Bose-Chaudhuri-Hocquenghem codes

multiple error correcting generalization of Hamming codes. They are cyclic, there are several efficient algo. for decoding them based on their algebraic structure.

Both binary and non bin. version.

Reed-Solomons codes are an important subclass of non-bin. BCH codes.

~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ . ~ .

let's start from the general idea of designing a t-error correcting cyclic code.

consider cyclic code with generator polynomial $g(x)$ over $\mathbb{F}_q$.

$g(x)$ has degree K, the fundamental theorem of algebra says that g has K roots in a field extension $\mathbb{F}_{q^m}$. Let these K zeroes be $\beta_1 \dots \beta_K$ then we can write $g(x)$ as follows

$$g(x) = \operatorname{lcm}\left(m_{\beta_1}(x), \dots, m_{\beta_K}(x)\right)$$

(lcm: least common multiple (mcm in ITA))

where m_{β_i} is the minimal polynomial of β_i over $\mathbb{F}_q$ (β_i: primitive element)

Revising

now consider an element $\alpha \in \mathbb{F}_q$ with $q = 2^m$

A polynomial $a(x) \in \mathbb{F}_2[x]$ for which $a(\alpha) = 0$ we call it a characteristic polynomial for α.

The characteristic polynomial with the lowest degree is called the minimum polynomial of α.

Now let $r(x) = v(x) + e(x)$ be a recieved polynomial

($v(x)$: transmitted code poly.; $e(x)$: error polynomial)

If we evaluate $r(x)$ at the elements $\beta_i \in \mathbb{F}_{q^m}$ we find that $r(\beta_i) = e(\beta_i)$ because $v(x)$ is a multiple of $g(x)$ it gets nullified.

This leads to a set of K simultaneous equations in the unknows $e_0, e_1, \dots, e_{n-1}$

$$\begin{aligned} e_0 + e_1\beta_1^1 + \dots e_{n-1}\beta_1^{n-1} &= r(\beta_1) \\ e_0 + e_1\beta_2^1 + \dots e_{n-1}\beta_2^{n-1} &= r(\beta_2) \\ &\vdots \\ e_0 + e_1\beta_K^1 + \dots e_{n-1}\beta_K^{n-1} &= r(\beta_K) \end{aligned}$$

So we can phrase the creation of a t-error correcting cyclic code as follows

Choose a generator polynomial $g(x)$ with zeroes $\beta_1 \dots \beta_K$, such that the K simultaneous equations can be solved (hopefully efficently) whenever at most t of the e_i are non-zero

N.B.: if α is a primitive element of $\mathbb{F}_{q^m}$ a suitable set of zeros is $\beta_i = \alpha^i$, $i = 1, \dots 2t$

theorem: Primitive BCH codes

let m and $t < \frac{q^m-1}{2}$ integers. Then there is a q-ary BCH$[n,k,d]$-code with parameters

$n = q^m - 1 \qquad k \geq n - 2mt \qquad d \geq 2t+1$

this code is generated by $g(x)$, the lowest degree polynomial over $\mathbb{F}_q$ having as roots α^{c+i}, $i = 1, \dots, 2t$ where α is a primitive element of $\mathbb{F}_{q^m}$ and $c \in \mathbb{Z}$

↑ $\forall b \in \mathbb{F}_{q^m}$, $b = a^i$, $i \in \mathbb{Z}$

The parameter $d = 2t+1$ is called the designed distance of the code

proof: take the special $g(x)$ as above

and suppose $e(x) = \sum_{l=1}^{v} e_{i_l} x^{i_l}$ is a polynomial of weight $v < 2t+1$ then this can never be a code word because then we would have as equations

$$e_{i_1}(\alpha^{c+1})^{i_1} + \dots + e_{i_v}(\alpha^{c+1})^{i_v} = 0$$
$$\vdots$$
$$e_{i_1}(\alpha^{c+v})^{i_1} + \dots + e_{i_v}(\alpha^{c+v})^{i_v} = 0$$

the equations can be solved uniquely as long as the following determinant $\neq 0$

$$\det \begin{pmatrix} (\alpha^{c+1})^{i_1} & \dots & (\alpha^{c+1})^{i_v} \\ \vdots & & \vdots \\ (\alpha^{c+v})^{i_1} & \dots & (\alpha^{c+v})^{i_v} \end{pmatrix} = \alpha^{(c+1)(i_1+\dots+i_v)} \cdot \det \begin{pmatrix} (\alpha^{i_1})^0 & \dots & (\alpha^{i_v})^0 \\ \vdots & & \vdots \\ (\alpha^{i_1})^{v-1} & \dots & (\alpha^{i_v})^{v-1} \end{pmatrix} = \alpha^{(c+1)(i_1+\dots+i_v)} \cdot \prod_{k \neq \lambda} (a^{i_k} - a^{i_\lambda})$$

↑ formula for the Vandermonde det.

Because $\alpha^{i_k} \neq a^{i_\lambda}$ whenever $i_k \neq i_\lambda$ and both exponents are smaller than $q^m - 1$ $\det \neq 0$

and the only possible solution is the zero solution.

So a poly. with weight $< 2t+1$ can never be a codeword.

to find the parameters:

we take n as big as we can. Because of the condition on the i_k it must be $q^m - 1$

The degree of g is smaller than $2mt$ because the degree of α is m and therefore the degree of every power of α is at most n.

recall: in $\mathbb{F}_{2^m}$ $(x+y)^2 = x^2 + y^2$

this implies that for any polynomial f we have that $f(x^2) = f(x)^2$.

if α is a root of f then $f(\alpha^2) = f(\alpha)^2 = 0$, so α^2 is also a root of f.

Hence the elements of α and α^2 have the same minimum polynomial.

For a binary BCH code we can form the generator polynomial by considering only the odd powers of the primitive element α.

$g(x) = \operatorname{lcm}(m_\alpha(x), m_{\alpha^2}(x), \dots, m_{\alpha^{2t}}(x)) = \operatorname{lcm}(m_\alpha(x), m_{\alpha^3}(x), \dots, m_{\alpha^{2t-1}}(x))$

this shows that with bin. codes $\deg(g(x)) \leq mt$ so we have $K \geq 2^m - mt$

when $n = q^m - 1$ we speak of a primitive BCH code

if c ? $= 0$ the code is a narrow sense BCH code.

Code construction

Algorithm constructing a narrow sense BCH-code

t-error correcting, length q^m-1

1) Find a degree m primitive polynomial $\pi(X)$ over $\mathbb{F}_q$
2) use $\pi(X)$ to construct $\mathbb{F}_{q^m}$ ← irreducible pols. that generates the field
3) let α be a primitive element of $\mathbb{F}_{q^m}$
4) find $m_{\alpha^i}(X)$ the minimal polynomial for α^i, for $i=1,2\dots 2t$
5) let $g(X)$ be the minimal degree pols. with the $m_{\alpha^i}(X)$ as factors

$$g(X) = \text{lcm}(m_{\alpha^1}(X), m_{\alpha^2}(X) \dots m_{\alpha^{2t}}(X))$$

Examples

Single error correcting binary BCH codes

let $\pi(X)$ be a degree m binary primitive poly., such that $\pi(X)$ is also the minimal polynomial of a primitive element α in $\mathbb{F}_{2^m}$.

This is not always the case, f.i. the roots of $x^4+x^3+x^2+x+1$ are not primitive elements over $\mathbb{F}_{2^4}$.

If it does $\pi(X)$ generates a $[2^m-1, 2^m-m-1]$ code.

It also is in fact an Hamming code bcz it has the same parameters

Double error correcting BCH codes

Let $\pi(X) = 1+X+X^4$ let $t=2$ and $m=4$, then:

$$g(X) = \text{lcm}(m_\alpha, m_{\alpha^3}) =$$
$$= (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1$$

we designed a $[15, 7]$ BCH code with $d \geq 5$.

Note that $g(X)$ has $w=5$, and since it is a codeword $d=5$

triple error correcting

$\pi(X) = 1+X+X^4$, $t=3$ $m=4$

$$g(X) = (m_\alpha, m_{\alpha^3}, m_{\alpha^5}) =$$
$$= (x^4+x+1)(x^4+x^3+x^2+x+1)(1+x+x^2) = x^{10}+x^8+x^5+x^4+x^2+x+1$$

this is a $[15, 5, 7]$ code ↑ weight 7

Decoding

Since they've cyclic we could just use normal algorithms.

The special structure of narrow-sense BCH codes yields to lower complexity

$g(x)$ was chosen specifically such that it has zeroes at $\alpha, \alpha^2, \dots \alpha^{2t}$, where α is a primitive element of $\mathbb{F}_{q^m}$, this implies:

$$r(\alpha^i) = e(\alpha^i), \quad i = 1, \dots 2t$$

where $r(x)$ and $e(x)$ are the recieved poly and the error poly.

for $j = 1, \dots, 2t$ we define the j-th syndrome for the received polynomial $r(x)$ as:

$$S_j = r(\alpha^j) = \sum_{l=1}^{n} e_l (\alpha^j)^l$$

suppose v errors occurred, located in position $i_1, i_2, \dots i_v$ $(v \leq t)$

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} \dots + e_{i_v} x^{i_v}$$

then the powers of X define the error location and the coefficients the order of magnitudes.

In the case of binary codes that is always 1.

$$S_1 = e_{i_1} \alpha^{i_1} + e_{i_2} \alpha^{i_2} + \dots + e_{i_v} \alpha^{i_v}$$
$$S_2 = e_{i_1} (\alpha^{i_1})^2 + e_{i_2} (\alpha^{i_2})^2 + \dots + e_{i_v} (\alpha^{i_v})^2$$
$$\vdots$$
$$S_{2t} = e_{i_1} (\alpha^{i_1})^{2t} + e_{i_2} (\alpha^{i_2})^{2t} + \dots + e_{i_v} (\alpha^{i_v})^{2t}$$

we need to solve these equations for the α^{i_l} and e_{i_l}

Once we do that we can take logarithms (base α) in $\mathbb{F}_{q^m}$

$$\log_\alpha X = j \iff \alpha^j = X \text{ and } 1 \leq j \leq n$$

to find the error location numbers i_l, and correct the symbols by subtracting the corresponding order of magnitude

to avoid confusion we can use $X_l = \alpha^{i_l}$ and $Y_l = e_{i_l}$

$$S_1 = Y_1 X_1 + Y_2 X_2 + \dots + Y_v X_v$$
$$S_2 = Y_1 X_1^2 \dots \quad \leftarrow \text{power-sum symmetric functions}$$
$$\vdots$$
$$S_{2t} = Y_1 X_1^{2t} \dots + Y_v X_v^{2t}$$

the methods to solve this kind of equations are decoding methods for BCH-codes

If we know the error locations it's really easy, the hard part is finding them

example

single error correction

$S_1 = Y_1 X_1 \Rightarrow X_1 = S_2/S_1, \; Y_1 = S_1^2/S_2$ if $S_2/S_1 = \alpha^i$ the error is at that position i and its value Y_1

$S_2 = Y_1 X_1^2$

it becomes harder with more errors

$F_2[X]/\ x^3+x+1 \quad t=1,\ q=2,\ m=3$

$\alpha^3 = \alpha+1$

$2t=2 \quad 2' = 2^2$

$\alpha^0 = 1$
$\alpha^1 = \alpha \qquad x^3+x+1$
$\alpha^2 = \alpha^2 \qquad x^3+x+1$
$\alpha^3 = \alpha+1 \qquad x^3+x^2+1$

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