LC-005

誤りバイト数を制限したスポッティバイト誤り制御符号
A General Class of Error Control Codes for Spotty Byte Errors Occurred in a Limited Number of Bytes

鈴木 一克† 清水 護† 樫山 俊彦† 藤原 英二†
Kazuyoshi Suzuki Mamoru Shimizu Toshihiko Kashiyama Eiji Fujiwara

1. まえがき

スポッティバイト誤り制御符号は, 広い入出力幅 ($b = 8, 16$ または, 32 ビット) を有する近年の高密度 DRAM チップを搭載した半導体メモリシステムにおいて生ずる誤りを訂正/検出するのに最も適している [1, 2, 3]. スポッティバイト誤りは長さ b ビットのバイト内におけるランダムな $t(\leq b)$ ビット以下の誤りと定義され [1], m-スポッティバイト誤りはバイト内における複数のスポッティバイト誤りと定義される [3]. 半導体メモリシステムにおいて, 一般に, 誤りが生じる RAM チップは高々 2, 3 個程度である. すなわち, 符号語中の誤りを有するバイト数は高々 2, 3 程度である. これらの状況を考慮して, 本稿では, 限られた数のバイトに生じたスポッティバイト誤りのみを訂正または検出する新しい m-スポッティバイト誤り制御符号を提案する. 提案する符号は従来の m-スポッティバイト誤り制御符号および RS 符号よりも少ない検査ビット長で構成できる. また, 提案する符号の復号アルゴリズムを明らかにする.

2. m-スポッティバイト誤り制御符号

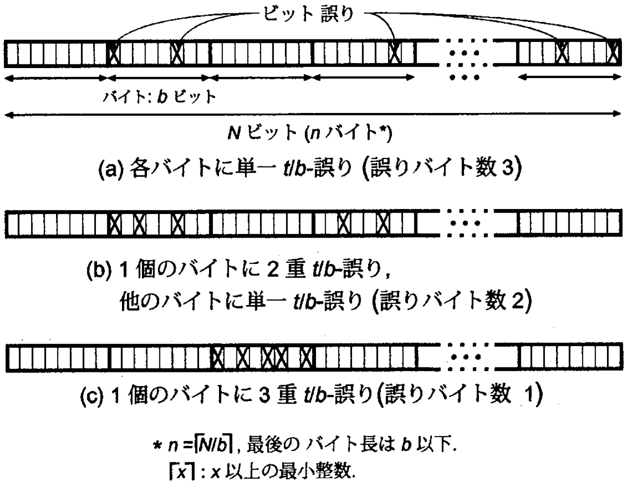
2.1 準備

定義 1 [1] b ビットからなる 1 バイトに $t(1 \leq t \leq b)$ ビット以下の誤りが存在するとき, この誤りをスポッティバイト誤り, または t/b-誤りと称する. □

図 1 は, $b = 8, t = 2$ における 3 重スポッティバイト誤りを有する語の例である. 図 1(a) では, 語中に誤りを有するバイトが 3 個あり, 各バイト内の誤りビット数の最大値は $t = 2$ を超えない. すなわち, いずれのバイトにも 1 個の t/b-誤りがある. 一方, 図 1(b) では, 二番目のバイトに 3 ビット誤りが生じている. $\lceil 3/t \rceil = \lceil 3/2 \rceil = 2$ より, これはバイト内 2 重 t/b-誤りである. ここで, 記号 $\lceil x \rceil$ は x 以上の最小整数を表す. 他の誤りバイトには 1 個の t/b-誤りがあることから, t/b-誤りの総数は 3 である. したがって, この場合も 3 重スポッティバイト誤りとする. 図 1(c) では, 誤りバイトが 1 個であり, バイト中には 5 ビットの誤りがある. $\lceil 5/t \rceil = \lceil 5/2 \rceil = 3$ より, 語中には 3 重 t/b-誤りを有する.

定義 2 [3] 記号 e を誤りベクトルとし, e_i をそのi バイト目のベクトルとする. ここで, $0 \leq i \leq n-1$ とする. 誤りベクトル e におけるスポッティバイト誤りの数 $w_{\mathrm{M}}(e)$ は次式で定義される:

$$w_{\mathrm{M}}(e) = \sum_{i=0}^{n-1} \left\lceil \frac{w_{\mathrm{H}}(e_i)}{t} \right\rceil .$$



(a) 各バイトに単一 t/b-誤り (誤りバイト数 3)

(b) 1 個のバイトに 2 重 t/b-誤り, 他のバイトに単一 t/b-誤り (誤りバイト数 2)

(c) 1 個のバイトに 3 重 t/b-誤り (誤りバイト数 1)

図 1: 3 重スポッティバイト誤り ($b = 8, t = 2$) の例.

もし $w_{\mathrm{M}}(e) = \mu$ であれば, この誤りを μ 重 m-スポッティバイト誤りと称する. ここで, $w_{\mathrm{H}}(e_i)$ は, ベクトル e_i のハミング重みを表す. □

本稿では, p_1 個以下のバイトに生じた μ_1 個以下の m-スポッティバイト誤りを訂正し, p_2 個以下のバイトに生じた μ_2 個以下の m-スポッティバイト誤りを検出する符号を $[\mu_{1\ t/b}\mathrm{EC}]_{p_1}$-$[\mu_{2\ t/b}\mathrm{ED}]_{p_2}$ 符号と表す. 特に, $\mu_1 = \mu_2 = \mu$ かつ $p_1 = p_2 = p$ のとき, p 個以下のバイトに生じた μ 個以下の m-スポッティバイト誤りを訂正する符号となる. これを $[\mu_{t/b}\mathrm{EC}]_p$ 符号と表す. また, $\mu_1 = 0$ かつ $p_1 = 0$ のとき, p_2 個以下のバイトに生じた μ_2 個以下の m-スポッティバイト誤りを検出する符号となり, $\mu_2 = \mu$, $p_2 = p$ としてこれを $[\mu_{t/b}\mathrm{ED}]_p$ 符号と表す.

定理 1 $H_i(0 \leq i \leq n-1)$ を $R \times b$ の部分行列とする. $H = [H_0 H_1 H_2 H_3 \cdots H_{n-1}]$ の零空間が線形 $[\mu_{1\ t/b}\mathrm{EC}]_{p_1}$-$[\mu_{2\ t/b}\mathrm{ED}]_{p_2}$ 符号であるための必要十分条件は式 (1) で表される. ただし, $i_1, i_2, \cdots, i_{v_1+\cdots+v_\lambda}$ $(0 \leq i_1, i_2, \cdots, i_{v_1+\cdots+v_\lambda} \leq n-1)$ は相異なり, $\lambda = \lceil b/t \rceil$ とする. また, $\min(x, y)$ は x, y のうち小さいほうの値を表し, $\lfloor \delta \rfloor$ は δ 以下の最大整数を表す.

この定理は, $p_1 + p_2$ 個以下のバイトに生じた $\mu_1 + \mu_2$ 個以下のスポッティバイト誤りのシンドローム和が 0 とならないことを示すことで証明できる.

定理 2 線形 $[\mu_{1\ t/b}\mathrm{EC}]_{p_1}$-$[\mu_{2\ t/b}\mathrm{ED}]_{p_2}$ 符号は少なくとも $(\mu_1 + \mu_2)t$ ビットの検査長を有する. □

この定理は, 定理 1 に示した必要十分条件より, 検査行列の $(\mu_1 + \mu_2)t$ 列が線形独立であることを用いて証明できる.

†東京工業大学大学院情報理工学研究科

$$\begin{aligned} &e_{i_1}\cdot H_{i_1}^T+\cdots+e_{i_{v_1}}\cdot H_{i_{v_1}}^T+e_{i_{v_1+1}}\cdot H_{i_{v_1+1}}^T+\cdots+e_{i_{v_1+v_2}}\cdot H_{i_{v_1+v_2}}^T \\ &\quad+\cdots+e_{i_{v_1+v_2+\cdots+v_{\lambda-1}+1}}\cdot H^T_{i_{v_1+v_2+\cdots+v_{\lambda-1}+1}}+\cdots+e_{i_{v_1+v_2+\cdots+v_\lambda}}\cdot H^T_{i_{v_1+v_2+\cdots+v_\lambda}}\neq 0 \qquad (1) \\ &for\ \ w_{\mathrm{M}}(e_{i_1})=\cdots=w_{\mathrm{M}}(e_{i_{v_1}})=1,\ w_{\mathrm{M}}(e_{i_{v_1+1}})=\cdots=w_{\mathrm{M}}(e_{i_{v_1+v_2}})=2, \\ &\qquad\cdots,\ w_{\mathrm{M}}(e_{i_{v_1+v_2+\cdots+v_{\lambda-1}+1}})=\cdots=w_{\mathrm{M}}(e_{i_{v_1+v_2+\cdots+v_\lambda}})=\lambda, \\ &0<\sum_{x=1}^{v_1+v_2+\cdots+v_\lambda}\le\mu_1+\mu_2,\quad 0<\sum_{x=1}^{\lambda}v_x\le p_1+p_2, \\ &0\le v_1\le p_1+p_2,\ \ 0\le v_2\le\min(\lfloor(\mu_1+\mu_2)/2\rfloor,\ p_1+p_2),\ \ \cdots,0\le v_\lambda\le\min(\lfloor(\mu_1+\mu_2)/\lambda\rfloor,\ p_1+p_2). \end{aligned}$$

定理 3 N が b の倍数であるとき，$(N,\ N-R)$ $[\mu_{t/b}EC]_p$ 符号は次の関係式を満たす．

$$2^R-1\ge\sum_{j=1}^{\mu}S_j^p(N/b).$$

ここで，$S_j^p(N/b)$ は p 個以下のバイトに生じた j 重 m-スポッティバイト誤りパターンの総数を表し，次式で定義される：

$$\begin{aligned} S_j^p(n) &= \sum_{\substack{\delta_1,\ \delta_2,\ \cdots,\ \delta_\lambda\ge 0\\ \delta_1+\delta_2+\cdots+\delta_\lambda\le p\\ \delta_1+2\delta_2+\cdots+\lambda\delta_\lambda=j}}\left\{\binom{n}{\delta_1+\delta_2+\cdots+\delta_\lambda}\right. \\ &\times\binom{\delta_1+\delta_2+\cdots+\delta_\lambda}{\delta_1,\ \delta_2,\ \ldots,\ \delta_\lambda} \\ &\left.\times\prod_{z=1}^{\lambda}\left\{\sum_{i=(z-1)\cdot t+1}^{\min(z\cdot t,\ b)}\binom{b}{i}\right\}^{\delta_z}\right\}. \end{aligned}$$

ここで，$N/b=n$ とする．また，

$$\binom{\delta_1+\delta_2+\cdots+\delta_\lambda}{\delta_1,\ \delta_2,\ \ldots,\ \delta_\lambda}=\frac{(\delta_1+\delta_2+\cdots+\delta_\lambda)!}{\delta_1!\times\delta_2!\times\cdots\times\delta_\lambda!}$$

である． □

定理 3 は，p 個以下のバイトに生じた μ 個以下のすべての m-スポッティバイト誤りのシンドロームが異なることから証明できる．

2.2 符号構成法

定義 3 行列 $H'=[h'_0\ h'_1\ \cdots\ h'_{b-1}]$ を $\min((\mu_1+\mu_2)t,\ b)$ 個以下の任意の列ベクトルが線形独立な $q\times b$ 行列とする．ここで，$h'_0,\ h'_1,\ \cdots,\ h'_{b-1}$ は $\mathrm{GF}(2^q)$ の元であり，それぞれ q 次列ベクトルである．また，行列 $H''=[h''_0\ h''_1\ \cdots\ h''_{b-1}]$ を $\min(\lfloor(\mu_1+\mu_2)/2\rfloor t,\ b)$ 個以下の任意の列ベクトルが線形独立な $r\times b$ 行列とする．ここで，$h''_0,\ h''_1,\ \cdots,\ h''_{b-1}$ は $\mathrm{GF}(2^r)$ の元であり，それぞれ r 次列ベクトルである． □

$\min((\mu_1+\mu_2)t,\ b)=b$ のとき，行列 H' は，b 次単位行列を含む b 次正則行列である．一方，$\min((\mu_1+\mu_2)t,\ b)=(\mu_1+\mu_2)t$ のとき，行列 H' はハミング距離 $(\mu_1+\mu_2)t+1$ を有する $(b,\ b-q)$ 符号の検査行列である．また，$\min(\lfloor(\mu_1+\mu_2)/2\rfloor t,\ b)=b$ のとき，行列 H'' は，b 次単位行列を含む b 次正則行列である．一方，$\min(\lfloor(\mu_1+\mu_2)/2\rfloor t,\ b)=\lfloor(\mu_1+\mu_2)/2\rfloor t$ のとき，行列 H'' はハミング距離 $\lfloor(\mu_1+\mu_2)/2\rfloor t+1$ を有する $(b,\ b-r)$ 符号の検査行列である．

定理 4 γ を $\mathrm{GF}(2^r)$ の原始元とする．以下に示す行列は，検査長 $R=q+(p_1+p_2-1)r$ ビット，符号長 $N=b\cdot n$ ビットを有する線形 $[\mu_{1\ t/b}\mathrm{EC}]_{p_1}$-$[\mu_{2\ t/b}\mathrm{ED}]_{p_2}$ 符号の検査行列である．

$$H=\begin{bmatrix} H' & H' & \cdots & H' \\ \gamma^0H'' & \gamma^1H'' & \cdots & \gamma^{n-1}H'' \\ \gamma^0H'' & \gamma^2H'' & \cdots & \gamma^{2(n-1)}H'' \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^0H'' & \gamma^{(p_1+p_2-1)}H'' & \cdots & \gamma^{(p_1+p_2-1)(n-1)}H'' \end{bmatrix}$$

ここで，$n=2^r-1$，$\gamma^iH''=\left[\gamma^ih''_0\ \ \gamma^ih''_1\ \ \cdots\ \ \gamma^ih''_{b-1}\right]$，$0\le i\le n-1$ とする． □

定理 4 は，検査行列 H が定理 1 に示す必要十分条件を満たすことを示すことで証明できる．$b/\lfloor(\mu_1+\mu_2)/2\rfloor\le t\le b$ において H' および H'' は b 次正則行列となり，特にそれらを b 次単位行列とすれば，定理 4 に示す符号は RS 符号と一致する．

誤り訂正符号の例として，パラメータ $\mu_1=\mu_2=3$，$p_1=p_2=2$，$b=8$ ビット，$t=2$ ビット，情報長 $K=128$ ビットを有する，2 バイト以内に生じた 3 重 m-スポッティバイト誤りを訂正する符号，すなわち，(157, 128) $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号の検査行列を図 2 に示す．本符号の最大符号長は $N=1{,}016$ ビットである．ここで，γ は原始多項式 $p(x)=x^7+x+1$ で定義される $\mathrm{GF}(2^7)$ の原始元，H' は 8 次単位行列，H'' は次に示す任意の 7 個以下の列ベクトルが線形独立な 7×8 行列である．

$$\begin{aligned} H'' &= [\ h''_0\ \ h''_1\ \ h''_2\ \ h''_3\ \ h''_4\ \ h''_5\ \ h''_6\ \ h''_7\ ] \\ &= [\ \gamma^0\ \ \gamma^1\ \ \gamma^2\ \ \gamma^3\ \ \gamma^4\ \ \gamma^5\ \ \gamma^6\ \ \gamma^{121}\ ] \\ &= \begin{bmatrix} 1&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&1\\ 0&0&1&0&0&0&0&1\\ 0&0&0&1&0&0&0&1\\ 0&0&0&0&1&0&0&1\\ 0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&1 \end{bmatrix} \end{aligned}$$

従来の 3 バイト以内に生じた 3 重 m-スポッティバイト誤りを訂正する符号（$\mathrm{T}_{2/8}\mathrm{EC}$ 符号）が $R=43$ ビットの検査長を必要とするのに対し，2 バイト以内に生じた 3 重 m-スポッティバイト誤りを訂正する符号（$[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号）の検査長は $R=29$ ビットである．

$$
\left[\begin{array}{cccccccccccccccccccc}
10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000000 & 10000 \\
01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000000 & 01000 \\
00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100000 & 00100 \\
00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010000 & 00010 \\
00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001000 & 00001 \\
00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000100 & 00000 \\
00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000010 & 00000 \\
00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000001 & 00000 \\
\hline
10000001 & 00000011 & 00000101 & 00001001 & 00010001 & 00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100 \\
01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000111 & 10001110 & 00011110 & 00111100 & 01111000 & 11110 \\
00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000111 & 10001110 & 00011110 & 00111100 & 01111 \\
00010001 & 00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000111 & 10001110 & 00011110 & 00111 \\
00001001 & 00010001 & 00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000111 & 10001110 & 00011 \\
00000101 & 00001001 & 00010001 & 00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000111 & 10001 \\
00000011 & 00000101 & 00001001 & 00010001 & 00100001 & 01000001 & 10000010 & 00000110 & 00001100 & 00011000 & 00110000 & 01100000 & 11000011 & 10000100 & 00001010 & 00010100 & 00101000 & 01010000 & 10100011 & 01000 \\
\hline
10000001 & 00000101 & 00010001 & 01000001 & 00000110 & 00011000 & 01100000 & 10000100 & 00010100 & 01010000 & 01000111 & 00011110 & 01111000 & 11100100 & 10010000 & 01000100 & 00010111 & 01011001 & 01100110 & 10011 \\
01000001 & 00000110 & 00011000 & 01100000 & 10000100 & 00010100 & 01010000 & 01000111 & 00011110 & 01111000 & 11100100 & 10010000 & 01000100 & 00010111 & 01011001 & 01100110 & 10011100 & 01110100 & 11010100 & 01010 \\
00100001 & 10000010 & 00001100 & 00110000 & 11000011 & 00001010 & 00101000 & 10100011 & 10001110 & 00111100 & 11110011 & 11001001 & 00100010 & 10001011 & 00101101 & 10110010 & 11001111 & 00111010 & 11101011 & 10101 \\
00010001 & 01000001 & 00000110 & 00011000 & 01100000 & 10000100 & 00010100 & 01010000 & 01000111 & 00011110 & 01111000 & 11100100 & 10010000 & 01000100 & 00010111 & 01011001 & 01100110 & 10011100 & 01110100 & 11010 \\
00001001 & 00100001 & 10000010 & 00001100 & 00110000 & 11000011 & 00001010 & 00101000 & 10100011 & 10001110 & 00111100 & 11110011 & 11001001 & 00100010 & 10001011 & 00101101 & 10110010 & 11001111 & 00111010 & 11101 \\
00000101 & 00010001 & 01000001 & 00000110 & 00011000 & 01100000 & 10000100 & 00010100 & 01010000 & 01000111 & 00011110 & 01111000 & 11100100 & 10010000 & 01000100 & 00010111 & 01011001 & 01100110 & 10011100 & 01110 \\
00000011 & 00001001 & 00100001 & 10000010 & 00001100 & 00110000 & 11000011 & 00001010 & 00101000 & 10100011 & 10001110 & 00111100 & 11110011 & 11001001 & 00100010 & 10001011 & 00101101 & 10110010 & 11001111 & 00111 \\
\hline
10000001 & 00001001 & 01000001 & 00001100 & 01100000 & 00001010 & 01010000 & 10001110 & 01111000 & 11001001 & 01000100 & 00101101 & 01100110 & 00111010 & 11010100 & 10100110 & 00111111 & 11110101 & 10100000 & 00001 \\
01000001 & 00001100 & 01100000 & 00001010 & 01010000 & 10001110 & 01111000 & 11001001 & 01000100 & 00101101 & 01100110 & 00111010 & 11010100 & 10100110 & 00111111 & 11110101 & 10100000 & 00001111 & 01110001 & 10001 \\
00100001 & 00000110 & 00110000 & 10000100 & 00101000 & 01000111 & 00111100 & 11100100 & 00100010 & 00010111 & 10110010 & 10011100 & 11101011 & 01010011 & 10011111 & 11111010 & 11010001 & 10000111 & 00111001 & 11000 \\
00010001 & 10000010 & 00011000 & 11000011 & 00010100 & 10100011 & 00011110 & 11110011 & 10010000 & 10001011 & 01011001 & 11001111 & 01110100 & 10101001 & 01001110 & 01111101 & 11101000 & 01000010 & 00011101 & 11100 \\
00001001 & 01000001 & 00001100 & 01100000 & 00001010 & 01010000 & 10001110 & 01111000 & 11001001 & 01000100 & 00101101 & 01100110 & 00111010 & 11010100 & 10100110 & 00111111 & 11110101 & 10100000 & 00001111 & 01110 \\
00000101 & 00100001 & 00000110 & 00110000 & 10000100 & 00101000 & 01000111 & 00111100 & 11100100 & 00100010 & 00010111 & 10110010 & 10011100 & 11101011 & 01010011 & 10011111 & 11111010 & 11010001 & 10000111 & 00111 \\
00000011 & 00010001 & 10000010 & 00011000 & 11000011 & 00010100 & 10100011 & 00011110 & 11110011 & 10010000 & 10001011 & 01011001 & 11001111 & 01110100 & 10101001 & 01001110 & 01111101 & 11101000 & 01000010 & 00011
\end{array}\right]
$$

図 2: (157, 128) $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号のパリティ検査行列.

$$
S = \left[\begin{array}{c}
e_{i_1} \cdot H'^T + e_{i_2} \cdot H'^T + \cdots + e_{i_\rho} \cdot H'^T \\
\gamma^{i_1} e_{i_1} \cdot H''^T + \gamma^{i_2} e_{i_2} \cdot H''^T + \cdots + \gamma^{i_\rho} e_{i_\rho} \cdot H''^T \\
\gamma^{2i_1} e_{i_1} \cdot H''^T + \gamma^{2i_2} e_{i_2} \cdot H''^T + \cdots + \gamma^{2i_\rho} e_{i_\rho} \cdot H''^T \\
\vdots \\
\gamma^{(2p-1)i_1} e_{i_1} \cdot H''^T + \gamma^{(2p-1)i_2} e_{i_2} \cdot H''^T + \cdots + \gamma^{(2p-1)i_\rho} e_{i_\rho} \cdot H''^T
\end{array}\right]^T \tag{2}
$$

次に，伸長符号の検査行列を示す.

定理 5 γ を $\mathrm{GF}(2^{r'})$ の原始元とする. 以下に示す行列は, 検査長 $R = q + (p_1 + p_2 - 1)r'$ ビット, 符号長 $N = b \cdot (n+1) + r'$ ビットを有する 2 次伸長符号の検査行列である.

$$
H = \left[\begin{array}{cccccc}
H' & H' & \cdots & H' & H' & O \\
\gamma^0 H'' & \gamma^1 H'' & \cdots & \gamma^{n-1} H'' & O & O \\
\gamma^0 H'' & \gamma^2 H'' & \cdots & \gamma^{2(n-1)} H'' & O & O \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
\gamma^0 H'' & \gamma^{(p_1+p_2-1)} H'' & \cdots & \gamma^{(p_1+p_2-1)(n-1)} H'' & O & I_{r'}
\end{array}\right]
$$

ただし, $n = 2^{r'} - 1$, $\gamma^i H'' = [\gamma^i \phi(h''_0)\ \gamma^i \phi(h''_1)\ \cdots\ \gamma^i \phi(h''_{b-1})]$, $0 \le i \le n-1$ とする. $\phi:\ \mathrm{GF}(2^r) \to \mathrm{GF}(2^{r'})$ は加法に関する単射準同型写像である. □

本定理は定理 4 と同様にして証明できる.

2.3 復号

定理 4 に示したスポッティバイト誤り制御符号においてパラメータを $\mu_1 = \mu_2 = \mu$, $p_1 = p_2 = p$ として得られる $[\mu_{t/b}\mathrm{EC}]_p$ 符号の復号法を示す.

1. シンドローム生成
   v を受信語, c を符号語, e を誤りベクトルとすると, シンドローム S は以下のように表される.

$$
\begin{aligned}
S &= [\ s_0\ \ s_1\ \ s_2\ \ \cdots\ \ s_{2p-1}\ ] \\
&= v \cdot H^T = (c + e) \cdot H^T = e \cdot H^T
\end{aligned}
$$

   ここで, $s_0 \in \mathrm{GF}(2^q)$ は q ビットの行ベクトル, $s_1, s_2, \cdots, s_{2p-1} \in \mathrm{GF}(2^r)$ はそれぞれ r ビットの行ベクトルである. 例えば, 符号語 c の $i_1, i_2, \cdots, i_\rho$ ($\rho \le p$) 番目のバイトに合計 μ 個以下のスポッティバイト誤り $e_{i_1}, e_{i_2}, \cdots, e_{i_\rho} \in \mathrm{GF}(2^b)$ がそれぞれ生じたとする. すなわち, $\sum_{x=1}^{\rho} w_{\mathrm{M}}(e_{i_x}) \le \mu$ とする. ここで, $\rho \le p \le \mu$ である. このとき, シンドロームは式 (2) で表される.
2. 誤り位置情報の生成と $\mathrm{GF}(2^r)$ 上の誤りパターン生成
   $\sum_{x=1}^{\rho} e_{i_x} = e^*$ とする. 関係式 $s_0 = e^* \cdot H'$ より e^* が得られる. これは, $q \times b$ 行列 H' が μ 重 t/b-誤り訂正符号のパリティ検査行列であることによる. e^* に右から H''^T を掛けると $e^* \cdot H''^T$ が得られる. ここで, 式 (2) の第 1 成分を $e^* \cdot H''^T$ で置き換え, $e_{i_1} \cdot H''^T$, $e_{i_2} \cdot H''^T$, $\cdots$, $e_{i_\rho} \cdot H''^T \in \mathrm{GF}(2^r)$ をそれぞれ ε_{i_1}, ε_{i_2}, $\cdots$, $\varepsilon_{i_\rho} \in \mathrm{GF}(2^r)$ とすれば, 次式が得られる.

$$
S' = \left[\begin{array}{c}
\varepsilon_{i_1} + \varepsilon_{i_2} + \cdots + \varepsilon_{i_\rho} \\
\gamma^{i_1} \varepsilon_{i_1} + \gamma^{i_2} \varepsilon_{i_2} + \cdots + \gamma^{i_\rho} \varepsilon_{i_\rho} \\
\gamma^{2i_1} \varepsilon_{i_1} + \gamma^{2i_2} \varepsilon_{i_2} + \cdots + \gamma^{2i_\rho} \varepsilon_{i_\rho} \\
\vdots \\
\gamma^{(2p-1)i_1} \varepsilon_{i_1} + \gamma^{(2p-1)i_2} \varepsilon_{i_2} + \cdots + \gamma^{(2p-1)i_\rho} \varepsilon_{i_\rho}
\end{array}\right]^T \tag{3}
$$

   式 (3) に示すシンドロームは, $\mathrm{GF}(2^r)$ 上の RS 符号において, $i_1, i_2, \cdots, i_\rho$ バイト目にそれぞれ ε_{i_1}, $\varepsilon_{i_2}, \cdots, \varepsilon_{i_\rho}$ の誤りが生じた場合のシンドロームと一致する. よって, 並列復号法 [4], ユークリッド法, Berlekamp-Massey アルゴリズム [5] 等の RS 符号の復号法を適用することにより, 式 (3) より誤りの位置 $i_1, i_2, \cdots, i_p$, 及び $\mathrm{GF}(2^r)$ 上の誤りパターン $\varepsilon_{i_1}, \varepsilon_{i_2}, \cdots, \varepsilon_{i_\rho}$ を得ることができる.

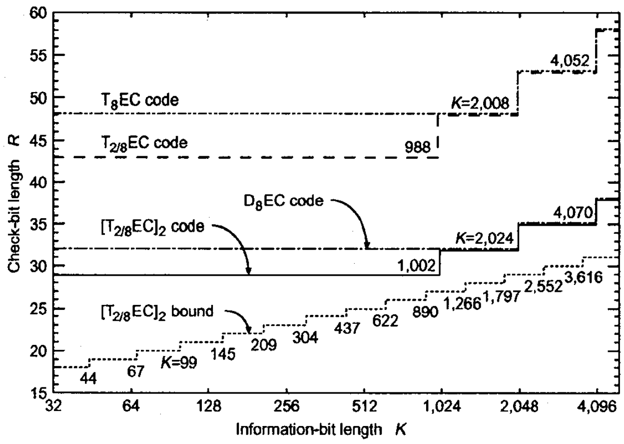


図 3: $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号における情報長と検査長の関係 (参考: $\mathrm{T}_{2/8}\mathrm{EC}$ 符号, $\mathrm{D}_8\mathrm{EC}$ 符号, 及び $\mathrm{T}_8\mathrm{EC}$ 符号).

3. GF(2^b) 上の誤りパターン生成
GF(2^r) 上の誤りパターン ε_{i_1}, ε_{i_2}, $\cdots$, ε_{i_ρ} より GF(2^b) 上の誤りパターン e_{i_1}, e_{i_2}, $\cdots$, e_{i_ρ} を導出する. H' は $\min(\mu t,\, b)$ 以下の列ベクトルが線形独立な行列, すなわち, ハミング距離 $\mu t+1$ を有する誤り制御符号の検査行列である. いま, この符号を $\lfloor \mu/2 \rfloor t$ ビット誤り訂正符号または $\lfloor \mu/2 \rfloor t$ ビット誤り訂正・$(\lfloor \mu/2 \rfloor+1)t$ ビット誤り検出符号とみなす. GF(2^r) の誤りパターン ε_x $(x = 1,\, 2,\, \cdots,\, \rho)$ から GF(2^b) の $\lfloor \mu/2 \rfloor t$ ビット以下の誤りパターン $\widehat{e_{i_x}}$ への 1 対 1 の対応関係を定めたマッピングテーブルをあらかじめ用意しておく. ε_x から $\widehat{e_{i_x}}$ への変換において誤訂正されるもの, すなわち, $\widehat{e_{i_x}} \neq e_{i_x}$ であるもの, または対応関係が存在しないものは高々 1 個である. $\widehat{e_{i_x}}$ が実際の誤りパターン e_{i_x} と一致するか否かは次の関係式を用いて判定される. すなわち, $\widehat{e_{i_x}}$ が次の関係式を満たすならば, それは e_{i_x} に等しい. さもなくば, $\widehat{e_{i_x}} \neq e_{i_x}$ である.

$$w_{\mathrm{M}}(\widehat{e_{i_x}} + e^*) \leq \mu - w_{\mathrm{M}}(\widehat{e_{i_x}})$$

この不等式は, $w_{\mathrm{M}}(e)$ が三角不等式を満たすことを用いて証明できる [6].

3. 評価

図 3 は, パラメータ $\mu_1 = \mu_2 = 3$, $p_1 = p_2 = 2$, $b = 8$ ビット, $t = 2$ ビットの場合における $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号, 従来の 3 重 m-スポッティバイト誤り訂正 ($\mathrm{T}_{2/8}\mathrm{EC}$) 符号 [3], 2 バイト誤り訂正 ($\mathrm{D}_8\mathrm{EC}$) 符号, および 3 バイト誤り訂正 ($\mathrm{T}_8\mathrm{EC}$) 符号における情報長と検査長の関係を示す. ここで, "限界" は定理 2 および 3 に示す限界である. これから, 例えば, 従来の 3 バイト以内に生じた 3 重スポッティバイト誤りを訂正する $\mathrm{T}_{2/8}\mathrm{EC}$ 符号と比較して, 本題の符号である 2 バイト以内に生じた 3 重スポッティバイト誤りを訂正する $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号は, $K = 1,002$ ビット以下で 14 ビットの大幅な検査長の削減が可能である.

4. 結論

本論文では, 実用的な観点より, 誤りバイト数を制限するという条件を付加することにより, より効率の良い実用性の高い m-スポッティバイト誤り制御符号の構成法を示した. 具体的には, p_1 個以下のバイトに生じた μ_1 個以下の m-スポッティバイト誤りを訂正し, p_2 個以下のバイトに生じた μ_2 個以下の m-スポッティバイト誤りを検出する新しい m-スポッティバイト誤り制御符号, すなわち, $[\mu_1\ _{t/b}\mathrm{EC}]_{p_1}$-$[\mu_2\ _{t/b}\mathrm{ED}]_{p_2}$ 符号の一般的構成法を提案した. $\mu_1 = p_1$ かつ $\mu_= p_2$ のとき, 提案符号は従来の m-スポッティバイト誤り制御符号と一致する. また, $b/\lfloor(\mu_1+\mu_2)/2\rfloor \leq t \leq b$ ならば, 提案符号は RS 符号と一致する. すなわち, 提案符号は RS 符号を包含する符号である. 一方, $t < b/\lfloor(\mu_1+\mu_2)/2\rfloor$ ならば, 提案符号は, 従来の m-スポッティバイト誤り制御符号および RS 符号と比較して大幅な検査ビット長の削減が可能である. 具体的には, 実用的な情報長 $K = 128$ ビットに対して, 2 バイト以内に生じた 3 重スポッティバイト誤りを訂正する $[\mathrm{T}_{2/8}\mathrm{EC}]_2$ 符号が 29 ビットの検査長で構成されることを示した. これは, 従来の 3 重 m-スポッティバイト誤り訂正符号のそれより 14 ビット短く, 2 バイト誤り訂正 RS 符号より 3 ビット短い.

参考文献

[1] G. Umanesan and E. Fujiwara, "A Class of Random Multiple Bits in a Byte Error Correcting and Single Byte Error Detecting ($\mathrm{S}_{t/b}$EC-SbED) Codes," *IEEE Trans. Computers*, vol.52, no.7, pp.835–847, July 2003.

[2] T. Kashiyama and E. Fujiwara, "A General Class of Byte Error Control Codes for S-Spotty Byte Errors," *Proc. ISITA*, pp.1297–1302, Parma, Italy, October 2004.

[3] K. Suzuki, T. Kashiyama, and E. Fujiwara, "A General Class of M-Spotty Byte Error Control Codes," *Proc. Asia-Europe Workshop on Information Theory*, pp. 24–26, Viareggio, Italy, October 2004.

[4] E. Fujiwara, K. Namba, and M. Kitakami, "Parallel Decoding for Burst Error Control Codes," *Electronics and Communications in Japan*, Wiley Pub., vol.87, no.1, pp.38–48, January 2004.

[5] S. B. Wicker, V. K. Bhargava, *Reed-Solomon Codes and Their Applications*, IEEE Press, 1994.

[6] 今井秀樹, 藤谷宏, "復号の簡単な誤り訂正符号の一構成法," 電子通信学会論文誌, vol. 62-A, pp. 271–277, May 1979.