Strongly Regular Graphs and Their Symmetries

Eric Swartz

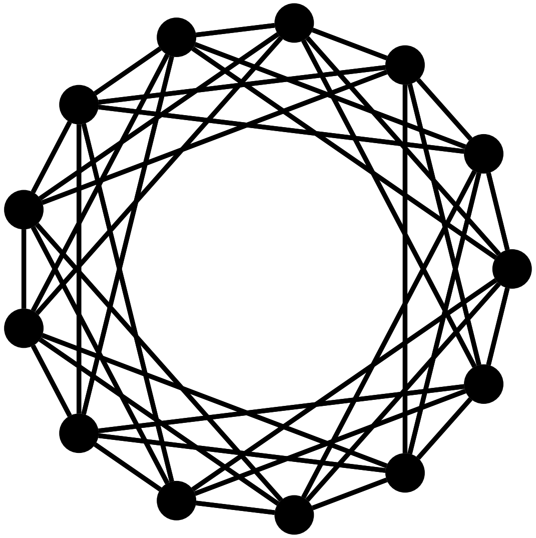
William & Mary

October 25, 2023

Graphs

Definition

- graph Γ: vertices $V(\Gamma)$ and edges $E(\Gamma)$ (unordered pairs of distinct vertices)
- Edges are undirected, and there are no "loops" or "multiple edges"



What do we mean by symmetry?

Formally:

Definition

- automorphism: bijection $g : V(\Gamma) \to V(\Gamma)$ that sends edges to edges and non-edges to non-edges
- set of all automorphisms of Γ: $\mathrm{Aut}(\Gamma)$.

What do we mean by symmetry?

Formally:

Definition

- automorphism: bijection $g : V(\Gamma) \to V(\Gamma)$ that sends edges to edges and non-edges to non-edges
- set of all automorphisms of Γ: $\mathrm{Aut}(\Gamma)$.

- Every graph has at least one automorphism: the identity map that sends every vertex to itself! We will denote the identity simply by 1.

What do we mean by symmetry?

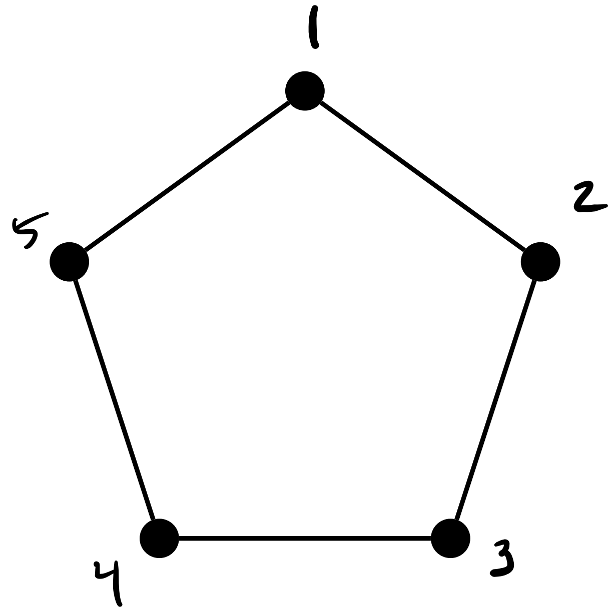
Formally:

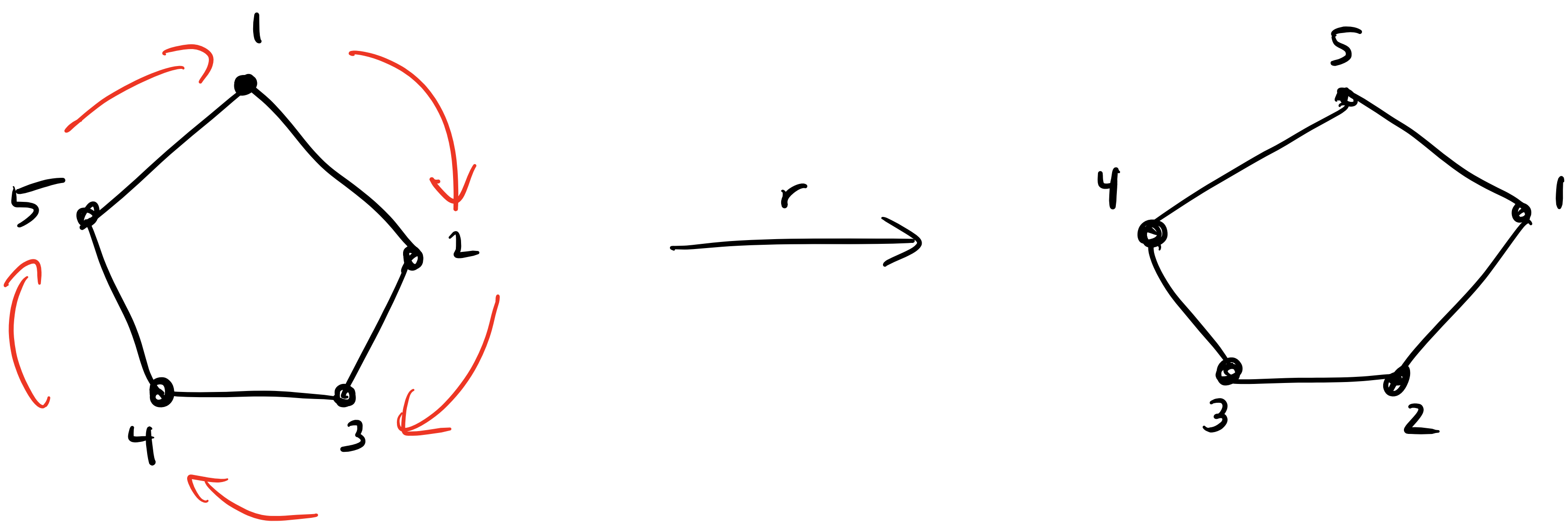
Definition

- automorphism: bijection $g : V(\Gamma) \to V(\Gamma)$ that sends edges to edges and non-edges to non-edges
- set of all automorphisms of Γ: $\mathrm{Aut}(\Gamma)$.

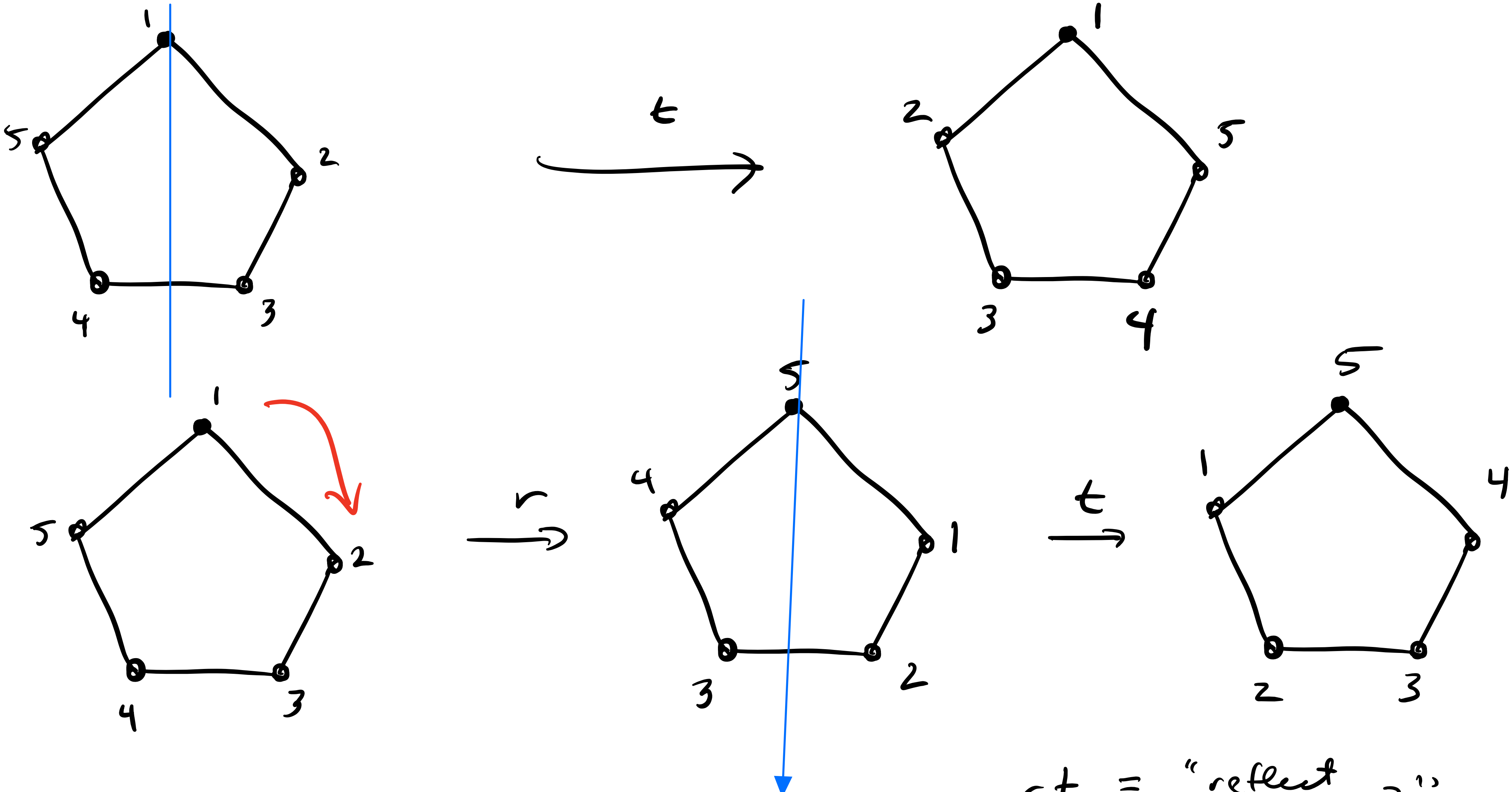
- Every graph has at least one automorphism: the identity map that sends every vertex to itself! We will denote the identity simply by 1.
- If you know some abstract algebra, $\mathrm{Aut}(\Gamma)$ is a group with binary operation composition of functions: it is associative, has an identity 1, and every automorphism has an inverse.

Consider the 5-cycle, C_5.

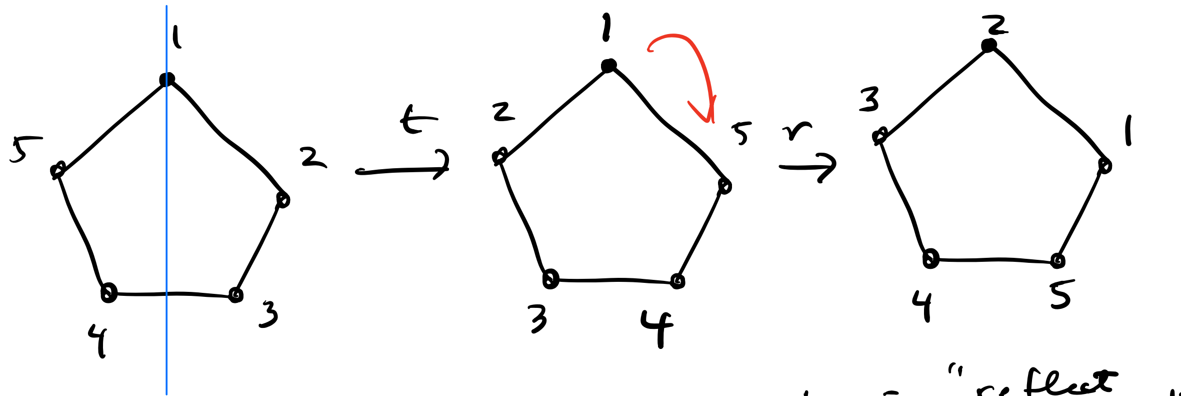




5-cycle, cont.



$rt =$ "reflect through 3"



tr = "reflect through 4"

$$\mathrm{Aut}(C_5) = D_5 = \{\overbrace{1,\ r,\ r^2,\ r^3,\ r^4}^{\text{rotations}},\ \underbrace{t,\ tr,\ tr^2,\ tr^3,\ tr^4}_{\text{"reflections"}}\}$$

Can we impose symmetry?

Definition

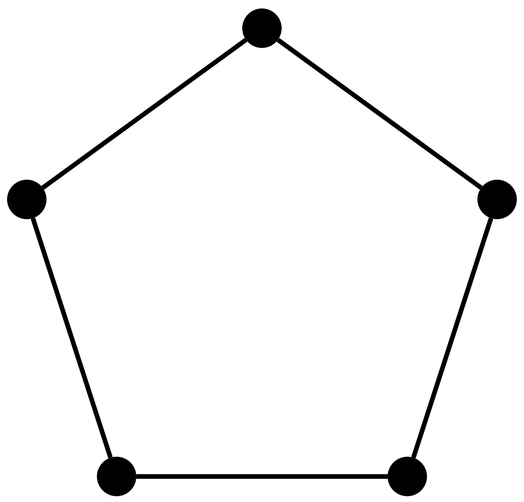
- regular graph: all vertices have the same number of neighbors
- k-regular: every vertex has k neighbors

Can we impose symmetry?

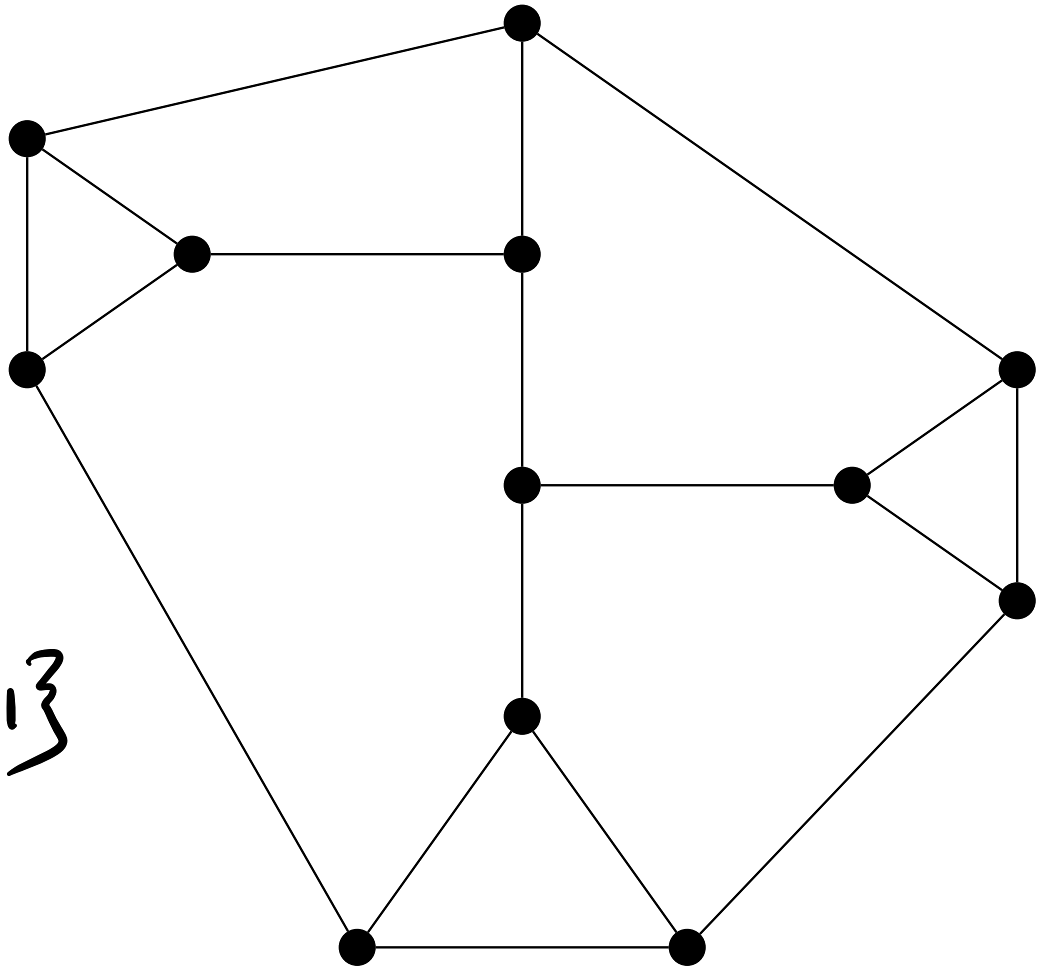
Definition

- regular graph: all vertices have the same number of neighbors
- k-regular: every vertex has k neighbors

The 5-cycle C_5 is 2-regular:



Frucht Graph $\mathcal{F}$



$\mathrm{Aut}(\mathcal{F}) = \{1\}$

Strongly Regular Graphs

Definition

(v, k, λ, μ)-strongly regular graph (SRG):

- v vertices
- k-regular (every vertex has k neighbors)
- every two neighbors have λ common neighbors
- every two non-neighbors have μ common neighbors

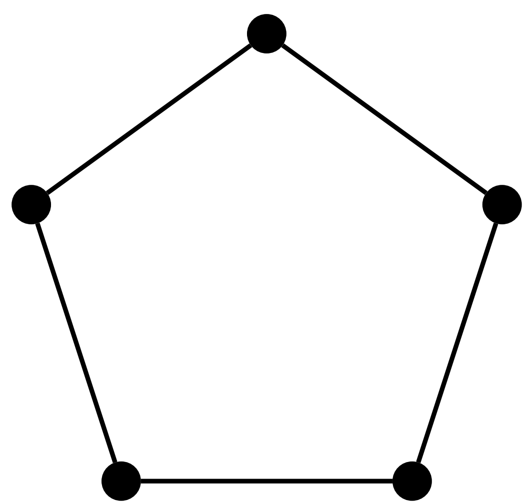
Strongly Regular Graphs

Definition

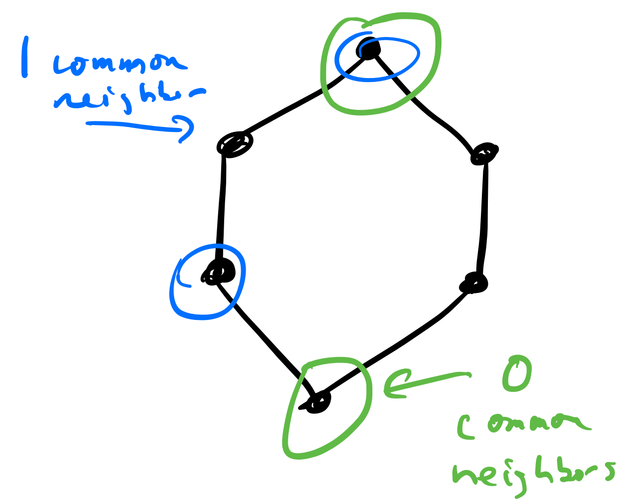
(v, k, λ, μ)-strongly regular graph (SRG):

- v vertices
- k-regular (every vertex has k neighbors)
- every two neighbors have λ common neighbors
- every two non-neighbors have μ common neighbors

5-cycle is a $(5, 2, 0, 1)$-SRG

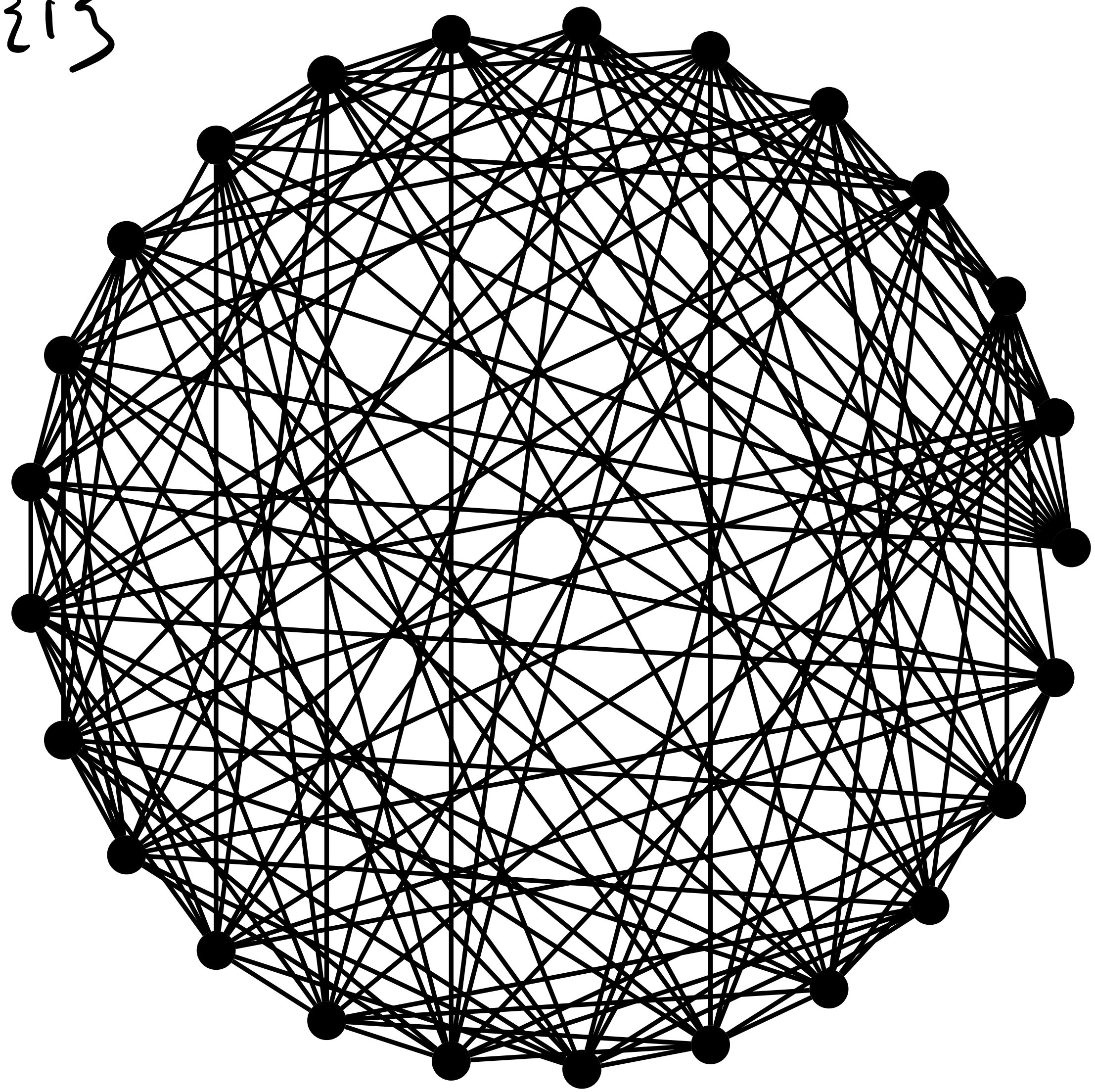


__Ex__ C_6 : __not__ a SRG



A (25,12,5,6)-SRG : $\mathcal{P}$

$\mathrm{Aut}(\mathcal{P}) = \{1\}$



SRGs are difficult!

"Strongly regular graphs stand on the cusp between the random and the highly structured."
-Peter Cameron

SRGs are difficult!

"Strongly regular graphs stand on the cusp between the random and the highly structured."
-Peter Cameron

Example

- 11084874829 SRGs with parameters $(57, 24, 11, 9)$ arising from Steiner triple systems
- 11084710071 have trivial automorphism group!

SRGs are difficult!

"Strongly regular graphs stand on the cusp between the random and the highly structured."
-Peter Cameron

Example

- 11084874829 SRGs with parameters $(57, 24, 11, 9)$ arising from Steiner triple systems
- 11084710071 have trivial automorphism group!

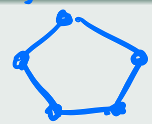
In fact, SRGs are one of the primary roadblocks preventing isomorphism testing of graphs in polynomial time.

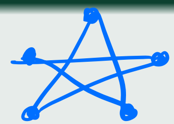
Some Combinatorics

Proposition

Let Γ be a (v, k, λ, μ)-SRG.

C_5





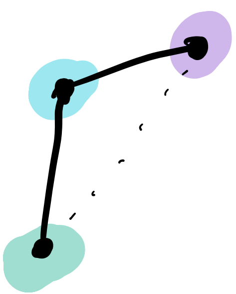
- *The complement (switch edges and non-edges) is a $(v, v-k-1, v-2k+\mu-2, v-2k+\lambda)$-SRG.*
- $k(k-\lambda-1) = (v-k-1)\mu$.

neighbors of one vertex

of neighbors of that neighbor that are not adjacent to or equal to 1st vertex

common neighbors

Pick the 2ND vertex first



Ex $v = 57$, $k = 24$

$$\boxed{24(23-\lambda) = 32\mu}$$

Linear algebra is really useful

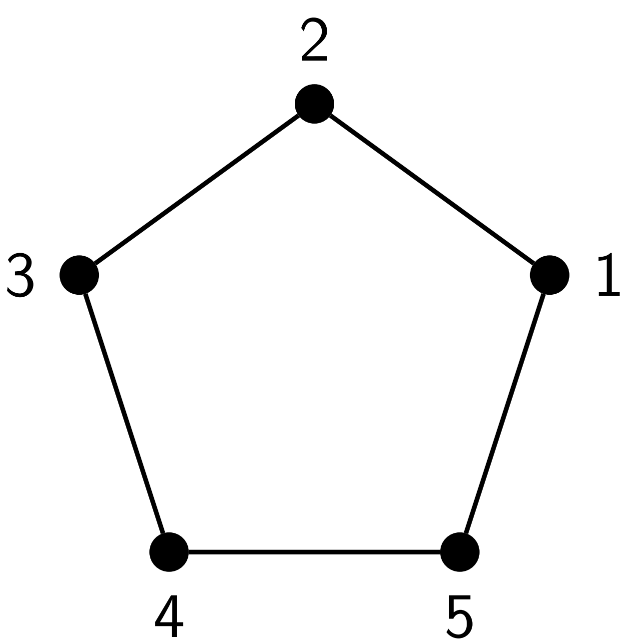
Definition

- Γ: graph with v vertices
- adjacency matrix of Γ: $v \times v$ matrix $A = (a_{ij})$, with rows/columns labeled by vertices
- $a_{ij} = \begin{cases} 1 & \text{if } ij \text{ is an edge,} \\ 0 & \text{otherwise.} \end{cases}$

Linear algebra is really useful

Definition

- Γ: graph with v vertices
- adjacency matrix of Γ: $v \times v$ matrix $A = (a_{ij})$, with rows/columns labeled by vertices
- $a_{ij} = \begin{cases} 1 & \text{if } ij \text{ is an edge,} \\ 0 & \text{otherwise.} \end{cases}$



$$A = \begin{array}{c c} & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Proposition

The i,j-entry of A^n counts the number of walks of length n from i to j.

$$A^2 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 & 1 & 0 \\ & & & & \\ & & \text{etc.} & & \\ & & & & \\ & & & & \end{pmatrix}$$

$$(A^2)_{ij} = \sum_k a_{ik} a_{kj}$$

SRGs and their spectrum

$$A^2 = kI + \lambda A + (J - I - A)\mu$$

J: all 1's matrix

so: $$A^2 - (\lambda - \mu)A - (k-\mu)I = \mu J$$

Since every vertex has k neighbors

$$A\vec{1} = k\vec{1}$$ ("Perron root")

<u>FACT</u>! A (real, symmetric), so other eigenvalues are <u>orthogonal</u> to $\vec{1}$

Suppose $A\vec{v} = \theta\vec{v}$ $\quad (\vec{v} \cdot \vec{1} = 0)$

SRGs and their spectrum, cont.

$$\left(A^2 - (\lambda-\mu)A - (k-\mu)I\right)\vec{v} = \mu J \vec{v}$$

Again: $A\vec{v} = \theta\vec{v}$, $\vec{1}\cdot\vec{v} = 0$

$$\left(\theta^2 - (\lambda-\mu)\theta - (k-\mu)\right)\vec{v} = \vec{0}$$

SRGs and their spectrum, cont.

Proposition

Γ: (v, k, λ, μ)-SRG with adjacency matrix A. Let $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. The eigenvalues of A are:

- k, with multiplicity 1
- $\theta_1 = \frac{1}{2}\left((\lambda - \mu) + \sqrt{\Delta}\right)$, with multiplicity $m_1 = \frac{1}{2}\left((v-1) - \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}}\right)$
- $\theta_2 = \frac{1}{2}\left((\lambda - \mu) - \sqrt{\Delta}\right)$, with multiplicity $m_2 = \frac{1}{2}\left((v-1) + \frac{2k+(v-1)(\lambda-\mu)}{\sqrt{\Delta}}\right)$

Furthermore, if $k \neq \frac{v-1}{2}$, then θ_1 and θ_2 are integers.

Cayley Graphs

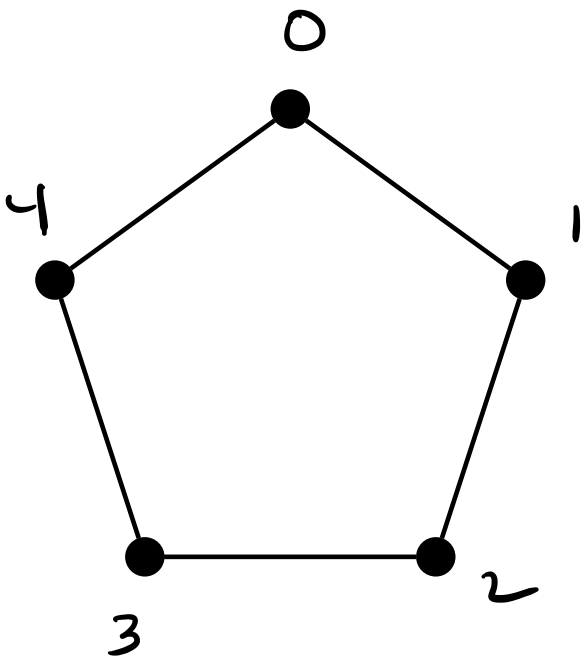
Definition

Cayley graph $\mathrm{Cay}(G, S)$

- G: group
- $S \subset G$
- $1 \notin S$, $S = S^{(-1)}$
- $\mathrm{Cay}(G, S)$ has vertex set G
- $g \sim h$ when $gh^{-1} \in S$

if $x \in S$,
then $x^{-1} \in S$

Example: 5-cycle



$G = (\mathbb{Z}/5\mathbb{Z}, +)$

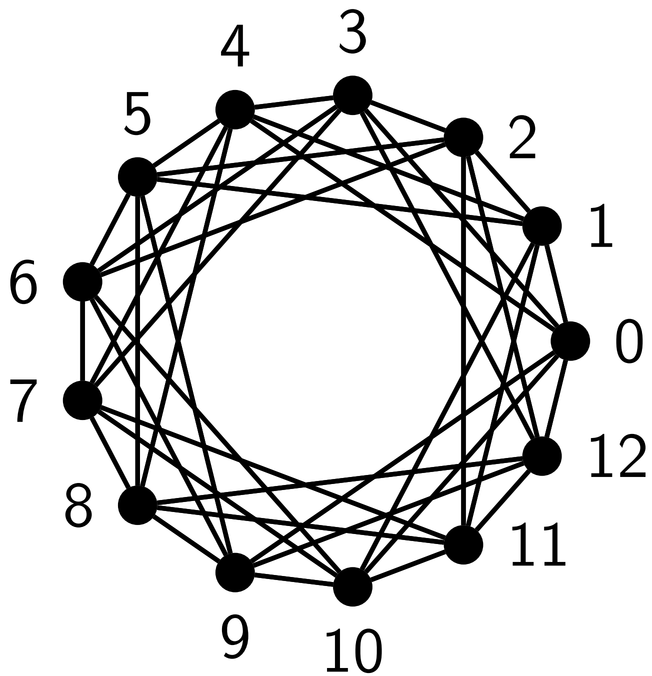
$= \{0, 1, 2, 3, 4\}$

Here, "gh^{-1}" means "$g - h$" since operation is $+$

$S = \{1, 4\} = \{\pm 1\}$

Example: Paley(13)

- $G = \mathbb{Z}/13\mathbb{Z}$, operation: $+$
- $S = \{1, 3, 4, 9, 10, 12\}$ nonzero squares mod 13
- $x \sim y$ when $x - y \in S$
- $\mathrm{Cay}(G, S)$ is a $(13, 6, 2, 3)$-SRG

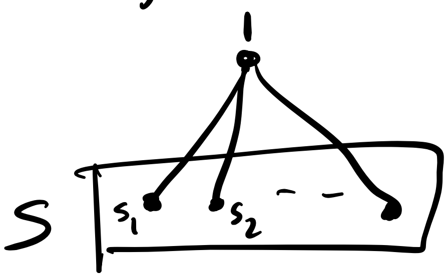


How Cayley graphs work

$\mathrm{Cay}(G,S)$: group G, $S \subseteq G$

$x \sim y \iff xy^{-1} \in S$

Neighbors of $1 \in G$:



Suppose $\underbrace{x \sim y}_{xy^{-1} \in S}$, $g \in G$

$$(xg)(yg)^{-1} = (xg)(g^{-1}y^{-1})$$
$$= xy^{-1} \in S$$

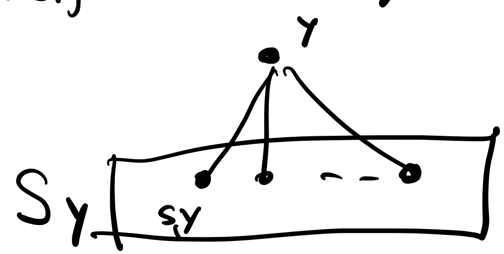
Sending each vertex $x \longmapsto xg$ is an automorphism

Let $x \in G$. If $x \sim y$,

then $xy^{-1} \in S \Rightarrow xy^{-1} = s \in S$

$x = sy$

Neighbors of y:



Partial Difference Sets

Definition

G: group
$S \subset G$
S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,

Partial Difference Sets

Definition

G: group
$S \subset G$
S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,

Partial Difference Sets

Definition

G: group

$S \subset G$

S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and

Partial Difference Sets

Definition

G: group
$S \subset G$
S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and
- if $1 \neq g \in G$ and $g \notin S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly μ different ways.

Partial Difference Sets

Definition

G: group

$S \subset G$

S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and
- if $1 \neq g \in G$ and $g \notin S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly μ different ways.

S is called regular if $1 \notin S$ and $S = S^{-1}$.

Partial Difference Sets

Definition

G: group

$S \subset G$

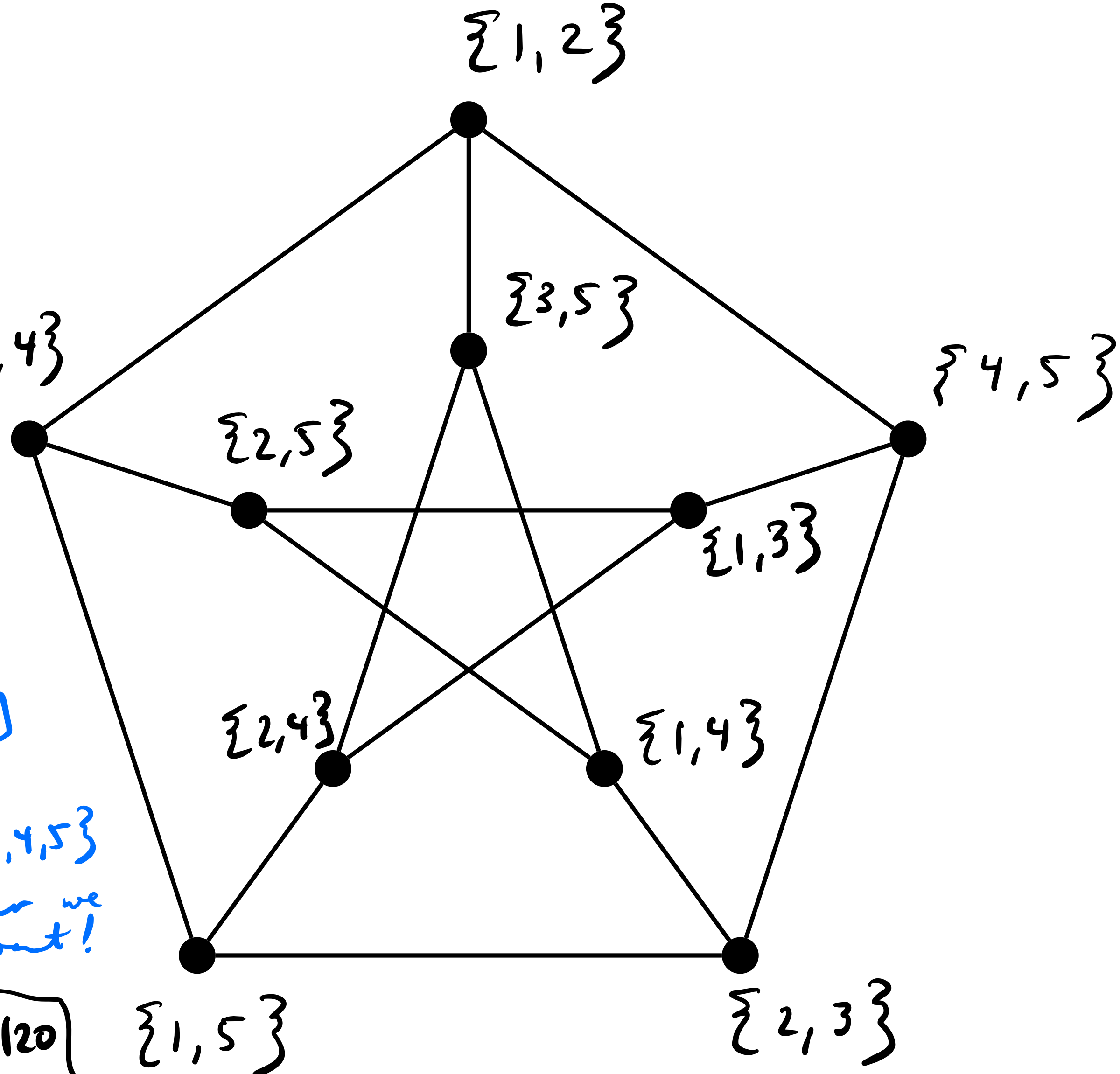
S is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and
- if $1 \neq g \in G$ and $g \notin S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly μ different ways.

S is called regular if $1 \notin S$ and $S = S^{-1}$.

S: regular (v, k, λ, μ)-PDS $\iff \mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG.

Petersen graph $\mathcal{P}$ $(10, 3, 0, 1)$



$\mathrm{Aut}(\mathcal{P}) \cong \underbrace{S_5}$

permute {1, 2, 3, 4, 5} however we want!

$\boxed{|\mathrm{Aut}(\mathcal{P})| = 5! = 120}$

Petersen graph is not a Cayley graph!

IDEA: Two groups w/ ten elements:

$(\mathbb{Z}/10, +)$, D_5

Similar here!

abelian, and so

$s, t \in S \Rightarrow s^{-1}, t^{-1} \in S$

$\underbrace{s^{-1} t^{-1} s t}_{\text{4-cycle}} = 1$

$\Rightarrow \Leftarrow$

Petersen not Cayley, cont.

A useful theorem

Theorem (De Winter, Kamischke, Wang (2016))

- $\mathrm{Cay}(G, S)$*: (v, k, λ, μ)-SRG*
- *(S: (v, k, λ, μ)-PDS)*

A useful theorem

Theorem (De Winter, Kamischke, Wang (2016))

- $\mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG
- (S: (v, k, λ, μ)-PDS)
- x: nonidentity element of G
- $d_1(x)$: number of vertices x sends to adjacent vertices

A useful theorem

Theorem (De Winter, Kamischke, Wang (2016))

- $\mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG
- (S: (v, k, λ, μ)-PDS)
- x: nonidentity element of G
- $d_1(x)$: number of vertices x sends to adjacent vertices
- $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$
- eigenvalues $k > \theta_1 > \theta_2$

A useful theorem

Theorem (De Winter, Kamischke, Wang (2016))

- $\mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG
- (S: (v, k, λ, μ)-PDS)
- x: nonidentity element of G
- $d_1(x)$: number of vertices x sends to adjacent vertices
- $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$
- eigenvalues $k > \theta_1 > \theta_2$

$$k - \theta_2 \equiv \mu - \theta_2(\theta_1 + 1) \equiv d_1(x) \pmod{\sqrt{\Delta}}$$

Some recent results

$x^G = \{g^{-1}xg : g \in G\}$

Theorem (S., Tauscheck (2021))

- S: (v, k, λ, μ)-PDS in group G
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$C_G(x) = \{y \in G : yx = xy\}$

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

In particular, if $\sqrt{\Delta}$ does not divide $\mu - \theta_2(\theta_1 + 1)$, then every nonidentity conjugacy class meets S.

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

In particular, if $\sqrt{\Delta}$ does not divide $\mu - \theta_2(\theta_1 + 1)$, then every nonidentity conjugacy class meets S.

Example

- Petersen graph: $(10, 3, 0, 1)$-SRG

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

In particular, if $\sqrt{\Delta}$ does not divide $\mu - \theta_2(\theta_1 + 1)$, then every nonidentity conjugacy class meets S.

Example

- Petersen graph: $(10, 3, 0, 1)$-SRG
- $\theta_1 = 1$, $\theta_2 = -2$, $\sqrt{\Delta} = 3$

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

In particular, if $\sqrt{\Delta}$ does not divide $\mu - \theta_2(\theta_1 + 1)$, then every nonidentity conjugacy class meets S.

Example

- Petersen graph: $(10, 3, 0, 1)$-SRG
- $\theta_1 = 1$, $\theta_2 = -2$, $\sqrt{\Delta} = 3$
- $3 \nmid 1 - (-2)(1 + 1)$: every nontrivial conjugacy class of group of order 10 would meet a $(10, 3, 0, 1)$-PDS (size 3)

Some recent results

Theorem (S., Tauscheck (2021))

- *S: (v, k, λ, μ)-PDS in group G*
- $\Phi(x) := |x^G \cap S||C_G(x)|$

$$\Phi(x) \equiv \mu - \theta_2(\theta_1 + 1) \pmod{\sqrt{\Delta}}$$

In particular, if $\sqrt{\Delta}$ does not divide $\mu - \theta_2(\theta_1 + 1)$, then every nonidentity conjugacy class meets S.

Example

- Petersen graph: $(10, 3, 0, 1)$-SRG
- $\theta_1 = 1$, $\theta_2 = -2$, $\sqrt{\Delta} = 3$
- $3 \nmid 1 - (-2)(1 + 1)$: every nontrivial conjugacy class of group of order 10 would meet a $(10, 3, 0, 1)$-PDS (size 3)
- C_{10}: 9 nontrivial classes, D_5: 4 nontrivial classes... not possible!

Some recent results, cont.

Corollary (S., Tauscheck (2021))

If $\sqrt{\Delta}$ divides neither $\mu - \theta_2(\theta_1 + 1)$ nor $v - 2k + \lambda - \theta_2(\theta_1 + 1)$, then a group with a nontrivial center cannot contain a (v, k, λ, μ)-PDS.

IDEA: Apply previous theorem to the graph *and* its complement!

Thank you!