup of $\langle Y \rangle$ is (K_3, n) -bounded.

Taking into account that $Y \subseteq B = X^2 \subseteq A^2$, write

$$|A| \leq \frac{2}{\epsilon}|X| \leq \frac{2}{\epsilon}|X^2| \leq \frac{2}{\epsilon} \left(\frac{2}{\eta}|Y| \right),$$

and

$$(5) \quad |\langle Y \rangle \cap A^2| \geq |Y \cap A^2| = |Y| \geq \frac{\epsilon\eta}{4}|A| = \gamma|A|,$$

for $\gamma = \epsilon\eta/4$.

Finally, as

$$|AY| \leq |A^3| \leq K^2|A| \leq K^2 \frac{4}{\epsilon\eta} |Y|,$$

it follows from [?, Lemma 2.4.4] (Ruzsa's covering lemma) that there exists a subset $F \subseteq A$ with $|F| \leq 4K^2/(\epsilon\eta)$ such that $A \subseteq FY^2$. Therefore A is contained in the union of at most $4K^2/(\epsilon\eta)$ left cosets of $\langle Y \rangle$ (note that this follows also from (??) and Lemma 7.1.5 in [?]). \square

4. The converse statements

In this section we prove Proposition ?? and Proposition ??, which are roughly converse to Theorem ?? and Theorem ??, respectively.

We will also often use without mention the fact that if S, T are subsets of a finite group G and $g \in S$ then $|g^T| \leq |[S, T]|$, because the map $g^T \rightarrow \{[g, x] \mid x \in T\}$ defined by $g^x \mapsto g^{-1}g^x$ is a bijection.

Proposition ??. *Let A, B be subsets and T a subgroup of a finite group G . Set $\gamma = |A \cap B|/|A|$, $n = [G : T]$ and $m = |[T, \langle B \rangle]|$. Then $\Pr(A, G) \geq \frac{\gamma}{nm}$.*

PROOF. Note that

$$|A \cap \langle B \rangle| \geq |A \cap B| \geq \gamma|A|,$$

so $|A \cap \langle B \rangle|/|A| \geq \gamma$ and without loss of generality we can assume that B is a subgroup. Moreover, if $g \in A \cap B$, then

$$[G : C_G(g)] \leq [G : T] [T : C_T(G)] \leq nm,$$

since $|[T, \langle B \rangle]| = m$. Therefore

$$\begin{aligned} \Pr(A, G) &= \frac{1}{|A|} \sum_{a \in A} \frac{|C_G(a)|}{|G|} \geq \frac{1}{|A|} \sum_{g \in A \cap B} \frac{|C_G(g)|}{|G|} \\ &\geq \frac{|A \cap B|}{nm|A|} \geq \frac{\gamma}{nm}. \end{aligned}$$

\square

Proposition ??. *Let A be a K -approximate subgroup of a finite group G , and let $C \leq G$ be a subgroup. Set $\gamma = |C \cap A^2|/|A|$ and $s = |C'|$. Then*

$$\Pr(A^2, A^2) \geq \frac{\gamma^2}{K^4 s}.$$

PROOF. Since $|C \cap A^2| = \gamma|A|$, it follows from [?, Lemma 7.1.5] that A is contained in the union of $n \leq \gamma^{-1}K^2$ left cosets of C , say

$$A \subseteq \bigcup_{1 \leq i \leq n} f_i C.$$

As A is symmetric, for every $a \in A$ we have $a^{-1} \in \bigcup_i f_i C$, whence $a = (f_i c)^{-1} = c^{-1} f_i^{-1}$ for some $i \leq n$ and $c \in C$. It follows that

$$A \subseteq \bigcup_{1 \leq i \leq n} C f_i^{-1}.$$

Therefore, for every $g \in G$ we have

$$|g^A| \leq |g^{\bigcup_{1 \leq i \leq n} C f_i^{-1}}| \leq \sum_{i=1}^n |(g^C)^{f_i^{-1}}| = n|g^C|.$$

When $g \in C \cap A^2$ we also have $|g^C| \leq s$, since $|C'| = s$, hence

$$(6) \quad \frac{1}{|g^A|} \geq \frac{1}{ns}.$$

Moreover, by Lemma ?? (b), $|g^A| \geq |A|/|C_{A^2}(g)| \geq |A^2|/(K|C_{A^2}(g)|)$, which gives

$$(7) \quad \frac{|C_{A^2}(g)|}{|A^2|} \geq \frac{1}{K|g^A|}.$$

Now, by (??) and (??)

$$\begin{aligned} \Pr(A^2, A^2) &= \frac{1}{|A^2|} \sum_{a \in A^2} \frac{|C_{A^2}(a)|}{|A^2|} \geq \frac{1}{|A^2|} \sum_{g \in C \cap A^2} \frac{|C_{A^2}(g)|}{|A^2|} \\ &\geq \frac{1}{|A^2|} \sum_{g \in C \cap A^2} \frac{1}{K|g^A|} \\ &\geq \frac{|C \cap A^2|}{Kns|A^2|}. \end{aligned}$$

Moreover, as $|A^2| \leq K|A|$,

$$|C \cap A^2| = \gamma|A| \geq \gamma|A^2|/K.$$

Therefore

$$\Pr(A^2, A^2) \geq \frac{|C \cap A^2|}{Kns|A^2|} \geq \frac{\gamma}{K^2ns}.$$

Since $n \leq \gamma^{-1}K^2$, we conclude that $\Pr(A^2, A^2) \geq \gamma^2/(K^4s)$, as claimed. \square

Acknowledgements. The first and second authors are members of GNSAGA (INDAM), and the third author was supported by FAPDF and CNPq. The authors are grateful to the anonymous referee for many helpful suggestions.

References

- [1] E. Breuillard, B. J. Green and T. Tao, The structure of approximate groups. *Publ. Math. IHES* **116** (2012), 115–221.
- [2] E. Detomi, P. Shumyatsky, On the commuting probability for subgroups of a finite group, *Proc. Roy. Soc. Edinburgh Sect. A* **152** (2022), 1551–1564.
- [3] S. Eberhard, Commuting probabilities of finite groups, *Bull. London Math. Soc.* **47** (2015), 796–808.
- [4] A. Erfanian, R. Rezaei, P. Lescot, On the Relative Commutativity Degree of a Subgroup of a Finite Group, *Comm. Algebra* **35** (2007), 4183–4197.
- [5] R. K. Nath, M. K. Yadav, Some results on relative commutativity degree, *Rend. Circ. Mat. Palermo* **64** (2) (2015), 229–239.
- [6] P. M. Neumann, Two Combinatorial Problems in Group Theory, *Bull. London Math. Soc.* **21** (1989), 456–458.
- [7] P. Shumyatsky, Bounded conjugacy classes, commutators, and approximate subgroups, *Q. J. Math.* **73** (2022), 679–684.
- [8] T. Tao, Product set estimates for non-commutative groups. *Combinatorica* **28** (2008), 547–594.
- [9] M. C. H. Tointon, Introduction to approximate groups. London Mathematical Society Student Texts, 94. Cambridge University Press, Cambridge, 2020.

DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”, UNIVERSITÀ DI
PADOVA, VIA TRIESTE 63, 35121 PADOVA, ITALY,
Email address: `eloisa.detomi@unipd.it`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI BOLOGNA, PIAZZA DI PORTA
SAN DONATO 5, 40126 BOLOGNA, ITALY
Email address: `marta.morigi@unibo.it`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRASILIA, BRASILIA-DF,
70910-900 BRAZIL
Email address: `pavel@unb.br`