LC-006

# スポッティバイト誤り制御符号
# Spotty Byte Error Control Codes

**樫山 俊彦** † **鈴木 一克** † **藤原 英二** †
Toshihiko Kashiyama Kazuyoshi Suzuki Eiji Fujiwara

## 1. まえがき

磁気ディスク，光ディスク，半導体メモリ，等のメモリシステムにおいて，従来よりバイト誤りを制御する符号として Reed-Solomon 符号 (以下，“RS 符号” と称する) が多用されている [1]．バイト誤りはバイト中に生じるすべての誤りを表すのに対し，最近，バイト中に生じる少数のビット誤りをスポッティバイト誤りと称し [2][3]，そのための誤り制御符号が提案されている．すなわち，スポッティバイト誤りとは，$b$ ビットを有するバイト中に生じる $t(<b)$ ビット以下の誤り (以下，“$t/b$ 誤り” と称する) であり，単一スポッティバイト誤りを訂正する符号が提案されている [2][3]．

スポッティバイト誤りの典型的な例として，DRAM チップにおける誤りがあげられる．近年，DRAM チップは広い I/O 幅 (バイト長 $b = 8, 16, 32$ ビット) を持つようになり，強力な電磁波や放射性粒子により複数のランダムビット誤りが生じやすい．これら複数のランダムビット誤りは，高々2, 3 ビット程度であり，各 DRAM チップが物理的に独立であるためバイト内に限定される．よって，これらの誤りの主体はスポッティバイト誤りであり，スポッティバイト誤り制御符号は従来のバイト誤り制御符号に比べて大幅な検査ビットの削減が期待できる．

本論文では，GF($2^b$) 上の最小距離 $d$(以下，“距離 $d$” と称する) を有するスポッティバイト誤り制御符号を提案する．本符号は，$b/2 \le t \le b$ において，距離 $d$ を有する RS 符号に一致する．

## 2. スポッティバイト誤り制御符号

### 2.1 準備

**定義 1** $b$ ビットからなる 1 バイトに $t(1 \le t \le b)$ 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． □

**定理 1** $H_i(0 \le i \le n-1)$ を $R \times b$ の部分行列とし，$H = [H_0 H_1 H_2 H_3 \cdots H_{n-1}]$ とする．また，$E_{t/b} = \{e \in \mathrm{GF}(2^b) \mid 1 \le w_H(e) \le t\}$ をすべての $t/b$ 誤りの集合とする．ただし，$w_H(e)$ はベクトル $e$ のハミング重みである．このとき，距離 $d$ を有するスポッティバイト誤り制御符号の必要十分条件は以下の式で表される．

(i) $(e_1 + e_2) \cdot H_{i_1}^T + (e_3 + e_4) \cdot H_{i_2}^T + \cdots + (e_{2k-1} + e_{2k}) \cdot H_{i_k}^T \neq o$ for $\forall k \in \{k | 2k \le d-1, k \ge 1\}$, $\forall e_1, e_2, \cdots, e_{d-1} \in E_{t/b}$ with $e_1 \neq e_2, e_3 \neq e_4, \cdots, e_{2k-1} \neq e_{2k}$

(ii) $(e_1 + e_2) \cdot H_{i_1}^T + \cdots + (e_{2k-1} + e_{2k}) \cdot H_{i_k}^T + e_{2k+1} \cdot H_{i_{k+1}}^T + \cdots + e_{2k+j} \cdot H_{i_{k+j}}^T \neq o$ for $\forall k, j \in \{k, j | 2k + j = d-1, k \ge 1, j \ge 1\}$, $\forall e_1, e_2, \cdots, e_{2k}, e_{2k+1}, \cdots, e_{2k+j} \in E_{t/b}$ with $e_1 \neq e_2, \cdots, e_{2k-1} \neq e_{2k}$

(iii) $e_1 \cdot H_{i_1}^T + e_2 \cdot H_{i_2}^T + \cdots + e_{d-1} \cdot H_{i_{d-1}}^T \neq o$ for $\forall e_1, e_2, \cdots, e_{d-1} \in E_{t/b}$

ただし，$i_1, i_2, \cdots, i_{d-1} (0 \le i_1, i_2, \cdots, i_{d-1} \le n-1)$ はすべて異なり，$o = (0, 0, \cdots, 0)$ である． □

定理 1 は $d-1$ 個以下のスポッティバイト誤りのシンドローム和が $o$ とならないことを示すことで証明できる．(詳細な証明はスペースの関係から略する．以下同様．)

**定理 2** 距離 $d$ を有するスポッティバイト誤り制御符号は少なくとも $(d-1)t$ ビットの検査長を有する． □

定理 2 は定理 1 に示す必要十分条件より，検査行列の $(d-1)t$ 列が線形独立であることより証明できる．

**定理 3** 距離 $d$ が奇数のとき，符号長 $N$ ビット，検査長 $R$ ビットを有するスポッティバイト誤り制御符号は以下の関係式を満たす．

$$2^R - 1 \ge \sum_{j=1}^{(d-1)/2} \binom{\lceil N/b \rceil - 1}{j} \left\{ \sum_{i=1}^{t} \binom{b}{i} \right\}^j + \sum_{j=0}^{(d-1)/2-1} \binom{\lceil N/b \rceil - 1}{j} \left\{ \sum_{i=1}^{t} \binom{b}{i} \right\}^j \times \left\{ \sum_{i=1}^{\min(t, N-b(\lceil N/b \rceil - 1))} \binom{N - b(\lceil N/b \rceil - 1)}{i} \right\}$$

ここで，$\lceil x \rceil$ は $x$ 以上である最小の整数，$\min(x, y)$ は，$x < y$ のとき $\min(x, y) = x$，$x \ge y$ のとき $\min(x, y) = y$ を表す． □

定理 3 は $(d-1)/2$ 個以下のすべてのスポッティバイト誤りのシンドロームが異なることにより証明できる．

### 2.2 符号構成法

**定義 2** $H' = [h'_0\ h'_1\ \cdots\ h'_{b-1}]$ を階数 $\min(2t, b)$ を有する $r \times b$ 行列とする．ここで，$h'_0, h'_1, \cdots h'_{b-1}$ は GF($2^r$) 上の列ベクトルである． □

$\min(2t, b) = b$ のとき，行列 $H'$ は $b$ 次の正則行列 ($b$ 次の単位行列を含む) である．一方，$\min(2t, b) = 2t$ のとき，行列 $H'$ は GF(2) 上のハミング距離 $2t+1$ を有する $(b, b-r)$ 符号，すなわち $t$ ビット誤り訂正符号の検査行列となる．以下の定理は，定義 2 に示した $H'$ を用いて構成した距離 $d$ を有するスポッティバイト誤り制御符号の検査行列を示す．

† 東京工業大学大学院情報理工学研究科

$$H = \begin{bmatrix} H' & H' & H' & H' & H' & H' & H' & H' & H' & H' & H' \\ \gamma^0 H' & \gamma^1 H' & \gamma^2 H' & \gamma^3 H' & \gamma^4 H' & \gamma^5 H' & \gamma^6 H' & \gamma^7 H' & \gamma^8 H' & \gamma^9 H' & \gamma^{10} H' \\ \gamma^0 H' & \gamma^2 H' & \gamma^4 H' & \gamma^6 H' & \gamma^8 H' & \gamma^{10} H' & \gamma^{12} H' & \gamma^{14} H' & \gamma^{16} H' & \gamma^{18} H' & \gamma^{20} H' \\ \gamma^0 H' & \gamma^3 H' & \gamma^6 H' & \gamma^9 H' & \gamma^{12} H' & \gamma^{15} H' & \gamma^{18} H' & \gamma^{21} H' & \gamma^{24} H' & \gamma^{27} H' & \gamma^{30} H' \end{bmatrix} \quad (1)$$

**定理 4** $\gamma$ を GF $(2^r)$ の原始元とする．距離 $d$ を有し，かつ検査長 $R = (d-1)r$ ビット，符号長 $N = b \cdot (2^r - 1)$ ビットを有するスポッティバイト誤り制御符号の検査行列は以下に示される．

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

ここで，$n = 2^r - 1$,

$$\gamma^i H' = \begin{bmatrix} \gamma^i h'_0 & \gamma^i h'_1 & \cdots & \gamma^i h'_{b-1} \end{bmatrix}, 0 \le i \le n-1$$

□

定理 4 は検査行列 $H$ が定理 1 に示す必要十分条件を満足することを示すことで証明できる．$b/2 \le t \le b$ において $H'$ は $b$ 次の正則行列となり，$H'$ を $b$ 次の単位行列とすると，定理 4 に示す符号は RS 符号に一致する．

**定理 5** 定理 4 に示す構成法による符号の検査長下界は

$$R \ge \left\lceil \log_2 \left( \sum_{i=0}^{t} \binom{b}{i} \right) \right\rceil (d-1)$$

で表される． □

定理 5 は $H'$ の検査長 $r$ の下界が $\left\lceil \log_2 \left( \sum_{i=0}^{t} \binom{b}{i} \right) \right\rceil$ で表され，$(d-1)$ 段構成であることから証明できる．

符号例として，$d = 5$，$b = 8$ ビット，$t = 2$ ビット，情報長 $K = 64$ ビットの短縮化 2 重スポッティバイト誤り訂正 ($D_{2/8}EC$) 符号の検査行列を式 (1) に示す．ここで，$\gamma$ は原始多項式 $p(x) = x^6 + x + 1$ で定義される GF$(2^6)$ の原始元，$H'$ は以下に示す階数 4 を有する $6 \times 8$ 行列である．

$$H' = \begin{bmatrix} \gamma^0 & \gamma^1 & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 & \gamma^{18} & \gamma^{20} \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,1\,0 \\ 0\,1\,0\,0\,0\,0\,1\,0 \\ 0\,0\,1\,0\,0\,0\,1\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,0\,1\,0\,0\,1 \\ 0\,0\,0\,0\,0\,1\,0\,1 \end{bmatrix}$$

情報長 $K = 64$ ビットの場合，距離 $d = 5$ の RS 符号では検査長 $R = 32$ ビット，ランダム 4 ビット誤り訂正 BCH 符号では検査長 $R = 28$ ビット必要とするのに対し，本符号は検査長 $R = 24$ ビットで構成できる．

次に，伸長スポッティバイト誤り制御符号の検査行列を示す．

**定理 6** $R \ge (d-1)r$ かつ $(R-r)$ を $(d-2)$ の倍数とし，$\gamma$ を GF$(2^{(R-r)/(d-2)})$ の原始元とする．距離 $d$ を有し，かつ検査長 $R$ ビット，符号長 $N = b(2^{(R-r)/(d-2)} + 1)$ ビットを有する 2 次伸長スポッティバイト誤り制御符号の検査行列は以下に示される．

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

ただし，$n = 2^{(R-r)/(d-2)} - 1$,

$$\gamma^i H' = \begin{bmatrix} \gamma^i \phi(h'_0) & \gamma^i \phi(h'_1) & \cdots & \gamma^i \phi(h'_{b-1}) \end{bmatrix}, \quad 0 \le i \le n-1$$

$\phi$ : GF$(2^r) \to$ GF$(2^{(R-r)/(d-2)})$ は加法に関する準同型写像． □

定理 6 は定理 4 と同様に証明できる．また，定理 4 に示す符号と同様，$b/2 \le t \le b$，かつ $(R-r)/(d-2) = r$(すなわち $R = (d-1)r$) のとき，GF$(2^b)$ 上の 2 次伸長 RS 符号に一致する．

図 1 に $d = 5$，$b = 8$ ビットの場合における 2 重スポッティバイト誤り訂正 ($D_{t/8}EC$，$t = 2$ または 3 ビット) 符号，及び 2 重バイト誤り訂正 ($D_8EC$，$4 \le t \le 8$ ビット) 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，及び定理 3 に示す限界である．

$d = 5$，$b = 16$ ビットの場合，例えば，$t = 3$ ビット，情報長 $K = 256$ ビットとすると，RS 符号では検査長 $R = 64$ ビット，ランダム 6 ビット誤り訂正 BCH 符号では検査長 $R = 54$ ビット必要とするのに対し，本符号は検査長 $R = 44$ ビットで構成できる．

### 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の復号法を示す．$v$ 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．

$$\begin{aligned} S &= \begin{bmatrix} s_1 & s_2 & s_3 & \cdots & s_{d-1} \end{bmatrix} \\ &= v \cdot H^T = (c+e) \cdot H^T = e \cdot H^T \end{aligned}$$

ここで，$s_1, s_2, s_3, \cdots, s_{d-1} \in$GF$(2^r)$ はそれぞれ $r$ ビットの行ベクトルである．例えば，受信語 $v$ の $i_1, i_2, \cdots, i_p$ 番目のバイトにそれぞれ $e_1, e_2, \cdots, e_p \in$GF$(2^b)$，$w_H(e_i) \le t, i = 1, 2, \cdots, p$ のスポッティバイト誤りが生じたとすると，シンドロームは式 (2) に示される．ここで，$e_1 \cdot H'^T, e_2 \cdot H'^T, \cdots, e_p \cdot H'^T \in$GF$(2^r)$ をそれぞれ

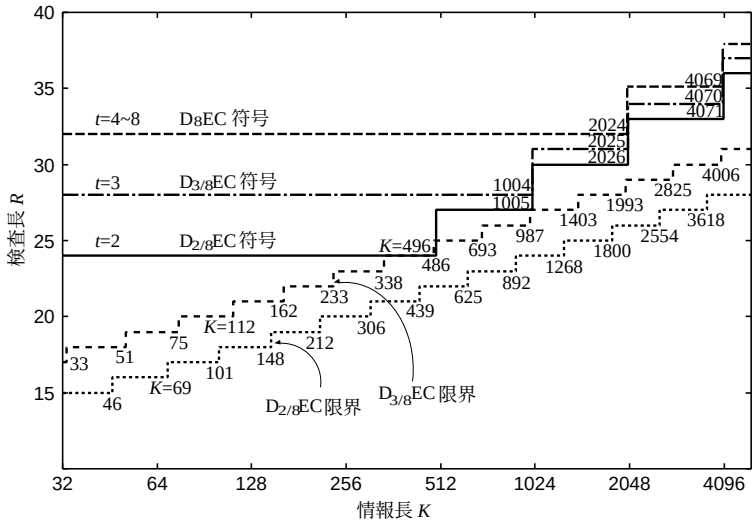


図 1: 距離 $d = 5$ を有する $\mathrm{D}_{t/8}$EC 符号，及び $\mathrm{D}_8$EC 符号における情報長と検査長の関係

$$S = \begin{bmatrix} e_1 \cdot H'^T + e_2 \cdot H'^T + \cdots + e_p \cdot H'^T \\ \gamma^{i_1} e_1 \cdot H'^T + \gamma^{i_2} e_2 \cdot H'^T + \cdots + \gamma^{i_p} e_p \cdot H'^T \\ \gamma^{2i_1} e_1 \cdot H'^T + \gamma^{2i_2} e_2 \cdot H'^T + \cdots + \gamma^{2i_p} e_p \cdot H'^T \\ \vdots \\ \gamma^{(d-2)i_1} e_1 \cdot H'^T + \gamma^{(d-2)i_2} e_2 \cdot H'^T + \cdots + \gamma^{(d-2)i_p} e_p \cdot H'^T \end{bmatrix}^T \tag{2}$$

$e'_1, e'_2, \cdots, e'_p \in \mathrm{GF}(2^r)$ とすると，式 (2) に示すシンドロームは以下のように表せる．

$$S = \begin{bmatrix} e'_1 + e'_2 + \cdots + e'_p \\ \gamma^{i_1} e'_1 + \gamma^{i_2} e'_2 + \cdots + \gamma^{i_p} e'_p \\ \gamma^{2i_1} e'_1 + \gamma^{2i_2} e'_2 + \cdots + \gamma^{2i_p} e'_p \\ \vdots \\ \gamma^{(d-2)i_1} e'_1 + \gamma^{(d-2)i_2} e'_2 + \cdots + \gamma^{(d-2)i_p} e'_p \end{bmatrix}^T \tag{3}$$

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，$i_1, i_2, \cdots, i_p$ 番目のバイトにそれぞれ $e'_1, e'_2, \cdots, e'_p$ の誤りが生じた場合のシンドロームと一致する．よって，式 (3) から誤りの位置 $i_1, i_2, \cdots, i_p$，及び $\mathrm{GF}(2^r)$ 上の誤りパターン $e'_1, e'_2, \cdots, e'_p$ を求めることができる．$d$ が小さい場合，組み合わせ回路のみで構成できる並列復号法 [4] を用いることができる．しかし，並列復号法は距離 $d$，及び符号長 $N$ が大きくなると回路量が大きくなる問題がある．そこで，$d$ が大きい場合，バーレカンプ・マッシィ法 [5] などの逐次復号法を用いる．

次に，$\mathrm{GF}(2^r)$ 上の誤りパターン $e'_1, e'_2, \cdots, e'_p$ より $\mathrm{GF}(2^b)$ 上の誤りパターン $e_1, e_2, \cdots, e_p$ を導出する．$H'$ は階数 $\min(2t, b)$ の行列，すなわち $t$ ビット誤り訂正符号の検査行列であるため，$e_1 \cdot H'^T = e'_1$, $e_2 \cdot H'^T = e'_2$, $\cdots$, $e_p \cdot H'^T = e'_p$ の関係から $\mathrm{GF}(2^b)$ 上の誤りパターン $e_1, e_2, \cdots, e_p$ を一意に定めることができる．$e_1, e_2, \cdots, e_p$ を求める回路は，バイト長 $b = 8, 16$ ビット程度であれば，逐次回路ではなく組み合わせ回路で実現できる．

定理 6 に示した伸長スポッティバイト誤り制御符号も同様にして復号できる．

## 3. 結論

本論文では，$\mathrm{GF}(2^b)$ 上の最小距離 $d$ を有する一般化したスポッティバイト誤り制御符号の構成法，及び復号法を提案した．従来の RS 符号と比較し，少ない検査長で構成でき，8, 16 ビットの入出力を有する DRAM 素子を使用した高速メモリシステムに十分適用可能である．なお，定理 3 における距離 $d$ が偶数の場合の関係式の導出は今後の課題である．

## 参考文献

[1] T. R. N. Rao and E. Fujiwara, “Error-Control Coding for Computer Systems,” Prentice Hall, 1989.

[2] Ganesan Umanesan and Eiji Fujiwara, “A Class of Codes for Correcting Single Spotty Byte Errors,” IEICE Trans. Fundamentals., Vol. E86-A, No. 3, pp 704 - 714 , March 2003.

[3] 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-S$b$ED) Codes,” IEEE Trans. Computers, Vol.52, No.7, pp.835-847, July 2003.

[4] Eiji Fujiwara, Kazuteru Namba, and Masato 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.