数理解析研究所講究録
第95巻 1970年 81-92

最適な二重誤り訂正二進非線形組織符号
——修正Preparata符号について

東大工学部　今井秀樹

1. まえがき

最近Preparataらによって最適な非線形二重誤り訂正符号が発見された[1][2][3]。この符号をPreparata符号（P－符号）と呼ぶ。P－符号は符号長が$2^{n+1}-1$，情報ビット数が$2^{n+1}-2n-2$（n：3以上の奇数）となる二進非線形組織符号*であり，符号語数がJohnsonの上界[3]に達するという意味で最適な符号である。

本稿では，このP－符号を基礎として新しい二重誤り訂正二進非線形組織符号が構成できることを示す。この符号を修正Preparata符号（mP－符号）と呼ぶことにする。mP－符号の符号長は$2^{n+1}-1+|J|$，情報ビット数は$2^{n+1}-2n-3+|J|$（n：3以上の奇数，$|J|$：ある条件を満たす正整数）

＊　本稿では情報シンボルと検査シンボルが区別できる符号を組織符号と呼ぶ．

であり，同一のnに対し，P－符号よりも符号長が長く，検査ビットが一ビット多い。またmP－符号は組織符号としては最適な符号であり，同一符号長の短縮化BCH符号の4倍の符号語数をもつ。しかもmP－符号は符号化および復号が比較的簡単に行える。

2. Preparata 符号

はじめに準備として，文献(3)のPreparata符号について簡単に述べておく。

nを3以上の奇数とし，$x^{2^n-1}+1$を法とするGF(2)の上の多項式環をR_nとする（R_nの元は2^n-2次以下の多項式で表わす）。以下多項式は原則としてR_nの元と考える。また$a(x)=\sum_i a_i x^i$（$\in R_n$）によって，多項式$a(x)$の係数からなる長さ2^n-1の系列$(a_{2^n-2}, a_{2^n-3}, \cdots, a_1, a_0)$をも表わす。

つぎに，αをGF(2^n)の原始元，$g_1(x)$をαの最小多項式とし，$\{m(x)\}$を$g_1(x)$によって生成されるハミング$(2^n-1, 2^n-n-1)$符号とする。また$1, \alpha, \alpha^3$を根として含む最小次数の多項式によって生成される二進BCH$(2^n-1, 2^n-2n-2)$符号を$\{a(x)\}$で表わす。また，0および単項式からなるR_nの部分集合$\{ax^l \mid a \in GF(2), 0 \leq l < 2^n-1\}$を$\{g(x)\}$

とおく。

さらに，$f(x)g_1(x)=0$，$f(\alpha)=1$ となる多項式 $f(x)$（このような $f(x)$ が存在することは文献(3) Lemma 3 参照）および $u(x)=(x^{2^n-1}+1)/(x+1)$ を定義しておく。

このとき，Preparata符号はつぎのように定義される。

定義1（Preparata 符号）：

$$v' = (m(x),\ i,\ (m(1)+i)u(x)+m(x)+a(x))$$

$$u' = (q(x),\ 0,\ q(x)f(x))$$

（$m(x)\in\{m(x)\}$，$i\in GF(2)$，$a(x)\in\{a(x)\}$，$q(x)\in\{q(x)\}$）

となる二種の $2^{n+1}-1$ 次元ベクトル v'，u' に対し $z'=v'+u'$ となる形のベクトルすべての集合をPreparata符号（P－符号）と呼ぶ。

P－符号は最小距離が5の非線形組織（$2^{n+1}-1$，$2^{n+1}-2n-2$）符号である。また，符号語数が Johnson の上界に達する最適な符号であり，しかも符号化および復号が比較的簡単に行える。

3．修正Preparata 符号

3．1　修正Preparata 符号の定義

2^n-1 を法とする整数の剰余環を Z_n とする（Z_n の元は 2^n-2 以下の非負の整数で表わす）．また J をつぎの条件

(*)を満たす Z_n の部分集合とする。

条件(*)：α のべきの集合 $\{\alpha^{3j} \mid j \in J\}$ において，任意の4つの異なる元の和 $\alpha^{3i}+\alpha^{3j}+\alpha^{3k}+\alpha^{3l}$ ($i<j<k<l$, $i, j, k, l \in J$) が0とならない。

また，J に含まれる元の数を $|J|$ で表わす。また，このような J に対応して，つぎのような R_n の部分集合を定義する。

$$\{C(x)\} = \{C(x) \mid C(x) = \sum_j c_j x^j,\ C(1)=0,\ c_j = 0\ (j \notin J)\}$$

さらに，$g_\lambda(x) = x^\lambda g_1(x)$ ($\lambda \in Z_n$)，$g_1(\alpha^3)=1$ となる多項式 $g_\lambda(x)$ を定義しておく。このような $g_\lambda(x)$ が存在することは容易に確かめられる。実際 $g_1(\alpha^3)=\alpha^t$ ($t \in Z_n$) であれば，$\lambda = -t\cdot 3^{-1}$ (3^{-1} は Z_n における3の逆元を示す) とすればよい。

ここで，修正Preparata符号を定義しよう。

定義2（修正Preparata符号）：

$$v = (m(x),\ i,\ (m(1)+i)u(x)+m(x)+s(x)+c(x)g_c(x),\ c(x))$$

$$u = (q(x),\ 0,\ q(x)f(x),\ 0)$$

となる二種の $3\cdot 2^n-2$ 次元ベクトル v, u に対し，$z = v+u$ となる形のベクトルすべての集合を修正Preparata符号（mP-符号）と呼ぶ。

mP－符号の符号長は見掛け上 $3\cdot 2^n-2$ であるが，実際には $C(x)$ の J に属さない次数の項の係数がすべて0となるから，符号長は $2^{n+1}-1+|J|$ と考えることができる。$|J|$ の値については次節で論ずる。また，mP－符号は組織符号となり，その情報ビット数は $\{m(x)\}$，$\{Q(x)\}$，$\{C(x)\}$ の情報ビット数がそれぞれ，2^n-1-n，2^n-2-2n，$|J|-1$ であり，さらに $g(x)$（$\in\{g(x)\}$）および λ（$\in GF(2)$）を自由に選べることから $2^{n+1}-2n-3+|J|$ となることが分る。

ところで，実際の符号化および復号を考えると，J として $\{0,1,2,\cdots,|J|-1\}$ となる集合で条件(*)を満たすものを選ぶことが望ましい。このとき $\{C(x)\}$ は $|J|-1$ 次以下の多項式となり，符号化および復号が簡単化される。このようにして選ばれた J を特に J^0 と書き，J^0 を用いて構成されたmP－符号を特に0mP－符号と呼ぶことにする。

3.2 mP－符号の符号長

条件(*)を満たすある集合 J が与えられれば，J から任意に δ' 個の元を除いた集合 J' は再び条件(*)を満たすから，J' を用いて符号長 $2^{n+1}-1+|J|-\delta'$ のmP－符号を作ることができる。したがって J としては $|J|$ のできるだけ大きい集合を見出すことが望ましい。そこで，$|J|$ の可能な最大値を $|J|_{max}$ とし，この値の上界と下界について考える。

条件(*)は"$\{\alpha^{3j} \mid j \in J\}$の任意の異なる二つの元の和がすべて異なる"と言い換えることができるから，$|J|_{max}$は

$$\binom{|J|_{max}}{2} \leq 2^n - 1 \qquad (1)$$

を満たさねばならない。この式によって$|J|_{max}$の上界が与えられる。一方，$|J| + \binom{|J|}{3} < 2^n - 1$であれば，$GF(2^n)$の0でない元で，$\alpha^j$ ($j \in J$)または$\alpha^j + \alpha^k + \alpha^l$ ($j < k < l$, $j, k, l \in J$)という形では表わせないものが存在する。このような元の一つをα^iとし，Jにiを付け加えた集合をあらたにJとおくと，この集合Jは再び条件(*)を満たす。ゆえに，$|J|_{max}$は

$$|J|_{max} + \binom{|J|_{max}}{3} \geq 2^n - 1 \qquad (2)$$

を満たす。この式によって$|J|_{max}$の下界が得られる。

つぎに，omp－符号の場合について考えよう。$|J^0|$の可能な最大値は$GF(2^n)$の原始元αの選び方によって異なる。そこで，これを$|J^0(\alpha)|_{max}$と書こう。$|J^0(\alpha)|_{max}$の上界としては式(1)を用いることができる。また，下界が次式で与えられることは容易に導ける。

$$|J^0(\alpha)|_{max} \geq n + 1 \qquad (3)$$

さらに詳しく$|J^0(\alpha)|_{max}$を定めるためには個々の原始元αについて調べる必要がある。しかし，任意の原始元αに対し

$$|J^0(\alpha)|_{max} = |J^0(\alpha^{2^i})|_{max} \quad (i: \text{正整数}) \qquad (4)$$

$$|J^0(\alpha)|_{max} = |J^0(\alpha^{-1})|_{max} \qquad (5)$$

が成立することは，ただちに確かめられる。

次表に $n=3,5,7$ の場合について，すべての $GF(2^n)$ の原始元 α に対する $|J^0(\alpha)|_{max}$ とそれに対応する Omp－符号の符号長と情報ビット数を示す。ただし，式(4),(5)によって $|J^0(\alpha)|_{max}$ が等しくなるものは省略してある。また，各 n について式(1),(2)による $|J|_{max}$ の上界と下界もあわせ示してある。

表1．$n=3,5,7$ の Omp－符号の符号長と情報ビット数

n	$\|J\|_{max}$ 上界	$\|J\|_{max}$ 下界	α	$\|J^0(\alpha)\|_{max}$	符号長	情報ビット
3	4	4	α_0 , α_0^3	4	19	11
5	8	7	α_0 , α_0^3	6	69	57
			α_0^5	7	70	58
7	16	10	α_0, α_0^3, α_0^5, α_0^{19}	8	263	247
			α_0^{13}	9	264	248
			α_0^9 , α_0^{21}	10	265	249
			α_0^7 , α_0^{11}	11	266	250

(注) α_0 は $GF(2^n)$ の原始元でつぎのように定めてある。$n=3$ のとき $\alpha_0^3+\alpha_0^2+1=0$，$n=5$ のとき $\alpha_0^5+\alpha_0^2+1=0$，$n=7$ のとき $\alpha_0^7+\alpha_0^3+1=0$．

3.3 mP－符号の最小距離

mP－符号 $\mathcal{M}_n$ は非線形符号であるので，その最小距離 d_{min} は $\mathcal{M}_n$ の任意の二つの異なる符号語 $\boldsymbol{z}_0$，$\boldsymbol{z}_1$ の和の重み（成分中の1の数）の最小値として求めなければならない。すなわち，

$$d_{min} = \min_{\substack{\boldsymbol{z}_0, \boldsymbol{z}_1 \in \mathcal{M}_n \\ \boldsymbol{z}_0 \neq \boldsymbol{z}_1}} W[\boldsymbol{z}_0 + \boldsymbol{z}_1] \qquad (6)$$

ここに $W[\boldsymbol{z}]$ は $\boldsymbol{z}$ の重みを示す。

ここで，$\boldsymbol{z}_0 + \boldsymbol{z}_1$ に関する Preparata の結果（文献(3)，P. 384）を僅かに修正したつぎの補題を示しておこう。

補題1 ： $\boldsymbol{\zeta} = \boldsymbol{z}_0 + \boldsymbol{z}_1$ はつぎのように分解できる。

$$\begin{aligned}\boldsymbol{\zeta} &= (\zeta_0(x), \zeta, \zeta_1(x), \zeta_2(x)) \\ &= (m(x), i, (m(1)+i)u(x) + m(x) + o(x) + c(x)q_c(x), c(x)) \\ &\quad + (q(x), 0, q(x)f(x), 0) \\ &\quad + (0, 0, m'(x) + m'(1)u(x), 0)\end{aligned}$$

ここに，$m(x) \in \{m(x)\}$，$i \in GF(2)$，$o(x) \in \{o(x)\}$，$c(x) \in \{c(x)\}$，$q(x) \in \{q(x)\}$ である。また，$m'(x)$ は $m'(x) = q(x) + q_0(x) + q_1(x)$ （$q_0(x)$，$q_1(x) \in \{q(x)\}$），かつ $m'(x) \in \{m(x)\}$ となる多項式である（したがって，$q(x) = 0$ のときは $m'(x) = 0$，$q(x) \neq 0$ のときは $m'(x)$ は0または三項式となる）。

つぎに，$c(x)$ の重み $W[c(x)]$ に関して，つぎの補題を

導いておく。

補題2 ： $C(\alpha^3)=0$ を満たす0でない $C(x)\in\{C(x)\}$ が存在すれば，$W[C(x)]\geq 6$ となる。

(証) $C(\alpha^3)=0$ を満たす $C(x)$ は1，$\beta=\alpha^3$ を根として含む最小次数の多項式によって生成されるBCH符号の符号語である。したがって $W[C(x)]\geq 4$ であり，また $W[C(x)]$ は偶数である。ところが，Jの定義から $W[C(x)]=4$ となる $C(x)$ は存在しない。ゆえに $W[C(x)]\geq 6$ (Q.E.D.)

以上の準備の下につぎの定理を導こう。

定理 ： mP-符号の最小距離は5である。

(証) 補題1の ζ において $C(x)=0$ のときは ζ の重みはP-符号の二つの異なる符号語の和の重みと等しく，その最小値が5となることがPreparataにより導かれている。[3]

$C(x)\neq 0$ の場合を考えよう。ここで

$$w_0=W[\zeta_0(x)] \qquad w=\zeta^*$$
$$w_1=W[\zeta_1(x)] \qquad w_2=W[\zeta_2(x)]$$
$$w_t=W[\zeta]=w_0+w+w_1+w_2$$

とおき，表2に w_0，w，w_1，w_2，w_t のとり得る値を分類して示す。

---

* ζ は $GF(2)$ の元であるが，w は重みを表わし，実数として扱われる。

表2. ζ の重みの最小値 ($C(x) \neq 0$ の場合)

$q(x)$	$m(x)$	ι	$\zeta_1(x)$	重み				
				w_0	w	w_1	w_2	w_t
$=0$	$\neq 0$	$*$	$*$	$\geq 3^{(a)}$			$\geq 2^{(b)}$	≥ 5
	$=0$	$=0$	$\neq 0$			$\geq 3^{(c)}$	$\geq 2^{(b)}$	≥ 5
			$=0$				$\geq 6^{(d)}$	≥ 6
		$\neq 0$	$\neq 0^{(g)}$		1	$\geq 3^{(c)}$	$\geq 2^{(b)}$	≥ 6
$\neq 0$	$\neq 0$	$*$	$\neq 0^{(h)}$	$\geq 2^{(e)}$		≥ 1	$\geq 2^{(b)}$	≥ 5
	$=0$	$=0$	$\neq 0^{(h)}$	1		$\geq 2^{(f)}$	$\geq 2^{(b)}$	≥ 5
		$\neq 0$	$\neq 0^{(h)}$	1		≥ 1	$\geq 2^{(b)}$	≥ 5

(注) $*$ は $=0$ でも $\neq 0$ でもよいことを示す。

表中の (a) ~ (h) を説明しよう.

(a) $\zeta_0(x) = m(x) \neq 0$ であるから $w_0 \geq 3$.

(b) $C(x) \neq 0$, $C(1) = 0$ であるから $w_2 \geq 2$.

(c) $q(x) = 0$ から $\zeta_1(x) \in \{m(x)\}$, しかも $\zeta_1(x) \neq 0$ であるから $w_1 \geq 3$

(d) $q(x) = m'(x) = m(x) = 0$ であるから, $\zeta_1(x) = a(x) + C(x) g_c(x)$ となる. $\zeta_1(x) = 0$ であるから, $\zeta_1(\alpha^3) = C(\alpha^3) = 0$. ゆえに補題2から $w_2 \geq 6$. なお, $|J| < 6$ のときは $C(x) \neq 0$ のとき $\zeta_1(x) = 0$ となることはない.

(e) $w_0 \geq W[m(x)] - W[q(x)] \geq 2$

(f) $s_1(x) \neq 0$, $s_1(1) = 0$ であるから $w_1 \geq 2$。

(g) $s_1(1) = \lambda \neq 0$ であるから $s_1(x) = 0$ となることはない。

(h) $q(x) \neq 0$ のとき $s_1(\alpha) = q(\alpha) \neq 0$ であるから $s_1(x) = 0$ となることはない。

以上によって、いずれの場合も $w_t \geq 5$ となることが分る。

(Q.E.D.)

3.4 mp-符号のその他の性質

mp-符号は、また、組織符号であることが容易に示される。このmp-符号の組織符号としての形を用いれば、mp-符号の符号化は比較的簡単に行える。

さらに、mp-符号の符号長を N、情報ビット数を K とおくと、$2^{N-(K+1)} < \sum_{i=0}^{2} \binom{N}{i}$ となることが導ける。このことはmp-符号と同一符号長でmp-符号より多い情報ビット数をもつ二重誤り訂正組織符号は存在しないことを意味する。すなわち、mp-符号は組織符号としては最適な符号である。

また、mp-符号はP-符号と同様、BCH符号の復号に類似した代数的方法で比較的簡単に復号することができる。

4. むすび

以上mP-符号を定義し，その諸性質について述べた。組織的な方法で構成できる非線形符号は現在のところ，二重誤り訂正符号までしか知られていない。今後，非線形符号に関するより統一的な理論が期待される。

文　献

(1) A.W.Nordstrom and J.P.Robinson : "An optimum nonlinear code", Inform. Control, 11, p.613 (1968).

(2) F.P.Preparata : "Weight and distance structure of Nordstrom-Robinson quadratic code", Inform. Control, 12, p.466 (1968).

(3) F.P.Preparata : "A class of optimum nonlinear double-error correcting codes", Inform. Control, 13, p.378 (1968).