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.

§0. Background on group theory

In this course, a relatively small amount of knowledge of group theory will be needed, namely the following:

- Definition and elementary properties of groups
- Some well known examples of groups – e.g. C_n (cyclic), D_n (dihedral), A_n (alternating), S_n (symmetric)
- Subgroups, cosets, conjugacy, normal subgroups, factor groups, homomorphisms, isomorphisms, automorphisms
- Permutation groups (i.e. subgroups of symmetric groups)
- Generating sets for groups
- Presentation of groups by generators and relations.

Information about most of these things is available on Wikipedia.

§1. Basic applications of counting

Many theorems in combinatorics can be proved by counting the same thing in two different ways – e.g. the 'hand-shaking lemma' in graph theory ($2|E(X)| = \sum_{v \in V(X)} \deg(v)$).

The same thing happens in aspects of group theory.

Theorem (The 'Orbit-Stabiliser Theorem')
If G is a permutation group on a set Ω, and G_α and α^G are the stabiliser $\{g \in G \mid \alpha^g = \alpha\}$ and orbit $\{\alpha^g : g \in G\}$ of a point $\alpha \in \Omega$, then $|G| = |\alpha^G|\,|G_\alpha|$ for every $\alpha \in \Omega$.

Proof. Count the number of pairs $(g, \beta) \in G \times \Omega$ such that $\alpha^g = \beta$ in two different ways. On one hand, choosing g first gives the number as $|G|$, while on the other hand, choosing β first gives the number as $|\alpha^G|\,|G_\alpha|$, because if $\beta = \alpha^h$ for some h, then $\alpha^g = \beta$ iff $g \in G_\alpha h$, and $|G_\alpha h| = |G_\alpha|$. ∎

An application: Lagrange's Theorem

If H is a subgroup of the finite group G, then $|G| = |G\!:\!H|\,|H|$ – and in particular, both $|H|$ and $|G\!:\!H|$ are divisors of $|G|$.

Proof. Let G act on the right coset space $\{Hx : x \in G\}$ by right multiplication, with each element $g \in G$ inducing the permutation $\mu_g : Hx \mapsto Hxg$. Then the orbit of H is the entire coset space $(G : H)$, while the stabiliser of H is $\{g \in G \mid Hg = H\} = \{g \in G \mid g \in H\} = H$, so the Orbit-Stabiliser Theorem gives $|G| = |G\!:\!H|\,|H|$.

Exercise: Find a finite group G that has no subgroup of order d for some divisor d of $|G|$.

Some more applications (for finite groups)

Conjugacy: Let the group G act on itself by conjugation, with each $g \in G$ inducing the permutation $\tau_g \colon x \mapsto g^{-1}xg$.

The orbit of x is the conjugacy class $[x] = \{g^{-1}xg : g \in G\}$, and its stabiliser is the centraliser $C_G(x) = \{g \in G \mid xg = gx\}$, so the Orbit-Stabiliser Theorem gives $|G| = |[x]|\,|C_G(x)|$, or equivalently, $|[x]| = |G|/|C_g(x)| = |G\colon C_G(x)|$, for all $x \in G$.

Class equation: If $x_1, x_2, \ldots, x_k$ are representatives of the k distinct conjugacy classes of elements of the group G, then

$$|G| = \sum_{1 \le i \le k} |[x_i]| = \sum_{1 \le i \le k} |G : C_G(x_i)|.$$

Exercise: Use this to show that if G has order p^s for some prime p, then the centre $Z(G)$ of G has at least p elements.

Burnside's Lemma: If the finite group G acts on the set Ω, with exactly m orbits, and $F_\Omega(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$ is the set of fixed points of each $g \in G$, then $m = \dfrac{1}{|G|} \sum_{g \in G} |F_\Omega(g)|$.

Proof. Simply count pairs $(g, \alpha) \in G \times \Omega$ such that $\alpha^g = \alpha$.

On one hand, counting by g, this number is $\sum_{g \in G} |F_\Omega(g)|$.

On the other hand, for any $\alpha \in \Omega$, the number of g for which $\alpha^g = \alpha$ is $|G_\alpha| = |G|/|\Delta|$, where $\Delta = \alpha^G$ is the orbit of α. When this is counted over all $\alpha \in \Omega$, the term $|G|/|\Delta|$ is counted $|\Delta|$ times (once for each point in Δ), and so each orbit Δ contributes $|\Delta|\,(|G|/|\Delta|) = |G|$ to the total. Hence the total number is $m|G|$, giving $m|G| = \sum_{g \in G} |F_\Omega(g)|$. ∎

An application of Burnside's Lemma:

In how many inequivalent ways can the faces of a regular tetrahedron be coloured using up to k given colours with one colour/face (but allowing more than one face/colour)?

Two colourings are considered to be equivalent if one can be obtained from the other by a rotation of the tetrahedron. The rotation group is A_4, acting naturally on the 4 vertices (or 4 faces), so we need the number of orbits on colourings.

The identity fixes all k^4 colourings; a double-transposition $(a,b)(c,d)$ fixes k^2 colourings (with a and b coloured the same and c and d coloured the same); and a 3-cycle (a,b,c) fixes k^2 colourings (with a, b and c coloured the same).

By Burnside's Lemma, the total number of inequivalent colourings is $\frac{1}{12}(k^4 + 3k^2 + 8k^2) = \frac{1}{12}k^2(k^2 + 11)$.

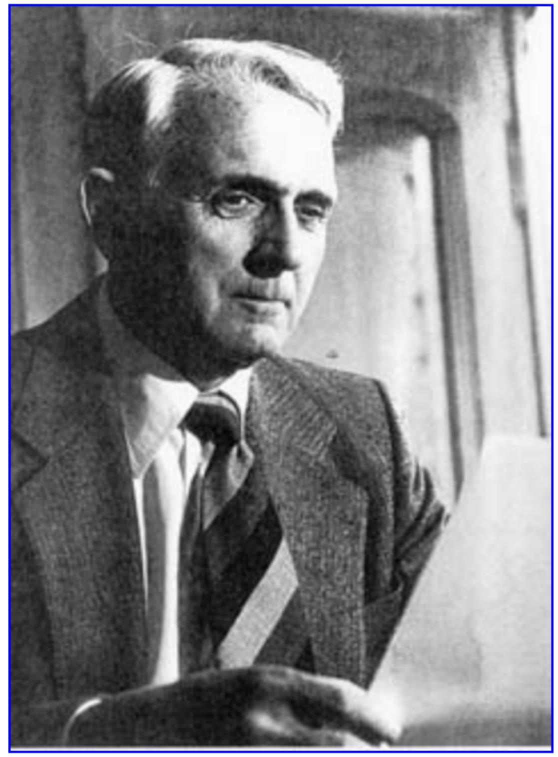
A combinatorial proof of some Sylow theory

If G is a finite group whose order $|G|$ is divisible by the prime p, and p^s is the largest power of p that divides $|G|$, then any subgroup of G of order p^s is called a Sylow p-subgroup of G.

Two of the main statements of Sylow theory are that every such G has at least one Sylow p-subgroup and that if n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \bmod p$.

Clearly the first property is a consequence of the second one, so we will prove the second one, using a combinatorial proof due to Helmut Wielandt.

Before doing that, we note that if G is cyclic of order n, generated by x, say, then G has exactly one subgroup of order p^s – namely the (cyclic) subgroup generated by x^{n/p^s}.



Helmut Wielandt (1910–2001)

Proof (that $n_p \equiv 1 \bmod p$):

Define Ω as the set of $\binom{|G|}{p^s}$ **subsets** of G of size p^s and then let G act on the set Ω by right multiplication, with each $g \in G$ taking S to $Sg = \{xg : x \in S\}$ for every $S \in \Omega$.

Note that if Δ is an orbit of G on Ω, then there exists at least one $S \in \Delta$ such that $1 \in S$ (because if $x \in T$ where $T \in \Delta$, then $1 = xx^{-1} \in Tx^{-1}$ with $Tx^{-1} \in \Delta$).

Now consider the stabiliser G_S of S in G. If $g \in G_S$ then $g = 1g \in Sg = S$ so $g \in S$, hence $G_S \subseteq S$, giving $|G_S| \leq |S|$.

We split the orbits of G on Ω into two types, according to whether or not $G_S = S$. [PTO]

Type (a) Suppose that $G_S = S$. Then S is a subgroup of G, and $\Delta = \{Sg : g \in G\}$ is the right coset space $(G\!:\!S)$. In particular, Δ contains only one subgroup (namely S itself), and also $|\Delta| = |G\!:\!S| = |G|/|S| = (p^s q)/(p^s) = q$. Conversely, if S is a Sylow p-subgroup of G, then Δ has type (a).

Type (b) Suppose that $G_S \subset S$. Then $|G_S| < |S| = p^s$ but also $|G_S| = |G|/|\Delta|$ divides $|G|$, so $|\Delta|$ is divisible by p.

These imply that G has n_p orbits of length q on Ω, with the lengths of all other orbits being divisible by p.

Thus $\binom{|G|}{p^s} = |\Omega| \equiv n_p\, q$ mod p. But as this also holds for the cyclic group of the same order $|G|$, for which $n_p = 1$, we find $n_p\, q \equiv \binom{|G|}{p^s} \equiv q$ mod p and so $n_p \equiv 1$ mod p. ■

Further Sylow theory

Let G be a finite group with order $p^s q$ (where p is prime) as before. Then the following hold:

- If P is a Sylow p-subgroup of G, and Q is any subgroup of G with order p^r for some r, then $Q \subseteq x^{-1}Px$ for some $x \in G$.
- If P and Q are Sylow p-subgroups of G, then $Q = x^{-1}Px$ for some $x \in G$. Hence under conjugation, G has a single orbit on Sylow p-subgroups.
- The number of Sylow p-subgroups of G divides q.

My favourite application: If $|G| = pqr$ where p, q and r are distinct primes, then G has a normal subgroup of order p, q or r. Hence in particular, no such group can be simple.

Proof. Assume the contrary. Let n_p, n_q and n_r be the numbers of Sylow p-, q- and r-subgroups (of orders p, q and r), respectively. If $n_p = 1$ then G has a unique Sylow p-subgroup P, and then $x^{-1}Px = P$ $\forall x \in G$, so $P \lhd G$, contradiction. Thus $n_p > 1$ and similarly $n_q > 1$ and $n_r > 1$.

Next, without loss of generality, we may suppose $p < q < r$.

By Sylow theory, n_r divides $|G|/r = pq$, so $n_r = p, q$ or pq. But also $n_r \equiv 1 \bmod r$ and hence $n_r > r > q > p$, so $n_r = pq$. Then because any two Sylow r-subgroups intersect trivially (by Lagrange's theorem and since r is prime), it follows that G has $pq(r-1)$ elements of order r.

Similarly, $n_q = r$ or pr, while also $n_p = q, r$ or qr, and hence G has at least $r(q-1)$ elements of order q, and at least $q(p-1)$ elements of order p.

It follows that the number of elements of prime order in G is at least $q(p-1)+r(q-1)+pq(r-1) = pqr - q + qr - r = pqr + (q-1)(r-1)$. But this is greater than $pqr = |G|$, contradiction! Hence proof. ∎

Exercises

- If $|G| = pq$ where p and q are distinct primes, then G cannot be simple.
- If $|G| = p^2q$ where p and q are distinct primes, then G cannot be simple.

§2. Generating random elements of a group

Q: How do we select elements randomly from a group?

But first, why would we want to? One reason is that many group-theoretic algorithms rely on being able to do this. (Examples: algorithms for working out the order of a group generated by given elements, or identifying the group itself.)

For some groups, finding random elements is easy:

- Cyclic groups $C_n = \langle\, x \mid x^n = 1 \,\rangle$

Just take x^k where k is a random element of $\{0, 1, 2, \ldots, k–1\}$

- Symmetric groups S_n

Just take a random permutation of $\{1, 2, 3, \ldots, n\}$

Exercises (or just possibilities to consider):

What about the following groups?

- Dihedral groups $D_n = \langle\, x, y \mid x^2 = y^n = 1,\ xyx = y^{-1}\,\rangle$

How do we find a random element of this group?

- Alternating groups A_n

How do we find a random **even** permutation of $\{1, 2, 3, \ldots, n\}$?

- A sharply 3-transitive group – such as PSL$(2, 2^s)$ in its action on the projective line over GF(2^s)? [Base & SGS]

- A group of order p^7 where p is prime? [PC-presentations]

- The Monster simple group? [Worth thinking about]

Clearly finding a good method may depend on the type of description we have for the group.

Digression: **Generating sets**

Let G be a group, and let X be a subset of G.

We say that X is a generating set for G if every element of G can be expressed as a 'word' $x_1^{e_1} x_2^{e_2} \dots x_k^{e_k}$ in elements of X and their inverses (with $x_i \in X$ and $e_i = \pm 1$ for $1 \leq i \leq k$).

Also if X is finite, then G is said to be finitely-generated, and the rank of G is defined as the smallest possible value of $|X|$ (over all such X). Otherwise G has infinite rank.

More generally, if S is the set of all such words on $X^{\pm}$, then S is a subgroup of G, called the subgroup generated by X and denoted by $\langle X \rangle$.

Examples:

- Cyclic groups $\equiv$ groups of rank 1
- Dihedral groups have rank 2 (generated by 2 reflections, or by a reflection and a rotation)
- The symmetric group S_n has rank 2 (e.g. generated by the transposition $(1,2)$ and the n-cycle $(1,2,\ldots,n)$), and is also generated by $\{(1,2),(2,3),\ldots,(n-1,n)\}$
- The alternating group A_n is the subgroup of S_n generated by the 3-cycles (a,b,c) ... and also has rank 2
- Every non-abelian simple group has rank 2 [Needs CFSG]

One further point (for later use):

Let G be a group of order n, with elements $g_1, g_2, \ldots, g_n$.

The multiplication table of a finite group G of order n is an $n \times n$ array with (i,j)th entry equal to the product $g_i\, g_j$. This is a Latin square. But much of its content is redundant!

If $X = \{x_1, x_2, \ldots, x_m\}$ is a generating set for G, of size m, then we can reduce the multiplication table to an $m \times n$ array with (i,j)th entry equal to the product $x_i\, g_j$.

We can call this a reduced Cayley table for the pair (G, X).

Note that any element of the full multiplication table, say $g_i\, g_j$, can be obtained by expressing g_i as a word on X, say $x_{i_1}^{e_1} x_{i_2}^{e_2} \ldots x_{i_k}^{e_k}$, and then working out $g_i\, g_j = x_{i_1}^{e_1} x_{i_2}^{e_2} \ldots x_{i_k}^{e_k}\, g_j$ by successive calls to the reduced Cayley table.

Now, back to generating random elements of a group ...

How do we select elements randomly from a finite group G when G does not have a nice canonical form that makes this easy?

One effective method was developed by Celler, Leedham-Green, Murray, Niemeyer and O'Brien (in 1995), and is now called the Product Replacement Algorithm.

The algorithm starts by taking an ordered generating set $X = \{x_1, x_2, \ldots, x_m\}$ for G of size $m >$ rank(G), and then performs the following basic operation a number of times:

> Choose two random integers i and j from $\{1, 2 \ldots, m\}$, and replace x_i by either $x_i x_j$ or $x_j x_i$, to give a new X.

If this is done sufficiently many times, then any element of the resulting set X may be taken as a random element of G.

Example (for a group G of rank less than 4):

$$
\begin{array}{lcllllll}
X_1 & = & \{ & x_1, & x_2, & x_3, & x_4 & \}, \\
X_2 & = & \{ & x_1, & x_4x_2, & x_3, & x_4 & \}, \\
X_3 & = & \{ & x_1x_3, & x_4x_2, & x_3, & x_4 & \}, \\
X_4 & = & \{ & x_1x_3x_4, & x_4x_2, & x_3, & x_4 & \}, \\
X_5 & = & \{ & x_1x_3x_4, & x_4x_2, & x_3x_4x_2, & x_4 & \}, \\
X_6 & = & \{ & x_1x_3x_4, & x_4x_4x_2, & x_3x_4x_2, & x_4 & \}, \\
X_7 & = & \{ & x_1x_3x_4, & x_4x_4x_2, & x_3x_4x_2, & x_1x_3x_4x_4 & \}, \\
 & \vdots & & & & & &
\end{array}
$$

Easy! And very quick!:

Features of the Product Replacement Algorithm:

- Easy to understand
- Very easy to implement
- Works for any finite group
- Very fast! Complexity $O(Nc)$ where $N =$ number of steps and $c =$ cost of a single multiplication in G.
- Elements found are well-distributed according to various criteria and statistical tests.

Let k be the maximal cardinality of a minimal generating set X for G, and suppose $m \geq 2k$. Also let $\mathcal{X}$ be the set of ordered m-tuples of elements of G that generate G, and let X_t be the element of $\mathcal{X}$ obtained by repeating the basic operation t times. Then for every $Y \in \mathcal{X}$, the probability that $X_t = Y$ tends to $1/|\mathcal{X}|$ as $t \to \infty$.

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!