Regular permutation groups

and Cayley graphs

Cheryl E Praeger

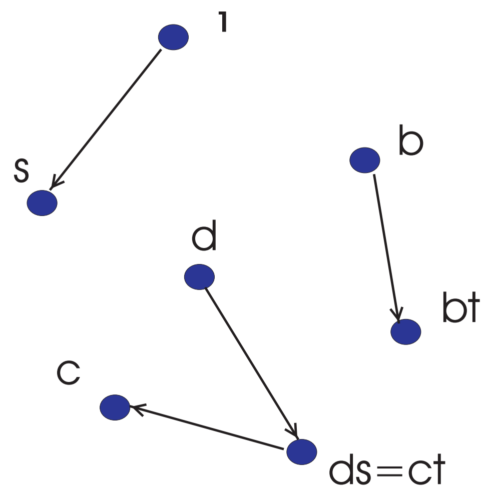
University of Western Australia

What are Cayley graphs?

Group : G with generating set $S = \{s, t, u, \ldots\}$

Group elements: 'words in S' $stu^{-1}s$ etc

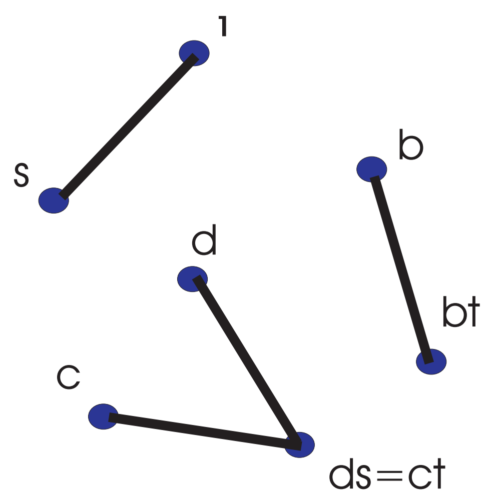
Cayley graph: Cay(G, S) vertices: group elements; edges: multiplication from S



What are Cayley graphs?

If S inverse closed: $s \in S \iff s^{-1} \in S$

Cayley graph Cay(G,S)**:** may use undirected edges



Some reasonable questions

Where: do they arise in mathematics today?

Where: did they originate?

What: kinds of groups G give interesting Cayley graphs Cay(G, S)?

Which graphs: arise as Cayley graphs?

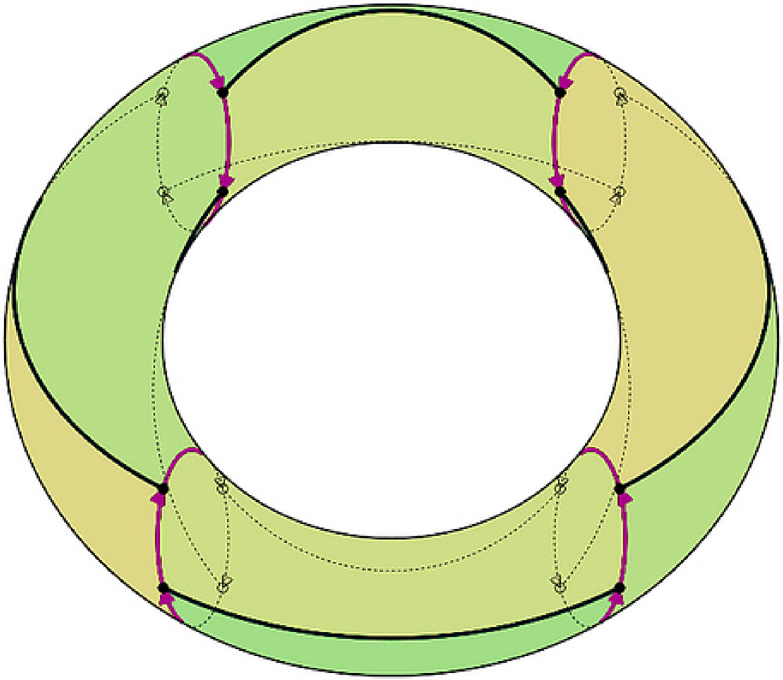
Does it matter: what S we choose?

Are: Cayley graphs important and why?

And: what about **regular permutation groups?**

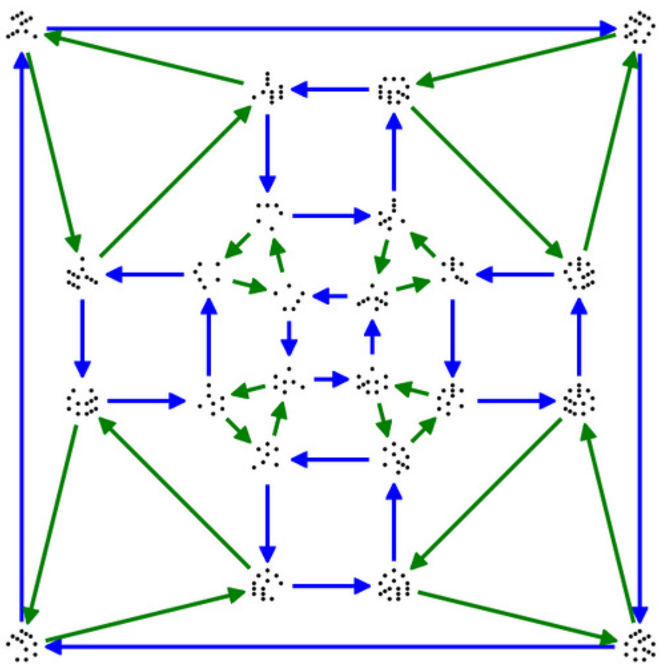
Let's see how I go with answers!

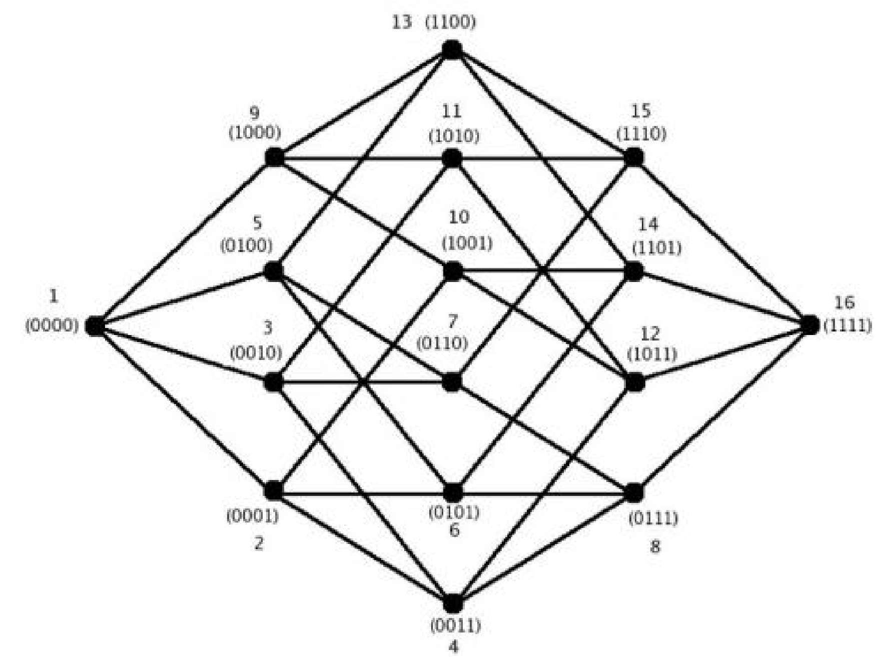
In Topology: Embedding maps in surfaces



Thanks to Ethan Hein: flickr.com

Computer networks; experimental layouts (statistics)





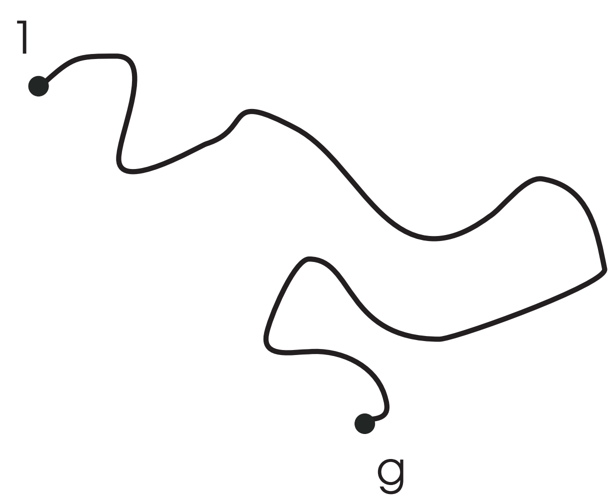
Thanks to Ethan Hein: flickr.com and Jason Twamley

Random walks on Cayley graphs

Applications: from percolation theory to group computation

How large n: g 'approximately random' in G? Independence?

Method: for random selection in groups – underpins randomised algorithms for group computation (Babai, 1991)



Fundamental importance for group actions in combinatorics and geometry

I will describe:

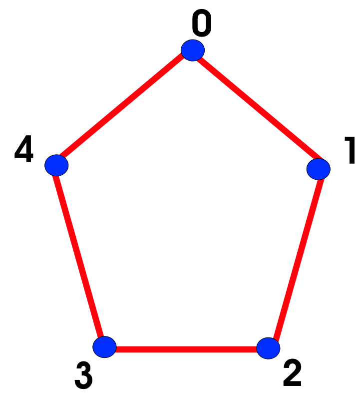
Regular permutation groups
Origins of Cayley graphs
Links with group theory
Some recent work and open problems
on primitive Cayley graphs

Permutation groups

Permutation :	of set Ω, bijection $g : \Omega \to \Omega$
Symmetric group Sym (Ω)**:**	group of all permutations of Ω 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 group on Ω**:**	$G \leq \mathrm{Sym}\,(\Omega)$, that is, subset closed under inverses and products (compositions)
Example:	$G = \langle (0,1,2,3,4) \rangle < \mathrm{Sym}\,(\Omega)$ on $\Omega = \{0,1,2,3,4\}$

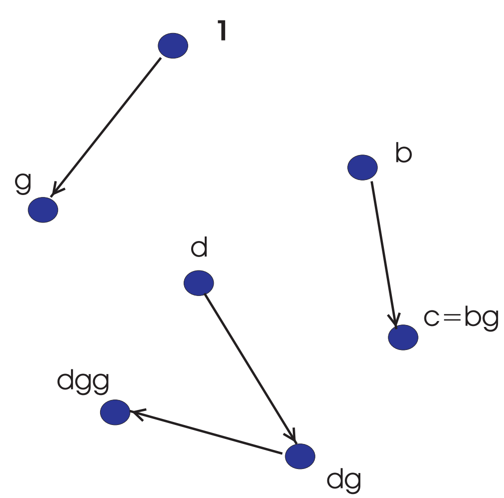
Regular permutation groups

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



To obtain a typical regular permutation group

Take any: group G, set $\Omega := G$
Define action: $\rho_g : x \to xg$ for $g \in G, x \in \Omega$ (ρ_g is bijection)
Form permutation group: $G_R = \{\rho_g | g \in G\} \leq \mathrm{Sym}(\Omega)$
$G_R \cong G$ and G_R **is regular**



Regular perm. groups ‘equal’ Cayley graphs!

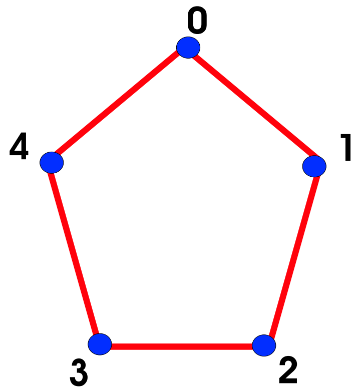
Given generating set S: $G = \langle S \rangle$ with $s \in S \iff s^{-1} \in S$

Define graph: vertex set $\Omega = G$, edges $\{g, sg\}$ for $g \in G, s \in S$

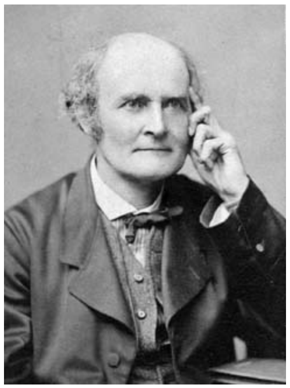
Cayley graph: $\Gamma = \mathrm{Cay}(G, S)$

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

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



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

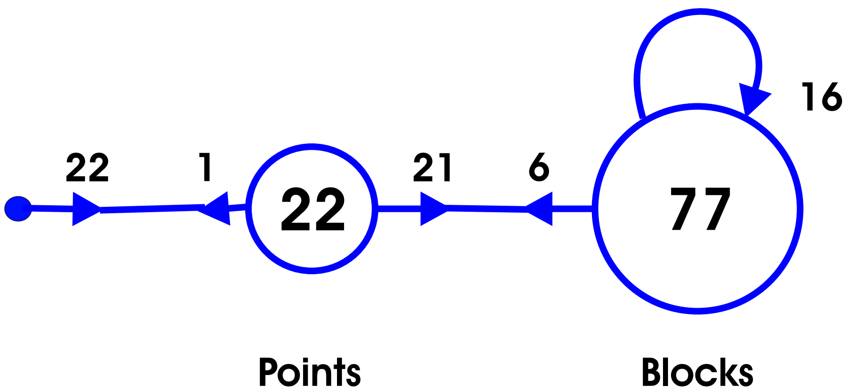
Still to come!

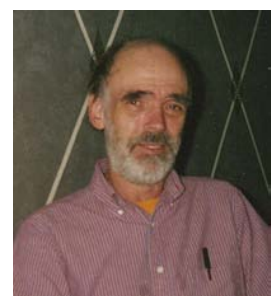
* Recognition problem
* Primitive Cayley graphs
* B-groups
* Burnside, Schur and Wielandt
* Exact group factorisations
* Use of finite simple groups

Slightly anachronistic – I use language of Cayley graphs

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: $\Gamma(HS) = \text{Cay}(G, S)$ for $G = (Z_5 \times Z_5) : [4]$

Recognising Cayley graphs

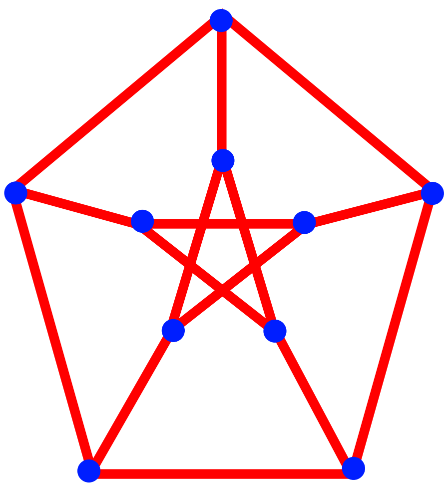
Aut (Γ)**:** may be much larger than G_R for $\Gamma = \text{Cay}(G, S)$
Some constructions: may hide the fact that Γ is a Cayley graph.
Question: How to decide if a given (vertex-transitive) graph Γ is a Cayley graph?

Characterisation: Γ is a Cayley graph $\iff \exists\, G \le \text{Aut}\,(\Gamma)$, with G a regular permutation group on the vertex set.

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

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

Petersen graph P is vertex-transitive and non-Cayley:
(smallest example)



Answer: first determine Aut (Γ); second search for regular G.
Both computationally difficult problems in general!

Empirical evidence: 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 research directions 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 **constraint-breaking** autos.

We will follow the last one in this lecture.

Primitive Cayley graphs

Given G: when can we find (interesting) primitive Cay(G, S)?

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

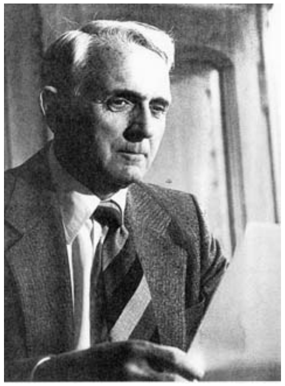
Wielandt 1935: Same result if G abelian, $|G|$ not prime, with at least one cyclic Sylow subgroup

Wielandt 1950: Same result 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: $G < H \leq \mathrm{Sym}(\Omega)$ with
G regular, $\Gamma = \mathrm{Cay}(G, S)$, $H = \mathrm{Aut}(\Gamma)$ primitive not 2-transitive

A group-theoretic problem

Find all 'Wielandt triples' (G, H, Ω): $G < H \leq \mathrm{Sym}(\Omega)$ with G regular, H primitive and not 2-transitive

Always yields: primitive $\Gamma = \mathrm{Cay}(G, S)$ with $H \leq \mathrm{Aut}(\Gamma)$

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

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

An illustration

G. A. Miller 1935: for $H \cong A_n$ (alternating group) gave examples of Wielandt triples (G, A_n, Ω), and also gave examples of n for which no Wielandt triples exist

George Abram Miller 1863-1951

Wiegold & Williamson 1980: classified all (G, H, Ω) with $H \cong A_n$ or S_n

A fascinating density result

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

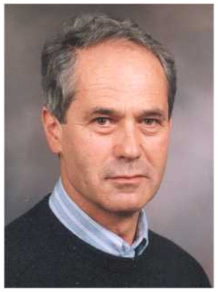
Technically: If $N(x)$:= Number of $n \leq x$ where $\exists\ H < S_n$ with H primitive and $H \neq A_n$, then $\frac{N(x)}{x} \to 0$ as $x \to \infty$

Immediate consequence: set of integers n such that no Wielandt triples (G, H, Ω) with G of order n, has density 1 in $\mathbb{N}$

Types of primitive groups H

Results of Liebeck, Praeger, Saxl 2000: (G, H, Ω) Wielandt triple
(1) from type of H clear always exists regular subgroup G
(2) H almost simple ($T \leq H \leq \mathrm{Aut}(T)$, T simple)
(3) H product action

Comments: (2) (resolved by LPS, 2009+) and (3) (still open);



Other work on Wielandt triples (G, H, Ω)

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 for case (2): H almost simple classical group (the heart of the problem)

Wielandt triples (G, H, Ω), H classical almost simple

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

Then comes: a lot of hard work

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

Then comes: a lot more hard work

LPS 2008+ Results

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

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 G in Wielandt triples

Complete information about almost simple groups G: when they occur in Wielandt triples (G, H, Ω), and the kinds of primitive groups H.

2: Suppose G almost simple. Then $\exists$ Wielandt triple $(G, H, \Omega) \iff$ G is simple or $G \in \{S_{p-2}$ (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 and (G, H, Ω) Wielandt triple. Then either
$G \times G \leq H \leq$ 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 $\Gamma = \mathrm{Cay}(G, S)$

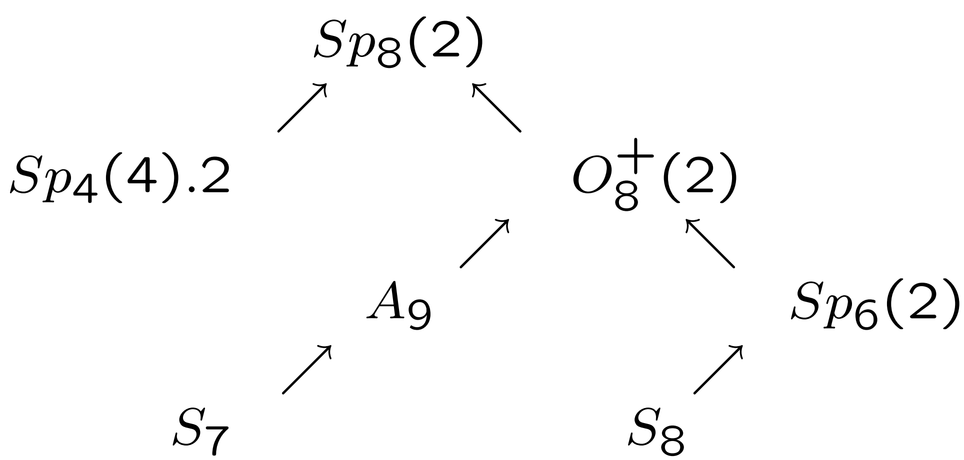
(1)	$S = G \setminus \{1\}$	$\mathrm{Aut}(\Gamma) = \mathrm{Sym}(G)$
(2)	$S =$ union of G-conjugacy classes	$\mathrm{Aut}(\Gamma) \geq G \times G$

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: curiosity

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



Summary

1: Cayley graphs arise in diverse areas of mathematics

2: Arose in early years of group theory

3: Group theoretic versions of primitive Cayley graph problems of intense interest for almost 100 years

4: Primitive Cayley graph classifications – require FSGC – astonishingly complete

5: Open problem – product case – subject of current research