代数系と符号理論 (O) 第3回板書プリント

制作：植松友彦

2014.4.22

第 2 回の復習

教科書を見ないでこれらの説明ができること。

- 生成行列
- 符号化規則
- 行基本操作
- 組織符号とその生成行列
- 双対符号
- パリティ検査行列
- 組織符号のパリティ検査行列
- ハミング距離とハミング重み
- 最小距離
- 線形符号の最小距離

1　通信路のモデル

2 元対称通信路 (2 元符号で主として取り扱う通信路)

2 元対称通信路 (binary symmetric channel (BSC)) は、図 3.1 のような通信路線図によって表される。

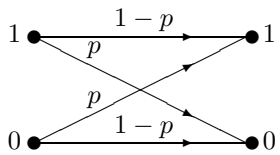

図 3.1 2 元対称通信路

この 2 元対称通信路において、入力列 $\boldsymbol{x} = 110$ を送信 (入力) して出力列 $\boldsymbol{y} = 010$ を受信 (出力) する確率 $P(010|110)$ は、

$$P(010|110) = P(0|1)P(1|1)P(0|0) = p(1-p)(1-p) = p(1-p)^2$$

となる。また、$\boldsymbol{x} = 000$ を送信して $\boldsymbol{y} = 111$ を受信する確率 $P(111|000)$ は、同様にして

$$P(111|000) = P(1|0)P(1|0)P(1|0) = p^3$$

となる。

加法的雑音通信路 (符号理論で主として取り扱う通信路)

入力アルファベット $\mathcal{X}$ が出力アルファベット $\mathcal{Y}$ の部分集合であり、出力アルファベット $\mathcal{Y}$ には加算 $+$ が定義されている。入力列 $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$ に $\mathcal{Y}$ 上の系列 $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathcal{Y}^n$ が加わって、受信列

$$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) = \boldsymbol{x} + \boldsymbol{e} = (x_1 + e_1, x_2 + e_2, \ldots, x_n + e_n)$$

が出力される通信路モデルを「加法的雑音通信路」と呼ぶ。系列 $\boldsymbol{e}$ を「誤り系列」あるいは「誤りベクトル」と呼び、系列 $\boldsymbol{e}$ は入力列 $\boldsymbol{x}$ と統計的に独立に発生すると仮定する。更に、系列 $\boldsymbol{e}$ の各要素 e_i $i = 1, 2, \ldots, n$ が同一の分布によって独立に発生するとき、加法的雑音通信路は無記憶通信路になる。

2 元対称通信路は、雑音 $e_i = 1$ が確率 p で、雑音 $e_i = 0$ が確率 $1-p$ でそれぞれ生起する加法的雑音通信路である。この p を「2 元対称通信路の誤り率」と呼ぶこともある。

例えば、2 元対称通信路において、入力列 $\boldsymbol{x} = (110)$ を入力して、出力列 $\boldsymbol{y} = (010)$ を得た場合、

$$\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{x} = (010) - (110) = (100)$$

から $\boldsymbol{e} = (100)$ が誤り系列である。この場合、この誤り系列を得る確率は

$$P(100) = p(1-p)(1-p) = p(1-p)^2$$

となり、これは上で求めた $P(010|110) = p(1-p)^2$ と一致する。

2　符号の最小距離と誤り訂正能力

[定理 **3.1**] ブロック符号 C が t 個以下の全ての誤りを訂正可能となるための必要十分条件は、$t < d/2$ である。但し、d は符号 C の最小距離である。従って、最小距離 d の符号は $\lfloor \frac{d-1}{2} \rfloor$ 個以下の全ての誤りを訂正可能である。

$d/2$ 個未満の誤りが訂正できること：教科書参照。

$d/2$ 個以上の誤りが訂正できないこと：反例を示す。例えば、最小距離 $d = 3$ を与える符号語の組が $\boldsymbol{c}_1 = (10010)$ と $\boldsymbol{c}_2 = (11100)$ ならば、$\boldsymbol{c}_1 - \boldsymbol{c}_2 = (01110)$ である。そこで、2 つの誤りを (01000) と (00110) とすれば、$\boldsymbol{c}_1$ に 1 個の誤り (01000) が生じて得られる (11010) は、$\boldsymbol{c}_2$ に 2 個の誤り (00110) が生じて得られる (11010) と一致する。すなわち、

$$(11010) = \boldsymbol{c}_1 + (01000) = \boldsymbol{c}_2 + (00110)$$

が成り立つ。従って、(11010) を受信したとき、$\boldsymbol{c}_1$ を送信したと判定すれば、$\boldsymbol{c}_2$ に生じた 2 個の誤りを訂正できない。また逆に、(11010) を受信したとき、$\boldsymbol{c}_2$ を送信したと判定すれば、今度は、$\boldsymbol{c}_1$ に生じた 1 個の誤りを訂正できない。以上のことから、2 個以下の全ての誤りが訂正できないことが結論される。

3　パリティ検査行列と最小距離との関係

[定理 **3.2** の例] 符号長 5 の 2 元符号のパリティ検査行列

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

において、1 列目と 4 列目を加えると零ベクトルになるので 1 列目と 4 列目の列ベクトルは線形従属である。これから、これらの列に対応する成分を 1 として得られる (10010) は符号語である。なぜなら、

$$(10010)H^T = (10010)\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = (000)$$

が成り立つからである。同様に 1 列目以外の 4 列を加えると零ベクトルになるので、2 列目から 5 列目までの列ベクトルは線形従属である。従って、(01111) は符号語である。

逆に、$(11101)H^T = \mathbf{0}$ なので、(11101) は符号語であり、4 個の列ベクトルに線形従属なのものが存在する。事実、この符号語の非零の成分に対応する H の 4 つの列ベクトル

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

の和は零ベクトルになり、これらの 4 つの列ベクトルは線形従属である。

[**2** 元符号の場合の定理 **3.2** の意味]

$$\begin{aligned} H \text{ の幾つかの列ベクトルの和が零} &\implies \text{その列に対応する成分を 1 にして得られる} \\ &\qquad 2 \text{ 元ベクトルは符号語} \\ \boldsymbol{c} \text{が 2 元符号の符号語} &\implies \boldsymbol{c} \text{の 1 の成分に対応する } H \text{ の列の集合は線形従属} \end{aligned}$$

2 元線形符号のパリティ検査行列 H の列ベクトルと最小距離の関係

- H の列ベクトルに零ベクトルがなければ、最小距離は 2 以上である。
- H の列ベクトルに零ベクトルがなく、かつ全て異なっていれば、最小距離は 3 以上である。

4　代表的な線形符号

2 元ハミング符号

$m = 4$ の場合、2 元ハミング符号のパリティ検査行列 H は、

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

である。

2 元ハミング符号のパラメータ

符号長：　$n = 2^m - 1$
次元：　$k = n - m = 2^m - m - 1$
最小距離：　$d = 3$

m	2	3	4	5	6
符号長 n	3	7	15	31	63
次元 k	1	4	11	26	57
最小距離 d	3	3	3	3	3

2 元拡大ハミング符号

$m = 4$ の場合の 2 元拡大ハミング符号のパリティ検査行列は、

$$H = \left[\begin{array}{cccccccccccccccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

である。

2 元拡大ハミング符号のパラメータ

符号長：　$n = 2^m$
次元：　$k = n - (m + 1) = 2^m - m - 1$
最小距離：　$d = 4$

m	2	3	4	5	6
符号長 n	4	8	16	32	64
次元 k	1	4	11	26	57
最小距離 d	4	4	4	4	4

5　2 元対称通信路と復号誤り確率の限界

[定理 **3.4** の計算例] p=0.001 の 2 元対称通信路において、ハミング (15,11) 符号を用いたときの復号に失敗する確率は、ハミング符号が 1 個までの誤りを訂正できることに注意して、定理 3.4 に $n = 15$、$t = 1$ を代入すると、

$$P_e = \sum_{j=2}^{15} \binom{15}{j} 0.001^j (1 - 0.001)^{15-j} = 0.000104094$$

が得られる。一方、近似式によれば、

$$P_e \approx \binom{15}{2} 0.001^2 (1-0.001)^{13} = 0.000103643$$

となり、よく一致している。

5 月の授業日程

5 月 13 日 (火)　講義 5
5 月 14 日 (水)　演習 3
5 月 21 日 (水)　講義 6
5 月 27 日 (火)　演習 4
5 月 28 日 (水)　講義 7