Matrix Description of Linear Codes

Mitsuru Takigahira

TL;DR

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 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 $\mathbf{r}_1, \ldots, \mathbf{r}_k$ 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 $\mathcal{C}$ を変更してしまうが、
得られた新たな符号と $\mathcal{C}$ 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 $\mathcal{C}_1, \mathcal{C}_2$ 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 $\mathcal{C}_1, \mathcal{C}_2$ 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 $\mathcal{C}_1$ 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
$\mathcal{C}_2$ が得られることを意味している。
つまり、$\mathcal{C}_1, \mathcal{C}_2$ 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

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

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 $\mathcal{C}$) を組織符号形式と呼ぶ。
この場合、各 $\mathbf{a} = a_1 \ldots a_k \in \mathbf{F}_k$ は

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

に符号化され、$a_1 \ldots a_k$ は情報桁、$a_{k+1} \ldots a_n = \mathbf{a}P$ 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。

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

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 $\pi = \begin{pmatrix} 1 & 7 & 4 & 5 & 2 & 6 & 3 \end{pmatrix}$ 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 $\mathcal{C}_1, \mathcal{C}_2$ 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、

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

とかけることからも明らかである。

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

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

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

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

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 からもこれを確認できる。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

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