BCH码的低时延分阶统计译码

Low-Latency Ordered Statistics Decoding of BCH Codes

- 陈立 教授
- 中山大学 电子与信息工程学院



Outline



- Background
- BCH Codes
- Ordered Statistics Decoding
- Low-Latency OSD
- Hybrid Soft Decoding

Background



Future scenarios featured by URLLC



Unmanned Driving



Wise Information Technology of Med (WITMED)



Factory Automation



Extended Reality (XR)



Short-to-medium length codes





n is short-to-medium \rightarrow near ML decoding, list decoding



4

Background



• Near ML decoding performance: rate R = 1/2 & length n = 128 [1]



[1] M. Shirvanimoghaddam *et al.*, "Short block-length codes for ultrareliable low latency communications," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 130–137, Feb. 2019.

BCH Codes



Encoding of BCH codes

 $(n, k) \text{ binary primitive BCH code} \begin{cases} \text{Primitive element of } \mathbb{F}_{2^m}: \sigma \\ \text{Codeword length: } n = 2^m - 1 \\ \text{Designed distance: } d = 2t + 1 \end{cases}$

□ Generator polynomial: $g(x) = g_0 + g_1 x + \dots + g_{n-k} x^{n-k} \in \mathbb{F}_2[x]$ is the minimal (deg g(x)) nonzero polynomial such that

$$g(\sigma) = g(\sigma^2) = \dots = g(\sigma^{2t}) = 0$$

□ Message $\underline{f} = (f_0, f_1, ..., f_{k-1}) \in \mathbb{F}_2^k$, in poly. $f(x) = f_0 + f_1 x + \dots + f_{k-1} x^{k-1} \in \mathbb{F}_2[x]$ Codeword $\underline{c} = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_2^n$, in poly. $c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} = f(x)g(x) \in \mathbb{F}_2[x]$ Parity-check condition: $c(\sigma) = c(\sigma^2) = \dots = c(\sigma^{2t}) = 0$

BCH Codes



- Encoding of BCH codes
 - □ Generator matrix:

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0\\ 0 & g_0 & \dots & \dots & g_{n-k} & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0\\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{bmatrix} \in \mathbb{F}_2^{k \times n}$$

Encoding process: $\underline{c} = \underline{f} \cdot \mathbf{G}$

□ Parity-check matrix:

Parity-check matrix of the (n, n - 2t) RS code

Parity-check equation:

$$c(\sigma) = c(\sigma^2) = \dots = c(\sigma^{2t}) = 0 \Leftrightarrow \underline{c} \cdot \mathbf{H}^{\mathrm{T}} = \underline{\mathbf{0}}$$

BCH Codes

- Decoding of BCH codes
 - □ Hard-decision decoding (utilizing algebraic structure)



Soft-decision decoding (utilizing soft information)









Overview of OSD

• MRIPs: most reliable independent positions

Ordered Statistics Decoding

• TEPs: test error patterns

Ordered Statistics Decoding

Construct the systematic generator matrix

Channel

- Received LLR sequence: $\underline{L} = (L_0, L_1, ..., L_{n-1}) \in \mathbb{R}^n$
- Hard-decision received word: $\underline{r} = (r_0, r_1, ..., r_{n-1}) \in \mathbb{F}_2^n$
- Sort based on reliability and determine the most reliable independent positions (MRIPs) -

$$\underline{\mathbf{r}}' = \Lambda(\underline{\mathbf{r}}) = (r_{j_0}, r_{j_1}, \dots, r_{j_{n-1}}) \qquad |L_{j_0}| \ge |L_{j_1}| \ge \dots \ge |L_{j_{n-1}}|$$

Construct the systematic generator matrix G_{BCH}

$$\mathbf{G} \longrightarrow \mathbf{G}' = \Lambda(\mathbf{G}) \longrightarrow \mathbf{G}_{\mathrm{BCH}}$$



Ordered Statistics Decoding

- Generate BCH candidate codewords
 - □ Re-encoding process

Initial message:
$$\underline{f}^{(0)} = (r_{j_0}, r_{j_1}, ..., r_{j_{k-1}}) \in \mathbb{F}_2^k$$

Test error pattern: $\underline{e}^{(\omega)} = (e_{j_0}^{(\omega)}, e_{j_1}^{(\omega)}, ..., e_{j_{k-1}}^{(\omega)}) \in \mathbb{F}_2^k$ $\omega = 0, 1, ..., N_{\text{TEPs}} - 1$
Test message: $\underline{f}^{(\omega)} = (f_{j_0}^{(\omega)}, f_{j_1}^{(\omega)}, ..., f_{j_{k-1}}^{(\omega)}) \in \mathbb{F}_2^k$
BCH codeword candidate: $\underline{\hat{c}}^{(\omega)} = (\hat{c}_0^{(\omega)}, \hat{c}_1^{(\omega)}, ..., \hat{c}_{n-1}^{(\omega)}) = \Lambda^{-1}(\underline{f}^{(\omega)} \cdot \mathbf{G}_{\text{BCH}}) \in \mathbb{F}_2^n$
Number of TEPs (= number of BCH codeword candidates)
OSD with order $\tau \longrightarrow d_{\text{H}}(\underline{e}^{(\omega)}, \underline{\mathbf{0}}) \leq \tau$
 $N_{\text{TEPs}} = \binom{k}{0} + \binom{k}{1} + \dots + \binom{k}{\tau}$
Number of TEPs $\underline{e}^{(\omega)}$ s.t. $d_{\text{H}}(\underline{e}^{(\omega)}, \underline{\mathbf{0}}) = 1$



Repetitive

processing

(parallel)

12

Ordered Statistics Decoding

Challenges of OSD

- Exponential complexity
- τ -OSD complexity: $O(k^{\tau})$

- Reduction of TEPs: skipping rule; stopping rule
- Trade off with performance: multiple bases; validation rule
-) Trade off with storage: box-and-match algorithm

Decoding latency bottleneck

• GE

- Offline computed systematic generator matrices
 Only an auxiliary method
- Alternative solution? Utilize algebra of the code

BCH codes and RS codes

Subfield subcode

Given two linear codes $\mathcal{C} \subset \mathbb{F}_2^n$ and $\mathcal{C}' \subset \mathbb{F}_{2^m}^n$, if $\mathcal{C} = \mathcal{C}' \cap \mathbb{F}_2^n$, \mathcal{C} is called the subfield subcode of \mathcal{C}' over \mathbb{F}_2 .

🗆 Lemma 1

Example 1

An (n, k) *t*-error-correcting BCH code defined over \mathbb{F}_2 is a subfield subcode of an (n, k') *t*-error-correcting RS code defined over \mathbb{F}_{2^m} . i.e., $\mathcal{C}_{BCH}[n, k, 2t + 1] = \mathcal{C}_{RS}[n, k', 2t + 1] \cap \mathbb{F}_2^n$

$$\begin{cases} BCH \text{ code } d = 2t + 1 < n - k + 1 \\ RS \text{ code } d = 2t + 1 = n - k' + 1 \text{ (MDS)} \end{cases}$$

Dimension: k < k'



The (7,4) BCH code is the binary subcode of the (7,5) RS code











- Generation of G_{RS}
 - Encoding of an (n, k') RS code

Message $\underline{u} = (u_0, u_1, \dots, u_{k'-1}) \in \mathbb{F}_{2^m}^{k''}$, in poly. $u(x) = u_0 + u_1 x + \dots + u_{k'-1} x^{k'-1} \in \mathbb{F}_{2^m}[x]$ Codeword $\underline{v} = (u(\alpha_0), u(\alpha_1), \dots, u(\alpha_{n-1})) \in \mathbb{F}_{2^m}^n$ $v_0 \quad v_1 \quad \dots \quad v_{n-1}$ $\alpha_0, \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_{2^m} \setminus \{0\}$ are the code locators

Example 2 For a (7, 5) RS code over \mathbb{F}_8

Message $\underline{u} = (2, 3, 5, 0, 1)$, in poly. $u(x) = 2 + 3x + 5x^2 + x^4$

Codeword $\underline{v} = (u(1), u(2), u(4), u(3), u(6), u(7), u(5)) = (5, 0, 4, 7, 6, 1, 3)$

- \mathbb{F}_8 is an extension field of \mathbb{F}_2 , defined by $p(x) = x^3 + x + 1$
- In \mathbb{F}_8 , $\{0, \sigma^0, \sigma^1, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\} = \{0, 1, 2, 4, 3, 6, 7, 5\}$

- Generation of G_{RS}
- Determine the MRIPs

Permuted received word: $\underline{\mathbf{r}}' = \Lambda(\underline{\mathbf{r}}) = (r_{j_0}, r_{j_1}, \dots, r_{j_{n-1}}) \quad \longleftarrow \quad |L_{j_0}| \ge |L_{j_1}| \ge \dots \ge |L_{j_{n-1}}|$

Most reliable positions (MRPs):

 $\Theta^{\mathsf{c}} = \{j_{k'}, j_{k'+1}, \dots, j_{n-1}\}$

 $\Theta = \{j_0, j_1, \dots, j_{k'-1}\}$







Generation of \mathbf{G}_{RS}

Message $\underline{u} = (r_{j_0}, r_{j_1}, ..., r_{j_{k'-1}}) \in \mathbb{F}_{2^m}^{k'}$, defined by $\Theta = \{j_0, j_1, ..., j_{k'-1}\}$

Construct the Lagrange interpolation polynomials

$$T_j(x) = \prod_{j' \in \Theta, j' \neq j} \frac{x - \alpha_{j'}}{\alpha_j - \alpha_{j'}}$$

where $T_i(\alpha_i) = 1$, and $T_i(\alpha_{i'}) = 0$ if $j' \in \Theta$ and $j' \neq j$.

Form the systematic message polynomial of $\underline{u} = (r_{j_0}, r_{j_1}, ..., r_{j_{k'-1}})$ $\mathcal{H}_{\underline{u}}(x) = \sum_{i \in \Theta} r_j T_j(x)$ $\mathcal{H}_{\underline{u}}(\alpha_j)$ generates

parity-check symbols, if $i \in \Theta^c$.



Example 3

Given a (7,4) BCH code and an LLR sequence $\underline{L} = (-2.447, 5.115, -4.771, -1.349, -7.096, 0.443, -3.485)$

- \square Mother code: (7,5) RS code
- □ Hard-decision received word: $\underline{r} = (1, 0, 1, 1, 1, 0, 1)$
- □ MRPs: $\Theta = \{4, 1, 2, 6, 0\}$
- □ Lagrange interpolation polynomials:

$$T_{4}(x) = \frac{x - \alpha_{1}}{\alpha_{4} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{4} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{4} - \alpha_{6}} \cdot \frac{x - \alpha_{0}}{\alpha_{4} - \alpha_{0}} \qquad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{1} - \alpha_{4}} \cdot \frac{x - \alpha_{2}}{\alpha_{1} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{1} - \alpha_{6}} \cdot \frac{x - \alpha_{0}}{\alpha_{1} - \alpha_{0}} \qquad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{1} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{1} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{1} - \alpha_{0}} \quad T_{6}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{0}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{0}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{0}} \quad T_{1}(x) = \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot$$



Generation of G_{RS}









- Generation of G_{RS}
 - □ The row-*i* column-*j* entry of G_{RS} :

n-1

where $j \in \Theta^{c}$

$$|\Theta| = k' \qquad \qquad |\Theta^{c}| = n - k$$

□ Relationship: systematic generator matrix & systematic parity-check matrix

□ Complexity of the generation of \mathbf{G}_{RS} : $2n \cdot \min\{n - k', k'\}$



- Generation of **G**_{RS}
 - □ **Example 4** continues from **Example 3** with MRPs being $\Theta = \{4, 1, 2, 6, 0\}$

$$\begin{split} \underline{u}_{4} &= (1,0,0,0,0) \longrightarrow \mathcal{H}_{\underline{u}_{4}}(x) = \frac{x - \alpha_{1}}{\alpha_{4} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{4} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{4} - \alpha_{6}} \cdot \frac{x - \alpha_{0}}{\alpha_{4} - \alpha_{0}} \\ \underline{u}_{1} &= (0,1,0,0,0) \longrightarrow \mathcal{H}_{\underline{u}_{1}}(x) = \frac{x - \alpha_{4}}{\alpha_{1} - \alpha_{4}} \cdot \frac{x - \alpha_{2}}{\alpha_{1} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{1} - \alpha_{6}} \cdot \frac{x - \alpha_{0}}{\alpha_{1} - \alpha_{0}} \\ \underline{u}_{2} &= (0,0,1,0,0) \longrightarrow \mathcal{H}_{\underline{u}_{2}}(x) = \frac{x - \alpha_{4}}{\alpha_{2} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{1} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{2} - \alpha_{6}} \cdot \frac{x - \alpha_{0}}{\alpha_{2} - \alpha_{0}} \\ \underline{u}_{6} &= (0,0,0,1,0) \longrightarrow \mathcal{H}_{\underline{u}_{6}}(x) = \frac{x - \alpha_{4}}{\alpha_{6} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{6} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{6} - \alpha_{2}} \cdot \frac{x - \alpha_{0}}{\alpha_{6} - \alpha_{0}} \\ \underline{u}_{0} &= (0,0,0,0,1) \longrightarrow \mathcal{H}_{\underline{u}_{0}}(x) = \frac{x - \alpha_{4}}{\alpha_{0} - \alpha_{4}} \cdot \frac{x - \alpha_{1}}{\alpha_{0} - \alpha_{1}} \cdot \frac{x - \alpha_{2}}{\alpha_{0} - \alpha_{2}} \cdot \frac{x - \alpha_{6}}{\alpha_{0} - \alpha_{6}} \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{3} - \alpha_{1}}{\alpha_{4} - \alpha_{1}} \cdot \frac{\alpha_{3} - \alpha_{2}}{\alpha_{4} - \alpha_{2}} \cdot \frac{\alpha_{3} - \alpha_{0}}{\alpha_{4} - \alpha_{6}} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{3}(\alpha_{3} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{4}(\alpha_{4} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{3}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{4}(\alpha_{4} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{4}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{4}(\alpha_{4} - \alpha_{5})} = 5 \\ \mathcal{H}_{\underline{u}_{4}}(\alpha_{4}) &= \frac{\alpha_{4}(\alpha_{4} - \alpha_{5})}{\alpha_{4}(\alpha_{4}$$



- Generation of BCH codeword candidates
 - □ Generate the initial codeword:

Initial message: $\underline{\boldsymbol{u}} = (r_{j_0}, r_{j_1}, \dots, r_{j_{k'-1}}) \in \mathbb{F}_2^{k'}$ Initial RS codeword: $\underline{\widehat{\boldsymbol{v}}}^{(0)} = (\widehat{\boldsymbol{v}}_0^{(0)}, \widehat{\boldsymbol{v}}_1^{(0)}, \dots, \widehat{\boldsymbol{v}}_{n-1}^{(0)}) = \underline{\boldsymbol{u}} \cdot \mathbf{G}_{\mathrm{RS}}$ $\widehat{\boldsymbol{v}}_j^{(0)} = r_j, \forall j \in \Theta$

□ Generate any (n, k') systematic RS codeword:

The ω -th test error pattern: $\underline{e}'^{(\omega)} = (e'_{j_0}^{(\omega)}, e'_{j_1}^{(\omega)}, \dots, e'_{j_{k'-1}}^{(\omega)}) \in \mathbb{F}_2^{k'}$ The ω -th test message: $\underline{u}^{(\omega)} = \underline{u} + \underline{e}'^{(\omega)}$ The ω -th systematic RS codeword: $\underline{\widehat{v}}^{(\omega)} = (\widehat{v}_0^{(\omega)}, \widehat{v}_1^{(\omega)}, \dots, \widehat{v}_{n-1}^{(\omega)}) \in \mathbb{F}_{2^m}^n$ $\widehat{v}^{(\omega)} = (\omega) - \widehat{v}^{(\omega)} = \widehat{v}^{(0)} + \widehat{v}^{(\omega)} - \widehat{v}^{(0)}$

$$\underline{\widehat{\boldsymbol{v}}}^{(\omega)} = \underline{\boldsymbol{u}}^{(\omega)} \cdot \mathbf{G}_{\mathrm{RS}} = \underline{\widehat{\boldsymbol{v}}}^{(0)} + \underline{\boldsymbol{e}'}^{(\omega)} \cdot \mathbf{G}_{\mathrm{RS}}$$



- Generation of BCH codeword candidates
 - Theorem 2 (Identify invalid TEPs)

If $\hat{v}_{j}^{(0)} + \sum_{i \in \Theta, e_{i}^{\prime(\omega)} \neq 0} \mathcal{H}_{\underline{u}_{i}}(\alpha_{j}) \in \{0,1\}, \forall j \in \Theta^{c}, \ \underline{\hat{v}}^{(\omega)}$ is a BCH codeword.





Parallel



OSD

The optimal

codeword

LLOSD

Parallel

Complexity comparison of LLOSD and OSD

Algorithms	Operations	Complexity
OSD (τ)	GE	$n \cdot (\min\{n-k,k\})^2$
	Compute $\hat{\underline{c}}^{(0)}$	$k \cdot (n-k)$
	Compute $\hat{\underline{c}}^{(\omega)}$	$(n-k)\cdot\sum_{\lambda=1}^{\tau}\lambda\binom{k}{\lambda}$
	Find $\hat{\underline{c}}_{opt}$	$n \cdot \sum_{\lambda=0}^{\tau} \binom{k}{\lambda}$
LLOSD (τ)	Compute G _{RS}	$2n \cdot \min\{n-k',k'\}$
	Compute $\underline{\widehat{v}}^{(0)}$	$k' \cdot (n-k')$
	Compute $\underline{\hat{c}}^{(\omega)}$	$\sum_{\lambda=1}^{\tau} \binom{k}{\lambda} + \tau \sum_{j'=1}^{n-k'} N_{j'}$
	Find $\hat{\underline{v}}_{opt}$	$nN_{n-k'}$



Key differences

Operation type : binary \rightarrow finite field

Compute $\mathbf{G}_{\mathrm{BCH}} / \mathbf{G}_{\mathrm{RS}} : O(n^3) \rightarrow O(n^2)$

sequential \rightarrow parallel

Candidate list : $\sum_{\lambda=0}^{\tau} \binom{k}{\lambda} \rightarrow N_{n-k'} = N_{\text{BCH}}$

 $N_{j'}$ is the number of TEPs that yield binary symbols after the j' th judgement as in **Theorem 2**.



Performance of the (63, 45) BCH code, AWGN, BPSK



[2] T. Kaneko et al., "An efficient maximum-likelihood-decoding algorithm for linear block codes with algebraic decoder," IEEE Trans. Inf. Theory, vol. 40, no. 2, pp. 320-327, 1994.



 Re-encoding complexity distribution: LLOSD (3) of the (63,45) BCH code with ML criterion, SNR = 5.0 dB



- Colors are used to distinguish the phases that the re-encoding terminates at
- Phase (i): the re-encoding phase for weight-i TEPs

Terminate at	Ratio	Ave. #Additions
Phase (0)	87.89%	171
Phase (1)	9.22%	181
Phase (2)	0.18%	273
Phase (3)	2.71%	94,216

Reasons for Multiple Peaks

For the re-encoding phase of TEPs with a larger weight

- The complexity is **greater**
- The ML criterion is more difficult to satisfy
- The probability of finding a BCH codeword is **lower**

- Segmented variation of LLOSD
 - Analysis
 - The error probability of the LLOSD is upper bounded by

 $P_{e,LLOSD}(\tau) \le P_{e,ML} + P_{list}(\tau)$

• $P_{e,ML}$: ML decoding error probability,

depends on the weight distribution of the code

• $P_{\text{list}}(\tau)$: List decoding error probability,

= Prob{the channel introduces more than τ errors in MRPs}





- Segmented variation of LLOSD
 - For OSD

If $\tau \ge \min\left\{ \left[\frac{d}{4} - 1 \right], k \right\} \rightarrow$ The list error probability of OSD: $P_{\text{list}}(\tau) \ll P_{\text{e,ML}}$

→ The OSD can produce ~ ML decoding performance

- We only need the decoding order of τ for the MRIPs



TEPs:
$$\underline{e}^{\prime(\omega)} = (\underbrace{e_{j_{0}}^{\prime(\omega)}, e_{j_{1}}^{\prime(\omega)}, \dots, e_{j_{k-1}}^{\prime(\omega)}, e_{j_{k}}^{\prime(\omega)}, e_{j_{k+1}}^{\prime(\omega)}, \dots, e_{j_{k'-1}}^{\prime(\omega)})}_{\tau_{1}} = \min\left\{ \begin{bmatrix} \frac{d}{4} - 1 \end{bmatrix}, k \right\} \text{ is sufficient extra order } \tau_{2}$$
Number of TEPs N_{TEPs} :
$$\sum_{i=0}^{\tau} \binom{k'}{i} \rightarrow \sum_{i_{1}=0}^{\tau_{1}} \binom{k}{i_{1}} \cdot \sum_{i_{2}=0}^{\tau_{2}} \binom{k'-k}{i_{2}}$$









Performance of the (63, 45) BCH code, AWGN, BPSK



Complexity and latency comparison

Algorithms	SNR	Complexity		Latency	
Aigoritims	(dB)	$\mathbb{F}_2/\mathbb{F}_{64}$ oper.	Floating oper.	(μs)	
	4	2.78×10^4	81	6.58×10^2	
OSD (1)	5	2.60×10^4	19	5.34×10^2	
	6	2.56×10^4	8	5.06×10^2	
	4	1.81×10^4	15	1.99×10^3	
LLOSD (3)	5	5.21×10^3	8	4.36×10^2	
	6	2.58×10^3	7	1.32×10^2	
Seg. LLOSD (1 45, 3)	4	3.69×10^3	8	2.71×10^2	
	5	2.64×10^3	7	1.44×10^2	
	6	2.45×10^3	7	1.17×10^2	

Simulation environment: Intel core i7-10710U CPU Stopping rule: ML criterion

Low-Latency OSD
• Concatenated perspective
• Systematic parity-check matrix
$$C_{RS}[n, k']$$
 Systematic generator matrix $\Lambda(H_{RS}) = [P - I_{n-k'}]$ $\Gamma_{RS}[n, k']$ Systematic generator matrix $\Lambda(H_{RS}) = [P - I_{n-k'}]$
• $F_{2^m} \cong F_2^m$
2. Row permutation
• $\Lambda(H_{BCH}) = \begin{bmatrix} p^{(0)} - I_{n-k'} \\ p^{(1)} \\ p^{(m-1)} \\ 0 \end{bmatrix} (over F_2) + \begin{bmatrix} P^{(0)} - I_{n-k'} \\ p^{*} \\ p^{*$

Concatenated perspective

• Example 6

$$\mathbf{H}_{\mathrm{RS}} = \begin{bmatrix} \sigma^{3} & 1 & \sigma^{3} & \sigma & \sigma & 1 & 0 \\ \sigma^{4} & 1 & \sigma^{5} & \sigma^{5} & \sigma^{4} & 0 & 1 \end{bmatrix} \xrightarrow{\mathbb{F}_{2}m \cong \mathbb{F}_{2}^{m}} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{\mathrm{row \, perm.}} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} = \mathbf{H}_{\mathrm{BCH}}$$

(1) $\underline{u}^{(\omega)} = (1, 0, 1, 1, 0): \underline{u}^{(\omega)} \cdot \mathbf{P}^{*T} = (1, 1, 0, 1)$

(2)
$$\underline{u}^{(\omega)} = (1, 0, 1, 0, 0): \underline{u}^{(\omega)} \cdot \mathbf{P}^{*^{\mathrm{T}}} = \underline{\mathbf{0}} \longrightarrow \begin{cases} \hat{c}_{5}^{(\omega)} = \underline{u}^{(\omega)} \cdot (1, 1, 1, 0, 0)^{\mathrm{T}} = 0\\ \hat{c}_{6}^{(\omega)} = \underline{u}^{(\omega)} \cdot (0, 1, 1, 1, 0)^{\mathrm{T}} = 1 \end{cases} \Longrightarrow \underline{\hat{c}}^{(\omega)} = (1, 0, 1, 1, 0, 0, 1)$$



- Concatenated perspective
 - □ For LLOSD (τ)
 - N_{TEPs} : number of TEPs

 $N_{\rm BCH}$: number of BCH codeword candidates:

□ Theorem 3

If the channel condition is sufficiently good (SNR $\rightarrow \infty$)

$$\Rightarrow N_{\rm BCH} = \sum_{i=0}^{\tau} A_i$$

 A_i : number of weight-*i* codewords in $C_{BCH}^{\Theta^c}[k',k]$

- The set of punctured positions Θ^c varies for each decoding event, and A_i varies accordingly
- In general

$$\sum_{i=0}^{\tau} A_i \ll \sum_{i=0}^{\tau} \binom{k'}{i}$$







- Concatenated perspective
 - □ The number of BCH codeword candidates N_{BCH} in decoding the C_{BCH} [63, 45] and C_{BCH} [31, 21]





• The average number of BCH codeword candidates in LLOSD (3) of the (63,45) BCH code

TEP weight	#Meight_i TEPs	N _{BCH}		
		SNR = 2dB	4dB	6dB
0	1	0.14	0.65	0.97
1	57	0.27	0.27	0.03
2	1,569	0.56	0.20	0.07
3	29,260	7.10	4.97	3.97

- Remarks
 - The probability of finding a BCH codeword decreases as the TEP weight increases
 - As the SNR increases, the likelihood of generating a BCH codeword using a weight-0 TEP increases, while the likelihood decreases when using a TEP of a larger weight

- LLOSD vs. Chase BM / GS
 - □ It remains challenging to decode longer BCH codes with LLOSD







Integrating LLOSD and Chase-GS decoding



Advantages

- LLOSD output list can be utilized
- Computation sharing
- Low complexity root-finding



Integrating LLOSD and Chase-GS decoding



- Key steps of HSD
 - Test-vector formulation

 $j_{n-\eta} | j_{n-\eta+1}$ $J_{k'-1}$ $J_{k'}$ J_{n-1} Jo J_1 ••• $\Psi = \{ j_{n-\eta}, j_{n-\eta+1}, \dots, j_{n-1} \}: \eta$ least reliable positions (LRPs) Θ (MRPs) ΘC The 2^{η} test-vectors can be formulated as 00...000 00...001 $\Lambda(\underline{\boldsymbol{r}}_{\omega}) = (r_{j_0}, r_{j_1}, \dots, r_{j_{n-\eta-1}}, r_{j_{n-\eta}}^{(\omega)}, \dots, r_{j_{n-1}}^{(\omega)})$ 00...010 $0 \le \omega \le 2^{\eta} - 1$ 00...011 11...110 11...111 \underline{r}_{ω} Skipping (based on candidate list)

If $d_{\rm H}(\hat{\boldsymbol{v}}, \underline{\boldsymbol{r}}_{\omega}) \leq t$, $\underline{\boldsymbol{r}}_{\omega}$ will be decoded as $\hat{\boldsymbol{v}} \longrightarrow \underline{\boldsymbol{r}}_{\omega}$ can be skipped



 Ψ (LRPs)





- Key steps of HSD
 - Re-encoding transform (based on the initial RS codeword)

Initial RS codeword (from LLOSD): $\underline{\hat{v}}^{(0)} = \underline{u} \cdot \mathbf{G}_{RS} \in \mathbb{F}_{2^m}^n$

Transformed test vector: $\underline{z}_{\omega} = \underline{r}_{\omega} - \underline{\hat{\nu}}^{(0)} \longrightarrow \Lambda(\underline{z}_{\omega}) = (0, 0, ..., 0, z_{j_{k'}}^{(\omega)}, ..., z_{j_{n-1}}^{(\omega)})$

Finding a Gröbner basis of the interpolation module

$$\mathcal{M}_{\omega} = \{ Q \in \mathbb{F}_{2^{m}}[x, y] \mid \deg_{y} Q \leq 1; Q\left(\alpha_{j}, z_{j}^{(\omega)} / V(\alpha_{j})\right) = 0, \forall j \in \Theta^{c} \}$$

Interpolation — module basis construction (based on the Lagrange polynomials)

Interpolation points:

$$(\alpha_{j_0}, 0), (\alpha_{j_1}, 0), \dots, (\alpha_{j_{k'-1}}, 0), (\alpha_{j_{k'}}, \frac{z_{j_{k'}}^{(\omega)}}{V(\alpha_{j_{k'}})}) \dots, (\alpha_{j_{n-1}}, \frac{z_{j_{n-1}}^{(\omega)}}{V(\alpha_{j_{n-1}})})$$
Interpolated by $V(x) = \prod_{j \in \Theta} (x - \alpha_j)$ Lagrange interpolation

- Key steps of HSD
 - Interpolation module basis construction (based on the Lagrange polynomials)
 - Seed polynomials:

$$\mathcal{G}(x) = \prod_{j \in \Theta^{\mathsf{c}}} (x - \alpha_j) \quad \& \quad R_{\omega}(x) = \sum_{j \in \Theta^{\mathsf{c}}} z_j^{(\omega)} T_j'(x)$$

For \underline{r}_{ω} (\underline{z}_{ω}), module \mathcal{M}_{ω} can be generated by

$$T'_{j}(x) = \frac{\prod_{j' \in \Theta^{c}, j' \neq j} (x - \alpha_{j'})}{\prod_{j'=0, j' \neq j}^{n-1} (\alpha_{j} - \alpha_{j'})}$$

Computed in generating **G**_{RS}

$$\begin{cases} P_{\omega,0}(x,y) = \mathcal{G}(x) & \text{Basis reduction} \\ P_{\omega,1}(x,y) = y - R_{\omega}(x) & \text{The Gröbner basis of } \mathcal{M}_{\omega} \\ & \text{The interpolation polynomial} \\ Q_{\omega}(x,y) = V(x)Q_{\omega}^{*^{(0)}}(x) + Q_{\omega}^{*^{(1)}}(x)y \end{cases}$$



- Key steps of HSD
 - Root-finding

Estimated message polynomial: $\hat{u}_{\omega}(x) = \frac{V(x)Q_{\omega}^{*^{(0)}}(x)}{Q_{\omega}^{*^{(1)}}(x)}$

Lemma 4

The evaluation values of polynomial $\hat{u}_{\omega}(x)$ over MRPs form a TEP of the LLOSD, i.e.,

$$\underline{\hat{\boldsymbol{e}}}_{\omega} = (\hat{\boldsymbol{u}}_{\omega}(\alpha_{j_0}), \hat{\boldsymbol{u}}_{\omega}(\alpha_{j_1}), \dots, \hat{\boldsymbol{u}}_{\omega}(\alpha_{j_{k'-1}}))$$

Codeword candidate of LLOSD: $\underline{\hat{\boldsymbol{v}}}^{(\omega)} = \underline{\boldsymbol{e}'}^{(\omega)} \cdot \mathbf{G}_{RS} + \underline{\hat{\boldsymbol{v}}}^{(0)}$

Codeword candidate of Chase-GS: $\underline{\widehat{v}}_{\omega} = (\widehat{u}_{\omega}(\alpha_0), \widehat{u}_{\omega}(\alpha_1), \dots, \widehat{u}_{\omega}(\alpha_{n-1})) + \underline{\widehat{v}}^{(0)}$

$$= \left(\hat{u}_{\omega}(\alpha_{j_0}), \hat{u}_{\omega}(\alpha_{j_1}), \dots, \hat{u}_{\omega}(\alpha_{j_{k'-1}}) \right) \cdot \mathbf{G}_{\mathrm{RS}} + \underline{\widehat{\nu}}^{(0)}$$
$$= \underline{\widehat{e}}_{\omega} \cdot \mathbf{G}_{\mathrm{RS}} + \underline{\widehat{\nu}}^{(0)}$$



- Key steps of HSD
 - \Box Partial root-finding (based on G_{RS})

The estimated TEP $\underline{\hat{e}}_{\omega} = (\hat{u}_{\omega}(\alpha_{j_0}), \hat{u}_{\omega}(\alpha_{j_1}), \dots, \hat{u}_{\omega}(\alpha_{j_{k'-1}}))$ can be determined as

$$\hat{u}_{\omega}(\alpha_{j}) = \begin{cases} 1, & \text{if } Q_{\omega}^{*^{(1)}}(\alpha_{j}) = 0 \\ & \forall j \in \Theta \\ 0, & \text{otherwise} \end{cases}$$

The estimated codeword
$$\underline{\widehat{v}}_{\omega}$$
 can be generated as

$$\underline{\widehat{v}}_{\omega} = (\widehat{u}_{\omega}(\alpha_{j_0}), \widehat{u}_{\omega}(\alpha_{j_1}), \dots, \widehat{u}_{\omega}(\alpha_{j_{k'-1}})) \cdot \mathbf{G}_{\mathrm{RS}} + \underline{\widehat{v}}^{(0)} = \underbrace{\underline{\widehat{e}}_{\omega}}_{\mathrm{LLOSD}} \cdot \mathbf{G}_{\mathrm{RS}} + \underline{\widehat{v}}^{(0)}$$



Performance of the (63, 39) BCH code





PLCC decoding is the progressive variant of the Chase-GS