数理解析研究所講究録
82巻 1970年 23-30

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$h_i = (h_{i1}, h_{i2}, \cdots, h_{in})$とベクトル$y = (y_1, y_2, \cdots, y_n)$との内積

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

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$y = (y_1, \cdots, y_n)$は送信された符号語$x = (x_1, \cdots, x_n) \in C$と誤りベクトル$e = (e_1, \cdots, e_n)$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

$$s_1 = \sum_{i=1}^{n} h_{1i} y_i = \sum_{i=1}^{n} h_{1i} e_i$$

$$\left.\begin{aligned} S_2 &= \sum_{i=1}^{n} h_{2i} y_i = \sum_{i=1}^{n} h_{2i} e_i \\ &\vdots \\ S_J &= \sum_{i=1}^{n} h_{Ji} y_i = \sum_{i=1}^{n} h_{Ji} e_i \end{aligned}\right\} \quad (1)$$

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

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

2) $\ell \neq \alpha_i$ $(1 \leq i \leq I)$ なる各 ℓ について，$h_{1\ell}, h_{2\ell}, \cdots, h_{J\ell}$ 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 が各ケタ i に対し，(i) に関し直交する少くとも $(d-1)$ 個の検査和をもてば，C の最短距離は少くとも 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 ケタに関し直交する $(d-1)$ 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 ケタが誤っていないときは，少くとも $d-1-\left[\frac{d-1}{2}\right]$ の検査和の値は 0 である．また，第 i ケタに誤り e が生じていれば，少くとも $d-1-\left(\left[\frac{d-1}{2}\right]-1\right)$ 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 ケタから 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 ケタはそのままでよい．

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．

T. 2[2]　$\bar{d}$ を双対符号の最短距離とするとき，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，

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

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．

$t_1 = \left[\frac{d-1}{2}\right]$ 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. $(\alpha_1^{(1)}, \cdots, \alpha_{i_1}^{(1)}), \cdots, (\alpha_1^{(u)}, \cdots, \alpha_{i_u}^{(u)})$ 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，$X_{\alpha_1}^{(l)} + X_{\alpha_2}^{(l)} + \cdots + X_{\alpha_{il}}^{(l)} = 0$ $(l = 1, \cdots, u)$ 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 $(\alpha_1^{(1)}, \ldots, \alpha_{i_1}^{(1)}), \ldots$ 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,

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

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元プリミタブBCH符号は, $m \geqq 5$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条件を満すとき, $(\alpha_1, \cdots, \alpha_I ; m_1, \cdots, m_S)$ に関し直交しているという. ここで, $1 \leqq \alpha_1 < \cdots < \alpha_I \leqq n$, $1 \leqq m_1 < \cdots < m_S \leqq n$.

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

2) h_{jm_t} は任意, $1 \leqq j \leqq J$, $1 \leqq t \leqq S$,

3) α_i $(1 \leqq i \leqq I)$, m_t $(1 \leqq t \leqq S)$ 以外の各lについて, $h_{1l}, h_{2l}, \cdots, h_{Jl}$ 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，$(\alpha_1,\cdots,\alpha_i;m_1,\cdots,m_s)$ に関する一般化されたパリティ検査式とは，$m_1,\cdots,m_s$ に誤りが起っていないとき，位置 $\alpha_1,\cdots,\alpha_i$ の誤りの和を与える式と定義され，$C(\alpha_1,\cdots,\alpha_i;m_1,\cdots,m_s)$ とかかれる．これは $m_1,\cdots,m_s$ の位置に誤りがないという条件のもとで $e_{\alpha_1}+e_{\alpha_2}+\cdots+e_{\alpha_i}$ 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．

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

<u>T. 5</u>　$\left[\frac{J}{2}\right]$ 重以下の誤りに対しては，$m_{s+j}^{(i)}$ 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

$$C(\alpha_1,\cdots,\alpha_i;m_1,\cdots,m_s,m_{s+1}^{(1)},\cdots,m_{s+j_1}^{(1)}),$$

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

$$\vdots$$

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

から，

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

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 $\left[\frac{J}{2}\right]$ 重以下の誤りに対して，$s+J-1$ の位置の任意の組合せ $(m_1, \cdots, m_s)$ について $(\alpha_1, \cdots, \alpha_i ; m_1, \cdots, m_s)$ 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 $\alpha_1, \cdots, \alpha_i$ における誤りの和 $C(\alpha_1, \cdots, \alpha_i)$ 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，$\left[\frac{d-1}{2}\right]$ 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の条件を満すように $J = d-1$ 個の $(\alpha_i ; m_1, \cdots, m_s)$ に関する一般化されたパリティ検査式を選べるこ

とを示せばよい.

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 $1, 2, \cdots, d$ 列に着目し, 行操作のみで, Hを図1の形でしかも $a_1 = \cdots = a_{d-1} = 1$, $b_1 b_2 \cdots b_{d-1} \neq 0$ となるように変形できる. 実際, 第2列, ・・・, 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

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

ここで, どの $a_1, \cdots, a_{d-1}$ 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, $a_1, \cdots, a_{d-1}$ 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, ・・・, 第 $(i-2)$ 列, 第 i 列, ・・, 第d列について行変形を行い, 少くとも一つ第1要素が0でなく, 第2, ・・・, $(i-2)$, i, ・・・, 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.