Probabilistic identities in finite groups

Avinoam Mann

Ischia Group Theory 2018

In Memoriam Michio Suzuki

March 20, 2018

Let G be a finite group, and let $w(x_1, ..., x_r)$ be a word in r variables, i.e. an element of the free group of rank r. The probability that $w = 1$ in G is defined by

$$Pr(w = 1 \ in \ G) = \frac{|\{(a_1, ..., a_r) \mid w(a_1, ..., a_r) = 1\}|}{|G|^r}.$$

We ask: what structural information on G we can deduce from the knowledge that $w = 1$ holds in G with some positive probability, or even from the more general assumption that *w has a large fiber in G*, i.e. for some fixed element $a \in G$ the probability that $w(x_1, ..., x_r) = a$ is large: $|\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}| > \epsilon|G|^r$.

Early papers discussed this question for specific words w and specific values of ϵ, e.g. *if more than 8/9 elements of G satisfy $x^4 = 1$, then G is a 2-group* (T.J.Laffey, 1979).
Recently there arose some interest in the general question above. The best results that are known so far seem to be:

Let G be a finite group, and let $w(x_1, ..., x_r)$ be a word in r variables, i.e. an element of the free group of rank r. The probability that $w = 1$ in G is defined by

$$Pr(w = 1 \ in \ G) = \frac{|\{(a_1, ..., a_r) \mid w(a_1, ..., a_r) = 1\}|}{|G|^r}.$$

We ask: what structural information on G we can deduce from the knowledge that $w = 1$ holds in G with some positive probability, or even from the more general assumption that *w has a large fiber in G*, i.e. for some fixed element $a \in G$ the probability that $w(x_1, ..., x_r) = a$ is large: $|\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}| > \epsilon|G|^r$.

Early papers discussed this question for specific words w and specific values of ϵ, e.g. *if more than 8/9 elements of G satisfy $x^4 = 1$, then G is a 2-group* (T.J.Laffey, 1979).
Recently there arose some interest in the general question above. The best results that are known so far seem to be:

Let G be a finite group, and let $w(x_1, ..., x_r)$ be a word in r variables, i.e. an element of the free group of rank r. The probability that $w = 1$ in G is defined by

$$Pr(w = 1 \ in \ G) = \frac{|\{(a_1, ..., a_r) \mid w(a_1, ..., a_r) = 1\}|}{|G|^r}.$$

We ask: what structural information on G we can deduce from the knowledge that $w = 1$ holds in G with some positive probability, or even from the more general assumption that *w has a large fiber in G*, i.e. for some fixed element $a \in G$ the probability that $w(x_1, ..., x_r) = a$ is large: $|\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}| > \epsilon |G|^r$.

Early papers discussed this question for specific words w and specific values of ϵ, e.g. *if more than 8/9 elements of G satisfy $x^4 = 1$, then G is a 2-group* (T.J.Laffey, 1979).

Recently there arose some interest in the general question above. The best results that are known so far seem to be:

Theorem 0:

Let w, G and a satisfy

$$|\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}| > \epsilon |G|^r.$$

Then there exists a number C, depending only on w and ϵ, such that

1. If G is a finite simple non-abelian group, then $|G| < C$ [J.Dixon-L.Pyber-A.Seress-A.Shalev, 2003].

2. Moreover, any non-abelian composition factor of G has size at most C [A.Bors, 2016, and M.Larsen-Shalev, 2017].

3. For some words w, the multiplicity of a non-abelian simple group S as a composition factor of G, is bounded by a number depending only on w, ϵ, and S [A.Bors, 2017].

These results are obtained using very deep tools, such as CFSG and algebraic groups. We will describe in this talk results whose proofs employ more elementary means, mostly just careful counting, but also some character theory.

Peter M. Neumann [1989] proved the following

Theorem 1:

Let G be a finite group such that $Pr(xy = yx \text{ in } G) > \epsilon$. Then G contains two normal subgroups, $N \triangleleft H \triangleleft G$, such that H/N is abelian, and $|N|$ and $|G : H|$ are bounded by some function of ϵ.

We express the conclusion of Theorem 1 by saying that G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded)*.

The premises of Theorem 1 can be put in another way. The number of pairs of commuting elements in G, i.e. $|\{(x, y)|x,\ y \in G \text{ and } xy = yx\}|$ equals $\sum_x |C_G(x)|$. Consider G as acting on itself by conjugation. Then we are summing the numbers of fixed points of all elements in this action. It is well known that the average number of fixed points (in any action) is the number of orbits of G. This fact is often termed *Burnside's Lemma*, or, more recently, *the non-Burnside Lemma* (I suggest to call it *the Orbit Lemma*). In our case, the number of orbits is the number $k(G)$ of conjugacy classes of G, and thus the number of pairs of commuting elements is $|G|k(G)$. This equality seems to have been first stated explicitly by K.A.Hirsch [1950], and has been rediscovered several times since. Thus Neumann's assumption is equivalent to $k(G) > \epsilon|G|$.

We can replace the equation $[x, y] = 1$ by $[x, y] = a$, where a is any element of G, i.e. we consider the fibers of the word $[x, y]$.

Proposition 2.

Let G be a finite group, and $a \in G$. If there are at least $\epsilon|G|^2$ pairs (x, y) such that $[x, y] = a$, then G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded).*

Proof.

By a formula of Frobenius, the number of ways to write a as a commutator is $\sum \frac{|G|}{\chi(1)}\chi(a)$, where the summation is taken over all irreducible characters χ of G. This sum is at most $\sum \frac{|G|}{\chi(1)}\chi(1) = |G|k(G)$, and thus $k(G) \geq \epsilon|G|$, and Theorem 1 applies.

Corollary 3.

If the probability that the equation $[x, y] = w(z_1, ..., z_r)$ holds in the finite group G is more than ϵ, then G is (ϵ*-bounded)-by-abelian-by-(*ϵ*-bounded)*. Here x and y are distinct from the $z_i's$.

Proof.

We find an r-tuple $(u_1, ..., u_r)$ such that the number of pairs (x, y) for which $[x, y] = w(z_1, ..., z_r)$ is at least $\epsilon|G|^2$. Write $a = w(u_1, ..., u_r)$ and apply the proposition.

The speaker has proved the following [1994]

Theorem 4.

If the probability that $x^2 = 1$ in the finite group G is more than ϵ, then G is (ϵ*-bounded)-by-abelian-by-(*ϵ*-bounded).*

This is essentially a corollary of Theorem 1. The number $N(2)$ of elements in G whose square is the identity equals, by a formula of Frobenius and Schur, $\sum t(\chi)\chi(1)$, where χ varies over all irreducible characters of G, and $t(\chi)$, the *Frobenius-Schur indicator* of χ, has one of the values $0, \ \pm 1$. Thus the Cauchy-Schwartz inequality shows that $N(2) \leq \sqrt{(\sum t(\chi)^2)(\sum \chi(1)^2)} \leq \sqrt{k(G)|G|}$. Our assumption $N(2) \geq \epsilon|G|$ implies then $k(G) \geq \epsilon^2|G|$, and we can quote Theorem 1.

Similar applications of the Cauchy-Schwartz inequality occur elsewhere, but the inequality for $N(2)$ occurs already, even in a slightly stronger form, in the seminal R.Brauer-K.A.Fowler paper of 1955, with an elementary, character free, proof. Theorem (2J) there states that $N(2)(N(2)-1) \leq (k(G)-1)|G|$ (actually, they replace $k(G)$ by the number $k_1(G)$ of real classes of G; this also follows from the proof given above, because $t(\chi) \neq 0$ exactly for the real characters. Note also that the BF inequality is best possible, for $G = A_5$ equality obtains).

This is essentially a corollary of Theorem 1. The number $N(2)$ of elements in G whose square is the identity equals, by a formula of Frobenius and Schur, $\sum t(\chi)\chi(1)$, where χ varies over all irreducible characters of G, and $t(\chi)$, the *Frobenius-Schur indicator* of χ, has one of the values $0, \ \pm 1$. Thus the Cauchy-Schwartz inequality shows that $N(2) \leq \sqrt{(\sum t(\chi)^2)(\sum \chi(1)^2)} \leq \sqrt{k(G)|G|}$. Our assumption $N(2) \geq \epsilon|G|$ implies then $k(G) \geq \epsilon^2|G|$, and we can quote Theorem 1.

Similar applications of the Cauchy-Schwartz inequality occur elsewhere, but the inequality for $N(2)$ occurs already, even in a slightly stronger form, in the seminal R.Brauer-K.A.Fowler paper of 1955, with an elementary, character free, proof. Theorem (2J) there states that $N(2)(N(2)-1) \leq (k(G)-1)|G|$ (actually, they replace $k(G)$ by the number $k_1(G)$ of real classes of G; this also follows from the proof given above, because $t(\chi) \neq 0$ exactly for the real characters. Note also that the BF inequality is best possible, for $G = A_5$ equality obtains).

Another way to obtain that inequality is by counting the number of solutions to $x^2 = y^2$. This turns out to be $k_1(G)|G|$, and it obviously is at least $N(2)^2$.

Analogously to Proposition 2 and Corollary 3, we have

Proposition 5

Let G be a finite group, and $a \in G$. If there are at least $\epsilon|G|$ elements $x \in G$ such that $x^2 = a$, or if the probability that the equation $x^2 = w(z_1, ..., z_r)$ holds in G, is at least ϵ, then G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded).*

For the proof we apply, as in the proof of the theorem, the general Frobenius-Schur formula, according to which the number of square roots of a is $\sum t(\chi)\chi(a) \leq \sqrt{\sum |\chi(a)|^2}\sqrt{\sum t(\chi)^2} \leq \sqrt{|C_G(a)|k(G)} \leq \sqrt{|G|k(G)}$, and this implies $k(G) \geq \epsilon^2|G|$ as above.

Another way to obtain that inequality is by counting the number of solutions to $x^2 = y^2$. This turns out to be $k_1(G)|G|$, and it obviously is at least $N(2)^2$.

Analogously to Proposition 2 and Corollary 3, we have

Proposition 5

Let G be a finite group, and $a \in G$. If there are at least $\epsilon|G|$ elements $x \in G$ such that $x^2 = a$, or if the probability that the equation $x^2 = w(z_1, ..., z_r)$ holds in G, is at least ϵ, then G is (ϵ*-bounded)-by-abelian-by-(*ϵ*-bounded)*.

For the proof we apply, as in the proof of the theorem, the general Frobenius-Schur formula, according to which the number of square roots of a is $\sum t(\chi)\chi(a) \leq \sqrt{\sum |\chi(a)|^2}\sqrt{\sum t(\chi)^2} \leq \sqrt{|C_G(a)|k(G)} \leq \sqrt{|G|k(G)}$, and this implies $k(G) \geq \epsilon^2|G|$ as above.

Another way to obtain that inequality is by counting the number of solutions to $x^2 = y^2$. This turns out to be $k_1(G)|G|$, and it obviously is at least $N(2)^2$.

Analogously to Proposition 2 and Corollary 3, we have

Proposition 5

Let G be a finite group, and $a \in G$. If there are at least $\epsilon|G|$ elements $x \in G$ such that $x^2 = a$, or if the probability that the equation $x^2 = w(z_1, ..., z_r)$ holds in G, is at least ϵ, then G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded)*.

For the proof we apply, as in the proof of the theorem, the general Frobenius-Schur formula, according to which the number of square roots of a is $\sum t(\chi)\chi(a) \leq \sqrt{\sum |\chi(a)|^2}\sqrt{\sum t(\chi)^2} \leq \sqrt{|C_G(a)|k(G)} \leq \sqrt{|G|k(G)}$, and this implies $k(G) \geq \epsilon^2|G|$ as above.

Aner Shalev [2018] recently generalized Theorem 1.

Theorem 6

Let the finite group G satisfy

$$Prob\ \{[x_1, x_2, ..., x_{k+1}] = a\} \geq \epsilon,$$

for some k, some ϵ, and some $a \in G$. Then G contains a nilpotent normal subgroup N, of nilpotence class at most k, such that G/N is isomorphic to a subgroup of S_n^l, for some l, where $n = \lfloor k/\epsilon \rfloor$.

For $k = 1$ the subgroup N is abelian. This result and Neumann's seem to be independent of each other. We do not know if a result analogous to Neumann's holds for $k > 1$.

Aner Shalev [2018] recently generalized Theorem 1.

Theorem 6

Let the finite group G satisfy

$$Prob\ \{[x_1, x_2, ..., x_{k+1}] = a\} \geq \epsilon,$$

for some k, some ϵ, and some $a \in G$. Then G contains a nilpotent normal subgroup N, of nilpotence class at most k, such that G/N is isomorphic to a subgroup of S_n^l, for some l, where $n = \lfloor k/\epsilon \rfloor$.

For $k = 1$ the subgroup N is abelian. This result and Neumann's seem to be independent of each other. We do not know if a result analogous to Neumann's holds for $k > 1$.

A variation on the proof of Theorem 6 yields:

Theorem 7

There exist numbers $0 < \epsilon_k < \zeta_k < \eta_k < 1$, such that if

$$Prob\ \{[x_1, x_2, ..., x_{k+1}] = a\} > \epsilon_k\ (respectively\ \zeta_k,\ \eta_k),$$

holds in the finite group G for some $a \in G$, then G is soluble (respectively nilpotent, nilpotent of class at most k).

E.g. we can take $\epsilon_3 = 7/40$, $\zeta_3 = 3/4$, $\eta_3 = 13/16$. We can also make G solvable of some bounded nilpotent height, or nilpotent of some bounded class.

The proof applies the following

Lemma 8

Let $x \in G$ have at most 9 conjugates. Then $x \in S(G)$, the maximal normal soluble subgroup of G.

Note that S_5 contains a conjugacy class consisting of 10 transpositions. But we can change the number 9 in the lemma to any other natural number n, provided we also allow $S(G)$ to have some non-abelian composition factors, namely ones occurring as composition factors of some subgroups of S_n.

The proof applies the following

Lemma 8

Let $x \in G$ have at most 9 conjugates. Then $x \in S(G)$, the maximal normal soluble subgroup of G.

Note that S_5 contains a conjugacy class consisting of 10 transpositions. But we can change the number 9 in the lemma to any other natural number n, provided we also allow $S(G)$ to have some non-abelian composition factors, namely ones occurring as composition factors of some subgroups of S_n.

Using Proposition 5, Shalev derives also

Theorem 9

Let the finite group G satisfy

$$Prob\ \{[x_1^2, x_2, ..., x_{k+1}] = a\} \geq \epsilon,$$

for some k, some ϵ, and some $a \in G$. Then G contains a nilpotent normal subgroup N, of nilpotence class at most k, such that G/N is isomorphic to a subgroup of S_n^l, for some l, and some $n = n(k, \epsilon)$.

Similarly, we can give results analogous to Theorem 7.

Theorem 10

There exist numbers $0 < \epsilon_{k,p} < \zeta_{k,p} < 1$, where p is a prime or $p = 4$, such that if

$$Prob\ \{[x_1^p, x_2, ..., x_{k+1}] = a\} \geq \epsilon_{k,p}\ (respectively\ \zeta_{k,p})$$

holds in the finite group G for some $a \in G$, then G is soluble (respectively nilpotent).

Using Proposition 5, Shalev derives also

Theorem 9

Let the finite group G satisfy

$$Prob\ \{[x_1^2, x_2, ..., x_{k+1}] = a\} \geq \epsilon,$$

for some k, some ϵ, and some $a \in G$. Then G contains a nilpotent normal subgroup N, of nilpotence class at most k, such that G/N is isomorphic to a subgroup of S_n^l, for some l, and some $n = n(k, \epsilon)$.

Similarly, we can give results analogous to Theorem 7.

Theorem 10

There exist numbers $0 < \epsilon_{k,p} < \zeta_{k,p} < 1$, where p is a prime or $p = 4$, such that if

$$Prob\ \{[x_1^p, x_2, ..., x_{k+1}] = a\} \geq \epsilon_{k,p}\ (respectively\ \zeta_{k,p})$$

holds in the finite group G for some $a \in G$, then G is soluble (respectively nilpotent).

For $p = 2$ or 3 we can also find lower bounds $\eta_{p,k}$ for the probability that bound the nilpotency class. This is impossible for the other values of p, for which there is no bound even for the nilpotency class of groups of exponent p.

For later applications, we consider two other equations. Let $cp(G)$, the *commuting probability of* G, be the probability that two random elements commute.

Proposition 11

If either the equation $(xyz)^2 = x^2y^2z^2$ or the equation $(xyz)^{-1} = x^{-1}y^{-1}z^{-1}$ holds in G with probability ϵ, then $cp(G) = \epsilon$.

Indication of Proof.

$(xyz)^2 = x^2y^2z^2$ is equivalent to $yz \cdot xy = xy \cdot yz$. We count the ways in which an arbitrary pair $u, v \in G$ can be written as $u = xy,\ v = yz$. Similarly for the other equation.

For $p = 2$ or 3 we can also find lower bounds $\eta_{p,k}$ for the probability that bound the nilpotency class. This is impossible for the other values of p, for which there is no bound even for the nilpotency class of groups of exponent p.

For later applications, we consider two other equations. Let $cp(G)$, the *commuting probability of* G, be the probability that two random elements commute.

Proposition 11

If either the equation $(xyz)^2 = x^2y^2z^2$ or the equation $(xyz)^{-1} = x^{-1}y^{-1}z^{-1}$ holds in G with probability ϵ, then $cp(G) = \epsilon$.

Indication of Proof.

$(xyz)^2 = x^2y^2z^2$ is equivalent to $yz \cdot xy = xy \cdot yz$. We count the ways in which an arbitrary pair $u, v \in G$ can be written as $u = xy,\ v = yz$. Similarly for the other equation.

Given a word $w(x_1, ..., x_r)$ and $a \in G$, let $f_w(a) = |\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}|$, the size of the a-fiber of w. As a function of a, this is a class function, and hence can be written as a linear combination of the irreducible characters of G,

$$f_w(a) = \sum c_{w,\chi}\chi(a).$$

Looking at the proofs Theorem 4 and Proposition 2 suggests the following two questions:

Problem 1.

For which words are the Fourier coefficients $c_{w,\chi}$ bounded, by a bound independent of G?

Problem 2.

For which words are the Fourier coefficients positive, for all finite groups G?

Given a word $w(x_1, ..., x_r)$ and $a \in G$, let $f_w(a) = |\{(x_1, ..., x_r) \mid w(x_1, ..., x_r) = a\}|$, the size of the a-fiber of w. As a function of a, this is a class function, and hence can be written as a linear combination of the irreducible characters of G,

$$f_w(a) = \sum c_{w,\chi}\chi(a).$$

Looking at the proofs Theorem 4 and Proposition 2 suggests the following two questions:

Problem 1.

For which words are the Fourier coefficients $c_{w,\chi}$ bounded, by a bound independent of G?

Problem 2.

For which words are the Fourier coefficients positive, for all finite groups G?

The first one is easy.

Proposition 12

The only words satisfying the requirements of Problem 1 are $1,\ x,\ x^{-1},\ x^2,\ x^{-2}$.

Proof.

Exercise.

Problem 2 seems to be open, but there are some examples. First, if two words w_1 and w_2 satisfy the requirements of Problem 2, then so does the word $w = w_1(x_1, ..., x_r)w_2(y_1, ..., y_s$, provided the sets $\{x_1, ..., x_r\}$ and $\{y_1, ..., y_s\}$ are disjoint. Thus, besides $[x_1, x_2]$, these requirements are met by the words $w_r := [x_1, x_2][x_3, x_4]...[x_{2k-1}, x_{2k}]$, and trivial variations, such as $x_1[x_2, x_3]$.

Other such words are, e.g., $v_r := x_1^2 ... x_{2r}^2$, $u_r := x_1 ... x_r x_1^{-1} ... x_r^{-1}$ [T.Tambour, 2000] and $[x_1, x_2] x_3 [x_1, x_4] x_3^{-1}$ [O.Parzanchevski-G.Schul (2014)]. Indeed, for w_r, v_r, and u_r the Fourier coefficients are positive integers, so that the corresponding functions f_w are characters.

Note that the equality $u_3 = 1$ is the same as the equality $(xyz)^{-1} = x^{-1} y^{-1} z^{-1}$, which was mentioned in Proposition 11. Therefore, if $f_{u_3}(a) = \epsilon |G|$, for some $a \in G$, then $cp(G) \geq \epsilon$.

Recall also that G is *r-rewritable*, if for any n-tuple $x_1, ..., x_n$ in G, there exist two permutations $\sigma, \tau \in S_r$, such that $x_{\sigma(1)} ... x_{\sigma(r)} = x_{\tau(1)} ... x_{\tau(r)}$.

Assume instead that this equality holds for only $\epsilon |G|^r$ tuples. Taking $r = 3$, for some pair of permutations the equality holds with probability at least $\epsilon / 15$, and it is easily seen that the probability of that equality is again equal to the commuting probability. Thus we can apply Theorem 1 in this situation as well.

First application - endomorphisms

Some authors have considered the following situation: G is a finite group having an automorphism σ which has many fixed points, or, more generally, for some k many elements are mapped onto their kth power. If σ is the identity, the last assumption is equivalent to many elements $x \in G$ satisfying $x^{k-1} = 1$. Thus this situation generalizes the one of having many elements of a given order, and some of the results in both cases are very similar. On the other hand, this situation implies the existence of probabilistic identities, indeed for this it suffices to assume that σ is an endomorphism, not necessarily an automorphism.

Theorem 13

Let the group G have an endomorphism σ, such that the equality $\sigma(x) = x^k$ holds in G with probability ϵ. Then there exists a number $\eta > 0$, depending only on ϵ, such that the equation $(xyz)^k = x^k y^k z^k$ holds in G with probability at least η. Moreover, if $\epsilon > 1/2$, then the same claim holds for the equation $(xy)^k = x^k y^k$.

First application - endomorphisms

Some authors have considered the following situation: G is a finite group having an automorphism σ which has many fixed points, or, more generally, for some k many elements are mapped onto their kth power. If σ is the identity, the last assumption is equivalent to many elements $x \in G$ satisfying $x^{k-1} = 1$. Thus this situation generalizes the one of having many elements of a given order, and some of the results in both cases are very similar. On the other hand, this situation implies the existence of probabilistic identities, indeed for this it suffices to assume that σ is an endomorphism, not necessarily an automorphism.

Theorem 13

Let the group G have an endomorphism σ, such that the equality $\sigma(x) = x^k$ holds in G with probability ϵ. Then there exists a number $\eta > 0$, depending only on ϵ, such that the equation $(xyz)^k = x^k y^k z^k$ holds in G with probability at least η. Moreover, if $\epsilon > 1/2$, then the same claim holds for the equation $(xy)^k = x^k y^k$.

Indication of proof.

Let S be the set of the elements that are mapped by σ to their kth power. Thus $|S| = \epsilon|G|$. First we assume that $\epsilon > 1/2$, and write $\epsilon = 1/2 + \alpha$. Then for each $x \in S$ we have $|S \cap xS| \geq 2\alpha|G|$. That means that we can find $2\alpha\epsilon|G|^2$ pairs $x, y \in S$ such that also $xy \in S$, and applying σ we have the identity $(xy)^k = x^k y^k$ with probability at least $2\alpha\epsilon$.

In the general case we can find $x, y \in S$ such that $xS \cap yS \neq \emptyset$, and proceed similarly.

If $k = 2$ or $k = -1$, we can now apply Proposition 11 and Theorem 1 and obtain

Corollary 14

Let σ be an endomorphism of the finite group G. If, for some $\epsilon > 0$, either the probability that $\sigma(x) = x^2$, or the probability that $\sigma(x) = x^{-1}$, is at least ϵ, then G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded)*.

However, not only for $k = -1,\ 2$, but also for $k = 3$, A.bors derived structural restrictions on G. For $k = -1,\ 2$, Theorem 13 implies his results, at least qualitatively. Moreover, Bors considers only automorphisms, not endomorphisms, and also applies the classification of the finite simple groups.

Taking σ to be the identity, the case $k = -1$ of Corollary 14 provides another proof of Theorem 4.

If $k = 2$ or $k = -1$, we can now apply Proposition 11 and Theorem 1 and obtain

Corollary 14

Let σ be an endomorphism of the finite group G. If, for some $\epsilon > 0$, either the probability that $\sigma(x) = x^2$, or the probability that $\sigma(x) = x^{-1}$, is at least ϵ, then G is *(ϵ-bounded)-by-abelian-by-(ϵ-bounded)*.

However, not only for $k = -1,\ 2$, but also for $k = 3$, A.bors derived structural restrictions on G. For $k = -1,\ 2$, Theorem 13 implies his results, at least qualitatively. Moreover, Bors considers only automorphisms, not endomorphisms, and also applies the classification of the finite simple groups.

Taking σ to be the identity, the case $k = -1$ of Corollary 14 provides another proof of Theorem 4.

Theorem 13 was generalized by Bors (2017):

Theorem 15

For a finite group G, let there be a homomorphism $\sigma : G^r \to G$, such that the equality $\sigma(x_1, ..., x_r) = w(x_1, ..., x_r)$ holds with probability ϵ. Then there exists a number $\eta > 0$, depending only on ϵ, such that the equation

$$w(x_1^{-1}y_1z_1, ..., x_r^{-1}y_rz_r) = w(x_1, ..., x_r)^{-1}w(y_1, ..., y_r)w(z_1, ..., z_r)$$

holds in G with probability at least η.

Second application - doubling

Following his characterization of sets of numbers with 'small doubling', G.A.Freiman initiated a programme of studying similar problems in groups. A group is termed a $DS(k)$-group if for each subset $X \subseteq G$ of size k we have $|X^2| < |X|^2$, and it is a DS-group if it is a $DS(k)$-group for some k. These concepts are not confined to finite groups, indeed any finite group is DS.

The $DS(2)$-groups are exactly the Dedekind groups [Freimann, 1981], the $DS(3)$-groups were determined P.Longobardi-M.Maj [1992], and the DS-groups were determined by M.Herzog-Longobardi-Maj [1993].

Proposition 16

Let G be finite. Suppose that for at least $\epsilon \cdot \binom{|G|}{k}$ subsets X of G of size k we have $|X^2| < |X|^2$, then G is $(\epsilon, k$*-bounded)-by-abelian-by-*$(\epsilon, k$*-bounded)*. Conversely, if G contains two normal subgroups, $N \triangleleft H \triangleleft G$, such that H/N is abelian, and $|N|$ and $|G : H|$ are bounded by some number C, then for at least $\epsilon |G|^k$ subsets X of G of size k we have $|X^2| < |X|^2$, where ϵ depends only on C.

Second application - doubling

Following his characterization of sets of numbers with 'small doubling', G.A.Freiman initiated a programme of studying similar problems in groups. A group is termed a $DS(k)$-group if for each subset $X \subseteq G$ of size k we have $|X^2| < |X|^2$, and it is a DS-group if it is a $DS(k)$-group for some k. These concepts are not confined to finite groups, indeed any finite group is DS.

The $DS(2)$-groups are exactly the Dedekind groups [Freimann, 1981], the $DS(3)$-groups were determined P.Longobardi-M.Maj [1992], and the DS-groups were determined by M.Herzog-Longobardi-Maj [1993].

Proposition 16

Let G be finite. Suppose that for at least $\epsilon \cdot \binom{|G|}{k}$ subsets X of G of size k we have $|X^2| < |X|^2$, then G is *$(\epsilon, k$-bounded)-by-abelian-by-(ϵ, k-bounded).* Conversely, if G contains two normal subgroups, $N \triangleleft H \triangleleft G$, such that H/N is abelian, and $|N|$ and $|G : H|$ are bounded by some number C, then for at least $\epsilon |G|^k$ subsets X of G of size k we have $|X^2| < |X|^2$, where ϵ depends only on C.

Proof.

Write $|G| = n$. We have at least $\epsilon \cdot \binom{n}{k}$ equalities of the type $ab = cd$, where a, b, c, d are not necessarily distinct, and it is possible that the same equality occurs several times, because the involved elements belong to more than one k-tuple.

If for many of our equalities we have $|\{a, b, c, d\}| = 4$, then any three of these elements determine the fourth, therefore the number of these equalities is at most n^3, while by assumption their number is a positive fraction of n^4. This bounds n. A similar argument applies if in many of the equalities we have $|\{a, b, c, d\}| = 3$.

We can now assume that for many of the equalities we have $|\{a, b, c, d\}| = 2$. Then the equalities are of type $xy = yx$ or $x^2 = y^2$, and previous results apply.

The converse follows from the inequality $cp(G) \geq 1/C^3$, which implies that at least $|G|^k/C^3$ k-tuples contain two commuting elements.

A weaker assumption than $DS(k)$ was also considered: *for some r and k, all k-tuples X from G satisfy $|X^r| < |X|^r$.* Correspondingly, we have

Proposition 17

Given $\epsilon > 0$, k, and r, there exists a number $\eta > 0$ and a word $w = w(x_1, ..., x_k)$, such that if in a finite group G at least $\epsilon \cdot \binom{|G|}{k}$ subsets X of G of size k satisfy $|X^r| < |X|^r$, then G satisfies $w = 1$ with probability at least η.

The proof is similar to the previous one.

THANK YOU!

A weaker assumption than $DS(k)$ was also considered: *for some r and k, all k-tuples X from G satisfy $|X^r| < |X|^r$.* Correspondingly, we have

Proposition 17

Given $\epsilon > 0$, k, and r, there exists a number $\eta > 0$ and a word $w = w(x_1, ..., x_k)$, such that if in a finite group G at least $\epsilon \cdot \binom{|G|}{k}$ subsets X of G of size k satisfy $|X^r| < |X|^r$, then G satisfies $w = 1$ with probability at least η.

The proof is similar to the previous one.

THANK YOU!