

代数系と符号理論 (O) 第4回板書プリント

制作：植松友彦

2014.4.23

第3回の復習

教科書を見ないでこれらの説明ができること。

- 2元対称通信路
- 加法的雑音通信路
- 符号の最小距離と誤り訂正能力の関係
- パリティ検査行列と最小距離との関係
- ハミング符号 (パリティ検査行列、パラメータ)
- 拡大ハミング符号 (パリティ検査行列、パラメータ)
- 2元対称通信路における復号誤り率の限界

1 シンドローム

[例 1] 体 F_2 上の $(7, 4)$ ハミング符号のパリティ検査行列を

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

によって定義する。このとき、ベクトル $r = (0011010)$ のシンドローム s は、

$$s = (0011010)H^T = (0011010) \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (110)$$

となる。また、このパリティ検査行列に対応する生成行列は

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

であり、 $\mathbf{r} = (0011010)$ に符号語 $\mathbf{c} = (1000110)$ を加えてできるベクトル

$$\mathbf{r} + \mathbf{c} = (1011100)$$

のシンδροーム $\mathbf{s}'$ は

$$\mathbf{s}' = (1011100)H^T = (110)$$

となり、 $\mathbf{r}$ に符号語 $\mathbf{c}$ を加えてもシンδροームには影響がないことが確認される。

[例 2] 2 元 (3, 1) 線形符号の生成行列が $G = [111]$ によって定められたとき、符号語の集合 C は

$$C = \{(000), (111)\}$$

である。従って、ベクトル $\mathbf{a} = (100)$ を含むコセットは、

$$\mathbf{a} + C = (100) + C = \{(100), (011)\}$$

である。これ以外のコセットは、

$$(010) + C = \{(010), (101)\}, (001) + C = \{(001), (110)\}, (000) + C = \{(000), (111)\}$$

である。この符号のパリティ検査行列は、

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

であり、コセット $(100) + C = \{(100), (011)\}$ に属するベクトルについて、

$$(100)H^T = (100) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = (11), \quad (011)H^T = (011) \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = (11)$$

が得られ、両者のシンδροームは一致している。他方、コセット $(010) + C$, $(001) + C$ ならびに $(000) + C$ に属するベクトルのシンδροームは、それぞれ (10) , (01) , (00) であり、コセットが異なればシンδροームが異なっている。

2 シンδροーム復号法

2.1 限界距離復号法とシンδροーム復号法との比較

第 3 回で説明した限界距離復号法を用いて線形 (n, k) 符号を復号する場合、 2^n 個のベクトルがどの符号語の復号領域に属するかを示すテーブルを用意するか、受信語と 2^k 個の全ての符号語の間のハミング距離を調べて一番近いものを探すことになる。従って、限界距離復号法の計算量は少なくとも 2^k のオーダーになる。これに対し、シンδροーム復号法では、 2^{n-k} 個のシンδροームと誤りベクトルとの対応表のみを用意すれば良い。従って、 $n - k$ が k よりも小さい場合、シンδροーム復号法は、限界距離復号法に比べて効率的である。

2.2 標準配列の作り方

[例 3] $H = [-P^T \ I]$ の形のパリティ検査行列

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

を持つ (6,3) 線形符号 C について、シンドローム復号法を行おう。まず、準備として、シンドロームとコセット代表元の対応表を作る。

- (1) まず、左上を零ベクトルとして、全ての符号語を一行に書く。 H に対応する生成行列 G は、

$$G = [I \ P] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

なので、次の表を得る。

シンドローム	コセット							
(000)	(000000)	(100110)	(010101)	(001011)	(110011)	(101101)	(011110)	(111000)

- (2) 次に 1 行目に出現しなかった 2 元ベクトルで、重みが最小のものを一つ選び、一行目のベクトルに加えたものを二行目に書く。選んだベクトル (コセット代表元であり、これが誤り訂正可能な誤りパターンとなる) を (100000) とすると、次の表が得られる。

シンドローム	コセット							
(000)	(000000)	(100110)	(010101)	(001011)	(110011)	(101101)	(011110)	(111000)
(110)	(100000)	(000110)	(110101)	(101011)	(010011)	(001101)	(111110)	(011000)

- (3) これまでに出現しなかった 2 元ベクトルで、重みが最小のものを一つ選び、一行目のベクトルに加えたものを三行目に書く。選んだベクトルを 010000 とすると、次の表が得られる。

シンドローム	コセット							
(000)	(000000)	(100110)	(010101)	(001011)	(110011)	(101101)	(011110)	(111000)
(110)	(100000)	(000110)	(110101)	(101011)	(010011)	(001101)	(111110)	(011000)
(101)	(010000)	(110110)	(000101)	(011011)	(100011)	(111101)	(001110)	(101000)

- (4) 上記の操作を繰り返し、全ての 2 元ベクトルが表に書かれるまで続けると、例えば次の表が得られる。

シンドローム	コセット							
(000)	(000000)	(100110)	(010101)	(001011)	(110011)	(101101)	(011110)	(111000)
(110)	(100000)	(000110)	(110101)	(101011)	(010011)	(001101)	(111110)	(011000)
(101)	(010000)	(110110)	(000101)	(011011)	(100011)	(111101)	(001110)	(101000)
(011)	(001000)	(101110)	(011101)	(000011)	(111011)	(100101)	(010110)	(110000)
(100)	(000100)	(100010)	(010001)	(001111)	(110111)	(101001)	(011010)	(111100)
(010)	(000010)	(100100)	(010111)	(001001)	(110001)	(101111)	(011100)	(111010)
(001)	(000001)	(100111)	(010100)	(001010)	(110010)	(101100)	(011111)	(111001)
(111)	(100001)	(000111)	(110100)	(101010)	(010010)	(001100)	(111111)	(011001)

標準配列を抜き出して、シンドロームとコセット代表元との対応表を作ると、次の表が得られる。

シンδροーム	コセット代表元 (訂正可能な誤りベクトル)
(000)	(000000)
(110)	(100000)
(101)	(010000)
(011)	(001000)
(100)	(000100)
(010)	(000010)
(001)	(000001)
(111)	(100001)

従って、 $\mathbf{r} = (100010)$ を受信した場合、シンδροーム

$$\mathbf{s} = \mathbf{r}H^T = (100010) \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (100)$$

に対応するコセット代表元は上の表から $\mathbf{e} = (000100)$ となり、シンδροーム復号法では、 $\mathbf{r} = (100010)$ は $\mathbf{c} = \mathbf{r} - \mathbf{e} = (100110)$ に復号される。

3 誤り訂正能力の限界式

3.1 Varshamov-Gilbert(VG) の下界式

VG の下界式は、所望のパラメータを有する符号が存在するための「十分条件」を示しており、この条件式を満たさない場合でも、所望のパラメータを有する符号が存在することがある。

[例 4] VG の下界式を用いて、最小距離 5 を持つ符号長 15 の 2 元符号の次元をどこまで大きくできるか調べてみよう。

$$1 + \binom{14}{1} + \binom{14}{2} + \binom{14}{3} = 470 < 2^{15-k}$$

を満たす最大の k は 6 である。従って、最小距離 5 の $(15, 6)$ 符号が存在する。しかしながら、後に学ぶ BCH 符号の中には、最小距離 5 で、より次元の大きな $(15, 7)$ 符号が存在する。

3.2 ハミング限界

[例 5] 2 元ハミング符号については、 $q = 2, n = 2^m - 1, k = n - m, t = 1$ であることから

$$2^k \sum_{j=0}^t \binom{n}{j} = 2^k \left\{ \binom{n}{0} + \binom{n}{1} \right\} = 2^k \cdot 2^m = 2^n$$

となり、ハミング限界の等号が成り立つ。このように、ハミング限界の等号を満たす符号のことを「完全符号 (perfect code)」という。2 元の完全符号は、符号長が奇数の繰返し符号 (生成行列 $G = [11 \cdots 1]$)、ハミング符号と Golay 符号しか知られていない。

3.3 Singleton 限界

[例 6] 2 元ハミング符号は、 $(2^m - 1, 2^m - m - 1)$ 線形符号であり、最小距離は $d = 3$ であるので、

$$n - k + 1 = (2^m - 1) - (2^m - m - 1) + 1 = m + 1 \geq d = 3$$

となり、当然ながら Singleton 限界を満たしている。また、 $m = 2$ のときは最大距離分離符号である。

単一パリティ検査符号 (SPC 符号) は $(n, n - 1)$ 線形符号であり、最小距離は 2 であるので、

$$2 = n - (n - 1) + 1$$

となり、最大距離分離符号である。

繰り返し符号 $\{(0 \dots 0), (1 \dots 1)\}$ は $(n, 1)$ 符号であり、最小距離は n であるので、

$$n = n - 1 + 1$$

となり、最大距離分離符号である。尚、2 元符号にはこれらの自明な最大距離分離符号しか存在せず、非 2 元の最大距離分離符号として Reed-Solomon 符号が知られている。

ハミング限界や Singleton 限界は、所望のパラメータを有する符号が存在するならば、絶対に満足しなければならない「必要条件」を示している。従って、これらの条件式を満足するからといって、所望の符号の存在を示したことはない。この意味において、ハミング限界や Singleton 限界は、VG の下界式と意味が異なる。