MINIMAL ZERO-SUM SEQUENCES IN $C_n \oplus C_n$

GÜNTER LETTL AND WOLFGANG A. SCHMID

Abstract. Minimal zero-sum sequences of maximal length in $C_n \oplus C_n$ are known to have $2n-1$ elements, and this paper presents some new results on the structure of such sequences.

It is conjectured that every such sequence contains some group element $n-1$ times, and this will be proved for sequences consisting of only three distinct group elements.

We prove, furthermore, that if p is an odd prime then any minimal zero-sum sequence of length $2p-1$ in $C_p \oplus C_p$ consists of at most p distinct group elements; this is best possible, as shown by well-known examples. Moreover, some structural properties of minimal zero-sum sequences in $C_p \oplus C_p$ of length $2p-1$ with p distinct elements are established.

The key result proving our second theorem can also be interpreted in terms of Hamming codes, as follows: for an odd prime power q each linear Hamming code $\mathcal{C} \subset \mathbb{F}_q^{q+1}$ contains a non-zero word with letters only 0 and 1.

1. Introduction and main results

Many problems in graph theory, additive number theory and factorization theory translate into questions about zero-sum sequences in finite abelian groups. Thus the interest to investigate such sequences is large, and the reader is referred e.g. to [1, 7, 11] or the book [10, Chapter 5] for more details and literature.

In this paper we use notation and terminology from [6]. We denote by C_n an (additively written) cyclic group of order n. Let $n \geq 2$ be an integer and let $G = C_n \oplus C_n$. Extensive studies were made to investigate the structure of minimal zero-sum sequences in G. A *sequence* (or a multi-set) S in G is an element

$$S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$$

of the free abelian (multiplicatively written) monoid generated by G. The *length* of S is denoted by $|S| = l$. Some $T \in \mathcal{F}(G)$ is called a *subsequence* of S if T divides S in $\mathcal{F}(G)$ (in symbols: $T \mid S$). The sequence S is called a *zero-sum sequence* if its sum $\sigma(S) = \sum_{i=1}^{l} g_i$ equals $0 \in G$, and it is called a *minimal* zero-sum sequence if additionally each proper non-trivial subsum does not equal 0.

The maximal length of a minimal zero-sum sequence in a finite abelian group is called Davenport's constant of the group. Among others, it is known that Davenport's constant of $C_m \oplus C_n$, where $m \mid n$, is equal to $n + m - 1$, in particular Davenport's constant of G equals $2n - 1$ (see [15]). Given S as above, let $\text{supp}(S) = \{g_1, \dots, g_l\} \subset G$ denote the support of S, i.e. the set of group elements appearing in the sequence S, and for $g \in G$

2000 *Mathematics Subject Classification.* Primary 11B75, secondary 20D60, 94B05.

The second author was supported by the Austrian Science Fund FWF (Project P16770-N12).

let $\mathsf{v}_g(S) = |\{i\colon 1 \le i \le l \text{ and } g_i = g\}|$ denote the multiplicity of the group element g in the sequence S. Further, let

$$\Sigma(S) = \Big\{\sum_{i\in I} g_i \colon \emptyset \ne I \subset \{1, \dots, l\}\Big\}$$

denote the set of sums of all (non-empty) subsequences of S.

First, let us recall [5, Proposition 6.3.1] and [6, Proposition 4.1.2(b)].

Proposition 1. *Let $n \ge 2$ be an integer, $G = C_n \oplus C_n$ and $S \in \mathcal{F}(G)$ be a minimal zero-sum sequence of maximal length, i.e., $|S| = 2n - 1$. Then one has:*

- **a)** *Any $g \in \operatorname{supp}(S)$ has maximal order, i.e., $\operatorname{ord}(g) = n$.*
- **b)** *For any $e_1 \in \operatorname{supp}(S)$ with $\mathsf{v}_{e_1}(S) = n - 1$, there exists some $e_2 \in G$ such that $\{e_1, e_2\}$ is a basis of G and*

$$S = e_1^{n-1} \prod_{i=1}^{n} (a_i e_1 + e_2)$$

with $a_i \in \mathbb{Z}$ and $\sum_{i=1}^n a_i \equiv 1 \mod (n)$. In particular, all elements occurring in S apart e_1 lie in a single coset of $\langle e_1 \rangle$ which has order n.

Notice that any sequence $S \in \mathcal{F}(G)$, given as in Proposition 1.b), is a minimal zero-sum sequence. Thus, this result provides a classification of all minimal zero-sum sequences of maximal lengths in G containing some group element with multiplicity $n - 1$. According to [6, Definition 3.2], a natural number $n \in \mathbb{N}$ is said to have *"Property B"*, if each minimal zero-sum sequence of maximal length in $C_n \oplus C_n$ contains some element with multiplicity $n - 1$. It is known that all $n \le 6$ have Property B [6, Proposition 4.2] and that there are arbitrarily large n with Property B [6, Theorem 8.1]. A (positive) answer to the question whether actually all n have Property B, would allow progress on various other problems (cf. [5, 6, 9]).

It is easy to see that any minimal zero-sum sequence of maximal length in G contains at least 3 different group elements. We will prove that if such a sequence contains exactly 3 different elements, then it contains some element with multiplicity $n - 1$.

Theorem 1. *Let $n \ge 2$ be an integer, $G = C_n \oplus C_n$ and $S = g_1^{\lambda_1} g_2^{\lambda_2} g_3^{\lambda_3} \in \mathcal{F}(G)$, with pairwise distinct $g_1, g_2, g_3 \in G$ and $n - 1 \ge \lambda_1 \ge \lambda_2 \ge \lambda_3 \ge 1$, be a minimal zero-sum sequence of maximal length, i.e., $|S| = \lambda_1 + \lambda_2 + \lambda_3 = 2n - 1$. Then*

$$\lambda_1 = n - 1\ .$$

For the rest of this section we will concentrate on the case where n is prime. We denote by $\mathbb{P}$ the set of rational primes. Then one has further information about the structure of minimal zero-sum sequences of maximal length (see [7, Corollary 6.3] and [6, Lemma 3.8.2]):

Proposition 2. *For $p \in \mathbb{P}$ let $G = C_p \oplus C_p$ and $S \in \mathcal{F}(G)$ be a minimal zero-sum sequence of maximal length, i.e., $|S| = 2p - 1$. Then one has:*

- **a)** *Any two distinct elements of $\operatorname{supp}(S)$ generate G.*
- **b)** $3 \le |\operatorname{supp}(S)| \le p + 1$.

For $p \geq 3$ there are examples for minimal zero-sum sequences in $C_p \oplus C_p$ with length $2p-1$ such that the support contains up to p different elements (see [5, Corollary 10.5.3]) and we will show that there exists no such sequence having a support with $p+1$ elements.

Theorem 2. *Let p be an odd prime and $G = C_p \oplus C_p$. Then for every minimal zero-sum sequence $S \in \mathcal{F}(G)$ of maximal length $|S| = 2p-1$ one has*

$$|\operatorname{supp}(S)| \leq p \ .$$

This result supports the belief that Property B holds for $p \in \mathbb{P}$, since the former would be an easy consequence of the latter together with Proposition 1.b).

In the following result we obtain some information on the structure of any minimal zero-sum sequence S in $C_p \oplus C_p$ with maximal length containing p different elements. We recall that by Proposition 2 any two different elements in the support of S generate distinct cyclic subgroups of order p of $C_p \oplus C_p$, and thus there exists a unique cyclic subgroup of order p of $C_p \oplus C_p$ that is not generated by an element occurring in S.

Theorem 3. *Let p be an odd prime, $G = C_p \oplus C_p$ and $S = \prod_{i=1}^p g_i^{\lambda_i} \in \mathcal{F}(G)$ a minimal zero-sum sequence of maximal length, i.e., $|S| = \sum_{i=1}^p \lambda_i = 2p-1$, with pairwise distinct $g_1, \ldots, g_p \in G$, and suppose that*

$$p-1 \geq \lambda_1 \geq \cdots \geq \lambda_m > \lambda_{m+1} = \cdots = \lambda_p = 1 \ .$$

Thus m denotes the number of indices i with $\lambda_i > 1$, and $2 \leq m \leq p-1$. Then we have the following:

- **a)** *Let $H \subset G$ be the cyclic subgroup of order p different from $\langle g_i \rangle$ for each $1 \leq i \leq p$. Then*
$$\{g_1, \ldots, g_m\} \subset g_1 + H.$$
- **b)** $m \leq \sqrt{2p-2}$.
- **c)** *Either $\lambda_1 = p-1$ or* $\dfrac{1+\sqrt{4p-3}}{2} \leq \lambda_1 < p - \sqrt[4]{p}$.

Theorem 3 can be seen as a further small step towards proving that Property B holds for $p \in \mathbb{P}$. Note that if $p \in \mathbb{P}$ has Property B, the sequence in Theorem 3 would have parameters $\lambda_1 = p-1$ and $\lambda_2 = m = 2$.

2. Proof of Theorem 1

First, we will show that the analog of Proposition 2.a) for composite n only holds for sequences S with $|\operatorname{supp}(S)| = 3$.

Lemma 1. *Let $G = C_n \oplus C_n$ and $S = \prod_{i=1}^r g_i^{\lambda_i} \in \mathcal{F}(G)$ with pairwise distinct $g_1, \ldots, g_r \in G$ be a minimal zero-sum sequence of maximal length, i.e., $|S| = \sum_{i=1}^r \lambda_i = 2n-1$. If for some $1 \leq j \leq r$ we have $\lambda_1 + \cdots + \lambda_j \geq n$, then $\{g_1, \ldots, g_j\}$ generates G.*

If three natural numbers $\lambda_i \leq n-1$ sum up to $2n-1$, then any two of them have a sum of at least n. Similarly, if four natural numbers $\lambda_4 \leq \cdots \leq \lambda_1 \leq n-1$ sum up to $2n-1$, then $\lambda_1+\lambda_2$, $\lambda_1+\lambda_3$, and either $\lambda_2+\lambda_3$ or $\lambda_1+\lambda_4$ have a sum of at least n. This observation yields the following corollary.

Corollary 1. *Let the notation be as in Lemma 1.*

a) *If* $r = 3$ *then any two elements of* $\mathrm{supp}(S) = \{g_1, g_2, g_3\}$ *form a basis of* G.

b) *If* $r = 4$ *then there exist (at least)* 3 *pairs of elements of* $\mathrm{supp}(S)$*, each of which is a basis of* G.

The following example shows that Proposition 2.a) does not generalize for composite n and sequences S with $|\mathrm{supp}(S)| > 3$, and also that in Lemma 1 the inequality $\lambda_1 + \cdots + \lambda_j \geq n$ is best possible. Let $n \in \mathbb{N}$ be a composite number, put $n = d_1 d_2$ with integers $d_i \geq 2$, and let e_1, e_2 be a basis of $G = C_n \oplus C_n$. Then

$$e_1^{n-1}\, e_2^{n-d_2-1}\, (d_1 e_1 + e_2)^{d_2}\, (e_1 + e_2)^1 \in \mathcal{F}(G)$$

is a minimal zero-sum sequence of maximal length, but $\{e_2, d_1 e_1 + e_2\}$ is not a basis of G and the multiplicities of these two elements sum up to $n - 1$.

Proof of Lemma 1.
Put $\lambda_1 + \cdots + \lambda_j = 2n - 1 - l$ with $0 \leq l \leq n-1$ and suppose to the contrary that $\{g_1, \ldots, g_j\}$ generates a proper subgroup G_0 of G. From Proposition 1.a) we have $G_0 \simeq C_n \oplus C_{n/m}$ with some $m > 1$ that divides n. Extending the canonical homomorphism $\pi : G \to G/G_0 \simeq C_m$ to $\mathcal{F}(G)$ we obtain a zero-sum sequence $S' = \pi(g_{j+1})^{\lambda_{j+1}} \ldots \pi(g_r)^{\lambda_r} \in \mathcal{F}(C_m)$ of length l. Now we can find minimal zero-sum sequences $A'_i \in \mathcal{F}(C_m)$ (with lengths at most m) such that $S' = A'_1 \ldots A'_k$ with $km \geq l$. From this we obtain some factorization $g_{j+1}^{\lambda_{j+1}} \ldots g_r^{\lambda_r} = A_1 \ldots A_k$ with $A_i \in \mathcal{F}(G)$ and $\pi(A_i) = A'_i$. Since A'_i are zero-sum sequences in C_m we have $\sigma(A_i) = a_i \in G_0$. Therefore $S_0 = g_1^{\lambda_1} \ldots g_j^{\lambda_j} a_1 \ldots a_k \in \mathcal{F}(G_0)$ is a zero-sum sequence in G_0 of length

$$\begin{aligned} |S_0| = \lambda_1 + \cdots + \lambda_j + k &\geq 2n - 1 - l + \frac{l}{m} = n + \frac{n}{m} - 1 + (1 - \frac{1}{m})(n - l) > \\ &> n + \frac{n}{m} - 1. \end{aligned}$$

Thus, the length of S_0 exceeds Davenport's constant of G_0 (cf. Introduction) and consequently the zero-sum sequence S_0 in G_0 is not minimal. It follows that the zero-sum sequence S in G is not minimal either, a contradiction. □

For an integer m let $|m|_n$ denote the smallest non-negative integer which is congruent to m modulo (n).

Proof of Theorem 1.
Let S be as in Theorem 1. Since by Corollary 1 any two elements of $\mathrm{supp}(S) = \{g_1, g_2, g_3\}$ are a basis of G, we have $g_3 = b g_1 + a g_2$ with some $1 \leq a, b \leq n - 1$ and $\gcd(a, n) = \gcd(b, n) = 1$. Knowing that S is a zero-sum sequence, we have

$$\lambda_1 + b\lambda_3 \equiv 0 \mod (n) \qquad \text{and} \qquad \lambda_2 + a\lambda_3 \equiv 0 \mod (n)\ . \tag{1}$$

Since S is minimal, there exists no $(x, y, z) \in \mathbb{N}^3$ with $0 < x \leq \lambda_1$, $0 < y \leq \lambda_2$ and $0 < z < \lambda_3$ satisfying

$$x + bz \equiv 0 \mod (n) \qquad \text{and} \qquad y + az \equiv 0 \mod (n)\ .$$

Put

$M_b = \{z : 1 \leq z \leq n-1 \text{ and there exists an } x \in \{1, 2, \ldots, \lambda_1\} \text{ with } x + bz \equiv 0 \mod (n)\}$

and

$M_a = \{z : 1 \le z \le n-1 \text{ and there exists a } y \in \{1,2,\dots,\lambda_2\} \text{ with } y + az \equiv 0 \mod (n)\}$.

With $\gcd(a,n) = \gcd(b,n) = 1$ one obtains $|M_b| = \lambda_1$ and $|M_a| = \lambda_2$. On the one hand we have $M_a \cap M_b \cap \{1,2,\dots,\lambda_3 - 1\} = \emptyset$, on the other hand

$$|M_a \cap M_b| = \lambda_1 + \lambda_2 - |M_a \cup M_b| \ge 2n - 1 - \lambda_3 - n + 1 = (n-1) - (\lambda_3 - 1) ,$$

so we conclude that $M_a \cap M_b = \{\lambda_3, \lambda_3 + 1, \dots, n-1\}$.
For $1 \le \nu \le n - \lambda_3$ we have $n - \nu \in M_a$, which means $1 \le |\nu a|_n \le \lambda_2$, and we get

(2) $$\big\{|\nu a|_n \colon 1 \le \nu \le n - \lambda_3\big\} \subset \{1,\dots,\lambda_2\} .$$

If $\lambda_3 = 1$ we immediately obtain $\lambda_2 = \lambda_1 = n-1$, which proves the assertion of the theorem in this case.

Now suppose that $\lambda_3 \ge 2$. Since S is a minimal zero-sum sequence, (1) and (2) hold and we can apply Lemma 2 below with $l = \lambda_3$ and $L = \lambda_2$. So $a = 1$, and the second congruence of (1) yields $\lambda_2 + \lambda_3 = n$, thus $\lambda_1 = n - 1$ as asserted. □

Lemma 2. *Let $a, n \in \mathbb{N}$ with $1 \le a \le n-1$ and $\gcd(a,n) = 1$. Further let $2 \le l \le L \in \mathbb{N}$ with $2L + l \le 2n - 1$ such that*

(3) $$-la \equiv L \mod (n)$$

and

(4) $$\{|\nu a|_n \colon 1 \le \nu \le n - l\} \subset \{1,2,\dots,L\}$$

hold. Then $a = 1$.

Proof.
From the suppositions of the lemma we obtain

(5) $$\frac{n+1}{3} \le n - l \le L \le n - \frac{l+1}{2} .$$

We will use the theory of (simple) continued fractions as explained e.g. in [12, Chapter X]. Let $\frac{a}{n} = [0; a_1, a_2, \dots, a_j]$ be the continued fraction expansion of $\frac{a}{n}$ with $a_j \ge 2$ and with convergents

$$\frac{p_0}{q_0} = \frac{0}{1} , \quad \frac{p_1}{q_1} = \frac{1}{a_1} , \quad \frac{p_2}{q_2} = \frac{a_2}{1 + a_1 a_2} , \ \dots , \ \frac{p_j}{q_j} = \frac{a}{n} .$$

It is well known (e.g. [12, Theorems 150−151]) that

(6) $$\left|\frac{a}{n} - \frac{p_{j-1}}{q_{j-1}}\right| = \frac{1}{nq_{j-1}} \qquad \text{and} \qquad \left|\frac{a}{n} - \frac{p_{j-2}}{q_{j-2}}\right| = \frac{a_j}{nq_{j-2}} .$$

Case 1: Suppose that j is odd.
If $j = 1$ we obtain $\frac{a}{n} = \frac{1}{a_1}$, and with $\gcd(a,n) = 1$ conclude that $a = 1$.
Now let $j \ge 3$. Since $\dfrac{p_{j-1}}{q_{j-1}} < \dfrac{p_j}{q_j} = \dfrac{a}{n} < \dfrac{p_{j-2}}{q_{j-2}}$ we can derive from (6) that

(7) $$q_{j-1} a \equiv 1 \mod (n) \qquad \text{and} \qquad q_{j-2} a \equiv n - a_j \mod (n) .$$

Having supposed that $a_j \ge 2$, we get $n = a_j q_{j-1} + q_{j-2} \ge 3q_{j-2}$, and with (5) we obtain $q_{j-2} \le \frac{n}{3} < n - l$. Therefore the second congruence of (7) together with (4) implies

$n - a_j \le L \le n-2$. Putting $m = L + a_j - n$ one has $0 \le m \le a_j - 2$, and adding m times the first congruence of (7) to the second one gives

$$(mq_{j-1} + q_{j-2})a \equiv m + n - a_j = L \mod (n) \ .$$

Using (3) and $1 \le mq_{j-1} + q_{j-2} \le n-1$ we obtain $mq_{j-1} + q_{j-2} = n - l$. Now we insert $L = n + m - a_j$ and $l = (a_j - m)q_{j-1}$ into the last inequality of (5) to get the contradiction

$$n \ge L + \frac{l+1}{2} = n + \frac{1}{2} + (a_j - m)\Big(\frac{q_{j-1}}{2} - 1\Big) \ge n + \frac{1}{2} \ ,$$

where we used $j - 1 \ge 2$ and $q_{j-1} \ge q_2 \ge 2$.

Case 2: Suppose that j is even.

From $0 < \frac{a}{n} < 1$ we see that $j \ge 2$, and j being even implies $\dfrac{p_{j-2}}{q_{j-2}} < \dfrac{p_j}{q_j} = \dfrac{a}{n} < \dfrac{p_{j-1}}{q_{j-1}}$. This time we derive from (6) that

$$\text{(8)} \qquad q_{j-1}a \equiv n-1 \mod (n) \qquad \text{and} \qquad q_{j-2}a \equiv a_j \mod (n) \ .$$

Now $n - 1 > L$ together with (4) implies $q_{j-1} > n - l > \frac{n}{3}$. On the other hand, $n = a_j q_{j-1} + q_{j-2} > a_j q_{j-1}$ gives $q_{j-1} < \frac{n}{a_j}$. Thus $a_j = 2$ must hold, and with $n = 2q_{j-1} + q_{j-2} \ge 2q_{j-1} + 1$ we obtain

$$\text{(9)} \qquad n - l < q_{j-1} \le \frac{n-1}{2} \ .$$

Let us first suppose that $j = 2$. Then $\frac{a}{n} = [0; a_1, 2] = \frac{2}{2a_1+1}$ implies $a = 2$, and with the estimation (9) we obtain

$$\{|\nu a|_n \colon 1 \le \nu \le n - l\} = \{2, 4, \ldots, 2(n-l)\} \ .$$

Using (4) and (5) we get $2(n-l) \le L \le n - \frac{l+1}{2}$, which yields $n - l \le \frac{n-1}{3}$ as a contradiction to (5). (Note that the inequalities (5) are just sharp enough to exclude the case $a = 2$.)

Now we may suppose that $j \ge 4$. Then $n = 2q_{j-1} + q_{j-2} = (2a_{j-1}+1)q_{j-2} + 2q_{j-3} > 5q_{j-3}$ yields $q_{j-1} - a_{j-1}q_{j-2} = q_{j-3} < \frac{n}{5} < n - l$, and from (9) we have $q_{j-1} > n - l$. Therefore we can choose an integer m with $1 \le m \le a_{j-1}$ such that

$$\text{(10)} \qquad q_{j-1} - mq_{j-2} \le n - l < q_{j-1} - (m-1)q_{j-2} \ .$$

Now subtracting m times the second congruence of (8) from the first one (remember that $a_j = 2$) yields

$$(q_{j-1} - mq_{j-2})a \equiv n - 1 - 2m \mod (n) \ ,$$

and from (10) and (4) we obtain $n - 1 - 2m \le L$. Inserting these lower bounds for L and l into (5) now yields the contradiction

$$\begin{aligned} n \ge L + \frac{l+1}{2} &> n - 1 - 2m + \frac{1}{2}(n - q_{j-1} + (m-1)q_{j-2}) + \frac{1}{2} = \\ &= n - 1 - 2m + \frac{1}{2}(q_{j-1} + mq_{j-2}) + \frac{1}{2} \ge n - 1 - 2m + \frac{1}{2}(2mq_{j-2} + 1) + \frac{1}{2} = \\ &= n + m(q_{j-2} - 2) \ge n \ , \end{aligned}$$

where we used $q_{j-1} = a_{j-1}q_{j-2} + q_{j-3} \ge mq_{j-2} + 1$ and $q_{j-2} \ge q_2 \ge 2$. □

3. Hamming codes and the proof of Theorem 2

For any prime power q let $\mathbb{F}_q$ denote a finite field with q elements. We use the following terminology. Given a sum $\sum_{i\in I} g_i$ of elements of an abelian group, we call $\sum_{i\in J} g_i$ for some $J \subset I$ a subsum of this sum; we call it a zero-subsum if $\sum_{i\in J} g_i = 0$ and we call it proper (non-trivial, resp.) if $J \neq I$ ($J \neq \emptyset$, resp.). We consider subsums given by distinct sets J, J' as distinct, even if their sums are equal. Moreover, given a subset A of an abelian group, for brevity, we say "subsum of A" instead of "subsum of $\sum_{g\in A} g$".

Proof of Theorem 2.
Suppose to the contrary that $\mathrm{supp}(S)$ contains $p+1$ elements, which by Proposition 2.a) are pairwise independent in $G \simeq \mathbb{F}_p^2$. Now Theorem 4.a) below shows that $\mathrm{supp}(S)$ has a non-trivial zero-subsum, contradicting the minimality of S. $\square$

Theorem 4. *Let $q \in \mathbb{N}$ be a power of an odd prime.*

- **a)** *Let $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_q \in \mathbb{F}_q^2$ be given such that any two of these vectors are linearly independent over $\mathbb{F}_q$. Then there exists a non-trivial zero-subsum of these vectors. Moreover, the number of all non-trivial zero-subsums of $\{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_q\}$ is odd. If furthermore $\sum_{i=0}^{q} \mathbf{v}_i = \mathbf{0}$, then there exists a proper non-trivial zero-subsum.*
- **b)** *Let $\mathcal{C} \subset \mathbb{F}_q^{q+1}$ be a (q-ary) linear Hamming code of order 2. Then there exists an odd number of non-zero codewords $\mathbf{x} \in \mathcal{C}$ whose coordinates are only 0's and 1's. If furthermore $\mathbf{1} = (1, 1, \dots, 1) \in \mathcal{C}$, then there exists a codeword $\mathbf{x} \in \mathcal{C} \setminus \{\mathbf{0}, \mathbf{1}\}$ whose coordinates are only 0's and 1's.*

Proof.
a) For $0 \le i \le q$ let $\mathbf{v}_i = \binom{\alpha_i}{\beta_i} \in \mathbb{F}_q^2$ be given such that each two of these vectors are linearly independent, and put

$$H = \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_q \\ \beta_0 & \beta_1 & \dots & \beta_q \end{pmatrix} \in M_{2,q+1}(\mathbb{F}_q) .$$

Then it is well known that H is the parity check matrix of the Hamming code

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^{q+1} \colon H\mathbf{x} = \binom{0}{0}\} \subset \mathbb{F}_q^{q+1} ,$$

and any linear Hamming code $\mathcal{C}' \subset \mathbb{F}_q^{q+1}$ can be obtained as above by a suitable choice of $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_q \in \mathbb{F}_q^2$ (see e.g. [16, pp. 253f]). It follows that assertions **a)** and **b)** are equivalent, and we will prove the latter one.

b) For any $\mathbf{x} \in \mathbb{F}_q^{q+1}$ let $\omega(\mathbf{x}) \in \{0, \dots, q+1\}$ denote the *weight* of $\mathbf{x}$, i.e. the number of non-zero coordinates of $\mathbf{x}$, and $B(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_q^{q+1} \colon \omega(\mathbf{x}-\mathbf{y}) \le 1\}$ the ball of radius 1 around $\mathbf{x}$, i.e. the set of all vectors $\mathbf{y}$ which differ from $\mathbf{x}$ in at most one coordinate. It is known that $\mathcal{C}$ as given above is a perfect code with minimal distance 3, i.e. the balls of radius 1 around the codewords yield a partition of the whole space:

$$\mathbb{F}_q^{q+1} = \dot{\bigcup_{\mathbf{x}\in\mathcal{C}}} B(\mathbf{x}) .$$

Put $W = \{0,1\}^{q+1} \subset \mathbb{F}_q^{q+1}$ the set of all vectors with coordinates 0 or 1, and partition $\mathcal{C} = \mathcal{C}_0 \mathbin{\dot\cup} \mathcal{C}_1 \mathbin{\dot\cup} \mathcal{C}_2$, where $\mathcal{C}_0$ ($\mathcal{C}_1$, $\mathcal{C}_2$, resp.) denotes the set of those codewords $\mathbf{x} \in \mathcal{C}$ with no (or exactly one, or at least two, resp.) coordinate(s) belonging to $\mathbb{F}_q \setminus \{0,1\}$. It is easy to check that in case $\mathbf{x} \in \mathcal{C}_0$ (or $\mathbf{x} \in \mathcal{C}_1$, or $\mathbf{x} \in \mathcal{C}_2$, resp.) one has

$$|B(\mathbf{x}) \cap W| = q+2 \quad \text{(or } 2, \text{ or } 0, \text{ resp.)},$$

and so we conclude that

$$2^{q+1} = |W| = \sum_{\mathbf{x} \in \mathcal{C}} |B(\mathbf{x}) \cap W| = (q+2)\,|\mathcal{C}_0| + 2\,|\mathcal{C}_1| \ . \tag{11}$$

Since $q+2$ is odd, $|\mathcal{C}_0|$ must be even, and since $\mathbf{0} \in \mathcal{C}_0$, $|\mathcal{C}_0|$ must be positive. Thus $\mathcal{C}_0 \setminus \{\mathbf{0}\}$ is non-empty and has odd cardinality, thus proving the first assertion of part **b)**.

If furthermore $\mathbf{1} \in \mathcal{C}$, one easily checks that the map

$$\begin{aligned} \varphi : \mathcal{C}_1 &\to \mathcal{C}_1 \\ \mathbf{x} &\mapsto \mathbf{1} - \mathbf{x} \end{aligned}$$

is an involution, i.e., $\varphi \circ \varphi = \mathrm{id}$, without fixed points, therefore $\mathcal{C}_1$ is the disjoint union of two-element sets $\{\mathbf{x}, \varphi(\mathbf{x})\}$ and $|\mathcal{C}_1|$ is even. Now from (11) we see that $|\mathcal{C}_0|$ is divisible by 4, and consequently $|\mathcal{C}_0| \geq 4$. □

Remark. With the same proof, Theorem 4 immediately generalizes for pairwise linearly independent $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N \in \mathbb{F}_q^r$ with even $r \geq 2$ and $N = (q^r-1)/(q-1)$, and thus for linear Hamming codes $\mathcal{C} \subset \mathbb{F}_q^N$ of even order r. But notice that only for the case $r = 2$ and $q \in \mathbb{P}$ the number N of given vectors $\mathbf{v}_i$ is less than Davenport's constant of the underlying additive group, so only in this case Theorem 4 gives new mathematical insight.

4. Proof of Theorem 3

Throughout this section we use the notation and assumptions of Theorem 3. Thus, p is an odd prime, $G = C_p \oplus C_p$, and

$$S = \prod_{i=1}^{p} g_i^{\lambda_i} \in \mathcal{F}(G)$$

is a minimal zero-sum sequence of maximal length, i.e., $|S| = \sum_{i=1}^{p} \lambda_i = 2p-1$. Moreover, $\mathrm{supp}(S) = \{g_1, \ldots, g_p\}$ consists of p elements, which are pairwise independent by Proposition 2.a), and

$$p-1 \geq \lambda_1 \geq \cdots \geq \lambda_m > \lambda_{m+1} = \cdots = \lambda_p = 1$$

with some $2 \leq m \leq p-1$. Let $H \subset G$ be the cyclic subgroup of order p that is different from $\langle g_i \rangle$ for each $1 \leq i \leq p$.

Lemma 3. *For each $h \in H \setminus \{0\}$ there exists a subset $I_h \subset \{1, \ldots, p\}$ such that*

$$\sum_{i \in I_h} g_i \ + h = 0 \ .$$

Furthermore, $I_h \cap I_{-h} \cap \{m+1, \ldots, p\} \neq \emptyset$.

Proof.
Let $h \in H \setminus \{0\}$. Since any two elements of the set $\{g_1, \dots, g_p, h\}$ are independent, this set has a non-trivial zero-subsum by Theorem 4.a). Since S is a minimal zero-sum sequence, this subsum has to contain h as a summand, thus proving the existence of I_h.
Put $I'_h = I_h \cap \{m+1, \dots, p\}$ and $I'_{-h} = I_{-h} \cap \{m+1, \dots, p\}$, and suppose that $I'_h \cap I'_{-h} = \emptyset$. We have

$$\sum_{i \in I_h} g_i + \sum_{j \in I_{-h}} g_j = 0 \tag{12}$$

and $T = \prod_{i \in I_h} g_i \prod_{j \in I_{-h}} g_j$ is a zero-sum sequence. Since $I'_h \cap I'_{-h} = \emptyset$, the sequence T is a subsequence of S and the minimality of S implies that indeed $S = T$. If $m \le p-2$, we have $\lambda_1 \ge 3$ and T is a proper subsequence of S, a contradiction. Thus only the case $m = p-1$ remains, which yields $\lambda_1 = \cdots = \lambda_{p-1} = 2$ and $\lambda_p = 1$. Since $S = T$, it follows that $I_h = \{1, \dots, p\}$ and $I_{-h} = \{1, \dots, p-1\}$, or vice versa, so let us assume $I_h = \{1, \dots, p\}$. Then $\sum_{i=1}^{p} g_i + h = 0$ and the second part of Theorem 4.a) shows that this sum has a proper non-trivial zero-subsum; clearly the complement of this zero-subsum is a proper non-trivial zero-subsum as well and only one of the two contains h, a contradiction to the minimality of S. Thus $I'_h \cap I'_{-h} \neq \emptyset$. □

We use the following notation: for $A, B \subset C_p$ and $k \in \mathbb{N}$ let

$$A + B = \{a + b \colon a \in A,\ b \in B\}$$

denote the sumset of the sets A and B, and

$$k^\wedge A = \Big\{ \sum_{a \in A_0} a \ : A_0 \subset A \text{ with } |A_0| = k \Big\}$$

the set of all sums of k different elements of A.
In the following we will make use of two well known results from Additive Number Theory, namely the Cauchy–Davenport Theorem [2, 3] and the Theorem of Dias da Silva–Hamidoune [4] (i.e., the confirmation of the Erdős–Heilbronn Conjecture), as well as of some consequences of these. For the convenience of the reader we recall these results in Proposition 3 below and refer to [14, Theorems 2.2 and 3.4] for a detailed exposition.
Moreover, in Proposition 3.e) we recall a recent result on the structure of sequences in C_p without zero-sum subsequences of length p that we need in the proof of Theorem 3. This question is closely related to the problem of evaluating Brakemeier's function for C_p — in fact, recent results on this function, obtained in [13], were part of our first reasonings towards our result.

Proposition 3. *Let $\emptyset \neq A, B \subset C_p$ and $k \in \mathbb{N}$. Then one has:*

a) (Cauchy–Davenport)

$$|A + B| \ge \min\{p, |A| + |B| - 1\}$$

b) *If $T \in \mathcal{F}(C_p \setminus \{0\})$, then $|\Sigma(T) \setminus \{0\}| \ge \min\{p-1, |T|\}$.*

c) (Dias da Silva–Hamidoune)

$$|k^\wedge A| \ge \min\{p, k(|A| - k) + 1\}$$

d) (cf. [4, Corollary 4.3]) *If $|A| \ge \sqrt{4p-7}$, then A has a non-trivial zero-subsum with at most $(\sqrt{4p-7}+1)/2$ summands.*

e) ([8, Theorem 2.2]) *If $T \in \mathcal{F}(C_p)$ has no zero-sum subsequence of length p, then T contains some element with multiplicity at least $|T| - p + 1$.*

To get Proposition 3.b), write $T = \prod_{i=1}^{k} t_i$ and apply part a) repeatedly to $|\{0, t_1\} + \cdots + \{0, t_k\}|$ and note that $\{0, t_1\} + \cdots + \{0, t_k\} = \Sigma(T) \cup \{0\}$; the definition of $\Sigma(\cdot)$ is given in the Introduction.

Proof of Theorem 3.
a) Let $S_0 = g_1^{\lambda_1 - 1} \dots g_m^{\lambda_m - 1}$, a subsequence of S with $|S_0| = p - 1$, and let

$$\pi : G \to G/H \simeq C_p$$

denote the canonical homomorphism. So $\pi(S_0) = \pi(g_1)^{\lambda_1 - 1} \dots \pi(g_m)^{\lambda_m - 1}$ is a sequence of length $p - 1$ in C_p.

Suppose that $\pi(S_0)$ has a non-trivial zero-sum subsequence. Then there are $0 \le \mu_i \le \lambda_i - 1$, not all vanishing, such that $\sum_{i=1}^{m} \mu_i g_i = h \in H$. The minimality of S implies that $h \ne 0$. Using Lemma 3, we get

$$\sum_{i \in I_h} g_i + \sum_{i=1}^{m} \mu_i g_i = 0$$

for a suitable $I_h \subset \{1, \dots, p\}$. The remaining arguments are similar to the ones in the proof of Lemma 3: the minimality of S implies $\mu_i = \lambda_i - 1$ for all $1 \le i \le m$ and $I_h = \{1, \dots, p\}$; so $\sum_{i=1}^{p} g_i + h = 0$, and again applying the second part of Theorem 4.a) we get a contradiction.
Therefore $\pi(S_0)$ has no non-trivial zero-sum subsequence, which implies $\pi(S_0) = \pi(g_1)^{p-1}$, and part **a)** of the theorem follows.

b) Let $S_1 = g_1^{\lambda_1} \dots g_m^{\lambda_m}$ be the subsequence of S of those elements with multiplicity at least 2, and let

$$\pi_0 : G = \langle g_1 \rangle \oplus H \to H \simeq C_p$$

denote the projection onto the subgroup H along $\langle g_1 \rangle$. Using part **a)** we have $g_k = g_1 + h_k$, where $h_2, \dots, h_m \in H \setminus \{0\}$ are pairwise different. Thus, any zero-sum subsequence of length p of the sequence

$$S' = \pi_0(S_1) = 0^{\lambda_1} h_2^{\lambda_2} \dots h_m^{\lambda_m} \in \mathcal{F}(C_p)$$

would give a proper zero-sum subsequence of S, contradicting the minimality of S. In order to obtain the claimed inequality for m, it suffices to prove the following:

Assertion 1: If $m > \sqrt{2p - 2}$, then S' has a zero-sum subsequence of length p.
Let $A = \mathrm{supp}(S') \subset C_p$, and put $m_1 = m_2 = \frac{m-1}{2}$ if m is odd, and $m_1 = \frac{m}{2} - 1$ and $m_2 = \frac{m}{2}$ if m is even. Then we have by Proposition 3.c)

$$|m_1^\wedge A| \ge \min\{p, m_1(|A| - m_1) + 1\} = \min\{p, m_1 m_2 + m_1 + 1\},$$

and similarly $|m_2^\wedge A| \ge \min\{p, m_2 m_1 + m_2 + 1\}$. Since, assuming $m > \sqrt{2p - 2}$, we have

$$|m_1^\wedge A| + |m_2^\wedge A| \ge 2 m_1 m_2 + m_1 + m_2 + 2 = 2(m_1 + 1/2)(m_2 + 1/2) + 3/2 > p,$$

it follows (cf. Proposition 3.a)) that $m_1^\wedge A + m_2^\wedge A = C_p$. Consequently, we can find a subsequence $T \mid S'$ with $\sigma(T) = \sigma(S')$ and $|T| = m_1 + m_2 = m - 1$. Since $|S'| = p + m - 1$, the sequence T' satisfying $TT' = S'$ is a zero-sum subsequence of S' with length p, which proves Assertion 1.

c) From $\lambda_1 + \cdots + \lambda_m = p + m - 1$ we obtain $\lambda_1 \ge \frac{p-1}{m} + 1$. Moreover, the sequence S', considered in **b)**, contains no zero-sum subsequence of length p, so we may apply Proposition 3.e) to obtain $\lambda_1 \ge m$. Combining these inequalities, we have

$$\lambda_1 \ge \max\Big\{\frac{p-1}{m} + 1, m\Big\} \ge \frac{1+\sqrt{4p-3}}{2},$$

the lower bound for λ_1.

Now, put $r = p - \lambda_1$ and suppose that $r \ge 2$. We have to show that $r > \sqrt[4]{p}$, and first prove the following:

Assertion 2: For every $h \in H \setminus \{0\}$ we have $|\pi_0^{-1}(h) \cap \operatorname{supp}(S)| < r$.

Assume to the contrary that there exists some $h \in H\setminus\{0\}$ with $|\pi_0^{-1}(h) \cap \operatorname{supp}(S)| \ge r$. Let $D \mid S$ be a squarefree (i.e. each element has multiplicity 1) subsequence of S with length r such that $\pi_0(D) = h^r$ and put $S = g_1^{\lambda_1} D D'$. Since $|D'| = p-1$ and $\operatorname{supp}(\pi_0(D')) \subset H\setminus\{0\}$, Proposition 3.b) shows that $H\setminus\{0\} \subset \Sigma(\pi_0(D'))$. In particular, there exists a subsequence $T \mid D'$ such that $\sigma(\pi_0(T)) = -h$. Therefore

$$\big\{\sigma(gT)\colon g \mid D\big\} \subset \langle g_1 \rangle \setminus \{0\}$$

is a set of cardinality r, and we can find some $g' \mid D$ such that $\sigma(g'T) = j g_1$ with some $r \le j \le p-1$. But then the sequence $g' T g_1^{p-j}$ is a proper zero-sum subsequence of S, a contradiction proving Assertion 2.

So we know that $|\pi_0^{-1}(h) \cap \operatorname{supp}(S)| < r$ for every $h \in H\setminus\{0\}$. Since by Proposition 2.a) $\pi_0^{-1}(0) \cap \operatorname{supp}(S) = \{g_1\}$, and since $|\operatorname{supp}(S)| = p$, it follows that

$$|\operatorname{supp}(\pi_0(S)) \setminus \{0\}| \ge \frac{p-1}{r-1}\ . \tag{13}$$

Assertion 3: If $r \le \sqrt[4]{p}$, then for $1 \le i \le r$ there exist non-empty sequences $U_i \in \mathcal{F}(G)$ with $\sigma(\pi_0(U_i)) = 0$, such that $\prod_{i=1}^r U_i$ is a proper subsequence of $\prod_{i=2}^p g_i^{\lambda_i}$.

By Proposition 3.d), any set of at least $\sqrt{4p-7}$ elements of $\operatorname{supp}(\pi_0(S))$ has a zero-subsum with at most $(\sqrt{4p-7}+1)/2$ summands. Consequently, providing that

$$|\operatorname{supp}(\pi_0(S)) \setminus \{0\}| - (r-1)\frac{\sqrt{4p-7}+1}{2} \ge \sqrt{4p-7}\ ,$$

we get r pairwise disjoint zero-subsums of $\operatorname{supp}(\pi_0(S)) \setminus \{0\}$. To each of these zero-subsums corresponds a (squarefree) subsequence U_i of $\prod_{i=2}^p g_i^{\lambda_i}$ such that $\sigma(\pi_0(U_i)) = 0$. Since the zero-subsums are disjoint, indeed $\prod_{i=1}^r \pi_0(U_i) \mid \prod_{i=2}^p \pi_0(g_i)$. Using (13), the above inequality holds if

$$0 \ge r^2(1+\sqrt{4p-7}) - 2r - 2p - \sqrt{4p-7} + 3\ ,$$

and the latter one is satisfied for $r \le \sqrt[4]{p}$. Finally, since $\lambda_2 \ge 2$, the product of the r sequences U_i is a proper subsequence of $\prod_{i=2}^p g_i^{\lambda_i}$, which proves Assertion 3.

Now assume that $r \le \sqrt[4]{p}$ and let U_i be given according to Assertion 3. Since S is minimal, we obtain $\sigma(U_i) = k_i g_1$ with some $1 \le k_i \le p-1$. But now Proposition 3.b) yields $|\Sigma(\prod_{i=1}^r (k_i g_1))| \ge r$, and we obtain a subset $\emptyset \ne I \subset \{1, \ldots, r\}$ with $\sigma(\prod_{i \in I} U_i) = k g_1$ for some $r \le k \le p$. Therefore the sequence $g_1^{p-k} \prod_{i \in I} U_i$ is a proper zero-sum subsequence of S, again a contradiction. $\square$

References

[1] Y. Caro, Zero-sum problems – A survey, *Discrete Math.* **152** (1996), 93-113, doi:10.1016/0012-365X(94)00308-6

[2] A. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813), 99–123.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[4] J.A. Dias da Silva and Y. ould Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146.

[5] W.D. Gao and A. Geroldinger, On long minimal zero sequences in finite abelian groups, *Period. Math. Hungar.* **38** (1999), 179-211.

[6] W.D. Gao and A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, *Integers* **3** (2003), Paper A08, 45pp; http://www.integers-ejcnt.org/d8/d8.pdf.

[7] W.D. Gao and A. Geroldinger, Zero-sum problems and coverings by proper cosets, *European J. Combin.* **24** (2003), 531-549, doi:10.1016/S0195-6698(03)00033-7

[8] W.D. Gao, A. Panigrahi, and R. Thangadurai, On the structure of p-zero-sum free sequences and its application to a variant of Erdős-Ginzburg-Ziv theorem, *Proc. Indian Acad. Sci. (Math. Sci.)* **115** (2005), 67-77.

[9] W.D. Gao and J.J. Zhuang, Sequences not containing long zero-sum subsequences, *European J. Combin.*, to appear, doi:10.1016/j.ejc.2005.06.001

[10] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory, Monographs and Textbooks in Pure and Applied Mathematics 278, Chapman & Hall/CRC, Boca Raton*, FL, USA, 2005.

[11] Y. ould Hamidoune, Subsequence Sums, *Combin. Probab. Comput.* **12** (2003), 413-425.

[12] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers, Fifth Edition, The Clarendon Press, Oxford University Press, New York*, NY, USA, 1979.

[13] F. Hennecart, La fonction de Brakemeier dans le problème d'Erdős-Ginzburg-Ziv, *Acta Arith.* **117** (2005), 35-50.

[14] M.B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics 165, Springer-Verlag New York*, NY, USA, 1996.

[15] J.E. Olson, A Combinatorial Problem on Finite Abelian Groups, II, *J. Number Th.* **1** (1969), 195-199, doi:10.1016/0022-314X(69)90037-7

[16] S. Roman, *Coding and Information Theory, Graduate Texts in Mathematics 134, Springer-Verlag New York*, NY, USA, 1992.

Institut für Mathematik und wissenschaftliches Rechnen, Karl-Franzens-Universität, Heinrichstrasse 36, A-8010 Graz, AUSTRIA

E-mail address: `guenter.lettl@uni-graz.at`

E-mail address: `wolfgang.schmid@uni-graz.at`