Coherent configurations Lecture 1 Centralizer algebra of a permutation group

Mikhail Klin (Ben-Gurion University)

September 2025

Algebraic graph theory

- Algebraic graph theory (briefly AGT) deals with "highly symmetric" graphs.
- Symmetry of a graph Γ may be measured in terms of the group $Aut(\Gamma)$, combinatorial invariants of Γ, or the spectrum of the adjacency matrix $A(\Gamma)$ of Γ.
- Special attention to infinite families and sporadic examples of "nice graphs".

Algebraic graph theory

- The name AGT was coined by Norman Biggs in his seminal book (1974), second edition (1993).
- At least a dozen of other books, in particular by Bannai & Ito (1984), Brouwer-Cohen-Neumaier (1989), Cameron & van Lint (1991), Cameron (1999), Godsil & Royle (2001).

Algebraic graph theory

- In a wider framework there is a big intersection with a part of mathematics called "algebraic combinatorics".
- Nowadays AC tends to mean mainly results related to enumerative combinatorics (e.g. in the sense of Richard Stanley).

Algebraic graph theory

- In this first lecture we start with initial simple concepts related to finite permutation groups and their centralizer algebras.

Permutation groups

- A permutation group G of degree n is a subgroup of the symmetric group S_n (of all permutations of n points).
- Typically G is presented via a (compact) set of generators, for example

$$S_n = \langle (1, 2, \dots, n), (1, 2) \rangle.$$

- For us each permutation group appears as a symmetry group of "something".

Relational structures

- According to the spirit of Marc Krasner, we may rely on relational structures (sets of relations of arbitrary arity).
- One can speak of relational algebras.
- In simple cases, just one of a few considered relations.

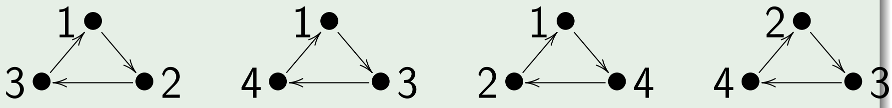
Example 1.1 (Alternating group A_4)

A_4 consists of all even permutations of $[1,4]$ and has order $\frac{1}{2} \cdot 4! = 12$.

- $A_4 = \{(), (2,3,4), (2,4,3), (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2), (1,4,3), (1,3)(2,4), (1,2)(3,4), (1,4)(2,3)\}$.
- $A_4 = \langle (1,2,3), (1,2,4) \rangle$.
- A_4 is 2-transitive (acts transitively on ordered pairs of distinct elements).

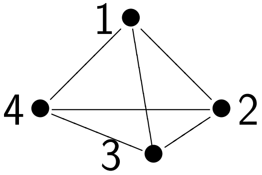
Example 1.1 (cont)

Relational structure $F = \{F_1, F_2, F_3, F_4\}$



F_1 F_2 F_3 F_4

- Clockwise orientation of the faces of the tetrahedron T:



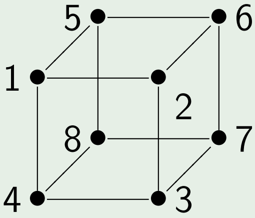
Arity

- Due to Example 1, A_4 has arity 3. This means that A_4 is the automorphism group of relation(s) of arity 3, while it is not the automorphism group of relation(s) of arity 2.
- Arity of a permutation group of degree n is a number in the range $[0, n-1]$.
- We are mainly interested in permutation groups of arity 2.

Graphs

- A (directed) graph $\Gamma = (V, R)$ consists of a set V of vertices and a set R of arcs.
- A color graph Γ is a collection of graphs on the same vertex set (we speak about colors of arcs).
- The automorphism group $Aut(\Gamma)$ of Γ consists of all automorphisms of Γ.
- An automorphism preserves each color in Γ.

Example 1.2 (3-dimensional cube Q_3)



$G = Aut(Q_3)$

- $|G| = 48$.
- $G = \langle (1,3)(5,7), (1,8)(2,7), (1,2)(3,4)(5,6)(7,8) \rangle$.
- $G \cong S_2 \times S_4$.
- As a permutation group: $G = S_2 \uparrow S_3$ (exponentiation of S_2 and S_3).

Example 1.3 (Regular elementary abelian group E_4)

$E_4 = \{e, (1,2)(3,4), (1,4)(2,3), (1,3)(2,4)\}$

- 

- $E_4 = Aut(\Gamma = \{\Gamma_1, \Gamma_2\})$.
- This is a color graph. A usual graph is not enough.

Adjacency matrices

- We use simultaneously adjacency matrices of graphs and permutation matrices.
- For a graph $\Gamma = ([1, n], R)$
  $A = A(\Gamma)$ is a square matrix of order n such that for the entry a_{ij} of A on the intersection of row i and column j

$$a_{ij} = \begin{cases} 0 & (i,j) \notin R, \\ 1 & (i,j) \in R. \end{cases}$$

Adjacency matrices

- Matrix A is symmetric

$$\Updownarrow$$

  Γ is an undirected graph.
- Let I be the identity matrix of order n; it is the adjacency matrix of a full reflexive graph (its arcs are all loops (i, i), $i \in [1, n]$).

Adjacency matrices

- For a permutation g, acting on the set $[1, n]$, we denote by $j = i^g$ the image j of i under the permutation g.
- To each permutation g we associate its (directed) graph $D(g)$ (diagram of G) with the arc set $\{(i, i^g) | i \in [1, n]\}$ and permutation matrix $M(g) = A(D(g))$.

Permutations

- Let us discuss a few convenient ways of representing permutations:
- In a two-row table associated with $g \in S(\Omega)$, all elements of Ω are presented in the first row with corresponding images in the second row, i.e.,

$$g = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1^g & 2^g & 3^g & \dots & n^g \end{pmatrix}.$$

Permutations

- The diagram $D(g)$ of g is a directed graph, the vertices of which are labeled by the elements of Ω with an arc drawn from each $x \in \Omega$ to its image x^g.

Permutations

- Let $\Omega = \{1, 2, \ldots, n\}$ and let $M(g)$ be the adjacency matrix of the diagram $D(g)$, i.e.,

$$M(g) = (m_{ij})_{1 \le i,j \le n}$$

where

$$m_{ij} = \begin{cases} 1 & \text{if} \quad j = i^g \\ 0 & \text{otherwise.} \end{cases}$$

The matrix $M(g)$ is called a permutation matrix. It has precisely one nonzero entry (equal to 1) in each row and column.

Permutations

- It is evident that $M(g^{-1}) = (M(g))^{-1} = (M(g))^t$, where M^t denotes the matrix transpose of M. The permutation matrix which corresponds to the identity permutation e on Ω is the unit matrix (or identity matrix) of order n, and is denoted by $M(e) = I_n$.

Permutations

- For each permutation $g \in S(\Omega)$ the diagram $D(g)$ is a union of disjoint oriented cycles. This enables us to encode each $g \in S(\Omega)$ by means of a cycle representation for g (equivalently, decomposition as a product of disjoint cycles).

Permutations

- Thus the diagram $D(g)$ will consist of l disjoint cycles of respective lengths $k_1, k_2, \dots, k_l$, and consequently its cycle representation will be

$$g = (a_1, a_2, \dots, a_{k_1})\,(b_1, b_2, \dots, b_{k_2}) \dots (u_1, u_2, \dots, u_{k_l}).$$

Example 1.4

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 5 & 9 & 6 & 2 & 7 & 4 & 8 & 10 \end{pmatrix}.$$

- We give three different cycle representations for g, the last of which is canonical:

$$\begin{aligned} g &= (5,6,2,1,3)(7)(9,8,4)(10) \\ &= (7)(10)(8,4,9)(2,1,3,5,6) \\ &= (1,3,5,6,2)(4,9,8). \end{aligned}$$

Example 1.4

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 5 & 9 & 6 & 2 & 7 & 4 & 8 & 10 \end{pmatrix}.$$

- The corresponding permutation matrix $M(g)$ is:

$$M(g) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Permutation groups

- Given a set G of permutations on a finite set Ω, the routine procedure for proving that G is a group is to check that it is closed under composition.

Example 1.3 (cont.)

- Let $\Omega = \{1, 2, 3, 4\}$, and $G = \{g_1, g_2, g_3, g_4\}$ where $g_1 = e,\ g_2 = (1, 2)(3, 4),\ g_3 = (1, 3)(2, 4),\ g_4 = (1, 4)(2, 3)$.
- Since $g_2 g_3 = g_3 g_2 = g_4,\ g_2 g_4 = g_4 g_2 = g_3,\ g_3 g_4 = g_4 g_3 = g_2,\ g_1^2 = g_2^2 = g_3^2 = g_4^2 = e$, the set G is seen to be closed under composition. Hence (G, Ω) is a permutation group.

Example 1.5

- Let $\Omega = \{1,2,3,4\}$, and let G consist of all permutations from $S(\Omega)$ which preserve the partition $\{\{1,2\},\{3,4\}\}$ of Ω (i.e., for all $g \in G$ either $\{1^g, 2^g\} = \{1,2\}$ or $\{1^g, 2^g\} = \{3,4\}$).
- Then one can assert, without any specific determination of the elements of G, that (G, Ω) is a permutation group.

Example 1.5 (cont.)

- In fact, as the reader can easily verify, $G = \{e,\ (1,2),\ (3,4),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3),\ (1,3,2,4),\ (1,4,2,3)\}$.

Stabilizers

- Let (G, Ω) be a permutation group, and let $X = \{x_1, x_2, \ldots, x_k\}$ be a subset of Ω.
- We define

$$G_{x_1,\ldots,x_k} := \{g \in G \mid \forall i : x_i^g = x_i\},$$

$$G_X = G_{\{x_1,\ldots,x_k\}} := \{g \in G \mid X^g = X\},$$

where $X^g = \{x_1^g, x_2^g, \ldots, x_k^g\}$.

Stabilizers

- Again it is easy to see that $G_{x_1,\dots,x_k}$ and $G_{\{x_1,\dots,x_k\}}$ are subgroups of G which are called the pointwise stabilizer of X in G and the setwise stabilizer of X in G, respectively. (If $X = \{x\}$, the notions of G_x and $G_{\{x\}}$ coincide and only the first notation will be used.)

Orbits

- We say $x, y \in \Omega$ belong to the same orbit of the permutation group (G, Ω) if $y = x^g$ for some $g \in G$.
- Obviously, the set of all distinct orbits of (G, Ω) forms a partition of Ω, i.e., different orbits have empty intersection and the union of all orbits is equal to Ω.

Transitive groups

- The number $|\mathcal{O}|$ of elements which belong to an orbit $\mathcal{O}$ is called its length.
- A permutation group (G, Ω) is called transitive if Ω is its only orbit, otherwise it is intransitive.

Proposition 1.1 (Reformulation of Lagrange's theorem)

Let (G, Ω) be a permutation group, and for each $x \in \Omega$, let $\mathcal{O}(x)$ denote the orbit of (G, Ω) which contains x. Then
$|\mathcal{O}(x)| = [G : G_x]$, and consequently
$|G| = |G_x| \cdot |\mathcal{O}(x)|$.
In particular, the length of each orbit divides the order of the group.

Proof

Consider the partition of G into right cosets with respect to the stabilizer G_x of x. These cosets are clearly in one-to-one correspondence with the elements of $\mathcal{O}(x)$; indeed, the coset $G_x g$ consists of those and only those permutations of G which map x to x^g. The result follows.

- Proposition 1.1 is commonly called the Orbit-Stabilizer Theorem.

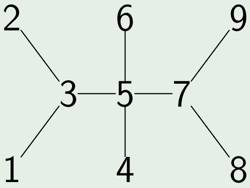
Induced action on Ω^2

- Let $g \in S(\Omega)$. The action of g on Ω can be extended to an induced action of g on Ω^2 by defining $(a, b)^g := (a^g, b^g)$ for each $(a, b) \in \Omega^2$.
- A subset $R \subset \Omega^2$ is called a binary relation on Ω. For any binary relation R on Ω and element $g \in S(\Omega)$, we define $R^g = \{(x, y)^g \mid (x, y) \in R\}$.

Invariant relations

- In general $R^g \neq R$.
- If $R^g = R$ we say g preserves R or, equivalently, that R is invariant with respect to g.
- Likewise, if $R^g = R$ for every $g \in (G, \Omega)$ then we say (G, Ω) preserves R or that R is invariant with respect to (G, Ω).

Example 1.6



- Consider the undirected graph $\Gamma = (\Omega, R)$ with vertex set $\Omega = \{1, 2, \ldots, 9\}$ and edges as depicted.
- Set $G = \mathrm{Aut}(\Gamma)$.
- We prove $|G| = 16$ by successively applying Proposition 1.1.

Example 1.6 (cont.)

- First, it is visually evident that the orbits of (G, Ω) are given by:

$$\{1, 2, 8, 9\}, \ \{3, 7\}, \ \{4, 6\}, \ \{5\}.$$

- Thus a first application of Proposition 1.1 gives $|G| = |\mathcal{O}(1)| \cdot |G_1| = 4 \cdot |G_1|$.
- Now, letting $\mathcal{O}_{G_1}(8)$ denote the orbit containing 8 under the action of (G_1, Ω), we get $|G_1| = |\mathcal{O}_{G_1}(8)| \cdot |G_{1,8}| = 2 \cdot |G_{1,8}|$.

Example 1.6 (cont.)

- One further application of 1.1, together with the observation that $G_{1,8,4} = \{e\}$, gives

$$|G_{1,8}| = |Orb_{G_{1,8}}(4)| \cdot |G_{1,8,4}| = 2 \cdot |G_{1,8,4}| = 2.$$

- So:

$$|G| = 4 \cdot 2 \cdot 2 = 16.$$

Proposition 1.2

Let $\Gamma = (\Omega, R)$ *be a graph. For* $g \in S(\Omega)$, *denote by* Γ^g *its isomorphic image* $\Gamma^g = (\Omega, R^g)$ *under* g. *Then*

$$A(\Gamma^g) = M(g)^{-1} A(\Gamma) M(g),$$

where $A(\Gamma)$ *and* $A(\Gamma^g)$ *are the respective adjacency matrices for* Γ *and* Γ^g *and* $M(g)$ *is the permutation matrix associated with* g.

Proposition 1.2

In particular $g \in \mathrm{Aut}(\Gamma)$ *if and only if*

$$M(g)^{-1}A(\Gamma)M(g) = A(\Gamma)$$

or, equivalently,

$$A(\Gamma)M(g) = M(g)A(\Gamma).$$

In words, the permutation g *is an automorphism of* Γ *if and only if* $A(\Gamma)$ *commutes with* $M(g)$.

Proof

- Let E_{ij} be the matrix of order $n = |\Omega|$ in which the (i, j)-entry is equal to 1 and all other entries are equal to 0.
- Clearly,
$$A(\Gamma) = \sum_{(i,j)\in R} E_{ij}.$$
- Setting $k = i^g$ and $l = j^g$, it is easy to see that $M(g)^{-1}E_{ij} = M(g^{-1})E_{ij} = E_{kj}$ and $E_{kj}M(g) = E_{kl}$.

Proof

- Thus, we have

$$M(g)^{-1}E_{ij}M(g) = E_{kl}.$$

- But then

$$M(g)^{-1}A(\Gamma)M(g) = M(g)^{-1}\Big(\sum_{(i,j)\in R} E_{ij}\Big)M(g) = \sum_{(i,j)\in R} M(g)^{-1}E_{ij}M(g) = \sum_{(i,j)\in R} E_{i^g j^g} = A(\Gamma^g).$$

Centralizer algebra

- Proposition 1.2 motivates us to define the centralizer ring and centralizer algebra of a permutation group.
- In what follows $\mathbb{Z}$ will denote the ring of integers, $\mathbb{C}$ the field of complex numbers, and $M_n(K)$ the set of order n matrices with values from K.

Centralizer algebra

- The centralizer ring of the permutation group (G, Ω) is the ring of all integer-valued matrices which commute with every permutation matrix $M(g)$, $g \in G$, i.e., $\mathcal{V}_{\mathbb{Z}}(G, \Omega) = \{A \in M_n(\mathbb{Z}) \mid AM(g) = M(g)A \;\; \forall g \in (G, \Omega)\}$.

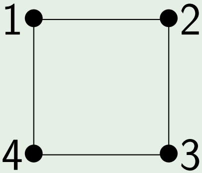
Centralizer algebra

- Analogously, replacing integer-valued matrices by complex-valued matrices, we obtain the definition for the centralizer algebra of (G, Ω):
  $\mathcal{V}_{\mathbb{C}}(G, \Omega) = \{A \in M_n(\mathbb{C}) \mid AM(g) = M(g)A \ \ \forall g \in (G, \Omega)\}$.

Centralizer algebra

- When there is no risk of confusion, or when the distinction is not considered to be crucial, we shall express each of $\mathcal{V}_{\mathbb{Z}}(G, \Omega)$ and $\mathcal{V}_{\mathbb{C}}(G, \Omega)$ simply as $\mathcal{V}(G, \Omega)$.

Example 1.7 (Cycle C_4)



- $Aut(C_4) = D_4$, dihedral group of order 8.
- $D_4 = \langle (1,2,3,4), (1,3) \rangle$.
- $$\underset{A(\Gamma)}{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}} \quad \underset{M((1,2,3,4))}{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}} \quad \underset{M((1,3))}{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}$$

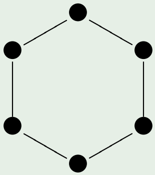
Centralizer algebra

- Start from a permutation group (G, Ω) of degree n.
- Consider it as a group of permutation matrices.
- Find its centralizer V in the algebra $M_n(F)$ of matrices of order n.
- $V = V(G, \Omega)$ is called the centralizer algebra of (G, Ω).
- The name was coined by Issai Schur.

Centralizer algebra

- $V(G, \Omega)$ has (as a vector space) a special basis, which consists of $(0, 1)$-matrices.
- These matrices can be regarded as adjacency matrices of graphs with n vertices.
- V is the same as full color graph.
- In addition, we get structure constants of the algebra V.

Example 1.8 (Cycle C_6)

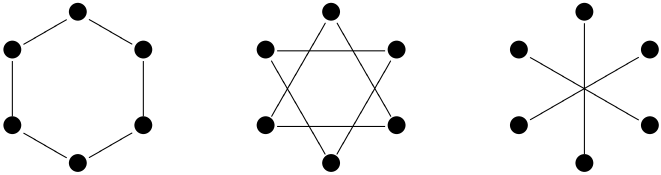


- $Aut(C_6) = D_6$, dihedral group of order 12.
- $V(D_6)$ has dimension (rank) 4.
- Basic matrices:

$$\begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&1\\ 1&0&1&0&0&0\\ 0&1&0&1&0&0\\ 0&0&1&0&1&0\\ 0&0&0&1&0&1\\ 1&0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1&0\\ 0&0&0&1&0&1\\ 1&0&0&0&1&0\\ 0&1&0&0&0&1\\ 1&0&1&0&0&0\\ 0&1&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0 \end{pmatrix}$$

Example 1.8 (cont.)

- Corresponding graphs:



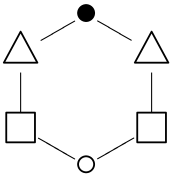
Γ_1 Γ_2 Γ_3

- intersection matrices:

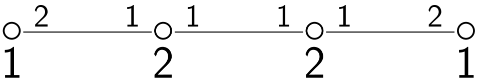
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Example 1.8 (cont.)

- Distance decomposition:



- Intersection diagram:



Intersection algebra

- Matrix algebra $V(G, \Omega)$ consists of matrices of order n.
- Intersection algebra $P(G, \Omega)$ consists of matrices of order r.

Intersection algebra

Theorem 1.1

Algebras $V(G, \Omega)$ and $P(G, \Omega)$ are isomorphic as matrix algebras.

- In Example 1.8, $n = 6$, $r = 4$.
- Typically, the difference is more essential.

Proof outline

- See theorem 3.4 of Cameron's book.
- A helpful identity for intersection numbers.
- Proof of the identity (combinatorial or algebraic).
- Combinatorial hints.
- This is really isomorphism.

Historical comments

- Bose & Mesner (1959) in particular case.
- Tradition to attribute general result to H. Wielandt.
- (Discussion at the evening.)

Main references

P.J. Cameron, "Permutation Groups," London Mathematical Society Student Texts, 45, Cambridge University Press, Cambridge, 1999.

Thank You!