

多数決素子による復号法について

阪大基礎工 都倉信樹

§ 1. 多数決素子による復号法

群符号 C はそのパリティ検査行列 H で規定される. H は $GF(q)$ の上の $r \times n$ 行列とする. n は符号長, r は検査点数. H の行ベクトルで張られる r 次元空間のベクトル $h_i = (h_{i1}, h_{i2}, \dots, h_{in})$ とベクトル $y = (y_1, y_2, \dots, y_n)$ との内積

$$h_i \cdot y = h_{i1}y_1 + h_{i2}y_2 + \dots + h_{in}y_n$$

をパリティ検査和とよぶ. $h_i \cdot y = 0$ となるとき, y はパリティ検査 h_i を満すという. C は H の行のパリティ検査をすべて満すベクトルの全体である. 受信ベクトル $y = (y_1, \dots, y_n)$ は送信された符号語 $x = (x_1, \dots, x_n) \in C$ と誤りベクトル $e = (e_1, \dots, e_n)$ のベクトル和である.

受信ベクトル y に対する J 個のパリティ検査和

$$s_j = \sum_{i=1}^n h_{ji} y_i = \sum_{i=1}^n h_{ji} e_i \quad \Bigg\}$$

$$\left. \begin{aligned} s_2 &= \sum_{i=1}^n h_{2i} y_i = \sum_{i=1}^n h_{2i} e_i \\ &\vdots \\ s_J &= \sum_{i=1}^n h_{Ji} y_i = \sum_{i=1}^n h_{Ji} e_i \end{aligned} \right\} \quad (1)$$

を考える。(1) は以下の条件 1), 2) を満すとき $(\alpha_1, \dots, \alpha_I)$ に関し直交しているという。ここで, $1 \leq \alpha_1 < \dots < \alpha_I \leq n$.

$$1) \quad h_{j\alpha_i} = 1, \quad 1 \leq j \leq J, \quad 1 \leq i \leq I,$$

2) $l \neq \alpha_i \quad (1 \leq i \leq I)$ なる各 l について, $h_{1l}, h_{2l}, \dots, h_{Jl}$ のうち, 高々一つを除いてすべて 0.

次の結果がよく知られている.⁽¹⁾

T. 1 符号 C が各ベクトル i に対し, (i) に関し直交する少なくとも $(d-1)$ 個の検査和をもてば, C の最短距離は少なくとも d である.

直交検査和は多数決素子による復号に利用される.

第 i ベクトルに関し直交する $(d-1)$ 個の検査和があるとする. $\left[\frac{d-1}{2}\right]$ 個以下の誤りが起った場合を考える. 第 i ベクトルが誤っていないときは, 少なくとも $d-1 - \left[\frac{d-1}{2}\right]$ の検査和の値は 0 である. また, 第 i ベクトルに誤り e が生じていければ, 少なくとも $d-1 - \left(\left[\frac{d-1}{2}\right] - 1\right)$ 個の検査和の値は e である. したがって, 過半数をとる値 e があれば, 第 i ベクトルから e を差引いて訂正する. それ以外のときは半数以上が 0 となるが, このときは第 i ベクトルはそのままよい.

この復号法は一段の多数決素子のみを用いるので、1ステップ復号法とよばれる。次の結果はその必要条件である。

Ⅱ. 2⁽²⁾ $\bar{d}$ を双対符号の最短距離とすると、1ステップ復号法で訂正できる誤りの数を t_1 とすると、

$$t_1 \leq \frac{n-1}{2(\bar{d}-1)}.$$

これより、Golay の3重誤り訂正 (23, 12) 符号では、 $t_1 = 1$ 。また、(63, 32) Reed-Solomon 符号 (RS 符号) では $t_1 = 0$ 等、多くの RS 符号ではきわめてわずかの誤りしか訂正できない。

$t_1 = \left\lfloor \frac{d-1}{2} \right\rfloor$ なる符号は1ステップで完全に直交化可能であるといわれる。つぎに、

1. $(\alpha_1^{(1)}, \dots, \alpha_{i_1}^{(1)}), \dots, (\alpha_1^{(u)}, \dots, \alpha_{i_u}^{(u)})$ に関して直交するそれぞれ $(d-1)$ 個のパリティ検査和があり、

2. もとの符号の、 $X_{\alpha_1^{(l)}} + X_{\alpha_2^{(l)}} + \dots + X_{\alpha_{i_l}^{(l)}} = 0$ ($l = 1, \dots, u$) なる新しいパリティ検査を満す部分符号が

($L-1$) ステップ直交化可能

であるような $(\alpha_1^{(1)}, \dots, \alpha_{i_1}^{(1)}), \dots$ が存在するような符号を L ステップ直交化可能であるという。

Reed-Muller 符号は L ステップ復号可能な代表的符号である。

T. 3 L ステップ復号法で訂正できる誤りの数を t_L とすると,

$$t_L \leq \frac{2n - \bar{d}}{2\bar{d}}.$$

上の2つの定理は1ステップと L ステップで訂正能力に差のあることを示している。しかし、 L ステップ復号法によっても、本来の訂正能力まで訂正できない符号がある。たとえば、拡大RS符号は(自明なものを除き)いかなる L に対しても L ステップ直交化不能である⁽⁴⁾。また、2重誤り訂正2元フリミタフ BCH 符号は、 $m \geq 5$ なら L ステップ直交化不能である⁽³⁾。

§ 2. 一般化されたパリティ検査

J 個のパリティ検査和 (1) は次の3条件を満たすとき、
 $(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ に関し直交しているという。
 ここで、 $1 \leq \alpha_1 < \dots < \alpha_i \leq n$, $1 \leq m_1 < \dots < m_s \leq n$.

- 1) $h_{j\alpha_i} = 1$, $1 \leq j \leq J$, $1 \leq i \leq I$,
- 2) h_{jm_t} は任意, $1 \leq j \leq J$, $1 \leq t \leq s$,
- 3) α_i ($1 \leq i \leq I$), m_t ($1 \leq t \leq s$) 以外の各 l について, $h_{1l}, h_{2l}, \dots, h_{Jl}$ のうち、高々1つを除いて、すべて0.

たとえば、次のように係数を行列形に書いた $J = 4$ 個のパリティ検査和は $(1, 3; 2, 5, 7)$ に関し直交している。

$$\begin{bmatrix} 1 & \beta_1 & 1 & 0 & \beta_2 & \gamma_1 & \beta_3 & 0 & 0 \\ 1 & \beta_4 & 1 & 0 & \beta_5 & 0 & \beta_6 & 0 & \gamma_2 \\ 1 & \beta_7 & 1 & \gamma_3 & \beta_8 & 0 & \beta_9 & 0 & 0 \\ 1 & \beta_{10} & 1 & 0 & \beta_{11} & 0 & \beta_{12} & \gamma_4 & 0 \end{bmatrix}.$$

つぎに、 $(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ に関する一般化されたパリティ検査式とは、 $m_1, \dots, m_s$ に誤りが起っていないとき、位置 $\alpha_1, \dots, \alpha_i$ の誤りの和を与える式と定義され、 $C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ とかけられる。これは $m_1, \dots, m_s$ の位置に誤りが無いという条件のもとで $e_{\alpha_1} + e_{\alpha_2} + \dots + e_{\alpha_i}$ の推定値を与える論理式である。Gore⁽⁴⁾ は上の定義のもとに次の3つの定理を示している。

T. 4 $\left[\frac{J}{2}\right]$ 重以下の誤りに対しては、 $(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ に関し直交する J 個のパリティ検査和から、 $C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ の値が求められる。

T. 5 $\left[\frac{J}{2}\right]$ 重以下の誤りに対しては、 $m_{s+j_i}^{(i)}$ がすべて相異なるとして、 J 個の一般化されたパリティ検査式

$$C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s, m_{s+1}^{(1)}, \dots, m_{s+j_i}^{(i)}),$$

$$C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s, m_{s+1}^{(2)}, \dots, m_{s+j_2}^{(2)}),$$

$$\vdots$$

$$C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s, m_{s+1}^{(J)}, \dots, m_{s+j_J}^{(J)})$$

から,

$$C(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$$

の値が求められる.

(T. 5 は Gore より一般の形で示している.)

T. 6 $\left\lfloor \frac{J}{2} \right\rfloor$ 重以下の誤りに対して, $s + J - 1$ の位置の任意の組合せ $(m_1, \dots, m_s)$ について $(\alpha_1, \dots, \alpha_i; m_1, \dots, m_s)$ に関する一般化されたパリティ検査式が作られるなら, 位置 $\alpha_1, \dots, \alpha_i$ における誤りの和 $C(\alpha_1, \dots, \alpha_i)$ を正しく求めることができる.

Gore は上の定理により, RS 符号が復号可能であることを示しているが, 本文ではさらに任意の群符号が同様に復号できることを示す.

T. 7 任意の群符号 C は次の意味で多数決素子で復号可能である. すなわち, $\left\lfloor \frac{d-1}{2} \right\rfloor$ 重以下の誤りに対して, 任意の情報点 α_i について, $C(\alpha_i)$ が一般化されたパリティ検査式によって正しく求められる. d は C の最短距離.

証明. T. 6 の条件を満たすように $J = d - 1$ 個の $(\alpha_i; m_1, \dots, m_s)$ に関する一般化されたパリティ検査式を選ぶこ

と示せばよい.

C のパリティ検査行列 H のどの $(d-1)$ 列も一次独立である. いま, 一般性を失うことなく $1, 2, \dots, d$ 列に着目し, 行操作のみで, H を図1の形でしかも $a_1 = \dots = a_{d-1} = 1$, $b_1, b_2, \dots, b_{d-1} \neq 0$ となるように変形できる. 実際, 第2列, $\dots$, 第 d 列は一次独立ゆえ行操作により図1のように変形できる.

図1

$$\left[\begin{array}{cccc|cccc} a_1 & b_1 & & & & & & \\ & a_2 & & b_2 & & 0 & & \\ & \vdots & & & \ddots & & & \\ & & 0 & & & & & \\ a_{d-1} & & & & & & b_{d-1} & \end{array} \right]$$

ここで, どの $a_1, \dots, a_{d-1}$ も0でないなら, 各行 (必要なら正規化して), はじめの $(d-1)$ 行の第1要素をすべて1とできるからよい. もし, $a_1, \dots, a_{d-1}$ の中に0となるものがあれば, その各々につき次の操作を行う.

$a_i = 0$ のとき, H の第1列, $\dots$, 第 $(i-2)$ 列, 第 i 列, $\dots$, 第 d 列について行変形を行い, 少なくとも一つ第1要素が0でなく, 第2, $\dots$, $(i-2)$, i , $\dots$, d 要素が0であるような行 y を作りうる. もし, y の第 $(i-1)$ 要素

が0でなければこの行を先の第 i 行のかわりに用い、さもなければ、先の第 i 行に y を加えこめばよい。(証明終)

Gore の T. 6 の証明は復号回路の一つの構成に対応するが、その方法によれば、 s 段の多数決素子から成る回路となり相当複雑である。T. 5 は Gore の結果を拡張したものであるが、できるだけ、 j_t ($1 \leq t \leq J$) を大きく選ぶようにすることにより、Gore の回路より若干複雑さが緩和される。

文 献

1. Massey, J. L., Threshold Decoding, MIT, 1963.
2. Weldon, E. J. Jr., "Some results on majority-logic decoding," in Error Correcting Codes, H. B. Mann (ed.) Wiley, 1969.
3. Chow, D. K., "On threshold decoding of cyclic codes," Inf. and Contr., 13, 471-483, 1968.
4. Gore, W. C., "Generalized threshold decoding and the Reed-Solomon codes," IEEE Transactions on IT., vol. IT-15, 78-81, 1969.