数理解析研究所講究録
第82巻 1970年 12-22

12

Reed-Muller 符号の重み構造について

大阪大 基礎工 嵩 忠雄

§1 はじめに

以下2値符号について考える。$[GF(2)]^n$ の k 次元部分空間を長さ n，情報点 k の線形符号[1]という。ベクトルの0でない成分の数をその重みという。符号がどのような重みのベクトルから成り立っているかに関する問題が重み構造の問題である。とくに与えられた重みをもつ符号ベクトルの数を与える公式を求めるのが重み分布の問題である。2元対称通話路における誤り検出確率は分布公式から直ちに求まる[1]。

BCH-符号[1,2]，Reed-Muller 符号[1~3]，有限幾何符号[2]など主要な符号を統一的に扱うために多項式符号が導入された[4]。記号の数が素数の巾の場合に容易に拡張できるが，ここでは2値の場合について説明する。m，S を正整数とし，b を 2^S-1 の約数とし，$a=(2^S-1)/b$，$n=(2^{mS}-1)/b$ とおく。$X_1,\cdots,X_m$ を $GF(2^S)$ の上の変数とし，つぎ

のような条件をみたす $GF(2^s)$ の上の $X_1, \cdots, X_m$ に関する多項式全体の集合を $Q(m, s, \mu, b)$ とする。

1) f の任意の項を $C_{\nu_1 \cdots \nu_m} X_1^{\nu_1} \cdots X_m^{\nu_m}$ とすると、$C_{\nu_1 \cdots \nu_m} \neq 0$ ならば、$\sum_{i=1}^{m} \nu_i = jb$, $0 \leq j \leq \mu \leq ma$.

2) $f^2 = f$.

$GF(2^{ms})$ の原始元の一つを α とする。各 $(a_1, \cdots, a_m) \in [GF(2^s)]^m$ に対して、つぎのような $\beta \in GF(2^{ms})$

$$\beta = \sum_{i=1}^{m} a_i \alpha^{i-1}$$

を対応させ、簡単のため $f(\beta) = f(a_1, \cdots, a_m)$ とかく。

$f \in Q(m, s, \mu, b)$ に対して、

$$\bar{v}(f) = (f(\alpha^0), f(\alpha^1), \cdots, f(\alpha^{n-1}))$$

とおく。$\bar{v}(f) \in [GF(2)]^n$

(n, m, s, μ)-多項式符号はつぎのようなベクトルの集合として定義される。

$$\{\bar{v}(f) \mid f \in Q(m, s, \mu, b)\}$$

定義から、容易に (n, m, s, μ)-多項式符号は長さ n の巡回符号であることがわかる。巡回符号は生成多項式によって特性づけられる。

j を 2^{ms} より小さい非負整数とする。j を 2^s 進表示したとき

$$j = \delta_1 + \delta_2 2^s + \cdots + \delta_m 2^{(m-1)s}, \quad 0 \leq \delta_i < 2^s$$

の係数和 $\sum_{i=1}^{m} \delta_i$ を $W_s(j)$ とかく。次の定理が成立する。[4]

定理1：1) α^h が (n, m, s, μ)-多項式符号の生成多項式の根であるための必要十分条件は，h が b で割り切れかつ

$$\min_{0 \leq l < s} W_s(h2^l) = jb, \quad 0 < j < ma - \mu.$$

2) $m(2^s-1)-\mu b$ を 2^s-1 で割った時の商と余りを Q, R とすると，(n, m, s, μ)-多項式符号の最小の重みは少くとも

$$\lceil (R+1)2^{Qs} - 1 \rceil / b$$

定理1：1) より designed distance d, 長さ n, $m_0=1$ の BCH-符号[1,2]（以下 d-BCH-符号という。）は $(n, 1, s, n-d)$-多項式符号に他ならない。また μ 次（修正）Reed-Muller 符号[5]（全パリテイ検査ビットを省き，ベクトル成分の順番を適当に入れかえたもの）は $(n, m, 1, \mu)$-多項式符号である。さらに，ユークリッド幾何符号[2]，射影幾何符号の双対符号もまた多項式符号である。[4]

定理1：2）は一般には最小の重みの下界にすぎないが，i）$R=0$ あるいは ii）$s=1$ あるいは iii）長さ a の R/b-BCH-符号が存在し，その最小の重みが R/b に等しい時は，最小の重みはちょうど $[(R+1)2^{Qs}-1]/b$ に等しく，かつ同じ最小の重みをもつBCH-符号の部分符号となっている。(4)

以下，$b=1$ すなわち $n=2^{ms}-1$ の場合を考える。全パリテイ検査ビット一つを付け加えて得られる長さ $n+1$ の符号をもとの符号の拡大符号というが，$b=1$ の多項式符号の拡大符号はベクトル成分の位置に関するある2重可遷置換群で不変に保たれる。この性質から拡大符号の重み分布がわかれば，もとの符号の分布も求まる。すなわち，もとの符号およびその拡大符号の重み w をもつ符号ベクトルの数を N_w, N'_w とすれば，偶数の w について

$$N_{w-1}=wN'_w/(n+1) \qquad (1)$$

一方，もとの多項式符号は $(1,1,\cdots,1)$ を符号ベクトルとして含んでいるから，

$$N_{n-w}=N_w\ ,\quad N'_{n+1-w}=N'_w$$

これと(1)より,

$$(n+1-w)N_{w-1} = wN_w \qquad (2)$$

が成立する。[2] 一般に符号ベクトルの数が n^2 のオーダー以下の符号で，拡大符号が上述の2重可遷置換群で不変なものについては，重み分布公式が求まっている。[6]

μ次 Reed-Muller 符号（以下 R-M符号とかく）は上述のように修正 R-M符号 [$((2^m-1), m, 1, \mu)$-多項式符号] の拡大符号であり，つぎのような長さ 2^m のベクトルの集合

$\{(f(0), f(\alpha^0), f(\alpha^1), \cdots, f(\alpha^{2^m-2})) \mid f$ は変数 $X_1, \cdots, X_m$ に関する μ次以下の $GF(2)$ の上の多項式$\}$

として定義される。この定義からもわかるように，多項式符号の拡大符号のなかで，もっとも簡単なクラスと考えられる。

比較的簡単な，復号法が存在すること，パラメータが大きくない所では，BCH-符号に比してそれほど能率（同じ最小の重みに対する k/n）が悪くないことなど，実用上の興味の他，つぎの系で示されるように多項式符号のなかで占める位置から，理論上も興味がもたれている。

系2： $b=1$ のとき，$(2^m-1, m, s, \mu)$-多項式符号

の拡大符号の双対符号は $m-1-\mu$ 次の R-M 符号の部分符号である。

定理1-1) と $W_s(j) \geq W_1(j)$ から証明される。

系2より，もし $m-1-\mu$ 次 R-M 符号について，限られた w についてのみ $N_w \neq 0$ であることが示されたら，$(2^m-1, m, s, \mu)$-多項式符号の拡大符号の双対符号についても同じことがいえる。一般に未知の N_w の個数が，双対符号の最小の重み以下であれば，Pless の等式[2]から，N_w が求まる。また，N_w がすべて求まれば，双対符号の重み分布は MacWilliams の等式[2]より求まる。たとえば，2次の R-M 符号ベクトルの重みは，

$$2^{m-1} + \varepsilon 2^{(m+i)/2-1}$$

ここで，ε は 0，1 または -1，

i は m 以下の非負整数で $m+i$ は偶数

の形であることが示される。[7] このことと，BCH-下界，Carlitz-Uchiyama の下界を使って，いくつかのクラスの BCH-符号や他の巡回符号について，Pless の等式から分布公式が求められている。[2,7] R-M 符号の重み構造についての今後の解明が，他の重要な符号の構造の研究の一つの手がかりになることが期待される。

§2 R-M符号の小さい重みについての分布公式

変数 $X_1, \cdots, X_m$ に関する μ 次以下の $GF(2)$ の上の多項式全体の集合を P_μ とかく。$f \in P_\mu$ について，$(f(0), f(\alpha^0), f(\alpha^1), \cdots, f(\alpha^{2^m-2}))$ の重みを $|f|$ とかく。

$f \in P_\mu$，$|f| \neq 0$ ならばよく知られているように

$$|f| \geq 2^{m-\mu}$$

（定理1：2）の特殊の場合）

一般の場合についてはまだわかっていないが，ここでは

$$2^{m-\mu} \leq |f| < 2^{m-\mu+1}$$

をみたす $f \in P_\mu$ を完全に特性づけることを考える。

変数の変換

$$X_i = c_{i0} + \sum_{j=1}^{m} c_{ij} Y_j, \quad c_{i0}, c_{ij} \in GF(2), \quad 1 \leq i \leq m$$

において，係数行列式が0でないとき，A-変換とよぶことにする。$f(X_1, \cdots, X_m)$ において，各 X_i に上式の右辺を代入して，$Y_1, \cdots, Y_m$ の多項式として表わすとき，変数にA-変換を行うという。$f \in P_\mu$ にA-変換を行って，得られた多項式は P_μ に属し，重みも変らない。（A-変換

は，符号ベクトル成分間のある置換をひき起す。R-M符号はこのような置換に対して不変である。）A－変換によって標準形に変換することができる。[8]

補題3：$f \in P_\mu$，$\mu \geq 2$，$0 < |f| < 2^{m-\mu+1}$ならば，適当にA－変換を行なうことによって，

1) $f = Y_1 \cdots Y_{\mu-\nu}(Y_{\mu-\nu+1} \cdots Y_\mu + Y_{\mu+1} \cdots Y_{\mu+\nu})$
ここで $m \geq \mu+\nu$，$\mu \geq \nu \geq 3$

と表わされるか，

2) $f = Y_1 \cdots Y_{\mu-2}(Y_{\mu-1}Y_\mu + Y_{\mu+1}Y_{\mu+2} + \cdots + Y_{\mu+2\nu-3}Y_{\mu+2\nu-2})$
ここで $m - \mu + 2 \geq 2\nu \geq 2$

と表わされるかのいづれかである。また，1)，2）の場合とも，

$$|f| = 2^{m-\mu+1} - 2^{m-\mu+1-\nu}$$

証明は長いので省略する。これから次の分布公式が得られる。$N_{m,\mu,w}$は長さ2^mのμ次R-M符号の重みwをもつ符号ベクトルの数を表わす。

定理4：[8] $\mu \geq 0$, $2^{m-\mu+1} > w > 0$ のとき,

1) $w = 2^{m-\mu+1} - 2^{m-\mu+1-\nu}$, $(m-\mu+1)/2 \geq \nu \geq 1$

のとき以外は, $N_{m,\mu,w} = 0$

以下, $w = 2^{m-\mu+1} - 2^{m-\mu+1-\nu}$, $u = \min(m-\mu, \mu)$, $v = (m-\mu+2)/2$ とおく。

2) $\nu = 1$ のとき

$$N_{m,\mu,w} = 2^{\mu} \prod_{i=0}^{\mu-1} (2^m - 2^i) / (2^{\mu} - 2^i)$$

3) $\nu = 2$ または, $\max(u, 2) < \nu \leq v$ のとき,

$$N_{m,\mu,w} = 2^{\mu-2+\nu(\nu+1)} \left[\prod_{i=0}^{\mu+2\nu-3} (2^{m-i} - 1) \right] / \left[\prod_{i=0}^{\mu-3} (2^{\mu-2-i} - 1) \prod_{i=0}^{\nu-1} (4^{i+1} - 1) \right]$$

4) $\max(v, 2) < \nu \leq u$ のとき,

$$N_{m,\mu,w} = 2^{\mu(\mu+3)-\nu-1} \left[\prod_{i=0}^{3\mu-\nu-1} (2^{m-i} - 1) \right] / \prod_{i=0}^{\mu-\nu-1} (2^{\mu-\nu-i} - 1) \cdot \left\{ \prod_{i=0}^{\mu-1} (2^{\mu-i} - 1) \right\}^2$$

5) $3 \leq \nu \leq \min(u, v)$ のとき, $N_{m,\mu,w}$ は 3) と 4) の和として与えられる。

上の定理は $\mu=2$ の場合について, Berlekamp-Sloane の結果[ ] の拡張となっている。上の公式と, MacWilliams の等式(の変形)からいくつかのR-M符号の完全な重み分布が数値的に求まる。

文 献

(1) W.W. Peterson, "Error-Correcting Codes", Wiley, 1961

(2) E.R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, 1968

(3) D.E. Muller, "Applications of Boolean algebra to switching circuit design and to error detection", IRE Trans. EC-3, 6-12, 1954.

(4) T. Kasami, S. Lin and W.W. Peterson, "Polynomial codes", IEEE Trans., IT-14, 807-814, 1968

(5) 〃 , "New generalizations of the Reed-Muller codes-Part 1: Primitive codes," IEEE Trans. IT-14, 189-199, 1968

(6) 〃 , "Some results on

cyclic codes which are invariant under the Affins group and their applications, Inf. and Control, vol. 11, 475-496, 1967

(7) T. Kasami, "Weight distribution of BCH codes", Ch.20 in R.C. Bose and T.A. Dowling (eds.) "Proc of the Conf. on Combinational Math. and its Applications", North Carolina Univ. Press, 1969

(8)嵩, 都倉, 畑中, "Read-Muller 符号の重み構造について", 電子通信学会, インホメーション理論研究会資料, 1969-01.

(9) E.R. Berlekamp and N.J. Sloans, "The weight enumerator for 2nd order Reed-Muller codes," To appear

(10) 〃 , "Restrictions on weight distribution of Reed-Muller codes", To appear