

最適な多元不均一誤り制御符号 Optimal q -Ary Unequal Error Control Codes

金子 晴彦*
Haruhiko Kaneko

藤原 英二*
Eiji Fujiwara

1 まえがき

符号語内に誤り制御能力の異なる2個の領域を有する不均一誤り制御 (Unequal Error Control: UEC) 符号について、従来の最適な2元符号 [1] をガロア体 $GF(q)$ 上へ一般化した多元 UEC 符号を3種提案する。また、これらの符号が理論的境界を満足する最適な符号であることを示す。本符号は、符号語中に誤り率の高い領域と低い領域が存在し、かつ情報の符号化に誤り制御符号と固定長の記録符号を併用するホログラフィックメモリ等に対し適用可能である。

2 符号機能の定義

本稿で提案する符号の符号語は、長さ l を有する固定領域 X_0 と、長さ $n-l$ を有するそれ以外の領域 X_1 の2個の領域からなる。ただし、 n は符号長である。領域 X_0 は一般性を失わず符号語の左端に配置するものとする (図1)。本稿では、領域 X_0 に強い誤り制御機能を有する以下の3種の最適な多元 UEC 符号を提案する。ここで、“固定領域誤り”とは固定領域中の任意の誤りを称する。

- X_0 における固定領域誤りを訂正し、 X_1 における1シンボル誤りを訂正する (Fixed l -symbol Error Correcting | Single-symbol Error Correcting: $F_lEC|SEC$) 符号。
- X_0 における固定領域誤りと、 X_1 における1シンボル誤りの同時誤りを訂正する (Fixed l -symbol plus Single-symbol Error Correcting: $(F_l+S)EC$) 符号。
- X_0 における固定領域誤りを訂正し、 X_1 における1シンボル誤りを訂正し、 X_1 における2シンボル誤りを検出する (Fixed l -symbol Error Correcting | Single-symbol Error Correcting - Double-symbol Error Detecting: $F_lEC|SEC-DED$) 符号。

3 $F_lEC|SEC$ 符号

領域 X_0 における固定領域誤りパターンの集合を E_0 、領域 X_1 における1シンボル誤りパターンの集合を E_1 とする。ただし、誤りパターンは長さ n を有する $GF(q)$ 上のベクトルで表現する。

定理 3.1 $GF(q)$ 上の行列 H が線形 $F_lEC|SEC$ 符号の検査行列であるための必要十分条件は以下のとおりである。

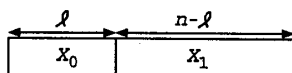


図1 符号語の構成

*東京工業大学 大学院情報理工学研究所, Graduate School of Information Science and Engineering, Tokyo Institute of Technology

$$1. eH^T \neq 0 \text{ for } \forall e \in (E_0 \cup E_1)$$

$$2. e_p H^T \neq e_q H^T \text{ for } \forall e_p, e_q \in E_0, e_p \neq e_q$$

$$3. e_i H^T \neq e_j H^T \text{ for } \forall e_i, e_j \in E_1, e_i \neq e_j$$

$$4. e_p H^T \neq e_i H^T \text{ for } \forall e_p \in E_0, e_i \in E_1$$

ただし、 $0 = (0, 0, \dots, 0)$ である。 □

定理 3.2 $GF(q)$ 上の線形 $F_lEC|SEC$ 符号の符号長 n と検査シンボル長 r は次式に示す関係を満たす。

$$n \leq \frac{q^r - q^l}{q-1} + l$$

(証明) 領域 X_0 における固定領域誤り訂正のために $q^l - 1$ 個のシンδροーム、 X_1 における1シンボル誤り訂正のために $(q-1)(n-l)$ 個のシンδροームがそれぞれ必要である。よって、 $q^r - 1 \geq q^l - 1 + (q-1)(n-l)$ であるから定理は成立する。 □

検査シンボル数 $r-l$ を有する $GF(q)$ 上の1シンボル誤り訂正ハミング符号の検査行列を $H'_{r-l} = [h_0 \ h_1 \ \dots \ h_{n'-1}]$ とする。ただし、 h_i ($0 \leq i \leq n'-1$) は $GF(q)$ 上の長さ $r-l$ を有する互いに線形独立な列ベクトルであり、 $n' = (q^{r-l} - 1)/(q-1)$ である。また、 $r-l=1$ の場合、 $H'_1 = [1]$ とする。 $(r-l)$ 行 q^l 列を有する行列 Q_i ($0 \leq i \leq n'-1$) を $Q_i = [h_i \ h_i \ \dots \ h_i]$ とする。

定理 3.3 次に示す行列 H は、定理 3.2 に示す符号長境界を満足する $GF(q)$ 上の最適な $F_lEC|SEC$ 符号の検査行列である。

$$H = \left[\begin{array}{c|ccc} I_l & M & M & \dots & M \\ \hline O_{(r-l) \times l} & Q_0 & Q_1 & \dots & Q_{n'-1} \end{array} \right]$$

ただし、 $I_l, O_{(r-l) \times l}, M$ は以下に定義する行列である。

I_l : $l \times l$ 単位行列

$O_{(r-l) \times l}$: すべての要素が0である $(r-l) \times l$ 行列

M : 互いに異なる列ベクトルからなる $l \times q^l$ 行列 □

4 $(F_l+S)EC$ 符号

定理 4.1 $GF(q)$ 上の行列 H が線形 $(F_l+S)EC$ 符号の検査行列となるための必要十分条件は、定理 3.1 の条件1から条件4に以下の条件5を加えたものである。

$$5. (e_i + e_p)H^T \neq (e_j + e_q)H^T$$

for $\forall e_p, e_q \in E_0, e_i, e_j \in E_1, e_p \neq e_q, e_i \neq e_j$ □

定理 4.2 $GF(q)$ 上の線形 $(F_l+S)EC$ 符号の符号長 n と検査シンボル長 r は次式に示す関係を満たす。

$$n \leq \frac{q^{r-l} - 1}{q-1} + l \quad (1) \quad \square$$

定理 4.3 次に示す行列 H は、定理 4.2 に示す符号長限界を満足する $GF(q)$ 上の最適な (F_l+S) EC 符号の検査行列である。

$$H = \left[\begin{array}{c|c|c} I_l & O_{l \times (n-l-r)} & I_r \\ \hline P & Q & \end{array} \right]$$

ただし、部分行列 P, Q はそれぞれ以下のように定める。

P : ハミング重みが 2 以上の列ベクトルで構成され、任意の 2 列ベクトルが線形独立な $(r-l) \times l$ 行列。

Q : ハミング重みが 2 以上の列ベクトルで構成され、任意の 2 列ベクトルが線形独立な $(r-l) \times (n-l-r)$ 行列。ただし、 P に含まれる列ベクトルは除く。□

5 F_l EC|SEC-DED 符号

定理 5.1 $GF(q)$ 上の行列 H が線形 F_l EC|SEC-DED 符号の検査行列となるための必要十分条件は、定理 3.1 の条件 1 から条件 4 に以下の条件 5, 6 を加えたものである。

- 5. $e_p H^T \neq (e_i + e_j) H^T$
for $\forall e_p \in E_0, e_i, e_j \in E_1, e_i \neq e_j$
- 6. $(e_i + e_j) H^T \neq e_k H^T$
for $\forall e_i, e_j, e_k \in E_1, e_i \neq e_j, e_i \neq e_k, e_j \neq e_k$ □

定理 5.2 $GF(q)$ 上の線形 F_l EC|SEC-DED 符号の符号長 n と検査シンボル長 r は式 (1) に示す関係を満たす。□

定理 5.3 次に示す行列 H は、定理 5.2 に示す符号長限界を満足する $GF(q)$ 上の最適な F_l EC|SEC-DED 符号の検査行列である。

$$H = \left[\begin{array}{c|c} I_l & O \\ \hline H_0 & H_1 \end{array} \right] = \left[\begin{array}{c|c} I_l & O \\ \hline O & A_{r-l} \end{array} \right]$$

ただし、 A_{r-l} は $(r-l) + \lfloor (r-l)/2 \rfloor$ 行 $(q^{r-l}-1)/(q-1)$ 列を有する行列であり、図 2 に示すように再帰的に定義する。ここで、 α は $GF(q)$ の原始元、 $F_{x,y} = x^2 + y^2 + cxy$ であり、 $c \in GF(q)$ は任意の $z \in GF(q)$ に対し $z^2 + cz + 1 \neq 0$ を満たす定数である。□

(証明) 関数 $F_{x,y}$ の定義より、以下の行列 D の 3 列ベクトルは線形独立である [2]。

$$D = \begin{bmatrix} 1 & 1 & 1 \\ F_{x_0,y_0} & F_{x_1,y_1} & F_{x_2,y_2} \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{bmatrix}$$

ただし、 $x_i, y_i \in GF(q), (x_i, y_i) \neq (x_j, y_j), 0 \leq i \neq j \leq 2$ である。これを用いて、部分行列 H_1 の任意の 3 列ベクトルが線形独立であることが証明できる。また、 A_{r-l} の定義より H_1 の下 $r-l$ 行からなる部分行列は $GF(q)$ 上の 1 シンボル訂正ハミング符号の検査行列となっている。これらより、 H は定理 3.1、及び定理 5.1 の条件 1 から条件 6 を満たすことが証明できる。さらに、 A_{r-l} の列数は $(q^{r-l}-1)/(q-1)$ であるから、本符号は最適な F_l EC|SEC-DED 符号である。□

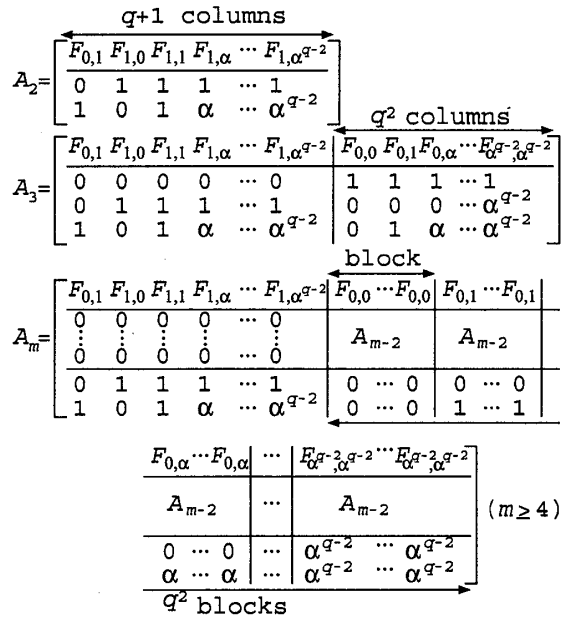


図 2 行列 A_{r-l} の定義

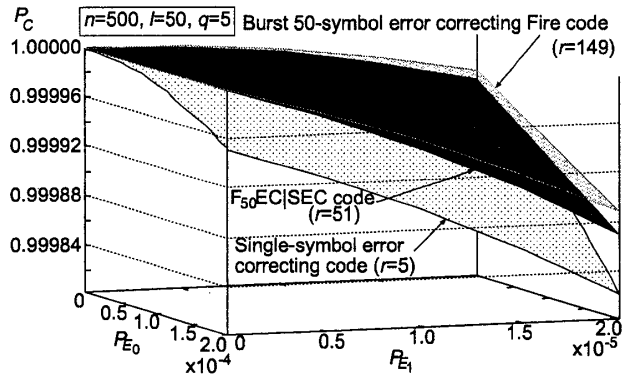


図 3 F_{50} EC|SEC 符号の正復号率 ($n = 500, q = 5$)

6 評価

領域 X_0 におけるシンボル誤り率を P_{E_0} 、領域 X_1 におけるシンボル誤り率を $P_{E_1} (< P_{E_0})$ とする。符号長 $n = 500$ を有する $GF(5)$ 上の F_{50} EC|SEC 符号の正復号率 P_C 、すなわち、復号した語に誤りが存在しない確率、を図 3 に示す。また、比較として均一な誤り制御能力を有する 50 シンボルバースト誤り訂正ファイア符号、及び 1 シンボル誤り訂正ハミング符号の正復号率を示す。 P_{E_1} が十分小さい場合、本符号は約 3 倍の検査シンボルを必要とするバースト誤り訂正ファイア符号に近い正復号率を有する。

参考文献

- [1] E. Fujiwara, T. Ritthongpitak, and M. Kitakami, "Optimal Two-Level Unequal Error Control Codes for Computer Systems," IEEE Trans. Comp., vol.47, no.12, pp.1313-1325, Dec. 1998.
- [2] G. L. Feng, S. Xiao, X. Shi, and T. R. N. Rao, "Construction of the SbEC-DbED and DbEC Codes, and Their Applications," IEEE Int. Workshop on Defect and Fault Tolerance in VLSI Systems, pp.278-286, Aug. 1995.