Block Labellings of Resolvable 1-Rotational Steiner 2-Designs

Dylan Lusi, Charles J. Colbourn

December 20, 2021

Abstract

Given an ordering of the blocks of a design, for each point of the design, the point sum is the sum of the indices of blocks containing that point. Optimizing the access-balancing of the files of storage systems modeled as designs, entails making these point sums as equal as possible. Block orderings of certain resolvable 1-rotational Steiner 2-designs are given which, in all but one case, make the point sums equal. A recursive construction is also shown to yield designs whose point sums are equal.

1 Introduction

1.1 Design-Theoretic Preliminaries

A *set system* is a pair $\mathcal{S} = (X, B)$, where X is a set of *points* and $\mathcal{B}$ is a multiset of subsets of X (*blocks*). A *Steiner system* with parameters t, k, and v, or $S(t, k, v)$, is a set system $D = (V, \mathcal{B})$, where V is a set of v points and $\mathcal{B}$ is a set of k-subsets of V (*blocks*) of V such that every t-subset of V occurs in exactly one block. Any Steiner system $S(2, k, v)$ is called a *Steiner 2-design* of order v and block size k. The *dual* of an $S(t, k, v)$ $D = (V, \mathcal{B})$ is the set system $D' = (\mathcal{B}, V)$, where the dual point $B \in \mathcal{B}$ is "contained" in the dual block $x \in V$ if $x \in B$ in D.

A *group-divisible design* (GDD) is a triple $(X, \mathcal{G}, \mathcal{A})$, where X is a set of points, $\mathcal{G}$ is a partition of X into at least two nonempty subsets (*groups*), and $\mathcal{A}$ is a set of subsets of X (*blocks*) such that (1) $|A| \geq 2$ for all $A \in \mathcal{A}$, (2) $|G \cap A| \leq 1$ for all $G \in \mathcal{G}$ and $A \in \mathcal{A}$, and (3) every pair of points from distinct groups is contained in exactly one block. When $|G| = 1$ for each $G \in \mathcal{G}$, the pair $(X, \mathcal{A})$ is a Steiner 2-design.

Let $\mathcal{B}$ be the block set of a GDD or a Steiner 2-design on point set V. An *automorphism* α of $\mathcal{B}$ is a permutation of V such that

$$\{\{\alpha(x) : x \in B\} : B \in \mathcal{B}\} = \mathcal{B}.$$

Moreover, an *automorphism group* G of $\mathcal{B}$ is a group of automorphisms of $\mathcal{B}$. A Steiner 2-design of order v is *s-rotational* if it has an automorphism consisting of a single fixed point and s disjoint cycles of length length $(v-1)/s$.

A Steiner 2-design $(V, \mathcal{B})$ is *resolvable* if there exists a partition (*resolution*) of $\mathcal{B}$ into sets called *parallel classes*, each of which partitions V. A resolvable Steiner 2-design is *cyclically resolvable* if it admits a cyclic automorphism group acting regularly on a resolution of the design.

Let G be an additive group of order v, N a subgroup of G of order n, and k a positive integer. For any two subsets $S, S' \subset G$ with $S' = \{s'_0, \ldots, s'_{|S'|-1}\}$, define

$$S + s'_0 + s'_1 + \cdots + s'_{|S'|-1} = \{s + s'_0 + \cdots + s'_{|S'|-1} : s \in S\},$$

and for any collection $\mathcal{C}$ of subsets of G and any subset $S' = \{s'_0, \ldots, s'_{|S'|-1}\}$ of G, define

$$\mathcal{C} + s'_0 + s'_1 + \cdots + s'_{|S'|-1} = \{S + s'_0 + \cdots + s'_{|S|-1} : S \in \mathcal{C}\}.$$

A $(G, N, k, 1)$ *difference family* is a set $\mathcal{F}$ of k-subsets of G (*base blocks*) such that $k(k-1)|\mathcal{F}| = |G \setminus N|$ and for each element $d \in G \setminus N$ there exists a unique ordered pair (g, h) of elements of some base block of $\mathcal{F}$ such that $d = g - h$. When G is cyclic of order v, we simply call $\mathcal{F}$ a $(v, n, k, 1)$ difference family. We say that $\mathcal{F}$ is *resolvable* if the union of its base blocks is a system of representatives of the nontrivial (right) cosets of N in G, and in that case we call it a $(G, N, k, 1)$-*RDF*.

Given a $(G, N, k, 1)$ difference family, $(X, \mathcal{C}, \mathcal{A})$ is a group divisible design, where $X = G$, $\mathcal{C}$ is the set of (right) cosets of N in G, and $\mathcal{A}$ is the set of all the (right) translates under G of the base blocks. Thus, when $N = \{0\}$, $(G, \mathcal{A})$ is an $\mathrm{S}(2, k, v)$; when $|N| = k$, $(G, \mathcal{A} \cup \mathcal{C})$ is also an $S(2, k, v)$. A $(G, N, k, 1)$ difference family $\mathcal{F}$ with $|N| = k - 1$ is a *1-rotational* difference family. If $\mathcal{F}$ is also resolvable, then it generates a resolvable 1-rotational Steiner 2-design.

Construction 1.1 ([4])**.** Let $\mathcal{F}$ be a 1-rotational $(G, N, k, 1)$-RDF. Put

$$\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$$

and let S be a complete system of representatives for the cosets of N in G. Then $\mathcal{R} = \{\mathcal{P}_0 + s : s \in S\}$ gives a resolution of an $S(2, k, |G| + 1)$.

This class of Steiner 2-designs is the central focus of our paper.

1.2 Block Labelling Preliminaries

Set systems with certain balance conditions, called *block designs*, have served as a basis for many physical systems, such as distributed storage systems [12, 20], systems for batch coding [21], and multiserver private information retrieval systems [13]. Dau and Milenkovic [11] propose ranking the popularity of the files making up a distributed storage system to improve its *access balancing*; that is, balancing access requests to storage units. Formally this amounts to equipping either $S(t, k, v)$ $D = (V, \mathcal{B})$ or its dual D' with a point labelling. A *point labelling* of a set system $\mathcal{S} = (V, \mathcal{B})$ is a bijection $\mathsf{rk} : V \to [0, |V|-1]$; in the application investigated by Dau and Milenkovic, this amounts to assigning a popularity rank to each point. A set system together with a point labelling is a *point-labelled set system*. Given a point-labelled set system $(\mathcal{S} = (V, \mathcal{B}), \mathsf{rk})$, for each $B \in \mathcal{B}$, the *block sum* with respect to rk, denoted $\mathsf{sum}(B, \mathsf{rk})$, is $\sum_{x \in B} \mathsf{rk}(x)$. With access-balancing in mind, Dau and Milenkovic propose a collection of metrics:

$$\begin{aligned}
\mathsf{MinSum}(\mathcal{S}, \mathsf{rk}) &= \min(\mathsf{sum}(B, \mathsf{rk}) : B \in \mathcal{B}); \\
\mathsf{MaxSum}(\mathcal{S}, \mathsf{rk}) &= \max(\mathsf{sum}(B, \mathsf{rk}) : B \in \mathcal{B}); \\
\mathsf{DiffSum}(\mathcal{S}, \mathsf{rk}) &= \mathsf{MaxSum}(\mathcal{S}, \mathsf{rk}) - \mathsf{MinSum}(\mathcal{S}, \mathsf{rk}); \text{ and} \\
\mathsf{RatioSum}(\mathcal{S}, \mathsf{rk}) &= \mathsf{MaxSum}(\mathcal{S}, \mathsf{rk}) / \mathsf{MinSum}(\mathcal{S}, \mathsf{rk}).
\end{aligned}$$

Under this regime, access balancing is optimized by minimizing the DiffSum or RatioSum; given their similarity, it is customary to focus on the DiffSum. Let $\mathcal{R}_{\mathcal{S}}$ denote the set of all point labellings of $\mathcal{S}$. Then define

$$\mathsf{DiffSum}(\mathcal{S}) = \min(\mathsf{DiffSum}(\mathcal{S}, \mathsf{rk}) : \mathsf{rk} \in \mathcal{R}_{\mathcal{S}}).$$

While one can obtain a design-specific labelling with optimal DiffSum (over all labellings of that design), it is more interesting to instead derive a DiffSum-optimal labelling over an entire class of set systems. For example, let $\mathcal{D}_{t,k,v}$ denote the set of all $S(t,k,v)$s and $\mathcal{D}'_{t,k,v}$ the set of duals of all $S(t,k,v)$. Then define

$$\begin{aligned}\mathsf{DiffSum}(t,k,v) &= \min(\mathsf{DiffSum}(D) : D \in \mathcal{D}_{t,k,v}), \text{ and}\\ \mathsf{DiffSum}'(t,k,v) &= \min(\mathsf{DiffSum}(D') : D' \in \mathcal{D}'_{t,k,v})\end{aligned}$$

Bounds on $\mathsf{DiffSum}(t,k,v)$ and $\mathsf{DiffSum}'(t,k,v)$ and labellings that meet or come close to these bounds are investigated in [11, 8, 9]. A point-labelling of the dual of a Steiner system can be thought of as a labelling of the blocks of the (primal) Steiner system. Given an $S(t,k,v)$ $D = (V,\mathcal{B})$ a *block labelling* of D is a bijection $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$, which is nothing more than a point labelling of its dual D'. Henceforth, we use the block labelling representation.

Given a block labelling $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ of an $S(t,k,v)$ $D = (V,\mathcal{B})$ and a subset $S \subseteq [0, |\mathcal{B}| - 1]$, let $\mathsf{rk}^{-1}(S)$ denote the preimage of S under rk; that is, $\mathsf{rk}^{-1}(S) = \{B \in \mathcal{B} : \mathsf{rk}(B) \in S\}$. For each $x \in V$, the *point sum* with respect to rk, denoted $\mathsf{psum}(x, \mathsf{rk})$, is $\sum_{\{B \in \mathcal{B} : x \in B\}} \mathsf{rk}(B)$. With this, we can translate each of the four point labelling metrics of D', the dual of D, into equivalent block labelling metrics of D:

$$\begin{aligned}\mathsf{MinSum}(D,\mathsf{rk}) &= \min(\mathsf{psum}(x,\mathsf{rk}) : x \in V),\\ \mathsf{MaxSum}(D,\mathsf{rk}) &= \max(\mathsf{psum}(x,\mathsf{rk}) : x \in V),\\ \mathsf{DiffSum}(D,\mathsf{rk}) &= \mathsf{MaxSum}(D,\mathsf{rk}) - \mathsf{MinSum}(D,\mathsf{rk}), \text{ and}\\ \mathsf{RatioSum}(D,\mathsf{rk}) &= \mathsf{MaxSum}(D,\mathsf{rk})/\mathsf{MinSum}(D,\mathsf{rk}).\end{aligned}$$

The point and block sum metric notations are syntactically indistinguishable, so it is important to emphasize what kind of labelling rk is (block or point).

The DiffSum of any block labelling can be no less than zero, and any block labelling of an $S(t,k,v)$ that attains this is *egalitarian*. Dau and Milenkovic [11], provide block labellings of $S(2,3,v)$s having DiffSum $O(23v^3/1728)$. In [9], Colbourn constructs egalitarian labellings for an infinite family of $S(2,3,v)$s. In this work, given a certain kind of resolvable 1-rotational $S(2,k,v)$, we construct for it either an egalitarian labelling or a DiffSum $k+1$ labelling when no egalitarian labelling is possible.

2 Labelling resolvable 1-rotational $S(2,k,v)$s

Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G,N,k,1)$ difference family; hence, $S = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$ is a complete system of representatives of the cosets of N in G, which we write as $S = \{s_0 = 0, s_1, \ldots, s_{|S|-1}\}$. Applying Construction 1.1, put

$$\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\},$$

so that $\mathcal{R} = \{\mathcal{P}_0 + s : s \in S\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. An *$\mathcal{R}$-intervaled block labelling* of D is a block labelling $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ whose inverse rk^{-1} maps each sub-interval of $[0, |\mathcal{B}| - 1]$ of the form

$$[i((k-1)|\mathcal{F}| + 1), (i+1)(k-1)|\mathcal{F}|],$$

where $i \in [0, |S| - 1]$, to the blocks of a unique parallel class of $\mathcal{R}$ such that in particular rk assigns to $\mathcal{P}_0$ the first interval of labels $[0, (k-1)|\mathcal{F}|]$. For any such $\mathcal{R}$-intervaled block labelling, given a point $x \in V$, there exists a unique value $\ell_{x,i} \in [0, (k-1)|\mathcal{F}|]$ such that $x \in \mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + \ell_{x,i})$. Any such $\ell_{x,i}$ is a *parallel class-relative label* with respect to rk. We thus write the point sum of x with respect to rk as

$$\sum_{i=0}^{|S|-1} (i(k-1)|\mathcal{F}|) + \sum_{i=0}^{|S|-1} \ell_{x,i}. \tag{1}$$

The first summation of (1) is independent of x. The second summation is the *resolution-relative point sum of x (with respect to rk).* Labelling in this manner ensures that differences only arise in the second summation.

Let rk be an $\mathcal{R}$-intervaled block labelling of D, and suppose that $\iota = \mathsf{rk}(\{N \cup \{\infty\}\})$. Define the sequence

$$\begin{aligned} S &= (0, 1, \ldots, \iota - 1, \iota + 1, \iota + 2, \ldots, (k-1)|\mathcal{F}| - 1) \\ &= (s_0, s_1, \ldots, s_{(k-1)|\mathcal{F}|-1}), \end{aligned}$$

and for each $i \in [0, |\mathcal{F}| - 1]$, define the $(k-1)$-set $I_i = \{s_{i(k-1)}, \ldots, s_{i(k-1)+k-2}\}$. If $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, rk is an *$(\mathcal{R}, N)$-intervaled block labelling* of D provided that $\mathsf{rk}(\{B_i + n : n \in N\}) = I_i$ for each $i \in [0, |\mathcal{F}| - 1]$.

Let rk be an $\mathcal{R}$-intervaled block labelling of D. Then rk is *development-consistent with respect to S* if for all $i \in [0, (k-1)|\mathcal{F}|]$ and $j \in [1, |S| - 1]$,

$$\mathsf{rk}^{-1}(i + j((k-1)|\mathcal{F}| + 1)) = \mathsf{rk}^{-1}(i) + s_j.$$

In words, for each $B \in \mathcal{P}_0$, the labels assigned by rk to $\{B + s : s \in S\}$ can be arranged into an arithmetic sequence with common difference $((k-1)|\mathcal{F}| + 1)$.

Henceforth we focus on labellings that are both development-consistent and $(\mathcal{R}, N)$-intervaled. When rk is such a labelling and if S is a group, then for each $a \in [0, |\mathcal{F}| - 1]$, the multiset union

$$\bigcup_{b \in [0, |S|-1], c \in I_a} \mathsf{rk}^{-1}\left(b((k-1)|\mathcal{F}| + 1) + c\right)$$

is equal to k copies of G. This follows from the fact that for each $B \in \mathcal{F}$, the multiset $\{B + h + n : h \in S, n \in N\}$ consists of k copies of G.

We supply three distinct development-consistent $(\mathcal{R}, N)$-intervaled block labellings (given in Theorems 2.1, 2.3, and 2.5) for resolvable 1-rotational Steiner 2-designs generated by $(G, N, k, 1)$ difference families that satisfy the *labelling condition*: the union of the base blocks of the generating difference family together with $0 \in G$ is a group. Table 1 specifies for the four possible classes of such designs, determined by the parity of $|\mathcal{F}|$ and $|N|$, which labelling to apply and the resulting $\mathsf{DiffSum}$ (bound). We begin with a labelling of the first two classes.

Table 1: Summary of labellings with corresponding DiffSum (bound)

$\lvert\mathcal{F}\rvert$	$\lvert N\rvert$	Labelling to apply	DiffSum of labelling
even	even	Theorem 2.1	0 (egalitarian)
even	odd	Theorem 2.1	0 (egalitarian)
odd	even	Theorem 2.3	0 (egalitarian)
odd	odd	Theorem 2.5	$\geq k-1$ and $\leq k+1$

Theorem 2.1. *Suppose that $\mathcal{F}$, with $|\mathcal{F}|$ even, is a 1-rotational $(G, N, k, 1)$-RDF such that*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 1.1, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. Then D admits an egalitarian labelling.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \backslash \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, and $N = \{n_0, \ldots, n_{k-2}\}$. Consider the $\mathcal{R}$-intervaled block labelling $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ that is development-consistent with respect to H and satisfies the two conditions:

1. For all $i \in [0, |\mathcal{F}|/2 - 1]$ and $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)i + j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - (k-1)i - j) = B_{|\mathcal{F}|-1-i} + n_j$.
2. $\mathsf{rk}^{-1}((k-1)|\mathcal{F}|/2) = \{N \cup \{\infty\}\}$.

By the first condition, rk is $(\mathcal{R}, N)$-intervaled. Hence, for any $x \in G$,

$$\begin{aligned}\sum_{i=0}^{|H|-1} \ell_{x,i} &= k \sum_{i=0}^{(|\mathcal{F}|-2)/2} (i(k-1) + (k-1)|\mathcal{F}| - i(k-1)) + (k-1)|\mathcal{F}|/2 \\ &= k(|\mathcal{F}|/2)(k-1)|\mathcal{F}| + (k-1)|\mathcal{F}|/2 \\ &= \frac{(k-1)|\mathcal{F}|}{2}(k|\mathcal{F}| + 1).\end{aligned}$$

Similarly, the resolution-relative point sum of ∞ is

$$\sum_{i=0}^{|H|-1} \ell_{\infty,i} = (k|\mathcal{F}| + 1)(k-1)|\mathcal{F}|/2,$$

and thus rk is egalitarian. □

Next, our labelling for the third class of designs hinges on an auxiliary result.

Lemma 2.2. *For each even $n \geq 4$, there exist two permutations σ_n and σ'_n of $\mathbb{Z}_n$ such that*

$$\bigcup_{i \in \mathbb{Z}_n} (\sigma_n(i) + \sigma'_n(i)) = [n/2 - 1, n - 2] \cup [n, 3n/2 - 1].$$

Proof. Put $\sigma_n(i) = i$ for all $i \in \mathbb{Z}_n$. Suppose that $n \equiv 0 \pmod 4$. Then for all $i \in S = [0, n/4 - 1] \cup [3n/4, n - 1]$, put $\sigma'_n(i) = i + n/2 \pmod n$, so that

$$\bigcup_{i \in S} (\sigma_n(i) + \sigma'_n(i)) = \{n/2, n/2 + 2, \ldots, n - 2\} \cup \{n, n + 2, \ldots, 3n/2 - 2\}.$$

For all $j \in S' = [n/4, 3n/4 - 2]$, put $\sigma'_n(j) = j + n/2 + 1 \pmod n$, ensuring that

$$\bigcup_{j \in S'} (\sigma_n(j) + \sigma'_n(j)) = \{n + 1, n + 3, \ldots, 3n/2 - 3\} \cup \{n/2 - 1, n/2 + 1, \ldots, n - 3\}.$$

Finally, put $\sigma'_n(3n/4 - 1) = 3n/4$.

Now suppose that $n \equiv 2 \pmod 4$. Then for all $i \in T = [0, (n-6)/4] \cup [(3n-2)/4, n-1]$, put $\sigma'_n(i) = i + n/2 + 1 \pmod n$; it follows that

$$\bigcup_{i \in T} (\sigma_n(i) + \sigma'_n(i)) = \{n/2 + 1, n/2 + 3, \ldots, n - 2\} \cup \{n, n + 2, \ldots, 3n/2 - 1\}.$$

For all $j \in T' = [(n + 2)/4, (3n - 6)/4]$, put $\sigma'_n(j) = j + n/2 \pmod n$; hence,

$$\bigcup_{j \in T'} (\sigma_n(j) + \sigma'_n(j)) = \{n + 1, n + 3, \ldots, 3n/2 - 2\} \cup \{n/2, n/2 + 2, \ldots, n - 3\}.$$

Finally, put $\sigma'_n((n - 2)/4) = (n - 2)/4$. □

Corollary 2.2.1. *For each even $n \geq 4$, there exist two permutations σ_n, σ'_n of $\mathbb{Z}_n$ and one permutation σ_{n+1} of $\mathbb{Z}_{n+1}$ with $\sigma_{n+1}(n) = n/2$ such that for all $i \in \mathbb{Z}_n$, $\sigma_n(i) + \sigma'_n(i) + \sigma_{n+1}(i) = 3n/2 - 1$.*

Proof. Apply Lemma 2.2 to obtain two permutations σ_n and σ'_n. Then for each $i \in \mathbb{Z}_n$, there exists a unique $j \in [0, n/2 - 1] \cup [n/2 + 1, n]$ such that $\sigma_n(i) + \sigma'_n(i) = 3n/2 - 1 - j$, so put $\sigma_{n+1}(i) = j$. □

We now label the third class of Steiner 2-designs.

Theorem 2.3. *Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G, N, k, 1)$-RDF such that $|\mathcal{F}| \geq 3$ is odd, $|N| \geq 4$ is even, and*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 1.1, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. Then D admits an egalitarian labelling rk.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \backslash \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, and $N = \{n_0, \ldots, n_{k-2}\}$. Applying Corollary 2.2.1, let $\sigma_{k-1}, \sigma'_{k-1}$ be two permutations of $\mathbb{Z}_{k-1}$ and σ_k a permutation of $\mathbb{Z}_k$ with $\sigma_k((k-1)/2) = k - 1$ such that for all $i \in \mathbb{Z}_{k-1}$, $\sigma_{k-1}(i) + \sigma'_{k-1}(i) + \sigma_k(i) = 3(k-1)/2 - 1$. Suppose that $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ is $\mathcal{R}$-intervaled, development-consistent with respect to H, and has the three properties:

1. For all $i \in [1, (|\mathcal{F}|-3)/2]$ and $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)i+j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - (k-1)i - j) = B_{|\mathcal{F}|-i} + n_j$.
2. For $i \in [0, k-2]$,
   (a) $\mathsf{rk}^{-1}(\sigma_{k-1}(i)) = B_0 + n_i$, and
   (b) $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - k + 2 + \sigma'_{k-1}(i)) = B_{|\mathcal{F}|-1} + n_i$;

   and for $j \in [0, (k-3)/2] \cup [(k+1)/2, k-1]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}|-1)/2 + \sigma_k(j)) = B_{(|\mathcal{F}|-1)/2} + n_j$.
3. $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}|-1)/2 + (k-1)/2) = \{N \cup \{\infty\}\}$.

The first two properties imply that rk is $(\mathcal{R}, N)$-intervaled. This, as well as Corollary 2.2.1, imply that the resolution-relative point sum of any $x \in G$ is

$$k\left(\frac{|\mathcal{F}|-3}{2}(k-1)|\mathcal{F}| + \frac{3(k-1)-2}{2} + (k-1)|\mathcal{F}| - k + 2 + \frac{(k-1)(|\mathcal{F}|-1)}{2}\right) + (k-1)(|\mathcal{F}|-1)/2 + (k-1)/2 = \frac{|\mathcal{F}|(k-1)(|\mathcal{F}|k+1)}{2}.$$

Likewise, the resolution-relative point sum of ∞ is

$$(k|\mathcal{F}|+1)\left((k-1)(|\mathcal{F}|-1)/2 + (k-1)/2\right) = \frac{|\mathcal{F}|(k-1)(|\mathcal{F}|k+1)}{2},$$

and thus rk is egalitarian. □

The constituents of the fourth class of Steiner 2-designs, those for which both $|\mathcal{F}|$ and $|N|$ are odd, seem the most difficult to label well. Because $|\mathcal{F}|$ is odd, we cannot partition $\mathcal{F}$ into pairs of base blocks, as we did in the labelling of Theorem 2.1. Because $|N|$ is also odd, we cannot assign to each ∞-block the same (middle) parallel class-relative label, for this places a significant gap between the point sum of ∞ and the average point sum. Instead, we assign to $(|H|-1)/2$ ∞-blocks the parallel class-relative label $((k-1)|F|-1)/2$, and to the remaining $(|H|+1)/2$ ∞-blocks the parallel class-relative label $((k-1)|F|+1)/2$, getting the point sum of ∞ close to the average point sum. For this reason, our labelling cannot be development-consistent. Our strategy for this case follows: We select three base blocks $B_0, B_{(|\mathcal{F}|-1)/2}$, and $B_{\mathcal{F}-1}$, and arrange the blocks of the three $(k-1)$-sets $\{B_0+n : n \in N\}$, $\{B_{(|\mathcal{F}|-1)/2} + n : n \in N\}$, and $\{B_{|\mathcal{F}|-1} + n : n \in N\}$ using three permutations. We then partition the remaining base blocks into pairs.

Lemma 2.4. *For all odd $n \geq 3$, there exist three permutations $\sigma_{n,0}, \sigma_{n,1}, \sigma_{n,2}$ of $[0, n-1]$ such that for $i, j \in [0, n-1]$, $\sigma_{n,0}(i) + \sigma_{n,1}(i) + \sigma_{n,2}(i) = \sigma_{n,0}(j) + \sigma_{n,1}(j) + \sigma_{n,2}(j)$.*

Proof. Define $\sigma_{n,0}(i) = n-1-i$ for all $i \in [0, n-1]$, and define $\sigma_{n,1}(j) = (n-1)/2 - j \pmod n$ for all $j \in [0, n-1]$. Then for $i \in [0, (n-1)/2]$, $\sigma_{n,0}(i) + \sigma_{n,1}(i) = (3n-3)/2 - 2i$ and for $j \in [(n+1)/2, n-1]$, $\sigma_{n,0}(j) + \sigma_{n,0}(j) = n-1-j+(3n-1)/2-j = (5n-3)/2-2j$. Thus, the range of $\sigma_{n,0} + \sigma_{n,1}$ over $[0, n-1]$ is $[(n-1)/2, (3n-3)/2]$. Accordingly, for all $i \in [0, n-1]$, put $\sigma_{n,2}(i) = n-1-j$ whenever $\sigma_{n,0}(i) + \sigma_{n,1}(i) = (n-1)/2 + j$, so that $\sigma_{n,0}(h) + \sigma_{n,1}(h) + \sigma_{n,2}(h) = (3n-3)/2$ for all $h \in [0, n-1]$, as desired. □

Theorem 2.5. *Suppose that $\mathcal{F}$ is a resolvable 1-rotational $(G, N, k, 1)$ difference family such that $|\mathcal{F}|$ and $|N|$ are odd, $|\mathcal{F}| \geq 3$, and*

$$H = \{0\} \cup \bigcup_{B \in \mathcal{F}} B$$

is a subgroup of G. Applying Construction 1.1, designate H as the complete system of representatives for the cosets of N in G and put $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in N\} \cup \{N \cup \{\infty\}\}$, so that $\mathcal{R} = \{\mathcal{P}_0 + h : h \in H\}$ is a resolution of an $S(2, k, |G| + 1)$, say $D = (V, \mathcal{B})$. Then D admits a block labelling rk with $\mathsf{DiffSum}$ at most $k + 1$ and at least $k - 1$.

Proof. Let $\mathcal{F} = \{B_0, \ldots, B_{|\mathcal{F}|-1}\}$, $h_0 = 0$, $H \setminus \{0\} = \{h_1, \ldots, h_{k|\mathcal{F}|}\}$, $N = \{n_0, \ldots, n_{k-2}\}$, and $B_\infty = \{N \cup \{\infty\}\}$. Moreover, let $\sigma_{k-1,0}, \sigma_{k-1,1}$, and $\sigma_{k-1,2}$ denote the three permutations of $[0, k-2]$ from Lemma 2.4. Let $\mathsf{rk} : \mathcal{B} \to [0, |\mathcal{B}| - 1]$ be an $\mathcal{R}$-intervaled block labelling with the five properties:

P1. For all $i \in [0, ((k-1)|\mathcal{F}| - 3)/2] \cup [((k-1)|\mathcal{F}| + 3)/2, (k-1)|\mathcal{F}|]$ and $j \in [1, |H| - 1]$, $\mathsf{rk}^{-1}(i + j((k-1)|\mathcal{F}| + 1)) = \mathsf{rk}^{-1}(i) + h_j$.

P2. For all $i \in [1, (|\mathcal{F}| - 3)/2]$ and $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)i + j) = B_i + n_j$ and $\mathsf{rk}^{-1}((k-1)|\mathcal{F}| - (k-1)i - j) = B_{|\mathcal{F}|-i} + n_j$.

P3. (a) For all $j \in [0, k-2]$, $\mathsf{rk}^{-1}(\sigma_{k-1,0}(j)) = B_0 + n_j$.

(b) For all $j \in [0, k-2]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}| - 1) + 1 + \sigma_{k-1,1}(j)) = B_{|\mathcal{F}|-1} + n_j$.

(c) For $j \in [0, (k-4)/2]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}| - 1)/2 + j) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}(j)}$

(d) For $j \in [k/2, k-1]$, $\mathsf{rk}^{-1}((k-1)(|\mathcal{F}| - 1)/2 + j) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}(j-1)}$.

P4. (a) For all $i \in [0, (|H| - 3)/2]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + ((k-1)|\mathcal{F}| - 1)/2) = B_\infty + h_i$.

(b) For all $i \in [(|H| - 1)/2, |H| - 1]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + ((k-1)|\mathcal{F}| + 1)/2) = B_\infty + h_i$.

P5. (a) For all $i \in [0, (|H| - 3)/2]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + ((k-1)|\mathcal{F}| + 1)/2) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}((k-2)/2)} + h_i$.

(b) For all $i \in [(|H| - 1)/2, |H| - 1]$, $\mathsf{rk}^{-1}(i((k-1)|\mathcal{F}| + 1) + ((k-1)|\mathcal{F}| - 1)/2) = B_{(|\mathcal{F}|-1)/2} + n_{\sigma^{-1}_{k-1,2}((k-2)/2)} + h_i$.

By properties P4(a) and P4(b), rk is not development-consistent; yet by properties P2 and P3(a) - (d) it is $(\mathcal{R}, N)$-intervaled.

By properties P4(a) and P4(b), the resolution-relative point sum for ∞ is

$$\begin{aligned}
\sum_{i=0}^{|H|-1} \ell_{\infty,i} &= \frac{(|H| - 1)((k-1)|\mathcal{F}| - 1) + (|H| + 1)((k-1)|\mathcal{F}| + 1)}{4} \\
&= \frac{k|\mathcal{F}|((k-1)|\mathcal{F}| - 1) + (k|\mathcal{F}| + 2)((k-1)|\mathcal{F}| + 1)}{4} \\
&= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + 1}{2}
\end{aligned}$$

The resolution-relative point sum for $x \in G$ depends on which one of the following $2k + 4$ mutually exclusive types it is.

T1. $x \in H + n_i$ for some $i \in \{\sigma_{k-1,2}^{-1}(0), \sigma_{k-1,2}^{-1}(1), \ldots, \sigma_{k-1,2}^{-1}((k-4)/2)\}$ and either

(a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

(b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

T2. $x \in H + n_i$ for some $i \in \{\sigma_{k-1,2}^{-1}(k/2), \sigma_{k-1,2}^{-1}((k+2)/2), \ldots, \sigma_{k-1,2}^{-1}(k-2)\}$ and either

(a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

(b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

T3(α, β). There exists an α-set $S \subseteq [0, (|H|-3)/2]$ and a β-set $T \subseteq [(|H|-1)/2, |H|-1]$ such that for each $i \in S$, $x \in B_{(|\mathcal{F}|-1)/2} + n_{\sigma_{k-1,2}^{-1}((k-2)/2)} + h_i$ and each $j \in T$, $x \in B_{(|\mathcal{F}|-1)/2} + n_{\sigma_{k-1,2}^{-1}((k-2)/2)} + h_j$; and either

(a) $x \in B_\infty + h_j$ for some $j \in [0, (|H|-3)/2]$, or

(b) $x \in B_\infty + h_j$ for some $j \in [(|H|-1)/2, |H|-1]$.

In sum, we have the set of $2k+4$ point types

$$\{\text{T1(a)}, \text{T1(b)}, \text{T2(a)}, \text{T2(b)}\} \bigcup \bigcup_{\{(\alpha,\beta):\alpha+\beta=k\}} \{\text{T3}(\alpha,\beta)\text{(a)}, \text{T3}(\alpha,\beta)\text{(b)}\}.$$

If x is of type T1(a) then its resolution-relative point sum is

$$k\left(\frac{3k-6}{2} + \frac{3(k-1)(|\mathcal{F}|-1)+2}{2} + \frac{|\mathcal{F}|-3}{2} \cdot (k-1)|\mathcal{F}|\right) + \frac{(k-1)|\mathcal{F}|-1}{2}$$
$$= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k - 1}{2}.$$

Thus, if x is of type T1(b), its resolution-relative point sum is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k + 1}{2}.$$

If x is of type T2(a), its resolution-relative point sum is

$$k\left(\frac{3k-6}{2} + \frac{3(k-1)(|\mathcal{F}|-1)+4}{2} + \frac{|\mathcal{F}|-3}{2} \cdot (k-1)|\mathcal{F}|\right) + \frac{(k-1)|\mathcal{F}|-1}{2}$$
$$= \frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k - 1}{2}.$$

Hence, if x is of type T2(b), its resolution-relative point sum is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k + 1}{2}.$$

The calculations for the T3 types derive from the calculations of the T1 and T2 types. Indeed, the T3 types may be ordered increasingly by their corresponding resolution-relative point sums as the sequence

$$(\text{T3}(0,k)\text{(a)}, \text{T3}(0,k)\text{(b)}, \text{T3}(1,k-1)\text{(a)}, \text{T3}(1,k-1)\text{(b)}, \ldots, \text{T3}(k,0)\text{(b)}),$$

where a T3$(0,k)$(a) point has the least resolution-relative point sum, equal to the resolution-relative point sum of a T1(a) point, and a T3$(k,0)$(b) point has the greatest resolution-relative point sum, equal to the resolution-relative point sum of a T2(b) point. Thus, the DiffSum of rk is at most the difference between the resolution-relative point sums of a type T2(b) and a type T1(a) point, which is

$$\frac{|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| + k + 1 - (|\mathcal{F}|^2k^2 - |\mathcal{F}|^2k + |\mathcal{F}|k - |\mathcal{F}| - k - 1)}{2}$$
$$= k + 1.$$

Moreover, there must exist a point of type T1(a) or T1(b), and there must exist a point of type T2(a) or T2(b). Hence, the DiffSum is at least $k - 1$. □

We now verify that egalitarian labellings cannot exist for this fourth class of Steiner 2-designs. As noted in [9], the average point sum of an $S(t,k,v)$ D is $r(b-1)/2$, where r is the replication number and b is the number of blocks of D. Hence, if b is even and r is odd, then the average point sum is not integral, and thus D cannot admit an egalitarian labelling. Now let $\mathcal{B}$ be the block set of a resolvable 1-rotational Steiner 2-design D generated by a $(G,N,k,1)$-RDF $\mathcal{F}$. Then D has replication number $r = |G|/(k-1)$. Supposing that $|\mathcal{F}|$ and $|N|$ are odd, then since

$$|\mathcal{F}| = \frac{1}{k}\left(\frac{|G|}{|N|} - 1\right)$$
$$\iff |G| = (k|\mathcal{F}| + 1)|N|,$$

$|G|$ is odd, and hence r is odd. Moreover, a parallel class of $\mathcal{B}$ has $|\mathcal{F}| + 1$ blocks; that is, an even number of blocks, so that $|\mathcal{B}|$ is even.

3 Meeting the labelling condition

In this section we show that many of the difference families in the literature, both directly and recursively constructed, satisfy the labelling condition imposed on all the designs labelled in Section 2.

3.1 Direct Constructions

It is common to construct 1-rotational $(G,N,k,1)$-RDFs with the form: $G = \mathbb{F}_q \oplus H$ and $N = \{0\} \oplus H$, where H is an (additive) group. Following [1], this is the *standard form*. Given any such difference family, the union of its base blocks together with $0 \in G$ must be a subgroup of G, because any arbitrary system of representatives for the cosets of N in G is a group isomorphic to $\{0\} \oplus H$. To our knowledge, every direct construction in the literature of an infinite class of 1-rotational $(G,N,k,1)$-RDFs has the standard form. Small examples exist that do not have the standard form. For instance, Example 1.3 of [2] is a cyclic $(51,3,4,1)$-RDF, the union of whose base blocks together with 0 do not form a subgroup of $\mathbb{Z}_{51}$. As another instance, every 1-rotational KTS(33) is either a $(\mathbb{Z}_{32}, \{0,16\}, 3, 1)$-RDF or a $(Q_{32}, \{1, x^8\}, 3, 1)$-RDF, where Q_{32} is the dicyclic group of order 32 [5]. It is routine to verify that not one of the former kind of RDFs can satisfy the labelling condition.

3.2 Recursions

In [15] Jimbo and Vanstone present a recursive construction for cyclically-resolvable 1-rotational Steiner 2-designs. In [4] Buratti and Zuanni rephrase their construction in the language of the difference families. We first define a key ingredient of their construction. A $(w, k, 1)$ *difference matrix* is a $k \times w$ matrix $D = (d_{ij})$ with entries from $\mathbb{Z}_w$ such that for each $1 \leq i < j \leq k$,

$$\mathbb{Z}_w = \{d_{i\ell} - d_{j\ell} : 1 \leq \ell \leq k\}.$$

A $(w, k, 1)$ difference matrix D is *good* if no row of D contains any element of $\mathbb{Z}_w$ more than once.

Construction 3.1 (Buratti and Zuanni's restatement of the Jimbo-Vanstone construction [4])**.** Let $\mathcal{D} = \{D_i : i \in I\}$ and $\mathcal{E} = \{E_j : j \in J\}$ be resolvable $((k-1)v, k-1, k, 1)$ and $((k-1)w, k-1, k, 1)$ difference families, respectively. Suppose that $\gcd(w, k-1) = 1$ and let $D = (d_{ih})$ be a good $(w, k, 1)$ difference matrix. For each $D_i = \{d_{i1}, d_{i2}, \ldots, d_{ik}\} \in \mathcal{D}$ and each $h \in [1, w]$, put $D_{(i,h)} = \{d_{i1} + (k-1)va_{1h}, d_{i2} + (k-1)va_{2h}, \ldots, d_{ik} + (k-1)va_{kh}\}$. For each $E_j = \{e_{j1}, e_{j2}, \ldots, e_{jk}\} \in \mathcal{E}$, put $E_j^* = \{ve_{j1}, ve_{j2}, \ldots, ve_{jk}\}$. Then the set

$$\mathcal{F} = \{D_{(i,h)} \pmod{(k-1)vw} : i \in I, h \in [1, w]\} \cup \{E_j^* \pmod{(k-1)vw} : j \in J\}$$

is a $((k-1)vw, k-1, k, 1)$-RDF.

Any difference family yielded by an application of Construction 3.1 satisfies the labelling condition, provided that the ingredient families of the application also satisfy it.

Theorem 3.1. *Let $\mathcal{D} = \{D_i : i \in I\}$ and $\mathcal{E} = \{E_j : j \in J\}$ be resolvable $((k-1)v, k-1, k, 1)$ and $((k-1)w, k-1, k, 1)$ difference families, respectively, that each satisfy the labelling condition. Suppose that $\gcd(w, k-1) = 1$ and let $D = (d_{ih})$ be a good $(w, k, 1)$ difference matrix. Then with $\mathcal{D}$ and $\mathcal{E}$ as ingredients of Construction 3.1, the resulting $((k-1)vw, k-1, k, 1)$ difference family $\mathcal{F}$ also meets the labelling condition.*

Proof. By assumption, the set $\bigcup_{D \in \mathcal{D}} D \cup \{0\}$ is a subgroup of $\mathbb{Z}_{(k-1)v}$ of order v, and is thus precisely the set of all distinct multiples of $k-1$ modulo $(k-1)v$. Likewise, the union of the base blocks of $\mathcal{E}$ together with 0 is precisely the set of all distinct multiples of $k-1$ modulo $(k-1)w$. Hence, as $\mathcal{F}$ is resolvable, the union of its base blocks consists of all distinct nonzero multiples of $k-1$ modulo $(k-1)vw$. Thus, adjoining to this union the zero element must give us a subgroup (isomorphic to $\mathbb{Z}_{vw}$) of $\mathbb{Z}_{(k-1)vw}$. □

3.3 General asymptotic constructions

Here are some asymptotic constructions that instantiate the standard form.

Theorem 3.2 (Corollary 4.2 of [3])**.** *For any integer k and any prime $p \equiv k(k+1)+1 \pmod{2k(k+1)}$ sufficiently large there exists a $((k-1)p, k-1, k, 1)$-RDF.*

Hence applying Construction 1.1, we have:

Corollary 3.2.1. *For any integer k and any prime $p \equiv k(k+1)+1 \pmod{2k(k+1)}$ sufficiently large there exists a resolvable 1-rotational $S(2, k, (k-1)p+1)$.*

The next four results are from [10].

Theorem 3.3. *Let p be a prime power satisfying $p \equiv 3 \pmod 4$. Then for any prime power $q \equiv 1 \pmod{p+1}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p+1, pq+1)$.*

Theorem 3.4. *Let p and $p+2$ be twin prime powers satisfying $p > 2$. Then for any prime power $q \equiv 1 \pmod{p(p+2)+1}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p(p+2)+1, p(p+2)q+1)$.*

Theorem 3.5. *Let $m \geq 3$ be an integer. Then for any sufficiently large prime power $q \equiv 1 \pmod{2^m}$, there exists a resolvable 1-rotational $S(2, 2^m, (2^m-1)q+1)$.*

Theorem 3.6. *Let p be a prime power satisfying $p \equiv 1 \pmod 4$. Then for any prime power $q \equiv 1 \pmod{2p+2}$ sufficiently large, there exists a resolvable 1-rotational $S(2, p+1, pq+1)$.*

3.4 Existence tables for small k

Attention has focused on producing resolvable 1-rotational $S(2, k, v)$s of the standard form with $k \in [3, 9]$. In general the known orders v for such Steiner 2-designs do not originate solely from asymptotic constructions. Table 2 gives (some) orders v for which a resolvable 1-rotational $S(2, k, v)$ exists whose generating RDF satisfies the conditions of either Theorem 2.1 or Theorem 2.3, so that the design admits an egalitarian labelling. For $k = 3, 4$ we also provide the orders obtained by feeding the appropriate subset of the base set of orders obtained via the constructions of [19] and [18], respectively, into the Jimbo-Vanstone construction (JVC). For $k = 5$ we provide a collection of orders produced via an asymptotic construction [16] that is tailored to that specific blocksize. Table 3 gives (some) orders v for which a resolvable 1-rotational $S(2, k, v)$ exists whose generating RDF satisfies the conditions of Theorem 2.5, so that the design admits a (non-egalitarian) labelling having DiffSum at most $k+1$ and at least $k-1$.

Table 2: Orders of resolvable 1-rotational $S(2, k, v)$s with egalitarian labelling

k	v
3	$v \in \{8s+1 :$ each prime factor of s is congruent to 1 mod 6$\}$ [6], $v \in \{2s+1 :$ each prime factor of s is congruent to 1 mod 6$\}$([19] + JVC)
4	$v \in \{3s+1 : s$ is a product of primes, each congruent to 1 mod 4, such that the number of primes congruent to 5 mod 8 is even$\}$ ([18] + JVC)
5	$v \in \{125, 725, 845, 965, 1085, 1685, 2285, 2405, 2525, 2765, 3005, 3965\}$[1] and $v = 4p+1$ for p sufficiently large such that $p \equiv 1 \pmod{30}$ and $(11+5\sqrt{5})/2$ mod p is not a cube [16]
6	$v \in \{5p+1 : p = 12t+1$ is prime, $p \notin \{13, 37\}$, and $(p-1)/6 \equiv 0 \pmod 2\}$ [2]
7	$v \in \{1687, 5719, 13783, 17815, 27895, 35287, 37303, 37975, 39319, 45367, 49399,$ 52087,55447,58135$\}$[1]
8	$v = 1576$ [10] $v \in \{7p+1 : p = 8t+1$ is prime, $p \neq 17$, and $(p-1)/8 \equiv 0 \pmod 2\}$ [2]
9	$v \in \{7929, 12249, 52569, 77049\}$ [1]

Table 3: Orders of resolvable 1-rotational $S(2,k,v)$ admitting $k-1 \leq \mathsf{DiffSum} \leq k+1$ labelling

k	v
4	$v \in \{3s+1 : s$ is a product of primes, each congruent to 1 mod 4, such that the number of primes congruent to 5 mod 8 is odd$\}$ ([18] + JVC)
6	$v \in \{5p+1 : p = 12t+1$ is prime and $(p-1)/6 \equiv 1 \pmod 2\}$ [2]
8	$v \in \{624, 2976\}$ [10] $v \in \{7p+1 : p = 8t+1$ is prime, $p \neq 89$, and $(p-1)/8 \equiv 1 \pmod 2\}$ [2]

4 Improving the DiffSum bound for Moore Designs

The aim of this section is to demonstrate the existence of an infinite class of 1-rotational $(G, N, 4, 1)$-RDFs having an odd number of base blocks that generate Steiner 2-designs admitting labellings with DiffSum 3. Were one to apply Theorem 2.5 to label such a design, the DiffSum would, at worst, be $k+1 = 5$, and at best be $k-1 = 3$. However, that is not the approach we take.

The class of difference families that we intend to label differently from the techniques of Section 2 consists of $(\mathbb{F}_n \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDFs for each $n = 4t+1$ a prime power. For simplicity, for any $\sigma_i, \sigma_j \in \mathbb{F}_n$ and $c \in \mathbb{Z}_3$, denote $(\sigma_i, c) \oplus (\sigma_j, 0) = (\sigma_i + \sigma_j, c)$ by $(\sigma_i, c) \oplus \sigma_j$; also define $\infty \oplus \sigma_i = \infty$. For any subset $S \subseteq \mathbb{F}_n \times \mathbb{Z}_3$ define $S \oplus \sigma_j = \{(\sigma_i, c) \oplus \sigma_j : (\sigma_i, c) \in S\}$ and for any set $\mathcal{S}$ of subsets of $\mathbb{F}_n \times \mathbb{Z}_3$, define $\mathcal{S} \oplus \sigma_j = \{S \oplus \sigma_j : S \in \mathcal{S}\}$. For $\sigma_i, \sigma_j \in \mathbb{F}_n^\times$ and $c \in \mathbb{Z}_3$, let $(\sigma_i, c) \cdot \sigma_j = (\sigma_j \cdot \sigma_i, c)$, with multiplication performed over $\mathbb{F}_n^\times$. For any subset $S \subseteq \mathbb{F}_n \times \mathbb{Z}_3$, define $S \cdot \sigma_j = \{(\sigma_i, c) \cdot \sigma_j : (\sigma_i, c) \in S\}$.

Construction 4.1. (Moore construction [18]) Let $n = 4t+1$ be a prime power and x a primitive element of $\mathbb{F}_n$ (and thus $x^{2t} = -1 \in \mathbb{F}_n$). Then

$$\mathcal{F} = \{\{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\} : i \in [0, t-1]\}$$

is an $(\mathbb{F}_n \times \mathbb{Z}_3, \{0\} \times \mathbb{Z}_3, 4, 1)$-RDF.

A difference family produced by the Moore construction is a *Moore difference family*. A difference $(\sigma, c) - (\sigma', c)$ (with subtraction performed coordinate-wise) of any two points of a Moore difference family with the same second coordinate is a *pure difference*; a difference $(\sigma, c) - (\sigma', c')$, $c \not\equiv c' \pmod 3$ of any two points of a Moore difference family with distinct second coordinates is a *mixed difference*. An overview of the theory of mixed and pure differences is given in [14]. A Moore difference family has the standard form and thus meets the labelling condition, so any Moore difference family with an even number of base blocks (equivalently, t is even) admits an egalitarian labelling. When $|\mathcal{F}|$ is odd (equivalently, t is odd) we do not develop the base parallel class, henceforth denoted $\mathcal{P}_0 = \{B + n : B \in \mathcal{F}, n \in \{0\} \oplus \mathbb{Z}_3\}$, over the union of the base blocks of $\mathcal{F}$, but instead develop it, as Moore did in [18], over $\mathbb{F}_n \times \{0\}$, to obtain the *classical* resolution $\mathcal{R} = \{\mathcal{P}_0 \oplus \sigma : \sigma \in \mathbb{F}_n\}$. The resolvable 1-rotational $\mathrm{S}(2, 4, 3n+1)$ with classical resolution $\mathcal{R}$ is the *Moore design of order* $3n+1$ ($\mathrm{MD}(3n+1)$) and $\mathcal{F}$ is its *generating* Moore difference family. A block of $\mathrm{MD}(3n+1)$ in the generating Moore difference family is a *base* block. Blocks of $\mathrm{MD}(3n+1)$ having two points with second coordinate $i \pmod 3$ and two points with second coordinate $i+1 \pmod 3$ are

secants; blocks containing ∞ are ∞-*blocks*. A secant of MD($3n+1$) is of *type* i if the set of second coordinates of its constituent points is $\{i, (i+1) \bmod 3\}$.

Let $p = 4t+1$ be a prime, B a (secant) base block of MD($3p+1$), set

1. $\{c_0, c_1\} = \{0, 1\}$,
2. $D = \bigcup_{i=0}^{(p-1)/2} \{B \oplus i\}$,
3. $Y_{c_0} = \{y \in \mathbb{F}_p : \exists B_1, B_2 \in D, B_1 \neq B_2, \text{ s.t. } (y, c_0) \in B_1 \cap B_2\}$, and
4. $N_{c_1} = \{n \in \mathbb{F}_p : \forall B \in D, (n, c_1) \notin B\}$,

and define the *ordered* classical resolution to be the classical resolution $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{p-1}\}$ of the MD($3p+1$) such that $\mathcal{P}_i = \mathcal{P}_0 \oplus i$ for all $i \in [0, p-1]$. Then B is (c_0, c_1)-*special* if the two conditions are satisfied:

1. For $y \in Y_{c_0}$ the unique ∞-block that contains (y, c_0) occurs in $\mathcal{P}_j$ for some $j \in [0, (p-1)/2]$, and
2. for $z \in N_{c_1}$ the unique ∞-block that contains (z, c_1) occurs in $\mathcal{P}_j$ for some $j \in [(p+1)/2, p-1]$.

Equivalently, B is (c_0, c_1)-special if:

1. For $y \in Y_{c_0}$, $y \in [0, (p-1)/2]$, and
2. for $z \in N_{c_1}$, $z \in [(p+1)/2, p-1]$.

Lemma 4.1. *Let $p = 4t+1$ be a prime, x a primitive element of $\mathbb{F}_p$, $\{0,1\} = \{c_0, c_1\}$, and $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$ a (secant) base block of MD($3p+1$). Then B is either (c_0, c_1)-special or (c_1, c_0)-special if and only if*

$$x^i, x^{i+t} \pmod p \in [1, (p-1)/4] \cup [(3p+1)/4, p-1].$$

Proof. Set

1. $D = \bigcup_{i=0}^{(p-1)/2} \{B \oplus i\}$,
2. $Y_{c_0} = \{y \in \mathbb{F}_p : \exists B_1, B_2 \in D, B_1 \neq B_2, \text{ s.t. } (y, c_0) \in B_1 \cap B_2\}$, and
3. $N_{c_1} = \{n \in \mathbb{F}_p : \forall B \in D, (n, c_1) \notin B\}$.

For both directions of the proof of the biconditional, we suppose without loss of generality that $c_0 = 0$ and $c_1 = 1$.

The proof of the forward direction has two cases. First, suppose to the contrary that B is (c_0, c_1)-special and without loss of generality that $x^i \in [(p+3)/4, (p-1)/2]$; then $-x^i \in [(p+1)/2, (3p-3)/4]$. But

$$(p+3)/4 + (p-1)/2 = (3p+1)/4 > (3p-3)/4,$$

and thus there exists some $y > (p-1)/2$ with $y \in Y_{c_0}$, a contradiction. Second, suppose to the contrary and without loss of generality that $x^{i+t} \in [(p+3)/4, (p-1)/2]$; then $-x^{i+t} \in [(p+1)/2, (3p-3)/4]$. But

$$(3p-3)/4 + (p-1)/2 = (5p-5)/4 \equiv (p-5)/4 \pmod{p}$$

and $(p-5)/4 < (p-1)/4 < (p+3)/4$; thus $(p-1)/4 \in N_{c_1}$, a contradiction

For the reverse direction, suppose without loss of generality that $x^i, x^{i+t} \in [1, (p-1)/4]$ so that $-x^i, -x^{i+t} \pmod{p} \in [(3p+1)/4, p-1]$. But

$$(p-1)/4 + (p-1)/2 = (3p-3)/4 < (3p+1)/4$$

and therefore for all $y \in Y_{c_0}$, $y \leq (p-1)/2$. Moreover,

$$(3p+1)/4 + (p-1)/2 = (5p-1)/4 \equiv (p-1)/4 \pmod{p}$$

and hence for all $n \in N_{c_1}$, $n > (p-1)/2$. □

Lemma 4.2. *Let*

$$B_1 = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}, \text{ and}$$
$$B_2 = \{(x^j, 0), (-x^j, 0), (x^{j+t}, 1), (-x^{j+t}, 1)\}$$

be distinct base blocks of MD$(3p+1)$*, with* $p = 4t+1$ *a prime, so that* $i, j \in [0, t-1]$*. Choose* $\alpha_1 \in \{x^i, -x^i\}$*,* $\alpha_2 = \{x^j, -x^j\}$*,* $\beta_1 = \{x^{i+t}, -x^{i+t}\}$*, and* $\beta_2 = \{x^{j+t}, -x^{j+t}\}$ *such that* $S = \{\alpha_1, \alpha_2, \beta_1, \beta_2\} \subset [1, (p-1)/2]$*. Then if* $\max(S) - \min(S) \leq (p-1)/4$*, there exists a* (c_0, c_1)*-special base block of MD*$(3p+1)$*.*

Proof. There are four cases to treat:

1. $x^t\alpha_1 \equiv \beta_1 \pmod{p}$ and $x^t\alpha_2 \equiv \beta_2 \pmod{p}$,
2. $x^t\alpha_1 \equiv \beta_1 \pmod{p}$ and $x^t\alpha_2 \equiv -\beta_2 \pmod{p}$,
3. $x^t\alpha_1 \equiv -\beta_1 \pmod{p}$ and $x^t\alpha_2 \equiv \beta_2 \pmod{p}$, or
4. $x^t\alpha_1 \equiv -\beta_1 \pmod{p}$ and $x^t\alpha_2 \equiv -\beta_2 \pmod{p}$.

Supposing that $\max\{S\} - \min\{S\} \leq (p-1)/4$, then by Lemma 4.1, each of the following four sets, subject to the constraints of the corresponding case, gives the $\mathbb{F}_p$-coordinates of the points of a (c_0, c_1)-special base block of MD$(3p+1)$ (with all arithmetic performed modulo p):

1. $\{\alpha_1 - \alpha_2, -\alpha_1 + \alpha_2, x^t(\alpha_1 - \alpha_2), x^t(\alpha_2 - \alpha_1)\} = \{\alpha_1 - \alpha_2, -\alpha_1 + \alpha_2, \beta_1 - \beta_2, \beta_2 - \beta_1\}$,
2. $\{\alpha_2 - \beta_1, -\alpha_2 + \beta_1, x^t(\alpha_2 - \beta_1), x^t(-\alpha_2 + \beta_1)\} = \{\alpha_2 - \beta_1, -\alpha_2 + \beta_1, -\beta_2 + \alpha_1, \beta_2 - \alpha_1\}$,
3. $\{\alpha_1 - \beta_2, \beta_2 - \alpha_1, x^t(\alpha_1 - \beta_2), x^t(\beta_2 - \alpha_1)\} = \{\alpha_1 - \beta_2, \beta_2 - \alpha_1, -\beta_1 + \alpha_2, -\alpha_2 + \beta_1\}$, and
4. $\{-\alpha_1 + \alpha_2, \alpha_1 - \alpha_2, x^t(-\alpha_1 + \alpha_2), x^t(\alpha_1 - \alpha_2)\} = \{-\alpha_1 + \alpha_2, \alpha_1 - \alpha_2, \beta_1 - \beta_2, -\beta_1 + \beta_2\}$.

□

Let $p = 4t + 1$ be prime, $\mathcal{F}$ the generating Moore difference family for MD$(3p + 1)$, and $B \in \mathcal{F}$. Then $(\sigma, c) \in \mathbb{F}_p \times \{1, 2\}$ is a *mixed difference of* B (or the mixed difference *occurs in* B) if there exist $b_i, b_j \in B$ for which $(\sigma, c) = b_i - b_j$; specifically, (σ, c) is a *mixed difference (of* B*) between* b_i *and* b_j. There are two mixed differences that occur between b_i and b_j: one whose $\mathbb{F}_p$-coordinate, say σ, is in $[1, (p-1)/2]$ and the other whose $\mathbb{F}_p$-coordinate is $-\sigma \pmod p \in [(p + 1)/2, p - 1]$; the former is the *pairwise-minimum* mixed difference between b_i and b_j. As $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$, with $i \in [0, t - 1]$, a routine verification gives the following result:

Lemma 4.3. *Let $p = 4t + 1$ be prime, and $\mathcal{F}$ the generating Moore difference family for MD$(3p+1)$. Given $B \in \mathcal{F}$, if (σ, c_1) is a mixed difference that occurs between two elements of B, then (σ, c_2) is a mixed difference that occurs between the remaining two elements of B, where $\{c_1, c_2\} = \{1, 2\}$.*

A mixed difference of B is *split* if it occurs between one element whose $\mathbb{F}_p$-coordinate is in $[1, (p - 1)/2]$ and a second element whose $\mathbb{F}_p$-coordinate is in $[(p + 1)/2, p - 1]$. Conversely, a mixed difference of B is *joined* if it occurs between two elements, both of whose $\mathbb{F}_p$-coordinates are in $[1, (p - 1)/2]$, or between two elements, both of whose $\mathbb{F}_p$-coordinates are in $[(p + 1)/2, p - 1]$.

Lemma 4.4. *Let $p = 4t + 1$ be prime, and $\mathcal{F}$ the generating Moore difference family for MD$(3p + 1)$. If (σ, c) is a pairwise-minimum split mixed difference of some $B \in \mathcal{F}$, then there exists a (pairwise-minimum) joined mixed difference (σ', c) of B, with $\sigma' < \sigma$.*

Proof. Let $B = \{(x^i, 0), (-x^i, 0), (x^{i+t}, 1), (-x^{i+t}, 1)\}$, with $i \in [0, t - 1]$, and suppose without loss of generality that the two mixed differences between $(x^{i+t}, 1)$ and $(x^i, 0)$ are split, so that $x^i \in [1, (p - 1)/2]$ and $x^{i+t} \in [(p + 1)/2, p - 1]$. There are two major cases to cover, and henceforth, we assume that all arithmetic is performed modulo p.

Case 1. Suppose that $x^i < -x^{i+t}$. Then there are two subcases to cover:

1. $x^i - x^{i+t}$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum split mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$, or
2. $x^{i+t} - x^i$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum split mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$.

Suppose that the first subcase holds. Then $-x^{i+t} - x^i < x^i + -x^{i+t}$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^i - x^{i+t}$. Suppose that the second subcase holds. Then $-x^{i+t} - x^i < x^{i+t} - x^i$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^{i+t} - x^i$.

Case 2. Suppose that $-x^{i+t} < x^i$. Then there are two subcases to cover:

1. $x^i - x^{i+t}$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$, or
2. $x^{i+t} - x^i$ is the $\mathbb{F}_p$-coordinate of the pairwise-minimum mixed difference between $(x^{i+t}, 1)$ and $(x^i, 0)$.

Suppose that the first subcase holds. Then $x^i - (-x^{i+t}) < x^i - x^{i+t}$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(-x^{i+t}, 1)$ and $(x^i, 0)$ is less than $x^i - x^{i+t}$. Suppose that the second subcase holds. Then $x^{i+t} - (-x^i) < x^{i+t} - x^i$; that is, the $\mathbb{F}_p$-coordinate of the pairwise-minimum joined mixed difference between $(x^{i+t}, 1)$ and $(-x^i, 0)$ is less than $x^{i+t} - x^i$. □

Henceforth, we identify every point of a Moore difference family with its $\mathbb{F}_p$-coordinate.

Lemma 4.5. *Let $p = 4t+1$ be prime with $p \geq 13$, $\mathcal{F}$ the generating Moore difference family for MD$(3p+1)$, and $M = \{1, 2, 3, 4\}$ the four (pairwise-minimum) mixed differences of $\mathcal{F}$. Then every possible way in which distinct $m, m' \in M$ can occur as mixed differences in some $B \in \mathcal{F}$ is given, thus:*

1. *If mixed differences 1 and 2 occur in some $B \in \mathcal{F}$, then either $\{(p-3)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-3)/2, (p-1)/2, (p+3)/2\} \subset B$.*
2. *If mixed differences 1 and 3 occur in some $B \in \mathcal{F}$, then either $\{1, 2, p-1\} \subset B$ or $\{1, 2, p-2\} \subset B$.*
3. *If mixed differences 1 and 4 occur in some $B \in \mathcal{F}$, then either $\{(p-5)/2, (p-3)/2, (p+3)/2\} \subset B$ or $\{(p-5)/2, (p-3)/2, (p+5)/2\} \subset B$.*
4. *If mixed differences 2 and 3 occur in some $B \in \mathcal{F}$, then either $\{(p-5)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-5)/2, (p-1)/2, (p+5)/2\} \subset B$.*
5. *If mixed differences 2 and 4 occur in some $B \in \mathcal{F}$, then either $\{1, 3, p-3\} \subset B$ or $\{1, 3, p-1\} \subset B$.*
6. *If mixed differences 3 and 4 occur in some $B \in \mathcal{F}$, then either $\{(p-7)/2, (p-1)/2, (p+1)/2\} \subset B$ or $\{(p-7)/2, (p-1)/2, (p+7)/2\} \subset B$.*

Proof. By Lemma 4.3, p is sufficiently large that it cannot be the case that for distinct $m, m' \in M$, mixed difference m occurs between two elements of B, while m' occurs between the remaining two elements of B. Hence, at most two distinct mixed differences of M can occur in $B \in \mathcal{F}$, and these mixed differences occur between b and b_1 and b and b_2, where $b, b_1, b_2 \in B$ are distinct. It is routine to verify that this leaves only two possible valuations of the triple $\{b, b_1, b_2\}$ for each pair of mixed differences, as given in the statement of this lemma. □

We are now equipped to describe a procedure for obtaining a (c_0, c_1)-special base block.

Lemma 4.6. *Let $p = 4t + 1$ be prime with $p \geq 29$. Then MD$(3p+1)$ has a (c_0, c_1)-special base block.*

Proof. Let $\mathcal{F}$ be the generating Moore difference family for MD$(3p+1)$. There are sixteen potential cases to cover, depending on whether $1, 2, 3$, and 4 are the $\mathbb{F}_p$-coordinates of a (pairwise-minimum) joined or split mixed difference of $\mathcal{F}$. In fact, eight of these cases are without substance; by Lemma 4.4, 1 cannot be a split mixed difference. Here are the remaining eight:

1. 1 is joined, 2 is joined, 3 is joined, and 4 is joined.
2. 1 is joined, 2 is joined, 3 is joined, and 4 is split.

3. 1 is joined, 2 is joined, 3 is split, and 4 is joined.

4. 1 is joined, 2 is joined, 3 is split, and 4 is split.

5. 1 is joined, 2 is split, 3 is joined, and 4 is joined.

6. 1 is joined, 2 is split, 3 is joined, and 4 is split.

7. 1 is joined, 2 is split, 3 is split, and 4 is joined.

8. 1 is joined, 2 is split, 3 is split, and 4 is split.

Suppose that the first case holds. Then by Lemma 4.5, the blocks of $\mathcal{F}$ containing mixed differences $1, 2, 3,$ and 4 are distinct. For $i \in [1, 4]$, let B_i denote the block in $\mathcal{F}$ having mixed difference i, and suppose that $B_i \cap [1, (p-1)/2] = \{\alpha_i, \beta_i\}$. Now check if either $\{\alpha_1, \beta_1\}$ or $\{\alpha_2, \beta_2\}$ is contained in $[1, (p-1)/4]$; if so, then by Lemma 4.1, we are done. If not, then there are two subcases to consider:

1.1. $\{\alpha_1, \beta_1, \alpha_2, \beta_2\} \subset [(p-1)/4, (p-1)/2]$, or

1.2. there exists an $i \in \{1, 2\}$ such that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$, or vice-versa.

If subcase 1.1 holds, then by Lemma 4.2, we are done. If subcase 1.2 holds, then $\{\alpha_2, \beta_2\} = \{(p-5)/4, (p+3)/4\}$. If $\{\alpha_1, \beta_1\} \neq \{(p-3)/2, (p-1)/2\}$, then apply Lemma 4.2. Otherwise, if either $\{\alpha_3, \beta_3\}$ or $\{\alpha_4, \beta_4\}$ is contained in $[1, (p-1)/4]$, then by Lemma 4.1, we are done. If not, then there are two sub-subcases to consider:

1.2.1. $\{\alpha_3, \beta_3, \alpha_4, \beta_4\} \subset [(p-1)/4, (p-1)/2]$, or

1.2.2. there exists an $i \in \{3, 4\}$ such that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$, or vice-versa.

If subcase 1.2.1 holds, then apply Lemma 4.2. If subcase 1.2.2 holds, then $\{\alpha_4, \beta_4\} = \{(p-9)/4, (p+7)/4\}$ and $\{\alpha_3, \beta_3\} \subset [(p-1)/4, (p-5)/2]$. But setting $S = \{\alpha_3, \beta_3, \alpha_4, \beta_4\}$, then

$$\begin{aligned} \max\{S\} - \min\{S\} &\leq (p-5)/2 - (p-9)/4 \\ &= (p-1)/4, \end{aligned}$$

and thus an application of Lemma 4.2 finishes the job.

Suppose that the second case holds. Then by Lemma 4.4, there are three subcases to treat:

2.1. Mixed differences 1 and 4 occur in some $B \in \mathcal{F}$,

2.2. Mixed differences 2 and 4 occur in some $B \in \mathcal{F}$, or

2.3. Mixed differences 3 and 4 occur in some $B \in \mathcal{F}$.

If subcase 2.1 holds, then by Lemma 4.5, $\{(p-5)/2, (p-3)/2\} \subset B$. Let $\{\alpha_2, \beta_2\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 2 that is contained in $[1, (p-1)/2]$. If $\{\alpha_2, \beta_2\} \subset [1, (p-1)/4]$, then apply Lemma 4.1. If not, then there are two sub-subcases to consider:

2.1.1. $\{\alpha_2, \beta_2\} \subset [(p-1)/4, (p-1)/2]$

2.1.2. $\alpha_2 < (p-1)/4$ and $\beta_2 > (p-1)/4$, or vice-versa.

If sub-subcase 2.1.1 holds, then apply Lemma 4.2. If sub-subcase 2.1.2 holds, then $\{\alpha_2, \beta_2\} = \{(p-5)/4, (p+3)/4\}$, and $(p-3)/2 - (p-5)/4 = (p-1)/4$, so again apply Lemma 4.2. If subcase 2.2 holds, then by Lemma 4.5, $\{1, 3\} \subset B$; hence, B is (c_0, c_1)-special by Lemma 4.1. If subcase 2.3 holds, then by Lemma 4.5, $\{(p-7)/2, (p-1)/2\} \subset B$. Let $\{\alpha_1, \beta_1\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 1. If $\{\alpha_1, \beta_1\} \subset [1, (p-1)/4]$, then apply Lemma 4.1; otherwise, $\{\alpha_1, \beta_1\} \subset [(p-1)/4, (p-3)/2]$, so apply Lemma 4.2.

Suppose that the third case holds. Then by Lemma 4.4, there are two subcases to treat:

3.1. Mixed differences 1 and 3 occur in some $B \in \mathcal{F}$, or

3.2. Mixed differences 2 and 3 occur in some $B \in \mathcal{F}$.

If subcase 3.1 holds, then by Lemma 4.5, $\{1, 2\} \subset B$; hence B is (c_0, c_1)-special by Lemma 4.1. If subcase 3.2 holds, then by Lemma 4.5, $\{(p-5)/2, (p-1)/2\} \subset B$. Let $\{\alpha_1, \beta_1\}$ be the subset of the block of $\mathcal{F}$ containing (joined) mixed difference 1. If $\{\alpha_1, \beta_1\} \subset [1, (p-1)/4]$, then apply Lemma 4.1; otherwise, $\{\alpha_1, \beta_1\} \subset [(p-1)/4, (p-3)/2]$, so apply Lemma 4.2. Treat the fourth case in the same way that the third case was just treated.

Suppose that the fifth case holds. Then by Lemma 4.4 and 4.5, mixed differences 1 and 2 occur in some $B \in \mathcal{F}$ such that $\{(p-3)/2, (p-1)/2\} \subset B$. Let $\{\alpha_3, \beta_3\}$ and $\{\alpha_4, \beta_4\}$ be the subsets of the blocks of $\mathcal{F}$ containing (joined) mixed differences 3 and 4, respectively, contained in $[1, (p-1)/2]$. If for $i \in \{3, 4\}$, $\{\alpha_i, \beta_i\} \subset [1, (p-1)/4]$, then apply Lemma 4.1; if $\{\alpha_i, \beta_i\} \subset [(p-1)/4, (p-1)/2]$, then apply Lemma 4.2. Otherwise, we have without loss of generality that $\alpha_i < (p-1)/4$ and $\beta_i > (p-1)/4$; in this case, setting $S = \{\alpha_3, \beta_3, \alpha_4, \beta_4\}$, then $\max\{S\} - \min\{S\} \leq 5$ (hence our requirement that $p \geq 29$), so apply Lemma 4.2.

Suppose that the sixth case holds. Then by Lemmas 4.4 and 4.5 there exist two blocks $B, B' \in \mathcal{F}$ such that $\{(p-3)/2, (p-1)/2\} \subset B$ and $\{(p-7)/2, (p-1)/2\} \subset B'$. Hence, $B = B'$, so that $\{(p-7)/2, (p-3)/2, (p-1)/2\} \subset B$, but this is impossible, since every block of $\mathcal{F}$ has precisely two of its points contained in $[1, (p-1)/2]$.

Suppose that the seventh or eighth case holds. Then by Lemma 4.4, the mixed differences 1, 2, and 3 occur in the same block of $\mathcal{F}$, which is impossible by Lemma 4.3, since p is sufficiently large.

□

Let $\mathbb{F}_q = p^n$ be a finite field, with p prime. A fundamental result [17] in finite field theory is that if x is a primitive element of $\mathbb{F}_q$, then

$$\mathbb{F}_q = \bigcup_{\{a_0, \ldots, a_{n-1}\} \in \binom{\mathbb{F}_p}{n}} \left\{ \sum_{i=0}^{n-1} a_i x^i \right\},$$

with arithmetic performed over $\mathbb{F}_q$. A *polynomial-based indexing in x* of $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ is an indexing of the elements of $\mathbb{F}_q$ such that for each $i \in [0, p^{n-1} - 1]$ and any $f, g \in \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\}$, there exists a set $\{a_{i,1}, a_{i,2}, \ldots, a_{i,n-1}\} \subseteq \mathbb{F}_p$ such that

$$f = \alpha + \sum_{j=1}^{n-1} a_{i,j} x^i, \text{ and}$$

$$g = \beta + \sum_{j=1}^{n-1} a_{i,j} x^i,$$

with $\alpha, \beta \in \mathbb{F}_p$. In words, a polynomial-based indexing in x of $\mathbb{F}_q$ partitions the elements of $\mathbb{F}_q$ into p-sets, each consisting of those polynomials (treating x as an indeterminate) that have identical coefficients for each corresponding term of degree greater than zero. Now suppose in particular that $q = 4t + 1$, with t odd, and let $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ be a polynomial-based indexing in x of $\mathbb{F}_q$. For $i \in [0, p^{n-1} - 1]$, the *corresponding sub-Moore isomorphism of index i for MD*$(3q + 1)$ is the map

$$\varphi_i : \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\} \times \mathbb{Z}_3 \cup \{\infty\} \to \mathbb{F}_p \times \mathbb{Z}_3 \cup \{\infty\}$$

such that $\varphi_i(\infty) = \infty$ and $\varphi_i(f, c) = (\alpha, c)$ given $f = \alpha + \sum_{j=1}^{n-1} a_{i,j} x^i \in \mathbb{F}_q$. That is, φ_i "deletes" from f all terms of degree greater than zero.

Theorem 4.7 below allows us to get DiffSum 3 labellings of Moore designs having non-trivial prime power order.

Theorem 4.7. *Suppose that $q = p^n = 4t + 1$ with t odd and p prime, x a primitive element of $\mathbb{F}_q$, and let MD$(3q + 1) = (V = \mathbb{F}_q \times \mathbb{Z}_3, \mathcal{B})$ with ordered classical resolution $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{q-1}\}$. If $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ is a polynomial-based indexing in x of $\mathbb{F}_q$, then $\mathcal{B}$ contains p^{n-1} disjoint isomorphic copies of MD$(3p + 1)$, determined by the corresponding sub-Moore isomorphisms φ_i, $i \in [0, p^{n-1} - 1]$, for MD$(3q + 1)$, .*

Proof. Since $q = 4t + 1$ with t odd, $q \equiv 5 \pmod 8$. Thus, $p \equiv 5 \pmod 8$, say $p = 4s + 1$ with s odd, since $1, 3, 7 \in (\mathbb{Z}/8\mathbb{Z})^\times$ have orders 1, 2, and 2, respectively. Thus, if y is a primitive element of $\mathbb{F}_p$, then $y^s \in \mathbb{F}_p$ is a primitive fourth root of unity over $\mathbb{F}_q$, so that the group of fourth roots of unity over $\mathbb{F}_q$ is a subgroup of $\mathbb{F}_p^\times$.

Now for any integer α,

$$\begin{aligned} & \alpha \equiv 1 \pmod{\alpha - 1} \\ \iff & \alpha^n - 1 \equiv 1^n - 1 \pmod{\alpha - 1} \\ \iff & \alpha^n - 1 \equiv 0 \pmod{\alpha - 1}. \end{aligned}$$

Thus $p - 1 \mid p^n - 1$ and hence $s \mid t$. Now $z = x^{t/s}$ is a primitive element of $\mathbb{F}_p$, for suppose to the contrary that there exists some $i \in [1, 4s - 1]$ such that $z^i = 1$. Then $x^{it/s} = 1$ and $1 \le it/s < 4t$, contradicting that x is a primitive element of $\mathbb{F}_q$. Hence, z has order $4s$ in $\mathbb{F}_q^\times$, implying that $\langle z \rangle = \mathbb{F}_p^\times$.

That

$$\bigcup_{i \in [0, t-1]} \{x^i, -x^i, x^{i+t}, -x^{i+t}\} = \mathbb{F}_q^\times,$$

and the fact that x^t, a fourth root of unity over $\mathbb{F}_q$, must belong to $\mathbb{F}_p$, imply

$$\bigcup_{i \in [0, s-1]} \{x^{it/s}, -x^{it/s}, x^{it/s+t}, -x^{it/s+t}\} = \mathbb{F}_p^\times.$$

Hence, setting

$$\mathcal{P}_0' = \bigcup_{i \in [0, s-1], c \in \mathbb{Z}_3} \{\{(z^i, c), (-z^i, c), (z^{i+t}, c + 1), (-z^{i+t}, c + 1)\}\},$$

then $\mathcal{P}'_0 \subset \mathcal{P}_0$.

For each $i \in [0, p^{n-1} - 1]$, the set

$$\mathcal{B}'_i = \bigcup_{j \in [0,p-1]} (\mathcal{P}'_0 \oplus \sigma_{ip+j} \cup \{\infty, (\sigma_{ip+j}, 0), (\sigma_{ip+j}, 1), (\sigma_{ip+j}, 2)\}) \subset \mathcal{B}$$

is isomorphic to the blockset of MD$(3p + 1)$, the isomorphism being the sub-Moore isomorphism

$$\varphi_i : \{\sigma_{ip}, \ldots, \sigma_{ip+p-1}\} \times \mathbb{Z}_3 \cup \{\infty\} \to \mathbb{F}_p \times \mathbb{Z}_3 \cup \{\infty\}$$

of index i for MD$(3q + 1)$. □

We now have the tools to construct our DiffSum 3 labellings.

Lemma 4.8. *Suppose that $q = p^n = 4t + 1$ with t odd, p prime, and $n > 0$. If MD$(3p + 1)$ has a (c_0, c_1)-special base block, MD$(3q + 1) = (V = \mathbb{F}_q \times \mathbb{Z}_3 \cup \{\infty\}, \mathcal{B})$ admits a block labelling* rk *with DiffSum at most 3.*

Proof. Let x be a primitive element of $\mathbb{F}_q$, with $\mathbb{F}_q = \{\sigma_0 = 0, \ldots, \sigma_{q-1}\}$ a polynomial-based indexing in x of $\mathbb{F}_q$ such that φ_i is the corresponding sub-Moore isomorphism of index i, $i \in [0, p^{n-1} - 1]$, for MD$(3q + 1)$, and S a putative (c_0, c_1)-special base block of MD$(3p + 1)$. We refine our indexing of $\mathbb{F}_q$ by further requiring that:

1. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [0, p - 1]$, $\varphi_i(\sigma_{ip+j}, \cdot) = (j, \cdot)$, and
2. for all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [0, p - 1]$, $\varphi_i(\sigma_{ip+j}, \cdot) = (p - 1 - j, \cdot)$.

Finally, let $\mathcal{R} = \{\mathcal{P}_0, \ldots, \mathcal{P}_{3q}\}$ be the classical resolution of MD$(3q+1)$ such that $\mathcal{P}_i = \mathcal{P}_0 \oplus \sigma_i$ for all $i \in [0, q - 1]$.

Now suppose rk satisfies the ten conditions:

C1. $\mathcal{R}$-intervaled: For all $i \in [0, q - 1]$, $\mathsf{rk}^{-1}([i(3t + 1), 3t + i(3t + 1)]) = \mathcal{P}_i$.

C2. For all $i \in [0, (3t - 3)/2] \cup [(3t + 3)/2, 3t]$ and $j \in [0, q - 1]$,

$$\mathsf{rk}^{-1}(i + j(3t + 1)) = \mathsf{rk}^{-1}(i) \oplus \sigma_j.$$

C3. $\mathsf{rk}^{-1}(0)$ is a type 0 secant, $\mathsf{rk}^{-1}(1)$ is a type 2 secant, and $\mathsf{rk}^{-1}(2)$ is a type 1 secant.

C4. $\mathsf{rk}^{-1}(3t - 2)$ is a type 2 secant, $\mathsf{rk}^{-1}(3t - 1)$ is a type 1 secant, and $\mathsf{rk}^{-1}(3t)$ is a type 0 secant.

C5. For $j \in [1, (t - 3)/2]$ and $k \in \{0, 1, 2\}$, both $\mathsf{rk}^{-1}(3j + k)$ and $\mathsf{rk}^{-1}(3t - 3j - k)$ are type k secants.

C6. If $c_0 = 0$ and $c_1 = 1$, then $\mathsf{rk}^{-1}((3t - 3)/2)$ is a type 1 secant and $\mathsf{rk}^{-1}((3t + 3)/2)$ is a type 2 secant. Conversely, if $c_0 = 1$ and $c_1 = 0$, then $\mathsf{rk}^{-1}((3t - 3)/2)$ is a type 2 secant and $\mathsf{rk}^{-1}((3t + 3)/2)$ is a type 1 secant.

C7. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [0, (p - 1)/2]$,

$$\mathsf{rk}^{-1}((ip + j)(3t + 1) + (3t - 1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip + j)(3t + 1) + (3t + 1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C8. For all $i \in \{0, 2, 4, \ldots, p^{n-1} - 1\}$ and $j \in [(p+1)/2, p-1]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C9. For all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [0, (p-1)/2]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

C10. For all $i \in \{1, 3, 5, \ldots, p^{n-1} - 2\}$ and $j \in [(p+1)/2, p-1]$,

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t-1)/2)$$

is the ∞-block of $\mathcal{P}_{ip+j}$ and

$$\mathsf{rk}^{-1}((ip+j)(3t+1) + (3t+1)/2) = \varphi_i^{-1}(S) \oplus \sigma_{ip+j}.$$

Let $\rho \in V$. As $\mathcal{P}_i$ is a parallel class for each $i \in [0, q-1]$, there is a unique value $\ell_i \in [0, 3t]$ such that $\rho \in \mathsf{rk}^{-1}(i(3t+1)+\ell_i)$. The point sum of ρ with respect to rk may thus be written

$$\sum_{i=0}^{q-1}(i(3t+1) + \ell_i) = (3t+1)(4t+1)(2t) + \sum_{i=0}^{q-1} \ell_i,$$

so that the second summation is the resolution-relative point sum of ρ. Now consider any $(y, c) \in V - \{\infty\}$. By C5, the multiset of summands of the resolution-relative point sum of (y, c) $L = \{\ell_i : i \in [0, q-1]\}$ for (y, c) contains the multiset $M = \{3i+c, 3i+c, 3(t-i)-c, 3(t-i)-c, 3i+((c+2) \bmod 3), 3i+((c+2) \bmod 3), 3(t-i)-((c+2) \bmod 3), 3(t-i)-((c+2) \bmod 3) : i \in [1, (t-3)/2]\}$. We compute $L-M$ (multiset difference) on a case-by-case basis, depending on the value of c, as follows. For all cases, we suppose without loss of generality that $c_0 = 0$ and $c_1 = 1$.

Suppose that $c = 0$. Then L is given by the (multiset) union of M together with $M_{0,0}, M_{0,1}$, and $M_{0,2}$ defined thus:

1. $M_{0,0} = \{0, 0, 1, 1, 3t-2, 3t-2, 3t, 3t\}$ (C3 and C4)
2. $M_{0,1} = \{(3t+3)/2, (3t+3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 2 secant.)
3. $M_{0,2} = \{(3t-1)/2, (3t-1)/2, (3t-1)/2\}$ or $M_{0,2} = \{(3t-1)/2, (3t-1)/2, (3t+1)/2\}$ or $M_{0,2} = \{(3t-1)/2, (3t+1)/2, (3t+1)/2\}$.

Accounting for the variants of $M_{0,2}$ requires an explanation. Put

$$U = \bigcup_{i \in [0, p^{n-1}-1], j \in [0, p-1]} \left(\varphi_i^{-1}(S) \oplus \sigma_{ip+j}\right). \tag{2}$$

Then any point $(z, c') \in \mathbb{F}_q \times \{0, 2\}$ occurs in exactly two distinct blocks of U; say that $(y, 0)$ in particular occurs in blocks B_1 and B_2 of U. In fact, there exists some unique $i \in [0, p^{n-1} - 1]$ such that $B_1, B_2 \in \bigcup_{j=0}^{p-1} \mathcal{P}_{ip+j}$. Moreover, the unique ∞-block, say B_∞, that contains $(y, 0)$ occurs in $\mathcal{P}_{ip+k}$ for some unique $k \in [0, p-1]$ satisfying $\varphi_i(y, 0) = (k, 0)$. By C7 up to C10, together with the fact that S is a (c_0, c_1)-special base block of MD$(3p+1)$, there are exactly four ways that rk could assign labels to B_1, B_2, and B_∞, where $k_1, k_2, k_3 \in [ip, ip + p - 1]$:

1. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t + 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t + 1)/2$, and $\mathsf{rk}(B_\infty) = k_3(3t + 1) + (3t - 1)/2$;
2. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t - 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t + 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$;
3. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t + 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t - 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$; or
4. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t - 1)/2$ and $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t - 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$;

hence the three variations of $M_{0,2}$.

Suppose that $c = 1$. Then L is given by the (multiset) union of M together with $M_{1,0}, M_{1,1}$, and $M_{1,2}$, defined thus:

1. $M_{1,0} = \{0, 0, 2, 2, 3t - 1, 3t - 1, 3t, 3t\}$ (C3 and C4).
2. $M_{1,1} = \{(3t - 3)/2, (3t - 3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t - 3)/2)$ is a type 1 secant).
3. $M_{1,2} = \{(3t-1)/2, (3t-1)/2, (3t+1)/2\}$ or $M_{1,2} = \{(3t-1)/2, (3t+1)/2, (3t+1)/2\}$, or $M_{1,2} = \{(3t + 1)/2, (3t + 1)/2, (3t + 1)/2\}$.

Similar to $M_{0,2}$, $M_{1,2}$ is formed as follows. We know that that $(y, 1)$ occurs in two distinct blocks, say, B_1 and B_2 of U (see (2)). Indeed, there exists a unique $i \in [0, p^{n-1} - 1]$ for which $B_1, B_2 \in \bigcup_{j=0}^{p-1} \mathcal{P}_{ip+j}$. Moreover, the unique ∞-block, say B_∞, that contains $(y, 1)$ occurs in $\mathcal{P}_{ip+k}$ for some unique $k \in [0, p-1]$ satisfying $\varphi_i(y, 1) = (k, 1)$. By C7 up to C10, together with the fact that S is a (c_0, c_1)-special base block of MD$(3p+1)$, there are exactly four ways that rk could assign labels to B_1, B_2, and B_∞, where $k_1, k_2, k_3 \in [ip, ip + p - 1]$:

1. $\mathsf{rk}(B_1) = k_1(3t+1)+(3t-1)/2$, $\mathsf{rk}(B_2) = k_2(3t+1)+(3t-1)/2$, and $\mathsf{rk}(B_\infty) = (3t+1)/2$;
2. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t - 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t + 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$;
3. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t + 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t - 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$; or
4. $\mathsf{rk}(B_1) = k_1(3t + 1) + (3t + 1)/2$, $\mathsf{rk}(B_2) = k_2(3t + 1) + (3t + 1)/2$, and $\mathsf{rk}(B_\infty) \in \{k_3(3t + 1) + (3t + 1)/2, k'_3(3t + 1) + (3t - 1)/2\}$;

hence the three variations of $M_{1,2}$.

Finally, suppose that $c = 2$. Then L is given by the (multiset) union of M together with $M_{2,0}, M_{2,1}$, $M_{2,2}$, and $M_{2,3}$, defined thus:

1. $M_{2,0} = \{1, 1, 2, 2, 3t - 2, 3t - 2, 3t - 1, 3t - 1\}$ (C3 and C4).

2. $M_{2,1} = \{(3t-3)/2, (3t-3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t-3)/2)$ is a type 1 secant).

3. $M_{2,2} = \{(3t+3)/2, (3t+3)/2\}$ (by C6, $\mathsf{rk}^{-1}((3t+3)/2)$ is a type 2 secant).

4. $M_{2,3} = \{(3t-1)/2\}$ or $M_{2,3} = \{(3t+1)/2\}$ (this accounts for the ∞-block that contains $(y, 2)$ – see C7 up to C10).

We now compute the sum of the elements of each variant of L. If $c = 0$, then the sum of the elements of the multiset union $M_{0,0} \cup M_{0,1} \cup M_{0,2}$ falls in the interval $[18t+(3t-1)/2, 18t+(3t-1)/2+2]$, and thus the sum of the elements of L for any $(y, 0) \in V$ falls in the interval $[6t^2+(3t-1)/2, 6t^2+(3t-1)/2+2]$. If $c = 1$, then the sum of the elements of $M_{1,0} \cup M_{1,1} \cup M_{1,2}$ falls in the interval $[18t+(3t-1)/2-1, 18t+(3t-1)/2+1]$, and thus the sum of the elements of L for any $(y, 1) \in V$ falls in the interval $[6t^2 + (3t-1)/2 - 1, 6t^2 + (3t-1)/2 + 1]$. If $c = 2$, then the sum of the elements of $M_{2,0} \cup M_{2,1} \cup M_{2,2} \cup M_{2,3}$ falls in the interval $[18t + (3t-1)/2, 18t + (3t-1)/2 + 1]$, and thus the sum of the elements of L for any $(y, 2) \in V$ falls in the interval $[6t^2 + (3t-1)/2, 6t^2 + (3t-1)/2 + 1]$. At last, by C7 up to C10, the sum of the elements of L for $\infty \in V$ is

$$\begin{aligned}\frac{q-1}{2} \cdot \frac{3t+1}{2} + \frac{q+1}{2} \cdot \frac{3t-1}{2} &= \frac{3qt + q - 3t - 1 + 3qt - q + 3t - 1}{4} \\ &= \frac{3qt - 1}{2} \\ &= \frac{12t^2 + 3t - 1}{2} \\ &= 6t^2 + \frac{3t-1}{2}.\end{aligned}$$

Hence rk has $\mathsf{DiffSum}$ at most 3. □

Theorem 4.9. *Suppose that $q = p^n = 4t+1$ with t odd and $p \geq 13$ prime. Then MD$(3q+1)$ admits a labelling with $\mathsf{DiffSum}$ at most 3.*

Proof. Applying Lemmas 4.6 and 4.8, we obtain the desired labellings for each MD$(3q+1)$ with t odd and $p \geq 29$. Here are the three base blocks of the generating Moore difference family for MD(40), using 6 as the primitive element of $\mathbb{F}_{13}$:

$$\{(1,0),(12,0),(8,1),(5,1)\}, \{(6,0),(7,0),(9,1),(4,1)\}, \text{ and}$$
$$\{(10,0),(3,0),(2,1),(11,1)\}.$$

By Lemma 4.1, the third base block is (c_0, c_1)-special, and thus by Lemma 4.8, MD(40) admits the desired labelling. □

5 Concluding Remarks

The single base block of MD(16) is not (c_0, c_1)-special, and we have verified by computer that if $\mathcal{R}$ is the classical resolution of MD(16), then the least $\mathsf{DiffSum}$ of any $\mathcal{R}$-intervaled labelling of MD(16) is 6. In general, for $|\mathcal{F}|$ and $|N|$ odd, we do not believe that $k-1$ is the best possible $\mathsf{DiffSum}$. Indeed, we have devised $\mathsf{DiffSum}$ 1 labellings, which we do not present here, for an infinite class of $S(2, 4, v)$s. Moreover, with slight modification, many of the ideas presented in this paper can be applied to label resolvable $(k-1)$-rotational $S(2, k, v)$s. For related work, see [7].

References

[1] M. Buratti. Some constructions for 1-rotational BIBD's with block size 5. *Australasian Journal of Combinatorics*, 17:199–228, 1998.

[2] M. Buratti and N. Finizio. Existence results for 1-rotational resolvable Steiner 2-designs with block size 6 or 8. *Bull Inst. Combin. Appl*, 50:29–44, 2007.

[3] M. Buratti, J. Yan, and C. Wang. From a 1-rotational RBIBD to a partitioned difference family. *The Electronic Journal of Combinatorics*, pages R139–R139, 2010.

[4] M. Buratti and F. Zuanni. G-invariantly resolvable Steiner 2-designs which are 1-rotational over G. *Bulletin of the Belgian Mathematical Society-Simon Stevin*, 5(2/3):221–235, 1998.

[5] M. Buratti and F. Zuanni. The 1-rotational Kirkman triple systems of order 33. *Journal of Statistical Planning and Inference*, 86(2):369–377, 2000.

[6] M. Buratti and F. Zuanni. Explicit constructions for 1-rotational Kirkman triple systems. *Utilitas Mathematica*, 59:27–30, 2001.

[7] M. Buratti and F. Zuanni. Perfect Cayley designs as generalizations of perfect Mendelsohn designs. *Designs, Codes and Cryptography*, 23(2):233–248, 2001.

[8] Y. M. Chee, C. J. Colbourn, H. Dau, R. Gabrys, A. C. Ling, D. Lusi, and O. Milenkovic. Access balancing in storage systems by labeling partial Steiner systems. *Designs, Codes and Cryptography*, 88(11):2361–2376, 2020.

[9] C. J. Colbourn. Egalitarian Steiner triple systems for data popularity. *Designs, Codes and Cryptography*, pages 1–23, 2021.

[10] S. Costa, T. Feng, and X. Wang. Frame difference families and resolvable balanced incomplete block designs. *Designs, Codes and Cryptography*, 86(12):2725–2745, 2018.

[11] H. Dau and O. Milenkovic. Maxminsum Steiner systems for access balancing in distributed storage. *SIAM Journal on Discrete Mathematics*, 32(3):1644–1671, 2018.

[12] S. El Rouayheb and K. Ramchandran. Fractional repetition codes for repair in distributed storage systems. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1510–1517. IEEE, 2010.

[13] A. Fazeli, A. Vardy, and E. Yaakobi. Codes for distributed pir with low storage overhead. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2852–2856. IEEE, 2015.

[14] M. Hall. *Combinatorial theory*, volume 71. John Wiley & Sons, 1998.

[15] M. Jimbo and S. A. Vanstone. Recursive constructions for resolvable and doubly resolvable 1-rotational Steiner 2-designs. *Utilitas Mathematica*, 26:45–61, 1984.

[16] P. A. Leonard. Realizations for direct constructions of resolvable Steiner 2-designs with block size 5. *Journal of Combinatorial Designs*, 8(3):207–217, 2000.

[17] R. Lidl and H. Niederreiter. *Finite fields*. Number 20. Cambridge university press, 1997.

[18] E. H. Moore. Tactical memoranda I-III. *American Journal of Mathematics*, 18(3):264–290, 1896.

[19] D. K. Ray-Chaudhuri and R. M. Wilson. Solution of Kirkman's schoolgirl problem. In *Proc. symp. pure Math*, volume 19, pages 187–203, 1971.

[20] N. Silberstein and T. Etzion. Optimal fractional repetition codes based on graphs and designs. *IEEE Transactions on Information Theory*, 61(8):4164–4180, 2015.

[21] N. Silberstein and A. Gál. Optimal combinatorial batch codes based on block designs. *Designs, Codes and Cryptography*, 78(2):409–424, 2016.