# 論文 / 著書情報
# Article / Book Information

| | |
|---|---|
| 題目(和文) | 誤り位置指摘符号に関する研究 |
| Title(English) | |
| 著者(和文) | 北神正人 |
| Author(English) | Masato Kitakami |
| 出典(和文) | 学位:博士（工学）,<br>学位授与機関:東京工業大学,<br>報告番号:甲第3196号,<br>授与年月日:1996年3月26日,<br>学位の種別:課程博士,<br>審査員: |
| Citation(English) | Degree:Doctor of Engineering,<br>Conferring organization: Tokyo Institute of Technology,<br>Report number:甲第3196号,<br>Conferred date:1996/3/26,<br>Degree Type:Course doctor,<br>Examiner: |
| 学位種別(和文) | 博士論文 |
| Type(English) | Doctoral Thesis |

# 誤り位置指摘符号に関する研究

指導教官　藤原英二 教授

提出者　東京工業大学大学院 理工学研究科
博士課程 情報工学専攻
北神 正人

# 目 次

# 第1章　序論

## 1.1　背景

計算機システムの高集積化・高性能化によってもたらされた高度情報化社会の進展は, 我々の日常生活を従来よりも便利で快適なものにしており, 現代社会は計算機システムの存在無しには機能しなくなっているとさえいえる. しかし, 現代社会が計算機システムにあまりにも依存してしまっているため, ひとたび計算機システムに異常が生じると我々の生活に重大な影響を与えてしまう. そのため, 計算機システムの高信頼化への要請が年々高まっている.

計算機システムの高信頼化技術として注目されている技術にフォールトトレラント (fault tolerant) 技術がある. この技術はシステムの構成要素に冗長性をもたせることによって故障の影響を軽減させる技術である [1]. 誤り制御符号 [2], [3] はこのフォールトトレラント技術の中で重要な位置を占める技術であり, メモリシステムをはじめとする様々な分野に利用されている. 本研究はこの誤り制御符号の一機能である誤り位置指摘機能を有する符号を主な対象としている.

## 1.2　従来の研究

誤り制御符号の研究は 1948 年に発表された Shannon の論文 [4] に始まる. 具体的な符号構成法の提案は Hamming 符号 [5] が最初である. 計算機の半導体メモリシステムに最もよく使用されているのは上記の Hamming 符号を修正した単一ビット誤り訂正・二重ビット誤り検出符号 ($SEC-DED$ 符号)[6] である. 1 ビット出力素子で構成されたメモリシステムでは単一素子故障時の符号語に対する影響は 1 ビットであるので, このようなシステムにおいては $SEC-DED$ 符号は有効な符号である.

ところが, 最近使用されるようになってきた $b(\geq 2)$ ビット出力のメモリ素子を用いたシステムでは単一の素子故障の影響が符号語中の大きさ $b$ ビットの小ブロック (バイトと呼ぶ) におよぶことがある. そこで, このような素子を用いたシステム用の符号として単一バイト誤り訂正符号 ($S_bEC$ 符号)[7], 単一バイト誤り訂正・二重バイト誤り検出符号 ($S_bEC-D_bED$ 符号)[8],[9] などが提案された.

一方, 半導体メモリ素子における故障は主に $\alpha$ 線による一時故障であるとされ, この故障による誤りはバイト出力素子においても 1 ビット誤りにとどまるとされている. すなわち, 2 ビット

以上のビットが誤る単一バイト誤りが生じる確率は単一バイト誤りの生じる確率よりも極めて低い．そのため, 単一ビット誤りを訂正し (2 ビット以上の) 単一バイト誤りを検出する符号として, 単一ビット誤り訂正・単一バイト誤り検出符号 ($SEC-S_bED$ 符号)[10], 単一ビット誤り訂正・二重ビット誤り検出・単一バイト誤り検出符号 ($SEC-DED-S_bED$ 符号)[11], [12] が提案された．これらの符号は $S_bEC$ 符号よりも少ない検査ビット数で構成可能である．また, $S_bEC$ 符号と $S_bEC-D_bED$ 符号の中間的な機能を有する符号として単一バイト誤り訂正・二重ビット誤り検出符号 ($S_bEC-DED$ 符号)[13] 単一バイト誤り訂正・(単一ビット+単一バイト) 誤り検出符号 ($S_bEC-(S+S_b)ED$ 符号)[14] が提案された.

従来の誤り制御符号の機能は誤り訂正, 検出およびこれらを組み合わせたものがほとんどであった. 誤り訂正符号では誤りの位置と大きさの両者が分かる必要があるが, 誤り検出符号では誤りの位置も大きさも分かる必要がない. 誤りの位置と大きさに関する情報のうち, 誤りの位置のみが分かる場合でも, 通信に用いると再送信のコストが削減可能である．Wolf と Elspas は この点に注目して 1963 年に誤り位置指摘符号を提案した [15]. 誤り位置指摘符号は誤り位置の概略を知ることができる符号であり, 誤り訂正符号と検出符号の中間的機能を有する符号である．その後誤り位置指摘符号に関する研究が行なわれ，行列のテンソル積を用いた構成法 [16]-[18] や巡回符号としての構成法 [19] などが提案された.

上記の誤り位置指摘符号に関する研究はすべて 1963 年から 1967 年の間に発表されたものであり, それ以降新たな誤り位置指摘符号の構成法は提案されていない. 最近になって誤り位置指摘符号を集積回路のテストへ応用することが提案されたが [20], ここでは既存の誤り位置指摘符号を用いている．Vaidya と Pradhan は [21] において誤り訂正符号, 検出符号とともに誤り位置指摘符号についても述べているが, 新しい誤り位置指摘符号は提案していない.

最近, 誤り訂正, 検出符号を含む広い概念を有する符号として誤り識別符号が杜, 坂庭によって提案された [22], [23]．この符号は誤り識別集合と呼ばれる互いに素な誤りの集合に属す誤りが生じた場合に, その誤りがどの誤り識別集合に属す誤りであるかを受信語より一意に特定可能な符号である. 彼らはこの誤り識別符号の概念を利用して各種の多値誤り訂正・検出符号の必要十分条件を導出した [23], [24]. 誤り識別符号に関する文献 [22]-[24] では誤り位置的符号について言及していないが, 同一の位置に生じた誤りが同一の誤り識別集合に属すように誤り識別集合を選択すると, この誤りを識別する符号は誤り位置指摘符号となる. しかし, 誤り識別符号の組織的な構成法は明らかになっていないので, 誤り識別符号を利用して誤り位置指摘符号を構成することはできない.

以上より, 誤り位置指摘符号に関する従来の研究では, 誤り位置指摘符号の具体的構成法の提案が少ないこと, および誤り位置指摘機能と誤り訂正, 検出機能に関する理論的な関係が明らかになっていないことが分かる.

## 1.3　本論文の概要

本論文は 7 章からなる．第 2 章では誤り位置指摘の概念およびそれに関連する従来の研究を紹介し, 第 3 章で誤り位置指摘符号に対する新しい考え方を示している．第 4 章, 第 5 章では具体的な構成法を示し, 第 6 章では誤り位置指摘符号の距離構造に関して述べている．各章の詳しい内容を以下に示す.

第 2 章では誤り位置指摘符号の概念を説明し, 誤り位置指摘符号の応用例を示している．既存の誤り位置指摘符号としてバイト誤り位置指摘符号を紹介している．さらに, 誤り識別符号を紹介し, 誤り位置指摘符号との関係について述べている.

第 3 章ではバイト出力素子を搭載したメモリカード 1 個分の出力をブロックと定義し, ブロック単位での誤り位置指摘機能を提案している．半導体メモリシステムに適した誤り位置指摘符号の機能についてメモリシステムにおける誤りの傾向をもとに述べ, メモリシステムに生じる様々な誤りを統一的に扱うことを可能とする新しい誤りの表現方法を定義している．さらに, ブロック位置指摘符号としては最も基本的な機能を有する符号である故障バイト素子を含むメモリカードを指摘する符号を提案し, 構成法を示している.

第 4 章では単一ビット誤りを訂正し, 故障バイト素子の位置を指摘する符号 ($SEC-S_{e/b}EL$ 符号) について構成法および復号法を示し, 復号回路量や誤り検出率に関する評価も行なっている.

第 5 章では単一ビット誤りを訂正し, 故障バイト素子を含むメモリカードを指摘する符号 ($SEC-S_{b/p\times b}EL$ 符号) について 2 種類の構成法を提案し, それぞれの構成法で得られた符号に対する復号法を示している．また, 復号回路量や誤り検出率に関する評価も行なっている.

第 6 章では誤り位置指摘符号の距離構造を明らかにするため, 新しい距離等を提案し, それを利用して各種の符号条件を求めている．それをもとに誤り位置指摘符号の距離構造と誤り訂正, 検出符号の距離構造の関係を明らかにしている．さらに, 得られた距離構造より既存の符号の距離構造を導出している.

第 7 章では上記の章で得られた結果を総括し, 今後の課題について述べている.

# 第2章　誤り位置指摘符号

## 2.1　緒言

本章では誤り位置指摘の概念を説明し, 誤り位置指摘符号が従来提案されていた通信だけでなく, 計算機の故障診断, 集積回路にテストにも応用可能性であることを示す. 従来の誤り位置指摘符号として Wolf らの提案した誤り位置指摘符号を紹介する. 次に, 誤り識別符号を紹介して誤り位置指摘符号との関係について述べる.

## 2.2　誤り位置指摘の概念

これまで誤り制御符号の機能としては主に以下のものが考えられてきた.

- 誤り訂正 (Error Correction)
- 誤り検出 (Error Detection)

一般に誤り訂正符号では誤りの位置, 誤りの大きさの両者が分かる必要があるが，誤り検出符号では誤りの位置も誤りの大きさも分かる必要がない．例えば単一バイト誤り訂正符号 ($S_bEC$ 符号) では誤りを含むバイトの位置とそのバイト内の誤りの大きさ (誤りパターン) の両者が分からないと単一バイト誤りを訂正できないのに対し，単一バイト誤り検出符号 ($S_bED$ 符号) では誤りを含むバイトの位置もそのバイトの誤りのパターンも分かる必要がない.

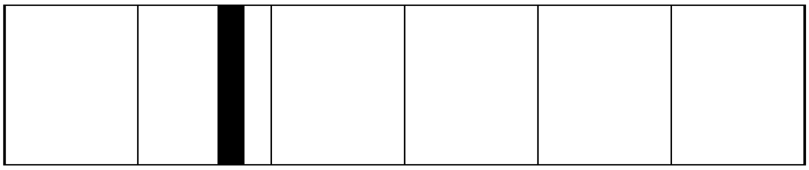
すると, これらの中間的な機能として以下の 2 種類の機能が考えられる.

1. 誤りの大きさは分かるが誤りの位置は分からない
2. 誤りの位置は分かるが誤りの大きさは分からない

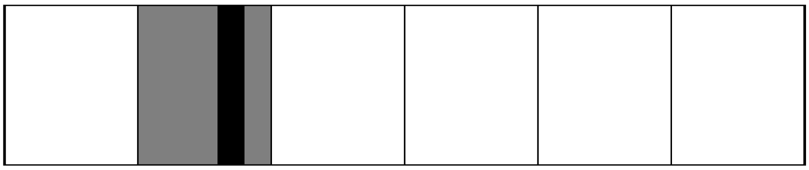
ここで, 上記の 機能 1 では 受信語による情報以外の情報 (例えば, 読み込み, 受信時の信号の状態等) を得ないと誤りの大きさに関する情報を利用できない. これらの情報がない場合, この機能は誤り検出機能と一致してしまう.

一方, 上記の機能 2 は次節にあげるように様々な利用方法が考えられるので, 有用な機能であるといえる. この機能を **誤り位置指摘**<u></u>*(Error Location)* と呼ぶ．この誤り位置指摘機能を加えると

- 誤り訂正 (Error Correction)



- 誤り位置指摘 (Error Location)



- 誤り検出 (Error Detection)

図 2.1: 符号の誤り制御機能

誤り制御符号の機能は3種類あることになる．図2.1 にこれらの機能の関係を示す．一般的に, ある誤りを訂正する符号の検査長はその誤りを検出する符号の検査長よりも長くなる. 明らかに, 誤り位置指摘は誤り訂正と誤り検出の中間的な機能であるので，誤り位置指摘符号を構成した場合, その検査長は誤り訂正符号の検査長と誤り検出符号の検査長の中間に位置する．

## 2.3　誤り位置指摘の応用

誤り位置指摘符号を最初に提案した J. K. Wolf と B. Elspas は誤り位置指摘符号を通信へ応用することを提案した [15]．誤り位置指摘符号を利用した通信では, あらかじめ定めた大きさ以内の誤りに対しては, 誤りの位置の概略を知ることができる. そこで, 再送信の際には誤りを含む部分のみを送信すればよいので. 再送信のコストが削減可能である.

誤り位置指摘符号は計算機にも応用可能である．セルフチェッキング回路で構成されたユニットにおいては出力が符号語であるか否かを調べることによってユニットのチェックを行なっている [1]．ここで用いられる符号は通常誤り検出符号であるが，これを誤り位置指摘符号に交換すると回路内のどの部分 (サブユニット) が故障しているかが特定可能であり，故障発生時の修理を迅速に行なうことができる．また，予備のサブユニットを持っているユニットでは故障したサブユニットを予備と切替えることによるシステムの自動修復を行なうことも可能である．

さらに，集積回路のテストにも応用可能である．集積回路のテスト法であるシグネチャ解析では，回路にランダムな入力を与え，その出力をシフトレジスタで圧縮し，その結果を正常な回路の出力を圧縮したものと比較することにより回路のテストを行なう [1]．このシフトレジスタを用いた圧縮は回路の出力を情報部とする巡回符号の検査部を計算する操作に相当する．このときの巡回符号も誤り検出符号として用いられている．この符号を巡回誤り位置指摘符号 [19] に置き換えると回路の故障部分が特定可能である [20]．集積回路内に予備回路を設けてある場合には故障回路を予備の回路と切替えることができる．その結果，この集積回路を正常な回路として使用することができ，集積回路の歩留まりの向上に役立つ．特に回路故障が避けられない WSI (Wafer Scale Integration) においてこの技術は重要な技術になると考えられる．

上に示した応用例は，いずれもこれまで誤り検出符号が用いられていたところへ誤り位置指摘符号を応用することによって性能を向上させることのできる例である．

## 2.4　従来の誤り位置指摘符号

J. K. Wolf と B. Elspas の提案した符号 [15] では符号語は長さ $b$ ビットのバイト $s$ 個に分割される．この誤り位置指摘符号は単一バイトに $e(<b)$ ビット以下の誤りが生じたときにそのバイトを指摘する符号である．この符号を **単一 $b$ ビットバイト中 $e$ ビット誤り位置指摘符号 ($S_{e/b}EL$ 符号)** と呼ぶ．$E_i(E_j)$ を第 $i(j)$ バイトに生じた $e$ ビット以下の誤りの集合とする．このとき，$S_{e/b}EL$ 符号は以下の条件を満足する．

$$e_1\boldsymbol{H}^T \neq e_2\boldsymbol{H}^T \neq \boldsymbol{0} \ \text{ for } \forall e_1 \in E_i, \forall e_2 \in E_j, i \neq j.$$

また，検査ビット長 $R$ の下限は以下の式で表される [15]．

$$R \geq \log_2 \left\{ 1 + s \sum_{i}^{[e/2]} \begin{pmatrix} b \\ i \end{pmatrix} \right\} \tag{2-1}$$

ただし，$[x]$ は $x$ を越えない最大の整数を表す．

一般に，誤り位置指摘符号はパリティ検査行列のテンソル積を用いて構成することが可能である [16]-[18]．以下に行列のテンソル積の定義を示す．

**定義 2.1** [25] 行列 $\boldsymbol{R} = (r_{ij})$ を $a$ 行 $b$ 列の行列とし，行列 $\boldsymbol{S} = (s_{ij})$ を $c$ 行 $d$ 列の行列とする．このとき，$\boldsymbol{R}$ と $\boldsymbol{S}$ のテンソル積 $\boldsymbol{T} = \boldsymbol{R} \otimes \boldsymbol{S}$ は $ac$ 行 $bd$ 列の行列であり，以下のような構造をして

いる．

$$\boldsymbol{T} = \boldsymbol{R} \otimes \boldsymbol{S} = \begin{bmatrix} r_{11}S & \cdots & r_{1b}S \\ \vdots & \ddots & \vdots \\ r_{a1}S & \cdots & r_{ab}S \end{bmatrix}$$

■

$\boldsymbol{H}_D$ を誤り集合 $E_D$ に属す誤りの検出が可能である2元 $(b, b-\rho)$ 符号 $C_D$ のパリティ検査行列とし，$\boldsymbol{H}_C$ を誤り集合 $E_C$ に属す誤りの訂正が可能である GF($2^\rho$) 上の $(s, s-m)$ 符号 $C_D$ のパリティ検査行列とする．このとき，

$$\boldsymbol{H}_L = \boldsymbol{H}_C \otimes \boldsymbol{H}_D \tag{2-2}$$

なる行列 $\boldsymbol{H}_L$ で定義される2元 $(bs, bs-\rho m)$ 符号 $C$ に関して以下の定理が成立する．

**定理 2.1** *[16, 17]* 1) 誤りの生じた全てのバイトにおいてバイト内の誤りが集合 $E_D$ に属し，2) 誤りの生じたバイトの配置が集合 $E_C$ に属す誤りパターンのいずれかと一致したならば，符号 $C$ はこの誤りを検出し，誤りを含むバイトの位置を指摘することができる．■

例えば，$C_D$ として $e$ 重ビット誤り検出符号を，$C_C$ として単一シンボル誤り訂正符号をとると，式 (2-2) の操作で得られる符号 $C$ は $S_{e/b}EL$ 符号になる．

**例 2.1** [15] $b=5, e=4$ とし，$C_D$ を多項式 $g(x) = x^4 + x^3 + x^2 + x + 1$ によって生成される2元 $(5,1)$ 4 ビット誤り検出符号とする．すると，$\rho = 4$ となる．さらに，$C_C$ を $g(x)$ が生成する体上の $(7,5)$ 単一シンボル誤り訂正符号とする．よって，$s=7, m=2$ となる．上記の2符号より得られる符号は以下に示す行列 $\boldsymbol{H}_L$ で定義される $(35,27)$ $S_{4/5}EL$ 符号である．

$$\begin{aligned}
\boldsymbol{H}_D &= \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \end{bmatrix} \\
&= \begin{bmatrix} 1 & & & & 1 \\ & 1 & & & 1 \\ & & 1 & & 1 \\ & & & 1 & 1 \end{bmatrix} \\
\boldsymbol{H}_C &= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \end{bmatrix} \\
\boldsymbol{H}_L &= \boldsymbol{H}_C \otimes \boldsymbol{H}_D
\end{aligned}$$

$$
= \left[\begin{array}{c|c|c|c|c|c|c}
10001 & & 10001 & 10001 & 10001 & 10001 & 10001 \\
01001 & 0 & 01001 & 01001 & 01001 & 01001 & 01001 \\
00101 & & 00101 & 00101 & 00101 & 00101 & 00101 \\
00011 & & 00011 & 00011 & 00011 & 00011 & 00011 \\
\hline
 & 10001 & 10001 & 00011 & 00110 & 01100 & 11000 \\
0 & 01001 & 01001 & 10010 & 00101 & 01010 & 10100 \\
 & 00101 & 00101 & 01010 & 10100 & 01001 & 10010 \\
 & 00011 & 00011 & 00110 & 01100 & 11000 & 10001
\end{array}\right]
$$

ただし, $\alpha$ は既約多項式 $g(x) = x^4 + x^3 + x^2 + x + 1$ の根であり, $\mathrm{GF}(2^4)$ の原始元である. ■

この $S_{e/b}EL$ 符号を $b$ ビット (バイト) 出力素子で構成されたメモリシステムに適用すると, 故障素子の位置を指摘する符号となる.

しかし, 任意の $e$ のに対して $S_{e/b}EL$ 符号が構成可能であるわけではない. $e = b$ のときには 以下の定理に示すように $S_{e/b}EL$ 符号が存在しない.

**定理 2.2** *[21]* 全ての単一バイト誤りを位置指摘可能な符号は単一バイト誤り訂正符号である.

## 2.5　誤り識別符号

杜, 坂庭 は 誤り訂正, 検出符号を全て包含する誤り制御符号として誤り識別符号を提案した [22], [23]. 本節では文献 [22] に提案されている誤り識別符号の概念を紹介する. 同文献では符号を整数環上で定義しているが, 本論文で扱う範囲ではガロア体上で定義しても同様の議論が成り立つので, 本論文では同符号をガロア体上で定義することにする.

**定義 2.2** [22] 誤り識別集合 $E_l$ $(l = 0, 1, 2, \cdots, K-1)$ は互いに素である $\{\mathrm{GF}(q)\}^{b\times n}$ の任意の部分集合として定義される. すなわち,

$$
\left.\begin{array}{c}
E_l \subseteq \{\mathrm{GF}(q)\}^{b\times n} \\
E_l \cap E_m = \phi, l \neq m
\end{array}\right\} l = 0, 1, 2, \cdots, K-1
$$

と定義する. このとき, $(E_0, E_1, E_2, \cdots, E_{K-1})$ を誤り識別集合の組と呼ぶ. ■

誤り識別集合には通常 $\{0\}$ が含まれる. そして, 誤りが生じていないときには $\{0\}$ に属す誤りが生じたと解釈する.

**定義 2.3** [22] 符号 $\mathcal{C}$ が $\displaystyle\bigcup_{l=0}^{K-1} E_l$ に属す任意の誤りについてどの誤り識別集合に属す誤りであるか一意に識別可能であるとき, $\mathcal{C}$ を $(E_0, E_1, \cdots, E_{K-1})$-誤り識別 (Error Discriminating) 符号と呼ぶ. ■

上記の誤り識別符号において, 全ての誤り識別集合の要素数が1のとき, この符号は $E\left(=\bigcup_{l=0}^{K-1}E_l\right)$ 誤り 訂正符号になり, $E_0=\{0\}$, $E_1\neq\phi$ のときは $E_1$ 誤り検出符号になる. すなわち, 誤り識別符号は誤り訂正符号, 検出符号 を特殊形として含んでいる [22].

以下に, 誤り識別符号の必要十分条件を示す. まず, 誤り識別符号の必要十分条件を表すのに用いる誤り差集合の定義を示す.

**定義 2.4** [22] 定義2.2に与えた誤り識別集合の組 $(E_0,E_1,\cdots,E_{K-1})$ に対し誤り差集合 $\Delta$ を以下のように定義する.

$$\Delta(E_0,E_1,\cdots,E_{K-1})=\{\boldsymbol{u}-\boldsymbol{v}|\boldsymbol{u}\in E_i,\boldsymbol{v}\in E_j,0\leq i,j\leq K-1,i\neq j\}$$

■

**定理 2.3** *[22]* 誤り識別集合の組 $(E_0,E_1,\cdots,E_{K-1})$ が与えられたとき, 符号 $\mathcal{C}$ が $(E_0,E_1,\cdots,E_{K-1})$-誤り識別符号であるための必要十分条件は

$$\boldsymbol{x}-\boldsymbol{y}\notin\Delta(E_0,E_1,\cdots,E_{K-1})\text{ for }\forall\boldsymbol{x},\forall\boldsymbol{y}\in\mathcal{C}$$

で与えられる. ■

文献 [22] では誤り識別符号と誤り位置指摘符号の関係について言及していないが, 誤り識別符号は誤り位置指摘符号をも含んでいる. すなわち, $E_0=\{0\}$ であり, 誤りバイト位置の配置が一致する誤りが同一の誤り識別集合に属すように $E_l$ $(1\leq l\leq K-1)$ が 構成されているならば, この符号は $E'\left(=\bigcup_{l=1}^{K-1}E_l\right)$ 誤り位置指摘符号になる. よって, 誤り識別符号は誤り位置指摘符号をも含む広い概念の符号であるといえる.

しかし, 文献 [22] には誤り識別符号の組織的な構成法は示されていないため, 同文献に示されている結果より誤り位置指摘符号の組織的な構成法を導くことはできない. また, 誤り位置指摘符号について言及していないため誤り位置指摘符号と誤り訂正符号, 誤り検出符号との関係についても明らかにはなっていない.

## 2.6　結言

本章では, 誤り位置指摘機能が誤り訂正機能と検出機能の中間に位置する機能であることを示し, 誤り位置指摘符号は通信のみならず計算機システムおよび集積回路にも応用可能であることを示した. 既存の誤り位置指摘符号として Wolf らの提案した符号を紹介した. 彼らの提案したテンソル積による構成法は各種の誤り位置指摘符号の構成に有効な構成法である. さらに本章では 誤

り位置指摘符号に関連した従来の研究として誤り識別符号を紹介した．この符号は誤り識別集合の選択によっては誤り訂正符号, 検出符号のみならず誤り位置指摘符号をも表現可能である．しかし, 現状では具体的な誤り位置指摘符号に対する組織的構成法, および誤り位置指摘と訂正, 検出に関する理論的関係については明らかになっていないことを示した．

# 第3章　新しい誤り位置指摘符号

## 3.1　緒言

本章では複数のバイト出力素子を搭載したメモリカードによって構成されたシステムに適した誤り位置指摘機能を提案する．本提案の位置指摘機能は, メモリカード1個分の出力するバイトの集合をブロックと定義し, ブロック単位で位置指摘を行なう機能である．また, 半導体メモリ素子における誤りの傾向をもとにメモリシステムに適した誤り制御機能を検討し, それらの誤りの扱いを容易にするために新しい誤りを定義する．さらに, ブロック誤り位置指摘符号の一例として単一バイト誤りが生じたときに誤りバイトをブロックの位置を指摘する符号を提案し, その構成法, 復号法を示す．

## 3.2　ブロックの概念の導入

図3.1にメモリカードを用いたメモリシステムの構成を示す．メモリカードとは複数のメモリ素子を搭載した小基板のことであり, その出力ビット数はバイト出力素子の出力ビット数の倍数になる．すなわち, $b(>2)$ ビット出力素子を搭載したメモリカードの出力ビット数は $B=p\times b$ ビットとなる．

上記のメモリカード1個分の出力はメモリの1ワードから見れば $p$ 個のバイトをまとめたものに見える．そこで, このようなバイトの集合を **ブロック** と呼ぶことにする．メモリカードを用いて構成したシステムでは, メモリ素子の故障が生じた際にメモリカード単位で交換するのが自然である．そこで, 誤りの位置指摘もメモリカード単位で行なえば十分であるといえる．単一のメモリ素子故障が1ワードに与える影響は高々1バイトであり, 1ブロック全体に及ぶことはない．したがって, 任意のバイト誤りを位置指摘する符号においてもブロック単位で位置指摘することにすれば, 定理 2.2に示したような誤り位置指摘符号が誤り訂正符号に一致するという不都合は生じない．

ブロック単位で誤り位置指摘を行なう符号の中で最も基本的な機能を持った符号は単一バイト誤りが生じたときにそのバイトを含むブロックを指摘する符号であり, $S_{b/p\times b}EL$ 符号と表すことにする．本章の第3.4節においてこの符号の構成法・復号法について述べる．

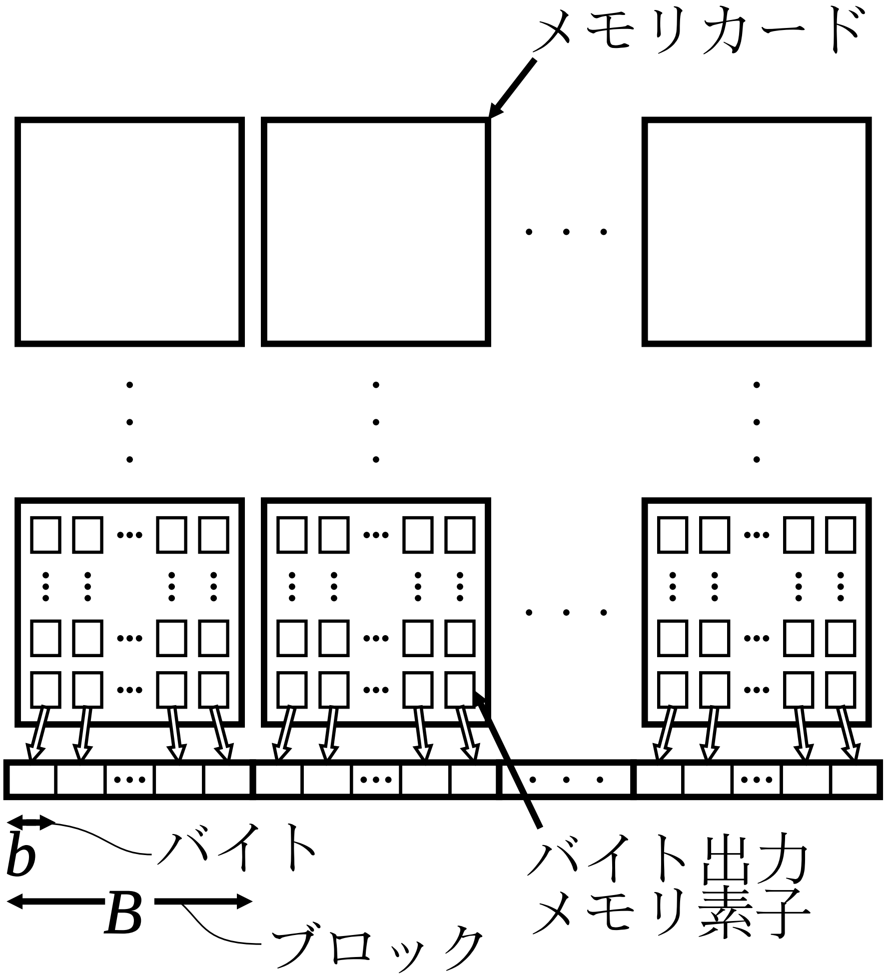



図 3.1: メモリカードを用いたメモリシステムの構成

## 3.3　誤り制御機能の組み合わせ

計算機の半導体メモリシステムにおいて生じる故障の大半は $\alpha$ 線による一時故障であるとされている．これは電荷を持った $\alpha$ 線がメモリチップ上に構成されたメモリセルやセンスアンプ等に衝突することによってその素子が記憶しているデータのビットが反転する, という故障である．この故障は一時故障なので, 故障が生じた素子でも正しいデータを再度書き込めばその後は正常に動作する．また, この故障によって 読み出しデータの1ワードに生じる誤りは $b$ ビット出力素子を用いた場合でも1ビットである．したがって, 単一ビット誤り訂正機能を有する符号を用いれば, 上記故障によって生じたワード中の誤りを訂正可能であり, 訂正したデータを再度書き込むことにより以後の読み出しデータに影響を与えない．以上より, 半導体メモリシステムでは単一ビット誤り訂正機能が有効であるといえる．

上述の通り, 半導体メモリシステムに生じる故障の大半は一時故障である．しかし, 固定故障の起きる確率を完全に無視することはできない．すなわち, 固定故障もある程度考慮する必要がある．バイト出力素子に固定故障が生じたときにはその素子の出力するビット全てが影響を受けるのでバイト誤りとなる可能性がある．よって, 半導体メモリシステムに用いる符号ではビット誤りとバイト誤りの両者を制御する必要がある．

ビット誤りとバイト誤りを統一的に扱うため, 以下に示す誤りを定義する．

**定義 3.1** 符号語の1バイト中に $e$ ビット以下の誤りがあるとき, この誤りを <u>$e/b$ **誤り**</u> と呼ぶ．■

**例 3.1** $S_bEC$ 符号は $S_{b/b}EC$ 符号と表せる．また, $SEC-S_bED$ 符号は $S_{1/b}EC-S_{b/b}ED$ 符号と表せる．■

すなわち $e=1, e=b$ とおくと, $e/b$ 誤りによってそれぞれ ビット誤り, バイト誤りを表現可能である．そこで, ビット誤り, バイト誤りの両者を制御する符号は $e=1, b$ である2種類の $e/b$ 誤りを制御する符号として扱うことができる．

次に, 計算機メモリシステムに適した誤り位置指摘符号を具体的に考える．素子の固定故障についても単一素子故障を考えれば十分であるといえるので, この符号に必要とされる機能は以下の通りである．

1. 単一ビット誤りが生じたときにその誤りを訂正する
2. 単一バイト誤りが生じたときにその誤りの位置を指摘する

上記の 2 で行なう位置指摘としては, 第2.4節に示した Wolf らの符号のようにバイト単位の位置指摘と第3.2節で示したようにブロック単位の位置指摘が考えられる．前者の場合, この符号は単一ビット誤り機能を有するバイト誤り位置指摘符号となり, 後者の場合には単一ビット誤り

機能を有するブロック誤り位置指摘符号となる．これらの符号をそれぞれ $SEC-S_{e/b}EL$ 符号, $SEC-S_{b/p\times b}EL$ と表すことにする．

上記の2符号は実用上重要であると考えられるので, 本論文ではこれらの2符号を提案する．第4章では $SEC-S_{e/b}EL$ 符号について述べ, 第5章では $SEC-S_{b/p\times b}EL$ 符号について述べる．

## 3.4　ブロックを指摘する符号の例

本節ではブロック位置指摘符号として最も基本的な機能を有する符号 ($S_{b/p\times b}EL$ 符号) の構成法および復号法について述べる．本符号は単一バイト誤りが生じた際にそのバイトを含むブロックの位置を指摘する符号である．単一バイト誤り訂正符号に対する新しい並列復号法を提案し, これを用いた $S_{b/p\times b}EL$ 符号の復号法を示している．

### 3.4.1　符号構成法

$S_{b/p\times b}EL$ 符号は単一バイト誤り訂正符号 ($S_bEC$ 符号) をもとにして容易に構成できる．構成法を以下の定理に示す．

**定理 3.1** *[26]* 以下に示す行列 $\boldsymbol{H}'$ を $S_bEC$ 符号のパリティ検査行列とする．

$$\boldsymbol{H}' = \left[\ \boldsymbol{H}_0 \,\middle|\, \boldsymbol{H}_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}_{n'-1}\ \right]$$

ただし，$n'$ はこの符号の符号バイト長とし，$\boldsymbol{H}_i$ を第 $i$ バイト目に対応する $\boldsymbol{H}'$ の部分行列とする．このとき，以下の行列 $\boldsymbol{H}$ をパリティ検査行列とする符号は $S_{b/p\times b}EL$ 符号となる．

$$\boldsymbol{H} = \left[\ \boldsymbol{H}_0 \cdots \boldsymbol{H}_0 \,\middle|\, \boldsymbol{H}_1 \cdots \boldsymbol{H}_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}_{n'-1} \cdots \boldsymbol{H}_{n'-1}\ \right]$$

∎

この定理は自明なので証明を省略する．

Hong と Patel によって提案された最大 $S_bEC$ 符号 [7] をもとにして構成すると，定理 3.1 に示した方法で構成した $S_{b/p\times b}EL$ 符号の符号ビット長 $N$ は以下の式で表される．

$$N = pb \cdot \frac{2^R - 1 - 2^b(2^c - 1)}{2^b - 1} + c \cdot p$$

ただし，$R = br + c\ (0 \leq c < b)$ は $S_{b/p\times b}EL$ 符号の検査ビット長である．

**定理 3.2** 以下に示す行列 $\boldsymbol{H}'$ を $S_{b/p\times b}EC$ 符号のパリティ検査行列とする．

$$\boldsymbol{H}' = \left[\ \boldsymbol{H}_0 \,\middle|\, \boldsymbol{H}_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}_{n'-1}\ \right]$$

ただし，$n'$ はこの符号の符号バイト長とし，$\boldsymbol{H}_i$ を第 $i$ バイト目に対応する $\boldsymbol{H}'$ の部分行列とする．このとき，以下の行列 $\boldsymbol{H}$ をパリティ検査行列とする符号もまた $S_{b/p'\times b}EL$ 符号となる．

$$\boldsymbol{H} = \left[\ \boldsymbol{H}_0 \cdots \boldsymbol{H}_0 \,\middle|\, \boldsymbol{H}_1 \cdots \boldsymbol{H}_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}_{n'-1} \cdots \boldsymbol{H}_{n'-1}\ \right]$$

ただし, $p'$ は $p$ の倍数である. ∎

この定理の証明も自明なので省略する．

図3.2 に $(b, p\times b) = (4, 16), (4, 32), (8, 32)$ に対する $S_{b/p\times b}EL$ 符号の情報ビット長と検査ビット長の関係を示す．

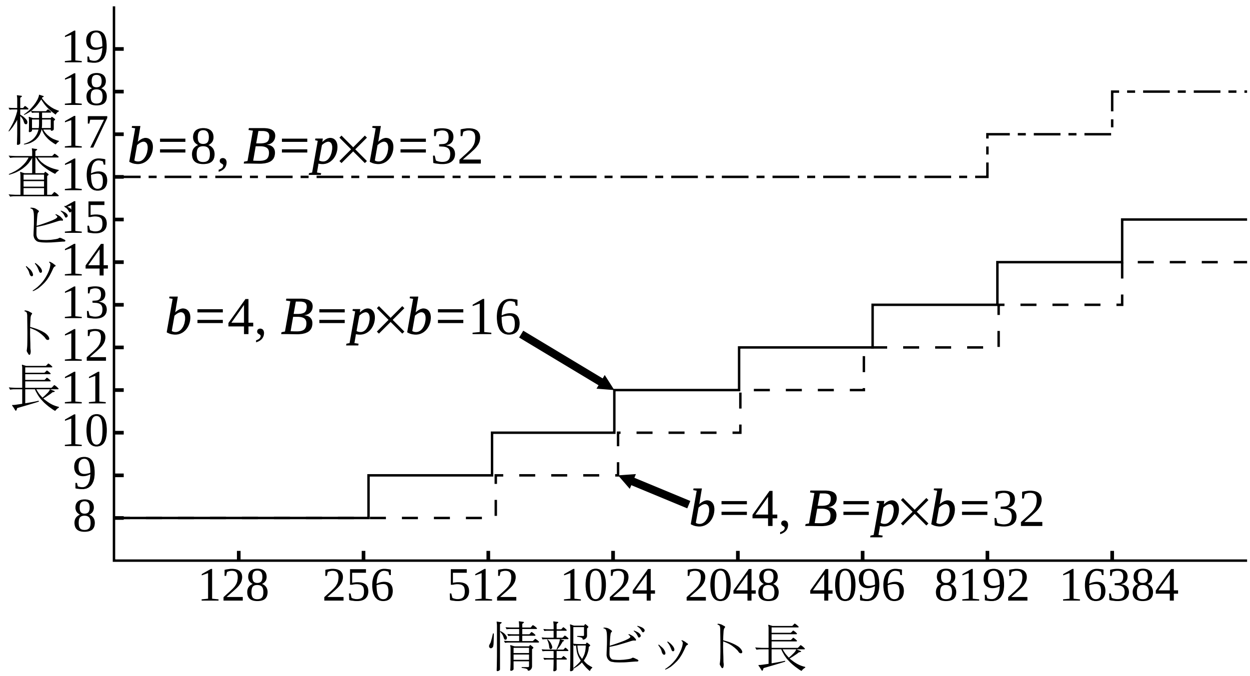



図 3.2: $S_{b/p\times b}EL$ 符号の検査ビット長

### 3.4.2　復号法

$S_{b/p\times b}EL$ 符号の復号は $S_bEC$ 符号の復号回路を利用して実行可能である. すなわち，受信語のシンドロームを計算して $S_bEC$ 符号の復号法を適用すればよい．これは $S_bEC$ 符号において誤りバイトの訂正の過程で誤りのあるバイトが特定されることを利用している．

従来の単一バイト誤り訂正機能を有する符号のパリティ検査行列は, GF$(2^b)$ 上の要素である $b\times b$ の 2 元随伴行列によって構成される [2]. 計算機のメモリシステムでは高速に復号する必要がある

ので並列復号が必須であるが, このような構成の符号ではシンドロームの一部が誤りパターンを表しているか, あるいは随伴行列の逆行列をもとに誤りパターンを得ることができ, 容易に並列復号を行なうことができる. しかし, 従来の並列復号法では誤りパターンの求め方が検査行列の構成に依存するため, 符号構成法を変えると誤りパターンの求め方もそれに合わせて変える必要がある. また, 最近提案された $S_bEC-(S+S_b)ED$ 符号 では随伴行列を用いないため [14], 従来の復号法は適用できない.

任意の単一バイト誤り訂正機能を有する符号に適用可能な並列復号法を以下に示す. この復号法は復号回路量の面でも従来の並列復号法よりも優れている.

バイト長 $b$ ビット, 符号長 $N=n\times b$ ビット, 検査長 $R$ ビットである単一バイト誤り訂正符号のパリティ検査行列を $\boldsymbol{H}$ とし, 符号語の第 $i$ バイトに対応する $\boldsymbol{H}$ の部分行列を $\boldsymbol{H_i}$ とする. すなわち, 検査行列 $\boldsymbol{H}$ は以下に示す構造を有する $R\times N$ 行列である.

$$\boldsymbol{H}=\left[\begin{array}{cccc}\boldsymbol{H}_0 & \boldsymbol{H}_1 & \cdots & \boldsymbol{H}_{n-1}\end{array}\right]$$

この $R\times b$ の行列 $\boldsymbol{H}_i$ に $R\times(R-b)$ の行列 $\boldsymbol{B}_i$ を付加して以下に示す $R\times R$ の正則行列 $\boldsymbol{A}_i$ を構成する.

$$\boldsymbol{A}_i=\left[\begin{array}{cc}\boldsymbol{H}_i & \boldsymbol{B}_i\end{array}\right]$$

さらに, $\boldsymbol{A}_i$ の逆行列 $\boldsymbol{A}_i^{-1}$ を以下のようにおく.

$$\boldsymbol{A}_i^{-1}=\left[\begin{array}{c}\boldsymbol{H}_i^{\dagger}\\ \boldsymbol{B}_i^{\dagger}\end{array}\right]$$

ただし, $\boldsymbol{H}_i^{\dagger},\boldsymbol{B}_i^{\dagger}$ はそれぞれ $b\times R$, $(R-b)\times R$ の行列である. このとき, $\boldsymbol{A}_i^{-1}\boldsymbol{A}_i=I$ より以下の式が成立する.

$$\begin{aligned}\boldsymbol{H}_i^{\dagger}\boldsymbol{H}_i &= \boldsymbol{I}_{b\times b}, & (3\text{-}1)\\ \boldsymbol{B}_i^{\dagger}\boldsymbol{H}_i &= \boldsymbol{O}_{(R-b)\times b}, & (3\text{-}2)\\ \boldsymbol{H}_i^{\dagger}\boldsymbol{B}_i &= \boldsymbol{O}_{b\times(R-b)}, &\\ \boldsymbol{B}_i^{\dagger}\boldsymbol{B}_i &= \boldsymbol{I}_{(R-b)\times(R-b)} &\end{aligned}$$

また, これらの行列に関して以下の 2 補題が成立する.

**補題 3.1** 長さ $b$ ビットの 2 元ベクトル $\boldsymbol{e},\boldsymbol{e}'$ において, $\boldsymbol{e}\neq\boldsymbol{o},\boldsymbol{s}=\boldsymbol{e}\boldsymbol{H}_i^T$ が成立するとき, $\boldsymbol{s}(\boldsymbol{H}_j^{\dagger})^T=\boldsymbol{e}',\boldsymbol{s}(\boldsymbol{B}_j^{\dagger})^T=\boldsymbol{o}$ が成立するための必要十分条件は $i=j,\boldsymbol{e}=\boldsymbol{e}'$ である.

**(証明)**

関係 $\boldsymbol{s}(\boldsymbol{H}_j^{\dagger})^T=\boldsymbol{e}',\boldsymbol{s}(\boldsymbol{B}_j^{\dagger})^T=\boldsymbol{o}$ が成立するとき, $\boldsymbol{s}\left[\begin{array}{cc}(\boldsymbol{H}_j^{\dagger})^T & (\boldsymbol{B}_j^{\dagger})^T\end{array}\right]=\left[\begin{array}{cc}\boldsymbol{e}' & \boldsymbol{o}\end{array}\right]$ より以下の関係が成立する.

$$\boldsymbol{s}(\boldsymbol{A}_j^{-1})^T=\left[\begin{array}{cc}\boldsymbol{e}' & \boldsymbol{o}\end{array}\right]$$

上式の両辺に右側から $\boldsymbol{A}_j^T$ をかけると $(\boldsymbol{A}_j^{-1})^T\boldsymbol{A}_j^T = (\boldsymbol{A}_j\boldsymbol{A}_j^{-1})^T = \boldsymbol{I}$ より以下の関係を得る.

$$\begin{aligned}\boldsymbol{s} &= \begin{bmatrix} \boldsymbol{e}' & \boldsymbol{o} \end{bmatrix} \boldsymbol{A}_j^T \\ &= \begin{bmatrix} \boldsymbol{e}' & \boldsymbol{o} \end{bmatrix} \begin{bmatrix} \boldsymbol{H}_j^T \\ \boldsymbol{B}_j^T \end{bmatrix} \\ &= \boldsymbol{e}'\boldsymbol{H}_j^T\end{aligned}$$

ここで, $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H}_i^T$ より

$$\boldsymbol{e}\boldsymbol{H}_i^T = \boldsymbol{e}'\boldsymbol{H}_j^T$$

が成立する. 上式の左辺は第 $i$ バイトに誤りパターン $\boldsymbol{e}$ の誤りが生じたときのシンドロームであり, 右辺は第 $j$ バイトに誤りパターン $\boldsymbol{e}'$ の誤りが生じたときのシンドロームである. この符号は単一バイト誤り訂正符号であるので, 上式より $i = j, \boldsymbol{e} = \boldsymbol{e}'$ が成立する.

逆が成立するのは明らかである. (Q.E.D.)

**補題 3.2** 大きさ $b$ ビットの任意の 2 元ベクトル $\boldsymbol{e}$ および $0 \leq i \leq n-1$ を満たす任意の自然数 $i$ に対して $\boldsymbol{s} \neq \boldsymbol{e}\boldsymbol{H}_i^T$ が成立するとき, $0 \leq j \leq n-1$ を満たす任意の自然数 $j$ について $\boldsymbol{s}(\boldsymbol{B}_j^\dagger)^T \neq \boldsymbol{o}$ が成立する.

**(証明)**

ある自然数 $j$ について $\boldsymbol{s}(\boldsymbol{B}_j^\dagger)^T = \boldsymbol{o}$ が成立すると仮定する. このとき, $\boldsymbol{s}(\boldsymbol{H}_j^\dagger)^T = \boldsymbol{e}'$ とおくと補題 3.1 の証明と同様にして以下の式を得る.

$$\boldsymbol{s}(\boldsymbol{A}_j^{-1})^T = \begin{bmatrix} \boldsymbol{e}' & \boldsymbol{o} \end{bmatrix}$$

上式の両辺に右側から $\boldsymbol{A}_j^T$ をかけると補題 3.1 の証明と同様にして以下の式を得る.

$$\boldsymbol{s} = \boldsymbol{e}'\boldsymbol{H}_j^T$$

上式は任意の $\boldsymbol{e}, i$ について $\boldsymbol{s} \neq \boldsymbol{e}\boldsymbol{H}_i^T$ が成立するという仮定と矛盾する. ゆえに, $\boldsymbol{s}(\boldsymbol{B}_j^\dagger)^T \neq \boldsymbol{o}$ が成立する. (Q.E.D.)

上記の 2 補題より以下の定理を得る.

**定理 3.3** 単一バイト誤り訂正機能を有する任意の符号において, $\boldsymbol{s}$ をシンドロームとするとき $\boldsymbol{s}(\boldsymbol{H}_i^\dagger)^T = \boldsymbol{e}$ かつ $\boldsymbol{s}(\boldsymbol{B}_i^\dagger)^T\boldsymbol{s} = \boldsymbol{o}$ が成立するのは第 $i$ バイト目に誤りパターン$\boldsymbol{e}$の誤りが生起したときであり, かつそのときに限る.

**(証明)**

補題3.1はシンドローム$\boldsymbol{s}$に対して$\boldsymbol{s}(\boldsymbol{H}_i^{\dagger})^T, \boldsymbol{s}(\boldsymbol{B}_i^{\dagger})^T$を各バイトにおいて計算することにより誤りバイトの位置と誤りパターンを正しく導出できることを示している．また，単一バイト誤り以外の誤りのシンドロームがどの単一バイト誤りによるシンドロームと一致しないときにその誤りを単一バイト誤りとして誤訂正しないことは補題3.2より明らかである．(Q.E.D.)

上記定理をもとにした復号法を以下に示す．

**アルゴリズム 3.1** 単一バイト誤り訂正の復号アルゴリズム

**Step 1:** シンドローム$\boldsymbol{s}$が零ベクトルのとき，誤りなし．

**Step 2:** $\boldsymbol{s}$が零ベクトルでないとき，各バイトにおいて$\boldsymbol{s}(\boldsymbol{B}_i^{\dagger})^T$を計算．これが零ベクトルならば，誤りは第$i$バイトに生じ，誤りパターンは$\boldsymbol{s}(\boldsymbol{H}_i^{\dagger})^T$.

**Step 3:** $\boldsymbol{s}$が零ベクトルでなく，かついかなるバイトにおいても$\boldsymbol{s}(\boldsymbol{B}_i^{\dagger})^T \neq \boldsymbol{o}$であるとき，訂正不可能な誤りが生じたとみなして誤りの検出のみ実行．

■

上記アルゴリズムを図3.3に図示する．

**例 3.2** 以下に示す行列は(8, 4) $S_2EC$符号の検査行列である．

$$
\begin{aligned}
\boldsymbol{H} &= \left[\begin{array}{c|c|c|c} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \boldsymbol{H}_2 & \boldsymbol{H}_3 \end{array}\right] \\
&= \left[\begin{array}{c|c|c|c} 10 & 10 & 10 & 10 \\ 01 & 01 & 01 & 01 \\ 10 & 01 & 11 & 00 \\ 01 & 11 & 10 & 00 \end{array}\right]
\end{aligned}
$$

上記符号の復号に使用される行列のうち第0バイトに対応する行列を以下に示す．

$$
\begin{aligned}
\boldsymbol{A}_0 &= \left[\begin{array}{c|c} \boldsymbol{H}_0 & \boldsymbol{B}_0 \end{array}\right] = \left[\begin{array}{c|c} 10 & 01 \\ 01 & 00 \\ 10 & 10 \\ 01 & 01 \end{array}\right] \\
\boldsymbol{A}_0^{-1} &= \left[\begin{array}{c} 1101 \\ 0100 \\ \hline 1111 \\ 0101 \end{array}\right] = \left[\begin{array}{c} \boldsymbol{H}_0^{\dagger} \\ \hline \boldsymbol{B}_0^{\dagger} \end{array}\right]
\end{aligned}
$$

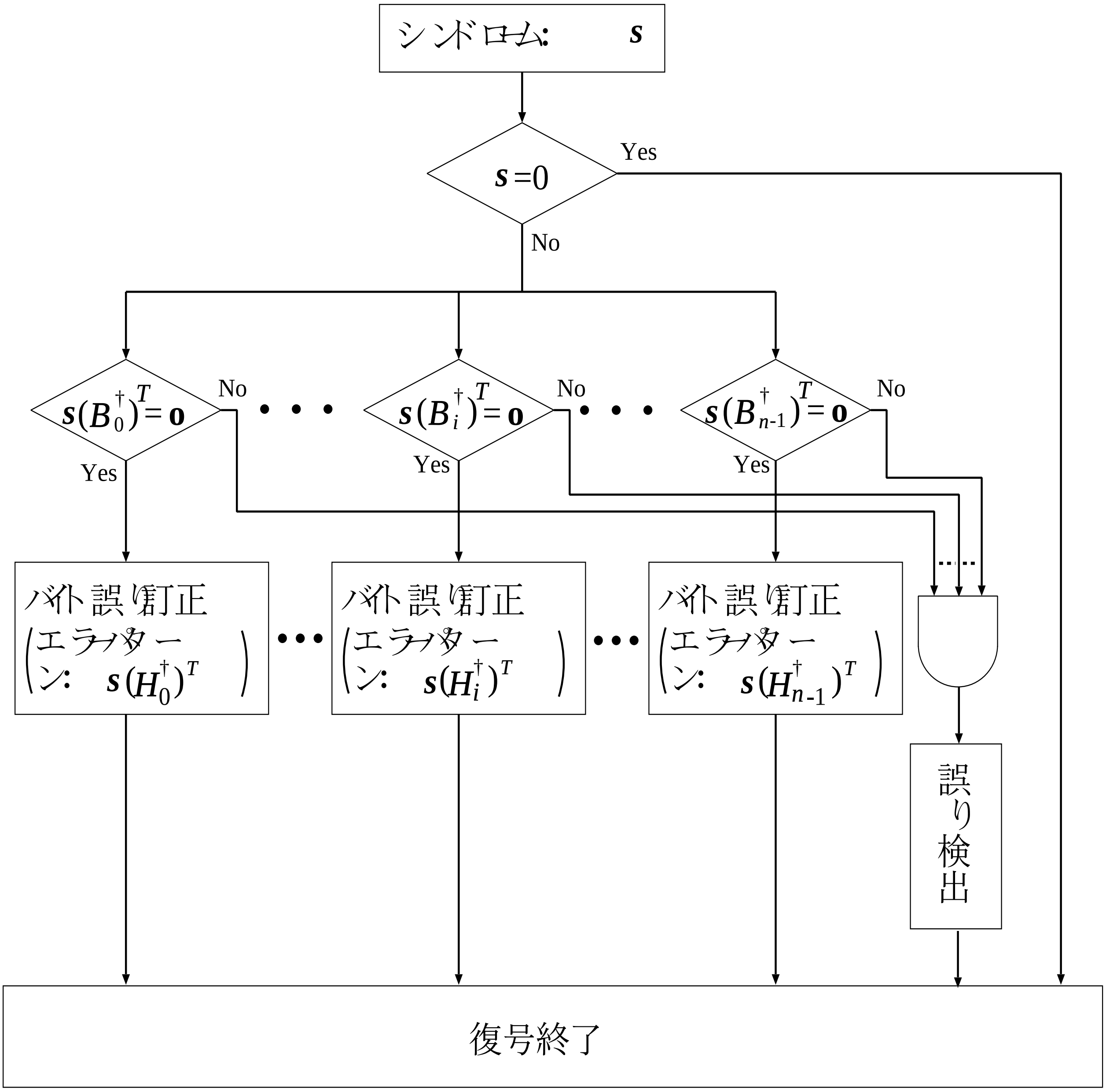



図 3.3: 単一バイト誤り訂正符号の復号アルゴリズム

上記より, 以下に示す行列 $\boldsymbol{H}_0^\dagger, \boldsymbol{B}_0^\dagger$ を得る.

$$\boldsymbol{H}_0^\dagger = \begin{bmatrix} 1101 \\ 0100 \end{bmatrix}$$

$$\boldsymbol{B}_0^\dagger = \begin{bmatrix} 1111 \\ 0101 \end{bmatrix}$$

■

上記復号法において, 逆行列 $\boldsymbol{A}_i^{-1}$ に含まれる "1" の数が少なくなればなるほど復号回路において積を計算するのに用いられる EX-OR ゲートの数は少ない. そこで, 与えられた部分行列 $\boldsymbol{H}_i$ に対する "1" の数が最も少ない $\boldsymbol{A}_i^{-1}$ を **最適な $\boldsymbol{A}_i^{-1}$** と呼ぶこととする.

逆行列 $\boldsymbol{A}_i^{-1}$ は与えられた部分行列 $\boldsymbol{H}_i$ に行列 $\boldsymbol{B}_i$ を付加して得られる正則行列 $\boldsymbol{A}_i$ より求められるが, 式 (3-1), (3-2) を満たす $\boldsymbol{H}_i^\dagger$, $\boldsymbol{B}_i^\dagger$ を求めれば $\boldsymbol{B}_i$ を定めることなく $\boldsymbol{A}_i^{-1}$ を求めることができる. さらに, $\boldsymbol{A}_i^{-1}$ を最適化する際には $\boldsymbol{H}_i^\dagger, \boldsymbol{B}_i^\dagger$ をそれぞれ独立に最適化することが可能である.

**例 3.3** 例 3.2 に示した行列 $\boldsymbol{H}_0$ より最適な $\boldsymbol{H}_i^\dagger, \boldsymbol{B}_i^\dagger$ を得る. 最適な $\boldsymbol{H}_0^\dagger, \boldsymbol{B}_0^\dagger$ の例を以下に示す.

$$\boldsymbol{H}_0^\dagger = \begin{bmatrix} 1000 \\ 0100 \end{bmatrix}$$

$$\boldsymbol{B}_0^\dagger = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$$

■

上記アルゴリズムに基づく復号法において, 行列 $\boldsymbol{H}_i$ はランクが $b$ であればよく, 本復号法は単一バイト誤り訂正機能を有する全ての符号に適用可能である. また, 上記の復号アルゴリズムでは従来の単一バイト誤り訂正符号の並列復号法と同様の復号を実施しているので, 付加する行列 $\boldsymbol{B}_i$ を選ぶことによって本提案の復号回路を従来の回路と一致させることができる. さらに, 本提案の復号法では逆行列 $\boldsymbol{A}_i^{-1}$ を最適化して復号回路のゲート数を削減することが可能である. ゆえに, GF$(2^b)$ 上の要素を用いて構成した単一バイト誤り訂正符号において, アルゴリズムに示した復号法による回路のゲート数は従来の並列復号回路のゲート数を上回ることはない.

さらに, 本復号法は $t$ バイト誤り訂正符号における並列 $t$ バイト誤り訂正にも応用可能である.

## 3.5　結言

本章では, メモリシステムに適する符号としてメモリカード単位での位置指摘機能, 半導体メモリシステムに適した誤り制御機能を提案した. また, メモリカード位置を指摘する符号を具体的に提案した. 本章によって得られた結果は以下の通りである.

(1) バイト出力のメモリ素子を搭載したメモリカードを用いたメモリシステムに適した誤り位置指摘機能として，ブロック単位で位置指摘を行なう新しい誤り位置指摘機能を提案した．ブロックは複数のバイトの集合であり，メモリカード1個分の出力に対応する．

(2) 半導体メモリシステムに生じる誤りは一時故障による単一ビット誤りが大半であるが，固定故障によるバイト誤りも無視できないことを示し，ビット誤りとバイト誤りの両者を制御する必要があることを示した．これらの誤りを統一的に扱うことのできる誤りとして大きさ $b$ ビットのバイト中における $e$ $(1 \leq e \leq b)$ ビット以下の誤りを $e/b$ 誤りと定義した．この誤りは $e = 1, b$ とするとそれぞれビット誤り，バイト誤りを表すことができるので，ビット誤りとバイト誤りの両者を制御する符号を2種類の $e/b$ 誤りを制御する符号として表現できる．

(3) 単一バイト誤りが生じた際にそのバイトを含むブロックの位置を指摘する機能を有する誤りブロック位置指摘符号としては最も基本的な機能の符号を提案し，その構成法および復号法を示した．本復号法は単一バイト誤り訂正符号の復号法を利用するものであるが，本章ではこれに利用可能な単一バイト誤り訂正符号の新しい並列復号法として検査行列の1バイト分に対応する部分行列に列ベクトルを付加して正則な正方行列を構成し，その逆行列を利用する方法を提案した．本復号法は $\mathrm{GF}(2^b)$ の要素である $b \times b$ 随伴行列を用いないで検査行列を構成した単一バイト誤り訂正符号にも適用可能な一般的復号法である．さらに，$\mathrm{GF}(2^b)$ の要素を用いて構成した単一バイト誤り訂正符号に対しては従来の並列復号法に比べて復号回路量が少ないという利点もある．

# 第4章　単一ビット誤り訂正機能を有するバイト誤り位置指摘符号

## 4.1　緒言

本章では単一ビット誤り訂正し, 故障バイト素子の位置を指摘する実用的な符号である $SEC-S_{e/b}EL$ 符号について述べている. 符号の必要十分条件, 符号の限界式を示し, 符号構成法及び復号法を提案している. また, 誤り検出率及び復号回路量の観点から本章に示した構成法で得られる符号の評価を行なっている.

## 4.2　準備

以下の定理に $SEC-S_{e/b}EL$ 符号の必要十分条件を示す.

**定理 4.1** 集合 $\boldsymbol{E}_s$ を単一ビット誤りの集合とし, $\boldsymbol{E}_i(\boldsymbol{E}_j)$ を第 $i(j)$ バイトに生じた大きさ 2 ビット以上 $e$ ビット以下の単一バイト誤りの集合とする. ただし, $e<b$ であり, $b$ はバイト長を表す. このとき, 任意の $i \neq j$ に対して $(\boldsymbol{E}_i \cup \boldsymbol{E}_j) \cap \boldsymbol{E}_s = \phi$ が成立する. ただし $\phi$ は空集合である.

検査行列 $\boldsymbol{H}$ で定義される線形符号が $\boldsymbol{E}_s$ に属す全ての誤りを訂正し, $\boldsymbol{E}_i$ $(\boldsymbol{E}_j)$ に属す全ての誤りを位置指摘可能できるのは以下の条件が成立するときであり, そのときに限る.

1. $\boldsymbol{e}_1 \cdot \boldsymbol{H}^T \neq \boldsymbol{e}_2 \cdot \boldsymbol{H}^T \neq 0$ for $\forall \boldsymbol{e}_1, \forall \boldsymbol{e}_2 \in \boldsymbol{E}_s, \boldsymbol{e}_1 \neq \boldsymbol{e}_2$
2. $\boldsymbol{e}_3 \cdot \boldsymbol{H}^T \neq \boldsymbol{e}_4 \cdot \boldsymbol{H}^T \neq 0$ for $\forall \boldsymbol{e}_3 \in \boldsymbol{E}_i,$ and $\forall \boldsymbol{e}_4 \in \boldsymbol{E}_j, i \neq j$
3. $\boldsymbol{e}_1 \cdot \boldsymbol{H}^T \neq \boldsymbol{e}_3 \cdot \boldsymbol{H}^T$ for $\forall \boldsymbol{e}_1 \in \boldsymbol{E}_s,$ and $\forall \boldsymbol{e}_3 \in \boldsymbol{E}_i$

ただし, $\boldsymbol{H}^T$ は $\boldsymbol{H}$ の転置である.

**(証明)**

条件 1,2 がそれぞれ単一ビット誤り訂正と $e$ ビット以下の単一バイト誤り位置指摘のための必要十分条件であることは明らかである. 条件 3 は単一ビット誤りと単一ビット誤りを除く単一バイ

ト誤りを区別するための必要十分条件である. ゆえに, $SEC-S_{e/b}EL$ 符号は上記の 3 条件を全て満たす.

逆に, ある符号が上記の 3 条件を全て満たすとき, 単一ビット誤りと単一ビット誤りを除く単一バイト誤りを区別することが可能である. また, 単一ビット誤りの訂正および単一バイト誤りの位置指摘も可能である. ゆえに, この符号は $SEC-S_{e/b}EL$ 符号である. (Q.E.D.)

**定理 4.2** 線形 $SEC-S_{e/b}EL$ 符号において以下の関係が成立する.

$$2 \leq e \leq b-1$$

**(証明)**

$e=1$ のとき, $SEC-S_{e/b}EL$ 符号が $SEC$ 符号に一致することは明らかである.

明らかに $SEC-S_{e/b}EL$ 符号は $S_{e/b}EL$ 符号であり, 定理 2.2 より $e=b$ のとき $S_{e/b}EL$ 符号は $S_bEC$ 符号と一致するため存在しない. よって, $e=b$ のとき $SEC-S_{e/b}EL$ 符号も存在しない.

以上より, $e=1,b$ のとき $SEC-S_{e/b}EL$ 符号が存在しないので, $SEC-S_{e/b}EL$ 符号が存在するための $e$ の値に関する条件は以下の通りである.

$$2 \leq e \leq b-1$$

(Q.E.D.)

以下に示す 2 定理は $SEC-S_{e/b}EL$ 符号における検査ビット長の下界を表している.

**定理 4.3** 線形 $(N, N-R)$ $SEC-S_{e/b}EL$ 符号において以下の関係が成立する.

$$2^R \geq \begin{cases} 1+\dfrac{N}{b}\displaystyle\sum_{i=1}^{(e+1)/2}\begin{pmatrix} b \\ i \end{pmatrix} & e\text{: 奇数} \\ 1+\dfrac{N}{b}\left\{\displaystyle\sum_{i=1}^{e/2}\begin{pmatrix} b \\ i \end{pmatrix}+\begin{pmatrix} b \\ (e+2)/2 \end{pmatrix}\Big/\left\lfloor\dfrac{2b}{e+2}\right\rfloor\right\} & e\text{: 偶数} \end{cases}$$

**(証明)**

$S_{e/b}EL$ 符号の検査ビット長限界は $e/2$ ビット以下の単一バイト誤りによるシンドロームが互いに異なる必要があることを利用して求めることが可能である [15]. これと同様の考え方に基づいて本定理の証明を行なう.

1. $e$ が奇数のとき:

   あるバイトに生じた $(e-1)/2$ ビット以下の誤りによるシンドロームは互いに異なる必要がある. これが成立しないとシンドロームが零ベクトルである $e-1$ ビット以下の誤りが存

在することになり, 定理 4.1 の条件 2 が成立しない. 条件 2, 3 より あるバイトに生じた $(e-1)/2+1=(e+1)/2$ ビット誤りによるシンドロームはそのバイトに生じた $(e-1)/2$ ビット以下の誤りによるシンドロームと異なる必要がある. これが成立しないと, シンドロームが零ベクトルである $e$ ビット以下の誤りが存在することになり, 符号条件を満足しない. よって, あるバイトに生じた $(e+1)/2$ ビット以下の誤りによるシンドロームは全て互いに異なる必要がある. あるバイトに生じた $(e+1)/2$ ビット以下の誤りによるシンドロームは明らかに他のバイトに生じた $(e+1)/2$ ビット以下の誤りによるシンドロームと異なる. ゆえに, 以下の関係が成立する.

$$2^R \geq 1+\frac{N}{b}\sum_{i=1}^{(e+1)/2}\begin{pmatrix} b \\ i \end{pmatrix}$$

2. $e$ が偶数のとき:

定理 4.1 の条件 2 より, あるバイトに生じた $e/2$ ビット以下の誤りによるシンドロームは互いに異なる. しかし, あるバイトに生じた $(e+2)/2$ ビット誤りによるシンドロームは同じバイトに生じた他の $(e+2)/2$ ビット誤りによるシンドロームと一致することが可能である. ただし, 一致することが可能なのは両者の $(e+2)/2$ ビット誤りにおいて同時に誤りビットとなるビットが存在しないときのみである. よって, 同一のシンドロームを有する $(e+2)/2$ ビット誤りの個数は最大で

$$\left\lfloor b/\left(\frac{e+2}{2}\right)\right\rfloor = \left\lfloor \frac{2b}{e+2}\right\rfloor$$

である. ただし, $\lfloor x \rfloor$ は $x$ を越えない最大の整数を表す. 定理 4.1 の条件 2, 3 より $(e+2)/2$ ビット誤りによるシンドロームは $e/2$ ビット以下の誤りによるシンドロームと異なる. よって, この符号には少なくとも以下に示す個数だけ互いに異なるシンドロームが必要である.

$$\frac{N}{b}\left\{\sum_{i=1}^{e/2}\begin{pmatrix} b \\ i \end{pmatrix} + \begin{pmatrix} b \\ (e+2)/2 \end{pmatrix} \bigg/ \left\lfloor \frac{2b}{e+2}\right\rfloor\right\}$$

ゆえに, 以下に示す関係が成立する.

$$2^R \geq 1+\frac{N}{b}\left\{\sum_{i=1}^{e/2}\begin{pmatrix} b \\ i \end{pmatrix} + \begin{pmatrix} b \\ (e+2)/2 \end{pmatrix} \bigg/ \left\lfloor \frac{2b}{e+2}\right\rfloor\right\}$$

(Q.E.D.)

**定理 4.4** 線形 $(N, N-R)$ $SEC-S_{e/b}EL$ 符号において以下の関係が成立する.

$$R \geq 2e$$

**(証明)**

$SEC-S_{e/b}EL$ 符号のあるバイトから $e$ ビットを選び, それに対応する $e$ 個の列ベクトルを 検査行列 $\boldsymbol{H}$ から選ぶ. そして, 上記バイト以外の 1 バイトにおいても $e$ ビットを選び, それに対応する $e$ 個の列ベクトルを選ぶ. 定理 4.1 の条件 2 より上で選んだ $2e$ 個の列ベクトルは線形独立である. よって, 検査行列のランクは $2e$ 以上である. ゆえに, 検査行列 $\boldsymbol{H}$ の行数すなわち検査ビット長 $R$ は $2e$ 以上である. (Q.E.D.)

次に, 次節で述べる $SEC-S_{e/b}EL$ 符号の構成法において符号パラメータ $e$ の値に制限を与えることになる関係式を以下の補題に示す.

**補題 4.1** 以下の関係を満たす符号パラメータ $d, n$ に対して $(n, n-r, d)$ 2 元線形符号は存在しない.

$$\frac{2}{3}n < d < n$$

**(証明)**

$d = n$ のとき, この符号は 繰り返し符号 (repetition code)[27] となり, 2 個の符号語しか含まない符号になる.

$0 < d \leq \frac{1}{2}n$ のとき, この符号は明らかに 4 個以上の符号語を含むことができる.

次に $\frac{1}{2}n < d < n$ の場合を考える. このとき, 線形 $(n, n-r, d)$ 符号に 3 個以上の符号語が存在すると仮定する. ここで, $\boldsymbol{c}_1, \boldsymbol{c}_2$ をこの線形符号の互いに異なる非零の符号語とする. すると, 以下の条件を満足する $\boldsymbol{c}_1, \boldsymbol{c}_2$ を選択することが可能である.

1. $w_H(\boldsymbol{c}_1) = w_H(\boldsymbol{c}_2) = d$
2. $\boldsymbol{c}_1, \boldsymbol{c}_2$ のいずれにおいても "0" となるようなビット位置が存在しない

ただし, $w_H(\boldsymbol{c})$ は符号語 $\boldsymbol{c}$ のハミング重みを表す. ここで, $\boldsymbol{c}_1, \boldsymbol{c}_2$ のいずれにおいても "1" となるようなビット位置の個数を $f$ とおく. すると, $\boldsymbol{c}_1 + \boldsymbol{c}_2$ のハミング重みは $w_H(\boldsymbol{c}_1 + \boldsymbol{c}_2) = n - f$ と表される. また, $\boldsymbol{c}_1 + \boldsymbol{c}_2$ も符号語であるので以下の関係が成立する.

$$n - f \geq d \tag{4-1}$$

また, $d > \frac{1}{2}n$ が成立するとき, 符号長 $n$ は以下のように表される.

$$n = 2d - f \tag{4-2}$$

式 (4-2) より, $f = 2d - n$ が成立する. これを 式 (4-1) に代入すると以下に示す関係が成立する.

$$\frac{1}{2}n < d \leq \frac{2}{3}n$$

上に示した以外の場合, すなわち $\frac{2}{3}n < d < n$ が成立するとき, $(n, n-r, d)$ 線形符号の符号語数は 2 個以下である．このとき, 2 個の符号語のいずれにおいても “0” であるビットが存在するのでこの符号の符号長は $n$ ビットよりも小さくなる．これは符号長が $n$ ビットであるという仮定に反する．

以上より $(n, n-r, d)$ 2 元線形符号は以下の条件の下では存在しない．

$$\frac{2}{3}n < d < n$$

(Q.E.D.)

## 4.3　符号構成法

定理 2.1 に示したように, 誤り訂正符号の検査行列と誤り検出符号の検査行列のテンソル積をとると誤り位置指摘符号が得られる．これと同様な手法で $SEC - S_{e/b}EL$ が構成可能である．すなわち, 単一バイト誤り訂正符号 ($S_bEC$ 符号) の検査行列と単一ビット誤り訂正・$e$ ビット誤り検出符号 ($SEC - eED$ 符号) の検査行列のテンソル積から $SEC - S_{e/b}EL$ 符号が得られる．

**定理 4.5** 以下に示す行列 $\boldsymbol{H}$ で定義される符号は 符号長 $N = b \times n$ ビットの $SEC - S_{e/b}EL$ 符号である．

$$\begin{aligned} \boldsymbol{H} &= \boldsymbol{H}' \otimes \boldsymbol{H}'' \\ &= \left[ \begin{array}{c|c|c|c} \boldsymbol{H}'_0 & \boldsymbol{H}'_1 & \cdots & \boldsymbol{H}'_{n-1} \end{array} \right] \otimes \boldsymbol{H}'' \\ &= \left[ \begin{array}{c|c|c|c} \boldsymbol{H}'_0 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_1 \cdot \boldsymbol{H}'' & \cdots & \boldsymbol{H}'_{n-1} \cdot \boldsymbol{H}'' \end{array} \right] \\ &= \left[ \begin{array}{c|c|c|c} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \cdots & \boldsymbol{H}_{n-1} \end{array} \right] \end{aligned}$$

ただし, $\otimes$ はテンソル積を表し, $\boldsymbol{H}'$ は 符号長 $n$ バイトの $S_{b'}EC$ 符号の検査行列を表し, $\boldsymbol{H}'_i$ は符号語の第 $i$ バイトに対応する $\boldsymbol{H}'$ の部分行列を表し, $\boldsymbol{H}''$ は $(b, b-b')$ $SEC - eED$ 符号の検査行列を表し, $\boldsymbol{H}_i$ は 符号語の第 $i$ バイトに対応する $\boldsymbol{H}$ の部分行列を表す．

**(証明)**

行列 $\boldsymbol{H}$ の各列は互いに異なるので, 定理 4.1 の条件 1 が成立する．部分行列 $\boldsymbol{H}_i$ は $\boldsymbol{H}'_i$ と $\boldsymbol{H}''$ の積であるので, $i \neq j$ のとき第 $i$ バイトに生じた誤りによるシンドロームは第 $j$ バイトに生じた誤りによるシンドロームと異なる．一般的に, $S_{b'}EC$ 符号の検査行列において全ての部分行列 $\boldsymbol{H}'_i$ は $b' \times b'$ 正則行列を含むので, 全ての $\boldsymbol{H}_i$ は $b' \times b'$ 正則行列と $\boldsymbol{H}''$ の積を含む．よって, $e$ ビット以下の単一バイト誤りによるシンドロームは非零であるので, 定理 4.1 の条件 2 が成立する．さらに, 上記のことより, 任意の単一ビット誤りによるシンドロームは任意の 2 ビット以上 $e$ ビット以下の

単一バイト誤りによるシンドロームと異なり, 定理 4.1 の条件 3 が成立する. ゆえに, 定理に示した行列 $\boldsymbol{H}$ は定理 4.1 の条件を全て満たすので, この行列によって定義される符号は $SEC-S_{e/b}EL$ 符号である. (Q.E.D.)

Hong と Patel の提案した 最大 $S_{b'}EC$ 符号 [7] を定理 4.1 に示す符号構成法に適用すると, $SEC-S_{e/b}EL$ 符号の符号ビット長は以下のようになる.

$$N = b\frac{2^R - 1 - 2^{b'}(2^c - 1)}{2^{b'} - 1} + b'' \tag{4-3}$$

ただし, $R$ は $SEC-S_{e/b}EL$ 符号の検査ビット長を表し, $b''$ は 検査長が $c$ ビット ($c = R \bmod b'$) である $SEC-eED$ 符号の符号ビット長を表す. 例えば, $e = 2$ のときは $b = 2^{b'-1}, b'' = 2^{c-1}$ となる.

**例 4.1** $(36, 30)$ $SEC-S_{2/4}EL$ 符号

$b = 4, e = 2, b' = 3$ のとき, 以下に示す行列 $\boldsymbol{H}', \boldsymbol{H}''$ はそれぞれ $(27, 21)$ $S_3EC$ 符号, $(4, 1)$ $SEC-DED$ 符号の検査行列である.

$$\boldsymbol{H}' = \left[\begin{array}{c|c|c|c|c|c|c|c|c} \boldsymbol{H}'_0 & \boldsymbol{H}'_1 & \boldsymbol{H}'_2 & \boldsymbol{H}'_3 & \boldsymbol{H}'_4 & \boldsymbol{H}'_5 & \boldsymbol{H}'_6 & \boldsymbol{H}'_7 & \boldsymbol{H}'_8 \end{array}\right]$$
$$= \left[\begin{array}{c|c|c|c|c|c|c|c|c} 100 & 000 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 010 & 000 & 010 & 010 & 010 & 010 & 010 & 010 & 010 \\ 001 & 000 & 001 & 001 & 001 & 001 & 001 & 001 & 001 \\ \hline 000 & 100 & 100 & 001 & 010 & 101 & 011 & 110 & 100 \\ 000 & 010 & 010 & 101 & 011 & 111 & 110 & 100 & 001 \\ 000 & 001 & 001 & 010 & 101 & 011 & 111 & 111 & 110 \end{array}\right]$$
$$\boldsymbol{H}'' = \left[\begin{array}{c} 1001 \\ 0101 \\ 0011 \end{array}\right]$$

上に示した 2 符号の検査行列のテンソル積をとると, 以下に示す $(36, 30)$ $SEC-S_{2/4}EL$ 符号の検査行列 $\boldsymbol{H}$ を得る.

$$\begin{aligned} \boldsymbol{H} &= \boldsymbol{H}' \otimes \boldsymbol{H}'' \\ &= \left[\begin{array}{c|c|c|c|c|} \boldsymbol{H}'_0 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_1 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_2 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_3 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_4 \cdot \boldsymbol{H}'' \end{array}\right. \\ &\qquad \left.\begin{array}{|c|c|c|c} \boldsymbol{H}'_5 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_6 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_7 \cdot \boldsymbol{H}'' & \boldsymbol{H}'_8 \cdot \boldsymbol{H}'' \end{array}\right] \\ &= \left[\begin{array}{c|c|c|c|c|c|c|c|c} 1001 & 0000 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 \\ 0101 & 0000 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\ 0011 & 0000 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\ \hline 0000 & 1001 & 1001 & 0011 & 0101 & 1010 & 0110 & 1100 & 1001 \\ 0000 & 0101 & 0101 & 1010 & 0110 & 1111 & 1100 & 1001 & 0011 \\ 0000 & 0011 & 0011 & 0101 & 1010 & 0110 & 1111 & 1111 & 1100 \end{array}\right] \end{aligned}$$

■

図 4.1 に $b = 8, e = 2, 6$ の場合の $SEC - S_{e/b}EL$ 符号の情報ビット長と検査ビット長の関係を示す．また, 定理 4.3, 4.4 によって得られる検査長の下界も同図に示した．さらに, 比較のために $SEC - DED - S_8ED$ 符号 [12] と $S_8EC$ 符号の検査ビット長も示した．同図より, 本提案の符号の検査長は $e$ の値が小さい場合と情報長が大きい場合に下界に近いことが分かる．また, 本提案の $SEC - S_{2/8}EL$ 符号と $SEC$ 符号における検査長との差がほぼ 1 ビットであることも分かる．同図には示さなかったが, 上記の提案符号は $SEC - DED$ 符号とほぼ等しい検査長を有することも分かっている．最大 $S_bEC$ 符号 [7] と効率の良い $SEC - eED$ 符号 (例えば $b < 1000, (e+2) < b/2$ が成立するときの最小距離 $e+2$ の BCH 符号, $e = 2$ が成立するときの $SEC - DED$ 符号, $e = b-2$ が成立するときの繰り返し符号など) を用いて符号を構成すると効率の良い $SEC - S_{e/b}EL$ 符号が得られる．

図 4.2 に (132, 124) $SEC - S_{2/4}EL$ 符号 を短縮して得た (72, 64) $SEC - S_{2/4}EL$ 符号 の例を示す．

本提案の構成法によって得られる $SEC - S_{e/b}EL$ 符号における $e$ の値には制限がある．以下の定理にその制限を示す．

**定理 4.6** $S_bEC$ 符号と $(b, b-b')$ $SEC - eED$ 符号のテンソル積によって得られる $SEC - S_{e/b}EL$ 符号は以下の条件が成立する時のみ存在する．

$$2 \le e \le \frac{2}{3}b - 2, \quad \text{and} \quad e = b - 2$$

**(証明)**

$e = b$ のとき $SEC - S_{e/b}EL$ 符号が $S_bEC$ 符号に一致する ことは定理 2.2 より容易に導くことができるので, このとき $SEC - S_{e/b}EL$ 符号は存在しない．

$e = b - 1$ のとき, $SEC - eED$ 符号の 最小距離は $e + 2 = b + 1$ 以上でなければならないが, このような距離を持つ $SEC - eED$ 符号 は存在しないので, $SEC - S_{e/b}EL$ 符号も存在しない．

補題 4.1 より 符号長 $b$ ビットの $SEC - eED$ 符号は $\frac{2}{3}b < d = e+2 < b$ すなわち $\frac{2}{3}b - 2 < e < b - 2$ が成立するとき存在しない．

以上より, $SEC - S_{e/b}EL$ 符号は下記の条件が成立する時にのみ存在する．

$$2 \le e \le \frac{2}{3}b - 2, \quad \text{and} \quad e = b - 2$$

(Q.E.D.)

上の定理より, 例えば $b = 8$ のときには $e = 4, 5$ に対する $SEC - eED$ 符号が存在しない．それが, 図 4.1 にこれらの値に対応した $SEC - S_{e/b}EL$ 符号の検査長を示していない理由である．

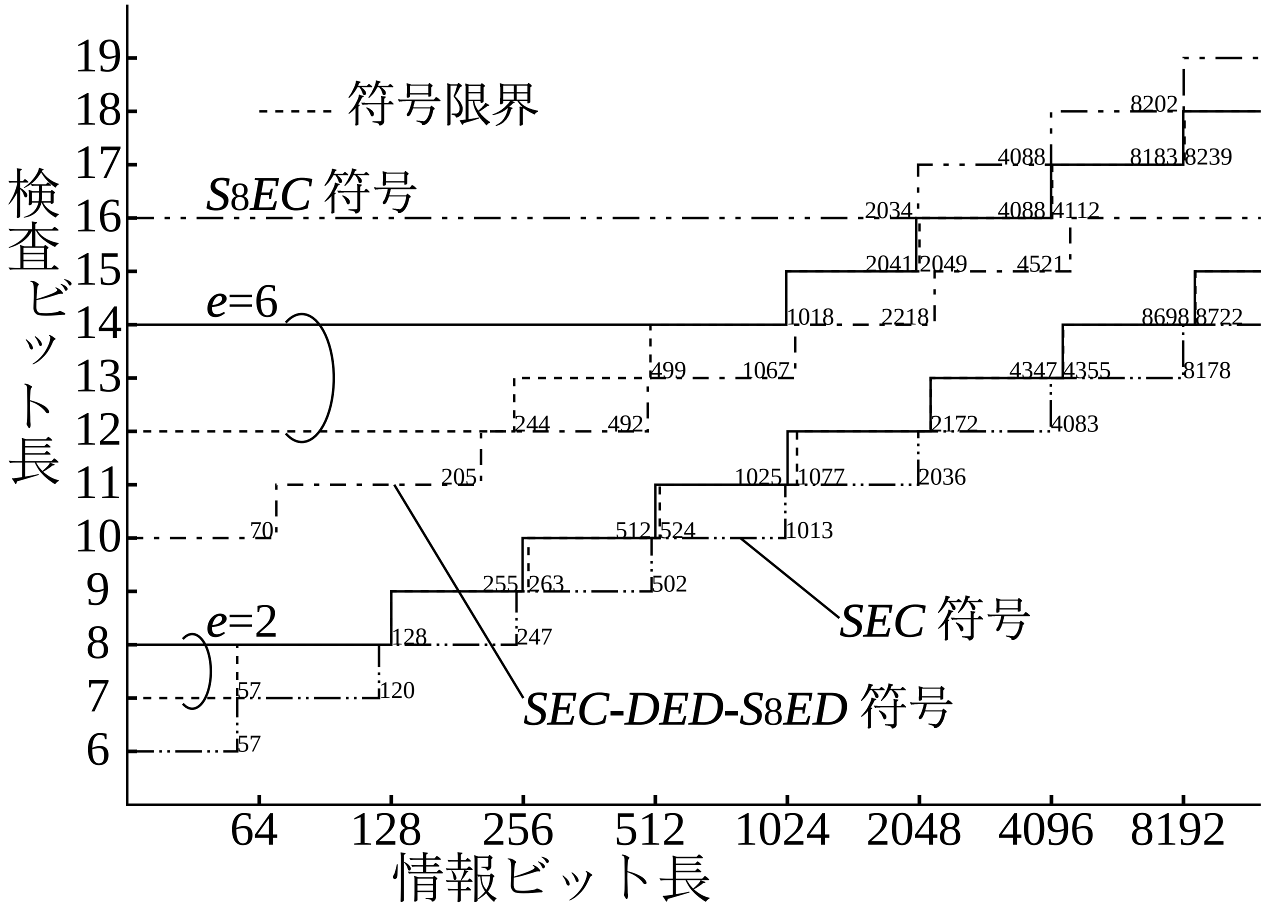



図 4.1: $SEC - S_{e/8}EL$ 符号の検査ビット長

$$
\boldsymbol{H} = \begin{bmatrix}
1001 & 0000 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 & 1001 \\
0101 & 0000 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 & 0101 \\
0011 & 0000 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 & 0011 \\
0000 & 1001 & 1001 & 0000 & 0000 & 0011 & 0110 & 1111 & 1100 & 1001 & 0011 & 0110 & 1100 & 1010 & 0110 & 1111 & 1111 & 1111 \\
0000 & 0101 & 0101 & 1001 & 0000 & 0011 & 0101 & 1001 & 0011 & 0101 & 1010 & 0101 & 1010 & 0110 & 1100 & 1001 & 0000 & 0000 \\
0000 & 0011 & 0011 & 0101 & 1001 & 0011 & 0101 & 1010 & 0101 & 1010 & 0110 & 1100 & 1001 & 0000 & 0000 & 0011 & 0110 & 1111 \\
0000 & 0000 & 0000 & 0011 & 0101 & 1001 & 0011 & 0101 & 1010 & 0101 & 1010 & 0110 & 1100 & 1001 & 0000 & 0000 & 0011 & 0110 \\
0000 & 0000 & 0000 & 0000 & 0011 & 0110 & 1111 & 1100 & 1001 & 0011 & 0110 & 1100 & 1010 & 0110 & 1111 & 1111 & 1111 & 1100
\end{bmatrix}
$$

図 4.2: (72, 64) $SEC - S_{2/4}EL$ 符号の例

## 4.4　復号法

明らかに，$SEC - S_{e/b}EL$ 符号では $SEC$ 符号における単一ビット誤りの訂正と同様の方法で単一ビット誤りの訂正が実行可能である．すなわち, シンドロームを 検査行列の列ベクトルと比較し, 一致した列が存在する場合にはその列に対応するビットを反転することによって単一ビット誤りが訂正可能である.

単一バイト誤りの位置指摘は $S_{b'}EC$ 符号の復号回路の一部を利用して実行可能である．これは $S_{b'}EC$ 符号の復号の際には誤りを含むバイトの位置を必ず求めてから訂正するからである．したがって, 3.4.2 に示した単一バイト誤り訂正符号の復号法を用いて誤り位置の指摘が可能である.

## 4.5　評価

$SEC - S_{e/b}EL$ は 全てのランダム二重ビット誤りおよび二重バイト誤りを検出できるわけではない. また, $e$ ビットを越える単一バイト誤りが常に位置指摘できるわけではない. 上記の誤りが生じると以下に示すような誤った復号を行なうことがある.

1. 誤りの生じていないバイトを誤りバイトとして指摘する (誤指摘)
2. 誤りの生じていないビットを訂正する (誤訂正)
3. シンドロームが零ベクトルになり誤り無しと判断してしまう (未検出)

しかし, 本提案の符号は以下に示すような安全な復号を行なうことがある.

4. 訂正や位置指摘は不可能だが, 誤りを検出する (検出)
5. 全ての誤りが 1 バイトに集中しているときに, そのバイトを指摘する (位置指摘)

図 4.2 に示した (72, 64) $SEC - S_{2/4}EL$ 符号において二重ビット誤り, 二重バイト誤り, 3 ビット以上の単一バイト誤りの生じた受信語を復号した際に上記 5 種類の場合の起きる確率を計算機で求めた結果を表 4.1 に示す. 同表より, この符号ではランダム二重ビット誤り, 二重バイト誤りの両者に対して約 50 % の確率で安全な復号が実行可能であることが分かる.

また, 上記の (72, 64) $SEC - S_{2/4}EL$ 符号 の復号回路量は (72, 64) $SEC - DED$ 符号のそれに比べて 約 47.4 % 増大する.

## 4.6　結言

本章では単一ビット誤り訂正し, 故障バイト素子の位置を指摘する実用性の高い符号である $SEC - S_{e/b}EL$ 符号について述べた. 本章において得られた結果は以下の通りである.

表 4.1: (72, 64) $SEC - S_{2/4}EL$ の復号確率

| | 二重ビット誤り | 二重バイト誤り | 3 ビット以上の単一バイト誤り |
|---|---|---|---|
| 1.　誤指摘 | 34.0 % | 27.0 % | 0 % |
| 2.　誤訂正 | 9.0 % | 29.5 % | 80.0 % |
| 3.　未検出 | 0 % | 0.5 % | 20.0 % |
| 4.　検出 | 52.8 % | 43.0 % | 0 % |
| 5.　位置指摘 | 4.2 % | 0 % | 0 % |

(1) 単一バイト誤り訂正符号の検査行列と単一ビット誤り訂正・$e$ ビット誤り検出符号の検査行列のテンソル積を用いた符号構成法を提案した.

(2) 符号評価の結果, 本構成法によって構成した符号の多くが限界検査ビット長に近い検査ビット長を有することを確認した. 特に, $e$ の値が小さい場合と情報長が大きい場合に検査ビット長が下界に近くなる. また, $e = 2, b = 8$ のとき, すなわち $SEC - S_{2/8}EL$ 符号の検査ビット長は $SEC - DED$ 符号のそれとほぼ一致する.

(3) 本章で提案した構成法を用いて構成した $SEC - S_{2/4}EL$ 符号について符号評価を行なった. 復号回路は $SEC - DED$ 符号の約 1.5 倍の回路量で構成可能であることを示した. ランダム二重ビット誤り, 二重バイト誤りといった誤り制御機能を越えた誤りに対しても約 50 % の確率で位置指摘または検出といった安全な復号が実行可能であることを確認した.

# 第5章　単一ビット誤り訂正機能を有するブロック誤り位置指摘符号

## 5.1　緒言

本章では単一ビット誤りを訂正し, 故障バイト出力素子を含むメモリカード位置を指摘する実用上重要な符号である $SEC-S_{b/p\times b}EL$ 符号について述べる. 符号の必要十分条件, 符号の限界式を示し, 符号構成法及び復号法を提案している. また, 検査ビット長, 誤り検出率及び復号回路量の観点から本章に示した構成法で得られる符号の評価を行なっている.

## 5.2　準備

行列 $\boldsymbol{H}$ を $SEC-S_{b/p\times b}EL$ 符号の検査行列とし, $\boldsymbol{H}_i$ を 符号語の第 $i$ ブロックに対応する $\boldsymbol{H}$ の部分行列とし, $\boldsymbol{H}_{i,j}$ を 符号語の第 $i$ ブロック第 $j$ バイトに対応する $\boldsymbol{H}_i$ の部分行列とする. 以下の定理は $SEC-S_{b/p\times b}EL$ 符号の必要十分条件を表している.

**定理 5.1** 集合 $\boldsymbol{E}_s$ を単一ビット誤りの集合とし, $\boldsymbol{E}_i(\boldsymbol{E}_j)$ を第 $i(j)$ ブロックに生じた 単一ビット誤りを除いた単一バイト誤りの集合とする. このとき, $(\boldsymbol{E}_i\cup\boldsymbol{E}_j)\cap\boldsymbol{E}_s=\phi$ が成立する. ただし, $\phi$ は空集合である.

行列 $\boldsymbol{H}$ で定義される線形符号が $\boldsymbol{E}_s$ に属す全ての誤りを訂正し, $\boldsymbol{E}_i$ $(\boldsymbol{E}_j)$ に属す誤りを全て位置指摘できるのは以下の条件が成立するときであり, かつそのときに限る.

1. $\boldsymbol{e}_1\boldsymbol{H}^T\neq\boldsymbol{e}_2\boldsymbol{H}^T\neq 0$ for $\forall\boldsymbol{e}_1,\forall\boldsymbol{e}_2\in\boldsymbol{E}_s,\boldsymbol{e}_1\neq\boldsymbol{e}_2$
2. $\boldsymbol{e}_3\boldsymbol{H}^T\neq\boldsymbol{e}_4\boldsymbol{H}^T\neq 0$ for $\forall\boldsymbol{e}_3\in\boldsymbol{E}_i,\forall\boldsymbol{e}_4\in\boldsymbol{E}_j,i\neq j$
3. $\boldsymbol{e}_1\boldsymbol{H}^T\neq\boldsymbol{e}_3\boldsymbol{H}^T$ for $\forall\boldsymbol{e}_1\in\boldsymbol{E}_s,\forall\boldsymbol{e}_3\in\boldsymbol{E}_i$ ■

**(証明)**

明らかに上の条件 1, 2 はそれぞれ単一ビット誤り訂正と単一バイト誤り位置指摘のための必要十分条件である. 条件 3 は単一ビット誤りと単一ビット誤りを除く単一バイト誤りを区別するた

めの必要十分条件である．ゆえに, 与えられた符号が $SEC-S_{b/p\times b}EL$ 符号ならば上記 3 条件が成立する．

逆に, 上記 3 条件が全て成立しているときは, 条件 3 より生じた誤りが単一ビット誤りであるか, (単一ビット誤りを除く) 単一バイト誤りであるか区別可能である．そこで, 条件 1, 2 によって誤りの訂正または位置指摘が実行可能である．ゆえに, 上記 3 条件を満たす線形符号は $SEC-S_{b/p\times b}EL$ 符号である． (Q.E.D.)

**定理 5.2** 線形 $(N, N-R)$ $SEC-S_{b/p\times b}EL$ 符号において以下の関係が成立する．

$$R \geq 2b$$

**(証明)**

パリティ検査行列の異なる 2 ブロックからそれぞれ 1 バイトに対応する $b$ 個の列ベクトルを取り出す．すると定理 5.1 よりこれらの $2b$ 個の列ベクトルは一次独立となる．したがって, パリティ検査行列の列ベクトル空間の次元は $2b$ 以上であるので, 検査行列の行数も $2b$ 以上である．

(Q.E.D.)

**定理 5.3** 線形 $(N, N-R)$ $SEC-S_{b/p\times b}EL$ 符号において以下の関係が成立する．

$$N \leq \frac{pb(2^R-1)}{pb+2^b-b-1} \tag{5-1}$$

**(証明)**

定理 5.1 より, $SEC-S_{b/p\times b}EL$ 符号では単一ビット誤りのシンドロームは互いに異なり, 単一ビット誤りを除く単一バイト誤りのシンドロームは単一ビット誤りのシンドロームと異なる．そこで, 1 ブロックに注目すると, そのブロックに必要な互いに異なるシンドロームの個数は少なくとも $pb+2^b-b-1$ である．ゆえに, 符号語全体で必要な互いに異なるシンドロームの総数は少なくとも $\dfrac{N}{pb}(pb+2^b-b-1)$ である．これより以下の関係を得る．

$$2^R \geq \frac{N}{pb}(pb+2^b-b-1)+1$$

上の式を変形して式 (5-1) を得る． (Q.E.D.)

## 5.3 符号構成法

### 5.3.1 テンソル積を用いた構成法 – 符号 I

以下の定理に $SEC-S_{b/p\times b}EL$ 符号のテンソル積による構成法を示す．本構成法では単一バイト誤り訂正符号 ($S_bEC$ 符号) と単一ビット誤り訂正・単一バイト誤り検出符号 ($SEC-S_bED$ 符号)[2], [10] の検査行列を利用する．

**定理 5.4** 以下に示す行列 $\boldsymbol{H}$ で定義される符号は $SEC-S_{b/p\times b}EL$ 符号である.

$$
\begin{aligned}
\boldsymbol{H} &= \boldsymbol{H}'_{b'} \otimes \boldsymbol{H}''_{b} \\
&= \left[\ \boldsymbol{H}'_0 \,\middle|\, \boldsymbol{H}'_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}'_{(N/B)-1}\ \right] \otimes \boldsymbol{H}''_b \\
&= \left[\ \boldsymbol{H}'_0 \cdot \boldsymbol{H}''_b \,\middle|\, \boldsymbol{H}'_1 \cdot \boldsymbol{H}''_b \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}'_{(N/B)-1} \cdot \boldsymbol{H}''_b\ \right] \\
&= \left[\ \boldsymbol{H}_0 \,\middle|\, \boldsymbol{H}_1 \,\middle|\, \cdots \,\middle|\, \boldsymbol{H}_{(N/B)-1}\ \right]
\end{aligned}
$$

ただし, $\otimes$ は行列のテンソル積を表し, $B=p\times b$ はブロック長を表し, $N$ は $SEC-S_{b/p\times b}EL$ 符号の符号ビット長をを表し, $\boldsymbol{H}'_{b'}$ は $S_{b'}EC$ 符号の検査行列を表し, $\boldsymbol{H}''_b$ は $(B, B-b')$ $SEC-S_bED$ 符号の検査行列を表し, $\boldsymbol{H}'_i$ は 符号語の第 $i$ バイトに対応する $\boldsymbol{H}'_{b'}$ の部分行列である.

**(証明)**

明らかに $\boldsymbol{H}$ の各列は互いに異なるので 定理 5.1 の条件 1 が成立する.

部分行列 $\boldsymbol{H}_i$ は $\boldsymbol{H}'_i$ と $\boldsymbol{H}''_b$ の積であるので, $i \neq j$ のとき第 $i$ ブロックに生じた単一バイト誤りのシンドロームは第 $j$ ブロックに生じた単一バイト誤りのシンドロームと一致しない. よって, 条件 2 が成立する.

一般的に, 部分行列 $\boldsymbol{H}'_i$ のランクは $b'$ であり, $b'\times b'$ の正則行列を部分行列として含むので [2], $\boldsymbol{H}_i$ は この正則行列と $\boldsymbol{H}''_b$ の積である $b'\times b$ 行列を部分行列として含む. よって, 任意の単一ビット誤りのシンドロームは単一ビット誤りを除く単一バイト誤りのシンドロームと一致しない. これと条件 2 より, 定理 5.1 の条件 3 が成立する.

ゆえに, 行列 $\boldsymbol{H}$ で定義された符号は $SEC-S_{b/p\times b}EL$ 符号である. (Q.E.D.)

**例 5.1** $b=4, b'=5$ のとき, 以下の行列 $\boldsymbol{H}'_{b'}$ は $S_5EC$ 符号の検査行列である.

$$
\begin{aligned}
\boldsymbol{H}'_{b'} &= \left[\ \boldsymbol{H}'_0 \middle| \boldsymbol{H}'_1 \middle| \boldsymbol{H}'_2 \middle| \boldsymbol{H}'_3 \middle| \cdots \middle| \boldsymbol{H}'_{32} \right] \\
&= \left[\begin{array}{c|c|c|c|c|c}
\boldsymbol{I}_5 & \boldsymbol{O}_5 & \boldsymbol{I}_5 & \boldsymbol{I}_5 & \cdots & \boldsymbol{I}_5 \\
\boldsymbol{O}_5 & \boldsymbol{I}_5 & \boldsymbol{I}_5 & \boldsymbol{T}_5 & \cdots & \boldsymbol{T}_5^{30}
\end{array}\right]
\end{aligned}
$$

ただし, $\boldsymbol{T}_5$ は GF($2^5$) の原始元であり, $\boldsymbol{O}_5$, $\boldsymbol{I}_5$ は GF($2^5$) のそれぞれ 零元, 単位元である.

$\boldsymbol{H}''_b$ を 検査長 $b'=5$ ビットの $(12,7)$ $SEC-S_4ED$ 符号 [10] の検査行列とする.

上記の 2 個の検査行列を用いると以下に示すような (396, 386) $SEC-S_{4/3\times 4}EL$ 符号の検査行列 $\boldsymbol{H}$ を得る.

$$
\begin{aligned}
\boldsymbol{H} &= \boldsymbol{H}'_{b'} \otimes \boldsymbol{H}''_b \\
&= \left[\begin{array}{c|c|c|c|c|c}
\boldsymbol{I}_5 & \boldsymbol{O}_5 & \boldsymbol{I}_5 & \boldsymbol{I}_5 & \cdots & \boldsymbol{I}_5 \\
\boldsymbol{O}_5 & \boldsymbol{I}_5 & \boldsymbol{I}_5 & \boldsymbol{T}_5 & \cdots & \boldsymbol{T}_5^{30}
\end{array}\right] \otimes \boldsymbol{H}''_b \\
&= \left[\begin{array}{c|c|c|c|c|c}
\boldsymbol{H}''_b & \boldsymbol{O}_5 & \boldsymbol{H}''_b & \boldsymbol{H}''_b & \cdots & \boldsymbol{H}''_b \\
\boldsymbol{O}_5 & \boldsymbol{H}''_b & \boldsymbol{H}''_b & \boldsymbol{T}_5 \cdot \boldsymbol{H}''_b & \cdots & \boldsymbol{T}_5^{30} \cdot \boldsymbol{H}''_b
\end{array}\right]
\end{aligned}
$$

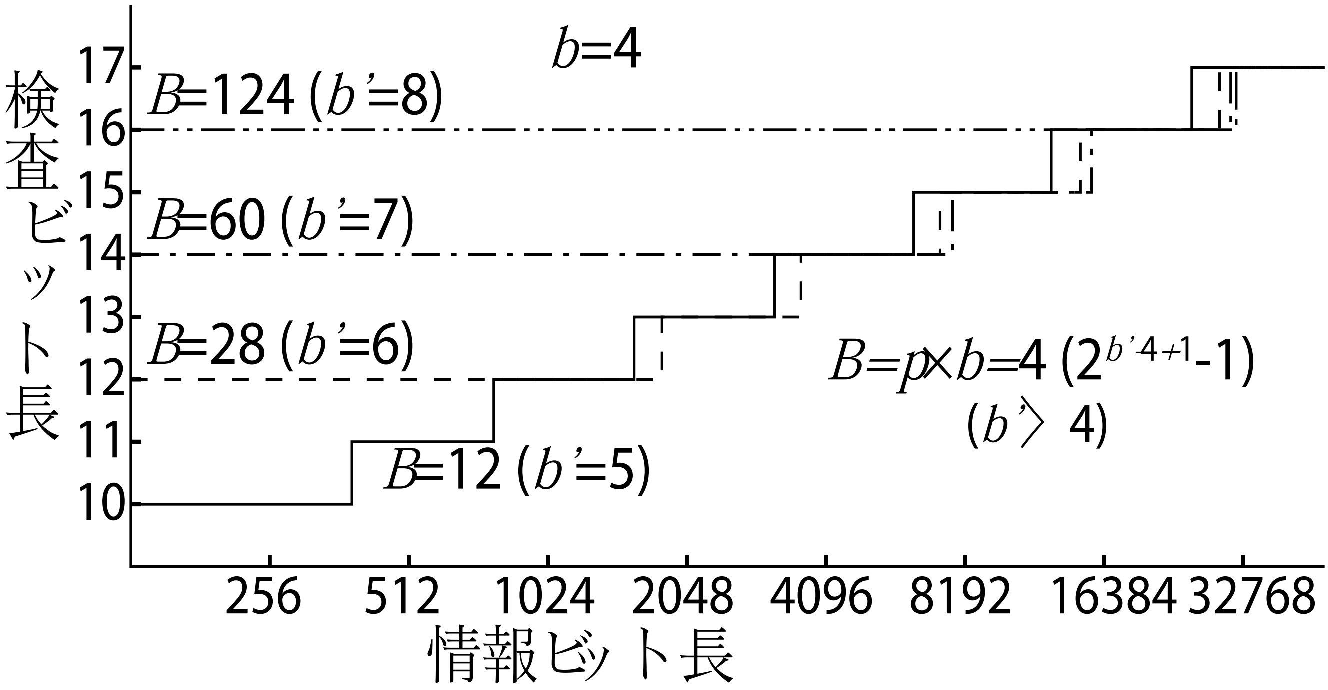



図 5.1: $SEC - S_{4/p\times b}EL$ 符号 I の検査ビット長

■

定理 5.4 に示した構成法で得られる $SEC - S_{b/p\times b}EL$ 符号の符号ビット長を以下に示す. このとき, $S_{b'}EC$ 符号には最大符号 [7] を用いている.

$$N \;=\; b(2^{b'-b+1}-1)\left(\frac{2^R-1-2^{b'}(2^c-1)}{2^{b'}-1}-1\right)+b(2^{b'+c-b+1}-1) \tag{5-2}$$

ただし, $R = b'r + c \ (0 \leq c < b')$ は $SEC - S_{b/p\times b}EL$ 符号の検査ビット長を表している.

図 5.1 に $b = 4$ のときの $SEC - S_{b/p\times b}EL$ 符号の情報ビット長と検査ビット長の関係を示す. この図では, $B = p \times b$ の値として $b'(> b)$ から得られる最大値を使用している.

### 5.3.2　正方行列を用いた構成法 – 符号 II

#### (1) 準備

**定義 5.1** 奇数重み列のみからなる $b \times b$ 正則行列を**奇数重み列正方行列**と呼ぶ. また, 同一の偶数重み列ベクトル $b$ 個からなる $b \times b$ 正方行列を**偶数重み列正方行列**と呼ぶ. ただし, 偶数重み列正方行列は零行列を含む.

明らかに, $b$ 次元の偶数重み列ベクトルは零ベクトルを含めると $2^{b-1}$ 個存在するので, 偶数重み列正方行列は $2^{b-1}$ 個存在する. 次に, 奇数重み列 $b \times b$ 正方行列の一般的な構成法の一例を示す.

**定義 5.2** 以下に示す行列 $\boldsymbol{M}_b$ は $b \times 2^{b-1}$ 奇数重み列行列である.

$$\begin{aligned}\boldsymbol{M}_b &= \begin{bmatrix} \boldsymbol{a}_0 & \boldsymbol{a}_1 & \boldsymbol{a}_2 & \cdots & \boldsymbol{a}_{2^{b-1}-1} \end{bmatrix} \\ &= \begin{bmatrix} p_0 & p_1 & p_2 & \cdots & p_{2^{b-1}-1} \\ \hline | & | & | & & | \\ 0 & \alpha^0 & \alpha & \cdots & \alpha^{2^{b-1}-2} \\ | & | & | & & | \end{bmatrix}_{b \times 2^{b-1}}\end{aligned}$$

ここで, $\alpha$ は $(b-1)$ 次の既約多項式 $g(x)$ の根であり, $\begin{matrix} | \\ \alpha^i \\ | \end{matrix}$ は $x^i \bmod g(x)$ の係数を並べてられる列ベクトルである. また, $p_i \in \{0,1\}$ は $\boldsymbol{a}_i(i = 0, 1, \cdots, 2^{b-1}-1)$ が奇数重みになるように付加する 1 ビットである.

**補題 5.1** 以下に示す $b \times b$ 正方行列 $\boldsymbol{A}_i$ は行列 $\boldsymbol{M}_b$ の連続する $b$ 列より構成されている.

$$\boldsymbol{A}_i = \begin{bmatrix} \boldsymbol{a}_{i_0} & \boldsymbol{a}_{i_1} & \cdots & \boldsymbol{a}_{i_{b-1}} \end{bmatrix}_{b \times b}$$

このとき, $\boldsymbol{A}_i$ は奇数重み正方行列である. ただし, $i_j \equiv i + j \bmod 2^{b-1}, 0 \leq j \leq b-1$ である.

**(証明)**

$b = 2$ のときは自明なので $b \geq 3$ のときの証明を行なう.

1. 行列 $\boldsymbol{A}_i$ が $\boldsymbol{a}_0 = (100 \cdots 0)^T$ を列ベクトルとして含む場合, 行列 $\boldsymbol{A}_i$ から $\boldsymbol{a}_0$ および $\boldsymbol{A}_i$ の 第 1 行を削除すると 正則行列である 随伴行列が得られる. この行列に $\boldsymbol{a}_0$ の下位 $(b-1)$ ビット, すなわち $(b-1)$ 次元の零行列を付加しても, この行列に含まれる列ベクトルの和が零ベクトルになることはない. ゆえに, 行列 $\boldsymbol{A}_i$ は正則行列である.

2. 行列 $\boldsymbol{A}_i$ が $\boldsymbol{a}_0 = (100 \cdots 0)^T$ を列ベクトルとして含まない場合, $\boldsymbol{A}_i$ の第 1 行を削除すると $b$ 個の列ベクトル $\alpha^i, \alpha^{i+1}, \cdots,$ and $\alpha^{i+b-1}$ が得られる. ここで, $\boldsymbol{A}_i$ に含まれる列ベクトルのある線形結合 (全ての列ベクトルの線形結合とは限らない) が零ベクトルになると仮定する. この線形結合には必ず $\alpha^i, \alpha^{i+b-1}$ が含まれるので, この線形結合に関して以下の関係が成立する.

$$\begin{aligned}\alpha^i + \cdots + \alpha^{i+b-1} &= 0 \\ 1 + \cdots + \alpha^{b-1} &= 0 \qquad (5\text{-}3)\end{aligned}$$

ただし, 式 (5-3) の左辺は全ての $\alpha^j (j = 0, 1, \cdots, b-1)$ の和であるとは限らない. 式 (5-3) より $\alpha$ は $GF(2)$ 上の $(b-1)$ 次多項式 (この式を $g(x)$ とおく) の根である. よって, $g(x)$ は $\alpha$

の最小多項式 [2] で割り切れる．一方, $\alpha$ は $GF(2^{b-1})$ の原始元であるので, $\alpha$ の最小多項式の次数は $b-1$ である．ゆえに, $g(x)$ は $\alpha$ の最小多項式であるので既約である．$GF(2)$ 上の既約多項式 $g(x)$ の項数は奇数であるので, 奇数個の $\alpha^j (j=0,1,\cdots,b-1)$ の和のみが零ベクトルになる可能性がある．しかし, $\boldsymbol{A}_i$ の列ベクトルは全て奇数重みなので奇数個の列ベクトルの和は零ベクトルにならない．これは仮定と矛盾するので, $\boldsymbol{A}_i$ は正則である．

以上のことより, 行列 $\boldsymbol{A}_i$ は正則である．　(Q.E.D.)

上の補題より, $2^{b-1}$ 個の奇数重み列 $b \times b$ 正則行列が得られることが分かる．

**例 5.2** $b=4$ のとき行列 $\boldsymbol{M}_4$ は以下のようになる．

$$\boldsymbol{M_4} = \left[\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

行列 $\boldsymbol{M}_4$ において, 第 $i$ 列 $(i=1,2,\cdots,7)$ から上位の 1 ビットを削除して得られる列ベクトルは $x^i \bmod g(x) = x^3+x+1$ の係数ベクトルである．また, $i=0$ のときは この列ベクトルの代わりに 3 次元の零ベクトルを使用する．

この行列 $\boldsymbol{M}_4$ から連続する 4 列を選ぶと, 8 個の奇数重み列 $4 \times 4$ 正方行列 $\boldsymbol{A}_0, \boldsymbol{A}_1, \cdots, \boldsymbol{A}_7$ が得られる．以下に, 一例として $\boldsymbol{A}_5$ を示す．

$$\boldsymbol{A}_5 = \left[\begin{array}{cccc} \boldsymbol{a}_5 & \boldsymbol{a}_6 & \boldsymbol{a}_7 & \boldsymbol{a}_0 \end{array}\right] = \left[\begin{array}{c} 1011 \\ 0110 \\ 1100 \\ 1110 \end{array}\right]$$

■

### (2) 検査行列の構成

奇数重み列正方行列の集合, 偶数重み列正方行列の集合をそれぞれ $\boldsymbol{A}, \boldsymbol{B}$ とおく．以下の補題から符号構成法に関する基本的な考え方が得られる．

**補題 5.2** 以下に示すベクトル $\boldsymbol{Q}, \boldsymbol{Q}'$ はいずれも奇数重み列正方行列, あるいは偶数重み列正方行列を $r$ 個並べて構成した互いに異なる列ベクトルとする．すなわち, $\boldsymbol{Q}_j, \boldsymbol{Q}'_j \in \boldsymbol{A} \cup \boldsymbol{B} (j=0,1,\cdots,r-1)$ である．さらに, $\boldsymbol{Q}, \boldsymbol{Q}'$ はいずれも $\boldsymbol{A}$ の要素が少なくとも 1 個含まれているとする．

$$\boldsymbol{Q} = \left[\begin{array}{c} \boldsymbol{Q}_0 \\ \boldsymbol{Q}_1 \\ \vdots \\ \boldsymbol{Q}_{r-1} \end{array}\right], \quad \boldsymbol{Q}' = \left[\begin{array}{c} \boldsymbol{Q}'_0 \\ \boldsymbol{Q}'_1 \\ \vdots \\ \boldsymbol{Q}'_{r-1} \end{array}\right]$$

ここで, $\boldsymbol{Q}, \boldsymbol{Q}'$ の第 $i$ 番目の要素 $\boldsymbol{Q}_i, \boldsymbol{Q}'_i$ が異なる種類の正方行列であると仮定する. すなわち, $\boldsymbol{Q}_i$ が奇数重み列正方行列であり $\boldsymbol{Q}'_i$ が偶数重み列正方行列である場合, もしくはその逆の場合を仮定する. このとき, $\boldsymbol{Q}, \boldsymbol{Q}'$ を $GF(2)$ の元を要素とする $rb \times b$ 行列と見ると, $\boldsymbol{Q}$ に属す列ベクトルの和と $\boldsymbol{Q}'$ に属す列ベクトルの和が一致することはない.

**(証明)**

行列 $\boldsymbol{Q}, \boldsymbol{Q}'$ に属す2元列ベクトルの和をそれぞれ $\boldsymbol{s}, \boldsymbol{s}'$ とおく. また, $\boldsymbol{s}, \boldsymbol{s}'$ は以下に示すように $GF(2)$ の元を要素とする $b$ 次元ベクトル $r$ 個からなるものとする.

$$\boldsymbol{s} = \begin{bmatrix} \boldsymbol{s}_0 \\ \boldsymbol{s}_1 \\ \vdots \\ \boldsymbol{s}_{r-1} \end{bmatrix}, \quad \boldsymbol{s}' = \begin{bmatrix} \boldsymbol{s}'_0 \\ \boldsymbol{s}'_1 \\ \vdots \\ \boldsymbol{s}'_{r-1} \end{bmatrix}$$

一般性を失うことなく $\boldsymbol{Q}_i, \boldsymbol{Q}'_i$ がそれぞれ奇数重み列正方行列, 偶数重み列正方行列であると仮定することができる. このとき, $\boldsymbol{s}_i = \boldsymbol{s}'_i$ であると仮定すると, $\boldsymbol{s}$ は $\boldsymbol{Q}$ に属す偶数個の列ベクトルの和であり, $\boldsymbol{s}'$ は $\boldsymbol{Q}'$ に属す奇数個の列ベクトルの和になる. ここで仮定より, $\boldsymbol{Q}'$ は少なくとも1個奇数重み列正方行列を含む. そこで, $\boldsymbol{Q}'$ に含まれる奇数重み列正方行列のうちの1個の位置を第 $l$ 番目とし, その正方行列を $\boldsymbol{Q}'_l$ とする. すると, $\boldsymbol{s}'_l$ は奇数重みであるのに対し, $\boldsymbol{s}_l$ は偶数重みである. したがって, 常に $\boldsymbol{s} \neq \boldsymbol{s}'$ が成立する. (Q.E.D.)

符号語の第 $i$ ブロックに対応する検査行列の部分行列 $\boldsymbol{H}_i$ を例えば以下のように表すことにする. すなわち, 第1行に $\boldsymbol{B}$ の要素である偶数重み列正方行列を使用したらその位置に $\mathcal{B}$ を書くことにする.

$$\boldsymbol{H}_i = \begin{bmatrix} \mathcal{B} \\ \mathcal{A} \\ \mathcal{A} \\ \vdots \end{bmatrix}$$

1ビット誤りと (1ビット誤りを除く)1バイト誤りを区別するためには各列は少なくとも1個 $\boldsymbol{A}$ の要素である $b \times b$ 単位行列を含む必要がある. そこで, 最上位の $\mathcal{A}$ を単位行列とする. すると, 上の部分行列 $\boldsymbol{H}_i$ は以下のように表される.

$$\boldsymbol{H}_i = \begin{bmatrix} \mathcal{B} \\ \mathcal{A} \\ \mathcal{A} \\ \vdots \end{bmatrix}$$

$$
=\left[\begin{array}{cccccccccccccc}
\boldsymbol{B}_0 & \boldsymbol{B}_1 & \cdots & \boldsymbol{B}_{2^{b-1}-1} & \boldsymbol{B}_0 & \boldsymbol{B}_1 & \cdots & \boldsymbol{B}_{2^{b-1}-1} & \cdots & \boldsymbol{B}_0 & \boldsymbol{B}_1 & \cdots & \boldsymbol{B}_{2^{b-1}-1} & \cdots \\
\boldsymbol{I}_b & \boldsymbol{I}_b & \cdots & \boldsymbol{I}_b & \boldsymbol{I}_b & \boldsymbol{I}_b & \cdots & \boldsymbol{I}_b & \cdots & \boldsymbol{I}_b & \boldsymbol{I}_b & \cdots & \boldsymbol{I}_b & \cdots \\
\boldsymbol{A}_0 & \boldsymbol{A}_0 & \cdots & \boldsymbol{A}_0 & \boldsymbol{A}_1 & \boldsymbol{A}_1 & \cdots & \boldsymbol{A}_1 & \cdots & \boldsymbol{A}_{2^b-1} & \boldsymbol{A}_{2^b-1} & \cdots & \boldsymbol{A}_{2^{b-1}-1} & \cdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \cdots
\end{array}\right]
$$

ただし, $\boldsymbol{A}_i \in \boldsymbol{A}, \boldsymbol{B}_i \in \boldsymbol{B}(0 \leq i \leq 2^{b-1}-1)$ であり, $\boldsymbol{I}_b = \boldsymbol{A}_0$ は $b \times b$ 単位行列である.

**定理 5.5** 以下に示す行列$\boldsymbol{H}$で定義される符号は 検査長 $R = br$ ビット, 符号長 $N$ ビットの $SEC - S_{b/p\times b}EL$ 符号である.

$$
\boldsymbol{H} = \left[\begin{array}{c|c|c|c|c} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \cdots & \boldsymbol{H}_{2^r-3} & \boldsymbol{H}_{2^r-2} \end{array}\right]
$$

$$
= \left[\begin{array}{c|c|c|c|c}
\mathcal{B} & \mathcal{B} & \cdots & \mathcal{A} & \mathcal{A} \\
\mathcal{B} & \mathcal{B} & \cdots & \mathcal{A} & \mathcal{A} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\mathcal{B} & \mathcal{A} & \cdots & \mathcal{A} & \mathcal{A} \\
\mathcal{A} & \mathcal{B} & \cdots & \mathcal{B} & \mathcal{A}
\end{array}\right]_{br \times N}
$$

ただし, $\mathcal{A}, \mathcal{B}$ はそれぞれ 奇数重み列正方行列, 偶数重み列正方行列からなる行ベクトルであり, 最上位の $\mathcal{A}$ は $b \times b$ 単位行列からなる行である. また, 各部分行列 $\boldsymbol{H}_i$ はそれぞれ異なる $\mathcal{A}, \mathcal{B}$ の組合せからなっており, 少なくとも 1 個 $\mathcal{A}$ を含んでいる.

上に示した符号の符号長は以下の式で表される.

$$
N = (2^r - 1)pb = b(2^r - 1)2^{(b-1)(r-1)} \tag{5-4}
$$

**(証明)**

明らかに, $\boldsymbol{H}$に属す 2 元列ベクトルは互いに異なっているので, 定理 5.1 の条件 1 が成立する. また, $i \neq j$ のとき, $\boldsymbol{H}_i, \boldsymbol{H}_j$ における $\mathcal{A}, \mathcal{B}$ の組合せは異なっているので, 補題 5.2 より定理 5.1 の条件 2 が成立する. また, 全ての列ベクトルには少なくとも 1 個単位行列が含まれるので, 定理 5.1 の条件 3 も成立する. ゆえに, $\boldsymbol{H}$で定義された符号は $SEC - S_{b/p\times b}EL$ 符号である.

最大のブロック数は $r$ 桁の符号なし 2 進数で表現可能な自然数の最大値に一致するので, $2^r - 1$ である. また, ブロック長 $B = p \times b$ の値は $r$ 個の奇数重み列正方行列, 偶数重み列正方行列を並べる並べ方の数によって決まる. 全ての $\boldsymbol{H}_i$ は少なくとも 1 個単位行列からなる行があることに注意してブロック長の最大値を求めると $b(2^{b-1})^{r-1} = b2^{(b-1)(r-1)}$ となる. ゆえに式 (5-4) が成立する. (Q.E.D.)

**例 5.3** $b = 4, R = 8$ のとき, 以下に示す行列 $\boldsymbol{H}$ によって定義される $(96, 88)$ $SEC - S_{4/8\times 4}EL$ 符号が得られる. また, 図 5.2 にこの検査行列を $GF(2)$ の要素で表した結果を示す.

$$
\boldsymbol{H} = \left[\begin{array}{c|c|c} \boldsymbol{H}_0 & \boldsymbol{H}_1 & \boldsymbol{H}_2 \end{array}\right]
$$

$$
\boldsymbol{H} = \left[\begin{array}{cccccccc|cccccccc|cccccccc}
0000 & 1111 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 \\
0000 & 1111 & 1111 & 0000 & 0000 & 0000 & 1111 & 1111 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 \\
0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 0000 & 1111 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 \\
0000 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1111 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 \\
\\
1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 0000 & 1111 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1000 & 0001 & 0010 & 0101 & 1011 & 0111 & 1110 & 1100 \\
0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0000 & 1111 & 1111 & 0000 & 0000 & 0000 & 1111 & 1111 & 0100 & 1001 & 0011 & 0110 & 1101 & 1010 & 0101 & 1010 \\
0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 0000 & 1111 & 0010 & 0101 & 1011 & 0111 & 1110 & 1100 & 1000 & 0001 \\
0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0000 & 0000 & 0000 & 1111 & 1111 & 0000 & 1111 & 1111 & 0001 & 0010 & 0101 & 1011 & 0111 & 1110 & 1100 & 1000
\end{array}\right]
$$

図 5.2: (96,88) $SEC-S_{4/8\times4}EL$ 符号

$$
\begin{aligned}
&= \left[\begin{array}{c|c|c} \mathcal{B} & \mathcal{A} & \mathcal{A} \\ \mathcal{A} & \mathcal{B} & \mathcal{A} \end{array}\right] \\
&= \left[\begin{array}{cccc|cccc|cccc} \boldsymbol{B}_0 & \boldsymbol{B}_1 & \cdots & \boldsymbol{B}_7 & \boldsymbol{I}_4 & \boldsymbol{I}_4 & \cdots & \boldsymbol{I}_4 & \boldsymbol{I}_4 & \boldsymbol{I}_4 & \cdots & \boldsymbol{I}_4 \\ \boldsymbol{I}_4 & \boldsymbol{I}_4 & \cdots & \boldsymbol{I}_4 & \boldsymbol{B}_0 & \boldsymbol{B}_1 & \cdots & \boldsymbol{B}_7 & \boldsymbol{A}_0 & \boldsymbol{A}_1 & \cdots & \boldsymbol{A}_7 \end{array}\right]
\end{aligned}
$$

### (3) 符号長の伸長

定理 5.5 に示した符号構成法は検査ビット長がバイト長 $b$ の倍数のときにしか適用できない．しかし, 以下の定理に示す方法を用いると $R \geq 2b$ を満たす任意の検査長 $R$ に対して構成可能になる．

**定理 5.6** 以下に示す行列 $\boldsymbol{H}$ を $SEC-S_{b/p\times b}EL$ 符号の検査行列とする． そして, その符号長が $b(2^r-1)2^{(b-1)(r-1)}$ ビット，検査長が $br$ ビットであるとする．

$$
\boldsymbol{H} = \left[\boldsymbol{H}_0 \middle| \boldsymbol{H}_1 \middle| \cdots \middle| \boldsymbol{H}_{n-1}\right]
$$

ただし, $\boldsymbol{H}_i (i = 0, 1, \cdots, n-1)$ は $\boldsymbol{H}$ の部分行列である．このとき, 以下に示す行列 $\boldsymbol{H}'$ は検査長 $(br+1)$ ビットの $SEC-S_{b/p\times b}EL$ 符号を表す．

$$
\boldsymbol{H}' = \left[\begin{array}{c|c|c|c|c|c|c} \boldsymbol{H}_0 & \boldsymbol{H}_0 & \boldsymbol{H}_1 & \boldsymbol{H}_1 & \cdots & \boldsymbol{H}_{n-1} & \boldsymbol{H}_{n-1} \\ 0\cdots0 & 1\cdots1 & 0\cdots0 & 1\cdots1 & & 0\cdots0 & 1\cdots1 \end{array}\right]
$$

この操作を行列 $\boldsymbol{H}$ に対して $c$ 回行なうと，検査長 $R = br + c$, $(0 \leq c < b)$ ビットの $SEC-S_{b/p\times b}EL$ 符号を得る. その符号長は以下の式で表される.

$$
N = (2^r-1)B = b(2^r-1)2^{(b-1)(r-1)+c} \tag{5-5}
$$

**(証明)**

行列 $\boldsymbol{H}$ は $SEC-S_{b/p\times b}EL$ 符号の検査行列なので, $\boldsymbol{H}$ に対して 定理 5.1 の条件 1, 2 が成立する．よって, $\boldsymbol{H}'$ に対してもこれらの条件が成立する．また, $\boldsymbol{H}'$ の最下行の構成と $\boldsymbol{H}_i$ には 単位行列のみで構成した行が存在することを考慮すると，各ブロックの前半に属すバイトに生じた

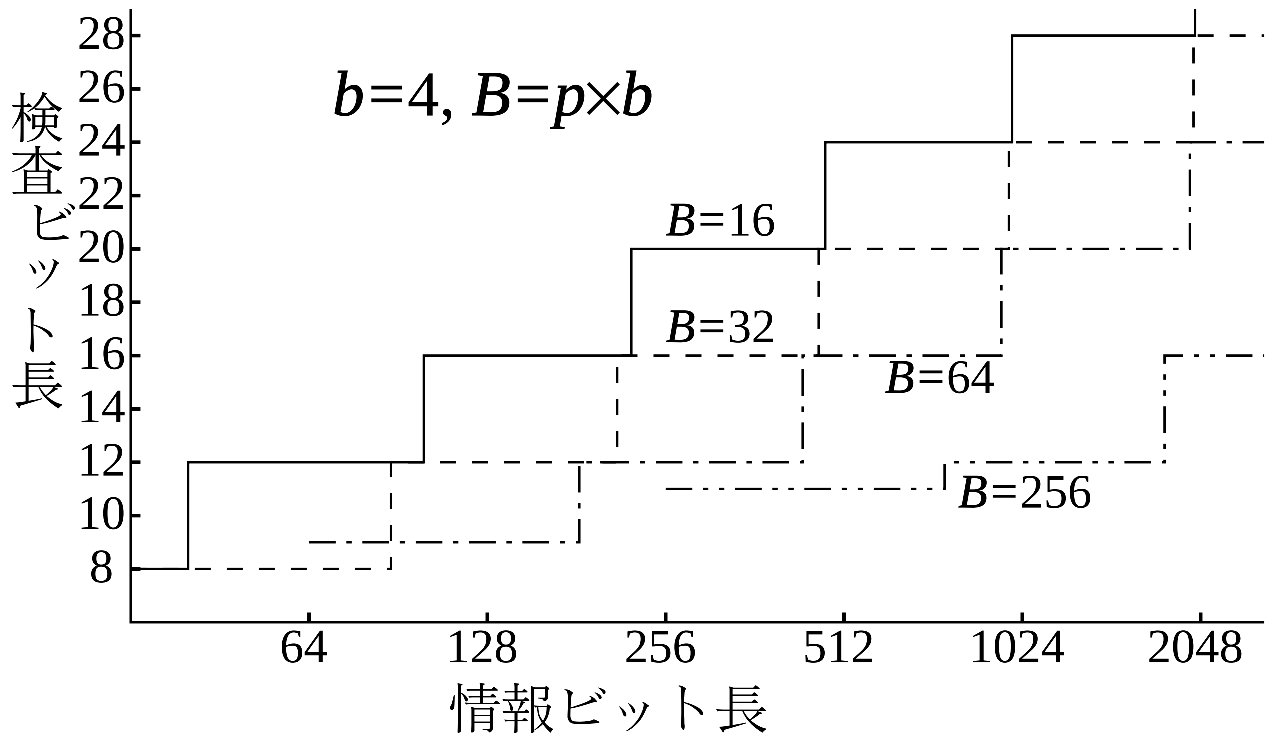



図 5.3: $SEC-S_{4/p\times b}EL$ 符号 II の検査長

1 ビット誤りのシンドロームは同じブロックの後半に属すバイトに生じた 1 バイト誤りのシンドロームと一致しない．各ブロックの後半に属すバイトに生じた 1 ビット誤りのシンドロームが同じブロックの前半に属すバイトに生じた 1 バイト誤りのシンドロームと一致しないことも同様にして確かめられる．よって, 定理 5.1 の条件 3 が成立する．ゆえに, 行列 $\boldsymbol{H}'$ で定義された符号は $SEC-S_{b/p\times b}EL$ 符号である．

上の定理に示した符号伸長法を $c$ 回行なうと符号長は元の符号の $2^c$ 倍になる．ゆえに, 式 (5-5) が成立する．　(Q.E.D.)

図 5.3 に 定理 5.5, 5.6 に示した構成法によって得られる $SEC-S_{b/p\times b}EL$ 符号の情報ビット長を検査ビット長の関係を $b=4$ の場合について示す．

## 5.4　復号法

明らかに，$SEC-S_{b/p\times b}EL$ 符号では単一ビット誤り訂正符号 ($SEC$ 符号) における 1 ビット誤りの訂正と同様の方法で 1 ビット誤りの訂正が実行可能である．すなわち, シンドロームを 検査行列の列ベクトルと比較し, 一致した列が存在する場合にはその列に対応するビットを反転することによって訂正可能である.

1バイト誤りの位置指摘の方法は符号構成法によって異なる．符号Iでは $S_{b'}EC$ 符号の復号回路の一部を利用して位置指摘可能である．これは $S_{b'}EC$ 符号の復号の際には誤りを含むバイトの位置を必ず求めてから訂正するからである．したがって, 3.4.2 に示した単一バイト誤り位置指摘符号の復号法を用いて誤り位置指摘を行なう．

一方, 符号 II では $R = br + c\ (0 \le c < b)$ ビットのシンドロームのうち上位 $br$ ビットを用いて復号する．シンドロームの上位 $br$ ビットを $\boldsymbol{s}$ とおき, これが以下に示すように $r$ 個の $b$ 次元ベクトル $\boldsymbol{s}_0, \boldsymbol{s}_1, \cdots, \boldsymbol{s}_{r-1}$ から構成されているとする．

$$
\begin{aligned}
\boldsymbol{s} &= \left[\begin{array}{cccc} \boldsymbol{s}_0 & \boldsymbol{s}_1 & \cdots & \boldsymbol{s}_{r-1} \end{array}\right] \\
&= \left[\begin{array}{c|c|c|c} s_{0,0}s_{0,1}\cdots s_{0,b-1} & s_{1,0}s_{1,1}\cdots s_{1,b-1} & \cdots & s_{r-1,0}s_{r-1,1}\cdots s_{r-1,b-1} \end{array}\right]
\end{aligned}
$$

$$
s_{l,m} \in \{0,1\}, \quad 0 \le l \le r-1, \quad 0 \le m \le b-1
$$

ここで, 誤りの生じたバイトの位置を第 $i$ ブロック第 $j$ バイトとおき, 誤りパターンとその位置に対応する検査行列の列ベクトルの第 $l$ 番目の要素である $b \times b$ 正方行列との積として得られるシンドロームを $\boldsymbol{s}_l$ とおく．誤りバイトを含むブロックの位置は $\boldsymbol{s}_l$ の重みを調べることによって得られる．そこで, $s_{l,m}$ を用いて定義する2種類の値 $p_l, z_l$ を以下のように定める．

$$
\begin{aligned}
p_l &= \sum_{m=0}^{b-1}{}^{\oplus} s_{l,m} \\
z_l &= \bigvee_{m=0}^{b-1} s_{l,m}
\end{aligned}
$$

ただし, $\sum^{\oplus}$ は2を法とする和である．次に, 上記の $p_l, z_l\ (0 \le l \le r-1)$ を用いて定義する2種類の値 $p', q_l$ を以下のように定義する．

$$
\begin{aligned}
p' &= \bigvee_{l=1}^{r-1} p_l \\
q_l &= p'p_l \vee \bar{p'}z_l
\end{aligned}
$$

ただし, $\bar{p'}$ は $p'$ の否定である．生じた誤りが奇数ビットの誤りのとき, $\boldsymbol{s}_l$ の少なくとも1個は奇数重みになり $p' = 1$ となる．このとき, $\boldsymbol{s}_l$ が奇数重み列正方行列との積であれば奇数重みになり, 偶数重み列正方行列との積であれば偶数重みになる．よって, $p_l$ の値によって, 誤りの生じたバイトに対応する検査行列の列ベクトルの第 $l$ 番目の要素がどちらの種類の正方行列であるか判定可能である．生じた誤りが偶数ビットの誤りのとき, $p' = 0$ となる．このときは, $z_l$ の値によって, 誤りの生じたバイトに対応する検査行列の列ベクトルの第 $l$ 番目の要素がどちらの種類の正方行列であるか判定可能である．変数 $q_l$ を用いると上記の2種類の場合をまとめることができる．すなわち, $q_l = 1$ のときは誤りの生じたバイトに対応する検査行列の列ベクトルの第 $l$ 番目の要素は奇数重み列正方行列であり, $q_l = 0$ のときは偶数重み列正方行列である．以上のことより, 符号語の第 $i$ ブロックが誤りを含むときは変数の系列 $q_0q_1\cdots q_{r-1}$ を $q_0$ を最上位ビットとする2進数と見たと

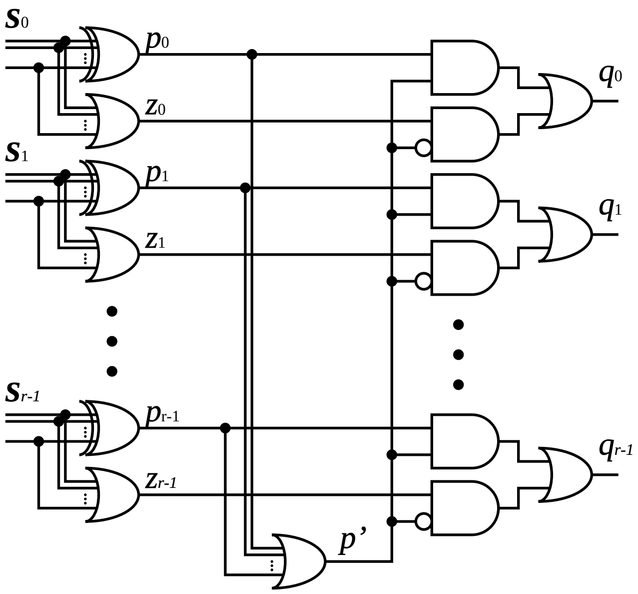



図 5.4: $SEC-S_{b/B}EL$ 符号 II の誤り位置指摘回路

きの値が $i+1$ になる．これは, 定理 5.5 に示した列ベクトル $\boldsymbol{H}_i$ において, $\mathcal{A}, \mathcal{B}$ をそれぞれ “1”, “0” と置き換えるとその 2 進数が $i+1$ を表すからである．この復号法に基づく誤り位置指摘回路を図 5.4 に示す.

## 5.5　評価

### (1) 検査ビット長

図 5.5 に 定理 5.2, 5.3 によって得られた $SEC-S_{4/15\times4}EL$ 符号の 検査ビット長の下界と符号 I, 符号 II の検査ビット長との比較を示す．同図より, 情報ビット長が小さいときは 符号 II の検査ビット長が下界に近く, 情報ビット長が大きいときは, 符号 I の検査ビット長が下界に近いことが分かる．したがって, 情報ビット長に応じて符号構成法を選択すれば, 検査ビット長が下界に近い符号が得られる.

### (2) 誤り検出率

$SEC-S_{b/p\times b}EL$ 符号は全ての ランダム二重ビット誤りや二重バイト誤りを検出できるわけではない．これらの誤りが生じたときには以下のような誤った復号をすることがある.

1. 誤りの生じていないブロックを誤りブロックとして指摘する (誤指摘)

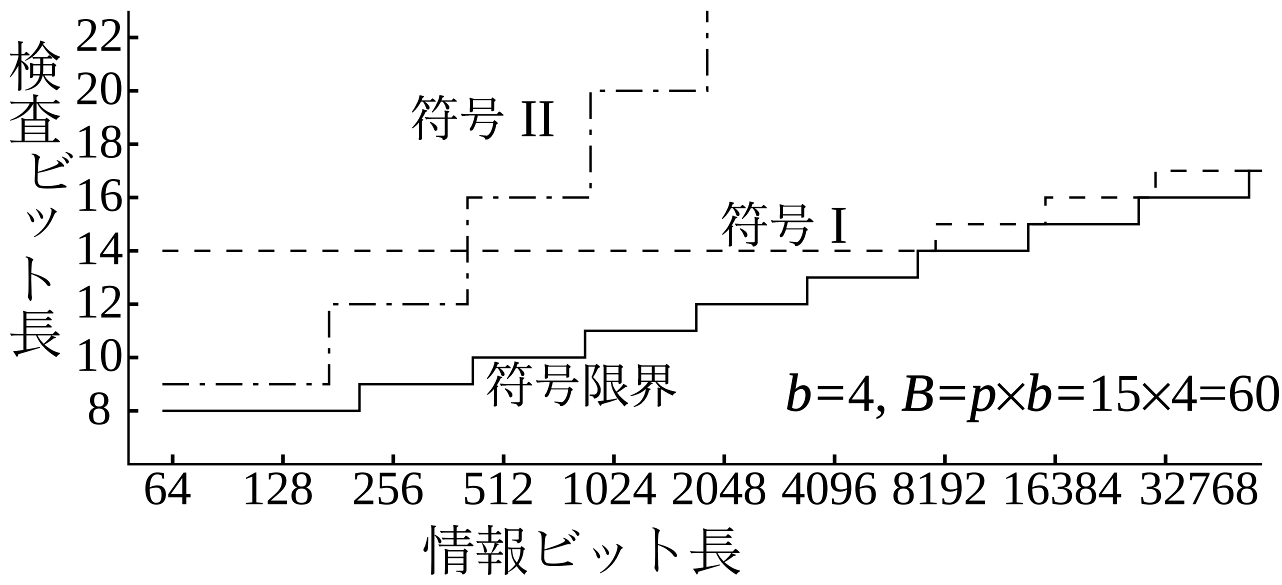



図 5.5: $SEC-S_{4/15\times4}EL$ 符号の検査ビット長と検査ビット長の下界の比較

2. 誤りの生じていないビットを訂正する (誤訂正)
3. シンドロームが零ベクトルになり誤り無しと判断してしまう (未検出)

しかし, 以下に示した場合のように安全な復号を行なう場合もある.

4. 訂正や位置指摘は不可能だが, 誤りを検出する (検出)
5. 全ての誤りが1ブロックに集中しているときに, そのブロックを指摘する (位置指摘)

図5.2に示した検査行列の最後尾の6バイト, すなわち24列を削除すると$(72, 64)$ $SEC-S_{4/8\times4}EL$ 符号の検査行列が得られる. このとき, 最後のブロックの大きさは8ビットになる. この符号において二重ビット誤り, 二重バイト誤りの生じた受信語を復号した際に上記5種類の場合の起きる確率を計算機シミュレーションで求めた結果を表5.1に示す. 同表より, この符号ではランダム二重ビット誤り, 二重バイト誤りの両者に対して約50 %の確率で安全な復号が実行可能であることが分かる.

**(3) 復号回路量**

図5.6に $SEC-S_{b/p\times b}EL$ 符号の $b=4, B=p\times b=16$ の場合における復号回路量を示す. ここでは, 4入力のAND/ORゲートを1ゲートとし, EX-ORゲートを2.5ゲートとしてゲート数を算出している.

表 5.1: (72, 64) $SEC - S_{4/32}EL$ 符号 II における2ビット誤り, 2バイト誤りの復号確率

| | 二重ビット誤り | 二重バイト誤り |
|---|---|---|
| 1.　誤指摘 | 31.0 % | 25.5 % |
| 2.　誤訂正 | 15.0 % | 27.0 % |
| 3.　未検出 | 0 % | 1.1 % |
| 4.　検出 | 49.8 % | 30.4 % |
| 5.　位置指摘 | 4.2 % | 16.0 % |

1ビット誤りを訂正する回路のゲート数が符号 I と符号 II で異なっているのは検査ビット長が異なるためである. 一方, 誤り位置指摘回路のゲート数が異なるのは誤り位置指摘の方法が符号 I と符号 II で異なるためである. すなわち, 符号 II ではシンドロームから誤りブロックの位置が直接求められるのに対し, 符号 I ではもとにした $S_{b'}EC$ 符号と $SEC - S_bED$ 符号の復号過程をとらなければならないからである.

$SEC - S_{4/4\times4}EL$ 符号の総復号回路量は $SEC - DED$ 符号のそれに比べて約15% 多いだけである. 回路量が $SEC - DED$ 符号に比べて増大する理由としては次のようなことが考えられる. 前者の符号の方が後者の符号よりも検査ビット長が大きい. そのため, 前者の符号の1ビット誤り訂正回路量は後者のそれより約 10% 大きくなる. さらに, 後者の復号回路には誤り位置指摘回路が付加されいる.

## 5.6　結言

本章では単一ビット誤りを訂正し, 故障バイト出力素子を含むメモリカード位置を指摘する実用上重要な符号である $SEC - S_{b/p\times b}EL$ 符号について, 符号限界を示し, 2種類の構成法および復号法を提案し, その評価を行なった. 本章によって得られた結果は以下の通りである.

(1) 2種類の符号構成法を提案した. 符号 I は単一バイト誤り訂正符号の検査行列と単一ビット誤り訂正・単一バイト誤り検出符号の検査行列のテンソル積を用いて構成する符号であり, 符号 II は奇数重み列正方行列, 偶数重み列正方行列と呼ばれる2種類の $b \times b$ 正方行列を要素とする検査行列より得られる符号である.

(2) 上記構成法で得られる符号の検査ビット長を符号限界と比較すると, 情報ビット長が小さいときは 符号 II の検査ビット長が下界に近く, 情報ビット長が大きいときは, 符号 I の検査ビット長が下界に近い.

(3) $SEC - S_{4/4\times4}EL$ 符号の復号回路量は情報長が等しい $SEC - DED$ 符号の復号回路に比

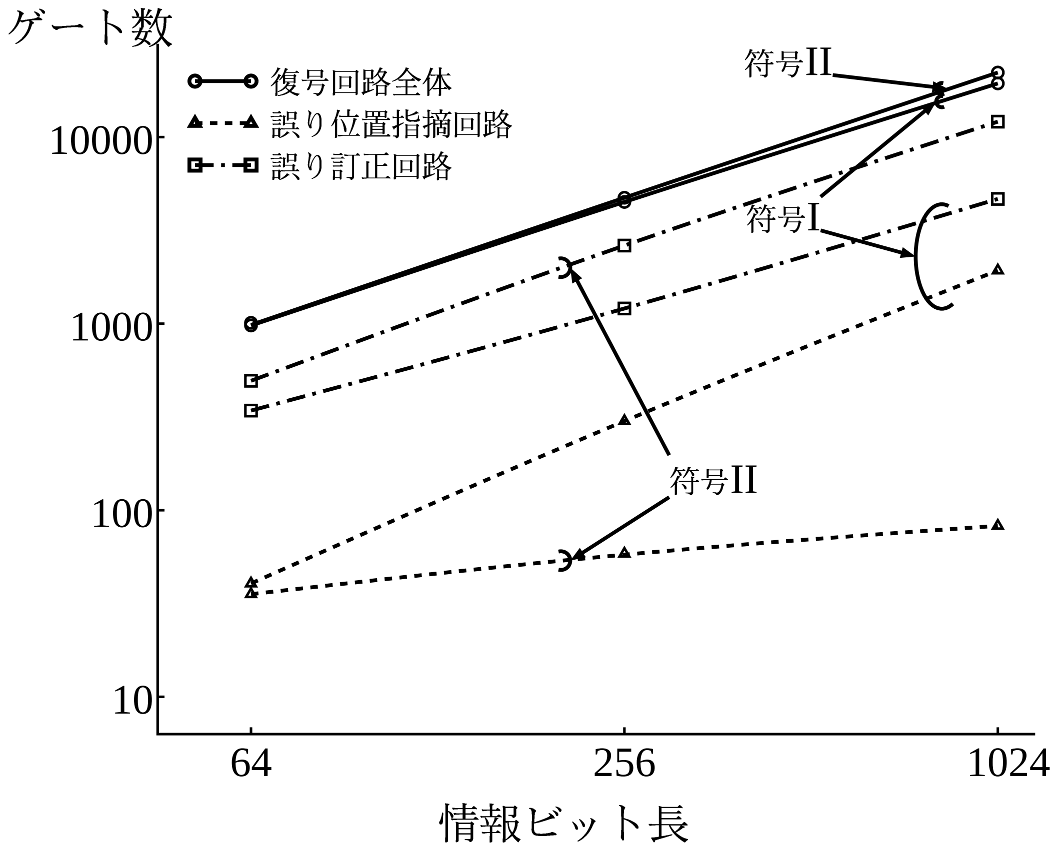



図 5.6: $SEC-S_{4/4\times4}EL$ 符号の復号回路量

べておよそ 15 % の冗長で済む．この冗長の大半は $SEC-S_{e/b}EL$ 符号の検査ビット長が $SEC-DED$ 符号の検査ビット長よりも大きいことによりシンドローム生成回路, 1 ビット誤り訂正回路の回路量が増大することによるものであり, 位置指摘回路による冗長は数%である.

(4) 本提案の $SEC-S_{4/8\times4}EL$ 符号ではランダム二重ビット誤り, 二重バイト誤りといった本符号の誤り制御能力を越えた誤りに対しても約 50 % の確率で安全な復号, すなわち検出または正しい位置指摘が実行可能である.

# 第6章　誤り位置指摘符号の距離構造

## 6.1　緒言

本章では誤り位置指摘符号の距離構造として, 距離を用いた符号条件について述べている. 新たに定義した距離および 2 符号語間の関係を表す関数を用いて $e/b$ 誤り訂正符号, 位置指摘符号, 検出符号およびこれらの機能を組み合わせた機能を有する符号の必要十分条件を導出している. 得られた結果を用いて, 誤り位置指摘符号の距離構造と誤り訂正符号, 誤り検出符号の距離構造の関係を明らかにし, 既存の符号の距離構造を導出している.

## 6.2　準備

符号語 $\boldsymbol{x}, \boldsymbol{y}$ の長さを $N = b \times n$ ビットとし, 長さ $b$ ビットのバイトに分割されているとする. $\boldsymbol{x}, \boldsymbol{y}$ の第 $i$ バイトを それぞれ $\boldsymbol{x}_i, \boldsymbol{y}_i$ とおく. ただし, $0 \leq i \leq n-1$ である.

**定義 6.1** ベクトル $\boldsymbol{x}, \boldsymbol{y}$ に対し関数 $D_e(\boldsymbol{x}, \boldsymbol{y})$ を以下のように定義する.

$$D_e(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=0}^{n-1} d_e(\boldsymbol{x}_i, \boldsymbol{y}_i)$$

ただし,

$$d_e(\boldsymbol{x}_i, \boldsymbol{y}_i) = \left\lceil \frac{d_H(\boldsymbol{x}_i, \boldsymbol{y}_i)}{e} \right\rceil e$$

であり, $\lceil x \rceil$ は $x$ 以上の整数のうち最小の整数を表し, $d_H(\cdot, \cdot)$ はハミング距離を表す. ∎

上記の $D_e(\cdot, \cdot)$ は距離 (metric) の公理 [2] を満たしている. それを以下の定理に示す.

**定理 6.1** 関数 $D_e(\cdot, \cdot)$ は距離の公理を満足する. すなわち任意のベクトル $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ に対して以下の関係が成立する.

1. $D_e(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ であり, 等号は $\boldsymbol{x} = \boldsymbol{y}$ のときのみ成立

2. $D_e(\boldsymbol{x}, \boldsymbol{y}) = D_e(\boldsymbol{y}, \boldsymbol{x})$

3. $D_e(\boldsymbol{x},\boldsymbol{y}) \le D_e(\boldsymbol{x},\boldsymbol{z}) + D_e(\boldsymbol{z},\boldsymbol{y})$

**(証明)**

上記の性質のうち 1, 2 が成立することは明らかなので 3 が成立することのみを示す.

ベクトル $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$ の第 $i$ バイトをそれぞれ $\boldsymbol{x}_i,\boldsymbol{y}_i,\boldsymbol{z}_i$ とおく. ハミング距離 $d_H(\cdot,\cdot)$ は距離の公理を満たすので

$$d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \le d_H(\boldsymbol{x}_i,\boldsymbol{z}_i) + d_H(\boldsymbol{z}_i,\boldsymbol{y}_i) \tag{6-1}$$

が成立する. また, 任意の自然数 $j_1, j_2$ に対して以下の関係が成立する.

$$j_1 \le j_2 \Longrightarrow \left\lceil \frac{j_1}{e} \right\rceil e \le \left\lceil \frac{j_2}{e} \right\rceil e \tag{6-2}$$

$$\left\lceil \frac{j_1+j_2}{e} \right\rceil e \le \left\lceil \frac{j_1}{e} \right\rceil e + \left\lceil \frac{j_2}{e} \right\rceil e \tag{6-3}$$

式 (6-2), (6-3) に示した性質を利用すると式 (6-1) より以下に示す関係が得られる.

$$\left\lceil \frac{d_H(\boldsymbol{x}_i,\boldsymbol{y}_i)}{e} \right\rceil e \le \left\lceil \frac{d_H(\boldsymbol{x}_i,\boldsymbol{z}_i)+d_H(\boldsymbol{z}_i,\boldsymbol{y}_i)}{e} \right\rceil e \le \left\lceil \frac{d_H(\boldsymbol{x}_i,\boldsymbol{z}_i)}{e} \right\rceil e + \left\lceil \frac{d_H(\boldsymbol{z}_i,\boldsymbol{y}_i)}{e} \right\rceil e$$

これは $d_e(\boldsymbol{x}_i,\boldsymbol{y}_i) \le d_e(\boldsymbol{x}_i,\boldsymbol{z}_i) + d_e(\boldsymbol{z}_i,\boldsymbol{y}_i)$ が成立することを示している. ゆえに, $D_e(\boldsymbol{x},\boldsymbol{y}) \le D_e(\boldsymbol{x},\boldsymbol{z}) + D_e(\boldsymbol{z},\boldsymbol{y})$ が成立し, 上記の関係 3 が成立する.

以上より, 関数 $D_e(\cdot,\cdot)$ は距離の公理を満足する. (Q.E.D.)

**定義 6.2** ベクトル $\boldsymbol{x},\boldsymbol{y}$ に対し, $\gamma_{f_1}^{f_2}(\boldsymbol{x},\boldsymbol{y})$ を以下のように定義する.

$$\gamma_{f_1}^{f_2}(\boldsymbol{x},\boldsymbol{y}) = \left| \{ i | f_1 \le d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \le f_2, 0 \le i \le n-1 \} \right|$$

ただし, $|A|$ は集合 $A$ の要素数を表し, $d_H(\cdot,\cdot)$ はハミング距離を表す. ■

以下, 本章では定義 3.1 で定義した $e/b$ 誤りを制御する誤り訂正符号, 位置指摘符号, 検出符号およびそれらを組み合わせた符号を扱うが, 訂正符号, 位置指摘符号, 検出符号をそれぞれ $t_{e_1/b}EC$ 符号, $l_{e_2/b}EL$ 符号, $m_{e_3/b}ED$ 符号, と表すことにする. ここで, 例えば $t_{e_1/b}EC$ 符号は $t$ 個以下の $e_1/b$ 誤りが訂正可能な符号である. さらに, これらを組み合わせた符号を $t_{e_1/b}EC - l_{e_2/b}EL$ 符号などと表すことにする. ただし, 符号のパラメータ $t, l, m$ には以下の関係が成立しているものとする.

$$t \le l \le m$$

また, $e_1 = e_2 = e_3$ が成立するときにはこれらの値を単に $e$ と表すこともある.

$e_p, e_q$ のうち値の大きい方を $e_{p,q}$ と定義する. すなわち $e_p \le e_q$ のとき $e_{p,q} = e_q$ であり, $e_p > e_q$ のとき $e_{p,q} = e_p$ である.

本章における議論の多くは主に GF(2) 上の符号に関して行なうが, 以下の議論は他のガロア体上の符号に対しても適用可能である.

## 6.3 単機能の誤り制御符号の距離構造

### 6.3.1 誤り訂正符号

**補題 6.1** ある符号 $\mathcal{C}$ が誤り集合 $E$ に属す全ての誤りを訂正可能であるための必要十分条件は以下の通りである.

$$\boldsymbol{x}+\boldsymbol{e}_x \neq \boldsymbol{y}+\boldsymbol{e}_y \text{ for } \forall \boldsymbol{x}, \forall \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}, \text{ and } \forall \boldsymbol{e}_x, \forall \boldsymbol{e}_y \in E$$

この補題の証明は定理 2.3 より明らかなので省略する.

**定理 6.2** 誤り訂正符号 $t_{e/b}EC$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x}, \boldsymbol{y}$ に対して以下の関係が成立することである.

$$\gamma_{2e+1}^{b}(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } D_e(\boldsymbol{x}, \boldsymbol{y}) \geq 2te+1$$

**(証明)**

$\boldsymbol{e}_x, \boldsymbol{e}_y$ の第 $i$ バイトをそれぞれ $\boldsymbol{e}_{xi}, \boldsymbol{e}_{yi}$ とおく.

条件 $\gamma_{2e+1}^{b}(\boldsymbol{x}, \boldsymbol{y}) \geq 1$ が成立するとき, あるバイト位置 (第 $i$ バイトとおく) において $d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \geq 2e+1$ が成立する. このとき, $\boldsymbol{x}, \boldsymbol{y}$ 両者の第 $i$ バイトに $e/b$ 誤りが生じても その結果得られるベクトルの第 $i$ バイトが一致することはない. ゆえに, 補題 6.1 よりこの符号は $t_{e/b}EC$ 符号である.

また, $t$ 個以下の $e/b$ 誤りからなる集合を $E_{t_{e/b}}$ とおくと, この集合に属す誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ について $D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) \leq te, D_e(\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_y) \leq te$ である. 定理 6.1 より関数 $D_e(\cdot,\cdot)$ は距離の公理を満たすので三角不等式が成立し,

$$D_e(\boldsymbol{x}, \boldsymbol{y}) \leq D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) + D_e(\boldsymbol{x}+\boldsymbol{e}_x, \boldsymbol{y}+\boldsymbol{e}_y) + D_e(\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_y)$$

となる. よって, $D_e(\boldsymbol{x}, \boldsymbol{y}) \geq 2te+1$ のときは

$$\begin{aligned} D_e(\boldsymbol{x}+\boldsymbol{e}_x, \boldsymbol{y}+\boldsymbol{e}_y) &\geq D_e(\boldsymbol{x}, \boldsymbol{y}) - D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) - D_e(\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{e}_y) \\ &\geq 1 \end{aligned}$$

となり, 常に $\boldsymbol{x}+\boldsymbol{e}_x \neq \boldsymbol{y}+\boldsymbol{e}_y$ が成立する. ゆえに, 補題 6.1 よりこの符号は $t_{e/b}EC$ 符号である.

逆に, $\gamma_{2e+1}^{b}(\boldsymbol{x}, \boldsymbol{y}) = 0$ かつ $D_e(\boldsymbol{x}, \boldsymbol{y}) < 2te+1$ のときは全てのバイトに対して $0 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq 2e$ が成立する. ここで, $e+1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq 2e$ が成立するバイトの個数を $w$ とすると, $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ が成立するバイトの個数は高々$2t-2w$ である. このとき, $e+1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq 2e$ が成立するバイトでは $\boldsymbol{e}_{xi} \neq 0, \boldsymbol{e}_{yi} \neq 0$ かつ $\boldsymbol{x}_i + \boldsymbol{e}_{xi} = \boldsymbol{y}_i + \boldsymbol{e}_{yi}$ が成立し, $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ が成立するバイトのうち最初の $t-w$ バイトでは $\boldsymbol{e}_{xi} = \boldsymbol{x}_i + \boldsymbol{y}_i, \boldsymbol{e}_{yi} = 0$ が成立し, それ以外の $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ が成立するバイトでは $\boldsymbol{e}_{xi} = 0, \boldsymbol{e}_{yi} = \boldsymbol{x}_i + \boldsymbol{y}_i$ が成立するように $\boldsymbol{e}_x, \boldsymbol{e}_y$ を選択すると $\boldsymbol{e}_x, \boldsymbol{e}_y \in E_{t_{e/b}}$, $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}+\boldsymbol{e}_x$ が成立する. よって, この符号は $t_{e/b}EC$ 符号ではない.

以上より, 定理に示した条件は $t_{e/b}EC$ 符号であるための必要十分条件である.　(Q.E.D.)

### 6.3.2　誤り検出符号

**補題 6.2** ある符号 $\mathcal{C}$ が誤り集合 $E$ に属す全ての誤りを検出可能であるための必要十分条件は以下の通りである.

$$\boldsymbol{x}+\boldsymbol{e}_x \neq \boldsymbol{y} \text{ for } \forall \boldsymbol{x}, \forall \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}, \text{ and } \forall \boldsymbol{e}_x \in E$$

この補題の証明は定理 2.3 より明らかなので省略する.

**定理 6.3** 誤り検出符号 $m_{e/b}ED$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x}, \boldsymbol{y}$ に対して以下の関係が成立することである.

$$\gamma^b_{e+1}(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } D_e(\boldsymbol{x}, \boldsymbol{y}) \geq me+1$$

**(証明)**

条件 $\gamma^b_{e+1}(\boldsymbol{x}, \boldsymbol{y}) \geq 1$ が成立するとき, あるバイト位置 (第 $i$ バイトとおく) において $d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \geq e+1$ が成立する. このとき, $\boldsymbol{x}$ の第 $i$ バイトに $e/b$ 誤りが生じても その結果得られるベクトルの第 $i$ バイトが $\boldsymbol{y}$ の第 $i$ バイトに一致することはない. ゆえに, 補題 6.2 よりこの符号は $m_{e/b}ED$ 符号である.

また, $m$ 個以下の $e/b$ 誤りからなる集合を $E_{m_{e/b}}$ とおくと, この集合に属す誤り $\boldsymbol{e}_x$ について $D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) \leq me$ である. ここで, 三角不等式より

$$D_e(\boldsymbol{x}, \boldsymbol{y}) \leq D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) + D_e(\boldsymbol{x}+\boldsymbol{e}_x, \boldsymbol{y})$$

となる. よって, $D_e(\boldsymbol{x}, \boldsymbol{y}) \geq me+1$ のときは

$$\begin{aligned} D_e(\boldsymbol{x}+\boldsymbol{e}_x, \boldsymbol{y}) &\geq D_e(\boldsymbol{x}, \boldsymbol{y}) - D_e(\boldsymbol{x}, \boldsymbol{x}+\boldsymbol{e}_x) \\ &\geq 1 \end{aligned}$$

となり, 常に $\boldsymbol{x}+\boldsymbol{e}_x \neq \boldsymbol{y}$ が成立する. ゆえに, 補題 6.2 よりこの符号は $m_{e/b}ED$ 符号である.

逆に, $\gamma^b_{e+1}(\boldsymbol{x}, \boldsymbol{y}) = 0$ かつ $D_e(\boldsymbol{x}, \boldsymbol{y}) < me+1$ のときは $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ であるバイトの個数は $m$ 個以下である. したがって, $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ であるバイトにおいて $\boldsymbol{e}_{xi} = \boldsymbol{x}_i + \boldsymbol{y}_i$, それ以外のバイトにおいて $\boldsymbol{e}_{xi} = 0$ が成立するように $\boldsymbol{e}_x$ を選ぶと $\boldsymbol{e}_x \in E_{m_{e/b}}$, $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}$ が成立するので, この符号は $m_{e/b}ED$ 符号ではない.

以上より, 定理に示した条件は $m_{e/b}ED$ 符号であるための必要十分条件である.　(Q.E.D.)

### 6.3.3　誤り位置指摘符号

**補題 6.3** 符号長 $N = n \times b$ ビットの 符号 $\mathcal{C}$ が誤り集合 $E$ に属す全ての誤りについて誤りの位置を指摘可能であるための必要十分条件は任意の互いに異なる符号語 $\boldsymbol{x}, \boldsymbol{y}$ と $E$ に属す任意の誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ について以下の関係が全て成立することである.

1. $\boldsymbol{x} + \boldsymbol{e}_x = \boldsymbol{y} + \boldsymbol{e}_y \quad \Rightarrow \quad (\boldsymbol{e}_{xi} = 0 \wedge \boldsymbol{e}_{yi} = 0)$ or $(\boldsymbol{e}_{xi} \neq 0 \wedge \boldsymbol{e}_{yi} \neq 0)$ for $\forall i, 0 \leq i \leq n-1$

2. $\boldsymbol{x} + \boldsymbol{e}_x \neq \boldsymbol{y}$

ただし, $\boldsymbol{e}_{xi}, \boldsymbol{e}_{yi}$ はそれぞれ $\boldsymbol{e}_x, \boldsymbol{e}_y$ の第 $i$ バイトを表している.

**(証明)**

条件 1 は 誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ の誤りバイト位置が全て同一であるときに限って $\boldsymbol{x} + \boldsymbol{e}_x = \boldsymbol{y} + \boldsymbol{e}_y$ が成立しても良いことを示している．このときには誤りを訂正して元の符号語を得ることはできないが, 誤りの生じたバイト位置は正しく指摘できる．また, 条件 2 は少なくとも誤り検出ができる必要があることを表している. (Q.E.D.)

第 2.5 節で述べたように, 誤り位置指摘符号は誤り識別符号に含まれるので, 定理 2.3 を用いてこの補題を証明することも可能である.

**定理 6.4** 誤り位置指摘符号 $l_{e/b}EL$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x}, \boldsymbol{y}$ に対して以下の関係が成立することである.

$$\gamma^b_{2e+1}(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } \gamma^e_1(\boldsymbol{x}, \boldsymbol{y}) = 0 \text{ or } D_e(\boldsymbol{x}, \boldsymbol{y}) \geq 2le + 1$$

**(証明)**

関係 $\gamma^b_{2e+1}(\boldsymbol{x}, \boldsymbol{y}) \geq 1$ または $D_e(\boldsymbol{x}, \boldsymbol{y}) \geq 2le+1$ が成立するときは定理 6.2 よりこの符号は $l_{e/b}EC$ 符号であるので $l_{e/b}EL$ 符号になる.

また, 関係 $\gamma^e_1(\boldsymbol{x}, \boldsymbol{y}) = 0$ が成立しているとき, ある誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ について $\boldsymbol{x} + \boldsymbol{e}_x = \boldsymbol{y} + \boldsymbol{e}_y$ が成立する可能性がある．しかし, このときには $d_H(\boldsymbol{x}_i, \boldsymbol{y}_i)$ の値は 0 または $e+1$ 以上である．したがって, $d_H(\boldsymbol{x}_i, \boldsymbol{y}_i)$ の値が $e+1$ 以上であるバイトでは $\boldsymbol{e}_{xi} \neq 0, \boldsymbol{e}_{yi} \neq 0$ であり, $d_H(\boldsymbol{x}_i, \boldsymbol{y}_i)$ の値が 0 であるバイトでは $\boldsymbol{e}_{xi} = \boldsymbol{e}_{yi}$ である．ただし, $\boldsymbol{e}_{xi}, \boldsymbol{e}_{yi}$ はそれぞれ $\boldsymbol{e}_x, \boldsymbol{e}_y$ の第 $i$ バイトを表している．したがって, 補題 6.4 よりこのときも $l_{e/b}EL$ 符号の条件を満たしている.

逆に, $\gamma^b_{2e+1}(\boldsymbol{x}, \boldsymbol{y}) = 0$ かつ $\gamma^e_1(\boldsymbol{x}, \boldsymbol{y}) \geq 1$ かつ $D_e(\boldsymbol{x}, \boldsymbol{y}) < 2le + 1$ が成立するときは, $1 \leq d_H(\boldsymbol{x}_i, \boldsymbol{y}_i) \leq e$ を満たすバイトが存在する．このバイトに対して $\boldsymbol{e}_{xi} \neq 0, \boldsymbol{e}_{yi} = 0$ となり, $\boldsymbol{x} + \boldsymbol{e}_x = \boldsymbol{y} + \boldsymbol{e}_y$ を満たす誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ を $l$ 個以下の $e/b$ 誤りからなる集合の中から選択することが可能である．ゆえに, 補題 6.4 よりこのときにはこの符号は $l_{e/b}EL$ 符号にならない.

以上より, 定理に示した条件は $l_{e/b}EL$ 符号であるための必要十分条件である. (Q.E.D.)

本節において示した符号の距離構造をまとめて表 6.1 に示す.

# 6.4　複数の機能を組み合わせた誤り制御符号の距離構造

## 6.4.1　誤り訂正・検出符号

**補題 6.4** 誤り訂正・検出符号 $t_{e_1/b}EC - m_{e_3/b}ED$ 符号において誤り訂正と検出が区別して実行可能であるための必要十分条件は以下の条件が成立することである.

$$\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$$
$$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1 + 1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3 + 1)$$

**(証明)**

条件 $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき, $d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \geq e_1+e_3+1$ を満たすバイトが存在する. このバイトは $\boldsymbol{x},\boldsymbol{y}$ にそれぞれ $e_1/b$ 誤り, $e_3/b$ 誤りが生じても一致しない. ゆえに, このとき $t$ 個以下の $e_1/b$ 誤りと $m$ 個以下の $e_3/b$ 誤りが区別可能である.

条件 $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ が成立するとき, $\boldsymbol{x},\boldsymbol{y}$ に生じる誤りをそれぞれ $\boldsymbol{e}_x,\boldsymbol{e}_y$ とおき, それぞれ $t$ 個以下の $e_1/b$ 誤り, $m$ 個以下の $e_3/b$ 誤りであるとする. このとき, $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}+\boldsymbol{e}_y$ を満たすには少なくとも $e_3+1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i)$ が成立するバイトにおいては $\boldsymbol{e}_{xi} \neq 0$ が成立する必要がある. しかし, このようなバイトは少なくとも $t+1$ 個必要であるので, $\boldsymbol{e}_x$ が $t$ 個以下の $e_1/b$ 誤りである時には $\boldsymbol{x}+\boldsymbol{e}_x \neq \boldsymbol{y}+\boldsymbol{e}_y$ となり, 誤りの区別が可能になる. 条件 $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ が成立するときに誤りの区別が可能であることも同様にして証明可能である.

また, 条件 $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1)$ が成立するとき, $t$ 個の $e_1/b$ 誤りと $m$ 個の $e_3/b$ 誤りが区別可能であることは定理 6.2 の証明と同様にして示すことができる.

逆に $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) = 0$ かつ $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) < m+1$ かつ $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) < t+1$ かつ $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) < (t+m)e_1+1 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) < (t+m)e_3+1)$ であるときを考える. まず, $e_1 \leq e_3$ が成立すると仮定し, $e_3+1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_1+e_3$ であるバイトの個数を $w$ とおく. このとき, $1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_1$ であるバイトの個数は高々$t+m-2w$ 個であり, $e_1+1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_3$ であるバイトの個数は高々$m-w$ 個である. このとき, 以下に示す条件を満たす $\boldsymbol{e}_x,\boldsymbol{e}_y$ を選択する

1. $e_3+1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_1+e_3$ であるバイトでは $\boldsymbol{e}_{xi} \neq 0, \boldsymbol{e}_{yi} \neq 0$, かつ $\boldsymbol{x}_i+\boldsymbol{e}_{xi} = \boldsymbol{y}_i+\boldsymbol{e}_{yi}$ が成立

2. $1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_1$ であるバイトのうちの最初の $t-w$ バイトでは $\boldsymbol{e}_{xi} = \boldsymbol{x}_i+\boldsymbol{y}_i, \boldsymbol{e}_{yi} = 0$ が成立

3. 上記 2 で選択されなかったバイトのうち $1 \leq d_H(\boldsymbol{x}_i,\boldsymbol{y}_i) \leq e_3$ が成立するバイトでは $\boldsymbol{e}_{xi} = 0, \boldsymbol{e}_{yi} = \boldsymbol{x}_i+\boldsymbol{y}_i$ が成立

上記条件を満たすように $\boldsymbol{e}_x,\boldsymbol{e}_y$ を選択すると, $\boldsymbol{e}_x,\boldsymbol{e}_y$ はそれぞれ $t$ 個以下の $e_1/b$ 誤り, $m$ 個以下の $e_3/b$ 誤りとなり, $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}+\boldsymbol{e}_y$ が成立する. よって, 誤りの区別は不可能である. また, $e_1 > e_3$

が成立すると仮定したときも同様にして $t$ 個以下の $e_1/b$ 誤り, $m$ 個以下の $e_3/b$ 誤りが区別不可能になることが証明可能である.

以上より補題に示した条件は誤りの訂正と検出が区別して実行可能となるための必要十分条件である. (Q.E.D.)

**定理 6.5** 誤り訂正・検出符号 $t_{e_1/b}EC - m_{e_3/b}ED$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x}, \boldsymbol{y}$ に対して以下の関係が成立することである.

$$\begin{aligned}
&\gamma^b_{e_1+e_{1,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1) \text{ or}\\
&D_{e_{1,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_{1,3}+1 \text{ or}\\
&(\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ if } e_1 \leq e_3) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_1 > e_3)
\end{aligned}$$

ただし, $(\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ if } e_1 \leq e_3)$ は $e_1 \leq e_3$ が成立する場合に限って $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ が成立することを表している.

**(証明)**

この符号の条件は以下の 3 条件が全て成立することと同値である.

1. $t$ 個以下の $e_1/b$ 誤りが訂正可能である
2. $m$ 個以下の $e_3/b$ 誤りが検出可能である
3. 誤りの訂正と検出が区別して実行可能である

定理 6.2, 6.3 および補題 6.4 より上記 3 条件は以下のそれぞれ以下の条件と同値である.

1. $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1$
2. $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq me_3+1$
3. $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$
   $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1)$

(I) $e_1 \leq e_3$ のとき

上記の条件 3 は以下の条件 3' と同値である.

3'. $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1$

ここで上記の条件 3' に注目する.

条件 3' に含まれる $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するときは明らかに $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1, \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ であるので条件 1, 2 も成立し, 全条件が成立する. また,$\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ が成立するときは $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2(t+1)e_1$ より全条件が成立し, $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ が成立する時も $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2(m+1)e_1, D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (m+1)e_3$ より全条件が成立する. さらに, $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1$ が成立するときも $t < m$ より全条件が成立する.

ゆえに 符号条件は以下のようになる.

$$\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$$
$$D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1$$

(II) $e_1 > e_3$ のとき

上記の条件 3 は以下の条件 3" と同値である.

3". $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$

ここで, 上記の条件 1 に注目する.

条件 1 に含まれる $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するときは明らかに $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1, \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ であるので条件 2, 3" も成立し, 全条件が成立する.

次に 条件 1 に含まれる $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1$ が成立するときを考える. このとき, 条件 3" に含まれる $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立すれば 条件 2 も成立し, 全条件が成立する. また, 条件 3" に含まれる $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ が成立するときも全条件が成立する. さらに, 条件 3" に含まれる $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$ が成立するときも全条件が成立する. このときの条件は $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1)$ であるが, これは $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$ と同値である.

ゆえに, 符号条件は以下のようになる.

$$\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or}$$
$$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1) \text{ or } D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$$

上記の条件のうち (I) に含まれる $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ と (II) に含まれる $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ は $\gamma^b_{e_1+e_{1,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ としてまとめることができる. また, (I) の $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1$ と (II) の $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$ は $D_{e_{1,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_{1,3}+1$ としてまとめることができる. さらに, (II) の $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)$ は $e_1 \leq e_3$ のとき (I) に含まれる $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ と同値である.

以上より, (I), (II) をまとめると以下に示す $t_{e_1/b}EC - m_{e_3/b}ED$ 符号の必要十分条件を得る.

$$\begin{aligned}
&\gamma^b_{e_1+e_{1,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1) \text{ or}\\
&D_{e_{1,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_{1,3}+1 \text{ or}\\
&(\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ if } e_1 \leq e_3) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_1 > e_3)
\end{aligned}$$

(Q.E.D.)

### 6.4.2　誤り訂正・位置指摘符号

**補題 6.5** 誤り訂正・位置指摘符号 $t_{e_1/b}EC - l_{e_2/b}EL$ 符号において誤り訂正と位置指摘が区別して実行可能であるための必要十分条件は以下の条件が成立することである.

$$\begin{aligned}
&\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1)
\end{aligned}$$

この補題の証明は補題 6.4 の証明と同様にして得られるので省略する.

**定理 6.6** 誤り訂正・位置指摘符号 $t_{e_1/b}EC - l_{e_2/b}EL$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x},\boldsymbol{y}$ に対して以下の関係が成立することである.

$$\begin{aligned}
&\gamma^b_{2e_{1,2}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0\ ) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1\ ) \text{ or}\\
&(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_1 \leq e_2) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_1 > e_2\ ) \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge\\
&\qquad (\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1) \text{ if } e_1 > e_2\ \} \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge (\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ if } e_1 > e_2\ \}
\end{aligned}$$

**(証明)**

この符号の条件は以下の 3 条件が全て成立することと同値である.

1. $t$ 個以下の $e_1/b$ 誤りが訂正可能である
2. $l$ 個以下の $e_2/b$ 誤りが位置指摘可能である
3. 誤りの訂正と位置指摘が区別して実行可能である

定理 6.2, 6.4 および補題 6.5 より上記 3 条件はそれぞれ以下の条件と同値である.

1. $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1$

2. $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1$

3. $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1$ $\wedge\ D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1)$

(I) $e_1 \leq e_2$ のとき

上記の条件 3 は以下の条件 3' と同値である.

3'. $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1$

ここで, 上記の条件 2 に注目する.

条件 2 に含まれる $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき, $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$, $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するので条件 1, 3' が成立し, 全条件を満足する. また, $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1$ が成立するときは, $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_1+1$ が成立し, $t < l$ より全条件が成立する.

次に, $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ が成立する場合を考える. 条件 3' に含まれる $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき, 全条件が成立し, 条件 3' に含まれる $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ が成立するときも 全条件が成立する. また, $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ が成立するときは $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ も成立するので上の場合に含まれる. さらに, 条件 3' に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1$ が成立するときは $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ も成立するので上の場合に含まれる.

ゆえに, 符号条件は以下のようになる.

$$\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \text{ or}$$
$$(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or } (\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1\ )$$

(II) $e_1 > e_2$ のとき

上記の条件 3 は以下の条件 3" と同値である.

3". $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1$

ここで, 上記の条件 1 に注目する.

(a) 条件 1 に含まれる $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき条件 1, 2 及び 3" が全て成立する.
(b) 条件 1 に含まれる $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1$ が成立するとき
    (a) 条件 3" に含まれる $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき, 条件 2 も成立し, 全条件が成立する.
    (b) 条件 3" に含まれる $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ が成立するとき
        (a) 条件 2 に含まれる $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するとき, 全条件が成立する.

(b) 条件 2 に含まれる $\gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0$ が成立するとき, 全条件が成立する.
(c) 条件 2 に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1$ が成立するとき, 全条件が成立する.

(c) 条件 3" に含まれる $D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1$ が成立するとき, $D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1$ は $D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1$ に含まれるので, この条件は $D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1$ と同値である.

(a) 条件 2 に含まれる $\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1$ が成立するとき, 全条件が成立する.
(b) 条件 2 に含まれる $\gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0$ が成立するとき, 全条件が成立する.
(c) 条件 2 に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1$ が成立するとき, 全条件が成立する.

ゆえに, 符号条件は以下のようになる.

$$
\begin{aligned}
&\gamma_{2e_1+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_1+e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1) \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq t+1 \wedge\\
&\qquad(\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1)\} \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1 \wedge\\
&\qquad(\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1)\}
\end{aligned}
$$

上記の条件のうち (I) に含まれる $\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1$ と (II) に含まれる $\gamma_{2e_1+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1$ は $\gamma_{2e_{1,2}+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1$ としてまとめることが可能である. また, (II) に含まれる $(D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1)$ は $e_1\leq e_2$ のとき (I) に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1$ と同値であり, (II) に含まれる $(D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq t+1 \wedge \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0)$ は $e_1\leq e_2$ のとき (I) に含まれる $(\gamma_{e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq t+1 \wedge \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0)$ と同値である.

以上より, (I), (II) をまとめると以下に示す $t_{e_1/b}EC-l_{e_2/b}EL$ 符号の必要十分条件を得る.

$$
\begin{aligned}
&\gamma_{2e_{1,2}+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq t+1 \wedge \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0\ ) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1\ ) \text{ or}\\
&(\gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0 \wedge \gamma_{e_1+e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ if } e_1\leq e_2) \text{ or}\\
&(D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_1+e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ if } e_1>e_2\ ) \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq 2te_1+1 \wedge \gamma_{e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq t+1 \wedge\\
&\qquad(\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y})\geq 2le_2+1) \text{ if } e_1>e_2\ \} \text{ or}\\
&\{D_{e_1}(\boldsymbol{x},\boldsymbol{y})\geq (t+l)e_1+1 \wedge (\gamma_{2e_2+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1 \text{ or } \gamma_1^{e_2}(\boldsymbol{x},\boldsymbol{y})=0) \text{ if } e_1>e_2\ \}
\end{aligned}
$$

(Q.E.D.)

### 6.4.3 誤り位置指摘・検出符号

**補題 6.6** 誤り位置指摘・検出符号 $l_{e_2/b}EL-m_{e_3/b}ED$ 符号において誤り訂正と位置指摘が区別して実行可能であるための必要十分条件は以下の条件が成立することである.

$$\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$$
$$(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0\ ) \text{ or}$$
$$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)$$

**(証明)**

条件 $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ または $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ または $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ または $(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)$ が成立するとき, $l$ 個以下の $e_2/b$ 誤りと $m$ 個以下の $e_3/b$ 誤りが区別可能であることは補題 6.4 と同様にして証明可能である.

条件 $(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0\ )$ が成立しているとき, 全てのバイトについて $d_H(\boldsymbol{x}_i,\boldsymbol{y}_i)$ は 0 または $e_{2,3}+1$ 以上である. ゆえに $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}+\boldsymbol{e}_y$ が成立するような誤り $\boldsymbol{e}_x, \boldsymbol{e}_y$ では誤りの生じたバイト位置が一致している. すなわち, 全てのバイトにおいて $\boldsymbol{e}_{xi}, \boldsymbol{e}_{yi}$ の両者が零ベクトルであるか, または両者が非零である. この場合には誤りの生じる前の符号語が $\boldsymbol{x}$ であっても, $\boldsymbol{y}$ であっても誤りの生じているバイト位置は同一なので正しく位置指摘できる. したがって, この場合についても位置指摘と検出が区別して実行可能であるといえる.

逆に, $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) = 0$ かつ $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) < l+1$ かつ $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) < m+1$ かつ $(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) \geq 1)$ かつ $(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) < (l+m)e_2+1$ or $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) < (l+m)e_3+1)$ が成立する時は補題 6.4 の証明と同様にして $\boldsymbol{x}+\boldsymbol{e}_x = \boldsymbol{y}+\boldsymbol{e}_y$ が成立するような $l$ 個以下の $e/b$ 誤り $\boldsymbol{e}_x$ と $m$ 個以下の $e/b$ 誤り $\boldsymbol{e}_y$ が存在することが証明可能である. このとき, $l$ 個以下の $e_2/b$ 誤りと $m$ 個以下の $e_3/b$ 誤りの区別は不可能であるので, 位置指摘と検出を区別して実行するのは不可能である.

以上より補題に示した条件は誤りの位置指摘と検出が区別して実行可能となるための必要十分条件である. (Q.E.D.)

**定理 6.7** 誤り位置指摘・検出符号 $l_{e_2/b}EL - m_{e_3/b}ED$ 符号の必要十分条件は任意の異なる2符号語 $\boldsymbol{x},\boldsymbol{y}$ に対して以下の関係が成立することである.

$$\gamma^b_{e_2+e_{2,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1) \text{ or}$$
$$\gamma^{e_{2,3}}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } D_{e_{2,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_{2,3}+1 \text{ or}$$
$$(\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ if } e_2 \leq e_3\ ) \text{ or}$$
$$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge \gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_2 > e_3)$$

**(証明)**

この符号の条件は以下の3条件が全て成立することと同値である.

1. $l$ 個以下の $e_2/b$ 誤りが位置指摘可能である
2. $m$ 個以下の $e_3/b$ 誤りが検出可能である
3. 誤りの訂正と位置指摘が区別して実行可能である

定理 6.4, 6.3 および補題 6.6 より上記 3 条件は以下のそれぞれ以下の条件と同値である.

1. $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1$
2. $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq me_3+1$
3. $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ or $(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0\ )$ or $(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)$

(I) $e_2 \leq e_3$ のとき

上記の条件 3 は以下の条件と同値である.

3'. $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ or $\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$

ここで上記の条件 3' に注目する.

条件 3' に含まれる $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するときは明らかに $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1, \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ であるので条件 1, 2 も成立し, 全条件が成立する. また, $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ が成立するときは $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2(l+1)e_1$ より全条件が成立し, $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ が成立するときも $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2(m+1)e_2, D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (m+1)e_3$ より全条件が成立する. 条件 3' に含まれる $\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ が成立するとき, $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$, $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立し, 全条件が成立する. さらに, $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$ が成立するときも $l < m$ より条全条件が成立する.

ゆえに 符号条件は以下のようになる.

$$\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or } \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \\ \text{or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$$

(II) $e_2 > e_3$ のとき

上記の条件 3 は以下の条件と同値である.

3". $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1$

ここで, 上記の条件 1 に注目する.

条件 1 に含まれる $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立するときは明らかに $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1, \gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ であるので全条件が成立する. また, $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ が成立するときも全条件が成立する

次に 条件 1 に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1$ が成立するときを考える. このとき, 条件 3" に含まれる $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ が成立すれば 条件 2 も成立し, 全条件が成立する. また, 条件 3" に含まれる $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ が成立するときも 全条件が成立する. さらに, 条件 3"

に含まれる $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1$ が成立するときも全条件が成立するが, このときの条件は $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1$ と同値である.

ゆえに, 符号条件は以下のようになる.

$$\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } (D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_1+1 \wedge \gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or}$$
$$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1) \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1$$

上記の条件のうち (I) に含まれる $\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ と (II) に含まれる $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ は $\gamma^b_{e_2+e_{2,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ としてまとめることが可能であり, (I) の $\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ と (II) の $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ も $\gamma^{e_{2,3}}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ としてまとめることが可能である. また, (I) の $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$ と (II) の $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_1+1$ は $D_{e_{2,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_{2,3}+1$ としてまとめることができる. さらに, (II) の $(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_2+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1\ )$ は $e_2 \leq e_3$ のとき (I) に含まれる $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ と同値である.

以上より, 上記の (I), (II) をまとめると以下に示す $l_{e/b}EL-m_{e/b}ED$ 符号の必要十分条件を得る.

$$\gamma^b_{e_2+e_{2,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1) \text{ or}$$
$$\gamma^{e_{2,3}}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } D_{e_{2,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_{2,3}+1 \text{ or}$$
$$(\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ if } e_2 \leq e_3\ ) \text{ or}$$
$$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge \gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ if } e_2 > e_3)$$

(Q.E.D.)

### 6.4.4　誤り訂正・位置指摘・検出符号

**定理 6.8** 誤り訂正・位置指摘・検出符号 $t_{e_1/b}EC-l_{e_2/b}EL-m_{e_3/b}ED$ 符号の必要十分条件は任意の異なる 2 符号語 $\boldsymbol{x},\boldsymbol{y}$ に対して以下の関係が成立することである.

(I) $e_1 \leq e_2 \leq e_3$ のとき

$$\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$$
$$\{\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge (\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)\} \text{ or}$$
$$D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$$

(II) $e_1 \leq e_3 < e_2$ のとき

$$\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or}$$
$$\{\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge$$
$$(\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1)\} \text{ or}$$
$$\{D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1 \wedge (\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)\} \text{ or}$$
$$D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1$$

(III) $e_2 < e_1 \leq e_3$ のとき

$$\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or } \gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or}$$
$$\{(\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1\ ) \wedge$$
$$(\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or } \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0\ )\} \text{ or}$$
$$D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1$$

(IV) $e_2 \leq e_3 < e_1$ のとき

$$\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge (\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1\ \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1)\} \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge (\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or}$$
$$\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or } \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)\} \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1 \wedge (\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1 \text{ or}$$
$$\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1 \text{ or } \gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)\}$$

(V) $e_3 < e_1 \leq e_2$ のとき

$$\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or}$$
$$\{\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge$$
$$(\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1)\} \text{ or}$$
$$\{D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge$$
$$(\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \text{ or } D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1)\}$$

(VI) $e_3 < e_2 < e_1$ のとき

$$\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge (\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0)\} \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge$$
$$(\gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1)\} \text{ or}$$
$$[D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \{(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ or}$$
$$(\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1)\}] \text{ or}$$
$$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge$$
$$(\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)\} \text{ or}$$
$$(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1) \text{ or}$$
$$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge$$
$$(\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)\} \text{ or}$$
$$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1\ )$$

**(証明)**

この符号の条件は以下の 6 条件が全て成立することと同値である.

1. $t$ 個以下の $e_1/b$ 誤りが訂正可能である
2. $l$ 個以下の $e_2/b$ 誤りが位置指摘可能である
3. $m$ 個以下の $e_3/b$ 誤りが検出可能である
4. 誤りの訂正と検出が区別して実行可能である
5. 誤りの訂正と位置指摘が区別して実行可能である
6. 誤りの位置指摘と検出が区別して実行可能である

定理 6.2, 6.4, 6.3 および補題 6.4, 6.5, 6.6 より上記 6 条件は以下のそれぞれ以下の条件と同値である.

1. $\gamma^b_{2e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1$
2. $\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1$
3. $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq me_3+1$
4. $\gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ or $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_1+1$ $\wedge\ D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_3+1)$
5. $\gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1$ or $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1$ $\wedge\ D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_2+1)$
6. $\gamma_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1$ or $\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ or $(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge$ $\gamma^{e_3}_1(\boldsymbol{x},\boldsymbol{y}) = 0)$ or $(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_2+1 \wedge D_{e_3}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_3+1)$

上記 6 条件より定理に示した符号条件が得られる. (Q.E.D.)

本節において示した距離構造のうち $t_{e_1/b}EC-l_{e_2/b}EL-m_{e_3/b}ED$ 符号の距離構造以外をまとめて表 6.1 に示す.

表 6.1: 誤り制御符号の距離構造

| | |
|---|---|
| $t_{e/b}EC$ 符号 | $\gamma^b_{2e+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2te+1$ |
| $l_{e/b}EL$ 符号 | $\gamma^b_{2e+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^e_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or $D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2le+1$ |
| $m_{e/b}ED$ 符号 | $\gamma^b_{e+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_e(\boldsymbol{x},\boldsymbol{y}) \geq me+1$ |
| $t_{e_1/b}EC - m_{e_3/b}ED$ 符号 | $\gamma^b_{e_1+e_{1,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1)$ or<br>$D_{e_{1,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)e_{1,3}+1$ or<br>$(\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ if $e_1 \leq e_3)^*$or<br>$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ if $e_1 > e_3)$ |
| $t_{e_1/b}EC - l_{e_2/b}EL$ 符号 | $\gamma^b_{2e_{1,2}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge \gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0)$ or<br>$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1\ )$ or<br>$(\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ if $e_1 \leq e_2)$ or<br>$(D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_1+e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ if $e_1 > e_2)$ or<br>$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq 2te_1+1 \wedge \gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq t+1 \wedge$<br>$(\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1)$ if $e_1 > e_2\ \}$ or<br>$\{D_{e_1}(\boldsymbol{x},\boldsymbol{y}) \geq (t+l)e_1+1 \wedge (\gamma^b_{2e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma^{e_2}_1(\boldsymbol{x},\boldsymbol{y}) = 0)$<br>if $e_1 > e_2\ \}$ |
| $l_{e_2/b}EL - m_{e_3/b}ED$ 符号 | $\gamma^b_{e_2+e_{2,3}+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_1+1 \wedge \gamma^b_{e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq l+1)$ or $\gamma^{e_{2,3}}_1(\boldsymbol{x},\boldsymbol{y}) = 0$ or<br>$D_{e_{2,3}}(\boldsymbol{x},\boldsymbol{y}) \geq (l+m)e_{2,3}+1$ or<br>$(\gamma^b_{e_2+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ if $e_2 \leq e_3\ )$ or<br>$(D_{e_2}(\boldsymbol{x},\boldsymbol{y}) \geq 2le_2+1 \wedge \gamma^b_{e_2+e_3+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1$ if $e_2 > e_3)$ |

∗ $e_1 \leq e_3$ が成立する場合に限って $\gamma^b_{e_1+1}(\boldsymbol{x},\boldsymbol{y}) \geq m+1$ が成立することを表している

## 6.5　位置指摘符号と訂正・検出符号における距離構造の関係

定理 6.2 と定理 6.4 を比較すると, 訂正符号 $t_{e/b}EC$ 符号と 位置指摘符号 $l_{e/b}EL$ 符号の相違点は後者の必要十分条件に $\gamma_1^e(\boldsymbol{x},\boldsymbol{y})=0$ が含まれている点であることが分かる. したがって, 位置指摘符号の方が $\gamma_1^e(\boldsymbol{x},\boldsymbol{y})=0$ の分だけ訂正符号よりも符号語数が多くなる. これと同様のことが誤り制御機能を組み合わせた符号に対してもいえる. すなわち, 定理 6.5 と 定理 6.7 を比較すると, $l_{e_2/b}EL-m_{e_3/b}ED$ 符号の条件と, $t_{e_1/b}EC-m_{e_3/b}ED$ 符号の条件の相違点は前者に $\gamma_1^{e_{2,3}}(\boldsymbol{x},\boldsymbol{y})=0$ が含まれる点である.

ここで, $e$ の値が増加して $b$ の値に近づくと $\gamma_1^e(\boldsymbol{x},\boldsymbol{y})=0$ が成立する場合が少なくなる. そのため, 位置指摘符号符号語数は 訂正符号のそれに近づく. あるベクトル $\boldsymbol{x}$ の第 $i$ バイトを $\boldsymbol{x}_i$ とすると $d_H(\boldsymbol{x}_i,\boldsymbol{y}_i)\geq e+1$ を満たす 長さ $b$ ビットのベクトル $\boldsymbol{y}_i$ の個数は

$$\sum_{i=e+1}^{b}\binom{b}{i}$$

で与えられる. この値は $e$ の値が $b$ に近づくと急速に減少するので, $e$ の値が $b$ に近づくと位置指摘符号は訂正符号に急速に近づくといえる.

特に, $e=b$ となったときは位置指摘符号と訂正符号の条件は完全に一致する. それを以下の定理に示す. この定理は定理 2.2 を一般化したものである.

**定理 6.9**　$e=b$ が成立するとき, $l_{e/b}EL$ 符号は $l_{e/b}EC$ 符号に一致する.

**(証明)**

$e=b$ のとき, 任意の互いに異なるベクトルに対して $\gamma_{2e+1}^b(\boldsymbol{x},\boldsymbol{y})=0$, $\gamma_1^e(\boldsymbol{x},\boldsymbol{y})\geq 1$ が成立するので, 定理 6.4 に示した $l_{e/b}EL$ 符号の条件は以下のようになる.

$$D_e(\boldsymbol{x},\boldsymbol{y})\geq 2le+1$$

これは定理 6.2 に示した $l_{e/b}EC$ 符号の条件の $e=b$ の場合と一致する. ゆえに, $e=b$ が成立するとき, $l_{e/b}EL$ 符号は $l_{e/b}EC$ 符号に一致する.　(Q.E.D.)

次に, 誤り位置指摘符号と誤り検出符号の関係を調べる.

定理 6.3 と定理 6.4 を比較すると, 前者に含まれる条件 $\gamma_1^e(\boldsymbol{x},\boldsymbol{y})=0$ が成立するとき, 後者に含まれる条件 $\gamma_{e+1}^b(\boldsymbol{x},\boldsymbol{y})\geq 1$ が成立する. 逆はバイト数が 1 のとき常に成立する. バイト数が 1 のとき, バイト長 $b$ は符号長に一致する. このとき, $l_{e/b}EL$ 符号, $m_{e/b}ED$ 符号の条件はそれぞれ上記の条件のみになる. ゆえに, 以下の定理が成立する.

**定理 6.10**　バイト長 $b$ が符号長に一致するとき, $l_{e/b}EL$ 符号は $l_{e/b}ED$ 符号に一致する.

**(証明)**

バイト長 $b$ が符号長に一致するとき, $l_{e/b}EL$ 符号の条件は定理 6.4 より以下のようになる.

$$\gamma_1^e(\boldsymbol{x}, \boldsymbol{y}) = 0 \tag{6-4}$$

またこのとき, $m_{e/b}ED$ 符号の条件は定理 6.3 より以下のようになる.

$$\gamma_{e+1}^b(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \tag{6-5}$$

バイト長 $b$ が符号長に一致するときは明らかにバイト数は 1 である. このとき, 式 (6-4), (6-5) に示した条件は同値である. ゆえに, このとき $l_{e/b}EL$ 符号は $l_{e/b}ED$ 符号に一致する.　(Q.E.D.)

定理 6.9, 6.10 より, 誤り位置指摘符号は誤り訂正符号と誤り検出符号を特殊形として含むということができる.

## 6.6　既存の符号の距離構造

第 6.3 節, 第 6.4 節に示した距離構造中のパラメータ $e_1, e_2, e_3, t, l, m$ へ数値を代入することにより従来から距離構造が明らかである誤り制御符号の距離構造が導出可能であり, その距離構造は従来のものと一致する. その例を本節の (1) から (4) に示す. また, 本章に示した距離構造より従来距離構造が明確でなかった誤り制御符号の距離構造も導出可能である. その例を本節の (5) から (11) に示す.

### (1) 単一ビット誤り訂正符号

定理 6.2 に示した条件に $t = 1, e = 1$ を代入すると以下に示す 単一ビット誤り訂正符号 ($SEC$ 符号) の条件を得る.

$$D_1(\boldsymbol{x}, \boldsymbol{y}) \geq 3$$

上記の $D_1(\boldsymbol{x}, \boldsymbol{y})$ が $\boldsymbol{x}, \boldsymbol{y}$ のハミング距離を表すのは明らかであるので, 上記条件は異なる任意の 2 符号語間のハミング距離が 3 以上という既知の条件と同値である.

### (2) 二重ビット誤り検出符号

定理 6.3 に示した条件に $t = 1, e = 2$ を代入すると以下に示す $S_{2/b}ED$ 符号の条件を得る.

$$\gamma_3^b(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } D_2(\boldsymbol{x}, \boldsymbol{y}) \geq 3$$

また, 同条件に $t = 2, e = 1$ を代入すると以下に示す $D_{1/b}ED$ 符号の条件を得る.

$$\gamma_2^b(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } D_1(\boldsymbol{x}, \boldsymbol{y}) \geq 3$$

上記 2 条件の論理積をとると以下に示す 二重ビット誤り検出符号 ($DED$ 符号) の条件を得る.

$$D_1(\boldsymbol{x}, \boldsymbol{y}) \geq 3$$

本条件も既知の条件と一致する.

### (3) 単一ビット誤り訂正・二重ビット誤り検出符号

定理 6.5 に示した条件に $t = m = 1, e_1 = 1, e_3 = 2$ を代入すると以下に示す $S_{1/b}EC - S_{2/b}ED$ 符号の条件を得る.

$$\gamma_2^b(\boldsymbol{x}, \boldsymbol{y}) \geq 2 \text{ or } D_2(\boldsymbol{x}, \boldsymbol{y}) \geq 5 \text{ or } \gamma_4^b(\boldsymbol{x}, \boldsymbol{y}) \geq 1$$

また, 同条件に $t = 1, m = 2, e_1 = e_3 = 1$ を代入すると以下に示す $S_{1/b}EC - D_{1/b}ED$ 符号の条件を得る.

$$\gamma_3^b(\boldsymbol{x}, \boldsymbol{y}) \geq 1 \text{ or } D_1(\boldsymbol{x}, \boldsymbol{y}) \geq 4$$

上記 2 条件の論理積をとると以下に示す単一ビット誤り訂正・二重ビット誤り検出符号 ($SEC-DED$ 符号) の条件を得る.

$$D_1(\boldsymbol{x}, \boldsymbol{y}) \geq 4$$

本条件も既知の条件と一致する.

### (4)$t$ バイト誤り訂正・$m$ バイト誤り検出符号

定理 6.5 に示した条件に $e_1 = e_3 = b$ を代入すると以下に示す $t$ バイト誤り訂正・$m$ バイト誤り検出符号 ($t_bEC - m_bED$ 符号) の条件を得る.

$$D_b(\boldsymbol{x}, \boldsymbol{y}) \geq (t + m)b + 1$$

上記条件は, 符号語を $\mathrm{GF}(2^b)$ 上のベクトルと見たときのハミング距離が $(t + m + 1)$ 以上であることを表しているので, 本条件は既知の条件と一致する.

### (5) 単一ビット誤り訂正・単一バイト誤り検出符号

定理 6.5 に示した条件に $t=m=1, e_1=1, e_3=b$ を代入すると, 以下に示す単一ビット誤り訂正・単一バイト誤り検出符号 ($SEC-S_bED$ 符号) の条件を得る.

$$\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \text{ or } D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1$$

### (6) 単一ビット誤り訂正・二重ビット誤り検出・単一バイト誤り検出符号

上記の $SEC-DED$ 符号と $SEC-S_bED$ 符号の条件の論理積をとると以下に示す単一ビット誤り訂正・二重ビット誤り検出・単一バイト誤り検出符号 ($SEC-DED-S_bED$) 符号の条件を得る.

$$\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \text{ or } (D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1 \wedge \gamma_3^b(\boldsymbol{x},\boldsymbol{y}) \geq 1) \text{ or } (D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1 \wedge D_1(\boldsymbol{x},\boldsymbol{y}) \geq 4)$$

### (7) 単一バイト誤り訂正・二重ビット誤り検出符号

定理 6.5 に示した条件より単一バイト誤り訂正・二重ビット誤り検出符号 ($S_bEC-DED$ 符号)[13] の条件が得られる. 明らかに $S_bEC-S_{2/b}ED$ 符号は $S_bEC$ 符号と同値であるので, $S_bEC-DED$ 符号は $S_bEC-D_{1/b}ED$ 符号と同値である. したがって, 上記条件に $t=1, m=2, e_1=e_3=1$ を代入すると以下に示す $S_bEC-DED$ 符号の条件を得る.

$$D_b(\boldsymbol{x},\boldsymbol{y}) \geq 3b+1 \text{ or } (\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \wedge D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1)$$

### (8) 単一ビット誤り訂正・単一 $b$ ビットバイト中 $e$ ビット誤り位置指摘符号

定理 6.6 に示した条件に $t=l=1, e_1=1, e_2=e$ を代入すると, 第 4 章で扱った $SEC-S_{e/b}EL$ 符号の条件を得る. 以下にその条件を示す.

$$\gamma_{2e+1}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (\gamma_{e+2}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \wedge\ \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ or}$$
$$(\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \text{ or } \wedge\ \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ or } D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1$$

### (9) 単一ビット誤り訂正・単一 $b$ ビットバイト中 $e$ ビット誤り位置指摘・二重ビット誤り検出符号

定理 6.8 に示した条件に $t=l=m=1, e_1=1, e_2=e, e_3=2$ を代入すると以下に示す $SEC-S_{e/b}EL-S_{2/b}ED$ 符号の条件を得る.

$$\gamma_{2e+1}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } (\gamma_{e+2}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \wedge\ \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ or}$$
$$(\gamma_{e+1}^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \text{ or } \wedge\ \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0) \text{ or } D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1$$

また, 同条件に $t=l=1, m=2, e_1=1, e_2=e, e_3=1$ を代入すると以下に示す $SEC-S_{e/b}EL-D_{1/b}ED$ 符号の条件を得る.

$$\begin{aligned}&\gamma^b_{2e+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_e(\boldsymbol{x},\boldsymbol{y}) \geq 3e+1 \text{ or}\\&\{\ D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1 \wedge (\gamma^b_{e+2}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^e_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } \gamma^b_2(\boldsymbol{x},\boldsymbol{y}) \geq 2\ )\ \}\end{aligned}$$

上記 2 条件の論理積をとることにより以下に示す $SEC-S_{e/b}EL-DED$ 符号の条件を得る. 本符号は 第 4 章で扱った符号に 2 ビット誤り検出機能を付加した符号である.

$$\begin{aligned}&\gamma^b_{2e+1}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } D_e(\boldsymbol{x},\boldsymbol{y}) \geq 3e+1 \text{ or}\\&\{\ D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1 \wedge (\gamma^b_{e+2}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^e_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } \gamma^b_2(\boldsymbol{x},\boldsymbol{y}) \geq 2\ )\ \}\end{aligned}$$

### (10) 単一 $p \times b$ ビットブロック中 1 バイト誤り位置指摘符号

符号語を $GF(2^b)$ 上のベクトルと考えると第 3.4 節に示した $S_{b/p\times b}EL$ 符号は $S_{1/p}EL$ 符号となる. そこで, 定理 6.4 に示した条件に $m=1, e=1$ を代入すると以下に示す $S_{b/p\times b}EL$ 符号 の条件を得る.

$$\gamma^p_3(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^1_1(\boldsymbol{x},\boldsymbol{y}) = 0 \text{ or } D_p(\boldsymbol{x},\boldsymbol{y}) \geq 2p+1$$

ただし, 上記の $\gamma^p_3(\boldsymbol{x},\boldsymbol{y}), \gamma^1_1(\boldsymbol{x},\boldsymbol{y}), D_p(\boldsymbol{x},\boldsymbol{y})$ は符号語を $GF(2^b)$ 上のベクトルとして計算する.

### (11) 単一バイト誤り訂正・単一 $p \times b$ ビットブロック中 $i$ バイト誤り検出符号

符号語を $GF(2^b)$ 上のベクトルと考えると単一バイト誤り訂正・単一 $p \times b$ ビットブロック中 $i$ バイト誤り検出符号 ($S_bEC-S_{i\times b/p\times b}ED$ 符号)[28] は $SEC-S_{i/p}ED$ 符号となる. そこで, 定理 6.5 に示した条件に $t=m=1, e_1=1, e_3=i$ を代入すると以下に示す $S_bEC-S_{i\times b/p\times b}ED$ 符号 の条件を得る.

$$\gamma^p_{i+2}(\boldsymbol{x},\boldsymbol{y}) \geq 1 \text{ or } \gamma^p_{i+1}(\boldsymbol{x},\boldsymbol{y}) \geq 2 \text{ or } D_p(\boldsymbol{x},\boldsymbol{y}) \geq 2p+1$$

ただし, 上記の $\gamma^p_{i+2}(\boldsymbol{x},\boldsymbol{y}), \gamma^p_{i+1}(\boldsymbol{x},\boldsymbol{y}), D_p(\boldsymbol{x},\boldsymbol{y})$ は符号語を $GF(2^b)$ 上のベクトルとして計算する.

本節において示した既存の符号の距離構造をまとめて表 6.2 に示す.

## 6.7 結言

本章では誤り位置指摘符号の距離構造を明らかにするため距離を定義し, それを用いて $e/b$ 誤りを制御する符号の必要十分条件を導出した. 本章において得られた結果は以下の通りである.

表 6.2: 既存の符号の距離構造

| 符号 | 符号条件 | $t$ | $l$ | $m$ | $e_1$ | $e_2$ | $e_3$ |
|---|---|---|---|---|---|---|---|
| $SEC$ 符号 | $D_1(\boldsymbol{x},\boldsymbol{y}) \geq 3$ | 1 | - | - | 1 | - | - |
| $DED$ 符号 | $D_1(\boldsymbol{x},\boldsymbol{y}) \geq 3$ | - | - | 1<br>2 | - | - | 2†<br>1 |
| $SEC-DED$ 符号 | $D_1(\boldsymbol{x},\boldsymbol{y}) \geq 4$ | 1 | - | 1<br>2 | 1 | - | 2<br>1 |
| $t_bEC-m_bED$ 符号 | $D_b(\boldsymbol{x},\boldsymbol{y}) \geq (t+m)b+1$ | $t$ | - | $m$ | $b$ | - | $b$ |
| $SEC-S_bED$ 符号 | $\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2$ or $D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1$ | 1 | - | 1 | 1 | - | $b$ |
| $SEC-DED-S_bED$ 符号 | $\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2$ or<br>$(D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1 \wedge \gamma_3^b(\boldsymbol{x},\boldsymbol{y}) \geq 1)$ or<br>$(D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1 \wedge D_1(\boldsymbol{x},\boldsymbol{y}) \geq 4)$ | 1 | - | 1<br>2<br>1 | 1 | - | 2<br>1<br>$b$ |
| $S_bEC-DED$ 符号 | $D_b(\boldsymbol{x},\boldsymbol{y}) \geq 3b+1$ or<br>$(\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \wedge D_b(\boldsymbol{x},\boldsymbol{y}) \geq 2b+1)$ | 1 | - | 2 | 1 | - | 1 |
| $SEC-S_{e/b}EL$ 符号 | $\gamma_{2e+1}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$(\gamma_{e+2}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1 \wedge \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0)$ or<br>$(\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2 \wedge \gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0)$ or<br>$D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1$ | 1 | 1 | - | 1 | $e$ | - |
| $SEC-S_{e/b}EL-DED$ 符号 | $\gamma_{2e+1}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$D_e(\boldsymbol{x},\boldsymbol{y}) \geq 3e+1$ or<br>$\{D_e(\boldsymbol{x},\boldsymbol{y}) \geq 2e+1 \wedge (\gamma_{e+2}^b(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or<br>$\gamma_1^e(\boldsymbol{x},\boldsymbol{y}) = 0$ or $\gamma_2^b(\boldsymbol{x},\boldsymbol{y}) \geq 2)\}$ | 1 | 1 | 1<br>2 | 1 | $e$ | 2<br>1 |
| $S_{b/p\times b}EL$ 符号 | $\gamma_3^p(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma_1^1(\boldsymbol{x},\boldsymbol{y}) = 0$ or<br>$D_p(\boldsymbol{x},\boldsymbol{y}) \geq 2p+1$ | - | 1 | - | - | 1 | - |
| $S_bEC-S_{i\times b/p\times b}ED$ 符号 | $\gamma_{i+2}^p(\boldsymbol{x},\boldsymbol{y}) \geq 1$ or $\gamma_{i+1}^p(\boldsymbol{x},\boldsymbol{y}) \geq 2$ or<br>$D_i(\boldsymbol{x},\boldsymbol{y}) \geq 2i+1$ | 1 | - | 1 | 1 | - | $i$ |

† $m = 1, e_3 = 2$ を代入して得られる条件と $m = 2, e_3 = 1$ を代入して得られる条件の論理積をとることによって得られた条件であることを意味している

(1) 符号語間の距離を両者が一致するために必要な $e/b$ 誤りの個数の $e$ 倍として定義した. 2 符号語における対応したバイトのハミング距離が所定の範囲となるバイトの個数を符号語に関する関数として定義した. これらを利用して誤り訂正符号, 位置指摘符号, 検出符号およびそれらを組み合わせた符号の符号条件を導出した.

(2) 得られた符号条件より誤り位置指摘符号は $e$ の値をバイト長 $b$ に一致させると誤り位置指摘符号は誤り訂正符号に一致し, バイト長 $b$ を符号長に一致させると誤り位置指摘符号は 誤り検出符号に一致することを示した. すなわち, 誤り位置指摘符号が誤り訂正符号, 検出符号を特殊形として含むことを示した.

(3) 得られた条件式中の $e$ の値や制御する $e/b$ 誤りの個数に具体的な数値を代入して既存の符号の条件を導出した. この結果は, 従来のものと一致する結果であり, 従来距離構造がこれまで明らかでなかったビット誤り・バイト誤りを複合的に制御する符号についても符号条件を示した.

# 第7章　結論

## 7.1　本研究により得られた成果

本論文では 誤り訂正と検出の中間的な機能を有する誤り位置指摘に注目し, 半導体メモリシステムに有効であると考えられる 2 種類の誤り位置指摘符号を提案した. さらに, 誤り位置指摘符号の距離構造を導出して誤り訂正符号, 検出符号との関係を明らかにした.

得られた結果については各章の結言に述べたが, さらにまとめると以下のようになる.

(1) 誤り位置指摘符号に関する従来の研究を紹介し, 誤り位置指摘符号の具体的構成法の提案が少ないこと, および誤り位置指摘機能と誤り訂正, 検出機能に関する理論的な関係が明らかになっていないことを示した.

(2) バイト出力素子を搭載したメモリカードの出力をブロックと定義し, このブロック単位で位置指摘を行なう新しい位置指摘のモデルを提案した.

(3) 半導体メモリシステムに生じる故障とそれによって生じる誤りの傾向を考慮し, メモリシステムではビット誤りとバイト誤りの両者を制御する必要があることを示した. これらの統一的に扱うために大きさ $b$ ビットのバイト中に生じた $e$ $(1 \leq e \leq b)$ ビット以下の誤りを $e/b$ 誤りと定義した. この誤りはビット誤り, バイト誤りをそれぞれ $e = 1, b$ の場合として含み, ビット誤りとバイト誤りの両者を制御する符号は $e$ の値が異なる複数の $e/b$ 誤りを制御する符号として扱うことができる

(4) 最も基本的なブロック誤り位置指摘機能を有する符号として故障バイト素子を含むメモリカードを位置指摘する符号を提案し, その構成法および復号法を示した.

(5) 単一ビット誤りを訂正し, 故障バイト素子の位置を指摘する符号を提案した.

  (i) 単一バイト誤り訂正符号の検査行列と単一ビット誤り訂正・$e$ ビット誤り検出符号の検査行列のテンソル積を用いる構成法を提案した.

  (ii) 符号評価の結果, 本構成法によって構成した符号の多くが限界検査ビット長に近い検査ビット長を有することを確認した. 特に, $e$ の値が小さい場合と情報長が大きい場合に検査ビット長が下界に近くなる.

(iii) $e, b$ の値がそれぞれ 2, 4 である符号に対し符号評価を行なった．復号回路量は $SEC-DED$ 符号に比べて約 47.4 % 増加する．ランダム二重ビット誤り, 二重バイト誤りといった誤り制御機能を越えた誤りに対して約 50 % の確率で検出または正しい位置指摘が実行可能である．

(6) 単一ビット誤りを訂正し, 故障バイト素子を含むメモリカードを指摘する符号を提案した．

(i) 単一バイト誤り訂正符号の検査行列と単一ビット誤り訂正・単一バイト誤り検出符号の検査行列のテンソル積を用いた構成法と奇数重み列, 偶数重み列を有する 2 種類の $b \times b$ の正方行列を要素とする検査行列を用いる構成法の 2 種類の構成法を提案した．

(ii) 符号評価を行なった．バイト長 4, ブロック長 32 の符号はランダム二重ビット誤り, 二重バイト誤りといった誤り制御機能を越えた誤りに対してもおよそ 50% の確率で位置指摘または検出が可能である．バイト長 4, ブロック長 16 の符号の復号回路量は $SEC-DED$ 符号に比べて約 15 % 増加する．

(7) 誤り位置指摘符号の距離構造を明らかにするため, $e/b$ 誤りを制御する符号の必要十分条件を距離を用いて表現した．

(i) 符号語間の距離を一方が他方に一致するために必要な $e/b$ 誤りの個数の $e$ 倍として定義し, 符号語に関する関数を 2 符号語における対応したバイトのハミング距離が所定の範囲となるバイトの個数として定義した．これらを用いて誤り位置指摘符号, 訂正符号, 検出符号, さらにこれらを組み合わせた機能を有する符号の必要十分条件を導出した．

(ii) 得られた符号条件より, 誤り位置指摘符号と誤り訂正符号, 誤り検出符号の関係を明らかにした．位置指摘可能なバイト誤りの最大ビット数 $e$ をバイト長 $b$ に一致させると誤り位置指摘符号は誤り訂正符号に一致する．また, 誤り位置指摘符号におけるバイト長 $b$ を符号長に一致させると誤り位置指摘符号は 誤り検出符号に一致する．すなわち, 誤り位置指摘符号は誤り訂正・検出符号を特殊形として含む．

(iii) 本章で得られた距離構造を従来から距離構造が明らかになっている符号に適用すると従来のものと一致する結果を得る．さらに, 本章で得られた距離構造により距離構造がこれまで明らかでなかったビット誤り・バイト誤りを複合的に制御する符号の距離構造も導出可能である．

## 7.2　今後の課題

本論文では第 3, 4 ,5 章で 3 種類の誤り位置指摘符号を提案したが, これ以外にも誤り位置指摘符号は存在する．そこで, これらの符号の構成法を検討することが今後の課題である．一方, 本論文で提案した誤り位置指摘符号の構成法の多くはテンソル積を用いた構成法であるが, この構成

法に基づく符号は情報長が大きくならないと検査長が下界に近づかない．例えば, 第 5 章に示した $SEC-S_{4/15\times4}EL$ 符号をテンソル積で構成すると, 検査長と下界の差が 1 ビット以内になるのは情報長が 2,000 ビット以上のときである．さらに第 4 章に示した $SEC-S_{e/b}EL$ 符号では $e$ の値に制限がある．そこで, 今後新たな符号の構成法を検討する際には, テンソル積に代わる一般的な誤り位置指摘符号の構成法を追求する必要がある.

本論文の第 6 章で距離構造を考察した符号では同時に生起する誤りは 1 種類であると仮定している．例えば, $t_{e_1/b}EC-l_{e_2/b}EL$ 符号は $e_1/b$ 誤りと $e_2/b$ 誤りをそれぞれ訂正, 位置指摘する符号であるが, $e_1/b$ 誤りと $e_2/b$ 誤りが同時に生起することは仮定していない．しかし, 現実の誤りモデルとしてはビット誤りとバイト誤りが同時に生起するを仮定することも十分あり得る．実際, $S_bEC-(S+S_b)ED$ 符号は固定故障による単一バイト誤りと一時故障による単一ビット誤りが同時に生じたときにその誤りを検出する符号として提案されている．そこで今後は異なる種類の誤りが同時に生じた場合に訂正, 位置指摘, 検出する符号の距離構造について考える必要がある.

本論文では対称誤りを制御する符号のみを扱ってきた．しかし, 単方向誤り, 非対称誤りといった誤りも存在し, 研究の対象となっている．そこで, これらの誤りが混在した誤りを制御する符号について, 第 6 章と同様に距離を用いた必要十分条件を導出し, これらの誤りの理論的な関係を明らかにすることも今後の課題である.

# 謝辞

本研究の全般に渡って 御指導, 御助言を頂いた 藤原 英二 教授に心より感謝致します. 本研究を進める上で大変参考になる誤り識別符号を紹介して頂いた 坂庭 好一 教授に心より感謝致します. また, 有益な御助言を頂いた 南谷 崇 教授, 荒木 純道 教授, 山田 功 助教授に深く感謝致します.

第 6 章の内容に関して貴重なコメントをいただいた 大学院 博士課程の蒋 曙新 さんに感謝いたします. さらに, 様々な御協力をいただいた藤原研究室の皆様に感謝します.

# 参考文献

[1] 当麻 喜弘 (編著) : “フォールトトレラントシステム論,” 電子情報通信学会, 1990.

[2] T. R. N. Rao and E. Fujiwara, *Error-control coding for computer systems,* Prentice-Hall,1989.

[3] 藤原, 岩垂 : “符号理論の FTC 技術への応用,” 信学論 (A), vol. J73-A No. 2, pp. 237-242, 1990.

[4] C. E. Shannon, “A Mathematical Theory of Communication,” *Bell System Technical Journal*, vol. 27, pp. 379–423, pp. 623–656, July, October, 1948.

[5] R. W. Hamming, “Error Detecting and Error Correcting Codes,” *Bell System Technical Journal*, vol. 29, pp. 147–160, April, 1950.

[6] M. Y. Hsiao, “A Class of Optimal Minimum Odd-Weight-Column SEC-DED Codes,” *IBM J. Res.* Dev. 14, pp. 395–401, July 1970.

[7] S. J. Hong and A. M. Patel, “A General Class of Maximal Codes for Computer Applications.” *IEEE Trans. Comput.*, vol. C-21, pp. 1322-31, December, 1972.

[8] I. S. Reed and G. Solomon, “Polynomial Codes over Certain Finite Fields,” *Journal Soc. Ind. Appl. Math.*, vol. 8, pp. 300-304, June, 1960.

[9] S. Kanada and E. Fujiwara, “Single Byte Error Correcting-Double Byte Error Detecting codes,” *IEEE Trans. Comput.*, vol. C-31, pp. 596-602, July, 1982.

[10] D. C. Bossen, L. C. Chang, and C. L. Chen, “Measurement and Generation of Error Correcting Code for Package Failures.” *IEEE Trans. Comput.*, vol. C-27, pp. 201-204, March, 1978.

[11] S. Kaneda, “A Class of Odd-Weight-Column SEC-DED-S$b$ED Codes for Memory System Applications,” *IEEE Trans. Comput.*, vol. C-33, pp. 737-739, August, 1984.

[12] L. A. Dunning, “SEC-BED-DED Codes for Error Control in Byte-Organized Memory System.” *IEEE Trans. Comput.*, vol. C-34, pp. 557-562, June, 1985.

[13] E. Fujiwara and M. Hamada, “Single $b$-Bit Byte Error Correcting and Double Bit Error Detecting Codes for High-Speed Memory Systems,” *IEICE Trans. Fundamentals*, vol. E76-A, pp. 1442-1448, September, 1993.

[14] M. Hamada and E. Fujiwara, “A Class of Error Control Codes for Byte Organized Memory Systems – S$b$EC-(S$b$+S)ED Codes –,” *to appear in IEEE Trans. Computers.*

[15] J. K. Wolf and B. Elspas, “Error-Locating Codes – A New Concept in Error Control,” *IEEE Trans. Inf. Theory*, vol. IT-9, pp. 113–117, April, 1963.

[16] J. K. Wolf, “On Codes Derivable from the Tensor Product of Check Matrices,” *IEEE Trans. Inf. Theory*, vol. IT-11, pp. 281–284, April, 1965.

[17] J. K. Wolf, “On an Extended Class of Error-Locating Codes,” *Inf. & Control*, vol. 8, pp. 163-169, 1965.

[18] S. -H. Chang and L. -J. Weng, “Error Locating Codes,” *IEEE Int. Conv. Rec.*, Part 7, pp. 252–258, 1965.

[19] J. M. Goethals, “Cyclic Error-Locating Codes,” *Inf. Control*, vol. 10, pp. 378-385, 1967.

[20] V. L. Geurkov and V. N. Dyn’kin, “Diagnosis of Digital Devices Using Error-Locating Codes,” *Automation and Remote Control*, vol. 50, Iss. 10, pp. 1428-1436 (October 1989). (Translated from Avtomatica i Telemekhanika, No. 10, pp. 148-159, October, 1989.)

[21] N. H. Vaidya and D. K. Pradhan, “A New Class of Bit- and Byte Error Control Codes,” *IEEE Trans. Inf. Theory*, vol.IT-38, pp.1617–1623, September, 1992.

[22] 杜, 坂庭 : “多値誤り識別符号に関する一考察,” 第 12 回情報理論とその応用に関するシンポジウム (SITA ’89) 予稿集, pp.121–125, December 6-9, 1989, Inuyama, Japan.

[23] L. -P. To, “Theory and Construction of $m$-ary Error Descriminating Codes,” 東京工業大学 大学院 電気電子工学専攻 修士論文, 1990.

[24] 坂庭, 杜 : “整数環上で構成される各種多値誤り訂正／検出符号の必要十分条件,” 信学技報, IT90-15, 1990.

[25] H. Imai and H. Fujiya “Generalized Tensor Product Codes,” *IEEE Trans. Inf. Theory*, vol.IT-27, pp.181–187, March, 1981.

[26] 永井 剛 : “バイト誤り位置指摘符号の研究,” 東京工業大学 電気電子工学科 卒業論文, 1992.

[27] F.J.McWilliams and N.J.A.Sloane, *The Theory of Error-Correcting Codes,* North-Holland, 1977.

[28] 田中 雅晴 : “多ビット出力メモリ素子を用いたシステムにおける誤り制御符号の研究,” 東京工業大学大学院 情報工学専攻 修士論文, 1994.

# 本研究に関連する発表論文

- **第3章**


  - 北神, 小林, 藤原 : “バイト誤り訂正符号における並列復号法,” 信学’95 ソ大, A-114, 1995.


- **第4章**


  - 北神, 藤原 : “単一バイト誤り位置指摘機能を有する単一ビット誤り訂正符号,” 信学’94 春大, A-360, 1994.
  - M. Kitakami and E. Fujiwara, “A Class of Error Locating Codes – $SEC - S_{e/b}EL$ Codes – ,” *Proc. of ISIT-94*, pp.248, June 27 - July 1, 1994, Trondheim, Norway.
  - M. Kitakami and E. Fujiwara, “A Class of Error Locating Codes – $SEC - S_{e/b}EL$ Codes – ,” *IEICE Trans. Fundamentals*, vol.E78-A, No.9, pp.1086–1091, September, 1995.


- **第5章**


  - 北神, 藤原 : “単一ビット誤り訂正・単一バイト誤り位置指摘符号,” 信学’92 秋大, D-114, 1992.
  - M. Kitakami and E. Fujiwara, “A Class of Error Locating Codes for Memory Systems,” 信学技報, IT92-99, 1992.
  - E. Fujiwara and M. Kitakami, “A Class of Error Locating Codes for Byte-Organized Memory Systems,” *Dig. FTCS-23*, pp.110–119, June 22-24, 1993, Toulouse, France.
  - E. Fujiwara and M. Kitakami, “A Class of Error Locating Codes for Byte-Organized Memory Systems,” *IEEE Trans. Inf. Theory*, vol.IT-40, pp.1857–1865, November, 1994.


- **第6章**

– 北神, 蒋, 藤原："誤り位置指摘符号の理論的構造," 信学'96 総大, A-244, 1996.


- 関連する内容の発表


– E. Fujiwara and M. Kitakami, "A Class of Optimal Fixed-Byte Error Protection Codes for Computer Systems," *Dig. FTCS-25*, pp.310–319, June 27-30, 1995, Pasadena, Ca, USA.

– T. Ritthongpitak, E. Fujiwara, and M. Kitakami, "A Class of Optimal Fixed-Byte Error Protection Code — (S+F*b*)EC Code —," *Proc of ISIT-95*, pp.148, September 17-22, 1995, Whistler, B.C. Canada.

– 北神, 清水, T.Ritthongpitak, 藤原："SEC-DED 機能を有する最適なバイト誤り保護符号," 信学技報, IT95-14, 1995.

– 清水, 北神, 藤原："SEC-DED 機能を有する最適なバイト誤り保護符号," 信学'95 ソ大, A-113, 1995.

– E. Fujiwara and M. Kitakami, "A Class of Optimal Fixed-Byte Error Protection Codes for Computer Systems," *submitted to IEEE Trans. Inf. Theory.*

– T.Ritthongpitak, M. Kitakami, and E. Fujiwara. "Optimal Two-Level Byte Error Protection Codes for Computer Systems," *submitted to FTCS-26.*

– T.Ritthongpitak, 北神, 藤原："3 段階の保護レベルを有するバイト誤り保護符号," 信学'96 総大, A-245, 1996.