AN ERDŐS–FUCHS TYPE THEOREM FOR FINITE GROUPS

VSEVOLOD F. LEV AND ANDRÁS SÁRKÖZY*

Dedicated to Melvyn B. Nathanson and Carl Pomerance on the occasion of their 65th birthday

Abstract. We establish a finite analogue of the Erdős-Fuchs theorem, showing that the representation function of a non-trivial subset of a finite abelian group cannot be nearly constant. Our results are, essentially, best possible.

1. Introduction.

For finite subsets $\mathcal{A}$ and $\mathcal{B}$ of an (additively written) abelian group G let

$$r_{\mathcal{A},\mathcal{B}}(g) := \big|\{(a,b) \in \mathcal{A} \times \mathcal{B}\colon\ g = a + b,\ a \in \mathcal{A},\ b \in \mathcal{B}\}\big|.$$

If $\mathcal{B} = \mathcal{A}$, we abbreviate this as $r_{\mathcal{A}}$ and call *the representation function* of the set $\mathcal{A}$.

In 1956 Erdős and Fuchs [EF56] proved two remarkable theorems on the representation functions of infinite sets of non-negative integers.

Theorem A. *If $\mathcal{A}$ is an infinite set of non-negative integers, then*

$$\sum_{k=1}^{n} r_{\mathcal{A}}(k) = cn + o\big(n^{1/4}\log^{-1/2} n\big)$$

with a positive constant c cannot hold.

Theorem B. *Let $\mathcal{A} = \{a_1, a_2, \dots\}$ be a set of non-negative integers written in increasing order, and let $c \ge 0$. If either $c > 0$, or $c = 0$ and $a_k < Ck^2$ for a constant C, then*

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \big(r_{\mathcal{A}}(k) - c\big)^2 > 0.$$

Theorem A is often called the *Erdős–Fuchs theorem*. Erdős and Fuchs wrote in [EF56]:

2010 *Mathematics Subject Classification.* Primary: 11B34.

Key words and phrases. Erdős–Fuchs theorem, representation function.

*Research partially supported by Hungarian National Foundation for Scientific Research, grants no. K67676 and K72731.

> If $a_k = k^2$ the estimation of $r(n)$ is the classical problem about lattice points in a circle. Here it follows from the results of Hardy and Landau that $r(n) \ne cn + dn^{1/2} + o\big(n^{1/4}\log^{1/4} n\big)$. It is rather surprising that our result for a general a_k is almost as good while its proof is much simpler.

In a survey paper [E96] written just before his death, Erdős refers to these results as follows:

> I should not forget our result with W. Fuchs which certainly will survive the authors by centuries.

Theorems A and B have been extended in various directions and sharpened by Montgomery and Vaughan in [MV90] but, to our knowledge, all extensions address infinite sets of integers. In this paper we establish a finite analogue of Theorem B showing that the representation function of a subset of a finite abelian group cannot be nearly constant, unless the subset contains too few or too many elements. Our main result is

Theorem 1. *If $\mathcal{A}$ is a subset of a finite non-trivial abelian group G of density $\alpha := |\mathcal{A}|/|G|$, then for any real number c we have*

$$\sum_{g\in G} \big(r_{\mathcal{A}}(g) - c\big)^2 \ge (1 - 1/|G|)^{-1}\, \alpha^2(1-\alpha)^2|G|^2.$$

Corollary 1. *Under the assumptions of Theorem 1, for any real number c we have*

$$\max_{g\in G} |r_{\mathcal{A}}(g) - c| \ge (1 - 1/|G|)^{-1/2}\, \alpha(1-\alpha)|G|^{1/2}.$$

Thus,

$$\max_{g\in G} r_{\mathcal{A}}(g) - \min_{g\in G} r_{\mathcal{A}}(g) \ge 2(1 - 1/|G|)^{-1/2}\, \alpha(1-\alpha)|G|^{1/2}.$$

Theorem 1 is proved in Section 2. As the proof readily shows, for the optimal choice of c, equality is attained in the estimate of the theorem if and only if $\mathcal{A}$ is a difference set in G; that is, every non-zero element of G has the same number of representations as a difference of two elements from $\mathcal{A}$. Unfortunately, there do not seem to exist many groups possessing difference sets and, with just one exception, all known difference sets have density very close to $1/2$ (see [DJ96] for a survey). Besides, difference sets do not provide any evidence on whether Corollary 1 is sharp, too. For this reason we give in Section 3 several examples showing that Theorem 1 and Corollary 1 are nearly best possible: specifically,

(i) if G is the additive group of a finite field of odd characteristic and $\mathcal{A} \subseteq G$ is the set of all non-zero squares of the field, then for the optimal choice of c the estimate of Theorem 1 is tight up to a lower-order term;
(ii) if G is a finite abelian group of odd order, and $\mathcal{A}$ is a random subset of G to which every group element is chosen to belong with probability α, independently of other elements, then the estimate of Corollary 1 is off by a logarithmic factor.

Furthermore, one cannot, in general, replace in Theorem 1 and Corollary 1 the representation function $r_{\mathcal{A}}$ by $r_{\mathcal{A},\mathcal{B}}$ with two distinct sets $\mathcal{A}$ and $\mathcal{B}$: say, if $\mathcal{A}$ is a union of cosets of a subgroup, and $\mathcal{B}$ is a union of several pairwise disjoint sets of coset representatives of this subgroup, then $r_{\mathcal{A},\mathcal{B}}$ is constant. One can expect, nevertheless, that there can be non-trivial estimates for the "skew representation function" $r_{u\mathcal{A},v\mathcal{A}}$, where u and v are integers and where, for integer w, we write

$$w\mathcal{A} = \{wa \colon a \in \mathcal{A}\}.$$

Indeed, in Section 2 we prove

Theorem 2. *If $\mathcal{A}$ is a non-trivial subset of a finite abelian group, and u and v are integers co-prime with the order of the group, then $r_{u\mathcal{A},v\mathcal{A}}$ is not constant.*

Theorem 2 appears to be manifestly weaker than Corollary 1, but in fact the former is, essentially, best possible: in Section 3 we provide examples showing that coprimality assumption cannot be dropped, and the conclusion cannot be strengthened in the sense that with u, v, and $\mathcal{A}$ as in the theorem, one can have

$$\max r_{u\mathcal{A},v\mathcal{A}} - \min r_{u\mathcal{A},v\mathcal{A}} = 1.$$

2. Proofs of Theorems 1 and 2.

Proof of Theorem 1. Let $S := \sum_{g\in G} \big(r_{\mathcal{A}}(g) - c\big)^2$. Since

$$\sum_{g\in G} r_{\mathcal{A}}(g) = \sum_{g\in G} \sum_{\substack{a_1,a_2\in\mathcal{A}\\ a_1+a_2=g}} 1 = \sum_{a_1,a_2\in\mathcal{A}} 1 = |\mathcal{A}|^2,$$

we have

$$S = \sum_{g\in G} r_{\mathcal{A}}^2(g) - 2c|\mathcal{A}|^2 + c^2|G|,$$

and minimization over c shows that

$$S \geq \sum_{g\in G} r_{\mathcal{A}}^2(g) - |\mathcal{A}|^4/|G|.$$

The sum in the right-hand side counts the number of solutions of the equation

$$a_1+a_2=a_3+a_4$$

in the variables $a_1,a_2,a_3,a_4\in\mathcal{A}$. Rearranging the terms, one can rewrite this equation as $a_1-a_3=a_4-a_2$, showing that the sum under consideration can also be written as $\sum_{g\in G} r^2_{\mathcal{A},-\mathcal{A}}(g)$. Hence, taking into account that $r_{\mathcal{A},-\mathcal{A}}(0)=|\mathcal{A}|$ and using the Cauchy-Schwarz inequality, we get

$$\begin{aligned}S&\ge\sum_{g\in G\setminus\{0\}} r^2_{\mathcal{A},-\mathcal{A}}(g)+|\mathcal{A}|^2-\frac{|\mathcal{A}|^4}{|G|}\\&\ge\frac{1}{|G|-1}\left(\sum_{g\in G\setminus\{0\}} r_{\mathcal{A},-\mathcal{A}}(g)\right)^2+|\mathcal{A}|^2-\frac{|\mathcal{A}|^4}{|G|}\\&=\frac{1}{|G|-1}\bigl(|\mathcal{A}|^2-|\mathcal{A}|\bigr)^2+|\mathcal{A}|^2-\frac{|\mathcal{A}|^4}{|G|}\\&=\frac{1}{|G|-1}\left(\frac{|\mathcal{A}|^4}{|G|}-2|\mathcal{A}|^3+|\mathcal{A}|^2|G|\right).\end{aligned}$$

Recalling that $|\mathcal{A}|=\alpha|G|$, we rewrite the right-hand side as

$$\frac{|G|^3}{|G|-1}\bigl(\alpha^4-2\alpha^3+\alpha^2\bigr)=(1-1/|G|)^{-1}\,\alpha^2(1-\alpha)^2|G|^2,$$

and the assertion follows. □

Proof of Theorem 2. Let G be a finite abelian group, $\mathcal{A}\subseteq G$, and suppose that u and v are integers with $\gcd(uv,|G|)=1$. For a set $\mathcal{B}\subseteq G$ and a character χ of G set

$$S_{\mathcal{B}}(\chi):=\sum_{b\in\mathcal{B}}\chi(b).$$

The key observation is that for any character χ we have

$$S_{u\mathcal{A}}(\chi)S_{v\mathcal{A}}(\chi)=\sum_{g\in G} r_{u\mathcal{A},v\mathcal{A}}(g)\chi(g)$$

(which, of course, is due to the fact that the Fourier transform of a convolution is the product of Fourier transforms); hence, if $r_{u\mathcal{A},v\mathcal{A}}$ is constant, then

$$S_{u\mathcal{A}}(\chi)S_{v\mathcal{A}}(\chi)=0 \tag{1}$$

for any non-trivial character χ.

Write $\omega:=\exp(2\pi i/|G|)$. Denote by $\mathbb{Q}$ the field of rational numbers, and for integer z, co-prime with $|G|$, let φ_z be the automorphism of the field $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, defined by $\varphi_z(\omega)=\omega^z$. We have then $\varphi_u(S_{\mathcal{A}}(\chi))=S_{u\mathcal{A}}(\chi)$ and $\varphi_v(S_{\mathcal{A}}(\chi))=S_{v\mathcal{A}}(\chi)$.

Consequently, (1) shows that $S_{\mathcal{A}}(\chi) = 0$ for each non-trivial character χ; as a result, we have either $\mathcal{A} = \varnothing$, or $\mathcal{A} = G$. □

3. Examples.

Example 1. Suppose that q is a power of an odd prime and let $\mathbb{F}_q$ denote the finite field of order q. Furthermore, let $\mathcal{A}$ be the set of all non-zero squares in $\mathbb{F}_q$; thus, the density of $\mathcal{A}$ is $(q-1)/(2q)$. The representation function of $\mathcal{A}$ can be easily expressed in terms of the quadratic character χ of the field $\mathbb{F}_q$: namely,

$$r_{\mathcal{A}}(0) = |\mathcal{A} \cap (-\mathcal{A})| = \frac{1}{4}\,(1+\chi(-1))(q-1),$$

and if $g \in \mathbb{F}_q^{\times}$, then

$$\begin{aligned} r_{\mathcal{A}}(g) &= \frac{1}{4} \sum_{z \in \mathbb{F}_q \setminus \{0,g\}} (1+\chi(z))(1+\chi(g-z)) \\ &= \frac{1}{4} \sum_{z \in \mathbb{F}_q} \chi(z(g-z)) - \frac{1}{2}\,\chi(g) + \frac{1}{4}\,(q-2) \\ &= \frac{1}{4}\,(q-2) - \frac{1}{4}\,\chi(-1) - \frac{1}{2}\,\chi(g). \end{aligned}$$

(We omit computing the sum of the values of χ on a quadratic polynomial, which is a well-known and easy exercise; see, for instance, [V54, Chapter 5].) Therefore, letting

$$c := \frac{1}{4}\,(q-2) - \frac{1}{4}\,\chi(-1),$$

we get

$$r_{\mathcal{A}}(g) - c = \begin{cases} \frac{1}{4}\,(1+\chi(-1)q), & g = 0, \\ -\frac{1}{2}\,\chi(g), & g \neq 0. \end{cases}$$

Thus,

$$\sum_{g \in \mathbb{F}_q} \big(r_{\mathcal{A}}(g) - c\big)^2 = \frac{1}{16}\,(q^2 + 2q\chi(-1) + 1) + \frac{1}{4}\,(q-1) = \frac{1}{16}\,q^2 + O(q),$$

which is just by $O(q)$ off from the estimate of Theorem 1.

An interesting feature of Example 1 is that the representation function $r_{\mathcal{A}}$ considered there is nearly constant on the underlying group, with the exception of just one group element. Reversible difference sets provide yet another example of this sort, but we are not going to elaborate here on it, nor on the possibility to extend Example 1 by considering higher-degree residues (which readily leads to the involved subject of cyclotomic numbers).

Our next example shows that for a random subset of an abelian group of odd order, the representation function does not deviate much from its expected value. We need a result which follows, for instance, by combining Theorems A.1.11 and A.1.13 from [AS08].

Proposition 1. *Suppose that $m \ge 1$ is an integer and $p \in (0,1)$ a real number, and let X be a random variable distributed binomially with the parameters n and p. Then for every $0 \le a \le \frac12 np$ we have*

$$\mathsf{P}\left(|X - pn| \ge a\right) < 2e^{-a^2/(4pn)}.$$

For a subset $\mathcal{A}$ of a finite abelian group G we write

$$r'_{\mathcal{A}}(g) := \bigl|\{(a',a'') \in \mathcal{A}\times\mathcal{A}\colon a'+a''=g,\ a'\ne a''\}\bigr|; \quad g\in G.$$

Thus, for instance, if G is of odd order, then for every group element g we have either $r'_{\mathcal{A}}(g) = r_{\mathcal{A}}(g)$, or $r'_{\mathcal{A}}(g) = r_{\mathcal{A}}(g) - 1$.

Example 2. Let G be a finite abelian group of odd order $m := |G|$, and suppose that $8\sqrt{\ln(4m)/m} \le \alpha < 1$. Consider the random subset $\mathcal{A} \subseteq G$ to which every element of G is chosen to belong with probability α, independently from other elements of G. We claim that with probability at least $1/2$ we have

$$\bigl|r'_{\mathcal{A}}(g) - \alpha^2(m-1)\bigr| < 2\sqrt{2m\ln(4m)}\,\alpha$$

for every $g \in G$. To see this we let $a := \sqrt{2m\ln(4m)}\,\alpha$ and observe that for each $g \in G$, the quantity $\frac12 r'_{\mathcal{A}}(g)$ is distributed binomially with the parameters $(m-1)/2$ and α^2, so that in view of Proposition 1,

$$\mathsf{P}\left(\bigl|\tfrac12 r'_{\mathcal{A}}(g) - \tfrac12\,\alpha^2(m-1)\bigr| \ge a\right) < 2e^{-a^2/(2\alpha^2(m-1))} < 2e^{-\ln(4m)} = \tfrac{1}{2m}.$$

Now the claim follows immediately.

With slightly more work we can also show that there is a constant C such that for any finite non-trivial abelian group G and integer $0 \le k \le |G|$, letting $m := |G|$ and $\alpha := k/m$, for a randomly chosen k-element subset $\mathcal{A} \subseteq G$, with probability greater than $1/2$ the inequality

$$|r_{\mathcal{A}}(g) - \alpha^2 m| < C\max\left\{1, \alpha(1-\alpha)\sqrt{m\log m}\,\right\}$$

holds for all $g \in G$.

Next, we present two examples showing that the assumption $\gcd(uv,|G|) = 1$ of Theorem 2 cannot be omitted.

Example 3. Suppose that G is the group of residues modulo a positive integer $m \equiv 4 \pmod 8$, and let

$$\mathcal{A} := \{1, 2, 5, 6, 9, 10, \dots, m-3, m-2\} \subseteq G.$$

Then $2\mathcal{A} = \{0, 2, 4, \dots, m-2\}$ and it is easy to check that every element of G has exactly $m/2$ representations as a sum of an element from $\mathcal{A}$ and an element from $2\mathcal{A}$; that is, $r_{\mathcal{A},2\mathcal{A}} = m/2$.

Example 4. Suppose that $n, t \geq 1$ are integers, denote by G the group of residues modulo $m := n^2 t$, and consider the set $\mathcal{A} := [0, nt) \subseteq G$. Then every element of G is easily seen to have exactly t representations as a sum of an element from $\mathcal{A}$ and an element from $n\mathcal{A} = \{0, n, 2n, \dots, m-n\}$; that is, $r_{\mathcal{A},n\mathcal{A}} = t$.

Example 4 can be slightly modified to show that the conclusion of Theorem 2 cannot be substantially strengthened.

Example 5. For $n, t \geq 1$ integers, denote by G the group of residues modulo $m := n^2 t + 1$, and let $\mathcal{A} := [0, nt) \subseteq G$. Then every element of G has either t or $t+1$ representations as a sum of an element from $\mathcal{A}$ and an element from $n\mathcal{A} = \{0, n, 2n, \dots, m-1-n\}$; thus, $r_{\mathcal{A},n\mathcal{A}}$ is nearly constant in this case.

We notice that in the last example we have $\gcd(n, |G|) = 1$, and that the density of $\mathcal{A}$ is $1/n$, which can range from 0 to 1.

References

[AS08] N. Alon and J.H. Spencer, The probabilistic method, Third edition, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., Hoboken, NJ, 2008. xviii+352 pp.

[DJ96] J.A. Davis and J. Jedwab, Survey on Hadamard difference sets, Proceedings of a special research quarter on Groups, difference sets, and the monster, Columbus, Ohio, United States, 1996, pp. 145 - 156. Publisher: Walter de Gruyter & Co., Hawthorne, NJ, USA

[E96] P. Erdős, On some of my favourite theorems, in: *Combinatorics, Paul Erdős is Eighty*, Vol. 2, eds. D. Miklós et al., Bolyai Soc. Math. Stud. 2, Budapest, 1996; 97–132.

[EF56] P. Erdős and W.H.J. Fuchs, On a problem of additive number theory, *J. London Mat. Soc.* **31** (1956), 67–73.

[MV90] H.L. Montgomery and R.C. Vaughan, On the Erdős–Fuchs theorems, in: *A Tribute to Paul Erdős*, Cambridge University Press, Cambridge, 1990, 331–338.

[V54] I.M. Vinogradov, *Elements of Number Theory*, Dover, 1954.

E-mail address: seva@math.haifa.ac.il

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel

E-mail address: sarkozy@cs.elte.hu

Eötvös Loránd University, Department of Algebra and Number Theory, H–1117 Budapest, Pázmány Péter sétány 1/C, Hungary