Inductive Methods and zero-sum free sequences

Gautami Bhowmik, Immanuel Halupczok, Jan-Christoph Schlage-Puchta

Inductive Methods and Zero-sum free sequences

(short title: Zero-sum free sequences)

by

Gautami Bhowmik,
Université de Lille 1,
Laboratoire Paul Painlevé,
U.M.R. CNRS 8524,
59655 Villeneuve d'Ascq Cedex,
France
bhowmik@math.univ-lille1.fr

Immanuel Halupczok,
DMA de l'ENS,
UMR 8553 du CNRS,
45, rue d'Ulm,
75230 Paris Cedex 05,
France
math@karimmi.de

Jan-Christoph Schlage-Puchta,
Albert-Ludwigs-Universität,
Mathematisches Institut,
Eckerstr. 1
79104 Freiburg,
Germany
jcp@math.uni-freiburg.de

MSC-Index 11B50, 20K01, 20F10, 20D60

INDUCTIVE METHODS AND ZERO-SUM FREE SEQUENCES

GAUTAMI BHOWMIK, IMMANUEL HALUPCZOK, AND JAN-CHRISTOPH SCHLAGE-PUCHTA

Abstract. A fairly long standing conjecture was that the Davenport constant of a group $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ with $n_1 | \ldots | n_k$ is $1 + \sum_{i=1}^{k}(n_i - 1)$. This conjecture is false in general, but the question remains for which groups it is true. By using inductive methods we prove that for two fixed integers k and ℓ it is possible to decide whether the conjecture is satisfied for all groups of the form $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ with n co-prime to k.

We also prove the conjecture for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_{3n} \oplus \mathbb{Z}_{3n}$, where n is co-prime to 6, assuming a conjecture about the maximal zero-sum free sets in $\mathbb{Z}_n^2$.

1. Introduction and Results

Let G be a finite abelian group written additively, $a_1, \ldots, a_k$ a sequence of elements in G. This sequence contains a zero-sum if there is some non-empty subsequence $1 \leq i_1 < i_2 < \cdots < i_\ell \leq k$ satisfying $a_{i_1} + \cdots + a_{i_\ell} = 0$, otherwise it is called zero-sum free. Denote by $D(G)$ the least integer k such that every sequence of length k contains a zero-sum, this number is usually called Davenport's constant, since the question of whether zero-sums exist was studied by Davenport in the context of algebraic number theory (where G is the class group of some number field, the elements a_i are given ideal classes from which one wants to construct a principal ideal). This line of research was continued in the study of domains with non-unique factorisation, for an overview see [10]. Among applications, Brüdern and Godinho [5] discovered that the existence of zero-sums can be used to simplify p-adic forms, which led to considerable progress towards Artin's conjecture on p-adic forms.

To avoid cumbersome notation we shall from now on always talk about multi-sets instead of sequences; in the sequel all sets are multi-sets unless explicitly stated otherwise. We shall write the multiplicity of an element as its exponent, e.g. $\{a^n, b^m\}$ is a multi-set containing $n+m$ elements, n of which are equal to a, and m are equal to b. We believe that the imprecision implied by the non-standard use of equality is more than outweighed by easier readability.

One approach to bound $D(G)$ is the so called inductive method, which runs as follows: If $N < G$ is a subgroup and n an integer such that every sequence of length n in G/N contains a system of $D(N)$ disjoint zero-sums, then $D(G) \leq n$. In fact, each zero-sum in G/N defines an element in N, choosing a zero-sum among these elements defines a zero-sum in G. Unfortunately, in general this method does not give the exact value for $D(G)$. For example, for $G = \mathbb{Z}_3^2 \oplus \mathbb{Z}_{3n}$, Delorme, Ordaz and Quiroz showed that $D(G) \leq 3n + 5$, which is 1 more than the exact value. The sub-optimality of this method stems from the fact that in general

The second author was supported by the Agence National de la Recherche (contract ANR-06-BLAN-0183-01).

we have many ways to choose a system of disjoint zero-sums, and it suffices to show that one of these systems yields a zero-sum in N. If the structure of all zero-sum free subsets in N of size close to $D(N)$ is sufficiently well understood one can use this information to choose an appropriate system of subsets in G/N. In this way one can show that for groups of the form $G = \mathbb{Z}_3^2 \oplus \mathbb{Z}_{3n}$ we always have $D(G) = 3n + 4$ (confer [3]); the corresponding lower bound being given by the mulitset $\{(1,0,0)^2, (0,1,0)^2, (0,0,1)^{3n-1}\}$. In fact, this example immediately generalises to arbitrary finite group: If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ with $n_1 | \ldots | n_k$, then $D(G) \geq M(G) := 1 + \sum_{i=1}^{k}(n_i - 1)$. The conjecture that $D(G) = M(G)$, which we shall refer to as the main conjecture, is proven for groups of rank 2, and fails for infinitely many groups of rank ≥ 4. It is not yet known whether it holds true for all groups of rank 3.

In this note we generalise the improved inductive method to other sequences of groups. We first give a decidability result. Suppose $k, \ell \in \mathbb{N}$ are fixed. Then one can check the main conjecture for all groups of the form $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ at once (in a finite amount of time), where n runs through all numbers co-prime to k. Note that in our case in fact $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n \cong \mathbb{Z}_k^{\ell-1} \oplus \mathbb{Z}_{kn}$. Moreover, we give a description of the set of numbers n such that the main conjecture holds for $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$.

Theorem 1. *Suppose k, ℓ are two integers. Let $\mathcal{N}$ be the set of integers n co-prime to k such that the main conjecture holds for $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$, i.e. such that $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) = (\ell - 1) \cdot (k - 1) + kn$.*

Then either $\mathcal{N}$ is finite, or there exists an integer $d > 0$ and a set $\mathcal{T}$ of divisors of d containing 1 such that $\mathcal{N}$ differs from the set

$$\mathcal{N}' := \{x \in \mathbb{N} \mid (x, d) \in \mathcal{T}\}$$

only in finitely many elements.

In addition, there is an algorithm which, given k and ℓ, prints out $\mathcal{N}$ if the latter is finite. Otherwise its output is d, $\mathcal{T}$ and the set of elements in which $\mathcal{N}$ and $\mathcal{N}'$ differ .

In principle, this means that a computer can be programmed to prove statements of the form "the main conjecture is true for $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ for all n co-prime to k". A straight-forward application of our algorithm would require astronomical running time even for very small k and ℓ, but we believe that by combining computer search with manual arguments one can prove the main conjecture for certain series of groups. In fact, in [3] the methods of this theorem have been explicitly applied to prove the main conjecture in the case $k = 3$, $\ell = 3$.

The proof of Theorem 1 makes much use of the simple structure of $\mathbb{Z}_n$ where there is essentially one single example of a large zero-sum free set. In our next theorem, we would like to replace $\mathbb{Z}_n$ by a larger group. However, for non-cyclic groups the structure of maximal zero-sum free sets is less clear and there are essentially different possibilities for such sets. Due to this complication, we can only deal with groups of rank 2. Though the structure of maximal zero-sum free sets is not known, there is a plausible conjecture concerning these sets. We say that an integer n satisfies property B if every zero-sum free subset $A \subseteq \mathbb{Z}_n^2$ contains an element a with multiplicity $\geq n - 2$.

Conjecture 2. *Every integer n satisfies property B.*

Gao and Geroldinger [8] showed that all integers $n \leq 7$ and all integers n of the form $3 \cdot 2^k$ satisfy property B. In work under preparation we are substantially extending this list. Here we will give an application of property B to Davenport's constant.

Theorem 3. *Let n be an integer co-prime to 6 such that $B(n)$ holds true. Then $D(\mathbb{Z}_3 \oplus \mathbb{Z}_{3n}^2) = 6n + 1$.*

We remark that even the simplest case dealt by this theorem, that is $\mathbb{Z}_3 \oplus \mathbb{Z}_{15}^2$, was till now undecided .

Although we tried to prove as much as possible by hand , the proof of this theorem needs a lemma on subsets of $\mathbb{Z}_3^3$ which we could only prove by massive case distinction, which has been done by our computer.

2. Auxiliary results

For an abelian group G, we denote by $D_m(G)$ the minimal n such that any subset of G of cardinality n contains m disjoint zero-sums.

Lemma 4. (1) *Let k and ℓ be integers. Then there exists a constant $c(k, \ell)$ such that $D_m(\mathbb{Z}_k^\ell) \leq km + c(k, \ell)$.*
(2) *We have $D_m(\mathbb{Z}_3^2) = 3m + 2$.*

Proof. (1) Form as many zero-sums as possible which are of the form $\{a^k\}$ for some $a \in \mathbb{Z}_k^\ell$. For each $a \in \mathbb{Z}_k^\ell$, there are at most $k-1$ copies of a in $\overline{A}$ which we can not use in this way, so $c(k, \ell) := (k-1) \cdot k^\ell$ is certainly sufficient.

(2) It is easy to check that every subset of 5 elements contains a zero-sum, and that every subset of 7 elements contains a zero-sum of length ≤ 3. Our claim now follows by induction on m. □

Lemma 5. *Let $A \in \mathbb{Z}^{k \times \ell}$, $k \leq \ell$, be a matrix, $b \in \mathbb{Z}^k$ a vector. Then either there exists an integer d, and a set $\mathcal{T}$ of divisors of d including 1, such that the system $Ax = b$ is solvable in $\mathbb{Z}_n$ if and only if $(d, n) \in \mathcal{T}$ or there exists a finite set of integers $\mathcal{N}$, such that the above system is solvable if and only if $n \in \mathcal{N}$.*

If all entries in A are of modulus $\leq M$, and all entries of b are of modulus $\leq N$, then $d \leq k! M^k$, and there is a constant c, independent of N and M, such that every element $x \in \mathcal{N}$ satisfies $x \leq (c\ell M)^{c\ell \log M}$.

Proof. Computing the Smith normal form of the matrix A, we see that there exist invertible matrices P, Q over $\mathbb{Z}$, such that $D = PAQ^{-1}$ has non-zero entries at most on the diagonal d_{ii} , $i \leq k$, and these entries satisfy $d_{ii} | d_{i+1,i+1}$. Since every matrix invertible over $\mathbb{Z}$ is also invertible over $\mathbb{Z}_n$, the equation $Ax = b$ is solvable in $\mathbb{Z}_n$ if and only if the equation $Dx = b'$ is solvable, where $b' = Pb$. A necessary condition for solvability is that in every row containing only zeros in D, the corresponding entry of b' vanishes, that is, $n | b'_j$ for every j such that $j > m$, where m is the greatest integer such that $d_{mm} \neq 0$. If one of these b'_j does not vanish, then there are at most finitely many n for which the equation is solvable, and our claim is true. If all these b'_j equal zero, the system is equivalent to the system $d_{ii} x_i = b'_i$, which is solvable if and only if $(n, d_{ii}) | (n, b'_i)$. Hence, we take d to be d_{mm} and since $d_{ii} | d$ for each $i \leq m$, we can express all these conditions in terms of (n, d), and our claim is justified.

For the numerical bounds note that d equals the greatest common divisor of all $m \times m$ sub-determinants of A. Since the $\mathbb{Q}$-rank of A equals m, there exists

a non-vanishing sub-determinant, containing only entries $\leq M$, which is therefore $\leq m!M^m \leq k!M^k$.

To estimate the entries in the set $\mathcal{N}$ we have to estimate the entries of P. A general estimate for the entries of the transformation matrices was obtained by Kannan and Bachem [11, Theorem 5]. They showed that there exists a constant c such that an $\ell \times \ell$-matrix A with integral entries of modulus $\leq M$ can be transformed into Smith normal form using matrices with entries of absolute value $\leq (c\ell M)^{c\ell \log M}$. It follows immediately from their proof that the same estimate remains valid for rectangular matrices, hence, the last claim follows as well. □

Corollary 6. *Consider the system $Ax = b$ as in the previous Lemma, and suppose that there are infinitely many n such that this system is solvable in $\mathbb{Z}_n$. Let n_0 be the least integer greater than 1 such that this system is solvable. Then $n_0 \leq \max\left(28, \frac{k\log(kM)}{\log 2}\right)$.*

Proof. If the system has infinitely many solutions, then there exists an integer $d \leq k!M^k$ such that the system is solvable in $\mathbb{Z}_n$ whenever $(n, d) = 1$. In particular, d is divisible by all prime number $p < n_0$. Since for $x \geq 29$, the product of all prime numbers up to x is $\geq 2^x$, our claim follows. □

The following result is essentially due to Bovey, Erdős and Niven [4].

Lemma 7. *Let $A \subseteq \mathbb{Z}_n$ be a zero-sum free multi-set containing N elements, where $N \geq 2n/3$. Then there exists an element a of $\mathbb{Z}_n$, which occurs in A with multiplicity greater than $2N - n$. Moreover, a is a generator of $\mathbb{Z}_n$.*

Proof. The statement on the multiplicity is [4]. Now suppose that a is not a generator of $\mathbb{Z}_n$, and let H be the subgroup generated by a. Denote by m the multiplicity of a. Among $(\mathbb{Z}_n : H)$ elements of $\mathbb{Z}_n/H$ we can choose a zero-sum, that is, among the $N - m$ elements of $A \setminus \{a^m\}$ we can choose a system of $\lfloor \frac{N-m}{(\mathbb{Z}_n:H)} \rfloor$ disjoint sets, each one adding up to an element in H. Since A is zero-sum free, we cannot obtain $|H|$ elements in this way, that is, $m + \lfloor \frac{N-m}{(\mathbb{Z}_n:H)} \rfloor \leq |H| - 1$, which implies $(\mathbb{Z}_n : H)m + N - m < n$. Since $m \geq 2N - n + 1$, and $(\mathbb{Z}_n : H) \geq 2$, we obtain $3N + 1 < 2n$, contradicting $N \geq 2n/3$. □

Corollary 8. *Let $A \subseteq \mathbb{Z}_n$ be a subset with $|A| \geq 3n/4$. Then A is zero-sum free if and only if $0 \notin A$ and there exists some invertible $\alpha \in \mathbb{Z}_n^\times$, such that $\sum_{a\in A} \iota(\alpha \cdot a) \leq n - 1$, where $\iota\colon \mathbb{Z}_n \to \mathbb{N}$ is the map sending x to the least non-negative residue contained in the class x.*

Proof. Obviously, if $0 \notin A$ and $\sum_{a\in A} \iota(\alpha \cdot a) \leq n-1$, then A is zero-sum free. Hence, we assume that A is zero-sum free and bound the sum. In view of Lemma 7 we may assume without loss that A contains the element 1 with multiplicity $m > n/2$. If A contains an element in the interval $[n/2, n]$, this element can be combined with a certain multiple of 1 to get a zero-sum. Let $x_1, \ldots, x_k$ be the list of all elements in A different from 1. Either $\sum \iota(x_i) \leq n - m - 1$, which is consistent with our claim, or there is a least ℓ such that $s = \sum_{i=1}^{\ell} \iota(x_i) > n - m - 1$. Since no single x_i satisfies $\iota(x_i) > n/2$, we have $s \in [n - m, n - 1]$, hence, s can be combined with a certain multiple of 1 to get a zero-sum, which is a contradiction. □

3. Proof of Theorem 1

Proof of Theorem 1. Let k and ℓ be fixed once and for all. We want to describe the set of n co-prime to k such that $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) = (\ell-1)\cdot(k-1)+kn$ holds. This is equivalent to the non-existence of a zero-sum free set $A \subset \mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ of cardinality $(\ell-1)\cdot(k-1)+kn$.

First note that such a set A can be described by its projection $\overline{A}$ onto $\mathbb{Z}_k^{\ell-1}$ and the multi-function $f\colon \overline{A} \to \mathbb{Z}_n$ such that $(a, f(a)) \in A$ is the preimage of $a \in \overline{A}$. Using this description, the existence of a set A as above is equivalent to the existence of a set $\overline{A} \subset \mathbb{Z}_k^\ell$ of cardinality $(\ell-1)\cdot(k-1)+kn$ and a multi-function $f\colon \overline{A} \to \mathbb{Z}_n$ (call $(\overline{A}, f)$ a "candidate") such that the following condition holds:

(*) For any zero-sum $Z \subset \overline{A}$, the sum $\sum_{a\in Z} f(a)$ is not equal to zero.

We will use the following terminology: A "constant" is a value which only depends on k and ℓ (but not on n); "bounded" means bounded by a constant (in the sense just described), and "almost all" means that the number of exceptions is bounded.

Here is the main part of the proof. We initially skip the proofs of the three following steps:

(1) Suppose $(\overline{A}, f)$ is a candidate and $(Z_i)_{i\le m}$ is a system of m disjoint zero-sum subsets of $\overline{A}$. From this we can form the multi-set $B := B((Z_i)_i) := \{\sum_{a\in Z_i} f(a) \mid 1 \le i \le m\} \subset \mathbb{Z}_n$. If $(\overline{A}, f)$ satisfies (*), then B has to be zero-sum free.

We will find a constant c_{defect} such that $(\overline{A}, f)$ satisfies (*) if and only if for all systems of $m := n - c_{\text{defect}}$ disjoint zero-sum subsets of $\overline{A}$, the corresponding set $B((Z_i)_i)$ is zero-sum free. From now on, we fix m like this.

(2) We will find a constant c_{card} such that if (*) holds for the candidate $(\overline{A}, f)$ and $(Z_i)_i$ is a system of m disjoint zero-sums of $\overline{A}$, then at most c_{card} of the sets Z_i do not have cardinality k.

(3) We will show that when checking whether a pair $(\overline{A}, f)$ satisfying (*) exists, it is enough to consider only certain pairs, the "main candidates", which are defined as follows. We will fix a suitable constant $c_{\text{different}}$. $(\overline{A}, f)$ is a main candidate if there exists an element $a_0 \in \mathbb{Z}_k^l$ such that there are at least $|\overline{A}| - c_{\text{different}}$ occurrences of a_0 in $\overline{A}$ with $f(a_0) = \frac{1}{k}$. Note that $\frac{1}{k}$ does make sense as k and n are co-prime. (Right now, we could as well have written $f(a_0) = 1$ instead of $f(a_0) = \frac{1}{k}$, but later, $\frac{1}{k}$ will be more handy.)

The remainder of the proof goes as follows:

(4) We describe sets $\overline{A}$ which occur in some main candidate $(\overline{A}, f)$ "independently of n" in the following way: in the next step we will choose a constant $c_{\text{var}} \ge c_{\text{different}}$. For any $\overline{A} \subset \mathbb{Z}_k^\ell$ suitable for a main candidate there is an element $a_0 \in \mathbb{Z}_k^\ell$ and a tuple $(a_j)_j \in (\mathbb{Z}_k^\ell)^{c_{\text{var}}}$ such that $\overline{A} = \overline{A}_0 \cup \overline{A}_1$, where $\overline{A}_0 := \{a_j \mid 1 \le j \le c_{\text{var}}\}$ and $\overline{A}_1 := \{a_0^{(\ell-1)\cdot(k-1)+kn-c_{\text{var}}}\}$.

In addition, if the set $\overline{A}$ of a main candidate $(\overline{A}, f)$ is given in that way, then we may suppose $f(a_0) = \frac{1}{k}$ for all $a_0 \in \overline{A}_1$. So to describe the function f of such a main candidate it is sufficient to choose values $f_j := f(a_j) \in \mathbb{Z}_n$ for $1 \le j \le c_{\text{var}}$.

(5) Suppose $(\overline{A}, f)$ is a main candidate which is given as in the previous step, and suppose $(Z_i)_i$ is a system of m disjoint zero-sum subsets of $\overline{A}$. At

least $m - c_{\text{card}} - c_{\text{different}} =: m - c_{\text{eq}}$ of the sets Z_i are of the form $\{a_0^k\}$ with $f(a_0) = \frac{1}{k}$ for all these occurrences of a_0. So by choosing c_{var} in such a way that $|\overline{A}_1| = k(m - c_{\text{eq}})$, we may suppose that the sets $(Z_i)_{i \le c_{\text{eq}}}$ form a system of c_{eq} disjoint zero-sums of $\overline{A}_0$, and all remaining sets Z_i ($c_{\text{eq}} < i \le m$) are subsets of $\overline{A}_1$ of the form $\{a_0^k\}$.

Note that in this way, all systems of disjoint zero-sums which we have to consider are described in a way which is independent of n.

(6) The set $B := B((Z_i)_i)$ corresponding to such a system is of the form $\{b_1, \dots, b_{c_{\text{eq}}}, 1^{m-c_{\text{eq}}}\}$, where $b_i = \sum_{a \in Z_i} f(a) = \sum_{\{j | a_j \in Z_i\}} f_j$. (Note that this already resembles a system of linear equations.)

(7) Suppose $m \ge \frac{3}{4}n$, i.e. $n \ge 4c_{\text{defect}}$. Then we can apply Corollary 8 to the set B and get that it is zero-sum free if and only if $b_i \ne 0$ for all i and $\sum_{i=1}^{c_{\text{eq}}} \iota(b_i) < n - (m - c_{\text{eq}}) = c_{\text{defect}} + c_{\text{eq}}$. (Here $\iota \colon \mathbb{Z}_n \to \mathbb{N}$ is defined as in Corollary 8.)

In particular, we get a set $C_0 \subset \mathbb{Z}^{c_{\text{eq}}}$ not depending on n such that B is zero-sum free if and only if the tuple $(b_i)_i$ lies in the image of C_0 under the projection $\pi \colon \mathbb{Z}^{c_{\text{eq}}} \twoheadrightarrow \mathbb{Z}_n^{c_{\text{eq}}}$.

(8) Putting all this together, we have: For sufficiently large n, there exists a pair $(\overline{A}, f)$ satisfying $(*)$ if and only if:

$$\bigvee_{(a_0,(a_j)_j) \in (\mathbb{Z}_k^\ell)^{1+c_{\text{var}}}} \exists (f_j)_j \in \mathbb{Z}_n^{c_{\text{var}}} \bigwedge_{\substack{(Z_i)_i \text{ system of} \\ c_{\text{eq}} \text{ disjoint} \\ \text{zero-sums in } \overline{A}_0}} \bigvee_{(c_i)_i \in C_0} \bigwedge_{1 \le i \le c_{\text{eq}}} \sum_{\{j | a_j \in Z_i\}} f_j = \pi(c_i)$$

We used big conjunctions and disjunctions $\bigwedge$ and $\bigvee$ as notation for universal and existential quantifiers to emphasise that their range is finite and independent of n.

Putting this formula into disjunctive normal form and moving the existential quantifier inside the $\bigvee$, we get that there exists a pair $(\overline{A}, f)$ satisfying $(*)$ if and only if at least one of a finite number of systems of linear equations has a solution in $\mathbb{Z}_n$.

By Lemma 5, each system either contributes only finitely many integers n such that $(\overline{A}, f)$ satisfies $(*)$, or the contributed set has the form $\{n \mid (n, d) \in \mathcal{T}\}$ for some integer d and some set $\mathcal{T}$ of divisors of d containing 1. The union of sets of this form again has this form, so the first part of the theorem is proven.

Concerning the algorithm it is enough to find computable bounds for the following: a bound n_0 such that the above formula holds for all $n \ge n_0$; a bound n_1 such that if the system of equations is solvable modulo n only for finitely many n, then these n are at most n_1; a bound d_0 such that if the system of equations is solvable for infinitely many n, then $d \le d_0$.

Clearly, all bounds which appear in this proof are computable, so we do get this result. In Section 3.1, we will even determine such bounds explicitly.

Now let us fill in the three remaining steps.

(1) Let $\overline{A} \subset \mathbb{Z}_k^\ell$ be of cardinality $(\ell - 1) \cdot (k - 1) + kn$, and suppose $Z \subset \overline{A}$ is any zero-sum subset. We want to construct a large system $(Z_i)_i$ of disjoint

zero-sums in $\overline{A}$ such that Z can be written as union of some of these zero-sums Z_i. This then implies the first step: if $B((Z_i)_i)$ is zero-sum free, then in particular the sum $\sum_{a\in Z} f(a)$ is not zero.

By Lemma 4 we can find at least $\lfloor\frac{|Z|-c(k,\ell)}{k}\rfloor$ disjoint zero-sums in Z and at least $\lfloor\frac{|\overline{A}\setminus Z|-c(k,\ell)}{k}\rfloor$ disjoint zero-sums in $\overline{A}\setminus Z$. We may suppose that Z is the union of the zero-sums we found inside. Together, we get $\lfloor\frac{|Z|-c(k,\ell)}{k}\rfloor+\lfloor\frac{|\overline{A}\setminus Z|-c(k,\ell)}{k}\rfloor\geq\lfloor\frac{|\overline{A}|-2c(k,\ell)}{k}\rfloor-1=:m=:n-c_{\mathrm{defect}}$ disjoint zero-sums in $\overline{A}$. Note that c_{defect} does not depend on n.

(2) Now suppose $\overline{A}\subset\mathbb{Z}_k^\ell$ is a candidate satisfying (*). We want to show that in systems of m disjoint zero-sums of $\overline{A}$, almost all sets have exactly k elements.

Suppose first that $\overline{A}$ contains N disjoint zero-sum sets which together have only $kN-c$ elements (for some value c). Then in the remaining $(\ell-1)\cdot(k-1)+k(n-N)+c$ elements of $\overline{A}$, we can find (by Lemma 4) $\lfloor\frac{(\ell-1)\cdot(k-1)+k(n-N)+c-c(k,\ell)}{k}\rfloor=n-N+\lfloor\frac{(\ell-1)\cdot(k-1)+c-c(k,\ell)}{k}\rfloor$ disjoint zero-sums. If $c\geq c(k,\ell)-(\ell-1)\cdot(k-1)=:c_{\mathrm{less}}+1$ these are $n-N$ disjoint zero-sums, and together with the other N ones, we get n disjoint zero-sums Z_i. But then the set of sums $B((Z_i)_i)\subset\mathbb{Z}_n$ can not be zero-sum free, which is a contradiction.

In particular, we just showed that there are at most c_{less} disjoint zero-sum subsets of $\overline{A}$ with cardinality less than k.

Now let $(Z_i)_i$ be a system of m disjoint zero-sum sets. To see that almost all of these sets have at most k elements, just note that there are not so many elements in $\overline{A}$ left over to make the sets bigger. More precisely, suppose that M of the sets Z_i have more than k elements, i.e. at least $k+1$ elements each. The remaining $m-M$ sets contain at least $k(m-M)-c_{\mathrm{less}}$ elements, so altogether we get the inequality $M(k+1)+k(m-M)-c_{\mathrm{less}}\leq|\overline{A}|=(\ell-1)\cdot(k-1)+kn$. This implies $M\leq(\ell-1)\cdot(k-1)+kn-km+c_{\mathrm{less}}=(\ell-1)\cdot(k-1)+k\cdot c_{\mathrm{defect}}+c_{\mathrm{less}}=:c_{\mathrm{more}}$.

Putting both together, we get that no system of m disjoint zero-sums has more than $c_{\mathrm{card}}:=c_{\mathrm{more}}+c_{\mathrm{less}}$ sets of cardinality different from k.

The third step requires some more work. We decompose it into several substeps. We use two kinds of arguments: (a) if $(\overline{A},f)$ is a candidate satisfying (*), then $(\overline{A},f)$ has some properties, and (b) if $(\overline{A},f)$ is a candidate satisfying (*), then there is also another candidate $(\overline{A}',f')$ with some additional properties.

(3.1) Suppose that n is sufficiently large. Then for any system $(Z_i)_i$ of m disjoint zero-sums in $\overline{A}$, almost all elements of the sum-set $B:=B((Z_i)_i)$ are equal to one single element $b\in\mathbb{Z}_n$ which generates $\mathbb{Z}_n$.

This follows from Lemma 7. We need $|B|=n-c_{\mathrm{defect}}\geq\frac{2}{3}n$, i.e. $n\geq 3c_{\mathrm{defect}}$. And we get an element with multiplicity at least $2|B|-n+1=m-c_{\mathrm{defect}}+1=:m-c_{\mathrm{ws}}$. (ws = wrong sum.)

(3.2) If $n\gg 0$, then the prevalent value b in $B((Z_i)_i)$ is the same for any system $(Z_i)_i$ of m disjoint zero-sums of $\overline{A}$.

Suppose $(Z_i)_i$ and $(Z_i')_i$ are two different systems of disjoint zero-sums, and denote the prevalent values is $B((Z_i)_i)$ and $B((Z_i')_i)$ by b and b' respectively. We choose $c_{\mathrm{ws}}+1$ of the sets Z_i which all have cardinality at

most k and all have $\mathbb{Z}_n$-sum b. This is possible if $m \geq c_{\text{more}} + 2c_{\text{ws}} + 1$. Without loss, our chosen sets are $Z_1, \ldots, Z_{c_{\text{ws}}+1}$.

Now we do the same for $(Z'_i)_i$, i.e. we choose $Z'_1, \ldots, Z'_{c_{\text{ws}}+1}$ to have at most k elements each and to have $\mathbb{Z}_n$-sum-values b'. But in addition, we want that these sets Z'_j (for $j \leq c_{\text{ws}} + 1$) are disjoint from the sets Z_i (for $i \leq c_{\text{ws}} + 1$). Each set Z_i can intersect at most k of the sets Z'_j, so the additional condition forbids at most $k \cdot (c_{\text{ws}} + 1)$ of the m sets Z_j. Therefore we can find our desired sets if $m \geq c_{\text{more}} + 2c_{\text{ws}} + 1 + k \cdot (c_{\text{ws}} + 1)$.

Now we use Lemma 4 to complete our chosen sets $(Z_i)_{i \leq c_{\text{ws}}+1}$ and $(Z'_i)_{i \leq c_{\text{ws}}+1}$ to a system of m disjoint zero-sum sets. By (3.1), there is a prevalent value b'' for this system, which leaves out at most c_{ws} sets. This implies that both b and b' are equal to b''.

Without loss, we will now suppose that the prevalent $\mathbb{Z}_n$-value of any m disjoint zero-sums is 1.

(3.3) There exists a constant $c_{\text{different}}$ such that for at most $c_{\text{different}}$ of the elements $a \in \overline{A}$, we have $f(a) \neq \frac{1}{k}$. In fact we will choose $c_{\text{different}}$ such that even a slightly stronger statement holds: for each $a \in \mathbb{Z}_k^\ell$, let r_a be number of copies of a in $\overline{A}$ with $f(a) = \frac{1}{k}$. Then $\sum_{a \in \mathbb{Z}_k^\ell} k \cdot \lfloor \frac{r_a}{k} \rfloor \geq |A| - c_{\text{different}}$.

Let us call a subset $Z \subset \overline{A}$ "neat" if it is of the form $\{a^k\}$ for some $a \in \mathbb{Z}_k^\ell$.

We construct a system $(Z_i)_i$ of m disjoint zero-sums with lots of neat sets in the following way: for each element $a \in \mathbb{Z}_k^\ell$ which appear with multiplicity i in $\overline{A}$, we form $\lfloor \frac{i}{k} \rfloor$ disjoint sets of the form $\{a^k\}$. If we get more than m sets in this way, we choose m of them. If we get less than m sets, then we use Lemma 4 on the remainder of $\overline{A}$ to complete our system. Denote by κ the number of neat sets we got in that way.

The minimal value of κ is attained if the multiplicity in $\overline{A}$ of each $a \in \mathbb{Z}_k^\ell$ is congruent $k-1$ modulo k. So we get $\kappa \geq \min\{m, \frac{1}{k}(|\overline{A}| - (k-1) \cdot k^\ell)\} =: m - c_{\text{nn}}$ (nn = not neat).

Among all systems of disjoint zero-sums in $\overline{A}$ which have κ neat sets now choose a system $(Z_i)_i$ where the number of neat sets Z_i with sum $\sum_{a \in Z_i} f(a)$ equal to 1 is minimal. At most c_{ws} sets have not sum 1 and at most c_{nn} are not neat, so even in this minimal choice we get at least $m - c_{\text{nn}} - c_{\text{ws}}$ neat sets with sum 1.

Choose $a \in \mathbb{Z}_k^\ell$, and let $\mathcal{N}$ be the union of all neat sets Z_i of the form $\{a^k\}$ with $\mathbb{Z}_n$-sum 1. We claim that if there are at least two such neat sets, then f is constant on $\mathcal{N}$; in particular this implies that the value of f on $\mathcal{N}$ is $\frac{1}{k}$. Suppose f is not constant on $\mathcal{N}$. Then there are two elements $a_1, a_2 \in \mathcal{N}$ with $f(a_1) \neq f(a_2)$ which belong to two different neat sets Z_{i_1}, Z_{i_2}. Modify the system $(Z_i)_i$ by exchanging a_1 and a_2. Then Z_{i_1} and Z_{i_2} do not have sum 1 anymore, so the new system contradicts the assumption that the old one had a minimal number of neat sets with sum 1.

In this construction, the number of elements a' of $\overline{A}$ for which we proved that $f(a') = \frac{1}{k}$ is minimal if for all but one $a \in \mathbb{Z}_k^\ell$, there is exactly one neat set with $\mathbb{Z}_n$-sum 1 of the form $\{a^k\}$. So there are at least $m - c_{\text{nn}} - c_{\text{ws}} - (k^\ell - 1)$ neat sets contributing elements with $f(a') = \frac{1}{k}$, which yields $k \cdot (m - c_{\text{nn}} - c_{\text{ws}} - (k^\ell - 1)) =: |A| - c_{\text{different}}$ such elements. As these

elements are contributed in groups of k, we also get the slightly stronger statement mentioned at the beginning of this step.

(3.4) The last part of step (3): if $(\overline{A}, f)$ satisfies (*), then there is also a main candidate $(\overline{A}', f')$ satisfying (*).

Remember that $(\overline{A}', f')$ is a main candidate if there is an element $a_0 \in \mathbb{Z}_k^\ell$ such that $\overline{A}'$ contains a lot of copies of a_0 with $f(a_0) = \frac{1}{k}$.

We construct $(\overline{A}', f')$ out of $(\overline{A}, f)$ in the following way. As before for $a \in \mathbb{Z}_k^\ell$ let r_a be number of copies $a' \in \overline{A}$ of a with $f(a') = \frac{1}{k}$. Choose $a_0 \in \mathbb{Z}_k^\ell$ such that r_{a_0} is maximal. Let $(\overline{A}', f')$ be equal to $(\overline{A}, f)$ with the following modification: For each $a \in \mathbb{Z}_k^\ell$, replace $k \cdot \lfloor \frac{r_a}{k} \rfloor$ copies $a' \in \overline{A}$ with $f(a') = \frac{1}{k}$ by the same number of copies of a_0 with $f'(a_0) = \frac{1}{k}$ on these copies. The previous step ensures that in this way, we indeed get a main candidate $(\overline{A}', f')$.

We are now only left to prove that for any system of disjoint zero-sums $(Z_i')_i$ of $(\overline{A}', f')$ we can find a system of disjoint zero-sums $(Z_i)_i$ of $(\overline{A}, f)$ such that $B((Z_i)_i) = B((Z_i')_i)$. (Then if $(\overline{A}', f')$ does not satisfy (*) because of $(Z_i')_i$, we get that $(\overline{A}, f)$ does not satisfy (*) because of $(Z_i)_i$.)

So suppose $(Z_i')_i$ is given. Remove all sets of the form $\{a_0^k\}$, where $f(a_0) = 1$ on all these copies of a_0 and denote the remaining system by $(Z_i)_i$. If the total number of elements in $\bigcup_i Z_i$ which are copies of a_0 and which have f-value 1 is at most r_{a_0} (the number of such elements in $\overline{A}$), then this $(Z_i)_i$ can be seen as a system of subsets of $\overline{A}$. This condition is satisfied for $n \gg 0$, as $|\bigcup_i Z_i|$ is bounded whereas $r_{a_0} \geq \frac{|A| - c_{\text{different}}}{k^\ell}$.

Finally add sets of the form $\{a^k\} \subset \overline{A}$ for appropriate $a \in \mathbb{Z}_k^\ell$ to $(Z_i)_i$, where $f(a) = \frac{1}{k}$ on all these copies of a, until we again get a system of m disjoint zero-sums. This is possible as $\overline{A}$ and $\overline{A}'$ differ only by "groups of k".

□

3.1. **Computation of the bounds.** The proof of Theorem 1 actually gives a little more than just decidability. In fact, for each k and ℓ, there is a computable constant n_0, such that the expected equation $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) = (\ell - 1) \cdot (k - 1) + kn$ holds true for all integers n co-prime to k if and only if it holds true for all integers $n \leq n_0$ which are co-prime to k. In this section we compute an upper bound for n_0. Unfortunately, $D(G)$ is computable only for very small groups G, while the value for n_0 obtained in this subsection is rather large. However, we still believe that the algorithm given above can be performed for several small values of k and ℓ, in particular if one does some manual improvements using the explicit knowledge of k and ℓ.

A bound for Lemma 4: Denote by $D^k(\mathbb{Z}_k^\ell)$ the least integer n such that every multi-set consisting of n elements in $\mathbb{Z}_k^\ell$ contains a zero-sum of length $\leq k$. Then $c(k, \ell) \leq D^k(\mathbb{Z}_k^\ell) - k$, since every multi-set containing $k(m-1) + D^k(\mathbb{Z}_k^\ell)$ elements contains a system of m disjoint zero-sums each of length $\leq k$. For $D^k(\mathbb{Z}_k^\ell)$ we have the trivial bound $k^{\ell+1}$, but also the estimate $D^k(\mathbb{Z}_k^\ell) \leq (256\ell \log \ell)^\ell \cdot k$ due to Alon and Dubiner [1]. For specific values of k and ℓ, great improvements on both bounds are possible; it is probably at this point that our estimates can be improved

most easily. To avoid some awkward expressions in the sequel, we shall express all constants occurring in the proof of Theorem 1 explicitly in terms of k, ℓ and $c(k,\ell)$, and give an explicit estimate using only the bound $c(k,\ell) \le k^{\ell+1}$.

Step (1): $c_{\rm defect} = 1 + \lceil \frac{2c(k,\ell)-(\ell-1)(k-1)}{k} \rceil \le 2k^{\ell+1}$

Step (2): $c_{\rm less} = c(k,\ell) - (\ell-1)(k-1) - 1 \le k^{\ell+1}$

Step (2): $c_{\rm more} = (\ell-1)\cdot(k-1) + k \cdot c_{\rm defect} + c_{\rm less} \le (2k+2)k^{\ell+1}$

Step (2): $c_{\rm card} = c_{\rm more} + c_{\rm less} \le (2k+3)k^{\ell+1}$

Step (3.1): $c_{\rm ws} = c_{\rm defect} - 1 \le 2k^{\ell+1}$

Step (3.1) needs $n \ge 3c_{\rm defect}$. So $n \ge 6k^{\ell+1}$ suffices.

Step (3.2) needs $n \ge c_{\rm defect} + c_{\rm more} + 2c_{\rm ws} + 1 + k\cdot(c_{\rm ws}+1)$. So $n \ge (4k+7)k^{\ell+1}$ suffices.

Step (3.3): $c_{\rm nn} = \max\{0, (k-1)\cdot k^{\ell-1} - \frac{1}{k}(\ell-1)(k-1) - c_{\rm defect}\}$. The estimates above yield $c_{\rm nn} = 0$, and we shall treat $c_{\rm nn}$ as 0 in the sequel, however, using more explicit estimates for $c(k,\ell)$ yields non-zero values for $c_{\rm nn}$ as well.

Step (3.3): $c_{\rm different} = (\ell-1)(k-1) + k(c_{\rm defect} + c_{\rm nn} + c_{\rm ws}) + k(k^\ell - 1) \le (4k+1)k^{\ell+1}$

Step (3.4): $|\bigcup_i Z_i| \le (\ell-1)(k-1) + k(c_{\rm defect} + c_{\rm card} + c_{\rm different})$; $r_{a_0} \ge \frac{(\ell-1)(k-1)+kn-c_{\rm different}}{k^\ell}$.

Step (3.4) needs $n \ge k^{\ell-1}(\ell-1)(k-1) + k^\ell(c_{\rm defect} + c_{\rm card} + c_{\rm different}) + \frac{1}{k}c_{\rm different} - \frac{1}{k}(\ell-1)(k-1)$. So $n \ge (6k+12)k^{2\ell+1}$ suffices.

Step (5): $c_{\rm eq} = c_{\rm card} + c_{\rm different} \le (6k+4)k^{\ell+1}$

Step (5): $c_{\rm var} = (\ell-1)\cdot(k-1) + kc_{\rm defect} + kc_{\rm eq} \le (6k+7)k^{\ell+2}$

Step (7) needs $n \ge 3c_{\rm defect}$. So $n \ge 8k^{\ell+1}$ suffices.

Step (7): The sum of all b_i (right hand sides of a system of equations corresponding to a single system of disjoint zero-sums) is less than $c_{\rm defect} + c_{\rm eq} \le (6k+6)k^{\ell+1}$.

Step (8): The number of variables in each system of equations is $c_{\rm var}$.

Step (8): The total number of equations (after putting the formula into disjunctive normal form and removing duplicate equations) is equal to the number of zero-sums in a set of cardinality $c_{\rm var}$ which are part of a system of $c_{\rm eq}$ disjoint zero-sums. Bounding this number by the number of all subsets gives $2^{c_{\rm var}} \le 2^{(6k+7)k^{\ell+2}}$.

Hence, we can apply Lemma 5 and Corollary 6 to obtain the following.

Proposition 9. *There exists a constant c such that the following holds true. Let k,ℓ be integers, such that there exists some n, co-prime to k, satisfying $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) \neq (\ell-1)(k-1)+kn$. Let n_1 be the least such n. Then we have $n_1 \le 2^{c2^{(6k+9)k^{\ell+2}}}$. If there are infinitely many such n, then we have $n_1 \le (6k+7)k^{\ell+2}$.*

Proof. Using the estimates above and Corrolary 6, we obtain

$$\begin{aligned} n_1 &\le (c2^{c_{\rm var}}(c_{\rm defect}+c_{\rm eq}))^{c2^{c_{\rm var}}\log(c_{\rm defect}+c_{\rm eq})} \\ &\le (c2^{(6k+7)k^{\ell+2}}(6k+6)k^{\ell+1})^{c2^{(6k+7)k^{\ell+2}}((\ell+2)\log k+\log 9)} \\ &\le 2^{c2^{(6k+9)k^{\ell+2}}}, \end{aligned}$$

and our claim follows. □

Note that the smallest case of interest would be $k=4, \ell=3$, that is, checking $D(\mathbb{Z}_4^2 \oplus \mathbb{Z}_{4n}) = 4n+6$ for all odd n up to 31744 would imply that this equation has only finitely many solutions. Unfortunately, even the case $n=3$ has not yet been decided , although it is within reach of modern computers.

4. Proof of Theorem 3

In this section we prove that $B(n)$ implies $D(\mathbb{Z}_3 \oplus \mathbb{Z}_{3n}^2) = 6n+1$ if n is co-prime to 6. We suggest that before reading the following lemmas, the reader goes directly to the main proof and starts reading it to get the main idea.

4.1. **Lemmas needed in the proof.**

Lemma 10. *Among 17 arbitrary elements in $\mathbb{Z}_3^3$ there is a zero-sum of length at most 3, and among 9* distinct *elements there is a zero-sum of length at most 3. Moreover, up to linear equivalence, there is precisely one set of 8 distinct elements without zero-sums of length at most 3, which is given as $\{x, y, z, x+y, x+y+z, x+2y+z, 2x+z, y+2z\}$.*

Proof. The second part is [3, Lemma 1 (ii)], the first part is folklore (and follows immediately from the second part). □

Lemma 11. *Suppose that $n \geq 5$ is an integer having property B, and B is a subset of $\mathbb{Z}_n^2$ with either $2n-3$ or $2n-4$ points. Then, with one exception, there always exists a group homomorphism $F\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n$ such that:*

1. *In the case $|B| = 2n-3$: For any c with $B \cup \{c\}$ zero-sum free, we have $F(c) = 1$.*
2. *In the case $|B| = 2n-4$: For any c_1, c_2 with $B \cup \{c_1, c_2\}$ zero-sum free, we have $F(c_i) \in \{0, 1\}$, and at least one of $F(c_1)$ and $F(c_2)$ is equal to 1.*

The exception is $B = \{b_1^{n-2}, b_2^{n-2}\}$, where b_1 and b_2 generate $\mathbb{Z}_n^2$.

Proof. Every completion of B to a zero-sum free set contains an element b with multiplicity $n-2$ or $n-1$ such that all other elements of the completion are contained in a Co-set of $\langle b\rangle$ which is a generator of $\mathbb{Z}_n^2/\langle b\rangle$. We will call an element of B *important* if it could get such an element after completion; i.e. an element $b \in B$ is important if its multiplicity is at least $n-3$ in the first case or $n-4$ in the second case, if its order is n and if all other elements of B are contained in a Co-set of $\langle b\rangle$ which is a generator of $\mathbb{Z}_n^2/\langle b\rangle$. B contains at least one important element. We will do case distinctions between the different possibilities for the important elements of B. But before we start, let us have a closer look at what can happen if B contains two important elements, say b_1 and b_2.

First note that these two elements generate $\mathbb{Z}_n^2$, as (by the importance of b_1) b_2 lies in a Co-set of $\langle b_1\rangle$ generating $\mathbb{Z}_n^2/\langle b_1\rangle$. Now b_2 fixes the Co-set of $\langle b_1\rangle$ and vice versa, so all elements of B other than b_1 and b_2 lie in both $b_2 + \langle b_1\rangle$ and $b_1 + \langle b_2\rangle$; we get $B = \{b_1^{m_1}, b_2^{m_2}, (b_1+b_2)^{|B|-m_1-m_2}\}$. In particular, B contains no third important element.

First consider the case $|B| = 2n-3$. We distinguish the following cases:

- B contains only one important element b. Then the other elements of B define a Co-set L of $\langle b\rangle$, and all elements c completing B either are equal to b or lie in L. If b has multiplicity $n-1$, then $c = b$ is impossible, so choose F such that $F(L) = 1$. If b has multiplicity $n-2$, then there are only two possibilities for c: $c = b$ and one other possibility on L (such that the sum of c and the elements of $B \cap L$ is equal to b). Choose F to be 1 on these two possibilies. If b has multiplicity $n-3$, then only $c = b$ is possible.

In the remaining cases, B contains two important elements, so $B = \{b_1^{m_1}, b_2^{m_2}, (b_1 + b_2)^{m_3}\}$ for some m_1, m_2, m_3 satisfying and $m_1+m_2+m_3 = 2n-3$. We may suppose $m_1 \geq m_2$.

- $m_1 = n-1$: All completions of B lie in $b_2 + \langle b_1 \rangle$.
- $m_1 = m_2 = n-2$, $m_3 = 1$: There are two possible completions: $c = b_1$ and $c = b_2$.
- $m_1 = n-2$, $m_2 = n-3$, $m_3 = 2$: There are two possible completions: $c = b_1$ and $c = b_2 - b_1$.
- $m_1 = m_2 = n-3$, $m_3 = 3$: There is no possible completion.

Now consider the case $|B| = 2n-4$. We distinguish the following cases:

- B contains only one important element b. Then the other elements of B define a Co-set L of $\langle b \rangle$, and for all completions $\{c_1, c_2\}$, both c_i lie in $L \cup \{b\}$. If the multiplicity of b in B is $n-1$ or $n-2$, we can take F to be the function which is 1 on L (and 0 on b). Otherwise at least one of the c_i is equal to b and the other one either es equal to b, too, or it lies on L and is determined by B. So a function F exists.

Again, in the remaining cases $B = \{b_1^{m_1}, b_2^{m_2}, (b_1 + b_2)^{m_3}\}$ with $m_1 \geq m_2$ and $m_1 + m_2 + m_3 = 2n-4$.

- $m_1 = m_2 = n-2$, $m_3 = 0$. This is the exception mentioned in the statement of the lemma.
- $m_1 = n-2$, $m_2 \leq n-3$: There are three types of completions: $c_1 = b_1$ and $c_2 \in b_2 + \langle b_1 \rangle$; $c_1 = c_2 = b_2$; both c_i lie in $b_2 + \langle b_1 \rangle$ with some condition on $c_1 + c_2$. (Note that in the case $m_2 = n-3$, we have $m_3 = 1$ and $c_1 = b_2$ implies $c_2 = b_1$.) So the function F which maps $b_2 + \langle b_1 \rangle$ to 1 does the job.
- $m_1 = m_2 = n-3$, $m_3 = 2$: There are four possible completions: $\{b_1^2\}$, $\{b_2^2\}$, $\{b_1, b_2 - b_1\}$ and $\{b_2, b_1 - b_2\}$. Take F to map b_1 and b_2 to 1.
- $m_1 = n-3$, $n_2 = n-4$, $m_3 = 3$: There are two possible completions: $\{b_1^2\}$ and $\{b_1, b_2 - 2b_1\}$. (Note that $\{b_2^2\}$ does not work.) Take F to map b_1 and $b_2 - 2b_1$ to 1.
- $m_1 = m_2 = n-4$, $m_3 = 4$: No completion is possible.

□

We will need the following refined version of part 2 of Lemma 11:

Lemma 12. *Suppose that $n \geq 5$ is an odd integer having property B. Suppose further that B is a subset of $\mathbb{Z}_n^2$ with $2n-4$ points. Let C be the set of two-element-sets $\{c_1, c_2\} \subset \mathbb{Z}_n^2$ such that $B \cup \{c_1, c_2\}$ is zero-sum free. Then, up to an automorphism of $\mathbb{Z}_n^2$, C is a subset of one of the following sets:*

(1) $C_1 = \big\{\{(x_1, 1), (x_2, 1)\} \mid x_1, x_2 \in \mathbb{Z}_n\big\}$.
(2) $C_2 = C_2' \cup C_2''$ *with* $C_2' = \big\{\{(1,0), (x,1)\}, \{(x,1), (1-x,1)\} \mid x \in \mathbb{Z}_n\big\}$ *and* $C_2'' = \big\{\{(0,1), (1,y)\}, \{(1,y), (1,1-y)\} \mid y \in \mathbb{Z}_n\big\}$.
(3) $C_3 = C_3' \cup C_3''$ *with* $C_3' = \big\{\{(1,0)^2\}, \{(1,0), (-1,1)\}\big\}$ *and* $C_3'' = \big\{\{(0,1)^2\}, \{(0,1), (1,-1)\}\big\}$.

Proof. As in the proof of Lemma 11, we consider the different possibilities for the important elements. If B contains only one important element, we can suppose that it is $(1,0)$ and that the other elements of B have y-coordinate one; we denote the multiplicity of $(1,0)$ by m_1. If there are two important elements, we suppose that $B = \{(1,0)^{m_1}, (0,1)^{m_2}, (1,1)^{m_3}\}$ with $m_1 \geq m_2$.

- One important element, $m_1 = n-1$: $C = C_1$.
- One important element, $m_1 = n-2$: apply an automorphism of $\mathbb{Z}_n^2$ fixing $(1,0)$ and mapping the sum of those $n-2$ elements of B with y-coordinate one to $(0,-2)$. Then $C = C_2' \subset C_2$.
- One important element, $m_1 = n-3$: apply an automorphism fixing $(1,0)$ and mapping the sum of those $n-1$ elements of B with y-coordinate one to $(2,-1)$. Then $C = C_3' \subset C_3$.
- One important element, $m_1 = n-4$: $C = \{\{(1,0)^2\}\} \subset C_3$.
- Two important elements, $m_1 = m_2 = n-2, m_3 = 0$: $C = C_2$.
- Two important elements, $m_1 = n-2, m_2 = n-3, m_3 = 1$: apply an automorphism fixing $(1,0)$ and mapping $(0,1)$ to $(\frac{1}{2},1)$. Then $C = C_2' \subset C_2$.
- Two important elements, $m_1 = n-2, m_2 = n-4, m_3 = 2$: apply an automorphism fixing $(1,0)$ and mapping $(0,1)$ to $(1,1)$. Then $C = C_2' \subset C_2$.
- Two important elements, $m_1 = m_2 = n-3, m_3 = 2$: $C = C_3$.
- Two important elements, $m_1 = n-3, m_2 = n-4, m_3 = 3$: apply an automorphism fixing $(1,0)$ and mapping $(0,1)$ to $(1,1)$. Then $C = C_3' \subset C_3$.
- Two important elements, $m_1 = m_2 = n-4, m_3 = 4$: $C = \emptyset$.

□

In addition, we will need the two following lemmas:

Lemma 13. *Suppose n is an integer co-prime to 6 and $\overline{A} \subseteq \mathbb{Z}_3^3$ has 10 elements. Suppose further that $\overline{A}$ has no zero-sum of length ≤ 3 and $\overline{A}$ has no two disjoint zero-sums. Then there is no multi-function $g\colon \overline{A} \to \mathbb{Z}_n$ (i.e. function which may take different values on different copies of an element $a \in \overline{A}$) such that for every zero-sum $Z \subseteq \overline{A}$ we have $\sum_{z\in Z} g(z) = 1$.*

Proof. If we would require g to be a real (i.e. single-valued) function, then this would be [3, Theorem 1]. So the only thing we have to check is that the existence of a multi-function g implies the existence of a real function g' with the same properties.

Define g' by taking for $g(a)$ the mean value of the values of $g(a)$. Note first that the maximal multiplicity of points in $\overline{A}$ is 2 (as $\overline{A}$ does not contain a zero-sum of length 3), so g can have at most two values at any point. In particular the mean value makes sense (because $2 \nmid n$).

Now consider any point $a \in \overline{A}$ where g has two values. The modification does not change $\sum_{z\in Z} g(z)$ if Z does not contain a or if Z contains both copies of a. However, no zero-sum Z can contain only one copy of $\overline{A}$, for otherwise, we would get two different values for $\sum_{z\in Z} g(z)$, which contradicts $\sum_{z\in Z} g(z) = 1$. □

Lemma 14. *Suppose n is an integer co-prime to 6, $\overline{A} \subseteq \mathbb{Z}_3^3$ has 13 elements, and $f\colon \overline{A} \to \mathbb{Z}_n^2$ is a multi-function. Suppose further that $\overline{A}$ has no zero-sum of length ≤ 3 and $\overline{A}$ has no three disjoint zero-sums. Let C be the set of two-element-sets $\{\sum_{z\in Z_1} f(z), \sum_{z\in Z_2} f(z)\}$, where Z_1 and Z_2 are two disjoint zero-sums in $\overline{A}$. Then C is not a subset of any of the three sets C_1, C_2 or C_3 of Lemma 12.*

Proof. This has been verified by our computer. For details on how this has been done see Section 5.

Note that concerning C_1, this is just an unnecessarily complicated way of saying that there is no function $g\colon \overline{A} \to \mathbb{Z}_n$ which maps any zero-sum of $\overline{A}$ which is disjoint to another zero-sum to one. □

4.2. **The proof itself.** We are now in a position to prove Theorem 3.

Proof of Theorem 3. Suppose n is co-prime to 6, $B(n)$ holds true, $G = \mathbb{Z}_3 \oplus \mathbb{Z}_{3n}^2$, and $A \subseteq G$ is a multi-set of $M(G) = 6n + 1$ elements. Suppose A contains no zero-sum. We have to get to a contradiction.

Let $\overline{A}$ be the projection of A onto $\mathbb{Z}_3^3$, and let $f\colon \overline{A} \to \mathbb{Z}_n^2$ be the multi-function such that $(a, f(a))$ is the preimage of $a \in \mathbb{Z}_3^3$ in A under the projection.

We remove zero-sums of length ≤ 3 from $\overline{A}$ as long as possible, ending in a set $\overline{A}^*$ with less than 17 points (by Lemma 10). Denote by B the multi-set in $\mathbb{Z}_n^2$ corresponding to the removed zero-sums: for each removed zero-sum $Z \subset \overline{A}$, put the element $\sum_{z\in Z} f(z)$ into B. As A is zero-sum free, so is B. The strategy in the remainder of the proof is to consider zero-sums $Z \in \overline{A}^*$ and their corresponding elements $c = \sum_{z\in Z} f(z)$ in $\mathbb{Z}_n^2$. If we find such a c such that $B \cup \{c\}$ does contain a zero-sum, we have our desired contradiction. When using this strategy, we may assume that while passing from $\overline{A}$ to $\overline{A}^*$ we never removed zero-sums of length < 3; otherwise $\overline{A}^*$ only gets bigger and the proof gets easier.

Hence $|\overline{A}^*|$ has the form $3i + 1$ and $|B| = 2n - i$. As B has no zero-sum, we have $|B| \leq 2n - 2$, so $i \geq 2$ and $|\overline{A}^*| \geq 7$. If $|\overline{A}^*| = 7$, then $\overline{A}^*$ itself still contains a zero-sum, so this is not possible either. Therefore $\overline{A}^*$ consists of 10, 13 or 16 points.

Suppose first that we end with $|\overline{A}^*| = 16$. Then we have 16 points without a zero-sum of length ≤ 3. As 9 distinct points would contain such a zero-sum (by Lemma 10) there are precisely 8 points taken twice. Since the only configuration of 8 distinct points without a zero-sum of length 3 is the one given in Lemma 10, we find that $\overline{A}^*$ equals this set with each point taken twice. But this set contains four disjoint zero-sums: $\{x, y, (x+y)^2\}$, $\{x, z^2, 2x+z\}$, $\{y, x+y+z, (x+2y+z)^2\}$ and $\{x+y+z, 2x+z, (y+2z)^2\}$. So we can enlarge B to a set with $2n - 1$ elements, which is a contradiction.

Next, suppose that $|\overline{A}^*| = 10$. Then B consists of $2n-3$ points in $\mathbb{Z}_n^2$, and each zero-sum Z in $\overline{A}^*$ yields an element $c = \sum_{z\in Z} f(z)$ of $\mathbb{Z}_n^2$ such that $B \cup \{c\}$ is zero-sum free. Since n satisfies property B (and is ≥ 5), we can apply Lemma 11 and obtain a linear function $F\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n$ such that for every c as above $F(c) = 1$. But now $g := F \circ f$ is a contradiction to Lemma 13.

Finally, consider the case $|\overline{A}^*| = 13$. Then B consists of $2n-4$ points in $\mathbb{Z}_n^2$. We check that $\overline{A}^*$ and f contradict Lemma 14. It is clear that $\overline{A}^*$ does not contain a zero-sum of length ≤ 3 and that $\overline{A}^*$ does not contain three disjoint zero-sums.

Denote by C the set of two-element-sets $\{\sum_{z\in Z_1} f(z), \sum_{z\in Z_2} f(z)\}$, where Z_1 and Z_2 are two disjoint zero-sums in $\overline{A}^*$. Each $\{c_1, c_2\} \in C$ completes B to a zero-sum free subset of $\mathbb{Z}_n^2$, so by Lemma 12, C is a subset of one of the three sets C_i mentioned in that lemma. This is exactly what we need to get a contradiction to Lemma 14. □

5. Computer proof of Lemma 14

Recall the statement of the lemma : we are given an integer n co-prime to 6, a set $\overline{A} \subseteq \mathbb{Z}_3^3$ consisting of 13 elements, and a multi-function $f\colon \overline{A} \to \mathbb{Z}_n^2$. We suppose

that $\overline{A}$ has no zero-sum of length ≤ 3 and no three disjoint zero-sums. We let C be the set of two-element-sets $\{\sum_{z\in Z_1} f(z), \sum_{z\in Z_2} f(z)\}$, where Z_1 and Z_2 are two disjoint zero-sums in $\overline{A}$. The statement is that C is not a subset of any of the three sets C_1, C_2 or C_3 of Lemma 12:

$$\begin{aligned}
C_1 =& \big\{\{(x_1,1),(x_2,1)\} \mid x_1,x_2 \in \mathbb{Z}_n\big\}\\
C_2 =& \big\{\{(1,0),(x,1)\},\{(x,1),(1-x,1)\} \mid x \in \mathbb{Z}_n\big\} \cup\\
& \big\{\{(0,1),(1,y)\},\{(1,y),(1,1-y)\} \mid y \in \mathbb{Z}_n\big\}\\
C_3 =& \big\{\{(1,0)^2\},\{(1,0),(-1,1)\},\ \{(0,1)^2\},\{(0,1),(1,-1)\}\big\}
\end{aligned}$$

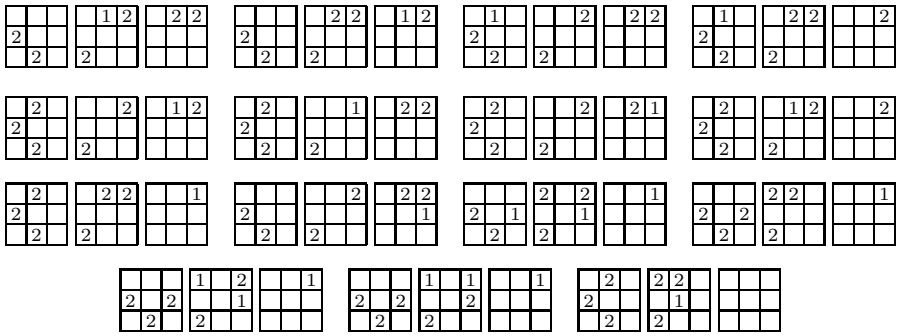
The program is divided into two parts. First find all possible multi-sets $\overline{A}$ (up to automorphism of $\mathbb{Z}_3^2$), regardless of the function f, and then, for each fixed set $\overline{A}$ and each $i \in \{1,2,3\}$, find all possible functions $f\colon \overline{A} \to \mathbb{Z}_n^2$ such that $C \subset C_i$. If no such f is found, then the lemma is proven.

5.1. **Finding all multi-sets $\overline{A}$.** The program recursively tries every possibility for $\overline{A}$ by starting with an empty set and successively adding elements. After adding an element, it checks right away if $\overline{A}$ still fulfils the above conditions before adding more elements.

To save some time, symmetry is exploited a bit. For example, if $\overline{A}$ contains exactly two elements of multiplicity 2, then we can suppose that $\overline{A}$ contains $(1,0,0)$ and $(0,1,0)$ with multiplicity 2 and $(0,0,1)$ with multiplicity 1.

As we do not exploit symmetry completely (this would be too complicated), the program finds a lot of solutions which are the same up to automorphism, so we need an algorithm to check whether there is an automorphism turning one multi-set into another one. It turns out that all solutions $\overline{A}$ do contain a basis of $\mathbb{Z}_3^2$ of elements of order two, so it is enough to try those automorphisms which map this basis of one of the sets to elements of order two of the other set.

The program finds the following 15 multi-sets. The three 3×3-grids represent the three planes of the cube $\mathbb{Z}_3^3$; the element $(0,0,0)$ is the lower left corner of the left-most plane. The numbers in the grids indicate the multiplicity of that element; empty squares mean that the element is not contained in the set.



5.2. **Finding all functions $f\colon \overline{A} \to \mathbb{Z}_n^2$.** Now fix a set $\overline{A}$ as above and fix $C := C_1$, $C := C_2$ or $C := C_3$. We have to check that there is no function $f\colon \overline{A} \to \mathbb{Z}_n^2$ such that for any pair of disjoint zero-sums Z_1 and Z_2 in $\overline{A}$, the pair $\{\sum_{z\in Z_1} f(z), \sum_{z\in Z_2} f(z)\}$ is contained in C.

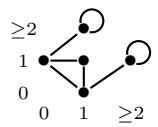
This can be reformulated as follows. From $\overline{A}$, we define the following graph $G = (V, E)$: the vertices V are the zero-sums $Z \subset \overline{A}$ such that there does exist a second zero-sum $Z' \subset \overline{A}$ which is disjoint to Z, and the edges E are the pairs $Z_1, Z_2 \in V$ which are disjoint. The set C defines another graph $G' = (V', E')$: V' consists of all elements which appear in some pair in C, and $E' = C$, i.e. the edges are just the pairs contained in C. Any function $f\colon \overline{A} \to \mathbb{Z}_n^2$ satisfying the above condition defines a graph homomorphism $\phi\colon G \to G'$, and a graph homomorphism $\phi\colon G \to G'$ yields a function f if and only if the following system of linear equations L_ϕ has a solution in $\mathbb{Z}_n$: we have two variables x_i and y_i ($i \in \{1, \dots, 13\}$) for the two coordinates of each $f(a_i), a_i \in \overline{A}$, and for each vertex zero-sum $Z = \{a_{i_1}, \dots, a_{i_k}\} \in V$ we have the two equations given by $\sum_{j=1}^{k} a_{i_j} = \phi(Z)$.

The idea of the algorithm is to try every graph homomorphism ϕ and to check that the corresponding system of linear equations L_ϕ has no solution for any n co-prime to 6. But before we can do that, we have to replace G' by a simpler graph G''.

To simplify G', we merge some of the points which differ only in one coordinate. Thus a graph homomorphism $\phi\colon G \to G''$ will give less equations in L_ϕ. We do not ensure that these equations are enough to prove the existence of f; we only need that if the equations have no solution, then no f exists.

In the case of C_1, all this graph homomorphism is overkill (as already noted directly after Lemma 12), but let us formulate it anyway so that we can treat all three cases similarly.

- Case C_3: No simplification necessary; $G'' = G'$.
- Case C_1: Merge all points of G' to one single point in G'' with a loop edge. Each zero-sum $Z \in V$ mapped to that point (i.e. all $Z \in V$) yields one equation in L_ϕ saying that the sum of the y-coordinates is equal to one.
- Case C_2: Merge all points $(1, y)$ for $y \geq 2$ into one point and all points $(x, 1)$ for $x \geq 2$ into one point. So G'' looks like this:



  Zero-sums which get mapped to $(1, 0)$, $(0, 1)$ or $(1, 1)$ still yield two equations in L_ϕ. Zero-sums which get mapped to $(1, \geq 2)$ or $(\geq 2, 1)$ yield only one equation saying that the sum of the x-coordinates resp. y-coordinates is equal to 1. In addition, we get equations for each edge which is mapped to the loop at $(1, \geq 2)$ (and, analogously, at $(\geq 2, 1)$): if $(1, y_1)$ and $(1, y_2)$ were connected in G', then $y_1 + y_2 = 1$. So if $Z_1, Z_2 \in V$ are connected and are both mapped to $(1, \geq 2)$, then the sum of the y-coordinates of all points in $Z_1 \cup Z_2$ is equal to 1.

Now our graph G'' is of reasonable size and it does make sense to try every possible homomorphism $\phi\colon G \to G''$. This is done by recursively fixing images $\phi(Z)$ for zero-sums $Z \in V$. After an image is fixed, the algorithm first checks whether the equations we already have do already yield a contradiction before going on.

The only thing left to describe is how to check whether a system of linear equations has no solution in $\mathbb{Z}_n$ for any n co-prime to 6. This could be done using the Smith normal form as in the proof of Lemma 5, but this would probably be too

slow. Instead, we use the following method, which proves in sufficiently many cases that no solution exists. (Note that we do not need an if-and-only-if algorithm.)

We apply Gaussian elimination over $\mathbb{Z}$ to our system of equations and then consider only the equations of the form "$a = 0$" for $a \neq 0$ which we get. Each such equation is interpreted as a condition on n, namely "n divides a". If, taking all these equations together, we get that n has only prime factors 2 and 3, then we have a contradiction.

The algorithm takes about one second in the case C_1, 70 minutes in the case C_2, and 5 minutes in the case C_3 (for all 15 sets $\overline{A}$ together).

One more practical remark: When recursively trying all possible maps $\phi\colon G \to G''$, we use a slightly intelligent method to choose which $\phi(Z)$ to fix next: if there is a $Z \in V$ for which there is only one possible image left, we take that one; otherwise, we take a $Z \in V$ with maximal degree.

References

[1] N. Alon, M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), 301–309.

[2] P.C. Baayen, Eeen combinatorisch probleem voor eindige Abelse groepen, Colloq. Discrete Wiskunde caput **3** Math Centre, Amsterdam (1968).

[3] G. Bhowmik, J.-C. Schlage-Puchta, Davenport's constant for Groups of the Form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, to appear in CRM Proceedings and Lecture Notes, volume 43 (2007).

[4] J. D. Bovey, P. Erdős, I. Niven, Conditions for a zero sum modulo n, *Canad. Math. Bull.* **18** (1975), 27–29.

[5] J. Brüdern, H. Godinho, On Artin's conjecture I. Systems of diagonal forms. *Bull. London Math. Soc.* **31** (1999), 305–313.

[6] C. Delorme, O. Ordaz, D. Quiroz, Some remarks on Davenport constant, *Discrete Math.* **237** (2001), 119–128.

[7] W. Gao, A. Geroldinger, On the structure of zerofree sequences, *Combinatorica* **18** (1998), 519–527.

[8] W. Gao, A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, *Integers* **3** (2003), A8.

[9] W. Gao, A. Geroldinger, Zero-sum problems and coverings by proper cosets, *European J. Combin.* **24** (2003), 531–549.

[10] A. Geroldinger, F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[11] R. Kannan, ; A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.* **8** (1979), no. 4, 499–507.

Gautami Bhowmik,
Université de Lille 1,
Laboratoire Paul Painlevé,
U.M.R. CNRS 8524,
59655 Villeneuve d'Ascq Cedex,
France
bhowmik@math.univ-lille1.fr

Immanuel Halupczok,
DMA de l'ENS,
UMR 8553 du CNRS,
45, rue d'Ulm,
75230 Paris Cedex 05,
France
math@karimmi.de

Jan-Christoph Schlage-Puchta,
Albert-Ludwigs-Universität,
Mathematisches Institut,
Eckerstr. 1
79104 Freiburg,
Germany
jcp@math.uni-freiburg.de