符号とは

計算機ネットワークや衛星通信などの通信路を通して，**送信者**が**受信者**に文章，画像，音声などの情報を送る際には，通常データを 0,1 の系列に変換して送信を行い，受信側で再びもとのデータに復元する.

ここで, 送信したいデータの集合 Ω を**情報源**と呼ぶ.

モデル化

$F=\{0,1\}$ とし，$F^n=\{(x_1,\ldots,x_n):x_i\in F\}$ とおくと，上の変換は次のように定義される．

$$f:\Omega\to F^n$$

写像 f を**符号化関数**と呼び，F^n の部分集合
$C=\{f(\alpha):\alpha\in\Omega\}$ を長さ n の**符号**，C の各元 $\mathbf{x}=f(\alpha)$ を**符号語**と呼ぶ．
逆に，符号化された F^n の元を対応する Ω の元に戻す，あるいは対応する Ω の元が存在しないときには，元 に対応させる写像を**復号化関数**と呼ぶ．$F=\{0,1\}$ とする代わりに，
$F=\{0,1,\ldots,q-1\}$ とし，Ω を F^n に符号化する場合には **q 進符号**と呼ばれる．

符号化の方法

符号化の方法としては，誤り検出可能な符号と誤り訂正可能な符号に分けられる.

- 誤りを検出可能な符号: 単一パリティ検査符号など
- 誤り訂正可能な符号: ハミング符号，BCH 符号，リードソロモン符号など

最尤復号法

通信路には多くの場合，通信を妨害する雑音が混入してくる． 雑音のある通信路としてもっともよく用いられる２元対称通信路（図１）を用いた符号の送信を考える．
($0 < p < 0.5$ とする.)

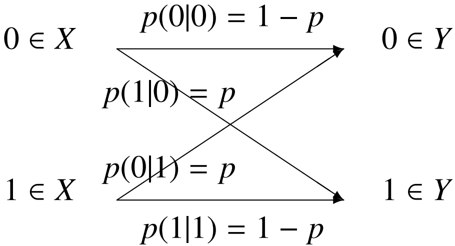

図１　２元対称通信路

最尤復号法

例えば２つの元からなる情報源 $\Omega = \{a, b\}$ から発生する情報を次のように符号化し，２元対称通信路を通して符号語を送信する．

Ω^2	符号 C
aa	$\mathbf{x}_1 = (0, 0, 0, 0)$
ab	$\mathbf{x}_2 = (1, 1, 1, 0)$
ba	$\mathbf{x}_3 = (1, 1, 0, 1)$
bb	$\mathbf{x}_4 = (1, 0, 1, 1)$

- 受信者が $\mathbf{y} = (1, 0, 0, 0)$ を受けとったとき，情報源の各要素が等確率で送信されると仮定するとき，送信者が送った情報は aa,ab,ba,bb のいずれであったと考えればよいだろうか．

最尤復号法

最尤復号法

符号 $C = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M\}$ の中のある符号語を送信したとき，$\mathbf{y}$ を受信したとする． このとき符号 C の中のすべての符号語 $\mathbf{x}_i$ $(i = 1, \ldots, M)$ に対して遷移確率 $p(\mathbf{y}|\mathbf{x}_i)$ を計算する. このとき $p(\mathbf{y}|\mathbf{x}_k)$ が最大値であるならば，符号語 $\mathbf{x}_k$ が送信されたものとみなし，$\mathbf{y}$ を $\mathbf{x}_k$ に復号する. この方法を**最尤復号法**と呼ぶ.

ただし，$p(\mathbf{y}|\mathbf{x}_k)$ が最大になる $\mathbf{x}_k$ がただ 1 つの場合に限り，$\mathbf{y}$ を $\mathbf{x}_k$ に一意的に復号することができることに注意する.

最尤復号法

問題

受信者が $\mathbf{y} = (1, 0, 0, 0)$ を受けとったとする. すべての符号語の出現確率が等しいとして、最尤復号法により復号せよ.

ハミング距離

$F = \{0, 1\}$, $F^n = \{(x_1, x_2, \ldots, x_n) : x_i \in F\}$ とし，C を F^n の部分集合とする．

定義 7

F^n 上の２点 $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ に対して，$\mathbf{x}$ と $\mathbf{y}$ の距離 $d(\mathbf{x}, \mathbf{y})$ を

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|$$

によって定義し，**ハミング距離**と呼ぶ．また

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

を $\mathbf{x}$ の**重み**，または**ウエイト**という．

最小距離

定義 7

符号 C の任意の異なる２つの符号語間のハミング距離の最小値を符号 C の**最小距離**という．符号語の長さ n, 符号語の数 M, 最小距離 d の符号を $[n, M, d]$-符号とよぶ.

問題 9

ハミング距離 $d(\mathbf{x}, \mathbf{y})$ が次の距離の公理を満たすことを示せ.

非負性　任意の $\mathbf{x}, \mathbf{y}$ に対して, $d(\mathbf{x}, \mathbf{y}) \geq 0$ である. また等号が成立するのは, $\mathbf{x} = \mathbf{y}$ のときに限る.

対称性　任意の $\mathbf{x}, \mathbf{y}$ に対して, $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ である.

三角不等式　$d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$

符号 C に含まれる各符号語に対して，距離が 1 のベクトルを求めてみると，次のようになる.

	符号語	ハミング距離 1
$\mathbf{x}_1$	$(0,0,0,0)$	$(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}$
$\mathbf{x}_2$	$(1,1,1,0)$	$(0,1,1,0), \underline{(1,0,1,0)}, \underline{(1,1,0,0)}, \underline{(1,1,1,1)}\}$
$\mathbf{x}_3$	$(1,1,0,1)$	$(0,1,0,1), \underline{(1,0,0,1)}, \underline{(1,1,1,1)}, \underline{(1,1,0,0)}\}$
$\mathbf{x}_4$	$(1,0,1,1)$	$(0,0,1,1), \underline{(1,1,1,1)}, \underline{(1,0,0,1)}, \underline{(1,0,1,0)}\}$

問題 10

(1) 符号 C の各符号語間のハミング距離と，最小距離を求めよ．

(2) 符号語 $\mathbf{x}_i$ を送信するとき，正しく復号される確率 $\bar{Q}(\mathbf{x}_i)$ と誤って復号される確率 $Q(\mathbf{x}_i)$, $i = 1, 2, 3, 4$ を求めよ．

(3) 符号 C の復号誤り確率 $P_e = \frac{1}{M}\sum_{i=1}^{M} Q(\mathbf{x}_i)$ を求めよ．

定理 18

最小距離が d の符号 C を用いると, 最尤復号法によって, $e = \lfloor \frac{d-1}{2} \rfloor$ 個以内の誤りは正確に元の符号語に復号することができる. ただし, $\lfloor x \rfloor$ は x を超えない最大の整数を表す.

逆に, e 個以内の誤りをすべて正確に復号することができる符号語の最小距離 d は $d \geq 2e+1$ を満たさなければならない.

e ビット以内の誤りを正確に復号することができる符号を e-誤り訂正符号と呼び, e をこの符号の誤り訂正能力という.

最尤復号法を利用した復号法

復号アルゴリズム

(1) 受信ベクトル $\mathbf{y}$ に対し，$d(\mathbf{x}, \mathbf{y}) \leq e$ なる符号語 $\mathbf{x}$ が存在するときは $\mathbf{x}$ に復号する.

(2) $d(\mathbf{x}, \mathbf{y}) \leq e$ なる符号語 $\mathbf{x}$ が存在しないときは，受信ベクトルに誤りがあったことを報告し，復号はしない

系 19

$[n, M, d]$-符号に対して上の復号法を用いたとき，ある符号語 $\mathbf{x}$ を送信して，その符号語に正確に復号される確率は

$$\sum_{i=0}^{e} \binom{n}{i} p^i (1-p)^{n-i}$$

である. ただし，$e = \lfloor \frac{d-1}{2} \rfloor$ である.

F^n の任意の元 $\mathbf{x}$ と任意の非負整数 r に対して,

$$S_r(\mathbf{x}) = \{\mathbf{y} \in F^n : d(\mathbf{x}, \mathbf{y}) \leq r\}$$

を $\mathbf{x}$ を中心とする半径 r のハミング球と呼ぶ.

定理 20

$[n, M, d]$-符号 C に対して,

$$2^n \geq M\{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}\}$$

が成り立つ. ただし, $e = \lfloor \frac{d-1}{2} \rfloor$ である.

定理 20 の不等式はハミングの上限界式と呼ばれ, 等号が成立する符号を完全符号という.

線形符号

定義 8

有限体 F_q 上の n 次元ベクトル空間を $V = F_q^n$, $C \subseteq V$ を V の k 次元部分空間とする．このとき符号 C を長さ n, 次元 k の線形符号であるといい，(n, k)-線形符号と書く．また最小距離が d である (n, k)-線形符号 C を (n, k, d)-線形符号という．

ここでは，$q = 2$ の場合すなわち $F = \{0, 1\}$ 上で考える．また，C が線形符号であるとき，$\forall \mathbf{x}, \mathbf{y} \in C$，$\lambda \in F_q$ に対し，

(1) $\mathbf{x} + \mathbf{y} \in C$

(2) $\lambda \mathbf{x} \in C$

が成り立つことに注意する．

線形符号

定理 21

C を線形符号とする．C の最小距離は，C の零ベクトル $\mathbf{0}$ でない符号語の重みの最小値（最小重み）に等しい．

問題 11

$C = \{(0,0,0,0,0), (1,1,1,0,0), (0,0,1,1,1), (1,1,0,1,1)\}$ とするとき，次の問いに答えよ．

(1) C が $V = F^5$ の 2 次元部分空間であることを確認せよ．

(2) $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ とするとき，$\{\mathbf{u}G : \mathbf{u} \in F^2\}$ を求めよ．

生成行列

C の符号語の中に k 個の線形独立なベクトルが存在する．これらのベクトルを $k \times n$ 行列に並べた行列 G を C の**生成行列**と呼ぶ．このとき

$$C = \{\mathbf{u}G : \mathbf{u} \in F^k\}$$

と書くことができ，C は 2^k の符号語からなる．

問題 12

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

を生成行列とするとき，次の問いに答えよ.

(1) 符号 C を求めよ.

(2) 符号 C は，(n, k, d)-線形符号である．n,k,d を与えよ.

(3) C に含まれるすべての符号語と直交するベクトルを求めなさい.

パリティ検査行列

(n, k)-線形符号 C を $(n-k) \times n$ 行列 H（ただし，H の階数は $n-k$ とする）を用いて，次のように表すこともできる．

$$C = \{\mathbf{x} \in F^n : \mathbf{x}H^T = \mathbf{0}\}$$

すなわち，C を一次連立方程式の解空間とみなす方法である．このとき H を符号 C のパリティ検査行列という．

パリティ検査行列

問題 13

問題 11 および 12 におけるパリティ検査行列を求めよ.

定理 22

線形符号 C の生成行列を G, パリティ検査行列を H とすると,

$$GH^T = \mathbf{0}$$

が成り立つ.

特に, G が $G = (I_k D)$ とかける場合には, H は $H = (D^T I_{n-k})$ とかける. ここに, I_k は $k \times k$ の単位行列を表し, D は $k \times (n-k)$ の行列を表す.

定理 23

(n,k)-線形符号 C のパリティ検査行列を H とし，H の n 個の列ベクトルを $h_1, h_2, \ldots, h_n$ とする．このとき，$h_1, h_2, \ldots, h_n$ のどの $d-1$ 個のベクトルも線形独立で，$h_1, h_2, \ldots, h_n$ の中に線形従属な d 個のベクトルが存在するならば，C の最小距離は d である．

問題 14

$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ をパリティ検査とする線形符号 C を求め，そのパラメータを答えよ．

定義 9

F^m のすべての非零ベクトルを列ベクトルとして並べてできる $m \times (2^m - 1)$ 行列 H をパリティ検査行列とする線形符号を $(2^m - 1, 2^m - m - 1)$-**ハミング符号**という.

上記の H は，どの 2 列も線形独立で，線形従属な 3 個の列ベクトルが存在するので，定理 23 より，H で定義されるハミング符号の最小距離は 3 となる.

問題 15

$m = 3$ としてハミング符号のパリティ検査行列 H を定め，符号 C を求めよ.

定理 24

ハミング符号は完全符号である.

線形符号 C に対して，生成行列 G が与えられたとき，適当な行に関する基本変形（と列の交換）を施せば，

$$G' = (I_k D)$$

のように変形することができた．
またこのとき，C のパリティ検査行列 H は，

$$H = (D^t I_{n-k}) = (H_1 I_{n-k})$$

と書ける．

$\mathbf{x} = (x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)$ を C の符号語とし,
$\mathbf{x}_1 = (x_1, \ldots, x_k)$, $\mathbf{x}_2 = (x_{k+1}, \ldots, x_n)$ とおく.
$x_1, x_2, \ldots, x_k$ を**情報ビット**, $x_{k+1}, \ldots, x_n$ を**パリティ検査ビット**という.

問題 16

$\mathbf{x}_2 = \mathbf{x}_1 H_1^t$ が成り立つことを示せ.

問題 17

次の行列 H をパリティ検査行列とする符号 C を考える.
パリティ検査ビット x_3, x_4, x_5 を情報ビット x_1, x_2 を用いて表せ.

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

F 上の (n,k)-線形符号 C のパリティ検査行列を H とする．
このとき，ベクトル $\mathbf{y} \in F^n$ の**シンドローム** $\mathbf{s} \in F^{n-k}$ を

$$\mathbf{s} = \mathbf{y}H^t$$

と定義する．
C の符号語 $\mathbf{x}$ を送信したとき，エラーベクトル $\mathbf{e}$ が加わり，
$\mathbf{y}$ を受信したとする．すなわち $\mathbf{y} = \mathbf{x} + \mathbf{e}$ と書ける．
このとき，受信語 $\mathbf{y}$ のシンドロームは，

$$\mathbf{s} = \mathbf{y}H^t = (\mathbf{x} + \mathbf{e})H^t = \mathbf{x}H^t + \mathbf{e}H^t = \mathbf{e}H^t$$

となり，シンドロームは送信された符号語に依存せずエラーベクトル $\mathbf{e}$ によって一意的に定まることがわかる．

任意の n 次元ベクトル $\mathbf{a} \in F^n$ に対し，ベクトル $\mathbf{a}$ を含むコセットを，全ての符号語に $\mathbf{a}$ を加えてできる F^n の部分集合

$$\mathbf{a} + C = \{\mathbf{a} + \mathbf{x} : \mathbf{x} \in C\}$$

と定義する.

定理 25

2 つのベクトルが同一のコセットに含まれるための必要十分条件は，それらのベクトルが同一のシンドロームを有することである.

上記の定理より，任意のシンドローム $\mathbf{s} \in F^{n-k}$ に対して，コセットを定義することもできる.

$$C(\mathbf{s}) = \{\mathbf{e} \in F^n : \mathbf{e}H^t = \mathbf{s}\}$$

とおくとき，$C(\mathbf{s})$ をシンドローム $\mathbf{s}$ を持つコセットという. また $C(\mathbf{s})$ に属するベクトルの中でハミング重みが最小のものを**コセットリーダー**という.

定理 26

F 上の (n,k)-線形符号 C が e 個までの誤りを訂正できるための必要十分条件は，重みが e 以下の全てのエラーベクトルがコセットリーダーとなることである．

R を重みが e 以下のコセットリーダーの集合とし，シンドロームとコセットリーダーの対応を用いて復号をすることができる.

シンドロームを用いた復号法

F 上の線形符号 C のパリティ検査行列を H とする.

(1) 受信語 $\mathbf{y}$ に対して，シンドローム $\mathbf{s} = \mathbf{y}H^t$ を求める.

(2)
 (i) $\mathbf{s} = \mathbf{0}$ であれば，送信した符号語 $\mathbf{x}$ は $\mathbf{y}$ であるとみなす.
 (ii) $\mathbf{e}H^t = \mathbf{s}$ を満たすコセットリーダー $e \in R$ が存在するとき，送信した符号語 $\mathbf{x}$ は $\mathbf{y} - \mathbf{e}$ であるとみなす.
 (iii) $\mathbf{e}H^t = \mathbf{s}$ を満たすコセットリーダー $e \in R$ が存在しないとき，復号不可能とする.

問題 18

問題 17 で与えられた線形符号に対して，次の問いに答えよ．

	コセット	シンドローム
C	$\{(0,0,0,0,0),(0,1,0,1,1),(1,0,1,1,0),(1,1,1,0,1)\}$	$(0,0,0)$
$C+(1,0,0,0,0)$	$\{(1,0,0,0,0),(1,1,0,1,1),(0,0,1,1,0),(0,1,1,0,1)\}$	$(1,1,0)$
$C+(0,1,0,0,0)$	$\{(0,1,0,0,0),(0,0,0,1,1),(1,1,1,1,0),(1,0,1,0,1)\}$	$(0,1,1)$
$C+(0,0,1,0,0)$	$\{(0,0,1,0,0),(0,1,1,1,1),(1,0,0,1,0),(1,1,0,0,1)\}$	$(1,0,0)$
$C+(0,0,0,1,0)$	$\{(0,0,0,1,0),(0,1,0,0,1),(1,0,1,0,0),(1,1,1,1,1)\}$	$(0,1,0)$
$C+(0,0,0,0,1)$	$\{(0,0,0,0,1),(0,1,0,1,0),(1,0,1,1,1),(1,1,1,0,0)\}$	$(0,0,1)$
$C+(1,1,0,0,0)$	$\{(1,1,0,0,0),(1,0,0,1,1),(0,1,1,1,0),(0,0,1,0,1)\}$	$(1,0,1)$
$C+(0,1,1,0,0)$	$\{(0,1,1,0,0),(0,0,1,1,1),(1,1,0,1,0),(1,0,0,0,1)\}$	$(1,1,1)$

(1) 受信ベクトルが $\mathrm{y}=(1,1,0,1,1)$ であるとき，シンドローム s を求め，復号できる場合には復号せよ．

(2) 受信ベクトルが $\mathrm{y}=(1,1,0,1,0)$ であるとき，シンドローム s を求め，復号できる場合には復号せよ．

C を線形符号とする．このとき，$\mathbf{x} = (x_1, \ldots, x_n) \in C$ ならば $(x_n, x_1, \ldots, x_{n-1}) \in C$ が成り立つとき，C は**巡回符号**であるという．

例 2

$C = \{(0,0,0), (1,1,1)\}$ は巡回符号である．

例 3

$$C = \{(0,0,0,0), (1,0,0,1), (0,1,0,1), (1,1,0,0), (0,0,1,1), (1,0,1,0), (0,1,1,0), (1,1,1,1)\}$$

は巡回符号である．

ベクトル $(a_0, a_1, \ldots, a_{n-1}) \in F^n$ に F 上の多項式
$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ を対応させ，
$m(x) = x^n - 1$ としたとき，$m(x)$ による剰余類環 $F[x]/(m(x))$ を考える．
すなわち，符号を環 $F[x]/(m(x))$ の部分集合とみなす．

$$(1, 1, 0, 1, 0, 1, 0) \Leftrightarrow 1 + x + x^3 + x^5 \in F[x]/(x^7 - 1)$$

問題 19

符号語を多項式に対応させたとき，符号 C が線形符号であるとは，$f(x), g(x) \in C, \alpha \in F$ に対し，以下の条件 (1),(2) が成り立つことであり，巡回符号であるとは，(1),(2) および (3) が成り立つことであることを示せ．

(1) $f(x) + g(x) \in C$

(2) $\alpha f(x) \in C$

(3) $xf(x) \pmod{x^n - 1} \in C$

定理 27

$F[x]/(x^n-1))$ 上の (n,k)-巡回符号 C において，$g(x)$ を符号多項式の中で次数最小のモニック多項式とする．このとき，次の性質が成り立つ．

(1) $g(x)$ は一意的に定まる．

(2) $g(x)$ は C の全ての符号多項式を割り切る．

(3) $g(x)$ は x^n-1 を割り切る．

(4) $k=n-\deg g(x)$ である．

上記の $g(x)$ を巡回符号 C の生成多項式と呼ぶ．

問題 20

例 1 および例 2 の巡回符号において生成多項式を求めよ.

- C: $F[x]/(x^n - 1))$ 上の巡回符号
- $g(x)$: C の生成多項式とする.

$\deg g(x) = n - k$ とすると，定理 27 より

$$C = \{a(x)g(x) : a(x) \text{ は } k-1 \text{ 次以下の多項式}\}$$

と書ける.
さらに，C の各符号語は，$a(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ とすると

$$a(x)g(x) = a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1}x^{k-1}g(x)$$

のように $g(x), xg(x), \ldots, x^{k-1}g(x)$ の線形結合として表される.

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$$

とすると，C の生成行列は

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & \ddots & & & & \ddots & & \\ & & & \ddots & & & & \ddots & \\ 0 & 0 & 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} \end{pmatrix}$$

となる．

一方，

$$h(x) = (x^n - 1)/g(x) = h_0 + h_1 x + \cdots h_k x^k$$

とおくと，$g(x)h(x) = 0 \ (\mathrm{mod}\ x^n - 1)$ である．$h(x)$ をパリティ検査多項式と呼ぶ．行列 H を

$$H = \begin{pmatrix} 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 \\ 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ & & & & & & & & \\ & & & & & & & & \\ h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

とおくと，

$$GH^t = \mathbf{0}$$

であり，H は C のパリティ検査行列である．

問題 21

$g(x) = 1 + x + x^3$ を生成多項式として，長さが 7 の巡回符号 C の生成行列 G と，パリティ検査行列 H を与え, $GH^t = \mathbf{0}$ が成り立つことを確認せよ.

$(2^m-1, 2^m-m-1)$ ハミング符号は，F^m のすべての非零ベクトルを列ベクトルとする $m \times (2^m-1)$ 行列 H をパリティ検査行列とする線形符号であったことを思い出そう．ここで，$n = 2^m - 1$ とおく．
また $\mathrm{GF}(2^m)$ の原始元を α とし，α の最小多項式を $g(x)$ とおく．α は原始元であるので，

$$1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$$

はすべて異なる．したがって α^i を m 次元のベクトルとみなしたとき，

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots \alpha^{2^m-2} \end{pmatrix}$$

をパリティ検査行列とするハミング符号 C を作ることができる．

$GF(2^3)$ の原始元 α，その最小多項式を x^3+x+1 とする．
$\alpha^3 = \alpha + 1$ の関係を用いると α のベキ乗は

$$
\begin{array}{ccccccccc}
\alpha^0 & = & 1 & & & & & & (100) \\
\alpha^1 & = & & & \alpha & & & & (010) \\
\alpha^2 & = & & & & & \alpha^2 & & (001) \\
\alpha^3 & = & 1 & + & \alpha & & & & (110) \\
\alpha^4 & = & & & \alpha & + & \alpha^2 & & (011) \\
\alpha^5 & = & 1 & + & \alpha & + & \alpha^2 & & (111) \\
\alpha^6 & = & 1 & & & + & \alpha^2 & & (101)
\end{array}
$$

となるので，これらの 3 次元ベクトルを列ベクトルとして
並べると，パリティ検査行列 H は

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

として表現できる．

さらに **f** $= (f_0, f_1, \ldots, f_{n-1})$ が C の符号語であるための必要十分条件は,

$$\mathbf{f}H^T = f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1} = 0$$

が成り立つことである.
すなわち $f(x) = f_0 + f_1x + \cdots + f_{n-1}x^{n-1}$ とおくとき, α が $f(x)$ の根となる　($f(\alpha) = 0$ を満たす) ことである.
したがって, 任意の $f(x) \in C$ に対して $f(x) = a(x)g(x)$ と書くことができるので, C は最小多項式 $g(x)$ を生成多項式にもつ巡回符号であり, 次の定理がいえる.

定理 28

$g(x)$ を GF(2) 上の m 次の原始既約多項式（GF(2^m) の原始元の最小多項式) とし，$g(x) = 0$ の 1 つの根を α とすると，$g(x)$ は $(n, k, 3)$-ハミング符号の生成多項式であり，パリティ検査行列

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots \alpha^{2^m-2} \end{pmatrix}$$

をもつ．ただし $n = 2^m - 1, k = n - m$ である．

例 4

GF(2) 上の 3 次の原始既約多項式 $g(x) = x^3 + x + 1$ により，$(7, 4, 3)$-巡回ハミング符号が生成できる．またそのパリティ検査行列は $g(x)$ の 1 つの根 α を用いて

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}$$

と表せる．

巡回ハミング符号の復号法

巡回ハミング符号は，単一誤りが訂正可能である．$g(x)$ を C の m 次の生成多項式とする．$c(x) = a(x)g(x)$ なる符号語を送信したとき，誤り $e(x)$ が付加されて $b(x) = c(x) + e(x)$ が受信されたとする．

(1) $b(x) \equiv s(x) \pmod{g(x)}$ なる $(n-k-1)$ 次以下の多項式 $s(x)$（シンドロームと呼ぶ) を求める．

(2) $s(x) \equiv e(x) \pmod{g(x)}$ が成り立つので，$e(x)$ と $s(x)$ の対応がわかれば，シンドロームから誤り多項式 $e(x)$ をみつけることができる．

(3) もし $s(x) = x^i$ であったならば，受信語 $b(x)$ は $b(x) + x^i$ に復号される．

問題 22

例 4 の巡回ハミング符号 C を用いて，送信多項式 $c(x) = x^6 + x^5 + x^4 + x^2$ に対して誤り $e(x) = x^3$ が付加されたとして，単一誤り訂正が行えることを確認しよう.

$\mathrm{GF}(2^m)$ の原始元を α とするとき，次のようなパリティ検査行列 H をもつ長さ $n = 2^m - 1$ の符号を C とする．ただし，α の最小多項式を $m_1(x)$, α^3 の最小多項式を $m_3(x)$ とする．

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 \cdots & \alpha^{3(2^m-2)} \end{pmatrix}$$

巡回ハミング符号の場合と同様に，任意の符号語 $\mathbf{f} = (f_0, f_1, \ldots, f_{n-1})$ が C の符号語であるための必要十分条件について考えてみる．

$$
\begin{aligned}
\mathbf{f} \in C \quad & \Leftrightarrow \quad \mathbf{f}H^T = 0 \\
& \Leftrightarrow \quad \sum_{i=0}^{n-1} f_i \alpha^i = 0 \text{ and } \sum_{i=0}^{n-1} f_i \alpha^{3i} = 0 \\
& \Leftrightarrow \quad f(\alpha) = 0 \text{ and } f(\alpha^3) = 0 \\
& \Leftrightarrow \quad m_1(x) | f(x) \text{ and } m_3(x) | f(x) = 0 \\
& \Leftrightarrow \quad \text{l.c.m.}\{m_1(x), m_3(x)\} | f(x) \\
& \Leftrightarrow \quad m_1(x)m_3(x) | f(x)
\end{aligned}
$$

すなわち，C は $g(x) = m_1(x)m_3(x)$ を生成多項式とする巡回符号となる．

$m_1(\alpha) = m_1(\alpha^2) = m_1(\alpha^4) = 0, m_3(\alpha) = 0$ であるので，$g(x)$ は $\alpha, \alpha^2, \alpha^3, \alpha^4$ という連続した 4 つの根を持つことに注意すると，パリティ検査行列 H は

$$H' = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots & \alpha^{2^m-2} \\ 1 & \alpha^2 & \alpha^4 \cdots & \alpha^{2(2^m-2)} \\ 1 & \alpha^3 & \alpha^6 \cdots & \alpha^{3(2^m-2)} \\ 1 & \alpha^4 & \alpha^8 \cdots & \alpha^{4(2^m-2)} \end{pmatrix}$$

のように表現することもできる.

では次にこの符号 C が 2 重誤り訂正可能な符号であることを確認しよう.
定理 18 より $e = 2$ 個以内の誤りが正確にもとの符号語に復号できるためには，最小距離 d は，$d \geq 2e + 1$ を満たさなければならないので，少なくとも 5 以上でなければならない.
また定理 23 より，パリティ検査行列 H の任意の $d - 1$ 個の列ベクトルが線形独立で，d 個の列ベクトルに線形従属なものが存在するなら，最小ハミング距離が d であったことを思い出すと，以下のことを示せばよいことがわかる.

定理 29

H' から任意に 4 列選んだ行列を

$$A = \begin{pmatrix} \alpha^{s_1} & \alpha^{s_2} & \alpha^{s_3} & \alpha^{s_4} \\ \alpha^{2s_1} & \alpha^{2s_2} & \alpha^{2s_3} & \alpha^{2s_4} \\ \alpha^{3s_1} & \alpha^{3s_2} & \alpha^{3s_3} & \alpha^{3s_4} \\ \alpha^{4s_1} & \alpha^{4s_2} & \alpha^{4s_3} & \alpha^{4s_4} \end{pmatrix}$$

としたとき，$det(A) \neq 0$ である．

定理 29 は次のヴァンデルモンドの行列式を用いて，証明できる．

Vandermonde（ヴァンデルモンド）の行列式

体 F 上の任意の元 $\beta_1, \beta_2, \ldots, \beta_t$ に対して，$t \times t$ 行列を

$$A = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{t-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta_t & \beta_t^2 & \cdots & \beta_t^{t-1} \end{pmatrix}$$

としたとき，

$$det(A) = \prod_{1 \le i < j \le t} (\beta_j - \beta_i)$$

である．

問題 23

ヴァンデルモンドの行列式を用いて, 定理 29 を示せ.

定理 29 より，H' の任意の 4 個の列ベクトルが線形独立であることから，$H(H')$ から作られる符号 C の最小距離は，少なくとも 5 以上であることがいえるので，C は２重誤り訂正可能な符号であることがわかる．以上のことをまとめると，次の定理が成り立つ．

定理 30

次の行列 H は符号長が $2^m - 1$ の２重 (2-error) 誤り訂正可能な符号のパリティ検査行列であり，この符号の生成多項式は，$g(x) = m_1(x)m_3(x)$ である．ただし α はを $\mathrm{GF}(2^m)$ の原始元であり，$m_i(x)$ は α^i を根に持つ m 次の最小多項式である．

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 \cdots & \alpha^{3(2^m-2)} \end{pmatrix}$$

定理 30 で与えられる符号を 2-error-correcting **BCH 符号**という．さらに上の定理を拡張して次のことがいえる．

定理 31

m を任意の整数とし, $n|2^m-1$ とする．α をを $\mathrm{GF}(2^m)$ 上の 1 の原始 n 乗根とし，$g(x)$ を x^n-1 を割り切る $(n-k)$ 次多項式とする．$g(x)=0$ の根 $\beta_1,\beta_2,\ldots,\beta_{n-k}$ の中に, $\alpha^a,\alpha^{a+1},\ldots,\alpha^{a+\delta-1}$ なる連続した δ 個の 1 の n 乗根が存在すると，$g(x)$ を生成多項式とする巡回符号の最小距離は $\delta+1$ 以上である．

定理 31 の条件を満たす巡回符号を，長さ n, 計画距離 $\delta + 1$ の BCH 符号と呼ぶ．特に $n = 2^m - 1$ のとき，原始 BCH 符号と呼ぶ．このときパリティ検査行列 H は，

$$H = \begin{pmatrix} 1 & \alpha^{a} & \alpha^{2a} & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{a+1} & \alpha^{2(a+1)} & \cdots & \alpha^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a+\delta-1} & \alpha^{2(a+\delta-1)} & \cdots & \alpha^{(n-1)(a+\delta-1)} \end{pmatrix}$$

で与えられ，ヴァンデルモンドの行列式を用いて H の任意の δ 列は線形独立であることが示される．定理 31 の例として，以下に３つの原始 BCH 符号の例を述べる．

例 5

例 4 の生成多項式 $g(x) = x^3 + x + 1$ は，$\mathrm{GF}(2^3)$ 上で連続する２個の根 α, α^2 を持つ.
このとき $g(x)$ で生成される巡回符号 C は，計画距離が３の符号（最小距離が少なくとも 3 以上）であるといえる.
また $g(x)$ は C の符号語であるので，C の最小重みは 3 以下である.
ゆえに C は，長さが 7, 最小距離が 3 の符号である.

例 6

GF(2^4) の原始元 α，α^3 の最小多項式をそれぞれ $m_1(x) = x^4 + x + 1$, $m_3(x) = x^4 + x^3 + x^2 + x + 1$ とする.
このとき $g(x) = m_1(x)m_3(x)$ で生成される巡回符号 C は，計画距離が 5 の符号（最小距離が少なくとも 5 以上）であるといえる.
また $g(x)$ は C の符号語であるので，C の最小重みが 5 以下であることがわかる.
ゆえに C は，長さが 15, 最小距離が 5 の BCH 符号である.

例 7

GF(2^4) の原始元 α，α^3, α^5 の最小多項式をそれぞれ
$m_1(x) = x^4 + x + 1, m_3(x) = x^4 + x^3 + x^2 + x + 1,$
$m_5(x) = x^2 + x + 1$ とする.
このとき $g(x) = m_1(x)m_3(x)m_5(x)$ で生成される巡回符号 C は，計画距離が 7 の符号（最小距離が少なくとも 7 以上）であるといえる.
また $g(x)$ は C の符号語であるので，C の最小重みが 7 以下であることがわかる.
ゆえに C は，長さが 15, 最小距離が 7 の BCH 符号であり 3-error correcting code となる.

問題 24

例 6，例 7 において，α^3 および α^5 の最小多項式が $m_3(x) = x^4 + x^3 + x^2 + x + 1$, $m_5(x) = x^2 + x + 1$ となることを示せ．また生成多項式 $g(x)$ に連続した根がいくつあるかを調べよ．

GF(2^4) の構成

GF(2^4) の原始元 α の最小多項式を $m_1(x) = x^4 + x + 1$ とするとき，GF(2^4) の 0 以外の元は α のベキ表現，α の 3 次以下の多項式表現，4 次元ベクトル表現で与えられる．

$$
\begin{array}{lcccccccl}
\alpha^0 & = & 1 & & & & & & (1000) \\
\alpha^1 & = & & & \alpha & & & & (0100) \\
\alpha^2 & = & & & & & \alpha^2 & & (0010) \\
\alpha^3 & = & & & & & & \alpha^3 & (0001) \\
\alpha^4 & = & 1 & + & \alpha & & & & (1100) \\
\alpha^5 & = & & & \alpha & + & \alpha^2 & & (0110) \\
\alpha^6 & = & & & & & \alpha^2 + & \alpha^3 & (0011) \\
\alpha^7 & = & 1 & + & \alpha & & + & \alpha^3 & (1101)
\end{array}
$$

$$
\begin{array}{rcccccccccl}
\alpha^8 & = & 1 & & & + & \alpha^2 & & & & (1010) \\
\alpha^9 & = & & & \alpha & & & + & \alpha^3 & & (0101) \\
\alpha^{10} & = & 1 & + & \alpha & + & \alpha^2 & & & & (1110) \\
\alpha^{11} & = & & & \alpha & + & \alpha^2 & + & \alpha^3 & & (0111) \\
\alpha^{12} & = & 1 & + & \alpha & + & \alpha^2 & + & \alpha^3 & & (1111) \\
\alpha^{13} & = & 1 & & & + & \alpha^2 & + & \alpha^3 & & (1011) \\
\alpha^{14} & = & 1 & & & & & + & \alpha^3 & & (1001)
\end{array}
$$

長さが $n = 2^m - 1$ の 2-error-correcting BCH 符号 C を例として，復号および誤り訂正を考える．H を次のような C のパリティ検査行列とし，受信した符号語 $\mathbf{y}$ の符号多項式を $y(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ とする．

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 \cdots & \alpha^{3(2^m-2)} \end{pmatrix}$$

このとき，以下の手順で復号する．

(1) $\mathbf{y}$ のシンドローム $\mathbf{s}$ を計算する.

$$\begin{aligned} \mathbf{y}H^T &= (y(\alpha), y(\alpha^3)) \\ &= (s_1, s_3) \end{aligned}$$

を計算する.

(2) $s_1 = s_3 = \mathbf{0}$ であれば，受信語に誤りはない.

(3) もしちょうど1ビットだけ誤りが生じていたとする（そのビット位置を a_i とする）と，誤り多項式 $e(x)$ は，$e(x) = x^i$ となる．したがって

$$\mathbf{y}H^T = eH^T = (e(\alpha), e(\alpha^3)) = (\alpha^i, \alpha^{3i}) = (s_1, s_3)$$

である．ゆえに $s_1^3 = s_3$ であった場合には，a_i が誤っている．

(4a) もし，a_i と a_j $(i \neq j)$ の２ビットに誤りがあったとすると，誤り多項式は，$e(x) = x^i + x^j$ であり，

$$\mathbf{y}H^T = eH^T = (e(\alpha), e(\alpha^3)) = (\alpha^i+\alpha^j, \alpha^{3i}+\alpha^{3j}) = (s_1, s_3)$$

となる．すなわち，

$$\begin{cases} s_1 & = & \alpha^i + \alpha^j \\ s_3 & = & \alpha^{3i} + \alpha^{3j} \end{cases}$$

(4b) そこで，α^i, α^j を根とする多項式 $s(x)$(誤り位置多項式と呼ぶ) を求めてみる.

$$\begin{aligned} s_1^3 &= (\alpha^i + \alpha^j)^3 \\ &= s_3 + \alpha^i \alpha^j s_1 \end{aligned}$$

より

$$\alpha^i \alpha^j = (s_1^3 + s_3)/s_1$$

となるので，$s(x)$ は次を満たしている.

$$\begin{aligned} s(x) &= (x + \alpha^i)(x + \alpha^j) \\ &= x^2 + s_1 x + s_1^2 + s_3/s_1 \end{aligned}$$

(4c) α^i, α^j は２次方程式 $s(x) = 0$ の根であるから，(4a) に示したようにシンドローム s_1, s_3 が計算されていれば，(*) から i, j (誤りがあったビット位置) を求めることができるので，それらの誤りを訂正する（ビットを反転する）.

(5) (*) の $s(x)$ に対し，もし式 $s(x) = 0$ が異なる２根を持たなかったならば，$\mathbf{y}$ は３つ以上の誤りビットを含んでいるので，誤りは訂正できない.

問題 25

例 6 の BCH 符号 C において，受信した符号語

$$\mathbf{y} = (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$$

を復号せよ.