L23

Friday, November 4, 2022 6:25 PM

BCH decoding.

* Assume the "narrow-sense" BCH code

I.e. $b=1$ and the consecutive

roots of $g(x)$ are $\in \mathbb{F}_{\boxed{m}}$

$$\beta^1, \beta^2, \cdots, \beta^{2\bar{t}}$$

define $2\bar{t} = \delta - 1$ for easier notation.

$\Rightarrow$ Any $t_0 \le \bar{t}$ errors can be corrected

---

* A decoding algorithm:

If the number of errors is $t_0 \le \bar{t}$, then the algorithm can be carried out from the beginning to the end, and the output is indeed the original codeword.

Corollary: If the decoding algorithm runs to an "exception" (fail to proceed), then it must mean $t_0 > \bar{t}$

* Remark: If $t_0 > \bar{t}$, it is possible
  1. the decoder fails in the middle.
  2. the decoder finishes, but the result is wrong
  3. the decoder finishes but the result is correct

* We don't care about which situation is which

---

* Suppose we have
  $c(x) = m(x) \cdot g(x)$

$$\Rightarrow r(x) = c(x) + e(x) = m(x) \cdot g(x) + e(x)$$

where $e(x)$ contains $t_0 \leq \bar{t}$ errors.

I.e. $e(x) = \sum_{i=1}^{t_0} e_{l_i} x^{l_i}$

where $0 \leq l_1 < l_2 < \cdots < l_{t_0} \leq n-1$
and $e_{l_i} \neq 0$ for all $1 \leq i \leq t_0$

Question to solve:
* We observe $r_0, \cdots, r_{n-1}$ values

* We observe $r_0, \cdots, r_{n-1}$ values

and we would like to find the error polynomial $e(x)$.

I.e. find the $l_1 < l_2 < \cdots < l_{t_0}$ values and $e_{l_1}, e_{l_2}, \cdots, e_{l_{t_0}}$ values.

* (Most) $\boxed{\text{BCH decoding algorithm}}$

* It consists of 3 major steps.

* Step 1: Compute

$$S_i = r(\beta^i), \quad \text{in } \mathbb{F}_{\boxed{m}} \quad i = 1, 2, \cdots, 2t$$

This is easily done since we know the coefficient $r_0, \cdots, r_{n-1}$

* Step 2: define the <u>error-location</u> polynomial

$$\Lambda(x) = \prod^{t_0} (1 - \beta^{l_i} x) = 1 + \lambda_1 x^1 + \cdots + \lambda_{t_0} x^{t_0}$$

$$\Lambda(x) = \prod_{i=1}^{t_0}\left(1 - \beta^{l_i} x\right) = 1 + \lambda_1 x^1 + \cdots + \lambda^{t_0} x^{t_0}$$

$$\boxed{\lambda^{t_0} \neq 0}$$

We find the entire polynomial $\Lambda(x)$ from $S_1, \cdots, S_{2\bar{t}}$ Berlekamp - Massey

Remark #1: As will be explained,

$S_1, \cdots, S_{2\bar{t}}$ and $\Lambda(x)$ satisfy some relationship, which is why this step works.

Remark #2: We do not know the t_0 value. We only know that $t_0 \leq \bar{t}$

$\boxed{\text{Remark 3:}}$ Once we know the entire polynomial $\Lambda(x)$, we can find its t_0 distinct roots by evaluating $\Lambda(x)$ for all

$\underline{1, \beta^1, \cdots, \beta^{n-1}},$

say $\Lambda(\beta^k) = 0$

$\Rightarrow$ the $(1 - \beta^{l_i} \beta^k) = 0$

$\Rightarrow$ then $(1-\beta^{l_i}\cdot\beta^{k})=0$

$\Rightarrow l_i=-k.$

That is, the t_0 roots β^{k_i} of $\Lambda(x)$ will give us the location indices $l_i=-k_i$ for $1\le i\le t_0$

Step 3: Find the error magnitudes e_{l_i}, $1\le i\le t_0$ by $S_1,\cdots,S_{2t}$ and $\Lambda(x)$ in Steps 1 and 2.

Remark: as long as $t_0\le\bar{t}$, the three steps can be carried out properly and the results are correct.

* It is possible that if $t_0>\bar{t}$, then the $S_1, S_2, \cdots S_{2\bar{t}}$ can lead to a $\tilde{\Lambda}(x)$ that is not $\Lambda(x)=\prod_{i=1}^{t_0}(1-\beta^{l_i}x)$

* Sometimes, we can "detect" this error. For example, $\tilde{\Lambda}(x)$ may have <u>repeated</u> roots, then $\boxed{\text{Remark 3}}$ cannot be carried out.
* Sometimes, the error cannot be detected. and we will have the wrong results.
* Overall, we dont care about $t_0 > \bar{t}$ scenario.

Step 1: Revisit:

$$
\begin{aligned}
S_i &= r(\beta^i) \\
&= c(\beta^i) + e(\beta^i) \\
&= 0 + e(\beta^i) \\
&= e_{l_1}(\beta^i)^{l_1} + e_{l_2}(\beta^i)^{l_2} + \cdots + e_{l_t}(\beta^i)^{l_t} \\
&= \sum_{j=1}^{t_0} e_{l_j} \cdot (\beta^{l_j})^i
\end{aligned}
$$

For simplicity we set $\bar{e}_j = e_{l_j}$

For simplicity we set $\bar{e}_j = e_{\ell_j}$

$\bar{\beta}_j = \beta^{\ell_j}$

$$\Rightarrow S_i = \sum_{j=1}^{t_0} \bar{e}_j \left(\bar{\beta}_j\right)^i \quad \text{for } i = 1, \cdots, 2\bar{t}$$

$\boxed{\text{Property:}}$

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_a \\ S_2 & S_3 & & \cdots & S_{a+1} \\ \vdots & & & & \\ S_a & & & & S_{2a-1} \end{bmatrix} \quad \text{is}$$

of full rank (invertible), if $a = t_0$,

is singular if $a > t_0$

$\boxed{\text{proof: Gorenstein \& Zierler 61 — A class of error-correcting codes in } p^m \text{ symbols.}}$

Example: $S_i = (-2)\cdot 1^i + 1\cdot 2^i$

$\Rightarrow S_1 = 0,\ S_2 = 2,\ S_3 = 6,\ S_4 = 14$

$S_5 = 30,\ S_6 = 62,\ S_7 = 126.$

$$\begin{bmatrix} 0 & 2 \\ 2 & 6 \end{bmatrix}$$ full rank.

$$\begin{bmatrix} 0 & 2 & 6 \\ 2 & 6 & 14 \\ 6 & 14 & 30 \end{bmatrix}$$ singular

$$\begin{bmatrix} 0 & 2 & 6 & 14 \\ 2 & 6 & 14 & 30 \\ 6 & 14 & 30 & 62 \\ 14 & 30 & 62 & 126 \end{bmatrix}$$ singular

* This result is very important.

E.g. we can find t_0 value now.

Method: Check

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_t \\ S_2 & & & \vdots \\ & & & \\ S_t & & & S_{2t-1} \end{bmatrix}$$

and see if it is full rank. If not, reduce the row & column, and try again. When we encounter the first full rank again. when we encounter the first full rank we have found t_0. (Under the assumption $t_0 \le \bar{t}$

* There are other implications of this result.

Define $S(x) = S_1 + S_2 x + \cdots + S_{2\bar{t}} x^{2\bar{t}-1}$

$$= \sum_{i=1}^{2\bar{t}} \left(\sum_{j=1}^{t_0} \bar{e_j} \, \bar{\beta_j}^{\,i} \right) \cdot x^{i-1}$$

rearrange

$$= \sum_{j=1}^{t_0} \overline{e_j} \cdot \overline{\beta_j} \cdot \sum_{i=1}^{2\bar{t}} (\bar{\beta_j} \cdot x)^{i-1}$$

Recall that $\Lambda(x) = \prod_{j=1}^{t_0} (1 - \beta^{\ell_j} x)$

$$= \prod_{j=1}^{t_0} (1 - \overline{\beta_j} x)$$

---

* The relationship between $S(x)$ and

$\Lambda(x)$:

- Define $Z_0(x) = S(x)\cdot\Lambda(x) \mod x^{2\bar{t}}$

that is, we take the product of $S(x)\cdot\Lambda(x)$ but then immediately discard those x^a with $a \geq 2\bar{t}$

* Since $$(1-\bar{\beta}_j x)\cdot\sum_{i=1}^{2\bar{t}}(\bar{\beta}_j x)^{i-1}$$

$$= 1-(\bar{\beta}_j x)^{2\bar{t}}$$

$$\Rightarrow Z_0(x) = \left(\prod_{j'=1}^{t_0}(1-\bar{\beta}_{j'}x)\right)\cdot\left(\sum_{j=1}^{t_0}\bar{e}_j\cdot\bar{\beta}_j\cdot\sum_{i=1}^{2\bar{t}}(\bar{\beta}_j x)^{i-1}\right) \mod x^{2\bar{t}}$$

$\because$ $\left(-(\bar{\beta}_j x)^{2\bar{t}}\right)$ will disappear after $\mod x^{2\bar{t}}$

$$= \sum_{j=1}^{t_0}\bar{e}_j\cdot\bar{\beta}_j\cdot\prod_{j'\neq j}^{t_0}(1-\bar{\beta}_{j'}x)\cdot(1)$$

$$\Rightarrow \boxed{Z_0(x) \text{ is of degree } \leq t_0-1}$$

$\Rightarrow \Lambda(x) \cdot S(x)$ will have coeff zero for all $x^{t_0}, x^{t_0+1}, \dots, x^{2\bar{t}-1}$

Recall $\Lambda(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_{t_0} x^{t_0}$

$S(x) = S_1 + S_2 x + S_3 x^2 + \cdots + S_{2\bar{t}} x^{2\bar{t}-1}$

Coefficient of x^{t_0} is:

$$S_1 \cdot \lambda_{t_0} + S_2 \lambda_{t_0-1} + \cdots + S_{t_0} \cdot \lambda_1 + S_{t_0+1} = 0$$

Coefficient of x^{t_0+1} is

$$S_2 \cdot \lambda_{t_0} + S_3 \cdot \lambda_{t_0-1} + \cdots + S_{t_0+1} \lambda_1 + S_{t_0+2} = 0$$

$\vdots$

Coefficient of $x^{2\bar{t}-1}$ is

$$S_{2\bar{t}-t_0} \lambda_{t_0} + S_{2\bar{t}-t_0+1} \lambda_{t_0-1} + \cdots + S_{2\bar{t}-1} \lambda_1 + S_{2\bar{t}} = 0$$

These are called the generalized Newton

These are called the generalized Newton's identities.

If we rewrite them in a matrix form, we have

$$\underbrace{\begin{bmatrix} S_1 & S_2 & \cdots & S_{t_0} \\ S_2 & S_3 & \cdots & S_{t_0+1} \\ S_3 & S_4 & \cdots & \\ \vdots & & & \\ S_{2\bar{t}-t_0}, & S_{2\bar{t}-t_0+1}, & \cdots & S_{2\bar{t}-1} \end{bmatrix}}_{\triangleq M_{t_0}} \cdot \begin{bmatrix} \lambda_{t_0} \\ \lambda_{t_0-1} \\ \vdots \\ \lambda_1 \end{bmatrix} = - \underbrace{\begin{bmatrix} S_{t_0+1} \\ S_{t_0+2} \\ \vdots \\ S_{2\bar{t}} \end{bmatrix}}_{\triangleq S_{2\bar{t}}^{t_0+1}}$$

General definition where a is not necessarily t_0, but is always $a \leq \bar{t}$

$$M_a \triangleq \begin{bmatrix} S_1 & \cdots & S_a \\ & & \vdots \\ & & S_{2\bar{t}-1} \end{bmatrix}$$

$$S_{2\bar{t}}^{a+1} = \begin{bmatrix} S_{a+1} \end{bmatrix}$$

$$S_{2\bar{t}}^{a+1} = \begin{bmatrix} S_{a+1} \\ \vdots \\ S_{2\bar{t}} \end{bmatrix}$$

Theorem: Suppose $t_0 \leq \bar{t}$. We then have

① $$M_{t_0} \cdot \begin{bmatrix} \lambda_{t_0} \\ \vdots \\ \lambda_1 \end{bmatrix} = -S_{2\bar{t}}^{t_0+1}$$

(2.1) For any $a \leq t_0 - 1$, the following equation has no feasible solution

$$M_a \cdot \begin{bmatrix} z \\ \\ \end{bmatrix} = -S_{2\bar{t}}^{a+1}$$

(2.2) $M_{t_0} \cdot z = -S_{2\bar{t}}^{t_0+1}$ has exactly one solution. (i.e. the solution described in ①)

---

proof: ① is true by examining $Z_0(x) = \Lambda(x) \cdot S(x)$.

(2.2) is proven by noting that

$$\underbrace{\overbrace{\begin{bmatrix} S_1 & S_2 & \cdots & S_{t_0} \\ & & & \vdots \\ & & & \vdots \\ & & & S_{2\bar{t}-1} \end{bmatrix}}^{t_0-1}}_{= M_{t_0}} \left.\right\}{\scriptstyle 2\bar{t}-t_0} \begin{bmatrix} z \end{bmatrix} = - \underbrace{\begin{bmatrix} \\ \\ \\ \end{bmatrix}}_{S_{2\bar{t}}^{t_0+1}}$$

By the $\boxed{\text{property}}$ before $\boxed{}$ is full rank $\Rightarrow$ (2.2) ✓

(2.1)

$$\overbrace{\begin{bmatrix} S_1 & S_2 & \cdots & S_a \\ & & & S_{a+1} \\ & & & \vdots \\ S_{1+t_0-a} & & & S_{t_0} \\ & & & \vdots \\ S_{2t_0-a} & & & S_{2t_0-1} \\ & & & \\ & & & S_{2\bar{t}-1} \end{bmatrix}}^{a-1} \left.\right\}{\scriptstyle 2\bar{t}-a} \begin{bmatrix} z \end{bmatrix} = - \begin{bmatrix} S_{a+1} \\ \vdots \\ S_{t_0+1} \\ \vdots \\ S_{2t_0} \\ \\ S_{2\bar{t}} \end{bmatrix}$$

$$\begin{bmatrix} & & \\ & & S_{2t-1} \end{bmatrix} \qquad \begin{bmatrix} \\ S_{2t} \end{bmatrix}$$

$$= M_a$$

Suppose we can find such $\vec{z}$.

Then by examining the red box we have

$$\begin{bmatrix} S_1 & \cdots & S_{1+t_0-a} & \cdots & S_{t_0} \\ \vdots & & & & \vdots \\ & & & & S_{2t_0-1} \end{bmatrix} \cdot \begin{bmatrix} \underbrace{0}_{t_0-a} \\ \underbrace{\vec{z}}_{a} \end{bmatrix} = - \begin{bmatrix} S_{t_0+1} \\ \vdots \\ S_{2t_0} \end{bmatrix}$$

$\Rightarrow$ there are two solutions to the above equation. One is the solution in ① $\begin{bmatrix} \lambda_{t_0} \\ \vdots \\ \lambda_1 \end{bmatrix}$ and the other is $\begin{bmatrix} 0 \\ \vec{z} \end{bmatrix}$

This is not possible because

$\begin{bmatrix} \; \end{bmatrix}$ is full rank by $\boxed{\text{property}}$

is full rank by $\boxed{\text{property}}$

This theorem says that when assuming $t_0 \le \bar{t}$, finding the $\Lambda(x) = 1 + \lambda_1 x + \cdots + \lambda_{t_0} x^{t_0}$ is equivalent to find the smallest $\underline{a}$ such that we can still satisfy

$$M_a \cdot \begin{bmatrix} \lambda_a \\ \vdots \\ \lambda_1 \end{bmatrix} = -S_{2\bar{t}}^{a+1}$$

Two ways to solve such a, and $\begin{bmatrix} \lambda_a \\ \vdots \\ \lambda_1 \end{bmatrix}$

Method #1: Peterson-Gorenstein-Zierler

$\boxed{\text{Try } a = \bar{t}, \text{ then try } a = \bar{t}-1, \cdots \text{ until } a = 1}$

Set $a = \bar{t}$, check.

$$\begin{bmatrix} S_1 & \cdots\cdots & S_a \end{bmatrix}$$

$$\begin{bmatrix} S_1 & \cdots & S_a \\ & & \\ S_a & & S_{2a-1} \end{bmatrix} = \text{full rank?}$$

If not set $a = a-1$, repeat.

Lemma: Assuming $t_0 \leq \bar{t}$, this process will stop at $a = t_0$. By $\boxed{\text{property}}$

(We don't care if $t_0 > \bar{t}$)

After finding $a = t_0$

Solve
$$\begin{bmatrix} S_1 & \cdots & S_{t_0} \\ \vdots & & \\ \vdots & & \\ & & S_{2t_0-1} \end{bmatrix} \begin{bmatrix} \lambda_{t_0} \\ \vdots \\ \lambda_1 \end{bmatrix} = -S_{2t_0}^{t_0+1}$$

Lemma: Assuming $t_0 \leq \bar{t}$, the above process will find the correct $\Lambda(x) = 1 + \lambda_1 x + \cdots + \lambda_{t_0} x^{t_0}$

Method #2: Berlekamp - Massey

Try $a=1$, then $a=2$, until $a=t$

* Given <u>any</u> $S_1 \cdots S_{2t}$ array.
Berlekamp-massey find the the smallest <u>a</u> value such that

$$M_a \cdot \begin{bmatrix} z \\ \\ \end{bmatrix} = -S_{2t}^{a+1}$$

It is als called the linear feedback shift register problem

* the output a may be anything between $1 \le a \le 2t-1$.
* The solution of z may not be unique.
* However, when assuming $S_1 \cdots S_{2t}$ are syndromes caused by $t_0 \le t$ errors
Since it finds the "smallest" such a, by Theorem, $\Rightarrow$ the result is exactly

the $\Lambda(x)$ we are looking for.

The construction is VERY neat.
Please see directly the 6 paged paper Massey, 69, "Shift register synthesis and BCH decoding"

B-M algorithm

Definition: for any $f(x)$, with deg d we say $f(x)$ generates $S_1\ S_2\ S_3 \cdots, S_a$

$$S_{d+1} + f_1 S_d + \cdots\cdots + f_d S_1 = 0$$
$$S_{d+2} + f_1 S_{d+1} + \cdots\cdots + f_d S_2 = 0$$
$$\vdots$$
$$S_a + f_1 S_{a-1} + \cdots\cdots + f_d S_{a-d} = 0$$

A more precise/accurate defn is

$$\boxed{S_b = (-1) \cdot \sum_{i=1}^{d} f_i S_{b-i} \quad \text{for all } b \in [d+1, a].}$$

A

for all $b \in [a+1, a]$.

It's actually a bit different than the equations. $\boxed{A}$

We will compute $\lambda^{(a)}(x)$ as a smallest degree polynomial $f(x)$ that generates $S_1, \cdots, S_a$

If $S_1, \cdots S_a$ are all zero, or empty string

we define $\lambda^{(a)}(x) = 1$ as conversion

Straightforward if using $\boxed{A}$

If $S_1 = 0, S_2 = 0, \cdots, S_{a-1} = 0, S_a \neq 0$.

We define $\lambda^{(a)}(x)$ can be anything ~~of the~~ form $\lambda^{(a)}(x) = 1 + bx^a$ where b can be arbitrary as conversion

Straightforward if using $\boxed{A}$

This is to create the $\lambda^{(a)} = 1 - S_a x^a$ for the first $S_a \neq 0$

Define $\lambda^{(0)}(x) = 1$ $B(x) = 1$ $b = 1$ $\ell = -1$

$S_a \neq 0$

Define $\lambda^{(0)}(x) = 1$. $\boxed{B(x) = 1,\ b = 1,\ \rho = -1}$

Obviously $\lambda^{(0)}(x)$ is the smallest $f(x)$ generates the empty string ϕ

For $a = a_0 + 1$, define $l_0 = \deg(\lambda^{(a_0)}(x))$

We compute
$$d = S_a + \lambda_1^{(a_0)} S_{a-1} + \lambda_2^{(a_0)} S_{a-2} + \cdots + \lambda_{l_0}^{(a_0)} \cdot S_{a-l_0}$$

If $d = 0$,

$$\lambda^{(a)}(x) = \lambda^{(a_0)}(x)$$

If $d \neq 0$

$$\lambda^{(a)}(x) = \lambda^{(a_0)}(x) - d \cdot b^{-1} \cdot x^{a_0 - \rho} \cdot B(x)$$

If $\deg(\lambda^{(a)}(x)) > \deg(\lambda^{(a_0)}(x))$

then $B(x) = \lambda^{(a_0)}(x)$

$b = d$

$\rho = a_0$

$B(x)$ is updated if the $\deg(\lambda^{(a)}(x))$ is changed.

$B(x)$ then store the prev. version.

b stores the previous d.

ρ stores the index (a_0) of the prev. version.

Run the algorithm until $a = 2\bar{t}$

the final $\lambda^{(2\bar{t})}(x)$ may have

① $\deg(\lambda^{(2\bar{t})}(x)) > \bar{t} \Longrightarrow$ Abort

② $\lambda^{(2\bar{t})}(x)$ may have repeated roots

$\Longrightarrow$ Abort

If neither ① nor ②

then set $t_0 = \deg(\lambda^{(2\bar{t})}(x))$, $\Lambda(x) = \lambda^{(2\bar{t})}(x)$

$$= 1 + \sum_{i=1}^{t_0} \lambda_i x^i$$

---

let β^{k_i}, $i = 1, \cdots, t_0$ be the t_0 distinct roots of $\Lambda(x)$.

the location indices are $l_i = -k_i$