

Equivalence of Linear Codes

Mitsuru Takigahira

線形空間は一般に一意の基底をもつわけではないため、
線形符号 C の生成行列 G とパリティ検査行列 H は一般に一意でない。
 G 及び H の形式を可能な限り簡単にすることは実用的であり、
例えば 0 の要素が多いほど、計算がより簡単になる。

行基本変形による生成行列の変更

G の行 $\mathbf{r}_1, \dots, \mathbf{r}_k$ は \mathcal{V} の要素で、 \mathcal{C} の基底をなすとみなせる。

行の基本変形、つまり以下の操作

- 行の交換
- 非零な定数と行との掛け算
- 行 \mathbf{r}_i を $\mathbf{r}_i + a\mathbf{r}_j$ で置き換える ($j \neq i, a \neq 0$)

を G に行う場合、 \mathcal{C} の基底は変更されるが、 G の各行が張る部分空間は変わらず \mathcal{C} のままである。

よって、これらの操作をどんな順番で G に対して行っても、得られる新たな生成行列も同じ \mathcal{C} の生成行列となる。

列の入れ替えによる生成行列の変更

G に対する列の入れ替えは C を変更してしまうが、
得られた新たな符号と C との違いは、各符号語のシンボルの順序の点のみである。
よってこの操作で得られた2つの符号は同じ n, k, d, t, M, R etc. の値を持ち、
そのためこれらは基本的にはほとんど変わらない。
このことは次の定義を導く

定義

2つの線形符号 C_1, C_2 が、それぞれ生成行列 G_1, G_2 を持ち

- 行基本変形
- 列の入れ替え

で一方から他方に変形できるとき、符号 C_1, C_2 は同値な符号であるという。
(列を定数倍したり、列に他の列を定数倍して足す操作は認めない)

これは C_1 の全符号語のシンボルの順序を一斉に入れ替えることによって
 C_2 が得られることを意味している。

つまり、 C_1, C_2 はそれぞれ異なる符号語から構成されているが、
実際には「同じ符号である」と考えてしまうということである。

組織符号

行の基本変形と列の入れ替えをうまく行えば、どんな生成行列も次の形にできる

$$G = (I_k \mid P) = \begin{pmatrix} 1 & & & * & * & \cdots & * \\ & 1 & & * & * & \cdots & * \\ & & \ddots & \vdots & \vdots & & \vdots \\ & & & 1 & * & * & \cdots & * \end{pmatrix}$$

I_k は $k \times k$ 単位行列で、 P は $*$ で表された k 行 $n - k$ 列の行列である。

このとき、この G (あるいは C) を組織符号形式と呼ぶ。

この場合、各 $\mathbf{a} = a_1 \dots a_k \in \mathbf{F}_k$ は

$$\mathbf{u} = \mathbf{a}G = a_1 \dots a_k a_{k+1} \dots a_n$$

に符号化され、 $a_1 \dots a_k$ は情報桁、 $a_{k+1} \dots a_n = \mathbf{a}P$ は $n - k$ 桁の検査桁となる。
情報桁は恣意的に決定でき、一方で検査桁は \mathbf{a} 及び G によって一意に決まり、 $\mathbf{a}P$ 中のシンボルとして簡単に計算される

例

例 7.18

§7.1 で扱った $\mathcal{R}_n, \mathcal{P}_n$ それぞれの生成行列 $G_{\mathcal{R}}, G_{\mathcal{P}}$ は組織符号形式である。

$$G_{\mathcal{R}} = (1 \quad 1 \quad \cdots \quad 1), G_{\mathcal{P}} = \begin{pmatrix} 1 & & & -1 \\ & 1 & & -1 \\ & & \ddots & \vdots \\ & & & 1 & -1 \end{pmatrix}$$

例

例 7.19

§7.1 で扱った以下の \mathcal{H}_7 の生成行列 G_1 は組織符号形式ではないが、

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

列の入れ替えによって同値な符号の生成行列 G_2 が得られ、これは組織符号形式。例えば 1 列目を 7 列目に移動するなどの巡回置換 $\pi = (1 \ 7 \ 4 \ 5 \ 2 \ 6 \ 3)$ は

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

を得る

練習問題

練習 7.3

例 7.19 の行列 G_1, G_2 はそれぞれ同値な符号 C_1, C_2 を生成する。
これらの符号は同一か、それとも異なるか？

解答

同一な符号である。

G_1 に対して行基本変形のみを行うことで G_2 を作ることができる為である。 G_1 の各行を $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4$ とおくと、

$$G_2 = \begin{pmatrix} \mathbf{r}_3 + \mathbf{r}_4 \\ \mathbf{r}_2 + \mathbf{r}_4 \\ \mathbf{r}_1 + \mathbf{r}_2 + \mathbf{r}_3 \\ \mathbf{r}_2 + \mathbf{r}_3 + \mathbf{r}_4 \end{pmatrix}$$

とかけることから明らかである。

組織符号形式のパリティ検査行列

線形符号 \mathcal{C} に対する生成行列が

$$G = (I_k \mid P)$$

なる組織符号形式になる場合、 \mathcal{C} に対するパリティ検査行列は

$$H = (-P^T \mid I_{n-k}) \quad (7.3)$$

となる。これはパリティ検査行列に対する組織符号形式である。

補題 7.17 からこれを確認できる。行列 H は $n-k$ 行 n 列で、単位行列 I_{n-k} が各行の線形独立性を保証してくれる。よってこの行列は階数 $n-k$ を持つ。最終的にブロック行列を掛け算することで以下を得る。

$$GH^T = I_k(-P) + PI_{n-k} = -P + P = 0$$

q が 2 の累乗の場合 $a + a = 2a = 0$ for all $a \in \mathbf{F}$ なので、
 $-a = a$ となりマイナスの符号を省略でき、 H をもっと簡単に次のように書ける

$$H = (P^T \mid I_{n-k})$$

例

例 7.20

例 7.1 でから \mathcal{R}_n の生成行列 G が組織符号形式であることがわかり、

$$P = (1 \quad 1 \quad \cdots \quad 1)$$

(P は $n-1$ 個の要素からなる) よって、 \mathcal{R}_n の組織符号形式のパリティ検査行列は

$$\begin{pmatrix} -1 & 1 & & & \\ -1 & & 1 & & \\ \vdots & & & \ddots & \\ -1 & & & & 1 \end{pmatrix}$$

となる。これは例 7.11 のパリティ検査行列とは異なるが、
同じ \mathcal{R}_n に対するパリティ検査方程式の組、つまり

$$-v_1 + v_i = 0 \text{ for } i = 2, \dots, n$$

を与える。

例

例 7.21

例 7.2 で得た \mathcal{P}_n の生成行列は組織符号形式で、

$$P = (-1 \quad -1 \quad \cdots \quad -1)^T$$

(これは $n - 1$ 個の要素からなる) を持つ。よって \mathcal{P}_n は組織符号形式のパリティ検査行列

$$H = (1 \quad 1 \quad \cdots \quad 1)$$

(これは n 個の要素からなる) を持つ。

例

例 7.22

例 7.19 で \mathcal{H}_7 の生成行列の組織符号形式が与えられ、これは

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

を持つ。 $q = 2$ より-の符号を無視し、 \mathcal{H}_7 は組織符号形式のパリティ検査行列

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

を持つ。

(厳密にはこれらは \mathcal{H}_7 と同値な符号の生成行列及びパリティ検査行列であり、 \mathcal{H}_7 のそれぞれの列の入れ替えによって得られるが、既に述べたように基本的に同値な符号を区別しないためこのように書く。)

定理 7.23

組織符号形式の生成行列を用いることで、
線形符号に対するシングルトン限界 (練習 6.18) の別の証明を得ることが出来る。

定理 7.23

C が線形符号で符号長 n 、次元 k 、最小距離 d を持つ場合、

$$d \leq 1 + n - k$$

となる

証明

同値な符号を使うことで、 C は組織符号形式の生成行列 $G = (I_k \mid P)$ を持つとみなせる。よって G の各行は非零の符号語で重みは最大で $1 + n - k$ となる。これは $(I_k$ 中の) ちょうど 1 桁の情報桁と $(P$ 中の) $n - k$ 桁の検査桁を持ち、そのため、その多くとも $1 + n - k$ 桁は非零になる。よって補題 6.8 から $d \leq 1 + n - k$ となる。

例 7.24

\mathcal{R}_n は $k = 1$ かつ $d = n$ でシングルトン限界に達し、 \mathcal{P}_n は $k = n - 1$ かつ $d = 2$ でシングルトン限界に達するが、
 \mathcal{H}_7 は $d = 3$ かつ $1 + n - k = 4$ でシングルトン限界に達さない。

系 7.24

系 7.24

t 重誤り訂正線形 $[n, k]$ 符号は少なくとも $2t$ 桁の検査桁を持つ。

証明

この符号は $n - k$ 桁の情報桁をもち、定理 7.23 と定理 6.10 から $n - k \geq d - 1 \geq 2t$ を得る。

例 7.26

線形符号 \mathcal{R}_3 と \mathcal{H}_7 はともに $t = 1$ を持ち、それぞれ検査桁を $n - k$ 桁、つまり 2 桁と 3 桁持つ。