A lattice point problem and additive number theory *

Noga Alon and Moshe Dubiner
Department of Mathematics
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv, Israel

Abstract

For every dimension $d \geq 1$ there exists a constant $c = c(d)$ such that for all $n \geq 1$, every set of at least cn lattice points in the d-dimensional Euclidean space contains a subset of cardinality precisely n whose centroid is also a lattice point. The proof combines techniques from additive number theory with results about the expansion properties of Cayley graphs with given eigenvalues.

1 Introduction

Let $f(n, d)$ denote the minimum possible number f so that every set of f lattice points in the d-dimensional Euclidean space contains a subset of cardinality n whose centroid is also a lattice point. The problem of determining or estimating $f(n, d)$ was suggested by Harborth [12], and studied by various authors.

By an old result of Erdős, Ginzburg and Ziv [8], $f(n, 1) = 2n-1$ for all n. For the general case, the following simple bounds are proved in [12]:

$$(n-1)2^d + 1 \leq f(n, d) \leq (n-1)n^d + 1 \tag{1}$$

$$f(n_1 n_2, d) \leq f(n_1, d) + n_1(f(n_2, d) - 1) \tag{2}$$

The inequality (2) implies that if equality holds in the lower bound of (1) for (n_1, d) and for (n_2, d), then equality holds for $(n_1 n_2, d)$ as well. Therefore, since it is easy to see that $f(2, d) = 2^d + 1$, it follows that $f(2^a, d) = (2^a - 1)2^d + 1$ for all $a \geq 1$. Similarly, as shown by Kemnitz [13], $f(p, 2) = 4p - 3$ for $p = 2, 3, 5, 7$ and hence $f(n, 2) = 4n - 3$ for all $n = 2^a 3^b 5^c 7^d$. It is conjectured

[*] Combinatorica, 15 (1995), 301-309.

in [13] that the lower bound in (1) is tight for $d = 2$, i.e., that $f(n, 2) = 4n - 3$ for all n, but this is still open, although in [2] it is shown that $f(n, 2) \leq 6n - 5$ for all n and that $f(p, 2) \leq 5p - 2$ for every sufficiently large prime p.

For $d > 2$ it is known that the lower bound in (1) is not tight, in general. Various researchers observed that $f(3, 3) \geq 19$ $(> 8 \cdot 2 + 1)$. Examples appear in [12], [7], [13], [14], where it is also shown that in fact $f(3, 3) = 19$. As shown in [13], $f(3, 4) = 41$. By the main result of [6], [10], $f(3, d) = o(3^d)$ as d tends to infinity. The problem of determining $f(n, d)$ precisely for all n and d seems extremely difficult.

In the present short paper we focus on the problem of estimating $f(n, d)$ for a fixed dimension d and large n, in an attempt to extend the results of [8] and [2] that deal with the cases $d = 1$ and $d = 2$, respectively. Our main result is that for every fixed dimension d, $f(n, d) \leq c(d)n$, where $c(d)$ is a constant depending only on the dimension d.

It is convenient to reformulate the definition of $f(n, d)$ in terms of sequences of elements of the abelian group Z_n^d. If S is a sequence of (not necessarily distinct) elements of an abelian group, and T is a subsequence of S containing m elements, T is an *m-subsequence*. If the sum of elements in T is the identity 0 of the group, T is a *zero-sum subsequence*. In this notation, $f(n, d)$ is the minimum possible f so that every sequence of f members of Z_n^d contains a zero-sum n-subsequence. Our main result is the following.

Theorem 1.1 *There exists an absolute constant $c > 0$ so that for all n, every sequence of at least $(cd \log_2 d)^d n$ (not necessarily distinct) elements of Z_n^d contains a 0-sum n-subsequence. Therefore, $f(n, d) \leq (cd \log_2 d)^d n$.*

The proof of Theorem 1.1 is presented in the next section. It combines techniques from additive number theory with results about the expansion properties of graphs with given eigenvalues. These expansion results are applied to appropriately defined Cayley graphs of abelian groups whose eigenvalues can be easily computed in terms of the multiplicative characters of the groups.

To simplify the presentation, we do not make any attempt to optimize the absolute constants in our various estimates. We also omit all floor and ceiling signs whenever these are not crucial.

2 The proof

It is not difficult to check that by (2) it suffices to prove Theorem 1.1 for primes $n = p$. For this case, Z_p^d is a linear space, and our proof proceeds by induction on the dimension d. The basic idea is, roughly, as follows. If our sequence contains sufficiently many members in a lower dimensional (affine) subspace we can apply induction. Otherwise, we show that *every* vector $v \in Z_p^d$ is a sum of precisely p members of the sequence. This is done by finding pairwise disjoint subsequences $A_1, \ldots, A_r$ of the given sequence so that the cardinality of $A_1 + \cdots + A_i$ grows sufficiently quickly to ensure that every vector is in the sum $A_1 + \cdots + A_r$, where $r \leq p$. The detailed proof combines tools from additive number theory with graph theoretical techniques and is presented in the next three subsections.

2.1 Adding linear bases of vector spaces

Let p be a prime. A *hyperplane* in Z_p^d is the set of all vectors v of Z_p^d so that $u \cdot v = b$, where here u is a nonzero vector in Z_p^d, $b \in Z_p$, and $u \cdot v$ denotes the usual inner product of u and v over the field Z_p. An *affine basis* of Z_p^d is a set of $d+1$ vectors in Z_p^d which is not contained in a hyperplane.

Proposition 2.1 *Let $x \leq p/4d$ be a power of 2, and let $A_1, A_2, \ldots, A_s$ be s affine bases of Z_p^d, where $s = 4xd$. Then*

$$|A_1 + A_2 + \cdots + A_s| \geq x^d.$$

The proof presented below is a rather simple consequence of the following result of Ruzsa, proved in [19] by applying the elegant graph theoretical technique of Plünnecke [18].

Lemma 2.2 ([19], Corollary 5.2) *If Y and B are finite subsets of an abelian group and $h \geq 1$ is an integer, then*

$$|Y + B| \geq |Y|(\frac{|hB|}{|Y|})^{1/h}.$$

Corollary 2.3 *Let Y be a subset of Z_p^d and let B be an affine basis of Z_p^d. If $|Y| \leq x^d$ for some integer $x \leq p/4d$ then $|Y + B| \geq |Y| 2^{1/(2x)}$.*

Proof By an affine transformation we may assume that B is the set consisting of the 0-vector and the d unit vectors. If $h = 2xd$, then hB contains all the vectors in which every coordinate is at most $2x$ and hence $|hB| \geq (2x)^d$. The desired result now follows from Lemma 2.2. □

Proof of Proposition 2.1 Start with the set Y_1 of cardinality 1 containing only the zero vector and with $x_1 = 2$ and repeatedly apply the last corollary, applying it first with $Y = Y_1$ and $B = A_1$, then with $Y = Y_1 + A_1$ $(= A_1)$ and with $B = A_2$ and so on. By the corollary, after $j \leq 2dx_1$ such steps the resulting set $Y = A_1 + \cdots + A_j$ is of size at least x_1^d. Define $x_2 = 2x_1$ and repeat this process with the next affine bases, until the set Y of sums given by $Y = A_1 + A_2 + \cdots + A_i$ contains at least x_2^d members. By the corollary, this will happen after at most $2dx_2$ additional steps. Continuing in this manner the desired result follows. □

Remark An alternative proof of Proposition 2.1 can be given, based on the main result of [15] (see also [3], Lemma 6.9). The proof presented above is somehwat shorter.

2.2 Expansion and set addition

In this subsection we prove the following result.

Proposition 2.4 *Suppose $W \geq 1$, let A be a sequence of elements of Z_p^d and suppose that no hyperplane contains more than $|A|/4W$ members of A. Then, for every subset $Y \subset Z_p^d$ of at most $p^d/2$ elements of Z_p^d there is an element $a \in A$ such that*

$$|(a+Y) \setminus Y| \geq \frac{W}{16p}|Y|.$$

In order to prove this assertion, we need the following known facts.

Lemma 2.5 ([9], see also [17], [1]) *Let Y be a finite subset of an abelian group G, suppose $a \in G$ and let i be a positive integer . Then*

$$|(-a+Y) \setminus Y| = |(a+Y) \setminus Y| \tag{3}$$

$$|(ia+Y) \setminus Y| \leq i \cdot |(a+Y) \setminus Y| \tag{4}$$

It is worth noting that some variant of (4) can be deduced from Lemma 2.2, but the estimate here is better for our purposes.

If $H = (V, E)$ is a loopless multigraph, the *adjacency matrix* of H is the symmetric matrix $(a_{uv})_{u,v \in V}$, where $a_{u,v}$ is the number of parallel edges between u and v. The *eigenvalues of H* are the eigenvalues of this matrix. Note that if H is Δ-regular the largest eigenvalue of H is Δ.

Lemma 2.6 ([4], see also [5], page 120) *Let $H = (V, E)$ be a Δ-regular loopless multigraph and let λ denote the second largest eigenvalue of H. Let $V = Y \cup Z$ be a partition of V into two disjoint sets, and let $e(Y, Z)$ denote the number of edges of H that have one end in Y and one end in Z. Then*

$$e(Y, Z) \geq (\Delta - \lambda)\frac{|Y||Z|}{|V|}.$$

Let G be a finite abelian group, and let S be a multiset of elements of G so that $0 \notin S$ and the number of occurences of each s in S is equal to the number of occurences of $-s$ in S. The *Cayley graph $H = H(G, S)$* is the $|S|$-regular (multi-) graph whose set of vertices is G in which for each $g \in G$ and each element s that appears l_s times in S there are l_s parallel edges joining g and $g + s$.

Lemma 2.7 (see, e.g., [16]) *Let G, S and $H = H(G,S)$ be as above. Then, the eigenvalues of H are the numbers*

$$\sum_{s \in S} \chi(s),$$

where χ ranges over all the multiplicative characters of G.

Proof of Proposition 2.4 Put $G = Z_p^d$. For each $a \in A$ let S_a be the multiset

$$\{a, 2a, 3a, \ldots, 2\lceil p/W \rceil a\} \cup \{-a, -2a, -3a, \ldots, -2\lceil p/W \rceil a\}.$$

Let S be the multiset of elements of G consisting of the union (with repetitions) of the multisets S_a, as a ranges over all members of A. Put $\Delta = |S| = 4\lceil p/w \rceil |A|$, and let $H = H(G,S)$ be the corresponding Cayley graph. This graph is Δ-regular. We claim that its second largest eigenvalue is at most $3\Delta/4$. To see this observe that by Lemma 2.7, each nontrivial eigenvalue of H is of the form

$$\sum_{s \in S} w^{v \cdot s} = \sum_{a \in A} \sum_{s \in S_a} w^{v \cdot s},$$

where here $w = e^{\frac{2\pi i}{p}}$, $\cdot$ denotes the usual product over Z_p, and v is some nonzero member of G. Fix such a v. For $a \in A$ let $v \cdot a$ be the product of a and v in Z_p represented so that $-p/2 < v \cdot a \le p/2$. By assumption, for each fixed $b \in Z_p$, there are at most $|A|/4W$ members a of A so that $v \cdot a = b$. Therefore, for at least $|A|/2$ members $a \in A$, $|v \cdot a| \ge p/W$. For each such a, if $l = |v \cdot a|$ $(\ge W)$ and $r = 2\lceil p/W \rceil$, then

$$\sum_{s \in S_a} w^{v \cdot s} = w^l(1 - w^{rl})/(1 - w^l) + w^{-l}(1 - w^{-rl})/(1 - w^{-l}).$$

Therefore

$$|\sum_{s \in S_a} w^{v \cdot s}| \le \frac{4}{|1 - w^l|} \le \frac{8}{W 2\pi/p} < 2p/W \le r.$$

Since this is the case for at least $|A|/2$ members of A, we conclude that

$$|\sum_{a \in A} \sum_{s \in S_a} w^{v \cdot s}| \le \frac{|A|}{2} r + \frac{|A|}{2} 2r = 3\Delta/4,$$

as claimed.

Let $Y \subset Z_p^d = G$ be a set of at most half the members of G. Put $Z = G \setminus Y$. By Lemma 2.6 and the above estimate for the eigenvalues of H there are at least $\frac{\Delta}{4}|Y||Z|/|G| \ge \Delta|Y|/8$ edges of H with one end in Y and another in $G \setminus Y$. This means that there are at least $\Delta|Y|/8$ ordered pairs (y, s) with $y \in Y$ and $s \in S$ so that $y + s \notin Y$. By averaging, it follows that there is some fixed $s' \in S$ so that the number of members y of Y for which $y + s' \notin Y$ is at least $|Y|/8$. By the definition of S, there is an $\epsilon \in \{-1,1\}$, a positive integer $j \leq 2p/W$ and an $a \in A$ so that $s' = \epsilon ja$. Hence $|(\epsilon ja+Y)\setminus Y| \geq |Y|/8$ and by the two parts of Lemma 2.5, $|(a+Y)\setminus Y| \geq |Y|/8j \geq \frac{W}{16p}|Y|$, completing the proof of the proposition. □

2.3 The proof of the main result

We can now prove Theorem 1.1. Observe, first, that it suffices to prove it for the case of prime $n = p$, since if $f(p,d) \leq cp$ for every prime p then $f(p,d) \leq 2cp - (2c-1)$ for every such p, and hence, by (2), $f(n,d) \leq 2cn - (2c-1) \leq 2cn$ for all n. We thus assume that $n = p$ is a prime and prove that

$$f(p,d) \leq c(d)p \tag{5}$$

for every prime p by induction on the dimension d, where the constants $c(d)$ are defined as follows.

$$c(1) = 2 \ \text{ and } \ c(d) = 256(d\log_2 d+5)c(d-1)+(d+1) \ \text{ for } \ d \geq 2 \tag{6}$$

It is easy to see that the constants $c(d)$ above satisfy, indeed, $c(d) \leq (cd\log_2 d)^d$ for some absolute constant c. Observe, also, that we may assume that, say, $p > 32d$ since otherwise the assertion of the theorem follows trivially from (1).

To start the induction note that since as proved in [8] $f(p,1) = 2p-1$ for all p, (5) holds for $d = 1$, with $c(1) = 2$. Assuming (5) holds for $d-1$ we prove it for d (≥ 2). Let S be a sequence of at least $c(d)p$ (not necessarily distinct) elements of Z_p^d. If there are at least $c(d-1)p$ elements of S on a hyperplane, then, by the induction hypothesis, there is a 0-sum p-subsequence among these, and there is nothing to prove. Hence, we may and will assume that there is no hyperplane containing at least $c(d-1)p$ members of S. We next show that in this case we can find pairwise disjoint subsets $A_1,\ldots,A_s,B_1,\ldots B_t,A'_1,\ldots A'_{s'},B'_1,\ldots,B'_{t'}$ of S, with the following properties. The cardinality of each A_i and each A'_i is $d+1$, the cardinality of each B_j and each B'_j is 2, $s+t+s'+t' \leq p$,

$$|A_1+\ldots+A_s+B_1+\ldots+B_t| > p^d/2, \tag{7}$$

and

$$|A'_1+\ldots+A'_{s'}+B'_1+\ldots+B'_{t'}| > p^d/2.$$

This will show that

$$A_1+\ldots+A_s+B_1+\ldots+B_t+A'_1+\ldots+A_{s'}+B'_1+\ldots+B'_{t'} = Z_p^d,$$

i.e., every element of Z_p^d is a sum of $s+t+s'+t'$ ($\leq p$) members of S. By choosing an arbitrary set of $p-s-t-s'-t'$ members of S that do not lie in the A_i, A'_i, B_j and B'_j and by writing the summation of their inverses as such a sum, we will get the desired 0-sum p-subsequence and complete the proof.

It remains to prove the existence of the sets A_i, A'_i, B_j, B'_j with the above properties. We construct these sets one by one, as shown below. Put $W = 64(d\log_2 d + 5)$ and observe that by (6),

$$\frac{c(d)p - p(d+1)}{4W} = c(d-1)p.$$

This means that even if we delete any set of at most $p(d+1)$ members of the sequence S, there is no hyperplane containing more than a fraction of $1/4W$ of the remaining part of the sequence. Therefore, even after some of the sets A_i, A'_i, B_j, B'_j will be defined, the remaining part of our sequence S will still satisfy the assumptions in Proposition 2.4 which will be useful in the definition of the other required sets.

We now turn to the construction of the above sets. The construction of the sets A_i, A'_i is simple. Let x be a power of 2 satisfying

$$\frac{p}{32d} \leq x \leq \frac{p}{16d}.$$

Put $s = s' = 4xd$ $(\leq p/4)$ and let $A_1, \ldots, A_s$ and $A'_1, \ldots, A'_{s'}$ be pairwise disjoint subsequences of S, each forming an affine basis of Z_p^d. Observe that these bases certainly exist, and can be extracted from S one by one, since during this procedure the remaining part of S cannot lie on a hyperplane (in fact, there is no hyperplane containing even a fraction of $1/4W$ of this remaining part). By proposition 2.1

$$|A_1 + \ldots + A_s| \geq x^d \geq (\frac{p}{32d})^d, \tag{8}$$

and a similar estimate holds for the sets A'_i.

We next define the sets $B_1, \ldots, B_t$. Put $Y = A_1 + \ldots + A_s$. If $|Y| > p^d/2$ we do not need any set B_i, as (7) already holds. Otherwise, let S' denote the subsequence of S without the members of the sets A_i and A'_i, let s' be an arbitrary member of S', and apply Proposition 2.4 to $A = -s' + S'$ and Y. By the proposition, there is an $a \in A$ so that

$$|(a+Y) \cup Y| \geq (1 + \frac{W}{16p})|Y|.$$

Define $B_1 = \{a + s', s'\}$ $(\subset S')$ and observe that

$$|Y + B_1| = |(a+Y) \cup Y| \geq (1 + \frac{W}{16p})|Y|.$$

Next, update Y to be $Y = A_1 + \ldots + A_s + B_1$ and update S' by omitting from it the elements of B_1. If, now, $|Y| > p^d/2$ there is no need for any other sets B_j. Otherwise, apply, again, Proposition 2.4 as above to get another set B_2 for which

$$|A_1 + \ldots A_s + B_1 + B_2| \geq (1 + \frac{W}{16p})|A_1 + \ldots A_s + B_1|.$$

Continuing in this manner we keep defining sets B_j until the required inequality (7) holds. Since in each step the cardinality of the sum $A_1 + \ldots + B_j$ is multiplied by at least $(1 + W/16p)$ it is easy to see that by (8), the number of steps will not exceed $\frac{16p}{W} \log((32d)^d) \leq p/4$. Once this happens, the sets B'_j can be defined in a similar manner, where the fact that Proposition 2.4 can be applied follows from the remark following the definition of W. This completes the description of the construction, and the assertion of Theorem 1.1 follows. □

3 Open problems

The problem of determining $f(n, d)$ precisely for all n and d remains, of course, wide open, and seems to be very difficult. It seems plausible to conjecture that the estimate in Theorem 1.1 can be improved and that in fact there exists some absolute constant c so that $f(n, d) \leq c^d n$ for all n and d.

Another conjecture, mentioned in Section 1, is the one in [13] asserting that $f(n, 2) = 4n - 3$ for all n. See [2] for some work on this question, including a proof that $f(n, 2) \leq 6n - 5$ for all n. This proof is based on algebraic tools, and does not yield any higher dimensional extensions.

The case of small n and large dimension d is also interesting. In [6], [10] it is shown that $f(3, d) = o(3^d)$ as d tends to infinity, but it is not known if there is an absolute $\delta > 0$ so that $f(3, d) \leq (3 - \delta)^d$ for all sufficiently large d. More generally, it is not difficult to deduce from the main result of [11] that for every fixed $n > 2$, $f(n, d) = o(n^d)$ as d tends to infinity, but the problem of finding a sharper estimate for this range of n and d remains open.

References

[1] N. Alon, *Subset sums*, J. Number Theory 27 (1987), 196-205.

[2] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, to appear.

[3] N. Alon, R. M. Karp, D. Peleg and D. B. West, *A graph-theoretic game and its application to the k-servers problem*, to appear.

[4] N. Alon and V. D. Milman, λ_1*, isoperimetric inequalities for graphs and superconcentrators*, J. Combinatorial Theory, Ser. B 38(1985), 73-88.

[5] N. Alon and J. H. Spencer, **The probabilistic method**, Wiley, 1991.

[6] T. C. Brown and J. C. Buhler, *A density version of a geometric Ramsey theorem*, J. Combinatorial Theory, Ser. A 32 (1982), 20-34.

[7] J. L. Brenner, Problem 6298, Amer. Math. Monthly 89 (1982), 279-280.

[8] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel 10F (1961), 41-43.

[9] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p*, Acta Arith. 9 (1964), 149-159.

[10] P. Frankl, R. L. Graham and V. Rödl, *On subsets of abelian groups with no 3-term arithmetic progression*, J. Combinatorial Theory Ser. A 45 (1987), 157-161.

[11] H. Furstenberg and Y. Katznelson, *An ergodic Szemerédi theorem for IP-systems and combinatorial theory*, J. d'Analyse Math. 45 (1985), 117-168.

[12] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. 262/263 (1973), 356-360.

[13] A. Kemnitz, *On a lattice point problem*, Ars Combinatoria 16b (1983), 151-160.

[14] B. Leeb and C. Stahlke, *A problem on lattice points*, Crux Mathematicorum 13 (1987), 104-108.

[15] L. H. Loomis and H. Whitney, *An inequality related to the isoperimetric inequality*, Bulletin AMS 55 (1949), 961-962.

[16] L. Lovász, **Combinatorial Problems and Exercises**, North Holland, Amsterdam, 1979, Problem 11.8.

[17] J. E. Olson, *An addition theorem modulo p*, J. Combinatorial Theory 5 (1968), 45-52.

[18] H. Plünnecke, *Eine zahlentheoretische Anwendung der Graphentheorie*, J. Reine Angew. Math. 243 (1970), 171-183.

[19] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia 3 (1989), 97-109.