$K := GF(q)$
C be an $[n, k, d]$ cyclic code over K, $\gcd(q, n) = 1$;
$g(X)$ the generator polynomial of C;

m the multiplicative order of $q \bmod n$;
$\mathbb{F}$ the splitting field of $X^n - 1$ over K;
α a primitive nth root of the unity;
$h(X)$ the generator polynomial of α;
t the correction capability of C;

$S_C := \{i : g(\alpha^i) = 0\} \subset \{i : 0 \leq i < n\}$ the *complete defining set* of C;

Then

- $\mathbb{F} = GF(q^m) = K[\alpha] = K[X]/h(X)$;
- $g(X) \mid X^n - 1$;
- $\deg(g) = n - k =: r$;
- $i \in S_C \implies iq^j \pmod n \in S_C$.
- $t = \lfloor (d-1)/2 \rfloor$.

A **defining set** of C is any set $S \subset S_C$:

$$S_C = \{iq^j \pmod n : i \in S, j \in \mathbb{N}\}$$

Let

$e(X) = \sum_{i=0}^{n-1} e_i X^i \in K[X]$ an error polynomial;
$J := \{j : e_j \neq 0, 0 \leq j < n\}$ the error positions;
$\mu := \#J$ the weight of the error (wlog $\mu \leq t$);
$\{\alpha^j : j \in J\} \subset \mathbb{F}$ the error locators;
$\mathsf{s}_i := e(\alpha^i) = \sum_{j \in J} e_j \alpha^{ij} \in \mathbb{F}, i \in S_C$, the syndromes;
$L_e := \prod_{j \in J}(1 - X\alpha^j)$ the error locator polynomial.

- A.B. III Cooper, Direct solution of BCH decoding equations, *Comm., Cont. and Sign. Proc., (1990) 281–286*
- *A.B. III Cooper, Finding BCH error locator polynomials in one step Electronic Letters,* **27** *(1991) 2090–2091*

Assume

$$q = 2, K = \mathbb{Z}_2, S = \{2i + 1, 0 \leq i < t\}$$

and set

$f_i := \sum_{j=1}^{t} X_j^{2i-1} - \mathsf{s}_{2i-1} \in \mathbb{F}[X_1, \ldots, X_t]$;

$\mathsf{I} := \mathbb{I}(f_1, \cdots, f_t) \subset \mathbb{F}[X_1, \ldots, X_t]$;

$\mathcal{Z}(\mathsf{I}) := \left\{\mathbf{a} = (a_1, \ldots, a_t) \in \mathbb{F}^t : f_i(\mathbf{a}) = 0\right\}$;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots X_n$;

$g \in \mathbb{F}[X_1]$ the unique polynomial : $G \cap \mathbb{F}[X_1] = \{g\}$;

$\mathsf{Z} := \{\xi : (\xi, a_2, \ldots, a_t) \in \mathcal{Z}(\mathsf{I})\}$.

$\mathsf{E} := \{\xi_1, \ldots, \xi_\mu\}$ the set of the error locators.

Then

- $\mathsf{E} = \mathsf{Z} = \{\xi : g(\xi) = 0\}$
- $\#\mathsf{E} = \mu = t = \deg(g)$;
- $g(X) = \prod_{\xi \in \mathsf{Z}}(X - \xi)$;
- $X^\mu g(X^{-1})$ is the error locator polynomial.

$S = \{1, 3\}$, $\mathcal{P} := K[\mathsf{s}_1, \mathsf{s}_3][X_1, X_2]$;
$\mathsf{I} := \mathbb{I}(X_1 + X_2 + \mathsf{s}_1, X_1^3 + X_2^3 + \mathsf{s}_3) \subset \mathcal{P}]$
$G = \{X_1^2\mathsf{s}_1 + X_1\mathsf{s}_1^2 + \mathsf{s}_1^3 + \mathsf{s}_3, X_2 + X_1 + \mathsf{s}_1\}$;
$g(X) = X^2\mathsf{s}_1 + X\mathsf{s}_1^2 + \mathsf{s}_1^3 + \mathsf{s}_3$;
id est (Berlekamp)

$$L_e(X) = 1 + X\mathsf{s}_1 + X^2\left(\frac{\mathsf{s}_1^3 + \mathsf{s}_3}{\mathsf{s}_1}\right).$$

$$\begin{aligned}
S &= \{1, -1\} \\
\mathsf{I} &:= \mathbb{I}(X_1 + X_2 + \mathsf{s}_1, Y_1 + Y_2 + \mathsf{s}_{-1}, \\
&\qquad X_1Y_1 + 1, X_2Y_2 + 1) \\
&\subset K[\mathsf{s}_1, \mathsf{s}_{-1}][Y_1, Y_2, X_1, X_2] \\
G &= \{ X_1^2\mathsf{s}_{-1} + X_1\mathsf{s}_1\mathsf{s}_{-1} + \mathsf{s}_1, \\
&\qquad Y_1\mathsf{s}_1 + X_1\mathsf{s}_{-1} + \mathsf{s}_1\mathsf{s}_{-1}, \\
&\qquad Y_1X_1 + 1, \\
&\qquad Y_2 + Y_1 + \mathsf{s}_{-1}, \\
&\qquad X_2 + X_1 + \mathsf{s}_1\} \\
g(X) &= X^2\mathsf{s}_{-1} + X\mathsf{s}_1\mathsf{s}_{-1} + \mathsf{s}_1
\end{aligned}$$

id est (Berlekamp)

$$L_e(X) = 1 + X\mathsf{s}_1 + X^2\left(\frac{\mathsf{s}_1}{\mathsf{s}_{-1}}\right).$$

There is in Cooper a designed ambiguity; the aritmetic is performed on the s_is in $K[\mathsf{s}_i, i \in J]$ but are interpreted as performed on α_i in $\mathbb{F}$.

$$
\begin{aligned}
S &= \{1,3,5\} \\
\mathsf{I} &:= \mathbb{I}(X_1+X_2+X_3+\mathsf{s}_1, \\
&\qquad X_1^3+X_2^3+X_3^3+\mathsf{s}_3, \\
&\qquad X_1^5+X_2^5+X_3^5+\mathsf{s}_5) \\
&\subset K[\mathsf{s}_1,\mathsf{s}_3,\mathsf{s}_5][X_1,X_2,X_3] \\
g(X) &= X^3(\mathsf{s}_1^3+\mathsf{s}_3)+X^2(\mathsf{s}_1^4+\mathsf{s}_1\mathsf{s}_3) \\
&+ X(\mathsf{s}_1^2\mathsf{s}_3+\mathsf{s}_5) \\
&+ \mathsf{s}_1^6+\mathsf{s}_1^3\mathsf{s}_3+\mathsf{s}_1\mathsf{s}_5+\mathsf{s}_3^2 \\
G &= \{ g(X_1), \\
&\quad X_2^2X_1+X_2^2\mathsf{s}_1+\cdots, \\
&\quad X_2^2(\mathsf{s}_1^3+\mathsf{s}_3)+\cdots, \\
&\quad X_3+X_2+X_1+\mathsf{s}_1\} \\
L_e(X) &= 1+X\mathsf{s}_1 \\
&+ X^2\left(\frac{\mathsf{s}_1^2\mathsf{s}_3+\mathsf{s}_5}{\mathsf{s}_1^3+\mathsf{s}_3}\right) \\
&+ X^3\left(\frac{\mathsf{s}_1^6+\mathsf{s}_1^3\mathsf{s}_3+\mathsf{s}_1\mathsf{s}_5+\mathsf{s}_3^2}{\mathsf{s}_1^3+\mathsf{s}_3}\right)
\end{aligned}
$$

$S = \{1, 3, 5\}$
$n = 15, m = 4, h(X) = X^4 + X + 1$
$\mathbb{F} = GF(16) = \mathbb{Z}_2[\alpha] = \mathbb{Z}_2[X]/h(X)$

$\beta_1 := \mathsf{s}_1^3 + \mathsf{s}_3$
$\beta_2 := \mathsf{s}_1^2\mathsf{s}_3 + \mathsf{s}_5$
$\beta_3 := \mathsf{s}_1^6 + \mathsf{s}_1^3\mathsf{s}_3 + \mathsf{s}_1\mathsf{s}_5 + \mathsf{s}_3^2 = \mathsf{s}_1\beta_2 + \beta_1^2$

$$L_e(X) = 1 + X\mathsf{s}_1 + X^2\beta_2\beta_1^{-1} + X^3\beta_3\beta_1^{-1}$$

- $e(X) = X^3$
  - $\mathsf{s}_1 = \alpha^3, \mathsf{s}_3 = \alpha^9, \mathsf{s}_5 = 1,$
  - $\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$
  - $L_e(X) = 1 + X\alpha^3.$
- $e(X) = X^3 + X^2$
  - $\mathsf{s}_1 = \alpha^6, \mathsf{s}_3 = \alpha^5, \mathsf{s}_5 = \alpha^5,$
  - $\beta_1 = \alpha^{11}, \beta_2 = \alpha, \beta_3 = 0$
  - $L_e(X) = 1 + X\alpha^6 + X^2\alpha^5$
  - $L_e(X) = (1 + X\alpha^2)(1 + X\alpha^3)$
- $e(X) = X^3 + X^2 + X$
  - $\mathsf{s}_1 = \alpha^{11}, \mathsf{s}_3 = \alpha^{11}, \mathsf{s}_5 = 0,$
  - $\beta_1 = \alpha^5, \beta_2 = \alpha^3, \beta_3 = \alpha^{11}$
  - $L_e(X) = 1 + X\alpha^{11} + X^2\alpha^{13} + X^3\alpha^6$
  - $L_e(X) = (1 + X\alpha)(1 + X\alpha^2)(1 + X\alpha^3)$

- X. Chen, I. S. Reed, T. Helleseth, K. Truong, Use of Gröbner Bases to Decode Binary Cyclic Codes up to the True Minimum Distance, *IEEE Trans. on Inf. Th.*, **40** (1994) , 1654–1661

Adapts Cooper's results by

1. discussing the structure of g in function of the relation between μ (the weight of the error) and t (the correction capabily);
2. fixing the arithmetics within $K[\mathsf{s}_i, i \in J]$ thus clarifying Cooper's ambiguity;
3. removing 'algebraic' solutions;

Let

$q = 2, K = \mathbb{Z}_2, S = \{2i + 1, 0 \leq i < t\}$;

$f_i := \sum_{j=1}^{t} Z_j^{2i-1} - \mathsf{s}_{2i-1} \in \mathbb{F}[Z_1, \ldots, Z_t]$;

$h_i := Z_i^{n+1} - Z_i \in \mathbb{F}[Z_1, \ldots, Z_t]$ (error locators are nth roots of unity);

$\mathsf{I} := \mathbb{I}(f_1, \cdots, f_t, h_1, \ldots, h_t) \subset K[Z_1, \ldots, Z_t]$;

$\mathcal{Z}(\mathsf{I}) := \left\{\mathbf{a} = (a_1, \ldots, a_t) \in \mathbb{F}^t : f_i(\mathbf{a}) = 0\right\}$;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $Z_1 < \cdots Z_n$;

$g \in \mathbb{F}[X_1]$ the unique polynomial : $G \cap \mathbb{F}[Z_1] = \{g\}$;

$\mathsf{Z} := \{\xi : (\xi, a_2, \ldots, a_t) \in \mathcal{Z}(\mathsf{I})\}$.

$\mathsf{E} := \{\xi_1, \ldots, \xi_\mu\}$ the set of the error locators.

Then

- $\mathsf{E} \subseteq \mathsf{Z} = \{\xi : g(\xi) = 0\}$
- $g(X) = \prod_{\xi \in \mathsf{Z}}(X - \xi)$;
- $\#\mathsf{E} = \mu \leq t = \deg(g)$.

Let

$q = 2, K = \mathbb{Z}_2, S = \{2i + 1, 0 \leq i < t\}$;

$f_i := \sum_{j=1}^{t} Z_j^{2i-1} - \mathsf{s}_{2i-1} \in \mathbb{F}[Z_1, \ldots, Z_t]$;

$h_i := Z_i^{n+1} - Z_i \in \mathbb{F}[Z_1, \ldots, Z_t]$;

$\mathsf{I} := \mathbb{I}(f_1, \cdots, f_t, h_1, \ldots, h_t) \subset K[Z_1, \ldots, Z_t]$;

$\mathcal{Z}(\mathsf{I}) := \left\{\mathbf{a} = (a_1, \ldots, a_t) \in \mathbb{F}^t : f_i(\mathbf{a}) = 0\right\}$;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $Z_1 < \cdots Z_n$;

$g \in \mathbb{F}[X_1]$ the unique polynomial : $G \cap \mathbb{F}[Z_1] = \{g\}$;

$\mathsf{Z} := \{\xi : (\xi, a_2, \ldots, a_t) \in \mathcal{Z}(\mathsf{I})\}$.

$\mathsf{E} := \{\xi_1, \ldots, \xi_\mu\}$ the set of the error locators.

Then

- $\mu = t \implies$
  - $\mathcal{Z}(\mathsf{I})$ consits of all coordinate permutations of the root $(\xi_1, \ldots, \xi_t)$.
  - $\mathsf{E} = \mathsf{Z}$,
  - $L_e(X) = X^\mu g(X^{-1})$
- $\mu = t - 1 \implies$
  - $(0, \xi_1, \ldots, \xi_\mu) \in \mathcal{Z}(\mathsf{I})$,
  - $\mathsf{E} = \mathsf{Z} \cup \{0\}$,
  - $g(X) = X \cdot \left(X^\mu L_e(X^{-1})\right)$
- $\mu \leq t - 2 \implies$
  - $(\zeta, \zeta, \xi_1, \ldots, \xi_t, 0 \cdots, 0) \in \mathcal{Z}(\mathsf{I})$, $\forall \zeta \in \mathbb{F}$,
  - $\mathsf{E} = \mathbb{F}$,
  - $g(X) = X^{n+1} + X$

- X. Chen, I. S. Reed, T. Helleseth, K. Truong, General Principles for the Algebraic Decoding of Cyclic Codes, *IEEE Trans. on Inf. Th.*, **40** (1994) , 1661–1663

1. generalize Cooper's approach to q-adic codes, giving a solution for decoding an error whose weight μ is assumed given;

2. give an alternative approach via Newton identity.

Assume $K = GF(q)$ and consider both the complete defining set S_C and a defining set S of C and set

$\mathcal{P} := \mathbb{F}[Z_1, \ldots, Z_\mu, Y_1, \ldots, Y_\mu]$

$f_i := \sum_{j=1}^{\mu} Y_j Z_j^i - \mathsf{s}_i \in \mathcal{P}, i \in S_C$;

$h_j := Z_j^n - 1 \in \mathcal{P}$

$\lambda_j := Y_j^{q-1} - 1 \in \mathcal{P}$ (Y_j represents the magnitude $e_j \in GF(q)$);

$\mathsf{I} := \mathbb{I}(f_i, g_j, \lambda_j : 1 \leq j \leq \mu, i \in S) \subset \mathcal{P}$;

$\mathcal{Z}(\mathsf{I}) \subset \mathbb{F}^{2\mu}$ the roots of I;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $Z_1 < \cdots Z_\mu < Y_1, \cdots, Z_\mu$;

$g \in \mathbb{F}[Z_1]$ the unique polynomial : $G \cap \mathbb{F}[Z_1] = \{g\}$;

$\mathsf{Z} := \{\xi : (\xi, a_2, \ldots, a_\mu, e_1, \ldots, e_\mu) \in \mathcal{Z}(\mathsf{I})\}$.

$\mathsf{E} := \{\xi_1, \ldots, \xi_\mu\}$ the set of the error locators of an error whose weight μ *is assumed to be known*

Then

- $\mathsf{E} = \mathsf{Z} = \{\xi : g(\xi) = 0\}$
- $\#\mathsf{E} = \mu = t = \deg(g)$;
- $g(X) = \prod_{\xi \in \mathsf{Z}}(X - \xi)$;
- $X^\mu g(X^{-1})$ is the error locator polynomial.

Let $h_i := \sum_{j=1}^{\mu} Y_j Z_j^i$ and $\sigma_j(Z_1, \ldots, Z_\mu)$ the jth elementary symmetric function.

Recall *Newton identity*

$$h_i + \sum_{j=1}^{\mu} \sigma_j h_{i-j} = 0, \mu \leq i \leq n$$

and remark that (in our setting) h_i represents the syndrome s_i and the error locator polynomial is $L_e = 1 + \sum_{j=1}^{\mu} \sigma_j Z^j$.

Thus setting
$R := \{l_1, \ldots, l_r\}$ such that

$$\{q^j l, l \in R, 0 \leq j < m\} = \{i, 1 \leq i \leq n, i \notin S_C\}$$

$\mathcal{P} := \mathbb{F}[T_1, \ldots, T_\mu, U_1, \ldots, U_r]$
$\pi : K[T_1, \ldots, T_\mu, X_1, \ldots, X_n] \to \mathcal{P}$ the evaluation

$$\pi(X_i) := \begin{cases} \mathsf{s}_i & i \in S_C \\ U_\ell^{j-1} & i = \ell_j \notin S_C \end{cases}$$

$f_i := \pi\left(X_i + \sum_{j=1}^{\mu} T_j X_{i-j}\right) \in \mathcal{P}, \mu \leq i < n;$
$p_j := U_j^{q^m} - U_j, 1 \leq j \leq r$
$q_l := T_l^{q^m} - T_l, 1 \leq l \leq \mu$
$\Gamma := \mathbb{I}(f_i, p_j, q_l : \mu \leq i < n, 1 \leq j \leq r, 1 \leq l \leq \mu) \subset \mathcal{P};$
g_l the monic primitive generator of $\Gamma \cap \mathbb{F}[T_l]$;

Then $g_l(T_l) = T_l - \sigma_l$.

Remark that each g_l can be obtained by an appropriate Gröbner basis computation.

- D. Augot, M. Bardet, J.-C. Faugere, Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases, *Proc. IEEE Int. Symp. Information Theory 2003*, (2003)

Assume $q = 2$ and let $h_i := \sum_{j=1}^{\mu} Z_j^i$ be the Waring functions and $\sigma_i(Z_1, \ldots, Z_\mu)$ the elementary symmetric function.

Recall *Newton identities*

$$h_i + \sum_{j=1}^{i-1} \sigma_j h_{i-j} + i\sigma_i = 0 \qquad 1 \leq i \leq \mu$$

$$h_i + \sum_{j=1}^{\mu} \sigma_j h_{i-j} = 0 \qquad \mu \leq i \leq n$$

and the existence of the Waring formulas

$$\mathfrak{W}_i(T_1, \ldots, T_\mu) : h_i = \mathfrak{W}_i(\sigma_1, \ldots, \sigma_\mu).$$

so that setting

$$\mathcal{Q} := \mathbb{Z}_2[Y_1, \ldots, Y_\mu, T_1, \ldots, T_\mu]$$
$$f_i := Y_i + \sum_{j=1}^{i-1} T_j Y_{i-j} + iT_i, 1 \leq i \leq \mu;$$
$$f_i := Y_i + \sum_{j=1}^{\mu} T_j Y_{i-j}, \mu \leq i \leq n;$$
$$q_l := T_l^{q^m} - T_l, 1 \leq l \leq \mu$$

$$\mathcal{Q} := \mathbb{Z}_2[Y_1, \ldots, Y_\mu, T_1, \ldots, T_\mu]$$
$$f_i := Y_i + \sum_{j=1}^{i-1} T_j Y_{i-j} + iT_i, 1 \leq i \leq \mu;$$
$$f_i := Y_i + \sum_{j=1}^{\mu} T_j Y_{i-j} \mu \leq i \leq n;$$
$$q_l := T_l^{q^m} - T_l, 1 \leq l \leq \mu$$

- a preprocessing Gröbner basis computation of the ideal

$$\mathbb{I}(f_i : 1 \leq i \leq n) \subset \mathcal{Q}$$

returns the basis

$$\{Y_i - \mathfrak{W}_i(T_1, \ldots, T_\mu), 1 \leq i \leq \mu\}.$$

- the Gröbner basis computation of the ideal

$$\mathbb{I}\left(\mathsf{s}_i - \mathfrak{W}_i(T_1, \ldots, T_\mu), q_l, i \in S_C, 1 \leq l \leq \mu\right)$$

returns the basis

$$\{T_1 - \sigma_1, \cdots, T_\mu - \sigma_\mu\}$$

and the error locator polynomial is

$$L_e = 1 + \sum_{j=1}^{\mu} \sigma_j Z_j.$$

"It seems that the behaviour of the G-basis computation is the same for all possible values of the syndrome, provided that it corrisponds to an error of a given weight" Therefore perform a preprocessing computation for each possible weight and use this as a *trace* for each decoding each error. At worst one gets the true solution and some more...

- X. Chen, I. S. Reed, T. Helleseth, K. Truong, Algebraic decoding of cyclic codes: A polynomial Ideal Point of View, *Contemporary Mathematics*, **168** (1994), 15–22

$K = GF(q)$

$S := \{l_1, \ldots, l_s\}$

$\mathcal{P} := \mathbb{F}[X_1, \ldots, X_s, Z_t, \ldots, Z_1, Y_1, \ldots, Y_t]$

$f_i := \sum_{j=1}^{t} Y_j Z_j^{l_i} - X_i \in \mathcal{P}, 1 \leq i \leq s;$

$h_j := Z_j^{n+1} - Z_j \in \mathcal{P}$

$\lambda_j := Y_j^q - 1 \in \mathcal{P};$

$\mathsf{I} := \mathbb{I}(f_i, g_j, \lambda_j : 1 \leq j \leq t, 1 \leq i \leq s) \subset \mathcal{P};$

$\mathcal{Z}(\mathsf{I}) \subset \mathbb{F}^{2\mu}$ the roots of I;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_s < Z_t < \cdots Z_1 < Y_1, \cdots, Y_t$;

Assume that G contains a *single* element $g_i \in \mathbb{F}[X_1, \ldots, X_s, Z_t, \ldots, Z_{t-i+1}]$ with *positive* degree in Z_{t-i+1} and set

$$g_i(X_1, \ldots, X_s, 0, \ldots, 0, Z_{t-i+1}) = \sum_{j=0}^{n_i} c_{i,j} Z_{t-i+1}^j$$

If an error has weight $\mu \leq t$ then:

1. the following conditions are equivalent:

   (a) there are exactly μ errors

   (b) $c_{1,0}(\mathsf{s}_{l_i}) = \cdots = c_{t-\mu,0}(\mathsf{s}_{l_i}) = 0$

2. $X^\mu L_e(X^{-1}) = \gcd\left(g_{t-\mu}(\mathsf{s}_{l_i}, 0, X), X^n - 1\right)$

$\mu := 1$
While $c_{\mu,0}(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}) = 0$ **do** $\mu := \mu + 1$
$g := \gcd\left(g_\mu(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}, 0, \ldots, 0, X), X^n - 1\right)$
$L(z) := X^\mu g(X^{-1})$

- P. Loustaunau, E.V. York, On the decoding of cyclic codes using Gröbner bases,*J AAECC*, **8** (1997) 469–483

1. remark that the CRHT assumption, in general, does not hold;
2. make a weak proposal to correct the CRHT algorithm
3. remark that the Gröbner computation suggested cannot be performed by the best softwares of the period (1997)*
4. therefore suggest to use, since the ideal is 0-dimensional, the FGLM algorithm;

- M. Caboara, The Chen-Reed-Helleseth-Truong Decoding Algorithm and the Gianni-Kalkbrener Gröbner Shape Theorem ,*J AAECC*, **13** (2002) 209–232

1. gives a stronger version of L-Y by using Gianni-Kalkbrener Theorem;
2. suggests to add the relations $X^{q^m} - X$ satisfied by the syndromes;
3. improves the telescope remark of CRHT.

* which is true; what is interesting is that Cooper's computation can be easily performed by the same software.

Gianni-Kalkbrener Gröbner Shape Theorem

Denote

k the algebraic closure of k;

$\mathcal{P} = k[X_1, \ldots, X_n]$

I $\subset \mathcal{P}$ a 0-dimensional ideal;

$\mathsf{I}_d := \mathsf{I} \cap k[X_1, \ldots, X_d]$, $d \leq n$;

$\mathcal{Z}(\mathsf{I}_d) \subset \mathsf{k}^d$ its roots;

$<$ the lex ordering induced by $X_1 < \ldots < X_n$;

$G := \{g_1, \ldots, g_s\}$ the Gröbner basis of I wrt $<$ ordered so that $\mathbf{T}(g_1) < \mathbf{T}(g_2) < \cdots < \mathbf{T}(g_s)$;

for each $d \leq n$ $G_d = G \cap k[X_1, \ldots, X_d]$;

$\alpha := (b_1, \ldots, b_d) \in \mathcal{Z}(\mathsf{I}_d)$;

$\Phi_\alpha : \mathcal{P} \to K[X_{d+1}, \ldots, X_n]$, :

$f(X) \to f(\alpha, X_{d+1}, \ldots, X_n)$.

Expresses each $g_i \in k[X_1, \ldots, X_j] \setminus k[X_1, \ldots, X_{j-1}]$ as

$$\begin{aligned} g_i &:= \sum_{l=0}^{\ell} g_{il}(X_1, \ldots, X_{j-1}) X_j^l \\ &= Lp(g_i) X_j^\ell + \ldots + g_{i1} X_j + Tp(g_i). \end{aligned}$$

Gianni-Kalkbrener Gröbner Shape Theorem

$G := \{g_1, \ldots, g_s\}$ the Gröbner basis of I wrt $<$ ordered so that $\mathbf{T}(g_1) < \mathbf{T}(g_2) < \cdots < \mathbf{T}(g_s)$;

for each $\iota \leq n$ $G_\iota = G \cap k[X_1, \ldots, X_\iota]$;

for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota-1} : \deg_{X_\iota}(g) = \ell\}$

$\alpha := (b_1, \ldots, b_d) \in \mathcal{Z}(\mathsf{I}_d)$;

$\Phi_\alpha : \mathcal{P} \to K[X_{d+1}, \ldots, X_n]$, :

$f(X) \to f(\alpha, X_{d+1}, \ldots, X_n)$.

For each $h \in G_{\iota\ell}$ we have $h = Lp(h)X_\iota^\ell + \ldots + Tp(h)$.

Let

σ be the minimal value such that $\Phi_\alpha(Lp(g_\sigma)) \neq 0$

j, δ the value such that $g_\sigma \in G_{j\delta}$

Then

1. $j = d + 1$,
2. for each $g \in G_{\iota\ell}$:
   - $\iota \leq d \implies \Phi_\alpha(g) = 0$,
   - $\iota = d + 1 = j, \ell < \delta \implies \Phi_\alpha(g) = 0$,
3. $\Phi_\alpha(g_\sigma) = \gcd\left(\Phi_\alpha(g) : g \in G_{d+1}\right) \in \mathsf{k}[X_{d+1}]$,
4. for each $b \in \mathsf{k}$,

$$(b_1, \ldots, b_d, b) \in \mathcal{Z}(\mathsf{I}_{d+1}) \iff \Phi_\alpha(g_\sigma)(b) = 0.$$

Let

$\mathcal{Q} := \mathbb{F}[X_1, \ldots, X_s]$

$\mathcal{P} := \mathbb{F}[X_1, \ldots, X_s, Z_t, \ldots, Z_1, Y_1, \ldots, Y_t]$

$f_i := \sum_{j=1}^{t} Y_j Z_j^{l_i} - X_i \in \mathcal{P}, 1 \leq i \leq s;$

$h_j := Z_j^{n+1} - Z_j \in \mathcal{P}$

$\lambda_j := Y_j^q - 1 \in \mathcal{P};$

$\sigma_i := X_i^{q^m} - X_i \in \mathcal{P}, 1 \leq i \leq s;$

$\mathsf{I} := \mathbb{I}(f_i, g_j, \lambda_j, \sigma_i : 1 \leq j \leq t, 1 \leq i \leq s) \subset \mathcal{P};$

$\mathcal{Z}(\mathsf{I}) \subset \mathbb{F}^{2\mu}$ the roots of I;

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_s < Z_t < \cdots Z_1 < Y_1 < \cdots < Y_t$;

for each $\iota \leq n$ $G_\iota = G \cap \mathcal{P}[Z_t, \cdots, Z_\iota]$;

for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota+1} : \deg_{X_\iota}(g) = \ell\}$

$\mathcal{Q} := \mathbb{F}[X_1, \ldots, X_s]$
$\mathcal{P} := \mathbb{F}[X_1, \ldots, X_s, Z_t, \ldots, Z_1, Y_1, \ldots, Y_t]$
G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_s < Z_t < \cdots Z_1 < Y_1, \cdots, Y_t$;
for each $\iota \leq n$ $G_\iota = G \cap \mathcal{P}[Z_t, \cdots, Z_\iota]$;
for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota+1} : \deg_{X_\iota}(g) = \ell\}$

Then the CRHT results implie
$\ell < \iota \implies G_{\iota\ell} = \emptyset$,
$\ell > \iota \implies \ell = n+1, G_{\iota\ell} = \{Z_\iota^{n+1} - Z_\iota\}$
If the error has weight μ, then, for each $g \in G_{\iota\iota}$,

1. if $\iota < \mu$ then $g(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}, 0, \ldots, 0, Z_\iota) = 0$;

2. if $\iota = \mu$ and $Lp(g) \neq 0$ then
$$0 \neq g(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}, 0, \ldots, 0, Z_\mu) = Z_\mu^\mu Le(Z_\mu^{-1});$$

3. if $\iota = \mu + 1$ and $Lp(g) \neq 0$ then
$$g(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}, 0, \ldots, 0, Z_\iota) = Z_\iota \cdot \left(Z_\iota^\mu Le(Z_\iota^{-1})\right);$$

4. if $\iota > \mu + 1$ and $Lp(g) \neq 0$ then
$$Z_\iota \cdot \left(Z_\iota^\mu Le(Z_\iota^{-1})\right) \mid g(\mathsf{s}_{l_1}, \ldots, \mathsf{s}_{l_s}, 0, \ldots, 0, Z_\iota)$$

$$S = \{1, 3, 5\}, K = \mathbb{Z}_2, n = 15, \mathbb{F} = GF(16)$$

$$
\begin{aligned}
g_{3\ 3\ 1} &= Z_3^3(\mathbf{X_2X_3^3 + X_2}) + Z_3^2X_1X_2X_3^3 + Z_3^2X_1X_2 + Z_3X_1^{11}X_2^3 \\
&+ Z_3X_1^8X_2^4X_3^3 + Z_3X_1^7X_2X_3^2 + Z_3X_1^6X_2^3X_3 + Z_3X_1^5X_2^{10} \\
&+ Z_3X_1^5X_2^5X_3^3 + Z_3X_1^5X_3^3 + Z_3X_1^4X_2^2X_3^2 + Z_3X_1^3X_2^4X_3 \\
&+ Z_3X_1^2X_2^{11}X_3^3 + Z_3X_1^2X_2^{11} + Z_3X_1^2X_2^6X_3^3 + Z_3X_1^2X_2^6 \\
&+ Z_3X_1X_2^8X_3^2 + Z_3X_1X_2^3X_3^2 + Z_3X_2^{10}X_3 \\
&+ Z_3X_2^5X_3 + Z_3X_3 \\
&+ \mathtt{X}_1^{12}\mathtt{X}_2^3 + \mathtt{X}_1^8\mathtt{X}_2\mathtt{X}_3^2 + \mathtt{X}_1^7\mathtt{X}_2^8\mathtt{X}_3 + \mathtt{X}_1^7\mathtt{X}_2^3\mathtt{X}_3 + \mathtt{X}_1^6\mathtt{X}_2^{10} \\
&+ \mathtt{X}_1^6\mathtt{X}_3^3 + \mathtt{X}_1^5\mathtt{X}_2^{12}\mathtt{X}_3^2 + \mathtt{X}_1^4\mathtt{X}_2^9\mathtt{X}_3 + \mathtt{X}_1^3\mathtt{X}_2^{11} + \mathtt{X}_1^3\mathtt{X}_2^6\mathtt{X}_3^3 \\
&+ \mathtt{X}_1^3\mathtt{X}_2^6 + \mathtt{X}_1^3\mathtt{X}_2\mathtt{X}_3^3 + \mathtt{X}_1^3\mathtt{X}_2 + \mathtt{X}_1^2\mathtt{X}_2^{13}\mathtt{X}_3^2 + \mathtt{X}_1\mathtt{X}_2^{15}\mathtt{X}_3 \\
&+ \mathtt{X}_1\mathtt{X}_2^{10}\mathtt{X}_3 + \mathtt{X}_1\mathtt{X}_3 + \mathtt{X}_2^{12}\mathtt{X}_3^3 + \mathtt{X}_2^7\mathtt{X}_3^3 + \mathtt{X}_2^2, \\
g_{3\ 3\ 2} &= Z_3^3(\mathbf{X_2^5 + X_3^3}) + Z_3^2X_1X_2^5 + Z_3^2X_1X_3^3 + Z_3X_1^{11}X_2^2 \\
&+ Z_3X_1^8X_2^{13}X_3^3 + Z_3X_1^8X_2^8 + Z_3X_1^8X_2^3 + Z_3X_1^7X_2^5X_3^2 \\
&+ Z_3X_1^6X_2^7X_3 + Z_3X_1^5X_2^{14}X_3^3 + Z_3X_1^5X_2^9X_3^3 + Z_3X_1^5X_2^9 \\
&+ Z_3X_1^4X_2X_3^2 + Z_3X_1^3X_2^{13}X_3 + Z_3X_1^2X_2^{10}X_3^3 \\
&+ Z_3X_1^2X_2^5X_3^3 + Z_3X_1^2X_2^5 + Z_3X_1^2 + Z_3X_1X_2^{12}X_3^2 \\
&+ Z_3X_1X_2^7X_3^2 + Z_3X_2^9X_3 + \mathtt{X}_1^{12}\mathtt{X}_2^2 + \mathtt{X}_1^8\mathtt{X}_2^5\mathtt{X}_3^2 \\
&+ \mathtt{X}_1^7\mathtt{X}_2^{12}\mathtt{X}_3 + \mathtt{X}_1^7\mathtt{X}_2^2\mathtt{X}_3 + \mathtt{X}_1^6\mathtt{X}_2^9\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^4 + \mathtt{X}_1^5\mathtt{X}_2\mathtt{X}_3^2 \\
&+ \mathtt{X}_1^4\mathtt{X}_2^{13}\mathtt{X}_3 + \mathtt{X}_1^3\mathtt{X}_2^{15} + \mathtt{X}_1^3\mathtt{X}_2^{10}\mathtt{X}_3^3 + \mathtt{X}_1^3\mathtt{X}_2^{10} \\
&+ \mathtt{X}_1^3\mathtt{X}_3^3 + \mathtt{X}_1^3 + \mathtt{X}_1^2\mathtt{X}_2^2\mathtt{X}_3^2 + \mathtt{X}_1\mathtt{X}_2^9\mathtt{X}_3 + \mathtt{X}_2^{11}, \\
g_{3\ 3\ 3} &= Z_3^3(\mathbf{X_1 + X_2^2X_3^2}) + Z_3^2X_1^2 + Z_3^2X_1X_2^2X_3^2 + Z_3X_1^{12}X_2^2 \\
&+ Z_3X_1^8X_2^5X_3^2 + Z_3X_1^8X_3^2 + Z_3X_1^7X_2^{12}X_3 + Z_3X_1^7X_2^7X_3 \\
&+ Z_3X_1^7X_2^2X_3 + Z_3X_1^6X_2^{14}X_3^3 + Z_3X_1^6X_2^9X_3^3 + Z_3X_1^6X_2^9 \\
&+ Z_3X_1^5X_2^{11}X_3^2 + Z_3X_1^5X_2X_3^2 + Z_3X_1^4X_2^{13}X_3 \\
&+ Z_3X_1^4X_2^8X_3 + Z_3X_1^4X_2^3X_3 + Z_3X_1^3X_2^{10}X_3^3 + Z_3X_1^3X_2^{10} \\
&+ Z_3X_1^3X_2^5X_3^3 + Z_3X_1^3X_2^5 + Z_3X_1^2X_2^{12}X_3^2 + Z_3X_1X_2^4X_3 \\
&+ Z_3X_2^{11}X_3^3 + Z_3X_2^6X_3^3 + \mathtt{X}_1^{10}\mathtt{X}_2^3 + \mathtt{X}_1^8\mathtt{X}_2^{12}\mathtt{X}_3 \\
&+ \mathtt{X}_1^8\mathtt{X}_2^7\mathtt{X}_3 + \mathtt{X}_1^7\mathtt{X}_2^4\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^{11}\mathtt{X}_3^2 + \mathtt{X}_1^6\mathtt{X}_2^6\mathtt{X}_3^2 + \mathtt{X}_1^5\mathtt{X}_2^8\mathtt{X}_3 \\
&+ \mathtt{X}_1^5\mathtt{X}_2^3\mathtt{X}_3 + \mathtt{X}_1^4\mathtt{X}_2^{15} + \mathtt{X}_1^4\mathtt{X}_2^{10} + \mathtt{X}_1^4\mathtt{X}_2^5\mathtt{X}_3^3 \\
&+ \mathtt{X}_1^3\mathtt{X}_2^7\mathtt{X}_3^2 + \mathtt{X}_1^2\mathtt{X}_2^4\mathtt{X}_3 + \mathtt{X}_1\mathtt{X}_2^{11} + \mathtt{X}_1\mathtt{X}_2^6\mathtt{X}_3^3 + \mathtt{X}_1\mathtt{X}_2^6 \\
&+ \mathtt{X}_2^{13}\mathtt{X}_3^2 + \mathtt{X}_2^8\mathtt{X}_3^2,
\end{aligned}
$$

$$
\begin{aligned}
g_{3\ 16\ 1} &= Z_3^{16} + Z_3, \\
g_{2\ 2\ 1} &= Z_2^2(\mathbf{X_2X_3^3 + X_2}) + Z_2Z_3(\mathbf{X_2X_3^3 + X_2}) \\
&+ Z_2X_1(\mathbf{X_2X_3^3 + X_2}) \\
&+ Z_3^2X_2X_3^3 + Z_3^2X_2 + Z_3X_1X_2X_3^3 + Z_3X_1X_2 + \mathtt{X}_1^{11}\mathtt{X}_2^3 \\
&+ \mathtt{X}_1^8\mathtt{X}_2^4\mathtt{X}_3^3 + \mathtt{X}_1^7\mathtt{X}_2\mathtt{X}_3^2 + \mathtt{X}_1^6\mathtt{X}_2^3\mathtt{X}_3 + \mathtt{X}_1^5\mathtt{X}_2^{10} \\
&+ \mathtt{X}_1^5\mathtt{X}_2^5\mathtt{X}_3^3 + \mathtt{X}_1^5\mathtt{X}_3^3 + \mathtt{X}_1^4\mathtt{X}_2^2\mathtt{X}_3^2 + \mathtt{X}_1^3\mathtt{X}_2^4\mathtt{X}_3 \\
&+ \mathtt{X}_1^2\mathtt{X}_2^{11}\mathtt{X}_3^3 + \mathtt{X}_1^2\mathtt{X}_2^{11} + \mathtt{X}_1^2\mathtt{X}_2^6\mathtt{X}_3^3 + \mathtt{X}_1^2\mathtt{X}_2^6 + \mathtt{X}_1\mathtt{X}_2^8\mathtt{X}_3^2 \\
&+ \mathtt{X}_1\mathtt{X}_2^3\mathtt{X}_3^2 + \mathtt{X}_2^{10}\mathtt{X}_3 + \mathtt{X}_2^5\mathtt{X}_3 + \mathtt{X}_3, \\
g_{2\ 2\ 2} &= Z_2^2(\mathbf{X_2^5 + X_3^3}) + Z_2Z_3(\mathbf{X_2^5 + X_3^3}) \\
&+ Z_2X_1(\mathbf{X_2^5 + X_3^3}) \\
&+ Z_3^2X_2^5 + Z_3^2X_3^3 + Z_3X_1X_2^5 + Z_3X_1X_3^3 + \mathtt{X}_1^{11}\mathtt{X}_2^2 \\
&+ \mathtt{X}_1^8\mathtt{X}_2^{13}\mathtt{X}_3^3 + \mathtt{X}_1^8\mathtt{X}_2^8 + \mathtt{X}_1^8\mathtt{X}_2^3 + \mathtt{X}_1^7\mathtt{X}_2^5\mathtt{X}_3^2 + \mathtt{X}_1^6\mathtt{X}_2^7\mathtt{X}_3 \\
&+ \mathtt{X}_1^5\mathtt{X}_2^{14}\mathtt{X}_3^3 + \mathtt{X}_1^5\mathtt{X}_2^9\mathtt{X}_3^3 + \mathtt{X}_1^5\mathtt{X}_2^9 + \mathtt{X}_1^4\mathtt{X}_2\mathtt{X}_3^2 \\
&+ \mathtt{X}_1^3\mathtt{X}_2^{13}\mathtt{X}_3 + \mathtt{X}_1^2\mathtt{X}_2^{10}\mathtt{X}_3^3 + \mathtt{X}_1^2\mathtt{X}_2^5\mathtt{X}_3^3 + \mathtt{X}_1^2\mathtt{X}_2^5 \\
&+ \mathtt{X}_1^2 + \mathtt{X}_1\mathtt{X}_2^{12}\mathtt{X}_3^2 + \mathtt{X}_1\mathtt{X}_2^7\mathtt{X}_3^2 + \mathtt{X}_2^9\mathtt{X}_3, \\
g_{2\ 2\ 3} &= Z_2^2(\mathbf{X_1 + X_2^2X_3^2}) + Z_2Z_3(\mathbf{X_1 + X_2^2X_3^2}) \\
&+ Z_2X_1(\mathbf{X_1 + X_2^2X_3^2}) + Z_3^2X_1 + Z_3^2X_2^2X_3^2 + Z_3X_1^2 \\
&+ Z_3X_1X_2^2X_3^2 + \mathtt{X}_1^{12}\mathtt{X}_2^2 + \mathtt{X}_1^8\mathtt{X}_2^5\mathtt{X}_3^2 + \mathtt{X}_1^8\mathtt{X}_3^2 + \mathtt{X}_1^7\mathtt{X}_2^{12}\mathtt{X}_3 + \mathtt{X}_1^7\mathtt{X}_2^7\mathtt{X}_3 \\
&+ \mathtt{X}_1^7\mathtt{X}_2^2\mathtt{X}_3 + \mathtt{X}_1^6\mathtt{X}_2^{14}\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^9\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^9 \\
&+ \mathtt{X}_1^5\mathtt{X}_2^{11}\mathtt{X}_3^2 + \mathtt{X}_1^5\mathtt{X}_2\mathtt{X}_3^2 + \mathtt{X}_1^4\mathtt{X}_2^{13}\mathtt{X}_3 + \mathtt{X}_1^4\mathtt{X}_2^8\mathtt{X}_3 \\
&+ \mathtt{X}_1^4\mathtt{X}_2^3\mathtt{X}_3 + \mathtt{X}_1^3\mathtt{X}_2^{10}\mathtt{X}_3^3 + \mathtt{X}_1^3\mathtt{X}_2^{10} + \mathtt{X}_1^3\mathtt{X}_2^5\mathtt{X}_3^3 \\
&+ \mathtt{X}_1^3\mathtt{X}_2^5 + \mathtt{X}_1^2\mathtt{X}_2^{12}\mathtt{X}_3^2 + \mathtt{X}_1\mathtt{X}_2^4\mathtt{X}_3 + \mathtt{X}_2^{11}\mathtt{X}_3^3 + \mathtt{X}_2^6\mathtt{X}_3^3, \\
g_{2\ 2\ 4} &= Z_2^2(\mathbf{Z_3 + X_2^2X_3^2}) + Z_2Z_3(\mathbf{Z_3 + X_2^2X_3^2}) \\
&+ Z_2X_1(\mathbf{Z_3 + X_2^2X_3^2}) + Z_3^2X_2^2X_3^2 + Z_3X_1X_2^2X_3^2 + \mathtt{X}_1^{12}\mathtt{X}_2^2 \\
&+ \mathtt{X}_1^8\mathtt{X}_2^5\mathtt{X}_3^2 + \mathtt{X}_1^8\mathtt{X}_3^2 + \mathtt{X}_1^7\mathtt{X}_2^{12}\mathtt{X}_3 + \mathtt{X}_1^7\mathtt{X}_2^7\mathtt{X}_3 \\
&+ \mathtt{X}_1^7\mathtt{X}_2^2\mathtt{X}_3 + \mathtt{X}_1^6\mathtt{X}_2^{14}\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^9\mathtt{X}_3^3 + \mathtt{X}_1^6\mathtt{X}_2^9 + \mathtt{X}_1^5\mathtt{X}_2^{11}\mathtt{X}_3^2 \\
&+ \mathtt{X}_1^5\mathtt{X}_2\mathtt{X}_3^2 + \mathtt{X}_1^4\mathtt{X}_2^{13}\mathtt{X}_3 + \mathtt{X}_1^4\mathtt{X}_2^8\mathtt{X}_3 + \mathtt{X}_1^4\mathtt{X}_2^3\mathtt{X}_3 \\
&+ \mathtt{X}_1^3\mathtt{X}_2^{10}\mathtt{X}_3^3 + \mathtt{X}_1^3\mathtt{X}_2^{10} + \mathtt{X}_1^3\mathtt{X}_2^5\mathtt{X}_3^3 + \mathtt{X}_1^3\mathtt{X}_2^5 + \mathtt{X}_1^3 \\
&+ \mathtt{X}_1^2\mathtt{X}_2^{12}\mathtt{X}_3^2 + \mathtt{X}_1\mathtt{X}_2^4\mathtt{X}_3 + \mathtt{X}_2^{11}\mathtt{X}_3^3 + \mathtt{X}_2^6\mathtt{X}_3^3 + \mathtt{X}_2, \\
g_{2\ 16\ 1} &= Z_2^{16} + Z_2, \\
g_{1\ 1\ 1} &= Z_1 + Z_2 + Z_3 + X_1.
\end{aligned}
$$

Warning: from now on, I write s_i to mean s_{l_i}.

$$
\begin{aligned}
g_{3\ 3\ 1} &= Z_3^3(\mathbf{X_2X_3^3 + X_2}) + \cdots \\
g_{3\ 3\ 2} &= Z_3^3(\mathbf{X_2^5 + X_3^3}) + \cdots \\
g_{3\ 3\ 3} &= Z_3^3(\mathbf{X_1 + X_2^3X_3^2}) + \cdots \\
g_{3\ 16\ 1} &= Z_3^{16} + Z_3, \\
g_{2\ 2\ 1} &= Z_2^2(\mathbf{X_2X_3^3 + X_2}) + \cdots \\
g_{2\ 2\ 2} &= Z_2^2(\mathbf{X_2^5 + X_3^3}) + \cdots \\
g_{2\ 2\ 3} &= Z_2^2(\mathbf{X_1 + X_2^3X_3^2}) + \cdots \\
g_{2\ 2\ 4} &= Z_2^2(\mathbf{Z_3 + X_2^2X_3^2}) + \cdots \\
g_{2\ 16\ 1} &= Z_2^{16} + Z_2, \\
g_{1\ 1\ 1} &= Z_1 + Z_2 + Z_3 + X_1.
\end{aligned}
$$

Note that

$$
\begin{aligned}
Lp(g_{3\ 3\ 1}) &= Lp(g_{2\ 2\ 1}), \\
Lp(g_{3\ 3\ 2}) &= Lp(g_{2\ 2\ 2}), \\
Lp(g_{3\ 3\ 3}) &= Lp(g_{2\ 2\ 3}),
\end{aligned}
$$

and remark that

$$
\begin{aligned}
g_{3\ 3\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) &= Zg_{2\ 2\ 1}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, Z) + Tp(g_{3\ 3\ 1}), \\
g_{3\ 3\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) &= Zg_{2\ 2\ 2}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, Z) + Tp(g_{3\ 3\ 2}), \\
g_{3\ 3\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, Z) &= Zg_{2\ 2\ 3}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, Z) + Tp(g_{3\ 3\ 3}), \\
g_{2\ 2\ *}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, 0, Z) &= ZLp(g_{2\ 2\ *})(Z + X_1) + Tp(g_{2\ 2\ *}).
\end{aligned}
$$

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_s < Z_t < \cdots Z_1 < Y_1 < \cdots < Y_t$;

for each $\iota \leq n$ $G_\iota = G \cap \mathcal{Q}[Z_t, \cdots, Z_\iota]$;

for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota+1} : \deg_{X_\iota}(g) = \ell\}$

Enumerate each $G_{\iota\ell}$ as

$$G := \{g_{\iota\ell 1}, \ldots, g_{\iota\ell j_{\iota\ell}}\}, \mathbf{T}(g_{\iota\ell 1}) < \cdots < \mathbf{T}(g_{\iota\ell j_{\iota\ell}}).$$

We have $g_{\iota\ell j} = Lp(g_{\iota\ell j})X_\iota^\ell + \ldots + g_{i1}X_j + Tp(g_{\iota\ell j})$.

$\mu := t$, $g := 1$,

Repeat

$j := 0$
Repeat $j := j + 1$
Until $Lp(g_{\mu\mu j})(s, 0) \neq 0$ **or** $j > j_{\mu\mu}$
If $j > j_{\mu\mu}$ **then** $\mu := \mu - 1$
else
If $Tp(g_{\mu\mu j})(s, 0) = 0$ **do** $\mu := \mu - 1$
else
$g(Z) := g_{\mu\mu j}(s, 0, Z)$;

Until $g \neq 1$ **or** $\mu = 0$

Output μ, $X^\mu g(X^{-1})$

$$
\begin{aligned}
g_{3\ 3\ 1} &= Z_3^3(\mathbf{X_2X_3^3 + X_2}) + \cdots + A \\
g_{3\ 3\ 2} &= Z_3^3(\mathbf{X_2^5 + X_3^3}) + \cdots + B \\
g_{3\ 3\ 3} &= Z_3^3(\mathbf{X_1 + X_2^2X_3^2}) + \cdots + C \\
g_{3\ 16\ 1} &= Z_3^{16} + Z_3, \\
g_{2\ 2\ 1} &= Z_2^2(\mathbf{X_2X_3^3 + X_2}) + \cdots + D \\
g_{2\ 2\ 2} &= Z_2^2(\mathbf{X_2^5 + X_3^3}) + \cdots + E \\
g_{2\ 2\ 3} &= Z_2^2(\mathbf{X_1 + X_2^2X_3^2}) + \cdots + F \\
g_{2\ 2\ 4} &= Z_2^2(\mathbf{Z_3 + X_2^2X_3^2}) + \cdots + G \\
g_{2\ 16\ 1} &= Z_2^{16} + Z_2, \\
g_{1\ 1\ 1} &= Z_1 + Z_2 + Z_3 + X_1.
\end{aligned}
$$

$$
\begin{array}{llllll}
\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 \neq 0 & A \neq 0 & & & & \Longrightarrow\ g_{3\ 3\ 1} \\
& A = 0 & D \neq 0 & & & \Longrightarrow\ g_{2\ 2\ 1} \\
& & D = 0 & & & \Longrightarrow\ g_{1\ 1\ 1} \\
\mathsf{s}_2\mathsf{s}_3^3 + \mathsf{s}_2 = 0 & \mathsf{s}_2^5 + \mathsf{s}_3^3 \neq 0 & B \neq 0 & & & \Longrightarrow\ g_{3\ 3\ 2} \\
& & B = 0 & E \neq 0 & & \Longrightarrow\ g_{2\ 2\ 2} \\
& & & E = 0 & & \Longrightarrow\ g_{1\ 1\ 1} \\
& \mathsf{s}_2^5 + \mathsf{s}_3^3 = 0 & \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0 & C \neq 0 & & \Longrightarrow\ g_{3\ 3\ 3} \\
& & & C = 0 & F \neq 0 & \Longrightarrow\ g_{2\ 2\ 3} \\
& & & & F = 0 & \Longrightarrow\ g_{1\ 1\ 1} \\
& & \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2 = 0 & \mathsf{s}_2^2\mathsf{s}_3^2 \neq 0 & G \neq 0 & \Longrightarrow\ g_{2\ 2\ 4} \\
& & & & G = 0 & \mathsf{s}_1 \neq 0 \Longrightarrow\ g_{1\ 1\ 1} \\
& & & & & \mathsf{s}_1 = 0 \Longrightarrow\ 1 \\
& & & \mathsf{s}_2^2\mathsf{s}_3^2 = 0 & \mathsf{s}_1 \neq 0 & \Longrightarrow\ g_{1\ 1\ 1} \\
& & & & \mathsf{s}_1 = 0 & \Longrightarrow\ 1
\end{array}
$$

- M. Caboara, E. Orsini, M. Sala, *Fast decoding of cyclic codes via the syndrome variety* (2002).

1. Perform postprocessing using Gröbner technology to improve the syndome test.

2. compute and process, for each $\mu, 1 \leq \mu \leq t$, the Gröbner basis of the ideal encoding only the case in which there are *exactly* μ *errors*.

$$
\begin{array}{lll}
\mathsf{s}_2 = 0 & \mathsf{s}_3 = 0 & \Longrightarrow L = 1 \\
\mathsf{s}_2 = 0 & \mathsf{s}_3 \neq 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 + Z^2\mathsf{s}_1^2 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 = 0\ \mathsf{s}_1 = 0 & \Longrightarrow L = 1 + Z^3\mathsf{s}_2 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 = 0\ \mathsf{s}_1 \neq 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 \\
 & & \quad + Z^2\left(\mathsf{s}_1^{11}\mathsf{s}_2^2\mathsf{s}_1^5\mathsf{s}_2^4\right) + Z^3\mathsf{s}_1^9\mathsf{s}_2^3 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 \neq 0\ \sigma = 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 \\
\mathsf{s}_2^5 + 1 = 0 & \mathsf{s}_3 \neq 0\ \sigma \neq 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 \\
 & & \quad + Z^2\left(\mathsf{s}_1^2 + \mathsf{s}_2^4\mathsf{s}_3^4\right)\left(\mathsf{s}_1^5\mathsf{s}_3^2 + \sigma^{-1}\right) \\
 & & \quad + Z^3\mathsf{s}_1^2\mathsf{s}_2^2\mathsf{s}_3\left(\mathsf{s}_1^5 + \mathsf{s}_2^{10}\mathsf{s}_3^{10}\right)\sigma^{-1} \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3 = 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 + Z^2\mathsf{s}_1^2\mathsf{s}_2^5 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0\ \mathsf{s}_1 = 0 & \Longrightarrow L = 1 + Z^2\mathsf{s}_2^{-1}\mathsf{s}_3 + Z^3\mathsf{s}_2 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0\ \rho = 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 + Z^2\mathsf{s}_2^9\mathsf{s}_3 \\
\mathsf{s}_2^6 + \mathsf{s}_2 \neq 0 & \mathsf{s}_3^3 \neq 0\ \mathsf{s}_1\rho \neq 0 & \Longrightarrow L = 1 + Z\mathsf{s}_1 \\
 & & \quad + Z^2\left(\mathsf{s}_1^5\mathsf{s}_2^8\mathsf{s}_3 + \mathsf{s}_1^3\mathsf{s}_2^2\mathsf{s}_3^2\right)\rho^{-1} \\
 & & \quad + Z^2\left(\mathsf{s}_1^2\mathsf{s}_2^9\mathsf{s}_3 + \mathsf{s}_2^{13}\mathsf{s}_3^2\right)\rho^{-1} \\
 & & \quad + Z^3\mathsf{s}_1^4\mathsf{s}_2^3\mathsf{s}_3 \\
 & & \quad + Z^3\mathsf{s}_1^3\mathsf{s}_2^5 + \mathsf{s}_1\mathsf{s}_2^{-1}\mathsf{s}_3 + \mathsf{s}_2^{-4}
\end{array}
$$

where

$$
\begin{aligned}
\rho &:= \mathsf{s}_1^2 + \mathsf{s}_1\mathsf{s}_2^2\mathsf{s}_3^2 + \mathsf{s}_2^{-1}\mathsf{s}_3 \\
\sigma &:= \mathsf{s}_1 + \mathsf{s}_2^2\mathsf{s}_3^2.
\end{aligned}
$$

- E. Orsini, M. Sala, Correcting errors and erasures via the syndrome variety, *J. Pure Appl. Algebra*, **200** (2005), 191–226,

- Remove the *spurious* solutions
  - $(0, \xi_1, \ldots, \xi_\mu)$
  - $(\zeta, \zeta, \xi_1, \ldots, \xi_t, 0 \cdots, 0)$
- Introduce and compute the *general error locator polynomial*

Let

$q = 2$

C an $[n, k, d]$ binary cyclic code, n odd;

$\mathcal{Q} := \mathbb{F}[X_1, \ldots, X_{n-k}]$

$\mathcal{P} := \mathbb{F}[X_1, \ldots, X_{n-k}, Z_t, \ldots, Z_1]$

$f_i := \sum_{j=1}^{t} Z_j^{l_i} - X_i \in \mathcal{P}, 1 \leq i \leq n-k;$

$h_j := Z_j^{n+1} - Z_j \in \mathcal{P}, 1 \leq j \leq t;$

$\sigma_i := X_i^{q^m} - X_i \in \mathcal{P}, 1 \leq i \leq n-k;$

$p_{jl} := \frac{Z_l Z_j \left(Z_l^n - Z_j^n\right)}{Z_l - Z_j}, 1 \leq l < j \leq t;$

$\mathsf{I} := \mathbb{I}(f_i, h_j, \sigma_i, p_{jl}) \subset \mathcal{P};$

G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_{n-k} < Z_t < \cdots Z_1$;

for each $\iota \leq n$ $G_\iota = G \cap \mathcal{Q}[Z_t, \cdots, Z_\iota]$;

for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota+1} : \deg_{X_\iota}(g) = \ell\}$

C an $[n, k, d]$ binary cyclic code, n odd
$\mathcal{Q} := \mathbb{F}[X_1, \ldots, X_{n-k}]$
$\mathcal{P} := \mathbb{F}[X_1, \ldots, X_{n-k}, Z_t, \ldots, Z_1]$
G the reduced Gröbner basis of I w.r.t. the lex ordering $<$ induced by $X_1 < \cdots < X_{n-k} < Z_t < \cdots Z_1 < Y_1 < \cdots < Y_t$;
for each $\iota \leq n$ $G_\iota = G \cap \mathcal{P}[Z_t, \cdots, Z_\iota]$;
for each $\ell \in \mathbb{N}$ $G_{\iota\ell} := \{g \in G_\iota \backslash G_{\iota+1} : \deg_{X_\iota}(g) = \ell\}$

Then

- $G_{ii} = \{g_{ii1}\}$;
- $Lp(g_{ii1}) = 1$;
- $g_{ii1} = Z_i^i + \cdots$;
- denoting $g_{tt1} = Z_t^t + \sum_{l=1}^{t} a_{t-l} Z_t^{t-l} \in \mathcal{Q}[Z_t]$ the following properties are equivalent;
  - there are exactly μ errors;
  - $a_{t-l}(\mathsf{s}) = 0$ for $l > \mu$ and $a_{t-\mu}(\mathsf{s}) \neq 0$;
  - $g_{tt1}(\mathsf{s}, Z_t) = Z^{t-\mu} \cdot \left(Z_t^\mu + \sum_{l=1}^{\mu} a_{t-l}(\mathsf{s}) Z_t^{\mu-l}\right)$;

  and imply that $L_e(Z) = Z^\mu g_{tt1}(\mathsf{s}, Z^{-1})$.

$g_{tt1}(Z) \in \mathcal{Q}[Z]$ is the unique monic polynomial in $\mathcal{Q}[Z]$ which satisfies the following property;

> given a syndrome vector $\mathsf{s} = (\mathsf{s}_1, \ldots, \mathsf{s}_{n-k}) \in \mathbb{F}^{n-k}$ corresponding to an error with weight $\mu \leq t$, then its t roots are the μ error locations plus zero counted with multiplicity $t - \mu$

and is called the **general error locator polynomial** of C

In the present example

$$S = \{1, 3, 5\}, K = \mathbb{Z}_2, K = 15, \mathbb{F} = GF(16)$$

the result is already smallish

$$\begin{aligned}
g_{331} &:= \mathbf{z_3^3} + z_3^2 x_1 \\
&+ z_3(x_3 x_2^9 + x_3 x_2^8 x_1^3 + x_3 x_2^4 + x_3 x_2 x_1^9) \\
&+ z_3(x_2^{15} x_1^2 + x_2^{14} x_1^5 + x_2^{13} x_1^8 + x_2^{12} x_1^{11} + x_2^{11} x_1^{14}) \\
&+ z_3(x_2^{10} x_1^2 + x_2^7 x_1^{11} + x_2^6 x_1^{14} + x_2^5 x_1^2 + x_2^3 x_1^8 + x_2^2 x_1^{11} + x_1^2) \\
&+ x_3 x_2^9 x_1 + x_3 x_2^8 x_1^4 + x_3 x_2^4 x_1 + x_3 x_2 x_1^{10} + x_2^{15} x_1^3 + x_2^{14} x_1^6 \\
&+ x_2^{13} x_1^9 + x_2^{12} x_1^{12} + x_2^{11} x_1^{15} + x_2^{10} x_1^3 + x_2^7 x_1^{12} + x_2^6 x_1^{15} + x_2^5 x_1^3 \\
&+ x_2^3 x_1^9 + x_2^2 x_1^{12} + x_2
\end{aligned}$$

but clever guessing inspired by eye-inspection gives even a more compact presentation

$$g_{331} = A^3 + AE + B$$

where

$$\begin{aligned}
A &:= x_1 + z_3 \\
B &:= x_2 + x_1^3 \\
C &:= x_3 + x_1^5 \\
D &:= x_2^8 + x_2^7 x_1^3 + x_2^3 + x_1^9 \\
E &:= x_1^2(B^{15} - 1) - C x_2 D
\end{aligned}$$

- E. Orsini, M. Sala, Correcting errors and erasures via the syndrome variety, *J. Pure Appl. Algebra*, **200** (2005), 191–226,

Let C be a binary $[n, k, d]$-code with $n \leq 61$ and $d = 3, 4$ $[t = 1]$.

Denote S a defining set of C and

$$\mathcal{L}_C \in \mathcal{F}[x_1, \ldots, x_{n-k}][Z]$$

its general error locator polynomial.

Then there are only four cases

1) C has a defining set of type $S = \{m\}$, with $(n, m) = 1$ and $\mathcal{L}_C = Z + x_1^k$.

2) C has a defining set of type $S = \{m, h\}$, with $(m, h) = 1$ and

$$\mathcal{L}_C = Z + x_1^{m'} x_2^{h'}.$$

where $m', h' \in \mathbb{Z}$ denote the value satisfying the Bezot's identity $mm' + hh' = 1$

3) C is a sub-code of a code C' of type 1) or 2) and $\mathcal{L}_C = \mathcal{L}_{C'}$

4) C is equivalent to a code C' of type 1), 2) or 3) and $\mathcal{L}_C$ can be trivially obtained from $\mathcal{L}_{C'}$.

Let C be a binary $[n, k, d]$-code with $7 \leq n < 63$ (n odd). and $d = 5, 6$, $[t = 2]$.

Then $\mathcal{L}_C = Z^2 + x_1 Z + b(x_1, \ldots, x_{n-k})$ and there are seven cases:

1. either n is such that the code with defining set $\{0, 1\}$ has distance at least 5,
2. or C is a BCH code, i.e. $S_C = \{1, 3\}$ and
$$b = X_2 X_1^{yn-1} + X_1^2, y \in \mathbb{N}$$
3. or C admits a defining set of type $S_C = \{1, n-1, l\}$, with $l = 0, n/3$, and
$$b = \begin{cases} x_1 x_2^{-1}(1 + x_3) & l = 0 \\ \frac{x_3^3+1}{x_1^{n/3} x_2^{2/3n} x_3+1} & l = n/3 \end{cases}$$
4. or C admits a defining set of type $S_C = \{1, n/l\}$, for some $l \geq 3$,
5. or C is one of the following
   - $n = 31$, $S_C = \{1, 15\}$,
   - $n = 31$, $S_C = \{1, 5\}$,
   - $n = 45$, $S_C = \{1, 21\}$,
   - $n = 51$, $S_C = \{1, 9\}$,
   - $n = 51$, $S_C = \{0, 1, 5\}$.
6. or C is a sub-code of one of the codes of the above cases,
7. or C is equivalent to one of the codes of the above cases.

In all cases b is listed, it is always very short and in most cases a formula can be given.