Low-parameter difference multisets

Abstract

Difference multiset is a combinatorial design introduced by Buratti [3] and used to construct other combinatorial designs, for example regular difference families. In this paper difference multisets are investigated using an algebraic approach. Our methods yield new perspective, general constraints and constructions for the multiplicities of elements in difference multiset. We also focused on some particular cases with small parameter values and found all the difference multisets over $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3$. A link between the difference multisets over $\mathbb{Z}_3$ and other topics was also discovered.

Keywords: Difference multisets, Difference covers, Löschian numbers

1 Difference multisets and notation used

For convenience, let's start by introducing a notation

Definition 1.1. Given a group G, M is called a (G, k)-multiset if

$$|M| = k \wedge \forall g \in M : g \in G \tag{1}$$

We will denote the multiplicity function by n: the number of instances i is found in M will be denoted as $n(i, M)$ or simply n_i if the multiset is clear from the context.

In this article we investigate the existence of such (G, k)-multisets that the differences of their elements produce the elements of G. Given a $M = \{m_1, \ldots m_k\}$ we only consider the differences $m_i - m_j$ where $i \neq j$ excluding the so called trivial differences between an element and itself. Let's denote the multiset generated by this operation: $\mathcal{D}(M) = \{m_i - m_j \mid m_i, m_j \in M \wedge i \neq j\}$

Definition 1.2. A (G, k)-multiset M is called a (G, k)-difference cover if $\forall g \in G : g \in \mathcal{D}(M)$.

In particular we are interested in certain difference covers that produce a regular multiset by the aforementioned subtractions – such that each of the G elements is produced the same amount of times.

Definition 1.3. A (G, k)-difference cover M is called a (G, k)-difference multiset (a.k.a. regular difference cover) if $\exists \lambda \forall g \in G : \lambda = n(g, \mathcal{D}(M))$.

One might notice that the use of symbols λ and k is consistent with their roles as parameters of the common difference sets. They serve the same purpose here and we will also use the classic $v = |G|$. Commonly a (G, k)-difference multiset would be called a (G, k, λ) (or (v, k, λ)) difference multiset, but we find the λ superfluous as it's a function of v and k as will be shown further down the article (and has been shown before by every author discussing this topic).

Other authors have used combinatorial methods [3], group rings, character thoery [2] and other tools [1, 6] but nearly all of the proposed methods construct a difference multiset using a difference set and the nonexistence results mimic those holding for difference sets. As the result the number of constructed difference multisets is proportional to number of known difference sets which is unlikely to reflect tha actual situation. The amount of (G, k)-multisets is noticably greater than that of subsets of G. Accordingly there should be a lot more (G, k)-difference multisets than there are (G, k, λ)-difference sets.

We, in contrast, analyze the situation using algebraic and even geometrical perspective to obtain results that link difference multisets to number theory.

Remark 1.4. The definitions stated in this chapter do not exploit all of the group properties. We could actually take any quasigroup Q instead of G and the definitions would work the same. Some authors [4] have also investigated sum covers which produce the elements of a group as sums instead of differences. However, Cayley table of sums in one quasigroup is a table of differences in another and vice versa. Thus, by letting quasigroups on board we can treat both of the cases as either sum or difference multisets.

2   The mathematical apparatus

Let's note that the cardinality of (G, k)-difference multiset will inevitably equal the total of multiplicities.

$$\sum n_i = k \tag{2}$$

Now let's restate definition 1.3 algebraically. Each element i must appear as a difference λ times. For non-identity i we just multiply the multiplicities $n_{i+j} n_j$ and sum over all j to get the number of i's occurences. For i that is an identity we must also take help from Kronecker delta to discount the trivial differences.

$$\forall g \in G \colon \lambda = \sum (n_i(n_{g+i} - \delta_{i,g+i})) \tag{3}$$

Remark 2.1. One of the ways to easily construct equations (3) is as follows: take the Cayley table of the quasigroup in question. For all i, j replace element j in row of i with $n_j - \delta i, j$. Multiply the row vector of all the multiplicities $(n_1, n_2, \ldots)$ with the obtained matrix. Every component of the obtained vector must then be equal to λ.

We could derive the following from the previous statements, but let's simply observe that the number of non-trivial differences is equal to number of (G, k)-difference multiset element pairs (sub-multisets of order 2) $k(k-1)$ and it's

required to contain each of the $v = |G|$ elements λ times.

$$v\lambda = k(k-1) \tag{4}$$

Together these equations serve as the main tools in our investigations. Finding a (G, k)-difference multiset is the same as finding a set of non-negative integer n_i's that solve the above equations. It's also useful to notice that (2) is a hyperplane and (3) define second-order surfaces. Under this interpretation we are looking for lattice points on the intersection of all the surfaces defined by these equations.

Beware that (3) gives us up to v equations and combined with (2) and (4) we have $v + 2$ equations. If we are interested in finding the n_i's for given G and k, we should select only v equations or we might discover that $0 = 0$.

3 Smallest difference multisets

3.1 Trivial cases

Let's get these out of the way first. While not interesting on their own, these cases may turn out useful when looking for patterns and drawing parallels with other research.

If $v = 1$ (the trivial group) there is a $(\{0\}, k)$-difference multiset for any value of k: just take the identity k times and all the rules will be satisfied.

The cases of $k = 0$ and $k = 1$ is also universally good. For any group G you can take no elements to make a $(G, 0)$-difference multiset or a single element once to form a $(G, 1)$-difference multiset. In both of these cases $\lambda = 0$ i.e. the difference multiset produces every element of G exactly 0 times.

The above results are also true for nearly every quasigroup. The exception is the empty quasigroup combined with $k = 1$ as one can't take a single element from it so there is no $(\{\ \}, 1)$-difference multiset unfourtunately.

3.2 The two-element group

There is only one quasigroup with two elements which also happens to be a group. Let's take it in the form $\mathbb{Z}_2$.

This case was solved by Buratti [3]. We reproduce the solution using our approach and notation for it's similarity on the treatment for the following cases.

Theorem 3.1. $(\mathbb{Z}_2, k)$-difference multiset exists iff k is a perfect square. In that case $n_0 = \frac{k \pm \sqrt{k}}{2}$ and $n_1 = \frac{k \mp \sqrt{k}}{2}$.

Proof. Write (3) for the non-identity element, (2) and (4).

$$\begin{cases} n_0 + n_1 = k \\ 2n_0 n_1 = \lambda \\ 2\lambda = k(k-1) \end{cases} \tag{5}$$

The (3) for identity element is not included as it's truthness follows from these three.

We can combine the system into the following

$$\begin{cases} n_0 = k - n_1 \\ 2n_1(k - n_1) = \lambda \end{cases} \qquad (6)$$

That can be explicitly solved for n_0 and n_1. The solution combined with $2\lambda = k(k-1)$ takes the form as stated. $\qquad\square$

4 Difference multisets over three element group

There is only one group of three elements. Let's take it in form of $\mathbb{Z}_3$. What must the k be for $(\mathbb{Z}_3, k)$-difference multiset to exist? What are these difference multisets and how many of them are there for a particular value of k?

To answer these questions we shall write down (3) for a non-identity element and combine it with (2) and (4) to form a system of equations.

$$\begin{cases} 3\lambda = k(k-1) \\ \sum n_i = k \\ \sum n_i n_{i+1} = \lambda \end{cases} \qquad (7)$$

We may now combine the equations to discover a relation between multiplicities of elements.

Theorem 4.1. *Multiplicities of different $(\mathbb{Z}_3, k)$-difference multiset elements i un j are related via*

$$n_{i \neq j} = \frac{k - n_j \pm \sqrt{\frac{4k - (k - 3n_j)^2}{3}}}{2} \qquad (8)$$

Proof. Take any element $\gamma \in \mathbb{Z}_3$ and assign $c = n_\gamma$. Let's use α and β to name the remaining elements of $\mathbb{Z}_3$. The system (7) can now be rewritten:

$$\begin{cases} n_\alpha + n_\beta = k - c \\ n_\alpha n_\beta + c(n_\alpha + n_\beta) = \lambda \end{cases} \qquad (9)$$

Substitute $k' = k - c$ and $\lambda' = \lambda + c^2 - kc$ to obtain

$$\begin{cases} n_\alpha + n_\beta = k' \\ n_\alpha n_\beta = \lambda' \end{cases} \qquad (10)$$

Eliminating n_β we arrive at a quadratic equation that is solved into

$$n_\alpha = \frac{k' \pm \sqrt{k'^2 - 4\lambda'}}{2} \qquad (11)$$

Undo the substitutions and you're done. $\qquad\square$

4

Considering the multiplicities in form of $n_i = \frac{k+\Delta_i}{3}$, we can restate (8) into the following.

$$n_{i \neq j} = \frac{k - n_j \pm \sqrt{\frac{4k - \Delta_j^2}{3}}}{2} \tag{12}$$

The rest of analysis focuses on the Δ_i and it's effect on the above equation. The behaviour of expression under the root is tied to a topic in number theory called Löschian numbers [8]. These numbers make an appearance in a variety of fields (see comments in [8]).

Definition 4.2. Number k is called a Löschian number if $\exists a, b \in \mathbb{Z} \colon a^2 + ab + b^2 = k$.

For our purposes (to eliminate unnecessary symmetries) we will only consider a, b such that $a \geq b \geq 0$. This, however, doesn't change the scope of Löschian numbers.

Lemma 4.3. *For any Löschian number k we can find $a, b \in \mathbb{Z}$ such that $a^2 + ab + b^2 = k$ and $a \geq b \geq 0$.*

Proof. As k is a Löschian number there are $a', b' \colon a'^2 + a'b' + b'^2 = k$. We can construct a, b such that $a^2 + ab + b^2 = k$ and $a \geq b \geq 0$ as follows:

- If $a' \geq 0$ and $b' \geq 0$ just take $a = a'$ and $b = b'$ or swap them if $a' < b'$.

- If $a' < 0, b' < 0$ take $a' = -a, b' = -b$ or swap them if $a' > b'$.

- If $ab < 0$ take either $a' = |a|, b' = |a + b|$ or $a' = |a + b|, b' = |b|$. Swap places as necessary to ensure $a \geq b \geq 0$.

$\square$

Having introduced the term, we may now introduce the promised link.

Lemma 4.4. *There exists a Δ that makes $\frac{4k - \Delta^2}{3}$ a perfect square iff k is Löschian number.*
Δ values that does the job are $\pm(2a + b), \pm(a + 2b), \pm(a - b)$, where a, b are such that $a \geq b \geq 0$ and $a^2 + ab + b^2 = k$. There is no other Δ that makes $\frac{4k - \Delta^2}{3}$ into square.

Proof. For a Löschian number $k = a^2 + ab + b^2$ take Δ equal to $\pm(2a + b)$, $\pm(a + 2b)$ or $\pm(a - b)$ and obtain the value of expression in question to be b^2, a^2 or $(a + b)^2$ which are clearly squares.
On the other hand, if $\frac{4k - \Delta^2}{3}$ is square, assign:

$$z^2 = \frac{4k - \Delta^2}{3} \tag{13}$$

Rewrite

$$\frac{3z^2 + \Delta^2}{4} = k \tag{14}$$

5

Noticing that 4 divides $3z^2 + \Delta^2$ we can conclude that z and Δ are of the same parity (because $z^2 \equiv \Delta^2 \mod 4$). Thus 2 divides both $\Delta - z$ and $\Delta + z$.

We can now find integers a, b such that $a \geq b \geq 0$ and $a^2 + ab + b^2 = k$ (thus k is a Löschian number) and the Δ can be expressed in one of the expressions stated in lemma.

- If $z \geq \Delta$ take $a = \frac{z+\Delta}{2}$ and $b = \frac{z-\Delta}{2}$. Then $a - b = \Delta$.

- If $\Delta \geq z \geq \frac{\Delta}{3}$ take $a = z$ and $b = \frac{\Delta-z}{2}$. Then $a + 2b = \Delta$.

- If $\frac{\Delta}{3} \geq z$ take $a = \frac{\Delta-z}{2}$ and $b = z$. Then $2a + b = \Delta$.

$\square$

Let's introduce the following notation for the three values used in lemma 4.4. The rest can be expressed as $-\Delta_i$:

$$\Delta_\alpha = 2a + b, \Delta_\beta = -a - 2b, \Delta_\gamma = -a + b \tag{15}$$

These Δ_i will be used in the following theorem and α, β and γ are labels that, as before, we use to label the elements of $\mathbb{Z}_3$ in arbitrary order. We can now state our main result which is both construction and existence criterion for $(\mathbb{Z}_3, k)$-difference multisets.

Theorem 4.5. *For every pair $a, b \in \mathbb{Z}$ such that $k = a^2 + ab + b^2$ and $a \geq b \geq 0$ there are exactly $-(k + 1) \mod 3$ (up to automorphisms) $(\mathbb{Z}_3, k)$-difference multisets and the multiplicities of their elements are*

- $n_i = \frac{k+\Delta_i}{3}$ *for one and* $n_i = \frac{k-\Delta_i}{3}$ *for the other if* $3 \mid k$.

- $n_i = \frac{k+\Delta_i}{3}$ *if* $3 \nmid k$ *un* $b - a \equiv 1 \mod 3$.

- $n_i = \frac{k-\Delta_i}{3}$ *if* $3 \nmid k$ *un* $a - b \equiv 1 \mod 3$.

Proof. According to lemma 4.4, the expression (12) will equal integer only if k is a Löschian number and Δ_j is one of the listed on (15) or a negative of that.

Insert the constructions listed in (4.5) into (8) to check that these are indeed multiplicities that make up a difference multiset if the numbers are whole. One can also check that using Δ_α to construct one of the multiplicities you will notice Δ_β and Δ_γ used for the others and the same is true in any order.

Considering remainders one may check the following:

- If $a \equiv b \mod 3$ then $3 \mid k$ and all the multiplicities in both the constructions $n_i = \frac{k+\Delta_i}{3}$ and $n_i = \frac{k-\Delta_i}{3}$ are integers.

- If $a \equiv b - 1 \mod 3$ then $k \equiv 1 \mod 3$ and only the multiplicities constructed by $n_i = \frac{k+\Delta_i}{3}$ are all integer.

- If $a \equiv b + 1 \mod 3$ then $k \equiv 1 \mod 3$ and only the multiplicities constructed by $n_i = \frac{k-\Delta_i}{3}$ are all integer.

$\square$

Remark 4.6. Allowing a, b such that $a \geq b \geq 0$ wouldn't hold, we'd obtain the same $\Delta_\alpha, \Delta_\beta, \Delta_\gamma$ in different order thus making the same difference multisets again (up to automorphism). This constraint is intended to exclude such symmetries. Different $a \geq b \geq 0$ pairs with $a^2 + ab + b^2 = k$ will lead to different value of $a - b$ and thus all the constructions mentioned in 4.5 will be distinct. Consequently the number of $(\mathbb{Z}_3, k)$ will be proportional to number of unique a, b pairs (respecting constraints) and the coefficient of proportionality is $-(k+1)$ mod 3.

4.1 Estimating numbers

Despite our effort, the exact number of solutions is still elusive. This aspect is now reduced to a number-theoretic question – how many unique solutions are there for $k = a^2 + ab + b^2$ such that $a \geq b \geq 0$.

The number of solutions without the constraint is known [5]. Denote

$$k = 3^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots q_1^{\beta_1} q_2^{\beta_2} \ldots \tag{16}$$

where p_i are primes such that $p_i \equiv 1 \mod 3$ and q_i are primes such that $q_i \equiv 2 \mod 3$. If any of the β_i are odd, there are no integer solutions to $k = a^2 + ab + b^2$. But if all of β_i are even, the number of solutions is $6 \prod(\alpha_i + 1)$.

It is hypothesised [7] that the number of solutions (if every β_i is even) having $a \geq b \geq 0$ is $1/2 + \prod(\alpha_i + 1)/2$ if all the α_i are even and $\prod(\alpha_i + 1)/2$ otherwise. We checked this to be true for a thousand Löschian numbers. However, for most of the Löschian numbers this remains unchecked.

4.2 Other structures of the same size

As mentioned in the opening sections, one might also consider $(\mathbb{Z}_3, k)$-sum multisets where the elements of $\mathbb{Z}_3$ must be produced as the sums of elements. This turns out to be a simple case.

Similarly to (3) we start by writing down the ways to obtain each of the elements and requiring them to be equal $(\forall j \in \mathbb{Z}_3 \lambda = \sum(n_i(n_{i-j} - \delta_{i,i-j})))$. Adding the $\sum n_i = k$ and using $3\lambda = k(k-1)$ we may form a system of equations.

$$\begin{cases} n_0(n_0 - 1) + 2n_1 n_2 = \frac{k(k-1)}{3} \\ n_1(n_1 - 1) + 2n_2 n_0 = \frac{k(k-1)}{3} \\ n_2(n_2 - 1) + 2n_0 n_1 = \frac{k(k-1)}{3} \\ n_0 + n_1 + n_2 = k \end{cases} \tag{17}$$

It can be noticed with ease that (17) possesses symmetry with respect to all the elements of $\mathbb{Z}_3$. Besides this system can easily be solved explicitly – valid multisets of n_i are $\{\frac{k}{3}, \frac{k}{3}, \frac{k}{3}\}$ and $\{\frac{k-1}{3}, \frac{k-1}{3}, \frac{k+2}{3}\}$.

So, we can conclude that there can be at most one (up to automorphisms) $(\mathbb{Z}_3, k)$-sum multiset for a given value k. Specifically there is one if $3 \mid k$ or $k \equiv 1$ mod 3 and the multiplicities of elements are $\{\frac{k}{3}, \frac{k}{3}, \frac{k}{3}\}$ and $\{\frac{k-1}{3}, \frac{k-1}{3}, \frac{k+2}{3}\}$ respectively. And there are none if $k \equiv 2 \mod 3$ which eerily reminds of the situations with difference multisets.

Recall remark 1.4. If we consider any other quasigroup of order 3, it turns out that in every case the difference multisets and sum multisets give raise to either system (7) or the system (17). There are only 5 quasigroups of order 3 so this can be checked on a case by case basis. We have thus solved the problem for every quasigroup of size 3.

5 Difference multisets over $\mathbb{Z}_2 \times \mathbb{Z}_2$

Let us now consider group $\mathbb{Z}_2 \times \mathbb{Z}_2$. In this case our apparatus gives raise to the following system of equations.

$$
\begin{cases}
\sum n_i^2 = k + \lambda \\
\sum n_i = k \\
4\lambda = k(k-1) \\
2n_{00}n_{01} + 2n_{10}n_{11} = \lambda \\
2n_{00}n_{10} + 2n_{01}n_{11} = \lambda \\
2n_{00}n_{11} + 2n_{10}n_{01} = \lambda
\end{cases}
\tag{18}
$$

Theorem 5.1. *$(\mathbb{Z}_2 \times \mathbb{Z}_2, k)$–difference multisets exist iff $\sqrt{k} \equiv 0 \mod 4$ or $\sqrt{k} \equiv \pm 1 \mod 4$. The multiplicities are:*

- $\frac{k+3\sqrt{k}}{4}$ *for one element and $\frac{k-\sqrt{k}}{4}$ for the other three if $\sqrt{k} \equiv 1 \mod 4$.*

- $\frac{k-3\sqrt{k}}{4}$ *for one element and $\frac{k+\sqrt{k}}{4}$ for the other three if $\sqrt{k} \equiv -1 \mod 4$.*

- $\frac{k\pm 3\sqrt{k}}{4}$ *for one element and $\frac{k\mp\sqrt{k}}{4}$ for the other three if $4 \mid \sqrt{k}$.*

Proof. Solve (18) to find eight solutions each having one $n_i = \frac{k\pm 3\sqrt{k}}{4}$ and the rest $n_{j\neq i} = \frac{k\mp\sqrt{k}}{4}$.

Notice that these numbers are integers in and only in the cases described in theorem. Exclude the permutations of n_i as permutations of elements are all automorphisms for $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\qquad\square$

6 Other particular cases

6.1 Difference multisets over $\mathbb{Z}_4$

Our apparatus used in group $\mathbb{Z}_4$ produces one too few equations to solve this exactly.

$$\begin{cases} \sum n_i^2 = k + \lambda \\ \sum n_i = k \\ 4\lambda = k(k-1) \\ n_0 n_1 + n_1 n_2 + n_2 n_3 + n_3 n_0 = \lambda \\ 2n_0 n_2 + 2n_1 n_3 = \lambda \end{cases} \tag{19}$$

Theorem 6.1. *The multiplicities of elements in $(\mathbb{Z}_4, k)$-difference multisets are linked by:*

$$\begin{aligned} n_0 + n_2 &= \frac{k \pm \sqrt{k}}{2} \\ n_1 + n_3 &= \frac{k \mp \sqrt{k}}{2} \end{aligned} \tag{20}$$

Proof. Take few of the (19) equations.

$$\begin{cases} n_0^2 + n_1^2 + n_2^2 + n_3^2 = k + \lambda \\ n_0 n_1 + n_1 n_2 + n_2 n_3 + n_3 n_0 = \lambda \\ 2n_0 n_2 + 2n_1 n_3 = \lambda \end{cases} \tag{21}$$

Sum these equations to obtain one.

$$n_0(n_0 + n_1 + n_2 + n_3) + n_2(n_2 + n_1 + n_0 + n_3) + (n_1 + n_3)^2 = k + 3\lambda \tag{22}$$

Exploit $\sum n_i = k$ to transform it and $4\lambda = k(k-1)$ to eliminate λ.

$$(n_0 + n_2)k + (k - (n_0 + n_2))^2 = \frac{3k^2 + k}{4} \tag{23}$$

This is a quadratic equation with respect to $n_0 + n_2$ that we can solve directly into the form given in theorem.

$$n_0 + n_2 = \frac{k \pm \sqrt{k}}{2} \tag{24}$$

And the form of $n_1 + n_3$ is a obtained from the above result by exploiting $\sum n_i = k$. $\square$

A direct consequence – $(\mathbb{Z}_4, k)$-difference multisets are only possible for square k. But not for all of those – if $\lambda = \frac{k(k-1)}{4}$ is odd, a difference multiset is not possible because if $i - j = 0$ then also $j - i = 0$ so identity element
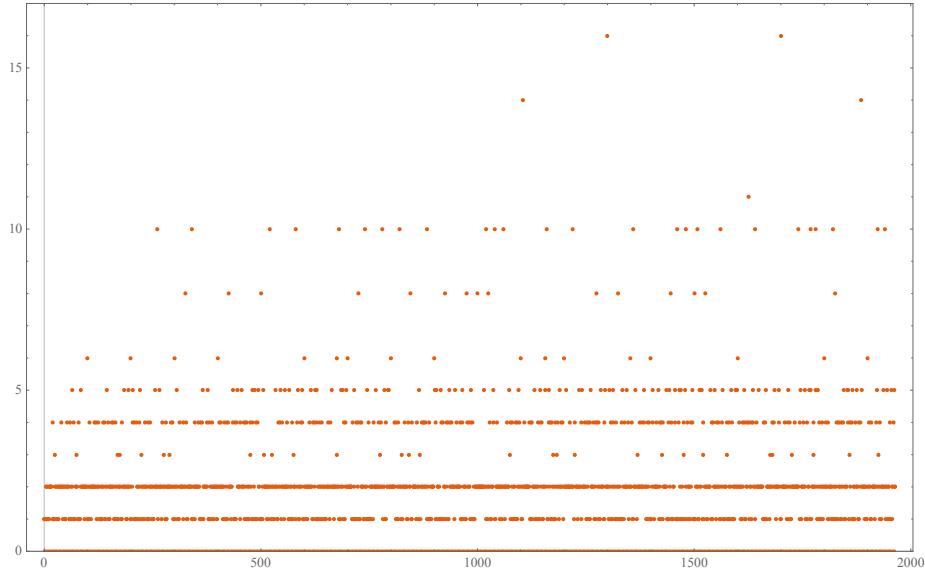
9

Figure 1: Number of $(\mathbb{Z}_4, k)$-difference multisets (excluding automorphisms) with respect to $\sqrt{k}$.

will always be produced even number of times in any difference multiset and λ may never be odd.

It is easy to check that all of the solutions stated in theorem 5.1 also work here, so it's clear that a solution exists if and only if $\sqrt{k} \in \mathbb{Z}$ and $\sqrt{k} \not\equiv 2 \mod 4$ (i.e. whenever λ is even).

However, our numerical experiments show that the one or two solutions given in 5.1 are not the only ones working for this group. Smallest of the solutions not constructed in theorem 5.1 arises for $k = 25$ where a difference multiset can have multiplicities not only $\{5, 5, 5, 10\}$, but also $\{3, 6, 7, 9\}$.

The numbers of solutions for k not too large are depicted in figure 1. One can observe that with k increasing we have cases of more and more solutions that can't be explained by the known construction.

6.2 Difference multisets over $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Similarly to the previous case, this is not yet solved, but we have some observations.

Theorem 6.2. *A $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, k)$-difference multiset can be constructed by taking the multiplicities n_i in the following ways:*

- *If $\sqrt{k} \equiv -1 \mod 8$ take $n_i = \frac{k - 7\sqrt{k}}{8}$ for some i and $n_j = \frac{k + \sqrt{k}}{8}$ for other $j \neq i$.*

10

- *If $\sqrt{k} \equiv 1 \mod 8$ take $n_i = \frac{k+7\sqrt{k}}{8}$ for some i and $n_j = \frac{k-\sqrt{k}}{8}$ for other $j \neq i$.*

- *If $\sqrt{k} \equiv\equiv 0 \mod 8$ take multiplicity $\frac{k\pm5\sqrt{k}}{8}$ for one element, $\frac{k\pm\sqrt{k}}{8}$ for four others and $\frac{k\mp3\sqrt{k}}{8}$ for the remaining three elements. And both of the above solutions will work as well.*

Proof. Write down (2) and (3) for this case:

$$
\begin{cases}
n_{000} + n_{001} + n_{010} + n_{011} + n_{100} + n_{101} + n_{110} + n_{111} = k \\
n_{001}^2 + n_{010}^2 + n_{010}^2 + n_{011}^2 + n_{100}^2 + n_{101}^2 + n_{110}^2 + n_{111}^2 = k + \lambda \\
2n_{001}n_{000} + 2n_{010}n_{011} + 2n_{101}n_{100} + 2n_{111}n_{110} = \lambda \\
2n_{010}n_{000} + 2n_{011}n_{001} + 2n_{110}n_{101} + 2n_{111}n_{101} = \lambda \\
2n_{100}n_{000} + 2n_{101}n_{001} + 2n_{110}n_{010} + 2n_{111}n_{011} = \lambda \\
2n_{011}n_{000} + 2n_{010}n_{001} + 2n_{111}n_{100} + 2n_{110}n_{101} = \lambda \\
2n_{101}n_{000} + 2n_{110}n_{011} + 2n_{111}n_{010} + 2n_{100}n_{001} = \lambda \\
2n_{110}n_{000} + 2n_{111}n_{001} + 2n_{101}n_{011} + 2n_{100}n_{010} = \lambda \\
2n_{111}n_{000} + 2n_{001}n_{110} + 2n_{010}n_{101} + 2n_{100}n_{011} = \lambda
\end{cases}
\tag{25}
$$

Check that the given solution satisfy the equations and notice that they are integers whenever $\sqrt{k}$ behaves as described in the cases of theorem. $\square$

We have not managed to exclude existence of other solutions, but computational evidence show that these are the only solutions for $k \leq 10000$.

7 A universal regular construction

We also managed to generalise a construction that worked in $\mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Such construction also works in many other cases (whenever k is close to a multiple of v), but unlike before, it is not necessarily the only possible construction.

Theorem 7.1. *(G, k)-difference multiset exists if $v \mid \sqrt{k}$ or $\sqrt{k} \equiv \pm 1 \mod v$ and it's multiplicities are*

- *If $\sqrt{k} \equiv 1 \mod v$ then $n_i = \frac{k+(v-1)\sqrt{k}}{v}$ for any element i and $n_{j \neq i} = \frac{k-\sqrt{k}}{v}$ for the other elements.*

- *If $\sqrt{k} \equiv -1 \mod v$ then $n_i = \frac{k-(v-1)\sqrt{k}}{v}$ for any element i and $n_{j \neq i} = \frac{k+\sqrt{k}}{v}$ for the other elements.*

- *Both of the above if $v \mid \sqrt{k}$.*

Proof. The conditions in theorem guarantees the multiplicities to be integers. All that is left is to demonstrate that they actually make up a difference multiset and we will do that using our main equations as usual.

Inserting the proposed multiplicities into (2) we get a true equation.

$$\sum n_i = \frac{k \pm (v-1)\sqrt{k}}{v} + (v-1)\frac{k \mp \sqrt{k}}{v} = k \tag{26}$$

Writing down (3) for the identity element we obtain $\sum n_i(n_i - 1) = \lambda$. Using (2) we may simplify to $\sum n_i^2 = \lambda + k$ as done previously. Now insert the proposed multiplicities to obtain the following.

$$\begin{aligned}
\sum n_i^2 &= \left(\frac{k \pm (v-1)\sqrt{k}}{v}\right)^2 + (v-1)\left(\frac{k \mp \sqrt{k}}{v}\right)^2 \\
&= \frac{k^2 + (v-1)^2 k + (v-1)k^2 + (v-1)k}{v^2} \\
&= \frac{k^2 + (v-1)k}{v} \\
&= \frac{k(k-1)}{v} + k
\end{aligned} \tag{27}$$

Per (4) we have $\frac{k(k-1)}{v} = \lambda$ so the above equation equals $\lambda + k$ i.e. is true.

Finally, for non-identity g the (3) takes the form $\sum n_i n_{i+g} = \lambda$. A particular multiplicity will be involved in two of the products – once as i and once as $i+g$ (but not both at the same time as we consider non-identity g now). Other $v-2$ products are destined to contain other multiplicities solely. Thus we have it smooth again.

$$\begin{aligned}
\sum n_i n_{i+g} &= 2\left(\frac{k \pm (v-1)\sqrt{k}}{v}\right)\left(\frac{k \mp \sqrt{k}}{v}\right) + (v-2)\left(\frac{k \mp \sqrt{k}}{v}\right)^2 \\
&= 2\frac{k^2 - k(v-1) \pm (v-2)k\sqrt{k}}{v^2} + (v-2)\left(\frac{k^2 \mp 2k\sqrt{k} + k}{v^2}\right) \\
&= \frac{vk^2 - kv}{v^2} \\
&= \frac{k(k-1)}{v}
\end{aligned} \tag{28}$$

And the (4) still gives us $\frac{k(k-1)}{v} = \lambda$ making these equations true as well. $\square$

Remark 7.2. In case anyone still reads the remarks: this difference multiset construction is also applicable for all the quasigroups just like that. And consequently to all the sum multisets as well.
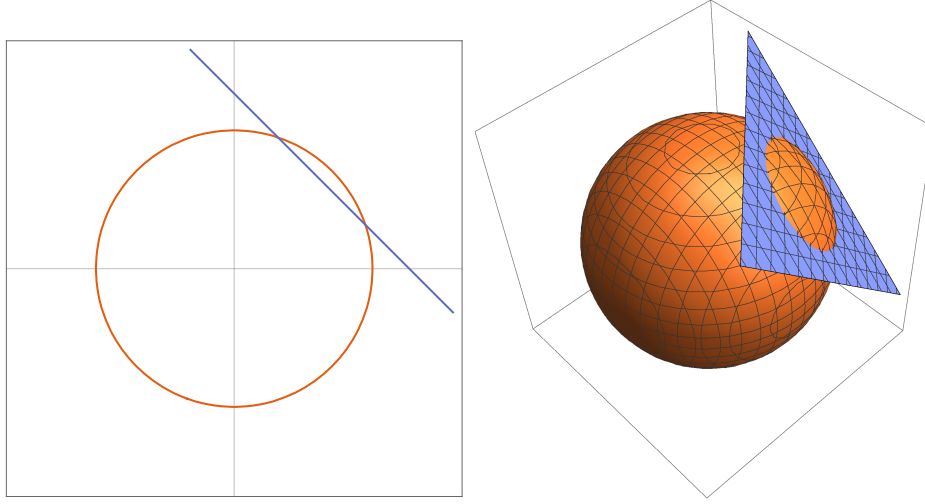
Figure 2: The $\sum n_i = k$ and $\sum n_i^2 = k + \lambda$ surfaces in two and three dimensions.

8   Limits for multiplicities

Applying our apparatus to (G, k)-difference multiset over arbitrary group we can notice that some of surfaces defined by our equations are always the same. There is always the hyperplane $\sum n_i = k$ and the hypersphere $\sum n_i^2 = k + \lambda$ centered at the origin (see figure 2). You could notice right away that the second equation connfines every multiplicity: $n_i \leq \sqrt{k + \lambda}$. By investigating the intersection more thoroughly we may discover that the multiplicities are actually bound to be near (in a sense) to their average – k/v.

Theorem 8.1. *If M is a (G, k)-difference multiset then*

$$\forall g \in G \colon \frac{k - (v - 1)\sqrt{k}}{v} \leq n(g, M) \leq \frac{k + (v - 1)\sqrt{k}}{v} \tag{29}$$

Proof. Take (3) for the identity element and (2) as constraints.

$$\begin{cases} \sum n_i = k \\ \sum (n_i(n_i - 1)) = \lambda \end{cases} \tag{30}$$

Let's optimize n_g respecting the constraints. We can add the first equation to the other to simplify the latter expression and let's also put all the terms on one side as follows.

$$\begin{cases} k - \sum n_i = 0 \\ k + \lambda - \sum n_i^2 = 0 \end{cases} \tag{31}$$

We may now use a common optimization technique – Lagrange multipliers to obtain the maximum and minimum of n_q honoring the constraints by using
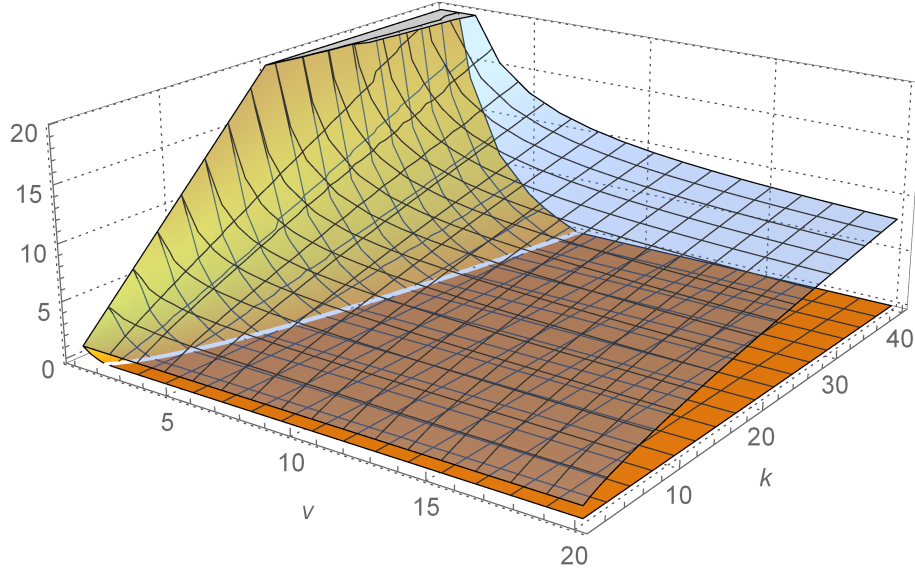
Figure 3: Lower and upper limits for the values of n_i with respect to v and k.

the following Lagrange function (note that Lagranage multipliers λ_1 and λ_2 are notated per tradition and have nothing in common with the parameter λ).

$$\mathcal{L} = n_g - \lambda_1(k - \sum n_i) - \lambda_2(k + \lambda - \sum n_i^2) \tag{32}$$

This gives the stated boundaries for any n_g in a difference multiset. The optimization calculations are not included as those are tedious and in no way novel. □

Theorem 8.1 might appear uninspiring at first but it greatly reduces the amount of options for every n_g. This simplification is a crucial stepping stone in making decent computer searches possible which allowed us to discover patterns that lead to results presented in this paper.

Remark 8.2. The results in this section are actually not specific to groups. They are true for any loop as the identity element is all that we need.

9 Conclusions

The algeabraic approach proves useful; let us outline the main achievements. Although this topic seems far from complete, we have reached multiple small breakthroughs in various directions.

The case of difference multisets over $\mathbb{Z}_3$ (theorem 4.5) shows that not only the very trivial cases can be solved explicitly. Although it is not straightforward to generalize our methods for arbitrary $\mathbb{Z}_k$, solving the problem for an odd

prime value of k seems promising. Furthermore the discovered link to Löschian numbers might provide further insight for other difference multisets or even some new perspective on the topics now linked through Löschian numbers.

The solved $\mathbb{Z}_2 \times \mathbb{Z}_2$ (theorem 5.1) is another promising direction. A new construction (theorem 7.1) was found generalizing ones of $\mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ and it feels a general solution for $G = \prod_{i=1}^{n} \mathbb{Z}_2$ should be in reach soon as the evidence for the case of $G = \prod_{i=1}^{3} \mathbb{Z}_2$ also suggests that there is a simple structure underneath.

And lastly, theorem 8.1 greatly narrows the space of options that has to be considered in computer searches thus allowing to inspect a wide range of difference multisets and draw conclusions through observations.

References

[1] KT Arasu, Ashwani K Bhandari, Siu-Lun Ma, and Surinder Sehgal. Regular difference covers. *Kyungpook Math. J*, 45:137–152, 2005.

[2] KT Arasu and Surinder Sehgal. Cyclic difference covers. *Austral. J. Combin*, 32:213–223, 2005.

[3] Marco Buratti. Old and new designs via difference multisets and strong difference families. *Journal of Combinatorial Designs*, 7(6):406–425, 1999.

[4] Harri Haanpää. Minimum sum and difference covers of abelian groups. *Journal of Integer Sequences*, 7(2):3, 2004.

[5] Oscar Marmon. Hexagonal lattice points on circles. *arXiv preprint math/0508201*, 2005.

[6] Koji Momihara. Strong difference families, difference covers, and their applications for relative difference families. *Designs, Codes and Cryptography*, 51(3):253–273, 2009.

[7] Umesh P Nair. Elementary results on the binary quadratic form a^ 2+ ab+ b^ 2. *arXiv preprint math/0408107*, 2004.

[8] Neil James Alexander Sloane. The On-Line Encyclopedia of Integer Sequences. . Sequence A003136.