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

§6. Double-coset graphs

Let G be a group, H a subgroup of G, and a an element of G such that $a^2 \in H$. Now define a graph $\Gamma = \Gamma(G, H, a)$ by

$$V(\Gamma) = \{Hg : g \in G\}$$

$$E(\Gamma) = \{\{Hx, Hy\} : x, y \in G \mid xy^{-1} \in HaH\}.$$

For example, vertex H is adjacent to Hah for all $h \in H$.

Now G induces a group of automorphisms of Γ by right multiplication, since $(xg)(yg)^{-1} = xgg^{-1}y^{-1} = xy^{-1} \in HaH$ whenever $\{Hx, Hy\} \in E(\Gamma)$).

This action is vertex-transitive (since $(Hx)x^{-1}y = Hy$), with vertex-stabiliser $G_H = \{g \in G : Hg = H\} = H$ itself, which acts transitively on the neighbours Hah of H.

Thus $\Gamma = \Gamma(G, H, a)$ is arc-transitive, or 'symmetric'.

Example: a double-coset graph for A_5

Let $G = A_5$ (the alternating group on 5 points), and take $H = \langle\, (1,2,3), (1,2)(4,5)\, \rangle \cong S_3$ and $a = (1,4)(2,5)$.

Then the coset graph $\Gamma(G, H, a)$ is a connected arc-transitive 3-valent graph of order 10 which turns out to be isomorphic to the Petersen graph.

This can also be constructed as a double-coset graph for $G = S_5$, using $H = \langle\, (1,2,3), (1,2), (4,5)\, \rangle \cong S_3 \times C_2$ and element $a = (1,4)(2,5)$.

In fact S_5 is the full automorphism group.

Special case: 3-valent arc-transitive graphs

• By work of Tutte and Djoković & Miller, it is known that if Γ is a finite connected 3-valent arc-transitive graph, then $G = \mathrm{Aut}\,\Gamma$ is a quotient of one of seven finitely-presented groups G_1, G_2^1, G_2^2, G_3, G_4^1, G_4^2, G_5.

• Conversely, if G is any non-degenerate quotient of one of those groups, then we can use the double-coset graph construction to obtain a finite connected 3-valent arc-transitive graph Γ on which G acts as a group of automorphisms.

• For example, $G = A_5$ is a quotient of the group

$$G_2^1 = \langle\, h, a, p \,|\, h^3 = a^2 = p^2 = 1,\ apa = p,\ php = h^{-1} \,\rangle$$

via $h \mapsto (1,2,3)$, $a \mapsto (1,4)(2,5)$, $p \mapsto (1,2)(4,5)$, and from this we get the Petersen graph (as before).

Small 3-valent symmetric graphs

- Take each one of G_1, G_2^1, G_2^2, G_3, G_4^1, G_4^2, G_5 in turn

- Use the 'Low Index Normal Subgroups' algorithm (e.g. in MAGMA) to find all normal subgroups of index up to n

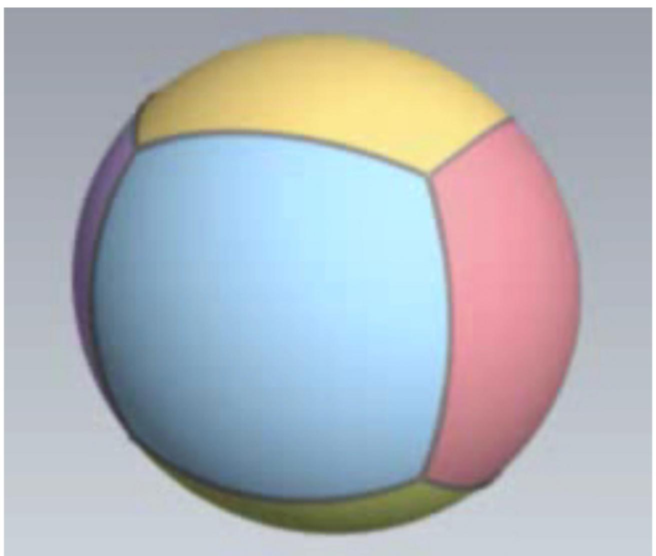
- For each normal subgroup K, let G be the quotient of the given group by K, and use the double-coset graph construction to obtain a finite connected 3-valent symmetric graph Γ on which G acts as a group of automorphisms

- Check whether G is the full automorphism group of Γ (using GAP or MAGMA); discard the graph if it's not

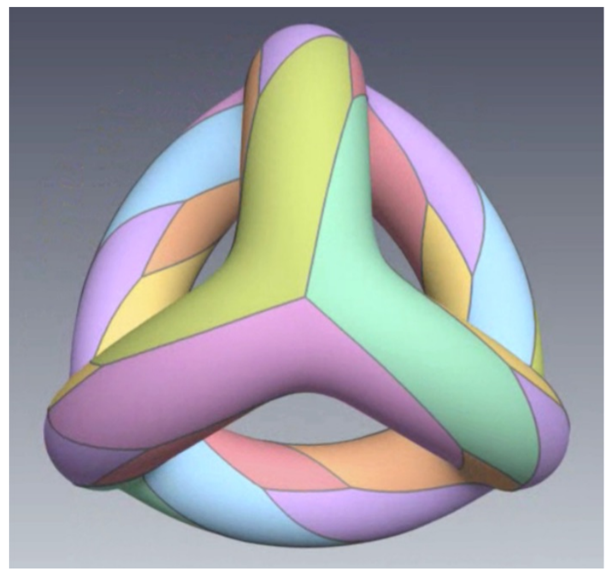
- This approach has provided a census of all such graphs on up to 10000 vertices.

Arc-transitive maps (sometimes called **regular maps**)

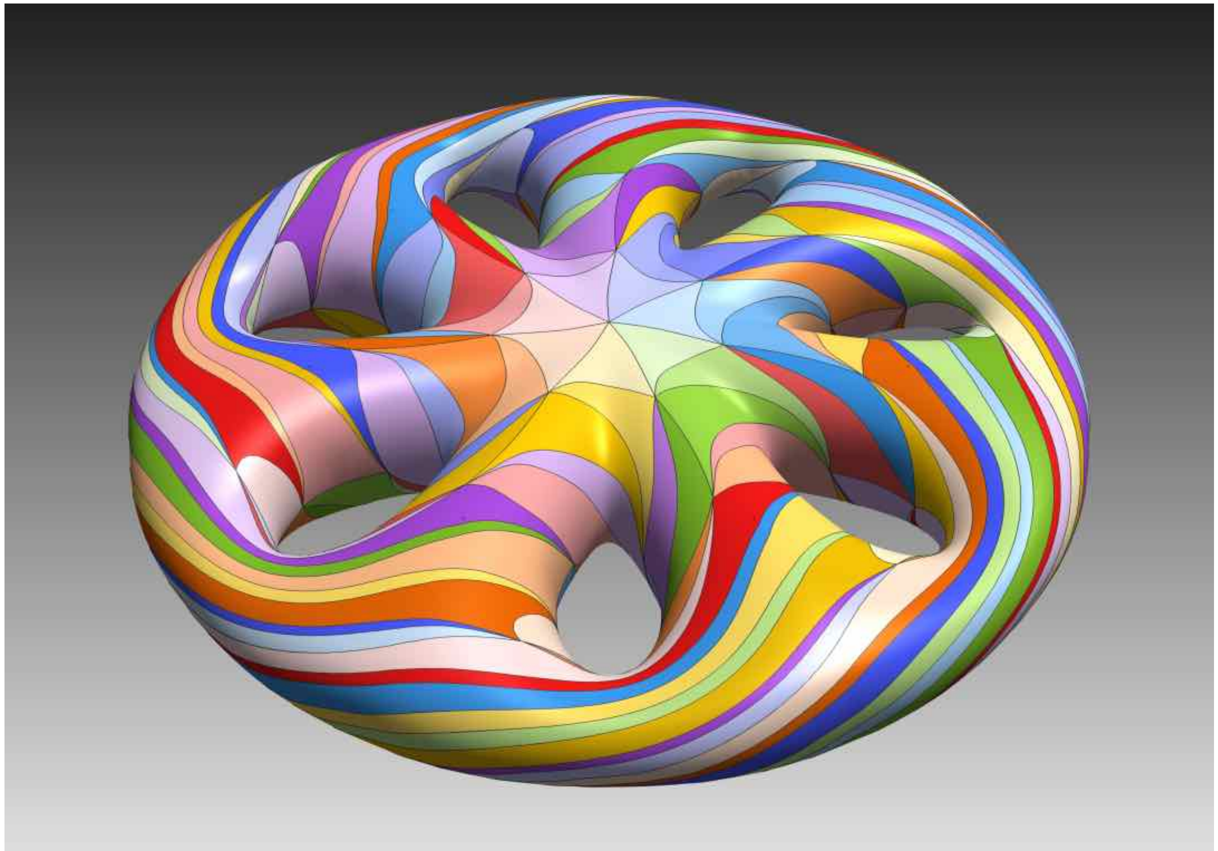
These are maximally symmetric 2-cell embeddings of connected graphs or multigraphs on surfaces:



Q_3 on sphere



Klein map (genus 3)



Hurwitz map of genus 7

[Image created by Jarke van Wijk (Eindhoven)]

Some key points:

A flag of a map is an incident vertex-edge-face triple (v, e, f).

An automorphism of a map M is a bijection taking vertices to vertices, edges to edges and faces to faces, preserving incidence between them.

Apart from some weird exceptions, every automorphism of a map M is uniquely determined by its effect on a given flag, and it follows that $|\text{Aut}(M)| \leq 4|E|$ where E is the edge set.

A map M is (fully) regular if Aut(M) is transitive on flags.

A map M on an orientable surface is orientably-regular if the orientation-preserving subgroup $\text{Aut}^+(M)$ of Aut(M) is transitive on arcs, and in that case $|\text{Aut}^+(M)| \leq 2|E|$.

Moreover, such a map M is either reflexible (when Aut(M) is transitive on all flags), or otherwise chiral (irreflexible).

Construction for arc-transitive maps

Let G be a group that is generated by two elements R and S such that $R^m = S^k = (RS)^2 = 1$, where $k, m \geq 2$.

Now construct the graph $\Gamma = \Gamma(G, \langle S \rangle, RS)$, on which the group G acts as an arc-transitive group of automorphisms, and define an embedding of this graph into a surface by taking as faces the cycles induced by R on the vertices of Γ.

This turns Γ into an arc-transitive map $M = M(G, R, S)$ on some orientable surface, with the given group G inducing its group $\mathrm{Aut}^o M$ of orientation-preserving automorphisms.

The cyclic subgroups of G generated by S, RS and R are stabilisers of a vertex, edge and face, respectively.

Similar construction for fully regular maps:

Let G be a group that is generated by three involutions a, b, c such that $(ab)^2 = (bc)^k = (ca)^m = 1$, where $k, m \geq 3$.

Now construct the graph $\Gamma = \Gamma(G, \langle b, c\rangle, a)$, and turn this into a regular map $M = M(G, a, b, c)$, by taking as faces the cycles induced by ca on the vertices of Γ.

The dihedral subgroups $\langle b, c\rangle$, $\langle a, b\rangle$ and $\langle a, c\rangle$ are stabilisers of a vertex, edge and face, respectively.

This map is orientable if and only if the subgroup generated by $R = ca$ and $S = bc$ has index 2 in G; otherwise, the latter subgroup has index 1 and the surface is non-orientable.

Regular maps of small genus

- Take the extended $(2, \infty, \infty)$ triangle group

$$\Delta = \langle\, a, b, c \mid a^2 = b^2 = c^2 = (ab)^2 = 1 \,\rangle$$

— that is, without specifying the orders of bc and ca

- Use the 'Low Index Normal Subgroups' algorithm to find all normal subgroups of small index in Δ

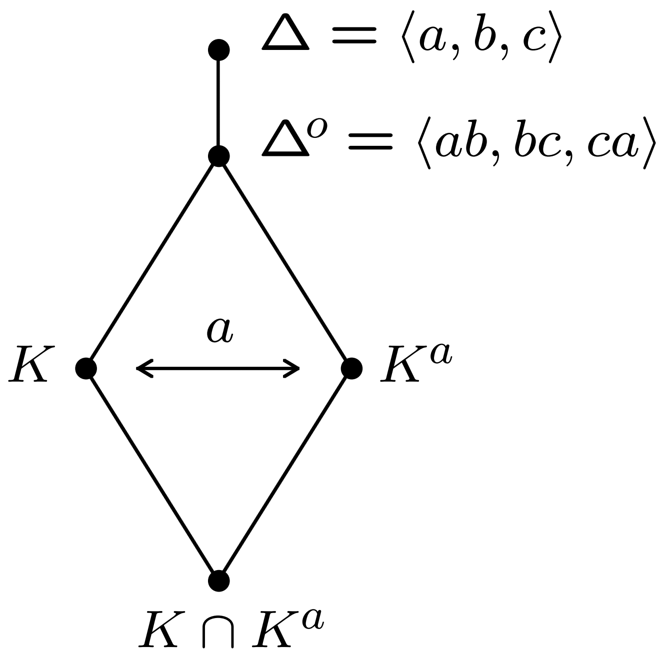
- For each torsion-free normal subgroup K, let $G = \Delta/K$, and use the previous construction to obtain a regular map (on which G acts as a group of automorphisms)

- Check the genus and orientability of the map

- This approach has provided a census of all regular maps of Euler characteristic -1 to -300.

Chiral arc-transitive maps

Use the arc-transitive maps construction, and check whether the kernel K in Δ^o is normal in the full triangle group Δ:



$K = K^a$ iff map M is reflexible

(when $\mathrm{Aut}^o M \cong \Delta^o / K$)

Regular and chiral polytopes

A similar approach can be taken to construct polytopes with large automorphism groups. Polytopes are generalisations of maps and polyhedra to higher dimensions.

The largest possible automorphism groups are quotients of Coxeter groups (or of subgroups of index 2 in Coxeter groups), satisfying an additional test on the intersections of certain subgroups
— in order to meet criteria of 'strong flag connectedness' and the 'diamond condition'.

This method was used to construct the first known examples of finite chiral polytopes (with maximum possible rotational symmetry) of ranks 5, 6, 7 and 8. The latter also enabled the recent construction of chiral n-polytopes for all $n \geq 3$.

§7. Möbius Inversion

In number theory, the Möbius function $\mu\colon \mathbb{N} \to \mathbb{Z}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is a product of an even no. of distinct primes} \\ -1 & \text{if } n \text{ is a product of an odd no. of distinct primes} \\ 0 & \text{if } n \text{ is divisible by the square of some prime.} \end{cases}$$

It has this nice property, called the Möbius inversion formula:

Theorem: If $f\colon \mathbb{N} \to \mathbb{C}$ and $g\colon \mathbb{N} \to \mathbb{C}$ are functions with f defined in terms of g by $f(n) = \sum_{d \mid n} g(d)$ for all $n \in \mathbb{N}$, then

$$g(n) = \sum_{d \mid n} \mu(d)\, f\left(\frac{n}{d}\right) \quad \text{for all } n \in \mathbb{N}.$$

In other words, μ helps determine g from the values of f.

Möbius Inversion (cont.)

The same thing can be proved in a more general setting, thanks to work by Louis Weisner and Philip Hall in the 1930s.

Setting: Let $\mathcal{P}$ be any partially ordered set with a maximum element M, and define the function $\mu\colon \mathcal{P} \to \mathbb{Z}$ by setting

$$\mu(x) = \sum_{s=0}^{\infty} (-1)^s \, n_s(x)$$

where $n_s(x)$ is the number of descending chains of the form $M = x_0 > x_1 > \cdots > x_s = x$ from M to x in $\mathcal{P}$.

Observe that $\mu(M) = 1$, while $\mu(x) = -1$ for every maximal element x of $\mathcal{P}$, and so on.

Key property of μ : $\sum_{x \geq y} \mu(x) = 0$ for every $y \in \mathcal{P} \setminus \{M\}$.

Proof. Observe that $\sum_{x \geq y} \mu(x) = \sum_{x \geq y} \sum_{s=0}^{\infty} (-1)^s n_s(x)$ can be split as the sum of $\sum_{s=0}^{\infty} (-1)^s n_s(y)$ and $\sum_{s=0}^{\infty} (-1)^s \sum_{x > y} n_s(x)$.

Every chain $M = y_0 > y_1 > \cdots > y_{s-1} > y_s = y$ of length s from M to y corresponds uniquely to a chain of length $s-1$ from M to the element $x = y_{s-1}$, and this is counted just once in the last of the above sums, with coefficient $(-1)^{s-1}$.

Hence the terms of $\sum_{s=0}^{\infty} (-1)^s n_s(y)$ and $\sum_{s=0}^{\infty} (-1)^s \sum_{x > y} n_s(x)$ cancel each other and give 0. ∎

Theorem: If $f : \mathcal{P} \to \mathbb{C}$ and $g : \mathcal{P} \to \mathbb{C}$ are functions with f defined in terms of g by $f(x) = \sum_{y \le x} g(y)$ for all $x \in \mathcal{P}$, then

$$g(M) = \sum_{x \in \mathcal{P}} \mu(x)\, f(x).$$

In other words, μ helps determine $g(M)$ from the values of f.

Proof. First we have $\sum_{x \in \mathcal{P}} \mu(x) f(x) = \sum_{x \in \mathcal{P}} \mu(x) \sum_{y \le x} g(y)$.

Now the right hand side rearranges to $\sum_{y \in \mathcal{P}} g(y) \sum_{x \ge y} \mu(x)$,

and then this splits according to whether $y = M$ or $y < M$.

Indeed since $\mu(M) = 1$ and $\sum_{x \ge y} \mu(x) = 0$ for all $y < M$, it

simplifies to just $g(M)\mu(M)$, which is $g(M)$. ■

The above theorem was proved by Weisner for lattices (with maximum element and minimum element, and 'meets' and 'joins'), but Hall proved it more generally for posets with a maximum element, using the 'key property' given earlier.

Exercise 1: Show how the number-theoretic Möbius inversion formula follows from the Hall-Weisner theorem. [Note: you may use symmetry of the lattices of divisors of n.]

Exercise 2: Show how the Inclusion-Exclusion Principle (for subsets of a finite set) follows from the Hall-Weisner thm. What are the values of the Möbius function μ in this case?

Also Philip Hall applied it to the poset of subgroups of a group (in some cases even when the group is infinite).

The Möbius function on a subgroup lattice:

For any finite group G, let $\mathcal{S}$ be the lattice of all subgroups of G, with $A \wedge B = A \cap B$ (intersection), and $A \vee B = \langle A, B \rangle$ (the subgroup generated by A and B, or equivalently, the intersection of all subgroups of G that contain A and B). Also let μ be the Möbius function on $\mathcal{S}$.

Exercise 3: Show how the values of μ on the subgroup lattice of an infinite cyclic group are related to those of the values of the number-theoretic Möbius function.

Exercise 4: The group A_4 has three subgroups of order 2, four of order 3, and one each of orders 1, 4 and 12, and no others. Find the values of μ on each of these subgroups.

Exercise 5: Find μ on the subgroup lattice of A_5.

Lemma: For every proper subgroup $H \leq G$, either $\mu(H) = 0$ or H is the intersection of some maximal subgroups of G.

Proof. We use induction on the index $|G:H|$.

First, if H itself is maximal in G, then $\mu(H) = -1$.

Now let J be the intersection of all maximal subgroups of G containing H, and suppose $H < J$. Then by the earlier 'key property' of μ, we know that $\mu(H) = -\sum_{K>H} \mu(K)$.

Next, by induction, we may suppose that $\mu(K) = 0$ for every subgroup $K > H$ that does not contain J (for then K cannot be the intersection maximal subgroups of G), and thus $\sum_{K>H} \mu(K) = \sum_{K \geq J} \mu(K)$, which is 0, by the 'key property'.

Hence either $H = J$, or $\mu(H) = -\sum_{K \geq J} \mu(K) = 0$. ■

Application of the Hall-Weisner theorem to groups:

Suppose we are interested in knowing whether the group G can be generated by a subset X that has a given property (P) – e.g. X is a set $\{a, b\}$ of two elements of orders 2 and 3.

Then we can define two functions f and g on the subgroup lattice $\mathcal{S}$ of G by setting for each subgroup H of G

$f(H) =$ number of subsets of type (P) contained in H, and
$g(H) =$ number of subsets of type (P) that generate H.

Since every subset generates a unique subgroup, we have $f(H) = \sum_{K \le H} g(K)$ for all $H \le G$, so by Möbius inversion, the total number of subsets of type (P) that generate G is $g(M) = \sum_{H \le G} \mu(H)\, f(H)$ – which is often easily computable.

Banal example: Is S_4 generated by two elements of order 4?

The only subgroups of S_4 containing an element of order 4 are the three cyclic subgroups of order 4, three dihedral subgroups of order 8, and S_4 itself. It follows easily that

$$f(H) = \begin{cases} 2^2 = 4 & \text{when } H \cong C_4 \\ 2^2 = 4 & \text{when } H \cong D_4 \\ 6^2 = 36 & \text{when } H = S_4 \\ 0 & \text{otherwise.} \end{cases}$$

Also $\mu(S_4) = 1$ and $\mu(H) = -1$ for all $H \cong D_4$ (maximal), and then since every C_4 subgroup of order 4 lies in just one D_4 subgroup, we find that $\mu(H) = 0$ for all $H \cong C_4$. Thus

$$g(S_4) = \sum_{H \le S_4} \mu(H)\, f(H) = 3(0\cdot 4) + 3(-1\cdot 4) + (1\cdot 36) = 24$$

so there are 24 generating pairs (x, y) with $o(x) = o(y) = 4$.

Some further applications/examples:

- Philip Hall found the no. of generating pairs (x, y) for PSL$(2, p)$ s.t. $x^2 = y^3 = 1$ for every prime p [Hall (1936)]

- Martin Downs extended this to PSL$(2, q)$ for every prime-power q [Downs (1991)]

- Martin Downs extended this further to generating pairs (x, y) for PSL$(2, q)$ s.t. $x^k = y^\ell = (xy)^m = 1$ [Downs (1997)]

- For every $s > 1$, the Suzuki group $Sz(2^s)$ can be generated by two elements x and y such that $x^2 = y^4 = (xy)^5 = 1$ (and moreover, is the automorphism group of a chiral map of type $\{4, 5\}$). [Jones & Silver (1993)]

Symmetric graphs and double-coset graphs

M.D.E. Conder, An infinite family of 5-arc-transitive cubic graphs, *Ars Combinatoria* 25A (1988), 95–108.

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

M.D.E. Conder & P. Dobcsányi, Trivalent symmetric graphs on up to 768 vertices, *J. Combin. Math. Combin. Computing* 40 (2002), 41–63.

M.D.E. Conder & P.J. Lorimer, Automorphism groups of symmetric graphs of valency 3, *J. Combin. Theory Ser. B* 47 (1989), 60–72.

M.D.E. Conder & C.G. Walker, The infinitude of 7-arc-transitive graphs, *J. Algebra* 208 (1998), 619–629.

D.Z. Djoković & G.L. Miller, Regular groups of automorphisms of cubic graphs, *J. Combin. Theory Ser. B* 29 (1980), 195–230.

V. Trofimov, On the action of a group on a graph, *Acta Appl. Math.* 29 (1992), 161–170.

W.T. Tutte, A family of cubical graphs, *Proc. Camb. Phil. Soc.* 43 (1947), 459–474.

W.T. Tutte, On the symmetry of cubic graphs, *Canad. J. Math.* 11 (1959), 621–624.

Richard Weiss, The non-existence of 8-transitive graphs, *Combinatorica* 1 (1981), 309–311.

Richard Weiss, Presentations for (G, s)-transitive graphs of small valency, *Math. Proc. Cambridge Philos. Soc.* 101 (1987), 7–20.

Construction of regular/chiral maps and polytopes

M.D.E. Conder, Regular maps and hypermaps of Euler characteristic −1 to −200, J. Combin. Theory Ser. B 99 (2009), 455–459.

M.D.E. Conder & P. Dobcsányi, Determination of all regular maps of small genus, *J. Combin. Theory Ser. B* 81 (2001), 224–242.

M.D.E. Conder, I. Hubard & T. Pisanski, Constructions for chiral polytopes, *J. London Math. Soc. (2)* 77 (2008), 115–129.

Möbius inversion

M. Downs, The Möbius function of $\mathrm{PSL}_2(q)$, with application to the maximal normal subgroups of the modular group, *J. London Math. Soc.* 43 (1991), 61–75.

M. Downs, Some enumerations of regular hypermaps with automorphism group isomorphic to $\mathrm{PSL}_2(q)$, *Quart. J. Math. Oxford* **48** (1997), 39–58.

P. Hall, The Eulerian functions of a group. *Quart. J. Math. Oxford* **7** (1936), 134–151.

G.A. Jones and S.A. Silver, Suzuki groups and surfaces *J. London Math. Soc.* **48** (1993), 117–125.

L. Weisner, Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.* 38 (1935), 474–484.

Other references

W. Bosma, J. Cannon & C. Playoust, The Magma Algebra System I: the user language, *J. Symbolic Comput.* 24 (1997), 235–265.

M.D.E. Conder, Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry, in: *Applications of Group Theory to Combinatorics* (ed. J. Koolen, J.H. Kwak & M.Y. Xu), Taylor & Francis, London, 2008, pp. 1–11.

J. Neubüser, *An elementary introduction to coset-table methods in computational group theory*, Groups – St. Andrews 1981, London Math. Soc. Lecture Note Series, vol. 71, 1982, pp. 1–45.

Thank you for listening!

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!