Partial difference sets in Abelian groups

Stefaan De Winter
Department of Mathematical Sciences
Michigan Technological University

Joint work with Ellen Kamischke and Zeying Wang

Partial differene sets

Let G be finite group of order v with identity e.

A (v, k, λ, μ) *partial difference set* (PDS) $\mathcal{D}$ in G is a k-subset of G with the property that the expressions gh^{-1}, $g, h \in \mathcal{D}$ 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*.

if $\lambda \neq \mu$ then $\mathcal{D}^{(-1)} = \mathcal{D}$ is automatically fulfilled.

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 $\lambda = \mu$).

Some examples

- $\mathcal{D} \cup \{e\}$ is a subgroup of G.
- $G \setminus \mathcal{D}$ is a subgroup of G.

These two examples are called *trivial*.

- Let q be an odd prime power, with $q \equiv 1 \pmod 4$. Then the non-zero squares of $\mathbb{F}_q$ form a PDS$(q, (q-1)/2, (q-5)/4, (q-1)/4)$ in the additive group of $\mathbb{F}_q$. PDS with these parameters are said to be of Paley type. For example $\{1, 3, 4, 9, 10, 12\} \subset \mathbb{F}_{13}, +$

- 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.
- Let $\mathcal{C}$ be a linear projective two-weight code of dimension k over the field $\mathbb{F}_q$ then $\mathcal{C}$ gives rise to a PDS in the elementary Abelian group of order q^k.

Most examples so far are in Abelian groups, however, this is not necessary condition for existence. In fact, the study of Paley type PDS in non-Abelian groups is rich and interesting. However, many open problems for PDS in Abelian groups remain, and for the rest of the talk we will always assume G is Abelian.

PDS and strongly regular graphs

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

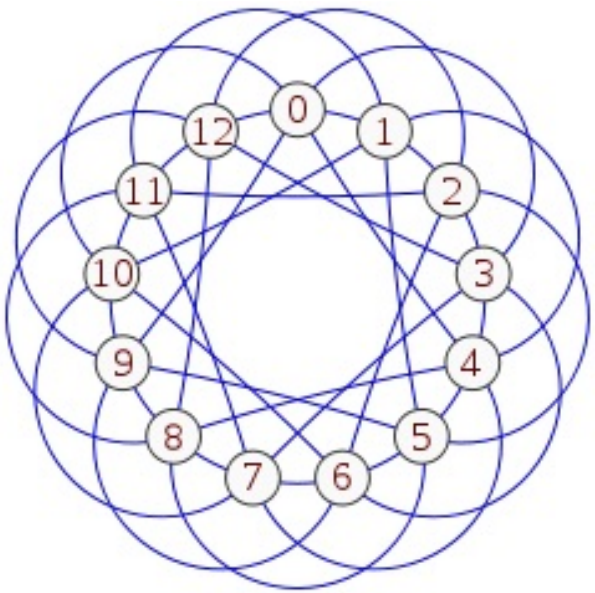
- it has v vertices;
- degree k;
- every two adjacent vertices have λ common neighbors;
- every two non-adjacent vertices have μ common neighbors.

This important class of graphs is widely studied and has many links to other combinatorial structures.

Let $\mathcal{D}$ be a regular PDS(v, k, λ, μ). 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 iff $gh^{-1} \in \mathcal{D}$.

Then the graph $\Gamma(G, \mathcal{D})$ is strongly regular with parameters srg(v, k, λ, μ).



Parameter restrictions

Assume $\mathcal{D}$ is a non-trivial regular PDS in the Abelian group G, then

- $(v+\lambda-\mu)^2-(\Delta-(\lambda-\mu)^2)(v-1)$ is a square;
- $k=(v+\lambda-\mu\pm\sqrt{(v+\lambda-\mu)^2-(\Delta-(\lambda-\mu)^2)(v-1)})/2$;
- $\lambda-\mu$ and Δ have the same parity;
- $v^2\equiv(2k-\lambda+\mu)^2\equiv((\lambda-\mu)^2-2(\lambda-\mu))v\equiv 0 \pmod{\Delta}$
- v, Δ, v^2/Δ have the same prime divisors;
- ...

where $\Delta=(\lambda-\mu)^2+4(k-\mu)$.

The key technique in the proof of almost all results on PDS is computations in the group ring. We will however follow a different, linear algebraic, path, using the adjaceny matrix of the strongly regular graph related to the PDS.

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 ij if vertex i is adjacent to vertex j, and 0 everywhere else.

Then A has eigenvalues

$$\nu_1 := k,$$

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

$$\nu_3 := \frac{1}{2}(\lambda - \mu - \sqrt{\Delta}),$$

where $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$.

These eigenvalues are integers, unless possibly when Γ is a conference graph.

The multiplicities of these eigenvalues are

$$m_1 := 1,$$

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

and

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

Ma's list

In 1994 S.L. Ma produced a list of all parameter sets (v, k, λ, μ) with $k \leq 100$ that survived the known restrictions. 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, leaving 19 unresolved cases.

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	
512	73	12	10	

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	
512	73	12	10	exists (1)

(1) Fiedler and Klin (1998), and Kohnert (2007)

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 $s \neq t$.

Hence

- when G has order 100, $G \cong (\mathbb{Z}_2)^2 \times (\mathbb{Z}_5)^2$
- when G has order 144, $G \cong (\mathbb{Z}_2)^4 \times (\mathbb{Z}_3)^2$ or $G \cong (\mathbb{Z}_4)^2 \times (\mathbb{Z}_3)^2$,
- when G has order 196, $G \cong (\mathbb{Z}_2)^2 \times (\mathbb{Z}_7)^2$,
- when G has order 216, $G \cong (\mathbb{Z}_2)^3 \times (\mathbb{Z}_3)^3$,
- when G has order 225, $G \cong (\mathbb{Z}_3)^2 \times (\mathbb{Z}_5)^2$,
- when G has order 392, $G \cong (\mathbb{Z}_2)^3 \times (\mathbb{Z}_7)^2$,
- when G has order 400, $G \cong (\mathbb{Z}_2)^4 \times (\mathbb{Z}_5)^2$ or $G \cong (\mathbb{Z}_4)^2 \times (\mathbb{Z}_5)^2$.

Benson's theorem

Theorem (Benson '70)

Let $\mathcal{Q}$ be a GQ(s,t), and let ϕ be an automorphism of $\mathcal{Q}$. If ϕ has f fixed points, and maps g points to collinear points then

$$(1+t)f + g \equiv (1+s)(1+t) \pmod{s+t}.$$

This theorem was generalized to a broader type of geometries in 2006 (SDW), and once more in 2009 (Temmermans, Thas and Van Maldeghem). Each time the considered geometries had strongly regular point graphs (or distance regular). Can we formulate a unifying theorem for strongly regular graphs?

Theorem

Let Γ be a strongly regular graph with Δ a perfect square. Let g 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

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

where f is the number of fixed vertices of g, and t is the number of vertices that are adjacent to their image under g. Furthermore a_d equals the multiplicity of the eigenvalue $\xi_d(\nu_2 - \nu_3)$ of the matrix $P(A - \nu_3 I)$, where ξ_d is a primitive dth root of unity, and P the permutation matrix corresponding to g.

Corollary

Let Γ be a strongly regular graph with Δ a perfect square, and let g be an automorphism of order n of Γ. Let s be an integer coprime with n. Then g and g^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. If $g \in \mathcal{D}$ and g has order r, then $g^s \in \mathcal{D}$ for all s with $\gcd(s, r) = 1$.

Proof. We have $g \in \mathcal{D}$ if and only if g has no fixed points and g maps every vertex to an adjacent vertex (in its natural action on the associated Cayley graph).

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 $\gcd(s, v) = 1$.

This result was originally proved by Ma using character theory.

Corollary

Let $\mathcal{D}$ be a regular (v, k, λ, μ) PDS in the Abelian group G. Furthermore assume Δ is a perfect square. Let $g \in G$ belong to $\mathcal{D}$. Then the set $\mathcal{D}(g) := \{g^s \mid \gcd(s, o(g)) = 1\}$ is a subset of $\mathcal{D}$ with cardinality $\phi(o(g))$, where ϕ is the Euler totient function. Furthermore if $h \in \mathcal{D}(g)$ then $\mathcal{D}(h) = \mathcal{D}(g)$. Hence $\mathcal{D}$ can be written as a partition $\mathcal{D} = \mathcal{D}(g_1) \cup \cdots \cup \mathcal{D}(g_r)$ for some elements $g_1, \ldots, g_r$.

Direct application of the LMT

Theorem

There is no PDS$(196, 65, 24, 20)$

Proof. The possible orders of non-identity elements of G are $2, 7$ and 14, with respective values of the Euler totient 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.

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	DNE
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	
512	73	12	10	exists

A counting argument

Let $\mathcal{D}$ be a regular (v, k, λ, μ) PDS in an Abelian group G. Let $\Gamma = (G, \mathcal{D})$ be the corresponding Cayley graph, and let A be its adjacency matrix. Let $P_1, P_2, \ldots, P_v$ be the $v \times v$ permutation matrices corresponding to the elements of G.

As $A - \nu_3 I, P_1, P_2, \ldots, P_v$ is a set of commuting and diagonalizable matrices, these matrices are simultaneously diagonalizable.

Let $u_0, u_1, \ldots, u_{v-1}$ be a common eigenbasis for these matrices, labeled in such a way that $(A - \nu_3 I)u_0 = (k - \nu_3)u_0$, $(A - \nu_3 I)u_i = (\nu_2 - \nu_3)u_i$ for $i = 1, 2, \ldots, m_2$, and $(A - \nu_3 I)u_i = 0$ for $i = m_2 + 1, m_2 + 2, \ldots, v - 1$

Set $U := \{u_1, \ldots, u_{m_2}\}$.

Lemma

Let $H = \mathbb{Z}_p^r$, p prime, be a subgroup of G. Then any of the vectors $u_i \in U$ is an eigenvector with eigenvalue 1 for either all or p^{r-1} of the elements of H. In the latter case the elements for which u_i appears with eigenvalue 1 form a subgroup of H.

Theorem

Let $H = \mathbb{Z}_p^r$, p prime, be a subgroup of G. Assume that $|H \cap \mathcal{D}| = s$. Let x be the number of vectors in U that appear with eigenvalue 1 for all elements of H. Finally let a_1 be the multiplicity of the eigenvalue $\nu_2 - \nu_3$ of the matrix $P(A - \nu_3 I)$, where P is an element of order p in $\mathcal{D}$, and let a_1' be the multiplicity of the eigenvalue $\nu_2 - \nu_3$ of the matrix $P(A - \nu_3 I)$, where P is not in $\mathcal{D}$. Then

$$m_2 + sa_1 + (p^r - 1 - s)a_1' = xp^r + (m_2 - x)p^{r-1}.$$

The general approach: PDS$(196, 60, 14, 20)$

We start by computing possible values for the a_d from Theorem 2, using Equation (1) together with the fact that $a_1 + 6a_7 = 135$. We obtain

$o(g) = 7$	a_1	a_7
$g \in \mathcal{D}$	27	18
$g \notin \mathcal{D}$	15	20

Applying Theorem 9 to $\mathbb{Z}_7 \times \mathbb{Z}_7 < G$, we obtain

$$135 + s27 + (48 - s)15 = x49 + (135 - x)7.$$

Hence $s = \frac{1}{2}(15 + 7x)$ with $(s, x) = (18, 3)$ as the only solution. It follows that $\mathcal{D}$ must contain exactly 18 elements of order 7.

As $\phi(14) = 6$ it follows that the total number of elements of order 14 in $\mathcal{D}$ is divisible by 6. Given that $k = 60$ and that there are 18 elements of order 7 we deduce that $6 \mid 60 - 18 - a$, where a is the number of elements of order 2 in $\mathcal{D}$. Hence $\mathcal{D}$ does not contain any element of order 2.

The only way to obtain an element of order 7 as a difference of two elements of $\mathcal{D}$ is as a difference of two elements of order 7 or as the difference of two elements of order 14.

There are exactly $18 \cdot 17$ differences of the former type.

The difference of two elements of order 14 will be of order 7 if and only if both elements have the same element of order 2 as their seventh power.

Let g_1, g_2 and g_3 be the three elements of order 2, and denote by A_i, $i = 1, 2, 3$, the number of elements of order 14 in $\mathcal{D}$ that have g_i as their seventh power. Then

$$\begin{cases} \Sigma_i A_i &= 42 \\ \Sigma_i A_i(A_i - 1) &= 18 \cdot 14 + 30 \cdot 20 - 18 \cdot 17 = 546 \end{cases}$$

It follows that

$$3\Sigma_i A_i^2 - (\Sigma_i A_i)^2 = 3 \cdot 588 - 42^2 = 0,$$

or that the variance of the A_i equals zero.

Consequently $A_1 = A_2 = A_3 = 42/3 = 14$. However, if g has order 14, then $|\mathcal{D}(g)| = 6$ and $h^7 = g^7$ for all $h \in \mathcal{D}(g)$. This means 6 divides A_i, a contradiction.

No PDS$(196, 60, 14, 20)$

Ma's table

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
512	73	12	10	exists

Questions and future work

- Do there exist PDS$(216, 40, 4, 8)$ or PDS$(216, 43, 10, 8)$ in $(\mathbb{Z}_2)^3 \times (\mathbb{Z}_3)^3$?
- Use our technique for PDS in Abelian groups of order $4p^2$ or p^2q^2. Is it true that PDS in these groups (with exception of order 36) always have Paley or PCP parameters?
- To what extend can we generalize the Benson type theorem to conference graphs with non-integer eigenvalues?
- Extend the Benson type theorem to distance regular graphs.

THANKS!