Algorithms to find subgroups

Alexander Hulpke

Department of Mathematics

Colorado State University

Fort Collins, CO, 80523-1874

hulpke@math.colostate.edu

http://www.math.colostate.edu/~hulpke

Setup

Let G be a finite group.

Task: Find subgroups of G

- up to conjugacy by G (or $\mathrm{Aut}(G)$)
- all or some
- build subgroups in small steps

Cyclic Extension

(One of the first algorithms in CGT, (NEUBÜSER 1960)).

If $U \leq G$ is not perfect, $U' \leq V < G$ then $U \leq N_G(V)$.

Use this for $p \mid [U:V]^a$, $p \nmid [V:U']$, U/V cyclic, to get a recursive construction:

- For each V compute $N_G(V)$.
- For each (class in) $N_G(V)$, extend U with a representative.

Atoms: Perfect groups,Cyclic subgroups of prime-power order.

Perfect subgroups can all be found in perfect residuum G^∞, use tabulated information about perfect groups (HOLT/PLESKEN)

Problem: Constructs same class often, removing duplicates tedious.

Cyclic extension II

Bookkeeping: A subgroup is determined uniquely by the cyclic subgroups of prime-power order (ZUPPOs) it contains. (Theorem of BENSON and CONWAY for lattices.)

Represent subgroups by bit-list corresponding to Zuppos.

Inclusion then is testable by bit-lists.

For each subgroup found, compute the normalizer and its Zuppos.

Then try extension with all these zuppos.

Check which subgroups (or conjugates of) are contained.

Elementary abelian extension

Suppose that $N \lhd G$ is elementary abelian and $U \leq G$.

Then either

- $N \leq U$ (so $U/N \leq G/N$), or
- $U \leq N$ (easily calculated), or
- $A = \langle N, U \rangle \geq N$, $B = N \cap U \leq N$(so A, B known) *and* U is complement to N/B in A/B.

Construct recursively first subgroups of G/N, then lift by computing complements (uses Cohomology).

Initial step ($G/\mathrm{Rad}(G)$) by cyclic extension or table lookup.

Performs better than pure cyclic extension, but eventually also runs into problems with number of subgroups.

The User wants

Typically only a few specific subgroups.

Or just that subgroups of a particular isomorphism type exist.

One can try to incorporate this in the construction.

What are good filter criteria?

- Can be implemented (Order – total and factored), composition factors.
- Fulfills the users need. (Isomorphism type, particular intersection with other subgroups. Arbitrary other properties)

The intersection of both property lists is rather short.

Subgroups of particular isomorphism type

I want to concentrate on two particular problems: Given G and H, find all subgroups of G that are isomorphic to H.

Special case: $H \cong G/N$, find only H that intersect trivially with N (complements).

(Assume N not solvable.)

First Attempt: Generating sets

- Find a generating set for H.
- Run through all possible images of this in G (up to conjugacy).
- Test.

(The same idea can be used for computing automorphism groups naively, or to find G-quotients of an FP group.)

Problem: Large number of possibilities, exponential search.

- Many choices for images of second, third,... generator
- p-groups require many generators.
- Apart from being a generating set, there is no “connecting” property that would limit the choices.

Idea:

Extend existing subgroups by adding elements that normalize it (or one of its subgroups).

Instead of generators use p-subgroup as start.

Advantages

- Take care of large generator number for p-groups
- Initial search restricted to Sylow subgroup.
- Isomorphism for p-groups: special methods, groups are smaller

Subgroup chain

Build a subgroup chain ("Sylow walk") from $\langle 1\rangle$ to H by the following steps:

- Start with a p_0-subgroup U_0.
- (Step A) If U_i is not self-normalizing, let $\underline{V}$ be a $\underline{p_i}$-Sylow subgroup of $N_G(U_i)$. Let $U_{i+1} = \langle U_i, V\rangle$.
- (Step B) Otherwise let $\underline{P}$ be a Sylow subgroup of U_i for some prime $\underline{p'}$. Let $N = N_G(P)$ and $\underline{V}$ be a $\underline{p_i}$-Sylow subgroup of N. Let $U_{i+1} = \langle U_i, V\rangle$.

(Underlined objects have to be chosen suitably)

Observation: For all groups tested so far, there exists such a walk that reaches G. *Does it hold in general?*

Note: It is sufficient to “reach" every prime factor of H: Every subgroup of a p-group is contained properly in its normalizer.

It is sufficient to show that the following directed graph posesses a hamilton path:

Vertices: Prime divisors

Edges: $p \rightarrow q$ if $q \mid |N_G(P)|$.

Finding subgroups

Subgroups isomorphic H are found accoding to the chosen walk:

Suppose all candidates for embeddings of U_i are known.

For each embedded group: Compute the normalizer N (in case of a step B of the appropriate subgroup(s)).

Find all candidates for p-subgroups V of N.

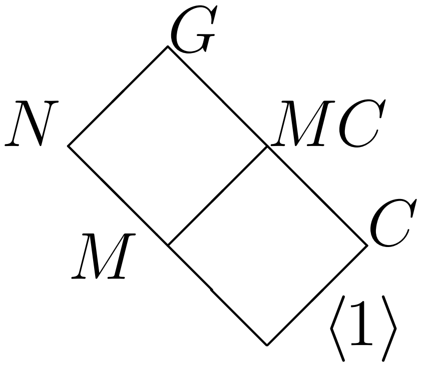
Form closure, check that is has right structure. (Use: Quick discarding if group gets too big.) This are the candidates for U_{i+1} for the next step.

Obvious Question: What is the “best” walk?

Application: Complements

Complements of $N \lhd G$ (monomorphisms from G/N into G, image must intersect trivially with N).

General "homomorphism principle" setup:



Let $M \leq N$, $M \lhd G$, C complement to N in G.

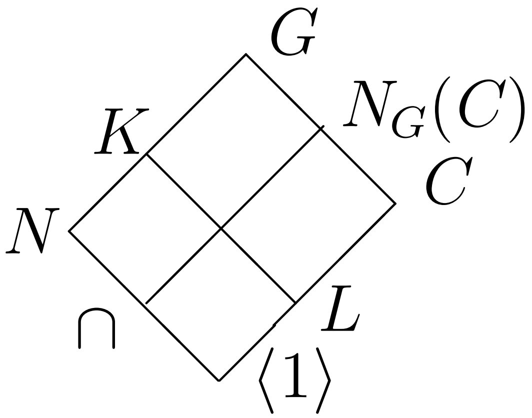
Then MC/M is complement to N/M in G/M and C is complement to M in MC.

Thus compute complements along chief series through N:

If $M_1, M_2 \lhd G$, $M_2 \leq M_1 \leq N$, compute first complements in G/M_1, for each complement C/M_1 compute complements to M_1/M_2 in C/M_2.

For classes, fuse under $N_G(C)$.If M_1/M_2 is elementary abelian, use cohomology.

Structure of G/N



Suppose $N \leq K \lhd G$, C complement to N.

Then there exists $L \lhd C$ with $NL = K$.

Thus $C \leq N_G(C)$, and C is complement to $N \cap N_G(C)$ in $N_G(C)$.

If K/N is elementary abelian, one can compute complements in a p-Sylow subgroup of K.

Therefore: Need walks only for simple G/N.

Remaining case

Now consider the case of N minimal normal, nonabelian.

Suppose we computed a Sylow walk for G/N. Build complements according to this walk.

All intermediate subgroups have to intersect trivially with N.

The inverse of the embedding is (given by) natural homomorphism of N.

We have to find p-subgroups of a subgroup $W \leq G$.

- Let $\bar{W}$ be the image of W in the factor and let $\bar{X}$ be the "right" (according to the chosen walk) p-subgroup of $\bar{W}$.
- Let P be a p-Sylow subgroup of X.
- The desired subgroups are complements to $P \cap N$ in P.
- As P is solvable, one can use cohomology for this.

Implementation

I have a trial implementation in GAP for complements.

In the cases tested (for example $A_5 \wr S_8$, $L_3(2) \wr S_7$, $A_6 \wr S_6$, $M_{11} \wr A_5$) work reasonably well.)

Step A extensions are harmless, Step B extensions can produce several thousand complements.

(Need efficient conjugation action on complements.)

Code will be used in the maximal subgroups routine to deal with the "twisted wreath" case.

Alternative Magma code by CANNON and HOLT.