Computing Minimal Polynomials
Max Neunhöffer

The Problem
An example
Order polynomials
The standard approach
The characteristic polynomial
The minimal polynomial

A Monte Carlo approach
Computing order polynomials
A Monte Carlo algorithm

Lehrstuhl D für Mathematik
RWTH Aachen

Oberwolfach in July 2006
All of this is joint work with Cheryl Praeger and is based on earlier ideas of Peter Neumann and Cheryl Praeger.
The Problem
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 $\chi_M$ of $M$ takes 8.5s
- the minimal polynomial $\mu_M$ 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?
Order polynomials

**Definition (Order polynomial)**

\[ \mathbb{F} \text{ field, } \mathcal{A} \text{ f.d. } \mathbb{F}\text{-algebra, } V \in \text{mod-}\mathcal{A}, \ v \in V, \ M \in \mathcal{A}. \]

Then the order polynomial \( q := \text{ord}_M(v) \in \mathbb{F}[x] \) 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 \( \text{ord}_M(v + W) \) the relative order polynomial of \( v + W \in V/W. \)

**Lemma (Generator of annihilator)**

The order polynomial \( \text{ord}_M(v) \) divides every polynomial \( q \in \mathbb{F}[x] \) with \( v \cdot q(M) = 0. \)
The standard approach

What is going on here?
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

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

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

$$\text{ord}_M(v + \langle v_1 \rangle_M) = x^{d_2} - \sum_{i=0}^{d_2-1} c_i x^i.$$  

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

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

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

\[ \rightarrow \text{compute the absolute order polynomials } \text{ord}_M(v_i) \]

instead the relative ones \( \text{ord}_M(v_i + \langle v_1, \ldots, v_{i-1} \rangle) \).

**Lemma (Minimal polynomial)**

If \( V = \langle v_1, \ldots, v_k \rangle_M \) then

\[ \mu_M = \text{lcm}(\text{ord}_M(v_1), \ldots, \text{ord}_M(v_k)). \]

**Problem:**

- \( \dim_F(V_i) - \dim_F(V_{i-1}) \) might be small
- even if \( \dim_F(V_i) \) is big.

(\( \text{set } V_i := \langle v_1, \ldots, v_i \rangle_M \))

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

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

(both worst case analysis)
A Monte Carlo approach

What can we do about it?
Two lemmas

Lemma (Order polynomials in cyclic spaces)

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

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

Lemma (Relative and absolute order polynomials)

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

$$\text{ord}_M(v) = q \cdot \text{ord}_M(v \cdot q(M)).$$
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 \( 1 \leq j \leq k \). Then

- compute \( q_j := \text{ord}_M(v + V_{j-1}) \) in \( V_j/V_{j-1} \)
  (gcd computation with \( \text{ord}_M(v_j + V_{j-1}) \)),
- evaluate \( v_j \cdot q_j(M) \in V_{j-1} \),
- proceed inductively,
- take product \( \prod_{i=1}^j q_j \).

→ use sparseness of \( YMY^{-1} \) by “thinking in basis \( Y \)”

Needs \( \leq (j + 8) \cdot D^2 + j \cdot D \) field ops. where \( D := \dim_F(V_j) \).
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:

$$\text{Prob} \left( \text{lcm}(\text{ord}_M(v_1), \ldots, \text{ord}_M(v_u)) = \mu_M \right)$$

is at least

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

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

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

Needs asymptotically $\leq 5n^3 + \text{FACTORISATION}(n)$ field ops.
Back to the example

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

Consider $M := a + b + ab \in \mathbb{F}_{2}^{4370 \times 4370}$

The new algorithm needs

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

How typical is this example?

Irreducible factors of $\chi_M$:

<table>
<thead>
<tr>
<th>deg</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>88</th>
<th>197</th>
<th>854</th>
<th>934</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_M$</td>
<td>2</td>
<td>2277</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\mu_M$</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

What we see is

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