THE SYNDROME VARIETY

Edgar Martínez Moro

Dept. Applied Mathematics

Universidad de Valladolid

edgar@maf.uva.es

S3CM: algebraic coding theory

July 2008

Introduction

The syndrome variety of a cyclic code

- Loustaunau-York “trick”
- Elimination

Descoding with the S.V.

- FGLM

Affine variety codes

- Decoding AVC
- Precomputing the error locators

Introduction

During this session we will review an algorithmic method for decoding cyclic codes using Gröbner basis.

Introduction

During this session we will review an algorithmic method for decoding cyclic codes using Gröbner basis.

P. Fitzpatrick proposed the use of Gröbner basis over modules as a theoretical tool for understanding the key equation and gives a method with similar complexity to the Berlekamp-Massey algorithm.

Introduction

During this session we will review an algorithmic method for decoding cyclic codes using Gröbner basis.

P. Fitzpatrick proposed the use of Gröbner basis over modules as a theoretical tool for understanding the key equation and gives a method with similar complexity to the Berlekamp-Massey algorithm.

A.B. Cooper showed an algorithm that can correct errors in a cyclic code up to its minimum distance. This algorithm can be stated in terms of elimination theory, thus it can be solved computing a Gröbner basis for each non-zero syndrome that we had received.

Introduction

During this session we will review an algorithmic method for decoding cyclic codes using Gröbner basis.

P. Fitzpatrick proposed the use of Gröbner basis over modules as a theoretical tool for understanding the key equation and gives a method with similar complexity to the Berlekamp-Massey algorithm.

A.B. Cooper showed an algorithm that can correct errors in a cyclic code up to its minimum distance. This algorithm can be stated in terms of elimination theory, thus it can be solved computing a Gröbner basis for each non-zero syndrome that we had received.X. Chen, I.S. Reed, T. Helleseth y K. Truong revisited the original Cooper's theory an they proposed to compute a generic Gröbner basis that can be used for all the possible syndromes.

Introduction

During this session we will review an algorithmic method for decoding cyclic codes using Gröbner basis.
P. Fitzpatrick proposed the use of Gröbner basis over modules as a theoretical tool for understanding the key equation and gives a method with similar complexity to the Berlekamp-Massey algorithm.
A.B. Cooper showed an algorithm that can correct errors in a cyclic code up to its minimum distance. This algorithm can be stated in terms of elimination theory, thus it can be solved computing a Gröbner basis for each non-zero syndrome that we had received.X. Chen, I.S. Reed, T. Helleseth y K. Truong revisited the original Cooper's theory an they proposed to compute a generic Gröbner basis that can be used for all the possible syndromes.Finally J. Fitzgerald y R.F. Lax applied this idea to affine variety codes.

The syndrome variety of a cyclic code

Let α be a primitive root of $x^n - 1$ in the corresponding extension field of $\mathbb{F}_q$ (as ussual we will asume that $\mathrm{mcd}(n, q) = 1$).

The syndrome variety of a cyclic code

Let α be a primitive root of $x^n - 1$ in the corresponding extension field of $\mathbb{F}_q$ (as ussual we will asume that $\mathrm{mcd}(n, q) = 1$). Let $g(x)$ be the generator polynomial of a cyclic code whose roots are $\alpha^{i_1}, \ldots, \alpha^{i_r}$ where $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n-1\}$. The code $\mathcal{C}$ generated by $g(x)$ can be seen as the kernel in $\mathbb{F}_q^n$ of the "parity check matrix"

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \cdots & \alpha^{i_1(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{i_r} & \cdots & \alpha^{i_r(n-1)} \end{pmatrix}. \qquad (1)$$

The syndrome variety of a cyclic code

Let $\tilde{\mathbf{c}} \in \mathbb{F}_q^n$ be a received vector where $\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}$ and $\mathbf{c} \in \mathcal{C}$, $\mathbf{e}$ the error.

The syndrome variety of a cyclic code

Let $\tilde{\mathbf{c}} \in \mathbb{F}_q^n$ be a received vector where $\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}$ and $\mathbf{c} \in \mathcal{C}$, $\mathbf{e}$ the error.The following system of equations relates the syndrome $\mathbf{s}$ corresponding to $\tilde{\mathbf{c}}$ with the error

$$[S] \quad e_0 + e_1\alpha^{i_j} + e_2\alpha^{2i_j} + \cdots + e_1\alpha^{(n-1)i_j} = s_j, \quad j = 1, \ldots, r. \quad (2)$$

The syndrome variety of a cyclic code

Let $\tilde{\mathbf{c}} \in \mathbb{F}_q^n$ be a received vector where $\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}$ and $\mathbf{c} \in \mathcal{C}$, $\mathbf{e}$ the error.The following system of equations relates the syndrome $\mathbf{s}$ corresponding to $\tilde{\mathbf{c}}$ with the error

$$[S] \quad e_0 + e_1\alpha^{i_j} + e_2\alpha^{2i_j} + \cdots + e_1\alpha^{(n-1)i_j} = s_j, \quad j = 1, \ldots, r. \quad (2)$$

Let us assume that $w(\mathbf{e}) = \tau \leq t$, where $2t + 1 = d$ the minimun distance of $\mathcal{C}$.

The syndrome variety of a cyclic code

Consider the following polynomials:

$$\begin{aligned} f_j &= y_1 z_1^{i_j} + y_2 z_2^{i_j} + \cdots + y_t z_t^{i_j} - x_j, \quad j = 1, \ldots, r. && (3) \\ h_k &= z_k^{n+1} - z_k, \quad k = 1, \ldots, t. && (4) \\ l_k &= y_k^{q-1} - 1, \quad k = 1, \ldots, t. && (5) \end{aligned}$$

$$F = \{f_j \mid j = 1, \ldots, r\} \cup \{h_k \mid k = 1, \ldots, t\} \cup \{l_k \mid k = 1, \ldots, t\}$$

The syndrome variety of a cyclic code

Consider the following polynomials:

$$\begin{aligned} f_j &= y_1 z_1^{i_j} + y_2 z_2^{i_j} + \cdots + y_t z_t^{i_j} - x_j, \quad j = 1, \ldots, r. && (3) \\ h_k &= z_k^{n+1} - z_k, \quad k = 1, \ldots, t. && (4) \\ l_k &= y_k^{q-1} - 1, \quad k = 1, \ldots, t. && (5) \end{aligned}$$

$$F = \{f_j \mid j = 1, \ldots, r\} \cup \{h_k \mid k = 1, \ldots, t\} \cup \{l_k \mid k = 1, \ldots, t\}$$

and the ideal $I \subset \mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]$ generated by F. We will define the syndrome variety as $\mathcal{V}(I)$, i.e.:

$$\left\{\mathbf{p} \in \mathbb{F}_{q^m}^{r+2t} \mid f_j(\mathbf{p}) = h_k(\mathbf{p}) = l_k(\mathbf{p}) = 0, \forall j = 1, \ldots, r, \ k = 1, \ldots, t\right\}$$

and I will be denoted as the syndrome ideal.

The syndrome variety of a cyclic code

The number of points in $\mathcal{V}(I)$ is $(q-1)^t(n+1)^t$ therefore I is a zero dimensional ideal.

The syndrome variety of a cyclic code

The number of points in $\mathcal{V}(I)$ is $(q-1)^t(n+1)^t$ therefore I is a zero dimensional ideal.

$\mathcal{V}(I)$ contains all the needed information (and more) to decode $\tilde{\mathbf{c}}$.

Suppose we have that

$$\mathbf{s} = H\tilde{\mathbf{c}} = H\mathbf{e}, \quad w(\mathbf{e}) = \tau \leq t,$$

there are points in $\mathcal{V}(I)$ such that detemine the error locators and error values of $\mathbf{e}$. Those points are given by

$$\mathbf{p} = (s_1, s_2, \ldots, s_r, 0, \ldots, 0, \alpha^{l_1}, \alpha^{l_2}, \ldots, \alpha^{l_\tau}, *, \ldots, *, \beta_1, \beta_2, \ldots, \beta_\tau),$$

where $s_1, s_2, \ldots, s_r$ corresponds to the syndrome (coordinates $\mathbf{x}$), the non zero values $\mathbf{e}$ (error positions) are located by the coordinates $l_1, l_2, \ldots, l_\tau$ and $\beta_1, \beta_2, \ldots, \beta_\tau$ are the corresponding error values. The symbol $*$ represents any non zero element in $\mathbb{F}_q$.

The syndrome variety of a cyclic code

For each syndrome **s** such that $w(\mathbf{e}) = \tau \leq t$ there are

$$\binom{t}{\tau}\tau!\,(q-1)^{t-\tau}$$

points in $\mathcal{V}(I)$ corresponding to the permutations on the variables in **z** and the same permutation in the variables in **y**. Moreover, they can be represented in other ways (Why?)

The syndrome variety of a cyclic code

For each syndrome $\mathbf{s}$ such that $w(\mathbf{e}) = \tau \leq t$ there are

$$\binom{t}{\tau}\tau!\,(q-1)^{t-\tau}$$

points in $\mathcal{V}(I)$ corresponding to the permutations on the variables in $\mathbf{z}$ and the same permutation in the variables in $\mathbf{y}$. Moreover, they can be represented in other ways (Why?)

Let $\mathcal{V}_{\mathbf{s}}$ be the number of points in the variety for a given syndrome $\mathbf{s}$ and $S \subset \mathbb{F}_q^r$ be the set of all non zero syndromes with weigth less or equal to t. Consider the set

$$\mathcal{E} = \bigcup_{\mathbf{s}\in S} \mathcal{V}_{\mathbf{s}}, \qquad (6)$$

The syndrome variety of a cyclic code

The number of elements in $\mathcal{E}$ is

$$(q-1)^t \sum_{j=1}^{t} \binom{n}{j} \binom{t}{j} j!$$

and in this set there is enought information for decoding any received word with less than t errors. But the syndrome variety has many more points that the set $\mathcal{E}$.

The syndrome variety of a cyclic code

The number of elements in $\mathcal{E}$ is

$$(q-1)^t \sum_{j=1}^{t} \binom{n}{j} \binom{t}{j} j!$$

and in this set there is enought information for decoding any received word with less than t errors. But the syndrome variety has many more points that the set $\mathcal{E}$.

Example.

Consider the primitive BCH code with $q = 2$, length 31, dimension 11 and $t = 5$, we have that

$$|\mathcal{V}(I)| = 33554432$$

$$|\mathcal{E}| = 24444275.$$

The syndrome variety of a cyclic code

If we add to F los $\binom{t}{2}$ the following polynomials

$$z_k z_\lambda \left(\frac{z_k^n - z_\lambda^n}{z_k - z_\lambda} \right), \quad k, \lambda = 1, \ldots, t. \tag{7}$$

that forces to z_k, z_λ be zero one of them or both of them non zero and different. Thus

$$\mathcal{E} = \mathcal{V} \left(F \bigcup \left\{ z_k z_\lambda \left(\frac{z_k^n - z_\lambda^n}{z_k - z_\lambda} \right) \right\}_{k,\lambda=1}^{t} \right). \tag{8}$$

The syndrome variety of a cyclic code

If we add to F los $\binom{t}{2}$ the following polynomials

$$z_k z_\lambda \left(\frac{z_k^n - z_\lambda^n}{z_k - z_\lambda} \right), \quad k, \lambda = 1, \ldots, t. \tag{7}$$

that forces to z_k, z_λ be zero one of them or both of them non zero and different. Thus

$$\mathcal{E} = \mathcal{V} \left(F \bigcup \left\{ z_k z_\lambda \left(\frac{z_k^n - z_\lambda^n}{z_k - z_\lambda} \right) \right\}_{k,\lambda=1}^{t} \right). \tag{8}$$

The direct computation of de $\mathcal{E}$ from the above variety (for example computing a Gröbner basis) can be very hard computationally, P. Loustaunau y E.V. York pointed an alternative strategy for dealing with this problem based in elimination theory.

Loustaunau-York "trick"

The key observation of L-Y work is the number of errors represented by the ("pure") point **p** is t minus the number of non zero coordinates of **p** in the positions corresponding to **z** and that this number of zeros can be computed by inspection of the different projections of the variety.

Loustaunau-York "trick"

The key observation of L-Y work is the number of errors represented by the ("pure") point **p** is t minus the number of non zero coordinates of **p** in the positions corresponding to **z** and that this number of zeros can be computed by inspection of the different projections of the variety.

Definition.

Let $X \subseteq \mathbb{F}_{q^m}^b$ be a set of points, for each $a \leq b$ we define the projection of X over the first a coordinates as

$$\prod_a (X) = \left\{ \mathbf{p} \in \mathbb{F}_{q^m}^a \mid \exists \mathbf{p}' \in \mathbb{F}_{q^m}^{b-a}, \text{ such that } (\mathbf{p}, \mathbf{p}') \in X \right\} \qquad (9)$$

Loustaunau-York "trick"

Theorem

Let $\mathbf{0}_k \in \mathbb{F}_q^k$ be the all zero vector. Given $\tilde{\mathbf{c}}$ and its corresponding syndrome $\mathbf{s}$, the errors in $\tilde{\mathbf{c}}$ are exactly τ if and only if

$$(\mathbf{s}, \mathbf{0}_k) \in \prod_{r+k}(\mathcal{V}(F)), \quad \forall k \leq t - \tau$$

and

$$(\mathbf{s}, \mathbf{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1}(\mathcal{V}(F)).$$

Proof of the theorem

Let $\mathbf{s}$ a syndrome corresponding to $\mathbf{e}$ such that $w(\mathbf{e}) = \tau \leq t$. There exist a point $\mathbf{p}$ and $(\mathbf{s}, \mathbf{0}_k) \in \prod_{r+k}(\mathcal{V}(F))$ for all $k \leq t - \tau$.

Proof of the theorem

Let $\mathbf{s}$ a syndrome corresponding to $\mathbf{e}$ such that $w(\mathbf{e}) = \tau \leq t$. There exist a point $\mathbf{p}$ and $(\mathbf{s}, \mathbf{0}_k) \in \prod_{r+k}(\mathcal{V}(F))$ for all $k \leq t - \tau$.Let us suppose that

$$\mathbf{p}' = (\mathbf{s}, \mathbf{0}_{t-\tau+1}) \in \prod_{r+t-\tau+1}(\mathcal{V}(F)),$$

i.e., $\mathbf{p}'$ extends to a point of the variety

$$\mathbf{p}_0 = \left(\mathbf{p}', \gamma_1, \ldots, \gamma_{\tau-1}, \eta_1, \ldots, \eta_t\right) = \left(\mathbf{p}', \gamma, \eta\right) \in \mathcal{V}(F).$$

Proof of the theorem (Cont. I)

The vector γ has a non zero entry (if not the syndrome would be $\mathbf{s} = \mathbf{0}$),

Proof of the theorem (Cont. I)

The vector γ has a non zero entry (if not the syndrome would be $\mathbf{s} = \mathbf{0}$), more over, their coordinates can not be pairwise different because in such a case it will represent an error and therefore we will have two different error vectors with weigth less than t associated to the samen syndrome Contradiction!.

Proof of the theorem (Cont. I)

The vector γ has a non zero entry (if not the syndrome would be $\mathbf{s} = \mathbf{0}$), more over, their coordinates can not be pairwise different because in such a case it will represent an error and therefore we will have two different error vectors with weigth less than t associated to the samen syndrome Contradiction!.

Thus there must exist two different i, j such that $\gamma_i = \gamma_j$ (i.e. $\mathbf{p}_0 \notin \mathcal{E}$).

Proof of the theorem (Cont. I)

The vector γ has a non zero entry (if not the syndrome would be $\mathbf{s} = \mathbf{0}$), more over, their coordinates can not be pairwise different because in such a case it will represent an error and therefore we will have two different error vectors with weigth less than t associated to the samen syndrome Contradiction!.
Thus there must exist two different i, j such that $\gamma_i = \gamma_j$ (i.e. $\mathbf{p}_0 \notin \mathcal{E}$).Suppose w.l.o.g. that $\gamma_1 = \gamma_2$ and consider

$$\begin{aligned}
\mathbf{p}_1 &= \left(\mathbf{p}', 0, \gamma_2, \ldots, \gamma_{\tau-1}, \eta_1, \eta_1 + \eta_2, \ldots, \eta_t\right) \text{ if } \eta_1 + \eta_2 \neq 0 \\
\mathbf{p}_1 &= \left(\mathbf{p}', 0, 0, \gamma_3, \ldots, \gamma_{\tau-1}, \eta_1, \eta_1, \ldots, \eta_t\right) \text{ in other case.}
\end{aligned}$$

Proof of the theorem (Cont. II)

Again $\mathbf{p}_1 \in \mathcal{V}(F)$ and we can repeat this costruction till we have that the coordinates in γ are all non zero and pairwise different. This will represent an error with weigth strictly less than τ Contradiction!,

Proof of the theorem (Cont. II)

Again $\mathbf{p}_1 \in \mathcal{V}(F)$ and we can repeat this costruction till we have that the coordinates in γ are all non zero and pairwise different. This will represent an error with weigth strictly less than τ Contradiction!,therefore

$$(\mathbf{s}, \mathbf{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1} (\mathcal{V}(F)).$$

Proof of the theorem (Cont. III)

To proof the other implication suppose that

$$(\mathbf{s}, \mathbf{0}_k) \in \prod_{r+k} (\mathcal{V}(F)), \quad \forall k \leq t - \tau$$

and $(\mathbf{s}, \mathbf{0}_{t-\tau+1}) \notin \prod_{r+t-\tau+1} (\mathcal{V}(F))$. Then $(\mathbf{s}, \mathbf{0}_{t-\tau})$ extends to a point in $\mathcal{V}(F)$, and this point can be associated to a unique error vector of weigth exactly τ. □

Loustaunau-York "trick"

Corollary

With the previous notation consider the set

$$\Gamma = \{\mathbf{p} \in \mathcal{V}(F) \mid \mathbf{p} = (\mathbf{s}, \mathbf{0}_{t-\tau}, *, *, \ldots, *)\}. \qquad (10)$$

Then the set $\prod_{r+t-\tau+1}(\Gamma)$ contains exactly τ different points with the following shape

$$(\mathbf{s}, \mathbf{0}_{t-\tau}, \alpha^{l_i}),$$

and the positions of the error correspond to the values l_i such that $i = 1, \ldots, \tau$.

Elimination

Lemma

$$\prod_{r+k}(\mathcal{V}(F)) = \mathcal{V}\left(I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]\right)$$

A proof can be found in [AL96, th. 2.5.3].

Elimination

Lemma

$$\prod_{r+k}(\mathcal{V}(F)) = \mathcal{V}\left(I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]\right)$$

A proof can be found in [AL96, th. 2.5.3].

Consider now a lexicographical ordering $\prec_{lex}$ in $\mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]$ such that

$$x_1 \prec_{lex} \cdots \prec_{lex} x_r \prec_{lex} z_1 \prec_{lex} \cdots \prec_{lex} z_t \prec_{lex} y_1 \prec_{lex} \cdots \prec_{lex} y_t,$$

and let G be a Gröbner basis of the syndrome ideal I w.r.t. $\prec_{lex}$, if we have in mind the theorem of elimination of variables then $G_k = G \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$ is a Gröbner basis of the elimination ideal $I \cap \mathbb{F}_q[\mathbf{x}, z_1, \ldots, z_k]$

Rewritting the Theorem

Theorem

With the previous notation, given $\tilde{\mathbf{c}}$ and its syndrome $\mathbf{s}$, the errors in $\tilde{\mathbf{c}}$ are exactly τ if and only if for each element $g \in G_k$ we have that

$$g(\mathbf{s}, \mathbf{0}_k) = 0, \quad \forall k \leq t - \tau$$

and there exists one element $g \in G_{t-\tau+1}$ such that

$$g(\mathbf{s}, \mathbf{0}_{t-\tau+1}) \neq 0.$$

Rewritting the Corollary

Corollary

Consider $G_{t-\tau+1} = \{g_1, \ldots, g_s\}$ and the vector $\xi_{t-\tau} = (\mathbf{s}, \mathbf{0}_{t-\tau}, z)$ where z is a new variable. The ideal

$$\langle G_{t-\tau+1}(\xi_{t-\tau})\rangle = \langle g_1(\xi_{t-\tau}), \ldots, g_s(\xi_{t-\tau})\rangle \subset \mathbb{F}_q[z] \qquad (11)$$

is generated by the error locator polynomial, moreover, this polynomial is one of the polynomials evaluated in

$$g_1(\xi_{t-\tau}), \ldots, g_s(\xi_{t-\tau}).$$

Proof.

First part of the corollary is a direct translation of the previous theorems and corollary. In oreder to proof the second part we must check that $G_{t-\tau+1}(\xi_{t-\tau})$ is a Gröbner basis, but this is always true in the zero dimensional w.r.t. a lexicographic ordering (see [Gia89]). □

Descoding with the S.V.

In the conditions of the previous corollary we could compute the error locator polynomial from the ideal $\langle G_{t-\tau}(\xi_{t-\tau-1})\rangle$ since this ideal is generated by z times the error locator polynomial.
This is true because in this case the variety are those points projecting points from $\mathcal{E}$. The points in $\mathcal{V}(F) \setminus \mathcal{E}$ whose coordinates in $\mathbf{x}$ corresponds to a syndrome $\mathbf{s}$ are the points of $\mathcal{V}_{\mathbf{s}}$ with two or more zero coordinates in $\mathbf{z}$ where substituted by the same element in $\mathbb{F}_q$. But for the $t-\tau$-th elimination ideal there is only one free variable in $\mathbf{z}$ thus the previous situation is impossible.

Descoding with the S.V.

In the conditions of the previous corollary we could compute the error locator polynomial from the ideal $\langle G_{t-\tau}(\xi_{t-\tau-1})\rangle$ since this ideal is generated by z times the error locator polynomial.
This is true because in this case the variety are those points projecting points from $\mathcal{E}$. The points in $\mathcal{V}(F) \setminus \mathcal{E}$ whose coordinates in $\mathbf{x}$ corresponds to a syndrome $\mathbf{s}$ are the points of $\mathcal{V}_{\mathbf{s}}$ with two or more zero coordinates in $\mathbf{z}$ where substituted by the same element in $\mathbb{F}_q$. But for the $t-\tau$-th elimination ideal there is only one free variable in $\mathbf{z}$ thus the previous situation is impossible.
In the same fashion we can obtain that the generator of the ideal $\langle G_k(\xi_{k-1})\rangle$ is $z^{n+1}-z$ for all $k<t-\tau$.

L-Y method for decoding

1. Compute the elimination ideals

$$G_k, \quad k = 1, \ldots, t.$$

(One Gröbner basis computation).

L-Y method for decoding

1. Compute the elimination ideals

$$G_k, \quad k = 1, \ldots, t.$$

   (One Gröbner basis computation).

2. Evaluate the generators of G_k in $\mathbf{x} = \mathbf{s}$ and check if the independent terms are zero or not.

L-Y method for decoding

1. Compute the elimination ideals

$$G_k, \quad k = 1, \ldots, t.$$

   (One Gröbner basis computation).
2. Evaluate the generators of G_k in $\mathbf{x} = \mathbf{s}$ and check if the independent terms are zero or not.
3. Once we have find the first non zero compute the error locator polynomial and factorize it.

Note that in the previous discussion we assume that we know the true minimum distance of the cyclic code. This is not a trivial problem in the general case, in some of the papers of de M. Sala it is shown how to compute it from the syndrome variety. The general case for an arbitrary linear code can be found in Borges-Borges-Martínez.

Example [Yor94]

Consider the BCH binary code with parameters $[15, 5, 7]$ with syndrome ideal generated by

$$\begin{aligned} F &= \{z_1 + z_2 + z_3 + x_1,\ z_1^3 + z_2^3 + z_3^3 + x_2,\ z_1^5 + z_2^5 + z_3^5 + x_3, \\ &\quad z_1^{16} - z_1,\ z_2^{16} - z_2,\ z_3^{16} - z_3\} \end{aligned}$$

where the variables in $\mathbf{y}$ are not included since we are in the binary case. If we compute a Gröbner w.r.t. the lexicographical ordering $x_1 \prec x_2 \prec x_3 \prec z_1 \prec z_2 \prec z_3$ we have the following (the polynomials involving only variables in $\mathbf{x}$ are ommited since they are 0 when evaluated at a syndrome).

Example [Yor94] (Cont. I)

$$\begin{aligned}
G_1 &= \left\{z_1^{16} - z_1,\ z_1^3x_2 + z_1^3x_1^3 + z_1^2x_1x_2 + z_1^2x_1^4 + z_1x_3 + z_1x_1^2x_2 + \right.\\
&\quad x_1x_3 + x_2^2 + x_1^3x_2 + x_1^6,\ z_1^3x_3 + z_1^3x_1^5 + z_1^2x_1x_3 + z_1^2x_1^6 + \\
&\quad z_1x_2^9x_3^2 + z_1x_1^3x_2^8x_3^2 + z_1x_2^4x_3^2 + z_1x_1^9x_2x_3^2 + z_1x_1^2x_3 + z_1x_1^{10}x_2^9 + \\
&\quad z_1x_1^{13}x_2^8 + z_1x_1^{10}x_2^4 + z_1x_1^4x_2 + z_1x_1^7 + x_1x_2^9x_3^2 + x_1^4x_2^8x_3^2 + \\
&\quad \left. x_1x_2^4x_3^2 + x_1^{10}x_2x_3^2 + x_2x_3 + x_1^{11}x_2^9 + x_1^{14}x_2^8 + x_1^{11}x_2^4\right\} \\
G_2 &= G_1 \cup \left\{z_2^{16} - z_2,\ z_1z_2^2 + z_2^2x_1 + z_1^2z_2 + z_2x_1^2 + z_1^2x_1 + z_1x_1^2 + \right.\\
&\quad x_2 + x_1^3,\ z_2^2x_2 + z_2^2x_1^3 + z_1z_2x_2 + z_1z_2x_1^3 + z_2x_1x_2 + z_2x_1^4 + \\
&\quad z_1^2x_2 + z_1^2x_1^3 + z_1x_1x_2 + z_1x_1^4 + x_3 + x_1^2x_2,\ z_2^2x_3 + z_2^2x_1^5 + \\
&\quad z_1z_2x_3 + z_1z_2x_1^5 + z_2x_1x_3 + z_2x_1^6 + z_1^2x_3 + z_1^2x_1^5 + z_1x_1x_3 + \\
&\quad z_1x_1^6 + x_2^9x_3^2 + x_1^3x_2^8x_3^2 + x_2^4x_3^2 + x_1^9x_2x_3^2 + x_1^2x_3 + x_1^{10}x_2^9 + \\
&\quad \left. x_1^{13}x_2^8 + x_1^{10}x_2^4 + x_1^4x_2 + x_1^7\right\} \\
G_3 &= G_2 \cup \left\{z_3 + z_2 + z_1 + x_1\right\}.
\end{aligned}$$

Example [Yor94] (Cont. II)

Let α be a primitive element in $\mathbb{F}_{16}$ such that $\alpha^4 + \alpha + 1 = 0$. Suppose we have sent the word $\mathbf{0}$.

Example [Yor94] (Cont. II)

Let α be a primitive element in $\mathbb{F}_{16}$ such that $\alpha^4 + \alpha + 1 = 0$. Suppose we have sent the word $\mathbf{0}$.

Suppose that an error has been made in position 2, the syndrome for that error is $\mathbf{s} = (\alpha, \alpha^3, \alpha^5)$, and evaluating

$$\begin{array}{rcl} G_1(\xi_0) & = & \{z^{16} + z\}, \\ G_2(\xi_1) & = & \{z^{16} + z,\ \alpha^2 z + \alpha z\}, \\ G_3(\xi_2) & = & \{z + \alpha\}. \end{array}$$

Thus the varieties generated by $G_1(\xi_0)$ and $G_2(\xi_1)$ has 0 among their points and $G_3(\xi_2)$ gives us the error locator polynomial $z + \alpha$. Moreover, $G_2(\xi_1)$ is generated by $z(z + \alpha)$ and $G_1(\xi_0)$ by $z^{15+1} + z$.

Example [Yor94] (Cont. III)

Suppose now two errors in positions 2 and 4. Now the syndrome is $\mathbf{s} = (\alpha^9, \alpha, \alpha^{10})$ and

$$\begin{array}{rcl} G_1(\xi_0) & = & \{z^{16}+z,\, \alpha^{13}z^3+\alpha^7z^2+\alpha^2z,\, \alpha^5z^3+\alpha^{14}z^2+\alpha^9z\}, \\ G_2(\xi_1) & = & \{z^{16}+z,\, \alpha^9z^2+\alpha^3z+\alpha^{13}, \\ & & \alpha^{13}z^2+\alpha^7z+\alpha^2,\, \alpha^5z^2+\alpha^{14}z+\alpha^9\}. \end{array}$$

The variety generated by $G_1(\xi_0)$ contains the point 0 and those elements not $z^{16}+z$ in $G_2(\xi_1)$ factorize as

$$\begin{array}{rcl} \alpha^9z^2+\alpha^3z+\alpha^{13} & = & \alpha^9(z+\alpha)(z+\alpha^3) \\ \alpha^{13}z^2+\alpha^7z+\alpha^2 & = & \alpha^{13}(z+\alpha)(z+\alpha^3) \\ \alpha^5z^2+\alpha^{14}z+\alpha^9 & = & \alpha^5(z+\alpha)(z+\alpha^3) \end{array}$$

i.e. the error locator polynomial is $(z+\alpha)(z+\alpha^3)$.

Example [Yor94] (Cont. IV)

Finally suppose three errors in positions 2,4 and 7. The corresponding syndrome is $\mathbf{s} = (\alpha + \alpha^2, \alpha + \alpha^3, \alpha^5)$ and

$$G_1(\xi_0) = \{z^{16} + z,\ \alpha^7 z^3 + \alpha^{12} z^2 + \alpha^8 z + \alpha^2,\ z^3 + \alpha^5 z^2 + \alpha z + \alpha^{10}\}$$

The elements not $z^{16} + z$ factorize as

$$\begin{aligned} \alpha^7 z^3 + \alpha^{12} z^2 + \alpha^8 z + \alpha^2 &= \alpha^7 (z^3 + \alpha^5 z^2 + \alpha z + \alpha^{10}) \\ &= \alpha^7 (z + \alpha)(z + \alpha^3)(z + \alpha^6). \end{aligned}$$

and the error locator polynomial is

$$(z + \alpha)(z + \alpha^3)(z + \alpha^6).$$

FGLM

Complexity of computing GB with Buchberger algorithm is double exponential with is a serious obstruction to the previous setting.

FGLM

Complexity of computing GB with Buchberger algorithm is double exponential with is a serious obstruction to the previous setting. We will show briefly how FGLM techniques (from J.C. Faugère, P. Gianni, D. Lazard, T. Mora [FGLM93]) for 0-dim ideals can help in this case. This techniques make use of the linear structure in the 0-dim case for computing a GB wrt a certain monomial ordering once we know the GB wrt another ordering.

FGLM

Our setting

$$\begin{aligned} f_j &= y_1 z_1^{i_j} + y_2 z_2^{i_j} + \cdots + y_t z_t^{i_j} - x_j, \quad j = 1, \ldots, r. \\ h_k &= z_k^{n+1} - z_k, \quad k = 1, \ldots, t. \\ l_k &= y_k^{q-1} - 1, \quad k = 1, \ldots, t. \end{aligned}$$

$$F = \{f_j \mid j = 1, \ldots, r\} \cup \{h_k \mid k = 1, \ldots, t\} \cup \{l_k \mid k = 1, \ldots, t\}$$

FGLM

Our setting

$$\begin{aligned} f_j &= y_1 z_1^{i_j} + y_2 z_2^{i_j} + \cdots + y_t z_t^{i_j} - x_j, \quad j = 1, \ldots, r. \\ h_k &= z_k^{n+1} - z_k, \quad k = 1, \ldots, t. \\ l_k &= y_k^{q-1} - 1, \quad k = 1, \ldots, t. \end{aligned}$$

$$F = \{f_j \mid j = 1, \ldots, r\} \cup \{h_k \mid k = 1, \ldots, t\} \cup \{l_k \mid k = 1, \ldots, t\}$$

Lema

F is a GB for $I \subset \mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]$ w.r.t. the lex. ordering with

$$y_1 \prec_1 \ldots \prec_1 y_t \prec_1 z_1 \ldots \prec_1 z_t \prec_1 x_1 \ldots \prec_1 x_r.$$

FGLM

Aim :

For decoding as Loustaunau-York we must compute the GB w.r.t. the lex ordering given by

$$x_1 \prec_2 \cdots \prec_2 x_r \prec_2 z_1 \prec_2 \cdots \prec_2 z_t \prec_2 y_1 \prec_2 \cdots \prec_2 y_t .$$

FGLM

Since F is a GB then the map

$$\begin{array}{rcl} r : \mathbb{F}_q[\mathbf{x},\mathbf{z},\mathbf{y}] & \longrightarrow & \mathbb{F}_q[\mathbf{x},\mathbf{z},\mathbf{y}]/I \\ f & \longmapsto & \overline{f}^F_{\prec_1} + I, \end{array}$$

is a vector space homomorphims and a basis of the vector space are the monomials

$$\prod_{i=0}^{t} y^{a_i} z^{b_i}, \quad 0 \leq a_i \leq q-2,\, 0 \leq b_i \leq n,$$

and the dimension of $\mathbb{F}_q[\mathbf{x},\mathbf{z},\mathbf{y}]/I$ as $\mathbb{F}_q$-vector space is $(n+1)^t(q-1)^t$.

FGLM

Order the monomials in $\mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]$ w.r.t. $\prec_2$, any monomial $\mathbf{x}^{\mathbf{a}}\mathbf{z}^{\mathbf{b}}\mathbf{y}^{\mathbf{c}}$ is either reduced w.r.t. F, or a multiple of a leader term in F.

FGLM

Order the monomials in $\mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]$ w.r.t. $\prec_2$, any monomial $\mathbf{x}^{\mathbf{a}}\mathbf{z}^{\mathbf{b}}\mathbf{y}^{\mathbf{c}}$ is either reduced w.r.t. F, or a multiple of a leader term in F.
I.e. any polynomial $f = \sum_{i=0}^{\nu} \sigma_i \mathbf{x}^{\mathbf{a}_i}\mathbf{z}^{\mathbf{b}_i}\mathbf{y}^{\mathbf{c}_i}$ with leader term $\mathbf{x}^{\mathbf{a}_\nu}\mathbf{z}^{\mathbf{b}_\nu}\mathbf{y}^{\mathbf{c}_\nu}$ w.r.t. $\prec_2$ and $(\sigma_0, \ldots, \sigma_\nu) \in \mathbb{F}_q^{\nu}$ is in the ideal I iff

$$r(\sum_{i=0}^{\nu} \sigma_i \mathbf{x}^{\mathbf{a}_i}\mathbf{z}^{\mathbf{b}_i}\mathbf{y}^{\mathbf{c}_i}) = \sum_{i=0}^{\nu} \sigma_i r(\mathbf{x}^{\mathbf{a}_i}\mathbf{z}^{\mathbf{b}_i}\mathbf{y}^{\mathbf{c}_i}) = 0. \qquad (12)$$

FGLM

The problem of finding leader terms w.r.t. $\prec_2$ reduces to compute an element σ in the kernel of a matrix $(\nu+1) \times (n+1)^t(q-1)^t$, moreover, since the system is 0-dim there are only a finite number of linear systems to solve. Also if we include a leader term we do not need to include its multiples (border).

FGLM: Loustaunau-York

Input: F GB w.r.t. $\prec_1$ and $\prec_2$.

Output: G reduced GB of $\langle F\rangle$ w.r.t $\prec_2$.

FGLM: Loustaunau-York

```
$\mathrm{LPP} \leftarrow [],\ G \leftarrow [],\ \mathrm{Mbasis} \leftarrow []$
$\mathrm{PowerProducts} \leftarrow [],\ \mathbf{x}_{(i)} \leftarrow 1$
while $\mathbf{x}_{(i)} \neq \mathrm{null}$ do
    if $\mathbf{x}_{(i)}$ not divisible by an element in $\mathrm{LPP}$ then
        $r(\mathbf{x}_{(i)}) \leftarrow \overline{\mathbf{x}_{(i)}}^{F}_{\prec_1}$,
        if there is a linear relation $r(\mathbf{x}_{(i)}) = \sum_{r(\mathbf{x}_{(j)}) \in \mathrm{Mbasis}} \sigma_j r(\mathbf{x}_{(j)})$ then
            $g_i \leftarrow \mathbf{x}_{(i)} - \sum_{r(\mathbf{x}_{(j)}) \in \mathrm{Mbasis}} \sigma_j r(\mathbf{x}_{(j)})$,
            $G \leftarrow [g_i, G]$,
            $\mathrm{LPP} \leftarrow [\mathbf{x}_{(i)}, \mathrm{LPP}]$
        else
            $\mathrm{Mbasis} \leftarrow [[\mathbf{x}_{(i)}, r(\mathbf{x}_{(i)})], \mathrm{Mbasis}]$,
            $\mathrm{InsertNext}(\mathbf{x}_{(i)})$.
        end if
        $\mathbf{x}_{(i)} \leftarrow \mathrm{NextMonom}$.
    end if
end while
```

FGLM: Loustaunau-York

Variables locales

- $\mathrm{PowerProducts}$: List of terms ordered w.r.t. $\prec_2$.
- LPP: Leader terms of G.
- Mbasis: List of pairs $[\mathbf{x}_{(i)}, r(\mathbf{x}_{(i)})]$ where $\mathbf{x}_{(i)}$ is an element of the basis of $\mathbb{F}_q[\mathbf{x}, \mathbf{z}, \mathbf{y}]/\langle G\rangle$

FGLM: Loustaunau-York

Procedures

- $\mathrm{NextMonom}$: Erases the 1st element in list $\mathrm{PowerProducts}$ and returns "null" if it is empty.
- $\mathrm{InsertNext}(\mathbf{x}_{(i)})$: Adds to the list $\mathrm{PowerProducts}$ the products $x_1\mathbf{x}_{(i)}, \ldots, x_r\mathbf{x}_{(i)}$, $z_1\mathbf{x}_{(i)}, \ldots, z_t\mathbf{x}_{(i)}$, $y_1\mathbf{x}_{(i)}, \ldots, y_t\mathbf{x}_{(i)}$ and order the list w.r.t. $\prec_2$.

FGLM: Loustaunau-York

Procedures

- $\mathrm{NextMonom}$: Erases the 1st element in list $\mathrm{PowerProducts}$ and returns “null” if it is empty.
- $\mathrm{InsertNext}(\mathbf{x}_{(i)})$: Adds to the list $\mathrm{PowerProducts}$ the products $x_1\mathbf{x}_{(i)}, \ldots, x_r\mathbf{x}_{(i)}$, $z_1\mathbf{x}_{(i)}, \ldots, z_t\mathbf{x}_{(i)}$, $y_1\mathbf{x}_{(i)}, \ldots, y_t\mathbf{x}_{(i)}$ and order the list w.r.t. $\prec_2$.

For our pourpose we do not need the complete GB sxince we are only interested in G_k, i.e., we can modify $\mathrm{InsertNext}$ so that the list will not include those monomials with a variable y_i.

Affine variety codes

J. Fitzgerald y R.F. Lax in [FL98] proppoSed the following evaluation codes. Let $I \subseteq \mathbb{F}_q[x_1, \ldots, x_s]$ be an ideal and consider the ideal

$$I_q = I + \left\langle x_1^q - x_1, \ldots, x_s^q - x_s \right\rangle . \qquad (13)$$

I.e., the variety $\mathcal{V}(I_q)$ are the $\mathbb{F}_q$-rational points in $\mathcal{V}(I)$ and I_q is a zero dim. ideal and radical.

$$\mathcal{V}(I_q) = \{P_1, P_2, \ldots, P_n\}, \qquad (14)$$

Affine variety codes

The evaluation is as follows

$$\begin{array}{rcl} ev : \mathbb{F}_q[x_1, \ldots, x_s]/I_q & \longrightarrow & \mathbb{F}_q^n \\ f + I_q & \longmapsto & (f(P_1), f(P_2), \ldots, f(P_n)) \end{array} \tag{15}$$

and it is an isomorphism (as $\mathbb{F}_q$-vector spaces).

Affine variety codes

The evaluation is as follows

$$\begin{array}{rcl} ev : \mathbb{F}_q[x_1, \ldots, x_s]/I_q & \longrightarrow & \mathbb{F}_q^n \\ f + I_q & \longmapsto & (f(P_1), f(P_2), \ldots, f(P_n)) \end{array} \tag{15}$$

and it is an isomorphism (as $\mathbb{F}_q$-vector spaces).

Definition.

Let L be a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q[x_1, \ldots, x_s]/I$. The affine variety code $C(I_q, L)$ is the image of L in the evaluation ev.

Affine variety codes

Example.
Sea $I = \left\langle x^{q-1} - 1 \right\rangle \subset \mathbb{F}_q[x]$, (i.e. $I_q = I$), and

$$L = \mathrm{span}_{\mathbb{F}_q}\{1 + I, x + I, x^2 + I, \ldots, x^k + I\} \subseteq \mathbb{F}_q[x]/I.$$

$C(I, L)$ is the Reed-Solomoncode of dimension k over $\mathbb{F}_q$.

Affine variety codes

Theorem

Every linear code $\mathcal{C}$ over $\mathbb{F}_q$ can be represented as an affine variety code.

Affine variety codes

Theorem

Every linear code $\mathcal{C}$ over $\mathbb{F}_q$ can be represented as an affine variety code.

Proof.

Let $\mathcal{C}$ be an [n,k,d] linear code over $\mathbb{F}_q$ with a generator matrix $G = (g_{ij})$ where $g_{ij} \in \mathbb{F}_q$, $1 \leq i \leq k$, $1 \leq j \leq n$. Choose an integer s such that $q^s \geq n$. Take n distinct points $P_1, \cdots, P_n$ where $P_j = (p_{j1}, p_{j2}, \ldots, p_{js})$. Consider the ideal $I = \mathcal{I}(\mathbf{P}) \subset \mathbb{F}_q[x_1, \ldots, x_s]$. The polynomials

$$\chi_j(x_1, \ldots, x_s) = \prod_{l=1}^{s} \left(1 - (x_l - p_{jl})^{q-1}\right), \quad j = 1, \ldots, n \qquad (16)$$

□

Affine variety codes

Proof (Cont.)

have the following property

$$\chi_j(P) = \begin{cases} 0 \text{ si } P \in \mathbb{F}_q^s \setminus \{P_j\} \\ 1 \text{ si } P = P_j \end{cases} .$$

Let $\chi_j + I_q \in F_q[x_1, \ldots, x_s]/I_q$ be the equivalence classes for $j = 1, \ldots, n$ and

$$f_i + I_q = \left[\sum_{j=1}^{n} g_{ij} \left(\chi_j + I_q \right) \right] \in F_q[x_1, \ldots, x_s]/I_q, \quad i = 1, \ldots, k.$$

Take L as $L = \mathrm{span}_{\mathbb{F}_q} \{f_i + I_q\}_{i=1}^{k}$ and it follows that $\mathcal{C} = C(I_q, L)$. □

Decoding AVC

$\mathcal{C} = C(I_q, L)^{\perp}$

$$\begin{array}{rcl} I & = & \langle g_1, g_2, \ldots, g_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_s] \\ L & = & \mathrm{span}_{\mathbb{F}_q} \left\{ f_1 + I_q, \ldots, f_r + I_q \right\}, \; f_i \in \mathbb{F}_q[x_1, \ldots, x_s], \; i = 1, \ldots, r \\ \mathcal{V}(I_q) & = & \{P_1, P_2, \ldots, P_n\} \subset \mathbb{F}_q^s. \end{array}$$

Decoding AVC

$\mathcal{C} = C(I_q, L)^\perp$

$$\begin{aligned} I &= \langle g_1, g_2, \dots, g_m \rangle \subset \mathbb{F}_q[x_1, \dots, x_s] \\ L &= \mathrm{span}_{\mathbb{F}_q} \{ f_1 + I_q, \dots, f_r + I_q \},\ f_i \in \mathbb{F}_q[x_1, \dots, x_s],\ i = 1, \dots, r \\ \mathcal{V}(I_q) &= \{P_1, P_2, \dots, P_n\} \subset \mathbb{F}_q^s. \end{aligned}$$

Suppose we have received the word $\mathbf{y} = (y_1, \dots, y_n)$, the corresponding syndrome $\mathbf{s}$ is

$$s_i = \sum_{j=1}^{n} y_i f_i(P_j), \quad i = 1, \dots, r. \tag{17}$$

Decoding AVC

If $\mathbf{y} = \mathbf{e} + \mathbf{c}$ where $\mathbf{c} \in \mathcal{C}$ and $w(\mathbf{e}) = t$ then

$$s_i = \sum_{j=1}^{n} e_i f_i(P_j), \quad i = 1, \ldots, r. \tag{18}$$

Decoding AVC

If $\mathbf{y} = \mathbf{e} + \mathbf{c}$ where $\mathbf{c} \in \mathcal{C}$ and $w(\mathbf{e}) = t$ then

$$s_i = \sum_{j=1}^{n} e_i f_i(P_j), \quad i = 1, \ldots, r. \tag{18}$$

Consider the polynomial ring (Note that $e_1, \ldots, e_t$ are now variables)

$$T = \mathbb{F}_q[x_{11}, \ldots, x_{1s}, \ldots, x_{t1}, \ldots, x_{ts}, e_1, \ldots, e_t] \tag{19}$$

and the following polynomials in the ring T

$$h_i = \sum_{j=1}^{t} e_j f_i(x_{j1}, \ldots, x_{js}) - s_i, \quad i = 1, \ldots, r \tag{20}$$

Decoding AVC

We will define the ideal

$$E_{\mathbf{y}} = \left(\left\langle g_l(x_{j1}, \ldots, x_{js}), h_i, e_j^{q-1} - 1 \right\rangle \right)_q \tag{21}$$

where $i = 1, \ldots, r$, $j = 1, \ldots, t$ and $l = 1, \ldots, m$. Note that despite the notation $E_{\mathbf{y}}$ the ideal is the same for all the words with same syndrome (i.e. in the same coset).

Decoding AVC

Theorem.

If there are exactly t errors (t as usual the error correcting capability) in the position corresponding to P_{i_j} and the error values are e_{i_j} $j = 1, \ldots, t$ then there are $t!$ points in the variety $\mathcal{V}(E_{\mathbf{y}})$ corresponding to

$$\left\{ \left(P_{i_{\sigma(1)}}, \ldots, P_{i_{\sigma(t)}}, e_{i_{\sigma(1)}}, \ldots, e_{i_{\sigma(t)}} \right) \right\}_{\sigma \in \mathcal{S}_t} \tag{22}$$

where $\mathcal{S}_t$ is the symmetric group acting on t elements.

Decoding AVC

Theorem.

If there are exactly t errors (t as usual the error correcting capability) in the position corresponding to P_{i_j} and the error values are e_{i_j} $j = 1, \dots, t$ then there are $t!$ points in the variety $\mathcal{V}(E_{\mathbf{y}})$ corresponding to

$$\left\{ \left(P_{i_{\sigma(1)}}, \dots, P_{i_{\sigma(t)}}, e_{i_{\sigma(1)}}, \dots, e_{i_{\sigma(t)}} \right) \right\}_{\sigma \in \mathcal{S}_t} \tag{22}$$

where $\mathcal{S}_t$ is the symmetric group acting on t elements.

Proof.

From the symmetry of the polynomials in $E_{\mathbf{y}}$ it is clear that the points in (22) are in $\mathcal{V}(E_{\mathbf{y}})$. Suppose that we have an extra point in the variety not in (22), this will be a contradiction with the fact that we have an unique error vector $\mathbf{e}$ of weight t. □

Decoding AVC

Consider the term ordering $\prec_1$ extending the lex. ordering with

$$x_{11} \prec_1 x_{12} \prec_1 \dots \prec_1 x_{1s} \prec_1 e_1$$

in the variables $x_{11}, x_{12}, \dots, x_{1s}, e_1$ and let $\prec_2$ any other term ordering in the rest of the variables. Given two monomials in T we have that¡ they are "like" $M_1 N_1$ and $M_2 N_2$, where M_1, M_2 involve only variables $x_{11}, x_{12}, \dots, x_{1s}, e_1$ and N_1, N_2 in the remaining variables. We define the following elimination ordering $\prec$ (for the variables $x_{11}, x_{12}, \dots, x_{1s}, e_1$) as follows

$$M_1 N_1 \prec M_2 N_2 \Longleftrightarrow \begin{cases} M_1 \prec_1 M_2 \\ \text{If } M_1 = M_2 \text{ then } N_1 \prec_2 N_2. \end{cases} \qquad (23)$$

Decoding AVC

Theorem.

Let G be a Gröbner basis for the ideal $E_{\mathbf{y}}$ w.r.t. the previous monomial ordering (23). We can compute the error positions and error values applying elimination to the ideal $E_{\mathbf{y}}$ over the variables $x_{11}, x_{12}, \ldots, x_{1s}, e_1$.

Decoding AVC

Theorem.

Let G be a Gröbner basis for the ideal $E_{\mathbf{y}}$ w.r.t. the previous monomial ordering (23). We can compute the error positions and error values applying elimination to the ideal $E_{\mathbf{y}}$ over the variables $x_{11}, x_{12}, \ldots, x_{1s}, e_1$.

Proof.

Consider the elimination ideals

$$\begin{aligned} J &= E_{\mathbf{y}} \cap \mathbb{F}_q[x_{11}, x_{12}, \ldots, x_{1s}, e_1] \\ J_i &= E_{\mathbf{y}} \cap \mathbb{F}_q[x_{11}, x_{12}, \ldots, x_{1i}],\ i = 1, \ldots, s. \end{aligned}$$

The set $G \cap \mathbb{F}_q[x_{11}, x_{12}, \ldots, x_{1s}, e_1]$ is a Gröbner basis of J w.r.t. the ordering $\prec_1$ thus $G \cap \mathbb{F}_q[x_{11}, x_{12}, \ldots, x_{1i}]$ is a GB for J_i wrt $\prec_1$ for all $i = 1, \ldots, s$. □

Decoding AVC

Proof. (Cont.)

Consider $\{g_1(x_{11})\} = G \cap \mathbb{F}_q[x_{11}]$ the generator of the (principal) ideal J_1. The roots of the polynomial g_1 are the first coordinate of the points in $\mathcal{V}(E_{\mathbf{y}})$. Substituting each of them in $G \cap \mathbb{F}_q[x_{11}, x_{12}]$ we get poly's in the variable x_{12} thus we can solve up to the variables s $x_{11}, x_{12}, \ldots, x_{1s}, e_1$ for each point in $\mathcal{V}(E_{\mathbf{y}})$. □

Example

Consider the ideal $I = \langle y^2 + y - x^3 \rangle \subset \mathbb{F}_4[x, y]$ and $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ where $\alpha^2 = \alpha + 1$. The points in $\mathcal{V}(I)$ are

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

Consider the vector space

$$L = \mathrm{span}_{\mathbb{F}_4} \left\{ 1 + I_4, x + I_4, y + I_4, x^2 + I_4, xy + I_4 \right\}.$$

Example ...

A parity check matrix for the code $\mathcal{C} = (L, I_4)^{\perp}$ is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \end{pmatrix}$$

and the code has minimal distance 5 (haha!!!! tricky).
Suppose we have recieved $\mathbf{y} = (0, 0, 1, 0, 0, \alpha, 0, 0)$, its syndrome is $\mathbf{s} = (\alpha^2, \alpha, \alpha^2, 0, 0)$.

Example ...

$E_{\mathbf{y}}$ in $\mathbb{F}_4[x_1, y_1, x_2, y_2, e_1, e_2]$ is generated by

$$
\begin{aligned}
& x_1^4 - x_1, y_1^4 - y_1, e_1^3 - 1, x_2^4 - x_2, y_2^4 - y_2, e_2^3 - 1, \\
& y_1^2 + y_1 - x_1^3, y_2^2 + y_2 - x_2^3, \\
& e_1 + e_2 - \alpha^2, e_1 x_1 + e_2 x_2 - \alpha, e_1 y_1 + e_2 y_2 - \alpha^2, e_1 x_1^2 + e_2 x_2^2, \\
& e_1 x_1 y_1 + e_2 x_2 y_2.
\end{aligned}
$$

A GB for $E_{\mathbf{y}}$ for the lex ordering extending $x_1 \prec y_1 \prec e_1 \prec x_2 \prec y_2 \prec e_2$ is

$$
\begin{aligned}
G \quad = \quad & \{x_1^2 + \alpha^2 x_1 + \alpha, y_1 + \alpha x_1, e_1 + x_1, x_2 + x_1 + \alpha^2, \\
& y_2 + \alpha x_1 + 1, e_2 + x_1 + \alpha^2\}.
\end{aligned}
$$

Example ...

The error locator roots (1st coordinate of the point locators) are the roots of the polynomial $x_1^2 + \alpha^2 x_1 + \alpha$, i.e. 1 and α. Plug them in $y_1 + \alpha x_1$ and we get the second coordinate α and α^2 respectively, i.e. the points are P_3 and P_6. Finally, equation $e_1 + x_1$ we get that the error value is the first coordinate of the points.

Precomputing the error locators

The previous algorithm is far away from being practical since we need to compute a GB for each different syndrome.

Precomputing the error locators

The previous algorithm is far away from being practical since we need to compute a GB for each different syndrome. J. Fitzgerald y R.F. Lax en [FL98] proppoised to add new variables $s_1, \ldots, s_r$ to the ring corresponding to the syndromes. Now computing the GB is more complex but we do it only once.

Precomputing the error locators

$$\mathcal{T} = T[s_1, \dots, s_r] \tag{24}$$

Consider the polynomials in $\mathcal{T}$

$$h_i = \sum_{j=1}^{t} e_j f_i(x_{j1}, \dots, x_{js}) - s_i, \quad i = 1, \dots, r \tag{25}$$

remember that now s_i $i = 1, \dots, r$ are variables.

Precomputing the error locators

$$\mathcal{T} = T[s_1, \ldots, s_r] \tag{24}$$

Consider the polynomials in $\mathcal{T}$

$$h_i = \sum_{j=1}^{t} e_j f_i(x_{j1}, \ldots, x_{js}) - s_i, \quad i = 1, \ldots, r \tag{25}$$

remember that now s_i $i = 1, \ldots, r$ are variables.Let

$$\mathcal{E} = \left(\left\langle g_l(x_{j1}, \ldots, x_{js}), h_i, e_j^{q-1} - 1 \right\rangle \right)_q \subset \mathcal{T} \tag{26}$$

with $i = 1, \ldots, r$, $j = 1, \ldots, t$ and $l = 1, \ldots, m$.

Precomputing the error locators

Let $\prec_s$ a (any) term ordering for the variables $s_1, \ldots, s_r$ and $\prec$ the term ordering defined in T before (23). Given two terms in $\mathcal{T}$ they look like $M_1 N_1$ and $M_2 N_2$ where M_1, M_2 involve only those variables in $s_1, \ldots, s_r$ and N_1, N_2 are monomials in T. Define the following ordering on $\mathcal{T}$ $\prec'$ asx follows

$$M_1 N_1 \prec' M_2 N_2 \Longleftrightarrow \begin{cases} M_1 \prec_s M_2 \\ \text{If } M_1 = M_2 \text{ then } N_1 \prec N_2. \end{cases} \tag{27}$$

Precomputing the error locators

Teorema.

Let G be a GB of the ideal $\mathcal{E}$ w.r.t. the monomial ordering $\prec'$ defined in (27) and suppose there are t errors. We can compute the error positions and error values applying elimination to the ideal with the value of the syndrome in the variables $s_1, \dots, s_r$.

Example

Same code as previous example. The ideal $\mathcal{E}$ en $\mathbb{F}_4[s_1, s_2, s_3, s_4, s_5, x_1, y_1, x_2, y_2, e_1, e_2]$ is generated by

$$\begin{gathered} x_1^4 - x_1, y_1^4 - y_1, e_1^3 - 1, x_2^4 - x_2, y_2^4 - y_2, e_2^3 - 1, \\ y_1^2 + y_1 - x_1^3, y_2^2 + y_2 - x_2^3, \\ e_1 + e_2 - s_1, e_1x_1 + e_2x_2 - s_2, e_1y_1 + e_2y_2 - s_3, e_1x_1^2 + e_2x_2^2 - s_4, \\ e_1x_1y_1 + e_2x_2y_2 - s_5 \end{gathered}$$

A GB computed with Macaulay wrt $\prec'$ where $\prec_s$ and $\prec_2$ are the dgrevlex contains 119 polynomials.