ulm university universität uulm

On Soft Decision Decoding of Block Codes

Martin Bossert

Institute of Communications Engineering, Ulm University

Coding and Skiing,
March 2019

Definition BCH Codes

Let α be a primitive element of the Field $\mathbb{F}_q$ with $q = 2^m$ and $\mathbb{F}_q[x]/(x^n - 1)$ the ring of polynomials with $n = q - 1$.

Generator Polynomial of $\mathcal{C}$

$\mathcal{M}$ is union of cyclotomic cosets $\mod n$, minimum distance d if $d - 1$ consecutive numbers in $\mathcal{M}$, dimension $k = n - |\mathcal{M}|$, Generatorpolynomial:

$$g(x) = \prod_{j=\mathcal{M}} (x - \alpha^{-j})$$

Dual Code $\mathcal{C}^\perp$

The dual code is also a BCH code with generator polynomial

$$h(x) = \frac{x^n - 1}{g(x)} \quad \text{(parity check polynomial)}$$

Properties for Decoding

Cyclic Convolution

For all $c(x) \in \mathcal{C}$ and all $b(x) \in \mathcal{C}^{\perp}$

$$c(x)b(x) = 0 \mod (x^n - 1)$$

Error: $\varepsilon(x) = x^{e_1} + x^{e_2} + \ldots + x^{e_\tau}$
Received: $r(x) = c(x) + \varepsilon(x)$

Syndrome

$$w(x) = r(x)b(x) = c(x)b(x) + \varepsilon(x)b(x) = \varepsilon(x)b(x) \mod (x^n - 1)$$

Minimal Weight Codeword ($d^{\perp}$), $b_1 = 0$

$$b(x) \in \mathcal{C}^{\perp},\ b(x) = x^{b_1} + x^{b_2} + \ldots + x^{b_{d^{\perp}}}$$

Interpretation of Syndrome

With the choice $b_1 = 0$

$$\begin{aligned} w(x) &= x^{b_1}\varepsilon(x) + x^{b_2}\varepsilon(x) \ldots + x^{b_{d^\perp}}\varepsilon(x) \mod (x^n - 1) \\ &= x^{e_1} + x^{e_2} + \ldots + x^{e_\tau} + \\ &\quad x^{e_1+b_2} + x^{e_2+b_2} + \ldots + x^{e_\tau+b_2} + \\ &\vdots \\ &\quad x^{e_1+b_{d^\perp}} + x^{e_2+b_{d^\perp}} + \ldots + x^{e_\tau+b_{d^\perp}}, \end{aligned}$$

!! All nonzero coefficients of $w(x)$ are errors or shifted errors !!

Use the $d^\perp$ Shifts

$$x^{b_j} w(x) \mod (x^n - 1), \text{ with } b_j \in \{0, -b_2, -b_3, \ldots, -b_{d^\perp}\}$$

Example: Code $\mathcal{C}(15,4,8)$ and $\mathcal{C}^{\perp}(15,11,3)$

Polynomials: $b^{[1]}(x) = x^4 + x + 1$ and $b^{[2]}(x) = x^{10} + x^5 + 1$

Syndromes for $\varepsilon(x) = x^6 + x^{12} + x^{13}$

$w^{[1]}(x) = x + x^2 + x^6 + x^7 + x^{10} + x^{12} + x^{14}$
$w^{[2]}(x) = x + x^2 + x^3 + x^6 + x^7 + x^{11} + x^{12} + x^{13}$

$w^{[1]} =$	0	1	1	0	0	0	1	1	0	0	1	0	1	0	1
$x^{-1}w^{[1]} =$	1	1	0	0	0	1	1	0	0	1	0	1	0	1	0
$x^{-4}w^{[1]} =$	0	0	1	1	0	0	1	0	1	0	1	0	1	1	0
$w^{[2]} =$	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0
$x^{-5}w^{[2]} =$	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0
$x^{-10}w^{[2]} =$	0	1	1	1	0	0	1	1	1	0	0	1	1	1	0
$\Phi =$	1	5	5	4	0	1	6	4	4	1	2	4	5	5	1

Shift-Sum Decoding Concept

Use L polynomials $b^{[\ell]}(x), \ell = 1, \dots, L$ of weight $d^{\perp}$. Count the number of ones in the $d^{\perp}$ shifts of each $w^{[\ell]}(x)$

Frequency of Occurrence

$$\Phi = \sum_{\ell=1}^{L} \sum_{j \in \sup b^{[\ell]}(x)}^{\notin \mathbb{F}_2} (x^{-j} w^{[\ell]}(x)) \mod (x^n - 1).$$

$0 \leq \Phi_i \leq L \cdot d^{\perp}$.

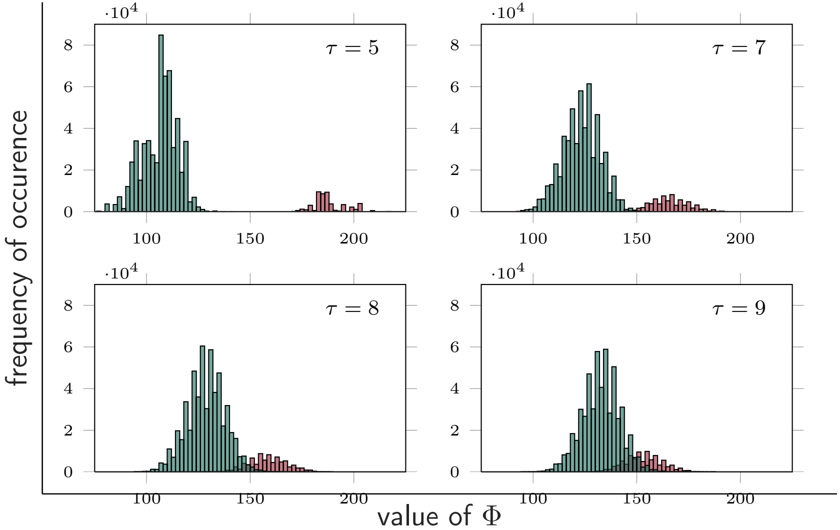
Expected number of ones at error positions per shift: $\frac{\mathrm{wt} w(x)}{d^{\perp}}$

Probability that error position is one: $\frac{\mathrm{wt} w(x)}{\tau d^{\perp}}$

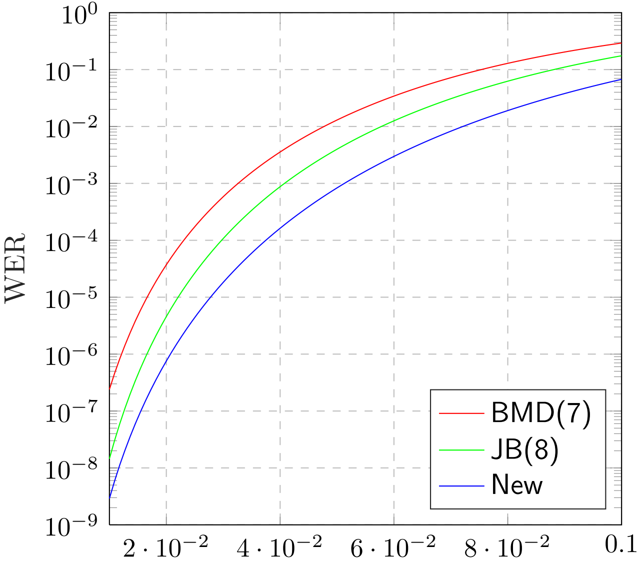
Expected value at error: $E[\Phi_e(\tau)] = \frac{\mathrm{wt} w(x)}{\tau} L$.

Expected value at non-error: $E[\Phi_c(\tau)] = \frac{d^{\perp}(\mathrm{wt} w(x) - \frac{\mathrm{wt} w(x)}{d^{\perp}})}{n-\tau} L$.

Overview of the Statistics of Φ



Results Hard (BSC) BCH(63,24,15)



Soft Decision Decoding

AWGN and BPSK

$$x_i = (-1)^{c_i}, c_i \in \mathbb{F}_2$$

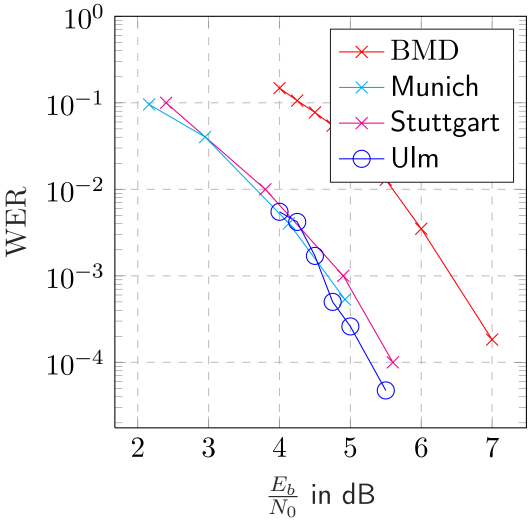
$$y_i = x_i + n_i, n_i \in \mathcal{N}(0, \sigma^2)$$

Decoding Algorithm

$$\Phi_i^s = \Phi_i + \min\{\lceil \frac{T_1}{|y_i|} \rceil, T_2\}$$

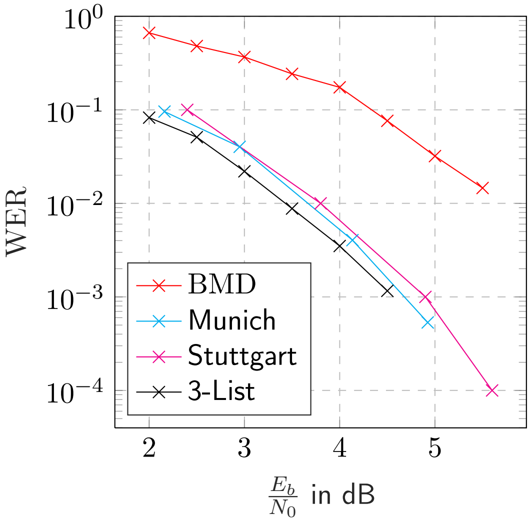
T_1 and T_2 are code dependent integers

Results Soft BCH vs. Polar 64, $R = .5$



Sources: http://webdemo.inue.uni-stuttgart.de
http://pretty-good-codes.org/polar.html

Results Soft List 3 Infoset Φ, $|y_i|$ and best of



Sources: http://webdemo.inue.uni-stuttgart.de
http://pretty-good-codes.org/polar.html

The Plotkin Construction for $\mathbb{F}_2$

Given $\mathcal{C}^{(1)}(n, k_1, d_1)$ and $\mathcal{C}^{(2)}(n, k_2, d_2)$ both $\subset \mathbb{F}_2^n$

$$\mathcal{C}(2n, k_1 + k_2, \min\{2d_1, d_2\}) = \{c = (c^{(1)} | c^{(1)} + c^{(2)}), c^{(i)} \in \mathcal{C}^{(i)}\}$$

The length $2n$ and the dimension $k = k_1 + k_2$ are obvious.
Possible decoder of $\mathcal{C}$:
BSC $r = c + e = (c^{(1)} + e^{(1)} | c^{(1)} + c^{(2)} + e^{(2)})$.
Addition: $c^{(1)} + e^{(1)} + c^{(1)} + c^{(2)} + e^{(2)} = c^{(2)} + e^{(1)} + e^{(2)}$.
Since $\mathrm{wt}(e) \geq \mathrm{wt}(e^{(1)} + e^{(2)})$: $c^{(2)}$ correct if $\tau = \mathrm{wt}(e) \leq \frac{d^{(2)}-1}{2}$
Known: $c^{(1)} + e^{(1)}$ add $c^{(2)}$: $c^{(1)} + e^{(2)}$
$d^{(1)} - 1$ errors in both halfs: either $c^{(1)} + e^{(1)}$ or $c^{(1)} + e^{(2)}$ contains $\leq \frac{d^{(1)}-1}{2}$ errors

M. Plotkin, Binary codes with specific minimum distances , IEEE Trans. on Inf. Theory, vol. 6, pp. 445-450, 1960.

The Plotkin Construction for BPSK: $\{1, -1\}$

NACHRICHTENTECHNIK Algebraic Coding

Define: $x^{(1)} \odot x^{(2)} = (x_0^{(1)} x_0^{(2)}, x_1^{(1)} x_1^{(2)}, \ldots, x_{n-1}^{(1)} x_{n-1}^{(2)})$

Operation $x_i = (-1)^{c_i}$

$$\{c = (c^{(1)} | c^{(1)} + c^{(2)})\} \Longleftrightarrow \{x = (x^{(1)} | x^{(1)} \odot x^{(2)})\}$$

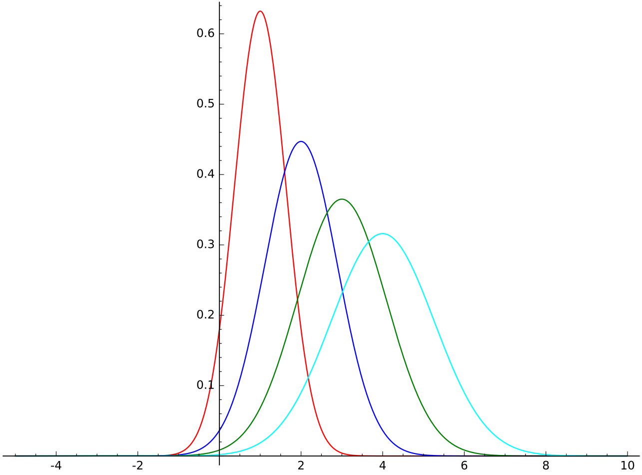
AWGN $y = x + n = (y^{(1)} | y^{(2)}) = (x^{(1)} + n^{(1)} | x^{(1)} \odot x^{(2)} + n^{(2)})$.
Add: $\hat{y}^{(2)} = y^{(1)} \odot y^{(2)}$ or $\hat{y}_i^{(2)} = \text{sign}(y_i^{(1)} y_i^{(2)}) \min\{|y_i^{(1)}|, |y_i^{(2)}|\}$
Soft decoding of $\hat{y}^{(2)}$ gives $x^{(2)}$ (assume correct)

Gain 3 dB

$$y^{(1)} + y^{(2)} \odot x^{(2)} = x^{(1)} + n^{(1)} + x^{(1)} + n^{(2)}$$

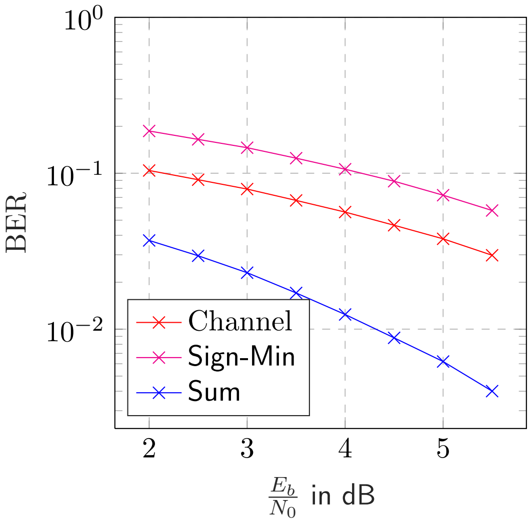
Proof: $x^{(1)} + n^{(1)}$ and $x^{(1)} + n^{(2)} \in \mathcal{N}(1, \sigma^2)$ or $\in \mathcal{N}(-1, \sigma^2)$
Sum is $\in \mathcal{N}(\pm 2, 2\sigma^2)$, Signal power: 4, Noise variance: 2 $\longrightarrow$ 3 dB

Distributions of $\mathcal{N}(a, a\sigma^2)$, $a = 1, 2, 3, 4$



Gaussian Channel BER for Plotkin Construction

NACHRICHTENTECHNIK Algebraic Coding



Literature for 3 dB gain

IEEE IT Paper, Gottfried Schnabl and Martin Bossert, 1995

$y^{(1)} + y^{(2)} \odot x^{(2)}$ used for decoding PC code in GMC decoder for RM codes

Schritt 2b, p. 418 in Bossert, Kanalcodierung, BG Teubner, 2. Auflage 1998

Step 2b, p. 376 in Bossert, Channel Coding for Telcommunications, Wiley, 1999

Dissertation (in German), Norbert Stolte, 2002

Rekursive Codes mit der Plotkin-Konstruction und ihre Decodierung

Equivalent channel SNR, $SNR_u = 2SNR_v$ sections 3.2.3 and 3.2.4, recursive Plotkin, OCBM (=polar) Fig. 3.11, p. 29

IEEE IT Paper, Erdal Arikan, 2009

Capacity based analysis, novel result: asymptotic capacity achieving.

Examples for Plotkin Construction with BCH

$\mathcal{C}^{(1)} = BCH(63,45,7)$ and $\mathcal{C}^{(2)} = BCH(63,18,21)$

$$\mathcal{C}(126,63,14)$$

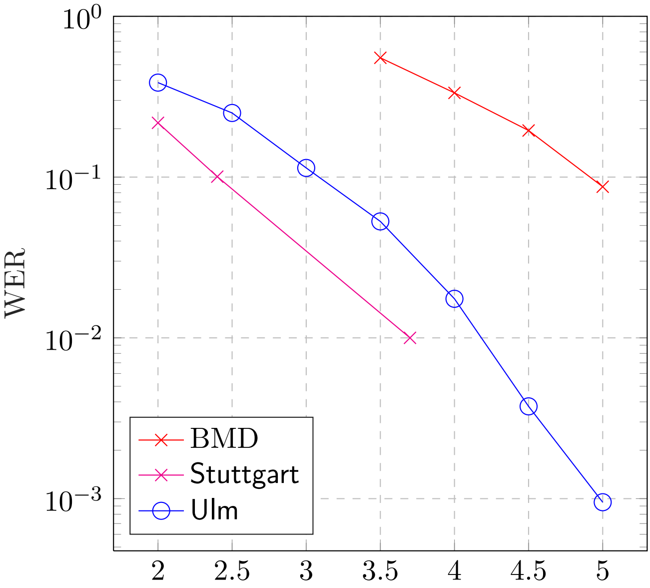
Soft decoding of $BCH(63,18,21)$ with 45 polys of wt=7
GMD Decoding of $BCH(63,45,7)$

$\mathcal{C}^{(1)} = BCH(63,39,9)$ and $\mathcal{C}^{(2)} = BCH(63,24,15)$

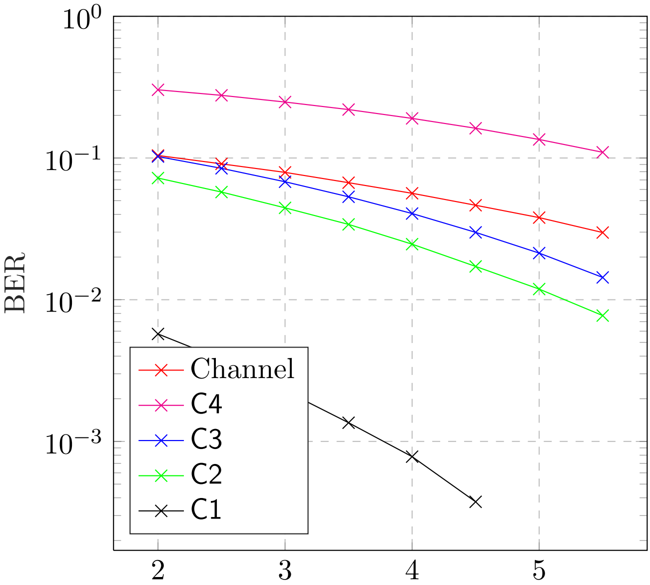
$$\mathcal{C}(126,63,15)$$

Soft decoding of $BCH(63,24,15)$ with 35 polys of wt=8
GMD Decoding of $BCH(63,39,9)$

WER for Plotkin Construction



AWGN BER for Double Plotkin Construction



Conclusions

Results are not so bad that one should stop investigations!

Many Open Problems

- Information Set Decoding (seems better)
- Dorsch Algoritm for Information Set Decoding
- Reliabiltiy Information (soft out decoding) for BSC; further usage?
- Usage of Reliability Information from Channel
- Further Examples for longer Codes
- Quadratic Residue (QR) Codes
- q-ary Codes
- .....

More check equations vs. iterations (multiple usage of few check equations)

Jim Massey's History of Channel Coding

Experts opinions

In the 50th and 60th

Coding is dead! All interesting problems are already solved.

In the 70th

Coding is dead as a doornail, except on the deep-space channel.

In the 80th Jahren

Coding is quite dead, except on wideband channels such as the deep-space channel and narrowband channels such as the telephone channel.

In the 90th Jahren

Coding is truly dead, except on single sender channels.