Open problems in Columbia, SC

Collected by Misha Rudnev

June 6, 2018

Abstract

This is the list of open problems contributed by { Participants of NSF-CBMS Conference on Additive Combinatorics from a Geometric Viewpoint } \ {Jozsef Solymosi} who gave quite a few as exercises.

Rafal Bystrzycki

Let G be an abelian group and let Γ be a dissociated set in G (a dissociated set is a set with all subset sums distinct). Let us define

$$\Sigma(\Gamma) := \left\{ \sum_{a \in A} a : A \subset \Gamma \right\}.$$

One can ask the following questions:

- Is Γ determined uniquely by $S = \Sigma(\Gamma)$?
- Can Γ be found with an efficient algorithm taking S as an input?

In general, already the answer to the first question is negative in some cases (i.e. if $|G|$ is even), but one can still try to get some conditions satisfied by a group G, which are sufficient to ensure positive answers to those questions. The most interesting case seems to be $G = \mathbb{Z}/p\mathbb{Z}$ for a large prime p and $|S| < p^{1-c}$ for some constant $0 < c < 1$.

Gregory Clark

In his 1977 paper [13], Newman proved the necessary and sufficient conditions for an integer tile $A = [a_1, ..., a_k]$, where k is a prime power, to tile the integer line. By his own admission:

"The very simplest interesting case is that of $k = 3$. If we normalize matters so that our triple is $0, a, b$ with $(a, b) = 1$ the theorem states that tessellation occurs if and only if a and b are, in some order, 1 and 2 $(mod\ 3)$. Surely this special case deserves to have a completely trivial proof-but we have not been able to find one!"

The necessity is immediate: such a tile will clearly tessellate; however, the sufficiency still requires proof.

Problems from Seva Lev and Ilya Shkredov were communicated by Misha Rudnev.

There has been progress made towards his main question: how can we extend the main theorem of Paper 1 to composite numbers (see [3]) but it appears the answer to Newman's "simple" question remains unanswered.

Alexander Clifton, asked by Bruce Landman

Definition 1 *For a set $D \subset \mathbb{N}$, a D-diffsequence of length k is a sequence $x_1 < x_2 < \cdots < x_k$ where $x_i - x_{i-1} \in D$ for $i = 2, \cdots, k$.*

Definition 2 *A set D is r-accessible if every r-coloring of $\mathbb{N}$ contains arbitrarily long monochromatic D-diffsequences.*

The set of primes is not 3-accessible. Is it 2-accessible? If so, what can be said about the smallest N such that every 2-coloring of $[1, N]$ contains a monochromatic {primes}-diffsequence of length k?

Joshua Cooper

The following problem is due to Dudeney (1917), and there very little known about it, despite its extraordinary simplicity and its connection with the important Heilbronn Triangle Problem. This is sometimes called the "no-three-in-a-line" problem.

Question 1 *What is the size* $\textsc{nothree}(n)$ *of the smallest subset S of $[n] \times [n]$ so that no three points of S are collinear?*

Call any such set S "triple-free". Erdős's construction for the Heilbronn Triangle Problem, appearing in the appendix of Roth's 1951 [16] paper on the topic, is the set $\{(x, x^2) : x \in \mathbb{Z}_n\}$ projected into $\mathbb{R}^2$, and the reason it provides a decent lower bound is precisely that it is triple-free. Clearly, if $|S| > 2n$, then by the Pigeonhole Principle at least three points will occur on the same line $\{j\} \times [n]$ for some $j \in [n]$, so $\textsc{nothree}(n) \leq 2n$. (Indeed, the same is true for the lines $[n] \times \{j\}$ as well.) Surely, there are enough lines intersecting $[n] \times [n]$ in many points so that $\textsc{nothree}(n) < 2n$? Indeed, Ellman and Pegg, Jr. (2005), correcting a mistake by Guy and Kelly [8], make a compelling heuristic argument that $\textsc{nothree}(n) = \pi/\sqrt{3} \cdot n + o(n) \approx 1.814n$. Surprisingly, however, there are constructions known for all $n \leq 46$ of $2n$ points in $[n] \times [n]$ with no three collinear.

From the other direction, Hall, Jackson, Sudbery, and Wild [10] showed that $\textsc{nothree}(n) \geq 3/2 \cdot n + o(n)$. Since one can easily show that any triple-free set of size exactly $2n$ can be decomposed into the disjoint union of the graphs of two permutations of n, it is reasonable to study these as well. Cooper and Solymosi [2] showed that any permutation σ of $\mathbb{Z}_n$, for n prime, must admit three collinear points in its graph $\{(x, \sigma(x)) : x \in \mathbb{Z}_n\}$; indeed, they showed that there are always at least $\lceil (n-1)/4 \rceil$ such collinear triples. However, there are many more collinearities in $\mathbb{Z}_n \times \mathbb{Z}_n$ than in $[n] \times [n]$, and they do not resolve this question for n composite.

Dong Dong: Boundedness of a trilinear operator in finite fields

This was asked by Bourgain and Chang [1]. Let p be a prime and $\mathbb{F}_p$ be the finite field. Define a trilinear operator by

$$T(f_1, f_2, f_3)(x) = \frac{1}{p} \sum_{y \in \mathbb{F}_p} f_1(x+y) f_2(x+y^2) f_3(x+y^3). \tag{1}$$

Is there a $\delta > 0$ such that

$$\|T(f_1, f_2, f_3) - Ef_1 Ef_2 Ef_3\|_1 \lesssim p^{-\delta} \|f_1\|_\infty \|f_2\|_\infty \|f_3\|_\infty \tag{2}$$

holds for all complex valued functions f_1, f_2, f_3 defined on $\mathbb{F}_p$? Here

$$Ef := \frac{1}{p} \sum_x f(x)$$

and

$$\|f\|_1 := \frac{1}{p} \sum_x |f(x)|.$$

The above estimate implies the polynomial Szemerédi theorem in finite fields: the main result in [15]. See also [1, 5, 14] for different treatments of the 3-term case. The estimate is proved to be true if we replace $p^{-\delta}$ with $o(p)$ on the right-hand-side [7].

Yifan Jing

Definition 3 *A* star edge coloring *of a graph G is a proper edge coloring of $E(G)$ without bicolored cycles of length 4 or paths of length 4. We use $\chi'(G)$ to denote the minimum number of colors we used in a star edge coloring of G.*

Conjecture 1 (Dvořák, Mohar and Šámal, 2010 [6]) $\chi'(K_n) = \Theta(n)$.

Instead of working on K_n, we can work on the graph $K_{n,n}$, which has a better structure in its line graph. Then the problem becomes the following: we color all the vertices in a $n \times n$ grid, such that every two vertices lie in the same row or column have different colors, and all the four vertices in a *zigzag path* of length four are not bi-colored. Here the four vertices on a *zigzag path* of length four have the form $(a,b),(c,b),(c,d),(e,d)$ or $(a,b),(a,c),(d,c),(d,e)$, see Figure 1.

The best lower bound of $\chi'(K_{n,n})$ is $(2-o(1))n$, by using a simple counting argument. The best upper bound is given by [6], which is still far away from $\Theta(n)$. Their method is the following. They colour the vertex (i,j) by $i+j$, and then remove all the arithmetic progressions of length 3.

Actually we can do it in a more general way. Suppose two sets A and B both have cardinality n, and we color the vertex (i,j) by $a_i + b_j$. In this general setting, probably we can improve the upper bound a little bit, but Szemerédi Theorem tells us we can never get a linear bound in this setting. A new construction is needed.

Figure 1: Zigzag paths of length four.

Seva Lev

1. Almost-blocking sets in finite affine planes. For an odd prime power q, a *blocking set* in the affine plane $\mathbb{F}_q^2$ is a set blocking (meeting) every line.

   A union of two non-parallel lines is a blocking set of size $2q-1$, and it is well-known that this is the smallest possible size of a blocking set in $\mathbb{F}_q^2$. A very simple proof goes as follows. Suppose that $B \subset \mathbb{F}_q^2$ is a blocking set. Translating B appropriately, we can assume that $0 \in B$, and we let then $B_0 := B \setminus \{0\}$. The new set B_0 blocks every line not passing through the origin; that is, every line of the form $ax+by=1$ with $a, b \in \mathbb{F}_q$ not equal to 0 simultaneously. As a result, the polynomial

   $$P(x,y) := \prod_{(a,b)\in B_0} (ax+by-1)$$

   vanishes at every point of $\mathbb{F}_q^2$ with the exception of the origin. Now, if we had $|B_0| < 2p-2$, then $P(x,y)$ would be a linear combination of monomials of the form $x^m y^n$ with $\min\{m,n\} < p-1$, while for every such monomial,

   $$\sum_{x,y\in\mathbb{F}_q} x^m y^n = 0;$$

   this would lead to

   $$\sum_{x,y\in\mathbb{F}_q} P(x,y) = 0,$$

   a contradiction.

   > Suppose now that $B \subset \mathbb{F}_q^2$ blocks every line *with the possible exception of at most one line in every direction*. What is the smallest possible size of such an "almost blocking" set?

   If $B \subset \mathbb{F}_q^2$ is almost blocking, then pairing in an arbitrary way the non-blocked lines and adding to B the intersection points of these pairs of lines we get a "usual" blocking set; since we had to add at most $(q+1)/2$ points, this gives

   $$|B| \geqslant (2q-1) - \frac{q+1}{2} = \frac{3}{2}(q-1).$$

On the other hand, it is not difficult to construct almost-blocking sets $B \subset \mathbb{F}_q^2$ with

$$|B| < 2q - \sqrt{q}.$$

Is the smallest possible size of an almost blocking set "essentially $\frac{3}{2}\,q$" or "essentially $2q$" (or neither)?

2. Weighting pencils. Suppose that p is a prime, and $k < p/2$ a positive integer.

   Consider a system of k pencils in the affine plane $\mathbb{F}_p^2$, where each pencil is just a set of p parallel lines in some direction (unique for each pencil). Suppose, furthermore, that the p lines of every pencil are assigned some integer weights so that the weight functions are not constant; that is, the lines of a pencil cannot all share the same common weight. To every point $x \in \mathbb{F}_p^2$ there corresponds a unique line from every pencil incident to x, and we define the weight of x to be the sum of the weights of these k lines. How many zero-weight points can there be?

   Clearly, for $k = 1$ we can have just p points with non-zero weights (and cannot have fewer than that). For $k = 2$ there can be as few as $2(p-1)$ non-zero-weight points; it is easy to prove this and to construct an example with that many non-zero-weight points. For $k = 3$ it is not difficult to assign the weights so that there are $3p - 5$ non-zero-weight points, which turns out to be sharp for p large enough.

   > Is it true that for any $3 \leqslant k < p/2$ there are at least $3p-5$ points with non-zero weights?

3. "Small" zero divisors in $\mathbb{C}[\mathbb{Z}/p\mathbb{Z}]$

   If p is a prime, and a, b are non-zero elements of the group algebra $\mathbb{C}[\mathbb{Z}/p\mathbb{Z}]$ satisfying $a * b = 0$, then

   $$|\text{supp } a| + |\text{supp } b| \geqslant p + 2.$$

   This is easy to prove using characters, but is there a reasonably simple elementary argument? Is this fact somehow related to the Cauchy-Davenport theorem? How does it extend onto the group algebras $\mathbb{C}[\mathbb{Z}/m\mathbb{Z}]$ with m composite?

Vlad Alexandru Matei

1. The first one has to do with the so-called diophantine tuples over finite fields. The starting paper is [4] I worked over the last summer with a group of high school trying to crack at least an elementary upper bound for a set $A \subset \mathbb{F}_p$ such that $ab + 1$ is a square for any $a \neq b \in A$. Unlike the Paley graph I could not see any elementary argument.

   What you can prove in a similar way is that you get a pseudorandom graph and you can control things a bit. What is sadder, is that I tried, without any luck, to get this work in $\mathbb{F}_p^2$ at least. It should be true that the maximum such set should have size p, with the obvious example being $\mathbb{F}_p$.

   Brendan Murphy showed me that you can use the same approach as for Paley using characters to show that you get the same bound as for Paley $\sqrt{p}$. This finishes the second part.

The question is whether we can go beyond $\sqrt{p}$. My guess is that this would as hard as Paley. Alternatively one can use the sum product graph to get a weaker bound $c\sqrt{p}$

2. Another intriguing numerical experiment that I did with my students, is to do $ab+$ a non-quad residue. It seems that there is actually a discrepancy in the maximal size of such a set with the maximal size for $ab+1$ even for small values of p.

3. The first problem is to show that if $p \equiv 1 \bmod 4$ is prime, and a set $A \subset \mathbb{F}_p$ has the property that the difference of any two elements of A is a square, then A is "small". (Basic details can be found here). If Q is the set of squares in $\mathbb{F}_p$, one can write the assumption as $A - A \subseteq Q$.

   The second problem, to my knowledge first posed by A. Sarkozy several years ago, is to determine whether the set of all squares is as a sumset; that is, whether $Q = A + B$ with some $A, B \subset \mathbb{F}_p$, each of cardinality at least 2. The conjectural answer is, of course, negative, provided that p is sufficiently large.

   Both problems just mentioned seem to be quite tough; but, maybe, the following combination of the two is more tractable:

   For a prime $p \equiv 1 \bmod 4$ does there exist $A \subset \mathbb{F}_p$ such that $Q = A - A$?

   Compared to the first of the two aforementioned problems, we now assume that every quadratic residue is representable as a difference of two elements of A; compared to the second problem we assume that $B =?A$. Is there a way to utilize these extra assumptions?

   A funny observation is that sets A with the property in question do exist for $p = 5$ and also for $p = 13$; however, it would be very plausible to conjecture that these values of p are exceptional. (In this direction, Peter Mueller has verified computationally that no other exceptions of this sort occur for $p < 1000$.)

Giorgis Petridis et al

1. Let $\Gamma \subset (\mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\})$ (prime p) be a multiplicative subgroup. Konyagin and Heath-Brown [9] proved that if $|\Gamma| \geq p^{2/3}$, then $|\Gamma + \Gamma| = \Omega(p)$. Can one do better? Does there exist an absolute $c > 0$ such that if $|\Gamma| \geq p^{2/3-c}$, then $|\Gamma + \Gamma| = \Omega_c(p)$?

2. (Misha Rudnev) Related to the above question.

   (a) V'yugin and Shkredov [18] boosted the [9] application of Stepanov's method to sums of multiplicative subgroups to a variant of the Szemerédi-Trotter incidence bound (with the same numerology), which applies in $\mathbb{F}_p^2$ to (sufficiently small in terms of p) sets of points and lines, which are Cartesian products of sets invariant with respect to multiplication by a multiplicative subgroup Γ. This enabled them to prove that $|\Gamma - \Gamma| \gg |\Gamma|^{5/3}$ (as well as $|\Gamma + \Gamma| \gg |\Gamma|^{8/5}$) but only for $|\Gamma| < \sqrt{p}$, regarding the previous question. For the state of the art estimates and references see [12].

   However, the Stepanov-type approach does not seem to work if one replaces the multiplicative subgroup by a geometric progression G, say $G = \{1, g, \dots, g^{|G|-1}\}$,

where g is a generator of $\mathbb{F}_p^\times$: one only knows, for any $|G|$ that $|G \pm G| \gg \min(|G|^{3/2}, p)$. *Problem:* improve this, say for $|G| < \sqrt{p}$.

(b) As far as similarity with applications of the Szemerédi-Trotter theorem to real/complex sets with "small but not too small" multiplicative doubling is concerned, [12] presents inequalities *with the same powers* of $|A|$ replacing $|\Gamma|$, for, say $A \subset \mathbb{R}: \ |AA| = K|A|$, the bound now also depending on powers of K, where $K \sim |A|^\epsilon$. For much smaller K the subspace theorem gives much stronger bounds but they break down around $K \sim \log |A|$.

Curiously, the above-mentioned "multiplicative subgroup Szemerédi-Trotter theorem" enables somewhat stronger consequences than the Szemerédi-Trotter theorem itself, applied to sets with small multiplicative doubling.

Namely, for a set A, let a *k-fence*, $k \geq 2$ be a subset $\{a_1, \dots, a_k\} \subset A$, which is fixed within A up to a translation. I.e., the set of $k-1$ differences $D_{k-1} := \{a_i - a_{i-1}, \ i = 2, \dots, k\}$ is fixed. What is the maximum number $M_k(A)$ of translated copies of a k-fence in a set A with small multiplicative doubling?

To this effect, V'yugin and Shkredov [18] prove that if $|\Gamma|$ is a sufficiently small multiplicative subgroup, then for any k-fence, $M_2(\Gamma) \ll |\Gamma|^{2/3}$, and then the maximum of $M_k(\Gamma)$ goes nicely to $|\Gamma|^{1/2}$ as k grows. Never mind that presumably $M_2(\Gamma) \lesssim 1$.

However, no estimate of this kind is known over the reals in the following context. Suppose $|AA| = K|A|$, for $A \subset \mathbb{R}$ and $K \sim |A|^\epsilon$. The Szemerédi-Trotter theorem easily implies that $M_2(A) \ll K^{4/3}|A|^{2/3}$. Can one prove $M_k(A) \ll_{K(k)} |A|^{2/3-\delta_k}$, where the symbol $\ll_{K(k)}$ swallows a power of K that would depend on k in a reasonable way? The known bound for the maximum number of appearances of a 3-fence inside A is just the one for a 2-fence, not better. A tempting 2D-analogue of this question is, of course, the maximum number of realisations of a given triangle in $A \subset \mathbb{R}^2$, where there seems to be no better known general bound than $O(|A|^{4/3})$ – the one for a single distance.

3. (Boris Bukh). Let $A \subset \mathbb{Z}$ (or even a subset of any commutative group). Define

$$A + 2.A = \{a + 2b : a, b \in A\}.$$

Suppose that $|A + A| \leq K|A|$. Plünnecke's inequality implies

$$|A + 2.A| \leq |A + A + A| \leq K^3|A|.$$

Can one do better? Does there exist an absolute $c > 0$ such that $|A + 2.A| \leq c^{-1}K^{3-c}|A|$? Both inequalities above are sharp in some cases but it seems unlikely that they would both be essentially sharp for the same set.

Cosmin Pohoata

A problem of Lê and Tao from [11] asks to estimate the size of the largest subset A inside $\{1, \dots, n\}$ such that $A - A \cap K = \{0\}$, where K represents the set of integers only having digits 0 or 1 in base 3. In the survey, they mention that the density Hales-Jewett theorem implies that

$|A| = o(n)$. I'd like to revive this nice question by also providing a short argument for the fact that $|A| = O(n/\log n)$.

Proof. Consider the translates of A of the form

$$A_k := A + \left\{1 + 3 + \ldots + 3^k\right\},$$

where $1 \leq k \leq \log_3 n$. Note that if A is in $\{1, .., n\}$ then A_k is in $\{1, \ldots, 2n\}$. Also, from $A - A \cap K = \{0\}$ it is easy to see that these sets are disjoint. In particular, $\log_3 n \cdot |A| \leq 2n$, which proves the claim.

□

It would be interesting to improve on this easy estimate. The simple argument resembles a bit the proof of the classical Minkowsky lattice point theorem theorem. It would be interesting if more (nontrivial) geometry of numbers could be used to say new things about intersective sets.

Also, two new questions:

1. What is the largest $A \subset \mathbb{F}_p^n$ with the property that if $(x, x + d, x + 2d)$ is a three-term progression in A^3 with $d \in 0, 1^n$, then $d = 0$?

   In the paper above, Lê mentions a construction of Alon, which provides an example of a set A in $\mathbb{F}_p^n$ of size $|A| \gg (p-1)^n/p\sqrt{n}$ with this property: consider the set of all vectors $(a_0, \ldots, a_{n-1})$ with $0 \leq a_i \leq p-2$ and such that

   $$\sum_{i=0}^{n-1} a_i = \left\lfloor \frac{n(p-2)}{2} \right\rfloor \quad \text{(as integers)}.$$

   In fact, this example has the stronger property that $A - A \cap \{0, 1\}^n = \{0\}$.

2. What is the largest $A \subset \{1, \ldots, n\}$ with the property that if $(x, x+d, x+2d)$ is a three-term progression in A^3 with $d \in K$, then $d = 0$? Here, K stands again for the set of integers only having digits 0 or 1 in base 3.

   Clearly, the Behrend subset of size $|A| \gg n \exp^{-c\sqrt{\log n}}$ without nontrivial three-term progressions is an example of such a set.

Ilya Shkredov

1. Let Γ be a subgroup of $\mathbb{F}_p^*$, $|\Gamma| > p^{\varepsilon}$. Prove that there is $k = k(\varepsilon)$ such that $(\Gamma - \Gamma)^k = \mathbb{F}_p$.

2. Let $A \subseteq \mathbb{F}_p$ be a sufficiently small set, say, $|A| < \sqrt{p}$ such that $|AA| \leqslant M|A|$. Prove that the number of collinear triples in $A \times A$ is $O_M(|A|^4)$. Prove that the number of solutions to the equation $a_1 + a_2 + a_3 = a_4 + a_5 + a_6$, $a_j \in A$ is $O_M(|A|^4)$.

George Shakan

1. Improve on the bound

   $$\sum_{b \in B} E^+(A, bA) \ll |A|^3 |B| (\max(|B|^{-1/3}, (p/|A|)^{-1/3}).$$

2. The Hilbert cube number is bounded by $(2r)^{2^m}$. Improve this.

3. Prove[†] that $|A+A| \gtrsim |A|^2 d^+(A)^{-1}$. See [17] for definitions and context. As a warm up, one may wish to prove $|A+A| \gtrsim |A|^{5/3} d^+(A)^{-2/3}$.

Michael Tait

Here is a problem which to my knowledge is open: what is the largest set of perfect squares up to n such that $x^2+y^2 = z^2+w^2$ implies that $\{x,y\} = \{z,w\}$? That is, what is the largest size of a Sidon subset of perfect squares? Cilleruelo and his student did some work on Sidon sequences of squares rather than sets. I'm not sure if anyone has published anything regarding this, but the best that I can do is to show that this largest size is somewhere between roughly $\frac{n^{1/3}}{\text{polylog}n}$ and $o(n^{1/2})$.

References

[1] J. Bourgain, M.C. Chang, *Nonlinear Roth type theorems in finite fields*, Israel J. Math. **221**(2): 853–867, 2017.

[2] J. Cooper, J. Solymosi, *Collinear points in permutations*, Ann. Comb. **9**(2): 169–175, 2005.

[3] E. M. Coven, A. Meyerowitz, *Tiling the Integers with Translates of One Finite Set,* J. Alg. **212,**(1): 161–174, 1999.

[4] A., Dujella, M. Kazalicki, *Diophantine m-tuples in finite fields and modular forms,* arXiv:1609.09356v2 [math.NT], 31 Jan. 2018.

[5] D. Dong, X. Li, W. Sawin, *Improved estimates for polynomial Roth type theorems in finite fields*, arXiv:1709.00080v3 [math.NT], 1 Oct 2017.

[6] Z. Dvořák, B. Mohar, R. Sámal, *Star chromatic index,* J. Graph Th., **3**: 313–326, 2013. https://arxiv.org/abs/1709.00080

[7] N. Frantzikinakis, B. Kra, *Polynomial averages converge to the product of integrals*, Israel J. Math. **148**: 267–276, 2005.

[8] R. K. Guy, P. A. Kelly, *The no-three-in-line problem*, Canad. Math. Bull. **11**: 527–531, 1968.

[9] R. D. Heath-Brown, S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum,* Q. J. Math. **51**(2): 221–235, 2000.

[10] R. R. Hall, T. H. Jackson, A. Sudbery, A., K. Wild, *Some advances in the no-three-in-line problem* J. Combinatorial Theory Ser. A **18**: 336–341, 1975.

[†]A monetary prize of USD 100 is offered.

[11] T. H. Lê, *Problems and Results on Intersective Sets.* In: Nathanson M. (eds) Combinatorial and Additive Number Theory. Springer Proceedings in Mathematics & Statistics, vol 101. Springer, New York, NY.

arXiv: [pdf, ps, other] math.CO

[12] B. Murphy, M. Rudnev, I. D. Shkredov, Yu. N. Shteinikov, *On the few products, many sums problem,* arXiv:1712.00410 [math.CO], 1 Dec 2017.

[13] D. J. Newman, *Tesselation of integers,* J. Num. Th., **9**(1): 107–111, 1997.

[14] S. Peluse, *Three-term polynomial progressions in subsets of finite fields*, arXiv:1707.05977 [math.CO], 19 Jul 2017.

[15] S. Peluse, *On the polynomial Szemerédi's theorem in finite fields*, arXiv:1802.02200 [math.NT], 6 Feb 2018.

[16] K. F. Roth, *On a problem of Heilbronn,* J. London Math. Soc. **26**: 198–204, 1951.

[17] G. Shakan, *On higher energy decompositions and the sum-product phenomenon,* arXiv:1803.04637 [math.NT], 13 Mar 2018.

[18] I. V. V'yugin, I. D. Shkredov, *On additive shifts of multiplicative subgroups,* Sb. Math. **203**(5-6): 844–863, 2012.