M4GB: An Efficient Gröbner Basis Algorithm

Rusydi H. Makarim[1,2] Marc Stevens[2]

[1]Mathematics Institute, University Leiden

[2]Cryptology Group, Centrum Wiskunde en Informatica (CWI)

ALGANT-DOC Meeting, 15th May 2017

1 Introduction

2 Gröbner Basis

3 M4GB Algorithm

4 Performance Comparison

5 Solving MQ Challenges

Table of Contents

1. Introduction
2. Gröbner Basis
3. M4GB Algorithm
4. Performance Comparison
5. Solving MQ Challenges

Problem

- $\mathbb{F}$ - A Field
- n - number of variables
- m - number of equations

Problem

- $\mathbb{F}$ - A Field
- n - number of variables
- m - number of equations

Problem (Multivariate Quadratic(MQ) problem)

Problem

- $\mathbb{F}$ - A Field
- n - number of variables
- m - number of equations

Problem (Multivariate Quadratic(MQ) problem)

- *Given :* $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, $\deg(f_i) = 2$

Problem

- $\mathbb{F}$ - A Field
- n - number of variables
- m - number of equations

Problem (Multivariate Quadratic(MQ) problem)

- *Given* : $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, $\deg(f_i) = 2$
- *Problem* : *Find a* $(v_1, \ldots, v_n) \in \mathbb{F}^n$ *such that*

$$\begin{aligned} f_1(v_1, \ldots, v_n) &= 0 \\ &\vdots \\ f_m(v_1, \ldots, v_n) &= 0 \end{aligned}$$

Why MQ Problem ?

- MQ-problem is NP-complete

Why MQ Problem ?

- MQ-problem is NP-complete
- Candidate for post-quantum public-key and digital-signature scheme

Why MQ Problem ?

- MQ-problem is NP-complete
- Candidate for post-quantum public-key and digital-signature scheme
- Need to understand its practical difficulty (How ?)

Why MQ Problem ?

- MQ-problem is NP-complete
- Candidate for post-quantum public-key and digital-signature scheme
- Need to understand its practical difficulty (How ?)

Open Public Challenge - MQChallenge

- Initiated at 2015
- Random and dense system
- Various parameters

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$			
$m \approx 2/3n$			

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
$m \approx 2/3n$			

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$m \approx 2/3n$			

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$m \approx 2/3n$	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$m \approx 2/3n$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$m \approx 2/3n$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

Require at least one month for Magma 2.19-9 to solve using Four 6-cores Intel(R) Xeon(R) CPU E5-4617 @ 2.9GHz and 1TB of RAM.

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$m \approx 2/3n$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

Require at least one month for Magma 2.19-9 to solve using Four 6-cores Intel(R) Xeon(R) CPU E5-4617 @ 2.9GHz and 1TB of RAM.

`https://www.mqchallenge.org`

Solving MQ-problem

- Linearization

Solving MQ-problem

- Linearization
- Extended Linearization (XL)

Solving MQ-problem

- Linearization
- Extended Linearization (XL)

This talk

Gröbner basis

Table of Contents

1. Introduction
2. Gröbner Basis
3. M4GB Algorithm
4. Performance Comparison
5. Solving MQ Challenges

Ordering Monomial in $\mathbb{F}[x_1, \ldots, x_n]$

Definition (Monomial Ordering)

$>$ is a monomial ordering if

Ordering Monomial in $\mathbb{F}[x_1, \ldots, x_n]$

Definition (Monomial Ordering)

$>$ is a monomial ordering if

1. Total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$

Ordering Monomial in $\mathbb{F}[x_1, \ldots, x_n]$

Definition (Monomial Ordering)

$>$ is a monomial ordering if

1. Total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$
2. Let $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ and $x = (x_1, \ldots, x_n)$

$$x^\alpha > x^\beta \Rightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

Ordering Monomial in $\mathbb{F}[x_1, \ldots, x_n]$

Definition (Monomial Ordering)

$>$ is a monomial ordering if

1. Total (or linear) ordering on $\mathbb{Z}^n_{\geq 0}$
2. Let $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ and $x = (x_1, \ldots, x_n)$

$$x^\alpha > x^\beta \Rightarrow x^\gamma x^\alpha > x^\gamma x^\beta$$

3. $>$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$

Monomial Ordering : Examples

Lexicographic

$$x^\alpha >_{\mathrm{lex}} x^\beta \Leftrightarrow \text{the leftmost nonzero entry of } \alpha - \beta \text{ is positive}$$

Monomial Ordering : Examples

Lexicographic

$$x^\alpha >_{\text{lex}} x^\beta \Leftrightarrow \text{the leftmost nonzero entry of } \alpha - \beta \text{ is positive}$$

Degree-Reverse Lexicographic (degrevlex)

$x^\alpha >_{\text{degrevlex}} x^\beta \Leftrightarrow$

Monomial Ordering : Examples

Lexicographic

$$x^\alpha >_{\text{lex}} x^\beta \Leftrightarrow \text{the leftmost nonzero entry of } \alpha - \beta \text{ is positive}$$

Degree-Reverse Lexicographic (degrevlex)

$x^\alpha >_{\text{degrevlex}} x^\beta \Leftrightarrow$

- $\sum_i \alpha_i > \sum_i \beta_i$ OR

Monomial Ordering : Examples

Lexicographic

$$x^\alpha >_{\text{lex}} x^\beta \Leftrightarrow \text{the leftmost nonzero entry of } \alpha - \beta \text{ is positive}$$

Degree-Reverse Lexicographic (degrevlex)

$x^\alpha >_{\text{degrevlex}} x^\beta \Leftrightarrow$

- $\sum_i \alpha_i > \sum_i \beta_i$ OR
- $\sum_i \alpha_i = \sum_i \beta_i$ and the rightmost nonzero entry of $\alpha - \beta$ is negative

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- LM(f) (the largest monomial of f w.r.t $>$)

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- $\mathrm{LM}(f)$ (the largest monomial of f w.r.t $>$)
- $\mathrm{LC}(f)$ (the coefficient correspond to $\mathrm{LM}(f)$)

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- $\mathrm{LM}(f)$ (the largest monomial of f w.r.t $>$)
- $\mathrm{LC}(f)$ (the coefficient correspond to $\mathrm{LM}(f)$)
- $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- $\mathrm{LM}(f)$ (the largest monomial of f w.r.t $>$)
- $\mathrm{LC}(f)$ (the coefficient correspond to $\mathrm{LM}(f)$)
- $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$
- $\mathrm{Tail}(f) = f - \mathrm{LT}(f)$

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- $\mathrm{LM}(f)$ (the largest monomial of f w.r.t $>$)
- $\mathrm{LC}(f)$ (the coefficient correspond to $\mathrm{LM}(f)$)
- $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$
- $\mathrm{Tail}(f) = f - \mathrm{LT}(f)$
- $\mathrm{Term}(f)$, $\mathrm{Mono}(f)$

Notations

$\mathbb{F}[x_1, \ldots, x_n]$ together with $>$

Notations

$f \in \mathbb{F}[x_1, \ldots, x_n]$, $f \neq 0$

- $\mathrm{LM}(f)$ (the largest monomial of f w.r.t $>$)
- $\mathrm{LC}(f)$ (the coefficient correspond to $\mathrm{LM}(f)$)
- $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$
- $\mathrm{Tail}(f) = f - \mathrm{LT}(f)$
- $\mathrm{Term}(f)$, $\mathrm{Mono}(f)$

$$F \subseteq \mathbb{F}[x_1, \ldots, x_n] \begin{cases} \mathrm{Tail}(F) = \cup_{f \in F} \mathrm{Tail}(f) \\ \mathrm{Term}(F) = \cup_{f \in F} \mathrm{Term}(f) \\ \mathrm{Mono}(F) = \cup_{f \in F} \mathrm{Mono}(f) \end{cases}$$

Polynomial Reduction

TODO

Gröbner Basis : Definition

Definition

Gröbner Basis : Definition

Definition

$I \neq \{0\}$ be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$

Gröbner Basis : Definition

Definition

$I \neq \{0\}$ be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$
$G \subseteq I$, $|G| < \infty$ that generates I is a Gröbner basis of I if,

Gröbner Basis : Definition

Definition

$I \neq \{0\}$ be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$
$G \subseteq I$, $|G| < \infty$ that generates I is a Gröbner basis of I if,

$$\text{for any } f \in I, \exists g \in G \text{ s.t. } \mathrm{LT}(g) \mid \mathrm{LT}(f)$$

Gröbner basis and Solving System of Equations

Gröbner basis and Solving System of Equations

Lexicographic Ordering

$$
\begin{gathered}
g_1(x_1), \ldots, \\
g_2(x_1, x_2), \ldots, g_{k_1}(x_1, x_2) \\
g_{k_1+1}(x_1, x_2, x_3), \ldots, \\
g_{k_n}(x_1, \ldots, x_n)
\end{gathered}
$$

Gröbner basis and Solving System of Equations

Lexicographic Ordering

$$
\begin{aligned}
& g_1(x_1), \ldots, \\
& g_2(x_1, x_2), \ldots, g_{k_1}(x_1, x_2) \\
& g_{k_1+1}(x_1, x_2, x_3), \ldots, \\
& g_{k_n}(x_1, \ldots, x_n)
\end{aligned}
$$

Unique Solution in the Base Field

$$
\begin{aligned}
g_1 &= x_1 + c_1, \\
&\vdots \\
g_n &= x_n + c_n
\end{aligned}
$$

S-Polynomial

S-Polynomial

- $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ with $f \neq 0, g \neq 0$

S-Polynomial

- $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ with $f \neq 0, g \neq 0$
- $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$

S-Polynomial

- $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ with $f \neq 0, g \neq 0$
- $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$

Definition

$$\mathrm{Spoly}(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

Buchberger's Algorithm

Input: A finite ordered subset $F \subseteq \mathbb{F}[x_1, \ldots, x_n]$
Result: A Gröbner basis G such that $\langle G \rangle = \langle F \rangle$

$P \leftarrow \{\{p, q\} : \forall p, q \in F$ **and** $p \neq q\}$
$G \leftarrow F$
while $P \neq \{\}$ **do**
  $\{p, q\} \leftarrow \textsc{Select}(P)$
  $P \leftarrow P \setminus \{\{p, q\}\}$
  $r \leftarrow \textsc{FullReduce}(\mathsf{Spoly}(p, q), G)$
  if $r \neq 0$ **then**
    $P \leftarrow P \cup \{\{r, g\} : \forall g \in G\}$
    $G \leftarrow G \cup \{r\}$
return G

Table of Contents

1. Introduction
2. Gröbner Basis
3. M4GB Algorithm
4. Performance Comparison
5. Solving MQ Challenges

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$

$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$

$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$

$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$

$G = \{g_1, g_2, g_3 \quad \}$

$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$

$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$

$g_3 = x_1 x_2 x_3 + x_1 x_3$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$
$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$

$$G = \{g_1, g_2, g_3 \quad \}$$
$$g_1 = x_1^2 x_2^3 + x_1 x_3^3 + x_4^2$$
$$g_2 = x_2^3 x_4 + x_2 x_3 + x_3 + 1$$
$$g_3 = x_1 x_2 x_3 + x_1 x_3$$

$$x_1 g_2 = x_1 x_2^3 x_4 + x_1 x_2 x_3 + x_1 x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$

$$G = \{g_1, g_2, g_3, g_4\}$$

$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$
$$g_4 = x_1g_2 - g_3 = x_1x_2^3x_4 + 1$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$

$$G = \{g_1, g_2, g_3, g_4\}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$
$$g_4 = x_1g_2 - g_3 = x_1x_2^3x_4 + 1$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$
$$f = f - g_4 = x_1^3x_4 + x_2x_3^2 + 1$$

$$G = \{g_1, g_2, g_3, g_4\}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$
$$g_4 = x_1g_2 - g_3 = x_1x_2^3x_4 + 1$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

Example

$\mathbb{F}_2[x_1, x_2, x_3, x_4]$ with *degrevlex* monomial ordering

$$f = x_1^2x_2^3 + x_1x_2^3x_4 + x_1x_3^3 + x_1^3x_4 + x_2x_3^2 + x_4^2$$
$$f = f - g_1 = x_1x_2^3x_4 + x_1^3x_4 + x_2x_3^2$$
$$f = f - g_4 = x_1^3x_4 + x_2x_3^2 + 1$$

$$G = \{g_1, g_2, g_3, g_4\}$$
$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$
$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$
$$g_3 = x_1x_2x_3 + x_1x_3$$
$$g_4 = x_1g_2 - g_3 = x_1x_2^3x_4 + 1$$

$$x_1g_2 = x_1x_2^3x_4 + x_1x_2x_3 + x_1x_3 + x_1$$

$$r = x_1^3x_4 + x_2x_3^2 + 1$$

1. Maintain tail-reduced polynomials (during reduction and when a new element for the basis is found)
2. Identify polynomial with their leading monomial (i.e. no two polynomials in G that have equal leading monomial)

M4GB Reduction

$\textsc{MulFullReduce}(G, u, f)$

```
r ← 0
forall t ∈ Term(f) do
    t′ ← u · t
    if ∃g ∈ G : LT(g) | t′ then
        (G, g) ← GetReductor(G, t′)
        r ← r − (t′/LT(g)) · Tail(g)
    else
        r ← r + t′
return (G, r)
```

M4GB Reduction

$\textsc{MulFullReduce}(G, u, f)$

1. $r \leftarrow 0$
2. **forall** $t \in \mathrm{Term}(f)$ **do**
    3. $t' \leftarrow u \cdot t$
    4. **if** $\exists g \in G : \mathrm{LT}(g) \mid t'$ **then**
        5. $(G, g) \leftarrow \textsc{GetReductor}(G, t')$
        6. $r \leftarrow r - (t'/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    7. **else**
        8. $r \leftarrow r + t'$
9. **return** (G, r)

$\textsc{GetReductor}(G, t)$

1. **if** $\exists g \in G : \mathrm{LM}(g) = \mathrm{LM}(t)$ **then**
    2. **return** (G, g)
3. $h \leftarrow \textsc{SelectReductor}(G, t)$
4. $(G, h) \leftarrow \textsc{MulFullReduce}(G, t/\mathrm{LT}(h), \mathrm{Tail}(h))$
5. $g \leftarrow t + h$
6. **return** $(G \cup \{g\}, g)$

$\textsc{UpdateReduce}(G, f)$

$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$Q \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$

while $\exists u \in Q : \mathrm{LM}(f) \mid u$ **do**
  $u \leftarrow \max\{\mathfrak{m} \in Q : \mathrm{LM}(f) \mid \mathfrak{m}\}$
  $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
  $H \leftarrow H \cup \{u + h\}$
  $Q \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$

while $H \neq \{\}$ **do**
  Select $h \in H$ such that $\mathrm{LM}(h) = \min \mathrm{LM}(H)$
  $H \leftarrow H \setminus \{h\}$
  $H \leftarrow \{g - ch : g \in H, c$ is a coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
  $G \leftarrow \{g - ch : g \in G, c$ is a coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
  $G \leftarrow G \cup \{h\}$

Table of Contents

1 Introduction

2 Gröbner Basis

3 M4GB Algorithm

4 Performance Comparison

5 Solving MQ Challenges

- Implemented using `C++11`

- Implemented using `C++11`
- Comparison with existing implementations
  1. FGb C Interface - Implementation by Jean Charles Faugere[1]
  2. Magma v2.20-6
  3. OpenF4 v1.0.1 - Open source implementation by Coladon, Vitse and Joux[2].

[1] Available at `http://www-polsys.lip6.fr/~jcf/FGb/C/index.html`

[2] Available at `https://github.com/nauotit/openf4`

- Implemented using `C++11`
- Comparison with existing implementations
  1. FGb C Interface - Implementation by Jean Charles Faugere[1]
  2. Magma v2.20-6
  3. OpenF4 v1.0.1 - Open source implementation by Coladon, Vitse and Joux[2].
- Test cases
  1. Dense polynomials with coefficients in $\mathbb{F}_{31}$
  2. $m = 2n$ and $m = n + 1$.

[1] Available at `http://www-polsys.lip6.fr/~jcf/FGb/C/index.html`

[2] Available at `https://github.com/nauotit/openf4`

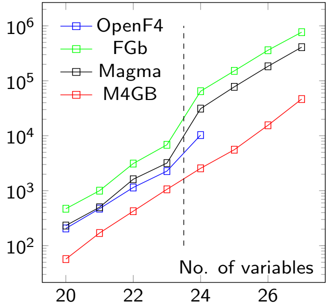
Benchmark for $m = 2n$

		Total CPU time (sec)			
n	m	M4GB	OpenF4	Magma	FGb
20	40	57	206	232	470
21	42	170	472	500	1002
22	44	424	1145	1617	3118
23	46	1060	2274	3185	6849
24	48	2556	10293	31168	64700
25	50	5575	-	77679	151653
26	52	15517	-	183629	360055
27	54	46548	-	409452	767543

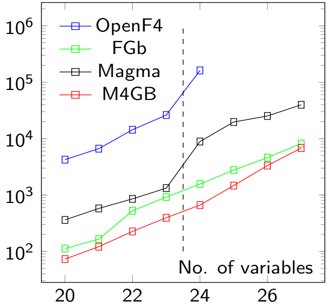
		Memory (MB)			
n	m	M4GB	FGb	Magma	OpenF4
20	40	73	112	362	4240
21	42	121	165	577	6640
22	44	226	525	859	14368
23	46	395	918	1324	26135
24	48	663	1561	8873	161945
25	50	1471	2765	19719	-
26	52	3328	4607	25197	-
27	54	6799	8180	39845	-

Graph for $m = 2n$

Total CPU time (sec)



Memory usage (MB)



Benchmark for $m = n + 1$

		Total CPU time (sec)			
n	m	M4GB	OpenF4	Magma	FGb
10	11	0.98	2.99	3.29	5
11	12	2.6	8.73	11.172	21
12	13	13.92	36.76	59.08	134
13	14	58.18	172.49	286.4	642
14	15	393.19	1258	2810.75	5850
15	16	2424	7225	17265.5	36361

		Memory (MB)			
n	m	M4GB	FGb	Magma	OpenF4
10	11	17	33	32	101
11	12	16	50	64	341
12	13	31	112	114	1463
13	14	74	323	281	7622
14	15	250	1098	1104	33460
15	16	837	4118	3320	117396

Graph for $m = n + 1$

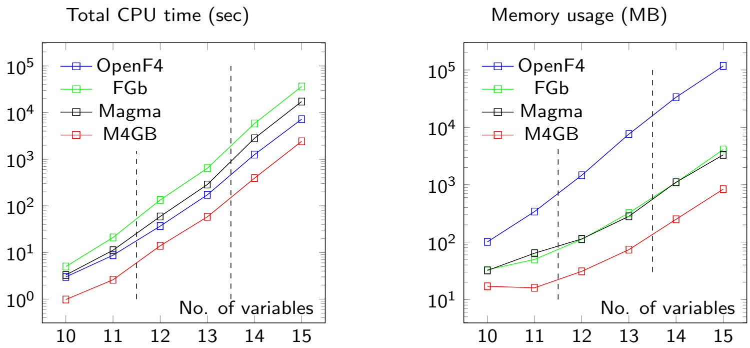


Table of Contents

1 Introduction

2 Gröbner Basis

3 M4GB Algorithm

4 Performance Comparison

5 Solving MQ Challenges

Solving Type V and VI of MQ Challenge

- Hybrid approach : trade-off between exhaustive search and computing Gröbner bases
- Idea :
  1. Select a random vector $(a_1, \dots, a_{n-m}) \in \mathbb{F}_q^{n-m}$
  2. Construct a new system with $n = m$

$$\tilde{F} = \{f(x_1, \dots, x_m, a_1, \dots, a_{n-m}) : \forall f \in F\}$$

  3. Select $k \in \{1, \dots, m\}$ and construct q^k subsystems from $\tilde{F}$ by substituting k variables with all elements of $\mathbb{F}_q^k$.
  4. Each subsystem generated can be solved in parallel.

Computational Resources

A) Desktop machine with Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz and 16GB RAM

Computational Resources

A) Desktop machine with Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz and 16GB RAM

B) NUMA machine with two nodes of Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM each.

Solved Challenges

Type	n/m	Machine Used	# Node	Duration

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16			
V	25/17			
V	27/18			

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16	A	1	$\approx$ 9.3 hours
V	25/17			
V	27/18			

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16	A	1	$\approx$ 9.3 hours
V	25/17	B	1	$\approx$ 46.33 hours
V	27/18	B	2	$\approx$ 10.9 days

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16	A	1	$\approx$ 9.3 hours
V	25/17	B	1	$\approx$ 46.33 hours
V	27/18	B	2	$\approx$ 10.9 days
VI	24/16			
VI	25/17			
VI	27/18			
VI	28/19			

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16	A	1	$\approx$ 9.3 hours
V	25/17	B	1	$\approx$ 46.33 hours
V	27/18	B	2	$\approx$ 10.9 days
VI	24/16	A	1	$\approx$ 1.2 hours
VI	25/17			
VI	27/18			
VI	28/19			

Solved Challenges

Type	n/m	Machine Used	# Node	Duration
V	24/16	A	1	$\approx$ 9.3 hours
V	25/17	B	1	$\approx$ 46.33 hours
V	27/18	B	2	$\approx$ 10.9 days
VI	24/16	A	1	$\approx$ 1.2 hours
VI	25/17	B	1	$\approx$ 9.87 hours
VI	27/18	B	1	$\approx$ 31.48 hours
VI	28/19	B	2	$\approx$ 7.61 days

https://github.com/cr-marcstevens/m4gb

Question ?