Finding normal subgroups of even order

Max Neunhöffer

Matrix groups
Finding normal subgroups
A helper theorem
The algorithm
Involution centralisers
Done?
Blind descent
Applications
Performance in examples
Imprimitive groups
What can go wrong?

University of St Andrews

Nikolaus-Blockseminar Aachen, 12.12.2009
The problem

Problem

Let \( 1 < N \trianglelefteq G = \langle g_1, \ldots, g_k \rangle \) be a finite group and \( N \) be a normal subgroup.

Produce a non-trivial element of \( N \) as a word in the \( g_i \) with “high probability”.

- Assume no more knowledge about \( G \) or \( N \).
- I shall tell you soon why we want to do this.
- We are looking for a randomised algorithm.
- Assume we can generate uniformly distributed random elements in \( G \).
- “High probability” means for the moment “higher than \( 1/[G : N]\)”.
Reduction in the imprimitive case

One case in the Matrix Group Recognition Project is:

**Situation**

Let $G \leq \text{GL}_n(F_q)$ acting linearly on $V := F_q^{1 \times n}$, such that $V$ is absolutely irreducible. Assume there is $N$ with $Z(G) < N \triangleleft G$ such that

$$V|_N = W_1 \oplus W_2 \oplus \cdots \oplus W_k,$$

all $W_i$ are invariant under $N$, and $G$ permutes the $W_i$ transitively. Then there is a homomorphism $\varphi : G \rightarrow S_k$.

We can compute the homomorphism once $N$ is found.

Since we can compute normal closures, our initial problem is exactly, what we need to do.
Finding even order normal subgroups

**Theorem**

Let $1 < N \trianglelefteq G$ with $2 \mid |N|$. Let $1 \neq x \in G \setminus Z(G)$ with $x^2 = 1$. Then, for $C := C_G(x)$, we have:

- $1 < C \cap N \trianglelefteq C$ and
- $2 \mid |C \cap N|$.

**Proof:** We have $xNx = N$ and $|N|$ is even. The orbits of $\langle x \rangle$ on $N$ have lengths 1 and 2, so there must be an even number of orbits of length 1.

In particular, $C \cap N$ contains an involution.

That is, we can replace $(N, G)$ with $(C \cap N, C)$ and use the statement again, provided we find another non-central involution.
Finding $N \triangleleft G$

We want to find an $N$ with $1 < N \triangleleft G$ and $2 | |N|$, or conclude that there is none.

Algorithm 1: INVOLUTIONDESCENT

Initialise $H := G$. Then

1. Find a non-central involution $x \in H$. If none found, goto 4.
2. Compute its involution centraliser $C := C_H(x)$.
3. Replace $H$ with $C$ and goto 1.
4. Let $D$ be the group generated by all central involutions we found.
5. For all $1 \neq x \in D$: Test if $\langle x^G \rangle \neq G$.
6. If no normal closure is properly contained, conclude that $G$ does not contain such an $|N|$ as assumed.

We find involutions by powering up random elements.
Computing involution centralisers

We can compute involution centralisers.
Finding $N \triangleleft G$

We want to find an $N$ with $1 < N \triangleleft G$ and $2 \divides |N|$, or conclude that there is none.

**Algorithm 1: INVOLUTIONDESCENT**

Initialise $H := G$. Then

1. **Find** a non-central involution $x \in H$. If none found, goto 4.
2. **Compute** its involution centraliser $C := C_H(x)$.
3. **Replace** $H$ with $C$ and goto 1.
4. Let $D$ be the group generated by all central involutions we found.
5. For all $1 \neq x \in D$: **Test** if $\langle x^G \rangle \neq G$.
6. If no normal closure is properly contained, conclude that $G$ does not contain such an $|N|$ as assumed.

How do we test if we have a proper normal subgroup?

What if $D$ is large?
Finding normal subgroups of even order
Max Neunhöffer

The problem
Matrix groups
Finding normal subgroups
A helper theorem
The algorithm
Involution centralisers
Done?

Blind descent
Applications
Performance in examples
Imprimitive groups
What can go wrong?

Blind descent (Babai, Beals)
Let $1 \neq x, y \in G$ and $G$ non-abelian.
Assume at least one of $x, y$ is contained in a non-trivial proper normal subgroup.
We do not know which!

Aim: Produce $1 \neq z \in G$ that is contained in a non-trivial proper normal subgroup.

Algorithm 3: B\textsc{lindDescent}

1. Consider $c := [x, y] := x^{-1} y^{-1} xy$, if $c \neq 1$, we take $z := c$.
2. If $c = 1$, the elements $x$ and $y$ commute.
   If $x \in Z(G)$, take $z := x$.
3. Compute generators $\{y_i\}$ for $Y := \langle y^G \rangle$.
   - If some $c_i := [x, y_i] \neq 1$, then take $z := c_i$ as in 1.
   - Otherwise $x \in C_G(Y)$ but $x \notin Z(G)$, thus $Y \neq G$, we take $z := y$. 
Combining Algorithms 1 and 3

Algorithm 4: FIND_ELMOEVENNORMALSUBGROUP

Let $G = \langle g_1, \ldots, g_k \rangle \leq GL(d, q)$.

1. Use Algorithm INVOLUTIONDESCENT to produce candidate elements.
   (If there are too many central involutions, select some randomly.)
2. Use BLINDDESCENT to combine them.
3. If any of the candidates is in a proper normal subgroup, then the result will be.

- One non-trivial group element is returned.
- The algorithm is Monte Carlo and could return a wrong result.
### Examples

This approach works well in many important cases:

<table>
<thead>
<tr>
<th>$G$</th>
<th>$N$</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_{20} \wr A_{30}$</td>
<td>$A_5 \times 30$</td>
<td>120</td>
</tr>
<tr>
<td>$\text{SL}(3, 3) \wr A_{10} &lt; \text{GL}(30, 3)$</td>
<td>$\text{SL}(3, 3) \times 10$</td>
<td>724</td>
</tr>
<tr>
<td>$\text{Sp}(6, 3) \otimes 2.O(7, 3) &lt; \text{GL}(48, 3)$ (computing projectively)</td>
<td>$\text{Sp}(6, 3) \otimes 1$ or $1 \otimes 2.O(7, 3)$</td>
<td>645</td>
</tr>
<tr>
<td>$6.\text{Suz} &lt; \text{GL}(12, 25)$</td>
<td>central 2</td>
<td>227</td>
</tr>
<tr>
<td>$S_{100}$</td>
<td>$A_{100}$</td>
<td>165</td>
</tr>
<tr>
<td>$A_{100}$</td>
<td>—</td>
<td>148</td>
</tr>
<tr>
<td>$\text{PSL}(10, 5)$</td>
<td>—</td>
<td>1248</td>
</tr>
<tr>
<td>$\text{PGL}(10, 5)$</td>
<td>$\text{PSL}(10, 5)$</td>
<td>1260</td>
</tr>
</tbody>
</table>

(here we have averaged over 10 runs, times in ms)

The success rate was 100% in all cases (using 200 runs).
Situation

Let $G \leq \text{GL}_n(\mathbb{F}_q)$ acting linearly on $V := \mathbb{F}_q^{1 \times n}$, such that $V$ is absolutely irreducible. Assume there is $N$ with $\text{Z}(G) < N \triangleleft G$ such that

$$V|_N = W_1 \oplus W_2 \oplus \cdots \oplus W_k,$$

all $W_i$ are invariant under $N$, and $G$ permutes the $W_i$ transitively. Then there is a homomorphism $\varphi : G \to S_k$.

We use Algorithm \texttt{FINDELM OF EVEN NORMAL SUBGROUP}, for the result $x$, do:

- compute the normal closure $M := \langle x^G \rangle$,
- use the MeatAxe to check whether $V|_M$ is reducible,
- if $x \in N$, we find a reduction.
Finding normal subgroups of even order

Max Neunhöffer

The problem

Matrix groups

Finding normal subgroups

A helper theorem

The algorithm

Involution centralisers

Done?

Blind descent

Applications

Performance in examples

Imprimitive groups

What can go wrong?

What can go wrong?

Actually, lots of things!

- We could have trouble to find elements of even order.
- An order computation could take unpleasantly long.
- There could be no non-central involutions.
- There could be extremely many central involutions.
- We could get an involution centraliser wrong.
- We might not find all non-central involutions.
- G might not have an even order normal subgroup.