Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim

Reductions

### Finding norma

Subgroups
A helper theorem

The algorithm
Involution centralise

#### Blind desce

#### Applications

Imprimitive groups

What can gwrong?

### Finding normal subgroups of even order

### Max Neunhöffer



University of St Andrews

Columbus, 8.10.2009

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding norma

A helper theorem
The algorithm
Involution centraliser

#### Blind desce

#### Applications

Imprimitive groups

What can gwrong?

# The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal

A helper theorem
The algorithm
Involution centralisers

#### Blind desce

#### Applications

Imprimitive groups

What can gwrong?

## The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centralise

#### Blind desce

#### Applications

Performance in example Imprimitive groups

What can gwrong?

### The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

Produce a non-trivial element of N as a word in the gi

Assume no more knowledge about G or N.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

#### Blind desce

### Applications

Performance in examples

What can g

## The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

- Assume no more knowledge about G or N.
- I shall tell you soon why we want to do this.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

#### Blind desce

#### Applications

Performance in examples Imprimitive groups

What can g wrong?

## The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

- 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.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centralise

#### Blind desce

Applications
Performance in examples

What can gwrong?

## The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  be a finite group and N be a normal subgroup.

- 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.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim
Reductions

## Finding normal subgroups

subgroups
A helper theorem
The algorithm
Involution centralises

#### Blind desce

Applications
Performance in examples

What can gwrong?

## The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  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.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim
Reductions

### Finding normal subgroups

Subgroups
A helper theorem
The algorithm
Involution centralise
Done?

#### Blind descer

Applications
Performance in examples

What can g

# The problem

### Problem

Let  $1 < N \triangleleft G = \langle g_1, \dots, g_k \rangle$  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]".

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim

Reduction

Finding normal

A helper theorem
The algorithm

Dlind dooo

Applications

Imprimitive groups

What can gwrong?

# Matrix groups . . .

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim

Reductions

Finding normal subgroups

A helper theorem
The algorithm
Involution centralisers

Blind desce

Applications

Imprimitive groups

What can gwrong?

## Matrix groups . . .

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given: 
$$M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$$

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Reduction

Finding normal subgroups

The algorithm
Involution centraliser
Done?

Blind desce

Applications

Performance in exami

Imprimitive groups

What can gwrong?

### Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given: 
$$M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$$

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Finding normal

A helper theorem
The algorithm
Involution centralisers

Blind descer

Applications

Performance in examp

What can g

## Matrix groups ....

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given: 
$$M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$$

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have 
$$|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$$

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theorem
The algorithm
Involution centraliser

Blind descent

Applications

Performance in examples

What can gwrong?

## Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have 
$$|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$$

### What do we want to determine about G?

• The group order |*G*|

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

Blind descen

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have 
$$|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$$

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theorem
The algorithm
Involution centralises

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

## Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have 
$$|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$$

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?
- Homomorphisms  $\varphi : G \rightarrow H$ ?

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theorem
The algorithm

Involution centralise
Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

## Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have 
$$|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$$

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?
- Homomorphisms  $\varphi : G \rightarrow H$ ?
- Kernels of homomorphisms? Is G simple?

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theorem
The algorithm
Involution centralises

Blind descen

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## Matrix groups ....

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$ .

It is finite, we have  $|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$ 

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?
- Homomorphisms  $\varphi : G \rightarrow H$ ?
- Kernels of homomorphisms? Is G simple?
- Comparison with known groups

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theorem The algorithm

Involution centralise
Done?

Blind descen

Applications

Performance in examples Imprimitive groups

What can gwrong?

## Matrix groups ....

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have  $|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$ 

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?
- Homomorphisms  $\varphi : G \rightarrow H$ ?
- Kernels of homomorphisms? Is G simple?
- Comparison with known groups
- (Maximal) subgroups?

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Finding normal subgroups

A helper theo

The algorithm
Involution centralise
Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## Matrix groups ...

Let  $\mathbb{F}_q$  be the field with q elements and

$$\operatorname{GL}_n(\mathbb{F}_q) := \{ M \in \mathbb{F}_q^{n \times n} \mid M \text{ invertible} \}$$

Given:  $M_1, \ldots, M_k \in \operatorname{GL}_n(\mathbb{F}_q)$ 

Then the  $M_i$  generate a group  $G \leq GL_n(\mathbb{F}_q)$ .

It is finite, we have  $|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$ 

- The group order |G|
- Membership test: Is  $M \in GL_n(\mathbb{F}_q)$  in G?
- Homomorphisms  $\varphi : G \rightarrow H$ ?
- Kernels of homomorphisms? Is *G* simple?
- Comparison with known groups
- (Maximal) subgroups?
- . . . .

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding norma

A helper theorem
The algorithm

Involution centralise
Done?

Blind descen

Applications

Performance in examples

What can gwrong?

# Constructive recognition

### Problem

Let  $\mathbb{F}_q$  be the field with q elements and

$$M_1,\ldots,M_k\in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for  $G := \langle M_1, \ldots, M_k \rangle$ :

- The group order |G| and
- an algorithm that, given  $M \in GL_n(\mathbb{F}_q)$ ,
  - decides, whether or not  $M \in G$ , and,
  - if so, expresses M as word in the  $M_i$ .

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

Involution centralise Done?

Applications

Performance in examples Imprimitive groups

What can gowrong?

## Constructive recognition

### Problem

Let  $\mathbb{F}_q$  be the field with q elements and

$$M_1,\ldots,M_k\in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for  $G := \langle M_1, \dots, M_k \rangle$ :

- The group order |G| and
- an algorithm that, given  $M \in \mathrm{GL}_n(\mathbb{F}_q)$ ,
  - decides, whether or not  $M \in G$ , and,
  - if so, expresses M as word in the Mi.
- The runtime should be bounded from above by a polynomial in n, k and log q.

Max Neunhöffer

The problem

Matrix groups The (immediate) aim

# Finding normal

**Applications** 

## Constructive recognition

### Problem

Let  $\mathbb{F}_q$  be the field with q elements and

$$M_1,\ldots,M_k\in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for  $G := \langle M_1, \ldots, M_k \rangle$ :

- The group order |G| and
- an algorithm that, given  $M \in GL_n(\mathbb{F}_q)$ ,
  - decides, whether or not  $M \in G$ , and,
  - if so, expresses M as word in the  $M_i$ .
- The runtime should be bounded from above by a polynomial in n, k and log q
- A Monte Carlo Algorithm is enough.

Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

Blind doccor

# Applications

Performance in examples

What can g wrong?

# Constructive recognition

### Problem

Let  $\mathbb{F}_q$  be the field with q elements and

$$M_1,\ldots,M_k\in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for  $G := \langle M_1, \dots, M_k \rangle$ :

- The group order |G| and
- an algorithm that, given  $M \in \mathrm{GL}_n(\mathbb{F}_q)$ ,
  - decides, whether or not  $M \in G$ , and.
  - if so, expresses M as word in the  $M_i$ .
- The runtime should be bounded from above by a polynomial in n, k and log q.
- A Monte Carlo Algorithm is enough. (Verification!)

#### Max Neunhöffer

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal

A helper theorem
The algorithm

The algorithm
Involution centralise
Done?

#### Blind descer

Applications
Performance in examples

What can go

# Constructive recognition

### Problem

Let  $\mathbb{F}_q$  be the field with q elements and

$$M_1,\ldots,M_k\in \mathrm{GL}_n(\mathbb{F}_q).$$

Find for  $G := \langle M_1, \ldots, M_k \rangle$ :

- The group order |G| and
- an algorithm that, given  $M \in GL_n(\mathbb{F}_q)$ ,
  - decides, whether or not  $M \in G$ , and.
  - if so, expresses M as word in the Mi.
- The runtime should be bounded from above by a polynomial in n, k and log q.
- A Monte Carlo Algorithm is enough. (Verification!)

If this problem is solved, we call  $\langle M_1, \ldots, M_k \rangle$  recognised constructively.

Max Neunhöffer

#### The problen

Matrix groups

#### Reductions

Finding norma

A helper theorem

Involution centralise
Done?

#### Blind desce

#### Applications

Imprimitive groups

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \ldots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

Max Neunhöffer

The problem

Matrix groups

Reductions

Finding normal

A helper theorem
The algorithm

Involution centralis
Done?

Blind descer

### Applications

Imprimitive groups

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \dots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

A reduction is a group homomorphism

$$\varphi: G \to H$$
 $M_i \mapsto P_i$  for all  $i$ 

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Reductions

Finding normal subgroups

A helper theorem.

Involution centralis
Done?

Blind desce

#### Applications

Performance in examples Imprimitive groups

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \ldots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

A reduction is a group homomorphism

$$\varphi: G \to H$$
 $M_i \mapsto P_i$  for all  $i$ 

with the following properties:

•  $\varphi(M)$  is explicitly computable for all  $M \in G$ 

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Reductions

Finding normal subgroups

A helper theo

The algorith

Involution centralis

Blind descer

Applications

Performance in example: Imprimitive groups

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \dots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

A reduction is a group homomorphism

$$\varphi: G \to H$$
 $M_i \mapsto P_i$  for all  $i$ 

- $\varphi(M)$  is explicitly computable for all  $M \in G$
- $\varphi$  is surjective:  $H = \langle P_1, \dots, P_k \rangle$

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Reductions
Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

Blind descer

Applications

Performance in examples

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \ldots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

A reduction is a group homomorphism

$$\varphi: G \to H$$
 $M_i \mapsto P_i$  for all  $i$ 

- $\varphi(M)$  is explicitly computable for all  $M \in G$
- $\varphi$  is surjective:  $H = \langle P_1, \dots, P_k \rangle$
- *H* is in some sense "smaller"
- or at least "easier to recognise constructively"

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Reductions
Finding normal subgroups

A helper theorem
The algorithm
Involution centralis

Done?

Applications

Performance in examples
Imprimitive groups

What can gwrong?

### What is a reduction?

Let 
$$G := \langle M_1, \dots, M_k \rangle \leq \operatorname{GL}_n(\mathbb{F}_q)$$
.

A reduction is a group homomorphism

$$\varphi: G \to H$$
 $M_i \mapsto P_i$  for all  $i$ 

- $\varphi(M)$  is explicitly computable for all  $M \in G$
- $\varphi$  is surjective:  $H = \langle P_1, \dots, P_k \rangle$
- H is in some sense "smaller"
- or at least "easier to recognise constructively"
- e.g.  $H \leq S_m$  or  $H \leq \operatorname{GL}_{n'}(\mathbb{F}_{q'})$  with  $n' \log q' < n \log q$

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim

Reductions

Finding norma

A helper theorem
The algorithm

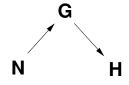
---

Applications

Imprimitive groups

What can g

# Recursion: composition trees We get a tree:



Up arrows: inclusions

Down arrows: homomorphisms

Max Neunhöffer

#### The problen

Matrix groups
The (ultimate) aim
The (immediate) aim

# Reductions Finding norma

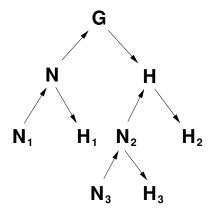
A helper theorem
The algorithm
Involution centralise

#### Blind desce

Performance in examples Imprimitive groups

What can gowrong?

# Recursion: composition trees We get a tree:



Up arrows: inclusions

Down arrows: homomorphisms

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Reductions

Finding normal

A helper theorem
The algorithm
Involution centralise

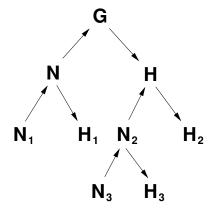
Blind descer Applications

Performance in examples

What can g wrong?

# Recursion: composition trees

We get a tree:



Up arrows: inclusions

Down arrows: homomorphisms

Old idea, substantial improvements are still being made

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim

Reductions

Finding norma

The algorithm
Involution centraliser

Blind desce

Applications

Performance in examp

Imprimitive groups

# Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

Reductions

The algorithm
Involution centralisers
Done?

Blind desce

Applications

Performance in example

What can g

## Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

### Situation

Let  $G \leq GL_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is irreducible.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Reductions
Finding normal

A helper theorem
The algorithm
Involution centralisers

Blind descer

Applications

Performance in examples Imprimitive groups

What can gwrong?

### Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

#### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is 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

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Reductions
Finding normal subgroups

A helper theorem
The algorithm
Involution centralisers

Blind descent Applications

Performance in examples Imprimitive groups

What can gwrong?

### Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

#### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is 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 reduction  $\varphi : G \to S_k$ .

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim
Reductions

Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser:

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

## Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

#### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is 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 reduction  $\varphi : G \to S_k$ .

We can compute the reduction once *N* is found.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Reductions
Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser

Blind descen

Applications
Performance in example

What can gwrong?

## Reduction in the imprimitive case

One case, in which we want to find a reduction, is:

#### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is 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 reduction  $\varphi : G \to S_k$ .

We can compute the reduction once *N* is found.

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

Max Neunhöffer

The probler

Makely ava

The (ultimate) aim

Finding norma

Subgroups
A helper theorem

A helper theore

Involution centralise

Blind desce

Amaliantiana

Imprimitive groups

What can gwrong?

# Finding even order normal subgroups

#### Theorem

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

Max Neunhöffer

The probler

Matrix groups

The (ultimate) aim

Reduction

Finding norma

A helper theorem

The algorithm

Involution centralise
Done?

Blind desce

Performance in example Imprimitive groups

What can gwrong?

# Finding even order normal subgroups

### Theorem

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

Let 
$$1 \neq x \in G \setminus Z(G)$$
 with  $x^2 = 1$ .

Max Neunhöffer

The probler

Matrix groups

The (ultimate) aim

Paductions

Finding norma

A helper theorem

The algorithm Involution centralise

Blind desce

Applications

Imprimitive groups

What can gwrong?

# Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  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:

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim

Reduction

Finding normal

A helper theorem

The election

Involution centralise

Blind descer

#### Applications

Performance in example Imprimitive groups

What can gwrong?

# Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  with 2 | |N|.

Let 
$$1 \neq x \in G \setminus Z(G)$$
 with  $x^2 = 1$ .

Then, for  $C := C_G(x)$ , we have:

- 1 < *C* ∩ *N* ⊴ *C* and
- $\bullet$  2 |  $|C \cap N|$ .

Max Neunhöffer

The problem

Matrix aro

The (ultimate) aim

Reduction

Finding normal

subgroups
A helper theorem

A helper theo

The algorithm Involution cent

D.: . .

Blind descen

Applications

Performance in example: Imprimitive groups

What can gwrong?

### Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  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:

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

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

The problem

Matrix groups

The (immediate) a

Finding normal

Subgroups
A helper theorem
The algorithm

Involution centra
Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

## Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  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:

- $1 < C \cap N \le C$  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.

The problem

Matrix groups
The (ultimate) aim

Reductions

Finding normal subgroups

A helper theorem

The algorithm Involution centr

Involution centralise Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

## Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  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:

- $1 < C \cap N \le C$  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.

#### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

subgroups
A helper theorem

The algorithm
Involution centralise
Done?

#### Blind descer

Applications
Performance in example

What can gwrong?

# Finding even order normal subgroups

#### Theorem

Let  $1 < N \le G$  with 2 | |N|.

Let 
$$1 \neq x \in G \setminus Z(G)$$
 with  $x^2 = 1$ .

Then, for  $C := C_G(x)$ , we have:

- 1 < *C* ∩ *N* ⊴ *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.

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding norma

A helper theore The algorithm

Involution centraliser Done?

Blind desce

Applications

Imprimitive groups

What can gwrong?

# Finding $N \triangleleft G$

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

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theorem
The algorithm

Done?

Blind desce

#### Applications

Performance in example Imprimitive groups

What can gwrong?

# Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

Initialise H := G. Then

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

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

Finding normal subgroups

A helper theor

Involution centralise

Blind descen

Applications
Performance in example

What can g

# Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

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

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Finding normal

A helper theorem
The algorithm

Involution centralise Done?

Blind descent
Applications

Performance in examples Imprimitive groups

What can gwrong?

### Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

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

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

Finding normal subgroups

A helper theor The algorithm

Involution centralise
Done?

Blind descent

Applications
Performance in example:
Imprimitive groups

What can gwrong?

### Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTIONDESCENT

- Find a non-central involution  $x \in H$ . If none found, goto 4.
- **2** Compute its involution centraliser  $C := C_H(x)$ .
- Replace H with C and goto 1.
- 4 Let D be the group generated by all central involutions we found.

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

Finding normal subgroups

A helper the

The algorithm Involution cent

Involution centralise Done?

Blind descent

Applications
Performance in example
Imprimitive groups

What can g

### Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

- Find a non-central involution  $x \in H$ . If none found, goto 4.
- **2** Compute its involution centraliser  $C := C_H(x)$ .
- Replace H with C and goto 1.
- Let D be the group generated by all central involutions we found.
- **5** For all  $1 \neq x \in D$ : Test if  $\langle x^G \rangle \neq G$ .

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

Finding normal subgroups

A helper theorem

The algorithm Involution centralis

Blind descen

Applications
Performance in example
Imprimitive groups

What can gwrong?

### Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

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

The problem

Matrix groups
The (ultimate) aim
The (immediate) ain

Finding normal subgroups

A helper theorem. The algorithm

Involution centralise
Done?

Blind descen

Applications
Performance in example:
Imprimitive groups

What can gwrong?

### Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

Initialise H := G. Then

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

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Reductions

Finding norma

A helper theorem

Involution centralisers

Blind desce

Applications

Imprimitive groups

What can gwrong?

# Involution centralisers

How can we compute the centraliser of an involution?

Max Neunhöffer

The problem

Matrix groups

The (immediate) aim
Reductions

Finding normal subgroups

A helper theo

The algorithm

Involution centralisers
Done?

Blind descent

Applications

Imprimitive groups

What can wrong?

### Involution centralisers

How can we compute the centraliser of an involution?

The following method by John Bray does the job:

### Algorithm 2: InvolutionCentraliser

**Input:**  $G = \langle g_1, \dots, g_k \rangle$  and an involution  $x \in G$ . initialise *gens* := [x] repeat

y := RANDOMELEMENT(G)

 $c := x^{-1}y^{-1}xy$  and o := ORDER(c)

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

The (immediate) aim
Reductions

Finding normal subgroups

A helper theo

The algorithm

Involution centralisers

Involution centralise Done?

Blind descen

Applications

Performance in examples

What can gwrong?

### Involution centralisers

How can we compute the centraliser of an involution?

The following method by John Bray does the job:

### Algorithm 2: InvolutionCentraliser

```
Input: G = \langle g_1, \dots, g_k \rangle and an involution x \in G. initialise gens := [x]
repeat
y := \mathsf{RANDOMELEMENT}(G)
c := x^{-1}y^{-1}xy \text{ and } o := \mathsf{ORDER}(c)
if o is even then
\mathsf{append}\ c^{o/2}\ \mathsf{and}\ (x^{-1}yxy^{-1})^{o/2}\ \mathsf{to}\ gens
else
\mathsf{append}\ z := y \cdot c^{(o-1)/2}\ \mathsf{to}\ gens
```

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

The (immediate) aim Reductions

Finding normal subgroups

A helper theor

The algorithm

Involution centralisers
Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can gwrong?

### Involution centralisers

How can we compute the centraliser of an involution?

The following method by John Bray does the job:

### Algorithm 2: InvolutionCentraliser

```
Input: G = \langle g_1, \dots, g_k \rangle and an involution x \in G.
initialise gens := [x]
repeat
      y := RANDOMELEMENT(G)
      c := x^{-1}y^{-1}xy and o := ORDER(c)
      if o is even then
            append c^{o/2} and (x^{-1}vxv^{-1})^{o/2} to gens
      else
            append z := y \cdot c^{(o-1)/2} to gens
until o was odd often enough or gens long enough
return gens
```

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theor

The algorithm

Involution centralisers
Done?

Blind descent

Performance in examples

What can g wrong?

### Involution centralisers

How can we compute the centraliser of an involution?

The following method by John Bray does the job:

### Algorithm 2: InvolutionCentraliser

```
Input: G = \langle g_1, \dots, g_k \rangle and an involution x \in G.
initialise gens := [x]
repeat
      y := RANDOMELEMENT(G)
      c := x^{-1}y^{-1}xy and o := ORDER(c)
      if o is even then
            append c^{o/2} and (x^{-1}vxv^{-1})^{o/2} to gens
      else
            append z := v \cdot c^{(o-1)/2} to gens
until o was odd often enough or gens long enough
return gens
```

Note: If xy = yx then  $c = 1_G$  and o = 1 and z = y.

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal subgroups

A helper theo

Involution centralisers

Blind descen

Applications
Performance in examples

What can go wrong?

### Involution centralisers

else

How can we compute the centraliser of an involution?

The following method by John Bray does the job:

### Algorithm 2: INVOLUTIONCENTRALISER

```
Input: G = \langle g_1, \dots, g_k \rangle and an involution x \in G. initialise gens := [x] repeat y := \mathsf{RANDOMELEMENT}(G) c := x^{-1}y^{-1}xy and o := \mathsf{ORDER}(c) if o is even then append c^{o/2} and (x^{-1}yxy^{-1})^{o/2} to gens
```

append  $z := y \cdot c^{(o-1)/2}$  to *gens* until o was odd often enough or gens long enough return *gens* 

Note: If xy = yx then  $c = 1_G$  and o = 1 and z = y. And: If o is odd, then z is uniformly distributed in  $C_G(x)$ .

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

The (immediate) aim Reductions

Finding normal subgroups
A helper theorem
The algorithm

Done?

Applications

Performance in examples Imprimitive groups

What can gwrong?

## Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

- Find a non-central involution  $x \in H$ . If none found, goto 4.
- ② Compute its involution centraliser  $C := C_H(x)$ .
- 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  $\langle x^G \rangle \neq G$ .
- $\bullet$  If no normal closure is properly contained, conclude that G does not contain such an |N| as assumed.

Max Neunhöffer

The problem

Matrix groups

The (immediate) ain Reductions

Finding normal subgroups A helper theorem The algorithm

Involution centralise
Done?

Blind descen

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## Finding $N \triangleleft G$

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

### Algorithm 1: INVOLUTION DESCENT

Initialise H := G. Then

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

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) aim
Reductions

Finding normal subgroups

A helper theor

The algorithm
Involution centralise

Blind descen

Applications
Performance in examples
Imprimitive groups

What can g wrong?

### Finding $N \triangleleft G$

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

### Algorithm 1: InvolutionDescent

Initialise H := G. Then

- Find a non-central involution  $x \in H$ . If none found, goto 4.
- **2** Compute its involution centraliser  $C := C_H(x)$ .
- 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  $\langle x^G \rangle \neq G$ .
- 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?

Max Neunhöffer

#### The problen

Matrix groups
The (ultimate) aim
The (immediate) aim

### Finding norma

A helper theorem
The algorithm
Involution centralises

#### Blind descent

#### Applications

Imprimitive groups

What can gwrong?

### Blind descent (Babai, Beals) Let $1 \neq x, y \in G$ and G non-abelian.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theorem
The algorithm
Involution centraliser

Blind descent

#### Applications

Performance in example Imprimitive groups

What can gwrong?

## 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.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Finding normal subgroups

A helper theorem
The algorithm
Involution centralisers

#### Blind descent

Applications

Performance in examples

Performance in example: Imprimitive groups

What can gwrong?

## 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!

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

Finding normal subgroups

The algorithm
Involution centralisers
Done?

# Blind descent Applications

Performance in examples Imprimitive groups

What can gwrong?

## 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.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

Finding normal

A helper theorem
The algorithm
Involution centralise

Blind descent

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## 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: BLINDDESCENT

• Consider  $c := [x, y] := x^{-1}y^{-1}xy$ , if  $c \ne 1$ , we take z := c.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim

The (immediate) air Reductions

Finding normal subgroups

The algorithm
Involution centrali

Blind descent

Applications
Performance in examples
Imprimitive groups

What can gwrong?

# 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: BLINDDESCENT

- Consider  $c := [x, y] := x^{-1}y^{-1}xy$ , if  $c \ne 1$ , we take z := c.
- If c = 1, the elements x and y commute. If  $x \in Z(G)$ , take z := x.

The problem

Matrix groups
The (ultimate) aim
The (immediate) ain

Finding normal subgroups

A helper theorem
The algorithm
Involution centra

Blind descent

Applications
Performance in examples

What can g

### 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: BLINDDESCENT

- Consider  $c := [x, y] := x^{-1}y^{-1}xy$ , if  $c \ne 1$ , we take z := c.
- 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.

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) ain

Finding normal subgroups

A helper theore

Done?

Blind descent

Applications
Performance in examples

What can gwrong?

## 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: BLINDDESCENT

- Consider  $c := [x, y] := x^{-1}y^{-1}xy$ , if  $c \ne 1$ , we take z := c.
- 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.

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain

Finding normal subgroups

A helper theorem
The algorithm

Involution centralise Done?

Blind descent

Applications
Performance in examples
Imprimitive groups

What can gwrong?

## Combining Algorithms 1 and 3

## Algorithm 4: FINDELMOFEVENNORMALSUBGROUP

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

- Use Algorithm InvolutionDescent to produce candidate elements.
  - (If there are too many central involutions, select some randomly.)
- Use BLINDDESCENT to combine them.

Max Neunhöffer

### The problem

Matrix groups

The (ultimate) aim
The (immediate) aim
Reductions

# Finding normal subgroups

A helper theorem
The algorithm

The algorithm Involution centralise Done?

# Blind descent Applications

Performance in examples Imprimitive groups

What can gwrong?

# Combining Algorithms 1 and 3

### Algorithm 4: FINDELMOFEVENNORMALSUBGROUP

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

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

Max Neunhöffer

The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

Finding normal subgroups

A helper theorem
The algorithm

The algorithm
Involution centralise
Done?

#### Blind descent

Applications
Performance in examples
Imprimitive groups

What can gwrong?

# Combining Algorithms 1 and 3

## Algorithm 4: FINDELMOFEVENNORMALSUBGROUP

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

- Use Algorithm INVOLUTIONDESCENT to produce candidate elements.
   (If there are too many central involutions, select
  - some randomly.)
- Use BLINDDESCENT to combine them.
- If any of the candidates is in a proper normal subgroup, then the result will be.
  - One non-trivial group element is returned.

#### Max Neunhöffer

### The problem

Matrix groups

The (ultimate) aim
The (immediate) ain
Reductions

# Finding normal subgroups

A helper theorem

The algorithm
Involution centralise
Done?

### Blind descent

Applications
Performance in examples
Imprimitive groups

What can gwrong?

# Combining Algorithms 1 and 3

## Algorithm 4: FINDELMOFEVENNORMALSUBGROUP

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

- Use Algorithm INVOLUTIONDESCENT to produce candidate elements.
   (If there are too many central involutions, select
- some randomly.)
- Use BLINDDESCENT to combine them.
- 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.

Max Neunhöffer

### The problen

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding norm

# Subgroups A helper theorem The algorithm

Blind descen

Performance in examples

What can g wrong?

## Examples

### This approach works well in many important cases:

G	N	time
<i>A</i> <sub>20</sub> ≀ <i>A</i> <sub>30</sub>	$A_5^{ imes 30}$	120
$SL(3,3) \wr A_{10} < GL(30,3)$	$SL(3,3)^{\times 10}$	724
$Sp(6,3) \otimes 2.O(7,3) < GL(48,3)$	Sp(6, 3) ⊗ 1	645
(computing projectively)	or $1 \otimes 2.0(7,3)$	
6.Suz < GL(12, 25)	central 2	227
S <sub>100</sub>	A <sub>100</sub>	165
A <sub>100</sub>	_	148
PSL(10,5)		1248
PGL(10, 5)	PSL(10, 5)	1260

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

Max Neunhöffer

### The problem

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding normal

# A helper theorem The algorithm

Blind doccon

Performance in examples
Imprimitive groups

What can g wrong?

## Examples

### This approach works well in many important cases:

G	N	time
<i>A</i> <sub>20</sub> ≀ <i>A</i> <sub>30</sub>	$A_5^{ imes 30}$	120
$SL(3,3) \wr A_{10} < GL(30,3)$	$SL(3,3)^{\times 10}$	724
$Sp(6,3) \otimes 2.O(7,3) < GL(48,3)$	Sp(6, 3) ⊗ 1	645
(computing projectively)	or $1 \otimes 2.0(7,3)$	
6.Suz < GL(12, 25)	central 2	227
S <sub>100</sub>	A <sub>100</sub>	165
A <sub>100</sub>		148
PSL(10,5)	_	1248
PGL(10, 5)	PSL(10, 5)	1260

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

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

Max Neunhöffer

The problem

Matrix groups

Finding normal

**Applications** 

Imprimitive groups

## Reductions for imprimitive matrix groups

### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that *V* is 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 reduction  $\varphi: G \to S_k$ .

### The problem

### Matrix groups

The (ultimate) aim
The (immediate) air
Reductions

## Finding normal subgroups

A helper theorei

The algorithm
Involution centralise
Done?

# Blind descen Applications

Performance in example: Imprimitive groups

What can gwrong?

# Reductions for imprimitive matrix groups

### Situation

Let  $G \leq \operatorname{GL}_n(\mathbb{F}_q)$  acting linearly on  $V := \mathbb{F}_q^{1 \times n}$ , such that V is 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 reduction  $\varphi : G \to S_k$ .

We use Algorithm FINDELMOFEVENNORMALSUBGROUP, 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.

### Max Neunhöffer

#### The problem

Matrix groups

The (immediate) air

### Finding norma

subgroups
A helper theorem

Involution centralise

#### Blind desce

### Applications

Imprimitive groups

# What can go wrong?

## What can go wrong?

Max Neunhöffer

The problem

Matrix groups
The (ultimate) aim
The (immediate) ain

Finding norma

A helper theorem
The algorithm
Involution centralisers

Blind desce

Applications

Performance in examples Imprimitive groups

What can go wrong?

# What can go wrong?

Max Neunhöffer

The problen

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding norma

A helper theorem
The algorithm
Involution centraliser

Blind desce

### Applications

Imprimitive groups

What can go wrong?

## What can go wrong?

## Actually, lots of things!

We could have trouble to find elements of even order.

Max Neunhöffer

#### The probler

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding normal subgroups

A helper theorem
The algorithm
Involution centralisers
Done?

#### Blind descei

### Applications

Performance in examples Imprimitive groups

What can go wrong?

## What can go wrong?

- We could have trouble to find elements of even order.
- An order computation could take unpleasantly long.

Max Neunhöffer

### The probler

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding normal subgroups

A helper theorem
The algorithm
Involution centralise
Done?

# Applications

Performance in example Imprimitive groups

What can go wrong?

## What can go wrong?

- We could have trouble to find elements of even order.
- An order computation could take unpleasantly long.
- There could be no non-central involutions.

Max Neunhöffer

#### The probler

Matrix groups
The (ultimate) aim
The (immediate) aim

# Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser
Done?

# Blind descen Applications

Performance in examples Imprimitive groups

What can go wrong?

## What can go wrong?

- 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.

Max Neunhöffer

#### The probler

Matrix groups
The (ultimate) aim
The (immediate) aim
Reductions

## Finding normal subgroups

A helper theorem
The algorithm
Involution centraliser
Done?

#### Blind desce

Applications
Performance in examples
Imprimitive groups

What can go wrong?

## What can go wrong?

- 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.

Max Neunhöffer

#### The probler

Matrix groups
The (ultimate) aim
The (immediate) aim

## Finding normal subgroups

A helper theorem
The algorithm
Involution centralises
Done?

#### Blind descer

Applications
Performance in examples
Imprimitive groups

What can go wrong?

## What can go wrong?

- 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.

Max Neunhöffer

### The probler

Matrix groups
The (ultimate) aim
The (immediate) ain
Reductions

## Finding normal subgroups

A helper theorem
The algorithm
Involution centralised
Done?

#### Blind descer

Applications
Performance in examples
Imprimitive groups

What can go wrong?

## What can go wrong?

- 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.