Some Generalizations of the BCH Bound

山口大学経済学部

柏木　芳美

1 はじめに

巡回符号という実用上重要な符号がある．その最小重さは BCH bound と呼ばれるもので評価される．それを改良した HT bound, Roos bound，Roos bound の変形を紹介する．

2 諸定義

- q を素数巾，$F = \mathrm{GF}(q)$ を位数 q の有限体，n を自然数とする．F^n の部分空間を長さ n の符号(code) という．基底が固定されていることに注意すること．

- C を次元が k で長さが n の符号とする．C の基底を行とする (k, n) 行列を C の生成行列という．

- $\mathbf{x} = (x_1, \cdots, x_n)$，$\mathbf{y} = (y_1, \cdots, y_n) \in F^n$ $(x_i,\ y_i \in F)$ に対して内積を

$$(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$$

により定める．

C を符号としたとき，

$$C^{\perp} = \{\mathbf{x} \in F^n \mid (\mathbf{x}, \mathbf{u}) = 0 \text{ for } \mathbf{u} \in C\}$$

により C の双対符号 (dual code) を定める．$C^{\perp}$ の生成行列を C のパリティ検査行列(parity check matrix) という．

- $\mathbf{u} = (u_1, u_2, \cdots, u_n) \in F^n$ としたとき，

$$w(\mathbf{u}) = |\{i \in \{1, \cdots, n\} : u_i \neq 0\}|$$

を元 $\mathbf{u}$ の weight(重さ) という.

C を $\{\mathbf{0}\}$ とは異なる符号とする.

$$\min\{w(\mathbf{u}) \,|\, \mathbf{u} \in C \setminus \{\mathbf{0}\}\}$$

を C の最小重さといい,

$$d(C)$$

と書くことにする.

$\dim C$ は送信できる情報量を表し，大きければ大きいほどよい. $d(C)$ は訂正できる誤りの量を表し，これも大きければ大きいほどよい．一方，これらには，Singleton bound

$$d(C) \leqq n - \dim C + 1$$

というトレイドオフの関係がある.

- C を長さ n の符号とする．$(u_1, u_2, \cdots, u_n)$ が C の元ならその巡回シフト $(u_n, u_1, \cdots, u_{n-1})$ も C の元であるとき，C は巡回符号(cyclic code) と呼ばれる.

  巡回符号は剰余環 $F[x]/(x^n - 1)$ のイデアルと同じものである.

- 以下，$(n, q) = 1$ とする．このとき，$x^n - 1$ は重根を持たない. モニックな F 係数の多項式 $g(x)$ が $x^n - 1$ を割るとする．剰余環 $F[x]/(x^n - 1)$ において $g(x)$ の生成するイデアルは巡回符号になり，任意の巡回符号はこの形で得られる．この巡回符号は

  $$< g(x) >$$

と書かれ，$g(x)$ はこの巡回符号の生成多項式といわれる．

$$\dim <g(x)>= n - \deg g(x)$$

となる．尚，巡回符号の元は，$n-1$ 次以下の多項式として扱うこともあるし，1，x，x^2，$\cdots$，x^{n-1} $(\bmod (x^n-1))$ を基底とする行ベクトルとして扱うこともある．

- 巡回符号はその生成多項式を定めれば定まる．ところで生成多項式は x^n-1 を割るので，その根は1の n 乗根である．

  C を巡回符号とし，N を1の n 乗根からなる集合とする．C の元を多項式と見る．$u(x) \in C$ であるための必要十分条件がすべての N の元 α に対して $u(\alpha)=0$ であるとき，N は C を定めるあるいは C は N で定まるということにする．

- $g(x) \in F[x]$ を既約な多項式とする．α を1の原始 n 乗根の1つとする．α^l $(0 \leqq l \leqq n-1)$ が $g(x)$ の根ならば，$(\alpha^l)^q = \alpha^{lq}$ も $g(x)$ の根である．従って，$g(x)$ の根全体は

  $$\{\alpha^l, \alpha^{lq}, \alpha^{lq^2}, \alpha^{lq^3}, \cdots\}$$

  の形をしている．肩の

  $$\{l, lq, lq^2, lq^3, \cdots\}$$

  を cyclotomic coset という．ただし，modulo n で考えている．

  生成多項式を既約因子に分解する．各既約因子は適当な cyclotomic coset の集合に対応している．このように，cyclotomic coset の集合を指定すれば巡回符号は定まる．

例 1. この例 ([7, Roos, Example 1, 1983]) はこれ以降でも再三使う．$n = 21$，$q = 2$ とする．α を 1 の原始 21 乗根の 1 つとする．1，3，7，9 を含む cyclotomic cosets は

$$\{1, 2, 4, 8, 16, 11\}, \qquad \{3, 6, 12\}, \qquad \{7, 14\}, \qquad \{9, 15, 18\}$$

となる．i を $n - 1 = 20$ 以下の奇数かまたは 0 とする．α^i を根に持つ monic な既約多項式を $m_i(x)$ と書くことにする．上の cyclotomic cosets に対応する既約多項式は $m_1(x)$，$m_3(x)$，$m_7(x)$，$m_9(x)$ となる．

$$g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$$

とおくと，$g(x)$ の根は

$$\{\alpha^i \mid i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18\} \tag{1}$$

となる．

$$C = < g(x) >$$

が今後具体例として扱う符号である． □

3 BCH bound

Bose と Ray-Chaudhuri([1, 1960]) および Hocquenghem([3, 1959]) は，巡回符号の最小重さに関する次の評価式を与えた．これは，最も基本的なものである．

命題 1 (BCH bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b を自然数，δ を 2 以

上の自然数として，連続した $\delta-1$ 個の

$$\alpha^{b+i} \quad (0 \leqq i \leqq \delta-2)$$

が $g(x)$ の根ならば，C の最小重さは δ 以上である．この δ を C の designed distance と呼ぶことがある．

言葉 M を1の n 乗根からなる集合とし，b，l を自然数とする．

$$M=\{\alpha^{b+i}\,|\,0 \leqq i \leqq l\}$$

となる1の原始 n 乗根 α が存在するとき，M を(1の n 乗根の) consecutive set という．また，巡回符号 C の生成多項式 $g(x)$ の根全体の集合が M を含むとき，C は M を consecutive set に持つという． □

例 2. 例1の巡回符号 $C=<g(x)>$ を考える．式(1)より，$g(x)$ はある1の原始 n 乗根 α を用いて

$$\{\alpha^i\,|\,i=1,2,3,4,6,7,8,9,11,12,14,15,16,18\}$$

をすべての根とした．C は例えば

$$\{\alpha^i\,|\,i=1,2,3,4\}$$

を consecutive set に持つ($\delta=5$)．よって BCH bound より，$d(C) \geqq 5$ となる．

尚，

$$\{\alpha^i\,|\,i=6,7,8,9\}$$

も consecutive set であることを注意しておく． □

1 の原始 n 乗根の取り方を変えると，consecutive set は次のような形になる．

α，β を 1 の原始 n 乗根とする．$\alpha = \beta^{c_1}$ となる自然数 c_1 が存在するが，α が原始 n 乗根なので $(n, c_1) = 1$ となる．b，l を自然数とし $f = bc_1$ とおくと，α に関する consecutive set

$$\alpha^b, \qquad \alpha^{b+1}, \qquad \alpha^{b+2}, \qquad \cdots, \qquad \alpha^{b+l}$$

は β を用いて

$$\beta^{c_1 b} = \beta^f, \qquad \beta^{f+c_1}, \qquad \beta^{f+2c_1}, \qquad \ldots, \qquad \beta^{f+lc_1}$$

と書ける．また逆に，下の形の集合は，上の形の α に関する consecutive set になる．

原始 n 乗根の取り方を考慮して BCH bound を書き直すと次のようになる．

命題 2. C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b を自然数，δ を 2 以上の自然数，c_1 を $(n, c_1) = 1$ となる自然数とする．

$$\alpha^{b+i_1 c_1} \quad (0 \leqq i_1 \leqq \delta - 2)$$

が $g(x)$ の根ならば，C の最小重さは δ 以上である．

4 HT bound

Hartmann と Tzeng は，命題 2 の形の BCH bound を次のように一般化した ([2, 1972]).

命題 3 (HT bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を1の原始 n 乗根の1つとする．b，s を自然数，δ を2以上の自然数とする．c_1 を $(n, c_1) = 1$ となる自然数とし，c_2 を $(n, c_2) < \delta$ となる自然数とする．このとき，

$$\alpha^{b+i_1c_1+i_2c_2} \quad (0 \leqq i_1 \leqq \delta - 2, \quad 0 \leqq i_2 \leqq s)$$

が $g(x)$ の根ならば，C の最小重さは $\delta + s$ 以上である．

例 3. 例2の巡回符号 C を考える．

$$\{\alpha^i \mid i = 1, 2, 3, 4\}, \qquad \{\alpha^i \mid i = 6, 7, 8, 9\}$$

は C の consecutive sets であった．命題3で

$$b = 1, \qquad c_1 = 1, \qquad c_2 = 5, \qquad \delta = 5, \qquad s = 1$$

として

$$b + i_1c_1 + i_2c_2 = 1 + i_1 + 5i_2 \qquad (0 \leqq i_1 \leqq 3, \quad 0 \leqq i_2 \leqq 1)$$

を考える．$i_2 = 0$ なら $1 + i_1$ は，1，2，3，4 になる．$i_2 = 1$ なら $6 + i_1$ は，6，7，8，9 になる．従って HT bound (命題 3) より，$d(C) \geqq \delta + s = 6$ となる．

BCH bound は5だったので改良されている． □

5 Roos bound

Roos は HT bound をさらに一般化した ([6, 1982]).

命題 4 (Roos bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b，s_i を自然数 $(1 \leqq i \leqq k)$，δ を 2 以上の自然数とする．c_i $(1 \leqq i \leqq k)$ を $(n, c_1) = 1$，$(n, c_j) < 2 + s_1 + s_2 + \cdots + s_{j-1}$ $(2 \leqq j \leqq k)$ となる自然数とする．このとき，

$$\alpha^{b+i_1c_1+i_2c_2+\cdots+i_kc_k} \quad (0 \leqq i_t \leqq s_t\,(1 \leqq t \leqq k))$$

が $g(x)$ の根ならば，C の最小重さは

$$2 + s_1 + s_2 + \cdots + s_k$$

以上である．

注意. $\delta - 2 = s_1$ とすると $\delta = 2 + s_1$ である．

6 Roos bound の変形

Roos bound は，命題 4 の形では使いにくい面がある．Roos は [7, 1983] で少し形を変えた．次の記号を導入する．

m を multiplicative order of q modulo n とする ($q^m \equiv 1 \mod n$ となる最小の自然数)．$K = \mathrm{GF}(q^m)(\supset F = \mathrm{GF}(q))$ とおく．

$N = \{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ を 1 の n 乗根からなる集合とする $(N \subset K)$．N に対し，

$$H_N = \begin{pmatrix} \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} & \alpha_1^n(=1) \\ \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} & \alpha_2^n(=1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{n-1} & \alpha_t^n(=1) \end{pmatrix}$$

とおく．巡回符号 C が N で定められると，H_N は C のパリティ検査行列になる．

K 上の長さ n の符号 C_N を

$$C_N = \{\mathbf{u} \in K^n \,|\, H_N \mathbf{u}^t = \mathbf{0}\}$$

により定める．$\mathbf{u} = (u_1, u_2, \cdots, u_n) \in K^n$ $(u_k \in K)$ としたとき，

$$\sum_{k=1}^{n} \alpha_i^k u_k = 0 \iff \sum_{k=1}^{n} \alpha_i^{k+1} u_k = 0 \qquad (i = 1, 2, \cdots, t)$$

なので，C_N は巡回符号になる．

$d_N = d(C_N)$ とおく．巡回符号 C が N で定められているとすると，集合として $C \subset C_N$ なので，

$$d(C) \geqq d_N$$

に注意しておく．

以上の記号の下で Roos は次を示した ([7])．尚，M，N が 1 の n 乗根からなる集合ならば $MN = \{\alpha\beta \,|\, \alpha \in M, \beta \in N\}$ も 1 の n 乗根からなる集合である．

命題 5. M，N を 1 の n 乗根からなる空でない集合とする．このとき，$M \subset \bar{M}$ かつ $|\bar{M}| \leqq |M| + d_N - 2$ を満たす consecutive set $\bar{M}$ が存在すれば，$d_{MN} \geqq |M| + d_N - 1$ となる．

M が必ずしも consecutive でないことがポイントである．

N が consecutive ならば $d_N = |N| + 1$ であることが示される．従って，次が得られる．

系 6. N，M，$\bar{M}$ を命題 5 と同じとする．もし N が consecutive で $|\bar{M}| \leqq |M| + |N| - 1$ ならば $d_{MN} \geqq |M| + |N|$ となる．更に C が MN で定まる巡回符号ならば $d(C) \geqq |M| + |N|$ となる．

例 4. 今までの巡回符号 C を考える．

$$N = \{\alpha^i \,|\, i = 2, 3, 4\} = \{\alpha^2, \alpha^3, \alpha^4\},$$
$$M = \{\beta^j \,|\, j = 0, 1, 3, 5\} = \{1, \beta, \beta^3, \beta^5\} = \{1, \alpha^4, \alpha^{12}, \alpha^{20}\}$$

とする．ただし，$\beta = \alpha^4$ も 1 の原始 21 乗根である ($(21, 4) = 1$ より)．

$$\begin{aligned} MN &= N \cup \alpha^4 N \cup \alpha^{12} N \cup \alpha^{20} N \\ &= \{\alpha^2, \alpha^3, \alpha^4\} \cup \{\alpha^6, \alpha^7, \alpha^8\} \cup \{\alpha^{14}, \alpha^{15}, \alpha^{16}\} \cup \{\alpha, \alpha^2, \alpha^3\} \\ &= \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8, \alpha^{14}, \alpha^{15}, \alpha^{16}\} \end{aligned}$$

となる．

ここで，生成多項式 $g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$ の根を考える．MN の元は $g(x)$ の根となっている．また，$\alpha = \alpha^1$，α^3，$\alpha^7 \in MN$ で，

$$9 \times 2^2 = 36 \equiv 15 \pmod{21}$$

より，$\alpha^{15} \in MN$ となっている．従って，MN で定まる巡回符号は $C = <g(x)>$ である．

次に系 6 を適用する．まず，$N = \{\alpha^i \,|\, i = 2, 3, 4\}$ は consecutive である．

$$\bar{M} = \{\beta^0, \beta^1, \beta^2, \beta^3, \beta^4, \beta^5\} (\supset M)$$

とすると $\bar{M}$ は consecutive である．また，

$$|\bar{M}| = 6 \leqq 4 + 3 - 1 = |M| + |N| - 1$$

となっている．従って，系 6 より

$$d(C) \geqq |M| + |N| = 7$$

となる． □

7 まとめ

巡回符号の最小重さを評価する BCH bound，HT bound，Roos bound および Roos bound を少し変形したものを簡単に紹介した．具体例の巡回符号 C の最小重さの評価は

$$\text{BCH bound} : d(C) \geqq 5,$$
$$\text{HT bound} : d(C) \geqq 6,$$
$$\text{Roos bound の変形} : d(C) \geqq 7$$

と，段々と良い評価が得られている．尚，この例の実際の最小重さは

$$d(C) = 8$$

となることが知られている ([4, Peterson and Weldon, 1972]).

また，$x^n - 1$ を $x^n - a$ $(a \in F \setminus \{0\})$ に変えた符号は constacyclic code と呼ばれるが，今まで述べてきたこととほぼ同様のことが成り立つことが知られている ([5, Radkova and Van Zanten, 2009]).

参考文献

[1] R. C. Bose and D. K. Ray-Chaudhuri, On a class of error-correcting binary group codes, Inform. Contr. 3, pp.68–79, 1960.

[2] C. R. P. Hartmann and K. K. Tzeng, Generalizations of the BCH-bound, Inform. Contr. 20, pp.489–498, 1972.

[3] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres (Paris) 2, pp.147–156, 1959.

[4] W. W. Peterson and E. J. Weldon, JR., Error-Correcting Codes, 2nd ed., MIT Press, Cambridge, Mass., 1972.

[5] D. Radkova and A. J. Van Zanten, Constacyclic codes as invariant subspaces, Linear Alg. and Its Applic. 430, pp.855–864, 2009.

[6] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, J. Comb. Theory Ser. A 33, pp.229–232, 1982.

[7] C. Roos, A new lower bound for the minimum distance of a cyclic code, IEEE Trans. Inform. Theory 29, pp.330–332, 1983.