

Automorphisms of strongly regular graphs and PDS in Abelian groups

Zeying Wang
Department of Mathematical Sciences
Michigan Technological University

Joint work with Stefaan De Winter and Ellen Kamischke

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.

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

Let Γ be a $\text{srg}(v, k, \lambda, \mu)$. Given a fixed labeling of the vertices $1, \dots, v$, 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

$$m_1 := 1,$$

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

and

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

History

- In 1970, C.T. Benson provided a congruence that relates the parameters of a finite generalized quadrangle to the number of fixed points and the number of points mapped to collinear points under an automorphism.

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

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

- In 2006, De Winter generalized the Benson Theorem to partial geometries.
- In 2010, Temmermans, Thas and Van Maldeghem generalized the Benson Theorem to partial quadrangles.

Main Theorem

Let Γ be a strongly regular graph $srg(v, k, \lambda, \mu)$ with Δ a perfect square. Let ϕ be an automorphism of order n of Γ , and let $\mu(\cdot)$ be the Möbius function. Then for every integer r and all positive divisors d of n , there are non-negative integers a_d and b_d such that

$$k - r + \sum_{d|n} a_d \mu(d)(\nu_2 - r) + \sum_{d|n} b_d \mu(d)(\nu_3 - r) = -rf + t \quad (1)$$

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

As a consequence the following equation holds:

$$k - \nu_3 + \sum_{d|n} a_d \mu(d)(\nu_2 - \nu_3) = -\nu_3 f + t \quad (2)$$

Here 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 d th root of unity, and P the permutation matrix corresponding to ϕ .

Corollary

Let Γ be a strongly regular graph $\text{srg}(v, k, \lambda, \mu)$ with Δ a perfect square, 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.

Partial difference sets (PDS)

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

A (v, k, λ, μ) *partial difference set* \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*. 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.

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 $\text{srg}(v, k, \lambda, \mu)$.

Parameter restrictions

Assume \mathcal{D} is a non-trivial regular (v, k, λ, μ) -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;
- $v^2 \equiv (2k - \lambda + \mu)^2 \equiv ((\lambda - \mu)^2 - 2(\lambda - \mu))v \equiv 0 \pmod{\Delta}$
- $v, \Delta, v^2/\Delta$ have the same prime divisors;
- ...

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

Corollary

Let Γ be a strongly regular graph $\text{srg}(v, k, \lambda, \mu)$ with Δ a perfect square, 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.

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. 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.

Ma's list

In 1994 S.L. Ma produced a list of all parameter sets (ν, 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)

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 $s \neq t$.

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 $G \cong (\mathbb{Z}_4)^2 \times (\mathbb{Z}_5)^2$.

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 $\mathcal{D} = \mathcal{D}(g_1) \cup \dots \cup \mathcal{D}(g_r)$ for some elements g_1, \dots, 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

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

$$m_2 + sa_1 + (p^r - 1 - s)a'_1 = xp^r + (m_2 - x)p^{r-1} \quad (3)$$

where a_1 is the multiplicity of the eigenvalue $\nu_2 - \nu_3$ of the matrix $P(A - \nu_3 I)$ where P corresponds to an element of order p in \mathcal{D} , and a'_1 is the multiplicity of the eigenvalue $\nu_2 - \nu_3$ of the matrix $Q(A - \nu_3 I)$ where Q corresponds to an element of order p not in \mathcal{D} .

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

We start by computing possible values for the a_d from the main theorem, using Equation (2) 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 the last theorem to $\mathbb{Z}_7 \times \mathbb{Z}_7 < G$, we obtain

$$135 + 27s + (48 - s)15 = x49 + (135 - x)7.$$

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. Also we can show that \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

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

It follows that

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

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 $\text{PDS}(216, 40, 4, 8)$ or $\text{PDS}(216, 43, 10, 8)$ 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 . Can we classify the parameters for which a PDS exists?
- To what extent can we generalize the Benson type theorem to conference graphs with non-integer eigenvalues?

THANKS!