

二次元符号

横浜國大・工 今井秀樹

§1. まえがき

符号理論では、これまで、符号はシンボルが一次元に配列されたものとして扱われてきた。これは従来の情報の伝達および処理が一次元的に行われてきたからであろう。しかし、将来、二次元情報の処理技術の発展に伴い、シンボルが二次元に配列された符号も必要になってくると思われる。

本稿では最近の二次元符号の研究について概説する。なお、ここでは簡単のため、シンボルが0, 1からなる二元符号についてのみ論ずる。

§2. 一次元符号について

はじめに、準備として、従来の符号——一次元符号について簡単に述べておこう。符号を用いる目的は、情報をできるだけ誤りなく伝えることである。いま、図1のように、ビットの情報 a_0, a_1, \dots, a_{k-1} を送りたいとしよう。 a_i は0または1

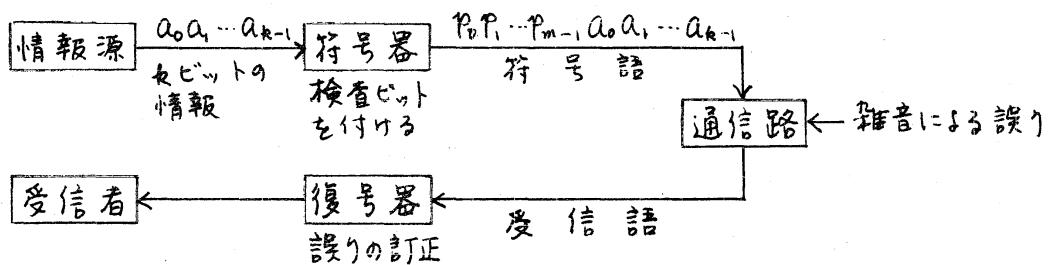


図1. 誤り訂正符号(組織符号)を用いる通信系

たは1であるが、これをGF(2)の元として扱うと便利である。また、 $a_0 a_1 \dots a_{k-1}$ としては、0, 1どちらなる長さのあらゆるパターンが現れ得るとする。これをそのまま送るのでは、通信路で誤りが生じたとき、それを訂正することができないから、信頼性を上げるためにには、符号器で何らかの冗長性を付与しなければならない。そこで、情報ビット a_0, a_1, \dots, a_{k-1} に m 個の検査ビット $p_0 p_1 \dots p_{m-1}$ をつけ加えて通信路に送り出すのである。これらの検査ビットは情報ビットの何らかの関数として定められる。たとえば、 $k=3, m=4$ として、検査ビットを

$$\left. \begin{array}{l} p_0 = a_0 + a_2 \\ p_1 = a_0 + a_1 + a_2 \\ p_2 = a_0 + a_1 \\ p_3 = a_1 + a_2 \end{array} \right\} \quad (1)$$

によって定めるものとしよう。ただし、これらはGF(2)上の式である。このとき、情報ビットのあらゆるパターンに対して、通信路に送り出される系列を示すと表1のようになる。このように系列の集合が符号であり、各系列が符号語である。

この符号においては符号語の長さが有
限で、しかもすべて等しい。このよう
な符号をブロック符号といふ。そして
符号語の長さ $n = k + m$ を符号長と
いう。

符号語の長さ $n = k + m$ を符号長と

いう。さらに、表1の符号は、情報ビットと検査ビットを区別できるといふ

意味で組織符号と呼ばれるものであり、

また、検査ビットが情報ビットの線形

周数で与えられるといふ意味で線形符

号と呼ばれるものである。いまでも

なく、線形符号は $GF(2)$ の上の n 次

元ベクトル空間の k 次元部分空間とな

す。

表1. 符号長7, 情報

ビット数3の線形符
号(巡回符号)。

検査
ビット 情報
ビット

$P_0 P_1 P_2 P_3$ $a_0 a_1 a_2$

0 0 0 0 0 0 0

1 1 1 0 1 0 0

0 1 1 1 0 1 0

1 0 0 1 1 1 0

1 1 0 1 0 0 1

0 0 1 1 1 0 1

1 0 1 0 0 1 1

0 1 0 0 1 1 1

さて、表1の符号はさらに興味深い特徴をもつている。それは、符号語を $C = (C_0, C_1, \dots, C_{n-1})$ とすると、そのシンボルを巡回置換した $(C_{n-1}, C_0, C_1, \dots, C_{n-2})$ も符号語になつてゐることである。このように任意の符号語の巡回置換が再び符号語となる線形符号を巡回符号と呼ぶ。巡回符号を論ずる場合には、符号語 C を $GF(2)$ の上の多项式

$$C(x) = C_0 + C_1 x + \dots + C_{n-1} x^{n-1} \quad (2)$$

で表わしておくと便利である。これを符号多項式と呼ぼう。ここで、符号長 n 、情報ビット数 k の巡回符号における最小次数の非零の符号多項式を $G(x)$ とおく。これは $n-k$ 次の多項式となる。そして、巡回符号のすべての符号多項式は $G(x)$ で割り切れ、また、 $G(x)$ で割り切れる $n-1$ 次以下の $GF(2)$ の上の多項式は、この巡回符号の符号多項式となることが導ける。このような $G(x)$ を巡回符号の 生成多項式 と呼ぶ。たとえば、表 1 の巡回符号の生成多項式は $G(x) = 1 + x + x^2 + x^4$ である。巡回符号は生成多項式によつて完全に特徴づけられ、また、生成多項式を用いることにより、簡単なシフトレジスター回路で符号化を行えるのである。

さて、符号理論では、通信路で生じる誤りとしてランダム誤りとバースト誤りの二つの型のものを考える。ランダム誤りとは、個々の誤りが他の誤りと統計的に独立に生じる場合をいう。これに対し、バースト誤りとは、誤りの塊に相関があり、密集して生じる誤りをいう。ランダム誤り訂正符号については文献に譲り、ここでは、バースト誤り訂正符号についてもう少し述べておこう。ふつう、バースト誤りの大きさを測るものとして、その長さが用いられる。バースト誤りの長さとは、最初の誤りから最後の誤りまでの長さである。たとえば、通信路で

--	--	--	--	--	--	--	--	--	--	--	--

(斜線部が誤り)

という誤りが生じたとしよう。これをバースト誤りと考えれば、長さは6である。もちろん、ランダム誤り訂正符号を用いてもバースト誤りを訂正することはできるが、誤り相互の瘤の相関を利用すれば、バースト誤りはより能率よく（より少數の検査ビットで）訂正できるはずである。このために、バースト誤り訂正符号が用いられるのである。

バースト誤り訂正符号としてよく知られているものにファイア符号がある。これは、生成多項式が

$$G(x) = P(x)(x^c - 1) \quad (3)$$

となる符号長 $n = \text{LCM}(e, c)$ の巡回符号である。 $T = t = 1$ 、
 $P(x)$ は既約多項式であり、 e は $P(x)$ の根の位数である。
また、 c は e で割り切れない正整数とする。 $P(x)$ の次数を
 m とすれば、この符号の検査ビット数は $c + m$ であり、長さ
 n が

$$t \leq m, \quad t \leq (c+1)/2 \quad (4)$$

を満たすバースト誤りを訂正できる。また、ファイア符号の
符号化および復号はシフトレジスターを用いて容易に行える。

ところで、 $n-1$ 次以下の多項式 $C(x)$ がファイア符号
の符号多項式となる必要十分条件は、もちろん $C(x)$ が
 $G(x)$ で割り切れることがあるが、これにまた、 $P(x)$ の積

$\alpha (\in GF(2^m))$ を用いて、

$$C(x) \equiv 0 \pmod{x^e - 1}, \quad C(\alpha) = 0 \quad (5)$$

とかけことに注意しておこう。

以上、一次元符号についてきわめて簡単に述べた。詳しくは文献(1)～(5)を参照されたい。

さて、符号理論では、以上のような誤り訂正符号の他に、ある種の周期系列を扱うことがある。その中で代表的なものはM系列(最大長シフトレジスター系列)である。これは、一定数の記憶素子をもつ入力のない線形シフトレジスターで発生し得る最長周期の系列であり、記憶素子数を m とすれば、周期は $2^m - 1$ である。M系列は m 次の原始多項式に対応した結線をもつ線形帰還シフトレジスターによって発生させることができ。たとえば、原始多項式 $1 + x + x^3$ に対する図2のシフトレジスターに非零の任意の初期状態を与えると、一周期が 1110100 となる周期7のM系列が発生する。

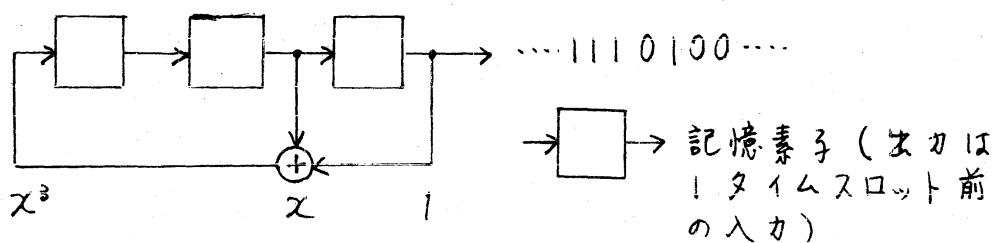


図2. 周期7のM系列発生回路

$\begin{array}{c} \downarrow \\ \oplus \end{array}$ mod 2 加算器

M系列はまた次のように表わすこともできる。 $GF(2^m)$ の原始元を α とし、 θ を $GF(2^m)$ から $GF(2)$ の上への任意の線形写像とすれば、 $s_i = \theta(\alpha^i)$ をオイ成分とする系列 $\{s_i\}$ は周期 $2^m - 1$ のM系列となるのである。

M系列は種々の興味深い性質をもつていて、その一つは自己相関関数である。いま、 η を $GF(2)$ から実数への

$$\eta(0) = +1, \quad \eta(1) = -1 \quad (6)$$

という写像とし、周期 n の系列 $\{s_i\}$ に対し、

$$\rho(k) = [\sum_{i=0}^{n-1} \eta(s_i) \eta(s_{i+k})] / n \quad (7)$$

で自己相関関数を定義すれば、M系列の自己相関関数は

$$\rho(k) = \begin{cases} 1 & ; k = hn \quad (h: \text{整数}) \\ -1/n & ; \text{その他の場合} \end{cases} \quad (8)$$

となることが導ける。つまり、周期の整数倍のところで鋭いピーカーを持ち、それ以外の点ではごく小さな値をとるのである。

§3. 二元符号

これまで述べてきた符号はシンボルが一次元に配列されていた。これに対し、符号語が

$$C = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n_2-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n_2-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n_1-1,0} & c_{n_1-1,1} & \cdots & c_{n_1-1,n_2-1} \end{bmatrix} \quad (9)$$

という形の符号を面積 $n_1 \times n_2$ の二次元符号と呼ぶ。このような二次元符号についても、線形符号は一次元符号の場合と全く同様に考えることができる。線形といふ性質に関する限り、一次元と二次元に本質的な差異はない。しかし巡回性については、一次元と二次元ではやや様相を異にする。二次元巡回符号は、式(9)の C が符号語であれば、

$$\begin{bmatrix} C_{n_1-1,0} & C_{n_1-1,1} & \cdots & C_{n_1-1,n_2-1} \\ C_{0,0} & C_{0,1} & \cdots & C_{0,n_2-1} \\ \vdots & \vdots & & \vdots \\ C_{n_1-2,0} & C_{n_1-2,1} & \cdots & C_{n_1-2,n_2-1} \end{bmatrix} \text{ および } \begin{bmatrix} C_{0,n_2-1} & C_{0,0} & \cdots & C_{0,n_2-2} \\ C_{1,n_2-1} & C_{1,0} & \cdots & C_{1,n_2-2} \\ \vdots & \vdots & & \vdots \\ C_{n_1-1,n_2-1} & C_{n_1-1,0} & \cdots & C_{n_1-1,n_2-2} \end{bmatrix} \quad (10)$$

が符号語となるような二次元線形符号と定義される。この場合にも符号語を

$$C(x, y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} c_{ij} x^i y^j \quad (11)$$

という GF(2) の上の二変数多項式で表わしておくと便利である。しかし、一般に、二次元巡回符号は、一次元巡回符号の場合のように单一の生成多項式で特徴づけることはできない。このため、二次元巡回符号の取り扱いは一次元の場合よりもかなり複雑となる。たとえば、一次元巡回符号の場合、検査ビットの位置については全く問題が生じない、ところが、二次元ではそうはいえない。二次元巡回符号の検査ビットの位置は、符号によつて様々な形をとるのである。

さて、二次元面上に生じたランダム誤りを訂正しようとい

う場合には、敢えて二次元符号を使う必要はない。一次元のランダム誤り訂正符号を適当に二次元に配列し直して用いればよいからである。これに対し、二次元面上にインキのしみのように生じた二次元バースト誤りは、二次元符号を用いることにより、より能率よく訂正できる。

二次元バースト誤りの場合、一次元バースト誤りの長さに応するものは面積である。これは、二次元面上のすべての誤りを含む最小の矩形の大きさと定義される。たとえば、図3のような誤りは面積 2×3 の二次元バースト誤りである。このような二次元バースト誤りを訂正する符号として代表的なものは二次元ファイア符号である。次節でこの符号について述べよう。

§4. 二次元ファイア符号

m_1, m_2 を正整数とし、 α を $GF(2^{m_1 m_2})$ の原始元とする。また、 e_1, e_2 を

$$e_1 e_2 = 2^{m_1 m_2} - 1 \quad (12)$$

$$e_1 | 2^k - 1 \text{ となる最小の正整数 } k = m_1 \quad (13)$$

$$\text{GCD}(e_1, e_2) = 1 \quad (14)$$

を満たす正整数とし、

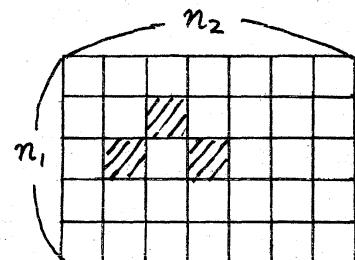


図3. 面積 2×3 の
二次元バースト誤り

$$\gamma = \alpha^{e_2}, \quad \beta = \alpha^{e_1} \quad (15)$$

とおく。つぎに、 c_1, c_2 をその積 $c_1 c_2$ が $2^{m_1 m_2} - 1$ で割り切れない正整数とし、

$$n_1 = \text{LCM}(c_1, e_1), \quad n_2 = \text{LCM}(c_2, e_2) \quad (16)$$

とおく。このとき、

$$\left. \begin{array}{l} C(x, y) \equiv 0 \pmod{x^{c_1}-1, y^{c_2}-1} \\ C(\gamma, \beta) = 0 \end{array} \right\} \quad (17)$$

を満たすスイッチして n_1 次未満、 y に満てて n_2 次未満の $\text{GF}(2)$ 上の多項式 $C(x, y)$ すべての集合が二元ファイア符号である。（より一般的な定義については文献(9)参照。）

この符号は面積 $n_1 \times n_2$ の二元巡回符号である。そして、 $c_1 c_2 + m_1 m_2$ 個の検査ビットをもち、これらは図4のような位置にとることができる。また、この符号は面積 $b_1 \times b_2$ が

$$\left. \begin{array}{l} b_1 \leq (c_1+1)/2, \quad b_2 \leq (c_2+1)/2 \\ b_1 \leq m_1, \quad b_2 \leq m_2 \end{array} \right\} \quad (18)$$

を満たす二元バースト誤り訂正

できることが導ける。たとえば、 $m_1 = m_2 = 2$ とすると、 $e_1 = 3, e_2 = 5$

は式(12)～(14)を満たす。いま、 $c_1 = 4, c_2 = 3$ とすれば、面積 12×15

の二元ファイア符号ができる。こ

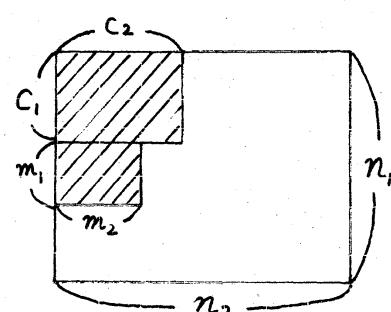


図4. 二元ファイア符号の検査ビットの位置
($m_2 \leq c_2$ とする)

の符号の検査ビット数は 16 であり、面積 2×2 以下の二次元バースト誤りを訂正できる。

二次元ファイア符号の符号化および復号は二次元に記憶要素を配列したシフトレジスターを用いて行える。詳しくは文献(9)を参照されたい。

なお、二次元バースト誤り訂正符号の他の構成法も二、三知られている⁽⁷⁾⁽⁸⁾。

§5. M 平面

つきに、二次元周期系列について考えよう。二次元系列

$$\{s_{i,j}\} = \begin{array}{c} \cdots : \cdots : \cdots : \cdots \\ \cdots s_{i-1,j-1} s_{i-1,j} s_{i-1,j+1} \cdots \\ \cdots s_{i,j-1} s_{i,j} s_{i,j+1} \cdots \\ \cdots s_{i+1,j-1} s_{i+1,j} s_{i+1,j+1} \cdots \\ \cdots : \cdots : \cdots : \cdots \end{array} \quad (19)$$

において、すべての整数 i, j に対し、

$$s_{i+n_1, j} = s_{i, j}, \quad s_{i, j+n_2} = s_{i, j} \quad (20)$$

を満たす最小の正整数 n_1, n_2 が存在するとき、 $\{s_{i,j}\}$ は周期 (n_1, n_2) の二次元周期系列であるといふ。二次元周期系列として重要なものは M 平面である。これは M 系列を二次元に拡張したもので、多くの興味深い性質をもつてゐる。

M 平面は様々な方法で定義できるが、前節式(15)の θ, β を用いて定義するのが最も簡単である。このことから M 平面はまた $\theta\beta$ 平面とも呼ばれる。ここで、 θ を $GF(2^{m_1 m_2})$

から GF(2) の上への仕事の線形写像

としよう。このとき

$$s_{ij} = \epsilon(\gamma^i \beta^j) \quad (21)$$

を (i, j) 要素とする二次元系列 $\{s_{ij}\}$

が M 平面となるのである。この M 平面の周期は $(n_1, n_2) = (e_1, e_2)$ である。

たとえば、 $m_1 = 3, m_2 = 2$ とすれば、 $e_1 = 7, e_2 = 9$ は式 (12) ~ (14) を満たす。いま、 α を原始多項式 $1 + x + x^6$ の根とし、 $\theta(\gamma^i \beta^j)$ を $\gamma^i \beta^j$ を $\alpha^0, \alpha^1, \dots, \alpha^5$ の線形結合で表わしたときの α^i の係数とすれば、一周期が図 5 のような M 平面ができる。

M 平面は、M 級列と同様、その自己相関関数に著しい特徴がある。式 (6) の式を用い、周期 (n_1, n_2) の二次元系列 $\{s_{ij}\}$ に対して

$$P(k, l) = \left[\sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \epsilon(s_{ij}) \epsilon(s_{i+k, j+l}) \right] / n_1 n_2 \quad (22)$$

で自己相関関数を定義すれば、M 平面の自己相関関数は

$$P(k, l) = \begin{cases} 1 & ; (k, l) = (h_1 n_1, h_2 n_2) (h_1, h_2: 整数) \\ -1/n_1 n_2 & ; 他の場合 \end{cases} \quad (23)$$

となることが導ける。

M 平面の一般化およびその詳しい性質については、文献 (10) ~ (13) を参照されたい。

1	0	0	1	0	1	0	0	1
0	1	1	1	0	1	1	1	0
1	0	1	0	0	0	1	0	1
0	0	1	1	0	1	1	0	0
0	1	0	0	0	0	0	1	0
1	1	1	0	0	0	1	1	1
1	1	0	1	0	1	0	1	1

図 5. 周期 (7, 9) の M 平面の一周期

文 献

符号理論全般に関するもの

- (1) W. W. Peterson, "Error-Correcting Codes," M. I. T. Press, Cambridge, Mass., 1961.
- (2) W. W. Peterson and E. J. Weldon, "Error-Correcting Codes," 2nd Edition, M. I. T. Press, 1972.
- (3) E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill Book Co., New York, 1968.
- (4) S. Lin, "An Introduction to Error-Correcting Codes," Prentice-Hall, Inc., Englewood Cliffs, N. J., 1970.
- (5) 宮川, 岩垂, 今井, "符号理論," 昭晃堂.

二次元符号に関するもの

- (6) 野村, 福田, "線形再帰平面と二次元巡回符号," 信学論(A), vol. 54-A, pp. 147-154, 昭和46年3月.
- (7) B. Elspas, "A Note on Multidimensional Coding," presented at the IEEE Int. Symp. Inform. Theory, San Remo, Italy, Sept. 1967.
- (8) 今井, "二次元バースト訂正符号," 信学論(A), vol. 55-A, pp. 385-392, 昭和47年8月.

- (9) H. Imai, "Two-Dimensional Fire Codes," submitted to IEEE Trans. Inform. Theory.
- (10) 野村, 宮川, 今井, 福田, "最大面積行列をもつ平面の構成法および諸性質," 信学論(A), vol. 54-A, pp. 250-257, 昭和46年5月.
- (11) _____, "SR₃-平面の諸性質と三次元への拡張," 信学論(A), vol. 54-A, pp. 402-409, 昭和46年7月.
- (12) T. Nemura, H. Miyakawa, H. Imai and A. Fukuda, "A Theory of Two-Dimensional Linear Recurring Arrays," IEEE Trans. Inform. Theory, vol. IT-18, pp. 775-785, Nov. 1972.
- (13) 中村, 岩垂, "SR₃-平面に関する一考察," 信学会全国大会, 1156, 昭和48年3月.