巡回符号における定義集合の相反的な性質について
On the Reciprocal Property of the Defining Set for Cyclic Codes

鄭　俊如 *　　戒田　高康 **
(*九州女子大学人間科学部) (**近畿大学産業理工学部)

1　はじめに

巡回符号の定義集合は，最小距離の限界を計算するための重要なパラメータとしてよく知られている．例えば，BCH 限界の計算は，定義集合の最大連続要素の個数で決められ，HT 限界の計算は，同間隔で一定の長さの連続要素の数で決められる．本稿では，まず巡回符号の定義集合について述べ，次に，定義集合の相反的な性質について議論する．

2　定義集合の相反的な性質

巡回符号 C は，有限体 $F = GF(q)$ 上の符号長 $n(q = p^m$，p は素数，m は正の整数，$\gcd(n, p) = 1$ とする) の $x^n - 1$ を割り切る多項式 $g(x)$ で生成され，多項式環 $F[x]/(x^n - 1)$ 上のイデアルである．E は有限体 F の拡大体であり，α は拡大体 E の元で，1 の原始 n 乗根とする．また，$\#A$ は集合 A の濃度，すなわち，要素の個数とする．

定義 1 有限体 F 上の $i \in Z_n$ のサイクロトミック集合（*cyclotomic set*）は

$$cs(i) = \{iq^r | 0 \le r < n\}$$

と定義する．特に，$Z_n \ni s = \min cs(i)$ ならば，$R_s = cs(i)$ と書く．

定義 2 定義集合 $D = \cup_{t=1}^{r} R_{s_t}$ に対して，D を持つ巡回符号 $C = C(D)$ は次のように定義する．

$$C = \{\boldsymbol{c} \in F^n \mid c(\alpha^i) = 0, {}^{\forall} i \in D\},$$

なお，$c(x) = \sum_{i=0}^{n-1} c_i x^i$ はベクトル $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$ からなる拡大体 E 上の多項式である．

本稿では，定義 1 で定義しているような 1 個のサイクロトミック集合，或いは幾つのサイクロトミック集合の和集合を完全な定義集合と呼ぶ．巡回符号 $C = C(D)$ は，完全な定義集合 D と 1 対 1 対応する．

定義 3 巡回符号 C の最小距離は次のように定義する．

$$d(C) = \min\{w(\boldsymbol{c}) \mid \boldsymbol{c} \in C \backslash \{\boldsymbol{0}\}\},$$

なお，$w(\boldsymbol{c}) = \#\{0 \le i < n | c_i \ne 0\}$ は，ベクトル $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$ のハミング重みである．

定義集合の連続要素のあり方によって，巡回符号の最小距離の限界の値が変わっていく．また，定義集合に次の性質が持っている．

性質 1 定義集合 D を持つ符号長 n の巡回符号 C に対して，b は $\gcd(b, n) = 1$ となるような正の整数とすると，b と $n - b$ に対する定義集合 D の *1* を除いたその他の要素は対称となる．

例 1 C は符号長 *21*，定義集合 $D = R_{1,3,7,9} = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18\}$ を持つ *2* 元巡回符号とする．条件 $\gcd(b, n) = 1$ を満足する，すなわち，符号長 n と互いに素な b の集合は，$b = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ となる．全ての b に対応する定義集合の要素は次の表で表し，b と $n - b$ に対する定義集合 D の要素（*1* を除く）は対称であることを示した． 例えば，$b = 5$ の時の *1* を除いた定義集合の要素は，$\{6, 11, 16, 15, 4, 9, 14, 3, 8, 18, 2, 7, 12\}$ となることに対して，$b = n - 5 = 16$ の時の *1* を除いた定義集合の要素は $\{12, 7, 2, 18, 8, 3, 14, 9, 4, 15, 16, 11, 6\}$ となり，定義集合の要素は対称となることが分かる．

b	定義集合 $D = R_{1,3,7,9}$
1	*1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18*
2	*1, 3, 7, 9, 11, 15, 2, 4, 6, 8, 12, 14, 16, 18*
4	*1, 9, 4, 8, 12, 16, 3, 7, 11, 15, 2, 6, 14, 18*
5	*1, 6, 11, 16, 15, 4, 9, 14, 3, 8, 18, 2, 7, 12*
8	*1, 9, 4, 12, 7, 15, 2, 18, 8, 16, 3, 11, 6, 14*
10	*1, 11, 9, 8, 18, 7, 6, 16, 15, 4, 14, 3, 2, 12*
11	*1, 12, 2, 3, 14, 4, 15, 16, 6, 7, 18, 8, 9, 11*
13	*1, 14, 6, 11, 3, 16, 8, 18, 2, 15, 7, 12, 4, 9*
16	*1, 12, 7, 2, 18, 8, 3, 14, 9, 4, 15, 16, 11, 6*
17	*1, 18, 14, 6, 2, 15, 11, 7, 3, 16, 12, 8, 4, 9*
19	*1, 18, 16, 14, 12, 8, 6, 4, 2, 15, 11, 9, 7, 3*
20	*1, 18, 16, 15, 14, 12, 11, 9, 8, 7, 6, 4, 3, 2*

3　まとめ

巡回符号 C に対して，符号長 n と互いに素な正の整数 b を用いて，最小距離の限界を計算する方法がある．Roos 限界はその手法を用いる限界としてよく知られている．b の選び方によって，Roos 限界の値に大きく影響を及ぼすため，Roos 限界を計算する際，全ての b に対して計算する必要がある．しかし，本稿で示した性質を用いると，半数の b について計算すれば良いことになり，計算量の削減ができるようになる．

参考文献

[1] M.van Eupen, J.H.van Lint, “On the minimum distance of ternary cyclic codes”, *IEEE Transaction on Information Theory*, Vol.39, No.2, pp.409-422, 1993.
[2] C.R.P.Hartmann, K.K.Tzeng, “Generalizations of the BCH bound”, *Information and Control*, Vol.20, pp.489-498, 1972.
[3] J. L. Massey, “Shift-register synthsis and BCH decoding”, *IEEE Transaction on Information Theory*, vol.IT-15, pp.122-127, Jan., 1969.
[4] R.Pellikaan, “The shift bound for cyclic, Reed-Muller and geometric Goppa codes”, *Arithmetic, Geometry and Coding Theory 4*, pp.155-174, Walter de Gruyter & Co, Berlin, 1996.
[5] W.W.Peterson, E.J. Weldon, Jr., “Error Correcting Codes”, *2nd ed. Cambridge*, MA: MIT Press, 1972.