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 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 Γ = 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.
Cayley Graph Example:

\[ G = C_2 \times C_2 \times C_2 \] (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

- Cay\((G, X)\) has order \(|G|\)
- Cay\((G, X)\) is connected if and only if \(G = \langle X \rangle\)
- Every closed walk in Cay\((G, X)\) corresponds to a relation satisfied by the generators from \(X\)
  
  [Why? \(x^e_k \ldots x^e_2 x^e_1 g = g\) if and only if \(x^e_k \ldots x^e_2 x^e_1 = 1\)]
- Cay\((G, X)\) is regular of valency \(|X^\pm| = |X \cup X^-|\)
- The group \(G\) acts transitively on the vertices of \(\Gamma = \text{Cay}(G, X)\) 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 \(\Gamma\) taking vertex 1 to vertex \(h\). ■
Conversely:

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

**Sketch proof.** Take any vertex $v$ of $\Gamma$, 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 $\Gamma$ is connected and is isomorphic to $\text{Cay}(G, X)$. ■
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 $\Gamma = \text{Cay}(G, X)$ 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 $\geq 2$. 
<table>
<thead>
<tr>
<th>d\k</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10</td>
<td>20</td>
<td>38</td>
<td>70</td>
<td>132</td>
<td>196</td>
<td>360</td>
<td>600</td>
<td>1250</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>41</td>
<td>98</td>
<td>364</td>
<td>740</td>
<td>1320</td>
<td>243</td>
<td>7575</td>
<td>17703</td>
</tr>
<tr>
<td>5</td>
<td>24</td>
<td>72</td>
<td>212</td>
<td>624</td>
<td>2772</td>
<td>5516</td>
<td>1703</td>
<td>57840</td>
<td>187056</td>
</tr>
<tr>
<td>6</td>
<td>32</td>
<td>111</td>
<td>390</td>
<td>1404</td>
<td>7917</td>
<td>19383</td>
<td>76461</td>
<td>331387</td>
<td>1253615</td>
</tr>
<tr>
<td>7</td>
<td>50</td>
<td>168</td>
<td>672</td>
<td>2756</td>
<td>11988</td>
<td>52768</td>
<td>249660</td>
<td>1223050</td>
<td>6007230</td>
</tr>
<tr>
<td>8</td>
<td>57</td>
<td>253</td>
<td>1100</td>
<td>5060</td>
<td>39672</td>
<td>131137</td>
<td>734820</td>
<td>4243100</td>
<td>24897161</td>
</tr>
<tr>
<td>9</td>
<td>74</td>
<td>585</td>
<td>1550</td>
<td>8268</td>
<td>75893</td>
<td>279616</td>
<td>1697688</td>
<td>12123288</td>
<td>65866350</td>
</tr>
<tr>
<td>10</td>
<td>91</td>
<td>650</td>
<td>2286</td>
<td>13140</td>
<td>134690</td>
<td>583083</td>
<td>4293452</td>
<td>27997191</td>
<td>201038922</td>
</tr>
<tr>
<td>11</td>
<td>104</td>
<td>715</td>
<td>3200</td>
<td>19500</td>
<td>156864</td>
<td>1001268</td>
<td>7442328</td>
<td>72933102</td>
<td>600380000</td>
</tr>
<tr>
<td>12</td>
<td>133</td>
<td>786</td>
<td>4680</td>
<td>29470</td>
<td>359772</td>
<td>1999500</td>
<td>15924326</td>
<td>158158875</td>
<td>1506252500</td>
</tr>
<tr>
<td>13</td>
<td>162</td>
<td>851</td>
<td>6560</td>
<td>40260</td>
<td>531440</td>
<td>3322080</td>
<td>29927790</td>
<td>249155760</td>
<td>3077200700</td>
</tr>
<tr>
<td>14</td>
<td>183</td>
<td>916</td>
<td>8200</td>
<td>57837</td>
<td>816294</td>
<td>6200460</td>
<td>55913932</td>
<td>600123780</td>
<td>7041746081</td>
</tr>
<tr>
<td>15</td>
<td>187</td>
<td>215</td>
<td>11712</td>
<td>76518</td>
<td>1417248</td>
<td>8599986</td>
<td>90001236</td>
<td>1171998164</td>
<td>1001234898</td>
</tr>
<tr>
<td>16</td>
<td>200</td>
<td>1600</td>
<td>14640</td>
<td>132496</td>
<td>1771560</td>
<td>14882658</td>
<td>140555416</td>
<td>2025125476</td>
<td>12951451931</td>
</tr>
<tr>
<td>17</td>
<td>274</td>
<td>1610</td>
<td>19040</td>
<td>133144</td>
<td>3217872</td>
<td>18495162</td>
<td>220990700</td>
<td>3372648954</td>
<td>153170720</td>
</tr>
<tr>
<td>18</td>
<td>307</td>
<td>1620</td>
<td>23800</td>
<td>171828</td>
<td>4022340</td>
<td>26515120</td>
<td>323037476</td>
<td>576897167</td>
<td>16659077632</td>
</tr>
<tr>
<td>19</td>
<td>338</td>
<td>1638</td>
<td>23970</td>
<td>221676</td>
<td>4024707</td>
<td>39123116</td>
<td>501001000</td>
<td>8855580344</td>
<td>18155097232</td>
</tr>
<tr>
<td>20</td>
<td>381</td>
<td>1958</td>
<td>34952</td>
<td>281820</td>
<td>8947848</td>
<td>55625185</td>
<td>762374779</td>
<td>12951451931</td>
<td>78186295824</td>
</tr>
</tbody>
</table>
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 \( \text{Aut}(G) \)) 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

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

Instead of checking possibilities for $G$ from among groups of order up to $n$, we can (directly) find all quotients of $G$ 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?
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 $\Omega$ of size $n$, we may form a graph with vertex-set $\Omega$, and with edges of the form $\alpha \rightarrow \alpha^{x_i}$ for $1 \leq i \leq d$.

e.g.

\[
\begin{array}{c}
\text{when } x_1 \mapsto (1, 2)(4, 5) \text{ and } x_2 \mapsto (2, 3, 5, 4).
\end{array}
\]
[Given any transitive permutation representation of \( G \) on a set \( \Omega \) of size \( n \), we may form a graph with vertex-set \( \Omega \), and with edges of the form \( \alpha \rightarrow \alpha^{x_i} \) 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 \( Hg \rightarrow Hgx_i \) for \( 1 \leq i \leq d \).

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

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

\[
g : x_1 \mapsto (1, 2)(4, 5) \quad \text{and} \quad x_2 \mapsto (2, 3, 5, 4).
\]
• Every circuit in $\Sigma$ based at the vertex labelled $H$ gives an element of $H$ expressed as a word on $X$

Why? Any path in $\Sigma$ 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 $w \in H$. 

\[ Hx_i \quad Hx_i x_j x_k^{-1} \]

\[ H = Hw \quad \text{etc.} \]
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:

\[
\begin{array}{c|cc|cc}
 x_1 & x_2 & x_1^{-1} & x_2^{-1} \\
1 & 2 & 1 & 2 & 1 \\
2 & 1 & 3 & 1 & 4 \\
3 & 3 & 5 & 3 & 2 \\
4 & 5 & 2 & 5 & 5 \\
5 & 4 & 4 & 4 & 3 \\
\end{array}
\]

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 \(D_1, D_2, D_3:\)

- \(D_1\) on 14 points, where the permutations generate a group isomorphic to \(\text{PSL}(2, 13)\)
- \(D_2\) on 64 points, where the permutations generate a group isomorphic to \(A_{64}\)
- \(D_3\) 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 $D$:

![Diagram with 6 vertices and connections]

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


**Schreier coset graphs**


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!