A linear algebraic approach to partial difference sets

Stefaan De Winter
Department of Mathematical Sciences
Michigan Technological University

May 24th, 2016

Strongly regular graphs

A (finite) graph $\Gamma = (V, E)$ is a (v, k, λ, μ) strongly regular graph if

- it has v vertices;
- each vertex is adjacent to k vertices;
- every two adjacent vertices have λ common neighbors;
- every two non-adjacent vertices have μ common neighbors.

Important graphs with links to geometry, coding theory, group theory, design theory, ...

Let Γ be a strongly regular graph with parameters (v, k, λ, μ). Then its adjacency matrix 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, except for $\mathrm{srg}(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ with v not a perfect square.

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

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

Cayley graphs

Let G be a finite group and let S be an inverse-closed subset of $G \setminus \{e\}$. Then the *Cayley graph* $\Gamma := \Gamma(G, S)$ is the graph with vertices the elements of G in which two vertices g and h are adjacent iff $gh^{-1} \in S$.

The Cayley graph Γ admits G as a group of automorphisms acting sharply transitively on the vertices of Γ.

Partial difference sets

A (v, k, λ, μ)-*partial difference set* (for short (v, k, λ, μ)-PDS) $\mathcal{D}$ in a finite group G of order v is a k-subset $\mathcal{D}$ 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.

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

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.

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

If $\mathcal{D}$ is a regular PDS in G, then so is $G \setminus (\mathcal{D} \cup \{e\})$.

Importance of PDS: The Cayley graph $\Gamma(G, \mathcal{D})$ is a strongly regular graph if and only if $\mathcal{D}$ is a regular PDS.

Study PDS through the associated SRG and its sharply transitive group of automorphisms

Theorem 1 (SDW - Kamischke - Wang '15)

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

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

and consequently

$$k - \nu_3 \equiv -\nu_3 f + g \pmod{\nu_2 - \nu_3}, \tag{2}$$

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.

Sketch of proof. Let A be the adjacency matrix of Γ, and let P the permutation matrix corresponding to the automorphism ϕ. Compute the trace of $P(A - \nu_3 I)$ once as the sum of the eigenvalues, and once as the sum of the diagonal entries.

The integer a_d in the statement of the theorem 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.

History of Theorem 1

1970 Benson's theorem for GQ(s, t):
$(1 + t)f + g \equiv (1 + s)(1 + t) \pmod{s + t}$.

2006 SDW: a generalization for partial geometries.

2010 Temmermans, Thas, Van Maldeghem: further generalizations for partial quadrangles (no nice congruence anymore).

All the above geometries have a strongly regular point graph, and hence these results are special cases of our Theorem 1. The main difference in our proof of Theorem 1 and the proofs of the above results is that we use the adjacency matrix of the graph, rather than the incidence matrix of some geometry.

Corollary

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

Sketch of proof. Because s is an integer coprime with n, every vertex fixed by ϕ is also fixed by ϕ^s, and vice versa. Hence $f_\phi = f_{\phi^s}$. From linear algebra it follows that the eigenvalues a_d in Equation (1) are the same for ϕ and ϕ^s. It follows that both ϕ and ϕ^s produce the same left side of Equation (1). Hence also $g_\phi = g_{\phi^s}$.

Local Multiplier Theorem

This corollary easily translates into the following result for PDS:

Theorem (LMT)

Let $\mathcal{D}$ be a regular PDS in the Abelian group G. Assume $\Gamma(G, \mathcal{D})$ has integer eigenvalues. 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 $\Gamma(G, \mathcal{D})$ has integer eigenvalues. Then $\mathcal{D}^{(s)} = \mathcal{D}$ for all s with $\gcd(s, v) = 1$.

This result was originally proved by Ma. Although the LMT seems to be stronger than the classical multiplier theorem, it turns out it is possible to prove the LMT directly from this classical result. However, the LMT turns out to be handier to work with.

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.

Theorem

Let $H = \mathbb{Z}_p^r$, p prime, be a subgroup of G. Assume that $|H \cap \mathcal{D}| = s$. There exists a non-negative integer x such that

$$m_2 + sa_1 + (p^r - 1 - s)a_1' = xp^r + (m_2 - x)p^{r-1} \tag{3}$$

where

$$a_1 = \frac{(p-1)(v + \nu_3 - k) + m_2(\nu_2 - \nu_3)}{(p-2)(\nu_2 - \nu_3)}$$

and

$$a_1' = \frac{(p-1)(\nu_3 - k) + m_2(\nu_2 - \nu_3)}{(p-2)(\nu_2 - \nu_3)}.$$

Importance: Equation (3) needs to be satisfied in the integers.

Combining restrictions on the structure of G previously obtained by Ma, the LMT, the above equality, and some counting arguments yields:

Theorem 2 (SDW - Kamischke - Wang '15)

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 at the Irsee '14 conference 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.

Up to complement, other than trivial examples, there are three regular PDS known in Abelian groups of order $4p^2$:

- $(2p, 2)$-PCP;
- $(2p, 3)$-PCP;
- a $(36, 14, 4, 6)$-PDS in $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$.

Proposition: [Ma 94] No non-trivial PDS exists in an Abelian group G with a cyclic Sylow-p-subgroup and $o(G) \neq p$.

As a consequence we only need to consider $G \cong \mathbb{Z}_2^2 \times \mathbb{Z}_p^2$.

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 $S_{ij} \subset \mathcal{D}$.

Proof. This is immediate from the LMT.

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.

In each case χ uniquely determines $\mathcal{D}$ and vice versa.

Let R_i denote the ith row of χ, and let $r_i = R_i \cdot R_i$.

Important observation: Let χ be a $4 \times (p+1)$ matrix with entries 0 or 1. Let $\mathcal{D}$ be the corresponding subset of G. The number of ways in which an element of S_{ij} can be represented as a "difference" gh^{-1} for $g, h \in \mathcal{D}$ only depends on the column type of column j.

For example, under the assumption that $\mathcal{D}$ contains no elements of order 2:

Lemma

If the jth column of χ is $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ *then the elements of S_{ij} 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* $i = 4$.

The key is that if $\mathcal{D}$ is supposed to be a PDS then all elements in $\mathcal{D}$ should have the same number λ of representations, while all elements not in $\mathcal{D}$ should have the same number μ of representations.

This now yields a large system of equations in the rows R_i of χ. A careful analysis then allows one to solve this system and hence classify all allowable χ.

Similar arguments are used in the case $|\mathbb{Z}_2^2 \cap \mathcal{D}| = 0$ and the case $|\mathbb{Z}_2^2 \cap \mathcal{D}| = 1$.

Theorem (SDW - 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

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

$\mathbb{Z}_2$ $\qquad$ $\mathbb{Z}_2 \times \mathbb{Z}_p$ $\qquad$ $\mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p$

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

complement of $(2p, 2)$-PCP $\qquad$ *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 $\mathbb{Z}_2^2 \times \mathbb{Z}_3^2$.

Some questions and future work

- Generalize Theorem 1 to SRG with non-integer eigenvalues. So far we have partial results for automorphisms of prime power order. Then apply these results to Paley type partial difference sets.
- We can prove an analogue of Theorem 1 for directed SRG. Applications to Hadamard matrices?
- 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 the characteristic matrix approach to classify PDS in Abelian groups of order p^2q^2.
- 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!