ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 2, 2012

ON THE EXISTENCE OF ZERO-SUM SUBSEQUENCES OF DISTINCT LENGTHS

BENJAMIN GIRARD

ABSTRACT. In this paper, we obtain a characterization of short normal sequences over a finite abelian p-group, thus answering positively a conjecture of Gao for a variety of such groups. Our main result is deduced from a theorem of Alon, Friedland and Kalai, originally proved so as to study the existence of regular subgraphs in almost regular graphs. In the special case of elementary p-groups, Gao's conjecture is solved using Alon's Combinatorial Nullstellensatz. To conclude, we show that, assuming every integer satisfies Property B, this conjecture holds in the case of finite abelian groups of rank two.

1. Introduction. Let $\mathcal{P}$ be the set of prime numbers, and let G be a finite abelian group, written additively. By $\exp(G)$ we denote the exponent of G. If G is cyclic of order n, it will be denoted by C_n. In the general case, we can decompose G as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $1 < n_1 | \cdots | n_r \in \mathbf{N}$. For each g in G, we denote by $\mathrm{ord}\,(g)$ its order in G, and by $\langle g \rangle$ the subgroup it generates.

By a *sequence* over G of *length* ℓ, we mean a finite sequence of ℓ elements from G, where repetitions are allowed and the order of elements is disregarded. We use multiplicative notation for sequences. Let

$$S = g_1 \cdot \ldots \cdot g_\ell = \prod_{g \in G} g^{\mathsf{v}_{g(S)}}$$

be a sequence over G, where, for all $g \in G$, $\mathsf{v}_g(S) \in \mathbf{N}$ is called the *multiplicity* of g in S. We call $\mathrm{Supp}\,(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\}$ the *support* of S and $\sigma(S) = \sum_{i=1}^{\ell} g_i = \sum_{g \in G} g\mathsf{v}_g(S)$ the *sum* of S. In addition, we say that $s \in G$ is a *subsum* of S when

$$s = \sum_{i \in I} g_i \text{ for some } \varnothing \subsetneq I \subseteq \{1, \ldots, \ell\}.$$

2010 AMS *Mathematics subject classification.* Primary 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05.
Received by the editors on August 25, 2009, and in revised form on October 1, 2009.
DOI:10.1216/RMJ-2012-42-2-583 Copyright ©2012 Rocky Mountain Mathematics Consortium

If 0 is not a subsum of S, we say that S is a *zero-sumfree sequence.* If $\sigma(S) = 0$, then S is said to be a *zero-sum sequence.* If, moreover, one has $\sigma(T) \neq 0$ for all proper subsequences $T \mid S$, then S is called a *minimal zero-sum sequence.*

By $\mathsf{D}(G)$ we denote the smallest integer $t \in \mathbf{N}^*$ such that every sequence S over G of length $|S| \geq t$ contains a non empty zero-sum subsequence. The number $\mathsf{D}(G)$ is called the *Davenport constant* of the group G. Even though its definition is purely combinatorial, the invariant $\mathsf{D}(G)$ found many applications in number theory (see for instance the book [**13**] which presents the various aspects of non-unique factorization theory and [**12**] for a recent survey). Thus, many direct and inverse problems related to $\mathsf{D}(G)$ have been studied during the last decades, and even if numerous results were proved (see [**13**, Chapter 5] and [**8**] for a survey), its exact value is known for very special types of groups only.

A sequence S over a finite abelian group G is said to be *dispersive* if it contains two non empty zero-sum subsequences S_1 and S_2 of distinct length, and *non-dispersive* otherwise, that is, when all non empty zero-sum subsequences of S have same length. One can readily notice, using the very definition of the Davenport constant, that every sequence S over G with $|S| \geq 2\mathsf{D}(G)$ is dispersive, since S has to contain at least two disjoint non empty zero-sum subsequences. So, one can ask for the smallest integer $t \in \mathbf{N}^*$ such that every sequence S over G with $|S| \geq t$ is dispersive. The associated inverse problem is then to make explicit the structure of non-dispersive sequences over a finite abelian group. Concerning this problem, Gao, Hamidoune and Wang recently proved [**11**] that every non-dispersive sequence of n elements in C_n has at most two distinct values, solving a conjecture of Graham reported in a paper of Erdős and Szemerédi [**4**]. This result was then generalized by Grynkiewicz in [**14**].

In this article, we study a still widely open conjecture, proposed by Gao in [**7**] on the structure of the so-called *normal sequences* over a finite abelian group G. A sequence S over G with $|S| \geq \mathsf{D}(G)$ is said to be *normal* if all its zero-sum subsequences S' satisfy $|S'| \leq |S| - \mathsf{D}(G) + 1$. Gao's conjecture is the following (see also [**8**, Conjecture 4.9]).

Conjecture 1. *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \cdots \mid n_r \in \mathbf{N}$, be a finite abelian group. Also let S be a normal sequence over G of length $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, n_1 - 1]\!]$. Then S is of the form $S = 0^i T$, where T is a zero-sumfree sequence.*

This notion of a normal sequence, first introduced in [**7**], happens to be crucial in the characterization of sequences S over G with $|S| = \mathsf{D}(G) + |G| - 2$ and which do not contain any zero-sum subsequence S' satisfying $|S'| = |G|$ (see Theorem 1.7 in [**7**]). The following two theorems, due to Gao (see Theorems 1.5 and 1.6 in [**7**]), are the only results known concerning the structure of normal sequences over a finite abelian group. Before stating these two results on Conjecture 1, we recall that an integer $n \geq 2$ is said to satisfy *Property* B if every minimal zero-sum sequence over C_n^2 with $|S| = 2n - 1$ contains some element repeated $n - 1$ times (see [**13**, subsection 5.8] and [**9, 10, 20**] for recent progress). It is conjectured that every $n \geq 2$ satisfies Property B.

Theorem 1.1. *Conjecture* 1 *holds whenever*:

(i) *G is a finite cyclic group.*

(ii) *$G \simeq C_n^2$, where n satisfies Property* B.

(iii) *$G \simeq C_p^r$, where $p \in \{2, 3, 5, 7\}$.*

Theorem 1.2. *Let G be a finite abelian group, and let p be the smallest prime divisor of* $\exp(G)$. *Then Conjecture* 1 *holds for every integer $i \leq \min(6, p - 1)$.*

2. New results and plan of the paper. In this paper, we use the notion of a dispersive sequence to obtain a characterization of short normal sequences over a finite abelian p-group, thus improving both Gao's results on this problem. The main theorem (Theorem 2.3) is proved in Section 3 yet, before giving this general result, we would like to emphasize its consequences.

Theorem 2.1. *Let G be a finite abelian p-group, and let S be a normal sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, p - 1]\!]$. Then S is of the form $S = 0^i T$, where T is a zero-sumfree sequence.*

Firstly, Theorem 2.1 improves Theorem 1.2 by showing that the assumption $i \leq 6$ is unnecessary for finite abelian p-groups. Secondly, it improves statement (iii) of Theorem 1.1 by settling Conjecture 1 for every elementary p-group. More generally, we can derive immediately from Theorem 2.1 the following corollary on Gao's conjecture.

Corollary 2.2. *Conjecture* 1 *holds for all groups of the form $G \simeq C_p \oplus H$, where H is any finite abelian p-group.*

The main result of this paper is deduced from a theorem of Alon, Friedland and Kalai (see [**2**, Theorem A.1]), originally proved so as to study the existence of regular subgraphs in almost regular graphs. Our result is the following.

Theorem 2.3. *Let G be a finite abelian p-group, and let S be a sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, p]\!]$. Also let $\mathcal{A}$ be any $(i-1)$-subset of $[\![1, p-1]\!]$. Then S contains a non-empty zero-sum subsequence S' such that*

$$|S'| \not\equiv b \pmod{p}, \text{ for all } b \in \mathcal{A}.$$

Consequently, Theorem 2.3 gives the existence of non-empty zero-sum subsequences whose length avoids certain remainders modulo p. In addition, this result applies to 'short' sequences, the length of which is close to $\mathsf{D}(G)$, thus allowing one to tackle Gao's conjecture, whereas other existing results with a similar flavor (see for instance [**19**, Theorem 1.2]) hold for longer sequences only. In particular, Theorem 2.3 provides the following insight into dispersive sequences.

Corollary 2.4. *Let G be a finite abelian p-group, and let S be a sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \geq 1$. The following two statements hold.*

(i) *If $i \geq 2$ and S contains a zero-sum subsequence S' with $p \nmid |S'|$, then S is dispersive.*

(ii) *If S contains no non-empty zero-sum subsequence S' with $p \mid |S'|$, then $i \leq p - 1$, and S has to contain at least i non-empty zero-sum subsequences with pairwise distinct lengths.*

In Section 4, we give a proof of Theorem 2.3, in the special case of elementary p-groups, using the polynomial method. Since this proof is short and may be relevant in its own right, we will present it in full.

In Section 5 we then prove the following theorem, which extends statement (ii) of Theorem 1.1 to every finite abelian group of rank two. The proof of this theorem relies on a structural result obtained by Schmid [**20**], which is a characterization of long minimal zero-sum sequences over these groups, provided that a suitable divisor of their exponent satisfies Property B.

Theorem 2.5. *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbf{N}^*$ and $m \geq 2$. Also let S be a normal sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, m-1]\!]$. If m satisfies Property* B*, then S is of the form $S = 0^i T$, where T is a zero-sumfree sequence.*

Finally, in Section 6, we propose two general conjectures suggested by the results proved in this paper.

3. The case of finite abelian p-groups. As stated in Section 2, we prove our Theorem 2.3 by using the following theorem of Alon, Friedland and Kalai (see [**2**, Theorem A.1]). Before stating this result, we need to introduce the following notation. Let $\mathbf{Z}$ be the set of integers. For $\mathcal{S} \subseteq \mathbf{Z}$ and $m \in \mathbf{Z}$, we denote by $\mathrm{card}_m(\mathcal{S})$ the number of distinct elements in $\mathcal{S}$ modulo m.

Theorem 3.1. *Let p be a prime, and let $1 \leq d_1 \leq \cdots \leq d_n$ be n integers. For $1 \leq j \leq n$, let $\mathcal{S}_j \subseteq \mathbf{Z}$ be a set of integers containing 0. For $1 \leq i \leq m$, let $(a_{i,1}, \ldots, a_{i,n})$ be a vector with integer coordinates. If*

$$m \geq \sum_{j=1}^{n} \left(p^{d_j} - \mathrm{card}_p(\mathcal{S}_j)\right) + 1,$$

then a subset $\varnothing \subsetneq I \subseteq \{1, \ldots, m\}$ and numbers $s_j \in \mathcal{S}_j$ $(1 \leq j \leq n)$ exist such that

$$\sum_{i \in I} a_{i,j} \equiv s_j \pmod{p^{d_j}}, \text{ for all } 1 \leq j \leq n.$$

For instance, it may be observed that Theorem 3.1 provides the exact value for the Davenport constant of a finite abelian p-group, which was originally obtained by van Emde Boas, Kruyswijk and Olson (see [**3, 16**]).

Indeed, let $G \simeq C_{p^{d_1}} \oplus \cdots \oplus C_{p^{d_r}}$, where $1 \leq d_1 \leq \cdots \leq d_r \in \mathbf{N}$, be a finite abelian p-group, and let us set $\mathsf{D}^*(G) = \sum_{i=1}^{r}(p^{d_i} - 1) + 1$. On the one hand, an elementary construction (see [**13**, Proposition 5.1.8]) implies that $\mathsf{D}(G) \geq \mathsf{D}^*(G)$. On the other hand, let $(e_1, \dots, e_r)$ be a basis of G, where $\operatorname{ord}(e_i) = p^{d_i}$ for all $i \in [\![1, r]\!]$, and let $S = g_1 \cdot \ldots \cdot g_m$ be a sequence over G of length $m = \mathsf{D}^*(G)$. Setting $g_i = a_{i,1}e_1 + \cdots + a_{i,r}e_r$ for all $i \in [\![1, m]\!]$ and $\mathcal{S}_j = \{0\}$ for every $j \in [\![1, r]\!]$, one readily obtains the converse inequality $\mathsf{D}(G) \leq \mathsf{D}^*(G)$ by Theorem 3.1, thus $\mathsf{D}(G) = \mathsf{D}^*(G)$ for every finite abelian p-group.

Using Theorem 3.1, we can now prove the main theorem of this paper.

Proof of Theorem 2.3. Let $G \simeq C_{p^{d_1}} \oplus \cdots \oplus C_{p^{d_r}}$, where $1 \leq d_1 \leq \cdots \leq d_r \in \mathbf{N}$, be a finite abelian p-group. Let $(e_1, \dots, e_r)$ be a basis of G, where $\operatorname{ord}(e_i) = p^{d_i}$ for all $i \in [\![1, r]\!]$, and let $S = g_1 \cdot \ldots \cdot g_m$ be a sequence over G of length $m = \mathsf{D}(G) + i - 1$, where $i \in [\![1, p]\!]$. The elements of S can be written in the following way:

$$\begin{array}{ccccc} g_1 & = a_{1,1}e_1 & + \cdots + & a_{1,r}e_r, \\ \vdots & \vdots & & \vdots \\ g_m & = a_{m,1}e_1 & + \cdots + & a_{m,r}e_r. \end{array}$$

Now, let us set $n = r + 1$ and $d_n = 1$. Also let $\mathcal{A}$ be a $(i-1)$-subset of $[\![1, p-1]\!]$, and $\overline{\mathcal{A}} = [\![0, p-1]\!] \backslash \mathcal{A}$. For all $j \in [\![1, n]\!]$, we set

$$\mathcal{S}_j = \begin{cases} \overline{\mathcal{A}} & \text{if } j = n, \\ \{0\} & \text{otherwise.} \end{cases}$$

Since $(p^{d_n} - \operatorname{card}_p(\mathcal{S}_n)) = (p - |\overline{\mathcal{A}}|) = |\mathcal{A}| = i - 1$, one obtains

$$\sum_{j=1}^{n} \left(p^{d_j} - \operatorname{card}_p(\mathcal{S}_j)\right) + 1 = \mathsf{D}(G) + i - 1 = m.$$

Therefore, using Theorem 3.1, there exists a subset $\varnothing \subsetneq I \subseteq \{1, \dots, m\}$ such that

$$\begin{cases} \sum_{i \in I} a_{i,j} \equiv 0 \pmod{p^{d_j}} & \text{for all } 1 \leq j \leq r, \\ \sum_{i \in I} 1 = |I| \equiv s \pmod{p} & \text{for some } s \in \overline{\mathcal{A}}. \end{cases}$$

Consequently, the sequence $S' = \prod_{i \in I} g_i$ is a non-empty zero-sum subsequence of S such that $|S'| = |I| \not\equiv b \pmod{p}$ for all $b \in \mathcal{A}$, which is the desired result. $\square$

We can now prove Theorem 2.1 and Corollary 2.4.

Proof of Theorem 2.1. We prove this theorem by induction on $i \in [\![1, p-1]\!]$. If $i = 1$, the desired result is straightforward. Now, let $i \geq 2$, and let us assume that the assertion of Theorem 2.1 is true for every $1 \leq k \leq i-1$. Let S be a normal sequence over G with $|S| = \mathsf{D}(G) + i - 1$, and let $\mathcal{A}$ be a $(i-1)$-subset satisfying $\{i\} \subseteq \mathcal{A} \subseteq [\![1, p-1]\!]$. Then, Theorem 2.3 gives the existence of a non-empty zero-sum subsequence $S' \mid S$ such that $|S'| \not\equiv i \pmod{p}$. In particular, one has $|S'| \neq i$, and since S is a normal sequence, we must have $|S'| \leq i - 1$. Now, let $T \mid S$ be the sequence such that $S = TS'$. Then $|T| = \mathsf{D}(G) + k - 1$, where $1 \leq k = i - |S'| \leq i - 1$. Moreover, since S is a normal sequence, every non-empty zero-sum subsequence $T' \mid T$ has to satisfy $|T'| \leq k = i - |S'|$, that is, T is also a normal sequence. Therefore, the induction hypothesis applied to T implies that S is of the form $S = 0^k U$. One has $|U| = \mathsf{D}(G) + \ell - 1$, where $1 \leq \ell = i - k \leq i - 1$, and since S is a normal sequence, every non empty zero-sum subsequence $U' \mid U$ has to satisfy $|U'| \leq \ell = i - k$, that is, U is also a normal sequence. Finally, the induction hypothesis applied to U implies that S is of the form $S = 0^k 0^{i-k} V = 0^i V$, where V is a zero-sumfree sequence over G, which completes the proof. $\square$

Proof of Corollary 2.4. (i) Let S be a sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \geq 2$, such that S contains a zero-sum subsequence S' with $p \nmid |S'|$. Then, one has $|S'| = qp + r$ for some integers $q \geq 0$ and $r \in [\![1, p-1]\!]$. Now, let T be any subsequence of S such that $|T| = \mathsf{D}(G) + 2 - 1$. Specifying $\mathcal{A} = \{r\}$ in Theorem 2.3, we obtain the existence of a non empty zero-sum subsequence $T' \mid T$ such that $|T'| \not\equiv r \pmod{p}$. In particular, one obtains $|T'| \not\equiv |S'| \pmod{p}$, which implies $|T'| \neq |S'|$. Since T' is also a zero-sum subsequence of S, the desired result is proved.

(ii) Let S be a sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \geq 1$, such that S contains no non empty zero-sum subsequence S' with

$p \mid |S'|$. If one had $i \geq p$, we would obtain, specifying $\mathcal{A} = [\![1, p-1]\!]$ in Theorem 2.3, that every subsequence $T \mid S$ with $|T| = \mathsf{D}(G) + p - 1$ contains a non empty zero-sum subsequence T' such that $p \mid |T'|$, which contradicts the assumption made on S. Now, we can prove the second part of the assertion, by induction on $k \in [\![1, i]\!]$. If $k = 1$, then since $|S| \geq \mathsf{D}(G)$, S has to contain a zero-sum subsequence S_1 such that $p \nmid |S_1|$, and we are done. Now, let $k \in [\![2, i]\!]$, and let us assume the assertion is true for $k-1$, that is, S contains at least $k-1$ non empty zero-sum subsequences $S_1, \ldots, S_{k-1}$ with pairwise distinct lengths. By hypothesis, one has $p \nmid |S_j|$ for all $j \in [\![1, k-1]\!]$, and we can write $|S_j| = q_j p + r_j$, where $q_j \geq 0$ and $r_j \in [\![1, p-1]\!]$. Now, let $\mathcal{A}$ be a $(i-1)$-subset satisfying $\{r_1, \ldots, r_{k-1}\} \subseteq \mathcal{A} \subseteq [\![1, p-1]\!]$. Then, by Theorem 2.3, we obtain the existence of a non-empty zero-sum subsequence $S_k \mid S$ such that $|S_k| \not\equiv b \pmod p$ for all $b \in \mathcal{A}$. In particular, $|S_k| \neq |S_j|$ for all $j \in [\![1, k-1]\!]$, and consequently, S contains at least k non empty zero-sum subsequences $S_1, \ldots, S_k$ with pairwise distinct lengths, and the proof is complete. $\square$

4. The special case of elementary p-groups. In this section, we propose an alternative proof of Theorem 2.3, in the special case of elementary p-groups, which uses an algebraic tool introduced by Alon and is called *Combinatorial Nullstellensatz* (see [**1**] for a survey on this method). This polynomial method uses the fact that a non-zero multivariate polynomial over a field cannot vanish on 'large' Cartesian products so as to derive a variety of results in combinatorics, additive number theory and graph theory. This method relies on the following theorem.

Theorem 4.1 (Combinatorial Nullstellensatz). *Let $\mathbf{F}$ be a field and f a polynomial in $\mathbf{F}[x_1, \ldots, x_n]$ of total degree $\deg(f)$, admitting a monomial of the following form:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \text{ of degree } \sum_{i=1}^{n} \alpha_i = \deg(f).$$

Then, for any choice of n subsets $S_1, \ldots, S_n \subseteq \mathbf{F}$ such that $|S_i| > \alpha_i$ for all $i \in [\![1, n]\!]$, there exists an element $(s_1, \ldots, s_n) \in S_1 \times S_2 \times \cdots \times S_n$ such that one has $f(s_1, \ldots, s_n) \neq 0$.

Proof of Theorem 2.3 *in the special case of elementary p-groups.* Let p be a prime, and let $G \simeq C_p^r$ be an elementary p-group of rank r. Also let $(e_1, \dots, e_r)$ be a basis of G, and let $S = g_1 \cdot \ldots \cdot g_m$ be a sequence over G of length $m = \mathsf{D}(G) + k - 1$, where $k \in [\![1, p]\!]$. The elements of S can be written in the following way:

$$\begin{aligned} g_1 &= a_{1,1}e_1 + \cdots + a_{1,r}e_r, \\ &\vdots \qquad\quad \vdots \qquad\qquad \vdots \\ g_m &= a_{m,1}e_1 + \cdots + a_{m,r}e_r. \end{aligned}$$

Let $\mathcal{A}$ be a $(k-1)$-subset of $[\![1, p-1]\!]$, and also let $P \in \mathbf{F}_p[x_1, \dots, x_m]$ be the following polynomial over the finite field $\mathbf{F}_p$ of order p,

$$\begin{aligned} P(x_1, \dots, x_m) = {} & \prod_{h=1}^{r} \prod_{j=1}^{p-1} \left(\sum_{i=1}^{m} a_{i,h} x_i^{p-1} - j \right) \prod_{j \in \mathcal{A}} \left(\sum_{i=1}^{m} x_i^{p-1} - j \right) \\ & - \delta \prod_{i=1}^{m} \left(x_i^{p-1} - 1 \right), \end{aligned}$$

where $\delta \in \mathbf{F}_p$ is chosen such that $P(0, \dots, 0) = 0$. In particular, since no element of $\mathcal{A}$ is a multiple of p, one has $\delta \neq 0$. Moreover, the total degree of

$$\prod_{h=1}^{r} \prod_{j=1}^{p-1} \left(\sum_{i=1}^{m} a_{i,h} x_i^{p-1} - j \right) \prod_{j \in \mathcal{A}} \left(\sum_{i=1}^{m} x_i^{p-1} - j \right)$$

being $(r(p-1) + (k-1))(p-1) = (\mathsf{D}(G) + k - 2)(p-1) < m(p-1)$, we deduce that $\deg(P) = m(p-1)$. Now, since the coefficient of $\prod_{i=1}^{m} x_i^{p-1}$ is $-\delta \neq 0$, Theorem 4.1 implies that there exists a non-zero element $x = (x_1, \dots, x_m) \in \mathbf{F}_p^m$ such that $P(x_1, \dots, x_m) \neq 0$. Consequently, setting $I = \{i \in [\![1, m]\!] \mid x_i \neq 0\}$, we obtain that $S' = \prod_{i \in I} g_i$ is a non empty zero-sum subsequence of S satisfying $|S'| = |I| \not\equiv b \pmod{p}$ for all $b \in \mathcal{A}$, which completes the proof. □

5. The case of finite abelian groups of rank two. In this section, we prove a result extending statement (ii) of Theorem 1.1 to every finite abelian group of rank two. The proof of this theorem relies on the following result of Schmid [**20**], which gives a structural characterization of minimal zero-sum sequences of length $\mathsf{D}(G) = m + mn - 1$ over the group $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbf{N}^*$ and $m \geq 2$, under the hypothesis that m satisfies Property B.

Theorem 5.1. *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbf{N}^*$ and $m \geq 2$ are a finite abelian group of rank two. The following sequences are minimal zero-sum sequences of maximal length.*

(i) $S = e_j^{\mathrm{ord}\,(e_j)-1} \prod_{i=1}^{\mathrm{ord}\,(e_k)} (-x_i e_j + e_k)$ *where (e_1, e_2) is a basis of G with* $\mathrm{ord}\,(e_2) = mn$, *$\{j,k\} = \{1,2\}$, and $x_i \in \mathbf{N}$ with $\sum_{i=1}^{\mathrm{ord}\,(e_k)} x_i \equiv -1$* $(\mathrm{mod}\ \mathrm{ord}\,(e_j))$.

(ii) $S = g_1^{sm-1} \prod_{i=1}^{(n+1-s)m} (-x_i g_1 + g_2)$ *where $s \in [\![1, n]\!]$, $\{g_1, g_2\}$ is a generating set of G with* $\mathrm{ord}\,(g_2) = mn$ *and such that $s = 1$ or $mg_1 = mg_2$, and $x_i \in \mathbf{N}$ with $\sum_{i=1}^{(n+1-s)m} x_i = m - 1$.*

In addition, if m satisfies Property B, *then all minimal zero-sum sequences of maximal length over G are of this form.*

Moreover, Gao and Zhuang proved a useful structural result on normal sequences (see [**7**, Theorem 1.2]). In this section, we will use the following corollary of this theorem.

Theorem 5.2. *Let G be a finite abelian group, and let S be a normal sequence over G. Then S is of the form $S = 0^k TU$, where T is a zero-sumfree sequence with $|T| = \mathsf{D}(G) - 1$, and U is a sequence over G such that* $\mathrm{Supp}\,(U) \subseteq \mathrm{Supp}\,(T)$.

Using the above two results, we can now prove the following theorem.

Theorem 5.3. *Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbf{N}^*$ and $m \geq 2$, be a finite abelian group of rank two. Let T be a zero-sumfree sequence over G with $|T| = \mathsf{D}(G) - 1$, and let U be a non-empty sequence over G such that* $\mathrm{Supp}\,(U) \subseteq \mathrm{Supp}\,(T)$. *If m satisfies Property* B, *then every non empty zero-sum subsequence S' of $S = TU$ has length $|S'| \geq m$.*

Proof of Theorem 5.3. Let G and $S = TU$ be as in the statement of the theorem. By Theorem 5.1, and since $T' = T(-\sigma(T))$ is a minimal zero-sum sequence over G, $S = TU$ can be written in the following fashion

$$S = g_1^{\ell_1} \prod_{i=1}^{\ell_2} (-x_i g_1 + g_2)\,,$$

where $\{g_1, g_2\}$ is a generating set of G with $\operatorname{ord}(g_2) = mn$, and $\ell_1, \ell_2 \in \mathbf{N}$ are such that $\ell_1 + \ell_2 = |S|$. In particular, one has $mg_1 \in \langle mg_2 \rangle$, and $ag_1 \in \langle g_2 \rangle$ if and only if $m \mid a$. Since $|S| \geq \mathsf{D}(G)$, it has to contain a non empty zero-sum subsequence S'. Now, let us write $S' = VW$ where $V \mid g_1^{\ell_1}$ and $W = \prod_{i \in I}(-x_i g_1 + g_2)$, for some $I \subseteq [\![1, \ell_2]\!]$. We obtain

$$\sigma(S') = |V|\, g_1 - \left(\sum_{i \in I} x_i\right) g_1 + |W|\, g_2 = 0.$$

Since $\sigma(S') = 0 \in \langle g_2 \rangle$, we have

$$m \mid |V| - \left(\sum_{i \in I} x_i\right)$$

which implies that, for some $a \in \mathbf{N}$, one has

$$|V| - \left(\sum_{i \in I} x_i\right) = amg_2.$$

Thus, $\sigma(S') = (am + |W|)g_2 = 0$, which gives $m \mid \operatorname{ord}(g_2) \mid am + |W|$. Consequently, $m \mid |W|$. If $|W| \geq m$, then we are done. Otherwise, one has $|W| = |I| = 0$, and $\sigma(S') = |V| g_1 = 0 \in \langle g_2 \rangle$. Thus, $m \mid |V| = |S'|$, and since S' is a non empty zero-sum subsequence of S, we obtain $|S'| \geq m$, which is the desired result. □

Theorem 2.5 is now an easy corollary of Theorem 5.3.

Proof of Theorem 2.5. Let $G \simeq C_m \oplus C_{mn}$, where $m, n \in \mathbf{N}^*$ and $m \geq 2$, be a finite abelian group of rank two. Also let S be a normal sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, m-1]\!]$. By Theorem 5.2, S is of the form $S = 0^k TU$, where T is a zero-sumfree sequence with $|T| = \mathsf{D}(G) - 1$, and U is a sequence over G such that

Supp $(U) \subseteq$ Supp (T). Since $m > i$, S does not contain any zero-sum subsequence S' with $|S'| \geq m$. So, it follows from Theorem 5.3 that U is empty, which implies $k = i$ and completes the proof. □

6. Two concluding remarks. In this section, we would like to present two conjectures suggested by the results proved in this paper. The first one may be interpreted as a more general version of Theorem 2.3 and would imply Conjecture 1 in the same way as Theorem 2.3 implies Theorem 2.1.

Conjecture 2. *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \cdots \mid n_r \in \mathbf{N}$, be a finite abelian group, and let S be a sequence over G with $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, n_1]\!]$. Also let $\mathcal{A}$ be any $(i-1)$-subset of $[\![1, n_1 - 1]\!]$. Then S contains a non-empty zero-sum subsequence S' such that*

$$|S'| \not\equiv b \pmod{n_1}, \quad \textit{for all } b \in \mathcal{A}.$$

Let G be a finite abelian group of exponent m. By $\mathsf{s}_{m\mathbf{N}}(G)$ we denote the smallest $t \in \mathbf{N}^*$ such that every sequence S over G with $|S| \geq t$ contains a non empty zero-sum subsequence S' with $|S'| \equiv 0 \pmod{m}$. The exact value of the invariant $\mathsf{s}_{m\mathbf{N}}(G)$ is currently known for finite abelian groups of rank $r \leq 2$, and finite abelian p-groups only (see [**8**, Theorem 6.7]). For instance, Conjecture 2 implies that, for all integers $n, r \geq 1$, one has $\mathsf{s}_{n\mathbf{N}}(C_n^r) = (r+1)(n-1)+1$. This conjecture would also help to tackle the inverse problem associated to $\mathsf{s}_{m\mathbf{N}}(G)$, by giving an account of the variety of zero-sum subsequences contained in a long sequence without any non empty zero-sum subsequence of length congruent to 0 modulo m. Finally, any progress on this conjecture would provide new insight into the structure of sequences over C_n without any zero-sum subsequence of length n (see [**8**, Theorem 7.5, Conjecture 7.6], as well as [**18**]).

Let G be a finite abelian group of exponent m, and let $\ell \geq 1$ be an integer. By $\eta_{\ell m}(G)$, we denote the smallest $t \in \mathbf{N}^*$ such that every sequence S over G with $|S| \geq t$ contains a non empty zero-sum subsequence S' with $|S'| \leq \ell m$. It may be observed that, for every $\ell \geq \lceil \mathsf{D}(G)/m \rceil$, one has the equality $\eta_{\ell m}(G) = \mathsf{D}(G)$. Now, our second conjecture is the following.

Conjecture 3. *Let G be a finite abelian group of exponent m, and let S be a sequence over G with $|S| = \eta_{\ell m}(G) + i - 1$, where $i \in [\![1, \ell m]\!]$. Then S contains a zero-sum subsequence S' of length $i \le |S'| \le \ell m$.*

Let G be a finite abelian group of order n and exponent m. For instance, if $\ell = 1$ in Conjecture 3, one obtains a generalization of Conjecture 6.5 in [**8**], due to Gao. If $\ell = n/m$, then, since it is known that $\mathsf{D}(G) \le n = \ell m$, we obtain $\eta_{\ell m}(G) = \mathsf{D}(G)$. Therefore, Conjecture 3 implies that every sequence S over G such that $|S| = \mathsf{D}(G) + i - 1$, where $i \in [\![1, n]\!]$, has to contain a zero-sum subsequence S' with $i \le |S'| \le n$, which can be seen as a generalization of Gao's theorem (see [**5**, Theorem 1]). Finally, if $\ell = \lceil \mathsf{D}(G)/m \rceil$ and $i = \ell m$, then Conjecture 3 implies that every sequence S over G with $|S| = \mathsf{D}(G) + \ell m - 1$ has to contain a zero-sum subsequence S' with $|S'| = \ell m$, which would provide an answer to a problem of Gao (see [**6**, Section 3] and [**8**, Theorem 6.12]).

Note added in proof. Shortly after this paper was accepted for publication, Reiher [**17**] proved that Property B holds for all primes. It follows from the results of [**9**] that all integers $n \ge 2$ satisfy Property B. Thus, our Theorem 2.5 holds unconditionally, which gives a positive answer to Conjecture 1 for all abelian groups of rank two. Further progress has since been made on this conjecture [**15**].

Acknowledgments. This work was supported by a postdoctoral grant awarded by the École Polytechnique, Paris. I am also grateful to Melvyn Nathanson and to the City University of New York's Graduate Center for all their hospitality and for providing an excellent atmosphere for research.

REFERENCES

1. N. Alon, *Combinatorial Nullstellensatz*, Comb. Probab. Comput. **8** (1999), 7–29.

2. N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs*, J. Combin. Theory **37** (1984), 79–91.

3. P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups*, Reports ZW-1967-009, Math. Centre, Amsterdam, 1967.

4. P. Erdős and E. Szemerédi, *On a problem of Graham*, Publ. Math. Debrecen **23** (1976), 123–127.

5. W.D. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory **58** (1996), 100–103.

6. ———, *On zero-sum subsequences of restricted size* II, Discrete Math. **271** (2003), 51–59.

7. W.D. Gao and J.J. Zhuang, *Sequences not containing long zero-sum subsequences*, Europ. J. Comb. **27** (2006), 777–787.

8. W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. **24** (2006), 337–369.

9. W. Gao, A. Geroldinger and D. Grynkiewicz, *Inverse zero-sum problems* III, Acta Arith. **141** (2010), 103–152.

10. W. Gao, A. Geroldinger and W.A. Schmid, *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245–279.

11. W. Gao, Y. Hamidoune and G. Wang, *Distinct lengths modular zero-sum subsequences: A proof of Graham's conjecture*, J. Number Theory **130** (2010), 1425–1431.

12. A. Geroldinger, *Additive group theory and non-unique factorizations*, in *Combinatorial number theory and additive group theory*, A. Geroldinger and I. Ruzsa, eds., Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser, 2009.

13. A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure Appl. Math. **278**, Chapman & Hall/CRC, Boca Raton, 2006.

14. D. Grynkiewicz, *Note on a conjecture of Graham*, Europ. J. Comb. **32** (2011), 1336–1344.

15. H. Guan, P. Yuan and X. Zeng, *Normal sequences over finite abelian groups*, J. Combin. Theory **118** (2011), 1519–1524.

16. J.E. Olson, *A combinatorial problem on finite abelian groups*, I, J. Number Theory **1** (1969), 8–10.

17. C. Reiher, *A proof of the theorem according to which every prime number possesses Property* B, manuscript.

18. S. Savchev and F. Chen, *Long n-zero-free sequences in finite cyclic groups*, Discrete Math. **308** (2008), 1–8.

19. W.A. Schmid, *On zero-sum subsequences in finite abelian groups*, Integers **1** (2001), #A01.

20. ———, *Inverse zero-sum problems* II, Acta Arith. **143** (2010), 333–343.

Graduate Center's Department of Mathematics, The City University of New York, 365 Fifth Avenue, New York City, NY 10016
Email address: bgirard@gc.cuny.edu