# Low-parameter difference multisets

**Abstract**

The abstract is outdated... 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 we obtain some general constraints and constructions for the multiplicities of elements in difference multiset. We also focused on a few particular cases with small parameter values and found all the difference multisets over $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3$. An interesting 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

Difference multiset is a combinatorial design similar to difference set. But a multiset. The classical difference set $D \subseteq G$ is such a set that produces every non-zero $g \in G$ the same number of times when taking the differences between elements of $D$. A simple example is $\{ 0, 1 \} \subset \mathbb{Z}_3$ as $1 - 0 = 1$ and $0 - 1 = 2$ thus producing both of the non-zero elements of $\mathbb{Z}_3$. Curiosly, the same pair is also a difference set in $\mathbb{Z}_2$, but that's boring as $G$ is always a difference set of $G$. A tiny bit less trivial and more classical example is $\{ 0, 1, 3 \} \subset \mathbb{Z}_7$.

If we take a multiset instead, we can produce the whole $G$, including the identity. For example, considering the differences between elements of $\{ 0, 0, 1 \} \subset \mathbb{Z}_3$ we obtain $\{ 0, 0, 1, 1, 2, 2 \}$. This is what we call a difference multiset. Take note that we take differences from a pair of elements not an element and itself (i.e. there was $0 - 0 = 0$ as first zero subtracted from the second and vice verse but not first zero from itself and no $1 - 1$).

These designs were first studied on their own by Buratti [3] who noticed the indirect use of these designs and the related strong difference families in constructions of various combinatorial designs. The paper defined the concept of difference multiset and obtained some theorems and constructions. The topic was developed further and renamed to regular difference covers by other authors [2, 1] who introduced new constructions and a notable amount of nonexistence theorems.

The results in the foundational articles are mostly analogous to those of difference sets, almost all of the constructions are using some difference set

construction. As a result the number of constructed difference multisets is proportional to that of difference sets which is unlikely to reflect the real situation as there are infinitely more multisets over a given finite $G$ than there are subsets. Some constructions producing difference multisets of arbitrary size over fixed $G$ were uncovered in [6] and we strive to expand in this direction—constructing arbitrarily large multisets in a fixed, mainly small algebra.

## 2 Definitions and notation used

Let's start by introducing a notation.

**Definition 2.1.** Given a quasigroup $Q$, $M$ is called a $(Q, k)$-multiset if

$$|M| = k \wedge \forall q \in M \colon q \in Q \tag{1}$$

When describing large or arbitrary multisets over a fixed quasigroup, it's convenient to use 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 obvious from the context.

In this article we investigate the existence of such $(Q, k)$-multisets that the differences of their elements produce the elements of $Q$. Given a $M = \{ m_1, \dots m_k \}$ we only consider the differences $m_i - m_j$ where $i \neq j$ excluding the 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 2.2.** A $(Q, k)$-multiset $M$ is called a $(Q, k)$-difference cover if $\forall q \in Q \colon g \in \mathcal{D}(M)$.

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

**Definition 2.3.** A $(Q, k)$-difference cover $M$ is called a $(Q, k)$-difference multiset (a.k.a. regular difference cover) if $\exists \lambda \forall q \in Q \colon \lambda = n(q, \mathcal{D}(M))$.

One might notice that the use of symbols $\lambda$ 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 $v = |Q|$. Commonly a $(Q, k)$-difference multiset would be called a $(Q, k, \lambda)$ (or $(v, k, \lambda)$) difference multiset, but we omit the $\lambda$ 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).

*Remark* 2.4. We will use additive terminology and notation in this article because of esthetics and tradition in the field (the other authors sadly tend to limit the definitions to additive groups only). Unless stated otherwise, the definitions and results apply in any group-like algebra where the inverse operation (subtraction) is possible, i.e. we're working in a quasigroup. 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.

# 3 The mathematical apparatus

Let's note that the cardinality of $(Q, k)$-difference multiset will inevitably equal the total of multiplicities. We will omit the summation index and bounds if possible. Suppose that all sums are over $i \in Q$ if it seems reasonable.

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

Now let's restate definition 2.3 in terms of $n$. Each element $q$ must appear $\lambda$ times as a difference $(i + q) - i$. For non-identity $q$ we obtain the number of $q$'s occurences by multiplying the multiplicities $n_{i+q}n_i$ and summing over $i \in Q$. For $q$ that is an identity we will involve Kronecker delta to discount the trivial differences.

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

*Remark* 3.1. We may informally but usefully (mostly for computer implementations) rewrite (3) as

$$Cf = \boldsymbol{\lambda} \tag{4}$$

where $C$ is the Cayley table of $Q$, $\boldsymbol{\lambda}_q = \lambda$ and $f_q : i \to (n_i - \delta_{i,q})n_q$. And note that in $Cf$ you should treat $C_{ij}f_j$ as $f_j$ acting on $C_{ij}$.

Let's also observe that the number of non-trivial differences is equal to the number of $(Q, k)$-difference multiset element pairs (sub-multisets of order 2) $k(k - 1)$ and it's required to contain each of the $v = |Q|$ elements $\lambda$ times.

$$v\lambda = k(k - 1) \tag{5}$$

These equations serve as the main tools in our investigation. Finding a $(Q, k)$-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.

Let's apply the substitution $n_i = \frac{k+d_i\sqrt{k}}{v}$. We can rewrite the previous equations in terms of digressions $d_i$:

$$\sum d_i = 0 \tag{6}$$

$$\forall q \in Q\colon \sum (d_i(d_{q+i} - \frac{\delta_{i,q+i}}{\sqrt{k}}) - v\delta_{i,q+i}) = -v \tag{7}$$

This transformation is especially cute in the case of loops where the latter equation simplifies even futher and no longer depend on $k$:

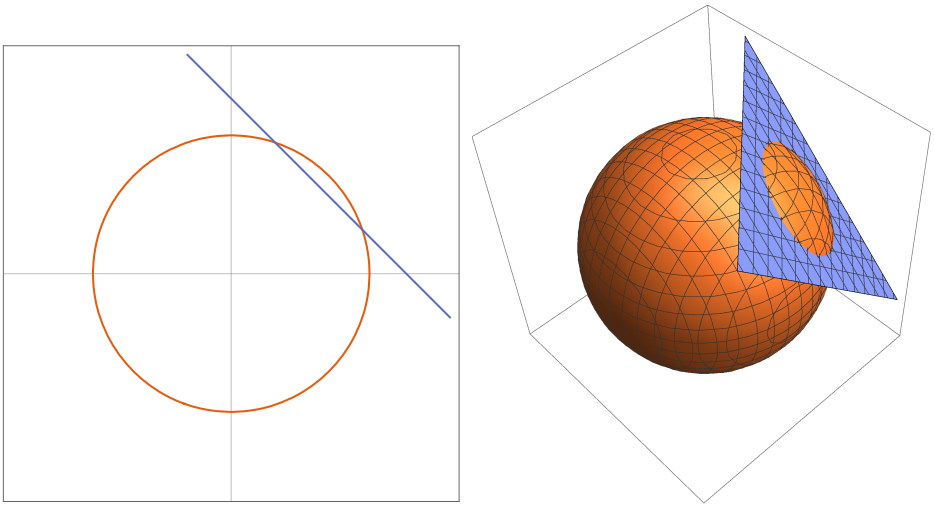

Figure 1: The $\sum n_i = k$ and $\sum n_i^2 = k+\lambda$ surfaces in two and three dimensions.

$$\forall q \in Q\colon \sum d_i d_{q+i} = v(v\delta_{q0} - 1) \tag{8}$$

Thus it is a bit simpler to find a solution, but the cost is that we must afterwards test if the solution produces integer $n_i$'s.

*Remark* 3.2. System (7) can be rewritten in the informal matrix form as

$$Cg = \mathbf{v} \tag{9}$$

where $C$ is the Cayley table of $Q$, $\mathbf{v}_q = -v$ and $g_q : i \to (d_i(d_q - \frac{\delta_{i,q+i}}{\sqrt{k}}) - v\delta_{i,q+i})$. And remember that in $Cg$ you should treat $C_{ij}g_j$ as $g_j$ acting on $C_{ij}$.

# 4 General results

## 4.1 Limits for multiplicities

Applying our apparatus to $(Q, k)$-difference multiset over arbitrary loop (quasigroup with an identity) we can notice that some of the 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 1). You could notice right away that the second equation confines 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 4.1.** *If $M$ is a $(Q, k)$-difference multiset then*

$$\forall q \in Q\colon \frac{k - (v-1)\sqrt{k}}{v} \leq n(q, M) \leq \frac{k + (v-1)\sqrt{k}}{v} \tag{10}$$

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

$$\begin{cases} \sum n_i = k \\ \sum(n_i(n_i - 1)) = \lambda \end{cases} \tag{11}$$

Let's optimize $n_q$ 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.

$$\begin{cases} k - \sum n_i = 0 \\ k + \lambda - \sum n_i^2 = 0 \end{cases} \tag{12}$$

We may now use a common optimization technique – Lagrange multipliers to obtain the maximum and minimum of $n_q$ honoring the constraints by using the following Lagrange function (note that Lagranage multipliers $\lambda_1$ and $\lambda_2$ are notated per tradition and have nothing in common with the parameter $\lambda$).

$$\mathcal{L} = n_q - \lambda_1(k - \sum n_i) - \lambda_2(k + \lambda - \sum n_i^2) \tag{13}$$

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

Theorem 4.1 might appear uninspiring at first but it greatly reduces the amount of options for every $n_q$. 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.

## 4.2 A universal regular construction

Based on particular results discussed further, we have discovered a construction that works whenever $k$ is close to a multiple of $v$.

**Theorem 4.2.** *$(Q, k)$-difference multiset exists if $v \mid \sqrt{k}$ or $\sqrt{k} \equiv \pm 1 \mod v$ and it's digressions are*

- *If $\sqrt{k} \equiv 1 \mod v$ then $d_i = v - 1$ for any element $i$ and $d_{j \neq i} = -1$ for the other elements.*
- *If $\sqrt{k} \equiv -1 \mod v$ then $d_i = 1 - v$ for any element $i$ and $d_{j \neq i} = 1$ 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 in terms of digressions.

Considering (8) for non-identity elements we can notice that a any particular multiplicity will be involved in two of the products—once as $i$ and once as $i + q$

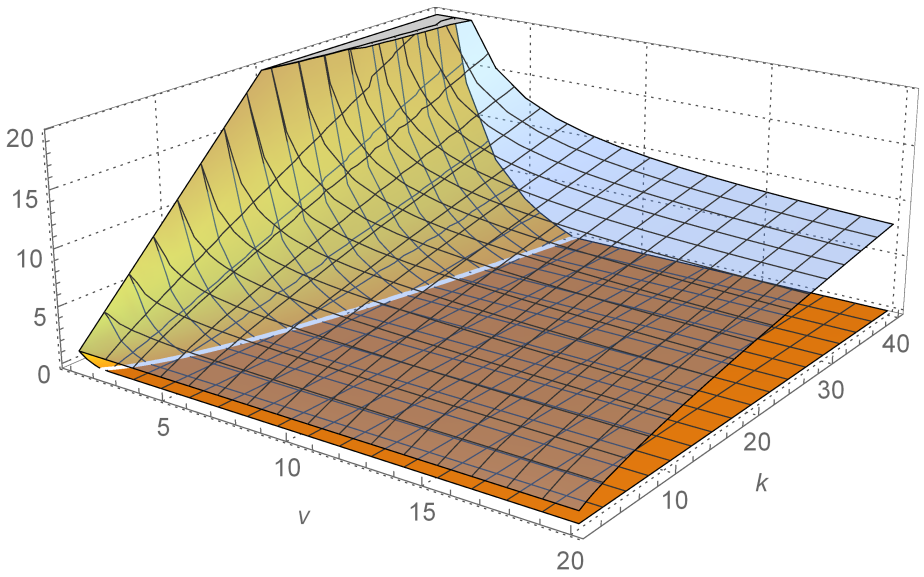


Figure 2: Lower and upper limits for the values of $n_q$ with respect to $v$ and $k$.

(but not both at the same time as we consider non-identity $q$ now). Other $v-2$ products are destined to contain other multiplicities solely which leads us to true equation.

$$\sum d_i d_{i+q} = -2(v-1) + (v-2) = -v \tag{14}$$

In case we're dealing with a loop, we must consider the case of $q$ being the identity which is also shown to be true.

$$\sum d_i^2 = (\pm(v-1))^2 + (v-1)(\mp 1)^2 = v^2 - v \tag{15}$$

It is straightforward to check that (6) turns out true as well. □

### 4.3 Difference multisets for cyclic groups of even size

For loops we can rewrite (9):

$$Cg' = \mathbf{v}' \tag{16}$$

where $g'_q : i \to (d_i d_q)$ and $v'_q = v(v\delta_{q0} - 1)$.

As the operation of $g'$ is pretty trivial, we can write it even more nicely:

$$Dd = \mathbf{v}' \tag{17}$$

where $D_{ij} = d_{C_{ij}}$ (i.e. replace elements in Cayley table with their digressions) and $d_q = d_q$.

As the title suggests, we will be dealing with cyclic groups in this section. That's because of the nice Cayley table they possess. The Cayley table of cyclic groups of size $v$ takes the following form:

$$\begin{pmatrix} 0 & 1 & 2 & \cdots & v-2 & v-1 \\ 1 & 2 & 3 & \cdots & v-1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ v-2 & v-1 & 0 & \cdots & v-4 & v-3 \\ v-1 & 0 & 1 & \cdots & v-3 & v-2 \end{pmatrix} \tag{18}$$

This is a special case of Hankel matrix sometimes called *anticirculant matrix*. The structure of the corresponding $D$ will be the same.

### 4.3.1 Solving equations with anticirculant matrices

We weren't able to track down a source dealing with matrices like (18), however it's fairly straightforward to apply the same methods as with circulant matrices [9].

Let's consider the equation $Ax = b$ with an anticirculant $v \times v$ matrix

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{v-1} \\ a_1 & a_2 & a_3 & \cdots & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} \tag{19}$$

and a vector $b = (b_0, b_1, b_2, \dot{:})^T$.

Denote $a = (a_1, \ldots, a_{v-1})$. We can now express the equation row by row (please consider indices $\mod v$):

$$b_j = \sum_{k=0}^{v-1} a_{j+k} x_k \tag{20}$$

Apply discrete Fourier transform:

$$\mathcal{F}(b)_m = \sum_{j=0}^{v-1} b_j \exp\left(-2\pi i \frac{jm}{v}\right) \tag{21}$$

Insert $b_j$ obtaining

$$\begin{aligned} \mathcal{F}(b)_m &= \sum_{j=0}^{v-1} \sum_{k=0}^{v-1} a_{j+k} x_k \exp\left(-2\pi i \frac{jm}{v}\right) \\ &= \sum_{j=0}^{v-1} \sum_{k=0}^{v-1} x_k \exp\left(2\pi i \frac{km}{v}\right) a_{j+k} \exp\left(-2\pi i \frac{(j+k)m}{v}\right) \\ &= \sum_{k=0}^{v-1} x_k \exp\left(2\pi i \frac{km}{v}\right) \sum_{j'=k}^{v+k-1} a_{j'} \exp\left(-2\pi i \frac{j'm}{v}\right) \end{aligned} \tag{22}$$

Looking at the inner sum we should note that not only we take indices mod $v$ but the $j'$ in the exponent can be taken mod $v$ as well. Let's use $j'' = j' \mod v$.

$$\sum_{j'=k}^{v+k-1} a_{j'} \exp\left(-2\pi i \frac{j'm}{v}\right) = \sum_{j''=0}^{v-1} a_{j''} \exp\left(-2\pi i \frac{j''m}{v}\right) = \mathcal{F}(a)_m \tag{23}$$

We can now finish the transformation:

$$\begin{aligned} \mathcal{F}(b)_m &= \sum_{k=0}^{v-1} x_k \exp\left(2\pi i \frac{km}{v}\right) \mathcal{F}(a)_m \\ &= \mathcal{F}(a)_m (\sum_{k=0}^{v-1} x_k^* \exp\left(-2\pi i \frac{km}{v}\right))^* \\ &= \mathcal{F}(a)_m \mathcal{F}^*(x^*)_m = v\mathcal{F}(a)_m \mathcal{F}^{-1}(x)_m \end{aligned} \tag{24}$$

The final form (exploiting the Fourier transform property $\mathcal{F}^{-1}(x) = \mathcal{F}^*(x^*)/v$) was included for completeness as it allows to explicitly express $x = \mathcal{F}\left(\frac{1}{v}\frac{\mathcal{F}(b)}{\mathcal{F}(a)}\right)$. However, we will use $\mathcal{F}(b)_m = \mathcal{F}(a)_m \mathcal{F}^*(x^*)_m$.

## 4.4 Solving the digression equation

The $D$ and $d$ in equation $Dd = \mathbf{v}'$ is linked in the same way as $A$ and $a$ in subsection 4.3.1. The image of $Dd = \mathbf{v}'$ is

$$\mathcal{F}(\mathbf{v}')_m = \mathcal{F}(d)_m \mathcal{F}^*(d^*)_m \tag{25}$$

As we are only interested in real $d$, we can even simplify it to

$$\mathcal{F}(\mathbf{v}')_m = \mathcal{F}(d)_m \mathcal{F}^*(d)_m = |\mathcal{F}(d)_m|^2 \tag{26}$$

Putting the identity first we have $\mathbf{v}' = (v^2 - v, -v, -v, \ldots)$ and $\mathcal{F}(\mathbf{v}') = (0, v^2, v^2, \ldots)$. Thus (26) becomes

$$\left|\sum_{j=0}^{v-1} d_j \exp\left(-2\pi i \frac{jm}{v}\right)\right| = v(1 - \delta_{m0}) \tag{27}$$

Note that for any $m|v$

$$\left|\sum_{j=0}^{v-1} d_j e^{\frac{-2\pi i m j}{v}}\right| = \left|\sum_{j=0}^{v/m-1} \sum_{k=0}^{m-1} d_{j+kv/m} e^{\frac{-2\pi i m j}{v}}\right| = v(1 - \delta_{m0}) \tag{28}$$

as

$$e^{\frac{-2\pi i m(j+kv/m)}{v}} = e^{\frac{-2\pi i m j}{v}} e^{-2\pi i k} = e^{\frac{-2\pi i m j}{v}} \tag{29}$$

**Theorem 4.3.** *In cyclic groups of even cardinality* $\sum_{k=0}^{v/2-1} d_{2k} = \pm\frac{v}{2}$ *and* $\sum_{k=0}^{v/2-1} d_{2k+1} = \mp\frac{v}{2}$.

*Proof.* Take (28) for $m = v/2$

$$\left| \sum_{k=0}^{v/2-1} d_{2k} - \sum_{k=0}^{v/2-1} d_{2k+1} \right| = v \tag{30}$$

We've split $d$ in half and got that total of one half is by $v$ larger than the total of the other half. The statement of the theorem follows as soon as we remember the grand total $\sum d_i = 0$. □

# 5 Smallest difference multisets

Bulk of our results concern difference multisets with small $v$. But let's start from zero.

## 5.1 Trivial cases

We should 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 quasigroup $Q$ you can take no elements to make a $(Q, 0)$-difference multiset or a single element once to form a $(Q, 1)$-difference multiset. In both of these cases $\lambda = 0$ i.e. the difference multiset produces every element of $Q$ exactly 0 times.

An exception to the above arises when we take the empty quasigroup combined with $k = 1$—one can't take a single element from it so there is no $(\{\,\}, 1)$-difference multiset unfourtunately.

## 5.2 The two-element group

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

This case was solved by Buratti [3]. We will provide a solution for this case for completeness of low-parameter cases.

**Theorem 5.1.** $(\mathbb{Z}_2, k)$*-difference multiset exists whenever* $k$ *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.* Theorem 4.3 provides $d_0 = \pm 1$ and $d_1 = \mp - 1$.

Notice that these $d_i$ produce integer $n_i = \frac{k+d_i\sqrt{k}}{2}$ whenever $k$ is a square. □

*Remark* 5.2. We did not bother to discuss the case of non-square $k$ as it is proven in [2] (see theorem 2.3) that there can only be a difference multiset over abelian group with an even $v = |G|$ if the $k$ is square.

# 6 Difference multisets over the 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 (5) to form a system of equations.

$$\begin{cases} 3\lambda = k(k-1) \\ \sum n_i = k \\ \sum n_i n_{i+1} = \lambda \end{cases} \tag{31}$$

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

**Theorem 6.1.** *Multiplicities of different $(\mathbb{Z}_3, k)$-difference multiset elements $i$ un $j$ are related via*

$$n_{i \neq j} = \frac{k - n_j \pm \sqrt{\frac{4k-(k-3n_j)^2}{3}}}{2} \tag{32}$$

*Proof.* Take any element $\gamma \in \mathbb{Z}_3$ and assign $c = n_\gamma$. Let's use $\alpha$ and $\beta$ to name the remaining elements of $\mathbb{Z}_3$. The system (31) can now be rewritten:

$$\begin{cases} n_\alpha + n_\beta = k - c \\ n_\alpha n_\beta + c(n_\alpha + n_\beta) = \lambda \end{cases} \tag{33}$$

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

$$\begin{cases} n_\alpha + n_\beta = k' \\ n_\alpha n_\beta = \lambda' \end{cases} \tag{34}$$

Eliminating $n_\beta$ we arrive at a quadratic equation that is solved into

$$n_\alpha = \frac{k' \pm \sqrt{k'^2 - 4\lambda'}}{2} \tag{35}$$

Undo the substitutions and you're done. □

Considering the multiplicities in form of $n_i = \frac{k+\Delta_i}{3}$, we can restate (32) into the following.

$$n_{i\neq j} = \frac{k - n_j \pm \sqrt{\frac{4k-\Delta_j^2}{3}}}{2} \tag{36}$$

The rest of analysis focuses on the $\Delta_i$ 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 6.2.** Number $k$ is called a Löschian number if $\exists a, b \in \mathbb{Z}$: $a^2 + ab + b^2 = k$.

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 6.3.** *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 $a', b'$: $a'^2 + a'b' + b'^2 = k$. 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 $a \geq b \geq 0$.

□

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

**Lemma 6.4.** *There exists a $\Delta$ that makes $\frac{4k-\Delta^2}{3}$ a perfect square iff $k$ is Löschian number.*

*$\Delta$ 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 $\Delta$ that makes $\frac{4k-\Delta^2}{3}$ into square.*

*Proof.* For a Löschian number $k = a^2 + ab + b^2$ take $\Delta$ 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:

$$z^2 = \frac{4k - \Delta^2}{3} \tag{37}$$

Rewrite

$$\frac{3z^2 + \Delta^2}{4} = k \tag{38}$$

Noticing that 4 divides $3z^2 + \Delta^2$ we can conclude that $z$ and $\Delta$ 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 $\Delta$ 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 $2a + b = \Delta$.

□

Let's introduce the following notation for the three values used in lemma 6.4. The rest can be expressed as $-\Delta_i$:

$$\Delta_\alpha = 2a + b, \Delta_\beta = -a - 2b, \Delta_\gamma = -a + b \tag{39}$$

These $\Delta_i$ will be used in the following theorem and $\alpha$, $\beta$ and $\gamma$ 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 6.5.** *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 6.4, the expression (36) will equal integer only if $k$ is a Löschian number and $\Delta_j$ is one of the listed on (39) or a negative of that.

Insert the constructions listed in (6.5) into (32) to check that these are indeed multiplicities that make up a difference multiset if the numbers are whole. One can also check that using $\Delta_\alpha$ to construct one of the multiplicities you will notice $\Delta_\beta$ and $\Delta_\gamma$ 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.

□

*Remark* 6.6. 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 6.5 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 $-(k+1) \mod 3$.

## 6.1 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

$$k = 3^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots q_1^{\beta_1} q_2^{\beta_2} \dots \tag{40}$$

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 $\beta_i$ are odd, there are no integer solutions to $k = a^2 + ab + b^2$. But if all of $\beta_i$ are even, the number of solutions is $6 \prod(\alpha_i + 1)$.

It is hypothesised [7] that the number of solutions (if every $\beta_i$ is even) having $a \geq b \geq 0$ is $1/2 + \prod(\alpha_i + 1)/2$ if all the $\alpha_i$ 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.

## 6.2 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.

$$\begin{cases} n_0(n_0 - 1) + 2n_1 n_2 = \frac{k(k-1)}{3} \\ n_1(n_1 - 1) + 2n_2 n_0 = \frac{k(k-1)}{3} \\ n_2(n_2 - 1) + 2n_0 n_1 = \frac{k(k-1)}{3} \\ n_0 + n_1 + n_2 = k \end{cases} \tag{41}$$

It can be noticed with ease that (41) 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 2.4. 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 (31) or the system (41). 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.

# 7 Other decent cases

## 7.1 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.

$$\begin{cases} \sum d_i^2 = 12 \\ \sum d_i = 0 \\ d_{00}d_{01} + d_{10}d_{11} = -2 \\ d_{00}d_{10} + d_{01}d_{11} = -2 \\ d_{00}d_{11} + d_{10}d_{01} = -2 \end{cases} \tag{42}$$

**Theorem 7.1.** *$(\mathbb{Z}_2 \times \mathbb{Z}_2, k)$–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 (42) to find eight solutions each having one $d_i = \pm 3$ and the rest $d_{j\neq i} = \mp 1$.

Notice that these numbers yield integer $n_i = \frac{k+d_i\sqrt{k}}{4}$ values in and only in the cases described in theorem. □

## 7.2 Difference multisets over $\mathbb{Z}_4$

It is easy to check that all of the solutions stated in theorem 7.1 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 $\lambda$ is even).

However, our numerical experiments show that the one or two solutions given in 7.1 are not the only ones working for this group. Smallest of the solutions

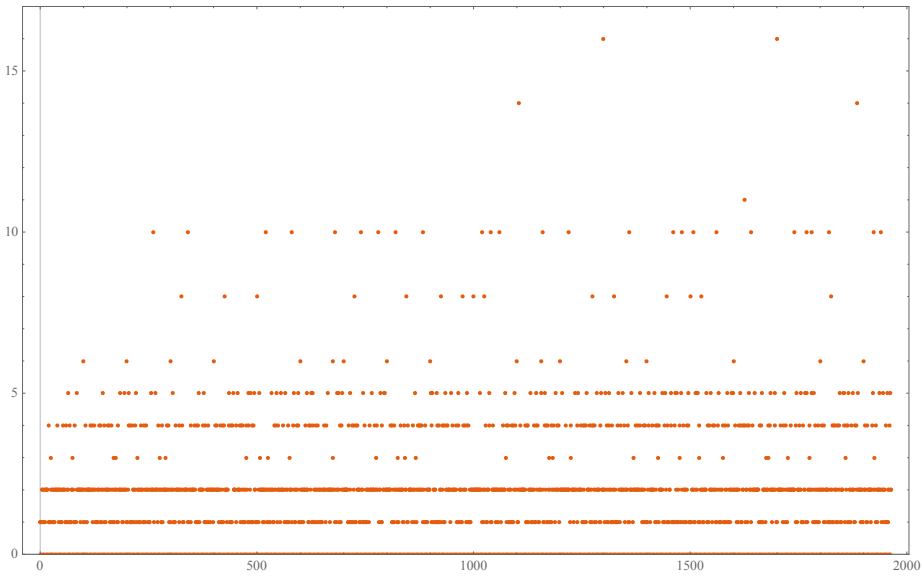


Figure 3: Number of $(\mathbb{Z}_4, k)$-difference multisets (excluding automorphisms) with respect to $\sqrt{k}$.

not constructed in theorem 7.1 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 3. One can observe that with $k$ increasing we have cases of more and more solutions that can't be explained by the known construction.

### 7.3 Difference multisets over $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

**Theorem 7.2.** *A $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, k)$-difference multiset can only be constructed by taking multiplicities $n_i$ with the following digressions:*

- *If $\sqrt{k} \equiv -1 \mod 8$ take $d_i = -7$ for any $i$ and $d_j = 1$ for other $j \neq i$.*
- *If $\sqrt{k} \equiv 1 \mod 8$ take $d_i = 7$ for any $i$ and $d_j = -1$ for other $j \neq i$.*
- *If $\sqrt{k} \equiv 0 \mod 8$ choose any element $i$ and three distinct elements $j_1, j_2, j_3$ such that $j_1 + j_2 + j_3 = 0$. Set $d_i = \pm 5$ and $d_{i+j_1} = d_{i+j_2} = d_{i+j_3} = \mp 3$ and let the other four $d_k = \pm 1$. Besides, both of the above solutions will work as well.*

*Proof.* Write down (6) and (8) for this case:

$$\begin{cases} d_{000}+d_{001}+d_{010}+d_{011}+d_{100}+d_{101}+d_{110}+d_{111}=0 \\ d_{001}^2+d_{010}^2+d_{010}^2+d_{011}^2+d_{100}^2+d_{101}^2+d_{110}^2+d_{111}^2=56 \\ d_{000}d_{001}+d_{010}d_{011}+d_{100}d_{101}+d_{110}d_{111}=-4 \\ d_{000}d_{010}+d_{001}d_{011}+d_{100}d_{110}+d_{101}d_{111}=-4 \\ d_{000}d_{011}+d_{001}d_{010}+d_{100}d_{111}+d_{101}d_{110}=-4 \\ d_{000}d_{100}+d_{001}d_{101}+d_{010}d_{110}+d_{011}d_{111}=-4 \\ d_{000}d_{101}+d_{001}d_{100}+d_{010}d_{111}+d_{011}d_{110}=-4 \\ d_{000}d_{110}+d_{001}d_{111}+d_{010}d_{100}+d_{011}d_{101}=-4 \\ d_{000}d_{111}+d_{001}d_{110}+d_{010}d_{101}+d_{011}d_{100}=-4 \end{cases} \tag{43}$$

Solve to obtain the given solutions and notice that they yield integer $n_i = \frac{k+d_i\sqrt{k}}{8}$ whenever $\sqrt{k}$ behaves as described in the cases of theorem. □

# 8 Conclusions

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 6.5) 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 $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is another promising direction. A new construction (theorem 4.2) 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.

And lastly, theorem 4.1 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.

[9] Wikipedia contributors. Circulant matrix — Wikipedia, the free encyclopedia, 2018. [Online; accessed 19-September-2018].