Improved decoding of affine-variety codes

Chiara Marcolla,
Emmanuela Orsini, Massimiliano Sala

University of Trento, Italy
Department of Mathematics

Trento, 2012

Affine-variety codes: decoding and small weight

Affine-variety codes

Let $\mathbb{F}_q$ be a finite field.
Let $I \in \mathbb{F}_q[X] = \mathbb{F}_q[x_1, \ldots, x_m]$ be a zero-dimensional and radical ideal. Let $\mathcal{V}(I) = \mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ its variety.

Definition

Let $P_0 = (\overline{x}_{0,1}, \ldots, \overline{x}_{0,m}) \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$.
We say that P_0 is an optimal ghost point if there is a $1 \leq j \leq m$ such that the hyperplane $x_j = \overline{x}_{0,j}$ does not intersect the variety.

We call evaluation map

$$ev_{\mathcal{P}} : R = \mathbb{F}_q[x_1, \ldots, x_m]/I \longrightarrow (\mathbb{F}_q)^n$$

$$ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

Affine-variety codes

Let $\mathbb{F}_q$ be a finite field.
Let $I \in \mathbb{F}_q[X] = \mathbb{F}_q[x_1, \ldots, x_m]$ be a zero-dimensional and radical ideal. Let $\mathcal{V}(I) = \mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ its variety.

Definition

Let $P_0 = (\overline{x}_{0,1}, \ldots, \overline{x}_{0,m}) \in (\mathbb{F}_q)^m \setminus \mathcal{V}(I)$.
We say that P_0 is an optimal ghost point if there is a $1 \leq j \leq m$ such that the hyperplane $x_j = \overline{x}_{0,j}$ does not intersect the variety.

We call evaluation map

$$ev_{\mathcal{P}} : R = \mathbb{F}_q[x_1, \ldots, x_m]/I \longrightarrow (\mathbb{F}_q)^n$$

$$ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

Affine-variety codes

Let $L \subseteq R$ be an $\mathbb{F}_q$ vector subspace of R with dimension r.

Definition

The affine-variety code $C(I, L)$ is the image $ev_{\mathcal{P}}(L)$ and the affine-variety code

$$C^{\perp}(I, L) = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in L\}$$

is its dual code

Let $L = \langle b_1, \ldots, b_r \rangle$, then the parity - check matrix for $C^{\perp}(I, L)$ is

$$H = \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

Hermitian code

We consider the Hermitian curve χ over $\mathbb{F}_{q^2}$

$$x^{q+1} = y^q + y$$

This curve has $n = q^3$ rational points that we call $\mathcal{P} = \{P_1, \ldots, P_n\}$.

Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid qr + (q+1)s \leq m,\ 0 \leq s \leq q-1, 0 \leq r \leq q^2 - 1\}.$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q} \rangle.$$

Therefore

$$C_m = (E_m)^{\perp} = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in \mathcal{B}_{m,q}\}$$

is called Hermitian code. The parity-check matrix $\mathbf{H}$ of $C(m,q)$ is

$$\mathbf{H} = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \ldots & f_i(P_n) \end{pmatrix} \text{ where } f_j \in \mathcal{B}_{m,q}.$$

Hermitian code

We consider the Hermitian curve χ over $\mathbb{F}_{q^2}$

$$x^{q+1} = y^q + y$$

This curve has $n = q^3$ rational points that we call $\mathcal{P} = \{P_1, \ldots, P_n\}$.
Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid qr + (q+1)s \leq m,\ 0 \leq s \leq q-1, 0 \leq r \leq q^2 - 1\}.$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q} \rangle.$$

Therefore

$$C_m = (E_m)^{\perp} = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in \mathcal{B}_{m,q}\}$$

is called Hermitian code. The parity-check matrix $\mathbf{H}$ of $C(m,q)$ is

$$\mathbf{H} = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \ldots & f_i(P_n) \end{pmatrix} \text{ where } f_j \in \mathcal{B}_{m,q}.$$

Hermitian code

We consider the Hermitian curve χ over $\mathbb{F}_{q^2}$

$$x^{q+1} = y^q + y$$

This curve has $n = q^3$ rational points that we call $\mathcal{P} = \{P_1, \dots, P_n\}$.
Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid qr + (q+1)s \leq m,\ 0 \leq s \leq q-1, 0 \leq r \leq q^2 - 1\}.$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q} \rangle.$$

Therefore

$$C_m = (E_m)^{\perp} = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in \mathcal{B}_{m,q}\}$$

is called Hermitian code. The parity-check matrix $\mathbf{H}$ of $C(m, q)$ is

$$\mathbf{H} = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \dots & f_i(P_n) \end{pmatrix} \text{ where } f_j \in \mathcal{B}_{m,q}.$$

Affine-variety codes: decoding and small weights

Weakly stratified ideal

Let $J \subset \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_1, \mathcal{T}] = \mathbb{K}[\mathcal{S}, \mathcal{A}, \mathcal{T}]$ be a zero-dimensional ideal, with

$$\mathcal{S} = \{s_1, \ldots, s_N\},\ \mathcal{A}_j = \{a_{j,1}, \ldots, a_{j,m}\},\ \mathcal{T} = \{t_1, \ldots, t_K\}.$$

Definition

We say that J is a weakly stratified ideal if

$$\Sigma_l^{j,i} \neq \emptyset \qquad \text{for } 1 \leq l \leq \eta(j,i),\ 1 \leq i \leq m,\ 1 \leq j \leq L.$$

where $\eta(j,i)$ is the maximum number of extensions at any level $\Sigma_l^{j,i}$ and

$$\Sigma_l^{j,i} = \{(\bar{\mathcal{S}}, \bar{\mathcal{A}}_L, \ldots, \bar{\mathcal{A}}_{j+1}, \bar{a}_{j,1}, \ldots, \bar{a}_{j,i-1}) \in \mathcal{V}(J_{(j,i-1)}) \mid \exists \text{ exactly } l \text{ distinct values } \{\bar{a}_{j,i}^{(1)}, \ldots, \bar{a}_{j,i}^{(l)}\} \text{ s.t. } (\bar{\mathcal{S}}, \bar{\mathcal{A}}_L, \ldots, \bar{\mathcal{A}}_{j+1}, \bar{a}_{j,1}, \ldots, \bar{a}_{j,i-1}, \bar{a}_{j,i}^{(\ell)}) \text{ is in } \mathcal{V}(J_{(j,i)}), 1 \leq \ell \leq l\}, \quad i = 2, \ldots, m,\ j = 1, \ldots, L-1.$$

Example ($L = 2$, $m = 1$)

Let $\mathcal{S} = \{s_1\}$, $\mathcal{A}_1 = \{a_{1,1}\}$, $\mathcal{A}_2 = \{a_{2,1}\}$ and $\mathcal{T} = \{t_1\}$. Let $J = \mathcal{I}(Z)$ with $Z = \{(0,0,0,0), (0,1,1,0), (0,2,2,0)\}$.

$$\mathcal{V}(J_{\mathcal{S}}) = \{0\}, \quad \mathcal{V}(J_{\mathcal{S},a_{2,1}}) = \{(0,0),(0,1),(0,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},a_{2,1},a_{1,1}}) = \{(0,0,0),(0,1,1),(0,2,2)\}.$$

Let us consider the projection

$$\pi_2 : \mathcal{V}(J_{\mathcal{S},a_{2,1}}) \to \mathcal{V}(J_{\mathcal{S}}).$$

Then $|\pi_2^{-1}(\{0\})| = 3$ and we have $\sum_3^{2,1} = \{0\}$. So $\eta(2,1) = 3$. But $\sum_1^{2,1} = \emptyset$, $\sum_2^{2,1} = \emptyset$ and J is not a weakly stratified ideal.

Example ($L = 2, m = 1$)

Let $\mathcal{S} = \{s_1\}$, $\mathcal{A}_1 = \{a_{1,1}\}$, $\mathcal{A}_2 = \{a_{2,1}\}$ and $\mathcal{T} = \{t_1\}$. Let $J = \mathcal{I}(Z)$ with $Z = \{(0,0,0,0),\ (0,1,1,0),\ (0,2,2,0)\}$.

$$\mathcal{V}(J_{\mathcal{S}}) = \{0\}, \quad \mathcal{V}(J_{\mathcal{S},a_{2,1}}) = \{(0,0),(0,1),(0,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},a_{2,1},a_{1,1}}) = \{(0,0,0),(0,1,1),(0,2,2)\}.$$

Let us consider the projection

$$\pi_2 : \mathcal{V}(J_{\mathcal{S},a_{2,1}}) \to \mathcal{V}(J_{\mathcal{S}}).$$

Then $|\pi_2^{-1}(\{0\})| = 3$ and we have $\sum_3^{2,1} = \{0\}$. So $\eta(2,1) = 3$.
But $\sum_1^{2,1} = \emptyset$, $\sum_2^{2,1} = \emptyset$ and J is not a weakly stratified ideal.

Example ($L = 2, m = 1$)

Let $\mathcal{S} = \{s_1\}$, $\mathcal{A}_1 = \{a_{1,1}\}$, $\mathcal{A}_2 = \{a_{2,1}\}$ and $\mathcal{T} = \{t_1\}$. Let $J = \mathcal{I}(Z)$ with $Z = \{(0,0,0,0),\ (0,1,1,0),\ (0,2,2,0)\}$.

$$\mathcal{V}(J_{\mathcal{S}}) = \{0\}, \quad \mathcal{V}(J_{\mathcal{S},a_{2,1}}) = \{(0,0),(0,1),(0,2)\},$$
$$\mathcal{V}(J_{\mathcal{S},a_{2,1},a_{1,1}}) = \{(0,0,0),(0,1,1),(0,2,2)\}.$$

Let us consider the projection

$$\pi_2 : \mathcal{V}(J_{\mathcal{S},a_{2,1}}) \to \mathcal{V}(J_{\mathcal{S}}).$$

Then $|\pi_2^{-1}(\{0\})| = 3$ and we have $\sum_3^{2,1} = \{0\}$. So $\eta(2,1) = 3$. But $\sum_1^{2,1} = \emptyset$, $\sum_2^{2,1} = \emptyset$ and J is not a weakly stratified ideal.

Example ($L = 3$, $m = 1$)

Let $\mathcal{S} = \{\mathrm{s}_1\}$, $\mathcal{A}_1 = \{\mathrm{a}_{1,1}\}$, $\mathcal{A}_2 = \{\mathrm{a}_{2,1}\}$, $\mathcal{A}_3 = \{\mathrm{a}_{3,1}\}$, $\mathcal{T} = \{\mathrm{t}_1\}$.
Let $J = \mathcal{I}(Z) \subset \mathbb{C}[\mathrm{s}_1, \mathrm{a}_{3,1}, \mathrm{a}_{2,1}, \mathrm{a}_{1,1}, \mathrm{t}_1]$ with

$$Z = \{(0,1,0,0,0),\ (0,2,1,1,2),\ (2,2,2,0,0)\}.$$

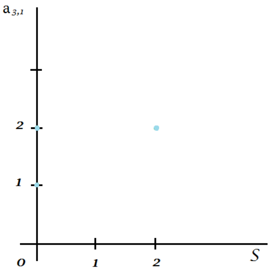
The order $<$ is $s_1 < a_{3,1} < a_{2,1} < a_{1,1} < t_1$ and the varieties are

$$\mathcal{V}(J_{\mathcal{S}}) = \{0,2\}, \quad \mathcal{V}(J_{\mathcal{S},\mathrm{a}_{3,1}}) = \{(0,1),(0,2),(2,2)\},$$

$$\mathcal{V}(J_{\mathcal{S},\mathrm{a}_{3,1},\mathrm{a}_{2,1}}) = \{(0,1,0),(0,2,1),(2,2,2)\},$$

$$\mathcal{V}(J_{\mathcal{S},\mathrm{a}_{3,1},\mathrm{a}_{2,1},\mathrm{a}_{1,1}}) = \{(0,1,0,0),(0,2,1,1),(2,2,2,0)\}.$$

Example ($L = 3, m = 1$)



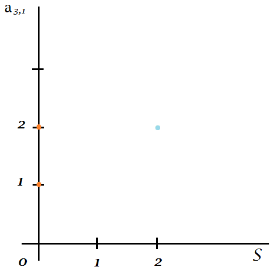
Let us consider the projection

$$\pi_3 : \mathcal{V}(\mathcal{J}_{\mathcal{S},a_{3,1}}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}}).$$

where

$$\mathcal{V}(J_{\mathcal{S}}) = \{0, 2\},$$
$$\mathcal{V}(J_{\mathcal{S},a_{3,1}}) = \{(0,1),(0,2),(2,2)\}.$$

Example ($L = 3, m = 1$)



Let us consider the projection

$$\pi_3 : \mathcal{V}(\mathcal{J}_{\mathcal{S},a_{3,1}}) \to \mathcal{V}(\mathcal{J}_{\mathcal{S}}).$$

where

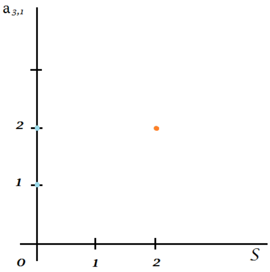
$$\mathcal{V}(J_{\mathcal{S}}) = \{0, 2\},$$
$$\mathcal{V}(J_{\mathcal{S},a_{3,1}}) = \{(0,1), (0,2), (2,2)\}.$$

Then

$$|\pi_3^{-1}(\{0\})| = 2 \quad \text{and} \quad |\pi_3^{-1}(\{2\})| = 1.$$

So $\sum_2^{3,1} = \{0\}$.

Example ($L = 3$, $m = 1$)



Let us consider the projection

$$\pi_3 : \mathcal{V}(\mathcal{J}_{\mathcal{S},\mathrm{a}_{3,1}}) \rightarrow \mathcal{V}(\mathcal{J}_{\mathcal{S}}).$$

where

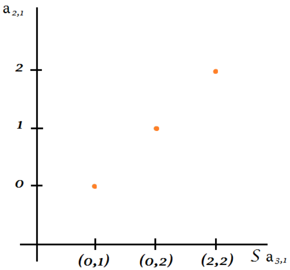
$$\mathcal{V}(J_{\mathcal{S}}) = \{0, 2\},$$
$$\mathcal{V}(J_{\mathcal{S},\mathrm{a}_{3,1}}) = \{(0,1), (0,2), (2,2)\}.$$

Then

$$|\pi_3^{-1}(\{0\})| = 2 \quad \text{and} \quad |\pi_3^{-1}(\{2\})| = 1.$$

So $\sum_2^{3,1} = \{0\}$, $\sum_1^{3,1} = \{2\}$.

Example ($L = 3$, $m = 1$)



Let us consider the projection

$$\pi_2 : \mathcal{V}(J_{\mathcal{S},a_{3,1},a_{2,1}}) \to \mathcal{V}(J_{\mathcal{S},a_{3,1}}).$$

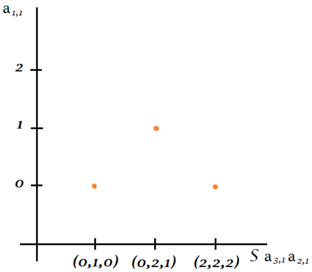
where

$$\mathcal{V}(J_{\mathcal{S},a_{3,1}}) = \{(0,1),(0,2),(2,2)\}$$
$$\mathcal{V}(J_{\mathcal{S},a_{3,1},a_{2,1}}) = \{(0,1,0),(0,2,1),(2,2,2)\}.$$

Then

$$\sum_{1}^{2,1} = \{(0,1),(0,2),(2,2)\} \text{ and } \eta(2,1) = 1.$$

Example ($L = 3$, $m = 1$)



Let us consider the projection

$$\pi_1 : \mathcal{V}(J_{\mathcal{S},a_{3,1},a_{2,1},a_{1,1}}) \to \mathcal{V}(J_{\mathcal{S},a_{3,1},a_{2,1}}).$$

where

$$\mathcal{V}(J_{(2,1)}) = \{(0,1,0),(0,2,1),(2,2,2)\},$$
$$\mathcal{V}(J_{(1,1)}) = \{(0,1,0,0),(0,2,1,1),(2,2,2,0)\}.$$

Then

$$\sum_{1}^{1,1} = \{(0,1,0),(0,2,1),(2,2,2)\} \text{ and } \eta(1,1) = 1.$$

So J is a weakly stratified.

Stuffed ideal

Let $\mathcal{R} = \mathbb{K}[\mathcal{S}, \mathcal{A}_L, \ldots, \mathcal{A}_{j+1}, \mathrm{a}_{j,1}, \ldots, \mathrm{a}_{j,i-1}]$. Let $K \subset \mathcal{R}[\mathrm{a}_{j,i}]$ be a zero-dimensional ideal and let $P_h \in \Sigma_h^{j,i}$ where $1 \leq h \leq \delta - 1$, then exist $g \in G = \mathrm{GB}(K)$ such that

$$g(P_h, \mathrm{a}_{j,i}) = \mathrm{a}_{j,i}^{\delta} + \alpha_{\delta-1}\mathrm{a}_{j,i}^{\delta-1} + \ldots + \alpha_0 \in \mathbb{K}[\mathrm{a}_{j,i}]$$

where $\alpha_i \in \mathbb{K}$ and $\delta = \eta(j, i)$.

Definition

We say that K is stuffed if for any $1 \leq h \leq \delta - 1$ and for any $P_h \in \Sigma_h^{j,i}$, the equation

$$g(P_h, \mathrm{a}_{j,i}) = 0$$

has h distinct solutions in $\mathbb{K}$.

Multi-dimensional general error locator polynomials

Let $C = C^{\perp}(I, L)$ be an affine-variety code.
Let P_0 be a ghost point and let $t_i = \min\{t, |\{\pi_i(P) | P \in \mathcal{V}(I) \cup P_0\}|\}$ where $\pi_i(\bar{x}_1, \ldots, \bar{x}_m) = \bar{x}_i$.
We consider

$$\mathcal{L}_i(S, x_1, \ldots, x_i) = x_i^{t_i} + a_{t_i-1} x_i^{t_i-1} + \ldots + a_0,$$

where $S = \{s_1, \ldots, s_r\}$ and $a_j \in \mathbb{F}_q[S, x_1, \ldots, x_{i-1}]$.
Let $\mathbf{e}$ be an error s.t. $\mathrm{w}(\mathbf{e}) = \mu \leq \mathbf{t}$, $\mathbf{s} \in (\mathbb{F}_q)^r$ is the corresponding syndrome and $(\bar{x}_{1,1}, \ldots, \bar{x}_{1,m}), \ldots, (\bar{x}_{\mu,1}, \ldots, \bar{x}_{\mu,m})$ are error locations.
Let $\mathbf{x}^j = (\bar{x}_{j,1}, \ldots, \bar{x}_{j,i-1})$. Then, if the roots of

$$\mathcal{L}_i(\mathbf{s}, \mathbf{x}^j, x_i)$$

are $\{\bar{x}_{h,i} \mid \bar{\mathbf{x}}^h = \bar{\mathbf{x}}^j,\ 1 \leq h \leq \mu, \text{ when } \mu = t \text{ or } 0 \leq h \leq \mu, \text{ when } \mu \leq t-1\}$,
then $\{\mathcal{L}_i\}_{1 \leq i \leq m}$ is a set of multi-dimensional general error locator polynomials for C.

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points . The syndrome is .

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is
$\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{array}{lcl} \mathcal{P}_x(S,x) & = & x^2 + f(S)\,x \\ \mathcal{P}_{xy}(S,x,y) & = & y^2 + f_1(S)\,y + f_2(S)\,x + f_3(S) \end{array}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is
$\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{aligned} \mathcal{P}_x(\mathbf{s}, x) &= x^2 + x = x(x-1) \\ \mathcal{P}_{xy}(S, x, y) &= y^2 + f_1(S)\,y + f_2(S)\,x + f_3(S) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is $\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{array}{rcl} \mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x = x(x-1) \\ \mathcal{P}_{xy}(\mathbf{s}, 0, y) & = & y^2 + y = y(y-1) \end{array}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is $\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{array}{lll} \mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x = x(x-1) \\ \mathcal{P}_{xy}(\mathbf{s}, 0, y) & = & y^2 + y = y(y-1) \end{array}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1,1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1,\ldots,s_5,x)$ and $\mathcal{P}_{xy}(s_1,\ldots,s_5,x,y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is
$\mathbf{s} = (0,1,1,1,0)$.

$$\begin{aligned}
\mathcal{P}_x(\mathbf{s},x) &= x^2 + x = x(x-1)\\
\mathcal{P}_{xy}(\mathbf{s},0,y) &= y^2 + y = y(y-1)
\end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \dots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \dots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is

$\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{aligned}
\mathcal{P}_x(\mathbf{s}, x) &= x^2 + x = x(x-1) \\
\mathcal{P}_{xy}(\mathbf{s}, 1, y) &= y^2 + y = y(y-1)
\end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is

$\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{array}{lcl} \mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x = x(x-1) \\ \mathcal{P}_{xy}(\mathbf{s}, 1, y) & = & y^2 + y = y(y-1) \end{array} \quad \Longrightarrow (1,0) \notin \chi$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is
$\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{array}{lcll} \mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x = x(x-1) & \Longrightarrow (1,0) \notin \chi \\ \mathcal{P}_{xy}(\mathbf{s}, 1, y) & = & y^2 + y = y(y-1) & \Longrightarrow (1,1) \notin \chi \end{array}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{aligned} \mathcal{P}_x(S, x) &= x^2 + f(S)\,x \\ \mathcal{P}_{xy}(S, x, y) &= y^2 + f_1(S)\,y + f_2(S)\,x + f_3(S) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1,1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1,\dots,s_5,x)$ and $\mathcal{P}_{xy}(s_1,\dots,s_5,x,y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$\mathbf{s} = (\alpha+1, 0, \alpha, 0, 0)$.

$$\begin{aligned} \mathcal{P}_x(\mathbf{s},x) &= x^2+x+1 = (x-\alpha)(x-\alpha^2) \\ \mathcal{P}_{xy}(S,x,y) &= y^2 + f_1(S)\,y + f_2(S)\,x + f_3(S) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is $\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{aligned} \mathcal{P}_x(\mathbf{s}, x) &= x^2 + x + 1 = (x - \alpha)(x - \alpha^2) \\ \mathcal{P}_{xy}(\mathbf{s}, \alpha, y) &= y^2 + y + 1 = (y - \alpha)(y - \alpha^2) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is
$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{array}{lcl} \mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x + 1 = (x - \alpha)(x - \alpha^2) \\ \mathcal{P}_{xy}(\mathbf{s}, \alpha, y) & = & y^2 + y + 1 = (y - \alpha)(y - \alpha^2) \end{array}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1,1)$ is the ghost point and Hermitian points are

$$
\begin{array}{llll}
P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\
P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2).
\end{array}
$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \ldots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \ldots, s_5, x, y)$ be the *polynomials* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0).$$

$$
\begin{array}{lcl}
\mathcal{P}_x(\mathbf{s}, x) & = & x^2 + x + 1 = (x - \alpha)(x - \alpha^2) \\
\mathcal{P}_{xy}(\mathbf{s}, \alpha, y) & = & y^2 + y + 1 = (y - \alpha)(y - \alpha^2)
\end{array}
$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{P}_x(s_1, \dots, s_5, x)$ and $\mathcal{P}_{xy}(s_1, \dots, s_5, x, y)$ be the *weakly locators* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\mathcal{P}_x(\mathbf{s}, x) = x^2 + x + 1 = (x - \alpha)(x - \alpha^2)$$
$$\mathcal{P}_{xy}(\mathbf{s}, \alpha^2, y) = y^2 + y + 1 = (y - \alpha)(y - \alpha^2)$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \ldots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \ldots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is
$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{array}{lcl} \mathcal{L}_x(S,x) & = & x^2 + a(S)\,x + b(S) \\ \mathcal{L}_{xy}(S,x,y) & = & y^2 + A(S)\,y + B(S)\,x + C(S) \end{array}$$

We *stuff* the ideal I.

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1,1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \dots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \dots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{aligned} \mathcal{L}_x(\mathbf{s}, x) &= x^2 + x + 1 = (x - \alpha)(x - \alpha^2) \\ \mathcal{L}_{xy}(S, x, y) &= y^2 + A(S)\,y + B(S)\,x + C(S) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \dots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \dots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is
$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0)$.

$$\begin{aligned} \mathcal{L}_x(\mathbf{s}, x) &= x^2 + x + 1 = (x - \alpha)(x - \alpha^2) \\ \mathcal{L}_{xy}(\mathbf{s}, \alpha, y) &= y^2 + \alpha = (y - \alpha^2)^2 \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0),\quad P_2 = (0,1),\quad P_3 = (1,\alpha),\quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha),\quad P_6 = (\alpha,\alpha^2),\quad P_7 = (\alpha^2,\alpha),\quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \dots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \dots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_6 and P_7 . The syndrome is

$\mathbf{s} = (\alpha + 1, 0, \alpha, 0, 0).$

$$\mathcal{L}_x(\mathbf{s}, x) = x^2 + x + 1 = (x - \alpha)(x - \alpha^2)$$
$$\mathcal{L}_{xy}(\mathbf{s}, \alpha^2, y) = y^2 + \alpha^2 = (y - \alpha)^2$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$\begin{array}{llll} P_1 = (0,0), & P_2 = (0,1), & P_3 = (1,\alpha), & P_4 = (1,\alpha^2), \\ P_5 = (\alpha,\alpha), & P_6 = (\alpha,\alpha^2), & P_7 = (\alpha^2,\alpha), & P_8 = (\alpha^2,\alpha^2). \end{array}$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \ldots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \ldots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is $\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{aligned} \mathcal{L}_x(\mathbf{s}, x) &= x^2 \\ \mathcal{L}_{xy}(S, x, y) &= y^2 + A(S)\,y + B(S)\,x + C(S) \end{aligned}$$

Example (Hermitian code $q = 2$)

Let $x^3 = y^2 + y$ be the Hermitian curve over $\mathbb{F}_4$.

The $P_0 = (1, 1)$ is the ghost point and Hermitian points are

$$P_1 = (0,0), \quad P_2 = (0,1), \quad P_3 = (1,\alpha), \quad P_4 = (1,\alpha^2),$$
$$P_5 = (\alpha,\alpha), \quad P_6 = (\alpha,\alpha^2), \quad P_7 = (\alpha^2,\alpha), \quad P_8 = (\alpha^2,\alpha^2).$$

Let C be the Hermitian code with $\mathcal{B}_{m,2} = \{1, x, y, x^2, xy\}$.
Let $\mathcal{L}_x(s_1, \ldots, s_5, x)$ and $\mathcal{L}_{xy}(s_1, \ldots, s_5, x, y)$ be the *locators* in the Gröbner basis G.

Two errors occur at the points P_1 and P_2. The syndrome is $\mathbf{s} = (0, 1, 1, 1, 0)$.

$$\begin{aligned} \mathcal{L}_x(\mathbf{s}, x) &= x^2 \\ \mathcal{L}_{xy}(\mathbf{s}, 0, y) &= y^2 + y = y(y-1) \end{aligned}$$

Thank you for your attention!