The current state of the recog package

Max Neunhöffer

University of St Andrews

Edinburgh, 28.7.2009

Finding even order normal subgroups

Theorem

Let $1 < N \trianglelefteq G$ *with* $2 \mid |N|$.

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* $x^2 = 1$.

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:*

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*
- $2 \mid |C \cap N|$.

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*
- $2 \mid |C \cap N|$.

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

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*
- $2 \mid |C \cap N|$.

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

Proof: We have $xNx = N$ and $|N|$ is even.

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*
- $2 \mid |C \cap N|$.

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

Proof: We have $xNx = N$ and $|N|$ is even. Thus 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. ∎

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*
- $2 \mid |C \cap N|$.

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

Proof: We have $xNx = N$ and $|N|$ is even. Thus 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. ∎

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 $N \lhd G$

Let $1 < N \unlhd G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: Initialise $H := G$. Then

1. Find a non-central involution $x \in H$. If none found, goto 4.

Finding $N \lhd G$

Let $1 < N \unlhd G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: Initialise $H := G$. Then

1. Find a non-central involution $x \in H$. If none found, goto 4.
2. Compute its involution centraliser $C := C_H(x)$.

Finding $N \triangleleft G$

Let $1 < N \trianglelefteq G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: 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.

Finding $N \lhd G$

Let $1 < N \unlhd G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: 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.

Finding $N \lhd G$

Let $1 < N \unlhd G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: 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 $\langle x^G \rangle \neq G$.

Finding $N \lhd G$

Let $1 < N \trianglelefteq G$ with $2 \mid |N|$ and $N \neq G$.

We can proceed as follows: 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.

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups
- Verification using presentations

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups
- Verification using presentations
- Non-random kernel computation using presentations

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups
- Verification using presentations
- Non-random kernel computation using presentations
- Aschbacher recognition methods for Imprimitive and Tensor

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups
- Verification using presentations
- Non-random kernel computation using presentations
- Aschbacher recognition methods for Imprimitive and Tensor
- Composition series for matrix stabiliser chain leaf

What is missing?

Things we never got around to implement:

- Leedham-Green/O'Brien for classical natural rep
- Lot's of leaf cases
- Any change of representation for leafs
- O'Brien/Wilson base point hints for sporadic groups
- Verification using presentations
- Non-random kernel computation using presentations
- Aschbacher recognition methods for Imprimitive and Tensor
- Composition series for matrix stabiliser chain leaf
- Probably some more I forgot here!

An Idea

We seem not to be able to find polynomial-time algorithms to decide membership in some Aschbacher classes like “Imprimitive” ($\mathcal{C}_2$).

An Idea

We seem not to be able to find polynomial-time algorithms to decide membership in some Aschbacher classes like “Imprimitive” ($\mathcal{C}_2$).

Then lets not do it!

An Idea

We seem not to be able to find polynomial-time algorithms to decide membership in some Aschbacher classes like “Imprimitive” ($\mathcal{C}_2$).

Then lets not do it!

Define for example:

An Idea

We seem not to be able to find polynomial-time algorithms to decide membership in some Aschbacher classes like “Imprimitive” ($\mathcal{C}_2$).

Then lets not do it!

Define for example:

Definition of class $\mathcal{D}_2$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_2$ if

- the natural module V is absolutely irreducible and
- there is $Z(G) < N \lhd G$ such that $V|_N = \bigoplus_{i=1}^k W_i$ and the W_i are absolutely irreducible $\mathbb{F}_q N$-modules and not all isomorphic.

An Idea

We seem not to be able to find polynomial-time algorithms to decide membership in some Aschbacher classes like “Imprimitive” ($\mathcal{C}_2$).

Then lets not do it!

Define for example:

Definition of class $\mathcal{D}_2$

$G \leq \mathrm{GL}_n(\mathbb{F}_q)$ lies in $\mathcal{D}_2$ if

- the natural module V is absolutely irreducible and
- there is $Z(G) < N \lhd G$ such that $V|_N = \bigoplus_{i=1}^k W_i$ and the W_i are absolutely irreducible $\mathbb{F}_q N$-modules and not all isomorphic.

Can we find a polynomial-time algorithm to decide membership in $\mathcal{D}_2$?