数理解析研究所講究録 1395 巻 2004 年 104-110

多項式GCDを用いた復号法に関する研究

上原 剛
UEHARA GO
愛媛大学大学院 理工学研究科
GRADUATE SCHOOL OF SCIENCE AND ENGENEERING, EHIME UNIVERSITY*

甲斐 博
KAI HIROSHI
愛媛大学 工学部
DEPARTMENT OF COMPUTER SCIENCE, EHIME UNIVERSITY†

野田 松太郎
NODA MATU-TAROW
愛媛大学 工学部
DEPARTMENT OF COMPUTER SCIENCE, EHIME UNIVERSITY‡

1 はじめに

誤り訂正符号は通信路の信頼性向上を目的とした技術である．広く用いられている符号の一つに Reed-Solomon(RS) 符号がある．近年，Gao により RS 符号の新しい復号法 (以下，Gao 復号法と呼ぶ) が提案されている [1]．その手法には，符号化する前の情報語を直接求めることができるという特徴がある．Gao 復号法は，他の復号問題へも応用が可能とされているが，その詳細については明らかにされていない．そこで本研究では Gao 復号法の応用について考える．代数幾何符号は復号コストの問題で未だ実用までには至っていないが，非常に広範囲の符号であり，その中には良い性能を持つ符号がいくつか存在することが知られている．RS 符号が一変数多項式上で定義されるのに対し，それらを多変数多項式上にまで一般化したものが代数幾何符号である．その中でも代表的なものの一つに，エルミート曲線符号が存在する．本研究では Gao 復号法を多変数にまで拡張するステップとして，エルミート曲線符号を対象とし，擬除算による手法について考える．

2 Gao復号法

Gao 復号法は，有限体上の多項式補間と，拡張ユークリッドアルゴリズム (EEA) を用いた RS 符号復号アルゴリズムである．有限体 $\mathbf{F}_q$ 上の RS 符号は次のように定義される．

*uehara@hpc.cs.ehime-u.ac.jp
†kai@cs.ehime-u.ac.jp
‡noda@cs.ehime-u.ac.jp

定義 1 (RS 符号) n, k を $1 \leq k < n \leq q$ となる整数とし，それぞれ定義する符号の情報長，符号長とする．$\mathbf{F}_q$ の n 個の元 $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbf{F}_q$ を定める．$\mathbf{F}_q$ の元を係数とする一変数多項式の集合を $\mathbf{F}_q[x]$ とすると，情報語 $f(x) \in \mathbf{F}_q[x]$，符号語 $\mathbf{c} \in \mathbf{F}^n$ は，

$$f(x) \in \mathbf{F}_q[x], \quad (\deg(f(x)) < k) \tag{1}$$

$$\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \quad (c_i = f(\alpha_i) \quad \alpha_i \in \mathbf{F}_q) \tag{2}$$

となる．

符号語 $\mathbf{c}$ に誤り $\mathbf{e}$ が加わったものを受信語 $\mathbf{r}$ とする．復号問題とは $\mathbf{r}$ から符号語 $\mathbf{c}$ を求め，対応する $f(x)$ を求めることである．Gao 復号法では直接 $f(x)$ を求める．Gao アルゴリズムは以下のようなものである．

アルゴリズム 1 (Gao 復号法)
入力 受信語 $\mathbf{r} = (r_1, r_2, \ldots, r_{n-1}) \in \mathbf{F}_q^n$
出力 情報語 $f(x)$，もしくはエラーメッセージ

1. **(Interpolation)** $n-1$ 次以下で，$g_1(\alpha_i) = r_i$ $(0 \leq i \leq n-1)$ となるような $g_1(x)$ を求める．
2. **(Partial GCD)** $g_1(x)$，$g_0(x)$ に，EEA を適用する．このとき，$g(x) = u(x)g_0(x) + v(x)g_1(x)$ となる $g(x)$ が EEA の各ステップで求まるが，$g(x)$ の次数が $\frac{1}{2}(n+k)$ より小さくなったとき EEA を停止する．
3. **(Division)** $g(x)$ を $v(x)$ で割る．もし，余りが 0 なら商を出力し，これが情報語 $f(x)$ となる．余りが 0 でないなら，エラーメッセージを出力．

Gao 復号法は次の補助定理をベースとしている [1].

補助定理 1 ある二組の一変数多項式 $g_0(x)$，$g_1(x)$ が，

$$g_0(x) = w_0(x)a_0(x) + \epsilon_0(x) \tag{3}$$

$$g_1(x) = w_0(x)a_1(x) + \epsilon_1(x) \qquad (\gcd(a_0(x), a_1(x)) = 1) \tag{4}$$

となるような多項式であるとする．さらに，式 (3)，(4) が次の条件を満たすとする．

$$\deg(a_i(x)) \leq t, \quad \deg(\epsilon_i(x)) \leq l \quad (i = 0, 1) \tag{5}$$

$$\deg(w_0(x)) \geq d_0 > l + t \tag{6}$$

このとき，EEA を $g_0(x)$，$g_1(x)$ に適用する．EEA により求まる剰余を $g(x)$ とする．また，そのときの $g_0(x)$，$g_1(x)$ の係数をそれぞれ $u(x)$，$v(x)$ とする．すなわち $g(x) = u(x)g_0(x) + v(x)g_1(x)$ となる．このとき，$g(x)$ の次数が d_0 より小さくなるまで EEA を実行すれば，

$$u(x) = -\alpha a_1(x), \quad v(x) = \alpha a_0(x) \quad (\alpha \in \mathbf{F}_q) \tag{7}$$

となる．

Gao復号法では，全点で解を持つ多項式を $g_0(x)$，受信語 $\mathbf{r}$ を多項式補間したものを $g_1(x)$ として補助定理1を適用する．誤り位置 ($e_i \neq 0$ となる i) でのみ α_i を解として持つ多項式を $w(x)$，逆に誤り位置以外 ($e_i = 0$ となる i) でのみ解を持つ多項式を $w_0(x)$ とする．すなわち，

$$w(x) = \prod_{e_i \neq 0}(x - \alpha_i), \quad w_0(x) = \prod_{e_i = 0}(x - \alpha_i) \quad (0 \leq i \leq n-1) \tag{8}$$

とする．また，$\bar{w}(x)$ を以下のように定義する．

$$\bar{w}(\alpha_i) = \frac{e_i}{w_0(\alpha_i)} \quad (0 \leq i \leq n-1) \tag{9}$$

このとき，$g_0(x)$，$g_1(x)$ は次のようになる [1]．

$$g_0(x) = w_0(x)w(x) \tag{10}$$

$$g_1(x) = w_0(x)\bar{w}(x) + f(x) \tag{11}$$

補助定理1を，$a_0(x)$，$a_1(x)$ をそれぞれ $w(x)$，$\bar{w}(x)$ とし，$\epsilon_0(x)$，$\epsilon_1(x)$ をそれぞれ 0，$f(x)$ として適用する．式 (7)，(10)，(11) より，

$$\begin{aligned} g(x) &= \alpha\bar{w}(x)g_0(x) - \alpha w(x)g_1(x) \\ &= w_0(x)(\alpha w(x)\bar{w}(x) - \alpha\bar{w}(x)w(x)) - \alpha w(x)f(x) \\ &= -\alpha w(x)f(x) \end{aligned} \tag{12}$$

となる $\alpha w(x)$，$g(x)$ が得られる．ゆえに，$f(x)$ を得ることが可能となる．

3 エルミート曲線符号

エルミート曲線符号は代数幾何符号の一種である．代数幾何符号には，EvaluationCodes とその双対として定義される符号とが存在する [2]．本論では以降，特に断らない限り代数幾何符号といえばEvaluationCodes を指すことにする．代数幾何符号は，重み付き次数による項順序を用いて定義される．$\mathbf{F}[X] = \mathbf{F}[x_1, x_2, \ldots, x_m]$ を有限体 $\mathbf{F}$ 上の $x_1, x_2, \ldots, x_m$ を変数とする多変数多項式環とする．X_i $(0 \leq i \leq n-1)$ をある重み付き次数 ρ により定義され，全ての X_i で，$\rho(X_i) < \rho(X_{i+1})$ が成立するような基底とする．また，I を $\mathbf{F}[X]$ のあるイデアルとし，$\mathbf{P} = \{P_0, P_1, \ldots, P_{n-1}\}$ を I の零点集合とする．

定義 2 (代数幾何符号) $\mathbf{F}[X]/I$ において X_{k-1} までの基底の線形結合により生成される多項式を情報語 $f(X) = \sum_{i=0}^{k-1} f_i X_i, (f_i \in \mathbf{F})$ とする．代数幾何符号の符号化は，

$$(f_0, f_1, \ldots, f_{k-1}) \longrightarrow (f(P_0), f(P_1), \ldots, f(P_{n-1})) \tag{13}$$

となる．

エルミート曲線符号は $\mathbf{F} = \mathrm{GF}(\mathrm{q}^2)$ 上で，$\mathbf{F}[X] = \mathbf{F}[x, y]$ とし，$I = \{x^q + x - y^{q+1}, x^{q^2} - x, y^{q^2} - y\}$ により定義される．重み付き次数には $\rho(x^a y^b) = (q+1)a + qb$ が用いられる．

4 Gao復号法の適用 (擬除算による)

Gao復号法のエルミート曲線符号への適用について考える．$\mathbf{F} = \mathrm{GF}(\mathrm{q}^2)$ とする．$\mathbf{F}[X] = \mathbf{F}[x, y]$ とし，$I = I_G = \{x^q + x - y^{q+1}, y^{q^2} - y\}$，$\mathbf{P} = \{P_0, P_1, \ldots, P_{n-1}\}$ を I の零点集合とする．項順序には，

$\rho(x^a y^b) = (q+1)a + qb$ による重み付き辞書式順序 $(y \prec x)$ を用いる．Gao復号法を適用するためには，まず受信語 $\mathbf{r} = \mathbf{c} + \mathbf{e}$ の多項式補間 $\mathbf{F}^n \longrightarrow \mathbf{F}[X]/I$ を行なう必要がある．そのような多項式補間が可能であることを以下に示す．

補助定理 2 $\mathbf{P} = \{(\alpha_0, \beta_0), (\alpha_1, \beta_1), \ldots, (\alpha_{n-1}, \beta_{n-1})\}$ に対して，

$$\frac{y^{q^2} - y}{y - \beta_i} = \prod_{\{j | j \neq i\}} (y - \beta_j), \quad \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} = \prod_{\{j | \beta_j = \beta_i, \alpha_j \neq \alpha_i\}} (x - \alpha_j) \tag{14}$$

が成立する．

証明 前者に関しては，$y^{q^2} - y$ が $\mathrm{GF}(\mathrm{q}^2)$ の全ての元を解として持つことから導かれる．後者も同様に考えることができる．今，$y = \beta_i$ を固定する．このとき $x^q + x - \beta_i^{q+1}$ の解は，$\{(\alpha_j, \beta_j) \mid \beta_j = \beta i\}$ となる．ゆえに，

$$\begin{aligned} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} &= \frac{1}{x - \alpha_i} \prod_{\{j | \beta_j = \beta_i\}} (x - \alpha_j) \\ &= \prod_{\{j | \beta_j = \beta_i, \alpha_j \neq \alpha_i\}} (x - \alpha_j) \end{aligned} \tag{15}$$

となり右辺が得られる．

定理 3 $\mathbf{F} = \mathrm{GF}(\mathrm{q}^2)$ とする．また，$\mathbf{F}[X] = \mathbf{F}[x, y]$，$I = I_G = \{y^{q^2} - y, x^q + x - y^{q+1}\} \in \mathbf{F}[X]$ とする．I の共通零点を $\mathbf{P} = \{P_0, P_1, \ldots, P_{n-1}\}$ とし，$P_i = (\alpha_i, \beta_i), (\alpha_i, \beta_i \in \mathbf{F})$ とする．さらに，$\mathbf{F}[X]/I$ の基底を $X_i, (0 \leq i \leq n-1)$ とする．今，

$$a(x, y) = \sum_{i=0}^{n-1} a_i X_i \in \mathbf{F}[X]/I \tag{16}$$

$$\mathbf{A} = (A_0, A_1, \ldots, A_{n-1}) = (a(P_0), a(P_1), \ldots, a(P_{n-1})) \in \mathbf{F}^n \tag{17}$$

とする．このとき，

$$a(x, y) = -\sum_{i=0}^{n-1} A_i \frac{y^{q^2} - y}{y - \beta_i} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} \tag{18}$$

となる．

証明 一変数の場合の Lagrange 補間を拡張する．

$$f_i(\alpha_j, \beta_j) = f_i(P_j) = \begin{cases} 0 & (i \neq j) \\ 1 & (i = j) \end{cases} \tag{19}$$

となるような多項式 $f_i(x, y) \in \mathbf{F}[X]/I$ を考える．このとき，$a(x, y)$ は，

$$a(x, y) = \sum_{i=0}^{n-1} A_i f_i(x, y) \tag{20}$$

と表すことができる．

今，$f_i(x,y)$ を

$$f_i(x,y) = \frac{y^{q^2}-y}{y-\beta_i}\frac{x^q+x-\beta_i^{q+1}}{x-\alpha_i} \tag{21}$$

とし，条件を満たしていることを確認する．

補助定理 2 より，

$$f_i(\alpha_j,\beta_j) = 0 \quad (\beta_j \neq \beta_i \text{もしくは} \beta_j = \beta_i, \alpha_j \neq \alpha_i) \tag{22}$$

がいえる．また，$y^{q^2}-y$ は $y-\beta_i$ で割り切れることに注意すると，

$$\begin{aligned}\frac{y^{q^2}-y}{y-\beta_i} &= y^{q^2-1}+\beta_i y^{q^2-2}+\cdots+\beta_i^{q^2-2}y+\beta_i^{q^2-1}-1 \\ &= \beta_i^{q^2-1}\sum_{j=0}^{q^2-1} y^j\beta_i^{-j}-1\end{aligned} \tag{23}$$

が得られる．式 (23) を $f_{Yi}(y)$ とし，β_i を代入すると

$$\begin{aligned}f_{Yi}(\beta_i) &= \beta_i^{q^2-1}\sum_{j=0}^{q^2-1}\beta^j\beta_i^{-j}-1 = \beta_i^{q^2-1}\sum_{j=0}^{q^2-1}1-1 \\ &= q^2\beta_i^{q^2-1}-1\end{aligned} \tag{24}$$

を得る．今，GF(q^2) は GF(q) の拡大体であるので，式 (24) は，

$$f_{Yi}(\beta_i) = q^2\beta_i^{q^2-1}-1 = -1 \tag{25}$$

となる．同様に，$x^q+x-\beta_i^{q+1}$ と，$x-\alpha_i$ は，

$$\begin{aligned}\frac{x^q+x-\beta_i^{q+1}}{x-\alpha_i} &= x^{q-1}+\alpha_i x^{q-2}+\cdots+\alpha_i^{q-2}x+\alpha_i^{q-1}+1 \\ &= \alpha_i^{q-1}\sum_{j=0}^{q-1}x^j\alpha_i^{-j}+1\end{aligned} \tag{26}$$

を得る．式 (26) を $f_{Xi}(x)$ とし，α_i を代入すると，

$$f_{Xi}(\alpha_i) = q\alpha_i^{q-1}+1 = 1 \tag{27}$$

を得る．よって，式 (25)，(27) より，$f_i(x,y) = -f_{Yi}(y)f_{Xi}(x)$ とすれば，

$$f_i(\alpha_j,\beta_j) = 1 \quad (i=j) \tag{28}$$

を満たすことが分かる．

RS 符号，BCH 符号における Gao 復号法では，補間した多項式 $g_0(x)$ とある多項式 $g_1(x)$ との間で多項式 GCD を計算する．しかし，多変数の場合，GCD 計算を単純に行なうことはできない．そこで，y 変数のみに注目した擬除算による EEA を適用する．また，停止条件を y の次数により定義する．

符号化には I_G の全ての零点 $\mathbf{P}$ を用いることにする．すなわち $n=q^3$ とする．式 (18) より，誤りを $\mathbf{e}$，補間した多項式を $e'(x,y)$ とすると，

$$\begin{aligned}e'(x,y) &= -\sum_{i=0}^{n-1} e_i\frac{y^{q^2}-y}{y-\beta_i}\frac{x^q+x-\beta_i^{q+1}}{x-\alpha_i} \\ &= -\sum_{e_i\neq 0} e_i\frac{y^{q^2}-y}{y-\beta_i}\frac{x^q+x-\beta_i^{q+1}}{x-\alpha_i}\end{aligned} \tag{29}$$

となる．誤り位置 ($e_i \neq 0$ となる i) でのみ β_i を解として持つ y 変数多項式を $w(y)$，逆に誤り位置以外 ($e_i = 0$ となる i) でのみ β_i を解として持つ y 変数多項式を $w_0(y)$ とする．つまり，

$$w(y) = \prod_{e_i \neq 0}(y - \beta_i), \quad w_0(y) = \prod_{e_i = 0}(y - \beta_i) \quad (0 \leq i \leq n-1) \tag{30}$$

となる．式 (29) の分子分母に $w(y)$ をかけると，

$$\begin{aligned} e'(x,y) &= -\sum_{e_i \neq 0} e_i \frac{y^{q^2} - y}{w(y)} \frac{w(y)}{y - \beta_i} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} \\ &= -\frac{y^{q^2} - y}{w(y)} \sum_{e_i \neq 0} e_i \frac{w(y)}{y - \beta_i} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} \\ &= -w_0(y) \sum_{e_i \neq 0} e_i \frac{w(y)}{y - \beta_i} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} \end{aligned} \tag{31}$$

となる．式 (31) において，

$$\bar{w}(x,y) = \sum_{e_i \neq 0} e_i \frac{w(y)}{y - \beta_i} \frac{x^q + x - \beta_i^{q+1}}{x - \alpha_i} \tag{32}$$

とすると，

$$e'(x,y) = w_0(y)\bar{w}(x,y) \tag{33}$$

となる．

このとき，y 次数にのみ注目し擬除算による Gao 復号法を適用することが可能である．

補助定理 3 GF(q^2) 上のエルミート曲線符号において，誤りベクトル e を補間した多項式 $e'(x,y)$ を式 (33) で定義する．誤りの数を t とし，$0 \leq t \leq q^2$ であるとする．このとき，$w(y)$，$w_0(y)$ の y 次数 $\deg_y(w(y))$，$\deg_y(w_0(y))$ は，

$$\deg_y(w(y)) \leq t, \quad \deg_y(w_0(y)) \geq q^2 - t \tag{34}$$

となる．

証明 式 (30) より，$y^{q^2} - y = w_0(y)w(y)$ である．また，$e_i = e(\alpha_i, \beta_i)$ であり，$e_i \neq 0$ となる $P_i = (\alpha_i, \beta_i)$ で，相異なる β_i はせいぜい t 個となる．ゆえに，解の数と次数の関係より，

$$\deg_y(w(y)) \leq t \tag{35}$$

$$deg_y(w_0(y)) = \deg_y(y^{q^2} - y) - \deg_y(w(y)) \geq q^2 - t \tag{36}$$

となる．

以上より，y 変数のみに注目し Gao 復号法を適用することができる．

$g_0(y) = y^{q^2} - y$ (全ての β_i を解として持つ多項式) とする．$g_1(x,y) = e'(x,y) + f(x,y)$ とし，$g_0(y)$，$g_1(x,y)$ に補助定理 1 を適用することを考える．

補助定理 1 の，$a_0(x)$，$a_1(x)$ をそれぞれ $w(y)$，$\bar{w}(x,y)$，$\epsilon_0(x)$，$\epsilon_1(x)$ をそれぞれ 0，$f(x,y)$ とする．このとき，$w(y)$，$\bar{w}(x,y)$ は共通解を持たない．ゆえに，$\gcd(w(y), \bar{w}(x,y)) = 1$ である．また，その次数は，

$$\deg_y(w(y)) \leq t \tag{37}$$

$$\deg_y(w_0(y)) \geq q^2 - t \tag{38}$$

$$\deg_y(\bar{w}(x,y)) = \deg_y(g_1(x,y)) - \deg_y(w_0(y)) \geq q^2 - (q^2 - t) = t \tag{39}$$

となる．以上のことから次の定理が成立する．

定理 4 エルミート曲線符号において，$\deg_y(f(x,y)) = k_y - 1$ とする．このとき，

$$q^2 - 2t > k_y - 1 \tag{40}$$

が成立すれば，y 変数に注目した擬除算による Gao 復号法を用いて t 誤り訂正が可能である．

擬除算によるエルミート曲線符号の Gao 復号アルゴリズムは次のようになる．

アルゴリズム 2 (擬除算による Gao 復号法)
入力 受信語 $\mathbf{r} = (r_1, r_2, \ldots, r_{n-1}) \in \mathbf{F}_{q^2}^n$
出力 情報語 $f(x,y)$，もしくはエラーメッセージ

1. **(Interpolation)** 定理 3 に基づき多項式補間を行なう．
   $g_1(\alpha_i, \beta_i) = r_i \quad (0 \leq i \leq n-1)$.
2. **(Partial GCD)** $g_1(x,y)$, $g_0(y)$ に，擬除算による EEA を適用する．このとき，$g(x,y) = u(x,y)g_0(x,y) + v(x,y)g_1(x,y)$ となる $g(x,y)$ が EEA の各ステップで求まるが，$\deg_y(g(x,y))$ が $q^2 - t$ より小さくなったとき EEA を停止する．
3. **(Division)** $g(x,y)$ を $v(x,y)$ で割る．もし，余りが 0 なら商を出力し，これが情報語 $f(x,y)$ となる．余りが 0 でないなら，エラーメッセージを出力．

5 擬除算による手法の問題点

エルミート曲線符号の場合，符号長 n，情報長 k，最小距離 d は，$k + d \geq n + 1 - g$ となることが知られている (g は gaps と呼ばれる定数 [2])．定義 2 より，k は基底単項式の数と一致する．訂正能力 t は最小距離 d により，$t = \frac{d-1}{2}$ となる．ゆえに，t は k に依存し，t を 1 増やすためには基底を 2 減らすことになる．これに対し，式 (40) では，t を 1 増やすためには情報語 $f(x,y)$ の y 次数を 2 減らす必要がある．この場合，一方の変数の次数にのみ注目しているため，単項式基底による空間を有効に利用することができず，十分な訂正能力を得ることができない．ゆえに，真の意味で Gao 復号法を代数幾何符号の復号に応用するためには重み付き次数を考慮に入れた多項式イデアルとしての拡張が必要であると考えられる．加えて，EEA のような計算や，さらにそれを途中で停止するような条件を考える必要がある．

参 考 文 献

[1] S.Gao: A new algorithm for decoding Reed-Solomon codes, in *Communications, Information and Network Security* (V. Bhargava, H. V. Poor, V. Tarokh and S. Yoon, Eds.), Kluwer Academic Publishers, 2003, pp.55-68.

[2] T.Hoholdt and J.H. van Lint and R.Pellikaan: Algebraic geometry codes, in *Handbook of Coding Theory* vol 1, (V.S. Pless, W.C. Huffman and R.A. Brualdi, Eds.), Elsevier, Amsterdam 1998, pp.871-961.