M4GB: An Efficient Gröbner Bases Algorithm

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

[1]Mathematics Institute, University Leiden

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

ISSAC 2017 – Kaiserslautern, 27th July 2017

Motivation

Multivariate Quadratic (MQ) Problem

Given quadratic polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, find a $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$ such that $f_i(v_1, \ldots, v_n) = 0$ for all $i \in \{1, \ldots, m\}$

1. Gröbner Bases Algorithms
2. M4GB Algorithm
3. Fukuoka MQ Challenges
4. Implementation Results
5. Solving MQ Challenges

Table of Contents

1. Gröbner Bases Algorithms
2. M4GB Algorithm
3. Fukuoka MQ Challenges
4. Implementation Results
5. Solving MQ Challenges

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

1. $G \leftarrow F$

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
1 $G \leftarrow F$
2 repeat
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
1  $G \leftarrow F$
2  **repeat**
3      $G' \leftarrow G$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\mathrm{Spoly}(h_1, h_2), G')$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
**repeat**
    $G' \leftarrow G$
    **for all** $(h_1, h_2) \in G' \times G'$ **and** $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\mathrm{Spoly}(h_1, h_2), G')$
        **if** $r \neq 0$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\text{Spoly}(h_1, h_2), G')$
        if $r \neq 0$
            $G \leftarrow G \cup \{r\}$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\text{Spoly}(h_1, h_2), G')$
        if $r \neq 0$
            $G \leftarrow G \cup \{r\}$
until $G = G'$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\text{Spoly}(h_1, h_2), G')$
        if $r \neq 0$
            $G \leftarrow G \cup \{r\}$
until $G = G'$
return $G$
```

Buchberger's Algorithm (Buchberger, 1965)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$
repeat
    $G' \leftarrow G$
    for all $(h_1, h_2) \in G' \times G'$ and $h_1 \neq h_2$
        $r \leftarrow \textsc{FullReduce}(\text{Spoly}(h_1, h_2), G')$
        if $r \neq 0$
            $G \leftarrow G \cup \{r\}$
until $G = G'$
return $G$
```

Improvement

Detect zero reduction in advance – Buchberger's 1st and 2nd criterion (e.g. using Gebauer-Möller installation)

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \dots, f_m\} \subset \mathbb{F}[x_1, \dots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \dots, f_m \rangle$

1. $G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
1  $G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
2  $d \leftarrow 0$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \dots, f_m\} \subset \mathbb{F}[x_1, \dots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \dots, f_m \rangle$

```
1. $G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
2. $d \leftarrow 0$
3. $P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
1  $G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
2  $d \leftarrow 0$
3  $P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
4  while $P \neq \{\}$
5      $d \leftarrow d + 1$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                    $//P_d \subseteq P$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
1 $G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
2 $d \leftarrow 0$
3 $P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
4 while $P \neq \{\}$
5     $d \leftarrow d + 1$
6     $P_d \leftarrow \textsc{Select}(P)$                //$P_d \subseteq P$
7     $P \leftarrow P \setminus P_d$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                    $//P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                        //$P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$       //Construction of a coefficient matrix
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                         $//P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$        //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$  //Main reduction step
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                          //$P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$         //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$   //Main reduction step
    $\tilde{F}_d^+ \leftarrow \{f \in \tilde{F}_d : \mathrm{LM}(f) \notin \mathrm{LM}(F_d)\}$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                              //$P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$              //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$        //Main reduction step
    $\tilde{F}_d^+ \leftarrow \{f \in \tilde{F}_d : \mathrm{LM}(f) \notin \mathrm{LM}(F_d)\}$
    for $h \in \tilde{F}_d^+$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                          //$P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$          //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$    //Main reduction step
    $\tilde{F}_d^+ \leftarrow \{f \in \tilde{F}_d : \mathrm{LM}(f) \notin \mathrm{LM}(F_d)\}$
    for $h \in \tilde{F}_d^+$
        $P \leftarrow P \cup \{(h, g) : g \in G\}$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                                  $//P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$                  //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$            //Main reduction step
    $\tilde{F}_d^+ \leftarrow \{f \in \tilde{F}_d : \mathrm{LM}(f) \notin \mathrm{LM}(F_d)\}$
    for $h \in \tilde{F}_d^+$
        $P \leftarrow P \cup \{(h, g) : g \in G\}$
        $G \leftarrow G \cup \{h\}$
```

F_4 Algorithm (Faugère, 1999)

Input : $F = \{f_1, \ldots, f_m\} \subset \mathbb{F}[x_1, \ldots, x_n]$
Output : A Gröbner basis G of $\langle f_1, \ldots, f_m \rangle$

```
$G \leftarrow F$, $\tilde{F}_0^+ \leftarrow F$
$d \leftarrow 0$
$P \leftarrow \{(f_i, f_j) : f_i, f_j \in F, i > j\}$
while $P \neq \{\}$
    $d \leftarrow d + 1$
    $P_d \leftarrow \textsc{Select}(P)$                               //$P_d \subseteq P$
    $P \leftarrow P \setminus P_d$
    $L_d \leftarrow \textsc{Left}(P_d) \cup \textsc{Right}(P_d)$
    $F_d \leftarrow \textsc{SymbPreprocessing}(L_d, G)$          //Construction of a coefficient matrix
    $\tilde{F}_d \leftarrow \textsc{GaussianElimination}(F_d)$       //Main reduction step
    $\tilde{F}_d^+ \leftarrow \{f \in \tilde{F}_d : \mathrm{LM}(f) \notin \mathrm{LM}(F_d)\}$
    for $h \in \tilde{F}_d^+$
        $P \leftarrow P \cup \{(h, g) : g \in G\}$
        $G \leftarrow G \cup \{h\}$
return $G$
```

Improvement of F_4 : SIMPLIFY function

Improvement of F_4 : SIMPLIFY function

- Replace uf with $u'f'$ s.t. $\mathrm{LM}(uf) = \mathrm{LM}(u'f')$ where u, u' are monomials

Improvement of F_4 : SIMPLIFY function

- Replace uf with $u'f'$ s.t. $\mathrm{LM}(uf) = \mathrm{LM}(u'f')$ where u, u' are monomials
- More reductions are already applied on f'

Improvement of F_4 : SIMPLIFY function

- Replace uf with $u'f'$ s.t. $\mathrm{LM}(uf) = \mathrm{LM}(u'f')$ where u, u' are monomials
- More reductions are already applied on f'
- Requires all previously constructed intermediate matrices and their corresponding (reduced) row echelon form

Improvement of F_4 : SIMPLIFY function

- Replace uf with $u'f'$ s.t. $\mathrm{LM}(uf) = \mathrm{LM}(u'f')$ where u, u' are monomials
- More reductions are already applied on f'
- Requires all previously constructed intermediate matrices and their corresponding (reduced) row echelon form
- Rewriting reductors

F_4 : Advantages and Disadvantages

F_4 : Advantages and Disadvantages

Advantages

1. Parallel reduction of S-polynomials with efficient linear algebra

F_4 : Advantages and Disadvantages

Advantages

1. Parallel reduction of S-polynomials with efficient linear algebra

Disadvantages

1. Normal selection strategy $\Rightarrow$ Many critical pairs processed $\Rightarrow$ Large intermediate matrices
2. The cost of having SIMPLIFY function : high memory consumption

Table of Contents

1 Gröbner Bases Algorithms

2 M4GB Algorithm

3 Fukuoka MQ Challenges

4 Implementation Results

5 Solving MQ Challenges

- Let g be a reductor of $f \in \mathbb{F}[x_1, \ldots, x_n]$
- The term of f corresponding to LM(g) will be eliminated
- Less monomials in Tail(g) $\Rightarrow$ less operations

- Let g be a reductor of $f \in \mathbb{F}[x_1, \ldots, x_n]$
- The term of f corresponding to $\mathrm{LM}(g)$ will be eliminated
- Less monomials in $\mathrm{Tail}(g) \Rightarrow$ less operations

M4GB Main Strategy

The tail of every polynomial must be fully reduced

- M4GB is an extension of Buchberger's algorithm

- M4GB is an extension of Buchberger's algorithm
- Two main differences :

- M4GB is an extension of Buchberger's algorithm
- Two main differences :
    1. M4GB Reduction : prioritizes reduction on tail of reductors (recursive)
        - $\textsc{MulFullReduce}(G, t, f)$

- M4GB is an extension of Buchberger's algorithm
- Two main differences :
  1. M4GB Reduction : prioritizes reduction on tail of reductors (recursive)
     - MULFULLREDUCE(G, t, f)
  2. Reduction on tail of all polynomials using new element found in the ideal
     - UPDATEREDUCE(G, P, f)

M4GB Reduction

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

M4GB Reduction

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

1. $h \leftarrow 0$

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$
1. $h \leftarrow 0$
2. for all $s \in \mathrm{Term}(f)$
```

M4GB Reduction

```
MulFullReduce($G, t, f$)
$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
```

M4GB Reduction

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

```
$h \leftarrow 0$
for all $s \in \text{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \text{LT}(g) \mid r$ then
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
```

M4GB Reduction

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

```
$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

M4GB Reduction

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

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

```
$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

M4GB Reduction

```
MulFullReduce($G, t, f$)

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow$ GetReductor($G, r$)
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

```
GetReductor($G, r$)

if $\exists g \in G : \mathrm{LM}(g) = \mathrm{LM}(r)$ then
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

```
$\textsc{GetReductor}(G, r)$

if $\exists g \in G : \mathrm{LM}(g) = \mathrm{LM}(r)$ then
    return $(G, g)$
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \text{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \text{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\text{LT}(g)) \cdot \text{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

```
$\textsc{GetReductor}(G, r)$

if $\exists g \in G : \text{LM}(g) = \text{LM}(r)$ then
    return $(G, g)$
$f \leftarrow \textsc{ReduceSel}(G, r)$
```

M4GB Reduction

```
MulFullReduce$(G, t, f)$

$h \leftarrow 0$
for all $s \in \text{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \text{LT}(g) \mid r$ then
        $(G, g) \leftarrow$ GetReductor$(G, r)$
        $h \leftarrow h - (r/\text{LT}(g)) \cdot \text{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

```
GetReductor$(G, r)$

if $\exists g \in G : \text{LM}(g) = \text{LM}(r)$ then
    return $(G, g)$
$f \leftarrow$ ReduceSel$(G, r)$
$(G, h) \leftarrow$ MulFullReduce$(G, r/\text{LT}(f), \text{Tail}(f))$
```

M4GB Reduction

```
$\textsc{MulFullReduce}(G, t, f)$

$h \leftarrow 0$
for all $s \in \mathrm{Term}(f)$
    $r \leftarrow t \cdot s$
    if $\exists g \in G : \mathrm{LT}(g) \mid r$ then
        $(G, g) \leftarrow \textsc{GetReductor}(G, r)$
        $h \leftarrow h - (r/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
    else
        $h \leftarrow h + r$
return (G, h)
```

```
$\textsc{GetReductor}(G, r)$

if $\exists g \in G : \mathrm{LM}(g) = \mathrm{LM}(r)$ then
    return $(G, g)$
$f \leftarrow \textsc{ReduceSel}(G, r)$
$(G, h) \leftarrow \textsc{MulFullReduce}(G, r/\mathrm{LT}(f), \mathrm{Tail}(f))$
return $(G \cup \{r + h\}, r + h)$
```

UPDATEREDUCE(G, P, f)

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

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

UpdateReduce(G, P, f)

```
1  $H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
2  $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
3  while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
```

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

```
1 $H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
2 $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
3 while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
4     Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
```

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

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
```

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

```
1 $H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
2 $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
3 while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
4     Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
5     $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
6     $H \leftarrow H \cup \{u + h\}$
```

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

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
```

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

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $H \neq \{\}$ do
```

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

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $H \neq \{\}$ do
    Select $h \in H$ such that $\mathrm{LM}(h) = \min(\mathrm{LM}(H))$
```

```
$\textsc{UpdateReduce}(G, P, f)$
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $H \neq \{\}$ do
    Select $h \in H$ such that $\mathrm{LM}(h) = \min(\mathrm{LM}(H))$
    $H \leftarrow H \setminus \{h\}$
```

UpdateReduce(G, P, f)

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
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 the coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
```

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

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
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 the coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
    $G \leftarrow \{g - ch : g \in G, c$ is the coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
```

UPDATEREDUCE(G, P, f)

```
$H \leftarrow \{\mathrm{LC}(f)^{-1} \cdot f\}$
$S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
while $\exists u \in S : \mathrm{LM}(f) \mid u$ do
    Find the largest monomial $u \in S$ s.t. $\mathrm{LM}(f) \mid u$
    $(G, h) \leftarrow \textsc{MulFullReduce}(G, u/\mathrm{LT}(f), \mathrm{Tail}(f))$
    $H \leftarrow H \cup \{u + h\}$
    $S \leftarrow \mathrm{Mono}(\mathrm{Tail}(G \cup H)) \setminus \mathrm{LM}(H)$
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 the coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
    $G \leftarrow \{g - ch : g \in G, c$ is the coefficient of $\mathrm{LM}(h)$ in $\mathrm{Tail}(g)\}$
    $G \leftarrow G \cup \{h\}$
```

Implementation Specific Notes

Implementation Specific Notes

M4GB is efficient when polynomials in G are maintained based on the uniqueness of their leading monomial i.e., if $f, g \in G$ s.t. $\mathrm{LM}(f) = \mathrm{LM}(g)$ then $f = g$

Implementation Specific Notes

M4GB is efficient when polynomials in G are maintained based on the uniqueness of their leading monomial i.e., if $f, g \in G$ s.t. $\mathrm{LM}(f) = \mathrm{LM}(g)$ then $f = g$

- M : associative array that maintain all polynomials

Implementation Specific Notes

M4GB is efficient when polynomials in G are maintained based on the uniqueness of their leading monomial i.e., if $f, g \in G$ s.t. $\mathrm{LM}(f) = \mathrm{LM}(g)$ then $f = g$

- M : associative array that maintain all polynomials
- L : a set of monomials that mark which polynomials in M that constitute a minimal basis

Table of Contents

1 Gröbner Bases Algorithms

2 M4GB Algorithm

3 Fukuoka MQ Challenges

4 Implementation Results

5 Solving MQ Challenges

MQ Challenges

MQ Challenges

- A series of open public challenge to solve MQ problems over finite field.

MQ Challenges

- A series of open public challenge to solve MQ problems over finite field.
- Random and dense polynomials

MQ Challenges

- A series of open public challenge to solve MQ problems over finite field.
- Random and dense polynomials
- Goal : understand its practical difficulty

MQ Challenges

- A series of open public challenge to solve MQ problems over finite field.
- Random and dense polynomials
- Goal : understand its practical difficulty

`https://www.mqchallenge.org`

MQ Challenge Types

	I	II	III
	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
	I	II	III
	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
$n \approx 1.5m$	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	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
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

- Time to solve : at least one month

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

- Time to solve : at least one month
- Using Magma 2.19-9

MQ Challenge Types

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Parameter Choice

- Time to solve : at least one month
- Using Magma 2.19-9
- CPU Used : Four 6-cores Intel(R) Xeon(R) CPU E5-4617 @ 2.9GHz and 1TB of RAM

Table of Contents

1 Gröbner Bases Algorithms

2 M4GB Algorithm

3 Fukuoka MQ Challenges

4 Implementation Results

5 Solving MQ Challenges

- Implemented using `C++11`

- Implemented using `C++11`
- Comparison with existing implementations
  1. FGb C Interface - Implementation by Jean-Charles Faugère[1]
  2. Magma v2.20-6 - Implementation by Allan Steel
  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 Faugère[1]
    2. Magma v2.20-6 - Implementation by Allan Steel
    3. OpenF4 v1.0.1 - Open source implementation by Coladon, Vitse and Joux[2].
- Test cases
    1. Dense quadratic 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 $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

		Memory Usage Ratio			
n	m				
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1			
21	42	1			
22	44	1			
23	46	1			
24	48	1			
25	50	1			
26	52	1			
27	54	1			

		Memory Usage Ratio			
n	m				
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61		
21	42	1	2.78		
22	44	1	2.70		
23	46	1	2.15		
24	48	1	4.03		
25	50	1	-		
26	52	1	-		
27	54	1	-		

		Memory Usage Ratio			
n	m				
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	
21	42	1	2.78	2.94	
22	44	1	2.70	3.81	
23	46	1	2.15	3.00	
24	48	1	4.03	12.19	
25	50	1	-	13.93	
26	52	1	-	11.83	
27	54	1	-	8.8	

		Memory Usage Ratio			
n	m				
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

		Memory Usage Ratio			
n	m				
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
20	40				
21	42				
22	44				
23	46				
24	48				
25	50				
26	52				
27	54				

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
20	40	1			
21	42	1			
22	44	1			
23	46	1			
24	48	1			
25	50	1			
26	52	1			
27	54	1			

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
20	40	1	1.53		
21	42	1	1.36		
22	44	1	2.32		
23	46	1	2.32		
24	48	1	2.35		
25	50	1	1.88		
26	52	1	1.38		
27	54	1	1.2		

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

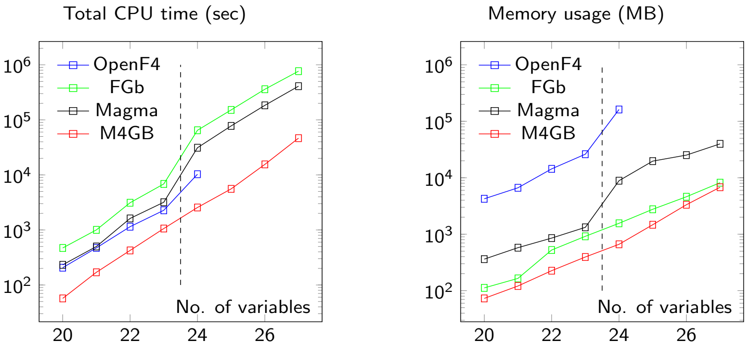
		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
20	40	1	1.53	4.96	
21	42	1	1.36	4.77	
22	44	1	2.32	3.8	
23	46	1	2.32	3.35	
24	48	1	2.35	13.38	
25	50	1	1.88	13.4	
26	52	1	1.38	7.57	
27	54	1	1.2	5.86	

Benchmark for $m = 2n$: Ratio

		CPU time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
20	40	1	3.61	4.07	8.25
21	42	1	2.78	2.94	5.89
22	44	1	2.70	3.81	7.35
23	46	1	2.15	3.00	6.46
24	48	1	4.03	12.19	25.31
25	50	1	-	13.93	27.2
26	52	1	-	11.83	23.20
27	54	1	-	8.8	16.49

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
20	40	1	1.53	4.96	58.08
21	42	1	1.36	4.77	54.88
22	44	1	2.32	3.8	63.57
23	46	1	2.32	3.35	66.16
24	48	1	2.35	13.38	244.26
25	50	1	1.88	13.4	-
26	52	1	1.38	7.57	-
27	54	1	1.2	5.86	-

Graph for $m = 2n$



Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

		Memory Usage Ratio			
n	m				
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1			
11	12	1			
12	13	1			
13	14	1			
14	15	1			
15	16	1			

		Memory Usage Ratio			
n	m				
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05		
11	12	1	3.36		
12	13	1	2.64		
13	14	1	2.96		
14	15	1	3.2		
15	16	1	2.98		

		Memory Usage Ratio			
n	m				
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	
11	12	1	3.36	4.3	
12	13	1	2.64	4.24	
13	14	1	2.96	4.92	
14	15	1	3.2	7.15	
15	16	1	2.98	7.12	

		Memory Usage Ratio			
n	m				
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

		Memory Usage Ratio			
n	m				
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
10	11				
11	12				
12	13				
13	14				
14	15				
15	16				

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
10	11	1			
11	12	1			
12	13	1			
13	14	1			
14	15	1			
15	16	1			

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
10	11	1	1.94		
11	12	1	3.12		
12	13	1	3.61		
13	14	1	4.36		
14	15	1	4.39		
15	16	1	4.92		

Benchmark for $m = n + 1$: Ratio

		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

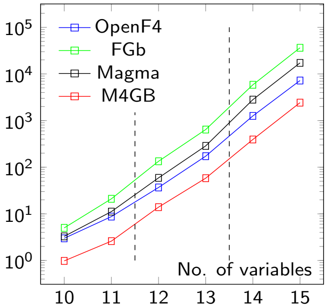
		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
10	11	1	1.94	1.88	
11	12	1	3.12	4	
12	13	1	3.61	3.68	
13	14	1	4.36	3.8	
14	15	1	4.39	4.42	
15	16	1	4.92	3.97	

Benchmark for $m = n + 1$: Ratio

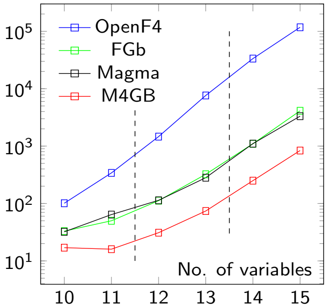
		CPU Time Ratio			
n	m	M4GB	OpenF4	Magma	FGb
10	11	1	3.05	3.36	5.1
11	12	1	3.36	4.3	8.08
12	13	1	2.64	4.24	9.63
13	14	1	2.96	4.92	11.03
14	15	1	3.2	7.15	14.88
15	16	1	2.98	7.12	15

		Memory Usage Ratio			
n	m	M4GB	FGb	Magma	OpenF4
10	11	1	1.94	1.88	5.94
11	12	1	3.12	4	21.31
12	13	1	3.61	3.68	47.19
13	14	1	4.36	3.8	103
14	15	1	4.39	4.42	133.84
15	16	1	4.92	3.97	140.26

Graph for $m = n + 1$



Total CPU time (sec)



Memory usage (MB)

Table of Contents

1. Gröbner Bases Algorithms
2. M4GB Algorithm
3. Fukuoka MQ Challenges
4. Implementation Results
5. Solving MQ Challenges

Solved MQ Challenges

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Solved MQ Challenges

	$\mathbb{F}_2$	$\mathbb{F}_{2^8}$	$\mathbb{F}_{31}$
$m = 2n$	I	II	III
	$n \geq 55$	$n \geq 35$	$n \geq 34$
$n \approx 1.5m$	IV	V	VI
	$m \geq 55$	$m \geq 16$	$m \geq 16$

Solving Strategy (Bettale, Faugère and Perret, 2009)

F

$(n > m)$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$$

$$\begin{tikzcd} F \arrow[r] & \bar{F} \end{tikzcd}$$

$(n > m)$ $(\#\mathrm{var} = m)$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$$

$$\begin{tikzcd}
 & & \bar{F}_1 \\
 & & \bar{F}_2 \\
F \arrow[r] & \bar{F} \arrow[uur] \arrow[ur] \arrow[ddr] & \\
(n > m) & (\#\mathrm{var} = m) & \vdots \\
 & & \bar{F}_{q^k}
\end{tikzcd}$$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$

$$\begin{tikzcd}
 & & \bar{F}_1 \arrow[r] & \bar{G}_1 \\
 & & \bar{F}_2 \arrow[r] & \bar{G}_2 \\
F \arrow[r] & \bar{F} \arrow[uur] \arrow[ur] \arrow[ddr] & & \\
(n > m) & (\#\mathrm{var} = m) & \vdots & \vdots \\
 & & \bar{F}_{q^k} \arrow[r] & \bar{G}_{q^k}
\end{tikzcd}$$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$

$$\begin{tikzcd}
 & & \bar{F}_1 \arrow[r] & \bar{G}_1 \\
F \arrow[r] & \bar{F} \arrow[ur] \arrow[r] \arrow[ddr] & \bar{F}_2 \arrow[r] & \bar{G}_2 \\
(n > m) & (\#\text{var} = m) & \vdots & \vdots \\
 & & \bar{F}_{q^k} \arrow[r] & \bar{G}_{q^k}
\end{tikzcd}$$

$\bar{G}_i$ is the reduced Gröbner basis of $\bar{F}_i$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$$

$$\begin{tikzcd}
 & & \bar{F}_1 \arrow[r] & \bar{G}_1 \\
F \arrow[r] & \bar{F} \arrow[ur] \arrow[r] \arrow[ddr] & \bar{F}_2 \arrow[r] & \bar{G}_2 \\
(n > m) & (\#\mathrm{var} = m) & \vdots & \vdots \\
 & & \bar{F}_{q^k} \arrow[r] & \bar{G}_{q^k}
\end{tikzcd}$$

$\bar{G}_i$ is the reduced Gröbner basis of $\bar{F}_i$

Assume $\bar{F}$ has a unique solution in $\mathbb{F}_q^m \Rightarrow \exists i \in \{1, \ldots, q^k\}$ such that

$$\bar{G}_i = \{x_1 + c_1, \ldots, x_m + c_m : c_1, \ldots, c_m \in \mathbb{F}_q\}$$

Solving Strategy (Bettale, Faugère and Perret, 2009)

$\bar{F} = F(x_1, \ldots, x_m, a_1, \ldots, a_{n-m})$

$$\begin{tikzcd}
& & \bar{F}_1 \arrow[r] & \bar{G}_1 \\
& & \bar{F}_2 \arrow[r] & \bar{G}_2 \\
F \arrow[r] & \bar{F} \arrow[uur] \arrow[ur] \arrow[ddr] & & \\
(n > m) & (\#\mathrm{var} = m) & \vdots & \vdots \\
& & \bar{F}_{q^k} \arrow[r] & \bar{G}_{q^k}
\end{tikzcd}$$

$\bar{G}_i$ is the reduced Gröbner basis of $\bar{F}_i$

Assume $\bar{F}$ has a unique solution in $\mathbb{F}_q^m \Rightarrow \exists i \in \{1, \ldots, q^k\}$ such that

$$\bar{G}_i = \{x_1 + c_1, \ldots, x_m + c_m : c_1, \ldots, c_m \in \mathbb{F}_q\}$$

Solution

$$(-c_1, \ldots, -c_m, a_1, \ldots, a_{n-m}) \in \mathbb{F}_q^n$$

Summary of Solved Challenges

Type	n/m	Machine Used	# Node	Duration

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of Solved Challenges

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

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of Solved Challenges

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

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of 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

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of 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			

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of 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			

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

Summary of Solved Challenges

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

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

B) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz and 128GB RAM (NUMA)

New Record

Type	n/m	Machine Used	# Node	Duration
VI	30/20	B	2	$\approx$ 11.32 days

Future Work

- Implementation for sparse system of equations
- Vectorization / Parallelization using GPU
- Larger finite field
- Adapting signature in M4GB

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

Question ?