リードソロモン符号

1　基礎知識

1.1　多項式環

R を可換環とするとき、R 上の元を係数とする多項式全体の集合

$$R[T] := \left\{ a_0 + a_1 T^1 + \cdots + a_n T^n \;\middle|\; n \in \mathbb{Z}, 0 \leq n, a_0, \ldots a_n \in R \right\}$$

は可換環を成す。これを多項式環という。

Proof. hoge □

また、$R[T]$ 上のある元 $f(T)$ が

$$f(T) = a_0 + a_1 T^1 + \cdots + a_n T^n$$

と書かれて $a_n \neq 0$ であるとき、n を $f(T)$ の次数といい deg(f(T)) と書く。

1.2　多項式環上での除法

ある体 K による多項式環 $K[T]$ に除法が定義される。

定理 1 : 除法 ある $f(T), g(T) \in K[T], g(T) \neq 0$ に対して

$$f(T) = q(T)g(T) + r(T) \quad (\deg(\mathrm{r(T)}) < \deg(\mathrm{g(T)}))$$

を満たす $q(T), r(T) \in K[T]$ の組が唯一つ存在し $q(T)$ を商、$r(T)$ を剰余という。また $r(T)$ が $r(T) = 0$ であるとき、$g(T)$ は $f(T)$ を割り切るといい $g(T) \mid f(T)$ と書く。そして 2 つの多項式 $f(T), g(T) \in K[T]$ を割り切るモニックな多項式を最大公約多項式という。ここでモニックな多項式とは最高次数の係数が 1 であるような多項式のことである。

1.2.1　イデアル

定理 2 : イデアル ある可換環 R に対して、R の部分集合 I が以下の 2 つを満たすとき、I を R のイデアルという。

1. $a, b \in I \Rightarrow a + b \in I$
2. $a \in I, r \in R \Rightarrow ar \in I$

ある $a \in R$ によって

$$(a) = \{ax \mid x \in R\}$$

と書かれる (a) はイデアルであり、a によって生成される単項イデアルという。また、$a, b \in R$ によって

$$(a, b) = \{ax + by \mid x, y \in R\}$$

と書かれる [tex: (a, b)] もイデアルである。

体 K 上の多項式環 $K[T]$ も可換環であるため $K[T]$ にもイデアルが存在する。このとき、$K[T]$ のイデアルは単項イデアルしか存在しない。

Proof. $I \neq \{0\}$ を $K[T]$ のイデアルとする。I の元のうち最も次元が小さい元を $f(T)$ とする。

ここで、任意に $g(T)$ をとる。そして $g(T)$ を $f(T)$ で割ると

$$g(T) = q(T)f(T) + r(T) \quad (\deg(\mathrm{r(T)}) < \deg(\mathrm{f(T)}))$$

を満たす $q(T), r(T) \in K[T]$ が存在する。また式を変形すると

$$\begin{aligned} g(T) &= q(T)f(T) + r(T) \\ \rightleftharpoons r(T) &= g - q(T)f(T) \\ \rightleftharpoons r(T) &= g + q(T)(-f(T)) \end{aligned}$$

となる。$f(T), g(T) \in I$ であったこととイデアルの定義から $r(T) \in I$ が得られる。ここで、$r(T) \neq 0$ とすると $\deg(\mathrm{r(T)}) < \deg(\mathrm{f(T)})$ であることから $f(T)$ の最小性に矛盾する。したがって $r(T) = 0$ である。よって $g(T) = q(T)f(T)$ となり $g(T) \in (f(T))$ となる。したがって $I \subset (f(T))$ である。

逆に $f(T) \in I$ であるため $(f(T)) \subset I$ でもある。

以上より $I = (f(T))$ が示された。 □

また、$f(T), g(T) \in K[T]$ によって生成されるイデアル $(f(T), g(T))$ は $f(T)$ と $g(T)$ の最大公約多項式を $h(T)$ とすると

$$(f(T), g(T)) = (h(T))$$

が成立する。

Proof. 上述の定理により、ある $n(T) \in K[T]$ が存在し

$$(f(T), g(T)) = (n(T))$$

である。ここで、$f(T), g(T) \in (f(T), g(T))$ なので $f(T), g(T) \in (n(T))$ である。よって $n(T) \mid f(T)$ かつ $n(T) \mid g(T)$ であり、$n(T)$ は $f(T), g(T)$ の公約多項式となる。したがって $n(T) \mid h(T)$ である。

次に、$n(T) \in (f(T), g(T))$ であるため、$n(T) = f(T)x_0(T) + g(T)y_0(T)$ となる $x_0(T), y_0(T) \in K[T]$ が存在する。したがって $h(T) \mid n(T)$ である。

以上より $n(T) \mid h(T)$ かつ $h(T) \mid n(T)$ であるから、ある $q(T), p(T) \in K[T]$ によって

$$h(T) = p(T)n(T)\ n(T) = q(T)h(T)$$

と表される。この式から $n(T)$ を消去すると $h(T) = p(T)q(T)h(T)$ となり、$h(T) \neq 0$ であるため

$$p(T)q(T) = 1$$

となる。したがって $p(T) = q(T) = \pm 1$ となり、$n(T) = h(T), n(T) = -h(T)$ となる。また、$(h(T)) = (-h(T))$ であるため $(f(T), g(T)) = (h(T))$ が示された。 □

1.2.2 不定方程式

さて $(f(T), g(T)) = (h(T))$ であるため、多項式環 $K[T]$ 上の $x(T), y(T) \in K[T]$ を不定元とする不定方程式

$$x(T)f(T) + y(T)g(T) = z(T)$$

は $z(T)$ を $f(T)$ と $g(T)$ の最大公約多項式によって割り切ることできるときに解が存在する。また $x(T) = x\_0(T), y(T) = y\_0(T)$ を一つの解とすると

$$(x_0(T) + m(T)g(T))f(T) + (y_0(T) - m(T)f(T))g(T) = z(T)$$

は任意の $m(T) \in K[T]$ に対して成立する。

したがって、ある不定方程式

$$x(T)f(T) + y(T)g(T) = z(T)$$

の解を一つ得ることができれば他の解も得ることができる。

2 概要

F_q を位数 q のガロア体として行ベクトル $\mathbf{m}, \mathbf{w}, \mathbf{y}$ をそれぞれ

$$\mathbf{m} = (m_0, \cdots, m_{k-1})$$
$$\mathbf{w} = (w_0, \cdots, w_{n-1})$$
$$\mathbf{y} = (y_0, \cdots, y_{n-1})$$

とする。$\mathbf{m}, \mathbf{w}, \mathbf{y}$ はどれも F_q 上のベクトルである。このとき $\mathbf{m}$ を情報系列、$\mathbf{w}$ を符号語、$\mathbf{y}$ を受信語という。また、符号語 $\mathbf{w}$ は F_q 上の $k \times n$ 行列に G よって

$$\mathbf{w} = \mathbf{m}G$$

と表される。この G は F_q 上の原始根 α によって

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \cdots & \alpha^{(k-1)(n-1)} \end{pmatrix}$$

と定義する。そして受信語 $\mathbf{y}$ は符号語 $\mathbf{w}$ が通信路で雑音等によって確率的に変化したものとする。さらに $n-k \times n$ の行列

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \cdots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$

に対して

$$G^t H = 0$$

が成立する。ここで G によって得られる符号語の集合を

$$W = \left\{ \mathbf{m}G \;\middle|\; \mathbf{m} \in F_q^k \right\}$$

とすると、任意の $\mathbf{w} \in W$ に対して

$$\begin{aligned} \mathbf{w}^t H &= \mathbf{m}G^t H \\ &= \mathbf{m}0 \\ &= 0 \end{aligned}$$

となるため、

$$\mathbf{w} \text{ が符号語である} \Rightarrow \mathbf{w}^t H = 0$$

が成立する。また、この符号語全体の集合 W を符号という。

情報系列 $\mathbf{m}$ の各要素を用いて多項式 $m(x)$ を

$$m(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-1} x^{k-1}$$

とすると符号語の各成分 w_i $(i = 0, 1, \cdots, n-1)$ は

$$w_i = m\left(\alpha^i\right)$$

と書くことができる。したがって、$w_i = 0$ となることと $m(x)$ の根に α^i が含まれることは同値である。また、$m(x)$ はたかだか $k-1$ 次の多項式なので根はたかだか $k-1$ 個となる。$n = q$ とすれば任意の i, j に対して

$$\alpha^i \neq \alpha^j$$

となり、ゼロである w_i はたかだか $k-1$ 個であることがわかる。つまり w_i の非ゼロな要素は $n-k+1$ 以上である。これは F_q 上の n 次元ゼロベクトルと符号語とのハミング距離の最小値が $n-K+1$ であることを示している。さらにゼロベクトルと符号語とのハミング距離の最小値は符号語同士のハミング距離の最小値と等しいため、$d_{min} \leq n-k+1$ である。また、シングルトン限界から最大値が $n-k+1$ によってバウンドされるため

$$n-k+1 \leq d_{min} \leq n-k+1 \Leftrightarrow d_{min} = n-k+1$$

が得られ、符号語を探索する半径 t を

$$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$$

とすることで、受信語 $\mathbf{y}$ に対してハミング距離 t の範囲の符号語が一意に定まる。

参考文献

[1] “3 章 リード・ソロモン符号とその復号法 - J-Stage”，https://www.jstage.jst.go.jp/article/itej/70/7/70_571/_pdf，参照 Mar.9,2020.