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 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

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

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 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るが、一方検査桁は一意に $\mathbf{a}$ 及び G によって決定され、$\mathbf{a}P$ 中のシンボルとして簡単に計算される