Coding Theory

(BCH and Reed-Solomon codes)

Lector: Nikolai L. Manev

Institute of Mathematics and Informatics, Sofia, Bulgaria

Zeros of a code

Let $q = p^k$ be a prime power and n be an integer such that $(n, q) = 1$. Then $x^n - 1 = p_1(x) \dots p_k(x)$, where $p_i(x)$ are different irreducible polynomials over $\mathbb{F} = GF(q)$. Obviously, the roots of all polynomials $p_i(x)$ are n-th roots of unity. Let $\mathbb{K} = GF(q^m)$ be the splitting field of $x^n - 1$, i.e., the minimal extension of $\mathbb{F}$ which contains all n-th roots of unity.
The set of all n-th roots of unity is a multiplicative subgroup of $\mathbb{K}^*$, and it is thus cyclic, that is, there exists a $\beta \in \mathbb{K}^*$ such that all roots of $x^n - 1$ are $\{1, \beta, \beta^2, \dots, \beta^{n-1}\}$. If α is a primitive element of $\mathbb{K}$, then we can take $\beta = \alpha^{\frac{q^m-1}{n}}$. The extension degree $m = [\mathbb{K} : \mathbb{F}]$ of $\mathbb{F}$ is the smallest positive integer such that $q^m \equiv 1 \pmod{n}$.

Definition. The *multiplicative order of q modulo n* is the smallest integer m such that n divides $q^m - 1$.

Zeros of a code

Definition. A *cyclotomic coset of i modulo n with respect to q* is called the set

$$C_i = \{i, iq, \ldots, iq^{m_i-1}\},$$

where $iq^{m_i} \equiv i \pmod{n}$ and m_i is the smallest positive integer with this property.

Recall that if β^i is a root of a irreducible factor, $p(x)$, of $x^n - 1$, then any other root of $p(x)$ has the form β^{iq^s}, for a suitable integer s. Hence, there is an one-to-one correspondence between irreducible factors $p_i(x)$ of $x^n - 1$ and cyclotomic cosets modulo n.

Zeros of a code

Let $\mathcal{C} = (g(x))$ be a cyclic code. Then its generator polynomial is $g(x) = p_{k_1}(x)p_{k_2}(x)\dots p_{k_s}(x)$.

Definition. Let $\mathcal{C} = (g(x))$ be a cyclic code with a generator polynomial

$$g(x) = \prod_{j \in P}(x - \beta^j), \quad P \subset \{0, 1, \dots, n-1\}$$

(P is an union of cyclotomic classes.) The set $\{\beta^j | j \in P\}$ is called the *set of zeros* of $\mathcal{C}$, and the set $\{\beta^j | j \notin P\}$ is referred to as the *set of non-zeros*.

Proposition. $c(x) \in \mathcal{C}$ if and only if $c(\beta^j) = 0$ for any $j \in P$, that is,

$$\mathcal{C} = (g(x)) = \{c(x) \mid c(\beta^j) = 0,\ j \in P\}.$$

Proposition. γ is a zero of $\mathcal{C}^\perp$ if and only if γ^{-1} is a non-zero of $\mathcal{C}$.

BCH bound

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$, $s = |P|$, be the set of zeros of the code $\mathcal{C} = (g(x))$. Then $\mathcal{C} = \{\mathbf{c} \in \mathbb{F}^n \mid \mathbf{c}\mathbf{H}^\tau = 0\}$, where

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ . & . & . & . & . \\ 1 & \alpha_s & \alpha_s^2 & \ldots & \alpha_s^{n-1} \end{pmatrix}.$$

Obviously, it is sufficient to take only those α_j that are roots of different irreducible factors of $g(x)$.

Theorem. Let $\mathcal{C} = (g(x))$ be a cyclic code over $\mathbb{F}$ such that for some integers $b \geq 0$ and $\delta \geq 1$

$$g(\beta^b) = g(\beta^{b+1}) = \cdots = g(\beta^{b+\delta-2}) = 0.$$

Then the minimum distance of $\mathcal{C}$ is at least δ.

BCH (Bose-Chaudhudri-Hocquenghem) codes 1

Definition. The cyclic code $\mathcal{C} = (g(x))$ of length n over $\mathbb{F}$ is called *BCH code with design distance* δ if for some integer $b \geq 0$ its generator polynomial $g(x)$ is the least common multiple of the minimal polynomials of $\beta^b, \beta^{b+1}, \ldots, \beta^{b+\delta-2}$ where β is a primitive n^{th} root of unity. If $n = q^m - 1$, then the BCH code is called *primitive*. Usually we take $b = 1$ and refer to the resulting code as a *narrow-sense BCH* code.

Example. (*BCH code correcting 2 errors*) Let $\mathbb{F} = GF(2)$, $n = 2^m - 1$ and α be a primitive element of $GF(2^m)$. Consider the primitive narrow-sense BCH code with design distance 5, that is, the BCH code with zeros $\alpha, \alpha^2, \alpha^3, \alpha^4$, whose generator polynomial is

$$g(x) = l.c.m.[M_1(x), M_3(x)] = M_1(x)M_3(x),$$

where $M_i(x) = \text{irr}_F \alpha^i$ is the minimal polynomial of α^i.

BCH (Bose-Chaudhudri-Hocquenghem) codes 1

Note that $M_1(x) \neq M_3(x)$, since $3 \not\equiv 2^l \pmod{2^m - 1}$ and the cyclotomic classes C_1 and C_3 are thus different, but $|C_1| = |C_3| = m$. Hence, $\dim \mathcal{C} = n - \deg g(x) = 2^m - 1 - 2m$. Therefore, $\mathcal{C}$ is a $[2^m - 1,\ 2^m - 1 - 2m,\ d]$ code, where $d \geq 5$ by the BCH bound. A vector $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ if and only if $\mathbf{c}\tilde{\mathbf{H}}^\tau = \mathbf{o}$, where

$$\tilde{\mathbf{H}} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{3(n-1)} \end{pmatrix}.$$

Example. (*Some Hamming codes are cyclic*) Let $n = \frac{q^m - 1}{q - 1}$, α be a primitive element of $GF(q^m)$ and $\beta = \alpha^{q-1}$. The q-ary cyclic code

$$\mathcal{C} = \{c(x) \in \mathcal{F}_n \mid c(\beta) = 0\},$$

is an $[n, n - m, 3]$ code if and only if $(m, q - 1) = 1$.

Reed-Solomon (RS) codes

Definition. A *Reed-Solomon (RS) code over* $\mathbb{F} = GF(q)$, $q = p^m$, is a q-ary BCH code $\mathcal{C} = (g(x))$ of length $N = q - 1$. Let α be a primitive element of $GF(q)$. Then a Reed-Solomon code with design distance δ has generator polynomial

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

Since $\deg g(x) = \delta - 1$, the dimension of the $\mathcal{C}$ is $N - \delta + 1$, that is, $\delta = N - K + 1$. But according to the Singleton bound the minimum distance $D \leq N - K + 1$ and $D \geq \delta$ by the BCH bound.
Therefore, the Reed-Solomon code $\mathcal{C}$ is an MDS code with

$$[N, K, N - K + 1]$$

Weight distribution of MDS code

Theorem. A number A_j of codewords with weight j in a q-ary $[n, k]$ MDS code is given by

$$A_j = \binom{n}{j}(q-1)\sum_{i=0}^{j-d}(-1)^j\binom{j-1}{i}q^{j-d-i}, \quad j = d, d+1, \ldots.$$

(Recall that $d = n - k + 1$)

Since Reed-Solomon codes are MDS codes, the above formula give their weight distributions.

Decoding by zeros of the code

Let $\beta \in GF(q^m)$ be a primitive n^{th} root of unity, where m is the multiplicative order of q modulo n. Let $\mathcal{C} = (g(x))$ be a cyclic code of length n over $\mathbb{F} = GF(q)$ with zeros $\beta^{k_1}, \beta^{k_2}, \ldots, \beta^{k_r}$.

Suppose a codeword $c(x)$ is sent across the channel and the vector $v(x) = c(x) + e(x)$ is received. For the syndrome $s(x) = [v(x)]_{g(x)} = [e(x)]_{g(x)}$ and $j = 1, 2, \ldots, r$ we have

$$s(\beta^{k_j}) = v(\beta^{k_j}) = e(\beta^{k_j}) = e_{i_1}\beta^{i_1 k_j} + e_{i_2}\beta^{i_2 k_j} + \cdots + e_{i_w}\beta^{i_w k_j}$$
$$= E_1 X_1^{k_j} + E_2 X_2^{k_j} + \cdots + E_w X_w^{k_j},$$

where $X_l = \beta^{i_l}$, $E_l = e_{i_l}$, and w is the weight of $e(x)$. The elements $X_1, X_2, \ldots, X_w$ are called *error locators*.

Definition. The elements

$$S_k = s(\beta^k) = E_1 X_1^k + E_2 X_2^k + \cdots + E_w X_w^k,$$

are called *generalized power-sum symmetric functions*, and very often they are referred to as *syndrome sequence*.
The polynomial

$$\begin{aligned}\sigma(x) &= (x - X_1)(x - X_2)\ldots(x - X_w) \\ &= x^w - \sigma_1 x^{w-1} + \sigma_2 x^{w-2} - \cdots + (-1)^w \sigma_w\end{aligned}$$

is said to be *error locator polynomial*, where σ_i denotes the i-th elementary symmetric function of $\{X_l\}$.

Since X_l are roots of $\sigma(x)$, then for $l = 1, 2, \ldots, w$ we have

$$X_l^w - a_1 X_l^{w-1} - a_2 X_l^{w-2} - \cdots - a_w = 0,$$

where $a_i = (-1)^{i-1}\sigma_i,\ i = 1, \ldots, w$.
After some algebraic manipulations we can conclude that

Decoding by zeros of the code

the sequence $\{S_j\}$ satisfies the recursion

$$S_{j+w} = a_1 S_{j+w-1} + a_2 S_{j+w-2} + \cdots + a_w S_j, \quad j = 0, 1.2, \ldots,$$

called *generalized Newton's identities*.

The maximum likelihood decoding requires the polynomial $\sigma(x)$ to be of the smallest possible degree, that is, the decoding is based on the following task:

Given the syndrome sequence $S_{k_1}, S_{k_2}, \ldots, S_{k_r}$ find the recursion of the smallest order this sequence satisfies.

Knowing the error locator polynomial we can determine the erroneous positions, and then the magnitudes E_l of errors (in binary case the latter is not necessary). This approach works well when consecutive members of $\{S_j\}$ are known, what is the case of BCH and Reed-Solomon codes.

Algorithm.

1. At receiving $\mathbf{v}$ compute the syndrome sequence $S_b, S_{b+1}, \ldots, S_{b+\delta-2}$, where $S_j = v(\beta^j)$. If every $S_j = 0$ then set $e(x) := 0$ and go to step 5.
2. Determine the error locator polynomial $\sigma(x)$.
3. Determine the roots $X_1, X_2, \ldots, X_w$ of $\sigma(x)$ and erroneous positions $i_1, \ldots, i_w$ by $X_l = \beta^{i_l}$.
4. Calculate the error magnitudes $E_l = e_{i_l}$, for example by

$$\begin{pmatrix} X_1^b & X_2^b & \ldots & X_w^b \\ \vdots & \vdots & \vdots & \\ X_1^{b+w-1} & X_2^{b+w-1} & \ldots & X_w^{b+w-1} \end{pmatrix} \begin{pmatrix} E_1 \\ \vdots \\ E_w \end{pmatrix} = \begin{pmatrix} S_b \\ \vdots \\ S_{b+w-1} \end{pmatrix}$$

5. $c(x) := v(x) - e(x)$ and stop.

Decoding by zeros of the code 5

Many variants of the algorithm are developed that differ each other mainly in the way of carrying out point 2. Here some of them

- Peterson-Gorenstein-Zierler decoding algorithm
- Berlekamp-Massey algorithm
- Euclid's algorithm

Indeed, the above algorithms use the reciprocal polynomial of $\sigma(x)$. Its roots are the inverses of the error locators X_j:

$$\Lambda(x) = \prod_{i=1}^{w}(1 - X_i x) = 1 - \sigma_1 x + \sigma_2 x^2 - \cdots + (-1)^w \sigma_w x^w.$$

It is also referred to as the error locator polynomial.

We shall describe in details only the last algorithm.

Euclid's algorithm

Let $2t$ consecutive syndromes, $S_b, S_{b+1}, \ldots, S_{b+2t-1}$, be known for the received vector $v(x)$. Let set

$$S(x) = S_b + S_{b+1}x + \ldots + S_{b+2t-1}x^{2t-1}.$$

It is not difficult to check that

$$S(x)\Lambda(x) + u(x).x^{2t} = \omega(x),$$

where

$$\omega(x) \stackrel{\text{def}}{=} \sum_{i=1}^{w} E_i X_i^b \prod_{i \neq j}^{w} (1 - X_j x), \qquad \deg \omega(x) = w - 1 < t,$$

$$u(x) \stackrel{\text{def}}{=} \sum_{i=1}^{w} E_i X_i^{b+2t} \prod_{i \neq j}^{w} (1 - X_j x), \qquad \deg u(x) = w - 1 < t,$$

Note that $(u(x), \Lambda(x)) = 1$.

Euclid's algorithm

It is important that based on the Euclid's algorithm one can determine $\Lambda(x), u(x)$ and $\omega(x)$ provided that $S(x)$ is given.

Theorem. For a given $S(x)$, there exist unique polynomials $u(x),\ \Lambda(x)$, and $\omega(x)$ such that

$$u(x).x^{2t} + \Lambda(x)S(x) = \omega(x),$$

and $\deg \omega(x) < t$, $\deg \Lambda(x) \leq t$, with $(u(x), \Lambda(x)) = 1$.

Theorem. Provided that $\Lambda(x)$ and $\omega(x)$ are known, then the error magnitudes are given by

$$E_k = -\frac{\omega(X_k^{-1})}{X_k^{b-1}\Lambda'(X_k^{-1})},$$

where $\Lambda'(x)$ is the formal derivative of $\Lambda(x)$.

Algorithm. Points 2 and 5 of the decoding algorithm.

Point 2:

Data: $S(x)$.

Output: $\omega(x),\ \Lambda(x)$.

Variables: $A=(A_1,A_2,A_3),\ B=(B_1,B_2,B_3),\ C=(C_1,C_2,C_3)$

$A:=(x^{2t},1,0),\ B:=(S(x),0,1),\ C:=(x^t,0,0).$

while $\deg C_1\geq t$ do

$q(x):=[A_1/B_1], C:=A-qB,\quad A:=B,\quad B:=C$

else

$\omega(x):=B_1,\ u(x):=B_2,\ \Lambda(x):=B_3.$

Point 5:

$$E_k=-\frac{\omega(X_k^{-1})}{X_k^{b-1}\Lambda'(X_k^{-1})}.$$

Example of a BCH code

Let α be a primitive element of $GF(2^4)$ with the minimal polynomial $\text{irr}\alpha = x^4 + x + 1$. Consider the binary $[15, 5, 7]$ code $\mathcal{C}$ with zeros $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. Therefore,

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$$
$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

The correspondence between multiplicative and polynomial form of the elements of $GF(16)$ is given by

mult.	polyn.	mult.	polyn.	mult.	polyn.	mult.	polyn.
0	0000	α^3	0001	α^7	1101	α^{11}	0111
1	1000	α^4	1100	α^8	1010	α^{12}	1111
α	0100	α^5	0110	α^9	0101	α^{13}	1011
α^2	0010	α^6	0011	α^{10}	1110	α^{14}	1001

Example of a BCH code

The code $\mathcal{C}$ can correct up to $t = 3$ errors. Let the vector
$v(x) = x^{10} + x^8 + x^7 + x^5 + x^4 + x + 1 = g(x) + x^2 + x^7$
be received.

First we calculate the syndrome sequence $\{S_j = v(\alpha^j)\}$:

$$S_1 = \alpha^2 + \alpha^7 = \alpha^{12}, \quad S_2 = \alpha^4 + \alpha^{14} = \alpha^9, \quad S_3 = \alpha^6 + \alpha^6 = 0,$$
$$S_4 = \alpha^8 + \alpha^{13} = \alpha^3, \quad S_5 = \alpha^{10} + \alpha^5 = 1, \quad S_6 = \alpha^{12} + \alpha^{12} = 0.$$

Hence $S(x) = \alpha^{12} + \alpha^9 x + \alpha^3 x^3 + x^4$.

x^6	1	0	$q(x)$
$S(x)$	0	1	$x^2 + \alpha^3 x + \alpha^6$
α^3	1	$x^2 + \alpha^3 x + \alpha^6$	

Example of a BCH code

At the first step of the Euclid's algorithm we reach the stopping condition. Therefore

$$\omega(x) = \alpha^3; \qquad u(x) = 1; \qquad \Lambda(x) = x^2 + \alpha^3 x - \alpha^6.$$

Then we determine the roots of $\Lambda(x)$: $X_1^{-1} = \alpha^{13},\ X_2^{-1} = \alpha^8$.

Hence the error locators are $X_1 = \alpha^2$ and $X_2 = \alpha^7$, that is the error vector is $e(x) = x^2 + x^7$.

Example of error+erasure decoding 1

Let α be a primitive element of $\mathbb{F} = GF(2^5)$ with the minimal polynomial $\text{irr}\alpha = x^5 + x^2 + 1$. Consider the $[31, 27, 7]$ RS code $\mathcal{C}$ with zeros $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. Therefore,

$$g(x) = x^6 + \alpha^{10}x^5 + \alpha^9 x^4 + \alpha^{24}x^3 + \alpha^{16}x^2 + \alpha^{24}x + \alpha^{21}$$

Let the receiver mark erasures with the symbol †.
Let the vector at the output of the receiver be

$$v(x) = x^7 + \dagger x^6 + \dagger x^5 + \alpha^{24}x^4 + \alpha^{24}x^2 + \alpha^{21}x$$

We now replace † by zero and compute the syndromes $S_i = v(\alpha^i)$:

$$S_1 = 0,\ S_2 = \alpha^{19},\ S_3 = \alpha^{10},\ S_4 = \alpha^{26},\ S_5 = \alpha^{17},\ S_6 = \alpha^9,$$

that is $S(x) = \alpha^9 x^5 + \alpha^{17}x^4 + \alpha^{26}x^3 + \alpha^{10}x^2 + \alpha^{19}x$.

Example of error+erasure decoding 2

The erasure positions correspond to $Y_1 = \alpha^5$ and $Y_2 = \alpha^6$. Hence

$$\Lambda(x) = (1 - \alpha^5 x)(1 - \alpha^6 x)\Lambda_1(x) = (\alpha^{11}x^2 + \alpha^{23}x + 1)\Lambda_1(x).$$

Let $T(x) = S(x)(\alpha^{11}x^2 + \alpha^{23}x + 1) =$

$$\alpha^{20}x^7 + \alpha^7 x^6 + \alpha^6 x^5 + \alpha^3 x^4 + \alpha^{21}x^3 + \alpha^{13}x^2 + \alpha^{16}x$$

We now look for $\Lambda_1(x), u(x), \omega(x)$ such that

$$T(x)\Lambda_1(x) + x^6.u(x) = \omega(x),$$

where $\deg \omega(x) < 3$, since the minimum distance is 7.

Since x divides both $T(x)$ and x^6, we can look for $\Lambda_1(x), u(x), \omega_1(x)$ such that

$$T_1(x)\Lambda_1(x) + x^5.u(x) = \omega_1(x),$$

where $T_1(x) = T(x)/x$, $\omega_1(x) = \omega(x)/x$, and $\deg \omega_1(x) < 2$.

Example of error+erasure decoding 3

$T_1(x)$	1	0	$\boldsymbol{q(x)}$
x^5	0	1	$\alpha^{20}x+\alpha^7$
$r(x)$	1	$\alpha^{20}x+\alpha^7$	$\alpha^{25}x+\alpha^{22}$
$r_1(x)$	$\alpha^{25}x+\alpha^{22}$	$\alpha^{14}x^2+\alpha^5x+\alpha^3$	

where

$$r(x)=\alpha^6x^4+\alpha^3x^3+\alpha^{28}x+\alpha^{19},$$

$$r_1(x)=\alpha^9x+\alpha^{10}.$$

$\deg r_1(x)<2$, then $\omega_1(x)=r_1(x),\ u(x)=\alpha^{14}x^2+\alpha^5x+\alpha^3$ and $\Lambda_1(x)=\alpha^{25}x+\alpha^{22}=\alpha^{22}(1+\alpha^3x)$. Therefore, the unknown erroneous position corresponds to x^3 and

$$\Lambda(x)=\alpha^5x^3+\alpha^{26}x^2+\alpha^2x+\alpha^{22},\qquad \Lambda'(x)=\alpha^5x^2+\alpha^2$$

Example of error+erasure decoding 4

The error vector is $e(x) = E_1 x^3 + E_2 x^5 + E_3 x^6$, where

$$E_1 = \frac{\omega(\alpha^{-3})}{\Lambda'(\alpha^{-3})} = \frac{(\alpha^3 + \alpha^7)}{\alpha^{30} + \alpha^2} = \alpha^{16}$$

$$E_2 = \frac{\omega(\alpha^{-5})}{\Lambda'(\alpha^{-5})} = \frac{(\alpha^{-1} + \alpha^5)}{\alpha^{26} + \alpha^2} = \alpha^{9}$$

$$E_3 = \frac{\omega(\alpha^{-6})}{\Lambda'(\alpha^{-6})} = \frac{(\alpha^{-3} + \alpha^4)}{\alpha^{24} + \alpha^2} = \alpha^{10}$$

The codeword sent across the channel is

$$c(x) = x^7 + \alpha^{10} x^6 + \alpha^9 x^5 + \alpha^{24} x^4 + \alpha^{16} x^3 + \alpha^{24} x^2 + \alpha^{21} x = x g(x).$$

The end of the part

Thank You for Attention!