線形代数だけで理解する代数幾何符号

松本 隆太郎
東京工業大学 電気電子工学科 坂庭研究室
〒 152-8552 目黒区大岡山 2-12-1
E-mail: ryutaroh@ss.titech.ac.jp
URL: http://tsk-www.ss.titech.ac.jp/~ryutaroh/

1999 年 12 月 11 日*

1 はじめに

Goppa により 1981 年に提案された代数幾何符号 [3] は文字通り代数幾何の概念を使って定義されるので, 代数幾何に馴染みの無い人には大変取っ付きにくい分野であった. しかし, Høholdt らにより導入された重み関数の概念を用いることにより, 代数幾何符号を代数幾何を用いずともごまかし無しに理解することが可能になった. 本稿では代数幾何符号の主要な概念を線形代数と初等環論のみを用いて解説する. 命題にはすべて完全な証明を付けている. 第 2 節では代数幾何符号の Feng-Rao 復号アルゴリズムと Feng-Rao 限界を任意の線形符号に適用できるように, 線形代数だけを用いて定義し直す. 第 3 節では Høholdt らにより提案された線形代数と初等環論だけを用いた代数幾何符号の定義を紹介する.

小文を通して, $\mathbf{F}_q$ を要素数 q の有限体とし, $\mathbf{F}_q^n$ を有限体の要素を n 個並べたベクトルからなる線形空間とする. また $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}, \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}, \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ を $\mathbf{F}_q^n$ の基底とする. W を $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ の空でない真部分集合とし, W の要素を検査行列の行に持つ線形符号を $C(W)$ で表す.

2 Feng-Rao 限界と Feng-Rao 復号アルゴリズム

この節では 1993 年に Feng と Rao により提案された復号アルゴリズム [1], および符号の誤り訂正能力を損なわずに検査シンボル数を減らす方法 [2] を紹介する. ここで紹介する内容は三浦の論文 [10, 3 章], [11] を多少一般化したものである.

2.1 Feng-Rao 限界

本小節では $C(W)$ の最小距離の下界を与える. ベクトル $\boldsymbol{a}, \boldsymbol{b} \in \mathbf{F}_q^n$ に対し $\boldsymbol{a} * \boldsymbol{b}$ は $\boldsymbol{a}$ と $\boldsymbol{b}$ を座標ごとに掛けて得られるベクトルとする.

定義 **2.1** $\mathcal{W}_i$ を $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_i$ で張られる線形空間とし $\mathcal{W}_0 = \{\boldsymbol{0}\}$ とする. $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ が, ある $1 \le s \le n$ に対し $\boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$ かつすべての $1 \le u \le i, 1 \le v \le j, (u, v) \ne (i, j)$ について $\boldsymbol{u}_u * \boldsymbol{v}_v \in \mathcal{W}_{s-1}$

*2000 年 6 月 1 日に参考文献の “to appear” になっている部分を実際の巻数, ページ数に更新した.

となるとき, 振舞いが良いという. $1 \le s \le n$ について $M(s) := \{(i, j) \mid \boldsymbol{u}_i * \boldsymbol{v}_j \in \mathcal{W}_s \setminus \mathcal{W}_{s-1}$ かつ $(\boldsymbol{u}_i, \boldsymbol{v}_j)$ は振舞いが良い $\}$ と定義する.

定義 **2.2** $C(W)$ に対する **Feng-Rao** 限界は

$$\delta_{\mathrm{FR}}(W) := \min\{\sharp M(s) \mid \boldsymbol{w}_s \notin W\}$$

で定義される. 但し, $\sharp M$ は集合 M の要素数を表す.

定義 **2.3** ベクトル $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ に対しシンドローム行列 $S(\boldsymbol{y})$ を

$$S(\boldsymbol{y}) := \begin{pmatrix} \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_n \end{pmatrix} \begin{pmatrix} y_1 & & \\ & \ddots & \\ & & y_n \end{pmatrix} \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix}^T$$

で定義する. また $w(\boldsymbol{y})$ で $\boldsymbol{y}$ のハミング重みを表す.

命題 **2.4** ベクトル $\boldsymbol{y}$ に対し $\operatorname{rank} S(\boldsymbol{y}) = w(\boldsymbol{y})$. また $S(\boldsymbol{y})$ の (i, j) 成分は $\langle \boldsymbol{y}, \boldsymbol{u}_i * \boldsymbol{v}_j \rangle$ で与えられる. 但し $\langle , \rangle$ はベクトルの内積を表す.

証明**:** 最初の主張は $S(\boldsymbol{y})$ の定義より明らか. また,

$$S(\boldsymbol{y}) = \begin{pmatrix} \boldsymbol{y} * \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{y} * \boldsymbol{u}_n \end{pmatrix} \begin{pmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_n \end{pmatrix}^T$$

であるので, $S(\boldsymbol{y})$ の (i, j) 成分は $\langle \boldsymbol{y} * \boldsymbol{u}_i, \boldsymbol{v}_j \rangle$ になるが, これは $\langle \boldsymbol{y}, \boldsymbol{u}_i * \boldsymbol{v}_j \rangle$ に等しい. ■

命題 **2.5** $C(W)$ の最小距離は $\delta_{\mathrm{FR}}(W)$ 以上である.

証明**:** $\boldsymbol{y}$ を $C(W)$ の $\boldsymbol{0}$ でない符号語とし, ある整数 s に対し $\langle \boldsymbol{y}, \boldsymbol{w}_1 \rangle = \cdots = \langle \boldsymbol{y}, \boldsymbol{w}_{s-1} \rangle = 0$, $\langle \boldsymbol{y}, \boldsymbol{w}_s \rangle \neq 0$ が成立しているとする. このとき $\boldsymbol{w}_s \notin W$ である. 一方, 任意の $(i, j) \in M(s)$ に対し $S(\boldsymbol{y})$ の (i, j) 成分は非零である. なぜならば $\boldsymbol{u}_i * \boldsymbol{v}_j$ は $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_s$ の線形結合で書け, 線形結合の $\boldsymbol{w}_s$ の係数は非零なので,

$$\begin{aligned} \langle \boldsymbol{y}, \boldsymbol{u}_i * \boldsymbol{v}_j \rangle &= \left\langle \boldsymbol{y}, \sum_{\ell=1}^{s} c_\ell \boldsymbol{w}_\ell \right\rangle \\ &= \sum_{\ell=1}^{s} c_\ell \langle \boldsymbol{y}, \boldsymbol{w}_\ell \rangle \\ &= c_s \langle \boldsymbol{y}, \boldsymbol{w}_s \rangle \\ &\neq 0. \end{aligned}$$

また同様にすべての $1 \le u \le i, 1 \le v \le j, (u, v) \neq (i, j)$ について $S(\boldsymbol{y})$ の (u, v) 要素は 0 である. $M(s)$ の要素は行列の右上から左下にかけて並んでいるので, $\operatorname{rank} S(\boldsymbol{y}) \ge \sharp M(s) \ge \delta_{\mathrm{FR}}(W)$ を得る.

■

例 **2.6 (Reed-Solomon 符号)** Reed-Solomon 符号の最小距離が Feng-Rao 限界の特殊な場合として得られることを例を挙げて示す. α を $\mathbf{F}_q$ の原始元, $i = 1, \ldots, n(= q-1)$ に対し $\boldsymbol{u}_i = \boldsymbol{v}_i = \boldsymbol{w}_i = (1^i, \alpha^i, \ldots, \alpha^{i(q-2)})$ とする. このとき $\boldsymbol{u}_i * \boldsymbol{v}_j = \boldsymbol{w}_{i+j-1}$ なので, $M(s) = \{(1,s), (2,s-1), \ldots, (s,1)\}$ となる. $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$ と取る. このとき $C(W)$ は $[q-1, q-1-r]$ Reed-Solomon 符号になり, $\delta_{\mathrm{FR}}(W) = r+1$ はその最小距離に等しい.

W として添え字が小さい順に $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$ と取るのが従来の代数幾何符号に相当するが, Feng と Rao は設計距離 d を実現するために集合 W を

$$W(d) := \{\boldsymbol{w}_s \mid \sharp M(s) \leq d-1\}$$

のように取ると検査シンボル数をより少なくできることを明らかにした [2]. この構成法は改良代数幾何符号と呼ばれる.

2.2 Feng-Rao 復号アルゴリズム

符号を実用に供するためには効率的な復号アルゴリズムが不可欠である. 本小節では $C(W)$ に通信の過程で生じた $\lfloor(\delta_{FR}(W)-1)/2\rfloor$ 個以下の誤りを $O(n^3)$ 回の有限体の演算で訂正する **Feng-Rao** 復号アルゴリズムを示す.

符号語 $\boldsymbol{c} \in C(W)$ が送信され $\boldsymbol{c}+\boldsymbol{e}$ が受信されたとする. $\langle \boldsymbol{e}, \boldsymbol{w}_1\rangle, \ldots, \langle \boldsymbol{e}, \boldsymbol{w}_n\rangle$ が分かれば行列の掛け算により $O(n^2)$ 回の演算で誤りベクトル $\boldsymbol{e}$ を求めることができる.

$\boldsymbol{w}_s \in W$ なら $\langle \boldsymbol{c}+\boldsymbol{e}, \boldsymbol{w}_s\rangle = \langle \boldsymbol{e}, \boldsymbol{w}_s\rangle$ である. 従って, $\boldsymbol{u}_i * \boldsymbol{v}_j$ が W の要素の線形結合で書ける場合, 受信語から $S(\boldsymbol{e})$ の (i,j) 成分を知ることができる. $S(\boldsymbol{e})$ の既知の部分から未知の部分を正しく推測するアルゴリズムを以下に示す.

A を対角成分がすべて 1 の $n \times n$ 下三角行列とする. $B := AS(\boldsymbol{e})$ とおく. B の各々の行 i につき A の左下部分を適当に設定して $\min\{j \mid B$ の (i,j) 成分は非零 $\}$ を最大化することを考える. 今ある行 i について $\min\{j' \mid B$ の (i,j') 成分は非零 $\}$ を最大化し j になったとする. このとき (i,j) を $S(\boldsymbol{e})$ の **discrepancy** と呼ぶ. 以下 $S(\boldsymbol{e})$ のすべての要素が分かっているという仮定のもとで discrepancy を求めるアルゴリズムを示す. B の (i,j) 成分が零になるように, B の i 行に $i'(<i)$ 行の定数倍を加える操作を, すべての (i,j) について行うだけのアルゴリズムである.

アルゴリズム **2.7**

A を単位行列に初期化する.
for $i = 1, \ldots, n$ **do**
  for $j = 1, \ldots, n$ **do**
    if $B_{ij} \neq 0$ かつ
    すべての $j' < j$ について $B_{ij'} = 0$ **then**
      if ある $i' < i$ が存在して $B_{i'j} \neq 0$ かつ
      すべての $j' < j$ について $B_{i'j'} = 0$ **then**
        A の i 行から A の i' 行を $B_{ij}/B_{i'j}$ 倍して引く. このとき $B_{ij} = 0$ となり (i,j) は discrepancy ではない.
      else

今 $B_{ij} \neq 0$ かつすべての $i' < i$, $j' < j$ について $B_{i'j} = B_{ij'} = 0$ である. $B_{ij} = \langle A$ の i 行, $S(\boldsymbol{e})$ の j 列 $\rangle$ である. また, i 番目が 1 で $i+1, \ldots, n$ 番目が 0 であるすべての横ベクトルは A の $1, \ldots, i$ 行の線形結合でかけるが, A の i 行をどのような A の $1, \ldots, i$ 行の線形結合 (但し A の i 行の係数は 1) で置き換えても B_{ij} を 0 にすることはできない. なぜならばすべての $j' < j$ について $B_{ij'} = 0$ だからである. したがって (i, j) は discrepancy である.

endif

else

$B_{ij} = 0$ または (i, j) の左に既に discrepancy があるので, (i, j) は discrepancy ではない.

endif

endfor

endfor

上記のアルゴリズムからすべての行 i について $\min\{j \mid B$ の (i, j) 成分は非零 $\}$ を最大にする行列 A が存在することと, 各行各列につき discrepancy は高々1 個しかないことがわかる. アルゴリズム2.7実行後 B の discrepancy に相当する成分の左にある成分および上にある成分はすべて 0 である. したがって B の階数は discrepancy の総数に等しく, $S(\boldsymbol{e})$ の階数は discrepancy の総数に等しい.

$L(s) := \{(u, v) \mid$ ある $t \leq s$ に対し $(i, j) \in M(t)$ が存在して $1 \leq u \leq i$, $1 \leq v \leq j$ かつ $(u, v) \neq (i, j)$ である $\}$ とする. $L(s)$ に対応する $S(\boldsymbol{y})$ のすべての成分がわかっているとする. このときアルゴリズム2.7を (i, j) 成分に対して実行するとき $S(\boldsymbol{e})$ のすべての (u, v) 成分 (但し $u \leq i$, $v \leq j$) が既知であればアルゴリズムが実行できるので, $L(s)$ に含まれる要素に限定してアルゴリズム2.7を実行することができる. このとき以下のように $\langle \boldsymbol{e}, \boldsymbol{w}_s \rangle$ の値を正しく推測することができる.

$(i, j) \in M(s)$ の左または上に discrepancy が無かった場合, $S(\boldsymbol{e})$ の (i, j) 成分を (i, j) が discrepancy にならないように推測する. 具体的には

$$-\sum_{i=1}^{i-1} A_{ik} S(\boldsymbol{e})_{kj}$$

と推測する. (i, j) 成分に対する推測値から $\langle \boldsymbol{e}, \boldsymbol{w}_s \rangle$ の推測値が決定される. この推測が真の値に等しい (i, j) の数を T, 間違っている数を F, $L(s)$ の中で既に見つかっている discrepancy の数を K とする. このとき推測が誤っているのは (i, j) が discrepancy になっているときだけなので $K + F \leq$ discrepancy の総数 $=$ rank $S(\boldsymbol{e}) = w(\boldsymbol{e})$ が成り立つ. また推測の仕方より $\sharp M(s) \leq T + F + 2K$ が成り立つ. もし $2w(\boldsymbol{e}) < \delta_{\mathrm{FR}}(W)$ $(\leq \sharp M(s))$ ならばこれらの不等式より $T > F$ が成り立つ. このとき $\langle \boldsymbol{e}, \boldsymbol{w}_s \rangle$ の推測値の中で多数を占めるものが正しい値になる. $\langle \boldsymbol{e}, \boldsymbol{w}_s \rangle$ の値から $L(s+1) \setminus L(s)$ にあたる $S(\boldsymbol{e})$ の成分が計算できる. このあと $L(s+1) \setminus L(s)$ の成分についてアルゴリズム2.7 を実行し, $S(\boldsymbol{e})$ の $M(s+1)$ に対応する成分を推測する. $M(s)$ に対応する $S(\boldsymbol{e})$ の成分を推測した後, $L(s)$ の成分についてアルゴリズム2.7を実行しても結果は変わらないので, 実行する必要はない.

より高速な復号アルゴリズムについては [13, 14] を参照せよ.

注 **2.8** 本稿では $\boldsymbol{u}_i = \boldsymbol{v}_i = \boldsymbol{w}_i$ となる例しか挙げないが, $\mathcal{L}$ 型代数幾何符号の復号では $\boldsymbol{u}_i \neq \boldsymbol{v}_i = \boldsymbol{w}_i$ とすると高い誤り訂正能力を実現できる [8].

3 線形代数だけを使った代数幾何符号の定義

Høholdt, van Lint, Pellikaan は [4, 5] において代数幾何符号を線形代数と重み関数という概念を使って定式化し直した. 本節では彼らの定式化を紹介する.

3.1 重み関数と符号

定義 **3.1** [5, Definition 3.5] R を $\mathbf{F}_q$ を含む可換環とし, $\mathbf{N}_0$ を非負整数の集合とする. このとき写像 $\rho : R \to \mathbf{N}_0 \cup \{-\infty\}$ がすべての $f, g \in R$ について以下の条件を満たすとき重み関数という.

1. $\rho(f) = -\infty \Leftrightarrow f = 0$.
2. すべての $0 \neq c \in \mathbf{F}_q$ について $\rho(cf) = \rho(f)$.
3. $\rho(f+g) \leq \max\{\rho(f), \rho(g)\}$. 等号は $\rho(f) \neq \rho(g)$ のとき成立.
4. $\rho(f) = \rho(g) \neq -\infty$ なら, $\rho(f - cg) < \rho(g)$ となる $c \in \mathbf{F}_q$ が存在する.
5. $\rho(fg) = \rho(f) + \rho(g)$.

d が $\rho(R \setminus \{0\})$ の最大公約数なら ρ/d も重み関数である. 簡単のため以降では重み関数 ρ の最大公約数は 1 とする. また $R \neq \mathbf{F}_q$ を常に仮定する.

命題 **3.2** [5, Proposition 3.12] お互いに重み関数 ρ の値が異なる R の $\mathbf{F}_q$ 基底が存在する.

証明**:** 各々の $i \in \rho(R \setminus \{0\})$ について $\rho(h_i) = i$ となる h_i を任意に選ぶ. このとき重み関数の定義より $\{h_i \mid i \in \rho(R \setminus \{0\})\}$ は $\mathbf{F}_q$ 上線形独立である. なぜなら線形結合 $d_1h_1 + \cdots + d_th_t$ に非零な係数があったとすると, $\rho(d_1h_1 + \cdots + d_th_t) = \max\{\rho(h_i) \mid d_i \neq 0\} \neq -\infty$ より $d_1h_1 + \cdots + d_th_t \neq 0$ だからである.

$g \in R \setminus \{0\}$ とすると, ある $c \in \mathbf{F}_q$ が存在し, $\rho(g - ch_{\rho(g)}) < \rho(g)$ とできる. この議論を高々 $(\rho(g)+1)$ 回繰り返すことにより

$$g - \sum_{i \in \rho(R \setminus \{0\})} c_i h_i$$

の重み関数 ρ の値を $-\infty$ にする $\{c_i \mid i \in \rho(R \setminus \{0\})\}$ が存在することが分かる. つまり g は $\{h_i\}$ の線形結合で書ける. ■

$\rho(f_i) < \rho(f_{i+1})$ を満たす R の基底 $\{f_i \mid i = 1, 2, \ldots\}$ をこれ以降固定する. また $\mathbf{F}_q^n$ に座標ごとの積を導入して環と見なし, 環の全射準同型 $\varphi : R \to \mathbf{F}_q^n$ が与えられているとする. $\{g_1, \ldots, g_n\} := \{f_i \mid \varphi(f_i)$ は $\varphi(f_1), \ldots, \varphi(f_{i-1})$ で張られる線形空間に属さない $\}$ とし $\rho(g_1) < \cdots < \rho(g_n)$ と添え字付けされているとする. 第 1 節に述べた $\mathbf{F}_q^n$ の基底 $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ などを $\boldsymbol{u}_i = \boldsymbol{v}_i = \boldsymbol{w}_i = \varphi(g_i)$ と定義する. 性能の良い線形符号を作るためには $\sharp M(s)$ は大きいほど良いが, 以上のように $\boldsymbol{u}_i$ などを定めたとき $\sharp M(s)$ はあまり小さくならないことを以下に示す.

補題 **3.3** $\rho(g_i) + \rho(g_j) = \rho(g_s)$ ならば $(i, j) \in M(s)$ である.

証明**:** $\rho(h) \leq \rho(g_s)$ である $h \in R$ について

$$\begin{aligned} \varphi(h) &\in \mathcal{W}_s \setminus \mathcal{W}_{s-1} \text{ if } \rho(h) = \rho(g_s), \\ \varphi(h) &\in \mathcal{W}_{s-1} \text{ if } \rho(h) < \rho(g_s) \end{aligned}$$

である. すべての $1 \leq u \leq i, 1 \leq v \leq j, (u, v) \neq (i, j)$ について $\rho(g_u g_v) < \rho(g_s)$ であることから主張は導かれる. ■

$g := \sharp(\mathbf{N}_0 \setminus \rho(R \setminus \{0\}))$ とする.

命題 **3.4** [5, Theorem 5.24] $\sharp M(s) \geq s - g$.

証明**:** まず $\rho(g_i f_j) = \rho(g_s)$ を満たす (g_i, f_j) の数を数える. ある g_i に対して $\rho(g_i f_j) = \rho(g_s)$ となる f_j が存在しないのは $\rho(g_s) - \rho(g_i) \in \mathbf{N}_0 \setminus \rho(R \setminus \{0\})$ となるときに限る. 従って $\rho(g_i f_j) = \rho(g_s)$ を満たす (g_i, f_j) の数は $s - g$ 以上である.

つぎに $\rho(g_i f_j) = \rho(g_s)$ なら $g_{j'} = f_j$ となる添え字 j' が存在することを示す. これが示されれば前補題より主張の証明が終了する. もしそのような添え字 j' が存在しないとすると

$$\varphi(f_j) = \sum_{\ell=1}^{j-1} c_\ell \varphi(f_\ell)$$

と書ける. 従って $\varphi(g_s)$ が

$$\begin{aligned} \varphi(g_s) &= d\varphi(g_i f_j) + \sum_{k=1}^{s-1} e_k \varphi(g_k) \\ &= \sum_{\ell=1}^{j-1} d c_\ell \varphi(g_i f_\ell) + \sum_{k=1}^{s-1} e_k \varphi(g_k) \end{aligned}$$

のように g_s より真に重み関数の値が小さい要素に写像 φ を作用させて得られるベクトルの線形和で書けることになり, g_s の定義に矛盾する. ■

命題3.4より, $W = \{\varphi(g_1), \ldots, \varphi(g_{n-k})\}$ と取ると, $C(W)$ は $[n, k, d]$ 線形符号 $(d \geq n - k + 1 - g)$ になることが分かる. 情報レート k/n に対し相対最小距離 d/n を大きくするためには g に比較して n を大きく取る必要がある. [7] の結果と Hasse-Weil-Serre の定理 [15, Theorem V.3.1] より n の最大値は $q + 1 + g\lfloor 2\sqrt{q} \rfloor$ であることがわかる. 符号長 n を g に対して大きく取れる環 R の構成法は次節で述べる.

3.2 可換環 R と重み関数 ρ の具体例

実際に符号を構成するためには $g_1, \ldots, g_n$ および φ が計算可能である必要がある. 以下符号構成が可能な可換環 R と重み関数 ρ の例を挙げる. $2 \leq a < b$ を互いに素な整数とし, $F(X, Y)$ を

$$Y^a + X^b + \sum_{ai+bj<ab} \alpha_{i,j} X^i Y^j$$

という形の二変数多項式とおく. I を $F(X, Y)$ で生成される二変数多項式環 $\mathbf{F}_q[X, Y]$ のイデアルとし, $R := \mathbf{F}_q[X, Y]/I$ とする. このとき

$$B := \{X^i Y^j \mid 0 \leq i,\ 0 \leq j \leq a - 1\},$$

とすると $\{X^i Y^j \bmod I \mid X^i Y^j \in B\}$ は剰余類環 R の基底になる. 単項式 $X^i Y^j$ の重み付き次数を $ai + bj$ と定め, 非零な多項式の重み付き次数を最大の重み付き次数を持つ項の重み付き次数とする. $G(X, Y)$ が B の要素の非零な線形結合で表される多項式であるとき, $G(X, Y) \bmod I \in R$ に対し重み関数 ρ の値を $G(X, Y)$ の重み付き次数と定め, $\rho(0) = -\infty$ と定める. B に含まれる単項式は互いに異なる重み付き次数を持つため, 上に定めた ρ が重み関数の定義を満たすことを確認するには, $f, g \in R$ に対し $\rho(fg) = \rho(f) + \rho(g)$ を確認すればよい.

$G_1(X, Y), G_2(X, Y)$ が非零な B の単項式の線形結合で表される多項式とし, 各々の重み付き次数が最高の項を $X^{i_1} Y^{j_1}, X^{i_2} Y^{j_2}$ とすると, $G_1(X, Y) G_2(X, Y)$ の重み付き次数最高の項は $X^{i_1+i_2} Y^{j_1+j_2}$

である. $G_1(X,Y)G_2(X,Y)$ を Y を変数とする一変数多項式と見て $F(X,Y)$ で割り算をすることにより得られる余りを $H(X,Y)$ とすると $G_1(X,Y)G_2(X,Y) \bmod I = H(X,Y) \bmod I$ であるが, $F(X,Y)$ の形から $H(X,Y)$ の重み付き次数は $a(i_1+i_2)+b(j_1+j_2)$ で $G_1(X,Y)$ と $G_2(X,Y)$ の重み付き次数の和に等しい. 従って上に定めた ρ が重み関数の定義を満たすことが確認できた. 従って, $\{f_1, f_2, \ldots\}$ は B に含まれる単項式で代表される R の剰余類に取ることができる.

$\sharp(\mathbf{N}_0 \setminus \rho(R \setminus \{0\}))$ が $\sharp M(s)$ の下界を決めたがこの場合

$$\mathbf{N}_0 \setminus \rho(R \setminus \{0\}) = \mathbf{N}_0 \setminus \{ia + bj \mid 0 \le i,\ 0 \le j \le a-1\}$$

であるので, $g = \sharp(\mathbf{N}_0 \setminus \rho(R \setminus \{0\})) = (a-1)(b-1)/2$ である.

最後に符号構成を行うために全射準同型 φ を具体的に計算する必要がある. $x := X \bmod I$, $y := Y \bmod I$ とし, $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)$ を方程式 $F(X,Y) = 0$ の $\mathbf{F}_q^2$ における相異なる解とする. M_i を R の $x - \alpha_i, y - \beta_i$ で生成される極大イデアルとすると, $G(X,Y) \bmod I \in R$ に $G(\alpha_i, \beta_i)$ を対応させる写像は $G(X,Y) \bmod I \in R$ に $G(X,Y) \bmod I$ で代表される剰余類環 R/M_i の要素を対応させているとみることができる. 写像

$$\begin{aligned} R &\longrightarrow \mathbf{F}_q^n, \\ G(X,Y) \bmod I &\longmapsto (G(\alpha_1, \beta_1), \ldots, G(\alpha_n, \beta_n)) \end{aligned}$$

は写像

$$\begin{aligned} R &\longrightarrow \mathbf{F}_q^n, \\ g &\longmapsto (g \bmod M_1, \ldots, g \bmod M_n) \end{aligned}$$

に等しく, $M_1, \ldots, M_n$ は相異なる極大イデアルなので, 中国の剰余定理[1]よりこの写像は全射になる. 従って φ として $F(X,Y) = 0$ の異なる解を代入する写像を選んで良い. $\{\varphi(g_1), \ldots, \varphi(g_n)\}$ は $\varphi(f_1), \varphi(f_2), \ldots$ を計算したあと線形従属なベクトルを除くことで得られる.

注 **3.5** (α, β) が $F(X,Y) = 0$ の解でなければ, $G(X,Y) \bmod I \in R$ に (α, β) を「代入」する操作はそもそも写像にならない. $G(X,Y) \bmod I$ と $G(X,Y) + F(X,Y) \bmod I$ は R に属する同じ要素だが $G(\alpha,\beta) \neq G(\alpha,\beta) + F(\alpha,\beta)$ だからである.

注 **3.6** 本小節で述べた形の多項式 $F(X,Y)$ は 1992 年に三浦により代数幾何符号の構成に必要な情報がすべてわかる代数曲線族 $\boldsymbol{C_a^b}$ 曲線として提案された [9].

例 **3.7** 情報レート k/n に対し相対最小距離 d/n が大きい符号を作るには $g = \sharp(\mathbf{N}_0 \setminus \rho(R \setminus \{0\})) = (a-1)(b-1)/2$ に対し解の数が多い多項式 $F(X,Y)$ が必要だが, 例えば

$$F(X,Y) = Y^q + Y - X^{q+1} = 0$$

は $\mathbf{F}_{q^2}$ 内に q^3 個の解を持ち, $g = q(q-1)/2$ となる多項式の中で $\mathbf{F}_{q^2}^2$ 内の解の数が最大の多項式である. g に対し解の数が多い多項式はコンピュータによる全数探索以外に見つける方法は無いと思われる. 多くの解を持つ多項式の表が [9] にある.

注 **3.8** 重み関数を持つ環の構成法は他に [5, Proposition 3.17, Example 3.22], [10, 定理 5.17], [12, p.1401 主定理] に示されている. 特に [10, 定理 5.17], [12, p.1401 主定理] は重み関数を持つすべての環を与える構成法になっている.

[1]初等代数の教科書を見よ.

3.3 従来の代数幾何符号との関係

本節で述べた Høholdt らの線形符号の構成法と従来の代数幾何符号の関係を述べる. 読者が代数幾何を用いて代数幾何符号を理解していることを前提として記述する. 特に断らない限り表記法は Stichtenoth の教科書 [15] に従う. $F/\mathbf{F}_q$ を一変数代数関数体, $P_1, \ldots, P_n, Q$ を相異なる一次の座, $D := P_1 + \cdots + P_n$ とする. このとき代数幾何符号 $C_\Omega(D, mQ)$ は符号

$$\{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(mQ)\}$$

の双対符号として与えられる. これは3.1節の構成法を使い以下のように構成できる. $\mathcal{L}(\infty Q) := \bigcup_{i=1}^{\infty} \mathcal{L}(iQ)$ とおくと $\mathcal{L}(\infty Q)$ は関数体 F の部分環になる. また ρ を Q における離散付値を -1 倍したものとすると ρ は $\mathcal{L}(\infty Q)$ の重み関数になる. $f \in \mathcal{L}(\infty Q)$ に $(f(P_1), \ldots, f(P_n))$ を対応させる写像 φ は $\mathcal{L}(\infty Q)$ から $\mathbf{F}_q^n$ への全射準同型である. $g_1, \ldots, g_n$ を3.1節のように定め, $W := \{\varphi(g_i) \mid \rho(g_i) \leq m\}$ とすれば $C(W)$ は $C_\Omega(D, mQ)$ に等しい. このとき命題3.4における g は関数体 F の種数に等しくなり, d を $C_\Omega(D, mQ)$ の最小距離とすると命題3.4から直ちに Goppa 限界 $d \geq \sharp W + 1 - g$ を導くことができる.

逆に3.1節で構成した符号と従来の代数幾何符号の関係は以下のようになる. 重み関数 ρ を持つ環 R は無限遠に唯一つの $\mathbf{F}_q$ 有理的な座 Q を持つアフィン代数曲線のアフィン座標環になり, 重み関数 ρ は Q における離散付値の負の整数倍で与えられることが示される [7]. R のもとになるアフィン代数曲線が非特異であるとき3.1節で示した符号は代数幾何符号 $C_\Omega(D, mQ)$ またはその改良代数幾何符号になる. 但し, 座 $P_1, \ldots, P_n$ は全射 φ から決まる.

アフィン代数曲線が特異なとき構成される符号は三浦により提案された特異曲線上の線形符号 [10, 12] に等しくなる. 但し, この場合曲線を正規化して得られる非特異曲線上の符号に比べて性能の良い符号は得られない [6].

4 まとめ

代数幾何符号のために提案された Feng-Rao 限界と Feng-Rao 復号アルゴリズムを線形代数だけを用いて定義し, 直し任意の線形符号に適用できるようにした三浦の結果を紹介した. また, 代数幾何符号の構成法を線形代数だけで定義した Høholdt らの結果を紹介した.

謝辞

原稿の間違いおよび分かりにくい部分を指摘して頂いた東工大の坂庭好一教授, ソニーの三浦晋示博士, 阪大の池上大介氏, 東工大の武井由智氏に感謝する.

参考文献

[1] G.L. Feng and T.R.N. Rao, “Decoding algebraic geometric codes up to the designed minimum distance,” IEEE Trans. Inform. Theory, vol.39, pp.36–47, 1993.
[2] ———, “Improved geometric Goppa codes part I, basic theory,” IEEE Trans. Inform. Theory, vol.41, no.6, pp.1678–1693, 1995.
[3] V.D. Goppa, “Codes on algebraic curves,” Soviet Math. Dokl., vol.24, no.1, pp.170–172, 1981.
[4] T. Høholdt, J.H. van Lint, and R. Pellikaan, “Order functions and evaluation codes,” Proc. AAECC-12, Lecture Notes in Computer Science, vol.1255, pp.138–150, Springer-Verlag, 1997.

[5] ———, “Algebraic geometry codes,” in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., pp.871–961, Elsevier, 1998.
[6] R. Matsumoto, “Linear codes on nonsingular curves are better than those on singular curves,” IEICE Trans. Fundamentals, vol.E82-A, no.4, pp.665–670, April 1999.
[7] ———, “Miura’s generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan’s generalization,” IEICE Trans. Fundamentals, vol.E82-A, no.10, pp.2007–2010, Oct. 1999.
[8] R. Matsumoto and S. Miura, “On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes,” IEICE Trans. Fundamentals, vol.E83-A, no.5, pp.923–926, May 2000.
[9] 三浦 晋示, “ある平面曲線上の代数幾何符号,” 電子情報通信学会論文誌, vol.J75-A, no.11, pp.1735–1745, Nov. 1992.
[10] ———, “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, May 1997.
[11] ———, “アフィン代数多様体上の線形符号,” 電子情報通信学会論文誌, vol.J81-A, no.10, pp.1386–1397, Oct. 1998.
[12] ———, “アフィン代数曲線上の線形符号,” 電子情報通信学会論文誌, vol.J81-A, no.10, pp.1398–1421, Oct. 1998.
[13] 阪田 省二郎, “代数幾何符号とその復号法について,” 数理科学, no.421, pp.33–40, July 1998.
[14] ———, “代数幾何符号とその復号法について (続),” 数理科学, no.422, pp.58–65, Aug. 1998.
[15] H. Stichtenoth, “Algebraic function fields and codes,” Springer-Verlag, 1993.