Matrix Description of Linear Codes

Mitsuru Takigahira

導入

6 章ではいくつかの線形符号を考え、補題 6.8 で最小距離の計算が線形符号は一般の符号よりも簡単であることを見た。
7 章では線形符号について、最小距離のより簡単な計算法を含む線形代数や行列の定理を適用することによって得られる他の利点に注目し、より詳しく見ていく。
定理的な背景として要求されるものには線形独立性や次元、行や列の演算などの話題が含まれるが、それらは通常大学 1 年生の線形代数の講義で扱われている。
しかしながらそのような講義ではしばしば実数上あるいは複素数上の線形空間や行列に制限しているので、全ての重要な結果や技法について有限体を含む任意の体に拡張する必要がある。
この章を通して $\mathbf{F}$ を何らかの素数 p の累乗数 $q = p^e$ に対して、位数 q の有限体 $\mathbf{F}_q$ とする。

生成行列

線形符号 $\mathcal{C} \subseteq \mathcal{V} = \mathbf{F}^n$ は $\mathcal{C}$ に対する基底 $\mathbf{u}_1, \ldots, \mathbf{u}_k$ を与えることで決定できる。
そのため、符号語 $\mathbf{u} \in \mathcal{C}$ は基底ベクトルの線形結合

$$a_1\mathbf{u}_1 + \cdots + a_k\mathbf{u}_k \ (a_i \in \mathbf{F})$$

で表される。
これは全ての $M = q^k$ 個のベクトルの代わりに、$k = \dim(\mathcal{C})$ の下 k 個のベクトルだけが必要である。
基底を決定する便利な方法には $\mathcal{C}$ の生成行列 G を与えるというものがある。この行列は k 行 n 列で、各行は $\mathcal{C}$ の基底ベクトルの 1 つである。
($\mathcal{C}$ は G をただひとつだけ決定するわけではないことに注意しよう。これは部分空間は多くの基底の組を持ち、与えられた基底ベクトルはどんな順で書いても良いためである。)

生成行列の例

例 7.1 反復符号の生成行列

反復符号 $\mathcal{R}_n$ は唯一の基底 $\mathbf{u}_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$ を持つので、生成行列 G は

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$$

となる

例 7.2 パリティ検査符号の生成行列

$\mathbf{F}$ 上のパリティ検査符号 $\mathcal{P}_n$ は $\mathbf{e}_1, \ldots, \mathbf{e}_n$ を $\mathcal{V}$ の標準基底ベクトルとして、$\mathbf{u}_i = \mathbf{e}_i - \mathbf{e}_n$ なる基底 $\mathbf{u}_1, \ldots, \mathbf{u}_{n-1}$ を持つ。よって生成行列 G は

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

となる

例 7.3 生成行列の例

2 元ハミング符号

2 元ハミング符号 $\mathcal{H}_7$ の基底
$\mathbf{u}_1 = 1110000, \mathbf{u}_2 = 1001100, \mathbf{u}_3 = 0101010, \mathbf{u}_4 = 1101001$ は例 6.5 で与えられた。
よってこの符号の生成行列 G は

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

となる

生成行列による符号の生成

線形符号 $\mathcal{C}$ が次元 k を持つ場合、k 次元の線形空間 $\mathcal{A} = \mathbf{F}^k$ を情報源として、この情報源が G から得られる線形同型写像 $\mathcal{A} \to \mathcal{C} \subseteq \mathcal{V} = \mathbf{F}^n$ によって符号化されるとみなすことが出来る。
具体的に、各語 $\mathbf{a} = a_1 \dots a_k \in \mathcal{A}$ は符号語 $\mathbf{u} = \mathbf{a}G$ ととして符号化され、$\mathcal{A} \to \mathcal{C}$ の間の同型写像 $\mathbf{a} \mapsto \mathbf{u}$ を与える。
そのようにして、符号化は定行列との掛け算で簡単に計算できる。

符号生成の例

例 7.4 反復符号の生成

反復符号 $\mathcal{R}_n$ は次元 $k = 1$ を持つので、$\mathcal{A} = \mathbf{F}^1 = \mathbf{F}$ である。各 $\mathbf{a} = a \in \mathcal{A}$ は $\mathbf{u} = \mathbf{a}G = a \ldots a \in \mathcal{R}_n$ として符号化される

例 7.5 パリティ検査符号の生成

$\mathcal{C} = \mathcal{P}_n$ の場合 $k = n - 1$ である。各 $\mathbf{a} = a_1 \ldots a_{n-1} \in \mathcal{A}$ は $\sum_i a_i = 0$ つまり $a_n = -(a_1 + \cdots + a_{n-1})$ として $\mathbf{u} = \mathbf{a}G = a_1 \ldots a_{n-1}a_n$ に符号化される。

例 7.6 2 元ハミング符号の生成

$\mathcal{C} = \mathcal{H}_7$ の場合 $n = 7, k = 4$ で $\mathcal{A} = \mathbf{F}_2^4$ である。各 $a_1 \ldots a_4 \in \mathcal{A}$ は $\mathbf{u} = \mathbf{a}G \in \mathcal{H}_7 \subset \mathbf{F}_2^7$ として符号化される。例えば、例 6.5 では $\mathbf{a} = 0110$ を

$$\mathbf{u} = \mathbf{a}G = \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

と符号化する。

符号の生成と連立方程式

線形符号 $\mathcal{C}$ に対して生成行列 G が与えられても、ある $\mathbf{v} \in \mathcal{V}$ が $\mathcal{C}$ に含まれるか、そうでない場合どの符号 $\mathbf{u} \in \mathcal{C}$ が最も近いかを決定するのは大変である。
これを簡単にするために、$\mathcal{C}$ の他の行列表現を探すことにしよう。
これを効率的に行う方法は、$\mathcal{C}$ の要素を決定する $n-k$ 個の連立方程式を与えることである。
つまり、あるベクトル $\mathbf{v} \in \mathcal{V}$ はその要素 v_i がそれらの連立方程式を満たすとき、かつそのときのみ $\mathcal{C}$ に含まれるということである。

符号を決定する連立方程式の例

例 7.7 反復符号

反復符号 $\mathcal{R}_n$ は $v_1 = \cdots = v_n$ を満たすベクトル $\mathbf{v} = v_1 \ldots v_n \in \mathcal{V}$ から構成され、これは $n - k = n - 1$ 個の連立方程式 $v_i - v_n = 0\ (i = 1, \ldots, n-1)$ とみなすことが出来る。

例 7.8 パリティ検査符号の例

パリティ検査符号 $\mathcal{P}_n$ ($n - k = 1$ をもつ) は、$\mathcal{V}$ の部分空間で、1 つの一次方程式 $v_1 + \cdots + v_n = 0$ で定義される。

例 7.9 ハミング符号の例

ハミング符号 $\mathcal{H}_7$ は以下の連立方程式を満たすベクトル $\mathbf{v} \in \mathcal{V} = \mathbf{F}_2^7$ から構成される。

$$v_4 + v_5 + v_6 + v_7 = 0$$

$$v_2 + v_3 + v_6 + v_7 = 0$$

$$v_1 + v_3 + v_5 + v_7 = 0$$

パリティ検査行列

一般的に、c 個の独立した一次方程式は次元 $n-c$ の線形部分空間 $\mathcal{V}$ を定義する。
よって、$c = n - k$ 個の独立した一次方程式が $\mathcal{C}$ を決定するのに必要である。
これらはパリティ検査方程式と呼ばれ、それらの係数の行列 H は
n 列で $n-k$ 個の独立した行からなり、$\mathcal{C}$ のパリティ検査行列と呼ばれる。
この連立方程式は $\mathbf{v}H^T = \mathbf{0}$ の形で書け、H^T は H の転置行列である。よって、次の効果的な $\mathcal{C}$ の符号語の検査方法が使える。

補題 7.10

- $\mathcal{C} \subseteq \mathcal{V}$: 線形符号
- H: $\mathcal{C}$ のパリティ検査行列
- $\mathbf{v} \in \mathcal{V}$

とおく。このとき、$\mathbf{v} \in \mathcal{C}$ は $\mathbf{v}H^T = \mathbf{0}$ となるとき、かつそのときのみである。

パリティ検査行列の例

例 7.11 反復符号

$i = 1, \ldots, n-1$ に対して $v_i - v_n = 0$ の連立方程式を使うと、以下の $n-1$ 行 n 列の行列を得る。

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

これは反復符号 $\mathcal{R}_n$ のパリティ検査行列である。

例 7.12 パリティ検査符号

$v_1 + \cdots + v_n = 0$ から、

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

が作れ、これはパリティ検査符号 $\mathcal{P}_n$ のパリティ検査行列である。

パリティ検査行列の例

例 7.13 ハミング符号

$\mathcal{H}_7$ には 3 つの 1 次方程式が例 7.9 で与えられていて、これからパリティ検査符号

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

を得る。

練習 7.1

練習 7.1

C を線形符号、G をその生成行列、H をそのパリティ検査行列とおく。拡大符号 $\bar{C}$ に対して生成行列 $\bar{G}$ 及びパリティ検査行列 $\bar{H}$ を求めよ。

解答

G の各行の和の逆元を追加したような行からなる行列を $\bar{G}$、H に全てが 0 の要素からなる列を追加し、その後すべての要素が 1 で構成される行を追加した行列を $\bar{H}$ とすれば良い。

練習 7.2

練習 7.2

$\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{V}$ を線形符号、それぞれの生成行列を G_1, G_2、それぞれのパリティ検査行列を H_1, H_2 とおく。
どのようにして $\mathcal{C}_1 + \mathcal{C}_2$ の生成行列及び、$\mathcal{C}_1 \cap \mathcal{C}_2$ のパリティ検査行列を見つければよいか？

解答

$\mathcal{C}_1 + \mathcal{C}_2$ の生成行列は G_1 の行を G_2 に追加し、線形従属な行を削除することによって得られる。
また、$\mathcal{C}_1 \cap \mathcal{C}_2$ のパリティ検査行列は H_1 の行を H_2 に追加し同様に、線形従属な行を削除することによって得られる。

双対符号

H は $h : \mathcal{V} \to \mathcal{W} = \mathbf{F}^{n-k}$ なる各 $\mathbf{v} \in \mathcal{V}$ を $h(\mathbf{v}) = \mathbf{v}H^T$ で移す線形変換と見れる。
よって、補題 7.10 は $\mathcal{C}$ が h の核 $\ker(h)$、つまり $\mathbf{0}$ に移されるベクトルの組かを検査している。
h の像 $\mathrm{im}(h)$ は H によって張られる $\mathcal{W}$ の部分空間である。 次元定理から
$\dim(\mathcal{V}) = \dim(\ker(h)) + \dim(\mathrm{im}(h))$ より $\dim(\mathrm{im}(h)) = n - k$ なので、
h は $\mathcal{V}$ から $\mathcal{W}$ への写像である。
H ($\mathcal{C}$ を表現する連立方程式) の $n - k$ 個の行は線形独立で、よってこれらは次元 k の線形部分空間 $\mathcal{D} \subseteq \mathcal{V}$ の基底を構成する。
これは線形符号で生成行列は H となり、これを $\mathcal{C}$ の双対符号と呼ぶ。

双対符号

$\mathcal{C}$ と $\mathcal{D}$ は直交性という点で関連している。ユークリッド空間 $\mathbf{R}^n$ でするように、以下によって内積を定義出来る。

$$\mathbf{u}.\mathbf{v} = u_1v_1 + \cdots + u_nv_n \tag{7.1}$$

ここで $\mathbf{u}, \mathbf{v}$ は $\mathbf{V}$ 上の任意のベクトルである。これは両方の変数に関して線形である。つまり

$$(a\mathbf{u}_1 + b\mathbf{u}_2).\mathbf{v} = a(\mathbf{u}_1.\mathbf{v}) + b\mathbf{u}_2.\mathbf{v} \text{ かつ } \mathbf{u}.(a\mathbf{v}_1 + b\mathbf{v}_2) = a\mathbf{u}.\mathbf{v}_1 + b\mathbf{u}.\mathbf{v}_2$$

がすべての $a, b \in \mathbf{F}$ に対して成立する。$\mathbf{u}.\mathbf{v} = 0$ となることを $\mathbf{u}$ と $\mathbf{v}$ が直交すると定義できる。
$\mathbf{R}^n$ と違い、非零ベクトルがそれ自信と直交することが可能である。例えば $\mathbf{u} = \mathbf{e}_1 + \mathbf{e}_2$ のとき、$\mathbf{u}.\mathbf{u} = 1^2 + 1^2 = 2$ より、$q = 2$ のとき $\mathbf{u}.\mathbf{u} = 0$ である。

双対符号

$\mathcal{C}$ を定義する方程式 $\mathbf{v}H^T = \mathbf{0}$ は、

- $\mathcal{C}$ がすべての H の行と直交するベクトルから構成されること、
- $\mathcal{D}$ のすべてのベクトルと直交する

(これらは同値である) ということと理解できる。
よって、$\mathcal{C}$ は $\mathcal{D}$ の直交符号 $\mathcal{D}^\perp = \{\mathbf{v} \in \mathcal{V} \mid \mathbf{v}.\mathbf{w} = 0 \text{ for all } \mathbf{w} \in \mathcal{D}\}$ で、
$\mathcal{C}$ と $\mathcal{D}$ の役割を入れ替えることで次の式を得る

$$\mathcal{D} = \mathcal{C}^\perp = \{\mathbf{w} \in \mathcal{V} \mid \mathbf{v}.\mathbf{w} = 0 \text{ for all } \mathbf{v} \in \mathcal{C}\}$$

このように、線形符号は互いに双対な組になっていて、ある線形符号の生成行列は他の線形符号のパリティ検査行列となっている。
しかし、いくつかの符号は自己双対つまり $\mathcal{C} = \mathcal{C}^\perp$ となることに注意しよう。2元反復符号 $\mathcal{R}_2$ はこの簡単な例である。より一般的には次の例がある。

例 7.14

$q = 2, n = 2m$ で、$\mathcal{C}$ を基底ベクトル $\mathbf{u}_i = \mathbf{e}_{2i-1} + \mathbf{e}_{2i}$ $(i = 1, \ldots, m)$ からなる線形符号とおく。
$\mathbf{u}_i.\mathbf{u}_j = 0$ $\forall i, j$ なので、$\mathcal{C} \subseteq \mathcal{C}^\perp$ で、次元を比較すると $\mathcal{C} = \mathcal{C}^\perp$ がわかる。

双対符号の例

例 7.15

反復符号 $\mathcal{R}_n$ は $\mathbf{1} = 1 \ldots 1$ で張られていて、よって

$$\mathcal{R}_n^{\perp} = \{\mathbf{w} \in \mathcal{V} \mid \mathbf{1}.\mathbf{v} = 0\} = \{\mathbf{w} \in \mathcal{V} \mid w_1 + \cdots + w_n = 0\} = \mathcal{P}_n$$

で、同様に

$$\mathcal{P}_n^{\perp} = \{\mathbf{w} \in \mathcal{V} \mid (\mathbf{e}_i - \mathbf{e}_n).\mathbf{w} = 0 \text{ for } i = 1, \ldots, n-1\}$$

$$= \{\mathbf{w} \in \mathcal{V} \mid w_i = w_n \text{ for } i = 1, \ldots, n-1\}$$

$$= \mathcal{R}_n$$

双対符号の例

例 7.15 (続き)

また既に、

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

が $\mathcal{P}_n$ の生成行列かつ、$\mathcal{R}_n$ のパリティ検査行列であること、一方

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

が $\mathcal{R}_n$ の生成行列かつ、$\mathcal{P}_n$ のパリティ検査行列であることを見た。

双対符号の例

例 7.15

$\mathcal{H}_7^{\perp}$ は $\mathbf{F}_2$ 上の線形 $[7, 3]$ 符号である。生成行列は $\mathcal{H}_7$ のパリティ検査行列

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

である。行の線形結合をとることによって、この符号の 7 つの非零の要素はすべて重み 4 を持つことがわかる、よって $d = 4$ である。

パリティ検査行列の決定

与えられた符号に対してどの行列がパリティ検査行列かどうかを決定する一般的な基準を挙げることでこの節を締めくくる。
以下では、0 はすべての要素が 0 となる行列を表す。

補題 7.17

$\mathcal{C}$ を $\mathbf{F}$ 上の線形 $[n,k]$ 符号で生成行列を G とおく。
H は $\mathbf{F}$ 上の行列で、n 列 $n-k$ 行を持つとする。このとき H が $\mathcal{C}$ のパリティ検査行列であるのは、
H が階数 $n-k$ をもち、$GH^T = 0$ を満たすとき、かつそのときのみである。

補題 7.17 証明

H の行が $\mathcal{V}$ の $n-k$ 個のベクトルを生成し、$GH^T = 0$ となることは、これらの行が G の各行と直交する。すなわち $\mathcal{C}^\perp$ に含まれることと同値である。
H は階数 $n-k$ をもち、これは各行が線形独立であることと同値で、すなわち $\mathcal{C}^\perp$ の基底を生成するということである。
よって、H が与えられた条件を満たすことは、H が $\mathcal{C}^\perp$ の生成行列、つまり $\mathcal{C}$ のパリティ検査行列となることと同値である。