Minimum Distance of Linear Codes

Mitsuru Takigahira

TL;DR

この節ではパリティ検査行列から線形符号の最小距離を得る方法を示す。

定理 7.27

定理 7.27

$\mathcal{C}$ を最小距離 d の線形符号, H を $\mathcal{C}$ のパリティ検査行列とおく。
このとき、d は線形従属となる H の列の最小個数となる。

証明

補題 7.10 から $\mathbf{v} = v_1 \dots v_n \in \mathcal{V}$ が符号語であることは、
$\mathbf{v}H^T = \mathbf{0}$ あるいは $\mathbf{c}_1, \dots, \mathbf{c}_n$ を H の各列として $\sum_i v_i \mathbf{c}_i = \mathbf{0}$ となることと同値である。
$\mathbf{v} \neq \mathbf{0}$ の場合、この式は列に対する線形従属関係となっていて、
逆にどんな列に対する線形従属関係も非零な符号語 $\mathbf{v}$ に対応している。つまり、
$\mathbf{v}$ の非零な要素 v_i の個数が式に現れる列の数であり、これは $\mathbf{v}$ の重みである。
よって、H の線形従属な列の最小個数が非零な符号語の最小重みに等しく、補題 6.8 からこれは d である

1 つあるいは 2 つの列が線形従属である場合

いくつかの例の前に H の 1 つ又は 2 つの列が線形従属となる意味を確認しよう。

単一の列 $\mathbf{c}_i$ が線形従属であるのは非零な v_i に対して $v_i\mathbf{c}_i = \mathbf{0}$ となるときであり、両辺に v_i^{-1} ($\mathbf{F}$ は体より存在する) をかけると、$\mathbf{c}_i = \mathbf{0}$ と同値であることがわかる。
よって、定理 7.27 から $d = 1$ と H が $\mathbf{0}$ を列に持つことは同値である。

2 つの列 $\mathbf{c}_i, \mathbf{c}_j$ が線形従属であるのは、共に非零な v_i, v_j に対して
$v_i\mathbf{c}_i + v_j\mathbf{c}_j = \mathbf{0}$ となることと同値で、よって条件を $a = -v_j/v_i \in \mathbf{F}\backslash\{0\}$ として
$\mathbf{c}_i = a\mathbf{c}_j$ と書き換えることが出来る。
よって、2 つの非零な列が線形従属であるのは、それぞれ一方が他方の定数倍であることと同値である。(部分的には $q = 2$ のとき $a \neq 0$ ならば $a = 1$ のみで、よって 2 元の場合、2 つの非零列が線形従属となる $\Leftrightarrow$ それぞれの列が等しい)

定理 7.27 から

$d \geq 3 \Leftrightarrow H$ の列がすべて非零で、2 つの列の組が一方が他方の定数倍でない。

2 元の場合、この右側は「H の各列が非零かつ互いに素である」と簡略化される。

例

例 7.28

$\mathcal{P}_n$ のパリティ検査行列 $H = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$ の各列は非零で互いに等しいので、最小距離 d は $d = 2$ である。

例 7.29

$\mathcal{R}_n$ のパリティ検査行列

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

はどんな $n-1$ 個の列も線形独立で、同時に $\mathbf{c}_1 + \cdots + \mathbf{c}_n = \mathbf{0}$ となる。
(これは符号語 $\mathbf{1} = 11\ldots1 \in \mathcal{R}_n$ に対応する) よって $d = n$ である。

例

例 7.30

2 元ハミング符号 $\mathcal{H}_7$ は以下のパリティ検査行列を持ち

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

各列は非零で互いに素より $d \geq 3$、つまり重み 1 または 2 の符号語は存在しない。
しかし、$\mathbf{c}_1 + \mathbf{c}_2 + \mathbf{c}_3 = \mathbf{0}$ で、3 個の線形従属な列があり、
これは $\mathbf{v} = 1110000$ が重み 3 の符号語になる事実に対応している。
(これは例 6.5 で扱った $\mathcal{H}_7$ の基底 $\mathbf{u}_1$ である)
よって、$\mathcal{H}_7$ は最小距離 $d = 3$ を持つ。

シングルトン限界の別証明

パリティ検査行列からシングルトン限界 (定理 7.23) の別証明を与えられる。
もし H が線形 $[n, k]$ 符号のパリティ検査行列ならば、$n - k$ 行は線形独立で、
どんな行列も行と列の階数は等しく、よって H は $n - k$ 個の独立な列を持ち、
同時にすべての $n - k + 1$ 個の列の組は線形従属となる。
よって定理 7.27 から $d \leq n - k + 1$ を得る。

系 7.31

系 7.31

F 上の t 重誤り訂正線形 $[n, k]$ 符号が存在することは、**F** 上に

- 階数 $n - k$
- そのすべての $2t$ 個の列の組が線形独立である

を満たす $(n - k) \times n$ 行列が存在することと同値である

証明 ($\Rightarrow$)

題意を満たす符号 C が与えられ、H が C のパリティ検査行列となるとする。
このとき、H は n 列と $n - k$ 個の独立な行を持つ。
定理 6.10 から C は最小距離 $d \geq 2t + 1$ を持ち、
定理 7.27 からすべての $d - 1$ 個以下の列の組は線形独立となる。
よってすべての $2t$ 個の列の組は線形独立となる。

系 7.31

証明 ($\Leftarrow$)

題意を満たす行列 H が存在し、
$\mathcal{V} = \mathbf{F}^n$、$\mathcal{C} = \{\mathbf{v} \in \mathcal{V} \mid \mathbf{v}H^T = \mathbf{0}\}$ なる $\mathbf{F}$ 上の符号長 n の線形符号とおく。
H は階数 $n-k$ をもち、その $n-k$ 行は線形独立であるため、$\mathcal{C}$ は次元 k を持つ。
仮定より、H のすべての線形従属な列は少なくとも $2t+1$ 個の列を含む。
よって定理 7.27 は $\mathcal{C}$ が最小距離 $d \geq 2t+1$ を持つことを示していて、
そしてそれ故に定理 6.10 から $\mathcal{C}$ は t 個の誤りを訂正する。