Computational group theory for young group theorists II

Jack Schmidt

University of Kentucky

2008-04-18

Computational group theory is a wonderful branch of science studying how to ask questions in group theory in ways amenable to computation and the corresponding methods of answering them algorithmically. Many of the results of this field are made available in the computer software GAP.

Outline

- Why should I avoid finitely presented groups like the plague?
- How do I compute with finite soluble groups?
- How do I search GAP libraries for small counterexamples?
- How do I construct my own finite soluble groups?

Finitely presented groups: friend or foe?

- Topologists love presentations: intrinsically topological and geometrical
- Homologicalists love presentations: intrinsically homological
- Everyone loves presentations: easy to read, deceptively easy to use for small groups
- There does not exist (now or ever) an algorithm that can take 13 elements of a free group on 4 generators, and decide whether the first is a product of conjugates of the others.
- No computer can reliably handle finitely presented groups!
- No one knows if $\langle x, y : x^2 = y^3 = (xy)^{13} = [x, y]^4 = 1 \rangle$ is an infinite group or a group of order $2^{20} \cdot 3^4 \cdot 5^2 \cdot 13^2$.

Finite soluble groups

- A composition series of a finite soluble groups has cyclic factors of prime order
- Let $\{g_1, \ldots, g_n\}$ be preimages of generators of the factors
- Let $G_i = \langle g_i, g_{i+1}, \ldots, g_n \rangle$ be the composition series
- G_{i+1} is normalized by g_i, so for $i < j$, $g_j \in G_{i+1}$ and

$$g_j^{g_i} = \prod_{k=i+1}^{n} g_k^{e_{i,j,k}}$$

- g_i generates G_i/G_{i+1}, so

$$g_i^{p_i} = \prod_{k=i+1}^{n} g_k^{e_{i,i,k}}$$

Collection

- $g_j^{g_i} = w_{i,j}$ can also be viewed as

$$g_j \cdot g_i \mapsto g_i w_{i,j}$$

- Note that $w_{i,j} \in G_{i+1}$ so the smaller indices are all on the left

- Repeatedly using these $\binom{n}{2}$ rules, we can collect any product of generators of G into the form

$$h = \prod_{i=1}^{n} g_i^{h(i)}$$

where the product is taken in order

$$h = g_1^{h(1)} \cdot g_2^{h(2)} \cdots g_n^{h(n)}$$

Polycyclic presentations

- Remember all elements are of the form:

$$h = g_1^{h(1)} \cdot g_2^{h(2)} \cdots g_n^{h(n)}$$

- Using the n rules $g_i^{p_i} \mapsto w_{i,i}$, with $w_{i,i} \in G_{i+1}$ we can ensure that $0 \leq h(i) < p_i$
- Hence the order of G is $\prod_{i=1}^{n} p_i$ and we have a unique expression for every element in the group
- G is completely determined by the n primes p_i, and the $2\binom{n}{3} + \binom{n}{2}$ numbers $e_{i,j,k}$ for $1 \leq i \leq j \leq n$, $i \leq k \leq n$, as they encode the multiplication table
- See chapter 9 of Robinson&Lennox, Sims, or Holt (Eick) for some theoretical information on these presentations
- The important point: in computational group theory, D_8 has three generators, not two

Collection example

- Just to give a feel for it, here is an example:

$$\langle a, b, c : a^3 \mapsto 1, b^2 \mapsto 1, c^2 \mapsto 1, ba \mapsto abc, ca \mapsto ab, cb \mapsto bc \rangle$$

$(p_i) = (3, 2, 2)$ and

$$(e_i) = \left(\begin{bmatrix} . & 0 & 0 \\ . & 1 & 1 \\ . & 1 & 0 \end{bmatrix}, \begin{bmatrix} . & . & . \\ . & . & 0 \\ . & . & 0 \end{bmatrix}, \begin{bmatrix} . & . & . \\ . & . & . \\ . & . & 0 \end{bmatrix} \right)$$

- $[1, 0, 1] \cdot [2, 1, 1]$, that is $a^1 b^0 c^1 \cdot a^2 b^1 c^1$:

$$a\underline{ca}abc = a(abc)\underline{a}bc = aa\underline{b(a}b)bc = aa(abc)\underline{bbc}$$

$$= aaab(\underline{bc)bc} = \underline{aaa}bb(\underline{bc)c} = ()b\underline{bb}() = b() = b$$

Reading finite soluble groups in GAP

- Let's create a finite soluble group in GAP:

```
gap> g := DihedralGroup(8);
<pc group of size 8 with 3 generators>
```

- Not a very unique description!

- Let's figure out who is who. The generators are g.1, g.2, and g.3:

```
gap> List( [g.1,g.2,g.3], Order );
[ 2, 4, 2 ]
```

- Now we know the subgroup generated by g.2 and g.3 is normal of order 4, so g.3 better be $g.2^2$

```
gap> g.2^2 = g.3;
true
```

- g.1 has order 2, so complements g.2, and so acts as inversion on it:

```
gap> g.2^g.1 = g.2^-1;
true
```

Reading off other results

- Notice the center is exhibited:

```
gap> Center(g);
Group([ f3 ]);
```

- Let's multiply two random elements:

```
gap> x := Random(g); y := Random(g); x*y;
f1*f3
f2
f1*f2*f3
```

- Let's multiply not so random elements:

```
gap> g.2*g.1;
f1*f2*f3
```

GAP technicality

- While permutation groups are all considered subgroups of sufficiently large symmetric groups, each PcGroup and each FpGroup is considered to be in its own universe, so if you aren't quite explicit about making subgroups, they are just different groups:

```
gap> DihedralGroup(8) = DihedralGroup(8);
false
gap> IsomorphismGroups(DihedralGroup(8),DihedralGroup(8));
[ f1, f2, f3 ] -> [ f1, f2, f3 ]
gap> g = Group(g.1,g.2);
true
```

Group libraries

- Besche, Eick, O'Brien catalogued the groups of order up to 2000

```
gap> SmallGroupsInformation(12);
There are 5 groups of order 12.
1 is of type 6.2.
2 is of type c12.
3 is of type A4.
4 is of type D12.
5 is of type 2^2x3.
The groups whose order factorises in at most 3 primes have
been classified by O. Hoelder.  This classification is
used in the SmallGroups library.
gap> NumberSmallGroups(12);
5
```

Creation and identification

- You can ask for groups to be created, and can ask for created groups to be identified:

```
gap> h := SmallGroup(8,4);
<pc group of size 8 with 3 generators>
gap> StructureDescription(h);
"Q8"
gap> IdGroup( DihedralGroup(8) );
[ 8, 3 ]
gap> StructureDescription(SmallGroup(8,3));
"D8"
```

Searching

- You can iterate through all small groups with:

```
gap> for n in [1..2000] do
> Print("Working on the ",NrSmallGroups(n)," groups
of order ",n,"\n");
> for k in [1..NrSmallGroups(n)] do
> sg:=SmallGroup(n,k);
> if mytestfunction(sg)
> then Error("Got one!  ",[n,k]);
> fi; od; od;
```

```
gap> IdsOfAllSmallGroups( Size, [3,6..12],
> IsAbelian, false,
> g -> IsNormal(g,SylowSubgroup(g,3)),true);
[ [ 6, 1 ], [ 12, 1 ], [ 12, 4 ] ]
```

Of course there are caveats

- Note that there are 49487365422 groups of order 1024, so it may take a few millennia to complete your search
- Far better is to study your problem and reduce the problem to something manageable
- Might as well have GAP search while you think though!
- There are also libraries of transitive, primitive, perfect, and irreducible groups

What if my group isn't there?

- You can construct your own PcGroups using finite presentations, and if you are careful, GAP will recognize them as PcGroups:

```
gap> f := FreeGroup( 3 );
<free group on the generators [ f1, f2, f3 ]>
gap> g := f/[f.1^2, f.2^2/f.3, f.3^2, f.2^f.1/f.2^-1,
f.3^f.1/f.3, f.3^f.2/f.3 ];
<fp group on the generators [ f1, f2, f3 ]>
gap> Order(g);
8
gap> hom := IsomorphismPcGroup(g);
[ f1, f2, f3 ] -> [ f2, f1, f3 ]
gap> h := Range(hom);; IsPcGroup(h);
true
```

- Notice how GAP decided to use a different composition series. If you are very careful, you can avoid this using a very picky function:

```
gap> PcGroupFpGroup(g);
<pc group of size 8 with 3 generators>
```

Semidirect products and extensions

- GAP has efficient methods for semidirect products and extensions of finite soluble groups

```
gap> g:=ElementaryAbelianGroup(4);;
gap> a:=AutomorphismGroup(g);;
gap> ag:=SemidirectProduct(a,g);
<pc group with 4 generators>
gap> StructureDescription(ag);
"S4"
```

- Extensions are a bit more technical, and I should probably cover them separately. If you are bold just read the help (and the papers):

```
??ExtensionRepresentatives
```

Exercises

- Find the smallest group whose Sylow 2-subgroup is quaternion of order 8, but such that the center of the Sylow subgroup is not central in the whole group
- Use structure description to understand the structure of this group. Why is the example now obvious/why does the example exist?
- Look up Glauberman's "Z* theorem" and "ZJ theorem" and notice that ZJ(Q8) is the center of Q8. These theorems show that this example is actually typical.
- How many non-abelian groups of order 27 and exponent 3 are there?
- Find the smallest group whose Sylow 3-subgroup is non-abelian of order 27 and exponent 3, but whose center is not normal in the whole group. Is the center of the Sylow subnormal in the whole group?
- (hard) If so, is there an example where it is not?

Summary

- Finitely presented groups often do not have answers!
- Polycyclically presented groups do!
- There is even software to answer such questions!
- You can access large libraries of precomputed groups!
- You can construct your own!

The End