p-group generation

- Go to p-Quotient Algorithm
- Go to Classification

Conclusion Lecture 2

Things we have discussed in the second lecture:

- the lower exponent-p series of a group G of p-class c is

$$G = P_0(G) > P_1(G) > \ldots > P_c(G) = 1$$

  where $P_{i+1}(G) = [G, P_i(G)]P_i(G)^p$; in particular, $P_1(G) = \Phi(G)$
- p-quotient algorithm: construct consistent wpcp of largest p-class c quotient of a finitely presented group (if it exists)
- if H has rank d and $H \cong F/R$ with F free of rank d, then the p-cover H^* is isomorphic to F/R^* where $R^* = [F, R]R^p$
- application: Burnside problems

Today: the p-group generation algorithm!

p-group generation: descendants

Idea: Constructing new p-groups from old ones!

Descendants of p-groups

Let G be a d-generator p-group of p-class c.
A **descendant** of G is a d-generator p-group H with $H/P_c(H) \cong G$; it is an **immediate descendant** if H has p-class $c+1$, that is, $P_c(H) > P_{c+1}(H) = 1$.

Example 18

The group $G = C_2 \times C_2$ has 2-class $c = 1$.

The 2-class of $D_8 = \langle x_1, x_2, x_3 \mid x_1^2,\ x_2^2 = x_3,\ x_3^2,\ [x_2, x_1] = x_3 \rangle$ is 2.
Since $D_8/P_1(D_8) \cong G$, the group D_8 is an immediate descendant of G.

The group D_{16} has 2-class 3 and satisfies $D_{16}/P_1(D_{16}) \cong C_2 \times C_2$.
Thus D_{16} is a descendant of G, but not an immediate descendant.

Every p-group K of p-class $c > 1$ is an immediate descendant of $K/P_{c-1}(K)$;
if $c = 1$, then $K \cong C_p^d$ is elementary abelian.

p-group generation: p-covering

Given: a d-generator p-group G of p-class c.
Want: list of all immediate descendants H of G (up to isomorphism)
Fact: each $H/P_c(H) \cong G$ and $P_c(H)$ is H-central elementary abelian.

Recall Theorem 13: If H is a d-generator p-group with $H/Z \cong G$ for some central elementary abelian $Z \leq H$, then H is a quotient of the p-cover G^*.

Theorem 19
Every immediate descendant of G is a quotient of the p-cover G^*.

In the following we discuss the p-**group generation algorithm**:

p-group generation algorithm
Input: a p-group G and description of its automorphism group
Output: wpcp's of all immediate descendants of G, up to isomorphism, and a description of their automorphism groups

Descriptions of the algorithm in the literature: Newman (1977), O'Brien (1999)

p-group generation: allowable subgroups

In the following: $G = F/R$ with p-class c, and $G^* = F/R^*$ with $R^* = [R,F]R^p$.

Problem: What quotients of G^* are immediate descendants of G?

Definition

- The p-**multiplicator** of G is the kernel of $G^* \to G$, that is, R/R^*.
- The **nucleus** of G is $P_c(G^*)$; note that $P_c(G^*) \leq R/R^*$.
- If H is an immediate descendant, then there is an epi $G^* \to H$ whose kernel lies in R/R^*. An **allowable subgroup** is a subgroup $Z < R/R^*$ such that G^*/Z is an immediate descendant of G.

The next lemma characterises allowable subgroups:

Lemma 20

A subgroup $Z < R/R^*$ is allowable if and only if $ZP_c(G^*) = R/R^*$.

Thus: $Z < R/R^*$ is allowable if and only if it supplements the nucleus.

p-group generation: allowable subgroups

Recall: $G = F/R$ with p-class c, and $G^* = F/R^*$ with $R^* = [R, F]R^p$.

Lemma 20

A subgroup $Z < R/R^*$ is allowable if and only if $ZP_c(G^*) = R/R^*$.

Proof.

If $Z = M/R^\star$ is allowable, then F/M is an immediate descendant, and so $G \cong (F/M)/(P_c(F)M/M)$. We also know that $G = F/R \cong (F/M)/(R/M)$ by the isomorphism theorem. Since $P_c(G) = P_c(F)R/R = 1$, we have $P_c(F)M \leq R$. Together, it follows that $R = P_c(F)M$, and so $R/R^\star = P_c(G^*)Z$, as claimed.

Conversely, if $Z = M/R^\star$ satisfies $R/R^* = ZP_c(G^*) = MP_c(F)/R^*$, then $R = MP_c(F)$; factoring out M yields $R/M = P_c(F)M/M$.
This shows that $H = G^*/Z = F/M$ satisfies $P_c(H) = P_c(F)M/M = R/M$, so $H/P_c(H) = F/R = G$ and H is immed. desc. since $P_c(H) > P_{c+1}(H) = 1$.

p-group generation: allowable subgroups

Example 21

The group $G = D_{16}$ has p-class $c = 3$ and 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_7 \mid a_1^2 = a_6,\ a_2^2 = a_3 a_4 a_7,\ a_3^2 = a_4 a_5,\ a_4^2 = a_5,\ [a_2, a_1] = a_3,\ [a_3, a_1] = a_4,\ [a_4, a_1] = a_5,\ a_5^2 = a_6^2 = a_7^2 = 1\rangle.$$

The multiplicator is $\langle a_5, a_6, a_7\rangle \cong C_2^3$; the nucleus is $P_c(G^*) = \langle a_5\rangle$.

The subgroups $\langle a_6, a_7\rangle$, $\langle a_5 a_6, a_7\rangle$, $\langle a_6, a_5 a_7\rangle$ are allowable and the corresponding immediate descendants have order 32.

The subgroup $\langle a_5 a_6, a_5 a_7\rangle$ is also allowable, but the resulting quotient is isomorphic to the quotient of G^* by $\langle a_6, a_5 a_7\rangle$.

Considering the factor groups of G^* by all allowable subgroups, a *complete* list of immediate descendants is obtained; this list usually contains isomorphic groups.

p-group generation: isomorphism problem

Recall: $G = F/R$ with p-cover $G^* = F/R^*$ and multiplicator R/R^*.

Equivalence of allowable subgroups

Two allowable subgroups U/R^* and V/R^* are **equivalent** if the corresponding immediate descendants F/U and F/V are isomorphic.

This definition of "equivalence" is useful ...

...only because the equivalence relation can be given a different characterisation by using the automorphism group of G.

p-group generation: isomorphism problem

Extended automorphism

Let $\alpha \in \mathrm{Aut}(G)$; suppose $G = F/R$ is generated by $a_1, a_2, \ldots, a_d$.
For $i = 1, \ldots, d$, let $x_i, y_i \in F$ such that $a_i = x_i R$ and $\alpha(a_i) = y_i R$ for all i.
Define $\alpha^*\colon G^* \to G^*$ by $\alpha^*(x_i R^*) = y_i R^*$ for all i.

Lemma 22

If $\alpha \in \mathrm{Aut}(G)$, then $\alpha^* \in \mathrm{Aut}(G^*)$ is an **extended automorphism**.
It is not uniquely defined by α, but its restriction to R/R^* is.

Proof [Sketch].
First show that α^* is a well-defined homomorphism; let $g = w(x_1, \ldots, x_d) \in F$:
If $g \in R$, then $1R = \alpha(gR) = w(y_1, \ldots, y_d)R$, so $w(y_1, \ldots, y_d) \in R$.
So if $g \in R^*$, then $w(y_1, \ldots, y_d) \in R^*$; recall $R^* = [F, R]R^p$.
The hom α^* is surjective: $G^* = \langle y_1 R^*, \ldots, y_d R^* \rangle$ since $R/R^* \leq \Phi(G^*)$.

Two extensions of α differ only by elements in R/R^*, and words in R are products of p-th powers and commutators. Since R/R^* is elementary abelian and central, the restriction of α^* to R/R^* is uniquely defined by α.

p-group generation: isomorphism problem

Lemma 23

Let $G = F/R$ be as before, and let U/R^* and V/R^* be allowable subgroups. Then $F/U \cong F/V$ if and only if $\alpha^*(U/R^*) = V/R^*$ for some $\alpha \in \mathrm{Aut}(G)$.

Proof [Sketch].

"$\Rightarrow$". Let $\varphi\colon F/U \to F/V$ be an isomorphism. Since F/U is an immed. desc., $(F/U)/P_c(F/U) = G$, and so $P_c(F/U) = R/U$; similarly, $P_c(F/V) = R/V$, and so $\varphi(R/U) = R/V$. Thus φ induces $\alpha \in \mathrm{Aut}(G)$ with extension $\alpha^* \in \mathrm{Aut}(G^*)$. Now we show that $\alpha^*(U/R^*) = V/R^*$: if $g = w(x_1, \ldots, x_d) \in U$, then

$$1V = \varphi(gU) = w(\varphi(x_1U), \ldots, \varphi(x_dU)) = w(y_1V, \ldots, y_dV) = w(y_1, \ldots, y_d)V,$$

which implies $\alpha^*(gR^*) = w(y_1, \ldots, y_d)R^* \in V/R^*$, and so $\alpha^*(U/R^*) = V/R^*$.

"$\Leftarrow$". If H is a group, $N \trianglelefteq H$, and $\gamma \in \mathrm{Aut}(H)$, then $H/N \cong H/\gamma(N)$. This shows that if $\alpha^* \in \mathrm{Aut}(G^*)$ maps U/R^* to V/R^*, then $F/U \cong F/V$.

Via α^*, every $\alpha \in \mathrm{Aut}(G)$ yields a unique permutation $\pi(\alpha)$ of allowable subgrps.

p-group generation: automorphisms

Given: $G = F/R$ and immediate desc. $H = F/M$ for some allowable M/R^*

Want: automorphisms of H, that is, *isomorphisms* $F/M \to F/M$

Recall: every $\alpha \in \mathrm{Aut}(G)$ yields a permutation $\pi(\alpha)$ of allowable subgrps.

Let Σ be the stabiliser of M/R^* under the action of $\mathrm{Aut}(G)$, that is,

$$\Sigma = \langle \zeta \in \mathrm{Aut}(G) \mid \pi(\zeta) \text{ stabilises } M/R^* \rangle.$$

Use Σ to compute

$$S = \langle \zeta^*|_{F/M} \mid \zeta \in \Sigma \rangle \leq \mathrm{Aut}(H),$$

and determine a generating set for

$$T = \langle \beta \in \mathrm{Aut}(H) \mid \beta|_G = \mathrm{id}_G \rangle.$$

Theorem 24

Using the previous notation, $\mathrm{Aut}(H) = \langle S, T, \mathrm{Inn}(H) \rangle$.

(see O'Brien, 1999)

p-group generation: the algorithm

p-group-generation(G, A, s)

Input: group $G = F/R$ of order p^n, its automorphism group A, integer $s \in \mathbb{N}$
Output: immediate descendants of G, up to isomorphism, of order p^{n+s}, and their automorphism groups

construct consistent wpcp of covering $G^* = F/R^*$
for each generator α of A **do**
    compute extension α^*
    compute permutation $\pi(\alpha)$ of allowable subgroups of index p^s in R/R^*
compute orbits of these allowable subgroups under the action of all $\pi(\alpha)$
for each orbit representative $Z = M/R^*$ **do**
    compute a wpcp of the immediate descendant $H = G^*/Z \cong F/M$
    compute generators of the automorphism group of H

p-group generation: example

Consider $G = \mathrm{Pc}\langle\, a_1,\, a_2 \mid a_1^2 = a_2^2 = 1\rangle$ with 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\; a_2^2 = a_5,\; [a_1, a_2] = a_3,\; a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

The multiplicator and nucleus coincide: $M = \langle a_3, a_4, a_5\rangle = P_1(G^*)$.

Thus: every proper subgroup of M is allowable.

Note that Aut$(G) \cong \mathrm{GL}_2(2)$, with generators and extensions

$$\alpha_1\colon (a_1, a_2) \mapsto (a_1 a_2, a_2) \qquad \alpha_1^*\colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_1 a_2, a_2, a_3, a_3 a_4 a_5, a_5)$$
$$\alpha_2\colon (a_1, a_2) \mapsto (a_2, a_1) \qquad \alpha_2^*\colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_2, a_1, a_3, a_5, a_4).$$

For example, observe that

$$\alpha_1^*(a_3) = \alpha_1^*([a_1, a_2]) = [a_1 a_2, a_2] = a_3$$
$$\alpha_1^*(a_4) = \alpha_1^*(a_1^2) = (a_1 a_2)^2 = a_1^2 a_2^2 a_3 = a_3 a_4 a_5$$
$$\alpha_1^*(a_5) = \alpha_1^*(a_2^2) = a_2^2 = a_5$$

p-group generation: example

Consider $G = \mathrm{Pc}\langle\, a_1,\, a_2 \mid a_1^2 = a_2^2 = 1\rangle$ with 2-covering

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

The multiplicator and nucleus coincide: $M = \langle a_3, a_4, a_5\rangle = P_1(G^*)$.

Thus: every proper subgroup of M is allowable.

Note that $\mathsf{Aut}(G) \cong \mathrm{GL}_2(2)$, with generators and extensions

$\alpha_1 \colon (a_1, a_2) \mapsto (a_1a_2, a_2)$ $\quad\alpha_1^* \colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_1a_2, a_2, a_3, a_3a_4a_5, a_5)$

$\alpha_2 \colon (a_1, a_2) \mapsto (a_2, a_1)$ $\quad\alpha_2^* \colon (a_1, a_2, a_3, a_4, a_5) \mapsto (a_2, a_1, a_3, a_5, a_4).$

Immediate descendants of $G = C_2 \times C_2$ of order 8:

There are 7 allowable subgroups of index 2 in M (that is, of rank 2), namely

$$\langle a_4, a_5\rangle,\ \langle a_4, a_3a_5\rangle,\ \langle a_3a_4, a_5\rangle,\ \langle a_3, a_5\rangle,\ \langle a_3, a_4a_5\rangle,\ \langle a_3, a_4\rangle,\ \langle a_3a_4, a_3a_5\rangle$$

There are 3 orbits of allowable subgroups induced by α_1^* and α_2^*:

$$\{\langle a_4, a_5\rangle, \langle a_4, a_3a_5\rangle, \langle a_3a_4, a_5\rangle\},\ \{\langle a_3a_4, a_3a_5\rangle\},\ \{\langle a_3, a_5\rangle, \langle a_3, a_4a_5\rangle, \langle a_3, a_4\rangle\}$$

p-group generation: example

Immediate descendants of $G = C_2 \times C_2$ of order 8

Recall that

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle$$

and allowable subgroups of rank 2 are

$$\{\langle a_4, a_5\rangle, \langle a_4, a_3a_5\rangle, \langle a_3a_4, a_5\rangle\}, \{\langle a_3a_4, a_3a_5\rangle\}, \{\langle a_3, a_5\rangle, \langle a_3, a_4a_5\rangle, \langle a_3, a_4\rangle\}.$$

Choose one rep from each orbit and factor it from G^* to obtain immediate descendants:

$$\begin{aligned}
&\mathrm{Pc}\langle\, a_1, a_2, a_3 \quad \mid \quad a_1^2 = a_2^2 = a_3^2,\ [a_2, a_1] = a_3 \,\rangle \cong D_8 \\
&\mathrm{Pc}\langle\, a_1, a_2, a_3 \quad \mid \quad a_1^2 = a_3,\ a_2^2 = a_3,\ a_3^2 = 1,\ [a_2, a_1] = a_3 \,\rangle \cong Q_8 \\
&\mathrm{Pc}\langle\, a_1, a_2, a_4 \quad \mid \quad a_1^2 = a_4,\ a_2^2 = a_4^2 = 1\rangle \cong C_2 \times C_4
\end{aligned}$$

p-group generation: example

Immediate descendants of $G = C_2 \times C_2$ of order 16

Recall that

$$G^* = \mathrm{Pc}\langle a_1, \ldots, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5,\ [a_1, a_2] = a_3,\ a_3^2 = a_4^2 = a_5^2 = 1\rangle.$$

Allowable subgroups of index 4 are $\langle a_3\rangle$, $\langle a_3^\delta a_4^\gamma a_5\rangle$, $\langle a_3^\zeta a_4\rangle$, with $\delta, \gamma, \zeta \in \{0, 1\}$. The orbits induced by α_1^* and α_2^* are

$$\{\langle a_3\rangle\},\ \ \{\langle a_5\rangle, \langle a_3 a_4 a_5\rangle, \langle a_4\rangle\},\ \ \{\langle a_4 a_5\rangle, \langle a_3 a_5\rangle, \langle a_3 a_4\rangle\}.$$

Choose one rep from each orbit to obtain 3 immediate descendants of order 16. Get $C_4 \times C_4$ and $C_2 \ltimes (C_2 \times C_4)$ and $C_4 \ltimes C_4$, for example,

$$G^*/\langle a_3\rangle = \mathrm{Pc}\langle\, a_1, a_2, a_4, a_5 \mid a_1^2 = a_4,\ a_2^2 = a_5, a_4^2 = a_5^2 = 1\rangle \cong C_4 \times C_4.$$

Immediate descendants of $G = C_2 \times C_2$ of order 32

There is one immediate descendant of order 2^5, namely G^*.

p-group generation: practical issues

Central problem: number of allowable subspaces (and size of orbits)

Example: The immediate descendants of $G = C_p^d$ of order p^{d+s} have p-class 2.
For this group, $M = R/R^* = P_1(G^*)$ has rank $m = d(d+1)/2$;
and each of the $O(p^{(m-s)s})$ subspaces of dim $m - s$ is allowable.

Approach: exploit characteristic structure.
Each $\alpha \in \mathrm{Aut}(G)$ acts on $M \leq G^*$ via $\alpha^* \in \mathrm{Aut}(G^*)$; so M is $\mathrm{Aut}(G)$-module.
In the example, $M = P_1(G^*) = (G^*)^2(G^*)'$ is a characteristic decomposition.
In general, identify characteristic submodules, then process chain of submodules.

More comments on practical issues: see O'Brien (1999)

Classifying p-groups

Go to p-Group Generation
Go to Isomorphisms

GNU: group number

How many groups of order p^n exist?

The number $\mathrm{gnu}(n)$ of groups of order n (up to isomorphism) has been studied in detail[5]; we recall a few bounds:

- **Pyber (1993):** $\mathrm{gnu}(n) \leq n^{(2/27+o(1))\mu(n)^2}$,
  where $\mu(n)$ is largest exponent in the prime-power factorisation of n.
  Idea: count choices for Sylow subgroups, Fitting subgroup, quotients, extensions,. . .
- **Higman (1960):** $\mathrm{gnu}(p^n) \geq p^{2/27(n^3-6n^2)}$
  Idea: count groups of p-class 2
- **Sims (1965), Newman & Seeley (2007):** $\mathrm{gnu}(p^n) \leq p^{2n^3/27+O(n^{5/3})}$
  Idea: enumerate presentations which define groups of order p^n
  Trivial bound: $\mathrm{gnu}(p^n) \leq p^{(n^3-n)/6}$

In conclusion: $p^{(2/27)n^3-O(n^2)} \leq \mathrm{gnu}(p^n) \leq p^{(2/27)n^3+O(n^{5/3})}$ as $n \to \infty$.

[5] Blackburn, Neuman, Venkataraman "Enumeration of finite groups", 2007

GNU: some 2-groups

Besche, Eick & O'Brien (2001) used 2-group generation:

order	#
1	1
2	1
4	2
8	5
16	14
32	51
64	267

order	#
128	2,328
256	56,092
512	10,494,213
1024	49,487,365,422
2048	$>$1,774,274,116,992,170

Number of groups of order ≤ 2000: 49,910,529,484
Number of groups of order 2^{10}: 49,487,365,422
Number of groups of order 2^{10} and class 2: 48,803,495,722

Folklore Conjecture

Almost all groups are 2-groups of 2-class 2.

GNU: p-groups of small order

Number of groups of order p^k, for $k = 1, 2, \ldots, 6$:

$\# \setminus p$	2	3	≥ 5
p	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	X
p^6	267	504	Y

where

$$X = 2p + 61 + 2\gcd(p-1,3) + \gcd(p-1,4)$$
$$Y = 3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5)$$

Order dividing p^4: Cole, Glover, Hölder, Young (all $\sim$ 1893)

Order p^5: Bagnera, Miller, de Séguier, James (1898-1980)

Order p^6: *many* faulty classifications;
eventually Newman, O'Brien, Vaughan-Lee (2004)

GNU: p-groups of small order

Number of groups of order p^7: O'Brien & Vaughan-Lee (2005) computed

# \ p	**2**	**3**	**5**	**≥ 7**
p^7	$2,328$	$9,310$	$34,297$	Z

where

$$Z = 3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 \\ +(4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4) \\ +(3p+31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9)$$

Approach for $n = 5, 6, 7$:

- For $p < n$ use p-group generation.
- For $p \geq n$ use Baker-Campbell-Hausdorff formula and Lazard correspondence between category of nilpotent Lie rings of order p^n and category of p-groups of order p^n. Use analogue of p-group generation algorithm to classify the Lie rings.

GNU: PORC conjecture[6]

PORC Conjecture (Higman 1960)
For n fixed, $\mathrm{gnu}(p^n)$ is Polynomial On Residue Classes.

That is, there exists $m \in \mathbb{N}$ and polynomials $f_0, f_1, \ldots, f_{m-1}$ such that

$$\mathrm{gnu}(p^n) = f_{p \bmod m}(n).$$

Higman (1960): # groups of order p^n and p-class 2 is PORC.

Evseev (2008): # groups of order p^n whose Frattini subgroup is central is PORC.

Vaughan-Lee (2015): # groups of order p^8 and exponent p is PORC.

[6] For a survey see Vaughan-Lee "Graham Higman's PORC Conjecture" (2012)

Conclusion Lecture 3

Things we have discussed in the third lecture:

- (immediate) descendants
- p-group generation algorithm
- p-cover, nucleus, multiplicator, allowable subgroups, extended auts
- automorphism groups of immediate descendants
- the group number gnu for group order p^5, p^6, p^7
- PORC conjecture