Some Results on Partial Difference Sets

Zeying Wang

Department of Mathematics and Statistics
American University

July 4th, 2023

The co-authors

Ellen Kamischke

Stefaan De Winter

Eric J Neubert

Strongly regular graphs

A (finite) graph $\Gamma = (V, E)$ is called *strongly regular* with parameters $\text{srg}(v, k, \lambda, \mu)$ if

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

Let Γ be a $\text{srg}(v, k, \lambda, \mu)$. 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.

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.

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.

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

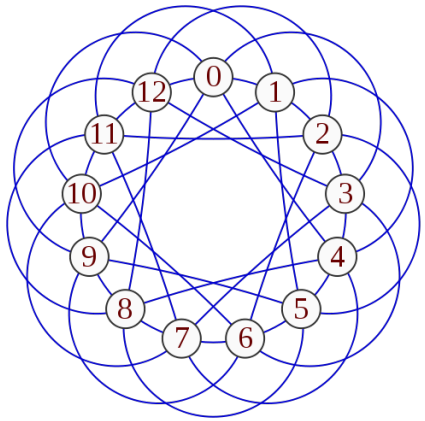
- the vertices of Γ are the elements of G;
- two vertices g and h are adjacent if and only if $gh^{-1} \in \mathcal{D}$.

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.



Theorem 1: A Benson type theorem for SRGs

Theorem (De Winter - Kamischke - Wang '16)

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

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

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.

Corollary

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 (Local multiplier theorem, De Winter - Kamischke - Wang '16)

Let $\mathcal{D}$ be a regular PDS in an Abelian group G. Assume $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ is a perfect square. Let $u \in G$ be an element of order r. Assume $\gcd(s, r) = 1$. *Then $u \in \mathcal{D}$ if and only if $u^s \in \mathcal{D}$.*

Proof. An element $u \in \mathcal{D}$ if and only if the corresponding automorphism u: $v \mapsto vu$ 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 an Abelian group G of order v. Assume $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ is a perfect square. Then $\mathcal{D}^{(s)} = \mathcal{D}$ for all s with $\gcd(s, v) = 1$.

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 $s \neq t$.

Direction application of the LMT

Theorem

There is no regular $(196, 65, 24, 20)$*-PDS in an Abelian group of order 196.*

Proof: By the proposition from [Ma 94],

$$G = \mathbb{Z}_2^2 \times \mathbb{Z}_7^2.$$

Thus the possible orders of non-identity elements of G are 2, 7, and 14, with respective values of the Euler phi function 1, 6, and 6. Hence we should be able to write 65 as $r_1 \cdot 1 + r_2 \cdot 6$, where $0 \leq r_1 \leq 3$, as G contains exactly 3 elements of order 2. Since $65 \equiv 5 \pmod 6$ and $5 > 3$ this is clearly impossible.

Theorem 2(De Winter - Kamischke - Wang '16)

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 $4p^2$

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.

Theorem 3 (De Winter - Wang '17)

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-type, or the $(36, 14, 4, 6)$-PDS in $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$.

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

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'17)

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.

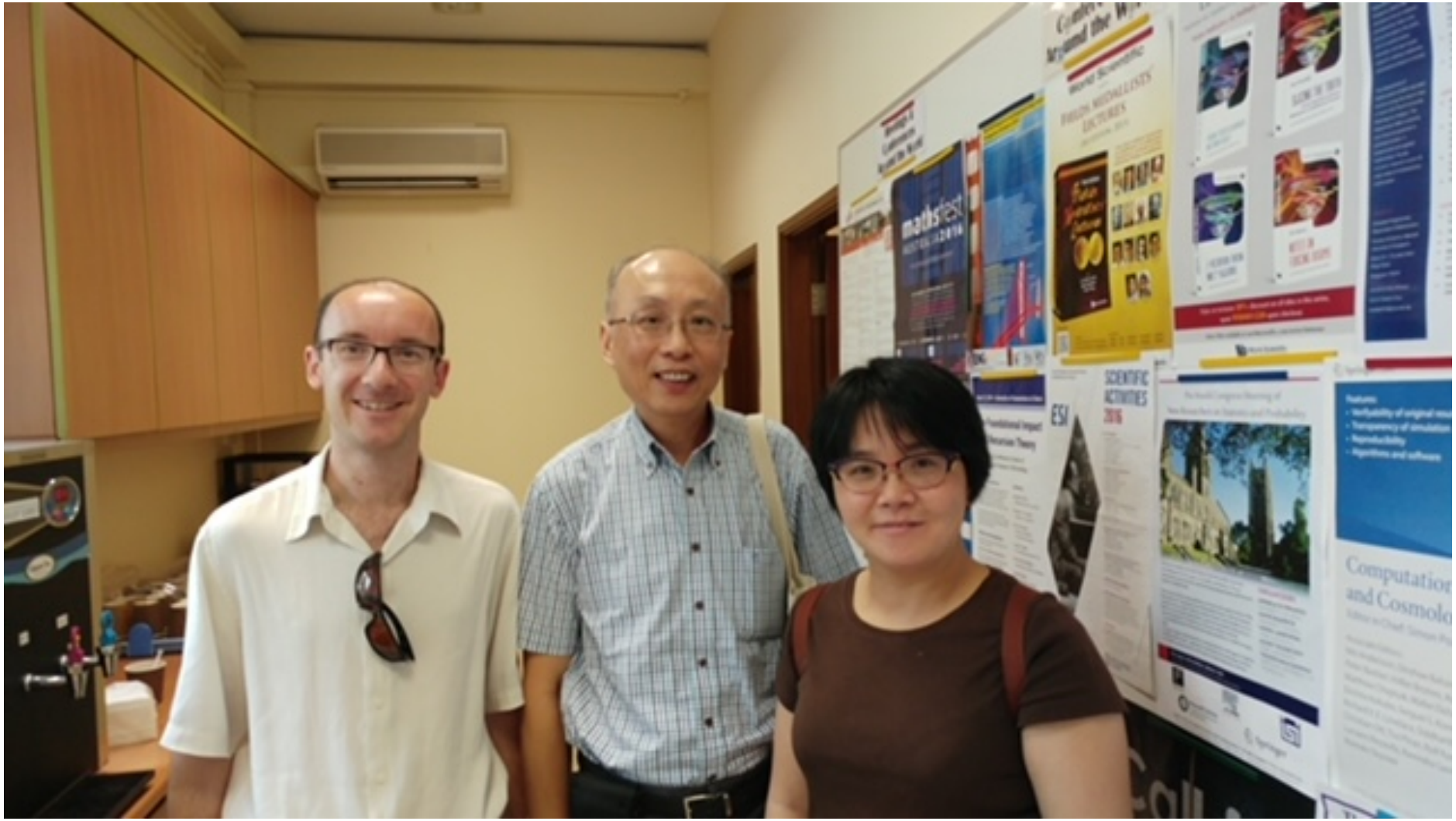
Since (216, 40, 4, 8) and (216, 43, 10, 8) are the only two parameter sets that survive the basic integrality and divisibility conditions of non-trivial partial difference sets, there are no non-trivial regular partial difference sets in Abelian groups of order 216.

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 (2017)
216	43	10	8	DNE (2017)
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

Theorem (De Winter–Wang '19)

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

With S.L. Ma in Singapore



Application 4: regular Paley-type PDSs in abelian groups:

Definition: A partial difference set with parameters $(v, (v-1)/2, (v-5)/4, (v-1)/4)$ is called a Paley type PDS.

Key Problems:

1. For which odd positive integer $v > 1$, can we find a regular Paley-type PDS in an abelian group of order v?
2. Given a group order, in which specific abelian groups of that order can we find regular Paley-type PDSs?

Known results on Question 1

- **Theorem [Ma 1984]**
  Let D be an abelian regular (v, k, λ, μ)-PDS, and assume that $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$ is not a perfect square. Then D is of Paley type; more precisely, D has parameters

$$(p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4),$$

  where p is a prime congruent to 1 modulo 4.
- For a prime power $q \equiv 1 \pmod 4$, we can always construct a regular Paley-type PDS in $(F_q, +)$ using the nonzero squares of the finite field F_q.

Remark: Since a regular Paley type PDS D has parameters $((v,(v-1)/2,(v-5)/4,(v-1)/4)$, we have

$$\Delta = (\lambda-\mu)^2+4(k-\mu) = (\frac{v-5}{4}-\frac{v-1}{4})^2+4(\frac{v-1}{2}-\frac{v-1}{4}) = v.$$

Using the previous two results, to answer Question 1, we only need to focus on the existence of Paley-type PDSs of order v when v is a perfect square and v is not a prime power.

Theorem (Ma 1994)

Let D be a nontrivial regular (v, k, λ, μ) partial difference set in an abelian group G. Suppose $\Delta = \delta^2$ is a perfect square. Let N be a subgroup of G such that $\gcd(|N|, |G|/|N|) = 1$ and $|G|/|N|$ is odd. Then $D_1 = N \cap D$ is a (not necessarily non-trivial) regular $(v_1, k_1, \lambda_1, \mu_1)$ partial difference set in N with

$$v_1 = |N|,\ \beta_1 = \lambda_1 - \mu_1 = \beta - 2\theta\pi,\ \Delta_1 = \beta_1^2 + 4(k_1 - \mu_1) = \pi^2,$$

$$k_1 = |N \cap D| = \frac{1}{2}\left[|N| + \beta_1 \pm \sqrt{(|N| + \beta_1)^2 - (\Delta_1 - \beta_1^2)(|N| - 1)}\right].$$

where $\pi = \gcd(|N|, \delta)$ and θ is the integer satisfying $(2\theta - 1)\pi \leq \beta < (2\theta + 1)\pi$. Moreover, if $D_1 \neq \emptyset$, $D_1 \neq N \setminus \{e\}$, and if $\delta = p^r\pi$, where $p \geq 5$ is a prime and $\pi > 1$ is relatively prime to p, then either r is even and $\theta \equiv 0 \pmod{p-1}$ or r is odd and $\theta \equiv (p-1)/2 \pmod{p-1}$.

Theorem (Wang, 2020)

Let G be an abelian group of order $p^{2r}u^2$, $p \geq 5$ a prime number, $u > 1$, and $\gcd(p, u) = 1$. If D is a Paley type partial difference set in G, then r is even.

Corollary

Let G be an abelian group, and $|G| = p_1^{2l_1} p_2^{2l_2} \cdots p_k^{2l_k}$, $k \geq 2$, p_1, p_2, $\cdots$, p_k are distinct odd prime numbers. If D is a Paley type PDS in G, then $|G| = n^4$ or $9n^4$, with $n > 1$ an odd positive integer.

Theorem (J. Polhill, 2010)

Let n be a positive odd number. Then there is a Paley partial difference set in an abelian group of order n^4 $(n > 1)$ and a Paley type PDS in an abelian group $9n^4$.

Combining the Corollary and the theorem of Polhill, our main theorem of Paley type PDS follows.

Theorem (Wang, 2020)

Let v be an odd positive integer > 1. Then there exists Paley type PDS in some abelian group G of order v if and only if v is a prime power and $v \equiv 1 \pmod 4$, or $v = n^4$ or $9n^4$, with $n > 1$ an odd positive integer.

Current and future work

- Generalize the Benson type Theorem to SRG with non-integer eigenvalues and directed strongly regular graphs.
- Find more constructions of PDS in Abelian groups using the Local Multiplier Theorem.
- Answer Question 2 of Paley type PDSs.
- Recently Swartz and Tauscheck (and later also Davis, Polhill and Smith) applied Theorem 1 (the Benson type Theorem on SRG) to provide restrictions on the parameters of a PDS in both Abelian and non-Abelian groups. Can we find more applications of Theorem 1?