Finding normal subgroups of small index in finitely-presented groups

Marston Conder
University of Auckland

m.conder@auckland.ac.nz

Dedicated (with best wishes and thanks) to John Cannon and Derek Holt on the occasions of their significant birthdays

Context/background

The problem of finding all 'small' homomorphic images of a finitely-presented group $G = \langle X \mid R \rangle$ is equivalent to finding all normal subgroups of small finite index in G.

This has numerous applications, e.g. to

- Symmetric 3-valent graphs – via the modular group
- Regular maps on surfaces – via triangle groups
- Regular/chiral polytopes – via Coxeter groups
- Large (and largest) groups of automorphisms of Riemann and Klein surfaces of given genus.

The low index subgroups algorithm

- Given $G = \langle X \mid R \rangle$ finitely-presented group
- Algorithm (due to Dietze & Schaps and Sims, in 1970s) finds a representative of each conjugacy class of subgroups of index $\leq n$ (for given n) in G
- Backtrack search through a tree, with nodes at level k corresponding to k-generator (pseudo-)subgroups H
- Enumeration (by Todd-Coxeter) of cosets of H
- Create branches to new nodes at the next level (if necessary) by identifying pairs of cosets: forcing $Hg_i = Hg_j$ is equivalent to adding $g_i g_j^{-1}$ to a set of generators for H

Low index subgroups algorithm (cont.)

- Output includes generators for the subgroup H, and/or permutations induced by generators (in X) on cosets of H

- Schreier's theorem shows every subgroup of finite index m in $G = \langle X \,|\, R \rangle$ is finitely-generated (and so will be found)

- Conjugates of subgroups found earlier may be eliminated easily (by a test on the coset table)

- This can facilitated by normal ordering of cosets in the coset table – where each 'new' coset is labelled with the smallest unused positive integer

- Example: (PTO)

	x_1	x_2	x_3	x_1^{-1}	x_2^{-1}	x_3^{-1}
1	2	3	4	5		
2				1		
3					1	
4						1
5	1					
:						

Level	Coincidence	Additional generator
1	$1 = 2$	x_1^{-1}
	$1 = 3$	x_2^{-1}
	$2 = 3$	$x_1 x_2^{-1}$
	:	:
	$1 = 5$	x_1
	$2 = 5$	x_1^2
	$3 = 5$	$x_2 x_1$
	:	:

Some applications

- Low index subgroups + Reidemeister-Schreier

or Low index subgroups + cohomological methods

$\Rightarrow$ can prove some G infinite (or find lower bound on $|G|$)

- Determine all factor groups of G that are isomorphic to permutation groups of small degree (from right representations of G on cosets of subgroups H)

- Can often find small degree transitive permutation representations that may be used as 'building blocks' for constructing representations of larger degree (e.g. using coset diagrams to show G has certain A_n or S_n as quotients)

Some adaptations

- Torsion-free subgroups (or subgroups complementary to a given subgroup) can be sought by avoiding all subgroups which contain any conjugates of specified elements, that is, by ignoring selected branch(es) of the search tree

- Possibility of starting/stopping the process at any node of the search tree

- Distributed computation – treat branches independently

- Finding only normal subgroups ...

Adaptation 1 to find normal subgroups

- One way is to just delete all subgroups that are not normal
- This works OK for some groups, but not for the modular group $\langle x, y \mid x^2 = y^3 = 1 \rangle$:

Up to index	# subgroups	# normal
1	1	1
5	7	3
10	69	5
15	826	6
20	16382	7
25	423693	9

There are better ways ...

Adaptation 2 to find normal subgroups

• When any coincidence $Hu = Hv$ is forced in the branching process, all conjugates of uv^{-1} must lie in H (if H normal), so uv^{-1} may be treated as an additional *relator* rather than an additional subgroup generator

• Advantage: very much faster than finding all subgroups and eliminating those which are non-normal

• Allows search up to much higher index

e.g. all normal subgroups of index up to 1000 in Hecke groups $C_2 * C_k = \langle\, x, y \mid x^2 = y^k = 1 \,\rangle$ easy to find

New variant (David Firth & Derek Holt, 2006)

- Finds small quotients of $\langle X|R\rangle$ by systematic enumeration of possibilities for a composition series for the quotient
- Still uses a branching process, but with nodes at level k corresponding to quotients that have a composition series of length k
- Needs database of simple groups of small order
- Can find quotients of order up to $100,000$ (and generally much faster than previous methods)
- Available in MAGMA (and GAP?)

Some examples (to illustrate capability)

- Modular group $C_2 * C_3 = \langle\, x, y \mid x^2 = y^3 = 1 \,\rangle$:

Up to index	# normal	Time
50	13	Seconds
500	95	Seconds
5000	1098	c. 75 mins

- $(2, 3, 7)$ triangle group $\langle\, x, y \mid x^2 = y^3 = (xy)^7 = 1 \,\rangle$:

Up to index	# normal	Time
500	2	Seconds
5000	8	Seconds
50000	22	c. 15 mins

Application: Symmetric cubic graphs

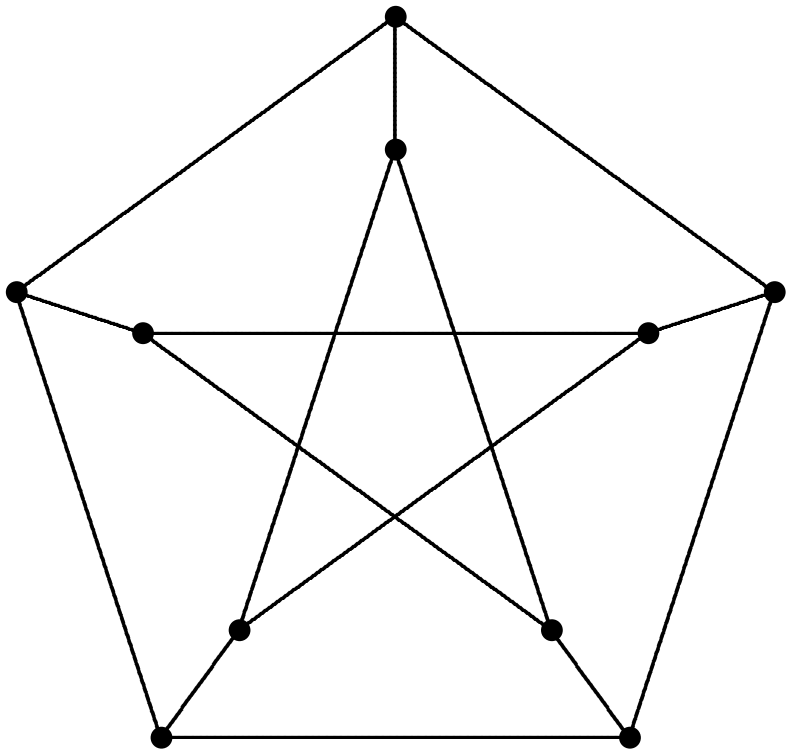
• The automorphism group $\mathrm{Aut}\,\Gamma$ of a simple graph Γ is the group of all bijections $V(\Gamma) \to V(\Gamma)$ preserving adjacency

• The graph Γ is symmetric if $\mathrm{Aut}\,\Gamma$ is transitive on the arcs (ordered pairs of adjacent vertices) of Γ

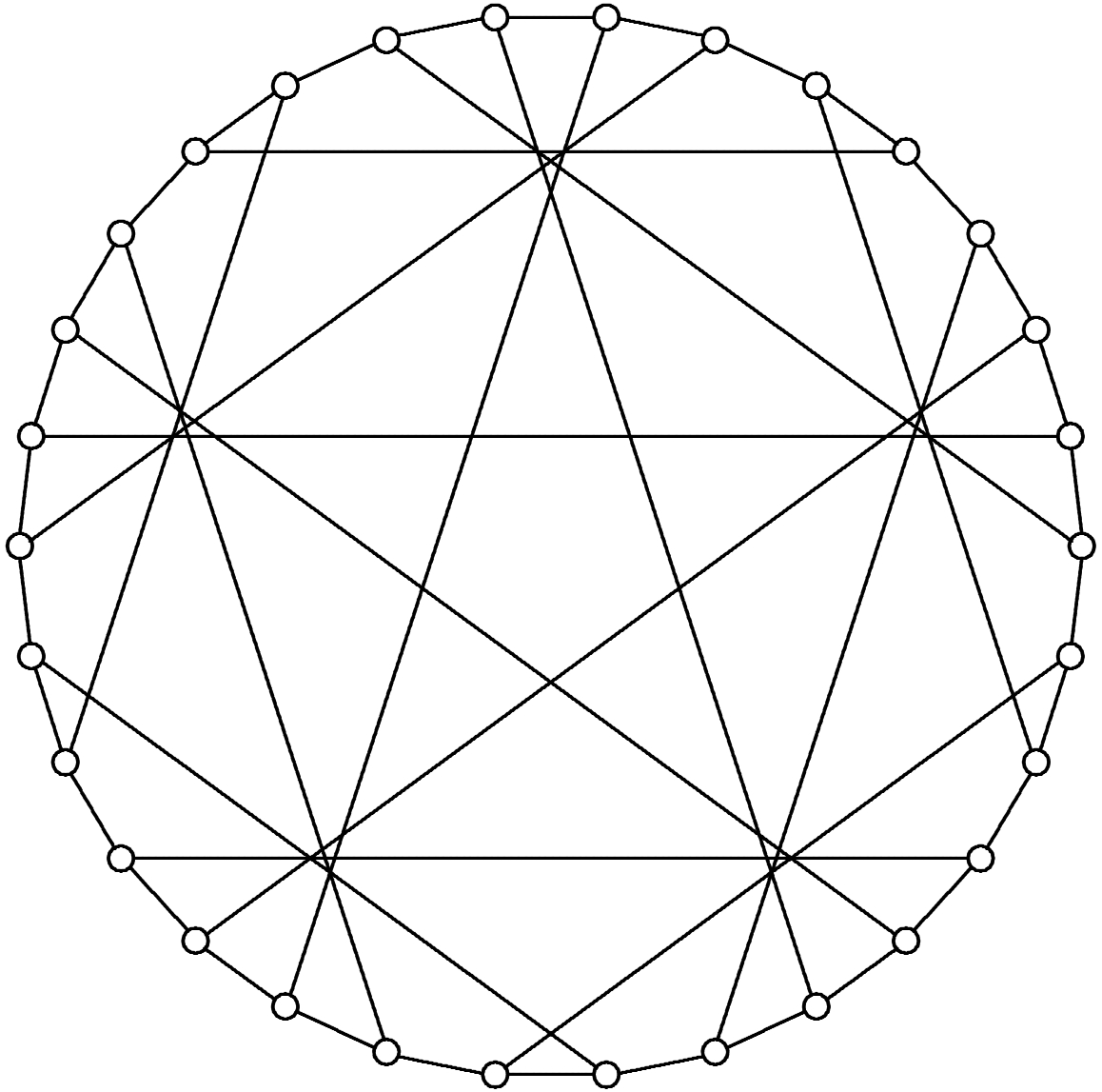
• The graph Γ is s-arc-transitive if $\mathrm{Aut}\,\Gamma$ has one orbit on directed walks of the form $v_0 - v_1 - v_2 - \ldots - v_{s-1} - v_s$ in which any three consecutive vertices are distinct

• A theorem of Tutte (1947) shows that every finite cubic (3-valent) graph is at most 5-arc-transitive

Example: The Petersen graph (3-arc-transitive)



Tutte's 8-cage (5-arc-transitive)



Symmetric cubic graphs (cont.)

- There are seven classes of finite s-arc-transitive cubic graphs (classified by the value of s and the existence of an involutory automorphism reversing a given edge)

- Associated with each of these 7 classes is an amalgamated free product of two small groups (corresponding to stabilizers of an edge and a vertex, with the arc-stabilizer subgroup amalgamated)

- The automorphism group of every finite symmetric cubic graph is a quotient of one of these seven finitely-presented groups G_1, G_2^1, G_2^2, G_3, G_4^1, G_4^2, G_5; conversely, every 'smooth' quotient of one of these groups (with torsion-free kernel) is an arc-transitive group of automorphisms of a cubic graph.

The Foster Census

- Census of most known small symmetric cubic graphs, of order up to 512 ... complied by R.M. Foster, engineer
- Peter Dobcsányi & MC (2002) used low index normal subgroups methods to fill gaps in this census and extend it to order 768
- Bonus find: smallest graph of type G_2^2 (has order 448)
- MC (2006) used the Firth-Holt procedure to extend the census to order 2048
- Bonus find: largest known connected 3-valent graph of diameter 10 (has order 1250)

Regular maps

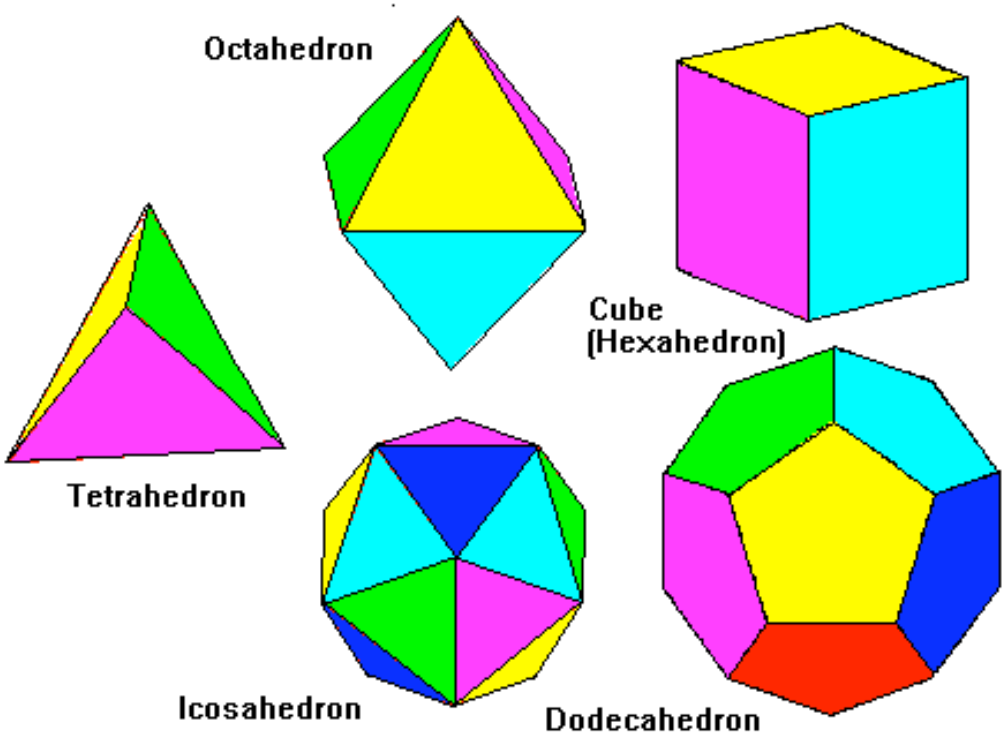
- A map is a 2-cell embedding of a connected graph (or multigraph) into a closed surface, breaking up the surface into simply-connected regions called faces

- An automorphism of a map M is any permutation of its edges that preserves incidence (with vertices and faces); each automorphism is uniquely determined by its effect on a given flag (incident vertex-edge-face triple)

- If M has automorphisms that act like a single-step rotation about any given face or given vertex, then M is regular

- If M has automorphisms that act (locally) like reflections, then M is reflexible; otherwise M is orientable, but chiral.

Platonic solids: regular maps on the sphere



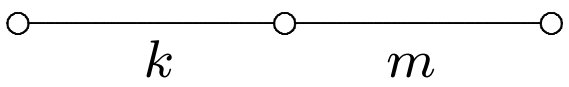
... also called 'Neolithic Scots' (c. 2000BC)

Transitivity, type and triangle groups

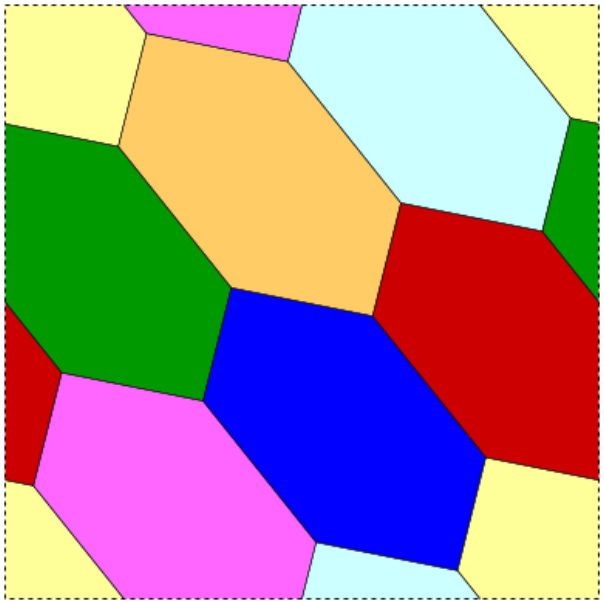
If M is a regular map, then its underlying graph is vertex-transitive, edge-transitive and face-transitive.

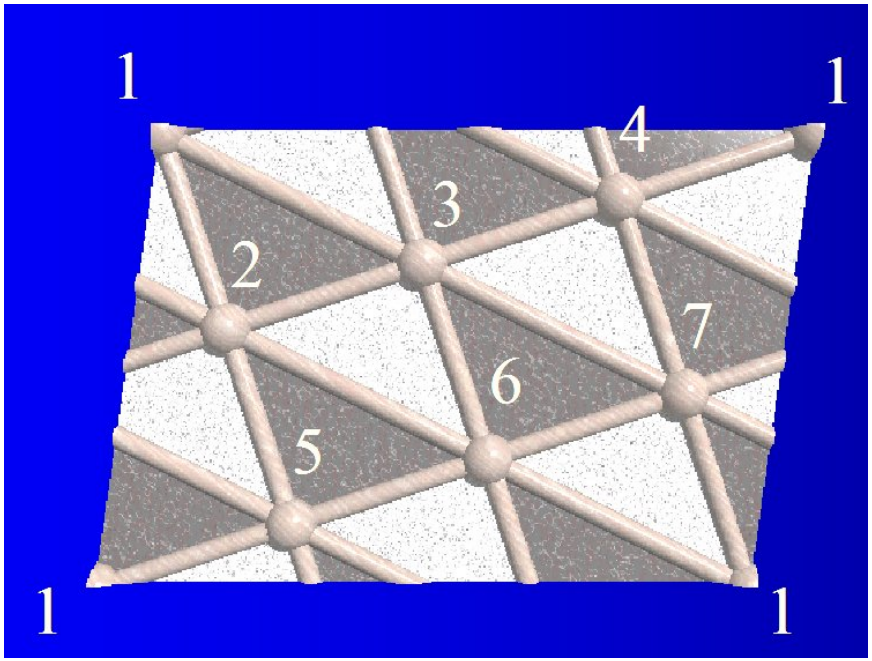
In particular, every face of must have the same number of edges (say k) and every vertex must have the same valency (say m). In this case we say that M has type $\{k, m\}$.

Moreover, $\mathrm{Aut}\, M$ contains elements R and S that act as single-step rotations about a face and an incident vertex, and satisfy the relations $R^k = S^m = (RS)^2 = 1$, which define the $(2, k, m)$ triangle group — a subgroup of index 2 in the $[k, m]$ Coxeter group



Example: a map of type $\{6,3\}$ on the torus





This is chiral, with automorphism group $\mathbb{Z}_7 : \mathbb{Z}_6$, and is dual to the type $\{3,6\}$ triangulation of the torus by K_7 (RHS).

History and classification

The study of regular maps dates back to Brahana (1920s)

Deep connections to algebraic geometry & Galois theory
— Belyi (1979), Grothendieck (1984), Jones et al (2007): the absolute Galois group can be studied by considering its action on maps given by the natural action of the group on coefficients of the defining polynomial of the corresponding Riemann surface over an algebraic number field

Such maps are usually viewed from three main perspectives:

— Classification by *surface*

— Classification by *underlying graph*

— Classification by *automorphism group.*

Census of regular maps of small genus

• Using the Firth-Holt algorithm to find all normal subgroups of small finite index in $(2, k, m)$ triangle groups, it is now possible to considerably extend the census of all regular maps on surfaces of small genus

• All regular maps are now known [MC, 2006] on surfaces of Euler characteristic $\chi = V - E + F$ for $2 \leq -\chi \leq 200$
... the previous range was only $2 \leq -\chi \leq 10$ (before 2001) and $2 \leq -\chi \leq 28$ (before 2006)

• This extended census reveals examples and patterns never seen before

Computational observations (using MAGMA)

Orientably-regular maps (up to isomorphism & duality)
Genus 2 to 7: 71 reflexible maps, 2 chiral pairs
Genus 2 to 15: 220 reflexible maps, 16 chiral pairs
Genus 2 to 101: 3378 reflexible maps, 594 chiral pairs

Non-orientable regular maps (up to isomorphism & duality)
Genus 2 to 202: 862 maps

There is no orientably-regular but chiral map of genus 2, 3, 4, 5, 6, 9, 13, 23, 24, 30, 36, 47, 48, 54, 60, 66, 84, 95, 108, 116, 120, 139, 150, 167, 168, 174, 180, 186 or 198

There is no regular orientable map of genus 20, 32, 38, 44, 62, 68, 74, 80 or 98 with simple underlying graph

New theorems [MC, Jozef Siráň & Tom Tucker]

- If M is an irreflexible (chiral) orientably-regular map of genus $p+1$ where p is prime, then

  either $p \equiv 1 \bmod 3$ and M has type $\{6,6\}$,
  or $p \equiv 1 \bmod 5$ and M has type $\{5,10\}$,
  or $p \equiv 1 \bmod 8$ and M has type $\{8,8\}$.

  In particular, there are no such maps of genus $p+1$ whenever p is a prime such that $p-1$ is not divisible by 3, 5 or 8.

- There is no reflexible regular map M with simple underlying graph on an orientable surface of genus $p+1$ where p is a prime congruent to 1 mod 6, for $p > 13$.

... to appear in *J. European Math. Soc.* 2010

Notes on these theorems:

- Computations showed the way but not needed for proof
- These are special cases of a more general theorem classifying such maps M where $|\mathrm{Aut}\, M|$ is coprime to χ or $\chi/2$
- Riemann-Hurwitz formula restricts values of parameters
- Can show $\mathrm{Aut}\, M$ is 'almost Sylow-cyclic' (and then use classification of such groups by Zassenhaus (1936), Suzuki (1955) and Wong (1966))
- Use Schur-Zassenhaus theory to finish off.

And more to come (e.g. regular embeddings of circulants).

Thank You!

Large groups of automorphisms of Riemann (and Klein) surfaces

• The Riemann-Hurwitz formula provides a bound on the order of any group of automorphisms of a compact Riemann surface of genus $g > 1$, and also restricts the set of possible signature types for automorphism groups of large order

e.g. $|G| \leq 168(g-1)$ [by Hurwitz, 1893], with equality if and only if the signature is $(0;\ +;\ [\ \ ];\ \{(2,3,7)\})$

• Examples can be found from the corresponding non–Euclidean crystallographic groups (NEC-groups) by low index subgroups (and other) methods

• Now have a list of the largest groups of automorphisms of a compact Riemann surface of genus g (preserving orientation, resp. containing reflections) for $2 \leq g \leq 201$.