Max Neunhöffer

The Problem

An example

Order polynomials

The standard

approach
The characteristic

polynomial The minimal polynomia

A Monte Carlo

approach
Computing order

A Monte Carlo algorithm

Rack to the example

Computing Minimal Polynomials

Max Neunhöffer

Lehrstuhl D für Mathematik RWTH Aachen

Oberwolfach in July 2006

Max Neunhöffer

The Problem

An example

Order polynomia

The standard approach

polynomial
The minimal polynomia

The minimal polynomia

approach

Computing or

polynomials

A Monte Carlo algorithm

Back to the example

All of this is joint work with Cheryl Praeger

and is based on earlier ideas of

Peter Neumann and Cheryl Praeger.

Max Neunhöffer

The Problem

Order polynomial

The standard

approach The characteristic

polynomial The minimal polynomia

A Monte Carl

approacn
Computing order

polynomials

Back to the example

The Problem

Max Neunhöffer

The Problem An example

The standard

An example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$

Max Neunhöffer

The Problem An example

The standard

An example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

Max Neunhöffer

The Problem

Order polynomials
The standard

approach
The characteristic

The characteristic polynomial The minimal polynomi

A Monte Carl approach

Computing order polynomials

A Monte Carlo algorit

Back to the example

An example

Baby Monster group $B=\langle a,b\rangle$ with $a,b\in\mathbb{F}_2^{4370\times4370}$ Consider $M:=a+b+ab\in\mathbb{F}_2^{4370\times4370}$ Computing

• the characteristic polynomial χ_M of M takes

Max Neunhöffer

The Problem

Order polynomials

The standard

approach
The characteristic

The characteristic polynomial The minimal polynomia

A Monte Carlo approach

Computing order polynomials

A Monte Carlo algori

A Monte Carlo algori

An example

Baby Monster group $B=\langle a,b\rangle$ with $a,b\in\mathbb{F}_2^{4370\times4370}$ Consider $M:=a+b+ab\in\mathbb{F}_2^{4370\times4370}$ Computing

• the characteristic polynomial χ_M of M takes 8.5s

Max Neunhöffer

The Problem An example

The standard

An example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

Computing

- the characteristic polynomial χ_M of M takes 8.5s
- the minimal polynomial μ_M of M takes

Max Neunhöffer

The Problem An example

The standard

A Monte Carlo

An example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

Computing

- the characteristic polynomial χ_M of M takes 8.5s
- the minimal polynomial μ_M of M takes 9600s

(times in GAP, other systems behave similarly).

Max Neunhöffer

The Problem
An example

Order polynomials
The standard

approach
The characteristic

The characteristic polynomial The minimal polynomia

A Monte Carlo approach

Computing order polynomials

polynomials

A Monte Carlo

Back to the example

An example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

Computing

- the characteristic polynomial χ_M of M takes 8.5s
- the minimal polynomial μ_M of M takes 9600s

(times in GAP, other systems behave similarly).

Questions

What is going on here?

Max Neunhöffer

The Problem
An example

Order polynomials

The standard

approach
The characteristic

The characteristic polynomial The minimal polynomia

A Monte Carlo approach

Computing order polynomials

polynomials

A Monte Carlo

Back to the example

An example

Baby Monster group $B=\langle a,b\rangle$ with $a,b\in\mathbb{F}_2^{4370\times4370}$ Consider $M:=a+b+ab\in\mathbb{F}_2^{4370\times4370}$

Computing

- the characteristic polynomial χ_M of M takes 8.5s
- the minimal polynomial μ_M of M takes 9600s

(times in GAP, other systems behave similarly).

Questions

What is going on here?

What can we do about this?

Max Neunhöffer

The Problem
An example

Order polynomials

The standard

approach
The characteristic

The characteristic polynomial The minimal polynomia

A Monte Carlo approach

Computing order polynomials

polynomials

A Monte Carlo

Back to the example

An example

Baby Monster group $B=\langle a,b\rangle$ with $a,b\in\mathbb{F}_2^{4370\times4370}$ Consider $M:=a+b+ab\in\mathbb{F}_2^{4370\times4370}$

Computing

- the characteristic polynomial χ_M of M takes 8.5s
- the minimal polynomial μ_M of M takes 9600s

(times in GAP, other systems behave similarly).

Questions

What is going on here?

What can we do about this?

Is this a typical example?

Max Neunhöffer

The Problem

Order polynomials

The standard

Order polynomials

Definition (Order polynomial)

 \mathbb{F} field, \mathcal{A} f.d. \mathbb{F} -algebra, $V \in \mathsf{mod}$ - \mathcal{A} , $v \in V$, $M \in \mathcal{A}$. Then the order polynomial $q := \operatorname{ord}_{M}(v) \in \mathbb{F}[x]$ is the monic polynomial of least degree such that $v \cdot q(M) = 0$.

Max Neunhöffer

The Problem

Order polynomials The standard

Order polynomials

Definition (Order polynomial)

 \mathbb{F} field, \mathcal{A} f.d. \mathbb{F} -algebra, $V \in \text{mod-}\mathcal{A}$, $v \in V$, $M \in \mathcal{A}$. Then the order polynomial $q := \operatorname{ord}_{M}(v) \in \mathbb{F}[x]$ is the monic polynomial of least degree such that $v \cdot q(M) = 0$.

Definition (Relative order polynomial)

If additionally W < V is M-invariant, then we call $\operatorname{ord}_{M}(v+W)$ the relative order polynomial of $v + W \in V/W$.

Max Neunhöffer

The Problem Order polynomials

The standard

Order polynomials

Definition (Order polynomial)

 \mathbb{F} field, \mathcal{A} f.d. \mathbb{F} -algebra, $V \in \mathsf{mod}$ - \mathcal{A} , $v \in V$, $M \in \mathcal{A}$. Then the order polynomial $q := \operatorname{ord}_{M}(v) \in \mathbb{F}[x]$ is the monic polynomial of least degree such that $v \cdot q(M) = 0$.

Definition (Relative order polynomial)

If additionally W < V is M-invariant, then we call $\operatorname{ord}_{M}(v+W)$ the relative order polynomial of $v + W \in V/W$.

Lemma (Generator of annihilator)

The order polynomial $\operatorname{ord}_{M}(v)$ divides every polynomial $q \in \mathbb{F}[x]$ with $v \cdot q(M) = 0$.

Max Neunhöffer

The Problem

Order polynomial

The standard

approach

polynomial
The minimal polynomia

The minimal polynomia

A Monte Car

Computing or

polynomials

A Monte Carlo algorithm

Back to the example

The standard approach

What is going on here?

Max Neunhöffer

The Problem

An example

Order polynomia

The standard

The characteristic polynomial

polynomial The minimal polynomia

A Monte Carlo

approach

Computing order

A Monte Carlo algorithm

Back to the examp

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span.

Max Neunhöffer

The Problem
An example
Order polynomials

The standard approach
The characteristic polynomial

polynomial The minimal polynomia

A Monte Carlo approach

Computing order polynomials

A Monte Carlo algorithm Back to the example

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span. Find smallest $d_1 \in \mathbb{N}$ such that $(v_1, v_1 M, v_1 M^2, \ldots, v_1 M^{d_1})$ is linearly dependent.

Max Neunhöffer

The Problem

The standard The characteristic

polynomial

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span. Find smallest $d_1 \in \mathbb{N}$ such that $(v_1, v_1 M, v_1 M^2, \dots, v_1 M^{d_1})$ is linearly dependent. If

$$v_1 M^{d_1} = \sum_{i=0}^{d_1-1} a_i v_1 M^i$$
 then $\operatorname{ord}_M(v_1) = x^{d_1} - \sum_{i=0}^{d_1-1} a_i x^i$.

Max Neunhöffer

The Problem
An example
Order polynomials

The standard approach
The characteristic polynomial

polynomial
The minimal polynomia

A Monte Carlo approach Computing order polynomials A Monte Carlo algorithm

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span. Find smallest $d_1 \in \mathbb{N}$ such that $(v_1, v_1 M, v_1 M^2, \ldots, v_1 M^{d_1})$ is linearly dependent. If

$$v_1 M^{d_1} = \sum_{i=0}^{d_1-1} a_i v_1 M^i$$
 then $\operatorname{ord}_M(v_1) = x^{d_1} - \sum_{i=0}^{d_1-1} a_i x^i$.

Choose some $v_2 \in V \setminus \langle v_1 \rangle_M$ and find smallest $d_2 \in \mathbb{N}$, such that $(v_1, v_1 M, \dots, v_1 M^{d_1-1}, v_2, v_2 M, \dots, v_2 M^{d_2})$ is linearly dependent.

Max Neunhöffer

The Problem
An example

The standard approach
The characteristic

polynomial
The minimal polynomia

A Monte Carl approach

Computing ord polynomials

A Monte Carl

Back to the example

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span. Find smallest $d_1 \in \mathbb{N}$ such that $(v_1, v_1 M, v_1 M^2, \ldots, v_1 M^{d_1})$ is linearly dependent. If

$$v_1 M^{d_1} = \sum_{i=0}^{d_1-1} a_i v_1 M^i$$
 then $\operatorname{ord}_M(v_1) = x^{d_1} - \sum_{i=0}^{d_1-1} a_i x^i$.

Choose some $v_2 \in V \setminus \langle v_1 \rangle_M$ and find smallest $d_2 \in \mathbb{N}$, such that $(v_1, v_1 M, \dots, v_1 M^{d_1-1}, v_2, v_2 M, \dots, v_2 M^{d_2})$ is linearly dependent. If

$$v_2 M^{d_2} = \sum_{i=0}^{d_1-1} b_i v_1 M^i + \sum_{i=0}^{d_2-1} c_i v_2 M^i$$
 then $\operatorname{ord}_M(v + \langle v_1 \rangle_M) = x^{d_2} - \sum_{i=0} c_i x^i.$

Max Neunhöffer

The Problem
An example

Order polynomi

The standard approach
The characteristic

The characteristic polynomial
The minimal polynomia

A Monte Carl approach

Computing ord polynomials

A Monte Carlo algorithm

Back to the example

The characteristic polynomial

Let $v_1, \ldots, v_i \in V$, and $V_i := \langle v_1, \ldots, v_i \rangle_M$ the $\mathbb{F}[M]$ -span. Find smallest $d_1 \in \mathbb{N}$ such that $(v_1, v_1 M, v_1 M^2, \ldots, v_1 M^{d_1})$ is linearly dependent. If

$$v_1 M^{d_1} = \sum_{i=0}^{d_1-1} a_i v_1 M^i$$
 then $\operatorname{ord}_M(v_1) = x^{d_1} - \sum_{i=0}^{d_1-1} a_i x^i$.

Choose some $v_2 \in V \setminus \langle v_1 \rangle_M$ and find smallest $d_2 \in \mathbb{N}$, such that $(v_1, v_1 M, \dots, v_1 M^{d_1-1}, v_2, v_2 M, \dots, v_2 M^{d_2})$ is linearly dependent. If

$$v_2 M^{d_2} = \sum_{i=0}^{d_1-1} b_i v_1 M^i + \sum_{i=0}^{d_2-1} c_i v_2 M^i$$
 then $\operatorname{ord}_M(v + \langle v_1 \rangle_M) = x^{d_2} - \sum c_i x^i.$

Going on like this we find an \mathbb{F} -basis Y of V:

$$Y := (v_1, v_1 M, \dots, v_1^{d_1-1}, \dots, v_k, v_k M, \dots, v_k M_k^{d_k-1}).$$

Max Neunhöffer

The Problem

An example

The standard

The characteristic

polynomial The minimal polynomi

A Monte Carlo

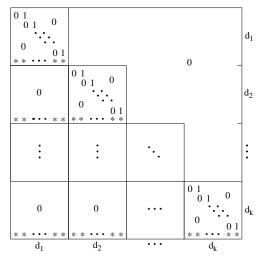
Computing o

polynomials

A Monte Carlo alg

Pool to the evernele

The matrix $Y \cdot M \cdot Y^{-1}$



- Block lower-triangular
- with companion matrices along diagonal
- some sparse garbage below the diagonal

Max Neunhöffer

The Problem

The standard

The minimal polynomial

The minimal polynomial

 \rightarrow compute the absolute order polynomials ord_M(v_i) instead the relative ones $\operatorname{ord}_M(v_i + \langle v_1, \dots, v_{i-1} \rangle)_M$.

Max Neunhöffer

The Problem

The standard

The minimal polynomial

The minimal polynomial

 \rightarrow compute the absolute order polynomials ord_M(v_i) instead the relative ones $\operatorname{ord}_M(v_i + \langle v_1, \dots, v_{i-1} \rangle)_M$.

Lemma (Minimal polynomial)

If
$$V = \langle v_1, \dots, v_k \rangle_M$$
 then $\mu_M = \operatorname{lcm}(\operatorname{ord}_M(v_1), \dots, \operatorname{ord}_M(v_k)).$

Max Neunhöffer

The Problem

Order polynomi

The standard approach

The character polynomial

The minimal polynomial

The minimal polyn

A Monte Carlo approach

Computing order polynomials

polynomials

A Monte Carlo a

Back to the example

The minimal polynomial

 \rightarrow compute the absolute order polynomials $\operatorname{ord}_M(v_i)$ instead the relative ones $\operatorname{ord}_M(v_i + \langle v_1, \dots, v_{i-1} \rangle)_M$.

Lemma (Minimal polynomial)

If
$$V = \langle v_1, \dots, v_k \rangle_M$$
 then $\mu_M = \operatorname{lcm}(\operatorname{ord}_M(v_1), \dots, \operatorname{ord}_M(v_k)).$

Problem:

- $\dim_{\mathbb{F}}(V_i) \dim_{\mathbb{F}}(V_{i-1})$ might be small
- even if $\dim_{\mathbb{F}}(V_i)$ is big.

(set
$$V_i := \langle v_1, \ldots, v_i \rangle_M$$
)

Max Neunhöffer

The Problem

The standard

The minimal polynomial

The minimal polynomial

 \rightarrow compute the absolute order polynomials ord_M(v_i) instead the relative ones $\operatorname{ord}_M(v_i + \langle v_1, \dots, v_{i-1} \rangle)_M$.

Lemma (Minimal polynomial)

If
$$V = \langle v_1, \dots, v_k \rangle_M$$
 then $\mu_M = \operatorname{lcm}(\operatorname{ord}_M(v_1), \dots, \operatorname{ord}_M(v_k)).$

Problem:

- $\dim_{\mathbb{F}}(V_i) \dim_{\mathbb{F}}(V_{i-1})$ might be small
- even if $\dim_{\mathbb{F}}(V_i)$ is big.

(set
$$V_i := \langle v_1, \ldots, v_i \rangle_M$$
)

Characteristic polynomial: asymptotically $\leq 5n^3$ field ops.

Max Neunhöffer

The Problem

The standard

The minimal polynomial

The minimal polynomial

 \rightarrow compute the absolute order polynomials ord_M(v_i) instead the relative ones $\operatorname{ord}_M(v_i + \langle v_1, \dots, v_{i-1} \rangle)_M$.

Lemma (Minimal polynomial)

If
$$V = \langle v_1, \dots, v_k \rangle_M$$
 then $\mu_M = \operatorname{lcm}(\operatorname{ord}_M(v_1), \dots, \operatorname{ord}_M(v_k)).$

Problem:

- $\dim_{\mathbb{F}}(V_i) \dim_{\mathbb{F}}(V_{i-1})$ might be small
- even if $\dim_{\mathbb{F}}(V_i)$ is big.

(set
$$V_i := \langle v_1, \ldots, v_i \rangle_M$$
)

Characteristic polynomial: asymptotically $\leq 5n^3$ field ops.

Minimal polynomial: asymptotically $\sim n^4$ field ops.

(both worst case analysis)

Max Neunhöffer

The Problem

The standard

A Monte Carlo approach

A Monte Carlo approach

What can we do about it?

Max Neunhöffer

The Problem

An example
Order polynomial

Order polynomials

The standard

approach

polynomial

The minimal polynomi

A Monte Carlo approach

Computing order polynomials

polynomials

A Monte Carlo alg

Back to the example

Two lemmas

Lemma (Order polynomials in cyclic spaces)

Let $W := \langle v \rangle_M < V$ be a cyclic subspace and $p := \operatorname{ord}_M(v)$ be the order polynomial of v. Let $w = v \cdot q(M) \in W$ with $\deg(q) < \deg(p)$. Then

$$\operatorname{ord}_M(w) = \frac{p}{\gcd(p,q)}.$$

Max Neunhöffer

The Problem

The standard

Computing order

Two lemmas

Lemma (Order polynomials in cyclic spaces)

Let $W := \langle v \rangle_M < V$ be a cyclic subspace and $p := \operatorname{ord}_{M}(v)$ be the order polynomial of v. Let $w = v \cdot q(M) \in W$ with $\deg(q) < \deg(p)$. Then

$$\operatorname{ord}_M(w) = \frac{p}{\gcd(p,q)}.$$

Lemma (Relative and absolute order polynomials)

Let W < V be M-invariant and $v \in V$. If $q := \operatorname{ord}_{M}(v + W)$ is the relative order polynomial of v, then $v \cdot q(M) \in W$ and

$$\operatorname{ord}_M(v) = q \cdot \operatorname{ord}_M(v \cdot q(M)).$$

Max Neunhöffer

The Problem

The standard

Computing order polynomials

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \cdots < V_k = V.$$

Max Neunhöffer

The Problem

An example
Order polynomia

The standard approach

The characteristic polynomial
The minimal polynomia

A Monte Carl
approach
Computing order

polynomials

A Monte Carlo al

Back to the exampl

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \dots < V_k = V.$$

Start with $v \in V_j$ for some $1 \le j \le k$. Then

• compute $q_j := \operatorname{ord}_M(v + V_{j-1})$ in V_j/V_{j-1} (gcd computation with $\operatorname{ord}_M(v_j + V_{j-1})$),

Max Neunhöffer

The Problem

The standard

Computing order

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \cdots < V_k = V.$$

Start with $v \in V_i$ for some $1 \le i \le k$. Then

- compute $q_i := \operatorname{ord}_M(v + V_{i-1})$ in V_i/V_{i-1} (gcd computation with ord_M($v_i + V_{i-1}$)),
- evaluate $v_i \cdot q_i(M) \in V_{i-1}$,

Max Neunhöffer

The Problem
An example

Order polynomials

The standard approach

The characteristic polynomial The minimal polynomia

A Monte Carl approach

Computing order polynomials

Back to the example

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \cdots < V_k = V.$$

Start with $v \in V_j$ for some $1 \le j \le k$. Then

- compute $q_j := \operatorname{ord}_M(v + V_{j-1})$ in V_j/V_{j-1} (gcd computation with $\operatorname{ord}_M(v_j + V_{j-1})$),
- evaluate $v_j \cdot q_j(M) \in V_{j-1}$,
- proceed inductively,

Max Neunhöffer

The Problem

The standard

Computing order

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \dots < V_k = V.$$

Start with $v \in V_i$ for some $1 \le j \le k$. Then

- compute $q_i := \operatorname{ord}_M(v + V_{i-1})$ in V_i/V_{i-1} (gcd computation with ord_M($v_i + V_{i-1}$)),
- evaluate $v_i \cdot q_i(M) \in V_{i-1}$,
- proceed inductively,
- take product $\prod_{i=1}^{j} q_i$.

The Problem
An example
Order polynomials

The standard approach

The characteristic aslumanial

The characteristic polynomial The minimal polynomial

approach
Computing order polynomials

A Monte Carlo algorithmack to the example

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \cdots < V_k = V.$$

Start with $v \in V_j$ for some $1 \le j \le k$. Then

- compute $q_j := \operatorname{ord}_M(v + V_{j-1})$ in V_j/V_{j-1} (gcd computation with $\operatorname{ord}_M(v_j + V_{j-1})$),
- evaluate $v_j \cdot q_j(M) \in V_{j-1}$,
- proceed inductively,
- take product $\prod_{i=1}^{j} q_i$.
- \rightarrow use sparseness of YMY^{-1} by "thinking in basis Y"

The Problem
An example
Order polynomials

The standard approach

The characteristic polynomial The minimal polynomial

A Monte Car approach Computing order

polynomials
A Monte Carlo algo

Back to the example

Computing order polynomials

We now use the filtration

$$0 = V_0 < V_1 < V_2 < \cdots < V_k = V.$$

Start with $v \in V_j$ for some $1 \le j \le k$. Then

- compute $q_j := \operatorname{ord}_M(v + V_{j-1})$ in V_j/V_{j-1} (gcd computation with $\operatorname{ord}_M(v_j + V_{j-1})$),
- evaluate $v_j \cdot q_j(M) \in V_{j-1}$,
- proceed inductively,
- take product $\prod_{i=1}^{j} q_i$.
- \rightarrow use sparseness of YMY^{-1} by "thinking in basis Y"

Needs $\leq (j+8) \cdot D^2 + j \cdot D$ field ops. where $D := \dim_{\mathbb{F}}(V_j)$.

Max Neunhöffer

The Problem

The standard

A Monte Carlo algorithm

A Monte Carlo algorithm

Proposition

Let $\mathbb{F} = \mathbb{F}_q$, randomise $v_1, \ldots, v_u \in V$ independently and uniformly distributed, $\chi_M = \prod_{i=1}^t q_i^{e_i}$. Then:

$$\mathsf{Prob}\left(\mathsf{lcm}(\mathsf{ord}_{M}(v_1),\ldots,\mathsf{ord}_{M}(v_u))=\mu_{M}\right)$$

is at least
$$\prod (1 - q^{-u \deg(q_i)})$$
.

The Problem An example

An example Order polynomia

The standard approach

The characteristic polynomial The minimal polynomia

A Monte Carlo

approach

Computing ord polynomials

polynomials

A Monte Carlo algorithm

Rack to the example

A Monte Carlo algorithm

Proposition

Let $\mathbb{F} = \mathbb{F}_q$, randomise $v_1, \ldots, v_u \in V$ independently and uniformly distributed, $\chi_M = \prod_{i=1}^t q_i^{e_i}$. Then:

$$\mathsf{Prob}\left(\mathsf{lcm}(\mathsf{ord}_{M}(v_1),\ldots,\mathsf{ord}_{M}(v_u))=\mu_{M}\right)$$

$$\prod_{i=1}^{l} (1-q^{-u\deg(q_i)}).$$

Algorithm: Input M, $0 < \epsilon < 1/2$

- Compute χ_M , Y, ord_M($v_i + V_{i-1}$) for $1 \le i \le k$
- Determine least u, such that probability $> 1 \epsilon$
- Compute $\operatorname{ord}_M(v_1), \ldots, \operatorname{ord}_M(v_u)$
- Return least common multiple

The Problem

Order polynomia

The standard

The characteristic polynomial

A Monte Carlo

Computing orde

polynomials

A Monte Carlo algorithm

Back to the example

A Monte Carlo algorithm

Proposition

Let $\mathbb{F} = \mathbb{F}_q$, randomise $v_1, \ldots, v_u \in V$ independently and uniformly distributed, $\chi_M = \prod_{i=1}^t q_i^{e_i}$. Then:

$$\mathsf{Prob}\left(\mathsf{lcm}(\mathsf{ord}_{M}(v_1),\ldots,\mathsf{ord}_{M}(v_u))=\mu_{M}\right)$$

$$\prod_{i=1}^t (1-q^{-u\deg(q_i)}).$$

Algorithm: Input M, $0 < \epsilon < 1/2$

- Compute χ_M , Y, ord_M($v_i + V_{i-1}$) for $1 \le i \le k$
- Determine least u, such that probability $> 1 \epsilon$
- Compute $\operatorname{ord}_M(v_1), \ldots, \operatorname{ord}_M(v_u)$
- Return least common multiple

Needs asymptotically $\leq 5n^3 + \mathsf{FACTORISATION}(n)$ field ops.

Max Neunhöffer

The Problem

The standard

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

Max Neunhöffer

The Problem

Order polynomia

The standard approach

polynomial
The minimal polynomia

A Monte Car approach

Computing order polynomials

Back to the example

Back to the example

Baby Monster group $B=\langle a,b\rangle$ with $a,b\in\mathbb{F}_2^{4370\times4370}$ Consider $M:=a+b+ab\in\mathbb{F}_2^{4370\times4370}$

The new algorithm needs

• 13.3 s to compute μ_M with $\epsilon = 1/100$

Max Neunhöffer

The Problem

The standard

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

Max Neunhöffer

The Problem

Order polynomia

The standard approach

The characteristic polynomial The minimal polynomia

A Monte Carlo

Computing ord polynomials

polynomials

A Monte Carlo

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

How typical is this example?

Max Neunhöffer

The Problem

The standard

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

How typical is this example?

Irreducible factors of χ_M :

deg	1	1	2	4	6	88	197	854	934
χм	2	2277	4	1	1	1	1	1	1
μ_{M}	1	5	4	1	1	1	1	1	1

Max Neunhöffer

The Problem
An example

The standard approach

The characteristic

The characteristic polynomial The minimal polynomi

A Monte Carlo

Computing order polynomials A Monte Carlo algorithm Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

How typical is this example?

Irreducible factors of χ_M :

deg	1	1	2	4	6	88	197	854	934
χм	2	2277	4	1	1	1	1	1	1
μ_{M}	1	5	4	1	1	1	1	1	1

What we see is

• typical behaviour for such matrices,

Max Neunhöffer

The Problem
An example

The standard approach

The characteristic

The characteristi polynomial The minimal poly

A Monte Carlo approach

Computing order polynomials

A Monte Carlo algorithm

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

How typical is this example?

Irreducible factors of χ_M :

deg	1	1	2	4	6	88	197	854	934
χм	2	2277	4	1	1	1	1	1	1
μ_{M}	1	5	4	1	1	1	1	1	1

What we see is

- typical behaviour for such matrices,
- most matrices are not of this type,

Max Neunhöffer

The Problem

The standard

Back to the example

Back to the example

Baby Monster group $B = \langle a, b \rangle$ with $a, b \in \mathbb{F}_2^{4370 \times 4370}$ Consider $M := a + b + ab \in \mathbb{F}_2^{4370 \times 4370}$

The new algorithm needs

- 13.3 s to compute μ_M with $\epsilon = 1/100$
- 30.0 s with deterministic verification afterwards

How typical is this example?

Irreducible factors of χ_M :

ſ	deg	1	1	2	4	6	88	197	854	934
	χм	2	2277	4	1	1	1	1	1	1
	μ_{M}	1	5	4	1	1	1	1	1	1

What we see is

- typical behaviour for such matrices,
- most matrices are not of this type,
- however, such matrices might occur in applications.