Combinatorial Methods in Group Theory (and Group-theoretic Methods in Combinatorics)

PhD Summer School, Rogla, July 2019

Marston Conder

University of Auckland

m.conder@auckland.ac.nz

Outline of topics

1. Basic applications of counting
2. Methods for generating random elements of a group
3. Cayley graphs
4. Schreier coset graphs and their applications
5. Back-track search to find small index subgroups
6. Double-coset graphs and some applications
7. Möbius inversion on lattices and applications

Copies of slides can be made available by email or USB stick.

§3. Cayley graphs

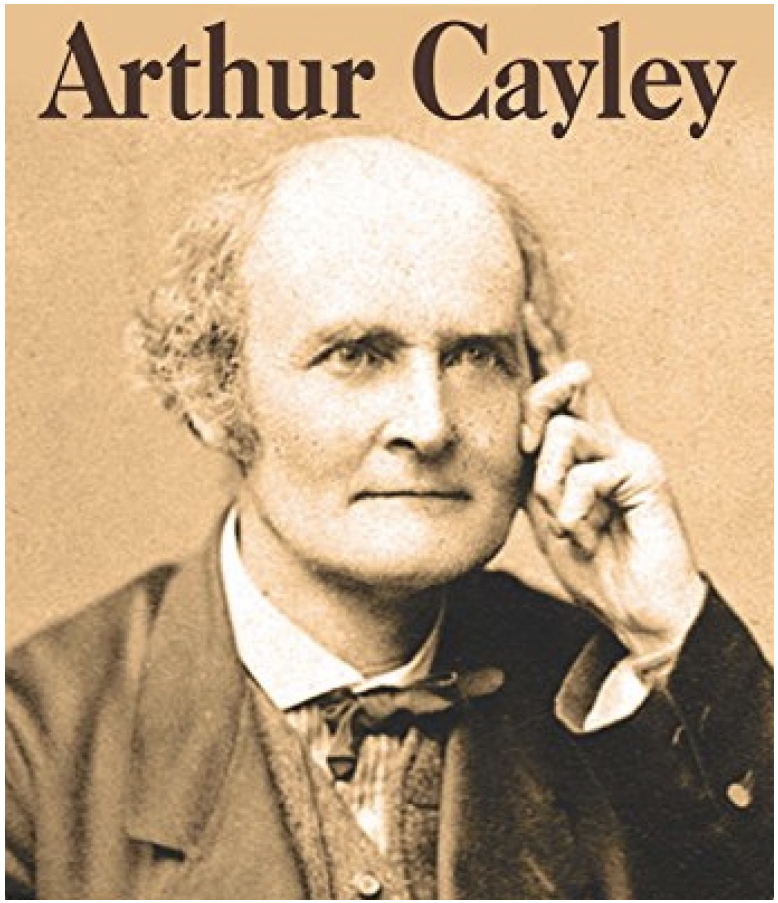
A Cayley graph $\mathrm{Cay}(G, X)$ is a graph with vertex-set a group G and edge-set $\{\{g, xg\} : g \in G,\, x \in X\}$ for some $X \subseteq G$.

This gives a diagrammatic representation of multiplication of elements of G by elements of X (on the left), and hence of the rows of the multiplication table for G corresponding to the elements of X.

Usually (but not necessarily) we assume that $\Gamma = \mathrm{Cay}(G, X)$ is finite, undirected, simple and connected – and hence that

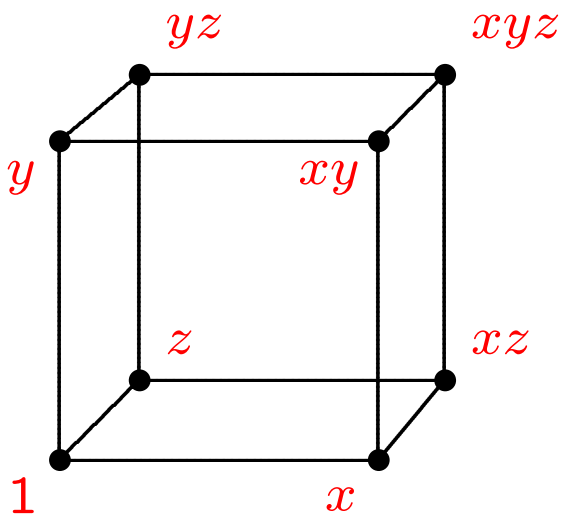
- G is finite,
- X does not contain the identity element of G, and
- X generates G.

Also we may assume that X is closed under taking inverses.



(1821–1895)

Cayley Graph Example:



(isomorphic to Q_3)

$G = C_2 \times C_2 \times C_2$ (abelian) with generating set $X = \{x, y, z\}$

Ex: Is Q_3 a Cayley graph for some other group of order 8?

Ex: For which groups of order n is the complete graph K_n a Cayley graph?

Some elementary properties of Cayley graphs

- $\mathrm{Cay}(G, X)$ has order $|G|$
- $\mathrm{Cay}(G, X)$ is connected if and only if $G = \langle X \rangle$
- Every closed walk in $\mathrm{Cay}(G, X)$ corresponds to a relation satisfied by the generators from X
  [Why? $x_k^{e_k} \dots x_2^{e_2} x_1^{e_1} g = g$ if and only if $x_k^{e_k} \dots x_2^{e_2} x_1^{e_1} = 1$]
- $\mathrm{Cay}(G, X)$ is regular of valency $|X^{\pm}| = |X \cup X^{-}|$
- The group G acts transitively on the vertices of $\Gamma = \mathrm{Cay}(G, X)$ as a group of automorphisms, and it follows that every Cayley graph is vertex-transitive.

  Proof. Right-multiplication by any element $h \in G$ takes an edge $\{g, xg\}$ to the edge $\{gh, xgh\}$, and hence gives an automorphism of Γ taking vertex 1 to vertex h. ■

Conversely:

Theorem Let Γ be a finite graph, and suppose $\mathrm{Aut}(\Gamma)$ contains a subgroup G that acts regularly (sharply-transitively) on the vertices of Γ. Then Γ is a connected Cayley graph.

Sketch proof. Take any vertex v of Γ, and label it 1. Now label each neighbour w of v with the unique element $g \in G$ that takes v to w, and let X be the set all such g for which w $(= v^g)$ is a neighbour of v. It follows fairly easily that Γ is connected and is isomorphic to $\mathrm{Cay}(G, X)$. ■

Another example: a Cayley graph for A_5

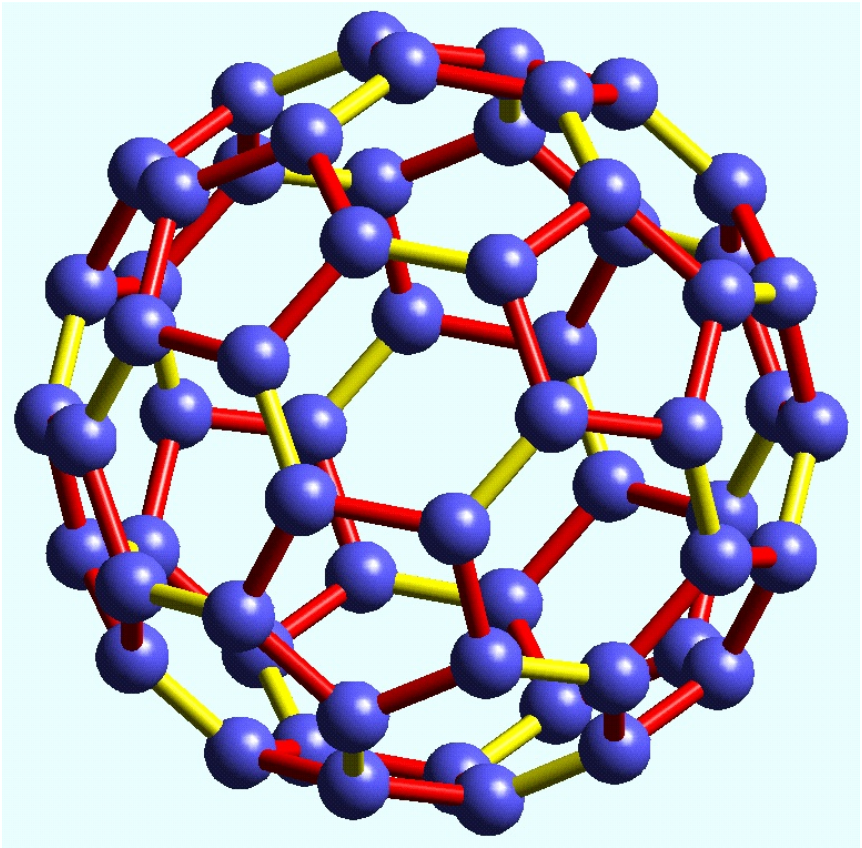
Let $G = A_5$ (the alternating group on 5 points)

and let $X = \{(1,2)(3,4), (1,2,3,4,5), (1,5,4,3,2)\}$.

Note that $(1,2)(3,4) \cdot (1,2,3,4,5) = (1,3,5)$, and it follows easily that the given set X generates G. Also X does not contain the identity element, and X is closed under inverses.

Hence the Cayley graph $\Gamma = \mathrm{Cay}(G, X)$ is a vertex-transitive, 3-valent connected graph of order 60.

This Cayley graph is the **chemical molecule** C_{60} (also known as Buckminsterfullerene):



Here it is again, in a possibly more recognisable form:

Some (other) common properties of Cayley graphs

- Symmetry (as we have seen: vertex-transitive)
- Rigidity (e.g. the C_{60} molecule)
- Good broadcast properties – many Cayley graphs have large order-to-diameter ratio or small order-to-girth ratio
- Some were used by Max Dehn (in the early 1900s) to solve the 'word problem' for the fundamental group of an orientable surface of genus ≥ 2.

The Degree-Diameter Table (as at June 2019)

$d\backslash k$	2	3	4	5	6	7	8	9	10
3	10	20	38	70	132	196	360	600	1 250
4	15	41	98	364	740	1 320	3 243	7 575	17 703
5	24	72	212	624	2 772	5 516	17 030	57 840	187 056
6	32	111	390	1 404	7 917	19 383	76 461	331 387	1 253 615
7	50	168	672	2 756	11 988	52 768	249 660	1 223 050	6 007 230
8	57	253	1 100	5 060	39 672	131 137	734 820	4 243 100	24 897 161
9	74	585	1 550	8 268	75 893	279 616	1 697 688	12 123 288	65 866 350
10	91	650	2 286	13 140	134 690	583 083	4 293 452	27 997 191	201 038 922
11	104	715	3 200	19 500	156 864	1 001 268	7 442 328	72 933 102	600 380 000
12	133	786	4 680	29 470	359 772	1 999 500	15 924 326	158 158 875	1 506 252 500
13	162	851	6 560	40 260	531 440	3 322 080	29 927 790	249 155 760	3 077 200 700
14	183	916	8 200	57 837	816 294	6 200 460	55 913 932	600 123 780	7 041 746 081
15	187	1 215	11 712	76 518	1 417 248	8 599 986	90 001 236	1 171 998 164	10 012 349 898
16	200	1 600	14 640	132 496	1 771 560	14 882 658	140 559 416	2 025 125 476	12 951 451 931
17	274	1 610	19 040	133 144	3 217 872	18 495 162	220 990 700	3 372 648 954	15 317 070 720
18	307	1 620	23 800	171 828	4 022 340	26 515 120	323 037 476	5 768 971 167	16 659 077 632
19	338	1 638	23 970	221 676	4 024 707	39 123 116	501 001 000	8 855 580 344	18 155 097 232
20	381	1 958	34 952	281 820	8 947 848	55 625 185	762 374 779	12 951 451 931	78 186 295 824

How do we find Cayley graphs?

– e.g. all connected Cayley graphs of order n and valency d?

For small n, one way is to use the database of groups of order up to 2000 (excepting 1024), as created by Besche, Eick and O'Brien (2000), and available in GAP and MAGMA.

For valency 3, for example, we can search over two types of generating set X for the group G:

- $X = \{a, b, c\}$ where a, b, c have order 2, and
- $X = \{x, y\}$ where x has order 2 and y has order > 2.

Also we can use conjugacy within G (or within Aut(G)) to reduce the number of possibilities.

Another way:

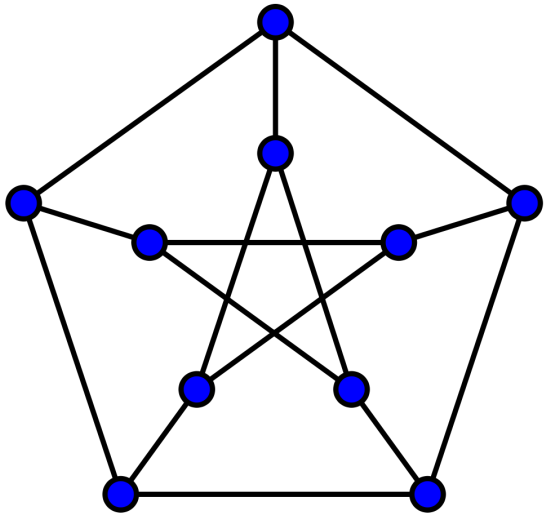
For the first type of Cayley graphs of valency 3, the generating set X consists of three involutions, so the group G is a quotient of the finitely-presented group

$$\mathcal{G} = \langle\, a, b, c \mid a^2 = b^2 = c^2 = 1 \,\rangle.$$

Instead of checking possibilities for G from among groups of order up to n, we can (directly) find all quotients of $\mathcal{G}$ of order up to n using an algorithm for finding all normal subgroups of up to given index in a finitely-presented group. [This algorithm will be described later.]

Finding all such 3-valent Cayley graphs of order up to 100 takes only a few minutes (using MAGMA).

Note: This method doesn't find the Petersen graph!



Reason: The Petersen graph is not a Cayley graph.

Why not? What are the possibilities for the generating set X in each of the groups of order 10? How does this relate to properties of the Petersen graph?

Answer(s):

By Sylow theory, every group of order 10 has at least one element of order 2, and has a normal subgroup of order 5. It follows easily that there are just two groups of order 10 – the cyclic group C_{10} and the dihedral group D_5.

If $G = C_{10}$ and u and v are two different elements of X, then $uv = vu$ so $u^{-1}v^{-1}uv = 1$, which gives a 4-cycle in the Cayley graph, but the Petersen graph has girth 5, so this is impossible. This leaves $G = D_5$ as the Cayley group.

Next, since the valency is odd, at least one element of X has order 2, say a. If the other elements of X are b and b^{-1} of order 5, then ab is a product of a reflection and a rotation and hence is a reflection (of order 2), and so $(ab)^2 = 1$, but

again this gives a 4-cycle, contradiction. Thus X consists of three involutions, say a, b, c. But this too is impossible, as:

- the Petersen graph has no proper 3-edge-colouring, or
- $w = ba$ has order 5, and the Cayley graph has a Hamilton cycle $(1, a, w, aw, w^2, aw^2, w^{-2}, aw^{-2}, w^{-1}, aw^{-1})$, or
- the involution c must be aw or aw^2 or aw^{-2}, and each of these three possibilities gives a 4-cycle (viz. $(1, a, w, aw)$ or $(1, a, w^{-2}, aw^2)$ or $(1, aw^{-2}, w^{-1}, aw^{-1})$, or easier:
- the resulting Cayley graph is bipartite!

Hence the Petersen graph is not a Cayley graph. ■

But: The Petersen graph is symmetric, and has some very nice properties, and is constructible as a double-coset graph.

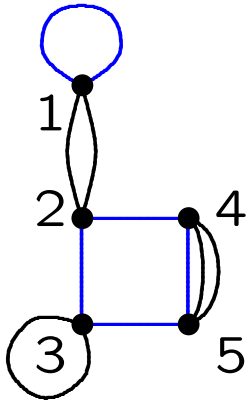
[See later]

§4. Schreier coset graphs & their applications

Let G be a group generated by a finite set $X = \{x_1, x_2, \ldots, x_d\}$.

Given any transitive permutation representation of G on a set Ω of size n, we may form a graph with vertex-set Ω, and with edges of the form $\alpha \text{ — } \alpha^{x_i}$ for $1 \leq i \leq d$.

e.g.



when $x_1 \mapsto (1,2)(4,5)$ and $x_2 \mapsto (2,3,5,4)$.

[Given any transitive permutation representation of G on a set Ω of size n, we may form a graph with vertex-set Ω, and with edges of the form $\alpha \text{ — } \alpha^{x_i}$ for $1 \leq i \leq d$.]

Similarly, if H is a subgroup of index n in G, we may form a graph whose vertices are the right cosets of H and whose edges are of the form $Hg \text{ — } Hgx_i$ for $1 \leq i \leq d$.

These two graphs are exactly the same when Ω is the coset space $(G:H)$ or when H is the stabilizer of a point of Ω.

The latter one is called the Schreier coset graph $\Sigma(G, X, H)$.

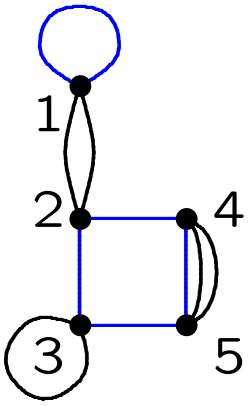
Each is a generalisation of a Cayley graph (which occurs when the subgroup H is trivial).

Otto Schreier (1901–1929)

Some elementary properties of Schreier coset graphs:

- The graph is connected (as the group action is transitive)
- There can be loops and/or multiple edges
- Edges may be directed or labelled/coloured ... or not!
- The action of G can be recovered from the graph
  – or indeed defined by it

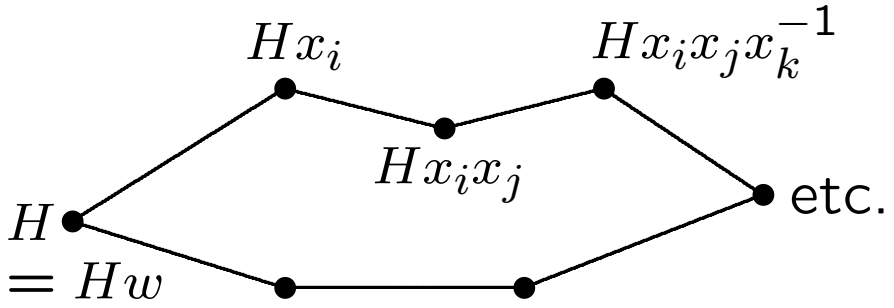
e.g.



gives $x_1 \mapsto (1,2)(4,5)$ and $x_2 \mapsto (2,3,5,4)$.

- Every circuit in Σ based at the vertex labelled H gives an element of H expressed as a word on X

Why? Any path in Σ corresponds to a word $w = w(X)$ in the generators of G, and such a path from H is closed whenever $Hw = H$, which occurs if and only if $w \in H$.



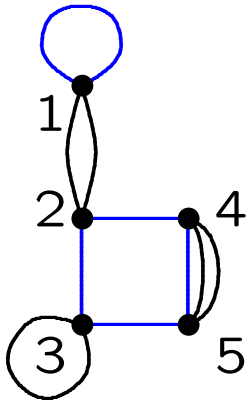
Importance/use of Schreier coset graphs [to follow]

- Visual representation (easier to see/understand than the permutations or 'coset table')
- Coset graphs can be used to construct representations (and build new ones from known representations)
- They give an easy proof of the Ree-Singerman theorem on necessary conditions for transitivity of a permutation representation of a finitely-generated group
- Depiction of Schreier transversals and Schreier generators
- Use in the Reidemeister-Schreier process (for finding a presentation for a given subgroup of finite index in a finitely-presented group)

Schreier coset graphs (cont.)

The Schreier coset graph $\Sigma(G, X, H)$ gives a diagrammatic representation of the natural action of G on cosets of H.

This action can also be given by a coset table, e.g. as on right in the following:



	x_1	x_2	x_1^{-1}	x_2^{-1}
1	2	1	2	1
2	1	3	1	4
3	3	5	3	2
4	5	2	5	5
5	4	4	4	3

when $x_1 \mapsto (1,2)(4,5)$ and $x_2 \mapsto (2,3,5,4)$.

Coset diagrams — simplified coset graphs

To make a Schreier coset graph easier to work with, we can sometimes simplify it by

- deleting loops (that occur for fixed points of generators)
- using single edges for 2-cycles of involutory generators
- ignoring the effect of redundant generators.

Special case: Triangle groups

Coset graphs for actions of the $(2, k, m)$ triangle group

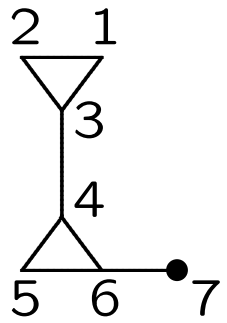
$$\langle\, x, y, z \mid x^2 = y^k = z^m = xyz = 1 \,\rangle$$

can be simplified by deleting z-edges, and using heavy dots for fixed points of y, and polygons for non-trivial cycles of y.

The resulting figures are called (Schreier) coset diagrams rather than coset graphs.

Example:

Below is a coset diagram for an action of the $(2,3,7)$ triangle group $\langle x, y, z \mid x^2 = y^3 = z^7 = xyz = 1 \rangle$ on 7 points:



$x \mapsto (3,4)(6,7)$

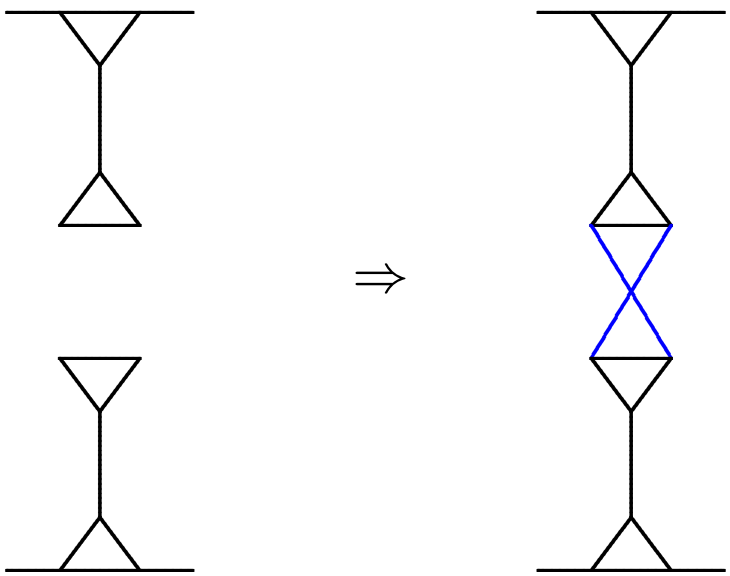
$y \mapsto (1,2,3)(4,5,6)$

$z \mapsto (1,4,7,6,5,3,2)$

Composition of coset diagrams:

Often two coset diagrams for the same group G on (say) m and n points can be composed to produce a transitive permutation representation of larger degree $m + n$,

e.g.



Ex: Check that relations $x^2 = y^3 = (xy)^m = 1$ are preserved.

What effect does this have?

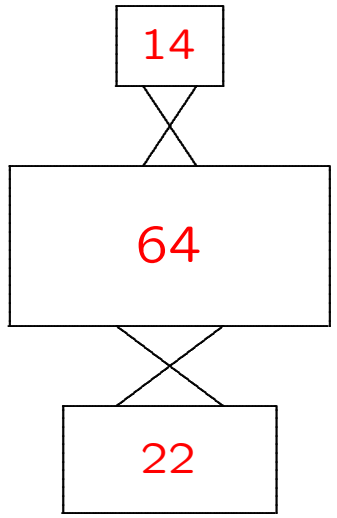
Strange things can happen! For example, consider coset diagrams for transitive actions of the $(2, 3, 7)$ triangle group.

One can join together three such diagrams D1, D2, D3:

D1 on 14 points, where the permutations generate a group isomorphic to PSL$(2, 13)$

D2 on 64 points, where the permutations generate a group isomorphic to A_{64}

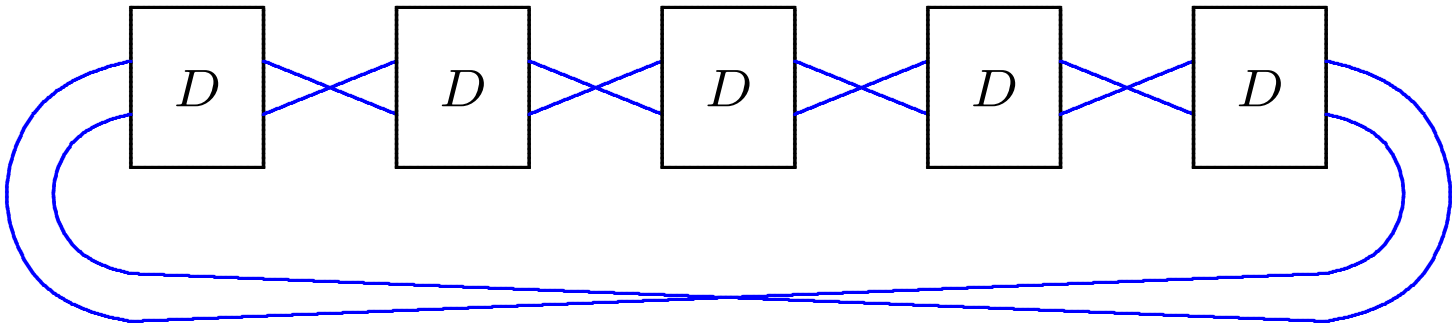
D3 on 22 points, where the permutations generate a group isomorphic to A_{22}



to get a diagram on 14+64+22 = 100 points, where the permutations generate the Hall-Janko group of order 604800.

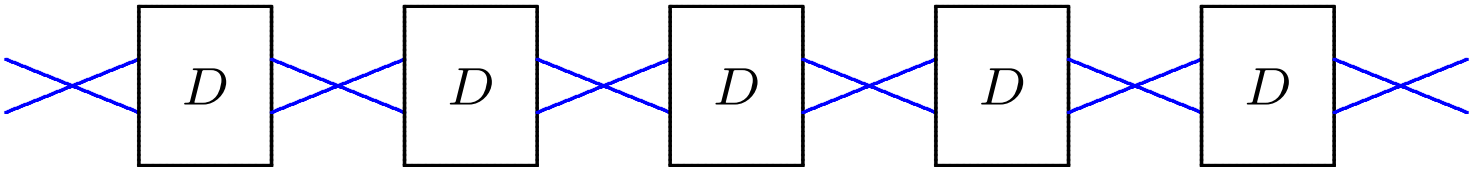
Abelian extensions:

In some cases, where a coset diagram D for a group G may be joined together to another copy of itself in two different places, it is possible to string together n copies of the diagram into a circular chain (like a necklace) and get a new diagram in which the permutations generate a larger group B with an abelian normal subgroup K of exponent n such that $B/K \cong G$.



Proving groups are infinite:

When the previous construction is possible, string together an infinite number of copies of the diagram D:



and get an infinite group!

This method can be used to prove that certain finitely-presented groups are infinite. It is equivalent to showing that some subgroup of finite index has infinite abelianization (... also achievable by the Reidemeister-Schreier process).

Exercise: Use a coset diagram with just 6 vertices to prove that the $(2, 3, 6)$ triangle group is infinite.

Alternating and symmetric quotients:

- If Diagrams P and Q with p points and q points have two 'handles' each (for attaching to other diagrams), then we can string together 'a' copies of P and 'b' copies of Q and get a much larger diagram on $m = ap + bq$ points.

- In particular, if $\gcd(p, q) = 1$ then the degree $m = ap + bq$ can be any sufficiently large positive integer.

- We can sometimes adjoin a single copy of an extra diagram R (with r points) to 'break symmetry', and make the permutations induced on the larger diagram generate the alternating group A_{m+r} or the symmetric group S_{m+r}.

- In this way, we can sometimes obtain all but finitely many A_n or S_n as quotients of a given finitely-presented group.

Some applications [by MC and students]

- For each $m \geq 7$, the $(2, 3, m)$ triangle group has all but finitely many alternating groups A_n among its quotients

- Every Fuchsian group has all but finitely many alternating groups A_n among its homomorphic images [Brent Everitt]

- There are infinitely many 5-arc-transitive connected finite 3-valent graphs

- There are infinitely many 7-arc-transitive connected finite 4-valent graphs [MC & Cameron Walker]

- There are infinitely many 5-arc-transitive Cayley graphs of valency 3, and infinitely many 7-arc-transitive Cayley graphs of valency $3^t + 1$ for each $t \geq 1$.

References

Cayley graphs

L. Babai & C.D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* 3 (1982), 9–15.

M.D.E. Conder, On symmetries of Cayley graphs and the graphs underlying regular maps, *J. Algebra* 321 (2009), 3112–3127.

P.R. Hafner, Large Cayley graphs and digraphs with small degree and diameter, in *Computational algebra and number theory (Sydney, 1992)*, Kluwer Acad. Publ. (Dordrecht), 1995, pp.291–302.

M-C. Heydemann, Cayley graphs and interconnection networks, in *Graph symmetry (Montreal, PQ, 1996)*, Kluwer Acad. Publ. (Dordrecht), 1997, pp.167–224.

W. Imrich & M.E. Watkins, On automorphism groups of Cayley graphs. *Period. Math. Hungar.* 7 (1976), 243–258.

S. Lakshmivarahan, J.S. Jwo & S.K. Dhall, Symmetry in interconnection networks based on Cayley graphs of permutation groups: a survey, *Parallel Comput.* 19 (1993), 361–407.

C.H. Li, On isomorphisms of finite Cayley graphs—a survey, *Discrete Math.* 256 (2002), 301–334.

Schreier coset graphs

M.D.E. Conder, Schreier coset graphs and their applications, *RIMS Kokyuroku* 794 (1992), 169–175.

M.D.E. Conder & J. McKay, A necessary condition for transitivity of a finite permutation group, *Bull. L.M.S.* 20 (1988), 235–238.

H.S.M. Coxeter & W.O.J. Moser, *Generators and Relations for Discrete Groups*, 4th ed. Springer-Verlag (Berlin), 1980.

A 3rd conference on Symmetries of Discrete Objects will be held the week 10-14 February 2020 in Rotorua, New Zealand

See www.math.auckland.ac.nz/∼conder/SODO-2020

All welcome!