

INFORMATION THEORY AND CHANNEL CODING LECTURE 8

- **BCH codes**
 - BCH codes: MWS7 (not MWS7.7), MWS9.1–5
 - Decoding BCH codes: MWS9.6, (MWS9.7)
- **Reed-Solomon codes**
 - RS codes: MWS10, selected parts

BCH CODES

- *Definition:* Consider a cyclic code \mathcal{C} of length n over $\text{GF}(q)$, let m be the smallest integer such that $n|q^m - 1$ and let $\alpha \in \text{GF}(q^m)$ be a primitive n th root of unity. Then \mathcal{C} is a *BCH code of designed distance δ* if for some $b \geq 0$ it has generator polynomial

$$g(x) = \text{lcm} \{p^{(b)}(x)p^{(b+1)}(x)p^{(b+\delta-2)}(x)\}$$

- A BCH code is said to be
 - * *narrow sense* if $b = 1$
 - * *primitive* if $n = q^m - 1$ ($\implies \alpha$ primitive in $\text{GF}(q^m)$)
- *Theorem:* A BCH code over $\text{GF}(q)$ of length n and designed distance δ has $d_{\min} \geq \delta$ and dimension $k \geq n - m(\delta - 1)$.
 - For $q = 2$, $b = 1$ and $\delta = 2t + 1$, it holds that $k \geq n - mt$.

THE BCH BOUND

- *Theorem:* Let \mathcal{C} be cyclic of length n with generator polynomial $g(x)$ over $\text{GF}(q)$. Let m be the smallest integer such that $n|q^m - 1$ and let $\alpha \in \text{GF}(q^m)$ be a primitive n th root of unity. Then, if for some integers $b \geq 0$ and $\delta \geq 2$ all the elements

$$\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$$

in $\text{GF}(q^m)$ are zeros of the code, it holds that $d_{\min} \geq \delta$.

$$\delta - 1 \text{ consecutive zeros} \implies d_{\min} \geq \delta$$

FURTHER RELATIONS BETWEEN CODE PARAMETERS

- *True minimum distance d_{\min} :* A BCH code \mathcal{C} ;
 - For $q = 2$, $b = 1$, $n = 2^m - 1$ and $\delta = 2t + 1$ the code has $d_{\min} = 2t + 1$ if

$$\sum_{i=0}^{t+1} \binom{n}{i} > 2^{mt}$$

- If $b = 1$ and $n = \delta p$ for some p , then $d_{\min} = \delta$
- If $b = 1$, $n = q^m - 1$ and $\delta = q^p - 1$ for some p then, $d_{\min} = \delta$
- If $n = q^m - 1$ then $d_{\min} \leq q\delta - 1$

- *Dimension k*: A BCH code \mathcal{C} ;
 - For $q = 2$, $b = 1$, $n = 2^m - 1$ and $\delta = 2t + 1$, with $2t - 1 < 2^{\lceil m/2 \rceil} + 1$, it holds that $k = 2^m - 1 - mt$
 - $n - k$ (degree of $g(x)$) is the number of i 's in the range $1 \leq i \leq q^m - 1$ such that some cyclic shift of the q -ary expansion of i is $\leq \delta - 1$
 - For $b = 1$, $n = q^m - 1$ and if $\delta = q^p$ for some p it holds that

$$k \leq \sum_{i=0}^s a_i \rho_i^m$$

with $s = m - p$ where a_0, \dots, a_s and ρ_0, \dots, ρ_s depend on s but not on m . Also $|\delta_i| < q$.

BCH CODES CANNOT ACHIEVE CAPACITY

- *Theorem*: There does not exist a sequence of $[n, k, d]$ primitive BCH codes over $\text{GF}(q)$ with both d/n and k/n bounded away from zero as $n \rightarrow \infty$.

EXAMPLES

- *Binary Hamming code*: Narrow sense and primitive binary BCH code with $n = 2^m - 1$, for some $m \geq 1$, and $g(x)$ = a primitive polynomial in $\text{GF}(2^m)$. Designed distance $\delta = 3 = \text{true } d_{\min}$
- *Hamming code over $\text{GF}(q)$* : A narrow sense and primitive BCH code, with m smallest integer such that $n|q^m - 1$, m and $q - 1$ relatively prime, and $g(x)$ = primitive polynomial in $\text{GF}(q^m)$. Designed distance $\delta = 3 = \text{true } d_{\min}$
- *Narrow sense and primitive binary BCH code with $\delta = 5$* : Let $n = 2^m - 1$ and α primitive in $\text{GF}(2^m)$. With $g(x) = p^{(1)}(x)p^{(3)}(x)$ we get $\delta = 5$. E.g., $n = 15 \implies$

$$g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$$

For this code, $n = 3 \cdot 5 \implies d_{\min} = \delta = 5$.

DECODING (BINARY) BCH CODES

- Let \mathcal{C} be a narrow-sense (and primitive) $[n, k, d]$ BCH code over $\text{GF}(2)$ of designed distance $\delta = 2\tau + 1$.
- Let $\alpha \in \text{GF}(2^m)$ be a primitive n th root of unity, with m the smallest integer such that $n|2^m - 1$
- Assume a codeword $\mathbf{c} = (c_0, \dots, c_{n-1}) \in \mathcal{C}$ is transmitted over a binary (memoryless) channel, resulting in

$$\mathbf{y} = (y_0, \dots, y_{n-1}) = \mathbf{c} + \mathbf{e}$$

with $\mathbf{e} = (e_0, \dots, e_{n-1}) \in \text{GF}^n(2)$ of weight w

- Polynomials:

$$c(x) = \sum_{m=0}^{n-1} c_m x^m, \quad y(x) = \sum_{m=0}^{n-1} y_m x^m, \quad e(x) = \sum_{m=0}^{n-1} e_m x^m$$

- The error locator polynomial $\sigma(x)$: Assume that the non-zero components of \mathbf{e} are e_{i_1}, \dots, e_{i_w} , and let

$$\sigma(z) = \prod_{r=1}^w (1 - X_r z)$$

where $X_r = \alpha^{i_r}$ are the error locators

- Roots of $\sigma(z)$ in $\text{GF}(2^m)$ known $\implies \mathbf{e}$ known
- Decoding:
 1. Compute $A_i = y(\alpha^i)$, $i = 1, \dots, \delta - 1$
 2. Find $\sigma(z)$ from $A_1, \dots, A_{\delta-1}$
 3. Compute the roots of $\sigma(z) \rightarrow e(x)$
 - Will correct all errors of weight $w \leq \tau$
 - Polynomial (not exponential) complexity!

- Compute $\sigma(z)$ from A_i , $i = 1, \dots, \delta - 1$:
 - Newton's identities (tailored to this problem):

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ A_2 & A_1 & 1 & 0 & 0 & \cdots & 0 \\ A_4 & A_3 & A_2 & A_1 & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \\ A_{2w-4} & A_{2w-5} & \cdots & & \cdots & A_{w-3} & \\ A_{2w-2} & A_{2w-3} & \cdots & & \cdots & A_{w-1} & \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_{w-1} \\ \sigma_w \end{bmatrix} = \begin{bmatrix} A_1 \\ A_3 \\ A_5 \\ \vdots \\ A_{2w-3} \\ A_{2w-1} \end{bmatrix}$$

as long as $w \leq \tau = (\delta - 1)/2$

- $\{A_i\} \rightarrow \sigma(z)$ not unique \implies choose $\sigma(z)$ of lowest degree,
 - * iterative technique described in MWS (c.f., Theorem 14)
- Newton's identities not feasible for large τ 's \implies use instead the Berlekamp algorithm to find $\sigma(z)$...

- Compute the power sums A_i , $i = 1, \dots, \delta - 1$:
 - Divide $y(x)$ by the minimal polynomial $p^{(i)}(x)$ of α^i ,

$$y(x) = q(x)p^{(i)}(x) + r(x),$$

and set $x = \alpha^i$ in the remainder $r(x)$, $A_i = y(\alpha^i) = r(\alpha^i)$

- * Easily implemented in hardware using less calculations than computing $y(\alpha^i)$ directly from $y(x)$...
- * Equivalent to computing the syndrome of $y(x)$...

– Note that

$$A_i = y(\alpha^i) = e(\alpha^i) = \sum_{j=1}^w X_j^i, \quad i = 1, \dots, \delta - 1$$

(“power sums”)

- Find the roots of $\sigma(z)$:
 - An error in coordinate $i \iff \sigma(\alpha^{-i}) = 0$;
 - * simply test $\sigma(\alpha^{-i}) = 0$ for $i = 1, \dots, n$ (Chien search)
- Nonbinary BCH codes: Same principles apply, some additional concepts found in MWS8 however needed...
- More than τ errors: The approach described only works for $\leq \tau = (\delta - 1)/2$ errors, i.e., full nearest neighbor decoding is not implemented;
 - Complete NN decoding algorithms (of polynomial complexity) known in many cases, but need often be tailored to specific codes...
 - Full search NN decoding always possible, but has exponential complexity...

REED–SOLOMON CODES

- *Definition:* A Reed–Solomon (RS) code over $\text{GF}(q)$ is a BCH code of length $N = q - 1$, that is,

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+\delta-2})$$

for some $b \geq 0$ and $\delta \geq 2$, and with α primitive $\in \text{GF}(q)$

- Zeros and symbols *in the same field*, $\text{GF}(q)$
- Dimension $K = N - \delta + 1$
- The Singleton bound $d_{\min} \leq N - K + 1 \implies$
 - * $d_{\min} = \delta$
 - * maximum distance separable code

DECODING RS CODES

- *RS codes are BCH codes:* Decode as non-binary BCH codes...
- *Alternative majority logic* decoding: See MWS10.10...

ENCODING RS CODES

- *RS codes are cyclic:* Encode as (non-binary) cyclic codes...
- *Alternative:* Assume an $[N, K]$ RS code, and let

$$u(x) = u_0 + u_1x + \cdots + u_{K-1}x^{K-1}$$

correspond to the message symbols $u_0, \dots, u_{K-1} \in \text{GF}(q)$, then

$$c(x) = u(1) + u(\alpha)x + u(\alpha^2)x^2 + \cdots + u(\alpha^{N-1})x^{N-1}$$

is a codeword.