Characterising bimodal collections of sets in finite groups

Sophie Huczynska*and Maura B. Paterson†

June 10, 2019

Abstract

A collection of disjoint subsets $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of a finite abelian group has the *bimodal* property if each non-zero group element δ either never occurs as a difference between an element of A_i and an element of A_j with $j \neq i$, or else for every element a_i in A_i there is an element $a_j \in A_j$ for some $j \neq i$ with $a_i - a_j = \delta$. This property arises in familiar situations, such as cosets of a fixed subgroup or in a group partition, and has applications to the construction of optimal algebraic manipulation detection codes. In this paper, we obtain a structural characterisation for bimodal collections of sets.

1 Introduction

Let G be a finite abelian group of order n, written additively, with identity 0. Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a collection of disjoint subsets of G. Then $\mathcal{A}$ is said to have the *bimodal property* if, for any non-identity element δ of G, either δ *never* occurs as a difference between an element of A_i and an element of some other set A_j, or else for *every* element a_i in A_i there is an element $a_j \in A_j$ for some $j \neq i$ such that $a_i - a_j = \delta$.

Let $k_i = |A_i|$ for $i = 1, 2, \ldots, m$. For each $\delta \in G \setminus \{0\}$, we let $N_i(\delta) = \Big|\{(a_i, a_j) \mid a_i \in A_i,\ a_j \in \cup_{i \neq h} A_h,\ a_i - a_j = \delta\}\Big|$. Then $\mathcal{A}$ has the bimodal property if $N_i(\delta) \in \{0, k_i\}$ for $i = 1, 2, \ldots, m$.

Although this property occurs in some familiar settings, it seems it has not received prior attention. It has applications to cryptography, having been defined by Huczynska and Paterson [4] in the context of studying optimal Algebraic Manipulation Detection (AMD) codes [1, 5]. Perhaps the most natural occurrence of this property is as follows:

*School of Mathematics and Statistics, University of St Andrews, UK. sh70@st-andrews.ac.uk

†Department of Economics, Mathematics and Statistics, Birkbeck, University of London. m.paterson@bbk.ac.uk

Lemma 1.1. *Let H be a subgroup of an abelian group G. If $\mathcal{C} = \{C_1, \ldots, C_m\}$ is a collection of cosets of H, then $\mathcal{C}$ has the bimodal property.*

Proof. For fixed i and $1 \leq j \leq m$ with $i \neq j$, the sets $C_i - C_j$ comprise $m-1$ distinct cosets of H. For any $\delta \in C_i - C_j$ and every $x \in C_i$ there exists a unique $y \in C_j$ such that $x - y = \delta$. For any $\delta \in G \setminus \cup_{j \neq i}(C_i - C_j)$, the element δ occurs zero times as a difference out of C_i. □

One might suspect that all bimodal collections of sets arise in this way. However, we shall see a much richer structure is possible.

2 Tools and Constructions

The bimodal property is defined in terms of differences between elements lying in distinct members of a collection $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of disjoint subsets of a group G (*external* differences). Let $A = \bigcup_{i=1}^{m} A_i$, and for j with $1 \leq j \leq m$ let $B_j = A \setminus A_j$. So for each $1 \leq j \leq m$, $A = A_j \sqcup B_j$ (where the notation $S \sqcup T$ denotes the union of disjoint sets S and T). We set $N_j(\delta) = |\{(a, b) : \delta = a - b,\ a \in A_j,\ b \in B_j\}|$. We refer to differences between elements of the same subset as *internal* differences.

Definition 2.1. Let A_i be a subset of a finite abelian group G. We define the *internal difference group* H_i of A_i to be the subgroup of G generated by all elements of the form $x - y$ with $x, y \in A_i$.

For the collection $\mathcal{C}$ of Lemma 1.1 we have $H_i = H$ for each set $C_i \in \mathcal{C}$.

Remark 2.2. The group H_i has the property that A_i is contained in a single coset of H_i, and is the smallest subgroup of G with this property. In the case where $|A_i| = 1$, the group $H_i = \{0\}$ and its cosets are the singleton sets.

We will view singleton sets as cosets of the identity subgroup. For any element $a \in A_i$ we have that $a + H_i$ is the coset of H_i containing A_i. In what follows we will select an arbitrary element $a_i \in A_i$ for $i = 1, 2, \ldots, m$ and represent the coset of H_i containing A_i by $a_i + H_i$. The following useful characterisation was established in [4].

Theorem 2.3 ([4])**.** *Let G be a finite abelian group and let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a collection of disjoint subsets of G. Then $\mathcal{A}$ has the bimodal property if and only if for each i the set B_i is a union of cosets of the subgroup H_i.*

Remark 2.4. Theorem 2.3 tells us that if an element v is contained in B_j for some j with $1 \leq j \leq m$ then B_j contains the entire coset $v + H_j$, i.e. we have that $v + h_j \in B_j$ for all $h_j \in H_j$.

Example 2.5. Theorem 2.3 shows that the trivial examples of a collection of subsets of size 1, or a collection consisting of a single subset of an abelian group G, are both bimodal.

We now exhibit a non-trivial example of a bimodal collection of sets appearing in [4], which is different in structure to our coset example, but also arises in a much-studied group theoretic context. For a group G we will let G^* denote $G \setminus \{0\}$.

Definition 2.6. Let G be a finite group. If G has subgroups $S_1, S_2, \ldots, S_m$ with the property that $S_1^*, S_2^*, \ldots, S_m^*$ partition G^*, then the collection of subgroups $S_1, S_2, \ldots, S_m$ is called a *group partition* of G. A group partition is called *trivial* if $m = 1$.

Lemma 2.7 ([4])**.** *Let the collection of subgroups $\{S_1, \ldots, S_m\}$ be a group partition of an abelian group G where $|S_i| > 2$ for each i. Then the collection of sets $\mathcal{C} = \{S_1^*, \ldots, S_m^*\}$ has the bimodal property.*

Proof. For each i, the internal difference group of S_i^* is S_i. It follows directly that the union $\bigcup_{j \neq i} S_j^*$ is $G \setminus S_i$, a union of cosets of S_i. □

Example 2.8. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. Let $A_1 = \{(1,1), (2,2)\}$, $A_2 = \{(0,1), (0,2)\}$, $A_3 = \{(1,2), (2,1)\}$ and $A_4 = \{(1,0), (2,0)\}$. For each A_i, the subgroup H_i is precisely $A_i \cup \{0\}$, and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ is bimodal.

Group partitions have been studied extensively; see Zappa [6] for a survey. The abelian groups that possess non-trivial group partitions are precisely the elementary abelian p-groups. These can be viewed as partitions of vector spaces over $\mathbb{Z}_p$, and have been widely studied in this context; for example, see Heden [3].

Extending this construction gives examples in more general groups:

Lemma 2.9 ([4])**.** *Let $\mathcal{A}$ be a collection $\mathcal{A} = \{A_1, \ldots, A_m\}$ of disjoint subsets of an abelian group G that partition G^* and have the property that any A_i with $|A_i| > 1$ is of the form S^* for some subgroup $S \leq G$. Then $\mathcal{A}$ is bimodal.*

Example 2.10. Let $G = \mathbb{Z}_{12}$. Then G has a subgroup $\{0, 4, 8\}$ of order 3 and a subgroup $\{0, 3, 6, 9\}$ of order 4. The sets $\{4, 8\}$, $\{3, 6, 9\}$, $\{1\}$, $\{2\}$, $\{5\}$, $\{7\}$, $\{10\}$, $\{11\}$ form a bimodal collection.

Having seen some examples of constructions of bimodal collections of sets, we now introduce some approaches to constructing new collections from old, which we exploit in Section 3. It is straightforward to show that a bimodal collection can undergo a shift without its bimodality being affected.

Lemma 2.11. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G. Then the collection $\mathcal{A}'$ given by $\{A_1 + g, A_2 + g, \ldots, A_m + g\}$ where $g \in G$ is also bimodal.*

We may also replace a coset by a partition of that coset into smaller cosets, a process we will refer to as *subdivision*:

Theorem 2.12. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G. Suppose that A_i is a coset of H_i for some i. Let $A_i^1, A_i^2, \ldots, A_i^r$ be disjoint subsets partitioning A_i, having internal difference groups $H_i^1, H_i^2, \ldots, H_i^r$ respectively, and which possess the property that for $j = 1, 2, \ldots, r$ the set A_i^j is a coset of H_i^j. Then the collection $\mathcal{A}' = \{A_1, A_2, \ldots, A_{i-1}, A_i^1, A_i^2, \ldots, A_i^r, A_{i+1}, \ldots, A_m\}$ satisfies the bimodal property. We shall refer to $\mathcal{A}'$ as a* subdivision *of $\mathcal{A}$.*

Proof. The union of elements in the collection is not changed by subdivision, so for sets A_j with $j \neq i$ it is still the case that B_j is a union of cosets of H_j. Consider a set A_i^t; we will denote $A \setminus A_i^t$ by B_i^t. We note that $H_i^t \leq H_i$, and so any coset of H_i is a union of cosets of H_i^t. Now, $B_i^t = (A_i \setminus A_i^t) \cup B_i$. We have that B_i is a union of cosets of H_i^t since it is a union of cosets of H_i, and $A_i \setminus A_i^t$ is a union of cosets of H_i^t as A_i is a union of cosets of H_i and A_i^t is itself a coset of H_i^t. Thus we deduce that the collection is bimodal as required. □

Example 2.13. Let G be the elementary abelian group of order 8. Write it as $G = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Then by Example 2.5, $\mathcal{A} = \{G\}$ is trivially bimodal. We can apply subdivision to obtain $\mathcal{A}'$, as follows. Define the following subgroups of G: $S_1 = \{(0,0,0), (0,0,1)\}$, $S_2 = \{(0,0,0), (1,0,0)\}$, $S_3 = \{(0,0,0), (0,1,1)\}$, $S_4 = \{(0,0,0), (1,1,0)\}$. Then G may be partitioned as: $A_1 = S_1$, $A_2 = (0,1,0)+S_2$, $A_3 = (1,0,0)+S_3$, $A_4 = (0,1,1)+S_4$. Take $\mathcal{A}' = \{A_1, A_2, A_3, A_4\}$. This is bimodal by Theorem 2.12. To see this directly, observe that the differences out of A_1 comprise every element 2 times except the elements of S_1 which occur zero times; and in general the differences out of A_i comprise every element twice except those in S_i, which do not occur. Thus for $\delta \in G^*$, if δ is one of the four non-zero elements of $\cup_{1 \leq i \leq 4} S_i$ then $N_i(\delta) = 0$ for precisely one value of $i \in \{1, 2, 3, 4\}$, whereas if δ is one of the three elements of G^* not in $\cup_{1 \leq i \leq 4} S_i$, then $N_i(\delta) > 0$ for all i.

3 Classification of bimodal collections of sets

We will now develop a complete characterisation of bimodal collections of sets, through a series of results that classify them according to the relationship between their sets A_i and the corresponding internal difference groups H_i.

Remark 3.1. For a bimodal collection $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of disjoint subsets of an abelian group G we have $|A_i| \leq |H_i|$ for each i. Without loss of generality, we suppose that the sets are labelled so that for $i = 1, 2, \ldots, r_{\mathcal{A}}$ we have $|A_i| < |H_i|$, and for $i = r_{\mathcal{A}} + 1, r_{\mathcal{A}} + 2, \ldots, m$ we have $|A_i| = |H_i|$, i.e. A_i fills the coset $a_i + H_i$ for $i > r_{\mathcal{A}}$.

Lemma 3.2. *Let $\mathcal{A}$ be a collection $A_1, A_2, \ldots, A_m$ of disjoint subsets of G that has the bimodal property. Then $A_k \cap (a_j + H_j) = \emptyset$ for any $k \neq j$.*

Proof. B_j is a union of cosets of H_j, which does not include the coset $a_j + H_j$. For $k \neq j$, we have $A_k \subseteq B_j$, and so $A_k \cap (a_j + H_j) = \emptyset$. So not only is A_k disjoint from A_j when $k \neq j$, it is also disjoint from the entire coset $a_j + H_j$. □

3.1 The case when $r_{\mathcal{A}} \geq 2$

We will consider three cases: the situation when there are at least two sets A_i that do not fill $a_i + H_i$ (i.e. $r_{\mathcal{A}} \geq 2$), the case when precisely one A_i does not fill $a_i + H_i$ (i.e. $r_{\mathcal{A}} = 1$), and the case when each of the sets in $\mathcal{A}$ fills the coset of H_i that contains it ($r_{\mathcal{A}} = 0$).

Lemma 3.3. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$. Then for $i, j \leq r_{\mathcal{A}}$ with $i \neq j$ we have that H_i is not a subgroup of H_j and H_j is not a subgroup of H_i.*

Proof. Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, and suppose that for some $i, j \leq r_{\mathcal{A}}$ with $i \neq j$ we have $H_i \leq H_j$. Since $|A_i| < |H_i|$ there are elements of $a_i + H_i \subseteq a_i + H_j$ that are not contained in B_j, and by Lemma 3.2 these elements are not contained in any other set in $\mathcal{A}$. It follows that B_j is not a union of cosets of H_j, and so $\mathcal{A}$ is not bimodal. □

Proposition 3.4. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$. Then there exists a nonempty subset $D_{\mathcal{A}} \subseteq G$ such that:*

1. *$a_i + H_i = A_i \sqcup D_{\mathcal{A}}$ for $i \leq r_{\mathcal{A}}$;*
2. *$(a_i + H_i) \cap (a_j + H_j) = D_{\mathcal{A}}$ for any $i, j \in 1, 2, \ldots, r_{\mathcal{A}}$ with $i \neq j$;*
3. *$D_{\mathcal{A}}$ is itself a coset of a subgroup of G.*

Proof. 1. Let $D_{\mathcal{A}} = (a_1 + H_1) \setminus A_1$. We will show that $D_{\mathcal{A}} = (a_i + H_i) \setminus A_i$ for each i with $1 \leq i \leq r_{\mathcal{A}}$. Let $v \in D_{\mathcal{A}}$. We observe that $v \notin A$, by Lemma 3.2; in particular, $v \notin A_i$ for any $i \neq 1$. For i with $2 \leq i \leq r_{\mathcal{A}}$ there exists $h_i \in H_i$ with $h_i \notin H_1$, by Lemma 3.3. As $a_1 \in B_i$, we have that $a_1 + h_i \in B_i$. But $a_1 + h_i \notin A_1$, so we also have $a_1 + h_i + h_1 \in B_1$ for any $h_1 \in H_1$. Taking $h_1 = v - a_1$, we deduce that $v + h_i \in B_1$.

We claim that $v + h_i \in A_i$. For, if it were in B_i this would imply that $v \in B_i$, which contradicts the fact that $v \notin A$. In turn, this implies $v \in a_i + H_i$. As $v \notin A$ we conclude that $v \in (a_i + H_i) \setminus A_i$. This shows that $D_{\mathcal{A}} \subseteq (a_i + H_i) \setminus A_i$; repeating the above argument starting with $v' \in (a_i + H_i) \setminus A_i$ allows us to show that $(a_i + H_i) \setminus A_i \subseteq D_{\mathcal{A}}$.

2. Follows immediately from 3.1.
3. The set $D_{\mathcal{A}}$ is precisely the intersection of all cosets $a_i + H_i$ with $i \leq r_{\mathcal{A}}$. This implies that $D_{\mathcal{A}}$ is a coset of the subgroup obtained by taking the intersection of H_i for all $i \leq r_{\mathcal{A}}$. □

A collection of sets $F_1, F_2, \ldots, F_k$ with the property that $F_i \cap F_j = D$ for all $i \neq j$ is said to be a *k-star with kernel D* [2][1]. Using this terminology, Proposition 3.4 shows that for i with $1 \leq i \leq r_{\mathcal{A}}$ the collection of cosets $a_i + H_i$ form an $r_{\mathcal{A}}$-star with kernel $D_{\mathcal{A}}$.

By Lemma 2.11, we can choose to shift a collection $\mathcal{A}$ with $r_{\mathcal{A}} \geq 2$ by an element of $D_{\mathcal{A}}$. This allows us to assume $D_{\mathcal{A}} \leq G$.

Definition 3.5. A bimodal collection $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$ will be said to be *in canonical position* if it has been shifted so that $D_{\mathcal{A}}$ is a subgroup of G.

Remark 3.6. We observe that if $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ is a bimodal collection of subsets with $r_{\mathcal{A}} \geq 2$ in canonical position we have

- $D_{\mathcal{A}}$ is the subgroup $\cap_{i=1}^{r_{\mathcal{A}}} H_i$;
- for $i = 1, 2, \ldots, r_{\mathcal{A}}$ we have that $A_i = H_i \setminus D_{\mathcal{A}}$;
- the subgroups $H_1, H_2, \ldots, H_{r_{\mathcal{A}}}$ form an $r_{\mathcal{A}}$-star with kernel $D_{\mathcal{A}}$.

We have thus seen that the sets A_1 to $A_{r_{\mathcal{A}}}$ of a bimodal collection with $r_{\mathcal{A}} \geq 2$ occur together in a very structured way. In fact, we will see that these sets also impose considerable structure on the remaining members of $\mathcal{A}$.

Proposition 3.7. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, in canonical position. Then*

$$(H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}) \setminus D_{\mathcal{A}}$$

is contained in $A = \cup_{i=1}^{m} A_i$.

Proof. We begin by showing that $(H_1+H_2)\setminus D_{\mathcal{A}} \subseteq A$. Let $h \in (H_1+H_2)\setminus D_{\mathcal{A}}$. Then $h = h_1 + h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$. If $h_1 \in D_{\mathcal{A}}$ then $h_1+h_2 \in H_2$ and hence in $A_2 \subseteq A$ as $h_1+h_2 \notin D_{\mathcal{A}}$. Otherwise, $h_1 \in A_1 \subseteq B_2$. This implies that $h_1 + h_2$ is also in $B_2 \subseteq A$, by Remark 2.4.

Now consider $h \in (H_1+H_2+H_3)\setminus D_{\mathcal{A}}$, so $h = h_1+h_2+h_3$ with $h_1 \in H_1$, $h_2 \in H_2$ and $h_3 \in H_3$. Suppose $h_1 + h_2 \in D_{\mathcal{A}}$. Then $h_1 + h_2 + h_3 \in H_3$ and hence $h_1 + h_2 + h_3 \in A_3$ as $h_1 + h_2 + h_3 \notin D_{\mathcal{A}}$. In the case where $h_1 + h_2 \notin D_{\mathcal{A}}$, the above argument shows that $h_1 + h_2 \in A = A_3 \cup B_3$. Now, if $h_1 + h_2 \in B_3$ then by Remark 2.4 we have that $h_1 + h_2 + h_3 \in B_3 \subset A$. If, however, $h_1 + h_2 \in A_3$, then $h_1 + h_2 + h_3 \in H_3$ and hence $h_1 + h_2 + h_3 \in A_3$.

Proceeding analogously for all $r_{\mathcal{A}}$ summands yields the desired result. □

[1]The terms Δ-*system* or *sunflower* are also used for these structures.

In some circumstances it may be the case that all elements of $(H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}) \setminus D_{\mathcal{A}}$ are contained in the union of the sets $A_1, A_2, \ldots, A_{r_{\mathcal{A}}}$, but in general this will not be true, and there may be other sets A_i with $i > r_{\mathcal{A}}$ containing elements of $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}$. Furthermore, there may also be elements of A that do not lie in $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}$. The following proposition tells us more about the sets A_i with $i > r_{\mathcal{A}}$.

Proposition 3.8. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, in canonical position. Then for A_i with $i \geq r_{\mathcal{A}} + 1$, the group H_i is a subgroup of $D_{\mathcal{A}}$.*

Proof. Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, in canonical position, and suppose there exists $i > r_{\mathcal{A}}$ for which H_i is not a subgroup of $D_{\mathcal{A}}$. Then there exists $h_i \in H_i$ with $h_i \notin D_{\mathcal{A}}$. We observe that there exists $j \leq r_{\mathcal{A}}$ with $h_i \notin H_j$, as the only elements common to all of the groups H_t with $t \leq r_{\mathcal{A}}$ are those of $D_{\mathcal{A}}$. As $a_j \in B_i$ we thus have $a_j + h_i \in B_i$, and furthermore $a_j + h_i \in B_j$. Let $v \in D_{\mathcal{A}}$. Then $v - a_j \in H_j$, and thus $a_j + h_i + (v - a_j) = v + h_i \in B_j$.

Now, $A = A_i \cup B_i$, and B_i is a union of cosets of H_i. Since $|A_i| = |H_i|$, this implies that in fact A is a union of cosets of H_i. However, we have just shown that $v + h_i \in A$. As we know that $v \notin A$ (since $v \in D_{\mathcal{A}}$,) this leads to a contradiction. □

This implies that each set A_i with $i > r_{\mathcal{A}}$ is a coset of a subgroup of $D_{\mathcal{A}}$, and hence is contained in a coset of $D_{\mathcal{A}}$. Hence each such set is either wholly contained within $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}} \setminus D_{\mathcal{A}}$, or else lies completely outside $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}$. Thus we now know that the set $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}} \setminus D_{\mathcal{A}}$ is entirely partitioned by sets from $\mathcal{A}$. We also know that any A_i occuring outside of this set is a coset of a subgroup of $D_{\mathcal{A}}$. The following proposition characterises the union of these A_i.

Proposition 3.9. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, in canonical position. Let H be the group $H = H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}$. If $A \setminus H$ is nonempty, then it consists of a union of cosets of H; further, the sets A_i which lie in $A \setminus H$ arise from a subdivision of these cosets of H.*

Proof. We must show that if there is an element $x \in A \setminus H$ then $x + h \in A$ for all $h \in H$. First suppose $h \in H_i$ for some $i \leq r_{\mathcal{A}}$. As $x \in A \setminus H$ we have $x \in B_i$, and so $x + h \in B_i$. Otherwise, h has the form $h_1 + h_2 + \cdots + h_{r_{\mathcal{A}}}$ with $h_1 \in H_1, \ldots, h_{r_{\mathcal{A}}} \in H_{r_{\mathcal{A}}}$. But $x \in B_1$ so $(x + h_1) \in B_1 \subset A$. Furthermore, as $x \notin H$ we have $x + h_1 \notin H$. Hence $x + h_1 \in B_2 \subset A$, from which we deduce $x + h_1 + h_2 \in B_2$. Continuing in this manner we conclude that $x + h_1 + h_2 + \cdots + h_{r_{\mathcal{A}}} \in B_{r_{\mathcal{A}}} \subset A$ as required. So $A \setminus H$ is a union of cosets of H. Since by Proposition 3.8, we have that $H_i \leq D_{\mathcal{A}} \leq H$ for all

$i \geq r_{\mathcal{A}} + 1$, each A_i in $A \setminus H$ must be wholly contained in a single coset of H. □

The following theorem fully summarises the structure that has been determined in the above propositions.

Theorem 3.10. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} \geq 2$, in canonical position. Then*

1. *The internal difference groups $H_1, H_2, \ldots, H_{r_{\mathcal{A}}}$ form an $r_{\mathcal{A}}$-star with kernel $D_{\mathcal{A}}$, and for each i with $1 \leq i \leq r_{\mathcal{A}}$ we have $A_i = H_i \setminus D_{\mathcal{A}}$.*
2. *Any set A_i with $i > r_{\mathcal{A}}$ is a coset of a subgroup of $D_{\mathcal{A}}$.*
3. *If H denotes the group $H_1 + H_2 + \cdots + H_{r_{\mathcal{A}}}$, then $H \setminus D_{\mathcal{A}}$ is contained in A. Furthermore, the sets in $\mathcal{A}$ can be labelled such that for some k with $r_{\mathcal{A}} \leq k \leq m$ we have that $H \setminus D_{\mathcal{A}}$ is partitioned by $A_1, A_2, \ldots, A_k$.*
4. *If $k < m$ then the sets A_i with $i > k$ arise from a subdivision of cosets of H.*

We will see that not only are the conditions of Theorem 3.10 necessary for a collection of sets to be bimodal, they are sufficient as well. We present a technique for constructing a bimodal collection of sets with $r_{\mathcal{A}} \geq 2$.

Theorem 3.11. *Let G be an abelian group, and for $t \geq 2$ let $H_1, H_2, \ldots, H_t$ be distinct subgroups of G forming a t-star with kernel D, such that $|H_i : D| > 2$ for i with $1 \leq i \leq t$. Let $H = H_1 + H_2 + \cdots + H_t$.*

Let $\mathcal{A}$ consist of the following subsets of G:

1. *all subsets of the form $A_i = H_i \setminus D$ for i with $1 \leq i \leq t$;*
2. *all cosets of D that are subsets of H, but are not in $\cup_{i=1}^{t} H_i$;*
3. *for any number of cosets of H, all the cosets of D that lie within those cosets of H.*

Then $\mathcal{A}$ is a bimodal collection of subsets of G with $r_{\mathcal{A}} = t$ in canonical position.

Proof. We will prove this result by applying Theorem 2.3 to each of the internal difference groups of the sets in $\mathcal{A}$. For any subset which is a coset of D, its internal difference group is the subgroup D itself. For any A_i with $1 \leq i \leq t$, its internal difference group is H_i: since the index of D in H_i is greater than 2, we know that A_i contains at least 2 distinct cosets of D. Fix an element $x \in A_i$ and consider all differences between x and the elements of A_i; these will give all elements of H_i except for those in the coset $x + D$. Now, pick an element $y \in A_i$ such that x and y lie in different cosets of D.

Taking all differences between y and the elements of A_i yields all elements of H_i except those in $y + D$. Hence all elements of H_i lie in the internal difference group of A_i, as required.

We observe that every set in $\mathcal{A}$ is a union of cosets of D. Thus for any set whose internal difference group is D, the union of the remaining sets is a union of cosets of D, as required. For A_i with $1 \leq i \leq t$, we note that $A_i \cup D = H_i$ by construction, so B_i consists of $H \setminus H_i$ together with a union of cosets of H, and is therefore a union of cosets of H_i. □

Remark 3.12. By Theorem 2.12, new bimodal collections can be obtained by subdividing those subsets in the above construction that are cosets of D. Comparing this construction with Theorem 3.10, we see that all bimodal collections of sets with $r_{\mathcal{A}} \geq 2$ arise in this way.

3.2 The case when $r_{\mathcal{A}} = 1$

In this case precisely one of the sets A_i does not fill the coset $a_i + H_i$.

Proposition 3.13. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} = 1$. Then*

1. *for all i with $2 \leq i \leq m$, A_i is a coset of H_i and $H_i \leq H_1$;*
2. *A_1 is a proper subset of a coset of H_1, and consists of a union of cosets of the group $D = H_2 + H_3 + \cdots + H_m$.*

Proof. 1. Suppose that for some i with $2 \leq i \leq m$ there exists $h_i \in H_i$ with $h_i \notin H_1$. Let $u \in (a_1 + H_1) \setminus A_1$, and let v be in A_1. Then $u - v \in H_1$. We have $v \in B_i$, so $v + h_i \in B_i$. Since $h_i \notin H_1$ we have that $v + h_i \in B_1$. This implies that $v + h_i + (u - v) \in B_1$, i.e. that $u + h_i \in B_1 \subseteq A$. Since A_i consists of a coset of H_i, we know that $A = A_i \sqcup B_i$ is a union of cosets of H_i. This implies that if $u + h_i \in A$ then $u \in A$. However, by Lemma 3.2 we know that no element of $(a_1 + H_1) \setminus A_1$ lies in A, which gives a contradiction. 2 Let $x \in A_1$. We want to show that for any $d \in D$ we have $x + d \in A_1$. Now $d = h_2 + h_3 + \cdots + h_m$ where $h_i \in H_i$ for $2 \leq i \leq m$. Since $x \in B_2$ we have $x + h_2 \in B_2$. However, by 3.2 we know $H_2 \leq H_1$, and so $x + h_2 \in B_2 \cap (a_1 + H_1) = A_1$. This implies $x + h_2 \in B_3$, whence $x + h_2 + h_3 \in B_3$. Proceeding in this manner we determine that $x + d \in A_1$ as required. □

Definition 3.14. A bimodal collection $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ of disjoint subsets of an abelian group G with $r_{\mathcal{A}} = 1$ will be said to be *in canonical position* if it has been shifted so that $A_1 \subseteq H_1$ and the subgroup $D = H_2 + H_3 + \cdots + H_m$ is contained in $H_1 \setminus A_1$.

We summarise the structural properties of the situation.

Theorem 3.15. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} = 1$, in canonical position. Let $D = H_2 + H_3 + \cdots + H_m$. Then*

1. *$A_1 \subseteq H_1 \setminus D$ and A_1 is a union of cosets of D;*
2. *Each set A_i with $2 \leq i \leq m$ is a coset of H_i, and $A_2, \ldots, A_m$ arise from a subdivision of cosets of H_1.*

Example 3.16. Let $G = \mathbb{Z}_{36}$. The collection $\mathcal{A}$ of subsets defined by $A_1 = \{12, 15, 30, 33\}, A_2 = \{1, 19\}, A_3 = \{4, 22\}, A_4 = \{7, 25\}, A_5 = \{10, 28\}, A_6 = \{13\}, A_7 = \{16\}, A_8 = \{31\}, A_9 = \{34\}$ is bimodal. We observe that $H_1 = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}$, and $H_2 = H_3 = H_4 = H_5 = \langle 18 \rangle = \{0, 18\}$, so $H_2 + H_3 + H_4 + H_5 + H_6 + H_7 + H_8 + H_9 = \langle 18 \rangle < H_1$. Note also that $\cup_{i=2}^{9} A_i$ is the coset $1 + H_1$, and that A_1 is a union of cosets of $\langle 18 \rangle$. Here we have $A_1 \subset H_1$, and we note that the set $H_1 \setminus A_1$ is not in fact a group, in contrast to the behaviour of bimodal collections with $r_{\mathcal{A}} \geq 2$.

The conditions of Theorem 3.15 are sufficient as well as necessary:

Theorem 3.17. *Suppose we have an abelian group G, a subgroup H_1 of G and a proper subset A_1 of H_1 whose internal differences generate H_1.*

1. *Let S be the set of all subgroups $J \leq G$ with the property that A_1 is a union of cosets of J.*
2. *For any number of cosets of H_1, partition these cosets of H_1 using only cosets of subgroups from S.*
3. *Take $\mathcal{A}$ to consist of A_1 together with the sets in the above partition.*

Then $\mathcal{A}$ forms a bimodal collection of subsets of G with $r_{\mathcal{A}} = 1$.

Proof. The bimodality of $\mathcal{A}$ is immediate, upon applying Theorem 2.3 to each of the internal difference groups of the sets in $\mathcal{A}$. □

3.3 The case when $r_{\mathcal{A}} = 0$

Theorem 3.18. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a bimodal collection of disjoint subsets of an abelian group G with $r_{\mathcal{A}} = 0$. Let H be the group $H = H_1 + H_2 + \cdots + H_m$. Then each A_i $(1 \leq i \leq m)$ is a coset of H_i, and these sets arise from a subdivision of cosets of H.*

Proof. For each i, A_i is a coset of H_i and B_i is a union of cosets of H_i, hence A is a union of cosets of H_i for all i. Let $x \in A$ and let $h \in H$. Then h has the form $h_1 + h_2 + \cdots + h_m$ with $h_i \in H_i$ for i with $1 \leq i \leq m$. As $x \in A$ we thus have $x + h_1 \in A$. In turn this implies $x + h_1 + h_2 \in A$ and so on, so we deduce $x + h \in A$, as required. Since $H_i \leq H$ for all $1 \leq i \leq m$, every A_i is wholly contained in a single coset of H, so $\mathcal{A}$ is a subdivision of the cosets of H. □

Remark 3.19. Subdividing the construction of Lemma 1.1 gives a bimodal collection of sets with $r_{\mathcal{A}} = 0$; Theorem 3.18 shows that every such collection arises in this manner.

4 Further Questions

The bimodal property arose from an application to optimal algebraic manipulation detection codes; it would be interesting to explore the potential for wider applications of this concept in related areas. Group partitions, and particularly vector space partitions, also have a range of applications, and the role played by bimodality in these structures warrants further investigation.

Group partitions exist for certain classes of nonabelian groups, such as Frobenius groups, and these have been shown to give rise to bimodal collections of sets [4]. It would be natural to seek a comparable understanding of bimodality in a nonabelian context, though care must be taken to refine relevant definitions where appropriate.

References

[1] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N. Smart, editor, *EUROCRYPT 2008*, LNCS vol. 4965, 471–488, 2008.

[2] Z. Füredi. On finite set-systems whose every intersection is a kernel of a star. *Discrete Math.*, 47:129 – 132, 1983.

[3] O. Heden. A survey of the different types of vector space partitions. *Discrete Math Algorithms Appl*, 4(1):1–14, 2012.

[4] S. Huczynska and M. B. Paterson. Weighted external difference families and R-optimal AMD codes. *Discrete Math.*, 342(3):855 – 867, 2019.

[5] M. B. Paterson and D. R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Math.*, 339(12):2891 – 2906, 2016.

[6] G. Zappa. Partitions and other coverings of finite groups. *Illinois J. Math.*, 47(1-2):571–580, 2003.