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—a multiset M over a group G such that the differences of elements of M produce every element of G in the same number of times. In this paper we obtain multiple new constructions of difference multisets as well as some constraints on structure of difference multisets. We paid special attention to a few cases with small parameter values and managed to find all of the difference multisets over some smaller algebraic structures, e.g. $\mathbb{Z}_3, \mathbb{Z}_2^2$ and $\mathbb{Z}_2^3$. It turned out that there is a link between difference multisets over $\mathbb{Z}_3$ and Löschian numbers.

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 [3], difference multisets were first investigated 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 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 [10] 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:

$$\mathcal{D}(M) = \{\, \mu_i - \mu_j \mid i, j \in \{1, 2, \ldots, k\} \wedge i \neq j \,\}. \tag{1}$$

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 (4) 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.

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

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):

$$\forall\gamma\in G\colon \sum(n_\mu(n_{\gamma+\mu}-\delta_{\gamma 0}))=\lambda. \tag{3}$$

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 [4]:

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

(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 (2) defines a hyperplane and equations (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:

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

$$\forall\gamma\in G\colon \sum d_\mu d_{\gamma+\mu} = v(v\delta_{\gamma 0}-1). \tag{6}$$

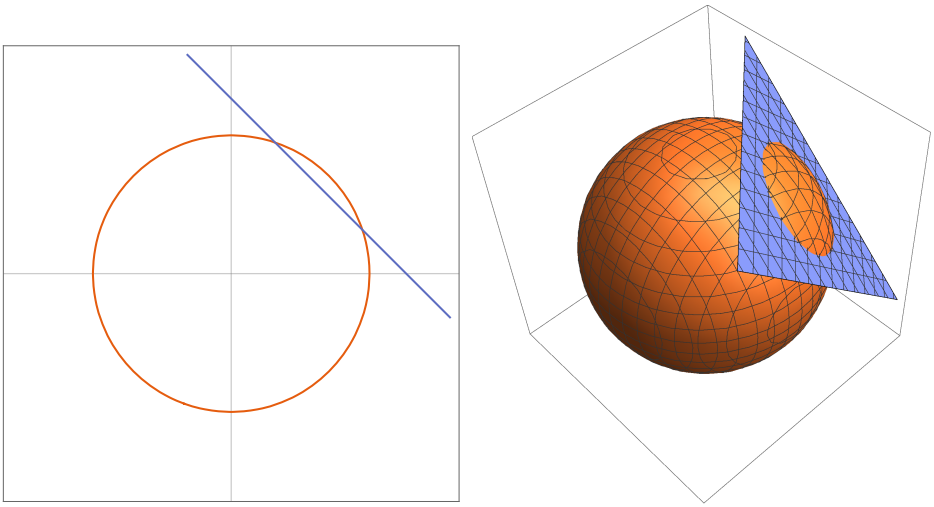

Figure 1: The $\sum n_\mu = k$ and $\sum n_\mu^2 = k+\lambda$ surfaces in two and three dimensions.

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.

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 (see Figure 2).

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

$$\forall \gamma \in G\colon \qquad \frac{k-(v-1)\sqrt{k}}{v} \leq n(\gamma, M) \leq \frac{k+(v-1)\sqrt{k}}{v} \tag{7}$$

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

$$\begin{cases} \sum n_\mu = k \\ \sum (n_\mu(n_\mu - 1)) = \lambda. \end{cases} \tag{8}$$

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:

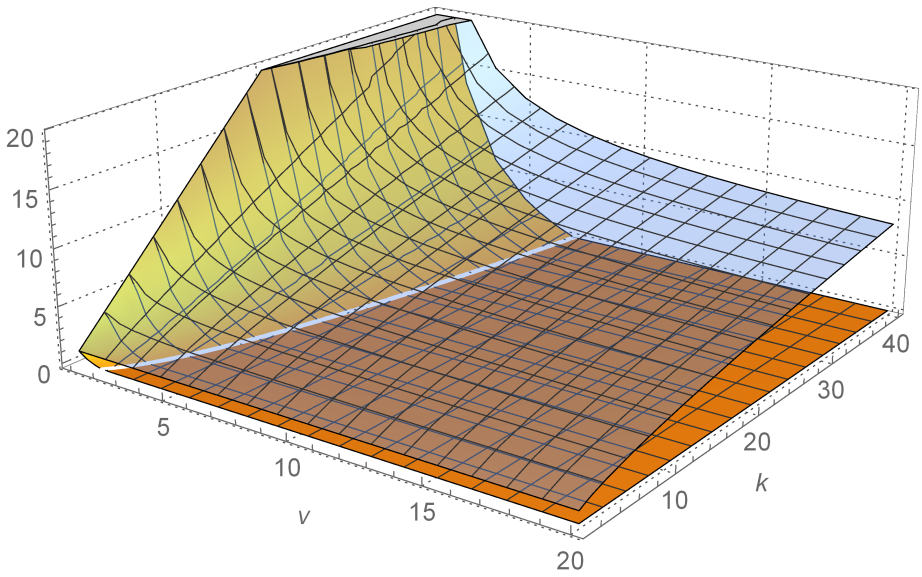

Figure 2: Lower and upper bounds for the values of n_γ with respect to v and k.

$$\begin{cases} k - \sum n_\mu = 0 \\ k + \lambda - \sum n_\mu^2 = 0. \end{cases} \tag{9}$$

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).

$$\mathcal{L} = n_\gamma - \lambda_1(k - \sum n_\mu) - \lambda_2(k + \lambda - \sum n_\mu^2) \tag{10}$$

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 $\pm 1 \pmod v$ then a (G, k)-difference multiset exists with the following digressions.*

- *If* $\sqrt{k} \equiv 1 \pmod{v}$ *then* $d_\mu = v - 1$ *for any single element* μ *and* $d_{\nu \neq \mu} = -1$ *for the other elements.*
- *If* $\sqrt{k} \equiv -1 \pmod{v}$ *then* $d_\mu = 1 - v$ *for any single element* μ *and* $d_{\nu \neq \mu} = 1$ *for the other elements.*
- *Both of the above constructions if* $\sqrt{k} \equiv 0 \pmod{v}$.

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 (6) 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:

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

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

$$\sum d_\mu^2 = (\pm(v-1))^2 + (v-1)(\mp 1)^2 = v^2 - v. \tag{12}$$

It is straightforward to check that equation (5) is satisfied as well. □

3.3 Difference multisets for cyclic groups

Let us consider (6) in matrix form

$$Dd = \mathbf{v} \tag{13}$$

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:

$$D = \begin{pmatrix} d_0 & d_1 & d_2 & \cdots & d_{v-1} \\ d_1 & d_2 & d_3 & \cdots & d_0 \\ d_2 & d_3 & d_4 & \cdots & d_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_{v-2} & d_{v-1} & d_0 & \cdots & d_{v-3} \\ d_{v-1} & d_0 & d_1 & \cdots & d_{v-2} \end{pmatrix}. \tag{14}$$

We will use the discrete Fourier transform:

$$\mathcal{F}(y)_m = \sum_{j=0}^{v-1} y_j \omega^{-jm} \tag{15}$$

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

$$\mathcal{F}(b)_m = \mathcal{F}(a)_m \mathcal{F}^*(x^*)_m, \tag{16}$$

where a is the first row of A.

This is particulary useful for equation (13) as the vector d is also the first row of matrix D. The image of $\mathbf{v} = \mathbf{Dd}$ is

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

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

$$\mathcal{F}(\mathbf{v})_m = \mathcal{F}(d)_m \mathcal{F}^*(d)_m = |\mathcal{F}(d)_m|^2. \tag{18}$$

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 (18) becomes

$$\left| \sum_{\mu=0}^{v-1} d_\mu \omega^{-\mu m} \right| = v(1 - \delta_{m0}). \tag{19}$$

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

$$\left| \sum_{\kappa=0}^{v/m-1} \omega^{-m\kappa} \cdot \sum_{\nu=0}^{m-1} d_{\kappa+\nu v/m} \right| = v \tag{20}$$

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

Proof. The theorem statement is obtained from (19).

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:

$$\omega^{-m(\kappa+\nu v/m)} = \omega^{-m\kappa}\omega^{-\nu v} = \omega^{-m\kappa}. \tag{21}$$

□

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 (20) for $m = v/2$

$$\left| \sum_{\mu=0}^{v/2-1} d_{2\mu} - \sum_{\mu=0}^{v/2-1} d_{2\mu+1} \right| = v. \tag{22}$$

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. □

Remark 3.5. Similar relation also holds true for some 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 $\mathbb{Z}_2^m$

Consider $\mathbb{Z}_2^m$ as an affine space over $\mathbb{Z}_2$. For a chosen affine frame F, each element $\mu \in \mathbb{Z}_2^m$ can be represented by its affine coordinates: $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$. For $i \in \{1, 2, \ldots, m\}$ we define subspaces H_i^F and $\widetilde{H}_i^F$ as follows:

$$\mu \in H_i^F \iff \begin{cases} \mu_j = 1 & \text{for } j < i \\ \mu_i = 0 \end{cases} \tag{23}$$

$$\mu \in \widetilde{H}_i^F \iff \mu_j = 1 \text{ for } j \le i \tag{24}$$

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

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

1. *For each $\mu \in H_i^F$ where $i \le r$, set $d_\mu = \xi_i$.*
2. *Select element $\nu \in \widetilde{H}_r^F$.*
3. *Set $d_\nu = (-1)^r v + \xi_{r+1}$.*
4. *Set $d_\mu = \xi_{r+1}$ for all $\mu \in \widetilde{H}_r^F \setminus \{\nu\}$.*

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

Proof. For a selected $r\colon 0 < r < m$ this construction provides us with 2^{m-i} digressions of value $d_\mu = \xi_i$ for each i $(1 \le i \le r)$, $2^{m-r} - 1$ digressions equal to ξ_{r+1} and one digression equal to $(-1)^r 2^m + \xi_{r+1}$.

It is easy to check that the equations $\sum d_\mu = 0$ and $\sum d_\mu^2 = v(v-1)$ are satisfied with these values.

It remains to check the equations (6) for non-identity γ.

For $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ let s be the smallest index for which $\gamma_s = 1$. Then we can observe the following behaviour of $\gamma + \mu$:

- If $s > r$ then $\mu \in H_i^F \iff \gamma + \mu \in H_i^F$ and $\mu \in \widetilde{H}_r^F \iff \gamma + \mu \in \widetilde{H}_r^F$.
- If $s \le r \wedge i < s$ for then $\mu \in H_i^F \iff \gamma + \mu \in H_i^F$.
- If $s \le r \wedge i = s$ then $\mu \in H_i^F \iff \gamma + \mu \in \widetilde{H}_i^F$.
- If $s \le r \wedge i > s \wedge i \le r$ then $\mu \in H_i^F \iff \gamma + \mu \in H_s^F$.
- If $s \le r$ then $\mu \in \widetilde{H}_r^F \iff \gamma + \mu \in H_s^F$

We shall consider the case $s \leq r$ first. The value of (6) is evaluated as follows

$$\sum d_\mu d_{\gamma+\mu} = \sum_{i<s} \sum_{\mu \in H_i^F} d_\mu d_{\gamma+\mu} + \sum_{i>s} \sum_{\mu \in H_i^F} d_\mu d_{\gamma+\mu} + \sum_{\mu \in H_s^F} d_\mu d_{\gamma+\mu}. \tag{25}$$

In the second and third sum one of μ and $\gamma+\mu$ belongs to H_s^F and the other belongs to H_i^F, thus either d_μ, or $d_{\gamma+\mu}$ is equal to ξ_s:

$$\sum d_\mu d_{\gamma+\mu} = \sum_{i<s} \sum_{\mu \in H_i^F} \xi_i^2 + 2 \sum_{i>s} \sum_{\mu \in H_i^F} \xi_s d_\mu. \tag{26}$$

Since $\sum d_\mu = 0$, we can replace $\sum_{i>s} \sum_{\mu \in H_i^F} d_\mu$ with $-\sum_{i \leq s} \sum_{\mu \in H_i^F} d_\mu$ and substitute $d_\mu = \xi_i$. We also substitute sums containing identical terms with multiplications:

$$\begin{aligned} \sum d_\mu d_{\gamma+\mu} &= \sum_{i<s} \sum_{\mu \in H_i^F} \xi_i^2 - 2\xi_s \sum_{i \leq s} \sum_{\mu \in H_i^F} \xi_i \\ &= \sum_{i<s} 2^{m-i} \xi_i^2 - 2\xi_s \sum_{i \leq s} 2^{m-i} \xi_i \\ &= -2^m = -v. \end{aligned} \tag{27}$$

The details of getting -2^m from the preceding expression are shown in Appendix A.

Considering the other case with $s > r$ we get the following:

$$\begin{aligned} \sum d_\mu d_{\gamma+\mu} &= \sum_{i \leq r} \sum_{\mu \in H_i^F} d_\mu + \sum_{\mu \in \widetilde{H}_r^F} d_\mu d_{\gamma+\mu} \\ &= \sum_{i \leq r} 2^{m-i} \xi_i^2 + (2^{m-r} - 2)\xi_{r+1}^2 + 2\xi_{r+1}((-1)^r 2^m + \xi_{r+1}) \\ &= -2^m = -v. \end{aligned} \tag{28}$$

The details of getting -2^m are once again in the Appendix A.

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

Remark 3.7. We could also allow the value $r = 0$ in Theorem 3.6. In that case the obtained difference multiset would be the one described in Theorem 3.2 and it would also produce integer multiplicities for $k \equiv 1 \pmod{v}$ or $k \equiv -1 \pmod{v}$.

Theorem 3.8. *There are no other difference multisets than those presented in Theorem 3.6 and Theorem 3.2 for $m < 4$.*

Proof. This result can be obtained by solving equations (5) and (6).

For $\mathbb{Z}_2$ it has already been shown before by Buratti [4].

For $\mathbb{Z}_2 \times \mathbb{Z}_2$ our constructions produce one digression equal to ± 3 and three other equal to ∓ 1. Equations (5) and (6) take the following form:

$$\begin{cases} d_{00} + d_{01} + d_{10} + d_{11} = 0 \\ d_{00}^2 + d_{01}^2 + d_{10}^2 + d_{11}^2 = 12 \\ 2d_{00}d_{01} + 2d_{10}d_{11} = -4 \\ 2d_{00}d_{10} + 2d_{01}d_{11} = -4 \\ 2d_{00}d_{11} + 2d_{01}d_{10} = -4 \end{cases}. \tag{29}$$

Clearly not all d_μ are 0 and at least one digression is positive, at least one is negative. From the latter three equations we can observe that it is impossible to have two positive and two negative digressions so there is exactly one positive or exactly one negative digression. In the former case WLOG suppose d_{00} is the only positive digression.

Adding the second and third equations we get $(d_{00}+d_{01})^2+(d_{10}+d_{11})^2 = 8$. Using $d_{10}+d_{11} = -(d_{00}+d_{01})$ from the first equation we obtain $2(d_{00}+d_{01})^2 = 8$ and $d_{00} + d_{01} = \pm 2$. The same can be shown about any pair of digressions.

Three times the first equation of system (29) can be rewritten as follows:

$$(d_{00}+d_{01})+(d_{00}+d_{10})+(d_{00}+d_{11})+(d_{01}+d_{10})+(d_{01}+d_{11})+(d_{10}+d_{11}) = 0.$$

We know that the summands are equal to ± 2 so three of them must be equal to $+2$ and three to -2. The "$+2$" ones are the first three as they need to contain the positive digression d_{00}. The other digressions are then obviously equal and of value -1 as their pairs sum to -2. And d_{00} is then 3.

In the case of a single negative digression, we similarly obtain that it is -3 and the others are 1.

For $\mathbb{Z}_2^3$ equations (5) and (6) take the following form:

$$\begin{cases} d_{000} + d_{001} + d_{010} + d_{011} + d_{100} + d_{101} + d_{110} + d_{111} = 0 \\ d_{000}^2 + d_{001}^2 + d_{010}^2 + d_{011}^2 + d_{100}^2 + d_{101}^2 + d_{110}^2 + d_{111}^2 = 56 \\ 2d_{000}d_{001} + 2d_{010}d_{011} + 2d_{100}d_{101} + 2d_{110}d_{111} = -8 \\ 2d_{000}d_{010} + 2d_{001}d_{011} + 2d_{100}d_{110} + 2d_{101}d_{111} = -8 \\ 2d_{000}d_{011} + 2d_{001}d_{010} + 2d_{100}d_{111} + 2d_{101}d_{110} = -8 \\ 2d_{000}d_{101} + 2d_{001}d_{100} + 2d_{010}d_{111} + 2d_{011}d_{110} = -8 \\ 2d_{000}d_{110} + 2d_{001}d_{111} + 2d_{010}d_{100} + 2d_{011}d_{101} = -8 \\ 2d_{000}d_{111} + 2d_{001}d_{110} + 2d_{010}d_{101} + 2d_{011}d_{100} = -8 \end{cases} \tag{30}$$

We solved this case with the help of a computer algebra system. The only solutions to this system are the ones presented in Theorem 3.6 and Theorem 3.2. □

3.5 Difference multisets over the three element group

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

For this group (4), (2) and (3) for a non-identity element form the following system of equations:

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

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

Theorem 3.9. *Multiplicities of different $(\mathbb{Z}_3, k)$-difference multiset elements μ and ν are related via*

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

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 (31) can now be rewritten:

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

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

It is useful to consider the multiplicities in the form $n_\mu = \frac{k+\Delta_\mu}{3}$, then (32) can be rewritten as follows:

$$n_\mu = \frac{k - n_\nu \pm \sqrt{\frac{4k-\Delta_\nu^2}{3}}}{2}. \tag{34}$$

The behaviour of expression under the root is tied to a topic in number theory called Löschian numbers [9, 11]. These numbers make an appearance in a variety of fields [8, 5, 12].

Definition 3.10. 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 3.11. *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 $a = \max(c, |a' + b'|)$, $b = \min(c, |a' + b'|)$.

□

Let us denote $\mathbb{D}_{ab} = \{ 2a + b, -a - 2b, -a + b \}$ (considered as a multiset: b can be equal to 0).

Lemma 3.12. *The value of the expression $\frac{4k-\Delta^2}{3}$ is a perfect square iff k is a Löschian number and $\Delta \in \mathbb{D}_{ab} \cup \mathbb{D}_{ba}$ where a, b are such that $a^2 + ab + b^2 = k$, $a \geq b \geq 0$.*

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:

$$z^2 = \frac{4k - \Delta^2}{3} \tag{35}$$

where $z \geq 0$. Rewrite:

$$\frac{3z^2 + \Delta^2}{4} = k. \tag{36}$$

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 an element of $\mathbb{D}_{ab} \cup D_{ba}$:

- If $z \geq |\Delta|$ take $a = max(\frac{z+\Delta}{2}, \frac{z-\Delta}{2})$, $b = min(\frac{z+\Delta}{2}, \frac{z-\Delta}{2})$. Then Δ can be expressed as either $a - b$ or $b - a$.
- If $\Delta > z$ take $a = max(\frac{\Delta-z}{2}, z)$, $b = min(\frac{\Delta-z}{2}, z)$. Then Δ can be expressed as either $a + 2b$ or $2a + b$.
- If $\Delta < -z$ take $a = max(\frac{-\Delta-z}{2}, z)$, $b = min(\frac{-\Delta-z}{2}, z)$. Then Δ can be expressed as either $-a - 2b$ or $-2a - b$.

□

Theorem 3.13. *The $(\mathbb{Z}_3, k)$-difference multisets exist iff k is a Löschian number. For each a, b such that $k = a^2 + ab + b^2$, $a \geq b \geq 0$, there are difference multisets with multiplicities $n_\mu = \frac{k+\Delta_\mu}{3}$ where:*

- *If $3 \nmid k$ and $a \equiv b - 1 \pmod 3$ then $\{ \Delta_\mu \mid \mu \in \mathbb{Z}_3 \} = \mathbb{D}_{ab}$.*
- *If $3 \nmid k$ and $a \equiv b + 1 \pmod 3$ then $\{ \Delta_\mu \mid \mu \in \mathbb{Z}_3 \} = \mathbb{D}_{ba}$.*
- *If $3 \mid k$ then $\{ \Delta_\mu \mid \mu \in \mathbb{Z}_3 \}$ can be either $\mathbb{D}_{ab}$ or $\mathbb{D}_{ba}$.*

There are no other difference multisets for the given k.

Proof. It follows from lemma 3.12 that the right hand side of relation (34) is integer iff k is a Löschian number and $\Delta_\mu \in \mathbb{D}_{ab} \cup \mathbb{D}_{ba}$.

Insert the constructions listed in the statement of theorem into (32) to verify that these are indeed multiplicities that make up a difference multiset whenever the numbers are integer.

Using equation (34) we can also check that using $\Delta_\nu \in \mathbb{D}_{ab}$ we will obtain the other two elements of $\mathbb{D}_{ab}$ for the values of Δ_μ related to the other multiplicities. It works the same for D_{ba}.

Considering a and b modulo 3 we observe which cases produce integer multiplicities:

- If $a \equiv b \pmod 3$ then $3 \mid k$ and all the multiplicities using either $\Delta_\mu \in \mathbb{D}_{ab}$ or $\Delta_\mu \in \mathbb{D}_{ab}$ are integers.
- If $a \equiv b - 1 \pmod 3$ then $k \equiv 1 \pmod 3$ and only the multiplicities obtained by using $\Delta_\mu \in \mathbb{D}_{ab}$ are all integer.
- If $a \equiv b + 1 \pmod 3$ then $k \equiv 1 \pmod 3$ and only the multiplicities obtained by using $\Delta_\mu \in \mathbb{D}_{ba}$ are all integer.

□

Remark 3.14. Without the $a \geq b \geq 0$ contraint we would obtain the same $\mathbb{D}_{ab}$ with various a, b pairs and produce the same difference multisets repeatedly. But different $a \geq b \geq 0$ pairs with $a^2 + ab + b^2 = k$ lead to different values of $a - b$ and thus all the constructions mentioned in Theorem 3.13 are distinct. Consequently the number of $(\mathbb{Z}_3, k)$-difference multisets is proportional to the number of unique a, b pairs (respecting constraints) and the coefficient of proportionality is 1 if $k \equiv 1 \pmod 3$ and 2 if $k \equiv 0 \pmod 3$. And there are no Löschian numbers that are congruent to 2 modulo 3, this can be observed considering all possibilities of $a - b$ modulo 3 as in the proof of Theorem 3.13.

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. The unique γ such that $\gamma \cdot \mu = \nu$ is called the right division ν/μ. Similarly the left division can be defined. Without loss of generality we shall consider the right division.

Let Q be a quasigroup. For a multiset M over Q to be a difference multiset, any element $\gamma \in Q$ must be obtained λ times as ν/μ where $\nu, \mu \in M$. Notice that if $\gamma = \nu/\mu$, then $\nu = \gamma\mu$. The generalization of equation (3) is:

$$\forall \gamma \in Q \colon \sum (n_\mu (n_{\gamma\mu} - \delta_{\mu,\gamma\mu})) = \lambda \tag{37}$$

which coincides with system (3) 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 (6) generalizes to something more complex:

$$\forall\gamma \in Q\colon \sum(d_\mu(d_{\gamma\mu} - \frac{v\delta_{\mu,\gamma\mu}}{\sqrt{k}}) - v\delta_{\mu,\gamma\mu}) = -v. \tag{38}$$

However, in the case of loops system (38) simplifies to system (6).

4.1 Generalized results

As the equation (6) applies for loops, Theorem 3.1 is true for all loops.

Theorem 3.2 is also true for loops as it was proved using equations that hold for loops. However, it also holds if there is only a one-sided identity element.

Theorem 4.1. *Suppose Q is a quasigroup with right division considered as difference. Then the construction given in Theorem 3.2 produces a difference multiset iff $\exists\gamma\forall\mu\colon \mu = \gamma\mu$.*

Proof. For $\gamma \in Q$ let $Q_\gamma = \{\mu \in Q \mid \mu = \gamma\mu\}$. Denote $v_\gamma = |Q_\gamma|$ and $\overline{v_\gamma} = v - v_\gamma$.

We can rewrite equation (38) for γ:

$$\sum_{\mu\in Q_\gamma}(d_\mu(d_\mu - \frac{v}{\sqrt{k}}) + \sum_{\mu\notin Q_\gamma} d_\mu d_{\gamma\mu} = v(v_\gamma - 1). \tag{39}$$

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

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

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

$$v_\gamma(1+\frac{v}{\sqrt{k}}) + 2(1-v) + \overline{v_\gamma} - 2 = -v + v\frac{v_\gamma}{\sqrt{k}} \tag{41}$$

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. □

Similarly it can be shown that left division difference multisets of same structure require a right identity element.

4.2 Other constructions over quasigroups of size 3

Considering $\mathbb{Z}_3$ with difference as the quasigroup operation, we obtain $(\mathbb{Z}_3, k)$-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 (37) we start by writing down the ways to obtain each of the elements and requiring them to be equal ($\forall\gamma \in \mathbb{Z}_3 \colon \lambda = \sum(n_\mu(n_{\gamma-\mu} - \delta_{\mu,\gamma-\mu}))$). Adding the equation $\sum n_\mu = k$ and using $3\lambda = k(k-1)$ we obtain a system of equations:

$$\begin{cases} n_0(n_0-1) + 2n_1n_2 = \frac{k(k-1)}{3} \\ n_1(n_1-1) + 2n_2n_0 = \frac{k(k-1)}{3} \\ n_2(n_2-1) + 2n_0n_1 = \frac{k(k-1)}{3} \\ n_0 + n_1 + n_2 = k \end{cases} . \tag{42}$$

The system (42) obviously possesses symmetry with respect to all the elements of $\mathbb{Z}_3$ and this system can easily be solved explicitly—valid multisets of n_μ are $\{\, \frac{k}{3}, \frac{k}{3}, \frac{k}{3} \,\}$ and $\{\, \frac{k-1}{3}, \frac{k-1}{3}, \frac{k+2}{3} \,\}$.

We can conclude that there can be at most one (up to automorphisms) $(\mathbb{Z}_3, k)$-sum multiset for a given value of k. Specifically there is one if $3 \mid k$ or $k \equiv 1 \pmod 3$ 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 $k \equiv 2 \pmod 3$ similarly to the situation with difference multisets over $\mathbb{Z}_3$.

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 (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 Summary and conclusions

We have found what are the difference multisets if the parameter values are small. Here we present a list of our findings. Some trivial cases that formally satisfy the constraints (e.g. some produce every element 0 times) and quasigroup cases are also included as those have helped spotting patterns.

Parameters	Difference multisets
$k = 0$	Empty multiset.
$k = 1$	Take single element, works for $v \geq 1$.
$v = 0$	Empty multiset.
$v = 1$	Take the identity k times for any k.
$v = 2$	Covered in Section 3.4 as a case of $\mathbb{Z}_2^i$.
$v = 3$	See section 4.2.
$G = \mathbb{Z}_2^i$	See section 3.4, possibly incomplete.
$G = \mathbb{Z}_3$	See section 3.5.

The case of difference multisets over $\mathbb{Z}_3$ (theorem 3.13) 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 odd prime values of i seems in the realm of possibility.

Theorem 3.1 and proposition 3.4 narrows the space of options that has to be considered in computer searches thus allowing to inspect a wider 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 (6) (or alternative forms) can be utilised to investigate some difference multisets or sets of their digressions in many small quasigroups.

6 Acknowledgements

We would like to express our gratitude to Anna Jansone for coming up with the concise proof of $\mathbb{Z}_2^2$ case in theorem 3.8 [7] and Mathematics Stack Exchange user B. Mehta who helped to complete the proof of lemma 3.12 [6].

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] Diane M Donovan, Terry S Griggs, Thomas A McCourt, Jakub Opršal, and David Stanovskỳ. Distributive and anti-distributive Mendelsohn triple systems. *Canadian Mathematical Bulletin*, 59(1):36–49, 2016.

[6] B. Mehta (https://math.stackexchange.com/users/418148/b mehta). Only certain values seem to make an expression into perfect square, can you help me prove or disprove it? Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/2537412 (version: 2017-11-26).

[7] Anna Jansone. Private communication.

[8] August Losch et al. Economics of location. 1954.

[9] John U Marshall. The Löschian numbers as a problem in number theory. *Geographical Analysis*, 7(4):421–426, 1975.

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

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

[12] Linda Stannard. Principles of virus architecture, 1995. [Online http://www.virology.uct.ac.za/vir/teaching/linda-stannard/principles-of-virus-architecture; accessed 16-January-2020].

A Calculation details for section 3.4

In this appendix we show how the sums in equations (27) and (28) are calculated.

A.1 Auxiliary results

For ease of reading let us repeat from 3.4 that $i \in \{1, 2, \ldots, m\}$ and the definition of ξ_i is as follows:

$$\xi_i = \frac{1-(-2)^{i+1}}{3}. \tag{43}$$

Evaluate the following expressions:

$$\xi_i^2 = \frac{1}{9}\left(1+(-2)^{i+2}+2^{2i+2}\right); \tag{44}$$

$$\xi_i(\xi_i - 2\xi_s) = -\frac{1}{9}\left(1+(-2)^{s+2}-2^{2i+2}-(-2)^{s+i+3}\right); \tag{45}$$

$$\xi_{r+1}(\xi_{r+1}+2(-2)^r) = \frac{1}{9}\left(1+(-2)^{r+1}+(-2)^{2r+3}\right) \tag{46}$$

We will also need the values of the following sums:

$$\sum_{i<s} 2^{-i} = 1-2^{1-s}; \tag{47}$$

$$\sum_{i<s} 2^{-i}(-2)^{s+2} = (-1)^s(2^{s+2}-2^3); \tag{48}$$

$$\sum_{i<s} 2^{-i}2^{2i+2} = \sum_{i<s} 2^{i+2} = 2^{s+2}-2^3; \tag{49}$$

$$\sum_{i<s} 2^{-i}(-2)^{s+i+3} = 2^{s+3}(-1)^{s+1}\sum_{i<s}(-1)^i = 2^{s+2}(1+(-1)^s); \tag{50}$$

$$\sum_{i\le r} 2^{-i} = 1-2^{-r}; \tag{51}$$

$$\sum_{i\le r} 2^{-i}(-2)^{i+2} = -2(1-(-1)^r); \tag{52}$$

$$\sum_{i\le r} 2^{-i}2^{2i+2} = 2^3(2^r-1). \tag{53}$$

A.2 Evaluation of expression in (27)

Let us start by separating case of $i = s$ out of the sum, factoring out 2^m and grouping the terms. We can evaluate the obtained expression using the notes on ξ_i from the previous section:

$$\begin{aligned}
&\sum_{i<s} 2^{m-i}\xi_i^2 - 2\xi_s \sum_{i\le s} 2^{m-i}\xi_i \\
=&2^m\left[-2^{1-s}\xi_s^2 + \sum_{i<s} 2^{-i}\xi_i(\xi_i - 2\xi_s)\right] \\
=&-\frac{2^m}{9}\left[2^{1-s}(1-(-2)^{s+1})^2 + \sum_{i<s} 2^{-i}\left(1+(-2)^{s+2} - 2^{2i+2} - (-2)^{s+i+3}\right)\right].
\end{aligned} \tag{54}$$

The sum can be expanded in terms from equations (47)–(50) and evaluated as follows:

$$\begin{aligned}
&\sum_{i<s} 2^{-i}\left(1+(-2)^{s+2} - 2^{2i+2} - (-2)^{s+i+3}\right) \\
=&-2^{s+3} - 2^{1-s} - 2^3(-1)^s + 9.
\end{aligned} \tag{55}$$

We can now finish the calculation:

$$\begin{aligned}
&\sum_{i<s} 2^{m-i}\xi_i^2 - 2\xi_s \sum_{i\le s} 2^{m-i}\xi_i \\
=&-\frac{2^m}{9}\left[2^{1-s}(1+(-2)^{s+2}+2^{2s+2}) - 2^{s+3} - 2^{1-s} - 2^3(-1)^s + 9\right] \\
=&-2^m.
\end{aligned} \tag{56}$$

A.3 Evaluation of expression in (28)

Start by rearranging the terms and factoring out the 2^m and 2^{-r}.

$$
\begin{aligned}
&\sum_{i\le r} 2^{m-i}\xi_i^2 + (2^{m-r}-2)\xi_{r+1}^2 + 2\xi_{r+1}((-1)^r 2^m + \xi_{r+1}) \\
=&\sum_{i\le r} 2^{m-i}\xi_i^2 + 2^{m-r}\xi_{r+1}^2 + 2^{m+1}(-1)^r\xi_{r+1} \\
=&2^m\left[\sum_{i\le r} 2^{-i}\xi_i^2 + 2^{-r}\xi_{r+1}\left(\xi_{r+1} + 2(-2)^r\right)\right].
\end{aligned}
\tag{57}
$$

The sum can be evaluated using results (44) and (51)–(53):

$$
\begin{aligned}
&\sum_{i\le r} 2^{-i}\xi_i^2 \\
=&\frac{1}{9}\sum_{i\le r} 2^{-i}\left(1 + (-2)^{i+2} + 2^{2i+2}\right) \\
=&\frac{1}{9}\left(2^{r+3} - 2^{-r} + 2(-1)^r - 9\right).
\end{aligned}
\tag{58}
$$

The other term was precalculated in (46). And we obtain the result:

$$
\begin{aligned}
&\sum_{i\le r} 2^{m-i}\xi_i^2 + (2^{m-r}-2)\xi_{r+1}^2 + 2\xi_{r+1}((-1)^r 2^m + \xi_{r+1}) \\
=&\frac{2^m}{9}\left[2^{r+3} - 2^{-r} + 2(-1)^r - 9 + 2^{-r}\left(1 + (-2)^{r+1} + (-2)^{2r+3}\right)\right] \\
=&-2^m.
\end{aligned}
\tag{59}
$$