Regular permutation groups

and Cayley graphs

Cheryl E Praeger

University of Western Australia

Permutation groups

Permutation :	of set Ω, bijection $g : \Omega \to \Omega$
Symmetric	group of all permutations of Ω
group $\mathrm{Sym}(\Omega)$**:**	under composition, for example
	$g = (1,2)$ followed by $h = (2,3)$ yields $gh = (1,3,2)$
	$g = (1,2,3)$ has inverse $g^{-1} = (3,2,1) = (1,3,2)$
Permutation	$G \leq \mathrm{Sym}(\Omega)$, that is, subset
group on Ω**:**	closed under inverses and products (compositions)
Example:	$G = \langle(0,1,2,3,4)\rangle < \mathrm{Sym}(\Omega)$ on $\Omega = \{0,1,2,3,4\}$

Interesting permutation groups occur in:

Graph Theory: Automorphism groups (edge-preserving perm's)

Geometry: Collineations (line-preserving permutations)

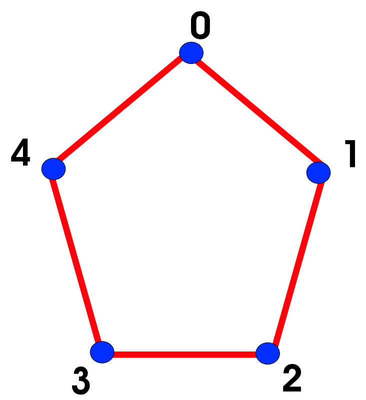
Number Theory and Cryptography: Galois groups, elliptic curves

Differential equations: Measure symmetry - affects nature of solutions

Many applications: basic measure of symmetry

Regular permutation groups

Permutation group:	$G \leq \mathrm{Sym}(\Omega)$
G transitive:	all points of Ω equivalent under elements of G
G regular:	'smallest possible transitive' that is only the identity element of G fixes a point
Example:	$G = \langle(0,1,2,3,4)\rangle$ on $\Omega = \{0,1,2,3,4\}$
Alternative view:	$G = \mathbb{Z}_5$ on $\Omega = \{0,1,2,3,4\}$ by addition



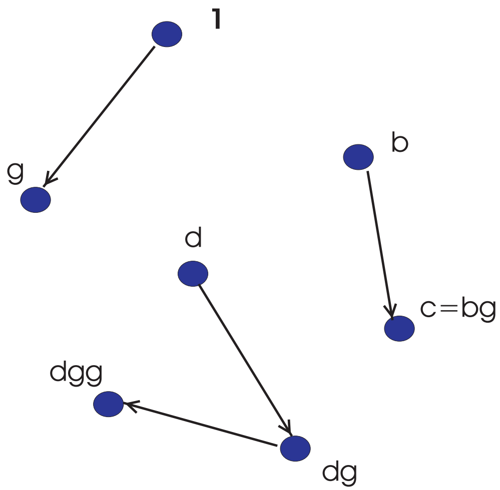
View of regular permutation groups

Take any: group G, set $\Omega := G$

Define action: $\rho_g : x \rightarrow xg$ for $g \in G, x \in \Omega$ (ρ_g is bijection)

Form permutation group: $G_R = \{\rho_g | g \in G\} \leq \text{Sym}(\Omega)$

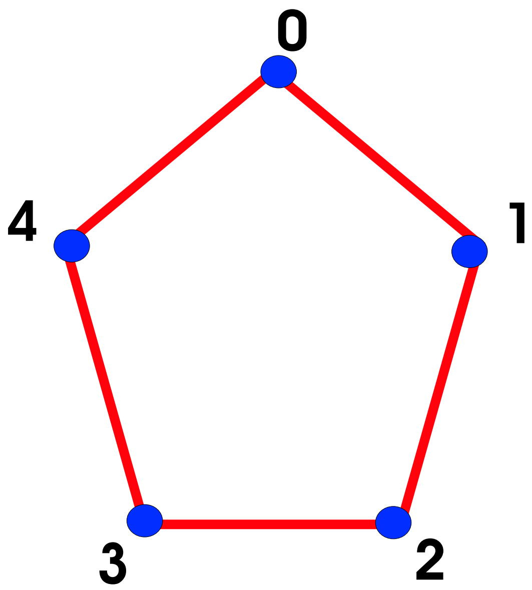
$G_R \cong G$ and G_R **is regular**



Visualise regular permutation groups as graphs

Given generating set S: $G = \langle S \rangle$ with $s \in S \iff s^{-1} \in S$
Define graph: vertex set $\Omega = G$, edges $\{g, sg\}$ for $g \in G, s \in S$

Example: $G = \mathbb{Z}_5$, $S = \{1, 4\}$, obtain $\Gamma = C_5$, $\mathrm{Aut}\,(\Gamma) = D_{10}$.



These are the Cayley graphs $\Gamma = \mathrm{Cay}(G, S)$

Always: $G_R \leq \mathrm{Aut}(\Gamma)$, so Cayley graphs are always vertex-transitive

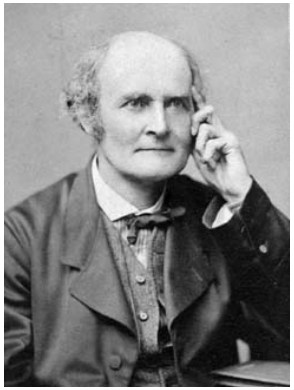
Why important: in combinatorics, statistical designs, computation

Circulant graphs: used in experimental layouts for statistical experiments, and for many constructions in combinatorics

Expander graphs: almost all regular graphs are expanders, but "explicit constructions very difficult"; Ramanujan graphs are Cayley graphs (Lubotzky-Phillips-Sarnak 1988)

Random selection in group computation: modelled and analysed as random walks on Cayley graphs

Arthur Cayley 1821-1895



'As for everything else, so for a mathematical theory: beauty can be perceived but not explained.'

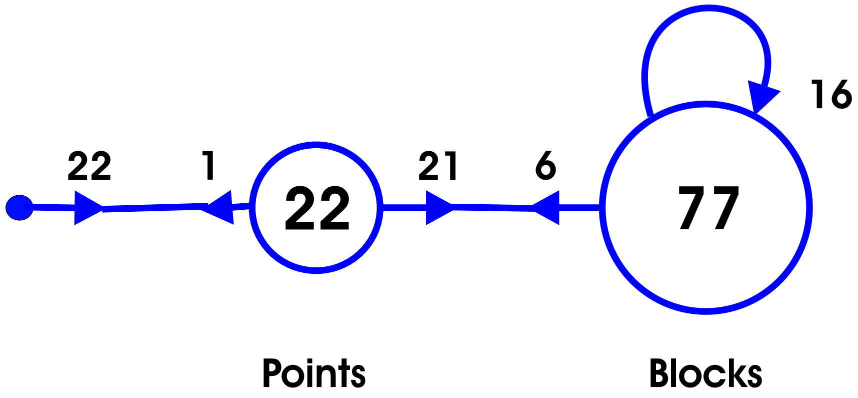
1849	admitted to the bar; 14 years as lawyer
1863	Sadleirian Professor (Pure Maths) Cambridge
Published	900 mathematical papers and notes
Matrices	led to Quantum mechanics (Heisenburg)
Also	geometry, group theory

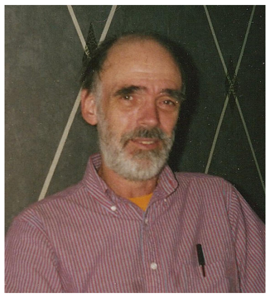
Still to come!

* Recognition problem
* Primitive Cayley graphs
* B-groups
* Burnside, Schur and Wielandt
* Exact group factorisations
* Use of finite simple groups

A recognition problem

Higman Sims graph $\Gamma = \Gamma(HS)$: 100 vertices, valency 22, $A :=$ Aut $(\Gamma) =$ HS.2 Related to Steiner system $S(3,6,22)$; $A_\alpha = M_{22}.2$.





Lead to discovery of: HS by D. G. Higman and C. C. Sims in 1967

Not obvious: $\Gamma(HS) = \mathrm{Cay}(G, S)$ for $G = (Z_5 \times Z_5)$: [4]

Recognising Cayley graphs

Aut(Γ)**:** may be much larger than G_R for $\Gamma = \mathrm{Cay}(G, S)$
Some constructions: may hide the fact that Γ is a Cayley graph.
Question: How to decide if a given (vertex-transitive) graph Γ is a Cayley graph?

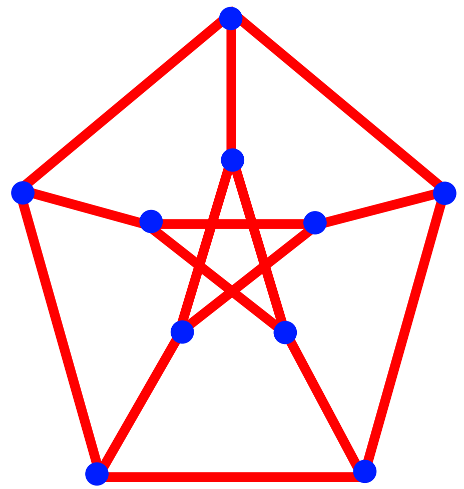
Characterisation: Γ is a Cayley graph $\iff \exists\ R \leq \mathrm{Aut}(\Gamma)$, with R regular on vertices.

In this case: $\Gamma \cong \mathrm{Cay}(R, S)$ for some S.

Not all vertex-trans graphs are Cayley, but ...

Petersen graph P is vertex-transitive and non-Cayley:
Check criterion: $\mathrm{Aut}\,(\Gamma) = S_5$. All involutions (elements of order 2) fix a vertex.

Any regular subgroup would have order 10 (even) so would contain involution fixing a vertex contradiction



Answer: first determine Aut (Γ); then search for R.
Both difficult problems in general!

Do we really care?: Cayley graphs seem 'common' among vertex-transitive graphs.

e.g. There are 15,506 vertex-transitive graphs with 24 vertices
Of these, 15,394 are Cayley graphs (Gordon Royle, 1987)

McKay-Praeger Conjecture: (empirically based) As $n \to \infty$

$$\frac{\text{Number of Cayley graphs on} \leq n \text{ vertices}}{\text{Number of vertex-transitive graphs on} \leq n \text{ vertices}} \longrightarrow 1$$

Various proposals regarding vertex-transitive/Cayley graph question

'Non-Cayley Project': For some n, all vertex-transitive graphs on n vertices are Cayley. Determine all such n. (Dragan Marušic)

Study 'normal Cayley graphs': that is, $G_R \lhd \mathrm{Aut}\,(\mathrm{Cay}(G,S))$ (Ming Yao Xu)

Study 'primitive Cayley graphs': that is, $\mathrm{Aut}\,(\mathrm{Cay}(G,S))$ vertex-primitive (only invariant vertex-partitions are trivial);
Note each $H < G$: gives G_R-invariant vertex-partition into H-cosets; for each H need extra autos **not preserving** the H-coset partition.

We will follow the last one in this lecture.

Primitive Cayley graphs

Given: $\Gamma = \text{Cay}(G, S)$, when is $\text{Aut}\,(\Gamma)$ vertex primitive?

Generic example: If $S = G\backslash\{1\}$ then $\Gamma = \text{Cay}(G, S)$ is the complete graph K_n, where $n = |G|$ and $\text{Aut}\,(\Gamma) = \text{Sym}\,(G) \cong S_n$ (and hence primitive)

Higman-Sims graph HS: is a primitive Cayley graph

William Burnside 1852-1927

1897: published *The Theory of Groups of Finite Order*, first treatise on group theory in English.

'Burnside 1911': If $G = Z_{p^m}$, p prime and $m \geq 2$, then the only primitive Cay(G, S) is complete graph K_{p^m}.

‘Burnside 1911’: If $G = Z_{p^m}$, p prime and $m \geq 2$, then the only primitive Cay(G, S) is complete graph K_{p^m}.

Burnside’s real result was

Burnside 1911: If $G = Z_{p^m}$, p prime and $m \geq 2$, then the only primitive groups H such that $G_R < H \leq S_{p^m}$ are 2-transitive.

[2-transitive means all ordered point-pairs equivalent under the group]

Work inspired by Burnside's result

Schur 1933: $G = Z_n$, n not prime, then the only primitive Cay(G, S) is complete graph K_n.

Issai Schur 1875-1941

Led to: Schur's theory of S-rings (Wielandt School); coherant configurations (D. G. Higman), and centraliser algebras and Hecke algebras.

Burnside 1921: had tried to prove same result for G abelian but not elementary abelian; error pointed out by Dorothy Manning 1936

Wielandt 1935: G abelian, $n = |G|$ not prime, at least one cyclic Sylow subgroup $\Rightarrow$ only primitive Cay(G, S) is complete graph K_n.

Wielandt 1950: Same result holds if G dihedral group (first infinite family of non-abelian such groups)

Wielandt 1955: Call a group G of order n a B-group if
Cay(G, S) primitive $\Rightarrow$ Cay$(G, S) = K_n$

Thus: Many abelian groups, certainly most cyclic groups and all dihedral groups are B-groups

Helmut Wielandt 1910-2001

1964: published influential book
Finite Permutation Groups

'It is to one of Schur's seminars that I owe the stimulus to work with permutation groups, my first research area. At that time the theory had nearly died out. . . . so completely superseded by the more generally applicable theory of abstract groups that by 1930 even important results were practically forgotten - to my mind unjustly.'

Back to Wielandt's theory of B-groups:

When proposed 1960's, 1970's: focus on the potential B-group; much interest in 2-transitive groups

Other work by Bercov, W. R. Scott, Enomote, Kanazawa in 1960's

Recent work: uses classification of the finite simple groups (FSGC) (e.g. all finite 2-transitive groups now known)

Focuses on pair (G, H): $G < H \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(\Omega)$ with G regular, H primitive, $\Gamma = \mathrm{Cay}(G, S)$

Aim to understand: primitive groups H; primitive Cayley graphs Γ, other applications (e.g. constructing semisimple Hopf algebras)

A group-theoretic factorisation problem

Wielandt condition: $G < H \leq \mathsf{Aut}(\Gamma) \leq \mathsf{Sym}(\Omega)$ with G regular, H primitive, and $\Gamma = \mathsf{Cay}(G, S)$

Equivalent to: for $\alpha \in \Omega$, $K := G_\alpha$ (stabiliser)

$$H = GK \text{ and } G \cap K = 1 \quad \text{(an exact factorisation of } H\text{)}$$

With: K maximal subgroup of H

Problem: Find all exact factorisations $H = GK$ with K maximal

Problem not new, but new methods available to attack it.

An example

G. A. Miller 1935: for $H = A_n$ (alternating group) gave examples of exact factorisations $H = GK$, and gave examples of n for which the only exact factorisations have $K = A_{n-1}$

George Abram Miller 1863-1951

Wiegold & Williamson 1980: classified all exact factorisations $H = GK$ with $H \cong A_n$ or S_n

A fascinating density result

Cameron, Neumann, Teague 1982: for 'almost all n', the only primitive groups on $\Omega = \{1, \ldots, n\}$ are A_n and $S_n = \mathrm{Sym}\,(\Omega)$.

Technically: If $N(x)$:= Number of $n \leq x$ where $\exists\ G < H \neq A_n, S_n$ with G regular, H primitive, then $\frac{N(x)}{x} \to 1$ as $x \to \infty$

Immediate consequence: for 'almost all n', every group G of order n is a B-group (we want those groups G that are **not** B groups)

Types of primitive groups H

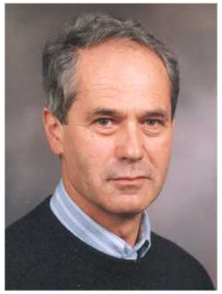
Results of Liebeck, Praeger, Saxl 2000: $G < H \neq A_n, S_n$ with G regular, H primitive $\Rightarrow$ one of

(1) H diagonal, or twisted wreath, or affine type
[here there always exists regular subgroup G]

(2) H almost simple ($T \leq H \leq \text{Aut}\,(T)$, T simple)

(3) H product action

Comments: (2) (resolved by LPS, 2007+) and (3) (still open);



$G < H \neq A_n, S_n$ with G regular, H primitive

G. A. Jones 2002: found all H with G cyclic

Cai Heng Li, 2003, 2007: found all H with G abelian or dihedral

Li & Seress, 2005: found all H if n squarefree and $G \subseteq \mathrm{Soc}(H)$.

Giudici, 2007: found all H, G if H sporadic almost simple

Baumeister, 2006, 2007: found all H, G, with H sporadic, or exceptional Lie type, or unitary or $O_8^+(q)$

Major open case: H almost simple classical group
(the heart of the problem)

$G < H < \mathrm{Sym}\,(\Omega)$, H classical, G regular

Principal tool: LPS 1990 classification of 'maximal factorisations' $H = AK$ of almost simple groups H, both A and K maximal

Implies: All (H, A, K) known such that (possibly) $G \le A <_{\mathrm{max}} H$

Then comes: a lot of hard work

Example: Hering's Theorem gives list of possible A, G for one class of maximal subgroups K in one class of classical groups H (1-space stabilisers in linear groups); we check list. Find examples $G \le \Gamma\mathrm{L}(1, q^d)$ (metacyclic)

LPS 2007+ approach

Series of theorems: for each type of classical group (PSL, PSp, PSU, PΩ^{ε}), classifying possibilities for transitive subgroups on various kinds of subspaces

Basic strategy: Must consider all possible ordered triples (H, A, K) where there exists maximal factorisation $H = AK$.
Seek $G \leq A$ such that $H = GK$ and $G \cap K = 1$.

Factorisation 'propagates': $A = (A \cap K)G$ and $(A \cap K) \cap G = 1$ (smaller exact factorisation)

LPS 2007+ Results

Main Theorem: Complete lists of all primitive actions of almost simple classical groups H, and lists of subgroups G such that G is regular

What does it teach us?: tight explicit restrictions on regular subgroups G of almost simple primitive groups $H \neq A_n, S_n$

1: $|\Omega| > 3 \times 29! \sim 2.65 \times 10^{31} \Rightarrow G$ one of
metacyclic, $|G| = (q^d - 1)/(q - 1)$
or subgroup of $\mathrm{A\Gamma L}(1, q)$, $|G| = q(q-1)/2$ odd
or $A_{p-1}, S_{p-1}, A_{p-2} \times Z_2$ for prime $p \equiv 1 \pmod 4$,
or A_{p^2-2} for prime $p \equiv 3 \pmod 4$
where q is a prime power, and p is prime [Compare with CNT result]

Almost simple groups as B-groups

Complete information about almost simple groups G: when they are B-groups, and if not, what primitive groups contain them as regular subgroups.

2: Suppose G is almost simple. Then G is a B-group $\iff$ G not simple, and $G \neq S_{p-2}$ (p prime), PSL$(2, 16)$.4, PSL$(3, 4)$.2

3: Suppose G is simple or one of S_{p-2}, PSL$(2, 16)$.4, PSL$(3, 4)$.2 If $G < H < \mathrm{Sym}\,(\Omega)$ with H primitive, G regular, then either $G \times G \leq H \leq \mathrm{Hol}(G).2$ with G simple, or H in explicit short list.

What does it teach us about primitive Cayley graphs?

Case of G simple: two types of primitive Cayley graphs $\Gamma = \mathrm{Cay}(G, S)$

(1)	$S = G \setminus \{1\}$	$\mathrm{Aut}(\Gamma) = \mathrm{Sym}(G)$
(2)	$S =$ union of G-conjugacy classes	$\mathrm{Aut}(\Gamma) \geq G \times G$

LPS: G simple and $\Gamma = \mathrm{Cay}(G, S)$ vertex-primitive $\Rightarrow$
(1) or (2) or $G = A_{p^2-2}$ for prime $p \equiv 3 \pmod 4$

In last case there are examples for each p

What else did we notice: coincidences

Seven: primitive groups of degree 120 share a common regular subgroup (namely S_5). Lattice of containments among these groups shown below.

$$
\begin{array}{ccccccc}
 & & & Sp_8(2) & & & \\
 & & \nearrow & & \nwarrow & & \\
 & Sp_4(4).2 & & & & O_8^+(2) & \\
 & & & & \nearrow & & \nwarrow \\
 & & & A_9 & & & & Sp_6(2) \\
 & & \nearrow & & & & \nearrow & \\
 & S_7 & & & & S_8 & &
\end{array}
$$

Classified: all instances where G contained in more than one almost simple primitive group

Some remaining open problems

1: Get a better understanding of which primitive product action groups contain regular subgroups

In particular: Are there product action examples not arising from an almost simple example?

2: Determine (non) B-groups among wider class of groups

3: Study the primitive Cayley graphs that arise.

4: Determine the kinds of regular subgroups that may exist in affine primitive groups, apart from the translation subgroup. (Some exist, Hegedüs 2000)