THE INDEPENDENCE NUMBER OF A SUBSET OF AN ABELIAN GROUP

Béla Bajnok[1]
Department of Mathematics, Gettysburg College, Gettysburg, PA 17325-1486, USA
bbajnok@gettysburg.edu

Imre Ruzsa[2]
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364, Hungary
ruzsa@renyi.hu

Received: 11/8/02, Accepted: 1/26/03, Published:1/27/03

Abstract

We call a subset A of the (additive) abelian group G *t-independent* if for all non-negative integers h and k with $h+k \leq t$, the sum of h (not necessarily distinct) elements of A does not equal the sum of k (not necessarily distinct) elements of A unless $h=k$ and the two sums contain the same terms in some order. A *weakly t-independent* set satisfies this property for sums of distinct terms. We give some exact values and asymptotic bounds for the size of a largest t-independent set and weakly t-independent set in abelian groups, particularly in the cyclic group $\mathbb{Z}_n$.

1. Introduction

Our motivation for studying the independence number of subsets of an abelian group comes from spherical combinatorics. It was shown by the first author in [4] that if the set of integers $A = \{a_1, a_2, \dots, a_m\}$ forms a 3-independent set in the cyclic group $\mathbb{Z}_n$ (as defined below), then the set of n points $X = \{x_1, x_2, \dots, x_n\}$ with

$$x_i = \frac{1}{\sqrt{m}} \cdot \left(\cos(\frac{2\pi i a_1}{n}), \sin(\frac{2\pi i a_1}{n}), \dots, \cos(\frac{2\pi i a_m}{n}), \sin(\frac{2\pi i a_m}{n}) \right)$$

($i = 1, 2, \dots, n$) forms a *spherical* 3-*design* on the unit sphere S^{2m-1} (the case of S^{2m} can be reduced to this case). We believe that the concept of t-independence in $\mathbb{Z}_n$ and other

[1] Supported by a Gettysburg College Professional Development Grant and by the Department of Mathematics at Cornell University.

[2] Supported by the Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 25617, T 29759, T 38396.

abelian groups, extending some of the most well known concepts from additive number theory such as sum-free sets, Sidon sets, and B_h-sequences, is of independent interest; here we intend to provide the framework for a general discussion.

Throughout this paper G denotes a finite abelian group with order $|G| = n \geq 2$, written in additive notation, and A is a subset of G of size $m \geq 1$. For a positive integer h, we use the notation

$$h \cdot A = \underbrace{A + A + \cdots + A}_{h} = \{a_1 + a_2 + \cdots + a_h | a_1, a_2, \ldots, a_h \in A\}.$$

We introduce the following measure for the degree of independence of $A \subseteq G$.

Definition 1 *Let t be a non-negative integer and $A = \{a_1, a_2, \ldots, a_m\}$. We say that A is a t-*independent set *in G, if whenever*

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_m a_m = 0$$

for some integers $\lambda_1, \lambda_2, \ldots, \lambda_m$ with

$$|\lambda_1| + |\lambda_2| + \cdots + |\lambda_m| \leq t,$$

we have $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$. We call the largest t for which A is t-independent the independence number *of A in G, and denote it by* $\mathrm{ind}(A)$.

Equivalently, A is a t-independent set in G, if for all non-negative integers h and k with $h + k \leq t$, the sum of h (not necessarily distinct) elements of A can only equal the sum of k (not necessarily distinct) elements of A in a *trivial* way, that is, $h = k$ and the two sums contain the same terms in some order. We can break up our definition of t-independence into the following three requirements:

$$0 \not\in h \cdot A \text{ for } 1 \leq h \leq t; \tag{1}$$

$$(h \cdot A) \cap (k \cdot A) = \emptyset \text{ for } 1 \leq h < k \leq t - h; \tag{2}$$

and

$$|h \cdot A| = \binom{m + h - 1}{h} \text{ for } 1 \leq h \leq \left\lfloor \tfrac{t}{2} \right\rfloor. \tag{3}$$

It is enough, in fact, to require these conditions for equations containing a total of t or $t - 1$ terms; therefore the total number of equations considered can be reduced to $2 + (t - 2) + 1 = t + 1$.

These conditions and their variations have been studied very vigorously for a long time; it might be worthwhile to briefly review some of the related classic and recent literature here.

Sets satisfying condition (1) (or its versions where there is no limit on the number of terms and/or the terms need to be distinct – see weak independence in Section 5) are called *zero-sum-free sets*. For example, Erdős and Heilbronn ([14], see also C15 in [18]) asked for the largest number of distinct elements in the cyclic group $\mathbb{Z}_n$ so that no subset has sum zero. Related results can be found in the papers of Alon and Dubiner [1], Caro [11], Gao and Hamidoune [16], Harcos and Ruzsa [20], and their references.

Sets satisfying the condition $(h \cdot A) \cap (k \cdot A) = \emptyset$ are called (h,k)*-sum-free sets*. The first of these, $(1,2)$-sum-free sets, are simply called *sum-free sets*, and have a vast literature. It is well known and not hard to see that, if $sf(G)$ denotes the maximum size of a sum-free set in G, then

$$\frac{2}{7}n \leq sf(G) \leq \frac{1}{2}n, \tag{4}$$

where both inequalities are sharp as $sf(\mathbb{Z}_7) = 2$ and $sf(\mathbb{Z}_2) = 1$. A comprehensive survey on sum-free sets in abelian groups can be found in Street's article [30]; see also the works of Erdős [12], Alon and Kleitman [2], and Cameron and Erdős [10]. Recently, (h,k)-sum-free sets have been investigated in cyclic groups of odd prime order by Bier and Chin [6]. Other recent work on (h,k)-sum-free sets (among the positive integers rather than groups) includes a study of $(1,k)$-sum-free sets for $k \geq 3$ by Calkin and Taylor [9], $(3,4)$-sum-free sets by Bilu [7], and (h,k)-sum-free sets by Schoen [28]. We return to sum-free sets in Section 2 as we study 3-independent sets.

Sets satisfying the condition that h-term sums of elements of A be distinct up to the rearrangement of terms, as in (3), are called B_h*-sequences*. They have been studied very extensively among the positive integers, see the book of Halberstam and Roth [19], sections C9 and C11 in Guy's book [18], and the survey paper of Graham [17]. The case $h = 2$ is worth special mentioning; a B_2-sequence is called a *Sidon-sequence* after Sidon who introduced them to study Fourier series [29]. An excellent extensive survey of Sidon-sequences was written (in Hungarian) by Erdős and Freud [13]. We review Sidon-sets and B_h-sequences as we study t-independence for $t \geq 4$ in Section 3.

There have recently been attempts to combine some of these conditions. For example, Nathanson [25] investigated sum-free Sidon sets in $\mathbb{Z}_n$; large Sidon sets were also used to construct small sum-free sets by Baltz, Schoen, and Srivastav [5]. The present paper provides a more general setting for a discussion of these conditions.

Zero-sum-free sets, (h,k)-sum-free sets, and B_h-sequences are only three of the many interesting families of linear equations among the integers or in an abelian group. For a survey of general results and other known cases, see the papers of Ruzsa [26] and [27], as well as sections C8 through C16, E12, E28, and E32 of Guy's wonderful book [18].

We note that some, but not all, of the methods that we describe below can easily be modified to treat t-independence in non-abelian groups. Sum-free (i.e. *product-free*) sets and Sidon sets in non-abelian groups were discussed by Babai and Sós [3]; see also the recent results of Kedlaya in [21] and [22].

Our objective in this paper is to study the size of a largest t-independent set in an abelian group G, which we denote by $s(G,t)$ (if G has no t-independent subsets, we set $s(G,t)=0$).

Since $0 \leq \mathrm{ind}(A) \leq n-1$ holds for every subset A of G (so no subset is "completely" independent), we see that $s(G,0)=n$ and $s(G,n)=0$. It is also clear that $\mathrm{ind}(A)=0$ if and only if $0 \in A$, hence $s(G,1)=n-1$. For the rest of the paper, we assume that $2 \leq t \leq n-1$.

First we derive an upper bound for $s(G,t)$ using a simple counting argument, as follows. Suppose that A is a t-independent set in G of size m. Define

$$\langle A, \lfloor t/2 \rfloor \rangle = \bigcup_{h=1}^{\lfloor t/2 \rfloor} h \cdot A.$$

Since A is t-independent, by conditions (2) and (3) we see that $\langle A, \lfloor t/2 \rfloor \rangle$ has size exactly

$$\sum_{h=1}^{\lfloor t/2 \rfloor} \binom{m+h-1}{h} = \binom{m+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor} - 1.$$

Therefore, the set $-\langle A, \lfloor t/2 \rfloor \rangle$, consisting of the negatives of the elements of $\langle A, \lfloor t/2 \rfloor \rangle$, also has this size; furthermore, we have

$$\langle A, \lfloor t/2 \rfloor \rangle \cap -\langle A, \lfloor t/2 \rfloor \rangle = \emptyset.$$

Additionally, by condition (1),

$$0 \notin \langle A, \lfloor t/2 \rfloor \rangle \cup -\langle A, \lfloor t/2 \rfloor \rangle,$$

so

$$n-1 \geq 2 \cdot |\langle A, \lfloor t/2 \rfloor \rangle|,$$

and therefore

$$n \geq 2 \cdot \binom{m+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor} - 1.$$

Since for $t \geq 2$,

$$2 \cdot \binom{m+\lfloor t/2 \rfloor}{\lfloor t/2 \rfloor} - 1 > 2 \cdot \frac{m^{\lfloor t/2 \rfloor}}{\lfloor t/2 \rfloor !},$$

we get the following result.

Proposition 2 *For every $t \geq 2$ we have*

$$s(G,t) < \left(\frac{1}{2}\left\lfloor\frac{t}{2}\right\rfloor!n\right)^{1/\lfloor t/2\rfloor}.$$

In section 3 we show that Proposition 2 gives the correct magnitude of $s(G,t)$ if G is the cyclic group $\mathbb{Z}_n$, that is

$$s(\mathbb{Z}_n,t) = \Theta(n^{1/\lfloor t/2\rfloor}).$$

Namely, we prove

Theorem 3 *For every $\epsilon > 0$, $t \geq 2$, and large enough n,*

$$s(\mathbb{Z}_n,t) > \left(\frac{1-\epsilon}{t\cdot\lfloor(t+1)/2\rfloor}\cdot n\right)^{1/\lfloor t/2\rfloor}.$$

We have succeeded in finding the exact values of $s(\mathbb{Z}_n,t)$ only for $t \leq 3$. We have already seen that $s(\mathbb{Z}_n,1) = n-1$, and we can easily verify that

$$s(\mathbb{Z}_n,2) = \lfloor(n-1)/2\rfloor \tag{5}$$

(the set $\{1,2,\ldots,\lfloor(n-1)/2\rfloor\}$ is 2-independent and has maximum size as we must have $A\cap -A = \emptyset$). For $t=3$, in Section 2 we prove

Theorem 4

$$s(\mathbb{Z}_n,3) = \begin{cases} \left\lfloor\frac{n}{4}\right\rfloor & \textit{if } n \textit{ is even} \\ \left(1+\frac{1}{p}\right)\frac{n}{6} & \textit{if } n \textit{ is odd, has prime divisors congruent to } 5 \pmod 6, \\ & \textit{and } p \textit{ is the smallest such divisor} \\ \left\lfloor\frac{n}{6}\right\rfloor & \textit{otherwise} \end{cases}$$

Note that these results imply that the coefficient of n in Theorem 3 cannot be improved for $t=2$ and $t=3$.

Let us now turn to general abelian groups. First note that, according to Proposition 2 and Theorem 3, the exponent of n in the upper bound on $s(G,t)$ given in Proposition 2 is sharp; for

$$S(t) = \limsup\frac{s(G,t)^{1/\lfloor t/2\rfloor}}{n}$$

we have

$$\frac{1}{t\cdot\lfloor(t+1)/2\rfloor} \leq S(t) \leq \frac{1}{2}\left\lfloor\frac{t}{2}\right\rfloor!.$$

These inequalities yield $S(2) = 1/2$, and we later prove that $S(3) = 1/4$. We do not know the values of $S(t)$ for $t \geq 4$.

As for lower bounds, it is clear that we cannot expect a lower bound for $s(G,t)$ in terms of $n=|G|$ only; in fact, if the exponent κ of G is not more than t, then obviously $s(G,t)=0$.

We will use the following notations. For a positive integer h, let the "h-torsion" subgroup of G be

$$\mathrm{Tor}(G,h)=\{x\in G|hx=0\};\tag{6}$$

then

$$\mathrm{Ord}(G,h)=\cup_{h=1}^{t}\mathrm{Tor}(G,h)\tag{7}$$

is the set of those elements of G which have order at most t. By condition (1), no element of $\mathrm{Ord}(G,h)$ can be in a t-independent set of G.

We have already noted that $s(G,1)=n-1$, and we can now easily determine the value of $s(G,2)$: to get a maximum 2-independent set in G, take exactly one of each element or its negative in $G\setminus\mathrm{Ord}(G,2)$, hence we have

$$s(G,2)=\frac{n-\mathrm{Ord}(G,2)}{2}.\tag{8}$$

As a special case, for the cyclic group of order n we have (5).

Note that if $\mathrm{Ord}(G,2)=G$ then $s(G,2)=0$; for $n\geq 2$ this occurs only for the elementary abelian 2-group. If $\mathrm{Ord}(G,2)\neq G$ then, since $\mathrm{Ord}(G,2)$ is a subgroup of G, we have $1\leq|\mathrm{Ord}(G,2)|\leq n/2$, and therefore we get the following.

Proposition 5 *If G is isomorphic to the elementary abelian 2-group, then $s(G,2)=0$. Otherwise*

$$\frac{1}{4}n\leq s(G,2)\leq\frac{1}{2}n.$$

Let us now consider $t=3$. As noted before, if $\mathrm{Ord}(G,3)=G$, then $s(G,3)=0$; this occurs if and only if G is isomorphic to the elementary abelian p-group for $p=2$ or $p=3$. In Section 2 we determine some exact values and sharp upper and lower bounds for $s(G,3)$ in terms of the exponent of G (see Theorem 12); in particular, we prove the following.

Theorem 6 *If G is isomorphic to the elementary abelian p-group for $p=2$ or $p=3$, then $s(G,3)=0$. Otherwise*

$$\frac{1}{9}n\leq s(G,3)\leq\frac{1}{4}n.$$

These bounds can be attained since $s(\mathbb{Z}_9,3)=1$ and $s(\mathbb{Z}_4,3)=1$.

Studying t-independent sets in G for larger values of t seems considerably more difficult. As a case in point, let $t \geq 4$, $\kappa > t$ be fixed, and consider the sequence of groups

$$G_k = \mathbb{Z}_2^k \times \mathbb{Z}_\kappa$$

($k = 1, 2, 3 \ldots$). Suppose that A is a t-independent set in G_k and that for some $a_1, a_2 \in \mathbb{Z}_2^k$ and $x \in \mathbb{Z}_\kappa$, $g_1 = (a_1, x)$ and $g_2 = (a_2, x)$ are elements of A. Then $g_1 + g_1 = g_2 + g_2$ is a non-trivial equation in G_k, thus we conclude that $g_1 = g_2$ and $|A| \leq \kappa$. This implies that, as k approaches infinity, we have $s(G_k, t) = O(1)$.

Therefore, in order to have a lower bound on $s(G, t)$ which tends to infinity with n, we must have more than just $\mathrm{Ord}(G, t) \neq G$ (as was the case for $t \leq 3$); although this will be sufficient for elementary abelian groups (see Corollary 8 below). In general, we require that $|\mathrm{Ord}(G, t)|$ be not too large compared to $|G| = n$; in Section 4, we make this more precise by setting

$$\sigma(G, t) = \sum_{k=1}^{t} |\mathrm{Tor}(G, k)| \tag{9}$$

and proving the following theorem.

Theorem 7 *With $\sigma(G, t)$ as in (9) above we have*

$$s(G, t) \geq \left\lfloor \left(\frac{n}{2\sigma(G, t)} \right)^{1/t} \right\rfloor.$$

Since obviously $\sigma(G, t) \leq t \cdot |\mathrm{Ord}(G, t)|$, we get the corollary that

$$s(G, t) \geq \left\lfloor \left(\frac{n}{2t \cdot |\mathrm{Ord}(G, t)|} \right)^{1/t} \right\rfloor.$$

It is worth comparing the lower bounds of Theorems 3 and 7 for the cyclic group. In $\mathbb{Z}_n$ we have

$$\sigma(\mathbb{Z}_n, t) = \sum_{h=1}^{t} |\mathrm{Tor}(\mathbb{Z}_n, h)| = \sum_{h=1}^{t} \gcd(h, n) \leq \frac{t(t+1)}{2}.$$

Therefore both the exponent of n and the coefficient are approximately twice as large in Theorem 3 as they are in Theorem 7.

Let us state a corollary of Theorem 7 for elementary abelian p-groups.

Corollary 8 *Let G be an elementary abelian p-group for a prime p. If $p \leq t$, then $s(G, t) = 0$; otherwise*

$$s(G, t) \geq \left(\frac{1}{2} n \right)^{1/t}.$$

Finally, in Section 5, we examine *weak t-independence*: where for all non-negative integers h and k with $h+k \leq t$, sums of h distinct elements of a set do not equal sums of k distinct elements in a non-trivial way. A comparison between sum-free and weak sum-free, as well as Sidon and weak Sidon sets, and B_h sequences versus weak B_h sequences, can be found in Ruzsa's papers [26] and [27]; there it was shown that their maximum sizes among the positive integers behave similarly. This certainly does not hold for t-independence in abelian groups. Denoting the maximum size of a weakly t-independent set in G by $w(G,t)$, we find that for each fixed t, $\liminf w(G,t)$ tends to infinity with $n = |G|$ (see Theorem 18), while obviously $\liminf s(G,t) = 0$ for each $t \geq 2$. Moreover, the weak independence number of each subset of G can be arbitrarily large, even infinity, while its independence number cannot be more than n.

This paper provides a modest attempt to discuss independence and weak independence in abelian groups. Numerous interesting questions remain open, warranting further study.

2. 3-independent sets in abelian groups

In this section we develop upper and lower bounds for $s(G,3)$, and provide exact values for some groups, including the cyclic group $\mathbb{Z}_n$.

Note that, by conditions (1), (2), and (3), a subset A of G is 3-independent, if and only if $0 \notin A, 0 \notin A+A, 0 \notin A+A+A$, and

$$(A+A) \cap A = \emptyset. \tag{10}$$

Sets satisfying (10) are called sum-free, and have been studied extensively; see [30] for a comprehensive survey.

It is not hard to determine bounds on the maximum size $sf(G)$ of a sum-free set in G. First, note that the set

$$\{\lfloor (n+1)/3 \rfloor, \lfloor (n+1)/3 \rfloor + 1, \ldots, 2\lfloor (n+1)/3 \rfloor - 1\}$$

is a sum-free set in $\mathbb{Z}_n$; when n is even, the larger set

$$\{1, 3, 5, \ldots, n-1\}$$

is also sum-free. Since $\lfloor (n+1)/3 \rfloor \geq \frac{2}{7}n$ when $n \geq 3$ is odd, we have $sf(\mathbb{Z}_n) \geq \frac{2}{7}n$. Clearly, if A is sum-free in $\mathbb{Z}_n$, then $H \times A$ is sum-free in $H \times \mathbb{Z}_n$ for any abelian group H, so the bound $sf(G) \geq \frac{2}{7}n$ holds for any G (with $n > 1$). On the other hand, if A is sum-free in G, then by (10) $n \geq |A+A| + |A| \geq 2|A|$, and we get the well known result that

$$\frac{2}{7}n \leq sf(G) \leq \frac{1}{2}n.$$

Note that these bounds are sharp, as $sf(\mathbb{Z}_7) = 2$ and $sf(\mathbb{Z}_2) = 1$.

Our goal is to prove a similar result for 3-independent sets. Let us start with the upper bound.

Proposition 9 *Suppose that A is a 3-independent set in G of size m.*

1. *If none of the divisors of n are congruent to $2 \pmod 3$, then $m \leq \frac{1}{6}n$.*
2. *Otherwise, let p be the smallest divisor of n which is congruent to $2 \pmod 3$. Then we have $m \leq \frac{1}{6}\left(1 + \frac{1}{p}\right) n$.*

Proof. Let $B = A \cup (-A)$. Since A is 3-independent, we have $A \cap (-A) = \emptyset$, thus $|B| = 2m$. Furthermore, we have

$$B \cap (B + B) = \emptyset.$$

We apply Kneser's theorem [24] to the set B. It asserts that either we have

$$|B + B| \geq 2|B|,$$

or there is a subgroup H and an integer k such that B is contained in k cosets of H, and $B + B$ is equal to the union of $2k - 1$ cosets.

In the first case we have

$$n \geq |B| + |B + B| \geq 3|B| = 6m$$

and we are done.

Assume that the second possibility holds. Write $|H| = d$ and $q = \frac{n}{d}$; we then have

$$2m = |B| \leq dk = \frac{n}{q}k,$$

hence

$$m \leq \frac{nk}{2q}. \tag{11}$$

Since B cannot intersect any of the $2k - 1$ cosets contained in $B + B$, we have

$$k + (2k - 1) = 3k - 1 \leq q;$$

if strict inequality holds here, then by (11) we have

$$m \le \frac{nk}{2(3k)} = \frac{1}{6}n,$$

and we are done again.

Otherwise, $q = 3k - 1 \equiv 2 \pmod 3$, and from (11) we get

$$m \le \frac{n}{2q}\frac{q+1}{3} = \frac{1}{6}\left(1 + \frac{1}{q}\right) n \le \frac{1}{6}\left(1 + \frac{1}{p}\right) n,$$

as claimed. $\square$

Note that when n is even, Proposition 9 yields $s(G, 3) \le \frac{1}{4}n$. This is clearly not sharp when $\mathrm{Ord}(G, 2)$ is large; by (8) we must have $s(G, 2)$ and therefore $s(G, 3)$ small. More precisely, we have the following upper bound.

Proposition 10 *Let κ be the exponent of G and $\mathrm{Ord}(G, 2)$ be the set of elements of G with order at most 2. If κ is congruent to $2 \pmod 4$, then $s(G, 3) \le \frac{1}{4}(n - |\mathrm{Ord}(G, 2)|)$.*

Proof. When $\kappa \equiv 2 \pmod 4$, we can write $G = \mathbf{Z}_2^i \times G_1$, $|G_1| = n_1$ where n_1 is odd. The case $n_1 = 1$ is obvious, so assume $n_1 \ge 3$. Let A be a 3-independent set in G and write $|A| = m$. We want to show that $m \le 2^{i-2}(n_1 - 1)$.

Following the proof (and the notations) of Proposition 9 above, we see that we either have

$$m \le \frac{1}{6}n,$$

or there is a subgroup H of G of index $q = 3k - 1$, such that $B = A \cup (-A)$ is contained in k cosets of H, and $B + B$ is equal to the union of $2k - 1$ cosets; in this case from (11) we have

$$m \le \frac{nk}{6k - 2}.$$

Since $n_1 \ge 3$ implies

$$\frac{1}{6}n \le 2^{i-2}(n_1 - 1),$$

we can assume that the second possibility holds. Furthermore, an easy computation shows that if $n_1 \ge 5$ and $k \ge 2$, then

$$\frac{nk}{6k - 2} \le 2^{i-2}(n_1 - 1),$$

so we only need to consider the cases of $n_1 = 3$ or $k = 1$.

If $n_1 = 3$, then $G = \mathbf{Z}_2^i \times \mathbf{Z}_3$. Let B_0, B_1, B_2 be the parts of B in the three cosets of $\mathbf{Z}_2^i$. We have $B_0 = \emptyset$, $B_2 = -B_1$ and $B_1 \cap (B_2 + B_2) = \emptyset$. Now by an obvious pigeonhole argument we have $|B_2| \le 2^{i-1}$, so $m \le n/6$ again. This concludes this case.

Finally assume $k = 1$. Thus H is a subgroup of index 2, B is contained in the coset $G \setminus H$ and $B + B = H$. Since $\mathrm{Ord}(G, 2)$ is a subgroup of G of order 2^i and H has order $2^{i-1}n_1$, we have $|H \cap \mathrm{Ord}(G, 2)| \leq 2^{i-1}$, and therefore $|B| \leq n/2 - 2^{i-1}$, from which our claim follows. $\square$

Now we turn to the lower bound.

Proposition 11 *Let κ be the exponent of G and $\mathrm{Ord}(G, 2)$ be the set of elements of G with order at most 2.*

1. *If κ is divisible by 4, then G contains a 3-independent set of size $\frac{1}{4}n$.*
2. *If κ is congruent to $2 \pmod 4$, then G contains a 3-independent set of size $\frac{1}{4}(n - |\mathrm{Ord}(G, 2)|)$.*
3. *Suppose that the odd positive integer d divides κ. Then G contains a 3-independent set of size $\frac{1}{d}\lfloor\frac{d+1}{6}\rfloor n$.*

Proof. We construct the desired set explicitly as follows. Suppose that the positive integer d divides κ, and choose a subgroup H and an element g of G so that G is the union of the d distinct cosets $H, H + g, \ldots, H + (d - 1)g$.

Consider first the set

$$A = \bigcup_{\frac{d}{6}<j<\frac{d}{3}} (H + jg).$$

It is clear that A is 3-independent. To determine the size of A, note that there are exactly

$$f(d) = \left\lfloor \frac{d-1}{3} \right\rfloor - \left\lceil \frac{d+1}{6} \right\rceil + 1$$

integers strictly between $\frac{d}{6}$ and $\frac{d}{3}$. When d is odd, $f(d) = \lfloor\frac{d+1}{6}\rfloor$, proving the last part of our Proposition. Also, $f(4) = 1$; so choosing $d = 4$ when κ is divisible by 4 proves the first case of our Proposition.

Assume now that κ is even, but not divisible by 4, and set $d = \kappa$. Define

$$A = \bigcup_{i=1}^{\lfloor\frac{\kappa}{4}\rfloor}(H + (2i - 1)g).$$

It is easy to see that A is 3-independent (note that κ is even). For the size of A we have

$$|A| = \left\lfloor \frac{\kappa}{4} \right\rfloor \cdot |H| = \frac{\kappa - 2}{4} \cdot \frac{n}{\kappa}.$$

We add some elements to A as follows. Let H' be a 2-independent set in H of maximum size, and define

$$A' = \{h' + \frac{\kappa}{2} g | h' \in H'\}.$$

Since $\frac{\kappa}{2}$ is odd, it is easy to check that $A \cup A'$ is 3-independent. Using (8), we get

$$|A'| = s(H,2) = \frac{\frac{n}{\kappa} - |\mathrm{Ord}(H,2)|}{2}.$$

But $G \cong H \times \mathbb{Z}_\kappa$, therefore $|\mathrm{Ord}(G,2)| = 2 \cdot |\mathrm{Ord}(H,2)|$, and we get

$$|A \cup A'| = \frac{\kappa - 2}{4} \cdot \frac{n}{\kappa} + \frac{\frac{n}{\kappa} - |\mathrm{Ord}(H,2)|}{2} = \frac{1}{4}(n - |\mathrm{Ord}(G,2)|),$$

as claimed. $\square$

We can now use Propositions 9, 10, and 11 to establish the following bounds and exact values for $s(G,3)$.

Theorem 12 *Let κ be the exponent of G.*

1. *If κ is divisible by 4, then*
$$s(G,3) = \frac{n}{4}.$$
2. *If κ is even but not divisible by 4, then*
$$s(G,3) = \frac{1}{4}(n - |\mathrm{Ord}(G,2)|).$$
3. *If κ (iff n) is odd and has prime divisors congruent to 5 $\pmod 6$, and p is the smallest such divisor, then*
$$s(G,3) = \left(1 + \frac{1}{p}\right)\frac{n}{6}.$$
4. *Finally, if κ (iff n) is odd and has no prime divisors congruent to 5 $\pmod 6$, then*
$$\left\lfloor \frac{\kappa}{6} \right\rfloor \frac{n}{\kappa} \leq s(G,3) \leq \frac{n}{6}.$$

Since the exponent of the cyclic group $\mathbb{Z}_n$ is n, we have settled the value of $S(\mathbb{Z}_n, 3)$; see Theorem 4.

In order to prove Theorem 6, we should estimate $|\mathrm{Ord}(G,2)|$ when κ is even. Let K be a cyclic subgroup of G of order κ, and write $H = G/K$. Then, since κ is even,

$|\mathrm{Ord}(G,2)| = 2\cdot|\mathrm{Ord}(H,2)|$. Since obviously $|\mathrm{Ord}(H,2)| \le |H| = \frac{n}{\kappa}$, we get $|\mathrm{Ord}(G,2)| \le \frac{2n}{\kappa}$, and the first two cases of Theorem 12 yield that when κ is even, we have

$$\left\lfloor \frac{\kappa}{4} \right\rfloor \frac{n}{\kappa} \le s(G,3) \le \frac{n}{4}.$$

So if $\kappa \ge 4$ is even, we get

$$\frac{n}{6} \le s(G,3) \le \frac{n}{4},$$

and when $\kappa \ge 5$ is odd, Theorem 12 implies

$$\frac{n}{9} \le s(G,3) \le \frac{n}{5}.$$

In particular, we have proved Theorem 6.

3. t-independent sets in the cyclic group

In this section we study the maximum size of a t-independent set in the cyclic group $\mathbb{Z}_n$. In view of (5) and Theorem 4, it is enough to focus on $4 \le t \le n-1$.

For $t = 4$ (in fact, for $t \ge 4$), condition (3) requires that pairwise sums (or, equivalently, pairwise differences) of elements of A be essentially distinct. This condition has been studied extensively among the set of positive integers. For a fixed positive integer N, a subset B of $\{1,2,\ldots,N\}$ with this property is called a *Sidon-sequence* after Sidon who introduced them to study Fourier series [29]. An excellent survey of Sidon-sequences was written (in Hungarian) by Erdős and Freud [13]. Denoting the maximum cardinality of a Sidon-sequence in $\{1,2,\ldots,N\}$ by $F_2(N)$, we have the classic result of Erdős and Turán [15] which says that for every $\epsilon > 0$, $\delta > 0$, and large enough N,

$$(1-\epsilon)\sqrt{N} < F_2(N) < (1+\delta)\sqrt{N}; \tag{12}$$

and it is a famous conjecture of Erdős that, in fact, $|F_2(N) - \sqrt{N}| = O(1)$.

More generally, a subset B of $\{1,2,\ldots,N\}$ with the property that all h-term sums of (not necessarily distinct) elements of B are distinct, except for the order of the terms, is called a B_h-sequence. Bose and Chowla [8] have shown that, if $F_h(N)$ denotes the maximum size of a B_h-sequence in $\{1,2,\ldots,N\}$, then for every $\epsilon > 0$ and large enough N, we have

$$F_h(N) > (1-\epsilon)N^{\frac{1}{h}}. \tag{13}$$

The simple counting argument leading to Proposition 2, noting that h-term sums of elements of B are in the interval $[1, hN]$, yields the upper bound

$$F_h(N) \le (hh!N)^{\frac{1}{h}};$$

reducing the coefficient of N is the subject of vigorous recent study (see C11 in [18] and its references). It is unknown whether the limit

$$\lim_{n\to\infty} \frac{F_h(N)}{N^{1/h}}$$

exists for any $h \geq 3$. For further references on B_h-sequences see the book by Halberstam and Roth [19]; sections C9 and C11 in Guy's book [18]; and the survey paper of Graham [17].

We use B_h-sequences to construct t-independent sets in the cyclic group $\mathbb{Z}_n$. Elements of $\mathbb{Z}_n$ will be denoted by $0, 1, 2, \ldots, n-1$.

Proposition 13 *Let* $3 \leq t \leq n-1$ *and*

$$N = \left\lfloor \frac{\lfloor n/t \rfloor}{\lfloor (t+1)/2 \rfloor} \right\rfloor, \tag{14}$$

and suppose that B *is a* $B_{\lfloor t/2 \rfloor}$*-sequence in the interval* $[1, N]$*. Then the set*

$$A = \{\lfloor n/t \rfloor - b | b \in B\}$$

is t*-independent in the cyclic group* $\mathbb{Z}_n$*.*

Proof. First note that $3 \leq t \leq n-1$ guarantees that $N < \lfloor n/t \rfloor$, and thus, for each $a \in A$, we have

$$0 < \lfloor n/t \rfloor - N \leq a \leq \lfloor n/t \rfloor - 1 < n/t.$$

We verify that requirements (1), (2), and (3) hold. (i) Let $1 \leq h \leq t$. Since $g \in h \cdot A$ satisfies

$$0 < h \cdot (\lfloor n/t \rfloor - N) \leq g \leq h \cdot (\lfloor n/t \rfloor - 1) < n,$$

we see that (1) holds.

(ii) To show (2), let $1 \leq h < k \leq t-h$, and suppose, indirectly, that $g \in h \cdot A \cap k \cdot A$. Then we must have

$$k \cdot (\lfloor n/t \rfloor - N) \leq g \leq h \cdot (\lfloor n/t \rfloor - 1).$$

Since $k \geq h+1$, this implies

$$(h+1) \cdot (\lfloor n/t \rfloor - N) \leq h \cdot (\lfloor n/t \rfloor - 1),$$

or, equivalently,

$$N \geq \frac{\lfloor n/t \rfloor + h}{h+1}.$$

But this contradicts (14), since $h \leq \lfloor (t-1)/2 \rfloor$.

(iii) Finally, (3) holds, since for $1 \leq h \leq \lfloor t/2 \rfloor$, B is a B_h-sequence in $[1, N]$ and, using self-explanatory notation,

$$a_1 + a_2 + \cdots + a_h = a'_1 + a'_2 + \cdots + a'_h \text{ in } \mathbb{Z}_n$$

implies

$$a_1 + a_2 + \cdots + a_h = a'_1 + a'_2 + \cdots + a'_h \text{ in } \mathbb{Z}$$

and this further implies

$$b_1 + b_2 + \cdots + b_h = b'_1 + b'_2 + \cdots + b'_h \text{ in } \mathbb{Z}.$$

□

Theorem 3 is now an easy corollary to Proposition 13 and (13) (also using (5) for $t = 2$).

It is worthwhile to further analyze the cases $t = 4$ and $t = 5$ as follows. Suppose that A is a t-independent set in $\mathbb{Z}_n$ where $t \geq 4$. Without loss of generality, we may assume that each $a \in A$ satisfies $1 \leq a \leq \lfloor \frac{n-1}{2} \rfloor$ (replace a by $n - a$, if necessary). Note that A is a Sidon-sequence in $\{1, 2, \ldots, \lfloor \frac{n-1}{2} \rfloor\}$. Therefore, by (12), we have

$$|A| \leq (1 + o(1)) \cdot \sqrt{n/2},$$

and this results in the following improvements.

Corollary 14 *For every $\epsilon > 0$, $\delta > 0$, and large enough n we have*

$$\left(\frac{1}{\sqrt{8}} - \epsilon\right) \cdot \sqrt{n} \leq s(\mathbb{Z}_n, 4) \leq \left(\frac{1}{\sqrt{2}} + \delta\right) \cdot \sqrt{n}.$$

$$\left(\frac{1}{\sqrt{15}} - \epsilon\right) \cdot \sqrt{n} \leq s(\mathbb{Z}_n, 5) \leq \left(\frac{1}{\sqrt{2}} + \delta\right) \cdot \sqrt{n}.$$

We have determined the values of $s(\mathbb{Z}_n, 4)$ and $s(\mathbb{Z}_n, 5)$ for all $n \leq 200$. While neither sequence is monotone, the values of $s(\mathbb{Z}_n, 4)$ tend to grow more uniformly; we venture to state the following conjectures.

Conjecture 15 *We have*

1. $\lim \frac{s(\mathbb{Z}_n,4)}{\sqrt{n}} = \frac{1}{\sqrt{3}}$,
2. $\lim \frac{s(\mathbb{Z}_n,5)}{\sqrt{n}}$ *does not exist.*

It is worth to recall, in comparison, that the sequence $s(\mathbb{Z}_n, 2)/n$ is convergent while $s(\mathbb{Z}_n, 3)/n$ is not. A further observation on these sequences: by Theorem 4, the sequence $s(\mathbb{Z}_n, 3)$ is monotone for even values of n (but not for the odd values); we find that, for $n \leq 200$, the sequence $s(\mathbb{Z}_n, 5)$ is monotone for odd values of n (but not for the even values).

4. t-independent sets in abelian groups

In this section we prove the general lower bound for $s(G,t)$ stated in Theorem 7.

Recall that for a positive integer h, we let the "h-torsion" subgroup of G be

$$\mathrm{Tor}(G,h) = \{x \in G | hx = 0\};$$

and we also defined

$$\sigma(G,t) = \sum_{h=1}^{t} |\mathrm{Tor}(G,h)|.$$

Proposition 16 *Suppose that m is a positive integer for which*

$$n > \sigma(G,t) \cdot \binom{2m-2+t}{t}.$$

Then G has a t-independent set of size m.

Proof. We use induction on m. For $m = 1$ we have $n > \sigma(G,t)$, thus we can choose an element

$$a \in G \setminus \bigcup_{h=1}^{t} \mathrm{Tor}(G,h).$$

Clearly, $\{a\}$ is then a t-independent set in G.

Assume now that our proposition holds for a positive integer m and suppose that

$$n > \sigma(G,t) \cdot \binom{2m+t}{t}.$$

Since this value is greater than

$$\sigma(G,t) \cdot \binom{2m-2+t}{t},$$

our inductive hypothesis implies that G has a t-independent set A of size m.

Define $B = A \cup (-A)$ and

$$\langle B,t \rangle = \bigcup_{h=1}^{t} h \cdot B.$$

First, note that $\langle B,t \rangle$ has size at most

$$\sum_{h=1}^{t} \binom{2m+h-1}{h} = \binom{2m+t}{t} - 1.$$

For a fixed positive integer h and group element g, define

$$\mathrm{Root}_h(g) = \{x \in G | hx = g\}.$$

We prove the following

Claim. If $\mathrm{Root}_h(g) \neq \emptyset$, then $|\mathrm{Root}_h(g)| = |\mathrm{Tor}(G,h)|$.

Proof of Claim. Fix $x \in \mathrm{Root}_h(g)$. Our claim follows from the fact that $y \in \mathrm{Root}_h(g)$, if and only if, $y - x \in \mathrm{Tor}(G,h)$.

Now define

$$C = \bigcup_{b \in \langle B,t\rangle} \bigcup_{h=1}^{t} \mathrm{Root}_h(b).$$

An obvious upper bound for the size of C is

$$\sigma(G,t) \cdot \left(\binom{2m+t}{t} - 1 \right).$$

Therefore, according to our inductive hypothesis, the set $G \backslash C$ is non-empty; fix $a \in G \backslash C$.

Claim. $A \cup \{a\}$ is a t-independent set of size $m+1$ in G.

Proof. To see that $A \cup \{a\}$ is of size $m+1$, note that

$$a \in G \setminus C \subseteq G \setminus \langle B,t\rangle \subseteq G \setminus B \subseteq G \setminus A.$$

Now let $A = \{a_1, a_2, \ldots, a_m\}$ and assume that

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_m a_m + \lambda a = 0$$

for some integers $\lambda_1, \lambda_2, \ldots, \lambda_m, \lambda$. Suppose, indirectly, that

$$1 \leq |\lambda_1| + |\lambda_2| + \cdots + |\lambda_m| + |\lambda| \leq t.$$

Set

$$x = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_m a_m.$$

Note that $x \in \langle B,t\rangle$ and therefore $-x \in \langle B,t\rangle$; we also have $a \in \mathrm{Root}_\lambda(-x)$.

Without loss of generality, we can assume that $\lambda \geq 0$. If $1 \leq \lambda \leq t$, then we have $a \in \mathrm{Root}_\lambda(-x) \subseteq C$, a contradiction with the choice of a. Otherwise, $\lambda = 0$, from which $x = 0$; a contradiction, since A is t-independent. This completes the proof of our claim and therefore our Proposition. $\square$

Now Theorem 7 follows from Propositions 16, by noting that

$$\begin{aligned}
\binom{2m-2+t}{t} &= \prod_{k=1}^{t} \frac{2m-2+k}{k} \\
&= \prod_{k=1}^{t} \frac{mk-(k-2)(m-1)}{k} \\
&\leq (2m-1)m^{t-1} \\
&< 2m^t.
\end{aligned}$$

5. Weakly t-independent sets in abelian groups

When discussing solutions of equations in a set, it is natural to consider the version when we restrict ourselves to distinct solutions; this is referred to as the *weak* property. A comparison between sum-free and weak sum-free, as well as Sidon and weak Sidon sets, and B_h sequences versus weak B_h sequences, can be found in Ruzsa's papers [26] and [27]; there it was shown that their maximum sizes among the positive integers behave similarly. This certainly does not hold for t-independence in abelian groups, as we see in this section.

For a positive integer h, we use the notation

$$h \star A = \{a_1 + a_2 + \cdots + a_h | a_1, a_2, \ldots, a_h \in A \text{ are distinct}\}.$$

We introduce the following measure for the degree of weak independence of $A \subseteq G$.

Definition 17 *Let t be a non-negative integer and $A = \{a_1, a_2, \ldots, a_m\}$. We say that A is a* weakly t-independent set *in G, if whenever*

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_m a_m = 0$$

for some integers $\lambda_1, \lambda_2, \ldots, \lambda_m \in \{-1, 0, 1\}$ with

$$|\lambda_1| + |\lambda_2| + \cdots + |\lambda_m| \leq t,$$

we have $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$. We call the largest t for which A is weakly t-independent the weak independence number *of A in G and denote it by* wind(A)*; if A is weakly t-independent for every t, we set* wind$(A) = \infty$.

Equivalently, A is a weakly t-independent set in G, if for all non-negative integers h and k with $h + k \leq t$, the sum of h distinct elements of A can only equal the sum of k

distinct elements of A in a *trivial* way, that is, $h = k$ and the two sums contain the same terms in some order.

This time, we have the following three requirements:

$$0 \notin h \star A \text{ for } 1 \leq h \leq t; \tag{15}$$

$$(h \star A) \cap (k \star A) = \emptyset \text{ for } 1 \leq h < k \leq t - h; \tag{16}$$

and

$$|h \star A| = \binom{m}{h} \text{ for } 1 \leq h \leq \left\lfloor \tfrac{t}{2} \right\rfloor. \tag{17}$$

The difference between independence and weak independence can be illustrated by the following examples in $G = \mathbb{Z}_{30}$: we see that $\mathrm{ind}(\{1, 2, 4, 8, 16\}) = 2$ (as $1 + 1 = 2$), and $\mathrm{wind}(\{1, 2, 4, 8, 16\}) = 3$ (we have $2 + 4 + 8 + 16 = 0$); but $\mathrm{ind}(\{1, 2, 4, 8\}) = 2$ still, yet $\mathrm{wind}(\{1, 2, 4, 8\}) = \infty$.

For a non-negative integer t, we let $w(G, t)$ denote the size of a maximum weakly t-independent set in G; we also set $w(G, \infty)$ to be the largest size of a subset A of G for which $\mathrm{wind}(A) = \infty$. It is easy to see that

$$w(G, 0) = n,$$

$$w(G, 1) = n - 1,$$

and

$$w(G, 2) = \frac{n + |\mathrm{Ord}(2)| - 2}{2};$$

the last equation results from the fact that no element of G, other than those of order 2, can be in a weakly 2-independent set together with its negative. On the other end, if the invariant factor decomposition of G contains s terms, then $w(G, \infty) \geq s$; in particular, if κ denotes the exponent of G, then

$$w(G, t) \geq w(G, \infty) \geq \frac{\log n}{\log \kappa}$$

holds for every t.

It is not hard to prove the following stronger result.

Theorem 18 *For $t \geq 2$ we have*

$$\left(\frac{t!}{2^t} n\right)^{1/t} - \frac{t}{2} < w(G, t) < \left(\left\lfloor \frac{t}{2} \right\rfloor ! n\right)^{1/\lfloor t/2 \rfloor} + \frac{t}{2}.$$

Proof. Let us first prove two claims.

Claim 1. Suppose that m is a positive integer for which

$$n > \sum_{h=1}^{t} \binom{2m-2}{h} + 1.$$

Then G has a weakly t-independent set of size m.

Proof of Claim 1. The proof will be similar (but simpler than) that of Proposition 16. We use induction on m. For $m = 1$ we have $n \geq 2$, and clearly $\{a\}$ is a weakly t-independent set in G whenever $a \neq 0$.

Assume now that our proposition holds for a positive integer m and suppose that

$$n > \sum_{h=1}^{t} \binom{2m}{h} + 1.$$

Since this value is greater than

$$\sum_{h=1}^{t} \binom{2m-2}{h} + 1,$$

our inductive hypothesis implies that G has a weakly t-independent set A of size m.

Define $B = A \cup (-A)$ and

$$\langle B, t \rangle^* = \bigcup_{h=1}^{t} h \star B.$$

Then $|\langle B, t \rangle^*| \leq \sum_{h=1}^{t} \binom{2m}{h}$. Therefore, we can choose an $a \in G \setminus \langle B, t \rangle^*$. Then clearly $a \notin A$, and, as in the proof of Proposition 16, we can show that $A \cup \{a\}$ is a weakly t-independent set of size $m+1$ in G.

Claim 2. Suppose that A is a weakly t-independent set in G of size m. Then

$$n \geq \sum_{h=1}^{\lfloor t/2 \rfloor} \binom{m}{h} + 1$$

.

Proof of Claim 2. Define

$$\langle A, \lfloor t/2 \rfloor \rangle^* = \bigcup_{h=1}^{\lfloor t/2 \rfloor} h \star A.$$

By (15), $0 \notin \langle A, \lfloor t/2 \rfloor \rangle^*$, so we have $n - 1 \geq |\langle A, \lfloor t/2 \rfloor \rangle^*|$. Furthermore, by conditions (16) and (17), we see that $\langle A, \lfloor t/2 \rfloor \rangle^*$ has size exactly

$$\sum_{h=1}^{\lfloor t/2 \rfloor} \binom{m}{h},$$

proving our Claim.

To derive our upper and lower bounds for $w(G,t)$, we use the (rather crude) estimates that for positive integers c and d we have

$$\frac{(d+2-c)^c}{c!} \leq \binom{d+1}{c} \leq \sum_{h=0}^{c} \binom{d}{h} \leq \binom{d+c}{c} \leq \frac{(d+c)^c}{c!}. \tag{18}$$

Namely, using Claim 1 and (18) for $d = 2m-2$ and $c = t$ we see that if

$$n > \frac{(2m-2+t)^t}{t!},$$

then G has a weakly t-independent set of size m, implying the lower bound

$$w(G,t) \geq \frac{(t!n)^{1/t} - t + 2}{2} - 1 = \left(\frac{t!}{2^t} n\right)^{1/t} - \frac{t}{2}.$$

The upper bound for $w(G,t)$ follows similarly from Claim 2 and (18). $\square$

Note that, for a fixed t, we have

$$\liminf w(G,t) = \infty$$

as $|G| = n$ approaches ∞, in contrast to

$$\liminf s(G,t) = 0$$

for each $t \geq 2$; in Section 1 we have seen that even

$$\liminf \{s(G,t) | \mathrm{Ord}(G,t) \neq G\} = O(1)$$

as $t \geq 4$. Thus t-independence and weak t-independence behave quite differently in abelian groups.

Acknowledgments

The values of $s(\mathbb{Z}_n, 4)$ and $s(\mathbb{Z}_n, 5)$ for $n \leq 200$, on which Conjecture 15 was based, were computed by Nick Laza; we thank him for his time and efforts.

References

[1] N. Alon and M. Dubiner. Zero-sum sets of prescribed size. In D. Miklós, V. T. Sós, and T. Szőnyi, editors, *Combinatorics, Paul Erdős is eighty*, Vol. 1., pages 33–50. Bolyai Society Mathematical Studies, Budapest, 1993.

[2] N. Alon and D. J. Kleitman. Sum-free subsets. In A. Baker, B. Bollobás, and A. Hajnal, editors, *A Tribute to Paul Erdős*, pages 13–26. Cambridge University Press, Cambridge, 1990.

[3] L. Babai and V. T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.*, 6/2:101–114, 1985.

[4] B. Bajnok. Constructions of spherical 3-designs. *Graphs Combin.*, 14/2:97–107, 1998.

[5] A. Baltz, T. Schoen, and A. Srivastav. Probabilistic construction of small strongly sum-free sets via large Sidon sets. *Colloq. Math.*, 86/2:171–176, 2000.

[6] T. Bier and A. Y. M. Chin. On (k,l)-sets in cyclic groups of odd prime order. *Bull. Austral. Math. Soc.*, 63/1:115–121, 2001.

[7] Y. Bilu. Sum-free sets and related sets. *Combinatorica*, 18/4:449–459, 1998.

[8] R. C. Bose and S. Chowla. Theorems in the additive theory of numbers. *Comment. Math. Helv.*, 37:141–147, 1962-63.

[9] N. J. Calkin and A. C. Taylor. Counting sets of integers, no k of which sum to another. *J. Number Theory.*, 57/2:323–327, 1996.

[10] P. J. Cameron and P. Erdős. Notes on sum-free and related sets. Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comp.*, 8/1-295–107, 1999.

[11] Y. Caro. Zero-sum subsequences in abelian non-cyclic groups. *Israel J. Math.*, 92/1-3:221–233, 1995.

[12] P. Erdős. Extremal problems in number theory. *Proc. Sympos. Pure Math.*, 8:181-189, Amer. Math. Soc., Providence, R.I., 1965.

[13] P. Erdős and R. Freud. A Sidon prowlémakör. *Mat. Lapok*, 1991/2:1–44, 1991.

[14] P. Erdős and H. Heilbronn. On the addition of residue classes mod p. *Acta Arith.*, 9:149–159, 1969.

[15] P. Erdős and P. Turán. On a problem of Sidon in additive number theory and some related problems. *J. London Math. Soc.*, 16:212–215, 1941.

[16] W. D. Gao and Y. O. Hamidoune. Zero sums in abelian groups. *Combin. Probab. Comp.*, 7/3:261–263, 1998.

[17] S. W. Graham. B_h sequences. In B. C. Berndt, H. G. Diamond, and A. J. Hildebrand, editors, *Analytic number theory, Vol.1. (Allerton Park, IL, 1995)*, pages 431-449, Progr. Math. 138, Birkhäuser Boston, Boston, MA, 1996.

[18] R. K. Guy. *Unsolved Problems in Number Theory*. Second edition. Springer-Verlag New York, 1994.

[19] H. Halberstam and K. F. Roth. *Sequences*. Second edition. Springer-Verlag New York – Berlin, 1983.

[20] G. Harcos and I. Ruzsa. A problem on zero subsums in abelian groups. *Period. Math. Hungar.*, 35/1-2:31–34, 1997.

[21] K. S. Kedlaya. Product-free subsets of groups. *Amer. Math. Monthly*, 105/10:900–906, 1998.

[22] K. S. Kedlaya. Large product-free subsets of finite groups. *J. Combin. Theory, Ser. A*, 77/2:339–343, 1997.

[23] J. Komlós, M. Sulyok, and E. Szemerédi. Linear problems in combinatorial number theory. *Acta Math. Acad. Sci. Hungar.*, 26:113–121, 1975.

[24] M. Kneser. Summenmengen in lokalkompakten abelschen Gruppen. *Math. Zeitschr.*, 66:88–110, 1956.

[25] M. B. Nathanson. N-graphs, modular Sidon and sum-free sets, and partition identities. *Ramanujan J.*, 4/1:59–67, 2000.

[26] I. Ruzsa. Solving linear equations in a set of integers I. *Acta Arith.*, 65/3:259–282, 1993.

[27] I. Ruzsa. Solving linear equations in a set of integers II. *Acta Arith.*, 72/4:385–397, 1995.

[28] T. Schoen. A note on the number of (k, l)-sum-free sets. *Electron. J. Combin.*, 7/1: Research Paper 30, 8pp (electronic), 2000.

[29] S. Sidon. Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen. *Math. Ann.*, 106:536–539, 1932.

[30] W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, *Lecture Notes in Mathematics*, Vol. 292, Part 3. Springer-Verlag, Berlin-New York, 1972.