On the Structure of Dissociated Sets in Cyclic Groups

Benjamin T. Shepard and Jacob E. Terkel

November 23, 2022

Abstract

A subset of a finite abelian group is dissociated if all of its subset sums are distinct. Recently, Bajnok proved that the maximum size of such a set in $\mathbb{Z}_n$ is $\lfloor \log_2 n \rfloor$. In this paper, we turn to the inverse problem of classifying the structure of dissociated subsets of this size when n is a power of two. We prove that a k-subset of $\mathbb{Z}_{2^k}$ is dissociated if and only if it is of the form $\{t_1, t_2 \cdot 2, \dots, t_k \cdot 2^{k-1}\}$ for some odd $t_1, \dots, t_k \in \mathbb{Z}_{2^k}$. This implies that there are $2^{(k^2-k)/2}$ dissociated subsets of maximum size in this group. Furthermore, we present an infinite family of cases that disagree with a previous conjecture made by Bajnok, and some other related results involving the dimension of a set.

1 Introduction

Let G be a finite abelian group of order n. When G is cyclic, we use the notation $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. We also let h be an arbitrary positive integer. Furthermore, we denote $\varphi(n)$ as the totient of n and $\text{ord}_n^\times(a)$ as the multiplicative order of a mod n. We will begin with some definitions.

Definition 1.1. Suppose that $A = \{a_1, \dots, a_m\} \subseteq G$. The quantity

$$h\hat{_\pm}A := \{\lambda_1 a_1 + \cdots + \lambda_m a_m \mid \lambda_i \in \{-1, 0, 1\},\ |\lambda_1| + \cdots + |\lambda_m| = h\}$$

is known as the *restricted h-fold signed sumset* of A.

When dealing with unsigned sums, we write $h\hat{}A$ instead. Note that these are both different from the so-called *h-fold dilation* of A, denoted by $h \cdot A = \{ha \mid a \in A\}$.

Definition 1.2. Let $A \subseteq G$ and define the sumset

$$\Sigma_\pm^\star A := \bigcup_{h=1}^{|A|} h\hat{_\pm}A.$$

We call A *dissociated* if $0 \notin \Sigma_\pm^\star A$. We call a dissociated set $\mathcal{M} \subseteq A$ *maximum* in A if there does not exist a dissociated subset $\mathcal{D} \subseteq A$ for which $|\mathcal{M}| < |\mathcal{D}|$.

This definition is equivalent to stating that the subset sums of A are distinct, i.e.

$$|\{a_1 + \cdots + a_k \mid a_i \in A,\, k \leq m\}| = \left| \bigcup_{h=0}^{|A|} h\hat{}A \right| = 2^{|A|}.$$

We will use these two definitions interchangeably. Dissociativity can also be thought of as the analogue of linear independence in abelian groups rather than vector spaces. In some cases, depending on the group, they can be thought of as equivalent concepts. In a vector space, linear independence and dimension are tied to the span of a set of vectors; likewise, dissociativity can give rise to analogous concepts of dimension and span in abelian groups.

Definition 1.3. Let $A \subseteq G$. The *dimension* of A in G is defined as

$$\dim A := \max\{|\mathcal{D}| \mid \mathcal{D} \subseteq A,\, 0 \notin \Sigma_{\pm}^{\star}\mathcal{D}\}.$$

In other words, $\mathcal{M} \subseteq A$ is maximum dissociated if and only if $\dim A = |\mathcal{M}|$.

Definition 1.4. Given a positive integer $m \leq n$, define

$$\dim(G, m) := \min\{\dim A \mid A \subseteq G,\, |A| = m\}.$$

That is, the minimum dimension of any subset of G with size m.

Note that since the only subset of G with size n is G itself, we have $\dim(G, n) = \dim G$. In 2018, Bajnok showed that the dimension of a group is bounded between a function of its order and the sum of the orders of its invariant factors. This implies equality in cyclic groups.

Theorem 1.5 (Bajnok [1]). Suppose that $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. Then we have

$$\lfloor \log_2 n_1 \rfloor + \cdots + \lfloor \log_2 n_r \rfloor \leq \dim G \leq \lfloor \log_2 n \rfloor.$$

Corollary 1.6. For all $n \in \mathbb{N}$, we have

$$\dim \mathbb{Z}_n = \lfloor \log_2 n \rfloor.$$

The last important fact that we will use is that $\dim(G, m)$ is monotone in m.

Lemma 1.7 (Shepard [2]). If $m_1 \leq m_2$ then

$$\dim(G, m_1) \leq \dim(G, m_2).$$

2 Main Results

2.1 A Classification of Dissociativity in Cyclic 2-Groups

In 2018, Bajnok [1] conjectured that every maximum dissociated subset of $\mathbb{Z}_{2^k}$ contains the element of order two, 2^{k-1}. Here we state the result as a theorem.

Theorem 2.1. Every maximum dissociated subset of $\mathbb{Z}_{2^k}$ contains the element 2^{k-1}.

Using this, we are able to obtain a complete classification of maximum dissociated subsets in this group, which is the main result of this section. It turns out that in fact, every maximum dissociated subset of $\mathbb{Z}_{2^k}$ contains an element of *every* possible order (except 1).

Theorem 2.2. A subset of $\mathbb{Z}_{2^k}$ is maximum dissociated if and only if it is of the form

$$\{t_1, t_2 \cdot 2, \ldots, t_k \cdot 2^{k-1}\}$$

for some odd $t_1, \ldots, t_k \in \mathbb{Z}_{2^k}$.

Corollary 2.3. There are exactly $2^{(k^2-k)/2}$ maximum dissociated subsets of $\mathbb{Z}_{2^k}$.

2.2 The Dimension of Cyclic Groups

As a more general version of Theorem 1.5, Bajnok [1] conjectured that

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 m \rfloor$$

for all $n \in \mathbb{N}$ and $m \leq n$. However, this was disproven [2], and the following table of values that are larger than the conjecture was presented:

G	m	$\dim(G, m)$	$\lfloor \log_2 m \rfloor$
$\mathbb{Z}_{17}$	$14, 15$	4	3
$\mathbb{Z}_{19}$	$14, 15$	4	3
$\mathbb{Z}_{22}$	15	4	3
$\mathbb{Z}_{23}$	$14, 15$	4	3
$\mathbb{Z}_{26}$	15	4	3
$\mathbb{Z}_{28}$	15	4	3
$\mathbb{Z}_{29}$	$14, 15$	4	3

Table 1: Values larger than the conjecture for $n < 30$.

Here, we aim to deal with some of these outstanding cases, as well as prove that the conjecture indeed holds for some particular values of m and n. We begin with the following, which provides an infinite family of counterexamples to the conjecture.

Theorem 2.4. If $n > 1$ is odd and m is at least

$$n - 2\frac{\varphi(n)}{\operatorname{ord}_n^\times(2)} + 1,$$

then

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 n \rfloor .$$

Corollary 2.5. If $k > 1$ is odd and m is at least

$$2k - 2\frac{\varphi(k)}{\operatorname{ord}_k^\times(2)} + 1,$$

then

$$\dim(\mathbb{Z}_{2k}, m) = \lfloor \log_2 2k \rfloor.$$

Note that Theorem 2.4 covers all odd values of n, whereas Corollary 2.5 covers only even values of n that are congruent to 2 mod 4.

These do not always give us a counterexample to the conjecture. However, when n is one more than a power of two, we can compute $\operatorname{ord}_n^\times(2) = 2k$, which gives us the following.

Corollary 2.6. Let $k \in \mathbb{N}$. If m is at least

$$2^k - \frac{\varphi(2^k+1)}{k} + 2,$$

then

$$\dim(\mathbb{Z}_{2^k+1}, m) = k.$$

Likewise, there is an even case that follows from this.

Corollary 2.7. Let $k \geq 2$. If m is at least

$$2^k - \frac{\varphi(2^{k-1}+1)}{k-1} + 3,$$

then

$$\dim(\mathbb{Z}_{2^k+2}, m) = k.$$

In each case, the number of counterexamples to the conjecture is unbounded. Let C_k be the number of counterexamples that Corollary 2.6 yields for a given k. Then

$$C_k = 2^k - \left(2^k - \frac{\varphi(2^k+1)}{k} + 2\right) = \frac{\varphi(2^k+1)}{k} - 2 \geq \frac{\sqrt{2^k+1}}{k} - 2.$$

Thus

$$\lim_{k\to\infty} C_k > \lim_{k\to\infty} \left(\frac{\sqrt{2^k+1}}{k} - 2\right)$$

which grows without bound. Furthermore, note that if m is a counterexample, $m < 2^k$ and

$$m \geq \left(2^k - \frac{\varphi(2^k+1)}{k} + 2\right) \geq \left(2^k - \frac{2^k}{k} + 2\right) > 2^{k-1}$$

so $2^{k-1} < m < 2^k$. Therefore,

$$\lfloor \log_2 m \rfloor = k - 1,$$

which implies

$$\dim(\mathbb{Z}_{2^k+1}, m) = k = \lfloor \log_2 m \rfloor + 1$$

and therefore each counterexample only yields a value of one larger than the conjecture. One can do a similar analysis for each of these observations in the context of Corollary 2.7.

It is also important to note that Theorem 2.4 and Corollary 2.5 give counterexamples besides those in Corollaries 2.6 and 2.7. For example, when $n = 2^k + 3$ or $n = 2^k + 5$.

k	$n = 2^k + 3$	C_k
8	259	8
10	1027	8
13	8195	12
14	16387	32
17	131075	4
19	524291	12
20	1048579	644
21	2097155	12

k	$n = 2^k + 5$	C_k
7	133	6
13	8197	6
14	16389	6
15	32773	42
16	65541	474
17	131077	10
19	524293	18
20	1048581	2

Table 2: Counterexamples that Corollary 2.6 yields for $n = 2^k + 3$ and $n = 2^k + 5$, for $k < 22$. Here, C_k denotes the number of m values that are counterexamples for a given k.

Moving on to cases that agree with the conjecture, we have the following.

Theorem 2.8. For all $n \in \mathbb{N}$ we have

$$\dim(\mathbb{Z}_n, n-1) = \lfloor \log_2(n-1) \rfloor .$$

We also can get an interesting upper bound involving subgroups, which turns out to be extremely useful in evaluating bounds for all types of groups.

Theorem 2.9. If H is a subgroup of G and $m \leq |H|$, then

$$\dim(G, m) \leq \dim(H, m).$$

This gives us an upper bound that agrees with the conjecture previously mentioned.

Corollary 2.10. If $d \geq m$ divides n, then

$$\dim(\mathbb{Z}_n, m) \leq \dim(\mathbb{Z}_d, m).$$

In particular, if m divides n, then

$$\dim(\mathbb{Z}_n, m) \leq \lfloor \log_2 m \rfloor .$$

Corollary 2.11. For all $k \in \mathbb{N}$ we have

$$\dim(\mathbb{Z}_{2^k}, m) \leq \lfloor \log_2 m \rfloor .$$

Finally, we have the following interesting results involving what elements the sumsets of a maximum dissociated set generate; these are closely related to so-called spanning sets.

Theorem 2.12. If $\mathcal{M}$ is maximum dissociated in $A \subseteq G$, then $A \cup (-A) \subseteq \Sigma_{\pm}^{\star}\mathcal{M}$.

Corollary 2.13. If $\mathcal{M}$ is maximum dissociated in G, then $\mathcal{M}$ spans $G \setminus \{0\}$.

The latter part of this statement is equivalent to asserting that $\Sigma_{\pm}^{\star}\mathcal{M} = G \setminus \{0\}$. This tells us that if a set is maximum dissociated in G, then its sumsets must generate the entire group besides 0 (which of course cannot be generated, by definition). Note that the converse of this statement is false; for example, the dissociated set $\{1, 2, 7\}$ spans $\mathbb{Z}_{19} \setminus \{0\}$.

3 Lemmas

This section contains all of the lemmas we will use to prove our main results.

Lemma 3.1. Let $A \subseteq G$ and let ϕ be an automorphism on G. The following are equivalent:

- A is dissociated;
- $\phi(A)$ is dissociated;
- $(A \setminus A_1) \cup (-A_1)$ is dissociated for all $A_1 \subseteq A$.

In particular, if A is dissociated, then so are $-A$ and $r \cdot A$ for all $r \in G$.

Proof. Suppose that A is dissociated. Note that if the set

$$(A \setminus \{a\}) \cup \{-a\}$$

is dissociated for all $a \in A$, then so is $f(A)$. Also, note that the only if directions follow from symmetry. Therefore, it suffices to prove that

(1) the set $(A \setminus \{a\}) \cup \{-a\}$ is dissociated, and

(2) the set $\phi(A)$ is dissociated.

For (1), let $a \in A$ and write $B = A \setminus \{a\}$. Then B is dissociated. If $a \in \Sigma^{\star}_{\pm}B$, then there is some $h_1 \in \mathbb{N}$ for which $a \in h_1 \hat{\pm} B$; then $a \in h_1 \hat{\pm} A$, and since $a \in A$ we have $0 \in (h_1 + 1)\hat{\pm} A$, a contradiction. Similarly, if $-a \in \Sigma^{\star}_{\pm}B$, then there is some $h_2 \in \mathbb{N}$ for which $-a \in h_2 \hat{\pm} B$; then $-a \in h_2 \hat{\pm} A$, and since $a \in A$ we have $0 \in (h_2 + 1)\hat{\pm} A$, a contradiction. Therefore, $\Sigma^{\star}_{\pm}B$ does not contain $\pm a$. This implies that $B \cup \{-a\}$ is dissociated, as claimed.

For (2), suppose there are $\lambda_1, \ldots, \lambda_i \in \{-1, 1\}$ and $a_1, \ldots, a_i \in A$ for which

$$\lambda_1 \phi(a_1) + \cdots + \lambda_i \phi(a_i) = 0.$$

Since ϕ is an automorphism, we have

$$\phi(\lambda_1 a_1 + \cdots + \lambda_i a_i) = 0$$

which implies that

$$\lambda_1 a_1 + \cdots + \lambda_i a_i = \phi^{-1}(0) = 0,$$

contradicting the fact that A is dissociated. $\blacksquare$

Lemma 3.2. If there are at least $n-m+1$ pairwise disjoint dissociated k-subsets of G, then

$$\dim(G, m) \geq k.$$

Proof. Let $\mathcal{D}_1, \dots, \mathcal{D}_{n-m+1}$ be pairwise disjoint dissociated k-subsets of G. Suppose indirectly that there is some $A \subseteq G$ with size m and $\dim A < k$. Then $\mathcal{D}_i \nsubseteq A$ for all i. Thus there is at least one element d_i from $\mathcal{D}_i$ for which $d_i \notin A$ for each i. Let

$$B = \bigcup_{i=1}^{n-m+1} \{d_i\}.$$

Then $B \cap A = \emptyset$ and we have

$$|B \cup A| = |B| + |A| = (n-m+1) + m = n+1,$$

a contradiction. ■

Lemma 3.3. Let $k = \lfloor \log_2 n \rfloor$. Then the set $\{1, 2, 4, \dots, 2^{k-1}\}$ is dissociated in $\mathbb{Z}_n$.

Proof. Suppose that there are weights $\lambda_1, \dots, \lambda_k \in \{-1, 0, 1\}$ for which

$$\lambda_1 + \lambda_2 \cdot 2 + \cdots + \lambda_k \cdot 2^{k-1} = 0. \tag{$*$}$$

Note that since

$$|\lambda_1 + \lambda_2 \cdot 2 + \cdots + \lambda_k \cdot 2^{k-1}| = |1 + 2 + \cdots + 2^{k-1}| = 2^k - 1 < 2^k = n,$$

equation $(*)$ must hold in $\mathbb{Z}$. Suppose indirectly that there is some $1 \leq i \leq k-1$ for which $\lambda_i \neq 0$, and let j be the smallest such index. Dividing $(*)$ in $\mathbb{Z}$ by $n = 2^k$, we obtain

$$\lambda_j + \lambda_{j+1} \cdot 2 + \cdots + \lambda_k \cdot 2^{k-1-j} = 0,$$

a contradiction since the left-hand side is odd. Hence, $\lambda_i = 0$ for all i, as claimed. ■

Lemma 3.4. For all $n \in \mathbb{N}$ we have

$$\dim(\mathbb{Z}_{2n}, n+m) \geq \dim(\mathbb{Z}_n, m) + 1.$$

Proof. Let $A \subseteq \mathbb{Z}_{2n}$ have size $n+m$ and set $\delta = \dim(\mathbb{Z}_n, m)$. We must prove $\dim A \geq \delta + 1$. By the pidgenhole principle, there must be m elements of A in the subgroup isomorphic to $\mathbb{Z}_n$. These m elements must be even in $\mathbb{Z}_{2n}$. Therefore, there is some m-subset $B \subseteq A$ that contains only even elements. By definition of δ, all m-subsets of $\mathbb{Z}_n$ have a dissociated δ-subset, so there is some dissociated δ-subset $\mathcal{D} \subseteq B$. Also, there is at least one odd element $t \in A$, since there are at most n even elements in $\mathbb{Z}_{2n}$ and $|A| > n$. Since every element of $\mathcal{D}$ is even, the set $\mathcal{D} \cup \{t\}$ is a dissociated $(\delta+1)$-subset of A, which implies that $\dim A \geq \delta + 1$. ■

Lemma 3.5. Suppose $\mathcal{D}$ is a dissociated subset of $A \subseteq G$ and let $x \in G \setminus \{0\}$. If $x \notin \Sigma^{\star}_{\pm}\mathcal{D}$, then $\mathcal{D} \cup \{x\}$ is dissociated. In particular, if $x \in A \setminus \mathcal{D}$, then $\mathcal{D}$ is not maximum in A.

Proof. Since $x \notin \Sigma^{\star}_{\pm}\mathcal{D}$, we have $-x \notin \Sigma^{\star}_{\pm}\mathcal{D}$. Suppose that there is some $h \in \mathbb{N}$ for which

$$0 \in h\hat{}_{\pm}(\mathcal{D} \cup \{x\}).$$

Then

$$\lambda_1 d_1 + \cdots + \lambda_{h-1} d_{h-1} \pm x = 0$$

for some weights $\lambda_i \in \{-1, 0, 1\}$ and elements $d_i \in \mathcal{D}$, and so

$$\lambda_1 d_1 + \cdots + \lambda_{h-1} d_{h-1} = \pm x.$$

However, $\pm x \notin \Sigma^{\star}_{\pm}\mathcal{D}$, a contradiction. ■

Lemma 3.6. Every maximum dissociated subset of $\mathbb{Z}_{2^k}$ contains 2^{k-1} if and only if

$$\dim(\mathbb{Z}_{2^k}, 2^k - 1) = k - 1$$

for all $k \in \mathbb{N}$.

Proof. For the if direction, note that

$$k - 1 = \dim(\mathbb{Z}_{2^k}, 2^{k-1}) \leq \dim(\mathbb{Z}_{2^k}, 2^k - 1) \leq \dim(\mathbb{Z}_{2^k}, 2^k) = k,$$

so suppose indirectly that

$$\dim(\mathbb{Z}_{2^k}, 2^k - 1) = k.$$

Then $\dim \mathbb{Z}_{2^k} \setminus \{a\} = k$ for all $a \in \mathbb{Z}_{2^k}$. In particular, there exists some dissociated k-subset $\mathcal{D}$ of $\mathbb{Z}_{2^k} \setminus \{a\}$, whence $a \notin \mathcal{D}$. However, for $a = 2^{k-1}$ we have $a \in \mathcal{D}$, a contradiction.

For the only if direction, let $\mathcal{D} \subseteq \mathbb{Z}_{2^k}$ be dissociated and have size k. Since

$$\dim(\mathbb{Z}_{2^k}, 2^k - 1) = k - 1,$$

there exists some $A = \mathbb{Z}_{2^k} \setminus \{v\}$ with $\dim A = k - 1$, where $v \in \mathbb{Z}_{2^k}$. Then every dissociated subset of A has size at most $k - 1$. By Lemma 3.1, the sets $\mathcal{D}$ and $-\mathcal{D}$ are dissociated and have size k, so we have $\pm\mathcal{D} \nsubseteq A$, which implies that $v \in \pm\mathcal{D}$. But then $v = -v$, so $\operatorname{ord}(v) = 2$. The only element of order 2 in $\mathbb{Z}_{2^k}$ is $v = 2^{k-1}$, which implies that $2^{k-1} \in \mathcal{D}$, as claimed. ■

4 Proofs

This section contains the proofs of our main results.

Proof of Theorem 2.1. Let A be a maximum dissociated subset of $\mathbb{Z}_{2^k}$. Then $|A| = k$, and since every subset sum of A must be distinct, we have

$$\left| \bigcup_{h=0}^{k} h\hat{\ }A \right| = 2^k,$$

which implies that every nonzero element of $\mathbb{Z}_{2^k}$ has a unique representation as the sum of distinct elements of A. Consider the element 2^{k-1} and in particular its unique representation

$$\lambda_1 a_1 + \cdots + \lambda_k a_k = 2^{k-1}$$

where $\lambda_i \in \{0, 1\}$ and $a_i \in A$. Choose some nonzero $a \in \{a_1, \ldots, a_k\}$ and set

$$\mathcal{S} = \bigcup_{h=1}^{k-1} h\hat{\ }(A \setminus \{a\}).$$

Note that $0 \notin \mathcal{S}$ since the set $A \setminus \{a\}$ is dissociated, which implies that $a \notin \mathcal{S} + a$. Also, $a \notin \mathcal{S}$, so $2^{k-1} \notin \mathcal{S}$. Therefore, the sets $\mathcal{S}$, $\mathcal{S} + a$, $\{a\}$, and $\{0\}$ are disjoint. Furthermore, note that

$$|\mathcal{S}| + |\mathcal{S} + a| + 2 = 2^k,$$

so we have the partition

$$\mathcal{S} \sqcup (\mathcal{S} + a) \sqcup \{a\} \sqcup \{0\} = \bigcup_{h=0}^{k} h\hat{\ }A.$$

The order of a is even, so suppose that $\operatorname{ord}(a) = 2u$. Then $2ua = 0$, so $\operatorname{ord}(ua) \leq 2$. This means that either $ua = 0$ or $ua = 2^{k-1}$, but since the former contradicts the minimality of $2u$, we must have $ua = 2^{k-1}$. It now suffices to prove that $u = 1$.

Suppose that u is even. Then $ua \neq a$, and by the above argument, $ua \neq 0$. If $ua \in \mathcal{S} + a$, then since u is even, $(u - r)a \in \mathcal{S}$ for all odd $r < u$, implying that $(u - (u - 1))a = a \in \mathcal{S}$, which is impossible. Using the partition, we now must have $ua = 2^{k-1} \in \mathcal{S}$, a contradiction. This implies that u is odd.

Since $\operatorname{ord}(a) \mid 2^k$, the order of a must be a power of two. Thus, either $u = 1$ or $u = 2^j$ for some $j \in \mathbb{N}$ — however, since u is odd, the latter is impossible and the result follows. ■

Proof of Theorem 2.2. Let $t_1, \dots, t_k$ be odd in $\mathbb{Z}_{2^k}$. We will first show that the set

$$\{t_1, t_2 \cdot 2, \dots, t_k \cdot 2^{k-1}\}$$

is maximum dissociated. Suppose that there are weights $\lambda_1, \dots, \lambda_k \in \{-1, 0, 1\}$ for which

$$\lambda_1 t_1 + \lambda_2 t \cdot 2 + \cdots + \lambda_k t_k \cdot 2^{k-1} = 0. \tag{$*$}$$

Note that (in $\mathbb{Z}$)

$$\lambda_1 t_1 + \lambda_2 t_2 \cdot 2 + \cdots + \lambda_k t_k \cdot 2^{k-1} = s \cdot 2^k$$

for some $s \in \mathbb{Z}$. Suppose indirectly that there is some $1 \le i \le k-1$ for which $\lambda_i \ne 0$, and let j be the smallest such index. Dividing $(*)$ by 2^i, we obtain

$$\lambda_j t_j + \lambda_{j+1} t_{j+1} \cdot 2 + \cdots + \lambda_k t_k \cdot 2^{k-1-j} = s \cdot 2^{k-i},$$

a contradiction since the left-hand side is odd. Hence, $\lambda_i = 0$ for all i, as claimed.

Now we will show that every maximum dissociated subset can be written as described. Let A be a maximum dissociated subset of $\mathbb{Z}_{2^k}$. By Theorem 2.1, we have $2^{k-1} \in A$. Define

$$\mathcal{D}_1 = 2 \cdot (A \setminus \{2^{k-1}\}) \cup \{1\} \quad \text{and} \quad \mathcal{D}_i = 2 \cdot (\mathcal{D}_{i-1} \setminus \{2^{k-1}\}) \cup \{1\}$$

for all $i \in \{2, \dots, k-1\}$. Note that $|\mathcal{D}_i| = k$. Since

$$\{0, 2^{k-1}\} \cap \Sigma^\star_\pm(\mathcal{D}_{i-1} \setminus \{2^{k-1}\}) = \emptyset,$$

$2 \cdot (\mathcal{D}_{i-1} \setminus \{2^{k-1}\})$ is dissociated, and it contains only even elements, so $\mathcal{D}_i$ is also dissociated. Therefore, by Theorem 2.1, we have $2^{k-1} \in \mathcal{D}_i$. Note that every element of $\mathcal{D}_i$ that is divisible by 2^i is of the form $a \cdot 2^i$ where $a \in A$. Thus there is some $a \in A$ for which $a \cdot 2^i = 2^{k-1}$. This implies that $a = t \cdot 2^{k-i-1}$ for some odd $t \in \mathbb{Z}_{2^k}$. Hence

$$a \cdot 2^{i+1} = t \cdot 2^{k-i-1} \cdot 2^{i+1} = t \cdot 2^k = 0$$

so $\operatorname{ord}(a) = 2^{i+1}$. Thus for all $i \in \{1, \dots, k-1\}$, there exists an element in A of order 2^{i+1}. Therefore, A contains one element of each possible order except 1, and the result follows. ∎

Proof of Corollary 2.3. Note that for each $i \in \{1, \dots, k-1\}$, there are exactly 2^{i+1} elements with order 2^i. Thus, the number of subsets of $\mathbb{Z}_{2^k}$ where all elements have distinct orders is

$$\prod_{i=1}^{k-1} 2^i = 2^{(k^2-k)/2}.$$

The claim now follows from Theorem 2.2. ∎

Proof of Theorem 2.4. Let $L = \lfloor \log_2 n \rfloor$ and set

$$\alpha = \frac{\varphi(n)}{\operatorname{ord}_n^\times(2)}.$$

Since L is an upper bound, it suffices to prove that

$$\dim(\mathbb{Z}_n, n - 2\alpha + 1) \geq L.$$

According to Lemma 3.2, it suffices to find at least

$$n - (n - 2\alpha + 2) + 1 = 2\alpha$$

pairwise disjoint dissociated L-subsets of $\mathbb{Z}_n$. By Lemmas 3.3 and 3.1, the sets

$$A = \{1, 2, 4, \dots, 2^{L-1}\}$$

and $-A$ are dissociated and disjoint. Consider the group of units $\mathbb{Z}_n^\times$. Since n is odd, we have $\langle 2 \rangle \leq \mathbb{Z}_n^\times$ and $A, -A \subset \langle 2 \rangle$. If $r \cdot \langle 2 \rangle$ is any nonzero coset, then the sets $r \cdot A$ and $r \cdot (-A)$ are subsets of $r \cdot \langle 2 \rangle$, are disjoint, and are dissociated by Lemma 3.1. Now, note that

$$[\mathbb{Z}_n^\times : \langle 2 \rangle] = \frac{|\mathbb{Z}_n^\times|}{|\langle 2 \rangle|} = \frac{\varphi(n)}{\operatorname{ord}_n^\times(2)} = \alpha,$$

so there are α nonzero cosets of $\langle 2 \rangle$. Using the fact that cosets are disjoint, this implies that there are at least α nonzero integers $r_1, \dots, r_\alpha$ such that the 2α subsets

$$r_1 \cdot A,\ r_1 \cdot (-A), \dots,\ r_\alpha \cdot A,\ r_\alpha \cdot (-A)$$

are dissociated and pairwise disjoint, as desired. ■

Proof of Corollary 2.5. By Lemma 3.4, for all odd $k \in \mathbb{N}$ we have

$$\dim\left(\mathbb{Z}_{2k},\ 2k - 2\frac{\varphi(k)}{\operatorname{ord}_n^\times(2)} + 1\right) \geq \dim\left(\mathbb{Z}_k,\ k - 2\frac{\varphi(k)}{\operatorname{ord}_n^\times(2)} + 1\right) + 1.$$

By Theorem 2.4, this implies

$$\dim\left(\mathbb{Z}_{2k},\ 2k - 2\frac{\varphi(k)}{\operatorname{ord}_n^\times(2)} + 1\right) \geq \lfloor \log_2 k \rfloor + 1 = \lfloor \log_2 2k \rfloor.$$

Since the upper bound follows clearly from Lemma 1.7, we are done. ■

Proof of Theorem 2.8. When n is a power of two, the result follows from Theorem 2.1 and Lemma 3.6. Suppose now that n is not a power of two. Note that in this case we then have $\lfloor \log_2 n \rfloor = \lfloor \log_2 (n-1) \rfloor$. Let $k = \lfloor \log_2 n \rfloor$. The upper bound is easily seen to be true since

$$\dim(\mathbb{Z}_n, n-1) \leq \dim \mathbb{Z}_n = k.$$

Let $B = \mathbb{Z}_n \setminus \{b\}$ for some $b \in \mathbb{Z}_n$ and suppose indirectly that $\dim B = k-1$. Let $\mathcal{D} \subseteq \mathbb{Z}_n$ be dissociated and have size k. By Lemma 3.1, the set $-\mathcal{D}$ is also dissociated. If it is the case that $|-\mathcal{D}| < k$, then we must have

$$\mathcal{D} \cap -\mathcal{D} \neq \emptyset,$$

so there is some $a \in \mathbb{Z}_n$ for which $a \in \pm\mathcal{D}$. This implies $a = -a$, so $\operatorname{ord}(a) = 2$. Otherwise, $|-\mathcal{D}| = k$, so we must have $\pm\mathcal{D} \nsubseteq B$, which implies $b \in \pm\mathcal{D}$ and $\operatorname{ord}(b) = 2$. In either case, $\mathcal{D}$ contains an element of order two. But since n is not a power of two, the dissociated set

$$\{1, 2, 4, \ldots, 2^{k-1}\}$$

does not contain an element of order two, a contradiction. ■

Proof of Theorem 2.9. Let $f : H \to G$ be an injective homomorphism and suppose that $A \subseteq H$ has minimum dimension. By the First Isomorphism Theorem, $H \cong f(G)$. Thus

$$\dim A = \dim f(A)$$

which implies

$$\dim(G, m) \leq \dim f(A) = \dim A = \dim(H, m),$$

as desired. ■

Proof of Corollary 2.10. Since $d \mid n$, we know that $\mathbb{Z}_d$ is a subgroup of $\mathbb{Z}_n$. Since $m \leq d$, by Lemma 1.7 and Theorem 2.9 we obtain

$$\dim(\mathbb{Z}_n, m) \leq \dim(\mathbb{Z}_n, d) \leq \dim(\mathbb{Z}_d, d) = \dim \mathbb{Z}_d = \lfloor \log_2 d \rfloor,$$

as desired. ■

Proof of Corollary 2.11. By Corollary 2.10, for all $\ell \in \{0, \ldots, k\}$ we have

$$\dim(\mathbb{Z}_{2^k}, 2^\ell) \leq \ell.$$

Thus, by Lemma 1.7, it suffices to prove the case $m = 2^\ell - 1$ for all $\ell \in \{1, \dots, k\}$. Let

$$A = 2^{k-\ell} \cdot (\mathbb{Z}_{2^\ell} \setminus \{2^{\ell-1}\}).$$

Then $|A| = 2^\ell - 1$ and $\dim A = \dim \mathbb{Z}_{2^\ell} \setminus \{2^{\ell-1}\}$, which by Theorem 2.1 is $\ell - 1$. Therefore,

$$\dim(\mathbb{Z}_{2^k}, 2^\ell - 1) \leq \ell - 1,$$

as needed. ■

Proof of Theorem 2.12. Suppose that there is some $x \in \pm A$ for which $x \notin \Sigma^\star_\pm \mathcal{M}$. Then $x \notin \mathcal{M}$. If $x \in A$ then by Lemma 3.5, the set $\mathcal{M} \cup \{x\}$ is dissociated, which contradicts $\mathcal{M}$ being maximum in A. Otherwise, we have $x \in -A$. By Lemma 3.1, $-\mathcal{M}$ is dissociated; note that it is also maximum in $-A$. Since $\Sigma^\star_\pm \mathcal{M} = \Sigma^\star_\pm(-\mathcal{M})$, by Lemma 3.5, the set $-\mathcal{M} \cup \{x\}$ is dissociated, which is again a contradiction. ■

5 Conclusion

There are still many open questions regarding dissociated sets. Now that we have given a complete classification of maximum dissociated subsets in cyclic 2-groups, we turn to the question of doing so in general cyclic groups.

Problem 5.1. Classify all maximum dissociated subsets of the cyclic group $\mathbb{Z}_n$.

Problem 5.2. Find the number of maximum dissociated subsets in $\mathbb{Z}_n$.

For a loose upper bound, note that the number of subsets of $\mathbb{Z}_n$ of size $\lfloor \log_2 n \rfloor$ that do not contain 0 is

$$\binom{n-1}{\lfloor \log_2 n \rfloor},$$

so the number of maximum dissociated subsets must be at most this quantity.

Additionally, we would like to further understand the counterexamples to the conjecture given in Theorem 2.4 and Corollary 2.5.

Question 5.3. What is the least positive integer m for which

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 n \rfloor?$$

Currently, the least positive integer that satisfies this condition that we know of is

$$n - 2\frac{\varphi(n)}{\mathrm{ord}_n^\times(2)} + 1$$

for odd n, but it is likely that there are lower values of m that also work.

Recall that every counterexample presented in Theorem 2.4 and Corollary 2.5 yielded a value one greater than the conjecture, i.e.

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 m \rfloor + 1.$$

We wish to find a counterexample that yields a value of more than one greater, if possible.

Problem 5.4. Find (or disprove the existence of) positive integers n and m for which

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 m \rfloor + 2.$$

We would also like to obtain a general lower bound for all n and m, which we still believe to be true, but have not made any progress towards proving.

Conjecture 5.5. For all $n \in \mathbb{N}$ and $m \leq n$ we have

$$\dim(\mathbb{Z}_n, m) \geq \lfloor \log_2 m \rfloor .$$

A related problem is to understand when the conjecture is actually true.

Question 5.6. For what values of n and m is it true that

$$\dim(\mathbb{Z}_n, m) = \lfloor \log_2 m \rfloor ?$$

Currently, we know that this holds for all $n \in \mathbb{N}$ when $m = n$ (by Theorem 1.6) and when $m = n - 1$ (by Theorem 2.8). We believe it to still be true in cyclic 2-groups for all m.

Conjecture 5.7. For all $k \in \mathbb{N}$ we have

$$\dim(\mathbb{Z}_{2^k}, m) = \lfloor \log_2 m \rfloor .$$

Note that by Lemma 1.7 and Corollary 2.11, it suffices to prove that

$$\dim(\mathbb{Z}_{2^k}, 2^\ell) \geq \ell \;\text{ and }\; \dim(\mathbb{Z}_{2^k}, 2^\ell - 1) \geq \ell - 1$$

for all $\ell \leq k$. This seems feasible.

Acknowledgements. The authors would like to thank Dr. Béla Bajnok for his guidance and support throughout the duration of this research.

References

[1] B. Bajnok. *Additive Combinatorics: A Menu of Research Problems.* CRC Press, 2018.

[2] B. Shepard. “Maximal Dissociated Subsets of Finite Abelian Groups”. In: *Research Papers in Mathematics, Gettysburg College* 23 (2021).