Integers **9** (2009), 1–22
DOI 10.1515/INTEG.2009.0xy

Inductive Methods and Zero-Sum Free Sequences

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

Abstract. A fairly long-standing conjecture is that the Davenport constant of a group $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ with $n_1 \mid \cdots \mid n_k$ is $1 + \sum_{i=1}^{k}(n_i - 1)$. This conjecture is false in general, but it remains to know 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 $\mathbb{Z}_n^2$.

Keywords. Zero-sum sequences, Davenport constant, inductive method, decidability.

AMS classification. 11B50, 20K01, 68R05.

1 Introduction and Results

Let G be a finite abelian group written additively, and $a_1, \ldots, a_k$ a sequence of elements in G. We say that this sequence contains a zero-sum if there is some non-empty subsequence $1 \le i_1 < i_2 < \cdots < i_\ell \le k$ 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 [12]. Among applications, Brüdern and Godinho [6] 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 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.

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

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 $D(G) \le n$. Indeed, given a multi-set in G, each zero-sum of its image in G/N defines an element in N, and 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 $D(G) \le 3n + 5$, which is 1 more than the exact value. The sub-optimality of this method stems from the fact that in general we have many ways to choose a system of disjoint zero-sums in G/N, 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 [4]), the corresponding lower bound being given by the multiset $\{(1,0,0)^2, (0,1,0)^2, (0,0,1)^{3n-1}\}$. In fact, this example immediately generalises to arbitrary finite groups: If $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ with $n_1 \mid \cdots \mid n_k$, then $D(G) \ge M(G) := 1 + \sum_{i=1}^{k}(n_i - 1)$. 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 article 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 $G := \mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ at once (in a finite amount of time), where n runs through all numbers co-prime to k. Note that $G \cong \mathbb{Z}_k^{\ell-1} \oplus \mathbb{Z}_{kn}$, so $M(G) = (\ell - 1) \cdot (k - 1) + kn$. Moreover, if the main conjecture does fail for some of the groups $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$, then we give a description of the set of numbers n where it fails.

It turns out that the same proof actually yields a bit more: if the main conjecture happens to be false for G one can ask about the difference $D(G) - M(G)$. Our results not only apply to the set of those n where the main conjecture fails, but also to set of such n where $D(G) - M(G) > \delta$ for any fixed δ. Here is the precise statement:

Theorem 1. *Suppose $k \ge 2$, $\ell \ge 1$ and δ are three integers. Let $\mathcal{N}$ be the set of integers n co-prime to k such that $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) > kn + \delta$. 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*

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

only in finitely many elements.

In addition, there is an algorithm which, given k, ℓ and δ, 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.

Choosing $\delta = (\ell - 1) \cdot (k - 1)$ yields:

Corollary 2. *Suppose $k \geq 2, \ell \geq 1$ are two integers. Let $\mathcal{N}$ be the set of integers n co-prime to k such that the main conjecture fails for $\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$. Then $\mathcal{N}$ has the form described in Theorem 1, and there is an algorithm which, given k and ℓ, describes $\mathcal{N}$ as above.*

In theory, 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". However, the reader should be aware that the existence of an algorithm often sounds better than it is: a straight-forward application of our algorithm would require astronomical running time even for very small k and ℓ (see constants appearing in Proposition 11). Still, we believe that by combining computer search with manual arguments one can prove the main conjecture for certain series of groups. In fact, in [4] the methods of this theorem have been explicitly applied to prove the main conjecture in the case $k = 3$, $\ell = 3$.

In the theorem, we mention that the set $\mathcal{T}$ of divisors contains 1. This is helpful to get a statement of the form "if there is a counter-example to the main conjecture, then there is a small one"; indeed, Proposition 11 is such a statement.

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 $A \subseteq \mathbb{Z}_n^2$ of cardinality $2n - 2$ contains an element a with multiplicity $\geq n - 2$.

Conjecture 3. Every integer n satisfies property B.

This conjecture is known to hold in several cases.

Proposition 4. (1) *If n and m satisfy property B, then so does nm.*

(2) *All prime numbers up to 23 satisfy property B.*

The first statement is essentially due to Gao, Geroldinger and Grynkiewicz [11], the second is proven in [3].

Theorem 5. *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 6. *The following both statements hold:*

(1) *For integers k and ℓ, there exists a constant $c(k,\ell)$ such that $D_m(\mathbb{Z}_k^\ell) \le km + c(k,\ell)$.*

(2) *We have $D_m(\mathbb{Z}_3^2) = 3m + 2$.*

Proof. (1) Given a multi-set $A \subset \mathbb{Z}_k^\ell$, 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 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 7. *Let k, ℓ be integers, $A \in \mathbb{Z}^{k\times\ell}$ a matrix, $b \in \mathbb{Z}^k$ a vector. Then either* (a) *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* (b) *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 $\le M$, and all entries of b are of modulus $\le N$, then in case (a) *$d \le \min(k,\ell)!M^{\min(k,\ell)}$, and there is a polynomial p, independent of k, ℓ, M and N, such that in case* (b)*, every element $x \in \mathcal{N}$ satisfies $x \le N2^{p(k\ell\log M)}$.*

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 $d_{ii}, i \le k$, and these entries satisfy $d_{ii} \mid d_{i+1,i+1}$. 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, $n \mid b'_j$ for every j such that $j > m$, where m is the greatest integer such that $d_{mm} \ne 0$. 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 $(n, d_{ii}) \mid b_i'$. We take d to be d_{mm}. Since $d_{ii} \mid d$ for each $i \leq m$, the set of n for which the system is solvable is of the form $\{n : (n, d) \in \mathcal{T}\}$ for some set $\mathcal{T}$. Moreover $(n, d) = 1$ implies $(n, d_{ii}) \mid b_i'$, so $1 \in \mathcal{T}$.

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 $\leq m! M^m \leq \min(k, \ell)! M^{\min(k,\ell)}$.

The entries in the set $\mathcal{N}$ are bounded by the entries in Pb, which in turn are bounded by kN times the entries of P. A general estimate for the entries of such transformation matrices was obtained by Kannan and Bachem [13, Theorem 5]. They found a polynomial algorithm which takes an $\ell' \times \ell'$-matrix A with integral entries, transforms it into Smith normal form PAQ^{-1}, and returns the transformation matrices P and Q. To apply this to our case, we enlarge our A to a square matrix by adding zeros (i.e., $\ell' = \max(k, \ell)$). Then the size of the input data is $(\ell')^2 \log M$, so the size of the output data – and in particular the number of digits of the entries of P and Q – is bounded by $p(\ell' \log M)$ for some polynomial p. After possibly changing p, this yields the claim. □

Corollary 8. *Consider the system $Ax = b$ as in the previous lemma, set $m := \min(k, \ell)$, and suppose that there are infinitely many n such that this system is solvable in $\mathbb{Z}_n$. Then for each $z \geq z_0 = \max\left(21, \frac{m \log(mM)}{\log 2}\right)$ the system is solvable for some $n \in [z, 2z]$.*

Proof. If the system has infinitely many solutions, then there exists an integer $d \leq m! M^m$ such that the system is solvable in $\mathbb{Z}_n$ whenever $(n, d) = 1$. If the system is unsolvable for all $n \in [z, 2z]$, then in particular d is divisible by all prime numbers in this interval. Since for $z \geq 21$, the product of all prime numbers in $[z, 2z]$ is $\geq 2^z$, our claim follows. □

The following result is essentially due to Bovey, Erdős and Niven [5].

Lemma 9. *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 [5]. 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 10. *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 $\iota : \mathbb{Z}_n \to \mathbb{N}$ 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 now assume that A is zero-sum free and bound the sum. In view of Lemma 9 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 $x_1, \dots, x_k$ 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 $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) > kn + \delta$ holds. More precisely, it suffices to describe this set for n sufficiently big, as long as the bound on n is computable.

By definition, $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) > kn + \delta$ holds if and only if there exists a zero-sum free set $A \subset \mathbb{Z}_k^\ell \oplus \mathbb{Z}_n$ of cardinality $kn + \delta$. Such a set A can be described by its projection $\overline{A}$ onto $\mathbb{Z}_k^\ell$ and the multi-function $f : \overline{A} \to \mathbb{Z}_n$ 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 $kn + \delta$ and a multi-function $f : \overline{A} \to \mathbb{Z}_n$ (call $(\overline{A}, f)$ a "candidate") such that the following condition holds:

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

The sum $\sum_{a\in Z} f(a)$ will often simply be called the "$\mathbb{Z}_n$-sum of Z". Moreover, we will use the following terminology: A "constant" is a value which only depends on k, ℓ and δ (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 two following steps:

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

We will find a constant c_{defect} such that for $m := n - c_{\text{defect}}$, we also have the converse: $(\overline{A}, f)$ satisfies $(*)$ if and only if for all systems $(Z_i)_{i\leq m}$ 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 show that if a candidate $(\overline{A}', f')$ satisfying $(*)$ exists, then there does already exist a candidate $(\overline{A}, f)$ of a particular form. Candidates of this form will be called "main candidates", and they are defined as follows. We will fix a suitable constant c_{var}. $(\overline{A}, f)$ is a main candidate if there exists an element $a_0 \in \mathbb{Z}_k^l$ such that there are at least $|\overline{A}| - c_{\text{var}}$ 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:

(3) A "datum for a main candidate" is a tuple $(a_0, (a_j)_j, (f_j)_j)$, where $a_0 \in \mathbb{Z}_k^\ell$, $(a_j)_j \in (\mathbb{Z}_k^\ell)^{c_{\text{var}}}$, and $(f_j)_j \in (\mathbb{Z}_n^\ell)^{c_{\text{var}}}$. Such a datum yields a main candidate $(\overline{A}, f)$ in the following way: $\overline{A} = \overline{A}_0 \cup \overline{A}_\star$, where $\overline{A}_0 := \{a_0^{kn+\delta-c_{\text{var}}}\}$ and $\overline{A}_\star := \{a_j : 1 \le j \le c_{\text{var}}\}$, $f(a_0) = \frac{1}{k}$ for each $a_0 \in \overline{A}_0$, and $f(a_j) = f_j$ for $a_j \in \overline{A}_\star$. Each main candidate can be described by such a datum.

Only the $(f_j)_j$ part of such a datum depends on n. Our goal now is to verify that after fixing a_0 and $(a_j)_j$, whether $(*)$ holds for the corresponding main candidate depends on $(f_j)_j$ in a simple way: we will construct systems of linear equations over $\mathbb{Z}$ such that $(*)$ holds if and only if the tuple $(f_j)_j$ is a solution of one of these systems modulo n. Then the theorem will follow using Lemma 7.

(4) Fix a datum $(a_0, (a_j)_j, (f_j)_j)$ and the corresponding main candidate $(\overline{A}, f)$ as in step (3). We claim that to check whether $(\overline{A}, f)$ satisfies $(*)$, it suffices to consider systems $(Z_i)_{i \le m}$ where for any $i > c_{\text{var}}$, we have $Z_i = \{a_0^k\}$. Indeed, suppose that $(Z_i)_{i \le m}$ is an arbitrary system of m disjoint zero-sums and that $B((Z_i)_i)$ does contain a zero-sum; denote by J the set of indices such that this zero-sum consists of the $\mathbb{Z}_n$-sums of the sets Z_j, $j \in J$. We will modify $(Z_i)_{i \le m}$ until it satisfies the condition of the claim, keeping the zero-sum intact.

By renumbering the sets Z_i, we may suppose $Z_i \subset \overline{A}_0$ for $i > c_{\text{var}}$; in particular, $Z_i = \{a_0^{r_i k}\}$ for some integers r_i. Now we replace each of these sets Z_i by its subset $\{a_0^k\}$. To compensate for this in the zero-sum, we have to find an $i_0 \in J$ with $i_0 \le c_{\text{var}}$; then we can repair the zero-sum by adding to Z_{i_0} all the elements which we removed from Z_i, $i \in J$, $i > c_{\text{var}}$.

Suppose that such an i_0 does not exist. Then our zero-sum is $\sum_{i \in J} \sum_{a \in Z_i} f(a) = \sum_{i \in J} |Z_i| \frac{1}{k} = \sum_{i \in J} r_i$. However, this can not be zero in $\mathbb{Z}_n$, as $\sum_{i > c_{\text{var}}} r_i \le \frac{kn+\delta-c_{\text{var}}}{k} < n$; for the last inequality, we suppose without loss $c_{\text{var}} > \delta$.

(5) From now on, we only consider systems $(Z_i)_{i \le m}$ as in step (4), i.e., with $Z_i = \{a_0^k\}$ for $i > c_{\text{var}}$. These are in bijection to the systems $(Z_i)_{i \le c_{\text{var}}}$ of c_{var} disjoint

zero-sums of $\overline{A} \setminus \{a_0^{k(m-c_{\mathrm{var}})}\} = \overline{A}_\star \cup \{a_0^{kc_{\mathrm{defect}}+\delta+(k-1)c_{\mathrm{var}}}\} =: \overline{A}_{\star\star}$. We see that the set $B := B((Z_i)_{i\le m}) \subset \mathbb{Z}_n$ corresponding to such a system is of the form $\{b_1, \dots, b_{c_{\mathrm{var}}}, 1^{m-c_{\mathrm{var}}}\}$, where $b_i = \sum_{a\in Z_i} f(a)$. This sum equals $\sum_{\{j\,:\,a_j\in Z_i\}} f_j + \frac{1}{k} z_i$ where $z_i = |Z_i \cap (\overline{A}_{\star\star} \setminus \overline{A}_\star)|$.

(6) Suppose $m \ge \frac{3}{4}n$, i.e., $n \ge 4c_{\mathrm{defect}}$. Then we can apply Corollary 10 to the set B and get that it is zero-sum free if and only if $b_i \ne 0$ for all $i \le c_{\mathrm{var}}$ and there exists some $\alpha \in \mathbb{Z}_n^\times$ such that $\sum_{b\in B} \iota(\alpha \cdot b) < n$ (with $\iota : \mathbb{Z}_n \to \mathbb{N}$ defined as in Corollary 10). Supposing $m - c_{\mathrm{var}} \ge n/2$, we get that only $\alpha = 1$ is possible, and the condition becomes $\sum_{i=1}^{c_{\mathrm{var}}} \iota(b_i) < n - (m - c_{\mathrm{var}}) = c_{\mathrm{defect}} + c_{\mathrm{var}}$.

(7) This can be reformulated as follows: Set $C_0 := \{(c_i)_{i\le c_{\mathrm{var}}} \in \mathbb{Z}^{c_{\mathrm{var}}} : c_i \ge 1 \text{ and } \sum_{i=1}^{c_{\mathrm{var}}} c_i < c_{\mathrm{defect}} + c_{\mathrm{var}}\}$ (note that C_0 does not depend on n), and denote by $\pi : \mathbb{Z}^{c_{\mathrm{var}}} \twoheadrightarrow \mathbb{Z}_n^{c_{\mathrm{var}}}$ the projection. Then B is zero-sum free if and only if $(b_i)_i = \pi((c_i)_i)$ for some $(c_i)_i \in C_0$. Moreover, we rewrite the equation $b_i = \pi(c_i)$ as $\sum_{\{j\,:\,a_j\in Z_i\}} kf_j = \pi(kc_i - z_i)$.

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

$$\overbrace{\bigvee_{\substack{a_0\in\mathbb{Z}_k^\ell \\ (a_j)_j\in(\mathbb{Z}_k^\ell)^{c_{\mathrm{var}}}}} \exists (f_j)_j \in \mathbb{Z}_n^{c_{\mathrm{var}}}}^{\text{Ex. main cand. s. th.}} \overbrace{\bigwedge_{\substack{(Z_i)_i \text{ system} \\ \text{of } c_{\mathrm{var}} \text{ disjoint} \\ \text{zero-sums in } \overline{A}_{\star\star}}}}^{\substack{\text{for all relevant} \\ \text{zero-sum systems}}} \overbrace{\bigvee_{(c_i)_i\in C_0} \bigwedge_{1\le i\le c_{\mathrm{var}}} \sum_{\{j\,:\,a_j\in Z_i\}} kf_j = \pi(kc_i - z_i)}^{\boldsymbol{B} \text{ is zero-sum free}}.$$

We used big conjunctions $\bigwedge$ and disjunctions $\bigvee$ as notation for some of the 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 (with coefficients in $\mathbb{Z}$ not depending on n) has a solution in $\mathbb{Z}_n$.

By Lemma 7, each system either contributes only finitely many integers n such that $(\overline{A}, f)$ satisfies $(*)$, or the contributed set has the form $\{n : (n, d) \in \mathcal{T}\}$ 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 two remaining steps.

(1) Let $\overline{A} \subset \mathbb{Z}_k^\ell$ be of cardinality $kn+\delta$, and suppose $Z \subset \overline{A}$ is any zero-sum subset. We will 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 6 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 $\lfloor \frac{|Z|-c(k,\ell)}{k} \rfloor + \lfloor \frac{|\overline{A}\setminus Z|-c(k,\ell)}{k} \rfloor \geq \lfloor \frac{|\overline{A}|-2c(k,\ell)}{k} \rfloor - 1 =: m =: n - c_{\text{defect}}$ disjoint zero-sums in $\overline{A}$. Note that c_{defect} does not depend on n.

The second step requires some more work, so we decompose it into several substeps. We suppose that $(\overline{A}, f)$ is a candidate satisfying $(*)$. In the first four substeps, we prove some properties of $(\overline{A}, f)$; in the last substep, we use this to construct another candidate $(\overline{A}', f')$ which will be a main candidate satisfying $(*)$.

(2.1) Claim: There is a constant c_{more} such that in any system $(Z_i)_i$ of m disjoint zero-sums of $\overline{A}$, at most c_{more} sets Z_i have more than k elements.

Let $(Z_i)_i$ be given and let r be the number of sets with more than k elements. Together, these sets have at least $r(k+1)$ elements. Remove these big sets from our system and instead use Lemma 6 to repartition them into disjoint zero-sums. After that, we have a new system $(Z_i')_i$ consisting of $m-r$ old sets and $\lfloor \frac{r(k+1)-c(k,\ell)}{k} \rfloor = r + \lfloor \frac{r-c(k,\ell)}{k} \rfloor$ new ones. By $(*)$, $B((Z_i')_i)$ does not contain a zero-sum, so this new system consists of at most $n-1$ sets; this implies $m + \lfloor \frac{r-c(k,\ell)}{k} \rfloor \leq n-1$, i.e., $r < c_{\text{defect}}k + c(k,\ell) =: c_{\text{more}}$.

(2.2) Claim: 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 9. We need $|B| = n - c_{\text{defect}} \geq \frac{2}{3}n$, i.e., $n \geq 3c_{\text{defect}}$. And we get an element b with multiplicity at least $2|B| - n + 1 = m - c_{\text{defect}} + 1 =: m - c_{\text{ws}}$ (ws = wrong sum).

(2.3) Claim: 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 of $B((Z_i)_i)$ and $B((Z_i')_i)$ by b and b' respectively. We choose $c_{\text{ws}}+1$ 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 $Z_1', \dots, Z_{c_{\mathrm{ws}}+1}'$ 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 $j \le c_{\mathrm{ws}}+1$) are disjoint from the sets Z_i (for $i \le c_{\mathrm{ws}}+1$). Each set Z_i can intersect at most k of the sets Z_j', so the additional condition forbids at most $k \cdot (c_{\mathrm{ws}}+1)$ of the m sets Z_j. Therefore we can find our desired sets if $m \ge c_{\mathrm{more}} + 2c_{\mathrm{ws}} + 1 + k \cdot (c_{\mathrm{ws}}+1)$.

Now we use Lemma 6 to complete our chosen sets $(Z_i)_{i \le c_{\mathrm{ws}}+1}$ and $(Z_i')_{i \le c_{\mathrm{ws}}+1}$ to a system of m disjoint zero-sum sets. By (2.2), 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.

(2.4) Claim: There exists a constant c_{var} such that for at most c_{var} of the elements $a \in \overline{A}$, we have $f(a) \ne \frac{1}{k}$. In fact we will choose c_{var} 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 $\sum_{a \in \mathbb{Z}_k^\ell} k \cdot \lfloor \frac{r_a}{k} \rfloor \ge |\overline{A}| - c_{\mathrm{var}}$.

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 appears with multiplicity μ in $\overline{A}$, we form $\lfloor \frac{\mu}{k} \rfloor$ 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 6 on the remainder of $\overline{A}$ to complete our system $(Z_i)_i$. Denote by κ the number of neat sets in $(Z_i)_i$.

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 $\kappa \ge \min\{m, \frac{1}{k}(|\overline{A}| - (k-1) \cdot k^\ell)\} =: m - c_{\mathrm{nn}}$ (nn = not neat; note that c_{nn} is constant).

Among all systems of m 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 $\mathbb{Z}_n$-sum 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 $m - c_{\mathrm{nn}} - c_{\mathrm{ws}}$ neat sets with sum 1. We fix this system $(Z_i)_i$ for the remainder of step (2.4).

Choose $a \in \mathbb{Z}_k^\ell$, and let $\mathcal{N}_a$ 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 $\mathcal{N}_a$; in particular this implies that the value of f on $\mathcal{N}_a$ is $\frac{1}{k}$. Suppose f is not constant on $\mathcal{N}_a$. Then there are two elements $a_1, a_2 \in \mathcal{N}_a$ with $f(a_1) \ne f(a_2)$ 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.

Doing the above construction for all $a \in \mathbb{Z}_k^\ell$ yields the claim: The union $\mathcal{N} := \bigcup_{a \in \mathbb{Z}_k^\ell} \mathcal{N}_a$ contains all neat sets Z_i with $\mathbb{Z}_n$-sum 1, so it has cardinality at least

$k(m - c_{\mathrm{nn}} - c_{\mathrm{ws}})$. On the other hand, if f is not constant equal to $\frac{1}{k}$ on a set $\mathcal{N}_a$, then $|\mathcal{N}_a| = k$, and this can happen for at most $k^\ell - 1$ of these sets. Thus f is equal to $\frac{1}{k}$ on at least $k(m - c_{\mathrm{nn}} - c_{\mathrm{ws}}) - k(k^\ell - 1) =: |\overline{A}| - c_{\mathrm{var}}$ elements. As these elements are contributed in groups of k, we also get the slightly stronger statement mentioned at the beginning of this step.

(2.5) Claim: There is a main candidate $(\overline{A}', f')$ satisfying $(*)$ (still assuming that $(\overline{A}, f)$ is an arbitrary candidate satisfying $(*)$).

Recall 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 at least $|\overline{A}'| - c_{\mathrm{var}}$ copies a of a_0 which moreover satisfy $f'(a) = \frac{1}{k}$.

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 of a in $\overline{A}$ with $f(a) = \frac{1}{k}$. Choose $a_0 \in \mathbb{Z}_k^\ell$ such that r_{a_0} is maximal; in particular $r_{a_0} \geq \frac{|\overline{A}| - c_{\mathrm{var}}}{k^\ell}$. 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 $a' \in \overline{A}$ of a satisfying $f(a') = \frac{1}{k}$ by the same number of copies a'' of a_0, and set $f'(a'') = \frac{1}{k}$ on these copies. Denote by ϕ the bijection from $\overline{A}$ to $\overline{A}'$ which describes these replacements.

Step (2.4) ensures that $(\overline{A}', f')$ is a main candidate; it remains to show that it satisfies $(*)$. To this end, for any zero-sum $Z' \subset \overline{A}'$, we construct a zero-sum $Z \subset \overline{A}$ which has the same $\mathbb{Z}_n$-sum as Z'. As $(\overline{A}, f)$ satisfies $(*)$, this $\mathbb{Z}_n$-sum is not equal to zero, so $(\overline{A}', f')$ satisfies $(*)$, too.

So suppose a zero-sum $Z' \subset \overline{A}'$ is given. Consider the set $\mathcal{M} \subset \overline{A}'$ of copies a' of a_0 with $f'(a') = \frac{1}{k}$, and for $a \in \mathbb{Z}_k^\ell$ define the subset $\mathcal{M}_a := \{a' \in \mathcal{M} : \phi^{-1}(a') \text{ is a copy of } a\}$. As $|\mathcal{M}_a|$ is a multiple of k for any $a \neq a_0$, and assuming $|\mathcal{M}_{a_0}| = r_{a_0} \geq k - 1$, in Z' we may replace elements of $\mathcal{M}$ by other elements of $\mathcal{M}$ such that $|\mathcal{M}_a \cap Z'|$ is a multiple of k for any $a \neq a_0$. (This changes neither the sum nor the $\mathbb{Z}_n$-sum of Z'.) Now take $Z := \phi^{-1}(Z')$. As elements are moved by groups of k, Z has the same sum as Z' (i.e., zero), and as $f' \circ \phi = f$, it has the same $\mathbb{Z}_n$-sum. □

3.1 Computation of the Bounds

The proof of Theorem 1 actually gives a little more than just decidability. In fact, for each k, ℓ and δ, there is a computable constant n_0, such that $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) \leq \delta + kn$ 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 subsection we compute an upper bound for n_0 (Proposition 11). 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.

We now compute all bounds appearing in the proof of Theorem 1.

A bound for Lemma 6: 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 $\le k$. Then $c(k,\ell) \le D^k(\mathbb{Z}_k^\ell) - k$, 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 $\le k$. For $D^k(\mathbb{Z}_k^\ell)$ we have the trivial bound $k^{\ell+1}$, but also the estimate $D^k(\mathbb{Z}_k^\ell) \le (256\ell\log\ell)^\ell \cdot k$ 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, δ and $c(k,\ell)$, and give an explicit estimate using only the bound $c(k,\ell) \le k^{\ell+1}$. (For the explicit estimates, we use that we may suppose $k \ge 2$, $\ell \ge 3$, $\delta \ge 2$.)

Step (1): $c_{\text{defect}} = 1 + \lceil \frac{2c(k,\ell)-\delta}{k} \rceil \le 3k^\ell$.

Step (2.1): $c_{\text{more}} = k \cdot c_{\text{defect}} + c(k,\ell) \le 4k^{\ell+1}$.

Step (2.2): $c_{\text{ws}} = c_{\text{defect}} - 1 \le 3k^\ell$.

Step (2.2) needs $n \ge 3c_{\text{defect}}$. So $n \ge 9k^\ell$ suffices.

Step (2.3) needs $n \ge c_{\text{defect}} + c_{\text{more}} + 2c_{\text{ws}} + 1 + k \cdot (c_{\text{ws}} + 1)$. So $n \ge 12k^{\ell+1}$ suffices.

Step (2.4): $c_{\text{nn}} = \max\{0, (k-1) \cdot k^{\ell-1} - \frac{1}{k}\delta - c_{\text{defect}}\}$. The proof of Theorem 1 allows us to assume $c_{\text{defect}} = 3k^\ell$, which yields $c_{\text{nn}} = 0$. (However, using more careful estimates for $c(k,\ell)$ could yield non-zero values for c_{nn}.)

Step (2.4): $c_{\text{var}} = \delta + k(c_{\text{defect}} + c_{\text{nn}} + c_{\text{ws}} + k^\ell - 1) \le 7k^{\ell+1} + \delta$.

Step (2.5) needs $\frac{kn+\delta-c_{\text{var}}}{k^\ell} \ge k-1$. So $n \ge 8k^\ell$ suffices.

Step (4) needs $c_{\text{var}} > \delta$, which is certainly the case.

Step (6) needs $n \ge 4c_{\text{defect}}$. So $n \ge 12k^\ell$ suffices.

Step (6) also needs $m - c_{\text{var}} \ge n/2$, i.e., $n \ge 2(c_{\text{defect}} + c_{\text{var}})$. Here $n \ge 17k^{\ell+1} + 2\delta$ suffices. This is the largest bound on n of the proof.

Concerning the systems of equations, we get:

Step (7): The coefficients of the equations are all equal to k.

Step (7): The absolute values of the right-hand sides of the equations are bounded by $\max(k(c_{\text{defect}} + c_{\text{var}}), |\overline{A}_{\star\star} \setminus \overline{A}_\star|) = k(c_{\text{defect}} + c_{\text{var}}) \le 9k^{\ell+2} + k\delta$.

Step (8): The number of variables in each system of equations is $c_{\text{var}} \le 7k^{\ell+1} + \delta$.

Step (8): The left-hand side of any equation is of the form $\sum_j k f_j$, where the sum runs over a subset of $\{1, \dots, c_{\text{var}}\}$; thus we may suppose that each system of equation consists of at most $2^{c_{\text{var}}} \le 2^{7k^{\ell+1}+\delta}$ equations.

Hence, we can apply Lemma 7 and Corollary 8 to obtain the following.

Proposition 11. *There exists a constant c such that the following holds true. Suppose that k, ℓ, δ are integers such that there exists some n, co-prime to k, satisfying $D(\mathbb{Z}_k^\ell \oplus \mathbb{Z}_n) > \delta + kn$. Denote by $\mathcal{N}$ the set of these n, and let n_1 be minimum of $\mathcal{N}$. Then we have $n_1 \leq 2^{2^{c(k^{\ell+1}+\delta)}}$. Moreover, if $\mathcal{N}$ is infinite, then we have $n_1 \leq 6\ell(7k^{\ell+1}+\delta)\log k\delta$.*

Proof. Using the estimates above and Lemma 7, in the case that $\mathcal{N}$ is finite, we obtain the bound

$$n_1 \leq (9k^{\ell+2}+k\delta)2^{p\left(2^{7k^{\ell+1}+\delta}\cdot(7k^{\ell+1}+\delta)\cdot\log k\right)} \leq 2^{2^{c(k^{\ell+1}+\delta)}},$$

and our claim follows in this case. If $\mathcal{N}$ is infinite, we additionally use Corollary 8 to find that the systems of linear equations are solvable for an $n \in [z, 2z]$, provided that $z \geq \max(z_0, 21)$, where

$$\begin{aligned} z_0 &\leq \tfrac{1}{\log 2} c_{\mathrm{var}} \log(c_{\mathrm{var}} k) \\ &\leq \tfrac{1}{\log 2}(7k^{\ell+1}+\delta)\log(7k^{\ell+2}+\delta k) \\ &\leq 3\ell(7k^{\ell+1}+\delta)\log k\delta, \end{aligned}$$

where we used the fact that we may suppose $\ell \geq 3$, $\delta \geq 2$. Hence, $n_1 \leq 2z_0$. To be sure to get an element of $\mathcal{N}$ in $[z, 2z]$, we moreover need $z \geq 17k^{\ell+1} + 2\delta$, which is less than the bound just computed. Thus there exists some $n \in \mathcal{N}$ which is at most two times our bound; this was our claim. □

Note that the smallest case of interest would be $k = 4, \ell = 3, \delta = 6$, that is, checking $D(\mathbb{Z}_4^2 \oplus \mathbb{Z}_{4n}) = 4n + 6$ for all odd n up to 3375 would imply that this equation has only finitely many counter-examples. Unfortunately, even the case $n = 3$ has not yet been decided, although it is within reach of modern computers.

4 Proof of Theorem 5

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 12. *Among* 17 *arbitrary elements in $\mathbb{Z}_3^3$ there is a zero-sum of length at most* 3*, and among nine* distinct *elements there is a zero-sum of length at most* 3*. Moreover, up to linear equivalence, there is precisely one set of eight 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 [4, Lemma 1 (ii)], the first part is folklore (and follows immediately from the second part). □

Lemma 13. *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 $F : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ 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 $\mathbb{Z}_n^2/\langle b\rangle$. We may suppose that 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 different 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 determines 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 possibilities. 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 13:

Lemma 14. *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) $C_1 = \big\{\{(x_1,1),(x_2,1)\} : x_1, x_2 \in \mathbb{Z}_n\big\}$.

(2) $C_2 = C_2' \cup C_2''$ *with* $C_2' = \big\{\{(1,0),(x,1)\},\{(x,1),(1-x,1)\} : x \in \mathbb{Z}_n\big\}$ *and* $C_2'' = \big\{\{(0,1),(1,y)\},\{(1,y),(1,1-y)\} : y \in \mathbb{Z}_n\big\}$.

(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 13, 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 following two lemmas:

Lemma 15. *Suppose n is an integer co-prime to 6 and $\overline{A} \subseteq \mathbb{Z}_3^3$ has ten 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 $g : \overline{A} \to \mathbb{Z}_n$ (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 [4, 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 where g has two different 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 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 16. *Suppose n is an integer co-prime to 6, $\overline{A} \subseteq \mathbb{Z}_3^3$ has thirteen elements, and $f : \overline{A} \to \mathbb{Z}_n^2$ 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 14.*

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 $g : \overline{A} \to \mathbb{Z}_n$ which sends to 1 any zero-sum of $\overline{A}$ which is disjoint to another zero-sum. □

4.2 The Proof Itself

We are now in a position to prove Theorem 5.

Proof of Theorem 5. 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 $f : \overline{A} \to \mathbb{Z}_n^2$ 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 12). 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 nine distinct points would contain such a zero-sum (by Lemma 12) there are precisely eight points taken twice. Since the only configuration of eight distinct points without a zero-sum of length 3 is the one given in Lemma 12, 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 13 and obtain a linear function $F : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ such that for every c as above $F(c) = 1$. But now $g := F \circ f$ is a contradiction to Lemma 15.

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 16. 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 14, 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 16. □

5 Computer Proof of Lemma 16

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 $f : \overline{A} \to \mathbb{Z}_n^2$. 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 14:

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

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 $f : \overline{A} \to \mathbb{Z}_n^2$ such that $C \subset C_i$. If no such f is found, then the lemma is proven.

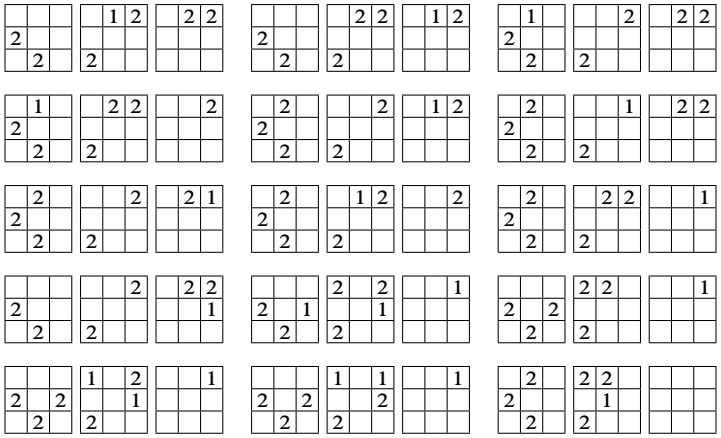
5.1 Finding All Multi-Sets $\overline{A}$

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 $f : \overline{A} \to \mathbb{Z}_n^2$

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 $f : \overline{A} \to \mathbb{Z}_n^2$ 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 from 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 $f : \overline{A} \to \mathbb{Z}_n^2$ satisfying the above condition defines a graph homomorphism $\phi : G \to G'$, and a graph homomorphism $\phi : G \to G'$ 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 ($i \in \{1, \ldots, 13\}$) for the two coordinates of

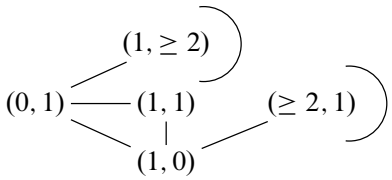
each $f(a_i), a_i \in \overline{A}$, and for each vertex zero-sum $Z = \{a_{i_1}, \dots, a_{i_k}\} \in V$ we have the two equations given by $\sum_{j=1}^{k} f(a_{i_j}) = \phi(Z)$.

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''; in particular, we need G'' to be independent of n.

To simplify G', we merge some of the points which differ only in one coordinate. Then f also defines a graph homomorphism $\psi : G \to G''$, but ψ does not completely determine $\phi : G \to G'$. In particular, if we only know ψ (and not ϕ), we only get a subset L_ψ of the equations L_ϕ. We do not ensure that these equations L_ψ 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, the graph homomorphism argument is overkill (as already noted directly after Lemma 14), 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_ψ 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_ψ. 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 we can iterate through every possible homomorphism $\psi : G \to G''$. This is done by recursively fixing images $\psi(Z)$ 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 7, 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 $\psi : G \to G''$, we use a slightly intelligent method to choose which $\psi(Z)$ 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 and 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, I. Halupczok and J.-C. Schlage-Puchta, The structure of maximal zero-sum free sequences, to appear in *Acta Arith.*

[4] G. Bhowmik and 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.

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

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

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

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

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

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

[11] W. Gao, A. Geroldinger and D. J. Grynkiewicz, Inverse zero-sum problems III, to appear in *Acta Arith.*

[12] A. Geroldinger and 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.

[13] R. Kannan and 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.

Received April 23, 2009; revised May 22, 2009; accepted May 25, 2009.

Author information

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

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

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