Difference multisets

Abstract

Difference multiset is a combinatorial design introduced by Buratti [4] 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. But a multiset.

The classical difference set $D \subseteq G$ is such a set 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 $\mathbb{Z}_3$. 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 bit less trivial and more famous 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 $1 - 1$).

While difference sets have been studied at least since 1939 [3], difference multisets were first studied on their own in 1999 by Buratti [4] 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 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 based on 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 [7] and we strive to expand in this direction—constructing arbitrarily large multisets in a fixed, mainly small algebras.

1.2 Synopsis

We study the difference multisets using a system of mostly (and at most) quadratic 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 us to make infinite (but not very dense) amount of difference multisets over any quasigroup. Focusing on groups $\mathbb{Z}_2^i$ we got a hold of a more dense construction that not only produces infinitely many difference multisets, but also produce every multiset there is for $\mathbb{Z}_2^i$ for at least $i \leq 3$ (we are not sure about larger values of i but we suspect there are some more difference multisets there).

We also managed to solve the problem of difference multisets of quasigroups of cardinality 3. An interesting link is found—the possible sizes of difference multisets over $\mathbb{Z}_3$ are Löschian numbers.

2 Definitions, notation and formulation of the problem

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

$$|M| = k \land \forall \gamma \in M \colon \gamma \in Q \tag{1}$$

When describing large or arbitrary multisets over a fixed quasigroup, it's convenient to use the multiplicity function n: the number of instances element μ is found in M will be denoted as $n(\mu, M)$ or simply n_μ 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 $M = \{\, \mu_1, \dots \mu_k \,\}$ we only consider the differences $\mu_i - \mu_j$ where $i \neq j$ excluding the differences between an element and itself. Let's denote the multiset generated by this operation: $\mathcal{D}(M) = \{\, \mu_i - \mu_j \mid \mu_i, \mu_j \in M \land i \neq j \,\}$

Definition 2.2. A (Q, k)-multiset M is called a (Q, k)-difference cover if $\forall \gamma \in Q \colon \gamma \in \mathcal{D}(M)$.

In particular we are currently 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 number 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 $\exists \lambda \forall \gamma \in Q \colon \lambda = n(\gamma, \mathcal{D}(M))$.

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 $v = |Q|$. Commonly a (Q, k)-difference multiset would be called a (Q, k, λ) (or (v, k, λ)) difference multiset, but we omit the λ 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 (some articles 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 [5] 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.

2.1 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 $\mu \in Q$ if it seems reasonable.

$$\sum n_\mu = k \tag{2}$$

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

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

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 λ times.

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

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_μ'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.

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:

$$\sum d_\mu = 0 \tag{5}$$

$$\forall\gamma \in Q\colon \sum(d_\mu(d_{\mu+\gamma} - \frac{\delta_{\mu,\mu+\gamma}}{\sqrt{k}}) - v\delta_{\mu,\mu+\gamma}) = -v \tag{6}$$

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

$$\forall\gamma \in Q\colon \sum d_\mu d_{\mu+\gamma} = v(v\delta_{\gamma 0} - 1) \tag{7}$$

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.

3 Main results

3.1 Limits for multiplicities

Considering difference multisets over an arbirary loop (quasigroup with an identity) 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). You could notice right away that the second equation confines every multiplicity: $n_\mu \leq \sqrt{k+\lambda}$. 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 3.1. *If M is a (Q,k)-difference multiset then*

$$\forall\gamma \in Q\colon \frac{k-(v-1)\sqrt{k}}{v} \leq n(\gamma, M) \leq \frac{k+(v-1)\sqrt{k}}{v} \tag{8}$$

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

$$\begin{cases} \sum n_\mu = k \\ \sum(n_\mu(n_\mu - 1)) = \lambda \end{cases} \tag{9}$$

Let's optimize n_γ 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.

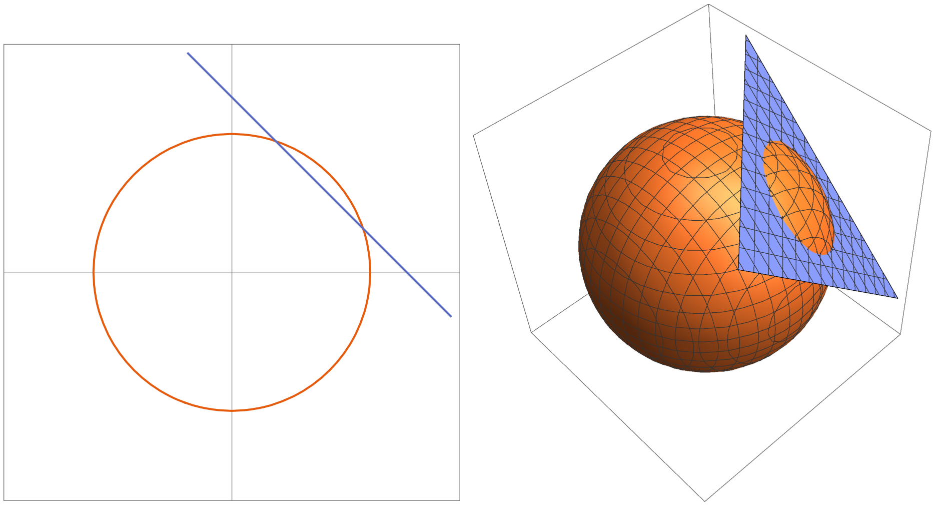

Figure 1: The $\sum n_\mu = k$ and $\sum n_\mu^2 = k+\lambda$ surfaces in two and three dimensions.

$$\begin{cases} k - \sum n_\mu = 0 \\ k + \lambda - \sum n_\mu^2 = 0 \end{cases} \tag{10}$$

We may now use a common optimization technique – Lagrange multipliers to obtain the maximum and minimum of n_γ honoring the constraints by using 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).

$$\mathcal{L} = n_\gamma - \lambda_1(k - \sum n_\mu) - \lambda_2(k + \lambda - \sum n_\mu^2) \tag{11}$$

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

Theorem 3.1 might appear uninspiring at first but it not only suggests using digressions instead of multiplicities (thus simplifying the equations) but also greatly reduces the amount of options for every n_γ. This simplification is a crucial stepping stone in making decent computer searches possible which allowed us to discover some of the patterns that lead to results presented in this paper.

3.2 A family of difference multisets for every quasigroup

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

Theorem 3.2. *(Q, k)-difference multiset exists if $v \mid \sqrt{k}$ or $\sqrt{k} \equiv \pm 1 \mod v$ and it's digressions are*

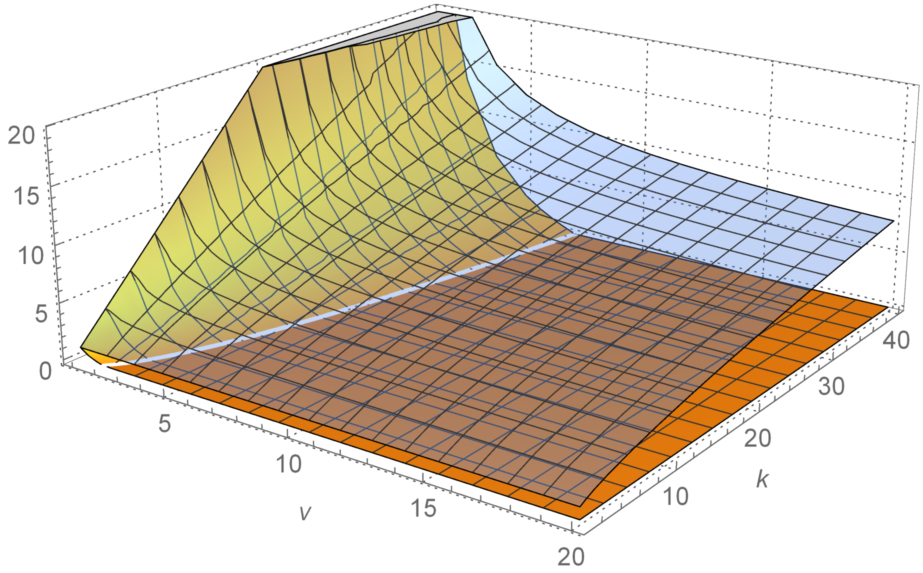

Figure 2: Lower and upper limits for the values of n_γ with respect to v and k.

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

Considering (7) for non-identity elements we can notice that a any particular multiplicity will be involved in two of the products—once as μ and once as $\mu+\gamma$ (but not both at the same time as we consider non-identity γ now). Other $v-2$ products are destined to contain other multiplicities solely which leads us to true equation.

$$\sum d_\mu d_{\mu+\gamma} = -2(v-1) + (v-2) = -v \tag{12}$$

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

$$\sum d_\mu^2 = (\pm(v-1))^2 + (v-1)(\mp 1)^2 = v^2 - v \tag{13}$$

It is straightforward to check that (5) turns out true as well. □

3.3 Difference multisets for cyclic groups

For cyclic matrices we can write (7) as

$$Dd = \mathbf{v} \tag{14}$$

where $d = (d_0, d_1, \ldots, d_{v-1})$, $D_{\mu\nu} = d_{\mu+\nu}$ and $\mathbf{v} = (\mathbf{v^2} - \mathbf{v}, -\mathbf{v}, -\mathbf{v}, \ldots)$.

The form of the matrix D is the following:

$$D = \begin{pmatrix} d_0 & d_1 & d_2 & \cdots & d_{v-1} \\ d_1 & d_2 & d_3 & \cdots & d_0 \\ d_2 & d_3 & d_4 & \cdots & d_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{v-2} & d_{v-1} & d_0 & \cdots & d_{v-3} \\ d_{v-1} & d_0 & d_1 & \cdots & d_{v-2} \end{pmatrix} \tag{15}$$

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

3.3.1 Solving equations with anticirculant matrices

We weren't able to track down a source dealing with matrices like (15), however we managed to apply the same methods as with circulant matrices [11].

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

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{v-1} \\ a_1 & a_2 & a_3 & \cdots & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} \tag{16}$$

and a vector $b = (b_0, b_1, b_2, \vdots)^T$.

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

$$b_j = \sum_{i=0}^{v-1} a_{j+i} x_i \tag{17}$$

Apply discrete Fourier transform:

$$\mathcal{F}(b)_m = \sum_{j=0}^{v-1} b_j \omega^{-jm} \tag{18}$$

where $\omega = \exp(\frac{2\pi i}{v})$—a root of unity (this is the only place where i is used to denote the imaginary unit).

Insert b_j obtaining

$$\begin{aligned}\mathcal{F}(b)_m &= \sum_{j=0}^{v-1}\sum_{i=0}^{v-1} a_{j+i}x_k\omega^{-jm} \\ &= \sum_{j=0}^{v-1}\sum_{i=0}^{v-1} x_i\omega^{im}a_{j+i}\omega^{-(j+i)m} \\ &= \sum_{i=0}^{v-1} x_i\omega^{im}\sum_{j'=i}^{v+i-1} a_{j'}\omega^{-j'm}\end{aligned} \tag{19}$$

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 $j'' = j' \mod v$.

$$\sum_{j'=i}^{v+i-1} a_{j'}\omega^{-j'm} = \sum_{j''=0}^{v-1} a_{j''}\omega^{-j''m} = \mathcal{F}(a)_m \tag{20}$$

We can now finish the transformation:

$$\begin{aligned}\mathcal{F}(b)_m &= \sum_{i=0}^{v-1} x_i\omega^{im}\mathcal{F}(a)_m \\ &= \mathcal{F}(a)_m(\sum_{i=0}^{v-1} x_i^*\omega^{-im})^* \\ &= \mathcal{F}(a)_m\mathcal{F}^*(x^*)_m = v\mathcal{F}(a)_m\mathcal{F}^{-1}(x)_m\end{aligned} \tag{21}$$

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 $\mathcal{F}(b)_m = \mathcal{F}(a)_m\mathcal{F}^*(x^*)_m$.

3.3.2 Solving the digression equation

The D and d in equation $Dd = \mathbf{v}$ is linked in the same way as A and a in section 3.3.1. The image of $Dd = \mathbf{v}$ is

$$\mathcal{F}(\mathbf{v})_m = \mathcal{F}(d)_m\mathcal{F}^*(d^*)_m \tag{22}$$

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

$$\mathcal{F}(\mathbf{v})_m = \mathcal{F}(d)_m\mathcal{F}^*(d)_m = |\mathcal{F}(d)_m|^2 \tag{23}$$

Remembering $\mathbf{v} = (v^2-v, -v, -v, \ldots)$ we can find that $\mathcal{F}(\mathbf{v}') = (0, v^2, v^2, \ldots)$ and (23) becomes

$$\left|\sum_{\mu=0}^{v-1} d_\mu\omega^{-\mu m}\right| = v(1 - \delta_{m0}) \tag{24}$$

For any $m|v$ we can note that $\delta_{m0} = 0$ and

$$\left|\sum_{\mu=0}^{v-1} d_\mu \omega^{-m\mu}\right| = \left|\sum_{\mu=0}^{v/m-1}\sum_{\nu=0}^{m-1} d_{\mu+\nu v/m}\omega^{-m\mu}\right| = v \tag{25}$$

as

$$e^{\frac{-2\pi i m(\mu+\nu v/m)}{v}} = e^{\frac{-2\pi i m\mu}{v}} e^{-2\pi i\nu} = e^{\frac{-2\pi i m\mu}{v}} \tag{26}$$

We consider expressions (24) and (25) as the main results of this section, here's how one can use it.

Proposition 3.3. *In 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 (25) for $m = v/2$

$$\left|\sum_{\mu=0}^{v/2-1} d_{2\mu} - \sum_{\mu=0}^{v/2-1} d_{2\mu+1}\right| = v \tag{27}$$

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 $\sum d_\mu = 0$. □

Remark 3.4. 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 $\mathbb{Z}_2^i$

We obtained a construction that produces plenty of difference multisets in $\mathbb{Z}_2^i$. We shall start by explaining the construction and then a proof and analysis of the construction will be presented.

3.4.1 Construction

Consider the elements $\mu \in \mathbb{Z}_2^i$ as i-tuples $\mu = (\mu_1, \ldots, \mu_i)$.

Select a hyperplane H_1 out of $\mathbb{Z}_2^i$ defined by equation $0 = a_0 + a_1\mu_1 + a_2\mu_2 + \ldots + a_i\mu_i$ $(0 = a_0 + a \cdot \mu)$ with $a_\nu \neq 0$ for at least one $\nu \neq 0$. Set $d_\eta = -1$ for every $\eta \in H_1$.

As for the remaining $(i-1)$-dimensional halfspace: take a hyperplane H_2 out of this and set $d_\eta = 3$ for every $\eta \in H_2$.

Repeat this process $0 \leq m \leq i-1$ times setting $d_\eta = \sum\limits_{j=0}^{k}(-2)^j$ for every $\eta \in H_k$.

You will end up with the final subspace H_f remaining. Select an element γ and set $d_\gamma = (-1)^m v + \sum\limits_{j=0}^{m+1}(-2)^j$. Set $d_\eta = \sum\limits_{j=0}^{m+1}(-2)^j$ for the remaining $\eta \in H_f$.

One can also flip the sign on every d_μ getting another bunch of difference multisets.

3.4.2 A few examples

Example 3.5. Take $i = 7$. Thus $v = 2^i = 128$. Take hyperplane H_1 defined by $0 = \mu_1$, and set $d_\eta = -1$ for all $\eta \in H_1$ i.e. set $d_{0000000} = d_{0000001} = \ldots = d_{0111111} = -1$.

Let's continue with the remaining subspace ($0 = 1 + \mu_1$). Select another halfpace H_2 defined by $0 = \mu_2$ and set $d_{1000000} = \ldots = d_{1011111} = 3$.

Let's choose $m = 4$. We must then repeat the bisections two more times setting $d_\eta = -5$ for $\eta \in H_3$ and $d_\eta = 11$ for $\eta \in H_4$.

We have 8 elements left. Let's set $d_{1111111} = (-1)^m v + \sum\limits_{j=0}^{m+1} (-2)^j = v - 21 = 107$ and it remains that the other $d_{1111000} = \ldots = d_{1111110} = -21$.

For tighter examples (with $m \geq i - 2$) the multiplicity of the final element will take form of $\sum (-2)^j$ as well. All the digressions will appear to be on the sequence $-1, 3, -5, 11, -21, 43, -85, \ldots$ [9].

Example 3.6. 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 3.7. 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.

Example 3.7 shows that some of the constructions (the ones with $m = i - 1$) produce a difference multiset that coincides with the $m = i - 2$ construction.

3.4.3 Proof

For a selected $0 \leq m \leq i - 1$ this construction provides us with 2^{i-l} digressions of value $d_\eta = \sum\limits_{j=0}^{l} (-2)^j$ for each $1 < l \leq m$ (none of these if $m = 0$), $2^{i-m} - 1$ digressions equal to $\sum\limits_{j=0}^{m+1} (-2)^j$ and one digression equal to $(-1)^m 2^i + \sum\limits_{j=0}^{m+1} (-2)^j$.

Checking equation $\sum d_\mu = 0$ and $\sum d_\mu^2 = v(v-1)$ is straightforward if you take into account that $\sum\limits_{j=0}^{l} (-2)^j = (1 - (-2)^{l+1})/3$.

Equations (7) are left to check. We began the construction by selecting a hyperplane H_1 defined by $0 = a_0 + a \cdot \mu$ where $a = (a_, a_2, \ldots)$ and $\mu = (\mu_1, \mu_2, \ldots)$ Depending on selection of $\gamma = (\gamma_1, \gamma_2, \ldots)$ there are two cases:

- If $1 \equiv a \cdot \gamma \mod 2$ then $\forall \mu \in H_1 : \mu + \gamma \notin H1$ and $\forall \mu \notin H_1 : \mu + \gamma \in H1$;
- If $0 \equiv a \cdot \gamma \mod 2$ then $\forall \mu \in H_1 : \mu + \gamma \in H1$ and $\forall \mu \notin H_1 : \mu + \gamma \notin H1$.

In the first case every $d_\mu d_{\mu+\gamma}$ involves factor -1. $\sum d_\mu d_{\mu+\gamma} = -2 \sum\limits_{i \notin H_1} d_\mu = -2(\sum d_\mu - \frac{v}{2}(-1)) = -v$.

In the second case $d_\mu d_{\mu+\gamma} = 1$ for every $\mu \in H_1$ and $\sum\limits_{\mu \in H_1} d_\mu d_{\mu+\gamma} = \frac{v}{2}$. So the remaining stuff must make up $-\frac{3v}{2}$ For the remaining stuff we are once again split into two cases depending on γ and the initial choice of H_2. Either both μ and $\mu + \gamma$ belong to the different sub-hyperplanes for every μ, or they belong to the same for every μ. That is, we either have $\sum\limits_{j=0}^{2}(-2)^j = 3$ in every factor or we continue the process.

In general for any γ we will end up at some step where we will have already summed up d_μ^2 for $\mu \in H_1 \cup H_2 \cup \ldots \cup H_r$ and at the next step we will have one of these cases:

- No more H_{r+1} has been constructed—only $2^{i-r} - 1$ elements with $d_\mu = \sum\limits_{j=0}^{r+1}(-2)^j$ and a single $d_\gamma = (-1)^m 2^i + \sum\limits_{j=0}^{r+1}(-2)^j$;
- $\mu \in H_{r+1}$ will have to be multiplied with the items outside H_{r+1} (like the first case in the previous fork).

The first case checks out:

$$\begin{aligned}\sum d_\mu^2 = &\sum_{H_1 \cup \ldots \cup H_r} d_\mu^2 \\ &+ (2^{i-r} - 2)\left(\sum_{j=0}^{r+1}(-2)^j\right)^2 \\ &+ 2\left(\sum_{j=0}^{r+1}(-2)^j\right)\left((-1)^r 2^i + \sum_{j=0}^{r+1}(-2)^j\right) \\ = &- 2^i = -v\end{aligned} \tag{28}$$

The second does as well:

$$\begin{aligned}\sum d_\mu^2 & \\ &= \sum_{H_1\cup\ldots\cup H_r} d_\mu^2 \\ &+2\left(\sum_{j=0}^{r+1}(-2)^j\right)\left(\sum_{l=r+2}^{m} 2^{i-l}\sum_{j=0}^{l}(-2)^j\right. \\ &\quad + (2^{i-m}-1)\sum_{j=0}^{m+1}(-2)^j \\ &\quad \left. + (-1)^m 2^i + \sum_{j=0}^{m+1}(-2)^j\right) \\ &= - 2^i = -v\end{aligned} \tag{29}$$

3.4.4 Analysis

For $i \leq 3$ the construction makes all the difference multisets there are. This can be shown explicitly by solving the digression equations.

We don't know about larger groups. Our construction produces 2^i different values for $i \leq 3$ but only 12, 16 and 20 different d_μ values for i of 4,5 and 6 respectively.

As for the number of difference multisets, this construction produces

$$2\sum_{j=2}^{i} 2^j \prod_{l=j+1}^{i}(2^{l+1}-2) \tag{30}$$

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.

The difference multisets (i.e. integer solutions $n_\mu = \frac{k+d_\mu\sqrt{k}}{v}$) themselves are produced whenever $v|\sqrt{k}$. In addition the cases of single $d_\gamma = \pm(v-1)$ and the rest $d_\mu = \mp 1$ we get integer n_μ for $k \equiv \mp 1 \mod v$.

3.5 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 (4) to form a system of equations.

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

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

Theorem 3.8. *Multiplicities of different $(\mathbb{Z}_3, k)$-difference multiset elements μ un ν are related via*

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

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 (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_β 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 $n_\mu = \frac{k+\Delta_\mu}{3}$, we can restate (32) into the following.

$$n_{\mu \neq \nu} = \frac{k - n_\nu \pm \sqrt{\frac{4k-\Delta_\nu^2}{3}}}{2} \tag{36}$$

The rest of analysis focuses on the Δ_μ 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 [10]. These numbers make an appearance in a variety of fields (see comments in [10]).

Definition 3.9. 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 3.10. *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 $a \geq b \geq 0$.

□

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

Lemma 3.11. *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:

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

Rewrite

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

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

□

Let's introduce the following notation for the three values used in lemma 3.11. The rest can be expressed as $-\Delta_i$:

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

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 3.12. *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 3.11, the expression (36) will equal integer only if k is a Löschian number and Δ_μ is one of the listed on (39) or a negative of that.

Insert the constructions listed in (3.12) 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 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 remainders one may check the following:

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

□

Remark 3.13. 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 3.12 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 $-(k+1) \mod 3$.

3.6 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 [6]. 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 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 [8] 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.

3.7 Other quasigroups of size 3

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 ($\forall \gamma \in \mathbb{Z}_3 \lambda = \sum(n_\mu(n_{\mu-\gamma} - \delta_{\mu,\mu+\gamma}))$). 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 (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_μ 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.

4 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 3.7.

The case of difference multisets over $\mathbb{Z}_3$ (theorem 3.12) 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 (7) (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] Raj Chandra Bose. On the construction of balanced incomplete block designs. *Annals of Eugenics*, 9(4):353–399, 1939.

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

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

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

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

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

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

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

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