這是說明的內容 12,9

解碼的概念 (RS 碼)

因爲 RS 碼的字母不一定只有 0 與 1 , 而是 $GF(2^r)$ 中的元素 , 所以當錯誤產生的時候 , 不但要找出錯誤的位置 (Location) , 而且要知道錯的量有多大 (Magnitude) 。爲了方便起見 , 錯誤的位置用錯誤數 (Error Location Number) 來表示 : 以 β^{j-1} 表示第 j 個位置 , 於是位置依次爲 $1, \beta, \beta^2, \cdots, \beta^{j-1}$ $(n = 2^r - 1)$, 至於錯誤數自然是 $GF(2^r)$ 中的元素 。

例. 在 $RS(8,3)$ 中 , 傳 $\mathrm{v} = \beta^3\beta^4 10000$, 收到 $\mathrm{w} = \beta^3\beta^4\beta^5 0000$, 則 $\mathrm{e} = 00\beta^4 0000$, 因爲 $\beta^4 + \beta^5 = \beta^4(1+\beta) = \beta^7 = 1$; 這裡的錯誤位置爲 β^2 , 錯誤數爲 β^4 。

接下來探討如何用一個演算法來解碼 。

首先 , 令 $C = RS(2^r, \delta)$ 碼的生成多項是爲 $g(x) = (x + \beta^{m+1})(x + \beta^{m+2}) \cdots (x + \beta^{m+\delta-1})$, 其中 β 爲 $GF(2^r)$ 的一個本元 (primitive 元素) ; 由於 $d(C) \geq \delta$, 令 $t = \lfloor \frac{\delta-1}{2} \rfloor$, $a_1, a_2, \cdots, a_e$ 與 $b_1, b_2, \cdots, b_e$ 分別爲錯誤位置和錯誤數 , $e \leq t$ 。爲了方便說明 , 令 $a_i = 0$, $e+1 \leq i \leq t$ 。這裡的假設主要來自錯誤位置的個數 , 並非一開始就知道 , 既然我們可以更正 t 個錯誤 , 我們直接假設錯誤的位置爲 $a_1, a_2, \cdots, a_t$; 如果沒有那麼多 , 在過程中也會被發現 , 如此才算是好的演算法 。

現在 , 計算 $\delta-1$ 個徵兆 (Syndromes) $s_j(x) = w(\beta^j)$, $m+1 \leq j \leq m+\delta-1$。

由於 $w(x) = c(x) + e(x)$, $e(x) = \sum_{i=0}^{n-1} e_i x^i$,

$$s_j = w(\beta^j) = e(\beta^j) = \sum_{i=0}^{n-1} e_i(\beta^j)^i = \sum_{i=0}^{n-1} e_i(\beta^i)^j = \sum_{i=1}^{t} b_i a_i^j \text{ 。}$$

這裡 , 我們共有 $\delta - 1$ 個方程式 , 它們將被用來解最多 $2t$ 個未知數 $a_1, a_2, \cdots, a_t$, $b_1, b_2, \cdots, b_t$ 。不過 , 這裡的方程式都不是線性方程式 , 所以比較複雜些 。

令 $\sigma_r(x) = (a_1 + x)(a_2 + x) \cdots (a_t + x)$

$$= \sigma_0 + \sigma_1 x + \cdots + \sigma_{t-1} x^{t-1} + x^t \qquad (*)$$

爲了解 $a_1, a_2, \cdots, a_t$; 先要求出 $\sigma_0, \sigma_1, \cdots, \sigma_{t-1}$ 。((註) 一但有了 (*) , 就可以依次代入 $GF(2^r)$ 中的元素來判斷那些元素是 $a_1, a_2, \cdots, a_t$ 。) 現在把 (*) 中的 x 以 a_i 代入 , 並且兩邊同乘 $\sum_{i=1}^{t} b_i a_i^j$, 於是

$$0 = \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_0 + \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_1 a_i + \cdots + \left(\sum_{i=1}^{t} b_i a_i^j\right)\sigma_{t-1} a_i^{t-1} + \left(\sum_{i=1}^{t} b_i a_i^j\right) a_i^t$$

$$= s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+t-1}\sigma_{t-1} + s_{j+t}$$

所以 $s_{j+t} = s_j\sigma_0 + s_{j+1}\sigma_1 + \cdots + s_{j+t-1}\sigma_{t-1}$。
現在利用已知的 $s_{m+1}, s_{m+2}, \cdots, s_{m+2t}$，可以求得

$$\begin{bmatrix} s_{m+1} & s_{m+2} & \cdots & s_{m+t} \\ s_{m+2} & s_{m+3} & \cdots & s_{m+t+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m+t} & s_{m+t+1} & \cdots & s_{m+2t-1} \end{bmatrix} \begin{bmatrix} \sigma_0 \\ \sigma_1 \\ \vdots \\ \sigma_{t-1} \end{bmatrix} = \begin{bmatrix} s_{m+t+1} \\ s_{m+t+2} \\ \vdots \\ s_{m+2t} \end{bmatrix} \qquad (**)$$

由於 (**) 中最左邊的矩陣 M 可以寫成以下的型式，所以該矩陣可逆，$\sigma_0, , \sigma_1, \cdots, \sigma_{t-1}$ 也可以順利解出來，當然這是在有 t 個錯誤時的狀況，如果有些 $a_i = 0$，則可以由它的階數 (Rank) 看出。

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_t \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{t-1} & a_2^{t-1} & \cdots & a_t^{t-1} \end{bmatrix} \begin{bmatrix} b_1 a_1^{m+1} & 0 & \cdots & 0 \\ 0 & b_2 a_2^{m+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_t a_t^{m+1} \end{bmatrix} \begin{bmatrix} 1 & a_1 & \cdots & a_1^{t-1} \\ 1 & a_2 & \cdots & a_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_t & \cdots & a_t^{t-1} \end{bmatrix}$$

有了 $\sigma_0, , \sigma_1, \cdots, \sigma_{t-1}$ 可以求出 $a_1, a_2, \cdots, a_t$；在利用

$$\begin{bmatrix} a_1^{m+1} & a_2^{m+1} & \cdots & a_t^{m+1} \\ a_1^{m+2} & a_2^{m+2} & \cdots & a_t^{m+2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{m+t} & a_2^{m+t} & \cdots & a_t^{m+t} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix} = \begin{bmatrix} s_{m+1} \\ s_{m+2} \\ \vdots \\ s_{m+t} \end{bmatrix} \qquad (***)$$

就可以算出 $b_1, b_2, \cdots, b_t$。

演算法：

1. 計算 $s_j(x) = w(\beta^j)$，$m+1 \le j \le m+2t$。

2. 求 $M' = \left[\begin{array}{c|c} & s_{m+t+1} \\ M & s_{m+t+2} \\ & \vdots \\ & s_{m+2t} \end{array}\right]$。

3. 解 (**)。

4. 求出 $a_1, a_2, \cdots, a_t$ (用代入法 , 或解方程式。)

5. 求 $b_1, b_2, \cdots, b_t$ (用 (***))。

例. $RS(2^4, 7)$ 碼 , $g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)(\beta^4+x)(\beta^5+x)$, $m = -1$, $t = 3$, $GF(2^4) = {Z_2[x]}/{< 1+x+x^4 >}$

$w(x) = 1 + \beta^4 x + \beta x^3 + \beta^9 x^5 + x^6$
$s_0 = w(\beta^0) = \beta^7$
$s_1 = w(\beta^1) = 1$
$s_2 = w(\beta^2) = \beta^9$
$s_3 = w(\beta^3) = \beta^{12}$
$s_4 = w(\beta^4) = \beta^9$
$s_5 = w(\beta^5) = \beta^7$

$$M' = \left[\begin{array}{ccc|c} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 1 & \beta^9 & \beta^{12} & \beta^9 \\ \beta^9 & \beta^{12} & \beta^9 & \beta^7 \end{array}\right] \leftrightarrow \left[\begin{array}{ccc|c} \beta^7 & 1 & \beta^9 & \beta^{12} \\ 0 & \beta^{12} & \beta^7 & \beta^6 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

所以 , $wt(e) = 2$, $\left[\begin{array}{cc} \beta^7 & 1 \\ 1 & \beta^9 \end{array}\right]\left[\begin{array}{c} \sigma_0 \\ \sigma_1 \end{array}\right] = \left[\begin{array}{c} \beta^9 \\ \beta^{12} \end{array}\right]$

求得 $\sigma_0 = \beta^6$, $\sigma_1 = \beta^{10}$
$\sigma_A(x) = \beta^6 + \beta^{10}x + x^2$, 於是 $a_1 = \beta^2$, $a_2 = \beta^4$。

再利用 $\left[\begin{array}{cc} 1 & 1 \\ \beta^2 & \beta^4 \end{array}\right]\left[\begin{array}{c} b_1 \\ b_2 \end{array}\right] = \left[\begin{array}{c} \beta^7 \\ 1 \end{array}\right]$ 求得 $b_1 = \beta^2$, $b_2 = \beta^{12}$。

所以 $\mathrm{c} = \mathrm{w} + \mathrm{e} = 1\beta^4\beta^2\beta\beta^{12}\beta^9 100000000$。

問題. 同上例子的數碼 , 解碼下列兩個收到的字 。

(1) $0\beta^3\beta\beta^5\beta^3\beta^2\beta^6\beta^{10}\beta 000000$ 。

(2) $\beta 0\beta^7 0\beta^{12}\beta^3\beta^3 10000000$ 。