数理解析研究所講究録
1106巻 1999年 50-60

線形符号の復号法について

大阪大学理学研究科　池上 大介　(Daisuke Ikegami) [1]

Abstract— This paper introduces a procedure for decoding linear codes up to half the Feng-Rao bound which is defined by R. Pellikaan [5]. G-L. Feng, K.K. Tzeng and T.R.N.Rao found the procedure [2], [1], and they showed it was a generalization of the Berlekamp-Massey algorithm [3] in their paper [1]. We summarize this decoding methods from the view due to Miura's thesis [4].

Keywords— Feng-Rao decoding, Feng-Rao designed distance, Feng-Rao bound, BCH decoding

1 はじめに

1.1 誤り訂正符号と復号問題とは

q 個の元からなる有限体を $\mathcal{F}_q$ と表す．$\mathcal{F} := \mathcal{F}_q$ とおく．正整数 n を固定する．

Definition 1 $\mathcal{F}_q$ 上の n 次元ベクトル空間の部分空間 C を線形符号，または単に 符号 と呼ぶ．

以下，特に断わらない限り $k := \dim_{\mathcal{F}} C$ とおく．n を符号 C の符号長，k を符号 C の次元と呼ぶ．

Definition 2 (Hamming 距離) $\mathbf{a} := (a_1, \ldots, a_n)$,
$\mathbf{b} := (b_1, \ldots, b_n) \in \mathcal{F}^n$ に対し，$\mathrm{d}(\mathbf{a}, \mathbf{b}) := \#\{i \mid a_i \neq b_i\}$ [1] を $\mathbf{a}$ と $\mathbf{b}$ の *Hamming* 距離 と呼ぶ．
Hamming 距離は距離の公理を満たす．
符号 C に対し，

$$\mathrm{d}(C, a) := \min_{C \ni \mathbf{c} \neq \mathbf{a}} \#\{i \mid c_i \neq a_i\}$$

と表す．また，

$$\mathrm{d}(C) := \min_{C \ni \mathbf{c}, \mathbf{c}', \mathbf{c} \neq \mathbf{c}'} \#\{i \mid c_i \neq c'_i\}$$

を符号 C の 最小距離 と呼ぶ．以下，特に断わらない限り $d := \mathrm{d}(C)$ とおく．

Definition 3 (Hamming 重み) $\mathrm{w}(a) := \#\{i \mid a_i \neq 0\}$ を $\mathbf{a}$ の *Hamming* 重み と呼ぶ．

正整数 $t \leq (\mathrm{d}(C) - 1)/2$ を固定する．この定義のもとで，t 限界距離復号を定義する．

[t 限界距離復号]

符号 C における t 限界距離復号とは次のアルゴリズムを言う:

Input: $\mathbf{y} \in \mathcal{F}^n$
Output: もし $\mathrm{d}(C, \mathbf{y}) \leq t$ ならば，
$\mathrm{d}(\mathbf{c}, \mathbf{y}) = \mathrm{d}(C, \mathbf{y})$ を満たす $\mathbf{c} \in C$.
さもなければ停止するか，
もしくは C の元を返す．

誤り訂正符号における復号問題を次に提示する．

[0] sm4003id@ex.ecip.osaka-u.ac.jp
[1] 有限集合 A に対し，$\#A$ を A の元の個数とする．

[復号問題]

符号 C および 正整数 $t \leq (\mathrm{d}(C)-1)/2$ が与えられたとき，C の t 限界距離復号をより少ないメモリー，計算量で行うアルゴリズムを求めよ．

この論文では Feng-Rao 復号法を紹介する．

1.2 線形符号とは

復号の対象である線形符号について，その性質をまとめる．

Definition 4 (生成行列) C の基底を各行とする $k \times n$ 行列を 生成行列 と呼ぶ．

Definition 5 $\mathbf{a}=(a_1,\ldots,a_n), \mathbf{b}=(b_1,\ldots,b_n) \in \mathcal{F}^n$ に対し

$$\begin{aligned} \mathbf{a}*\mathbf{b} &:= (a_1b_1, a_2b_2, \ldots, a_nb_n) \in \mathcal{F}^n \\ \langle \mathbf{a}, \mathbf{b} \rangle &:= \sum_{i=1}^{n} a_i b_i \in \mathcal{F} \end{aligned}$$

とする．

Definition 6

$$C^{\perp} := \{\mathbf{a} \in \mathcal{F}^n \mid \langle \mathbf{a}, \mathbf{c} \rangle = 0 \qquad for\ \forall \mathbf{c} \in C\}$$

とする．特に，$C^{\perp}$ の生成行列を H と表し，これを C の パリティ検査行列 と呼ぶ．$r := \dim_{\mathcal{F}} C^{\perp}$ とおく．H の各行ベクトルを $\{\mathbf{b_1},\ldots,\mathbf{b_r}\}$ と表す．

2 Feng-Rao 復号法

2.1 あらまし

この節では，まず Feng-Rao bound を定義し，そのうえで Feng-Rao 復号法を紹介する．Feng-Rao 復号法 の定義は三浦の博士論文 [4] による．

2.2 Feng-Rao bound

$C^{\perp}$ の基底 (行ベクトル) を $\{\mathbf{b}_1,\ldots,\mathbf{b}_r\}$ とし，
$\mathcal{F}^n \setminus C^{\perp}$ [2] の基底 (行ベクトル) を $\{\mathbf{b}_{r+1},\ldots,\mathbf{b}_n\}$ とする．この並び $\{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$ を固定する．

Definition 7 $i \in \{1,\ldots,n\}$ に対し，

$$\mathrm{Span}(\mathbf{b}_1,\ldots,\mathbf{b}_i) := \{\sum_{\ell=1}^{i} \lambda_\ell \mathbf{b}_\ell \mid \lambda_\ell \in \mathcal{F}\}$$

とする．

[2] $A \supset B$ に対し，$A \setminus B := \{a \in A \mid a \notin B\}$ とする．

Definition 8 $\mathbf{a} \in \mathcal{F}^n$ に対し，次の 2 つの写像 $\sigma, \tau : \mathcal{F}^n \to \{1, \ldots, n\}$ を定義する:

1. $\sigma(\mathbf{a}) = i \overset{\text{def}}{\Leftrightarrow}$
   $\mathbf{a} \in \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_i) \setminus \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$
2. $\tau(\mathbf{a}) = i \overset{\text{def}}{\Leftrightarrow}$
   $\mathbf{a} \in \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$ かつ
   $\mathbf{a} \notin \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_i)^{\perp}$

$\sigma(\mathbf{b}_i * \mathbf{b}_j) = s$ を満たすような対 $(\mathbf{b}_i, \mathbf{b}_j)$ に対し，σ の定義より $\mathbf{b}_i * \mathbf{b}_j$ は $\mathbf{b}_1, \ldots, \mathbf{b}_s$ の 1 次結合として一意にかける．そこで，

$$\mathbf{b}_i * \mathbf{b}_j = \sum_{\ell=1}^{s} \alpha_\ell^{(i,j)} \mathbf{b}_\ell \tag{1}$$

として，$\alpha_\ell^{(i,j)} \in \mathcal{F}^n$ を決める．このとき $\alpha_s^{(i,j)} \neq 0$ である．

Lemma 1 $0 \neq \mathbf{c} \in C$ に対して，次が成り立つ．

1. $r + 1 \leq \tau(\mathbf{c}) \leq n$
2. $l := \tau(\mathbf{c})$ とおく．このとき，$\langle \mathbf{c}, \mathbf{b}_l \rangle \neq 0, \langle \mathbf{c}, \mathbf{b}_i \rangle = 0 \quad \mathrm{for} 1 \leq {}^{\forall} i < l$
3. 特に対 $(\mathbf{b}_i, \mathbf{b}_j)$ が $\sigma(\mathbf{b}_i * \mathbf{b}_j) = l$ を満たすならば，$\langle \mathbf{c}, \mathbf{b}_i * \mathbf{b}_j \rangle \neq 0$，$\sigma(\mathbf{b}_i * \mathbf{b}_j) < l$ を満たすならば，$\langle \mathbf{c}, \mathbf{b}_i * \mathbf{b}_j \rangle = 0$ である．

Proof.

1. $C^{\perp}$ および $\{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ の定義から，$\mathbf{c} \in C \Leftrightarrow \langle \mathbf{c}, \mathbf{b}_i \rangle = 0 \, \mathrm{for} 1 \leq i \leq r$ が成り立つ．したがって定義から $\tau(\mathbf{c}) \geq r + 1$ が従う．また，$\mathbf{c} \neq \mathbf{0}$ であるから，$\mathbf{c} \notin \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_n)^{\perp}$ である．したがって定義から $\tau(\mathbf{c}) \leq n$ が従う．
2. $\tau(\mathbf{c})$ の定義から，いま $\mathbf{c} \in \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_{l-1})^{\perp}$ である．よって，$\langle \mathbf{c}, \mathbf{b}_i \rangle = 0 \, \mathrm{for} 1 \leq {}^{\forall} i < l$ がわかる．そこで $\langle \mathbf{c}, \mathbf{b}_l \rangle = 0$ と仮定すると，$\mathbf{c} \in \mathrm{Span}(\mathbf{b}_1, \ldots, \mathbf{b}_l)^{\perp}$ となり，$\tau(\mathbf{c}) = l$ の定義に矛盾する．ゆえに，$\langle \mathbf{c}, \mathbf{b}_l \rangle = 0$ が従う．
3. Definition 1. での基底表示から明らか．

□

Lemma 2 $\mathbf{c} \in C, \mathbf{e} \in \mathcal{F}^n, \mathbf{y} := \mathbf{c} + \mathbf{e}$ について，次が成り立つ．

1. $\langle \mathbf{c}, \mathbf{b}_i \rangle = 0$ *for* $1 \leq i \leq r$.
2. $\langle \mathbf{e}, \mathbf{b}_i \rangle = \langle \mathbf{y}, \mathbf{b}_i \rangle$ *for* $1 \leq i \leq r$.
3. $\sigma(\mathbf{b}_i * \mathbf{b}_j) \leq r$ ならば $\langle \mathbf{e}, \mathbf{b_i} * \mathbf{b_j} \rangle = \langle \mathbf{y}, \mathbf{b_i} * \mathbf{b_j} \rangle$.

Definition 9 便利のため，

$$(u, v) < (i, j) \overset{def}{\Leftrightarrow} u \leq i \text{ かつ } v \leq j \text{ かつ } (u, v) \neq (i, j)$$

と定義する．

Definition 10 (Well-behaved) 対 $(\mathbf{b}_i, \mathbf{b}_j)$ が

$$\sigma(\mathbf{b}_u * \mathbf{b}_v) < \sigma(\mathbf{b}_i * \mathbf{b}_j) \quad for \ {}^{\forall}(u, v) < (i, j)$$

をみたすとき，*well-behaved* と呼ぶ．

Definition 11 $s \in \{1,\ldots,n\}$ に対し,
$\mathrm{W}(s) := \#\{(i,j) \mid \sigma(\mathbf{b}_i * \mathbf{b}_j) = s$
かつ $(\mathbf{b}_i, \mathbf{b}_j)$ が well − behaved$\}$ とする.

Definition 12 $\mathcal{F}^n \ni \mathbf{a} := (a_1,\ldots,a_n)$ に対し, $n \times n$ 行列 $X(\mathbf{a})$ を次のように定める.

$$X(\mathbf{a}) := \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_n \end{pmatrix} \begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{pmatrix} \begin{pmatrix} {}^t\mathbf{b}_1 & \cdots & {}^t\mathbf{b}_n \end{pmatrix}$$

Lemma 3 $\mathrm{rank}(X(\mathbf{a})) = \mathrm{w}(\mathbf{a})$ である.

Proof. $\{\mathbf{b}_1,\ldots,\mathbf{b}_n\}$ は $\mathcal{F}^n$ の基底であるから,

$$\mathrm{rank}\left(\begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}\right) = \mathrm{rank}\left(\begin{pmatrix} {}^t\mathbf{b}_1 & \cdots & {}^t\mathbf{b}_n \end{pmatrix}\right) = n$$

である. また $\mathrm{w}(\mathbf{a})$ の定義から

$$\mathrm{rank}\left(\begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{pmatrix}\right) = \mathrm{w}(\mathbf{a})$$

が成り立つ. よって結論が従う. □

Lemma 4 $0 \neq \mathbf{c} \in C$ に対して, $\tau := \tau(\mathbf{c})$ とおくとき次が成り立つ.

$$\mathrm{w}(\mathbf{c}) \geq \mathrm{W}(\tau).$$

Proof. Definition 12 により, $n \times n$ 行列 $X := (x_{i,j}) := X(\mathbf{c})$ を定める. Lemma 3 より $\mathrm{w}(c) = \mathrm{rank}(X)$ である. そこで, $n \times n$ 行列 Y を次のようにして定める: $Y := (y_{i,j})$,

$$y_{i,j} := \begin{cases} x_{i,j} & \text{if } \sigma(\mathbf{b}_i * \mathbf{b}_j) = \tau \\ & \text{かつ } (\mathbf{b}_i, \mathbf{b}_j) \text{ が well − behaved} \\ & \cdots(*) \\ 0 & \text{otherwise} \end{cases}$$

このとき, $\mathrm{rank}(X) \geq \mathrm{rank}(Y)$ および $\mathrm{rank}(Y) = \mathrm{W}(\tau)$ を示す. まず, 先程示した Lemma 1 より, 条件 (*) をみたす $y_{i,j}$ について, $y_{i,j} = \langle \mathbf{c}, \mathbf{b}_i * \mathbf{b}_j \rangle \neq 0$ がわかっている. よって $\mathrm{rank}(X) \geq \mathrm{rank}(Y)$ および $\mathrm{rank}(Y) = \mathrm{W}(\tau)$ が従う. □

Proposition 1 以上の記法のもとで次が成り立つ.

$$\mathrm{d}(C) \geq \min\{\mathrm{W}(\tau) \mid r+1 \leq \tau \leq n\}$$

Proof. まず，$\mathrm{d}(C)$ の定義から，

$$\begin{aligned}\mathrm{d}(C) &= \min_{C\ni \mathbf{c}\neq\mathbf{c}'} \mathrm{d}(\mathbf{c},\mathbf{c}') \\ &= \min_{C\ni \mathbf{c}-\mathbf{c}'\neq\mathbf{0}} \mathrm{d}(\mathbf{c}-\mathbf{c}',\mathbf{0}) \\ &= \min_{C\ni \mathbf{c}\neq\mathbf{0}} \mathrm{w}(\mathbf{c})\end{aligned}$$

である．ゆえに Lemma 4. および Lemma 1 より結論が従う．□

Definition 13 $d_{FR} := \min\{\mathrm{W}(\tau) \mid r+1 \le \tau \le n\}$ と書き，これを *Feng-Rao bound* と呼ぶ．

2.3 Gauss の消去法

この節では Feng-Rao 復号法の鍵となる行列の Gauss の消去法について述べる．

Algorithm 1 (Image and Karnel of a matrix $\tilde{X}$) $\tilde{X} := (\tilde{x}_{i,j})$
$m \times n$ 行列 $(m \le n)$, $\tilde{x}_{i,j} \in F$ とする。$\tilde{X}$ の *image* と *kernel* を求める，*Gauss* の消去法を変形した次の *algorithm* を与える．

Input : $\tilde{X} := (\tilde{x}_{i,j})$ $\quad m \times n$ 行列
Output : $M = (m_{i,j})$ $\quad m \times n$ 行列 $\quad m_{i,j} = 0$ or 1,
$\mathbf{v}^{(s)} := (v_1^{(s)}, \ldots, v_n^{(s)})$ $\quad \mathbf{v}^{(s)} : \tilde{X}$ の *Kernel* $\quad 1 \le {}^{\forall}s \le \mathrm{rank}(\tilde{X})$

1. [Initialize] $r := 0, m_{i,j} = 0$ *for* ${}^{\forall}(i,j)$, $i := 1, j := 1$, $X := (x_{i,j}) := \tilde{X}$
2. [Scan Column] もし，$x_{i,j} \neq 0$ かつ $m_{u,j} = 0$ for $1 \le \forall u \le i$ ならば，$r := r+1, d_j := 0$ として，その (i,j) を保存して次に進め．この (i,j) を “ピボット” と呼ぶ．そうでなければ，*4* に行け．
3. [Eliminate] $x_{i,j} := -1$, $x_{i,v} := -x_{i,v}/x_{i,j}$ *for* $v = j+1, \ldots, n$ とする．
(a) $\ell := 1$ とする．
(b) $x_{\ell,j} := 0$ とする．
(i). $s := j+1$ とする．
(ii). $x_{\ell,s} := x_{\ell,s} + x_{\ell,j} m_{i,s}$
(iii). $s < n$ ならば，$s := s+1$ として *3(b)(ii)* へ行け．さもなければ次に進め．
(c) $\ell < m$ ならば，$\ell := \ell+1$ として *3b* へ行け．さもなければ次に進め．
(d) $m_{i,j} := 1, d_j = i$ とする．
4. [Finished?] もし $\ell < n$ ならば $\ell := \ell+1$ として *2* に飛べ．
5. [Output] $M = (m_{i,j})$ を返せ．$d_s = 0$ となるような $s \in \{1, \ldots, n\}$ はこの時点でちょうど $r = \mathrm{rank}(X)$ 個ある．それらに対して，

$$\mathbf{v}^{(s)} := (v_j^{(s)})_{1\le j\le n} = \begin{cases} x_{d_j,s} & \text{if} d_j > 0 \\ 1 & \text{if} j = s \\ 0 & \text{otherwise} \end{cases}$$

としてそれを返せ．

Lemma 5 $m \times n$ 行列 $\tilde{X}$ $(m \le n)$ に対して，*Algorithm 1* を適用して得る $M = (m_{i,j})$ について，次が成り立つ．

1. $\mathrm{rank}(\tilde{X}) = \#\{(i,j) \mid m_{i,j} = 1\}$ である.
2. $m_{i,j} = 1$ ならば $m_{u,j} = 0$ *for* $^{\forall}u < i$, かつ $m_{i,v} = 0$ *for* $^{\forall}v < j$ である.

2.4 多数決決定

この節では, Feng-Rao 復号の鍵となる多数決決定について述べる.
$r+1 \leq \ell \leq n$ を固定する. $\mathrm{w}(\mathbf{e}) \leq (d_{FR}-1)/2$ を仮定する.

Lemma 6 $\tilde{X} := (\langle \mathbf{e}, \mathbf{b}_i * \mathbf{b}_j \rangle)$ $n \times n$ 行列について, *Algorithm 1* を適用して得る行列を M とする. そこで,

$$
\begin{aligned}
U :=& \ \{(i,j) \mid \sigma(\mathbf{b}_i * \mathbf{b}_j) = \ell, (\mathbf{b}_i, \mathbf{b}_j) \text{ は } well-behaved\} \\
U_0 :=& \ \{(i,j) \mid \sigma(\mathbf{b}_i * \mathbf{b}_j) \leq \ell - 1, m_{i,j} = 1\} \\
U_1 :=& \ \{(i,j) \mid {}^{\exists}u < i \text{ s.t. } \sigma(\mathbf{b}_u * \mathbf{b}_j) \leq \ell - 1, m_{u,j} = 1\} \\
\cup& \ \{(i,j) \mid {}^{\exists}v < j \text{ s.t. } \sigma(\mathbf{b}_i * \mathbf{b}_v) \leq \ell - 1, m_{i,v} = 1\} \\
\cap& \ U \\
U_2 :=& \ \{(i,j) \mid m_{i,j} = 1\} \cap U \\
U_3 :=& \ U \setminus (U_1 \cup U_2) \\
u_i :=& \ \#U_i \text{ for } {}^{\forall}i = 0,1,2,3
\end{aligned}
$$

とおく. このとき,

1. $2\mathrm{w}(\mathbf{e}) + 1 \leq d_{FR} \leq \mathrm{W}(\ell)$
2. $u_1 + u_2 + u_3 = \#\{(i,j) \mid \sigma(\mathbf{b}_i * \mathbf{b}_j) = \ell, (\mathbf{b}_i, \mathbf{b}_j) \text{ は } well-behaved\} = \mathrm{W}(\ell)$
3. $u_1 \leq 2u_0$
4. $u_0 + u_2 \leq \mathrm{w}(\mathbf{e})$
5. $u_2 < u_3$
6. $(i,j) \in U_3$ に対して,

$$\langle \mathbf{e}, \mathbf{b}_i * \mathbf{b}_j \rangle = \sum_{\lambda=1}^{j-1} v_\lambda^{(j)} \langle \mathbf{e}, \mathbf{b}_\lambda * \mathbf{b}_j \rangle$$

がなりたつ.

Proof.

1. 仮定 $\mathrm{w}(\mathbf{e}) \leq (d_{FR}-1)/2$ より.
2. $U_1 \cap U_2 = \emptyset$ であることから従う.
3. U_0, U_1 の定義から従う.
4. $u_0 + u_2 \leq \#(i,j) \mid m_{i,j} = 1 = \mathrm{w}(\mathbf{e})$ より.
5. $2(u_0 + u_2) + 1 \leq W(\ell) = u_1 + u_2 + u_3$, および $u_1 \leq 2u_0$ から従う.
6. U_3 の定義から, X の第 j 列は第 $v\,(1 \leq v < j)$ 列の線形従属であることが従う.

□

2.5 Feng-Rao 復号法

基底表示 (Definition 1) から，$\ell \geq 1$ について

$$\alpha_{\ell+1}^{(i,j)}\langle \mathbf{e}, \mathbf{b}_{\ell+1}\rangle = \langle \mathbf{e}, \mathbf{b}_i * \mathbf{b}_j\rangle - \sum_{\mu=1}^{\ell} \alpha^{(i,j)}\langle \mathbf{e}, \mathbf{e}_\mu\rangle$$

が従う．一方 Lemma 6 (5),(6) から，$U \setminus U_1$ に属する (i,j) について，$\langle \mathbf{e}, \mathbf{b}_i * \mathbf{b}_j\rangle$ を多数決により決定すると正しい値であることが保証される．よって次の命題が成り立つ．

Proposition 2 (多数決決定) $Mwte \leq (d_{FR}-1)/2$ を仮定する．$\langle \mathbf{e}, \mathbf{b}_i\rangle$ *for* $1 \leq {}^{\forall} i \leq \ell$ が既知であるとする．U の元 (i,j) に対し，小行列 $\bar{X} := (\langle \mathbf{e}, \mathbf{b}_u * \mathbf{b}_v\rangle)\ 1 \leq u \leq i, 1 \leq v \leq j$ に対して *Algorithm 1* を適用する．各 $(i,j) \in U \setminus U_1 = U_2 \cap U_3$ に対して，

$$\sum_{\lambda=1}^{j-1} v_\lambda^{(j)}\langle \mathbf{e}, \mathbf{b}_\lambda * \mathbf{b}_j\rangle$$

を計算する．これを $\langle \mathbf{e}, \mathbf{b}_i * \mathbf{b}_j\rangle$ の推定値とする．$\mathbf{b}_i * \mathbf{b}_j$ の基底表示 *(Definition 1)* から得られる $\langle \mathbf{e}, \mathbf{b}_{\ell+1}\rangle$ のうち最も多く現れたものが真の値である．すなわち，

$$(\sum_{\lambda=1}^{j-1} v_\lambda^{(j)}\langle \mathbf{e}, \mathbf{b}_\lambda * \mathbf{b}_j\rangle - \sum_{\mu=1}^{\ell} \alpha_\mu^{(i,j)}\langle \mathbf{e}, \mathbf{b}_\mu\rangle)/\alpha_{\ell+1}^{(i,j)}$$

のうち最も多く現れた値が，$\langle \mathbf{e}, \mathbf{b}_{\ell+1}\rangle$ に等しい．

Definition 14 (Feng-Rao 復号アルゴリズム) つぎのものを準備する．$\sigma(\mathbf{b}_i * \mathbf{b}_j) \geq r+1$ をみたすような $(\mathbf{b}_i, \mathbf{b}_j)$ に対し，

$$\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^{\ell} \alpha_l^{(i,j)} \mathbf{b}_l$$

Input: $\mathbf{y} := \mathbf{c} + \mathbf{e}$

Output: $\mathbf{c}$ もしくは，途中で中断する．

1. [Initialize] $\langle \mathbf{e}, \mathbf{b}_l\rangle = \langle \mathbf{y}, \mathbf{b}_l\rangle$ *for* $1 \leq {}^{\forall} l \leq r$
   $s_{i,j} = \langle \mathbf{y}, \mathbf{b}_i * \mathbf{b}_j\rangle$ *for* ${}^{\forall}(i,j)$ *s.t.* $\sigma(\mathbf{b}_i * \mathbf{b}_j) \leq r$
   $\ell \leftarrow r+1$
2. [Apply Gauss algorithm] $S = (s_{i,j})$ に *Gauss algorithm (Algorithm 1)* を適用する．
3. [Calculate $\langle \mathbf{e}, \mathbf{b}_\ell\rangle$] *(*)* をみたす (i,j) について，

   $$(\sum_{\lambda=1}^{j-1} v_\lambda^{(j)}\langle \mathbf{e}, \mathbf{b}_\lambda * \mathbf{b}_j\rangle - \sum_{\mu=1}^{\ell} \alpha_\mu^{(i,j)}\langle \mathbf{e}, \mathbf{b}_\mu\rangle)/\alpha_{\ell+1}^{(i,j)}$$

   を計算し，もっとも多く現れた値を $\langle \mathbf{e}, \mathbf{b}_\ell + \mathbf{1}\rangle$ とする．ただし *(*)* とは，

   $$(\mathbf{b}_i, \mathbf{b}_j) \text{ が } well-behaved \text{ でかつ},$$
   $$\sigma(\mathbf{b}_i * \mathbf{b}_j) = \ell \text{でかつ},$$
   $$c_i > j \text{ かつ}, c_u \neq j \ for \ \forall u < i \ s.t. \ \sigma(\mathbf{b}_u * \mathbf{b}_v) \leq \ell - 1$$

   をみたす (i,j) をいう．*(*)* をみたす (i,j) が存在しなければ復号を諦める．

4. [Loop] $\ell < n$ ならば $\ell \leftarrow k+1$ として，*2*へ行け．

5. [Terminate]

$$ {}^t\mathbf{e} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix}^{-1} \begin{pmatrix} \langle \mathbf{e}, \mathbf{b}_1 \rangle \\ \vdots \\ \langle \mathbf{e}, \mathbf{b}_n \rangle \end{pmatrix} $$

を計算する． $\mathbf{c} := \mathbf{y} - \mathbf{e}$ を返す．

3 Feng-Rao 復号法と Berlekamp-Massey 復号法

3.1 あらまし

この節では， G-L. Feng, K.K.Tzeng が論文 [1] のなかで示した《Feng-Rao 復号法は BCH 符号の復号における Berlekamp-Massey 復号法を含む一般化である》ことを検証する．

BCH 符号における Vandermonde 行列を用いた Feng-Rao 復号法について，成分 $\langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle$ を推定する過程は，Berlekamp-Massey 復号法におけるエラー位置多項式の計算を行う過程と同じ行列の操作であることがわかる．

3.2 BCH 符号とは

Definition 15 (BCH 符号) β を $\mathcal{F}_{q^m}$ の原始 n 乗根とする．正整数 n, l, δ を与える．$\beta^l, \beta^{l+1}, \ldots, \beta^{l+\delta-2}$ の最小多項式の最小公倍多項式を $g(x)$ とおく．

環 $\mathcal{F}_q[x]/(x^n-1)$ のイデアル $\langle g(x) \rangle$ を考える．このとき，

$$ C := \{(c_0, \ldots, c_{n-1}) \in {\mathcal{F}_q}^n \mid \langle g(x) \rangle \ni c(x) = \sum_{i=0}^{n-1} c_i x^i\} $$

は $\mathcal{F}_q$ 上の符号となる． この C を *BCH (Bose-Chaudhuri-Hocquenghem)* 符号という．

BCH 符号について次の Lemma がなりたつ:

Lemma 7 $(\delta-1) \times n$ 行列 H を次のように定める．

$$ H := \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \ldots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \ldots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \ldots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix} $$

このとき， *BCH*符号 C は

$$ C = \{\mathbf{c} \in {\mathcal{F}_q}^n \mid H\ {}^t\mathbf{c} = \mathbf{0} \text{ in } \mathcal{F}_{q^m}^{(\delta-1)}\} $$

をみたす．

Definition 16 ${\mathcal{F}_q}^n \ni \mathbf{y}$ に対し,

$$H\ {}^t\mathbf{y} = \begin{pmatrix} S_0 \\ S_1 \\ \vdots \\ S_{\delta-2} \end{pmatrix}$$

とおく. $S_0, \ldots, S_{\delta-2}$ をシンドロームと呼ぶ.

3.3 Berlekamp-Massey 復号法とは

Definition 17 ${\mathcal{F}_{q^m}}^{\delta-1} \ni \mathbf{a} = (a_0, \ldots, a_{\delta-2})$ に対し,

$$\ell(\mathbf{a}) := \max \#\{i \mid a_u \neq 0 \text{ for } 0 \leq {}^{\forall}u \leq i\}$$

とする. $\ell(\mathbf{a})$ を $\mathbf{a}$ の 長さと呼ぶ.

J.L. Massey の論文 [3] によれば, この定義の下で BCH 符号における復号問題は次の問題におきかえることができる.

[Massey による BM 復号法の行列表示][3]

$$\begin{pmatrix} p_0 \\ \vdots \\ p_{\delta-2} \end{pmatrix} = \begin{pmatrix} 1 & & & 0 \\ c_1 & 1 & & \\ \vdots & \ddots & \ddots & \\ c_{\delta-2} & \cdots & c_1 & 1 \end{pmatrix} \begin{pmatrix} S_0 \\ \vdots \\ S_{\delta-2} \end{pmatrix}$$

をみたす $\mathbf{c} \in {\mathcal{F}_{q^m}}^{\delta-2}, \mathbf{p} \in {\mathcal{F}_{q^m}}^{\delta-1}$ のうち, $\ell(\mathbf{p})$ を最小にするものを, 右辺の行列を上の行から順に線形従属性を調べることで見つけよ.

このことは次のように言いかえることができる.

[BM 復号法の言いかえ]

$$\begin{pmatrix} S_0 & S_1 & \cdots & S_{\delta-2} \\ S_1 & \cdots & S_{\delta-2} & \\ \vdots & & & \\ S_{\delta-2} & & & 0 \end{pmatrix} \begin{pmatrix} 1 & c_1 & c_2 & \cdots & c_{\delta-2} \\ & 1 & c_1 & \cdots & c_{\delta-3} \\ & & \ddots & \ddots & \vdots \\ & & & 1 & c_1 \\ 0 & & & & 1 \end{pmatrix}$$
$$= \begin{pmatrix} p_0 & p_1 & \cdots & p_{\delta-2} \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$$

をみたす $\mathbf{c} \in {\mathcal{F}_{q^m}}^{\delta-2}, \mathbf{p} \in {\mathcal{F}_{q^m}}^{\delta-1}$ のうち, $\ell(\mathbf{p})$ を最小にするものを, 左辺の行列の積を左の列から順に Gauss の消去法を用いて線形従属性を調べることで見つけよ.

3.4 Vandermonde 行列を用いた BCH 符号の Feng-Rao 復号法

$n \times n$ 行列 B を,

$$B = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{n-1} & \beta^{2(n-1)} & \cdots & \beta^{(n-1)(n-1)} \end{pmatrix} \tag{2}$$

とおく. このとき B は Vandermonde 行列である. $\det B \neq 0$ であるから B の各 i 行を $\mathbf{b}_i$ とおくと $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ は $\mathcal{F}_{q^m}^n$ の基底をなす.

$$\begin{aligned} X'(\mathbf{e}) &:= B \begin{pmatrix} e_0 & & & & 0 \\ & \beta^l e_1 & & & \\ & & \beta^{2l} e_2 & & \\ & & & \ddots & \\ 0 & & & & \beta^{(n-1)l} e_{n-1} \end{pmatrix} {}^tB \\ &= \begin{pmatrix} S_0 & S_1 & \cdots & S_{\delta-2} & \langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle & * \\ S_1 & \cdots & S_{\delta-2} & \langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle & * & * \\ \vdots & & & & & \vdots \\ S_{\delta-2} & \langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle & * & * & * & * \\ \langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix} \end{aligned}$$

とする.

3.5 Feng-Rao 復号法と Berlekamp-Massey 復号法との比較

BCH 符号におけるこれら 2 つの復号法を比較する. $X'(\mathbf{e})$ を用いて BCH 符号の Feng-Rao 復号を行うとき, 成分 $\langle \mathbf{e}, \mathbf{b}_{\delta-1} \rangle$ を決定するための操作は Berlekamp-Massey 法における エラー位置多項式の係数ベクトル $\mathbf{c}$ を決定するための操作と同等である.

この後, Feng-Rao 復号法は各 $\langle \mathbf{e}, \mathbf{b}_i \rangle$ for $\delta \leq i \leq n$ を求めて B^{-1} との積をとって復号するのに対して, Berlekamp-Massey 法は $\mathbf{c}, \mathbf{p}$ を用いて決まるエラー位置多項式およびエラー評価多項式から復号する点が異なっている.

4 最後に

一般の線形符号における Feng-Rao 復号法を紹介した. Feng-Rao bound および Feng-Rao 復号法は, 符号 C および $C^\perp$ の基底 $\{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ および $\mathcal{F}^n \setminus C^\perp$ の基底 $\{\mathbf{b}_{r+1}, \ldots, \mathbf{b}_n\}$ の選びかたと並べかたに依存する. そこで, 符号 C が与えられたときに基底と並べかたをどのように選べばよいかという問題が残っている.

参考文献

[1] Gui-Liang Feng and Kenneth K. Tzeng, "A Generalization of the Berlekamp-Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes", IEEE Transactions on Information Theory, vol 37, No 1., pp. 1274-1287, Sep. 1991.

[2] Gui-Liang Feng and T.R.N.Rao, "Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance", IEEE Transactions on Information Theory, vol 39, No 1., pp. 37-45, Jan. 1993.

[3] James L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Transactions on Information Theory, vol IT-15, No 1., pp. 122-127, Jan. 1969.

[4] 三浦 晋示, 代数幾何に基づく誤り訂正符号の研究, 博士論文, 東京大学, 1997.

[5] Ruud Pellikaan, "The shift bound for cyclic, Reed-Muller and geometric Goppa codes", Appeared in *Arithmetic, Geometry and Coding Theory 4*, Luminy 1993 (R. Pellikaan, M. Perret and S.G. Vlăduţ eds.), Walter de Gruyter & Co, Berlin, pp. 155-174, 1996.