

代数系と符号理論 第13回板書プリント

植松友彦 2007.6.22

1 BCH 符号と RS 符号

1.1 BCH 符号の構成例

いま、 α を原始既約多項式 $x^4 + x + 1$ の根とし、 α を原始元とする有限体 F_{16} を考えよう。このとき、 F_{16} に属する各元の F_2 上の最小多項式は下の表のようになる。

元	最小多項式
1	$x + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$x^4 + x^3 + 1$

この表を利用して、符号長 15 で、 t 個の誤りを訂正できる BCH 符号の生成多項式を求めると下の表を得る。尚、有限体の原始元を用いて生成される BCH 符号のことを「狭義 BCH 符号」と呼ぶ。

t	根	生成多項式	生成多項式の全ての根	最小距離	次元
1	α, α^2	$x^4 + x + 1$	$\alpha, \alpha^2, \alpha^4, \alpha^8$	3	11
2	$\alpha, \alpha^2, \alpha^3, \alpha^4$	$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$	5	7
3	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$	$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \times (x^2 + x + 1)$	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12}$	7	5
4	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8$	$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \times (x^2 + x + 1)(x^4 + x^3 + 1)$	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$	15	1

他方、 $\beta = \alpha^3$ の位数が 5 なので、これを利用して、符号長 5 の BCH 符号を構成すると、以下の表のようになる。このように、有限体の原始元以外の元を利用して構成する BCH 符号のことを「広義 BCH 符号」と呼ぶ。

t	根	生成多項式	生成多項式の全ての根	最小距離	次元
1	β, β^2	$x^4 + x^3 + x^2 + x + 1$	$\beta, \beta^2, \beta^3, \beta^4$	5	1
2	$\beta, \beta^2, \beta^3, \beta^4$	$x^4 + x^3 + x^2 + x + 1$	$\beta, \beta^2, \beta^3, \beta^4$	5	1

1.2 BCH 符号と RS 符号の比較

例えば、 $n = 15$ において、

$$g(x) = \frac{x^{15} - 1}{x - 1} = x^{14} + x^{13} + x^{12} + \cdots + x + 1$$

は BCH 符号の生成多項式でもあるし、 F_{16} 上の RS 符号の生成多項式でもある。BCH 符号は 2 元であるから符号語は 0 と $g(x)$ しかない。他方、RS 符号は 16 元符号であるから、 $c \in F_{16}$ に対して、 $cg(x)$ は全て符号語であり、符号語は 16 個ある。このような BCH 符号と RS 符号の比較を表にまとめておく。但し α は F_{2^m} の原始元とする。

	BCH 符号	RS 符号
巡回符号	○	○
符号語の成分	F_2	F_{2^m}
符号長 n	$2^m - 1$ ($m = 1, 2, \dots$)	$2^m - 1$
設計距離 d_{des}	$d_{des} = 2t + 1$	d_{des} ($1 \leq d_{des} \leq n$)
最小距離 d	$d \geq d_{des}$	$d = d_{des}$
次元 k	$k \geq n - mt$	$k = n - d + 1$
符号語数	2^k	2^{mk}
生成多項式 $g(x)$	$\text{LCM}\{m_1(x), m_3(x), \dots, m_{2t-1}(x)\}$ $m_i(x)$: α^i の最小多項式	$(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1})$