Some experiments on locator polynomials.

Michela Ceria

Trento, 22/05/2013

The problem.

Given the *n*-tuples (syndromes, errors) we look for the *sparsest* first error locator polynomial.

We made some experiments with simple examples:

1. $\mathbb{F}_8$, 2 errors;
2. $\mathbb{F}_{16}$, 2 errors;
3. $\mathbb{F}_{16}$, 3 errors;

The problem.

Given the n-tuples (syndromes, errors) we look for the *sparsest* first error locator polynomial.

We made some experiments with simple examples:

1. $\mathbb{F}_8$, 2 errors;
2. $\mathbb{F}_{16}$, 2 errors;
3. $\mathbb{F}_{16}$, 3 errors;

The problem.

Given the *n*-tuples (syndromes, errors) we look for the *sparsest* first error locator polynomial.

We made some experiments with simple examples:

1. $\mathbb{F}_8$, 2 errors;
2. $\mathbb{F}_{16}$, 2 errors;
3. $\mathbb{F}_{16}$, 3 errors;

The problem.

Given the n-tuples (syndromes, errors) we look for the *sparsest* first error locator polynomial.

We made some experiments with simple examples:

1. $\mathbb{F}_8$, 2 errors;
2. $\mathbb{F}_{16}$, 2 errors;
3. $\mathbb{F}_{16}$, 3 errors;

The problem.

Given the n-tuples (syndromes, errors) we look for the *sparsest* first error locator polynomial.

We made some experiments with simple examples:

1. $\mathbb{F}_8$, 2 errors;
2. $\mathbb{F}_{16}$, 2 errors;
3. $\mathbb{F}_{16}$, 3 errors;

$\mathbb{F}_8$, 2 errors.

The base field is $\mathbb{F}_8 = \{0, a, a^2, a^3, a^4, a^5, a^6, 1\}$, with $a^3 = a + 1$.

The 64 points we need to study have the form

$$(x_1, x_2, z_1, z_2) := (a + b, a^3 + b^3, a, b),\ a, b \in \mathbb{F}_8.$$

First of all we studied the Groebner escalier. From this, we exclude the 8 4-tuples $(0, 0, a, a)$: if $x_1 = x_2 = 0$, we obtain the 8 couples of errors (a, a). So we reduce to study only 56 points.

$\mathbb{F}_8$, 2 errors.

The base field is $\mathbb{F}_8 = \{0, a, a^2, a^3, a^4, a^5, a^6, 1\}$, with $a^3 = a + 1$.

The 64 points we need to study have the form

$$(x_1, x_2, z_1, z_2) := (a + b, a^3 + b^3, a, b), \; a, b \in \mathbb{F}_8.$$

First of all we studied the Groebner escalier. From this, we exclude the 8 4-tuples $(0, 0, a, a)$: if $x_1 = x_2 = 0$, we obtain the 8 couples of errors (a, a). So we reduce to study only 56 points.

$\mathbb{F}_8$, 2 errors.

The base field is $\mathbb{F}_8 = \{0, a, a^2, a^3, a^4, a^5, a^6, 1\}$, with $a^3 = a + 1$.

The 64 points we need to study have the form

$$(x_1, x_2, z_1, z_2) := (a + b, a^3 + b^3, a, b),\ a, b \in \mathbb{F}_8.$$

First of all we studied the Groebner escalier. From this, we exclude the 8 4-tuples $(0, 0, a, a)$: if $x_1 = x_2 = 0$, we obtain the 8 couples of errors (a, a). So we reduce to study only 56 points.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

There are several algorithms in order to find the required locator from the points (x_1, x_2, z_1, z_2), so we previously decided which one to use, studying their performances.

Exploiting our algorithms we obtain $F_a := z_1 + f_a(x_1, x_2)$, $F_b := z_1 + f_b(x_1, x_2)$ and a partition of the given points in two sets Z_a, Z_b, with $|Z_a| = |Z_b| = 28$ such that:

- F_a vanishes on Z_a
- $F_b$vanishes on Z_b
- $(x_1, x_2, z_1, z_2) \in Z_a \Leftrightarrow (x_1, x_2, z_2, z_1) \in Z_b$.

We choose Z_a and compute F_a: then we have $z_2 = z_1 + x_1$.

We arrange the 56 points in 28 couples, w.r.t. their first 3 cordinates (the ones we want to study), i.e.

$$[(a+b, a^3+b^3, a, b), (a+b, a^3+b^3, b, a)].$$

The Groebner escalier is

x_2^3	$x_1x_2^3$	$x_1^2x_2^3$	$x_1^3x_2^3$	$x_1^4x_2^3$	$x_1^5x_2^3$	$x_1^6x_2^3$
x_2^2	$x_1x_2^2$	$x_1^2x_2^2$	$x_1^3x_2^2$	$x_1^4x_2^2$	$x_1^5x_2^2$	$x_1^6x_2^2$
x_2	x_1x_2	$x_1^2x_2$	$x_1^3x_2$	$x_1^4x_2$	$x_1^5x_2$	$x_1^6x_2$
1	x_1	x_1^2	x_1^3	x_1^4	x_1^5	x_1^6

We arrange the 56 points in 28 couples, w.r.t. their first 3 cordinates (the ones we want to study), i.e.

$$[(a+b, a^3+b^3, a, b), (a+b, a^3+b^3, b, a)].$$

The Groebner escalier is

x_2^3	$x_1x_2^3$	$x_1^2x_2^3$	$x_1^3x_2^3$	$x_1^4x_2^3$	$x_1^5x_2^3$	$x_1^6x_2^3$
x_2^2	$x_1x_2^2$	$x_1^2x_2^2$	$x_1^3x_2^2$	$x_1^4x_2^2$	$x_1^5x_2^2$	$x_1^6x_2^2$
x_2	x_1x_2	$x_1^2x_2$	$x_1^3x_2$	$x_1^4x_2$	$x_1^5x_2$	$x_1^6x_2$
1	x_1	x_1^2	x_1^3	x_1^4	x_1^5	x_1^6

If $\mathbf{X}$, with $|\mathbf{X}| = 28$ is the chosen set, the possible locators have at most $|\mathbf{X}| + 1 = 29$ terms.

The first configurations we found produced locators with 18 terms. They are very peculiar since they cyclically permute, representing the 7 7-cycles of powers of a.

If $\mathbf{X}$, with $|\mathbf{X}| = 28$ is the chosen set, the possible locators have at most $|\mathbf{X}| + 1 = 29$ terms.

The first configurations we found produced locators with 18 terms. They are very peculiar since they cyclically permute, representing the 7 7-cycles of powers of a.

In particular, they come from

Points	Third coordinate
7	a
6	a^2
5	a^3
4	a^4
3	a^5
2	a^6
1	1

and the cyclic permutations of this configuration.

Remark

Given a configuration of this form, the choice of the corresponding points is unique.

In particular, they come from

Points	Third coordinate
7	a
6	a^2
5	a^3
4	a^4
3	a^5
2	a^6
1	1

and the cyclic permutations of this configuration.

Remark

Given a configuration of this form, the choice of the corresponding points is unique.

The configuration above corresponds to the (unique) choice

$$[2,2,2,2,2,2,2,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]:$$

and

a,a^2,a^5	a^2,a^5,a^6	$a^3,1,a^4$	a^4,a^3,a^5	a^5,a^4,a^4	a^6,a^3,a^3	$1,a^6,a^4$
a,a^6,a^3	a^2,a^4,a^3	a^3,a^5,a^2	a^4,a,a^3	$a^5,1,a^2$	a^6,a^2,a^2	$1,a^3,a^2$
a,a,a^2	a^2,a^2,a	a^3,a,a	a^4,a^4,a	a^5,a^6,a	$a^6,1,a$	$1,a^5,a$
a,a^3,a	a^2,a^6,a^2	a^3,a^2,a^3	a^4,a^5,a^4	a^5,a,a^5	a^6,a^4,a^6	$1,1,1$

The corresponding polynomial has 18 terms:

$$z_1 + a^5x_1^5x_2^3 + a^3x_1^4x_2^3 + a^2x_1^3x_2^3 + a^6x_1^2x_2^3 + ax_1x_2^3 +$$
$$a^4x_2^3 + a^2x_1^6x_2^2 + a^6x_1^5x_2^2 + ax_1^4x_2^2 + a^4x_1^3x_2^2 + a^6x_1^2x_2^2 +$$
$$+a^4x_1^5x_2 + a^3x_1^3x_2 + a^6x_1x_2 + a^6x_1^4 + ax_1 + a^5$$

Permutations are important!

It is essential to take cyclic permutations: computational evidences showed that breaking this pattern and considering some other permutations, the obtained polynomials considerably worsen.

An example:

Consider the following permutation, which introduces zero.

Points	Third coordinate
7	a^2
6	a^3
5	a^4
4	a^5
3	a^6
2	1
1	0

This configuration leads to

a,a^2,a^5	a^2,a^5,a^6	$a^3,1,a^4$	a^4,a^3,a^5	a^5,a^4,a^4	a^6,a^3,a^3	$1,a^6,a^4$
a,a^6,a^3	a^2,a^4,a^3	a^3,a^5,a^2	a^4,a,a^3	$a^5,1,a^2$	a^6,a^2,a^2	$1,a^3,a^2$
a,a,a^2	a^2,a^2,a^4	$a^3,a,1$	a^4,a^4,a^2	a^5,a^6,a^6	$a^6,1,a^5$	$1,a^5,a^3$
$\mathbf{a,a^3,0}$	a^2,a^6,a^2	a^3,a^2,a^3	a^4,a^5,a^4	a^5,a,a^5	a^6,a^4,a^6	$1,1,1$

corresponds to

$$[1,2,2,2,2,2,2,2,2,2,2,2,2,1,1,1,1,1,1,1,1,1,1,1,1,1,1]$$

and to a polynomial with 25 terms:
$z_1 + x_1^6x_2^3 + a^5x_1^5x_2^3 + a^3x_1^4x_2^3 + a^2x_1^3x_2^3 + a^5x_1^3 + a^4x_1^5x_2 + a^6x_1^4 + a^6x_1^2x_2^3 + ax_1x_2^3 + a^4x_2^3 + a^2x_1^6x_2^2 + a^6x_1^5x_2^2 + a^6x_1^2 + a^5x_1^3x_2 + a^3x_1^5 + ax_1^4x_2^2 + a^4x_1^3x_2^2 + a^2x_1^2x_2^2 + ax_1x_2^2 + a^2x_2^2 + a^3x_1 + a^5 + a^3x_1x_2 + a^2x_1^6$

Properties of our configurations.

The 7 polynomials associated to the cyclic permutations lead to the following relations:

$$\begin{bmatrix} x_1^6 & 0 & 0 & C & 0 \\ x_1^5 & 0 & a^4 & D & A \\ x_1^4 & D & 0 & E & B \\ x_1^3 & 0 & B & F & C \\ x_1^2 & 0 & 0 & a^6 & D \\ x_1^1 & a & D & 0 & E \\ x_1^0 & A & 0 & 0 & F \\ & x_2^0 & x_2^1 & x_2^2 & x_2^3 \end{bmatrix}$$

Calling M the middle term of the configuration we have the following formulas (related to the cycles in $\mathbb{F}_8$):

$$A = aM,\ B = a^2M^2,\ C = a^4M^3,\ D = a^4M^4,\ E = a^2M^5,\ F = aM^6.$$

Properties of our configurations.

The 7 polynomials associated to the cyclic permutations lead to the following relations:

$$\begin{bmatrix} x_1^6 & 0 & 0 & C & 0 \\ x_1^5 & 0 & a^4 & D & A \\ x_1^4 & D & 0 & E & B \\ x_1^3 & 0 & B & F & C \\ x_1^2 & 0 & 0 & a^6 & D \\ x_1^1 & a & D & 0 & E \\ x_1^0 & A & 0 & 0 & F \\ & x_2^0 & x_2^1 & x_2^2 & x_2^3 \end{bmatrix}$$

Calling M the middle term of the configuration we have the following formulas (related to the cycles in $\mathbb{F}_8$):

$A = aM$, $B = a^2M^2$, $C = a^4M^3$, $D = a^4M^4$, $E = a^2M^5$, $F = aM^6$.

Properties of our configurations.

The 7 polynomials associated to the cyclic permutations lead to the following relations:

$$\begin{bmatrix} x_1^6 & 0 & 0 & C & 0 \\ x_1^5 & 0 & a^4 & D & A \\ x_1^4 & D & 0 & E & B \\ x_1^3 & 0 & B & F & C \\ x_1^2 & 0 & 0 & a^6 & D \\ x_1^1 & a & D & 0 & E \\ x_1^0 & A & 0 & 0 & F \\ & x_2^0 & x_2^1 & x_2^2 & x_2^3 \end{bmatrix}$$

Calling M the middle term of the configuration we have the following formulas (related to the cycles in $\mathbb{F}_8$):

$$A = aM,\ B = a^2M^2,\ C = a^4M^3,\ D = a^4M^4,\ E = a^2M^5,\ F = aM^6.$$

Minimal configurations?

The configurations above can be improved: some other ones lead to polynomials with 8 terms, abiding to analogous rules. They come by “cyclic permutations” from the configuration below:

Points	Third coordinate
0	0
1	a
5	a^4
5	a^6
5	1
4	a^2
4	a^3
4	a^5

The configuration corresponds to the following choice
[2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 1, 2, 2, 1, 2, 1, 1, 2, 2, 1, 2, 1, 2, 1, 2]
and the locator polynomial is:

$$z_1 + a^3 x_1^6 x_2^2 + a^6 x_1^3 x_2^2 + x_1^2 x_2^2 + a^6 x_1^6 x_2 + a^5 x_2 + a^3 x_1^5 + a^5 x_1^3.$$

The 7 polynomials we obtain this way follow the following rules:

$$\begin{pmatrix} x_1^6 & 0 & A & B & 0 \\ x_1^5 & B & 0 & 0 & 0 \\ x_1^4 & 0 & 0 & 0 & 0 \\ x_1^3 & C & 0 & A & 0 \\ x_1^2 & 0 & 0 & 1 & 0 \\ x_1 & 0 & 0 & 0 & 0 \\ 1 & 0 & C & 0 & 0 \\ & 1 & x_2 & x_2^2 & x_2^3 \end{pmatrix}$$

if M is the only value occurring once in the configuration we have $A = M^6$, $B = M^3$, $C = M^5$, representing a cycle in $\mathbb{F}_8$.

The configuration corresponds to the following choice
[2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 1, 2, 2, 1, 2, 1, 1, 2, 2, 1, 2, 1, 2, 1, 2]
and the locator polynomial is:
$z_1 + a^3 x_1^6 x_2^2 + a^6 x_1^3 x_2^2 + x_1^2 x_2^2 + a^6 x_1^6 x_2 + a^5 x_2 + a^3 x_1^5 + a^5 x_1^3.$

The 7 polynomials we obtain this way follow the following rules:

$$\begin{pmatrix} x_1^6 & 0 & A & B & 0 \\ x_1^5 & B & 0 & 0 & 0 \\ x_1^4 & 0 & 0 & 0 & 0 \\ x_1^3 & C & 0 & A & 0 \\ x_1^2 & 0 & 0 & 1 & 0 \\ x_1 & 0 & 0 & 0 & 0 \\ 1 & 0 & C & 0 & 0 \\ & 1 & x_2 & x_2^2 & x_2^3 \end{pmatrix}$$

if M is the only value occurring once in the configuration we have $A = M^6$, $B = M^3$, $C = M^5$, representing a cycle in $\mathbb{F}_8$.

Remarks:

We found 4 different blocks formed by 7 configurations of the form above, and all of them abide to similar rules and come from cyclic permutations.

Differently from the 18-terms configurations, the 8-terms points have a peculiarity:

the choice of the corresponding points is not unique.

Differently chosen point worsen the result. We need to study the syndromes in order to decide which is the best choice.

Remarks:

We found 4 different blocks formed by 7 configurations of the form above, and all of them abide to similar rules and come from cyclic permutations.

Differently from the 18-terms configurations, the 8-terms points have a peculiarity:

the choice of the corresponding points is not unique.

Differently chosen point worsen the result. We need to study the syndromes in order to decide which is the best choice.

Remarks:

We found 4 different blocks formed by 7 configurations of the form above, and all of them abide to similar rules and come from cyclic permutations.

Differently from the 18-terms configurations, the 8-terms points have a peculiarity:

the choice of the corresponding points is not unique.

Differently chosen point worsen the result. We need to study the syndromes in order to decide which is the best choice.

$\mathbb{F}_{16}$, 2 errors.

The base field is
$\mathbb{F}_{16} = \{0, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, 1\}$,
with minimal polynomial $a^4 + a + 1$.

We start with 256 points, but we exclude again the ones with two equal errors, so we work on 240 points, divided in 120 couples. We choose one point for each couple, w.r.t. the third coordinate.

We found some blocks formed by 15 configurations, exactly analogous to the 18-terms ones and leading to polynomials with 85 terms. For these configurations, the choice of the corresponding points is *unique*.

$\mathbb{F}_{16}$, 2 errors.

The base field is
$\mathbb{F}_{16} = \{0, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, 1\}$,
with minimal polynomial $a^4 + a + 1$.

We start with 256 points, but we exclude again the ones with two equal errors, so we work on 240 points, divided in 120 couples. We choose one point for each couple, w.r.t. the third coordinate.

We found some blocks formed by 15 configurations, exactly analogous to the 18-terms ones and leading to polynomials with 85 terms. For these configurations, the choice of the corresponding points is *unique*.

$\mathbb{F}_{16}$, 2 errors.

The base field is
$\mathbb{F}_{16} = \{0, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, 1\}$,
with minimal polynomial $a^4 + a + 1$.

We start with 256 points, but we exclude again the ones with two equal errors, so we work on 240 points, divided in 120 couples. We choose one point for each couple, w.r.t. the third coordinate.

We found some blocks formed by 15 configurations, exactly analogous to the 18-terms ones and leading to polynomials with 85 terms. For these configurations, the choice of the corresponding points is *unique*.

Points	Third coordinates
15	a
14	a^2
13	a^3
12	a^4
11	a^5
10	a^6
9	a^7
8	a^8
7	a^9
6	a^{10}
5	a^{11}
4	a^{12}
3	a^{13}
2	a^{14}
1	1

x_1^{14}	B	A	0	C	0	0	A	D
x_1^{13}	0	a^{12}	0	0	0	E	a^5	F
x_1^{12}	G	H	0	0	I	0	0	L
x_1^{11}	M	B	0	0	C	M	0	A
x_1^{10}	0	E	a^2	0	N	O	E	1
$x_1^9 I$	0	0	0	P	I	G	H	
x_1^8	C	M	0	0	D	C	M	B
x_1^7	0	0	0	a^{10}	F	N	O	E
x_1^6	P	I	G	0	L	P	I	G
x_1^5	D	C	M	0	A	D	C	M
x_1^4	0	N	O	0	a^9	F	N	O
x_1^3	L	0	0	G	0	L	P	I
x_1^2	A	D	C	0	B	A	D	C
x_1^1	a^{10}	0	N	0	0	a^{10}	F	N
x_1^0	H	L	P	0	G	H	L	P
	x_2^0	x_2^1	x_2^2	x_2^3	x_2^4	x_2^5	x_2^6	x_2^7

If M is the middle term for our configuration we get: $A = a^4 M^{14}$, $B = a^8 M^2$, $C = a^2 M^8$, $D = aM^{11}$, $E = a^{10} M^3$, $F = a^{10} M^{12}$ $G = aM^4$, $H = a^4 M$, $I = a^2 M^7$, $L = a^8 M^{13}$, $M = a^{15} M^5$, $N = a^5 M^9$, $O = a^5 M^6$, $P = a^{15} M^{10}$.

$\mathbb{F}_{16}$, 3 errors.

The 4096 points are
$(x_1, x_2, x_3, z_1, z_2, z_3) := (a + b + c, a^3 + b^3 + c^3, a^5 + b^5 + c^5, a, b, c)$,
$a, b, c \in \mathbb{F}_{16}$.

As before we exclude the ones with the same errors, reducing to 560 6-tuples.

We found a configuration leading to a polynomial with 288 terms.

It seems to be isolated for permutations, but it can depend on the choice of the corresponding points, which is not unique.

We show that also this configuration presents a sort of symmetry.

$\mathbb{F}_{16}$, 3 ERRORS.

The 4096 points are
$(x_1, x_2, x_3, z_1, z_2, z_3) := (a + b + c, a^3 + b^3 + c^3, a^5 + b^5 + c^5, a, b, c)$,
$a, b, c \in \mathbb{F}_{16}$.
As before we exclude the ones with the same errors, reducing to 560 6-tuples.
We found a configuration leading to a polynomial with 288 terms.
It seems to be isolated for permutations, but it can depend on the choice of the corresponding points, which is not unique.
We show that also this configuration presents a sort of symmetry.

$\mathbb{F}_{16}$, 3 errors.

The 4096 points are
$(x_1, x_2, x_3, z_1, z_2, z_3) := (a + b + c, a^3 + b^3 + c^3, a^5 + b^5 + c^5, a, b, c)$,
$a, b, c \in \mathbb{F}_{16}$.
As before we exclude the ones with the same errors, reducing to 560 6-tuples.
We found a configuration leading to a polynomial with 288 terms.
It seems to be isolated for permutations, but it can depend on the choice of the corresponding points, which is not unique.
We show that also this configuration presents a sort of symmetry.

$\mathbb{F}_{16}$, 3 errors.

The 4096 points are
$(x_1, x_2, x_3, z_1, z_2, z_3) := (a + b + c, a^3 + b^3 + c^3, a^5 + b^5 + c^5, a, b, c)$,
$a, b, c \in \mathbb{F}_{16}$.
As before we exclude the ones with the same errors, reducing to 560 6-tuples.
We found a configuration leading to a polynomial with 288 terms.
It seems to be isolated for permutations, but it can depend on the choice of the corresponding points, which is not unique.
We show that also this configuration presents a sort of symmetry.

Points	Third coordinate
0	0
14	a^1
26	a^2
36	a^3
44	a^4
50	a^5
54	a^6
56	a^7
56	a^8
54	a^9
50	a^{10}
44	a^{11}
36	a^{12}
26	a^{13}
14	a^{14}
0	1

Thanks for your attention!