Analyzing the Crossbred Algorithm for the MQ Problem

JNCF 2024

Damien VIDAL
Joint work with Claire Delaplace and Sorina Ionica

08/03/2024

MQ problem

MQ problem

Given a quadratic polynomials system of m polynomials $(f_1,\ f_2,\ ...,\ f_m)$ over $\mathbb{K}[x_1, \ldots, x_n]$. Find $a = (a_1,\ a_2,\ ...,\ a_n) \in \mathbb{K}^n$ such that : $f_1(a) = f_2(a) = ... = f_m(a) = 0$.

Interesting case for cryptography : polynomials defined over $\mathbb{F}_2$ and its extensions.

Solving methods

Known methods

- Linearisation
- Gröbner basis
- Exhaustive search

In practice : a mix of all of the above.

Crossbred algorithm

The algorithm has parameters D, d and k.

How it works

1. Generate new polynomials $p_1, \ldots, p_r$ s.t. $deg(p_i) \leq D$ and $deg_k(p_i) \leq d$.
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

Parameters $\boldsymbol{D}$, $\boldsymbol{d}$ and $\boldsymbol{k}$ are chosen so the system obtained at step 3 is solvable by linearisation.

Contributions

- Propose a block Crossbread algorithm.
- Study the choice of parameters of the block Crossbread.
- From that, deduce admissible parameters for the original Crossbred.

Notation

Macaulay matrix and its sub-matrix

- $Mac_{\leq D,m}$: Macaulay matrix of degree $\leq D$.
- $Mac^k_{\leq D,\geq d,m}$: Sub-matrix of $Mac_{\leq D,m}$ with rows uf_i s.t. u are monomials with $deg_k(u) \geq d-1$.
- $M^k_{\leq D,\geq d,m}$: Sub-matrix of $Mac^k_{\leq D,\geq d,m}$ whose columns correspond to monomials M s.t. $deg_k(M) \geq d+1$.

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

$$
\begin{array}{c}
 \\
f_1 \\
f_2 \\
x_3 f_1 \\
x_2 f_1 \\
x_1 f_1 \\
x_3 f_2 \\
x_2 f_2 \\
x_1 f_2
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
x_1x_2x_3 & x_1x_2 & x_1x_3 & x_2x_3 & x_1 & x_2 & x_3 & 1
\end{array} \\
\left(\begin{array}{cccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

	$x_1x_2x_3$	x_1x_2	x_1x_3	x_2x_3	x_1	x_2	x_3	1
f_1	0	1	0	1	1	0	0	1
f_2	0	0	1	0	0	1	0	0
x_3f_1	1	0	1	1	0	0	1	0
x_2f_1	0	0	0	1	0	1	0	0
x_1f_1	1	1	0	0	0	0	0	0
x_3f_2	0	0	1	1	0	0	0	0
x_2f_2	1	0	0	0	0	1	0	0
x_1f_2	0	1	1	0	0	0	0	0

$Mac^k_{\leq 3,\geq 1}$

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

	$x_1x_2x_3$	x_1x_2	x_1x_3	x_2x_3	x_1	x_2	x_3	1
f_1	0	1	0	1	1	0	0	1
f_2	0	0	1	0	0	1	0	0
x_3f_1	1	0	1	1	0	0	1	0
x_2f_1	0	0	0	1	0	1	0	0
x_1f_1	1	1	0	0	0	0	0	0
x_3f_2	0	0	1	1	0	0	0	0
x_2f_2	1	0	0	0	0	1	0	0
x_1f_2	0	1	1	0	0	0	0	0

$Mac^k_{\leq 3,\geq 1}$ $M^k_{\leq 3,\geq 1}$

Crossbred : in depth

The algorithm has parameters D, d and k

How it works

1. Generate new polynomials of degree at most d over the first k variables.
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

Crossbred : in depth

The algorithm has parameters D, d and k

How it works

1.
   - Generate $Mac^k_{\leq D,\geq d,m}$.
   - Extract $M^k_{\leq D,\geq d,m}$.
   - Compute all v_i such that $v_i M^k_{\leq D,\geq d,m} = 0$
   - Compute all $p_i = v_i Mac^k_{\leq D,\geq d,m}$
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

Crossbred : in depth

The algorithm has parameters D, d and k

How it works

1.
   - Generate $Mac^k_{\leq D,\geq d,m}$.
   - Extract $M^k_{\leq D,\geq d,m}$.
   - Compute all v_i such that $v_i M^k_{\leq D,\geq d,m} = 0$
   - Compute all $p_i = v_i Mac^k_{\leq D,\geq d,m}$.
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

Block Crossbread

Macaulay matrix and its sub-matrix

- $Mac_{\leq D,m}$: Macaulay matrix of degree $\leq D$.
- $Mac^k_{D,d,m}$: Sub-matrix of $Mac_{\leq D,m}$ with rows uf_i s.t. u are monomials with $deg(u) = D - 2$ and $deg_k(u) = d - 1$.
- $M^k_{D,d,m}$: Sub-matrix of $Mac^k_{D,d,m}$ whose columns correspond to monomials M s.t. $deg_k(M) = D$ and $deg_k(M) = d + 1$.

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

$$
\begin{array}{c}
 \\
f_1 \\
f_2 \\
x_3 f_1 \\
x_2 f_1 \\
x_1 f_1 \\
x_3 f_2 \\
x_2 f_2 \\
x_1 f_2
\end{array}
\begin{array}{c}
\begin{array}{cccccccc}
x_1x_2x_3 & x_1x_2 & x_1x_3 & x_2x_3 & x_1 & x_2 & x_3 & 1
\end{array} \\
\left(\begin{array}{cccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

$$
\begin{array}{c}
 & \begin{array}{cccccccc} x_1x_2x_3 & x_1x_2 & x_1x_3 & x_2x_3 & x_1 & x_2 & x_3 & 1 \end{array} \\
\begin{array}{c} f_1 \\ f_2 \\ x_3f_1 \\ x_2f_1 \\ x_1f_1 \\ x_3f_2 \\ x_2f_2 \\ x_1f_2 \end{array} &
\left(\begin{array}{cccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

$$Mac^k_{3,1}$$

Example

Parameters : $D = 3,\ d = 1,\ k = 2$

$$
\begin{array}{c}
 & \begin{array}{cccccccc} x_1x_2x_3 & x_1x_2 & x_1x_3 & x_2x_3 & x_1 & x_2 & x_3 & 1 \end{array} \\
\begin{array}{c} f_1 \\ f_2 \\ x_3f_1 \\ x_2f_1 \\ x_1f_1 \\ x_3f_2 \\ x_2f_2 \\ x_1f_2 \end{array} &
\left(\begin{array}{cccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

$M^k_{3,1}$ $\qquad$ $Mac^k_{3,1}$

Block Crossbred

The algorithm has parameters D, d and k

How it works

1.
   - Generate $Mac^k_{\leq D,\geq d,m}$.
   - Extract $M^k_{\leq D,\geq d,m}$.
   - Compute all v_i such that $v_i M^k_{\leq D,\geq d,m} = 0$
   - Compute all $p_i = v_i Mac^k_{\leq D,\geq d,m}$
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

Block Crossbred

The algorithm has parameters D, d and k

How it works

1.
   - Generate $Mac^k_{D,d,m}$.
   - Extract $M^k_{D,d,m}$.
   - Compute all v_i such that $v_i M^k_{D,d,m} = 0$
   - Compute all $p_i = v_i Mac^k_{D,d,m}$
2. Specify the $n-k$ last variables in $\mathbb{F}_2^{n-k}$.
3. Check if the system is consistent. If not, go back to step 2.

General and Frobenius criterion

Modified general criterion

If the row labeled by $t'f_m$ is a linear combination of previous rows in $Mac^k_{d_1,d_2,m}$, then t' is the leading term of a row labeled by tf_j in $\tilde{Mac}^k_{d_1-2,d_2-2,m-1}$.

Modified Frobenius criterion

If the row labeled by $t'f_m$ is a linear combination of previous rows in $Mac^k_{d_1,d_2,m}$, then t' is the leading term of a row labeled by tf_j in $\tilde{Mac}^k_{d_1-2,d_2-2,m}$.

Admissible parameters series

Definition

Given m and a set of parameters (D, d, k), we note :

$$h^k_{D,d,m} = \#Rows(M^k_{D,d,m}) - \#Cols(M^k_{D,d,m}).$$

Under semi-regularity hypothesis, if $h^k_{D,d,m} \geq 0$, then $h^k_{D,d,m}$ is equal to the co-rank of $M^k_{D,d,m}$.

A set of parameters (D, d, k) with $D \leq D_{reg}$ is called block-admissible if $h^k_{D,d,m} \geq 0$

Admissible parameters series

We get the following recurrence :

$$h^k_{D,d,m} = h^k_{D,d,m-1} - h^k_{D-2,d-2,m}.$$

Proposition

$$\sum_{D\geq 0, d\geq 0} h^k_{D,d,m} X^D Y^d = \frac{1}{Y}\left((1+X)^{n-k} - \frac{(1+XY)^k (1+X)^{n-k}}{(1+X^2Y^2)^m}\right).$$

From block Crossbred to J.V. Crossbred

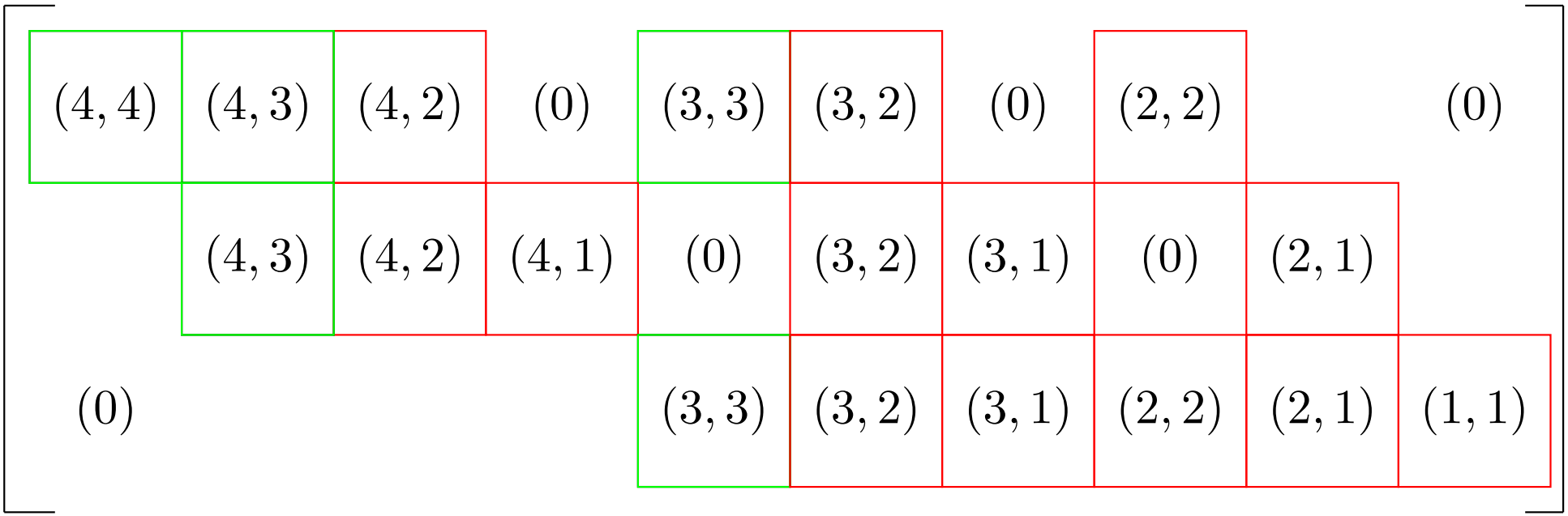
$$Mac^{k}_{\leq 4,\geq 2,m} = \left[\begin{array}{|c|}\hline uf_i : deg(u) = 2, deg_k(u) = 2 \\ \hline uf_i : deg(u) = 2, deg_k(u) = 1 \\ \hline uf_i : deg(u) = 1, deg_k(u) = 1 \\ \hline \end{array}\right]$$

From block Crossbred to J.V. Crossbred

(D, d) represent a sub-matrix corresponding to monomials of total degree D and of degree d over the first k variables.

$(4,4)$	$(4,3)$	$(4,2)$	(0)	$(3,3)$	$(3,2)$	(0)	$(2,2)$		(0)
	$(4,3)$	$(4,2)$	$(4,1)$	(0)	$(3,2)$	$(3,1)$	(0)	$(2,1)$	
(0)				$(3,3)$	$(3,2)$	$(3,1)$	$(2,2)$	$(2,1)$	$(1,1)$

From block Crossbred to J.V. Crossbred



From block Crossbred to J.V. Crossbred

$$M^{k}_{\leq 4,\geq 2,m} = \begin{bmatrix} (4,4) & (4,3) & (3,3) \\ & (4,3) & (0) \\ (0) & & (3,3) \end{bmatrix}$$

From block Crossbred to J.V. Crossbred

$$M^k_{\leq 4,\geq 2,m} = \begin{bmatrix} M^k_{4,3,m} & (4,3) & (3,3) \\ & M^k_{4,2,m} & (0) \\ (0) & & M^k_{3,2,m} \end{bmatrix}$$

From block Crossbred to J.V. Crossbred

If $(4, 2, k)$ and $(3, 2, k)$ are block-admissible

$$M^k_{\leq 4,\geq 2,m} = \begin{bmatrix} M^k_{4,3,m} & (4,3) & (3,3) \\ & M^k_{4,2,m} & (0) \\ (0) & & M^k_{3,2,m} \end{bmatrix}$$

From block Crossbred to J.V. Crossbred

If $(4, 2, k)$ and $(3, 2, k)$ are block-admissible

$$\tilde{M}^k_{\leq 4, \geq 2, m} = \begin{bmatrix} M^k_{4,3,m} & & (0) \\ & M^k_{4,2,m} & \\ (0) & & M^k_{3,2,m} \end{bmatrix}$$

From block Crossbred to J.V. Crossbred

Proposition

Let $\mathbf{h}^k_{D,d,m}$ be :

$$\mathbf{h}^k_{D,d,m} \quad = \quad \#Rows(M^k_{\leq D,\geq d,m}) - \#Cols(M^k_{\leq D,\geq d,m}).$$

Under semi-regularity hypothesis, if $\mathbf{h}^k_{D,d,m} \geq 0$, then $\mathbf{h}^k_{D,d,m}$ is the corank of the matrix $M^k_{\leq D,\geq d,m}$.

We have :

$$\mathbf{h}^k_{D,d,m} \quad = \quad \sum_{d_1 \leq D, d_2 \geq d} h^k_{d_1,d_2,m}.$$

A set of parameters (D, d, k) is affine admissible if $\mathbf{h}^k_{D,d,m} \geq 0$.

Specialisation

Definition

We suppose (D, d, k) are admissible parameters. We note $h'_{D,d,m}$ the number of "independent" polynomials obtained from $h_{D,d,m}$ after specialisation. As such :

$$h_{D,d,m} \geq h'_{D,d,m}.$$

Specialisation

Definition

We suppose (D, d, k) are admissible parameters. We note $h'_{D,d,m}$ the number of "independent" polynomials obtained from $h_{D,d,m}$ after specialisation. As such :

$$h_{D,d,m} \geq h'_{D,d,m}.$$

Open question

$$h_{D,d,m} = h'_{D,d,m}?$$

Specialisation

Definition

We suppose (D, d, k) are admissible parameters. We note $h'_{D,d,m}$ the number of "independent" polynomials obtained from $h_{D,d,m}$ after specialisation. As such :

$$h_{D,d,m} \geq h'_{D,d,m}.$$

Open question

$$h_{D,d,m} = h'_{D,d,m}?$$

What about Joux-Vitse Crossbred ?

$$\mathbf{h}'_{D,d,m} = \sum_{d<d_1\leq D} h'_{d_1,d_1-1,m}.$$

In progress

- Theoretical complexity
- What happens in other characteristic ? (in $\mathbb{F}_3$ or $\mathbb{F}_5$)