Difference multisets*

Juris Evertovskis and Juris Smotrovs

Faculty of Computing, University of Latvia

e-mail: juris.evertovskis@lu.lv, juris.smotrovs@lu.lv

Abstract

Difference multiset is a combinatorial design introduced by Buratti [5] and used to construct other combinatorial designs like regular difference families. In this paper we obtain multiple constructions and constraints for difference multisets. We also focused on a few particular cases with small parameter values and found all the difference multisets over some smaller algebraic structures. 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 Introduction

1.1 Difference multisets

Difference multiset is a combinatorial design similar to difference set.

The classical difference set D in a finite group G is such a subset of G that produces every non-zero $\gamma \in G$ 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 $\mathbb{Z}_3$. A less trivial and more famous example is the set $\{1, 2, 4\} \subset \mathbb{Z}_7$.

If we take a multiset instead, we can produce the whole G, including the identity element. 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 is called a difference multiset. Note that we take differences between pairs of elements not an element and itself (i.e. there was $0 - 0 = 0$ as first zero subtracted from the second zero and vice versa but not the first zero from itself and no $1 - 1$).

While difference sets have been studied at least since 1939 [4], difference multisets were first investigated on their own in 1999 by Buratti [5] who noticed that such designs (and the related strong difference families) are indirectly used by other authors in constructions of various combinatorial designs. The paper defined the concept of a difference multiset and presented its basic properties and some constructions. The topic was developed further by other authors [2, 1]

(they used the term "regular difference covers" instead of "difference multisets") who introduced new constructions and several nonexistence theorems.

The results in the foundational articles are mostly analogous to those of difference sets, almost all of the constructions are based on some difference set construction. As a result the number of difference multisets constructed in a given finite group 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 presented in [8] and we strive to expand in this direction—constructing arbitrarily large multisets in fixed, mainly small algebraic structures.

1.2 Synopsis

We study the difference multisets using a system of quadratic and linear equations on the multiplicities of their elements. We show that these multiplicities of any difference multiset over a loop are in a sense close to their average. This leads to the next idea of studying their digressions from the average which allows describing difference multisets with a simpler equation system.

Using these tools we find a construction that allows to produce an infinite number of difference multisets over any group. Focusing on groups $\mathbb{Z}_2^i$, we obtain a more general construction that includes the previous one as a special case, and also provides all multisets for $\mathbb{Z}_2^i$ for at least $i \leq 3$.

We also solve the problem of difference multisets of all quasigroups of cardinality 3. Interestingly, the possible sizes of difference multisets over $\mathbb{Z}_3$ turn out to be Löschian numbers.

2 Definitions, notation and statement of the problem

When describing large or arbitrary multisets over a fixed group, it's convenient to use the multiplicity function n: the number of instances an element μ is found in a multiset M will be denoted as $n(\mu, M)$ or simply n_μ if the multiset is obvious from the context.

Let G be an additive commutative group and $M = \{\mu_1, \mu_2, \ldots, \mu_k\}$ be a multiset over G. Let us denote by $\mathcal{D}(M)$ the multiset generated by the differences of elements of M with different indices: $\mathcal{D}(M) = \{\mu_i - \mu_j \mid i, j \in \{1, 2, \ldots, k\} \wedge i \neq j\}$.

Definition 2.1. A multiset M of cardinality k is called a (G, k)-difference cover iff $\forall \gamma \in G \colon \gamma \in \mathcal{D}(M)$.

In particular we are interested in difference covers for which $\mathcal{D}(M)$ is regular: it contains each element of G the same number of times.

Definition 2.2. A (G, k)-difference cover M is called a (G, k)-difference multiset (a.k.a. regular difference cover) if $\exists \lambda \forall \gamma \in G \colon \lambda = n(\gamma, \mathcal{D}(M))$.

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 notation $v = |G|$. Commonly a (G, k)-difference multiset would be called a (G, k, λ) (or (v, k, λ)) difference multiset, but we omit λ as it is a function of v and k (see identity (3) below).

2.1 The mathematical apparatus

First, note that the cardinality of (G, k)-difference multiset is equal to the total of multiplicities. We will omit the summation index and bounds where they are clear from the context. Suppose that all sums are over $\mu \in G$ unless stated otherwise.

$$\sum n_\mu = k. \tag{1}$$

Now let us restate definition 2.2 in terms of n. Each element γ must appear λ times as a difference $(\gamma + \mu) - \mu$. For non-identity γ we obtain the number of γ's occurrences by multiplying the multiplicities $n_{\gamma+\mu} n_\mu$ and summing over $\mu \in G$. For the identity we will use Kronecker delta to omit the trivial differences (i.e. $\mu_i - \mu_i$ where $M = \{\mu_1, \ldots, \mu_k\}$ is the multiset):

$$\forall \gamma \in G\colon \sum (n_\mu(n_{\gamma+\mu} - \delta_{\gamma 0})) = \lambda. \tag{2}$$

We can observe that the number of non-trivial differences is equal to the 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 [5]:

$$v\lambda = k(k-1). \tag{3}$$

(As is well known, a similar identity holds for the common difference sets.)

These equations serve as the main tools in our investigation. Finding a (G, k)-difference multiset is the same as finding a set of non-negative integer n_μ's that satisfy the above equations.

It is useful to notice that equation (1) defines a hyperplane and equations (2) define second-order surfaces. Under this interpretation we are looking for lattice points on the intersection of all the surfaces defined by these equations.

2.2 Digressions

By applying the substitution $n_\mu = \frac{k + d_\mu \sqrt{k}}{v}$ we can rewrite the previous equations in terms of digressions d_μ:

$$\sum d_\mu = 0 \tag{4}$$

$$\forall \gamma \in G\colon \sum d_\mu d_{\gamma+\mu} = v(v\delta_{\gamma 0} - 1). \tag{5}$$

This makes it a bit simpler to find a solution in terms of d_μ, but the cost is that we must afterwards test if the solution produces integer n_μ.
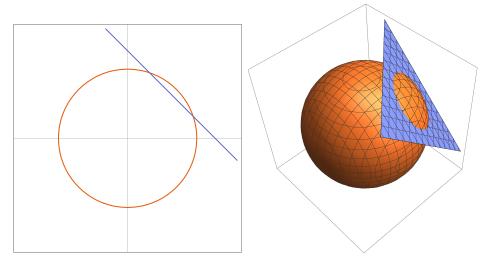
Figure 1: The $\sum n_\mu = k$ and $\sum n_\mu^2 = k + \lambda$ surfaces in two and three dimensions.

3 Main results

3.1 Limits for multiplicities

Considering difference multisets over an arbitrary abelian group one can notice that some of the surfaces defined by our equations are always the same. There is always the hyperplane $\sum n_\mu = k$ and the hypersphere $\sum n_\mu^2 = k + \lambda$ centered at the origin (see Figure 1).

The second equation confines every multiplicity: $n_\mu \leq \sqrt{k + \lambda}$. By investigating the intersection more thoroughly we discover that the multiplicities are actually bound to be near to their average k/v.

Theorem 3.1. *If M is a (G, k)-difference multiset and $|G| = v$ then*

$$\forall \gamma \in G \colon \qquad \frac{k - (v-1)\sqrt{k}}{v} \leq n(\gamma, M) \leq \frac{k + (v-1)\sqrt{k}}{v} \qquad (6)$$

Proof. Take equation (2) for the identity element and equation (1) as constraints:

$$\begin{cases} \sum n_\mu = k \\ \sum (n_\mu(n_\mu - 1)) = \lambda. \end{cases} \qquad (7)$$

Let us optimize $n_\gamma = n(\gamma, M)$ respecting the constraints. Add the first equation to the second and move all the terms to the left hand side:

$$\begin{cases} k - \sum n_\mu = 0 \\ k + \lambda - \sum n_\mu^2 = 0. \end{cases} \qquad (8)$$
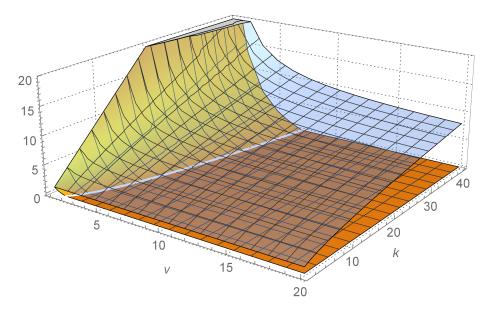
4

Figure 2: Lower and upper bounds for the values of n_γ with respect to v and k.

We apply the method of Lagrange multipliers to obtain the maximum and minimum of n_γ.

We use the following Lagrange function (λ_1 and λ_2 here is the standard Lagrange multiplier notation and have nothing in common with the parameter λ).

$$\mathcal{L} = n_\gamma - \lambda_1(k - \sum n_\mu) - \lambda_2(k + \lambda - \sum n_\mu^2) \tag{9}$$

By a standard application of this method the bounds of the theorem statement are obtained. We omit the routine calculations. □

Theorem 3.1 suggests using digressions instead of multiplicities (thus simplifying the equations) and greatly reduces the amount of options for every n_γ. This simplification allows decent computer searches which enabled us to discover some of the patterns that led to results presented in this paper.

3.2   A family of difference multisets for every abelian group

Theorem 3.2. *If $\sqrt{k}$ is integer and congruent to 0 or $\pm 1 \mod v$ then a (G, k)-difference multiset exists with the following digressions.*

- *If $\sqrt{k} \equiv 1 \mod v$ then $d_\mu = v - 1$ for any single element μ and $d_{\nu \neq \mu} = -1$ for the other elements.*

- *If $\sqrt{k} \equiv -1 \mod v$ then $d_\mu = 1 - v$ for any single element μ and $d_{\nu \neq \mu} = 1$ for the other elements.*

5

- *Both of the above constructions if $\sqrt{k} \equiv 0 \mod v$.*

Proof. The conditions on the values of k and d_μ guarantee that the multiplicities $n_\mu = \frac{k + d_\mu \sqrt{k}}{v}$ are integers. It is left to demonstrate that they form a difference multiset.

Considering equation (5) for non-identity elements we can notice that the digression $\pm(v-1)$ (as any other digression) is involved in two of the products— once as d_μ and once as $d_{\gamma+\mu}$.

Other $v - 2$ products are $(\pm 1) \cdot (\pm 1)$, thus the condition is satisfied:

$$\sum d_\mu d_{\gamma+\mu} = 2(\pm(v-1) \cdot (\mp 1)) + (v-2)(\mp 1)^2 = -v. \tag{10}$$

The condition for the identity $\gamma = 0$ is also satisfied:

$$\sum d_\mu^2 = (\pm(v-1))^2 + (v-1)(\mp 1)^2 = v^2 - v. \tag{11}$$

It is straightforward to check that equation (4) is satisfied as well. $\qquad\square$

3.3 Difference multisets for cyclic groups

Let us consider (5) in matrix form

$$Dd = \mathbf{v} \tag{12}$$

where $d = (d_0, d_1, \ldots, d_{v-1})^T$, $\mathbf{v} = (\mathbf{v^2} - \mathbf{v}, -\mathbf{v}, -\mathbf{v}, \ldots)^{\mathbf{T}}$ and $D_{\mu\nu} = d_{\mu+\nu}$, i.e. it is the Cayley table of the group in question.

For cyclic groups the matrix D takes the form of an *anticirculant* or *left circulant* matrix:

$$D = \begin{pmatrix} d_0 & d_1 & d_2 & \cdots & d_{v-1} \\ d_1 & d_2 & d_3 & \cdots & d_0 \\ d_2 & d_3 & d_4 & \cdots & d_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{v-2} & d_{v-1} & d_0 & \cdots & d_{v-3} \\ d_{v-1} & d_0 & d_1 & \cdots & d_{v-2} \end{pmatrix}. \tag{13}$$

We will use the discrete Fourier transform:

$$\mathcal{F}(y)_m = \sum_{j=0}^{v-1} y_j \omega^{-jm} \tag{14}$$

where $\omega = \exp(\frac{2\pi i}{v})$. Let us consider an equation $Ax = b$ with anticirculant matrix A. Applying the discrete Fourier transform to b we obtain

$$\mathcal{F}(b)_m = \mathcal{F}(a)_m \mathcal{F}^*(x^*)_m, \tag{15}$$

where a is the first row of A.

This is particulary useful for equation (12) as the vector d is also the first row of matrix D. The image of $\mathbf{v} = \mathbf{D}d$ is

$$\mathcal{F}(\mathbf{v})_m = \mathcal{F}(d)_m \mathcal{F}^*(d^*)_m. \tag{16}$$

As we are only interested in real d, we can simplify it further:

$$\mathcal{F}(\mathbf{v})_m = \mathcal{F}(d)_m \mathcal{F}^*(d)_m = |\mathcal{F}(d)_m|^2. \tag{17}$$

Since $\mathbf{v} = (v^2 - v, -v, -v, \ldots)^T$ we can find that $\mathcal{F}(\mathbf{v}) = (0, v^2, v^2, \ldots)$ and (17) becomes

$$\left| \sum_{\mu=0}^{v-1} d_\mu \omega^{-\mu m} \right| = v(1 - \delta_{m0}). \tag{18}$$

Theorem 3.3. *The digressions of a $(\mathbb{Z}_v, k)$-difference multiset are related via equation*

$$\left| \sum_{\kappa=0}^{v/m-1} \omega^{-m\kappa} \cdot \sum_{\nu=0}^{m-1} d_{\kappa + \nu v/m} \right| = v \tag{19}$$

where m is any divisor of v and $\omega = \exp(\frac{2\pi i}{v})$.

Proof. The theorem statement is obtained from (18).

Select a divisor m of v. Then $\delta_{m0} = 0$ on the right hand side. The left hand side is transformed and grouped into smaller cycles using the following relation:

$$\omega^{-m(\kappa + \nu v/m)} = \omega^{-m\kappa} \omega^{-\nu v} = \omega^{-m\kappa}. \tag{20}$$

$\square$

Proposition 3.4. *In difference multistes over cyclic groups of even cardinality $\sum_{\mu=0}^{v/2-1} d_{2\mu} = \pm\frac{v}{2}$ and $\sum_{\mu=0}^{v/2-1} d_{2\mu+1} = \mp\frac{v}{2}$.*

Proof. Take (19) for $m = v/2$

$$\left| \sum_{\mu=0}^{v/2-1} d_{2\mu} - \sum_{\mu=0}^{v/2-1} d_{2\mu+1} \right| = v. \tag{21}$$

I.e. the total of even d_μ's and the total of odd d_μ's differ by v. Take into account that the grand total is $\sum d_\mu = 0$ and the proposition follows. $\square$

Remark 3.5. Similar relation also holds true for some (many? all?) other structures that are not cyclic groups. For example in $\mathbb{Z}_2 \times \mathbb{Z}_2$ with elements $\{\mu, \nu, \zeta, \eta\}$ in any order we have $(d_\mu + d_\nu) - (d_\zeta + d_\eta) = \pm 4$.

3.4 Difference multisets over $\mathbb{Z}_2^i$

Consider $\mathbb{Z}_2^i$ as an affine space over $\mathbb{Z}_2$. For a chosen affine frame F, each element $\mu \in \mathbb{Z}_2^i$ can be represented by its affine coordinates: $\mu = (\mu_1, \mu_2, \ldots, \mu_i)$. For $r \in \{1, 2, \ldots, i\}$ we define a subspace H_r^F as follows:

$$\mu \in H_r^F \iff \begin{cases} \mu_j = 1 & \text{for } j < r \\ \mu_r = 0 \end{cases} \tag{22}$$

and denote $\xi_r = \sum_{j=0}^{r} (-2)^j = (1 - (-2)^{r+1})/3$.

Theorem 3.6. *For an arbitrary affine frame F of $\mathbb{Z}_2^i$ and integer $m \colon 0 < m < i$, the following construction produces a $(\mathbb{Z}_2^i, k)$-difference multiset iff k is square and $v | \sqrt{k}$:*

1. *For each $\mu \in H_r^F$ where $r \leq m$, set $d_\mu = \xi_r$.*

2. *Select element $\nu \in \tilde{H}$ where $\tilde{H}$ is the subset containg elements that do not have their digression set yet: $\mu \in \tilde{H} \iff \mu \notin \bigcup_{r \leq m} H_r$.*

3. *Set $d_\nu = (-1)^m v + \xi_{m+1}$.*

4. *Set $d_\mu = \xi_{m+1}$ for all $\mu \in \tilde{H}$ such that $\mu \neq \nu$.*

A difference multiset is also obtained if the opposite sign is used on every d_μ.

Proof. For a selected $m \colon 0 < m < i$ this construction provides us with 2^{i-r} digressions of value $d_\mu = \xi_r$ for each $1 \leq r \leq m$ (none of these if $m = 0$), $2^{i-m} - 1$ digressions equal to ξ_{m+1} and one digression equal to $(-1)^m 2^i + \xi_{m+1}$.

Equations $\sum d_\mu = 0$ and $\sum d_\mu^2 = v(v-1)$ can be shown to be satisfied inserting the values listed above. Relation (23) can be useful.

Equations (5) are left to check for non-identity γ.

Having $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_i)$ with $\gamma_g = 1$ for some index g and $\gamma_r = 0$ for all $r < g$ we can observe that:

- $\mu \in H_r \iff \gamma + \mu \in H_r$ if $r < g \vee g > m$;

- $\mu \in H_r \iff \gamma + \mu \in H_g$ if $r > g \wedge g \leq m$;

- $\mu \in H_g \iff \gamma + \mu \in H_r$ where $r > g$ if $g \leq m$.

The H_F also counts as one of the H_r subsets whenever $r < g$ is not required to be true, one could loosely treat it as H_i subset.

Depending on the choice of γ the final sum can either contain $(2^{i-m} - 1)\xi_{m+1}^2 + ((-1)^m 2^i + \xi_{m+1})^2$ or $(2^{i-m} - 2)\xi_{m+1}^2 + 2\xi_{m+1}((-1)^m 2^i + \xi_{m+1})$ either of which evaluates to

We shall consider $g \leq m$ first. The value of (5) is:

$$\sum d_\mu d_{\gamma+\mu} = \sum_{r<g} \sum_{\mu \in H_r} d_\mu d_{\gamma+\mu} + \sum_{r>g} \sum_{\mu \in H_r} d_\mu d_{\gamma+\mu} + \sum_{\mu \in H_g} d_\mu d_{\gamma+\mu}$$

$$= \sum_{r<g} \sum_{\mu \in H_r} \xi_r^2 + 2 \sum_{r>g} \sum_{\mu \in H_r} \xi_g d_\mu$$

$$= \sum_{r<g} \sum_{\mu \in H_r} \xi_r^2 - 2\xi_g \sum_{r \leq g} \sum_{\mu \in H_r} \xi_r \qquad (23)$$

$$= \sum_{r<g} 2^{i-r} \xi_r^2 - 2\xi_g \sum_{r \leq g} 2^{i-r} \xi_r$$

$$= -v.$$

Considering $g > m$ we get the following:

$$\sum d_\mu d_{\gamma+\mu} = \sum_{r \leq m} \sum_{\mu \in H_r} d_\mu + \sum_{\mu \in F} d_\mu d_{\gamma+\mu}$$

$$= \sum_{r \leq m} 2^{i-r} \xi_r^2 + (2^{i-m} - 2)\xi_{m+1}^2 + 2\xi_{m+1}((-1)^m 2^i + \xi_{m+1}) \qquad (24)$$

$$= -v.$$

Lastly, by inserting $d_\mu = \xi_r$ into $n_\mu = \frac{k + d_\mu \sqrt{k}}{v}$ we can observe that integer n_μ is produced iff $v|\sqrt{k}$. $\qquad \square$

Remark 3.7. We could also allow to select $m = 0$ in Theorem 3.6. In that case the constructed difference multiset would be the same one encountered in Section 3.2 and it would also produce integer multiplicities for $k \equiv 1 \mod v$ or $k \equiv -1 \mod v$.

Theorem 3.8. *There are no other difference multisets than those presented in Theorem 3.6 for $i < 4$.*

Proof. This result was found directly solving equations (4) and (5). For $\mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ it can be done by hand.

For the case of $\mathbb{Z}_2^3$ it was done with the help of a computer algebra system. The single-variable polynomial of Gröbner basis in the case of $\mathbb{Z}_2^3$ is

$$d_\mu^8 - 84d_\mu^6 + 1974d_\mu^4 - 12916d_\mu^2 + 11025 \qquad (25)$$

for which the roots are $\pm\xi_1, \pm\xi_2, \pm\xi_3, \pm(8 - \xi_1)$. $\qquad \square$

We must mention that the result for $\mathbb{Z}_2$ was already known before[5].
The construction provided in this section produces

$$2 \sum_{j=2}^{i} 2^j \prod_{l=j+1}^{i} (2^{l+1} - 2) \qquad (26)$$

9

solutions for d_μ over $\mathbb{Z}_2^i$. The counting argument is that we can select H_1 in $2^{i+1} - 2$ ways, H_2 in $2^i - 2$ etc. until you stop and choose one of the remaining 2^j elements. And twice everything as you can flip the signs.

Example 3.9. Take $i = 4$ and $m = 2$. You will have eight $d_\mu = -1$, four $d_\mu = 3$, three $d_\mu = -5$ and one $d_\mu = 11$.

Example 3.10. Let's take $i = 4$ and $m = 3$. You get half the digressions (eight) $d_\mu = -1$. You set another quarter—four digressions $d_\mu = 3$. Then you set two $d_\mu = -5$. Halfspace with two elements remains. All except one are set to $d_\mu = 11$. And the last one is $-v + 11 = -5$ Thus you end up with the same set of digressions as in the previous example.

3.5 Difference multisets over the three element group

There is only one group of three elements, $\mathbb{Z}_3$.

For this group (3), (1) and (2) for a non-identity element form the following system of equations:

$$
\begin{cases}
3\lambda = k(k-1) \\
\sum n_\mu = k \\
\sum n_\mu n_{\mu+1} = \lambda.
\end{cases}
\tag{27}
$$

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

Theorem 3.11. *Multiplicities of different $(\mathbb{Z}_3, k)$-difference multiset elements μ un ν are related via*

$$
n_\mu = \frac{k - n_\nu \pm \sqrt{\frac{4k - (k - 3n_\nu)^2}{3}}}{2}.
\tag{28}
$$

Proof. Take any element $\nu \in \mathbb{Z}_3$ and assign $c = n_\nu$. Let us denote the two remaining elements of $\mathbb{Z}_3$ by α and β. The system (28) can now be rewritten:

$$
\begin{cases}
n_\alpha + n_\beta = k - c \\
n_\alpha n_\beta + c(n_\alpha + n_\beta) = \lambda.
\end{cases}
\tag{29}
$$

That is equivalent to a quadratic equation with the solution for $n_\mu = n_{\alpha,\beta}$ presented in the statement of the theorem.

$\square$

It is useful to consider the multiplicities in the form $n_\mu = \frac{k + \Delta_\mu}{3}$, then (29) can be rewritten as follows:

$$
n_\mu = \frac{k - n_\nu \pm \sqrt{\frac{4k - \Delta_\nu^2}{3}}}{2}.
\tag{30}
$$

The behaviour of expression under the root is tied to a topic in number theory called Löschian numbers [11]. These numbers make an appearance in a variety of fields (see comments in [11]).

Definition 3.12. Number k is called a Löschian number iff $\exists a, b \in \mathbb{Z}: a^2 + ab + b^2 = k$.

To eliminate unnecessary symmetries we will only consider a, b such that $a \geq b \geq 0$. This doesn't change the scope of Löschian numbers:

Lemma 3.13. *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. Let k be a Löschian number, then there are $a', b' \in \mathbb{Z}: a'^2 + a'b' + b'^2 = k$. We can obtain a, b with $a \geq b \geq 0$ as follows:

- If $a'b' \geq 0$, take $a = \max(|a'|, |b'|)$ and $b = \min(|a'|, |b'|)$.

- If $a'b' < 0$, set $c = \min(|a'|, |b'|)$ and take $a = \max(c, |a' + b'|)$, $b = \min(|c|, |a' + b'|)$.

$\square$

Lemma 3.14. *There exists Δ such that $\frac{4k - \Delta^2}{3}$ is a perfect square iff k is a Löschian number.*
If $k = a^2 + ab + b^2$, $a \geq b \geq 0$ is a Löschian number then $\frac{4k - \Delta^2}{3}$ is a square iff Δ has one of the values $\pm(2a + b), \pm(a + 2b), \pm(a - b)$.

Proof. Substituting $k = a^2 + ab + b^2$ and $\Delta = \pm(2a + b), \pm(a + 2b)$ or $\pm(a - b)$ in the expression $\frac{4k - \Delta^2}{3}$, we obtain, respectively, the squares b^2, a^2 or $(a + b)^2$.

On the other hand, if $\frac{4k - \Delta^2}{3}$ is a square, denote:

$$z^2 = \frac{4k - \Delta^2}{3}. \tag{31}$$

Rewrite

$$\frac{3z^2 + \Delta^2}{4} = k. \tag{32}$$

Since 4 divides $3z^2 + \Delta^2$, z and Δ are of the same parity. Thus 2 divides both $\Delta - z$ and $\Delta + z$.

By taking the following values of a, b, we obtain that $a^2 + ab + b^2 = k$, $a \geq b \geq 0$ (thus k is a Löschian number) and Δ is 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 $2a + b = \Delta$.

11

$\square$

Let's introduce the following notation for the three values used in lemma 3.14. The rest can be expressed as $-\Delta_i$:

$$\Delta_\alpha = 2a + b, \Delta_\beta = -a - 2b, \Delta_\gamma = -a + b \tag{33}$$

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 3.15. *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*

- $n_\mu = \frac{k + \Delta_\mu}{3}$ *for one and $n_\nu = \frac{k - \Delta_\nu}{3}$ for the other if $3 \mid k$.*

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

- $n_\mu = \frac{k - \Delta_\mu}{3}$ *if $3 \nmid k$ un $a - b \equiv 1 \mod 3$.*

Proof. According to lemma 3.14, the right hand side of (31) is integer only if k is a Löschian number and Δ_μ is one of the listed on (34) or a negative of that.

Insert the constructions listed in the statement of theorem into (29) to check that these are indeed multiplicities that make up a difference multiset if the numbers are integer. One can also check that using Δ_α to construct one of the multiplicities you will find Δ_β and Δ_γ used for the others and the same is true in any order.

Considering a and b modulo 3 one may check the following:

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

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

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

$\square$

Remark 3.16. 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 values of $a - b$ and thus all the constructions mentioned in 3.15 will be distinct. Consequently the number of $(\mathbb{Z}_3, k)$-difference multisets will be proportional to the number of unique a, b pairs (respecting constraints) and the coefficient of proportionality is $-(k+1) \mod 3$.

3.6 Estimating numbers

The exact number of solutions is still a bit elusive. This question is now reduced to a number-theoretic question—how many unique solutions are there for $k = a^2 + ab + b^2$ such that $a \geq b \geq 0$.

It is supposedly known [11] and reportedly shown in [3].

The number of solutions without the constraint is known [7], supposedly also [6] and references therein. Denote

$$k = 3^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots q_1^{\beta_1} q_2^{\beta_2} \dots \tag{34}$$

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 [9] 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 Generalizations

The concept of difference multisets can be generalized to non-abelian groups or even any other algebraic structures where *differences* can be defined. Such structures are generally known as *quasigroups*—algebras with a unique solution to $\gamma \cdot \mu = \nu$ (both when solving for γ and when solving for μ).

We shall consider right division, but the same logic can be applied to left division in the same manner. The element γ of a quasigroup Q must be obtained λ times as $(\gamma \cdot \mu)/\mu$. The generalization of (2) is:

$$\forall \gamma \in Q \colon \sum (n_\mu (n_{\gamma+\mu} - \delta_{\mu,\gamma\mu})) = \lambda \tag{35}$$

which coincides with system (2) in case of loops (quasigroups with an identity element)—if there is an identity element then $\delta_{\gamma 0} = \delta\mu, \gamma\mu$.

The digression equation (5) is generally more complex:

$$\forall \gamma \in Q \colon \sum \left(d_\mu \left(d_{\gamma\mu} - \frac{v \delta_{\mu,\gamma\mu}}{\sqrt{k}} \right) - v \delta_{\mu,\gamma\mu} \right) = -v. \tag{36}$$

However, in the case of loops system (37) simplifies to system (5).

4.1 Results

As the equation (5) applies for loops, the Theorem 3.1 is true for all loops.

Theorem 3.2 is also true for loops as it is proved used the equations that also hold for loops. However, we can prove a stronger result.

Theorem 4.1. *The construction given in Theorem 3.2 produces a difference multiset (with differences being the right divisions) iff $\exists \gamma \colon \forall \mu \colon \mu = \gamma\mu$.*

Proof. Consider a particular element $\gamma \in Q$.

Let Q_γ be the subset of such elements for which γ is left-identity-like:

$$\mu = \gamma\mu \iff \mu \in Q_\gamma \tag{37}$$

Denote $v_\gamma = |Q_\gamma|$ and $\overline{v_\gamma} = v - v_\gamma$.

We can rewrite (37) for γ:

$$\sum_{\mu \in Q}(d_\mu(d_\mu - \frac{v}{\sqrt{k}})) + \sum_{\mu \notin Q} d_\mu d_{\gamma\mu} = v(v_\gamma - 1). \tag{38}$$

Let us try to construct a difference multiset by selecting element $\nu \in Q$ and setting $d_\nu = \pm(v-1)$ and $d_{\mu \neq \nu} = \mp 1$.

If $\nu \in Q_\gamma$ then $v_\gamma \neq 0$ and equation (39) becomes

$$(v-1)(v-1-\frac{v}{\sqrt{k}}) + (v_\gamma - 1)(1 + \frac{v}{\sqrt{k}}) + \overline{v_\gamma} = v^2 - v + v\frac{v}{\sqrt{k}}(v_\gamma - v) \tag{39}$$

which is only equal to $v(v_\gamma - 1)$ if $v_\gamma = v$.

If $\nu \notin Q_\gamma$ then $\overline{v_\gamma} \neq 0$ and equation (39) becomes

$$v_\gamma(1 + \frac{v}{\sqrt{k}}) + 2(1-v) + \overline{v_\gamma} - 2 = -v + v\frac{v_\gamma}{\sqrt{k}} \tag{40}$$

which is only equal to $v(v_\gamma - 1)$ if $v_\gamma = 0$.

The above conditions (v_γ always being 0 or v) are satisfied only if there is a left identity element γ. $\qquad\square$

The same can be shown for left division difference multisets of same structure which require a right identity element.

4.2   Other quasigroups of size 3

Šis vēl jāpārraksta, pagaidām tikai pārvietots uz šejieni. 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 (2) we start by writing down the ways to obtain each of the elements and requiring them to be equal ($\forall \gamma \in \mathbb{Z}_3 \lambda = \sum(n_\mu(n_{\mu-\gamma} - \delta_{\mu,\mu+\gamma}))$). Adding the $\sum n_\mu = k$ 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 (42) possesses symmetry with respect to all the elements of $\mathbb{Z}_3$. Besides this system can easily be solved explicitly – valid multisets of n_μ are $\{\frac{k}{3}, \frac{k}{3}, \frac{k}{3}\}$ and $\{\frac{k-1}{3}, \frac{k-1}{3}, \frac{k+2}{3}\}$.

14

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 over $\mathbb{Z}_3$ and $\mathbb{Z}_2^i$.

Recall remark **??**. 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 (28) or the system (42). 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   Conclusions

Here's a reference of difference multisets over small parameter values. Some trivial cases that formally satisfy the constraints (e.g. some produce every element 0 times) are also included as those have helped spotting patterns.

Parameters	Difference multisets
$v = 0$	Empty multiset works.
$k = 0$	Empty multiset.
$v = 1$	Take the identity k times for any k.
$k = 1$	Take single element, works for $v \geq 1$.
$\mathbb{Z}_2^i$	See section 3.4, possibly incomplete.
$\mathbb{Z}_3$	See section 3.5.
$v = 3$	See section 4.2.

The case of difference multisets over $\mathbb{Z}_3$ (theorem 3.15) shows that not only the very trivial cases can be solved explicitly. Although it is not straightforward to generalize our methods for arbitrary $\mathbb{Z}_i$, solving the problem for an odd prime value of i seems in the realm of possibility.

Theorem 3.1 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.

The mathematical apparatus we used is also applicable for many other cases. The results presented in this paper are the ones that are in some sense complete or general. Other than these cases the system (5) (or alternative forms) can be utilised to find some difference multisets or sets of their digressions in many small quasigroups.

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] Bruce C. Berndt. On a certain theta-function in a letter of ramanujan from fitzroy house. *Ganita*, 43(1-2):33–43, 1992.

[4] Raj Chandra Bose. On the construction of balanced incomplete block designs. *Annals of Eugenics*, 9(4):353–399, 1939.

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

[6] Michael Hirschhorn. A letter from fitzroy house. *American Mathematical Monthly*, 115, 06 2008.

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

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

[9] Umesh P Nair. Elementary results on the binary quadratic form aˆ 2+ ab+ bˆ 2. *arXiv preprint math/0408107*, 2004.

[10] Neil James Alexander Sloane. The On-Line Encyclopedia of Integer Sequences. . Sequence A077925.

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