Maximal Dissociated Subsets of Finite Abelian Groups

Benjamin T. Shepard

Department of Mathematics, Gettysburg College
E-mail: shepbe01@gettysburg.edu

May 12, 2021

Abstract

A subset A of an abelian group G is said to be dissociated if $0 \in G$ cannot be written as the signed sum of any of the elements of A. Furthermore, the dissociativity dimension of a set A, denoted $\dim A$, is the maximum size of a dissociated subset of A. We are interested in evaluating the function $\dim(G, m)$, which yields the minimum value of $\dim A$ when $A \subseteq G$ has size m. Here, we provide some basic values and bounds for this function, and evaluate it for certain elementary abelian p-groups. In particular, we obtain exact values when the lower bound is sharp for $p = 2$ and $p = 3$. We also disprove a conjecture made by B. Bajnok in 2018 regarding the exact value for cyclic groups.

1 Introduction

In this paper, we will refer to G as an arbitrary finite abelian group, and κ as its exponent. We will also let m be a positive integer. We begin with some definitions.

Definition 1. *Let G be a group. A subset $A = \{a_1, \ldots, a_m\} \subseteq G$ is dissociated if every possible equality of the form*

$$\sum_{i=1}^{m} \lambda_i a_i = 0,$$

where $\lambda_i \in \{-1, 0, 1\}$, implies that $\lambda_i = 0$ for all i. We usually denote the set of all possible sums as defined above by ΣA, and write $0 \notin \Sigma A$ if A is dissociated.

Dissociated subsets of a group have been investigated, however there is an interest in finding dissociated subsets of any subset of a group. For this, we define

Definition 2. *Let A be a subset of a group G. The quantity*

$$\dim A := \max\{|D| \mid D \subseteq A,\ D \text{ is dissociated}\}$$

is known as the dissociativity dimension of A in G.

Throughout this paper, we refer to $\dim A$ as simply the dimension of A. Finally, we will define the main function that we are interested in investigating.

Definition 3. *Let G be a group of order n, and $m \leq n$ be a positive integer. Define*

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

that is, the minimum dissociativity dimension of any subset of G of size m.

2 Previous results

We currently have the following:

Theorem 4 (**Lev and Luster, 2011; [1]**)**.** *For any $A \subseteq G$, we have*

$$r_A \leq \dim A \leq \lfloor r_A \cdot \log_2 \kappa \rfloor$$

where r_A is the rank of the subgroup $\langle A \rangle$ generated by A.

Proposition 5 (**Bajnok, 2018; [2]**)**.** *If G is of type $n_1, \ldots, n_r$ and order n, then*

$$\lfloor \log_2 n_1 \rfloor + \ldots + \lfloor \log_2 n_r \rfloor \leq \dim(G, n) \leq \lfloor \log_2 n \rfloor.$$

In particular, for all positive integers n, we have

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

Proposition 6 (**Bajnok, 2018; [2]**)**.** *For all groups G, we have* $\dim(G, 1) = 0$, $\dim(G, 2) = 1$, *and*

$$\dim(G, 3) = \begin{cases} 1 & \text{if } \kappa \geq 3; \\ 2 & \text{if } \kappa = 2. \end{cases}$$

3 Main results

We first evaluate the cases of $m = 4$ and $m = 5$ for all groups G in order to obtain an extension of Proposition 6.

Proposition 7. *For all G, we have*

$$\dim(G, 4) = 2$$

and

$$\dim(G, 5) = \begin{cases} 2 & \text{if } \kappa \geq 3; \\ 3 & \text{if } \kappa = 2. \end{cases}$$

Proof. When $\kappa = 2$, both claims follow from Theorem 14. Therefore, assume $\kappa \geq 3$. For $m = 4$, let

$$A = \{0, g_1, -g_1, g_2\}$$

such that $g_1, -g_1$, and g_2 are all nonzero and distinct. For $m = 5$, a non-boolean abelian group G of order at least 5 contains at least two elements $g_1, g_2 \in G$ such that $g_1, g_2 \neq 0, -g_1, -g_2$, so we can let

$$A_1 = A \cup \{-g_2\}$$

such that $A \cap \{-g_2\} = \emptyset$. Clearly both A and A_1 do not have a dissociated subset of size 3, so $\dim A \geq 2$ and $\dim A_1 \geq 2$. In both A and A_1, one can easily see that $0 \notin \Sigma\{g_1, g_2\}$, so $\dim A = \dim A_1 = 2$.

Since only subsets of a set of the form $\{0, g_1, -g_1\}$ have dimension less than 2, we have $\dim(G, 4) = \dim(G, 5) = 2$ as claimed. ■

We also introduce several bounds. This first proposition states that the dimension function is monotonically increasing over m, which is an important fact that will be used later.

Proposition 8. *If m_1 and m_2 are positive integers such that $m_1 \geq m_2$, then*

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

Proof. For simplicity, let $\delta_1 = \dim(G, m_1)$ and $\delta_2 = \dim(G, m_2)$. We must prove that every subset of G of size m_1 has dimension at least δ_2. Let $A \subseteq G$ be arbitrary and of size m_1. Since $|A| \geq m_2$, A contains at least one subset B of size m_2. By definition of δ_2, every subset of G of size m_2 has dimension at least δ_2, so $\dim B \geq \delta_2$. Thus B contains a dissociated subset D of size δ_2, and $B \subseteq A$, so we have $D \subseteq A$. By definition of dimension, $\dim A \geq |D| = \delta_2$ as claimed. ∎

Proposition 9. *For all G of order n, and all $m \leq n$, we have*

$$\dim(G, m) \leq \lfloor \log_2 n \rfloor.$$

Proof. By Proposition 5, $\dim(G, n) \leq \lfloor \log_2 n \rfloor$. Using Proposition 8, we obtain

$$\dim(G, m) \leq \dim(G, n) \leq \lfloor \log_2 m \rfloor$$

as claimed. ∎

Proposition 10. *For all m, and all G for which $|\mathrm{Ord}(G, 2)| < m/2$, we have*

$$\dim(G, m) \leq \left\lfloor \frac{m}{2} \right\rfloor.$$

Proof. Let $k = \lfloor \frac{m}{2} \rfloor$. If m is even, then $m = 2k$; if m is odd, then $m = 2k + 1$. Since less than $m/2$ elements in G have order 2, we may let

$$A = \{0\} \cup \bigcup_{i=1}^{k} \{a_i, -a_i\} \subset G$$

such that $a_i \neq -a_i \neq 0$ for all i and

$$\{a_i, -a_i\} \cap \{a_j, -a_j\} = \emptyset$$

for all $i \neq j$. If m is even, take A without $-a_k$. In either case, $|A| = m$.

Suppose that there exists a dissociated subset $D \subset A$ such that $|D| > k$. Since the smallest possible size of D is $k + 1$, if we choose $k + 1$ elements of A, we are forced to choose either 0 or both a_i and $-a_i$ for some $i \in \{1, \ldots, k\}$. In either case, $0 \in \Sigma D$, so we must have $|D| \leq k$, a contradiction. Therefore, $\dim A \leq k$, which directly implies that $\dim(G, m) \leq k$ as claimed. ∎

Note that these bounds are not generally sharp. For large m, Proposition 9 is better, but note that it is in terms of n, which loosens the bound.

In the next theorem, we introduce a lower bound for all G and m. First, we have a useful fact that assists with this theorem.

Lemma 11. *If G has invariant factorization*

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

then the group

$$H = \mathbb{Z}_{n_{r-k+1}} \times \cdots \times \mathbb{Z}_{n_r}$$

is the largest subgroup of G with rank k.

We will not provide a proof for this lemma here. However, it allows us to obtain the following result:

Theorem 12. *Suppose that G has invariant factorization*

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}.$$

Then for all m we have

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

for the unique k such that

$$\prod_{i=r}^{r-k+2} n_i < m \leq \prod_{i=r}^{r-k+1} n_i.$$

Proof. Let $A \subseteq G$ have size m. Since

$$\prod_{i=r}^{r-k+2} n_i < m,$$

the size of A is strictly greater than that of the subgroup

$$\mathbb{Z}_{n_{r-k+2}} \times \cdots \times \mathbb{Z}_{n_r}.$$

By Lemma 11, this is the largest subgroup of G with rank $k-1$. Therefore, $\langle A \rangle$ has rank $r_A \geq k$. Now from Theorem 4 we have $\dim A \geq k$, and the claim follows. ■

From this we immediately obtain

Corollary 13. *For all positive integers k and r, we have*

$$\dim(\mathbb{Z}_k^r, m) \geq \lceil \log_k m \rceil.$$

Proof. Since $k^{i-1} < m \leq k^i$ for some $i \in \{1, \ldots, r\}$, we have $i \geq \lceil \log_k m \rceil$. The claim now follows from Theorem 12. ∎

It should be noted that for $k > 3$, equality does not generally hold. For example, it is an immediate consequence from Theorem 4 that

$$\dim(\mathbb{Z}_k^r, k^r) \geq kr$$

for all r and $k \geq 4$, which is larger than the lower bound of r given here. We do not currently know much about other values of m.

It turns out that the bound in Corollary 13 is sharp for certain elementary abelian p-groups; in particular, $p = 2$ and $p = 3$. We obtain both

Theorem 14. *For all positive integers r and $m \leq 2^r$, we have*

$$\dim(\mathbb{Z}_2^r, m) = \lceil \log_2 m \rceil.$$

and

Theorem 15. *For all positive integers r and $m \leq 3^r$, we have*

$$\dim(\mathbb{Z}_3^r, m) = \lceil \log_3 m \rceil.$$

The proofs of Theorems 14 and 15 are similar, so here we prove both using a general construction.

Proof. Let $p \in \{2, 3\}$. Since p is prime, $\mathbb{Z}_p$ is a field and $\mathbb{Z}_p^r$ forms a vector space over $\mathbb{Z}_p$. Recall that for any $A \subseteq \mathbb{Z}_p^r$, the coefficients of sums in ΣA are given by $\lambda_i = \{0, 1, -1\}$. The scalars in $\mathbb{Z}_3^r$ are exactly λ_i. Also, since each element of $\mathbb{Z}_2^r$ is its own inverse, for $p = 2$ we only need to consider $\lambda_i = \{0, 1\}$, which are exactly the scalars in $\mathbb{Z}_2^r$. Therefore, for any $X \subseteq \mathbb{Z}_p^r$, we have an equivalence: X is dissociated if and only if the vectors in X are linearly independent.

We now use Proposition 8 to narrow down the cases; it suffices to prove that $\dim(\mathbb{Z}_p^r, p^k) = k$ and $\dim(\mathbb{Z}_p^r, p^k + 1) = k + 1$ for all positive integers $k \leq r$.

First, let $m = p^k$. From Theorem 13, we have $\dim(\mathbb{Z}_p^r, p^k) \geq k$, so it suffices to show the existence of subset of $\mathbb{Z}_p^r$ of size p^k and dimension k. Let

$$A = \{0\}^{r-k} \times \mathbb{Z}_p^k.$$

It is clear to see that $\dim A = \dim \mathbb{Z}_p^k$. Now, it is a well known fact that if a vector space V is spanned by k vectors, and $l > k$, then any set of l vectors in V is linearly dependent. Since the standard basis for $\mathbb{Z}_p^k$,

$$\mathcal{B} = \{(e_1, \ldots, e_k) \mid e_i = 1 \text{ for some } i \in \{1, \ldots, k\},\, e_j = 0 \text{ for } j \neq i\},$$

spans $\mathbb{Z}_p^k$ and has size k, any subset of $\mathbb{Z}_p^k$ must have size at most k to be dissociated. It is clear that $0 \notin \Sigma\mathcal{B}$ since $\mathcal{B}$ is linearly independent, so $\dim \mathbb{Z}_p^k = k$. Therefore, we obtain $\dim A = k$ as desired.

Now let $m = p^k + 1$. Theorem 13 yields $\dim(\mathbb{Z}_p^r, p^k + 1) \geq k + 1$, so it again suffices to show existence of a subset of $\mathbb{Z}_p^r$ of size $p^k + 1$ with dimension $k + 1$. Write

$$A_0 = A \cup \mathcal{B}_0$$

where

$$\mathcal{B}_0 = \{1\} \times \{0\}^{r-1}.$$

Since $\mathcal{B} \cap \mathcal{B}_0 = \emptyset$, the set

$$(\{0\}^{r-k} \times \mathcal{B}) \cup \mathcal{B}_0 \subset A_0$$

has size $k + 1$ and is clearly dissociated.

Now, suppose that there exists a dissociated subset $D \subset A_0$ with $|D| > k + 1$. Since $\dim A = k$, D cannot contain more than k elements of A. But since we have $|A_0| = k + 1$, it is impossible to put two more elements of A_0 into D. Hence $|D| \leq k + 1$, a contradiction. From this, we obtain $\dim A_0 = k + 1$ as desired. ■

This proof does not work for $p \geq 5$; even though $\mathbb{Z}_p^r$ is a vector space for all values of p, the only groups where equivalence holds between dissociativity and linear independence are $\mathbb{Z}_2^r$ and $\mathbb{Z}_3^r$.

Using Proposition 5, we can easily get equality for a few related groups when m is of maximum size.

Proposition 16. *For all positive integers r and k, we have*

$$\dim(\mathbb{Z}_2^r \times \mathbb{Z}_{2k}, 2^{r+1}k) = \lfloor \log_2 2^{r+1}k \rfloor.$$

Proof. From Proposition 5, we have

$$r + \lfloor \log_2 2k \rfloor \leq \dim(\mathbb{Z}_2^r \times \mathbb{Z}_{2k}, k2^{r+1}) \leq \lfloor \log_2 k2^{r+1} \rfloor.$$

Since clearly

$$r + \lfloor \log_2 2k \rfloor = r + 1 + \lfloor \log_2 k \rfloor$$

and

$$\lfloor \log_2 k2^{r+1} \rfloor = \lfloor \log_2 2^r \cdot 2 \rfloor + \lfloor \log_2 k \rfloor = r + 1 + \lfloor \log_2 k \rfloor,$$

the bounds are equal and equality holds. ∎

We now move on to cyclic groups $\mathbb{Z}_n$. In [2], B. Bajnok conjectured that for all positive integers n and $m \leq n$, the following equality holds:

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

Using the code provided by Francis in [3], we have the following table of values that disagree with this conjecture:

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.

All other groups below $n = 30$ agree exactly for all values of m. In light of these results, I believe that the lower bound still holds.

I propose the following more modest conjecture:

Conjecture 17. *For all positive integers n and $m \leq n$, we have*

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

I also believe that powers of two agree with Bajnok's conjecture.

Conjecture 18. *For all positive integers n and $m \leq n$, we have*

$$\dim(\mathbb{Z}_n, 2^k) = k.$$

It may also be more feasible to consider specific cyclic groups. For instance, the case when n is a power of two may be of particular interest.

4 Future work

Future projects should explore the validity of Conjectures 17 and 18. Additionally, since the upper bounds of Proposition 10 and 9 are not always sharp, future work should look into the possibility of improving these bounds.

Furthermore, since Corollary 13 is only sharp for $k = 2$ and $k = 3$, future work should attempt to improve the lower bound for $k \geq 4$, and possibly other elementary abelian p-groups for $p \geq 5$.

Acknowledgments. I would like to thank Dr. Bela Bajnok for his guidance throughout the duration of this research. I would also like to thank Peter Francis, for providing the code used to generate the cyclic group table (among many others), and Matt Torrence, for his general help throughout the semester. Finally, I would like to thank Dr. Michael Shepard for his contribution to a separate program for evaluating cyclic groups.

References

[1] V. Lev and R. Yuster. "On the Size of Dissociated Bases". In: *The Electronic Journal of Combinatorics* 18 (2011). DOI: `https://doi.org/10.37236/604`.

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

[3] Peter E. Francis. *Personal Communication.* URL: `https://bit.ly/3gJpzVf`.