Contemporary Mathematics

Davenport's constant for groups with large exponent

Gautami Bhowmik and Jan-Christoph Schlage-Puchta

Abstract. Let G be a finite abelian group. We show that $D(G) \le \exp(G) + \frac{|G|}{\exp(G)} - 1$, provided that $\exp(G) \ge \sqrt{|G|}$, and $D(G) \le 2\sqrt{|G|} - 1$, if $\exp(G) < \sqrt{|G|}$. This proves a conjecture by Balasubramanian and the first named author.

1. Introduction and results

For an abelian group G denote by $D(G)$ the least integer k, such that every sequence $g_1, \dots, g_k$ of elements in G contains a subsequence $g_{i_1}, \dots, g_{i_\ell}$ with $g_{i_1} + \dots + g_{i_\ell} = 0$, and $D^{\le n}(G)$ be the least integer k', such that every sequence of length k' contains a subsequence of length $\ell \le n$ adding up to 0.

Write $G = \mathbb{Z}/n_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_r\mathbb{Z}$ with $n_1 | \dots | n_r$, where $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Put $M(G) = \sum n_i - r + 1$. In several cases, including 2-generated groups and p-groups, the value of $D(G)$ matches the obvious lower bound $M(G)$, however, in general we have only rather crude upper bounds. One such bound, which is appealing for its simple structure, is the estimate $D(G) \le \exp(G)\big(1 + \log \frac{|G|}{\exp(G)}\big)$, due to van Emde Boas and Kruyswijk[**1**]. If $\frac{|G|}{\exp(G)}$ is small, this result is superseded by the bound $D(G) \le \frac{|G|}{k} + k - 1$, where k is an integer $\le \min(\frac{|G|}{\exp(G)}, 7)$, which is due to Bhowmik and Balasubramanian. They conjectured that one may replace the constant 7 by $\sqrt{|G|}$. Here we prove this conjecture. It turns out that the hypothesis that k be integral creates some technical difficulties, therefore we prove the following, slightly sharper result.

explained $\mathbb{Z}$

replaced n by $|G|$

Theorem 1.1. *For an abelian group G with $\exp(G) \ge \sqrt{|G|}$ we have $D(G) \le \exp(G) + \frac{|G|}{\exp(G)} - 1$, while for $\exp(G) < \sqrt{|G|}$ we have $D(G) \le 2\sqrt{|G|} - 1$.*

We use what is by now standard notation in the theory of zero-sums. For a finite abelian group G denote by $\eta(G)$ the least integer n, such that any sequence of length n in G contains a zero-sum of length $\le \exp(G)$, and by $\mathfrak{s}(G)$ the least integer n such that any sequence of length n in G contains a zero-sum of length equal to $\exp(G)$. For the proof we need the following bounds on η and $\mathfrak{s}$.

2000 *Mathematics Subject Classification.* Primary 11B13, 11B70.

THEOREM 1.2. (1) *We have* $\mathfrak{s}(\mathbb{Z}_3^3) = 19$, $\mathfrak{s}(\mathbb{Z}_3^4) = 41$, $\mathfrak{s}(\mathbb{Z}_3^5) = 91$, *and* $\mathfrak{s}(\mathbb{Z}_3^6) \leq 225$.
(2) *We have* $\mathfrak{s}(\mathbb{Z}_5^4) \leq 157$, $\mathfrak{s}(\mathbb{Z}_5^5) \leq 690$, *and* $\mathfrak{s}(\mathbb{Z}_5^6) \leq 3091$.
(3) *We have* $\mathfrak{s}(\mathbb{Z}_7^4) \leq 333$.
(4) *If* $p > 7$ *is prime and* $d \geq 3$, *then* $\eta(\mathbb{Z}_p^d) \leq \frac{p^d-p}{p^2-p}(3p-7)+4$.

inserted prime

The first result is due to Bose[**3**], Pelegrino[**6**], Edel, Ferret, Landjev and Storme[**4**], and Potechin[**7**], respectively. The second and third will be proven in section 3 using the density increment method, the last statement will be proven by combinatorial means in section 4.

We further need some information on the existence of zero-sums not much larger then $\exp(G)$.

THEOREM 1.3. *Let* p *be a prime,* $d \geq 3$ *an integer. Then a sequence of length* $(6p-4)p^{d-3}+1$ *in* $\mathbb{Z}_p^d$ *contains a zero-sum of length* $\leq \frac{3p-1}{2}$. *If* $d \geq 4$, *then a sequence of length* $(6p-4)p^{d-4}+1$ *in* $\mathbb{Z}_p^d$ *contains a zero-sum of length* $\leq 2p$.

The proof of Theorem 1.1 uses the inductive method. To deal with the inductive step we require the following.

THEOREM 1.4. *Let* p *be a prime,* $d \geq 2$ *an integer. Then there exist integers* N, M, *such that* $M \geq \eta(\mathbb{Z}_p^d)$, *every sequence of length* M *contains at least* N *disjoint zero-sums, and* $M \leq p^{d-1}+pN$.

Note that the statement is trivial if $\eta(\mathbb{Z}_p^d) \leq p^{d-1}$. We believe that this bound is true for all pairs (p,d), $p > 2$, with very few exceptions, in fact, from the Alon-Dubiner-theorem and Roth-type estimates one can deduce that this bound holds for all but finitely many pairs. However, dealing with the exceptional pairs by direct computation is way beyond current computational means. Moreover, this bound is false for $p = 2$ and all d, as well as the pairs $(3,3),(3,4),(3,5)$ and $(5,3)$, which is why we have to introduce the additional parameter N.

typo

2. Proof of Theorem 1.1

In this section we show that Theorem 1.4 implies Theorem 1.1.

LEMMA 2.1. *Let* G *be an abelian group of rank* $r \geq 3$. *Assume that Theorem 1.1 holds true for all proper subgroups of* G. *Then it holds true for* G *itself.*

shifted unnecessary definitions into the proof

PROOF. Let p be a prime divisor of $|G|$. Choose an elementary abelian subgroup $U \cong \mathbb{Z}_p^d$ of G, such that $d \geq 3$, $\exp(G) = p\exp(G/U)$, and $|U|$ is minimal under these assumptions. Put $H = G/U$. Let A be a set consisting of $\exp(G)+\frac{|G|}{\exp(G)}-1$ or $2\lfloor\sqrt{|G|}\rfloor-1$ elements, depending on whether $\exp(G) > \sqrt{|G|}$ or not. Denote by $\overline{A}$ the image of A in H. Then we obtain a zero-sum, by choosing a large system of disjoint zero-sums in $\mathbb{Z}_p^d$, and then choosing a zero-sum among the elements in H defined by these sums, provided that

$$D(H) \leq\leq \frac{|A|-M}{p}+N,$$

Replaced η by M. Becomes more correct and easier to read this way.

where $M \geq \eta(\mathbb{Z}_p^d)$ and $N = N(p,d,M)$ is defined as in Theorem 1.4. The left hand side can be estimated using the inductive hypothesis. We have $\exp(H) = \frac{\exp(G)}{p}$,

$|H| = \frac{|G|}{p^d}$, hence, if $\exp(G) \geq \sqrt{|G|}$ and $\exp(H) \geq \sqrt{|H|}$, our claim follows, provided that

$$\frac{\exp(G)}{p} + \frac{|G|}{\exp(G)p^d} - 1 \leq \frac{|A| - M}{p} + N,$$

inserting the choice of A and rearranging terms this becomes

$$\exp(G) + \frac{|G|}{\exp(G)p^{d-1}} - p \leq \exp(G) + \frac{|G|}{\exp(G)} - 1 - M - \delta + pN.$$

The quotient of G by its largest cyclic subgroup contains at least $\mathbb{Z}_p^{d-1}$, hence, $\frac{|G|}{\exp(G)} \geq p^{d-1}$. Clearly, by replacing $\frac{|G|}{\exp(|G|}$ with a lower bound we lose something, hence, it suffice to establish the relation

$$1 - p \leq p^{d-1} - 1 - M - \delta + pN.$$

However, this relation is implied by Theorem 1.4.

If $\exp(G) \geq \sqrt{|G|}$ and $\exp(H) < \sqrt{|H|}$, then added explanation

$$\sqrt{|G|/p^d} = \sqrt{|H|} > \exp(H) = \exp(G)/p \geq \sqrt{|G|/p^2},$$

thus $d < 2$, but this case was excluded from the outset.

If $\exp(H) < \sqrt{|H|}$, the same argument as in the first case yields $D(G) \leq 2\sqrt{G} - 1$, provided that

$$2p\sqrt{|H|} - p \leq 2\sqrt{|G|} - 1 - M - \delta + pN.$$

Since $|H| = \frac{|G|}{p^d}$ and $M - pN \leq p^{d-1}$ this becomes

$$(2 - 2p^{-(d-2)/2})\sqrt{|G|} \geq p^{d-1} - p + 1.$$

As $\exp(H) < \sqrt{H}$ we have that H is of rank at least 3, which by our assumption on the size of H implies that $|G| \geq p^{2d}$. This implies

$$(2 - 2p^{-(d-2)/2})\sqrt{|G|} \geq (2 - 2p^{-(d-2)/2})p^d > \frac{1}{2}p^d > p^{d-1} - p + 1,$$

and our claim is proven. □

Note that we proved $D(G) \leq 2\sqrt{|G|} - 1$ even in some cases that $\exp(G) > \sqrt{|G|}$, that is, in some cases our proof gives a stronger result than formulated in Theorem 1.1. However, formulating a general theorem along these lines would require one to impose rather technical conditions on the sequence $n_1, \ldots, n_r$. In other words: Let Thangadurai do it

We know that $D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}) = n_1 + n_2 - 1$, hence Theorem 1.1 holds true for all groups of rank ≤ 2. Hence Theorem 1.1 follows by induction over the group order. No need to repeat everything

3. Proof of Theorem 1.4: The case $p \leq 7$

LEMMA 3.1. *Let $d \geq 2$ be an integer, p a prime number. Then every sequence of length $(d+1)p - d$ in $\mathbb{Z}_p^d$ contains a zero-sum of length $\leq (d-1)p$.*

PROOF. Let $g_1, \ldots, g_{(d+1)p-d}$ be elements in $\mathbb{Z}_p^d$. Define the sequence g_1', $\ldots$, $g_{(d+1)p-d}'$ over $\mathbb{Z}_p^{d+1}$ by putting $g_j' = (g_j, 1)$. Since $D(\mathbb{Z}_p^{d+1}) = (d+1)p - d$, there exists a zero-sum $g_{i_1}' + \ldots g_{i_k}' = 0$. Looking only at the last coordinate we see that k is divisible by p, while looking at the first d coordinates we see that $g_{i_1} + \ldots g_{i_k} = 0$ is a zero-sum in $\mathbb{Z}_p^d$. We have $k \leq (d+1)p - d < (d+1)p$, while at the same time k is divisible by p, thus either $k \leq (d-1)p$ or $k = dp$. In the former case we have found

our zero-sum. If $k = dp$, then $k - 1 > D(\mathbb{Z}_p^d)$, hence, the sequence of $g_{i_1}, \dots, g_{i_{pd-1}}$ contains a zero-sum subsequence $g_{j_1}, \dots, g_{j_\ell}$. Then the complement of $g_{j_1}, \dots, g_{j_\ell}$ within $g_{i_1}, \dots, g_{i_{pd}}$ is also a zero-sum, and one of $\ell, pd - \ell$ must be smaller than $(d-1)p$. Hence, in this case we also found a zero-sum of length $\leq (d-1)p$. □

3.1. The primes 2 and 3.

LEMMA 3.2. *Every sequence of length $2^{d-1}+1$ in $\mathbb{Z}_2^d$ contains a zero-sum of length ≤ 3, and this bound is best possible. Every sequence of length $2^{(d+1)/2}+1$ in $\mathbb{Z}_2^d$ contains a zero-sum of length ≤ 4.*

proved a better bound

PROOF. Taking all vectors which have an odd number of entries 1 shows that the first bound is best possible. Now let $A \subseteq \mathbb{Z}_2^d$ be a set without zero-sums of length ≤ 3. Choose some element $a \in A$. Then if A intersects some pair $\{x, x+a\}$ in two points, we obtain a zero-sum of length ≤ 3, hence, $|A| \leq 2^{d-1}$.

Now let A be a set without zero-sums of length ≤ 4. Consider the set $A \dot{+} A = \{a+b, a, b \in A, a \neq b\}$. We claim that if A contains no zero-sum of length ≤ 4, then $|A \dot{+} A| \geq \frac{|A|(|A|-1)}{2}$. Suppose that $a+b = c+d$ with $a, b, c, d \in A$. Then $a+b+c+d = 0$, hence, two of the four elements must be equal. The equal elements cannot be a and b, for otherwise we would obtain a zero-sum of length 2. Hence we may assume that $a = c$, and substracting a we obtain $b = d$. We conclude that if A contains no zero-sum of length ≤ 4 then $|A|(|A|-1) < 2^{d+1}$. Solving for $|A|$ now implies our claim. □

To prove Theorem 1.4 for $p = 2$, we want to show that in a set of 2^d points we can find a system consisting of many disjoint zero-sums. We first remove one zero-sum of length ≤ 2, then zero-sums of length ≤ 3, until this is not possible anymore, and then we switch to zero-sums of length 4. Finally we remove zero-sums of length $\leq d+1$, which is possible in view of $D(\mathbb{Z}_2^d) = d+1$. In this way we obtain at least

changed order of argument

$$\frac{2^d-2}{3} + \frac{2^{d-1}+2-2^{(d+1)/2}-1}{4} + \frac{2^{(d+1)/2}-d-2}{d+1} + 1 = \frac{2^d}{4} + \frac{2^d+2}{24} - 2^{(d-3)/2} + \frac{2^{(d+1)/2}-1}{d+1}$$

zero-sums. Disregarding the last fraction we see that this quantity is $\geq 2^{d-2}$, provided that $d \geq 7$. For $3 \leq d \leq 6$ we obtain our claim by explicitly computing this bound.

Next we consider $p = 3$. For $d \geq 6$ we have

$$\eta(\mathbb{Z}_3^d) \leq \mathfrak{s}(\mathbb{Z}_3^d) \leq 3^{d-6}\mathfrak{s}(\mathbb{Z}_3^6) < 3^{d-1},$$

hence, Theorem 1.4 holds true with $N = 0$, $M = 3^{d-1}$. For $d = 5$ it follows from Lemma 3.1 that a sequence of length $\eta(\mathbb{Z}_3^5) - 3$ contains a system of $N = \lceil \frac{\eta(\mathbb{Z}_3^5)-2d-6}{3d-3} \rceil$ disjoint zero-sums, hence, our claim follows provided that

$$\eta(\mathbb{Z}_3^5) \leq 3\lceil \frac{\eta(\mathbb{Z}_3^5)-16}{12} \rceil + 3^4,$$

that is, $89 \leq 21 + 81$. In the same way we see that for $d = 4$ a sequence of length 39 in $\mathbb{Z}_3^4$ contains a system of 4 disjoint zero-sums, thus our claim follows from $39 \leq 12 + 27$. Finally it is shown in [**2**, Proposition 1], that a sequence of length 15 in $\mathbb{Z}_3^3$ contains a system of 3 disjoint zero-sums. Together with $\eta(\mathbb{Z}_3^3) = 17$ our claim follows in this case as well.

3.2. The primes 5 and 7. We begin by proving the second and third statement of Theorem 1.2. We do so by using a density increment argument together with explicit calculations. Define the Fourier bias $\|A\|_u$ of a sequence A over $\mathbb{F}_p^d$ as

$$\|A\|_u := \frac{1}{|A|} \max_{\xi \in \mathbb{F}_p^d \setminus \{0\}} \sum_{\alpha \in A} e(\langle \xi, \alpha \rangle).$$

Then we have the following.

LEMMA 3.3. *Let $p \geq 3$ be a prime number, A be a sequence over $\mathbb{F}_p^d$. Then A contains a zero-sum of length p, provided that*

$$\frac{|A|^{p-1}}{p^{(p-1)d}} > \|A\|_u^{p-3} \left(\|A\|_u + \frac{p-1}{2p^{d-1}} \right) + \binom{p}{2} \frac{|A|^{p-2}}{p^{(p-1)d}}$$

PROOF. Let N be the number of solutions of the equation $a_1 + \cdots + a_p = 0$ with $a_i \in A$. From [**10**, Lemma 4.13] we have

$$N \geq \frac{|A|^p}{p^d} - \|A\|_u^{p-2} |A| p^{(p-2)d}.$$

A solution $a_1 + \cdots + a_p = 0$ corresponds to a zero-sum of A, if $a_1, \ldots, a_p$ are distinct elements in A. Using Möbius inversion over the lattice of set partitions one could compute the overcount exactly, however, it turns out that the resulting terms are of negligible order, which is why we bound the error rather crudely. The number of solutions M in which not all elements are different is at most $\binom{p}{2}$ times the number of solutions of the equation $2a_1 + a_2 + \cdots + a_{p-1} = 0$. Since multiplication by 2 is a linear map in $\mathbb{F}_p^d$ we have that $\|2A\|_u = \|A\|$, using [**10**, Lemma 4.13] again we obtain

$$M \leq \frac{|A|^{p-1}}{p^d} + \|A\|_u^{p-3} |A| p^{(p-3)d}.$$

Hence the number of zero-sums is at least

$$N - M \geq \frac{|A|^p}{p^d} - \|A\|_u^{p-2} |A| p^{(p-2)d} - \frac{|A|^{p-1}}{p^d} - \|A\|_u^{p-3} |A| p^{(p-3)d},$$

and our claim follows. □

We now use this lemma recursively to obtain bounds for $\mathfrak{s}(\mathbb{Z}_p^d)$, $p = 5, 7$, starting from $\mathfrak{s}(\mathbb{Z}_p^3) = 9p - 8$.

We begin with the case $p = 5$. Consider a 3-dimensional subgroup U, and let $\xi \in \mathbb{Z}_5^4$ be a vector such that $v \perp U$. Let $n_1, \ldots, n_5$ be the number of elements of A in each of the 5 cosets of U, ζ be a fifth root of unity. If $\max(n_i) \geq 37$, we have a zero-sum of length p in one of the hyperplanes. Hence

$$\|A\|_u \leq \frac{1}{|A|} \max_{\substack{n_1 + \cdots + n_5 = |A| \\ 0 \leq n_i \leq 36}} |n_1 + n_2\zeta + \cdots + n_5\zeta^4|.$$

Since $1 + \zeta + \cdots + \zeta^4 = 0$, we have

$$n_1 + n_2\zeta + \cdots + n_5\zeta^4 = (36 - n_1) + (36 - n_2)\zeta + \cdots + (36 - n_5)\zeta^4,$$

that is,

$$\max_{\substack{n_1 + \cdots + n_5 = |A| \\ 0 \leq n_i \leq 36}} |n_1 + n_2\zeta + \cdots + n_5\zeta^4| = \max_{\substack{n_1 + \cdots + n_5 = 180 - |A| \\ 0 \leq n_i \leq 36}} |n_1 + n_2\zeta + \cdots + n_5\zeta^4|.$$

Fir $|A| \geq 144$ the right hand side equals $180 - |A|$, and we obtain a zero-sum, provided that

$$\left(\frac{|A|}{625}\right)^4 > \left(\frac{180-|A|}{|A|}\right)^2 \left(\frac{180-|A|}{|A|} + \frac{2}{125}\right) + \frac{2}{125}\left(\frac{|A|}{625}\right)^3.$$

One easily finds that this is the case for $|A| = 157$, and we deduce $\mathfrak{s}(\mathbb{Z}_5^4) \leq 157$. The same argument yields for $d = 5$ the inequality

$$\left(\frac{|A|}{3125}\right)^4 > \left(\frac{780-|A|}{|A|}\right)^2 \left(\frac{780-|A|}{|A|} + \frac{2}{625}\right) + \frac{2}{625}\left(\frac{|A|}{3125}\right)^3,$$

which is satisfied for $|A| \geq 690$, that is, we obtain $\mathfrak{s}(\mathbb{Z}_5^5) \leq 690$. Finally for $\mathbb{Z}_p^6$ we obtain

$$\left(\frac{|A|}{15625}\right)^4 > \left(\frac{3445-|A|}{|A|}\right)^2 \left(\frac{3445-|A|}{|A|} + \frac{2}{3125}\right) + \frac{2}{3125}\left(\frac{|A|}{3125}\right)^3,$$

which is satisfied for $|A| \geq 3091$, thus the last inequality follows as well.

Hence, Theorem 1.2(2) is proven.

We now turn to the case $p = 7$. We have $\mathfrak{s}(\mathbb{Z}_7^3) = 55$. The same argument as used for the case $p = 5$ shows that a sequence A over $\mathbb{F}_7^4$ contains a zero-sum, provided that

$$\left(\frac{|A|}{2401}\right)^6 > \left(\frac{378-|A|}{|A|}\right)^5 \left(\frac{378-|A|}{|A|} + \frac{3}{343}\right) + \frac{3}{343}\left(\frac{|A|}{2401}\right)^5.$$

The latter inequality is true for $|A| \geq 333$, and our claim follows.

For $p = 5$ and 7 we have $\eta(\mathbb{Z}_p^3) = 8p-7$, and among $8p-7$ elements we can find one zero-sum of length $\leq p$, one of length $\leq 2p$, and one more among the remaining $5p - 7 \geq 3p - 2$ points. Hence we can take $M = 8p - 7, N = 3$, and Theorem 1.4 follows. Moreover we have $\eta(\mathbb{Z}_p^4) \leq \mathfrak{s}(\mathbb{Z}_p^4) - (p-1) \leq p\mathfrak{s}(\mathbb{Z}_p^3) - (p-1) = 9p^2 - 9p + 1$, and among $9p^2 - 9p + 1$ elements we can find one zero-sum of length $\leq p$, $3p - 5$ zero-sums of length $\leq 2p$, and one more zero-sum, that is, we can take $N = 3p - 3$, and Theorem 1.4 follows for $d = 4$ as well.

For $(p, d) = (5, 5)$ we have $\eta(\mathbb{Z}_5^5) \leq \mathfrak{s}(\mathbb{Z}_5^5) - 4 \leq 686$, and among 686 points in $\mathbb{Z}_5$ we find 24 disjoint zero-sums of length ≤ 20, thus taking $M = 686$, $N = 24$, our claim follows since $M \leq 625 + 120$. For $p = 5$, $d \geq 6$ we have

$$\mathfrak{s}(\mathbb{Z}_p^d) \leq 5^{d-6}\mathfrak{s}(\mathbb{Z}_p^6) \leq 30915^{d-6} < 5^{d-1},$$

and our claim becomes trivial.

Simlarly, for $p = 7$, $d \geq 5$ we have

$$\mathfrak{s}(\mathbb{Z}_p^d) \leq 7^{d-4}\mathfrak{s}(\mathbb{Z}_p^4) \leq 3337^{d-4} < 7^{d-1},$$

and our claim holds true for $p = 7$ as well.

4. Proof of Theorem 1.4: The case $p \geq 11$

We begin by proving the last statement of Theorem 1.2.

LEMMA 4.1. *Let A be a sequence of length $3p - 3$ in $\mathbb{Z}_p^2$ without a zero-sum of length $\leq p$. Then $A = \{a^{p-1}, b^{p-1}, c^{p-1}\}$ for suitable elements $a, b, c \in \mathbb{Z}_p^2$.*

PROOF. Gao and Geroldinger[**5**] have shown that this holds true, if p has property B, and Reiher[**8**] has shown that every prime has property B. □

Now suppose that $p \geq 11$ is a prime number, and A is a sequence in $\mathbb{Z}_p^d$ with $|A| = n = \frac{p^d-p}{p^2-p}(3p-7)+4$ without zero-sums of length $\leq p$. Let ℓ be a one-dimensional subgroup of $\mathbb{Z}_p^d$, such that $m = |\ell \cap A|$ is maximal. Now consider all 2-dimensional subgroups containing ℓ. Each such subgroup contains p^2-p points outside ℓ. Each point of A is either contained in ℓ or occurs in $\frac{p^2-p}{p^d-p}$ of all such subgroups. Hence among all subgroups there is one which contains $\lceil \frac{p^2-p}{p^d-p}(n-m) \rceil$ points outside ℓ. Call this subgroup U. Therefore U contains at least

$$\left\lceil \frac{p^2-p}{p^d-p}(n-m) \right\rceil + m \geq \left\lceil 3p-7+m-\frac{m-4}{p+1} \right\rceil$$

elements of A. Since $\eta(\mathbb{Z}_p^2) = 3p-2$, this quantity is $\leq 3p-3$, which implies $m \leq 4$. Since every prime has property B, it also has property C, that is, if $|A \cap U| = 3p-3$, then $m = p-1$, which is impossible in view of > 7 and $m \leq 4$. Hence $m \leq 3$, and we find that U contains $3p-6+m \leq 3p-4$ points, that is, $m \leq 2$. However, this implies that each of the $p+1$ one-dimensional subgroups of U contain at most 2 elements of A, thus $3p-6 < |A \cap U| \leq 2p-2$, which implies $p < 8$, which was excluded.

Next we consider zerosums of length not much beyond p.

LEMMA 4.2. *Every sequence of length $6p-3$ in $\mathbb{Z}_p^3$ contains a zero-sum of length $\leq \frac{3p-1}{2}$, and every sequence of length $6p-3$ in $\mathbb{Z}_p^4$ contains a zero-sum of length $\leq 2p$.*

PROOF. It follows by an application of Reiher's method[**9**] that a sequence of length $6p-3$ in $\mathbb{Z}_p^3$ contains a zero-sum of length p or $3p$. In the first case we are done immediatelly, while in the second we find a zero-sum subsequence B of length $3p$. Since $D(\mathbb{Z}_p^3) = 3p-2 < 3p$ we can find a nontrvial zero-sum subsequence Z of B. Now $B \setminus Z$ and Z are both non-empty zero-sums, one of which has length $\leq \frac{3p-1}{2}$.

The second claim follows similarly starting from the fact that every sequence of lenght $6p-3$ in $\mathbb{Z}_p^4$ contains a zero-sum subsequence of length $p, 2p$ or $4p$. □

We now lift this result to higher dimension.

LEMMA 4.3. *A sequence of length $(6p-4)p^{d-3}+1$ in $\mathbb{Z}_p^d$ contains a zero-sum of length $\leq \frac{3p-1}{2}$. If $d \geq 4$, then a sequence of length $(6p-4)p^{d-4}+1$ in $\mathbb{Z}_p^d$ contains a zero-sum of length $\leq 2p$.*

PROOF. Let A be a sequence of length $(6p-4)p^{d-3}+1$. Let U be a 3-dimensional subgroup of $\mathbb{Z}_p^d$ chosen at random. Then the expected value of $|A \cap U$ is $> 6p-4$, hence there exists a subgroup U with $|A \cap U| \geq 6p-3$. But then $A \cap U$ contains a zero-sum of length $\leq \frac{3p-1}{2}$, and our first claim follows. The proof of the second claim is similar. □ Forgot the second claim

We can now prove Theorem 1.4 for $p \geq 11$. We begin with a sequence of length $\frac{p^d-p}{p^2-p}(3p-7)+4$, remove one zero-sum of length $\leq p$, then zero-sums of length $\leq \frac{3p-1}{2}$, until we have less then $(6p-4)p^{d-3}+1$ points left. If $d = 3$, then we obtain at least one more zero-sum in the remainder. If $d \geq 4$, we continue

removing zero-sums of length $\leq 2p$ until we have less than $(6p-4)p^{d-4}+1$ points left. Let N be the number of zero-sums obtained in this way. If $d=3$, then

$$\begin{aligned} N &\geq \left\lceil \frac{(p+1)(3p-7)+4-p-(6p-3)}{(3p-1)/2} \right\rceil + 2 \\ &= \left\lceil \frac{6p^2-21p}{3p-1} \right\rceil + 2 = 2p-4, \end{aligned}$$

that is, the required condition $M \leq p^{d-1}+pN$ becomes

$$(p+1)(3p-7)+4 \leq p^2+(2p-4)p,$$

which is $2p^2-4p-3 \leq 3p^2-4p$, which is certainly true. Hence our claim follows for $d=3$.

For $d \geq 4$ we get

$$\begin{aligned} N &\geq \left\lceil \frac{\frac{p^d-p}{p^2-p}(3p-7)+4-p-(6p-4)p^{d-3}-1}{(3p-1)/2} \right\rceil \\ &\quad + \left\lceil \frac{(6p-4)(p-1)p^{d-4}-(3p-1)/2}{2p} \right\rceil + 2 \\ &\geq \left\lceil \frac{6p^d-26p^{d-1}+20p^{d-2}-8p^{d-3}}{3p^2-4p+1} \right\rceil + (3p-2)(p-1)p^{d-5} \\ &\geq 2p^{d-2}-3p^{d-3}-3p^{d-4}+\frac{4p^{d-3}-8p^{d-4}+2p^{d-5}}{3p^2-4p+1} \\ &\geq 2p^{d-2}-3p^{d-3}-3p^{d-4} \end{aligned}$$

Now the required condition $M \leq p^{d-1}+pN$ becomes

$$\frac{p^d-p}{p^2-p}(3p-7)+4 \leq p^{d-1}+2p^{d-1}-3p^{d-2}-3p^{d-3},$$

that is

$$3p^d-7p^{d-1}-3p+11 \leq 3p^d-6p^{d-1}+3p^{d-3},$$

which becomes $p^{d-1}+3p^{d-3}+3p \geq 11$, which is certainly true. Hence our claim follows in this case as well.

fixed bibliography

References

1. P. van Emde Boas, D. Kruyswijk, A combinatorial problem on finite Abelian groups III, Math. Centrum Amsterdam Afd. Zuivere Wisk 1969 ZW-008.
2. G. Bhowmik, J.-C. Schlage-Puchta, Davenport's constant for Groups of the Form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, CRM Proceedings and Lecture Notes 43 (2007), 307–326.
3. R. C. Bose, Mathematical theory of the symmetrical factorial design, *Sankhya* **8** (1947), 107-166.
4. Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in AG$(5,3)$, *J. Combin. Theory* Ser. A **99** (2002), 95-110.
5. W. Gao, A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, *Integers* **3** (2003), A8.
6. G. Pellegrino, Sul massimo ordine delle calotte in $S_{4,3}$, *Matematiche (Catania)* **25** (1970), 149-157.
7. A. Potechin, Maximal caps in AG$(6,3)$, *Des. Codes Cryptogr.* **46** (2008), 243-259.
8. C. Reiher, A proof of the theorem according to which every prime number possesses property *B*, Ph.D. thesis, Rostock, 2010.
9. C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, *Ramanujan J.* **13** (2007), 333–337.

10. T. Tao, V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006.

Université de Lille 1, Laboratoire Paul Painlevé UMR CNRS 8524, 59655 Villeneuve d'Ascq Cedex, France
E-mail address: bhowmik@math.univ-lille1.fr

Universiteit Gent, Krijgslaan 281, Gebouw S22, 9000 Gent, Belgium
E-mail address: jcp@math.uni-freiburg.de