北海道大学工学部研究報告
第76号 (昭和50年)

Bulletin of the Faculty of Engineering,
Hokkaido University, No. 76 (1975)

高速復号化が可能な誤り制御符号

武智　真*　黒部貞一*　小川吉彦*

(昭和49年12月27日受理)

A Class of Fast Decodable Error Control Codes

Makoto TAKECHI　Teiichi KUROBE　Yoshihiko OGAWA

(Received December 27, 1974)

Abstract

The new class of codes developed and described in this paper is one-step majority-logic decodable and noncyclic. It can be constructed by means of balanced incomplete block design (BIBD). The redundancy of this class of codes is inferior to the conventional Hamming or BCH code, but it has a simple decoder and can be decoded at a very high speed. These codes are suitable for applications to computer memories, in particular where large scale integrated circuits are used.

1. まえがき

メモリ装置に誤り制御符号を用いると，誤りの原因によらずに誤りの検出訂正ができ，メモリ装置の信頼性が高められる[1]。誤り制御符号では一般に，符号長に対する冗長ビット数の比を小さくして能率を高くすると復号化が複雑になる。メモリ装置では冗長ビット数が直接メモリ本体の装置量を増加させるので高能率の符号が望ましいが，復号化による遅延も考慮しなければならない。ここでは並列演算系のメモリ装置への大規模集積回路 (LSI) メモリの適用を想定し，その大容量性によって能率に対する要求を多少緩め，復号法を簡単にして，その高速性を十分発揮できるような誤り訂正検出符号を考えた。

2. 並列復号化の問題点

高速復号化を実現するにはどのような構造をもつ復号器が要求されるだろうか。並列復号化における遅延は主に偶奇性検査のときに生じる。いま u 個の入力の偶奇性検査をするには u 個の入力をもつ EX-OR (排他的論理和) ゲートを用いればよい。しかし，u が大きくなると1個の EX-OR ゲートでは実現不可能になる。そこで入力数 v の EX-OR ゲートを複数個用いて図1の回路で偶奇性検査を行なう場合に，EX-OR ゲートが L 段必要であれば

$$L = \log_v u \qquad (1)$$

v は使用するゲートの種類で決まってしまうので段数を小さくするには入力数は小さい程よい。これから高速復号化を実現するには偶奇性検査行列 H の行の重み(1の総数)を小さくするとよい。

* 電子工学科　電子回路工学講座

また従来から用いられてきたHamming符号やBCH符号は高能率の符号として知られているが，これらを並列復号化する場合には復号器が記憶すべき誤りパターンの総数は符号長が大きくなるにつれて膨大になり現実に装置化することは困難になる[2]。従って並列復号化の場合には複雑で高い識別能力をもつ復号器よりも，構造が簡単で十分実現性があり，しかも高速復号化が可能な符号が望ましい。

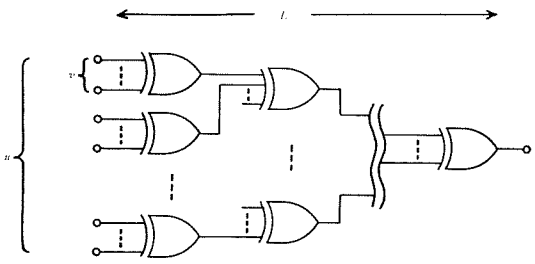


図1 多入力偶奇性検査回路

3. しきい値素子による復号法

BCH符号よりも能率の低い符号しか構成できないが，復号化が容易な復号法としてしきい値素子による復号法がある[3),4)]。これはある情報点 x_i の誤りビット e_i (x_i が誤りであれば $e_i=1$，そうでなければ $e_i=0$) に対して J 個の複合パリティ検査 $A_1, A_2, \cdots, A_J$ を考える。
これらは次のような形をしている。

$$A_j = e_i + \sum_{i' (\neq i)} e_{i'} \qquad (j=1, 2, \cdots, J;\ \mathrm{mod}\ 2) \qquad (2)$$

ここで e_i は J 個の複合パリティ検査のいずれにも含まれ，他の誤りビット $e_{i'}$ は J 個の複合パリティ検査中に高々一度含まれるものとする。このとき $A_1, A_2, \cdots, A_J$ は e_i に直交しているという。

いま t 個以内の誤りを生じたときに1となる複合パリティ検査の個数を調べる。x_i が誤りの場合には最大が J で x_i 以外の誤りが一つの複合パリティ検査中に偶数個生じた場合であり，最小が $J-(t-1)$ で t 個の誤りを生じたときに e_i 以外には同じ複合パリティ検査に2個以上の誤りがない場合である。x_i が誤りでない場合には最大が t で t 個の誤りを生じたときに同じ複合パリティ検査に2個以上の誤りがない場合であり，最小が0でこのときは誤りがないかまたは一つの複合パリティ検査に偶数個の誤りを生じた場合である。これらの複合パリティ検査からある情報点 x_i が誤りか否かを判定するには $J-(t-1)$ と t が区別できればよいので

$$J > 2t-1 \qquad (3)$$

なる関係があればよい。誤り訂正の方法は J 個の複合パリティ検査を入力とするしきい値 $J-(t-1)$ のしきい値素子の出力が1であれば x_i は誤りと見做し誤りを訂正できる。

4. 釣合い不完備ブロック計画

しきい値素子復号法が可能な符号を構成する準備として，釣り合い不完備ブロック計画[5)] (balanced incomplete block design 以下 BIBD と略す) について述べる。

$Y=\{y_1, y_2, \cdots, y_v\}$ を v 個の元からなる集合とする。Y の BIBD とは次のような条件を満足するような Y の h 個の元をもつ部分集合 b 個の集まりである。(h 個の元をもつ部分集合を $B_1, B_2, \cdots, B_b$ と表わし，ブロックと呼ぶことにする。)

1. 各々の元は b 個のブロック中にちょうど r 回現われる。
2. どの2個の元も b 個のブロック中にちょうど λ 回同時に現われる。
3. $h<v$

BIBD を表現するのに生起行列 N がよく使われる。これは行に Y の v 個の元を，列に b 個

のブロックを対応させた v 行 b 列の行列であり，もし元 y_i がブロック B_j に含まれるならば i 行 j 列の元 n_{ij} は 1，そうでなければ 0 という成分をもつ行列である。例えば $(v, h, b, r, \lambda)=(4, 2, 6, 3, 1)$ の BIBD の生起行列 N は図 2 のようになる。

$$N = \begin{array}{c} \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & & & \\ 1 & & & 1 & 1 & \\ & 1 & & 1 & & 1 \\ & & 1 & & 1 & 1 \end{bmatrix} \end{array}$$

図 2 $(v, h, b, r, \lambda)=(4, 2, 6, 3, 1)$ の BIBD の生起行列 N

BIBD では次のような関係* が成立する。

$$bh = vr \tag{4}$$

$$r(h-1) = \lambda(v-1) \tag{5}$$

$$b \geqq v \tag{6}$$

式(4)は生起行列 N に含まれる 1 の総数を表わし，式(5)はある特定の 1 個の元を含む 2 個の元からなる部分集合がブロック中に出現する回数を数えたものである。また式(6)は生起行列 N は常に横長になることを意味する。

5. パリティ検査行列 H の構造

いま k 個の情報点 $x_1, x_2, \cdots, x_k$ の中に含まれる t 個の誤りを訂正する為に m 個の検査点 $c_1, c_2, \cdots, c_m$ を付加するものとし，しきい値素子復号法が可能であるようにしたい。まずこの誤り訂正符号のパリティ検査行列 H を梯形正準形にし符号器の装置量を減らしたいので，m 行 n 列の行列 H を次のようにおく。

$$H = [Q \mid I_m] \tag{7}$$

ここで部分行列 I_m は m 次の単位行列，Q は m 行 k 列の行列である。複合パリティ検査と誤り訂正能力の関係は式(3)で与えられるが，復号器を簡単にする為に

$$J = 2t \tag{8}$$

とすると，各々の情報ビットに直交な複合パリティ検査が $2t$ 個あればよい。従って部分行列 Q の k 個の列の重みは $2t$ であり，m 個の行の重みをすべて等しく l とする。

次に BIBD を用いて部分行列 Q を決める。Q が横長，縦長の場合に分けて考える。

(i) $m \leqq k$ のとき　v 個の行を m，b 個の列を k に対応させ，各々の情報ビットに直交な複合パリティ検査を $2t$ 個作るには h を $2t$，λ を 1 とするとよいので (v, h, b, r, λ) を $(m, 2t, k, l, 1)$ に対応させる。すると式(4)と(5)から

$$k = \frac{\binom{m}{2}}{\binom{2t}{2}} \tag{9}$$

$$l = \frac{m-1}{2t-1} \tag{10}$$

が得られ，k, l が共に整数になるとき部分行列 Q は生起行列 N と同じ構造をもつ。このときパ

* 式(4), (5), (6)の詳細な証明は文献(5)の Theorem 14-5, 及び 14-7 を参照のこと。

リティ検査行列 H は

$$H=[N\,|\,I_m]. \tag{11}$$

(ii) $m>k$ のとき　この場合は式(6)より BIBD は構成できない。そこで次の定理を用いる。

[定理] $\lambda=1$ の BIBD の生起行列の転置行列 N^T を生起行列とする計画は $\lambda\leqq 1$ の PBIBD* である。

[証明] 背理法により，$\lambda=1$ である行列 N の任意の2個の列ベクトルは同じ元を2個以上含まないことを示す。いま任意に2個の列ベクトルを選んだときに同じ元が2個以上あったとする。すると同じ2個の元が b 個のブロック中に少なくとも2カ所で出現することになり，BIBD の条件2から $\lambda=1$ の BIBD と矛盾する。従って行列 N の任意の2個の列ベクトルは同じ元を同時に2個以上含まない。このことから行列 N^T の任意の2行の内積は1または0である。(証明終)

部分行列 Q を行列 N^T に対応させて決定するには v 個の列を k，b 個の行を m，r を $2t$，λ を1にすればよいので $(v,\ h,\ b,\ r,\ \lambda)$ を $(k,\ l,\ m,\ 2t,\ 1)$ で置き換える。このとき

$$k=\frac{m(2t-1)}{4t^2-m} \tag{12}$$

$$l=\frac{2t(2t-1)}{4t^2-m} \tag{13}$$

が共に整数になるときパリティ検査行列 H は，

$$H=[N^T\,|\,I_m]. \tag{14}$$

6. 誤り訂正検出符号

いままでは一語中で t 個までの誤りを訂正する符号について議論してきた。ここでは t 個までの誤りを訂正し，更に $(t+1)$ 個の誤りを検出する符号に拡張する。いま $(t+1)$ 個までの誤りが生じたとし，ある誤りビット e_i に直交な複合パリティ検査で1となるものを数える。$e_i=1$ のときは最小が $J-t$，$e_i=0$ のときは最大が $(t+1)$ となる。$(t+1)$ 個の誤りを検出するには両者を識別する必要がないので，$J=2t+1$ とすると

$$J=2t+1>2t-1 \tag{15}$$

となり，式(3)より t 個までの誤りを訂正し，$(t+1)$ 個の誤りを検出できる符号が構成される。

次に誤り検出の方法について述べる。式(7)のパリティ検査行列 H で部分行列 Q の列ベクトルの重みが $(2t+1)$ だから行列 H の列ベクトルはすべて奇数重みになる。行列 H から全部で m 個の複合パリティ検査が得られるが，これらをすべて加え合わせると

$$\begin{aligned}A_1+A_2+\cdots+A_m&=\sum_{i_1}^{l+1}e_{i_1}+\sum_{i_2}^{l+1}e_{i_2}+\cdots+\sum_{i_m}^{l+1}e_{i_m}\\&=(2t+1)(e_1+e_2+\cdots+e_k)+e_{k+1}+\cdots+e_n\\&=e_1+e_2+\cdots+e_k+e_{k+1}+\cdots+e_n\qquad(\mathrm{mod}\,2)\end{aligned} \tag{16}$$

ここで e_1 から e_k までは情報点に，e_{k+1} から e_n までは検査点に対応する誤りビットであり，式(16)は一語の全ビットにわたって偶奇性検査を行なったことを示している。この結果式(16)の値が1であれば奇数個の，0であれば偶数個の誤りが生じたと見做される。但し $(t+2)$ 個以上の誤りの一部は誤って訂正検出されることになる。

---

* partially balanced incomplete block design の略。生起行列の任意の2行の内積が一意にきまらないものをいう。厳密な定義は文献(6)の p. 144 参照。

7. 符 号 の 例

並列処理系のメモリ装置に用いられる比較的情報点数の小さな場合に適当と思われる一誤り訂正符号[7]，二誤り訂正符号，一誤り訂正二誤り検出符号について調べる。

(1) 一誤り訂正符号

非短縮符号の情報点数 k は式(9)より

$$k=\binom{m}{2} \qquad (k\geqq 1) \tag{17}$$

このとき $(n,\ k)=\left(\binom{m+1}{2},\ \binom{m}{2}\right)$ となる。いくつかのパリティ検査行列の例を図3に示す。

(1) (10, 6)

$$\begin{array}{c} \begin{array}{cccccccccc} 1 & & & & 5 & & & & & 10 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & & & & 1 & & & \\ 1 & & & 1 & 1 & & & 1 & & \\ & 1 & & 1 & & 1 & & & 1 & \\ & & 1 & & 1 & 1 & & & & 1 \end{bmatrix} \begin{array}{l} 1 \\ \\ \\ 4 \end{array} \end{array}$$

(2) (15, 10)

$$\begin{array}{c} \begin{array}{cccccccccccccc} 1 & & & & 5 & & & & & 10 & & & & & 15 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & & 1 & & & & \\ 1 & & & & 1 & 1 & 1 & & & & & 1 & & & \\ & 1 & & & 1 & & & 1 & 1 & & & & 1 & & \\ & & 1 & & & 1 & & 1 & & 1 & & & & 1 & \\ & & & 1 & & & 1 & & 1 & & 1 & & & & 1 \end{bmatrix} \begin{array}{l} 1 \\ \\ \\ \\ 5 \end{array} \end{array}$$

(3) (21, 15)

$$\begin{array}{c} \begin{array}{cccccccccccccccccccc} 1 & & & & & 5 & & & & & 10 & & & & & 15 & & & & & 20 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & & & & & & & & & & 1 & & & & & \\ 1 & & & & & 1 & 1 & 1 & 1 & & & & & & & 1 & & & & \\ & 1 & & & & 1 & & & & 1 & 1 & 1 & & & & & 1 & & & \\ & & 1 & & & & 1 & & & 1 & & & 1 & 1 & & & & 1 & & \\ & & & 1 & & & & 1 & & & 1 & & 1 & & 1 & & & & 1 & \\ & & & & 1 & & & & 1 & & & 1 & 1 & & & & & & & 1 \end{bmatrix} \begin{array}{l} 1 \\ \\ \\ \\ \\ 5 \end{array} \end{array}$$

図3 一誤り訂正符号のパリティ検査行列の例

また図4に (10, 6) 一誤り訂正符号の符号化及び復号化回路を示す。復号器に必要なゲートは複合パリティ検査を計算する為の m 個の EX-OR，誤りの有無を判定する k 個のしきい値素子，誤り訂正用の k 個の2入力 EX-OR ゲートが必要であり，符号器の検査点を付加する為の m 個の

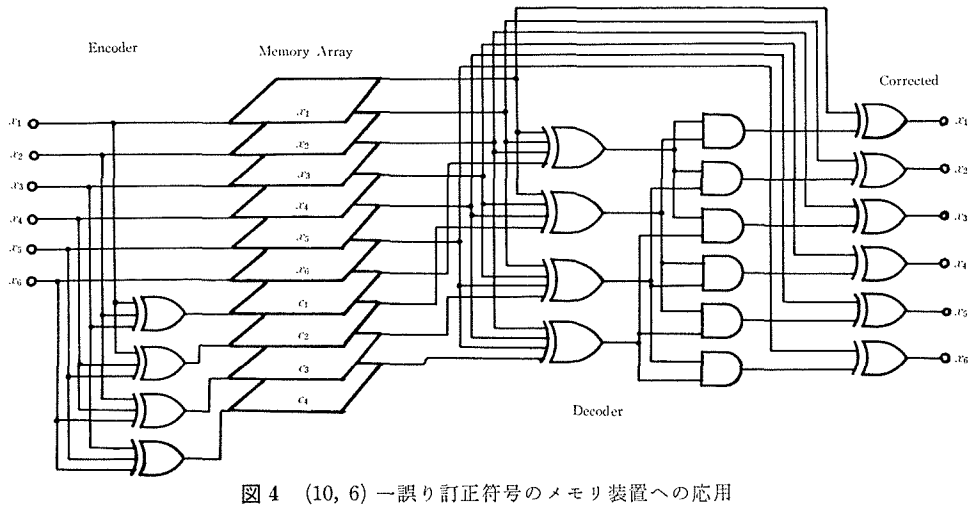


図4 (10, 6) 一誤り訂正符号のメモリ装置への応用

EX-OR ゲートは復号器の複合パリティ検査の計算回路と共通に使うことも可能である。

次に主要な遅延の原因となるパリティ検査行列の行の重みについて考える。行の平均の重みは，この一誤り訂正符号では

$$\frac{2k+m}{m}=\frac{2k}{m}+1 \tag{18}$$

非短縮の Hamming の一誤り訂正符号では

$$\frac{1}{m}\sum_{i=1}^{m} i\binom{m}{i}=\sum_{i=1}^{m}\binom{m-1}{i-1} \tag{19}$$

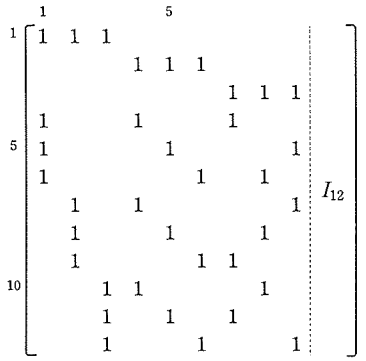
であり，同じ情報点数に対しては常に式(18)は式(19)より小さいことが示される。

(2) 二誤り訂正符号

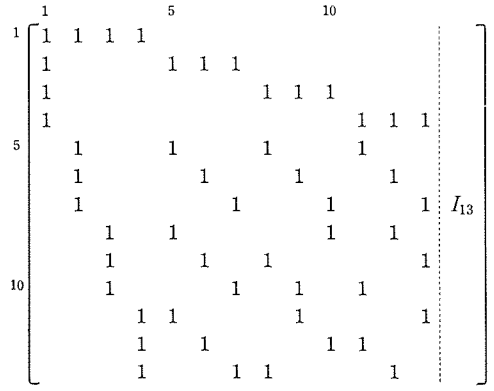
情報点数 k と検査点数 m の関係は式(9)と(12)より

$$k=\begin{cases}\dfrac{m(m-1)}{12} & (k\geqq m\geqq 13) \qquad (20)\\[2ex] \dfrac{48}{16-m}-3 & (k<m<13) \qquad (21)\end{cases}$$

(1) (21, 9)



(2) (26, 13)



(3) (36, 20)

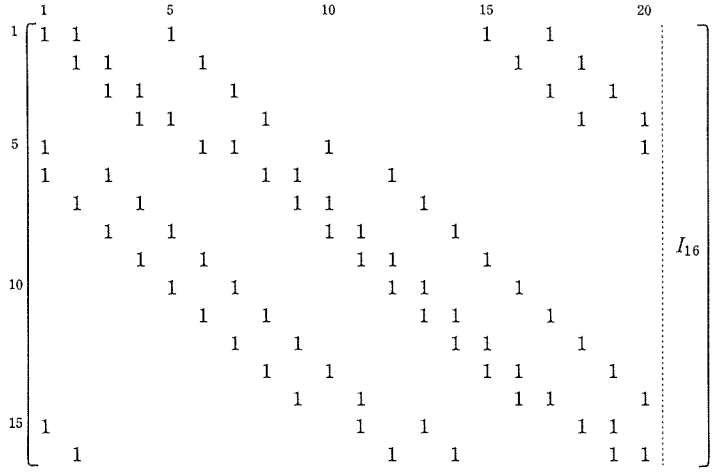


図 5 二誤り訂正符号のパリティ検査行列の例

非短縮の二誤り訂正符号は式(21)から，(15, 5)，(21, 9)，式(20)から(26, 13)，(36, 20)，(75, 50)等の符号が構成される。復号器のしきい値素子は，4入力でしきい値3のものが必要になる。図5にパリティ検査行列の例を示す。

(3) 一誤り訂正二誤り検出符号

このとき情報点数 k は

$$k=\begin{cases}\dfrac{m(m-1)}{6} & (k\geqq m\geqq 7) \qquad (22)\\[2ex] \dfrac{18}{9-m}-2 & (k<m<7) \qquad (23)\end{cases}$$

非短縮符号は式(23)から(10, 4)，式(22)から(14, 7)，(21, 12)，(39, 26)，(50, 35)等が得られる。誤り訂正は3入力をもち，しきい値が2のしきい値素子を用い，誤り検出は全複合パリティ検査にわたるパリティが1であれば1個，0であれば2個の誤りを生じたものとみなす。図6にいくつかのパリティ検査行列を示す。

(1) (10, 4)

$$\begin{array}{c} \begin{matrix} & 1 & & & 4 \end{matrix} \\ \begin{matrix} 1 \\ \\ \\ \\ 5 \end{matrix}\left[\begin{array}{cccc:c} 1 & 1 & & & \\ 1 & & 1 & & \\ 1 & & & 1 & \\ & 1 & 1 & & \\ & 1 & & 1 & \end{array}\right.\begin{matrix} \\ \\ \\ \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right] \end{matrix} \\ \\ \\ \\ \\ \\ \end{array}\begin{matrix} \\ \\ \\ \\ I_6 \end{matrix}$$

(2) (14, 7)

$$\begin{array}{c} \begin{matrix} & 1 & & & & 5 & & \end{matrix} \\ \begin{matrix} 1 \\ \\ \\ \\ \\ 5 \end{matrix}\left[\begin{array}{ccccccc:c} 1 & & & & & 1 & & 1 & \\ 1 & 1 & & & & & 1 & & \\ & 1 & 1 & & & & & 1 & \\ 1 & & 1 & 1 & & & & & \\ & 1 & & & 1 & 1 & & & \\ & & & 1 & & 1 & 1 & & \\ & & & & 1 & & 1 & 1 & \end{array}\right.\begin{matrix} \\ \\ \\ \\ \\ \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\\a\end{array}}\right] \end{matrix} \\ \\ \\ \\ \\ \\ \\ \end{array}\begin{matrix} \\ \\ \\ \\ \\ \\ I_7 \end{matrix}$$

(3) (21, 12)

$$\begin{array}{c} \begin{matrix} & 1 & & & & 5 & & & & 10 & & \end{matrix} \\ \begin{matrix} 1 \\ \\ \\ \\ 5 \end{matrix}\left[\begin{array}{ccccccccccc:c} 1 & & & 1 & & & 1 & & & 1 & & & \\ 1 & & & & 1 & & & 1 & & & 1 & & \\ 1 & & & & & 1 & & & 1 & & & 1 & \\ & 1 & & 1 & & & & 1 & & & & 1 & \\ & 1 & & & 1 & & & & 1 & 1 & & & \\ & 1 & & & & 1 & 1 & & & & 1 & & \\ & & 1 & 1 & & & & & 1 & & 1 & & \\ & & 1 & & 1 & & 1 & & & & & 1 & \\ & & 1 & & & 1 & & 1 & & & & & \end{array}\right.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\\a\\a\\a\end{array}}\right] \end{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ I_9 \end{matrix}$$

図6 一誤り訂正二誤り検出符号のパリティ検査行列の例

8. ま と め

並列演算系の誤動作を検出する為にパリティビットを用いる方法が行なわれてきた。しかし最近の LSI のように歩留りの悪い一括生産形態をもつメモリ素子を用いてメモリ装置を構成するとき，より高い訂正能力をもつ符号が必要になる。このときに通信で使われてきた符号を並列動作させるよりも，新たに BIBD を用いた幾何学的配置によってきめられたパリティ検査行列をもつ符号が並列処理に適していることを示した。またこれらの符号の復号器は装置量が少なくしかも同じパターンの繰り返しが多い為，復号器の信頼性は高い。今後も開発が予想される高速で大容量のメモリ素子の誤り制御にこれらの符号は適していると思われる。

参 考 文 献

1) M. Graham: "Error Correction in Batch-Fabricated Memories" IEEE Transaction on Computers, June 1969, pp. 566-567.
2) 武智, 黒部, 小川: "BCH 符号の並列復号化の複雑さについて" 昭和49年度電子通信学会全国大会論文集, 1412.
3) 宮川, 岩垂, 今井: "符号理論" 昭晃堂, 1973.
4) W. W. Peterson, and E. J. Weldon: "Error Correcting Codes" 2nd edition M.I.T., Press 1972.
5) C. L. Liu: "Introduction to Combinatorial Mathematics" McGraw-Hill 1968, pp. 370-374.
6) 石井: "実験計画法/配置の理論" 培風館, 1972.
7) 武智, 黒部, 小川: "高速復号化が可能な一誤り訂正符号について" 昭和49年度電気四学会北海道支部連合大会論文集, 138.