Partial Difference Sets in Abelian Groups

Zeying Wang
Department of Mathematical Sciences
Michigan Technological University

Finite Geometries–Fifth Irsee Conference

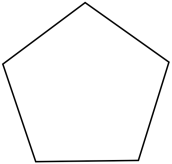
Definitions and background

A (finite) graph $\Gamma = (V, E)$ is called *strongly regular* with parameters srg(v, k, λ, μ) if

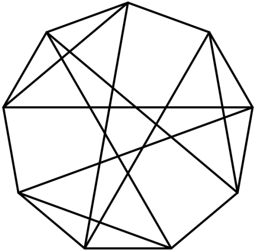
- it has v vertices;
- degree k;
- every two adjacent vertices have λ common neighbors;
- every two non-adjacent vertices have μ common neighbors.

Strongly regular graphs

Two examples.



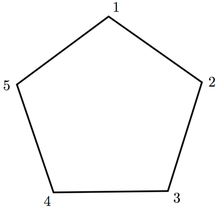
$\mathrm{srg}(5, 2, 0, 1)$



$\mathrm{srg}(9, 4, 1, 2)$

Let Γ be a srg(v, k, λ, μ). Given a fixed labeling of the vertices $1, \ldots, v$, the *adjacency matrix* A is the matrix with 1 in position (i, j) if vertex i is adjacent to vertex j, and 0 everywhere else.

For example, the adjacency matrix of the pentagon is



$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

A strongly regular graph with parameters srg($v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}$) is called a *conference graph*.

If Γ is an srg(v, k, λ, μ) then the adjacency matrix A has eigenvalues

$$\nu_1 := k,$$

$$\nu_2 := \frac{1}{2}(\lambda - \mu + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}),$$

$$\nu_3 := \frac{1}{2}(\lambda - \mu - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}).$$

Unless Γ is a conference graph on v vertices with v not a perfect square these eigenvalues are integers.

The multiplicities of these eigenvalues are

$$m_1 := 1,$$

$$m_2 := \frac{1}{2}\left(v - 1 - \frac{2k + (v-1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}\right)$$

and

$$m_3 = \frac{1}{2}\left(v - 1 + \frac{2k + (v-1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}\right).$$

Partial difference sets (PDS)

Let G be a finite group of order v with identity e and $\mathcal{D}$ be a subset of G with k elements. Then $\mathcal{D}$ is called a (v, k, λ, μ) *partial difference set* (PDS) if the expressions gh^{-1}, for g and h in $\mathcal{D}$ with $g \neq h$, represent

- each nonidentity element in $\mathcal{D}$ exactly λ times,
- each nonidentity element of G not in $\mathcal{D}$ exactly μ times.

If $\mathcal{D}^{(-1)} = \mathcal{D}$ and $e \notin \mathcal{D}$ then $\mathcal{D}$ is called *regular*. A regular PDS is called *trivial* if $\mathcal{D} \cup \{e\}$ or $G \setminus \mathcal{D}$ is a subgroup of G.

PDS were introduced by Bose and Cameron, named by Chakravarti. A systematic study started with S.L. Ma. PDS are a generalization of difference sets (which are PDS with $\lambda = \mu$).

Let $\mathcal{D}$ be a regular (v, k, λ, μ)-PDS. Define the Cayley graph $\Gamma(G, \mathcal{D})$ as follows:

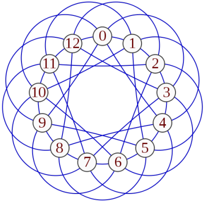
- the vertices of Γ are the elements of G;
- two vertices g and h are adjacent if and only if $gh^{-1} \in \mathcal{D}$.

Then the graph $\Gamma(G, \mathcal{D})$ is a strongly regular graph $\mathrm{srg}(v, k, \lambda, \mu)$ which admits G as sharply transitive group of automorphisms.

Examples of PDS

- Let q be an odd prime power, with $q \equiv 1 \pmod 4$. Then the non-zero squares of $\mathbb{F}_q$ form a partial difference set with parameters $v = q$, $k = (q-1)/2$, $\lambda = (q-5)/4$, $\mu = (q-1)/4$ in the additive group of $\mathbb{F}_q$. PDS with these parameters are said to be of Paley type. Note the corresponding graph will be a conference graph.

For example $\{1, 3, 4, 9, 10, 12\} \subset (\mathbb{F}_{13}, +)$ is a (13, 6, 2, 3) PDS.



A Benson type theorem for SRGs

Theorem (De Winter - Kamischke - Wang '15)

Let Γ be a strongly regular graph with integer eigenvalues. Let ϕ be an automorphism of order n of Γ, and let $\mu()$ be the Möbius function. Then for all positive divisors d of n, there are non-negative integers a_d such that

$$k - \nu_3 + \sum_{d|n} a_d \mu(d)(\nu_2 - \nu_3) = -\nu_3 f + g, \quad (1)$$

where f is the number of fixed vertices of ϕ and g is the number of vertices that are adjacent to their image under ϕ.

Variants of this theorem appeared before for a variety of geometries.

Theorem

Let $\mathcal{G}$ be a strongly regular graph srg(v, k, λ, μ) with integer eigenvalues, and let ϕ be an automorphism of order n of $\mathcal{G}$. Let s be an integer coprime with n. Then ϕ and ϕ^s map the same number of vertices to adjacent vertices.

Theorem (LMT)

Let $\mathcal{D}$ be a regular PDS in the Abelian group G. Assume Δ is a perfect square. Let $g \in G$ be an element of order r. Assume $\gcd(s, r) = 1$. *Then $g \in \mathcal{D}$ if and only if $g^s \in \mathcal{D}$.*

Proof. An element $g \in \mathcal{D}$ if and only if the corresponding automorphism g: $h \mapsto gh$ maps all vertices of $\Gamma(G, \mathcal{D})$ to adjacent vertices.

Classical multiplier theorem

The following well known result is an immediate consequence of our LMT.

Corollary

Let $\mathcal{D}$ be a regular PDS in the Abelian group G of order v. Assume Δ is a perfect square. Then $\mathcal{D}^{(s)} = \mathcal{D}$ for all s with $\gcd(s, v) = 1$.

Existence question

For strongly regular graphs many necessary conditions for existence are known, however, finding sufficient conditions seems to be hopeless, and for many hypothetical parameter sets the existence question has not been settled.

Clearly PDS have to satisfy all existence conditions for strongly regular graphs. Also several further conditions are known. However, here as well, no sufficient conditions are known, and for many hypothetical parameter sets the existence question has not been settled.

Application 1: non-existence of PDS with small parameters

In 1994 S.L. Ma produced a list of all parameter sets (v, k, λ, μ) with $k \leq 100$ that survived the known necessary conditions for regular PDS in Abelian groups. For all but 32 of these 187 parameter sets the existence of a PDS was known.

In 1997 Ma proved some further necessary conditions for the existence of PDS, and this excluded the existence of PDS in 13 more cases.

In 1998 Fiedler and Klin discovered a new $(512, 73, 12, 10)$-PDS.

This left 18 unresolved cases, and no progress had been made since then.

Ma's table

v	k	λ	μ	existence
100	33	8	12	
100	36	14	12	
144	39	6	12	
144	52	16	20	
144	55	22	20	
196	60	14	20	
196	65	24	20	
196	75	26	30	
196	78	32	30	
216	40	4	8	
216	43	10	8	
225	48	3	12	
225	80	25	30	
225	84	33	30	
225	96	39	42	
225	98	43	42	
392	51	10	6	
400	84	8	20	

Restrictions on the group

Proposition: [Ma 94] No non-trivial PDS exists in

- an Abelian group G with a cyclic Sylow-p-subgroup and $o(G) \neq p$;
- an Abelian group G with a Sylow-p-subgroup isomorphic to $\mathbb{Z}_{p^s} \times \mathbb{Z}_{p^t}$ where $s \neq t$.

Theorem 2(De Winter - Kamischke - Wang ’15)

Relying on the LMT and some further more technical counting arguments we obtained

v	k	λ	μ	existence
100	33	8	12	DNE
100	36	14	12	DNE
144	39	6	12	DNE
144	52	16	20	DNE
144	55	22	20	DNE
196	60	14	20	DNE
196	65	24	20	DNE
196	75	26	30	DNE
196	78	32	30	DNE
216	40	4	8	
216	43	10	8	
225	48	3	12	DNE
225	80	25	30	DNE
225	84	33	30	DNE
225	96	39	42	DNE
225	98	43	42	DNE
392	51	10	6	DNE
400	84	8	20	DNE

Application 2: PDS in Abelian groups of order $4p^2$

Noting that six of the examples from the previous list occur in groups of order $4p^2$, and motivated by a question of J. Davis we started to focus on PDS in Abelian groups of order $4p^2$, p an odd prime.

Key problem: The previous approach strongly depends on knowing the parameters of the hypothetical PDS, and the number of hypothetical parameters for which existence is not known in groups of order $4p^2$ grows rapidly with p.

The known examples

An (n, r)-*PCP* $\mathcal{P}$ in a group G of order n^2 is a set $\mathcal{P}$ of r subgroups of order n of G such that $U \cap V = \{e\}$ for any $U, V \in \mathcal{P}$. Given an (n, r)-PCP $\mathcal{P}$ in G, $\mathcal{D} := \bigcup_{U \in \mathcal{P}} U \setminus \{e\}$ is a regular PDS in G.

For example

$$(< (1, 0) > \cup < (0, 1) > \cup < (1, 1) >) \setminus \{(0, 0)\}$$

is a $(n, 3)$-PCP in $\mathbb{Z}_n \times \mathbb{Z}_n$.

PDS in Abelian groups of order $4p^2$

Note that 6 of the 16 cases we excluded occur in groups of order $4p^2$.
What is known on non-trivial PDS in these groups?

- The group must be isomorphic to $\mathbb{Z}_2^2 \times \mathbb{Z}_p^2$;
- a $(36, 14, 4, 6)$-PDS in $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$.
- the only other known examples are of PCP-type (up to complement);
- the number of parameters for which (non)existence has not been determined increases rapidly with p.

The key problem

Key problem: For general p it is not possible to explicitly list all possible parameters that would survive the known parameter restrictions. As a consequence the so far applied method fails in general because the counting argument, which strongly depends on knowing k, λ and μ, fails.

A new approach is needed.

The characteristic matrix

Let $G = \mathbb{Z}_2^2 \times \mathbb{Z}_p^2$, and let $\mathcal{D}$ be a regular PDS in G. Denote the identity of G by g_1, and the three elements of order 2 by g_2, g_3, and g_4. Furthermore, let H_1, H_2, $\cdots$, H_{p+1} denote the $p+1$ subgroups of order p in G, and set $S_{ij} = g_i H_j \setminus \{g_i\}$, for $i = 1$, 2, 3, 4 and $j = 1, 2, \cdots, p+1$.

Lemma

If $h \in \mathcal{D}$ and $h \in S_{ij}$, then $S_{ij} \subset \mathcal{D}$.

Definition: The characteristic matrix χ of $\mathcal{D}$ is the $4 \times (p+1)$ matrix whose entry in position (i, j) is a 1 iff $S_{ij} \subset \mathcal{D}$ and a 0 otherwise.

Without loss of generality we may assume that $\mathcal{D}$ contains either no elements of order two, or contains exactly one, say g_2.
Case 1: Assume that $\mathcal{D}$ contains no elements of order two.

Lemma

If the first column of χ is $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ *then the elements of S_{i1} can be written as a difference of elements of $\mathcal{D}$ in the following number of ways:*

- $2p + r_1 + r_2^2 + r_3^2 + r_4^2 - 3r_1 - 3r_2 - r_3 - r_4$ *when* $i = 1$;
- $2(p + r_1 r_2 + r_3 r_4 - r_1 - r_2 - R_1 \cdot R_2 - R_3 \cdot R_4)$ *when* $i = 2$;
- $2(r_1 r_3 + r_2 r_4 - r_3 - r_4 - R_1 \cdot R_3 - R_2 \cdot R_4)$ *when* $i = 3$;
- $2(r_1 r_4 + r_2 r_3 - r_3 - r_4 - R_1 \cdot R_4 - R_2 \cdot R_3)$ *when* $i = 4$.

Theorem (De Winter - Wang '16)

When $\mathbb{Z}_2^2 \cap \mathcal{D} = \emptyset$ the only possible (up to equivalence) characteristic matrices are

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$\mathbb{Z}_p$

$$\begin{pmatrix} 1 & \dots & 1 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \end{pmatrix}$$

$\mathbb{Z}_p \times \mathbb{Z}_p$

$$\begin{pmatrix} 1 & \dots & 1 \\ 1 & \dots & 1 \\ 1 & \dots & 1 \\ 1 & \dots & 1 \end{pmatrix}$$

complement of $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$\begin{pmatrix} 0 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \end{pmatrix}$$

complement of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_p$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & \dots & 1 \\ 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \end{pmatrix}$$

complement of $(2p, 3)$*-PCP*

Theorem (continued)

When $\mathbb{Z}_2^2 \cap \mathcal{D} = g_2$ the only possible (up to equivalence) characteristic matrices are

$$\underset{\mathbb{Z}_2}{\begin{pmatrix} 0 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \end{pmatrix}} \quad \underset{\mathbb{Z}_2 \times \mathbb{Z}_p}{\begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \end{pmatrix}} \quad \underset{\mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p}{\begin{pmatrix} 1 & \dots & 1 \\ 1 & \dots & 1 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \end{pmatrix}}$$

$$\begin{pmatrix} 0 & 0 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

complement of $(2p, 2)$*-PCP* *complement of* $(36, 14, 4, 6)$*-PDS*

Theorem 3 (SDW - Wang '16)

Every PDS (up to complement) in an Abelian group of order $4p^2$, with p is an odd prime, is one of the following: a subgroup, a PCP example, or the $(36, 14, 4, 6)$-PDS in $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$.

At this point there were still 2 open cases in Ma's table. Jointly with a student we succeeded in proving

Theorem (De Winter–Neubert– Wang'16)

No regular (216, 40, 4, 8)-PDS or (216, 43, 10, 8)-PDS exist in any Abelian groups of order 216.

The proof is based on weighing points and lines in a projective plane.
Since (216, 40, 4, 8) and (216, 43, 10, 8) are the only two parameter sets that survive the basic integrality and divisibility conditions of non-trivial partial difference sets, there are no non-trivial regular partial difference sets in Abelian groups of order 216.

v	k	λ	μ	existence
100	33	8	12	DNE
100	36	14	12	DNE
144	39	6	12	DNE
144	52	16	20	DNE
144	55	22	20	DNE
196	60	14	20	DNE
196	65	24	20	DNE
196	75	26	30	DNE
196	78	32	30	DNE
216	40	4	8	DNE (2016)
216	43	10	8	DNE (2016)
225	48	3	12	DNE
225	80	25	30	DNE
225	84	33	30	DNE
225	96	39	42	DNE
225	98	43	42	DNE
392	51	10	6	DNE
400	84	8	20	DNE

Application 3: PDS in Abelian groups of order $8p^3$

To our surprise, by computer search, for each small prime number p, in Abelian groups of order $8p^3$, only 2 or 4 parameter sets survive the basic integrality and divisibility conditions of non-trivial partial difference sets. This situation is very different from what happened in the case of groups of order $4p^2$. This motivated us to study PDS in Abelian groups of order $8p^3$. We recently obtained the following result:

Theorem 4 (De Winter–Wang '17)

Theorem

No non-trivial regular partial difference sets exist in Abelian groups of order $8p^3$, where p is a prime number ≥ 3.

Sketch of proof

Assume that D is a non-trivial PDS in an Abelian group G of order $8p^3$. Let $\beta = \lambda - \mu$, and $\Delta = \beta^2 + 4(k - \mu)$. Without loss of generality we may assume that $k \leq v/2$ (complement), $\Delta \leq v$ (duality) and $\mu > 0$ (nontriviality).

By some of Ma's results, we know that

- $G = \mathbb{Z}_2^3 \times \mathbb{Z}_p^3$.
- $\Delta = 4p^2$ or $\Delta = 16p^2$. (When G is Abelian, if D is nontrivial, then v, Δ, and v^2/Δ have the same prime divisors.)

Restrictions on k:

Lemma

If a non-trivial regular (v, k, λ, μ)-PDS exists in an Abelian group with $v = 8p^3$, $\Delta = 4p^2$ and $k \leq \frac{v}{2}$, then $k \leq p^2 + \frac{p}{4} - \frac{1}{2}$.

Lemma

If a non-trivial regular (v, k, λ, μ)-PDS exists in an Abelian group with $v = 8p^3$, $\Delta = 16p^2$ and $k \leq \frac{v}{2}$, then $k \leq 4p^2 + 3p - \frac{1}{2}$.

Restrictions on μ:
By a Ma's result, we know that $(2k - \beta)^2 \equiv 0 \pmod{\Delta}$. We can use this to show that

$$\mu = \frac{x^2 - 1}{8p} \tag{2}$$

when $\Delta = 4p^2$, and

$$\mu = \frac{x^2 - 1}{2p} \tag{3}$$

when $\Delta = 16p^2$ (for some integer x).

Combining the obtained restrictions on k and μ, and using that $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$ one can then obtain:

If $\Delta = 4p^2$ there cannot exist an nontrivial regular PDS in G

If $\Delta = 16p^2$ and D is a nontrivial regular PDS in G, than necessarily $x = 2p + 1$ or $x = 2p - 1$ and the parameters of D satisfy one of the following:

- $(8p^3, 4p^2 + 2p - 2, 2p - 2, 2p + 2)$–PDS;
- $(8p^3, 4p^2 + 2p + 1, 2p + 4, 2p + 2)$–PDS;
- $p = 4y^2 + 3y + 1$ and $\lambda - \mu = -8y - 4$ or $8y + 2$;
- $p = 4y^2 + 5y + 2$ and $\lambda - \mu = -8y - 6$ or $8y + 4$.

The case of a ($8p^3$, $4p^2+2p-2$, $2p-2$, $2p+2$)–PDS

By a Ma's result we can show that D contains either 0 or 4 elements of order 2.
Let $g_1, g_2, \cdots, g_{p^3-1}$ be all elements of order p in G, and let $\mathcal{B}_{g_i} = \{ag_i \mid o(a) = 1 \text{ or } 2,\ ag_i \in D\}$, and $B_i = |\mathcal{B}_{g_i}|$, $i = 1, 2, \cdots, p^3-1$. Then the LMT implies that

$$|\mathcal{B}_{g_i}| = |\mathcal{B}_{g_i^s}|, \text{ where } 1 \le s \le p-1.$$

By relabeling the g_i if necessary we have $C_j := B_{(j-1)(p-1)+1} = B_{(j-1)(p-1)+2} = \cdots = B_{(j-1)(p-1)+(p-1)}$ for $j = 1, 2, \cdots, p^2+p+1$, and $C_1 \ge C_2 \ge \cdots \ge C_{p^2+p+1}$.

First we assume that D contains 4 elements of order 2. We see that $\Sigma_i B_i = 4p^2 + 2p - 6$ and $\Sigma_i B_i(B_i - 1) = 14p - 14$.
It follows that

$$\Sigma_{i=1}^{p^2+p+1} C_i = 4p + 6 \quad \text{and} \quad \Sigma_{i=1}^{p^2+p+1} C_i^2 = 4p + 20 \qquad (4)$$

It is not hard to show the only nonnegative integer solutions, listed as decreasing $p^2 + p + 1$ tuples, are:

$$(4, 2, \underbrace{1, 1, \cdots, 1}_{4p}, 0, 0, \cdots, 0)$$

$$(3, 3, 2, \underbrace{1, 1, \cdots, 1}_{4p-2}, 0, 0, \cdots, 0)$$

$$(3, 2, 2, 2, 2, \underbrace{1, 1, \cdots, 1}_{4p-5}, 0, 0, \cdots, 0)$$

$$(2, 2, 2, 2, 2, 2, 2, \underbrace{1, 1, \cdots, 1}_{4p-8}, 0, 0, \cdots, 0)$$

Let N be the unique subgroup isomorphic to $\mathbb{Z}_2^3$ in G.

Let $P_1, \ldots, P_{p^2+p+1}$ be the $p^2 + p + 1$ subgroups of G isomorphic to $\mathbb{Z}_p$.

Let $L_1, \ldots, L_{p^2+p+1}$ be the $p^2 + p + 1$ subgroups of G isomorphic to $\mathbb{Z}_p^2$.

Let $\mathcal{P}$ be the incidence structure with points the subgroups $P_i \times N$, with blocks the subgroups $L_i \times N$, and with containment as incidence. Then it is easily seen that $\mathcal{P}$ is a $2-(p^2+p+1, p+1, 1)$ design, or equivalently, the unique projective plane of order p.

Next assign a weight to each point of $\mathcal{P}$ in the following way:

The weight of $P_i \times N$ is $\frac{1}{p-1}|((P_i \times N) \setminus N) \cap D|$.

In this way the weights of the points of $\mathcal{P}$ correspond to the values $C_1, C_2, \ldots, C_{p^2+p+1}$, that is, $\frac{1}{p-1}$-th of the number of elements of order p or $2p$ from D in the subgroup underlying the given point.

Without loss of generality $wt(P_i \times N) = C_i$.

The weight of a block will simply be the sum of the weights of the points in that block.

Assume that $|(L_i \times N) \cap D| = m$.

Counting the number of differences of elements of D that are in $L_i \times N$ in two ways, we obtain

$$m(m-1)+(k-m)(\frac{k-m-(p-1)}{p-1}) = \lambda m+\mu(8p^2-1-m), \quad (5)$$

where $(k, \lambda, \mu) = (4p^2 + 2p - 2, 2p - 2, 2p + 2)$. This yields that $m = 2(p + 1)$ or $2(3p - 1)$.

Define $m' := \frac{1}{p-1}|((L_i \times N) \setminus N) \cap D| = \frac{m-4}{p-1}$ (as D contains 4 elements of order 2).

We obtain $m' = 2$ or $m' = 6$.

We now note that the values m' must be the weights of the blocks of $\mathcal{P}$, and that in both cases these weights are even.

On the other hand, it is easy to see that no value C_j can be odd.

Since all the solutions contains at least one odd C_j, thus no such D exists.

Next assume that D contains no elements of order 2. We see that $\Sigma_i B_i = 4p^2 + 2p - 2$ and $\Sigma_i B_i(B_i - 1) = 14p + 14$.
By using similar notations as before, we have

$$\Sigma_j C_j = \frac{4p^2 + 2p - 2}{p - 1} = (4p + 6) + \frac{4}{p - 1} \quad (6)$$

$$\Sigma_j C_j^2 = \frac{4p^2 + 16p + 12}{p - 1} \quad (7)$$

It is clear that Equation (6) has integer solutions only when $\frac{4}{p-1}$ is an integer, that is when $p - 1 = 1, 2$, or 4. When $p = 3$, we have $v = 216$, and it is covered in the paper by De Winter, Neubert and Wang.

When $p = 5$, Equations (6) and (7) become $\Sigma_j C_j = 27$ and $\Sigma_j C_j^2 = 48$. Thus $\Sigma_j C_j(C_j - 1) = 21$, which contradicts with the fact that $C_j(C_j - 1)$ is an even number for any j. Thus no such D exists.

Current and future work

- Generalize Theorem 1 to SRG with non-integer eigenvalues and directed strongly regular graphs. Apply to Paley type PDS and skew Hadamard difference sets.
- Classify PDS in Abelian groups of order p^{2h+1}.
- Find more constructions of PDS in Abelian groups using the Local Multiplier Theorem.
- How useful is Theorem 1 and possible consequences in the case of PDS in non-Abelian groups? The LMT does not hold, but can we prove alternatives?

THANKS!