Sequences in Abelian Groups G of Odd Order without Zero-Sum Subsequences of Length $exp(G)$

Yves Edel*

Abstract

We present a new construction for sequences in the finite abelian group C_n^r without zero-sum subsequences of length n, for odd n. This construction improves the maximal known cardinality of such sequences for $r > 4$ and leads to simpler examples for $r > 2$. Moreover we explore a link to ternary affine caps and prove that the size of the second largest complete caps in $AG(5, 3)$ is 42.

Keywords zero-sum sequences, finite abelian groups, affine caps.

AMS classification[2000] 11B50, 20K01, 51E22

1 Introduction and Main Results

Let G be a finite abelian group, written additively. If $|G| > 1$, then there are uniquely determined integers $r, n_1, \ldots, n_r$ with $1 < n_1 \mid \ldots \mid n_r$ such that $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$. Then $r = \mathsf{r}(G)$ is the *rank* of G, and $n_r = \exp(G)$ is the *exponent* of G.

We denote by $\mathcal{F}(G)$ the free (multiplicative) monoid with basis G. An element $S \in \mathcal{F}(G)$ is called a *sequence over* G, written as

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G)\,,$$

where $\mathsf{v}_g(S)$ is called the *multiplicity of* g *in* S.

A sequence $S' \in \mathcal{F}(G)$ is called a *subsequence* of S if $\mathsf{v}_g(S') \le \mathsf{v}_g(S)$ for every $g \in G$. Equivalently $S' \mid S$. The product of two sequences R and S is $RS := \prod_{g \in G} g^{\mathsf{v}_g(R)+v_g(S)}$.

*Mathematisches Institut der Universität, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany, http://www.mathi.uni-heidelberg.de/∼yves, y.edel@mathi.uni-heidelberg.de

$$\sigma(S) = \sum_{g\in G} \mathsf{v}_g(S)g \in G \quad \text{denotes the } \textit{sum of } S.$$

$$|S| = \sum_{g\in G} \mathsf{v}_g(S) \in \mathbb{N}_0 \quad \text{denotes the } \textit{length} \text{ of } S.$$

We say that the sequence S is a *zero-sum sequence* if $\sigma(S) = 0$ and call a sequence *square free* if $\mathsf{v}_g(S) \le 1$ for all $g \in G$.

While problems in this area of additive number theory are usually stated in terms of sequences these equivalently can be viewed as multisets of group elements. The multiplication of sequences then translates to the union of multisets.

If we choose G as the homocyclic group $G = C_n^r$, C_n being the cyclic group of order n, then viewing the sequences as codes or, for prime n, as multisets of points in the affine space $AG(r, n)$ can be fruitful as we will see in Section 4.

Some central invariants in zero-sum theory are

- $\mathsf{s}(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence S of length l over G has a zero-sum subsequence T of length $|T| = n$,
- $\eta(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence S of length l over G has a zero-sum subsequence T of length $|T| \in [1, n]$,
- $\mathsf{g}(G)$ the smallest integer $l \in \mathbb{N}$ such that every square free sequence S of length l over G has a zero-sum subsequence T of length $|T| = n$.

For finite abelian groups of rank at most two, the invariants $\eta(G)$ and $\mathsf{s}(G)$ are completely determined.

Theorem A. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$. Then*

$$\eta(G) = 2n_1 + n_2 - 2 \quad \textit{and} \quad \mathsf{s}(G) = 2n_1 + 2n_2 - 3\,.$$

A proof of Theorem A was recently given in [12, Theorem 5.8.2]. It is based on a result by C. Reiher which states that $\mathsf{s}(C_p \oplus C_p) = 4p - 3$ for all prime p (see [18]). Note that Theorem A contains the Theorem of Erdös-Ginzburg-Ziv as the special case $n_1 = 1$.

Apart from this result only some sporadic exact results are known. These results mostly are for homocyclic groups $G = C_n^r$. From now on we only consider the case $G = C_n^r$, of rank r larger than two, and we start with the

discussion of lower bounds. We only formulate bounds for $\mathsf{s}(C_n^r)$. Bounds for $\eta(C_n^r)$ and $\mathsf{g}(C_n^r)$ follow from Lemma 4.

Theorem B. *Let $n \in \mathbb{N}_{\ge 2}$ and $r \in \mathbb{N}$.*

1. *The sequence S over C_n^r of all different* 0-1 *tuples has the property that S^{n-1} has no zero-sum subsequence of length n. In particular, we have $\mathsf{s}(C_n^r) \ge 2^r(n-1)+1$.*

2. *If n is odd, then there exists a sequence S over C_n^3 of length $|S| = 9$ such that S^{n-1} has no zero-sum subsequence of length n. In particular, we have $\mathsf{s}(C_n^3) \ge 9(n-1)+1$.*

3. *If n is odd, then there exists a sequence S over $C_n^4$of length $|S| = 20$ such that S^{n-1} has no zero-sum subsequence of length n. In particular, we have $\mathsf{s}(C_n^4) \ge 20(n-1)+1$.*

The first result is due to H. Harborth (see [13, Hilfssatz 1] or Proposition 10). The bound is known to be sharp if n is a power of two. The second result is due to C. Elsholtz [8], the third can be found in [7]. For larger r the best known bounds were obtained from these by a simple product construction, see Lemma 6. E.g. for odd n it was known that $\mathsf{s}(C_n^5) \ge 40(n-1)+1$, $\mathsf{s}(C_n^6) \ge 81(n-1)+1$, $\mathsf{s}(C_n^7) \ge 180(n-1)+1$, ...

In [11] W. Gao and R. Thangadurai conjecture that the lower bounds given in Theorem B.2 are the precise values, that is

$$\eta(C_n^3) = 8(n-1)+1 \quad \text{and} \quad \mathsf{s}(C_n^3) = 9(n-1)+1 \quad \text{for all odd} \quad n \in \mathbb{N}_{\ge 3}$$

In [10, Theorem 1.7] the conjecture has been confirmed for $n = 3^a 5^b$. Theorem 1.8 of the same paper states $\mathsf{s}(C_n^3) = \eta(C_n^3) + n - 1 = 8(n-1)+1$ for $n = 2^a 3$.

For an overview on the history of zero-sum sequences, further relations and references see [12, Section 5.7] and the recent survey [7]. We restrict ourself here to introduce what is necessary to understand the presented results.

The constructions of Theorem B can be seen as the construction of a sequence S in $\mathbb{Z}^r$ (r=2,3,4), such that S^{n-1} modulo n has the desired properties. It is clear that the result of Harborth can not be improved using an alphabet with only two entries, i.e. using sequences over $\{a,b\}^r \subset \mathbb{Z}^r$. The constructions mentioned in Theorem B.2 and B.3 are based on sequences over $\{0,1,2,3\}^r \subset \mathbb{Z}^r$.

The recursive construction presented in Section 3 of the present paper is based on sequences over $\{0,1,2\}^r \subset \mathbb{Z}^r$. For odd n we obtain sequences with the best known lengths for $r = 3, 4$ and for larger r we improve the lower bounds on $\mathsf{s}(C_n^r)$. The following will be shown:

Theorem 1. *For every odd natural number $n \geq 3$ there exist sequences*

$$S \in \mathcal{F}(C_n^5), |S| = 42, \quad S \in \mathcal{F}(C_n^6), |S| = 96, \quad S \in \mathcal{F}(C_n^7), |S| = 196.$$

such that S^{n-1} has no zero-sum subsequence of length n. In particular, we have

$$\mathsf{s}(C_n^5) \geq 42(n-1)+1, \quad \mathsf{s}(C_n^6) \geq 96(n-1)+1, \quad \mathsf{s}(C_n^7) \geq 196(n-1)+1.$$

For other values of r, improvements on the bound on $\mathsf{s}(C_n^r)$ can be achieved by applying the product construction, Lemma 6, with sequences of Theorem B and Theorem 1.

An *s-cap* in the affine space $AG(r,q)$ of dimension r over the finite field of order q is a set of s points, no three of which are collinear. A sequence S over C_3^r without a zero-sum subsequence T of length $|T| = 3$ is equivalent to a cap in $AG(r,3)$ (see Lemma 20).

This creates a link from zero-sum theory to the highly developed theory of affine caps. It has some interesting consequences. The length of sequences of the above type, e.g. sequences S in $\mathbb{Z}^r$, such that S^{n-1} modulo n has no zero-sum subsequence of length n for all odd n, is bounded by the maximal size of a cap in $AG(r,3)$. We reach this upper bound for $r = 1, 2, 3, 4$.

For $AG(5,3)$ it is known that the largest cap has size 45 [6]. The 42-cap obtained from the sequence here is complete, i.e. there are no points in $AG(5,3)$ that can be added to this cap , so that the extension is still a cap. In Section 4 we will prove

Theorem 2. *The size of the second largest complete caps in $AG(5,3)$ is 42.*

Hence if it is possible to find larger sequences over C_n^5 for all odd n, the restriction mod 3 will be contained in the uniquely determined 45-cap.

Also for larger r we note that better ternary affine caps are known (see e.g. [2, 7, 15]). On the other hand, again, the caps resulting from the sequences for $r = 6, 7$ are complete in $AG(r,3)$. So longer sequences can not be obtained by adding more elements to these sequences. This leaves us with the interesting question if longer sequences, for all odd n, can be found. Another open problem is to prove or disprove the statement that the extremal size of such sequences is already completely determined by the maximal size of an affine ternary cap, as it is the case for $r \leq 4$.

2 Notation and Basic Tools

In all constructed sequences, without zero-sum subsequence over $G = C_n^r$, every element will appear with frequency $n-1$. This motivates the following definition:

Definition 3. *We say a sequence $S \in \mathcal{F}(G)$ has Property D', if*

- *S has no zero-sum subsequence of length $n = \exp(G)$ and*
- *S can be written in the form $S = R^{n-1}$.*

Denote by $\mathsf{m}(G)$ the largest integer $l \in \mathbb{N}$ such that there exists a sequence $S = R^{n-1}$, $|R| = l$, with Property D'.

Lemma 4 establishes lower bounds on $\eta(G)$ and $\mathsf{g}(G)$.

Lemma 4. *Let G be a finite abelian group with $\exp(G) = n \geq 2$.*

1. $\mathsf{s}(G) \geq \mathsf{m}(G)(n-1) + 1$.
2. *Let $S \in \mathcal{F}(G)$ be a sequence which has no zero-sum subsequence of length n and suppose that $\max\{\mathsf{v}_g(S) \mid g \in G\} = n - 1$. Then $\eta(G) \geq |S| - n + 1$. In particular, if $|S| = \mathsf{s}(G) - 1$, then $\eta(G) = \mathsf{s}(G) - n + 1$.*
3. *Let $S \in \mathcal{F}(G)$ be a sequence which has no zero-sum subsequence of length n. Let H be a group with $|H| \geq \exp(G) - 1$ and $f : \{1, \ldots, n-1\} \mapsto H$ be an injective mapping. Then*

$$\prod_{g \in G} \prod_{i=1}^{v_g(S)} (f(i), g) \in \mathcal{F}(H \oplus G)$$

is a square free sequence which has no zero-sum subsequence of length n. In particular $\mathsf{g}(C_n^{r+1}) \geq \mathsf{s}(C_n^r)$.

Proof. 1.: is a direct consequence of Definition 3. For 2. and 3. see [7, Lemma 2.3]. □

Definition 5. *For groups G, H and sequences $S \in \mathcal{F}(G)$, $R \in \mathcal{F}(H)$ we define the sequence $S \oplus R \in \mathcal{F}(G \oplus H)$ as*

$$S \oplus R = \prod_{g \in G} \prod_{h \in H} (g, h)^{v_g(S) v_h(R)}$$

With this notation we can state the well known product construction (see. e.g. [7, Proposition 4.1]) as

Lemma 6 (The Product Construction)**.** *For G, H with $n = exp(G) = exp(H)$ and sequences $S \in \mathcal{F}(G)$ without a zero-sum subsequence of length n and $S' = R'^{n-1} \in \mathcal{F}(H)$ with Property D' the sequence*

$$P = S \oplus R' \in \mathcal{F}(G \oplus H)$$

has no zero-sum subsequence of length n.

If also S has Property D', then the sequence P has Property D'.

Corollary 7. *For G, H with $exp(G) = exp(H)$ we have*
$\mathsf{s}(G \oplus H) - 1 \geq (\mathsf{s}(G) - 1)m(H)$ *and* $m(G \oplus H) \geq m(G)m(H)$.

A slightly more general product construction will be useful later. It is proved just with the same argument as the ordinary Product Construction.

Lemma 8 (A More General Product Construction)**.** *Let G, H be groups with $n = exp(G) = exp(H)$ and $S_i \in \mathcal{F}(G)$, $1 \leq i \leq l$, be sequences without a zero-sum subsequence of length n. Moreover let $S' = R'^{n-1} \in \mathcal{F}(H)$ be a sequence with Property D'. For some partition R'_i of R' in l subsequences the sequence*

$$P = \prod_{i=1}^{l} (S_i \oplus R'_i) \in \mathcal{F}(G \oplus H)$$

has no zero-sum subsequence of length n.

If also the S_i, $1 \leq i \leq l$ have Property D', then P has Property D'.

Lemma 6 is a special case of Lemma 8 when $S_i = S$ for all i.

Definition 9. *Let R be a sequence in $\mathbb{Z}^r$, and $n \in \mathbb{N}$. Denote by R_n the sequence in $\mathcal{F}(C_n^r) = \mathcal{F}((\mathbb{Z}/(n\mathbb{Z}))^r)$ obtained from R by componentwise reduction* $(\mathrm{mod}\ n)$.

For a fixed representation of $\mathbb{Z}^r$ as $\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ define for an element $g = (g_1, \ldots, g_r) \in \mathbb{Z}^r$ the weight of g as $wt(g) = \sum_{i=1}^{r} g_i \in \mathbb{Z}$.

In some of the following arguments we jump between the global object, a sequence S over $\mathbb{Z}^r$ and the corresponding local object, the sequence S_n. The level and especially the arithmetic that has to be used will sometimes only be indicated by the absence or presence of the subscript $_n$.

3 The Construction

As already announced we want to construct sequence S over $\{0, 1, 2\}^r \subset \mathbb{Z}^r$, such that for all odd n, S_n^{n-1} has no zero-sum subsequence of length n, hence has Property D' .

3.1 Preparatory Section

Here we collect some notation, properties and arguments for future use. Some are quite trivial.

Proposition 10 (a la Harborth)**.** *Let R be a square free sequence of $\{0, a\}^r$. If $(a, n) = 1$ then R_n^{n-1} has property D'.*

Proof. Let T be a subsequence of length n, such that T_n is a zero sum subsequence. So only 0 or an are possible values in a coordinate of $\sigma(T)$ (as $(a, n) = 1$). Hence all n elements of T are identical, contradiction. □

Lemma 11. *Let R be a sequence over $\{0,1,2\} \subset \mathbb{Z}$. The only possible zero sum subsequences, T_n, of length n of R_n, $n \geq 3 \in \mathbb{N}$ odd, are:*

$$1.)\ 0^n \quad 2.)\ 2^n \quad 3.)\ 0^a 2^a 1^{n-2a}, \quad 0 \leq a < n/2$$

Proof. Let T be a subsequence of length n, such that T_n is a zero sum subsequence. So the only possible values for $\sigma(T)$ are 0, n or $2n$. Sum 0 is only possible if all summands are zero. Sum $2n$ occurs iff all summands are 2. Sum n: as n is odd, there have to be an odd number of 1 in the sum. If we have $n = a \cdot 2 + b \cdot 1$, so $b = n - 2a$. The number of zeros is $n - a - b = n - a - (n - 2a) = a$. □

The crucial argument in the construction (Theorem 16) will be that a zero sum subsequence would lead to a contradiction modulo two. The following definition and lemma will be the essence of this argument.

Definition 12 (Property P1)**.** *Let R be a sequence in $\mathbb{Z}^r$. We say a zero sum subsequence, T_n, of R_n^{n-1} of length n, for odd n, has property P1 (with respect to n), if we have that $wt(\sigma(T)) \equiv r \pmod 2$, where r is the rank of $\mathbb{Z}^r$.*

We say that the sequence R_n has property P1 if every zero sum subsequence, T_n, of length n of R_n^{n-1} has property P1.

Lemma 13. *Let R be a sequence in $\mathbb{Z}^r$, with $wt(g) \equiv 1 + r \pmod 2$ for all $g \in R$. Then, for every $n \geq 3 \in \mathbb{N}$ odd,* **no** *zero sum subsequence, of length n, of R_n^{n-1} has property P1.*

Proof. Let T_n be a zero sum subsequence, of length n, of R_n^{n-1}. As $n = |T|$ is odd, we have that $wt(\sigma(T)) \equiv 1 + r \pmod 2$.

If T has property P1 then $wt(\sigma(T)) \equiv r \pmod 2$, contradiction. □

The construction (Theorem 16) will need as input pairs of sequences with certain properties we define now. Moreover the following lemma helps to construct such pairs of sequences.

Definition 14 (Property P2 and P3)**.** *A pair of sequences (A, B), both over $\mathbb{Z}^r$, is said to have property P2 (with respect to n), if for $n \geq 3 \in \mathbb{N}$ odd we have*

- *the sequence $(AB)_n$ has property P1.*
- *A_n^{n-1} as well as B_n^{n-1} have property D'*

A pair (A, B) with property P2 is said to have property P3 if

- *$wt(a) \equiv r \pmod 2$ for all $a \in A$*
- *$wt(b) \equiv r + 1 \pmod 2$ for all $b \in B$*

Lemma 15. *If the pair of sequences (A, B), both over $\mathbb{Z}^r$, has property P3 than there exists a pair of sequences $(\bar{A}, \bar{B})$ over $\mathbb{Z}^{r+1}$ which has property P3 with $|\bar{A}| = |\bar{B}| = |A| + |B|$.*

Proof. If the pair (A, B), over $\mathbb{Z}^r$, has property P3, choose $\bar{A} = (A \oplus 1)(B \oplus 0)$ over $\mathbb{Z}^{r+1}$ and $\bar{B} = (A \oplus 2)(B \oplus 1)$ over $\mathbb{Z}^{r+1}$. We claim $(\bar{A}, \bar{B})$ has property P3.

Observe that for odd n the sequences $(0 \cdot 1)_n^{n-1}$, $(2 \cdot 1)_n^{n-1}$ and $(0 \cdot 2)_n^{n-1}$ have property D'. Property D' of the sequences $\bar{A}$ respectively $\bar{B}$ holds due to the product construction, Lemma 8.

We want to prove that $(\bar{A}\bar{B})_n$ has property P1. Assume there is a zero-sum subsequence T_n in $(\bar{A}\bar{B})_n^{n-1}$ not having property P1, e.g. the weight of $\sigma(T) \equiv r \pmod 2$.

As $(AB)_n$ has property P1 the sum of the projection to the first r coordinates of T_n has weight $\equiv r \pmod 2$. So we would have to have an even number of ones in the newly added coordinate $r + 1$. Lemma 11 yields that T_n is a subsequence of either $(B \oplus 0)_n^{n-1}$ or $(A \oplus 2)_n^{n-1}$ but these sequences contain no zero-sum subsequence of length n, contradiction.

The factors have been composed such that the weight condition, $wt(\bar{A}) \equiv r + 1 \pmod 2$ and $wt(\bar{B}) \equiv r \pmod 2$, are fulfilled. □

3.2 The Construction

If we have pairs of sequences which have property P3 it is very easy to construct sequences with property D'.

Theorem 16. *Let the pairs (A, B) over $\mathbb{Z}^r$ and (C, D) over $\mathbb{Z}^s$ have property P3. Let S be*

$$S = (A \oplus D)(B \oplus C) \text{ over } \mathbb{Z}^{r+s}$$

Then S_n^{n-1}, $n \geq 3 \in \mathbb{N}$ odd, has property D'. Hence

$$m(C_n^{r+s}) \geq |S| = |A||D| + |B||C|.$$

Proof. All elements of S have weight $\equiv r + 1 \pmod 2$ by construction. By Lemma 13 **no** zero sum subsequence, of length n, of $(S_n)^{n-1}$ has property P1.

On the other hand, A_n and B_n are disjoint (the elements have different weight modulo 2). Hence if there is a zero-sum subsequence whose projection to the first component consists of one element with multiplicity n, the zero-sum subsequence is a subsequence either of $(A \oplus D)_n^{n-1}$ or $(B \oplus C)_n^{n-1}$, both have property D' by Lemma 6, contradiction. By symmetry we also have that in the projection of the zero-sum subsequence to the second component every element has multiplicity less than n. With this information, as both $(AB)_n$ and $(CD)_n$ have property P1, we see that S_n has property P1.

If S_n^{n-1} would have a zero sum subsequence of length n, this would be a contradiction. □

The harder part, of course, is to construct good pairs of sequences which have property P3. Now we will give a direct construction for pairs with property P3. We will use it only for $r = 3$. But as the proof does not get simpler for this special case, we prove it in general.

Definition 17 $(\mathcal{A}, \mathcal{B})$**.** *Fix an even integer $0 < m \leq r$ Define $\mathcal{A}(r)$ over $\{0,1,2\}^r \subset \mathbb{Z}^r$ as the sequence of all points with m zeros and $r-m$ ones together with all points with m twos and $r-m$ ones. Hence $|\mathcal{A}(r)| = 2\binom{r}{m}$. As we usually want $|\mathcal{A}(r)|$ as large as possible, we choose m as close to $r/2$ as possible.*

Define $\mathcal{B}(r)$ over $\{0,1,2\}^r \subset \mathbb{Z}^r$ as the product over all odd $s \leq r$ of: the sequences of all points with s zeros and $r-s$ ones together with all points with s twos and $r-s$ ones. Hence $|\mathcal{B}(r)| = 2^r$.

Lemma 18. *The pair $(\mathcal{A}(r), \mathcal{B}(r))$ has property P3 for* **all** *odd $n \geq 3 \in \mathbb{N}$.*

Proof. The weight conditions are fulfilled.

We see that $\mathcal{A}(r)$ and $\mathcal{B}(r)$ admit the following symmetries:
(1) the permutation of the entry 0 and 2,
(2) an arbitrary permutation of the coordinates.

$\mathcal{B}(r)_n^{n-1}$ has property D': Assume there is a zero sum subsequence T_n. As every element of $\mathcal{B}(r)$ has weight $\equiv 1 + r \pmod 2$ and n is odd we have that $wt(\sigma(T)) \equiv 1 + r \pmod 2$, hence not all coordinates can sum up to n. So there has to be one coordinate that sums up to 0 or $2n$. Due to the symmetries we can assume the sum is zero in this coordinate. By definition the participating points are in $\{0,1\}^r$ and different. Proposition 10 yields a contradiction.

$\mathcal{A}(r)_n^{n-1}$ has property D': if there is a coordinate that sums up to 0 or $2n$ we get a contradiction by the same argument. So we can assume that all coordinates of the zero sum subsequence sum up to n.

Let $\mathcal{A}_0(r)$ consist of the elements of $\mathcal{A}(r)$ containing an entry 0 and $\mathcal{A}_2(r)$ of those containing an entry 2. Analogous notation is used for $\mathcal{B}(r)$.

Let T_n be a zero sum subsequence of length n in $\mathcal{A}(r)_n^{n-1}$. As n is odd and by symmetry it can be assumed that T has an odd number of elements in $\mathcal{A}_0(r)$. The total number of entries 0, taken over all coordinates, is an odd number times m and the total number of entries 2 is an even number times m. In particular those numbers are different, contradicting Lemma 11.

It remains to prove property P1: Let T_n be a zero sum subsequence of length n in $(\mathcal{A}(r)\mathcal{B}(r))_n^{n-1}$. We will prove that every coordinate of $\sigma(T)$ equals n. Clearly this implies Property P1.

So, by symmetry, assume that the first coordinate of $\sigma(T)$ equals 0. We then have that the zero sum subsequence is in $(\mathcal{A}_0(r)\mathcal{B}_0(r))_n^{n-1}$, contradicting Proposition 10. □

Lemma 19. *The following pairs of sequences $(A(r), B(r))$ over $\mathbb{Z}^r$ have property P3 for* **all** *odd $n \geq 3 \in \mathbb{N}$:*

$$A(1) = 1, \quad B(1) = 0 \cdot 2 \text{ over } \mathbb{Z}$$

$$A(2) = \binom{0}{0} \cdot \binom{1}{1} \cdot \binom{2}{0}, \quad B(2) = \binom{0}{1} \cdot \binom{1}{2} \cdot \binom{2}{1} \text{ over } \mathbb{Z}^2$$

Moreover there are pairs
$A(3), B(3)$ *over* $\mathbb{Z}^3$ *with* $|A(3)| = 6$ *and* $|B(3)| = 8$,
$A(4), B(4)$ *over* $\mathbb{Z}^4$ *with* $|A(4)| = 14$ *and* $|B(4)| = 14$.

Proof. For $r = 1$ the verification is trivial, for $r = 2$ apply Lemma 15. In case $r = 3$ this follows of Lemma 18, case $r = 4$ is implied by Lemma 15. □

Applying Theorem 16 with the pairs $(A(i), B(i))$, $(A(j), B(j))$ having property P3 given in Lemma 19 gives us the desired sequences for all odd n. We obtain sequences which reproduce the largest known sequences for $r = 2, 3, 4$. Consequently we have

$$m(C_n^2) \geq 4, \quad m(C_n^3) \geq 9, \quad m(C_n^4) \geq 20.$$

In case $r = 2$, by choosing $(i, j) = (1, 1)$, we obtain a sequence of length $4 = 1 \cdot 2 + 2 \cdot 1$. In case $r = 3$, by choosing $(i, j) = (1, 2)$, we obtain a sequence of length $9 = 1 \cdot 3 + 2 \cdot 3$. And in case $r = 4$, by choosing $(i, j) = (1, 3)$, we obtain a sequence of length $20 = 1 \cdot 8 + 2 \cdot 6$.

The application with $(i, j) = (2, 3)$ yields a sequence of length $42 = 3 \cdot 6 + 3 \cdot 8$ for $r = 5$. The application with $(i, j) = (3, 3)$ yields a sequence of length $96 = 6 \cdot 8 + 8 \cdot 6$ for $r = 6$. And the application with $(i, j) = (4, 3)$ yields a sequence of length $196 = 14 \cdot 6 + 14 \cdot 8$ for $r = 7$. Consequently we have

$$m(C_n^5) \geq 42, \quad m(C_n^6) \geq 96, \quad m(C_n^7) \geq 196,$$

which proves Theorem 1.

Rackham found the same bound for rank 5 independently [9].

4 Sequences over C_n^r and Ternary Affine Caps

A relation between sequences over $\{0, 1, 2\}$ of length 3 and ternary affine caps is not new, e.g. the widely known results of Calderbank and Fishburn [4] and of Meshulam [16] on affine ternary caps were formulated in the language of sequences. Also in the more general case there is some straightforward

relation between sequences over C_p^r and sets in $AG(r,p)$. Define $\mathrm{supp}(S) := \{g \in C_p^r \mid \mathsf{v}_g(S) > 0\} \subset C_p^r$ the *support* of the sequence S. For prime p

- we have C_p the additive group of $\mathbb{F}_p$,
- identify $G = C_p^r$ with the points of $AG(r,p)$,
- A sequence S leads to the subset of points of $AG(r,p)$ in $\mathrm{supp}(S)$,
- A zero-sum subsequence $T : \sum_{g\in G} \mathsf{v}_g(T)g = 0$ of length $p = exp(\mathbb{Z}_p^r)$ corresponds to a nontrivial, vanishing, affine linear combination of points in $AG(r,p)$. (By identifying $v_g(T) \in \{0,\ldots,p-1\}$ and $\mathbb{F}_p$ canonically.)

In $\mathbb{F}_3$ the only affine linear combinations with at most three coefficients, $\lambda_1, \lambda_2, \lambda_3$, are:

- $\{\lambda_1, \lambda_2\} = \{1, 2\}$. Such a linear combination vanishes iff the two points are equal.
- $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, 1)$ or $(2, 2, 2)$. Here the first linear combination vanishes iff the second linear combination vanishes.

This immediately leads to the following Lemma showing the equivalence of sequences over C_3^r without zero-sum subsequences of length 3 and affine caps in $AG(r,3)$.

Lemma 20.
- *If a sequence S over C_3^r has no zero-sum subsequence of length 3 then $R = \mathrm{supp}(S)$ is an affine cap in $AG(r,3)$.*
- *If R is an affine cap in $AG(r,3)$ then $S = R^2$ has no zero-sum subsequence of length 3.*
- $\mathsf{s}(C_3^r) = m_2^a(r,3) \cdot 2 + 1$.
  ($m_2^a(r,3)$ being the maximal size of a cap in $AG(r,3)$).

So the constructed series in C_n^r are, for $n = 3$, affine ternary caps. We have already mentioned in the introduction that for $r = 1, 2, 3, 4$ we get caps of maximal size this way, while for larger r better ternary caps are known. Let us have a closer look at the case $r = 5$.

The ternary 42-cap from the sequence is complete as a cap in $AG(5,3)$ and extendable to a complete 48-cap in $PG(5,3)$, which is the size of the second largest complete cap in $PG(5,3)$ (see [1]). By Theorem 2 we know that 42 is the size of the second largest complete cap in $AG(5,3)$. As a consequence and due to the uniqueness of the maximal affine 45-cap (see [6]) we have that, if we can construct a larger sequence with property D' for all odd n, its restriction to $n = 3$ is contained in the affine part of the Hill cap.

For the proof of Theorem 2 we need the following Lemma:

Lemma 21. *For every 43-cap K in $AG(5,3)$, there exists a pair of parallel hyperplanes H_0, H_1 such that H_0 intersects K in at least 18 points and H_1 intersects K in at least 17 points.*

Proof. For a n-cap K in $AG(k,q)$ denote by n_i the number of hyperplanes H in $AG(k,q)$ with $|K \cap H| = i$. Simple counting arguments yield the following identities:

$$\begin{aligned}
\sum_i n_i &= \frac{q^{k+1}-1}{q-1} - 1, \\
\sum_i i n_i &= n\frac{q^k-1}{q-1}, \\
\sum_i \binom{i}{2} n_i &= \binom{n}{2}\frac{q^{k-1}-1}{q-1}, \\
\sum_i \binom{i}{3} n_i &= \binom{n}{3}\frac{q^{k-2}-1}{q-1}.
\end{aligned}$$

Using these identities, for a 43-cap in $AG(5,3)$, we see that we have $\sum_i f(i)n_i = 0$ for the polynomial $f(X) := 2541\binom{X}{3} - 31581\binom{X}{2} + 2019409$.

As we are in $AG(k,3)$ the hyperplanes are grouped in triples of parallel hyperplanes which partition the cap. We want to have a closer look at the contribution of a triple of parallel hyperplanes to $\sum_i f(i)n_i$. We say that a triple of parallel hyperplanes has type (a,b,c) if the hyperplanes of that triple intersect the cap in a, b respectively c points. The maximal number of points of the cap in a hyperplane is the maximal size of a cap in $AG(4,3)$, i.e. 20 [14].

It is easily verified that for integers $20 \geq a \geq 18$ and $20 \geq b \geq 17$ we have that $f(a) + f(b) + f(43-a-b) < 0$. For all other possible types (a,b,c) of triples (i.e. (17,17,9) or integers $20 \geq a \geq b \geq c = 43-a-b \geq 0$ with $b < 17$) we have $f(a) + f(b) + f(43-a-b) > 0$. As the sum over all occurring triples of parallel hyperplanes is zero, triples of type (a,b,c), with $20 \geq a \geq 18$ and $20 \geq b \geq 17$ have to exist. □

With this we are ready to give the

Proof of Theorem 2. We already have seen that the 42 points from the sequence obtained from Theorem 16 with the pairs $(A(2), B(2))$, $(A(3), B(3))$ of Lemma 19, viewed modulo 3, are a 42-cap in $AG(5,3)$. The completeness of this cap can easily be verified by computer.

As we know that 45 is the largest size of a cap in $AG(5,3)$ (see [6]) it remains to show that there are no complete 43 and 44-caps in $AG(5,3)$.

From [17, 14], we know that there is a unique 20-cap in $AG(4,3)$. A computer search for all 18 and 19-caps in $AG(4,3)$ showed that there is a unique 19-cap and that there are 19 different 18-caps in $AG(4,3)$. Based on

this classification we use a similar computer search as in [5, 6] to prove the non-existence of complete 43 or 44-caps for all cases occurring in Lemma 21. □

References

[1] J. Barát, Y. Edel, R. Hill and L. Storme, On complete caps in the projective geometries over $\mathbb{F}_3$ II: New improvements, *Journal of Combinatorial Mathematics and Combinatorial Computing*, 49 (2004), pp. 9–31.

[2] J. Bierbrauer, Large caps, *J. Geom.*, 76 (2003), pp. 16–51.

[3] J. Bierbrauer and Y. Edel, Bounds on affine caps, *Journal of Combinatorial Designs*, 10 (2002), pp. 111–115.

[4] A. R. Calderbank and P. C. Fishburn, Maximal three-independent subsets of $\{0, 1, 2\}^n$, *Designs, Codes and Cryptography*, 4 (1994), pp. 203–211.

[5] Y. Edel and J. Bierbrauer, 41 is the largest size of a cap in PG$(4, 4)$, *Designs, Codes and Cryptography*, 16 No.2 (1999), pp. 151–160.

[6] Y. Edel, S. Ferret, I. Landjev and L. Storme, The classification of the largest caps in $AG(5, 3)$, *Journal of Combinatorial Theory (A)*, 99 (2002), pp. 95–110.

[7] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham, Zero-sum problems in finite abelian groups and affine caps, *Quarterly Journal of Mathematics*, 58 (2007), pp. 159–186.

[8] C. Elsholtz, Lower bounds for multidimensional zero sums, *Combinatorica*, 24 (2004), pp. 351–358.

[9] C. Elsholtz, private communication.

[10] W. D. Gao, Q. H. Hou, W. Schmid and R. Thangadurai, On short zero-sum subsequences II, *Integers: Electronic Journal of Combinatorial Number Theory*, 7 A21 (2007).

[11] W. Gao and R. Thangadurai, On zero-sum sequences of prescribed length, *Aequationes Math.*, to appear.

[12] A. Geroldinger and F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory. *Pure and Applied Mathematics, vol. 279,* Chapman & Hall/CRC, 2005.

[13] H. Harborth, Ein Extremalproblem für Gitterpunkte, *J. Reine Angew. Math.*, 262 (1973), pp. 356–360.

[14] R. Hill, On Pellegrino's 20-caps in $S_{4,3}$. *Ann. Discrete Math.*, 18 (1983), pp. 443–448.

[15] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces : Update 2001, *Finite Geometries*, Kluwer Academic Publishers, 2001, pp. 201–246.

[16] R. Meshulam: On subsets of finite abelian groups with no 3-term arithmetic progression, *Journal of Combinatorial Theory A*, 71 (1995), pp. 168–172.

[17] G. Pellegrino: Sul massimo ordine delle calotte in $S_{4,3}$, *Matematiche (Catania)* 25 (1970), pp. 1–9.

[18] C. Reiher, On Kemnitz' conjecture concerning lattice points in the plane, *Ramanujan J.* 13 (2007), pp. 333 – 337.