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

Table of Contents

Problem

$\mathbb{F}[x_1, \ldots, x_n]$ - a polynomial ring over a field $\mathbb{F}$ together with an admissible monomial ordering $<$.

Problem

$\mathbb{F}[x_1, \ldots, x_n]$ - a polynomial ring over a field $\mathbb{F}$ together with an admissible monomial ordering $<$.

Problem (MQ-problem)

Let $n, m \in \mathbb{Z}_{>0}$. Given $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ with f_i be quadratic polynomials, find a $(a_1, \ldots, a_n) \in \mathbb{F}^n$ such that $f_i(a_1, \ldots, a_n) = 0$ for all $i = 1, \ldots, m$.

Notations

Example

$$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$$

Notations

Example

$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$

- $\mathrm{LM}(f) = x^2$ (the leading monomial of f)

Notations

Example

$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$

- $\mathrm{LM}(f) = x^2$ (the leading monomial of f)
- $\mathrm{LC}(f) = -15$ (the leading coefficient of f)

Notations

Example

$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$

- $\mathrm{LM}(f) = x^2$ (the leading monomial of f)
- $\mathrm{LC}(f) = -15$ (the leading coefficient of f)
- $\mathrm{LT}(f) = -15x^2$ (the leading term of f)

Notations

Example

$f = -15x^2 + 8xy - 13z^2 - 4x + 11z \in \mathbb{F}_{31}[x, y, z]$

- $\mathrm{LM}(f) = x^2$ (the leading monomial of f)
- $\mathrm{LC}(f) = -15$ (the leading coefficient of f)
- $\mathrm{LT}(f) = -15x^2$ (the leading term of f)
- $\mathrm{Tail}(f) = 8xy - 13z^2 - 4x + 11z$ (the tail of f)

Polynomial Reduction

Theorem

Let $G = (g_1, \ldots, g_t)$ be a nonempty ordered finite subset of $\mathbb{F}[x_1, \ldots, x_n]$. Then every polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be written as

$$f = q_1 g_1 + \ldots + q_t g_t + r,$$

where $q_1, \ldots, q_t, r \in \mathbb{F}[x_1, \ldots, x_n]$ and either $r = 0$ or none of terms of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.

Polynomial Reduction

Theorem

Let $G = (g_1, \ldots, g_t)$ be a nonempty ordered finite subset of $\mathbb{F}[x_1, \ldots, x_n]$. Then every polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ can be written as

$$f = q_1 g_1 + \ldots + q_t g_t + r,$$

where $q_1, \ldots, q_t, r \in \mathbb{F}[x_1, \ldots, x_n]$ and either $r = 0$ or none of terms of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.

$$r \leftarrow \textsc{FullReduce}(f, G)$$

Gröbner basis

Definition

Let $I \neq \{0\}$ be an ideal of $\mathbb{F}[x_1, \ldots, x_n]$. A finite subset $G \subseteq I$ that generates I is a Gröbner basis of I if for all $f \in I$, there exists $g \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(f)$.

S-polynomial

Definition

Let $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ be nonzero polynomials and let $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. The S-polynomial of f and g is defined as

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

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**

  $\{p, q\} \leftarrow \textsc{Select}(P)$

  $P \leftarrow P \setminus \{\{p, q\}\}$

  $r \leftarrow \textsc{FullReduce}(\mathrm{Spoly}(p, q), G)$

  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

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

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

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

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

$$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$$

$$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$$

$$g_3 = x_1x_2x_3 + x_1x_3$$

Example

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

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

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

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

$g_1 = x_1^2x_2^3 + x_1x_3^3 + x_4^2$

$g_2 = x_2^3x_4 + x_2x_3 + x_3 + 1$

$g_3 = x_1x_2x_3 + x_1x_3$

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

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

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

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

Example

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

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

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

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

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

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

$$f = x_1^2 x_2^3 + x_1 x_2^3 x_4 + x_1 x_3^3 + x_1^3 x_4 + x_2 x_3^2 + x_4^2$$
$$f = f - g_1 = x_1 x_2^3 x_4 + x_1^3 x_4 + x_2 x_3^2$$
$$f = f - g_4 = x_1^3 x_4 + x_2 x_3^2 + 1$$

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

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

Example

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

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

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

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

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

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

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

$r \leftarrow 0$
forall $t \in \mathrm{Term}(f)$ **do**
  $t' \leftarrow u \cdot t$
  if $\exists g \in G : \mathrm{LT}(g) \mid t'$ **then**
    $(G, g) \leftarrow \textsc{GetReductor}(G, t')$
    $r \leftarrow r - (t'/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
  else
    $r \leftarrow r + t'$
return (G, r)

M4GB Reduction

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

$r \leftarrow 0$
forall $t \in \mathrm{Term}(f)$ **do**
  $t' \leftarrow u \cdot t$
  if $\exists g \in G : \mathrm{LT}(g) \mid t'$ **then**
    $(G, g) \leftarrow \textsc{GetReductor}(G, t')$
    $r \leftarrow r - (t'/\mathrm{LT}(g)) \cdot \mathrm{Tail}(g)$
  else
    $r \leftarrow r + t'$
return (G, r)

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

if $\exists g \in G : \mathrm{LM}(g) = \mathrm{LM}(t)$ **then**
  return (G, g)
$h \leftarrow \textsc{SelectReductor}(G, t)$
$(G, h) \leftarrow$
  $\textsc{MulFullReduce}(G, t/\mathrm{LT}(h), \mathrm{Tail}(h))$
$g \leftarrow t + h$
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

- 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`

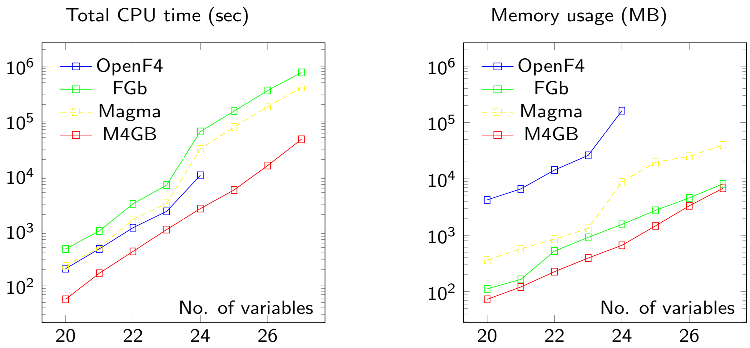
[2] Available at `https://github.com/nauotit/openf4`

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 $m = 2n$

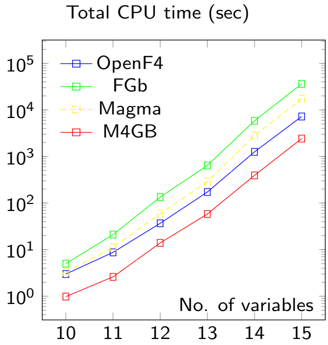


Benchmark for $m = n + 1$

		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 $m = n + 1$



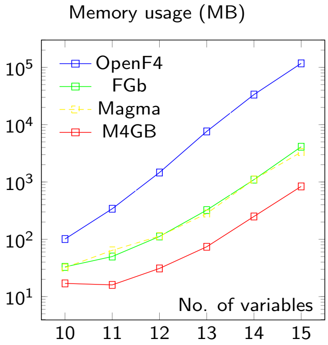


Table of Contents

- MQ-based public key and digital signature are candidates of post-quantum cryptography.
- Their security relies on the difficulty of finding a solution of an MQ problem.
- Need to understand its difficulty in practice

Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges

Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ($m = 2n$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.

Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ($m = 2n$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.
- Type IV, V, and VI are signature-type parameter ($n \approx 1.5m$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.

Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ($m = 2n$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.
- Type IV, V, and VI are signature-type parameter ($n \approx 1.5m$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.
- 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.

Fukuoka MQ Challenge

- Started on 1st April 2015
- Six different type of challenges
- Type I, II, and III are encryption-type parameter ($m = 2n$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.
- Type IV, V, and VI are signature-type parameter ($n \approx 1.5m$) and coefficients in $\mathbb{F}_2, \mathbb{F}_{2^8}, \mathbb{F}_{31}$ respectively.
- 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 Signature-type MQ Challenge

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

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

  3. Select $k \in \{1, \ldots, m\}$ 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	≈ 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

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

Question ?