「情報数理」第 2 部

符 号 理 論

平成 20 年 4 月 9 日

早稲田大学理工学部
経営システム工学科

平澤 茂一

目　次

I.

符号理論

情報理論 (information theory) は C.E.Shannon[Sha48] により情報を定量的に扱い，符号化という考え方を導入した情報に関する基礎的理論として誕生し，以来多くの研究が続けられた．また，情報理論は**符号理論** (coding theory, theory of error correcting codes) の研究にも多大なインパクトを与えた．すなわち，Shannon の通信路符号化定理を満たす符号化方式の探索と共に，実用的な誤り訂正・検出が可能な符号化・復号化方式の研究分野の進展である†．情報理論も符号理論も共に雑音のある通信路を扱うが，後者は特に組合せ数学など代数学を用いて，具体的符号の構成法と復号法を与えることが主眼である．

以下，第 1 章で記号導入，定義，重要な考え方などの準備を行い，第 2 章で Hamming 符号など重要な符号について述べる．第 3 章では，誤り訂正能力の限界について論じる．また第 4 章では，符号化をさらに詳しく論じるために，Galois 体など代数的な準備を行ない，第 5 章で Reed-Solomon(RS) 符号を含む Bose-Chaudhuri-Hocquenghem(BCH) 符号について，第 6 章で代数演算による復号アルゴリズムについて簡単に述べる．最後に第 7 章では，若干の応用例をとり上げる．

符号化方式には，大別してブロック符号 (block code) とたたみ込み符号 (convolutional code) の 2 種があるが，ここでは前者に限定して述べる．また，2 元符号化を前提として記述するが，q 元符号化への拡張は差程困難ではない．ただし，q, $q \geq 3$, は素数のべき乗とする．

† 符号理論は情報理論とほぼ同時期に誕生している [Gol49][Ham50].

1
符号化復号化システム

1.1 モデル化

符号理論の研究成果は多くの効率の良い優れた誤り訂正符号を生み出した [†]．符号化の目的は，雑音のある通信路に生じた誤りを訂正し，情報の信頼度を上げることである．**通信路** (channel) とは宇宙通信・衛星通信・無線通信回線や電話回線などの通信媒体，および主記憶装置や補助記憶装置などの記憶媒体を指す数学的モデルである．図 1.1.1 に**符号化復号化システム**を示す．図 1.1.1 で，$\boldsymbol{u}$ は情報記号系列（ベクトル），$\boldsymbol{v}$ は符号語系列（ベクトル），$\boldsymbol{e}$ は誤り系列（ベクトル），$\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}$ は受信系列（ベクトル），$\hat{\boldsymbol{v}}$ は復号された符号語系列（ベクトル）である．ここで，通信路は誤り確率 ε, $0 \leq \varepsilon \leq 0.5$, の **2 元対称通信路** (binary symmetric channel) を仮定する [††]．主記憶装置は図 1.1.2 のように示すことができる．

符号化復号化システムの主要な評価基準は極めて明快であり，次の通りである．

(1) 信頼性 (reliability) $\cdots$ **復号誤り確率** (probability of decoding error) $P(\varepsilon)$

(2) 効率 (efficiency) $\cdots$ **符号化比率** (rate) r

(3) 計算量 (amount of computation) $\cdots$ 復号器の**複雑さ** (complexity) χ

符号化は通常，符号パラメータ (n, k, d) を用いて評価される．n, k, d は，定義 1.2.2 で示す．

[†] 巻末単行本 [Pet61][Ber68][Lin70][MII73][Slo75][KTII75][MS77][MHI82][LC83][Bla83][Hil86][Ima90][EK96][HN99] 参照.

[††] 2 元対称通信路における誤りの生起は，誤りベクトルの要素の位置によらず互いに独立である．

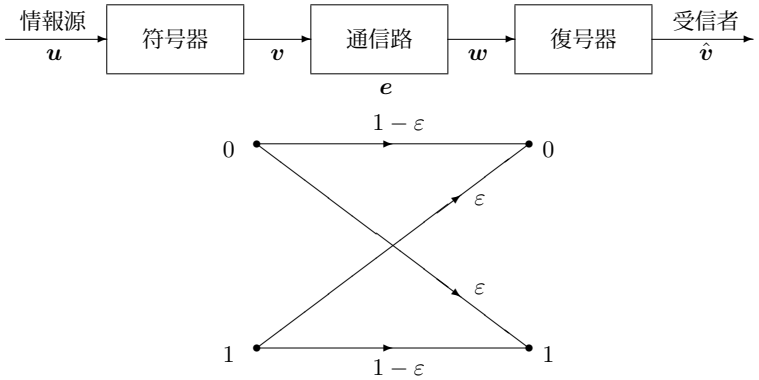


図 1.1.1: 符号化復号化システムと通信路のモデル

1.2 ブロック符号

2 元記号を要素とする長さ n の 2 つのベクトル $\boldsymbol{v}_m$ と $\boldsymbol{v}_{m'}$ を次のように与える.

$$\boldsymbol{v}_m = (v_{m1}, v_{m2}, \cdots, v_{mn}), \tag{1.2.1.a}$$

$$\boldsymbol{v}_{m'} = (v_{m'1}, v_{m'2}, \cdots, v_{m'n}), \tag{1.2.1.b}$$

ここで

$$v_{mi}, v_{m'i} \in \{0,1\} = \mathcal{B}, \quad i = 1, 2, \cdots, n,$$

である.

［**定義 1.2.1** ］**(Hamming 距離)** 2 つのベクトル $\boldsymbol{v}_m, \boldsymbol{v}_{m'}$ の Hamming 距離 $D_H(\cdot,\cdot)$ は次式で定義される.

$$D_H(\boldsymbol{v}_m, \boldsymbol{v}_{m'}) = \sum_{i=1}^{n} d_H(v_{mi}, v_{m'i}), \tag{1.2.2.a}$$

ここで

$$d_H(a,b) = \begin{cases} 0, & a = b; \\ 1, & a \neq b, \end{cases} \tag{1.2.2.b}$$

である†. □

† 2 元記号のとき, $a \neq b$ は $a = 0,\ b = 1$, または $a = 1,\ b = 0$ である.

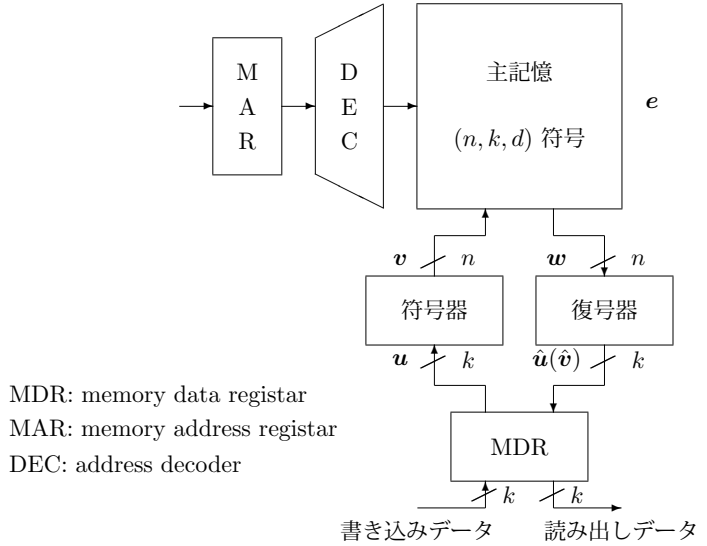


図 1.1.2: 主記憶装置のモデル

Hamming 距離は 2 つのベクトルの対応する位置の記号を比較したとき，異なるものの数である．式 (1.2.2.b) は非 2 元記号の場合にも定義される．また，ここではふれないが，符号理論では Lee 距離も用いられる．両者は，2 元記号の場合一致する．

［**定義 1.2.2** ］2 元 (n,k,d) **ブロック符号** (block code) $\mathcal{C}$ は長さ n の 2 元ベクトル $\boldsymbol{v}_m,\ m=1,2,\cdots,M,$ の集合である (図 1.2.1 参照)．ここで，$M=2^k$ であり，$\boldsymbol{v}_m,\ m=1,2,\cdots,M,$ を**符号語** (codeword) という†．また，n は**符号長** (code length)，k は**情報記号数** (number of information symbols)，d は**最小距離** (minimum distance) である††．□

ここで

$$d=\min_{1\le m,m'\le M,\, m\ne m'} D_H(\boldsymbol{v}_m,\boldsymbol{v}_{m'}), \tag{1.2.3}$$

† 符号 (語) 系列（符号 (語) ベクトル）を単に符号語と呼ぶことが多い．
†† 最小距離 d を特定しないときは (n,k) 符号と表す．

また，符号化比率 (code rate, rate) r は

$$\begin{aligned} r &= (\log_2 M)/n \\ &= k/n, \end{aligned} \tag{1.2.4}$$

で与えられる†.

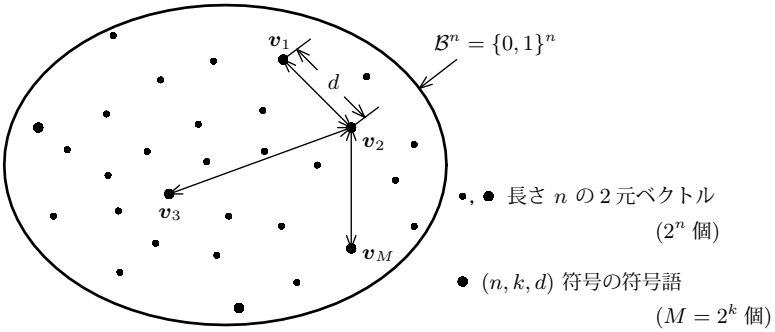


図 1.2.1: 符号化の概念

［**例 1.2.1** ］図 1.2.2 の**偶数（または奇数）パリティ検査符号** (even parity check code) は $(9,8,2)$ 符号である. □

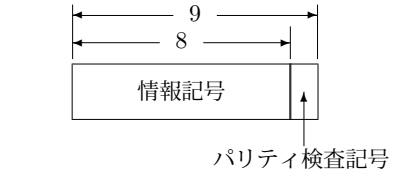
［**例 1.2.2** ］長さ n（奇数）の**反復符号** (repetition code) は $(n,1,n)$ 符号である. 例えば，$n=5$ のとき，符号語は次の 2 つである††.

00000
11111

□

† 符号構成は与えられた n と k で最大の d, したがって $\frac{k}{n} = r$ で最大の $\frac{d}{n}$ を求める問題である．また，(1) 信頼性（訂正能力）は $\frac{d}{n}$ で，(2) 効率は $\frac{k}{n}$ で，(3) 計算量は n のオーダでそれぞれ評価する．$\frac{d}{n}$ と $\frac{k}{n}$ の間には通常トレードオフの関係がある．以上より符号理論では，誤り訂正（復号化）が実現可能な復号手順を考慮しながら，誤り訂正能力の高い効率の良い符号を見出すことが主たるテーマの一つである.

†† 本文中，ベクトルは $(v_1, v_2, \cdots, v_n)$，または簡単に $v_1 v_2 \cdots v_n$ のように表す．例えば，$(0,1,1,0,1)$，または 01101 のように示す.



(例)

0	0	1	0	1	1	0	0	1
0	0	1	1	1	1	0	0	0

図 1.2.2: 偶数パリティ検査符号（偶数重み符号）

［**例 1.2.3** ］図 1.2.3 に，$\boldsymbol{\ell}$ **out of** $\boldsymbol{n}$ **符号**を示す．ただし，$n = 5$, $\ell = 2$ であり

$$M = \begin{pmatrix} n \\ \ell \end{pmatrix}$$
$$= 10,$$
$$r = (\log_2 M)/n \fallingdotseq 0.66,$$

である†. □

11000	01010
00011	01100
00101	10001
00110	10010
01001	10100

$$n = 5, \quad \ell = 2$$

図 1.2.3: ℓ out of n 符号（重み一定符号）の例

［**定義 1.2.3** ］**(Hamming 重み)** ベクトル $\boldsymbol{v}_m$ の Hamming 重み $W_H(\cdot)$ は $\boldsymbol{v}_m$ の n 記号中，非ゼロ記号の数である．すなわち

$$W_H(\boldsymbol{v}_m) = \sum_{i=1}^{n} w_H(v_{mi}), \tag{1.2.5.a}$$

† 長さ $n = 5$ で重みが $\ell = 2$ のパターンを符号語とする.

ここで

$$w_H(a) = \begin{cases} 0, & a = 0; \\ 1, & a \neq 0, \end{cases} \tag{1.2.5.b}$$

である†. □

定義 1.2.1 より容易に次式を得る.

$$D_H(\boldsymbol{v}_m, \boldsymbol{v}_{m'}) = W_H(\boldsymbol{v}_m + \boldsymbol{v}_{m'}), \tag{1.2.6.a}$$

ただし，$\boldsymbol{v}_m + \boldsymbol{v}_{m'} = \boldsymbol{v}_\ell$ とするとき

$$v_{\ell i} = v_{mi} + v_{m'i} \mod 2, \tag{1.2.6.b}$$

である‡.

［**例 1.2.4** ］

$$\begin{aligned} D_H(01001011, 01110010) &= W_H(00111001) \\ &= 4. \end{aligned}$$

□

［**定理 1.2.1** ］(n, k, d) 符号は $d-1$ 個以下のすべての誤りを検出できる．同様に t 個以下のすべての誤りを訂正できる．ここで，$d \geq 2t+1$ である（図 1.2.4 参照）. □

（証明） 演習問題 [問 1.2] 参照. □

定理 1.2.1 より容易に (n, k, d) 符号は t 個以下のすべての誤りを訂正でき，同時に $t+1$ 個以上 d' 個以下のすべての誤りを検出できる必要十分条件は，$d \geq t + d' + 1,\ d' > t$ であることがわかる（演習問題 [問 1.3] 参照）．偶数パリティ検査符号は 1 個‼の誤り検出，反復符号は $(n-1)/2$ 個の誤り訂正が可能である.

［**定義 1.2.4** ］(n, k, d) 符号のすべての符号語 $\boldsymbol{v}_m,\ m = 1, 2, \cdots, M,$ はすべて等確率で用いられるとする．$\boldsymbol{v}_m$ が送信され $\boldsymbol{w}$ が受信されたとき，**最尤復**

† 2 元符号のとき，$a \neq 0$ は $a = 1$ に等しい.
‡ ベクトルの要素間の演算には $GF(2)$ の加算（後出）を仮定している.
‼ 正確には奇数個.

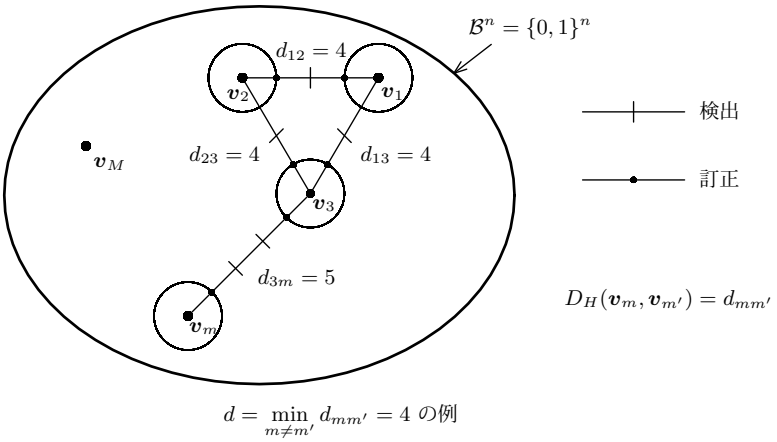


図 1.2.4: 誤りの検出と訂正

号 (maximum likelihood decoding : MLD) **法**は $\boldsymbol{w}$ から次式を満足する $\boldsymbol{v}_{\hat{m}}$ を見つけ出すことである.

$$\boldsymbol{w} \to \boldsymbol{v}_{\hat{m}} \left| \left[\max_{1 \leq i \leq M} P(\boldsymbol{w}|\boldsymbol{v}_i) = P(\boldsymbol{w}|\boldsymbol{v}_{\hat{m}}) \right] . \right. \tag{1.2.7}$$

□

もし，$\hat{m} \neq m$ なら復号誤りが生起している．誤り確率 ε, $0 \leq \varepsilon < 0.5$, の 2 元対称通信路を仮定すると，MLD 法は**最小距離復号** (minimum distance decoding : MDD) **法**と同一である．すなわち

$$D_H(\boldsymbol{v}_{\hat{m}}, \boldsymbol{w}) = e, \tag{1.2.8}$$

とすると

$$P(\boldsymbol{w}|\boldsymbol{v}_{\hat{m}}) = \varepsilon^e (1-\varepsilon)^{n-e}, \tag{1.2.9}$$

であるから，もし e が最小なら $P(\cdot|\cdot)$ は最大である．したがって，Hamming 距離が $\boldsymbol{w}$ に最も近い符号語 $\boldsymbol{v}_{\hat{m}}$ を見出す方法が MLD 法といえる．しかしながら，通常の代数的復号法は $\boldsymbol{w}$ から

$$\boldsymbol{w} \to \boldsymbol{v}_{\hat{m}} \left| [D_H(\boldsymbol{v}_{\hat{m}}, \boldsymbol{w}) \leq \lfloor (d-1)/2 \rfloor \right] , \tag{1.2.10}$$

となる $\boldsymbol{v}_{\hat{m}}$ を見つけ出す．この方法は，**限界距離復号** (bounded distance decoding : BDD) **法**と呼ばれる．ここで，$\lfloor x \rfloor$ は x を越えない最大の整数を示す.

演習問題

[**問 1.1**] 式 (1.2.2.a)，式 (1.2.2.b) の Hamming 距離は距離の 3 公理を満たすことを示せ.

[**問 1.2**] 定理 1.2.1 を証明せよ.

[**問 1.3**] (n, k, d) 符号において，t 個以下のすべての誤りを訂正でき，$t+1$ 個以上 d' 個以下のすべての誤りを検出できる必要十分条件は，$d \geq t + d' + 1$, $d' > t$ であることを示せ.

2
重要な符号

2.1 線形符号

2 元線形符号を仮定し，符号構成法について行列と多項式を用いて記述しよう．

2.1.1 線形符号の性質

集合 $\mathcal{B}$ は 2 つの要素 $\{0,1\}$ からなり，加法，乗法は表 2.1.1 の通りとする†．

表 2.1.1: $GF(2)$ 上の加算と乗算

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

［**定義 2.1.1** ］2 元 (n,k,d) 線形符号は $\mathcal{B}^n = \{0,1\}^n$ の線形部分空間である． □

線形符号において，$\boldsymbol{v}_i$ と $\boldsymbol{v}_j$ が共に符号語とすると，$\boldsymbol{v}_i + \boldsymbol{v}_j = \boldsymbol{v}_l$ もその符号語でなければならない．したがって，2 元線形符号では $W_H(\boldsymbol{v}_l) = D_H(\boldsymbol{v}_i, \boldsymbol{v}_j)$ が成り立つ．

［**定理 2.1.1** ］線形符号の最小距離は非ゼロ符号語の最小重みに等しい． □

（証明） 式 (1.2.6.a) より明らか． □

† すなわち，**Galois 体** $GF(2)$ を仮定する．

［**例 2.1.1** ］例 1.2.1，例 1.2.2 の符号は線形であるが，例 1.2.3 の符号は線形ではない． □

2.1.2 生成行列とパリティ検査行列

線形部分空間の次元が k のとき，(n, k, d) 線形符号から互いに線形独立な k 個の符号語をとり出し，これを $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_k$ とする．このとき，**生成行列** (generator matrix) G は

$$G = \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_k \end{bmatrix}, \tag{2.1.1}$$

で与えられる．ここで，G は $k \times n$ の行列で，その階数 (rank) は k である．通常の行列の基本行操作と列置換により，次の結果が得られる．

［**定理 2.1.2** ］(n, k, d) 線形符号の生成行列 G は次の正準形で与えられる．

$$G = [I_k, P], \tag{2.1.2}$$

ここで，I_k は $k \times k$ の単位行列，P は $k \times (n-k)$ の行列である． □

（証明） 略 □

［**例 2.1.2** ］例 1.2.1，例 1.2.2 の生成行列は図 2.1.1 で与えられる． □

符号化される長さ k の情報記号（系列）を $\boldsymbol{u}$ とすると，これに 1 対 1 に対応する符号語 $\boldsymbol{v}$ は次式で与えられる．

$$\boldsymbol{u} = (u_1, u_2, \cdots, u_k), \tag{2.1.3}$$

$$\begin{aligned} \boldsymbol{v} &= \boldsymbol{u}G \\ &= (v_1, v_2, \cdots, v_n), \end{aligned} \tag{2.1.4}$$

ここで，G が式 (2.1.1) のような $k \times k$ の単位行列を持つとき，$u_i = v_i$, $i = 1, 2, \cdots, k$, である．このように k 個の情報記号と $n-k$ 個の検査記号が区別できるような符号を**組織符号** (systematic code) と呼ぶ（図 2.1.2 参照）．

$$\text{(1) 偶数パリティ検査符号 } : G = \begin{bmatrix} 100000001 \\ 010000001 \\ 001000001 \\ 000100001 \\ 000010001 \\ 000001001 \\ 000000101 \\ 000000011 \end{bmatrix}$$

$$\text{(2) 反復符号} \qquad : G = [11111]$$

図 2.1.1: 偶数パリティ検査符号と反復符号の生成行列

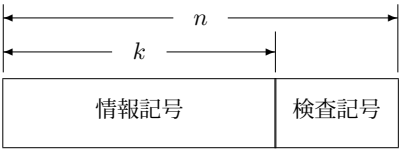


図 2.1.2: 組織符号の符号語

［**定義 2.1.2** ］2 つの符号において，それらの生成行列が基本行操作の下に同一のとき，これら 2 つの符号は**等価** (equivalent) であるという． □

［**定理 2.1.3** ］すべての線形符号は組織符号と等価である． □

（証明） 任意の線形符号はその生成行列の基本行操作により正準形が得られることから明らか． □

以後式 (2.1.2) の形の生成行列を用いる．線形符号 $\mathcal{C}$ が行列 G の行空間，すなわち (n, k, d) 符号を生成するとき，$\mathcal{C}$ は次の定理で**パリティ検査行列** (parity check matrix) H の直交空間である．ここで，$GH^{\mathrm{T}} = 0$ が成り立つ．ただし，行列 A の転置を A^{T} で示す．

［**定理 2.1.4** ］(n, k, d) 線形符号の生成行列 G が式 (2.1.2) で与えられるとき，パリティ検査行列 H は次式で与えられる．

$$H = [-P^{\mathrm{T}}, I_{n-k}], \tag{2.1.5}$$

ここで，I_{n-k} は $(n-k)\times(n-k)$ の単位行列，P^{T} は $(n-k)\times k$ の式 (2.1.2) で与えた行列 P の転置行列である． □

(証明) 式 (2.1.2)，式 (2.1.5) から直接 $GH^{\mathrm{T}}=0$ が成り立つことを導く． □

G を $\mathcal{C}$ に対する生成行列とするとき，H は $\mathcal{C}^{\perp}$ に対する生成行列となる．ここで，$\mathcal{C}^{\perp}$ は $\mathcal{C}$ の**双対符号** (dual code) である．また，H が $\mathcal{C}$ の検査行列のとき，G は $\mathcal{C}^{\perp}$ の検査行列となる．

2.1.3 標準配列

定義 1.2.4，および 2 元対称通信路から，式 (1.2.8) で与えた通り，復号化は与えられた受信系列 $\boldsymbol{w}$ と最小の距離にある符号語 $\boldsymbol{v}_{\hat{m}}$，すなわち最小重みの誤りパターン (誤り系列) $\boldsymbol{e}$ を見出すことである．(n,k,d) 線形符号 $\mathcal{C}$ は，$\mathcal{B}^n=\{0,1\}^n$ の部分空間である．これを

$$\mathcal{B}^n=\bigcup_{i=0}^{2^{n-k}-1}\bigcup_{\ell=0}^{2^k-1}(\boldsymbol{c}_i+\boldsymbol{v}_\ell),$$

$$\{\bigcup_{\ell=0}^{2^k-1}(\boldsymbol{c}_i+\boldsymbol{v}_\ell)\}\cap\{\bigcup_{\ell=0}^{2^k-1}(\boldsymbol{c}_j+\boldsymbol{v}_\ell)\}=\phi,\quad i\neq j,\qquad (2.1.6)$$

のように分割する．ここで，$\mathcal{C}=\{\boldsymbol{v}_0,\boldsymbol{v}_1,\cdots,\boldsymbol{v}_{2^k-1}\}$ は符号語の集合であり，$\cup_{\ell=0}^{2^k-1}(\boldsymbol{c}_i+\boldsymbol{v}_\ell)$ を**コセット** (coset)，$\boldsymbol{c}_i$ を**コセットリーダ** (coset leader) と呼ぶ†．これらを，表 2.1.2 のように配列したものが**標準配列** (standard array) である．

表 2.1.2: (n,k,d) 線形符号の標準配列

コセットリーダ $\boldsymbol{c}_0=0=\boldsymbol{v}_0$	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	$\cdots$	$\boldsymbol{v}_{2^k-1}$	シンドローム $\boldsymbol{s}_0$
$\boldsymbol{c}_1$	$\boldsymbol{c}_1+\boldsymbol{v}_1$	$\boldsymbol{c}_1+\boldsymbol{v}_2$	$\cdots$	$\boldsymbol{c}_1+\boldsymbol{v}_{2^k-1}$	$\boldsymbol{s}_1$
$\boldsymbol{c}_2$	$\boldsymbol{c}_2+\boldsymbol{v}_1$	$\boldsymbol{c}_2+\boldsymbol{v}_2$	$\cdots$	$\boldsymbol{c}_2+\boldsymbol{v}_{2^k-1}$	$\boldsymbol{s}_2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$\boldsymbol{c}_{2^{n-k}-1}$	$\boldsymbol{c}_{2^{n-k}-1}+\boldsymbol{v}_1$	$\boldsymbol{c}_{2^{n-k}-1}+\boldsymbol{v}_2$	$\cdots$	$\boldsymbol{c}_{2^{n-k}-1}+\boldsymbol{v}_{2^k-1}$	$\boldsymbol{s}_{2^{n-k}-1}$

もし，$\boldsymbol{w}=\boldsymbol{c}_i+\boldsymbol{v}_m$ ならば，推定誤り系列 $\boldsymbol{e}$ は $\cup_{\ell=0}^{2^k-1}(\boldsymbol{c}_i+\boldsymbol{v}_\ell)$ の要素であり，そのコセットの最小重みの $\boldsymbol{e}$ を見出す．ここで，コセットリーダ $\boldsymbol{c}_i$ にコ

† コセットは**副群**ともいう．また，コセットを**剰余類**とみたときコセットリーダを**剰余類首**という．

セットの中で最小重みのものを選べば $\boldsymbol{e} = \boldsymbol{c}_i$ である．よって，$\boldsymbol{v}_m = \boldsymbol{w} - \boldsymbol{e}$ を得る．

標準配列は，最上位の行に符号語の集合 $\mathcal{C}$ をおく．次に，$\boldsymbol{c}_0 = 0$ とし，$\boldsymbol{c}_i,\ i = 1, 2, \cdots, 2^{n-k} - 1$, は $\cup_{j=0}^{i-1} \cup_{\ell=0}^{2^k-1} (\boldsymbol{c}_j + \boldsymbol{v}_\ell)$ を除く最小重みのベクトルを選ぶ．その結果，$\boldsymbol{c}_i$ は $\boldsymbol{v}_0 = 0$ を送信したとき最も生起しやすい誤りパターンとなる．これで 2^n 個のすべてのベクトルが，唯一度配列の中に出現する．したがって，標準配列はその表の中で $\boldsymbol{w}$ を見出し，$\boldsymbol{w}$ を含む列の最上位の符号語に復号する意味で**復号表** (decoding table) を与える†．

［**定理 2.1.5** ］誤り確率 ε の 2 元対称通信路において，(n, k, d) 線形符号の標準配列による復号法を考える．正しく復号される確率 $P(\mathcal{C})$ は次式で与えられる．

$$P(\mathcal{C}) = \sum_{\ell=0}^{n} A_\ell \varepsilon^\ell (1-\varepsilon)^{n-\ell}, \tag{2.1.7}$$

ここで，A_ℓ は $W_H(\boldsymbol{c}_i) = \ell$ となるコセットリーダ $\boldsymbol{c}_i$ の数である．ただし，各符号語の生起は等確率とする． □

（証明） 演習問題 [問 2.1] 参照. □

［**系 2.1.1** ］定理 2.1.5 で示した復号法は，最小距離復号 (MDD) 法に等価である． □

（証明） 演習問題 [問 2.2] 参照. □

なお，各符号語の生起する事前確率が等しいとき，最小距離復号法は平均復号誤り確率を最小にする（演習問題 [問 2.3] 参照）．ここで，復号誤り確率 $P(\mathcal{E}) = \sum_{m=1}^{M} P(\boldsymbol{v}_m) P(\boldsymbol{w} \notin \mathcal{R}_m | \boldsymbol{v}_m)$ で定義され，$P(\boldsymbol{v}_m) = \frac{1}{M}$ のとき $P(\mathcal{E}) = 1 - P(\mathcal{C})$ である．ただし，$\mathcal{R}_m$ は $\forall m' \neq m,\ P(\boldsymbol{w}|\boldsymbol{v}_m) > P(\boldsymbol{w}|\boldsymbol{v}_{m'})$ ならば $\boldsymbol{w} \in \mathcal{R}_m$ から与えられる．なお，復号誤り確率 $P(\mathcal{E})$ は語単位で計数する．すなわち，長さ n のブロックで 1 シンボルでも誤っていれば復号誤りとする．

† ただし，ランダム誤り通信路を仮定している．

［**例 2.1.3** ］生成行列 G が次式で与えられたとき，標準配列は表 2.1.3 で与えられる．

$$G = \begin{bmatrix} 100101 \\ 010110 \\ 001111 \end{bmatrix}. \tag{2.1.8}$$

このとき，パリティ検査行列 H は

$$H = \begin{bmatrix} 111100 \\ 011010 \\ 101001 \end{bmatrix}, \tag{2.1.9}$$

で与えられる†．

表 2.1.3: 標準配列の例

コセットリーダ (誤りパターン)								シンドローム
$\boldsymbol{e}_0 = 000000$	100101	010110	110011	001111	101010	011001	111100	$\boldsymbol{s}_0 = 000$
$\boldsymbol{e}_1 = 100000$	000101	110110	010011	101111	001010	111001	011100	$\boldsymbol{s}_1 = 101$
$\boldsymbol{e}_2 = 010000$	110101	000110	100011	011111	111010	001001	101100	$\boldsymbol{s}_2 = 110$
$\boldsymbol{e}_3 = 001000$	101101	011110	111011	000111	100010	010001	110100	$\boldsymbol{s}_3 = 111$
$\boldsymbol{e}_4 = 000100$	100001	010010	110111	001011	101110	011101	111000	$\boldsymbol{s}_4 = 100$
$\boldsymbol{e}_5 = 000010$	100111	010100	110001	001101	101000	011011	111110	$\boldsymbol{s}_5 = 010$
$\boldsymbol{e}_6 = 000001$	100100	010111	110010	001110	101011	011000	111101	$\boldsymbol{s}_6 = 001$
$\boldsymbol{e}_7 = 000011$	100110	010101	110000	001100	101001	011010	111111	$\boldsymbol{s}_7 = 011$

もし，$\boldsymbol{w} = 110111$ のとき，このパターンは第 5 行第 4 列にあり，コセットリーダ $\boldsymbol{e}_4 = 000100$ を誤りパターンとし，最上位の行の $\boldsymbol{v}_3 = 110011$ に復号する．

例 2.1.3 の符号はすべての 1 ビット誤りを訂正するが，2 ビット誤りのすべてを訂正できないから，$(6, 3, 3)$ 符号である．第 1 行の 8 つの符号語が等確率で生起するとき，2 元対称通信路において復号誤り確率を最小にする復号表を与えている． □

2.1.4 シンドローム

次に，パリティ検査行列 H を用いて，受信系列 $\boldsymbol{w}$ から (n, k, d) 符号の適当な符号語に復号する方法について考えよう．

［**定義 2.1.3** ］(**シンドローム**) 受信系列 $\boldsymbol{w}$ の**シンドローム** (syndrome) $\boldsymbol{s}$ は次式で与えられる．

$$\boldsymbol{s} = \boldsymbol{w}H^{\mathrm{T}}. \tag{2.1.10}$$

□

† この符号は，例 2.2.1，式 (2.2.2.b) で与える Hamming 符号の短縮符号（後出）になっている．

いま，$\boldsymbol{v}$ が送信されたとし，これに 2 元対称通信路で雑音ベクトル $\boldsymbol{e}$ が加えられたとする．すなわち

$$\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}, \tag{2.1.11.a}$$

ここで

$$\boldsymbol{e} = (e_1, e_2, \cdots, e_n), \quad e_i \in GF(2),\ i = 1, 2, \cdots, n, \tag{2.1.11.b}$$

である．ここで，$e_i = 0$ のとき正しく，$e_i = 1$ のとき誤って受信されたことを示す．$GH^{\mathrm{T}} = 0$ であるから，次式が得られる．

$$\begin{aligned} \boldsymbol{s} &= \boldsymbol{w}H^{\mathrm{T}} \\ &= (\boldsymbol{v} + \boldsymbol{e})H^{\mathrm{T}} \\ &= (\boldsymbol{u}G + \boldsymbol{e})H^{\mathrm{T}} \\ &= \boldsymbol{e}H^{\mathrm{T}}, \end{aligned} \tag{2.1.12}$$

式 (2.1.11.b) より，シンドローム $\boldsymbol{s}$ は e_i が 1 に対する H の第 i 列 $\boldsymbol{h}_i$ の和の転置であることがわかる．

［**例 2.1.4** ］G が例 2.1.3 と同様，式 (2.1.8) で与えられたとする．このとき，定理 2.1.4 より

$$H = \begin{bmatrix} 111100 \\ 011010 \\ 101001 \end{bmatrix}, \tag{2.1.13.a}$$

ここで

$$P = \begin{bmatrix} 101 \\ 110 \\ 111 \end{bmatrix}, \tag{2.1.13.b}$$

である．これより

$$\begin{aligned} &\boldsymbol{e} = 00\cdots0 \text{ のとき}, \quad \boldsymbol{s} = 000, \\ &\boldsymbol{e} = 10\cdots0 \text{ のとき}, \quad \boldsymbol{s} = 101, \\ &\boldsymbol{e} = 01\cdots0 \text{ のとき}, \quad \boldsymbol{s} = 110, \\ &\qquad\qquad \vdots \\ &\boldsymbol{e} = 00\cdots1 \text{ のとき}, \quad \boldsymbol{s} = 001, \end{aligned} \tag{2.1.14}$$

となる．したがって，任意の 1 つの i に対し，$e_i = 1$, $e_{i'} = 0$, $i \neq i'$ のとき，$\boldsymbol{s}$ は H の i 番目の列の転置に等しい． □

式 (2.1.12) において，任意の符号語 $\boldsymbol{v}$ に対し $\boldsymbol{v}H^{\mathrm{T}} = 0$ であるから，同一のコセットのベクトルは同一のシンドロームをもつ．

［**定理 2.1.6** ］生成行列 G，またはパリティ検査行列 H が与えられたとき，誤りベクトル $\boldsymbol{e}_i$ とシンドローム $\boldsymbol{s}_i$ は 1 対 1 に対応する．ここで，$i = 0, 1, \cdots, 2^{n-k} - 1$ である†．□

（証明） $\boldsymbol{s}_i = \boldsymbol{e}_i H^{\mathrm{T}}$ より明らか（演習問題 [問 2.4] 参照）．□

この結果，標準配列による復号法とシンドロームによる復号法は等価であることがわかる．前者は 2^n 個の要素の表を必要とするが，後者は $2 \times 2^{n-k}$ 個でよい．

次に，最小距離 d を得るためにパリティ検査行列 H の列を選ぶ方法を与える重要な定理を述べる．

［**定理 2.1.7** ］2 元 (n, k, d) 線形符号を考える．そのパリティ検査行列は，非ゼロの任意の $d-1$ 個以下の列が $GF(2)$ で線形独立††である $(n-k) \times n$ の行列である．□

（証明） パリティ検査行列 $H = [\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_n]$ とする．ただし，$\boldsymbol{h}_i$ は長さ $(n-k)$ の列ベクトルである． $t = 1$ のとき，第 i ビットに誤りがあれば $\boldsymbol{s} = \boldsymbol{h}_i^{\mathrm{T}}$ ，第 j ビットに誤りがあれば $\boldsymbol{s}' = \boldsymbol{h}_j^{\mathrm{T}}$ である．ここで，ベクトル $\boldsymbol{a}$ の転置を $\boldsymbol{a}^{\mathrm{T}}$ で示す．これらが互いに異なれば区別できるから，$\boldsymbol{h}_i^{\mathrm{T}} \neq \boldsymbol{h}_j^{\mathrm{T}}$，すなわちすべての列ベクトルが異ならねばならない．

$t = 2$ のときを考える．第 i ，第 j ビットに誤りがあれば $\boldsymbol{s} = \boldsymbol{h}_i^{\mathrm{T}} + \boldsymbol{h}_j^{\mathrm{T}}$, これと異なる第 i' ，第 j' ビットに誤りがあれば $\boldsymbol{s}' = \boldsymbol{h}_{i'}^{\mathrm{T}} + \boldsymbol{h}_{j'}^{\mathrm{T}}$, となる．これらが互いに異なれば区別できるから $\boldsymbol{s} \neq \boldsymbol{s}'$, すなわち $\boldsymbol{h}_i^{\mathrm{T}} + \boldsymbol{h}_j^{\mathrm{T}} + \boldsymbol{h}_{i'}^{\mathrm{T}} + \boldsymbol{h}_{j'}^{\mathrm{T}} \neq 0$ でなければならない．第 l ビットに誤りのある 1 ビット誤りのシンドローム $\boldsymbol{s}''$ とも区別できなければならないから，結局 H の 4 個以下の列ベクトルの 2 を法とする和が非ゼロでなければならない．一般に $t = \lfloor \frac{d-1}{2} \rfloor$ 個以下の誤りを訂正するには H の任意の $2t = d-1$ 個以下の列ベクトルが線形独立でなければならない．□

† 誤りベクトル $\boldsymbol{e}_i$ は重み最小のコセットリーダ $\boldsymbol{c}_i$ である．

†† $d-1$ 個以下の列ベクトルの和が非ゼロと同じ．

［**例 2.1.5** ］$(15, 7, 5)$ 符号のパリティ検査行列 H の例を式 (2.1.15) に示す．

$$H = \begin{bmatrix} 100010011010111 \\ 010011010111100 \\ 001001101011110 \\ 000100110101111 \\ 100011000110001 \\ 000110001100011 \\ 001010010100101 \\ 011110111101111 \end{bmatrix}. \tag{2.1.15}$$

□

定理 2.1.7 は，もし H の d 個の列の和が 0 ならば，$\boldsymbol{v}H^{\mathrm{T}} = 0$ であるから重み d の符号語が存在し，$d-1$ 以下の重みの非ゼロの符号語は存在しいことから容易に理解できる．ここで，非ゼロの符号語 $\boldsymbol{v}$ の重みは少なくとも d であるからである．このことは，任意の $d-1$ 個以下の非ゼロ誤りベクトル $\boldsymbol{e}$ が $\boldsymbol{s} = \boldsymbol{e}H^{\mathrm{T}} \neq 0$ を満足することを示している．したがって，もし $\boldsymbol{s}$ が対応する $\boldsymbol{e}$ に対してすべて異なるならば，シンドロームより誤り訂正が可能であることもわかる．

最後に，限界距離復号 (BDD) 法による符号の性能を評価するための定理を与える．

［**定理 2.1.8** ］2 元 (n, k, d) 符号において，任意の t 個以下の誤り訂正をし，$t+1$ 個以上の誤りは復号できない（誤り検出）か，もしくは復号誤りを生ずるような復号法により復号されるとする．このとき，誤り確率 ε の 2 元対称通信路において，正しく復号される確率 $P(\mathcal{C})$ は次式で与えられる．

$$P(\mathcal{C}) = \sum_{i=0}^{t} \begin{pmatrix} n \\ i \end{pmatrix} \varepsilon^i (1-\varepsilon)^{n-i}, \tag{2.1.16}$$

ここで，$t = \lfloor (d-1)/2 \rfloor$ である． □

（証明） $t+1$ 個以上の誤りは訂正の対象としていないから，求める $P(\mathcal{C})$ は t 個以下の全ての誤りが生ずる確率の和で与えられる． □

なお，このとき式 (2.1.7) において，$A_i = \begin{pmatrix} n \\ i \end{pmatrix}$, $i = 1, 2, \cdots, t$, $A_i = 0$, $i = t+1, t+2, \cdots, n$, である．

2.2 Hamming 符号

Hamming 符号 [Ham50] は重要で最もよく知られた符号の 1 つである．後で述べるように，重み t 以下のすべてのパターンをコセットリーダとし，それ以外のパターンをコセットリーダとしてもたない符号を**完全符号** (perfect code) という†．Hamming 符号は数少ない完全符号の 1 つである．

［**定義 2.2.1** ］**(Hamming 符号)** m 行 2^m-1 列のパリティ検査行列 H を考える．2 元 (n,k,d) Hamming 符号は，すべてゼロのパターンを除く長さ m のすべての可能なパターンを列ベクトルとするパリティ検査行列 H で定義される符号である． □

2^m-1 個の任意の 2 つの列の和は非ゼロであるから，定理 2.1.7 より次の結果を得る．

［**定理 2.2.1** ］2 元 (n,k,d) Hamming 符号はすべての単一誤りを訂正できる．ここで，パラメータは次式で与えられる．

$$n = 2^m - 1, \tag{2.2.1.a}$$

$$k = 2^m - m - 1, \tag{2.2.1.b}$$

$$d = 3. \tag{2.2.1.c}$$

□

(証明) 定義 2.2.1 より n,k は明らか．また，パリティ検査行列 H の列ベクトルはすべて異なるから任意の 2 つの列の和は 0 とはならない．すなわち，$d-1=2$ である． □

［**例 2.2.1** ］2 元 $(7,4,3)$ Hamming 符号のパリティ検査行列 H の 1 つの例は

$$H = \begin{bmatrix} 0001111 \\ 0110011 \\ 1010101 \end{bmatrix}, \tag{2.2.2.a}$$

で与えられる．ここで，H の列は誤りの生じた位置をシンドロームが 2 進で直接示すように配置している．例えば，$\boldsymbol{e} = 0001000$ なら $\boldsymbol{s} = 100$ であり，$\boldsymbol{s}$ は 2 進数で 4

† 例 2.1.3 の符号は重み 1 のすべてのパターン $(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_6)$ をコセットリーダにもつが，重み 2 のパターン $(\boldsymbol{e}_7)$ を 1 つコセットリーダにもつから完全符号ではない．

であるから，$\boldsymbol{e}$ の 4 ビット目に誤りが生じたことを示している．なお，2 元 $(7,4,3)$ Hamming 符号の他の例は

$$H = \begin{bmatrix} 0111100 \\ 1011010 \\ 1101001 \end{bmatrix}, \tag{2.2.2.b}$$

で与えられる（例 2.1.3 はこの符号の短縮符号である）．さらに，他の例として

$$H = \begin{bmatrix} 1001110 \\ 0100111 \\ 0011101 \end{bmatrix}, \tag{2.2.2.c}$$

のように選ぶと，図 2.2.1 のような符号語が得られる（例 2.5.1 (1) 巡回 Hamming 符号参照）．□

0000000	0001011
1110100	1000101
0111010	1100010
0011101	0110001
1001110	1011000
0100111	0101100
1010011	0010110
1101001	1111111

図 2.2.1: 2 元 (7,4,3) Hamming 符号の符号語の例

［**定理 2.2.2** ］(n,k,d) 線形符号において，d を奇数とする．これに偶数パリティ検査記号を付加して，$(n+1,k,d')$ **拡大** (extended) **線形符号**が得られる．ここで，$d'=d+1$ である．□

（証明） (n,k,d) 線形符号を $\mathcal{C}$，$(n+1,k,d')$ 拡大線形符号を $\mathcal{C}'$ とする．$^\forall \boldsymbol{v},\boldsymbol{v}' \in \mathcal{C}'$ に対し附加した偶数パリティ検査記号が同じならば，$\min_{\boldsymbol{v}\neq\boldsymbol{v}'} D_H(\boldsymbol{v},\boldsymbol{v}')=d$，違っていれば，$\min_{\boldsymbol{v}\neq\boldsymbol{v}'} D_H(\boldsymbol{v},\boldsymbol{v}')=d+1$ である．符号 $\mathcal{C}'$ の符号語の重みは偶数であるから符号 $\mathcal{C}'$ の最小距離も偶数である．したがって，d が奇数のとき，符号 $\mathcal{C}'$ の最小距離は $d'=d+1$ である†．□

［**定理 2.2.3** ］(n,k,d) 線形組織符号において，s 個の情報記号を除去して $(n-s,k-s,d')$ **短縮** (shortened) **符号**が得られる．ここで，$d' \geq d$ である．

† もし d が偶数ならば，符号 $\mathcal{C}'$ の最小距離は d または $d+1$ である．

□

（証明） s 個をあらかじめ 0 と考えればよい．このような部分符号を考えても最小距離は小さくはならない†．□

［**定理 2.2.4** ］(n, k, d) 線形組織符号において，s 個の検査記号を除去して $(n-s, k, d')$ **削除** (punctured) **符号**が得られる．ここで，$d' \geq d-s$，$s < n-k$ である．□

（証明） 最小距離 d にある任意の 2 つの符号語において削除した s 個がすべて異なるとすれば，$d' = d - s$ である．重み d の符号語の非ゼロの記号の位置が削除した s 個の記号の位置と異なるとき，$d' \geq d - s + 1$ となる可能性がある．□

定理 2.2.3，定理 2.2.4 は非線形符号に対しても成り立つ．

［**系 2.2.1** ］2 元 (n, k, d) **拡大 Hamming 符号**は単一誤りの訂正，二重誤りの検出ができる．ここで，パラメータは次式で与えられる．

$$n = 2^m, \tag{2.2.3.a}$$

$$k = 2^m - m - 1, \tag{2.2.3.b}$$

$$d = 4. \tag{2.2.3.c}$$

□

（証明） 定理 2.2.2 より明らか．□

2.3 Golay 符号

Golay 符号 [Gol49] も，完全符号の 1 つとして知られている．まず，次式が成り立つことに注意しよう．

$$2^{12}\left[\begin{pmatrix} 23 \\ 0 \end{pmatrix} + \begin{pmatrix} 23 \\ 1 \end{pmatrix} + \begin{pmatrix} 23 \\ 2 \end{pmatrix} + \begin{pmatrix} 23 \\ 3 \end{pmatrix}\right] = 2^{23}. \tag{2.3.1}$$

これは，2 元 $(23, 12, 7)$ Golay 符号が完全符号であることを示している．次式にそのパリティ検査行列の P^{T} の例を与える [Gol49].

† パリティ検査行列 H の列をうまく選べば符号の最小距離が増加する可能性がある．

$$P^{\mathrm{T}} = \begin{bmatrix} 100111000111 \\ 101011011001 \\ 101101101010 \\ 101110110100 \\ 110011101100 \\ 110101110001 \\ 110110011010 \\ 111001010110 \\ 111010100011 \\ 111100001101 \\ 011111111111 \end{bmatrix}. \tag{2.3.2}$$

［**定理 2.3.1** ］2 元 $(23, 12, 7)$ Golay 符号 $\mathcal{G}_{23}$ は完全符号である． □

（証明） 演習問題 [問 5.1] 参照. □

この他，3 元 $(11, 6, 5)$ Golay 符号も完全符号である．しかし，次式が成り立つにもかかわらず，2 元 $(90, 78, 5)$ 符号は存在しないことが証明されている．

$$2^{78}\left[\begin{pmatrix} 90 \\ 0 \end{pmatrix} + \begin{pmatrix} 90 \\ 1 \end{pmatrix} + \begin{pmatrix} 90 \\ 2 \end{pmatrix}\right] = 2^{90}. \tag{2.3.3}$$

また，自明でない q 元完全符号は，Hamming 符号または Golay 符号と同一のパラメータを持つ．ここで，q は素数のべき乗である．

定理 2.2.2 は 2 元 $(23, 12, 7)$ Golay 符号 $\mathcal{G}_{23}$ から，興味ある性質をもつ 2 元 $(24, 12, 8)$ 拡大 Golay 符号 $\mathcal{G}_{24}$ を導く．

［**定理 2.3.2** ］拡大 Golay 符号 $\mathcal{G}_{24}$ は自己双対符号，すなわち $\mathcal{G}_{24}^{\perp} = \mathcal{G}_{24}$ である． □

（証明） 演習問題 [問 5.2] 参照. □

拡大 Golay 符号 $\mathcal{G}_{24}$ の符号語の重みは 4 の倍数である．また符号 $\mathcal{G}_{24}$ のすべての符号語から任意の位置の 1 つの記号を除去して符号 $\mathcal{G}_{23}$ が得られる．

2.4 Reed-Muller 符号

Reed-Muller(RM) **符号** [Ree54][Mul54] は，広範なパラメータをもつ符号の集合である．**直交符号**より拡張して得られる．

長さ $n = 2^m$ の 2 つの 2 元ベクトル $\boldsymbol{a}, \boldsymbol{b}$ を

$$\boldsymbol{a} = (a_1, a_2, \cdots, a_n), \tag{2.4.1.a}$$

$$\boldsymbol{b} = (b_1, b_2, \cdots, b_n), \tag{2.4.1.b}$$

とする．ここで，m は任意の正整数である．ベクトル積 $\boldsymbol{ab}$ を次式で定義する．

$$\boldsymbol{ab} = (a_1 b_1, a_2 b_2, \cdots, a_n b_n). \tag{2.4.2}$$

いま，$m = 4,\ n = 16$ のとき RM 符号の基底 $\boldsymbol{r}_0, \boldsymbol{r}_1, \cdots, \boldsymbol{r}_4$ を次のように与える．

$$\begin{aligned}
\boldsymbol{r}_0 &= 1111111111111111,\\
\boldsymbol{r}_1 &= 0000000011111111,\\
\boldsymbol{r}_2 &= 0000111100001111,\\
\boldsymbol{r}_3 &= 0011001100110011,\\
\boldsymbol{r}_4 &= 0101010101010101.
\end{aligned} \tag{2.4.3}$$

なお，$m > 4$ の場合も同様である．

［**定義 2.4.1** ］m+1 個の長さ $n = 2^m$ の基底 $\boldsymbol{r}_0, \boldsymbol{r}_1, \cdots, \boldsymbol{r}_m$ と $\boldsymbol{r}_1, \boldsymbol{r}_2, \cdots, \boldsymbol{r}_m$ の r 個までのすべての組合せのベクトル積を基底とする線形ベクトル空間を r 次 (n, k, d) RM 符号と呼ぶ．ただし，$m > r$ とする． □

［**定理 2.4.1** ］r 次 (n, k, d) RM 符号のパラメータは次式で与えられる．

$$n = 2^m, \tag{2.4.4.a}$$

$$k = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}, \tag{2.4.4.b}$$

$$d = 2^{m-r}. \tag{2.4.4.c}$$

□

（証明） 演習問題 [問 2.5] 参照. □

［**例 2.4.1** ］ $m = 4$, $r = 3$ のとき，15×16 の生成行列 G は

$$G = \begin{bmatrix} G_0 \\ G_1 \\ G_2 \\ G_3 \end{bmatrix}, \tag{2.4.5.a}$$

ただし

$$G_0 = \begin{bmatrix} \boldsymbol{r}_0 \end{bmatrix},$$

$$G_1 = \begin{bmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \\ \boldsymbol{r}_3 \\ \boldsymbol{r}_4 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} \boldsymbol{r}_1\boldsymbol{r}_2 \\ \boldsymbol{r}_1\boldsymbol{r}_3 \\ \boldsymbol{v}_1\boldsymbol{r}_4 \\ \boldsymbol{r}_2\boldsymbol{r}_3 \\ \boldsymbol{r}_2\boldsymbol{r}_4 \\ \boldsymbol{r}_3\boldsymbol{v}_4 \end{bmatrix}, \tag{2.4.5.b}$$

$$G_3 = \begin{bmatrix} \boldsymbol{r}_1\boldsymbol{r}_2\boldsymbol{r}_3 \\ \boldsymbol{r}_1\boldsymbol{v}_2\boldsymbol{r}_4 \\ \boldsymbol{v}_1\boldsymbol{r}_3\boldsymbol{r}_4 \\ \boldsymbol{r}_2\boldsymbol{r}_3\boldsymbol{v}_4 \end{bmatrix},$$

で与えられる．このとき，3 次 $(16, 15, 2)$ RM 符号が得られる． □

［**例 2.4.2** ］Mariner 9 号には，画像伝送のため 1 次 $(32, 6, 16)$ RM 符号が用いられている． □

式 (2.4.3) で

$$H = \begin{bmatrix} \boldsymbol{r}_0 \\ \boldsymbol{r}_1 \\ \vdots \\ \boldsymbol{r}_4 \end{bmatrix}, \tag{2.4.6}$$

とおけば，H は $(2^m, 2^m - m - 1, 4)$ 拡大 Hamming 符号のパリティ検査行列に等しい．ただし，$m = 4$ である．したがって，これは一般に $m - 2$ 次 RM

符号である．また，$G=[G_0,G_1,G_2]^{\mathrm{T}}$ とおけば，2 次 $(16,11,4)$ RM 符号が得られる．RM 符号は直交符号を基本としているため，復号化が容易という特長をもつ．

2.5 巡回符号

巡回符号 (cyclic code) は最もよく研究された符号の 1 つで，多くの性質が知られた重要な符号である．巡回符号は符号化比率の点でも優れ，**バースト誤り** (burst error) 訂正能力ももつ線形符号である．

［**定義 2.5.1** ］**(巡回符号)** 線形かつ符号語の巡回置換もまた符号語であるような符号 $\mathcal{C}$ を巡回符号と呼ぶ． □

定義 2.5.1 より

$$\boldsymbol{v}=(v_0,v_1,v_2,\cdots,v_{n-1})\in\mathcal{C}, \tag{2.5.1.a}$$

のとき

$$\boldsymbol{v}^{\mathrm{c}}=(v_{n-1},v_0,v_1,\cdots,v_{n-2})\in\mathcal{C}, \tag{2.5.1.b}$$

である†．ここで，$v_i\in GF(2)$, $i=1,2,\cdots,n$, である．

［**例 2.5.1** ］

(1) 例 1.2.2 の $(5,1,5)$ 反復符号，例 2.2.1，式 (2.2.2.c) の $(7,4,3)$ Hamming 符号は巡回符号である．

(2) 次の $(n,k,2)$ 符号は巡回置換に関し閉じている．ここで，$k=\log_2 n$ である．

$$\begin{aligned}\boldsymbol{v}_1&=(1,0,0,\cdots,0),\\ \boldsymbol{v}_2&=(0,1,0,\cdots,0),\\ &\vdots\\ \boldsymbol{v}_n&=(0,0,0,\cdots,1).\end{aligned} \tag{2.5.2}$$

しかし，この符号は線形ではないから巡回符号ではない．また符号語の重みは常に 1 で

$$D_H(\boldsymbol{v}_i,\boldsymbol{v}_j)=2,\quad i\neq j,\ i,j=1,2,\cdots,n, \tag{2.5.3}$$

であるから，**等距離符号** (equi-distance code) と呼ばれる．

† 前の記述では $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ としたが，後の多項式表現のため $\boldsymbol{v}=(v_0,v_1,\cdots,v_{n-1})$ のように表わす．

□

代数的記述を容易にするために，符号語 (符号ベクトル) $\boldsymbol{v}$ を

$$\boldsymbol{v} = (v_0, v_1, v_2, \cdots, v_{n-1}), \tag{2.5.4}$$

とするとき，これを**符号語多項式** $v(x)$

$$v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}, \tag{2.5.5}$$

に対応させる．

［**例 2.5.2** ］ベクトル $\boldsymbol{v} = 1001011$ は $v(x) = 1 + x^3 + x^5 + x^6$ と表現される．□

いま，$v(x)$ に x を乗じ，$x^n - 1$ を法とする多項式を求めると

$$\begin{aligned} xv(x) &= v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1} + v_{n-1} x^n \\ &= v_{n-1} + v_0 x + \cdots + v_{n-2} x^{n-1} \mod x^n - 1, \end{aligned} \tag{2.5.6}$$

となり，これは $\boldsymbol{v}$ を右に巡回置換したベクトルに対応する．代数的に言えば，後で述べるように**環** (ring) $\mathcal{R}_n$ の**イデアル** (ideal) $\mathcal{I}$ は，もし $v(x) \in \mathcal{I}$ ならば $xv(x) \in \mathcal{I}$ であるような $\mathcal{R}_n$ の線形部分空間である．したがって，$v(x) \in \mathcal{I}$ ならば $^\forall a(x) \in \mathcal{R}_n$ に対し $a(x)v(x) \in \mathcal{I}$ である．よって，長さ n の巡回符号は多項式環 $\mathcal{R}_n$ のイデアルである．

いま，情報記号ベクトルを $\boldsymbol{u} = (u_0, u_1, \cdots, u_{k-1})$ とし

$$u(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1}, \tag{2.5.7}$$

と表わそう．さらに，**生成多項式** (generator polynomial) $G(x)$ を

$$G(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}, \tag{2.5.8}$$

で与える．$G(x)$ は巡回符号 $\mathcal{C}$ の 0 でない最小次数の符号語多項式である．ここで，$G(x) | x^n - 1$，すなわち $G(x)$ は $x^n - 1$ を割り切る．このとき，符号語 $\boldsymbol{v} = (v_0, v_1, \cdots, v_{n-1})$ より符号語多項式 $v(x)$ は次の定理で与えられる．

［**定理 2.5.1** ］情報記号多項式を $u(x)$, 生成多項式を $G(x)$, $\deg G(x) = n-k$ とするとき，次式で与えられる符号語多項式 $v(x)$ の集合は符号長 n，情報記号数 k の巡回符号 $\mathcal{C}$ である．

$$v(x) = u(x)G(x), \tag{2.5.9}$$

ここで $\deg u(x) < k$, $G(x)|x^n - 1$ である†. □

(証明) $v(x) \in \mathcal{C}$ とする．巡回置換した $xv(x) \pmod{x^n - 1}$ も符号語であり，$^\forall i > 1$, $x^i v(x) \pmod{x^n - 1} \in \mathcal{C}$ である．$\mathcal{C}$ は線形符号であるから，これらの線形結合も巡回符号である．すなわち

$$\sum_i a_i x^i v(x) = a(x)v(x) \pmod{x^n - 1} \in \mathcal{C}, \quad a_i \in \{0, 1\} \tag{2.5.10}$$

である．いま，任意の符号語 $v(x)$ が

$$v(x) = q(x)G(x) + r(x) \tag{2.5.11}$$

になったとする．ただし，$\deg r(x) < \deg G(x)$ である．したがって

$$r(x) = v(x) - q(x)G(x) \tag{2.5.12}$$

となる．$\deg v(x) \leq n - 1$，$\deg q(x)G(x) \leq n - 1$ であり，$q(x)G(x) \in \mathcal{C}$ であるから，$r(x) \in \mathcal{C}$ である．ところが，$\deg r(x) < \deg G(x)$ より $r(x) = 0$ でなければならない．よって，

$$\forall v(x) = q(x)G(x) \tag{2.5.13}$$

となる． □

式 (2.5.9) より明らかな通り，任意の $u(x)$ に対する $v(x)$ は常に $G(x)$ によって割り切られなければならない．

［**例 2.5.3** ］$G(x) = 1 + x + x^3$ とし情報記号ベクトルが 1001 のとき，$u(x) = 1 + x^3$ であるから符号語多項式 $v(x)$ は

$$\begin{aligned} v(x) &= (1 + x^3)(1 + x + x^3) \\ &= 1 + x^3 + x + x^4 + x^3 + x^6 \\ &= 1 + x + x^4 + x^6, \end{aligned} \tag{2.5.14}$$

となり，符号ベクトルは 1100101 となる． □

例 2.5.3 でも明らかな通り，式 (2.5.9) では符号ベクトルの特定の位置に情報記号ベクトルが現れない．すなわち，非組織符号を生成する．そこで

$$u(x)x^{n-k} = q(x)G(x) + r(x), \tag{2.5.15}$$

となるように $u(x)$ に x^{n-k} を乗じ，これを $G(x)$ で割ったときの商を $q(x)$，剰余を $r(x)$ とすると次の定理が得られる．

† 定義 2.5.1 に代わり，これを巡回符号の定義とすることもある．前に述べた通り $\bmod x^n - 1$ の多項式環の剰余類環のイデアルとしても定義できる．

［**定理 2.5.2** ］組織的巡回符号の符号語 $v(x)$ は

$$\begin{aligned} v(x) &= u(x)x^{n-k} - r(x) \\ &= q(x)G(x), \end{aligned} \tag{2.5.16}$$

として生成される．□

［**例 2.5.4** ］例 2.5.3 と同一の条件において，組織的巡回符号の符号ベクトルは次のようにして求められる．

$$\begin{aligned} u(x)x^{n-k} &= (1+x^3)x^3 \\ &= x^3 + x^6 \\ &= (x+x^3)(1+x+x^3) + x + x^2, \\ q(x) &= x + x^3, \\ r(x) &= x + x^2, \\ v(x) &= x + x^2 + (1+x^3)x^3. \end{aligned} \tag{2.5.17}$$

ゆえに，符号ベクトルは 0111001 となる．□

ここで，$G(x), xG(x), \cdots, x^{k-1}G(x)$ は，明らかに巡回符号 $\mathcal{C}$ の線形独立な符号語である．したがって，次の定理を得る．

［**定理 2.5.3** ］生成多項式 $G(x)$ が式 (2.5.8) で与えられるとき，長さ n の巡回符号 $\mathcal{C}$ の生成行列 G は次式で与えられる．

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & 0 \\ 0 & & & & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}. \tag{2.5.18}$$

□

巡回符号は $x^n - 1$ を割り切る多項式 $G(x)$ によりきまるから，イデアルの**直交空間** (null sapce) を用いて次のように完全にきまる．

［**定義 2.5.2** ］巡回符号の生成多項式を $G(x)$ とするとき，**パリティ検査多項式** $H(x)$ は次式で与えられる．

$$H(x) = \frac{x^n - 1}{G(x)}. \tag{2.5.19}$$

□

この結果，符号語 $v(x) = u(x)G(x) \in \mathcal{C}$ は

$$\begin{aligned} v(x)H(x) &= u(x)G(x)H(x) \\ &= 0 \bmod x^n - 1, \end{aligned} \tag{2.5.20}$$

となる．また，パリティ検査行列 H は

$$H(x) = h_0 + h_1 x + \cdots + h_k x^k, \tag{2.5.21}$$

より

$$H = \begin{bmatrix} & & & h_k & \cdots & h_1 & h_0 \\ 0 & & h_k & \cdots & h_1 & h_0 & \\ & & \ddots & & & & 0 \\ h_k & \cdots & h_1 & h_0 & & & \end{bmatrix}, \tag{2.5.22}$$

として与えられる（演習問題 [問 2.7] 参照）．ここで，勿論 $\boldsymbol{v} \in \mathcal{C}$ ならば

$$\boldsymbol{v}H^{\mathrm{T}} = 0, \tag{2.5.23}$$

である．式 (2.5.21) より次の定理が得られる．

［**定理 2.5.4** ］(n, k) 巡回符号 $\mathcal{C}$ の双対符号 $\mathcal{C}^{\perp}$ は $(n, n-k)$ 巡回符号で，その生成多項式 $G^{\perp}(x)$ は次式で与えられる†．

$$G^{\perp}(x) = x^k H(\frac{1}{x}). \tag{2.5.24}$$

□

（証明） 演習問題 [問 2.8] 参照. □

［**例 2.5.5** ］

(1) 例 1.2.2 の $(n, 1, n)$ 反復符号の生成多項式 $G(x)$，パリティ検査多項式 $H(x)$ は

$$G(x) = 1 + x + x^2 + \cdots + x^{n-1}, \tag{2.5.25.a}$$

$$H(x) = 1 + x, \tag{2.5.25.b}$$

で与えられる．したがって，生成行列 G は例 2.1.2 の (2) で与えられ，パリティ検査行列 H は (1) のパリティ検査符号の G に等しい．よって，$(n, 1, n)$ 反復符号の双対符号は $(n, n-1, 2)$ パリティ検査符号である．

† $f_1(x)$ を m 次の多項式としたとき，$f_2(x) = x^m f_1(\frac{1}{x})$ を $f_1(x)$ の**相反多項式** (reciprocal polynomial) という．

(2) $n = 7,\ k = 4$ の巡回符号を考える．

$$x^7 - 1 = (1 + x^2 + x^3)(1 + x + x^3)(1 + x), \tag{2.5.26}$$

より

$$G(x) = 1 + x^2 + x^3, \tag{2.5.27.a}$$

に選ぶと

$$\begin{aligned} H(x) &= (1 + x + x^3)(1 + x), \\ &= 1 + x^2 + x^3 + x^4 \end{aligned} \tag{2.5.27.b}$$

となる．よって

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & & & \\ & 1 & 0 & 1 & 1 & & \\ & & 1 & 0 & 1 & 1 & \\ & & & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{2.5.28.a}$$

$$H = \begin{bmatrix} & & 1 & 1 & 1 & 0 & 1 \\ & 1 & 1 & 1 & 0 & 1 & \\ 1 & 1 & 1 & 0 & 1 & & \end{bmatrix}, \tag{2.5.28.b}$$

で与えられる．また，定理 2.5.2 を用い組織符号より求めると次の通りである．式 (2.5.16) において $u(x) = 1, x, x^2, x^3$ とおくと

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & & & \\ 1 & 1 & 1 & & 1 & & \\ 1 & 1 & 0 & & & 1 & \\ 0 & 1 & 1 & & & & 1 \end{bmatrix}. \tag{2.5.29.a}$$

したがって

$$H = \begin{bmatrix} 1 & & & 1 & 1 & 1 & 0 \\ & 1 & & 0 & 1 & 1 & 1 \\ & & 1 & 1 & 1 & 0 & 1 \end{bmatrix}, \tag{2.5.29.b}$$

である．これは明らかに，例 2.2.1，式 (2.2.2.c) で示した $(7, 4, 3)$ Hamming 符号に他ならない．

(3) 2 元 $(23, 12, 7)$ Golay 符号 $\mathcal{G}_{23}$ は巡回符号であり，その生成多項式 $G(x)$ は

$$G(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1, \tag{2.5.30}$$

で与えられる．ここで††

$$x^{23}-1=(x+1)G(x)\tilde{G}(x), \tag{2.5.31.a}$$

$$\begin{aligned} G^{\perp}(x) &= x^{11}G(x^{-1}) \\ &= x^{12}(1+\frac{1}{x})\tilde{G}(\frac{1}{x}) \\ &= (x+1)G(x) \end{aligned} \tag{2.5.31.b}$$

である．

□

式 (2.5.8) を与えたとき

$$G(x)|x^n-1, \tag{2.5.32}$$

を仮定した．ここで，$G(x)$ が式 (2.5.32) を満足する最小の整数 n を $G(x)$ の**周期** (period) という．また，m 次の既約多項式の周期は 2^m-1 の約数であるが，最大値 2^m-1 を周期とするとき，これを**原始多項式** (primitive polynomial) という．式 (2.5.32) は，式 (2.5.6) において $v(x)$ を巡回置換した $v^{\mathrm{c}}(x)$，すなわち

$$v^{\mathrm{c}}(x)=xv(x)-v_{n-1}(x^n-1), \tag{2.5.33}$$

が $G(x)$ で割り切れるための必要条件である．いま，もしこの条件を除くと，一般にもはや巡回置換に対し閉じていない．

［**定理 2.5.5** ］式 (2.5.32) が成り立たないとき，$G(x)$ で割り切れる $n-1$ 次以下の符号語多項式は**短縮巡回符号** (shortened cyclic code) である． □

（証明） $G(x)$ の周期を $\ell \neq n$ とし，$a\ell \geq n$ となる最小の整数を a とする．このとき，$G(x)$ から生成される符号は長さ $a\ell$ の巡回符号で，長さ n の符号はこれを短縮したものであることを示す．まず，$G(x)|x^{\ell}-1$ から $G(x)|x^{a\ell}-1$，よって $v(x)=u(x)G(x) \bmod x^{a\ell}-1$ となる長さ $a\ell$ の符号語 $v(x)$ の集合は巡回符号である．$v(x)$ の高次の $a\ell-n$ 個が常にゼロとなる符号語だけを考えると明らかに $G(x)$ で割り切れ，しかも $n-1$ 次の多項式で表現できる．したがって，n が ℓ の倍数でないとき，長さ $a\ell$ の巡回符号を短縮した符号が得られる． □

---

†† $x^{23}-1=(1+x)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)$
$=(1+x)G(x)\tilde{G}(x)$
とおいている．

［**例 2.5.6** ］次式の $G(x)$ で生成される符号を考える．

$$G(x) = x^{16} + x^{12} + x^5 + 1$$
$$= (x+1)P(x), \tag{2.5.34.a}$$
$$P(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1, \tag{2.5.34.b}$$

$G(x)$ は因数分解され $P(x)$ は 15 次の**既約多項式** (irreducible polynomial) †であるから，この符号は $(n, n-16, 4)$ 符号で $n < 2^{15} - 1 = 32767$ のとき短縮巡回符号となる‡．□

バースト誤りとは，一般に密集した誤りを指す．$\deg G(x) = n-k$，長さ b のバースト誤り多項式を $x^j b(x),\ j = 0, 1, 2, \cdots, n-b,\ \deg b(x) = b-1$ とすると $G(x)$ は x^j と互いに素であるから，$b-1 < n-k$ のとき，$G(x) \not| x^j b(x)$ である．したがって，次の定理が得られる．

［**定理 2.5.6** ］$G(x)$ で生成される（短縮）巡回符号は長さ $n-k$ 以下のすべての（単一集中）バースト誤りを検出する．□

$b > n-k$ のとき，受信系列から得られる非ゼロシンドロームがランダムに生起するとすれば，バースト誤りの見逃し確率は，$b = n-k+1$ のとき $2^{-(n-k)+1}$, $b > n-k+1$ のとき $2^{-(n-k)}$ と考えることができる．

［**例 2.5.7** ］式 (2.5.34.a) で与えられる符号のバースト誤りの見逃し確率 P_d は次のように与えられる．

$$\begin{aligned} &b \le 16 \text{ のとき} \quad P_d = 0, \\ &b = 17 \text{ のとき} \quad P_d = 2^{-15} \fallingdotseq 0.00003, \\ &b > 17 \text{ のとき} \quad P_d = 2^{-16} \fallingdotseq 0.00002. \end{aligned}$$

□

［**定理 2.5.7** ］m 次の**原始多項式**を生成多項式 $G(x)$ とする符号は $(2^m - 1, 2^m - 1 - m, 3)$ Hamming 符号である‡‡．□

（証明） 演習問題 [問 5.3] 参照． □

---

† m 次の多項式が $m-1$ 次以下の任意の多項式で割り切れないとき，これを既約多項式という（後出）．

‡ この符号は，コンピュータ通信システムなどで広く用いられているもので **CRC**(cyclic redundancy check) **符号**と呼ばれている．

‡‡ これを巡回 Hamming 符号と呼ぶ．

［**例 2.5.8** ］式 (2.5.27.a) の $G(x)$ は原始多項式である．したがって，$n = 2^3 - 1 = 7$ の例 2.5.5 (2) の符号は**巡回 Hamming 符号**である． □

［**定理 2.5.8** ］m 次, $m \geq 2$, の原始多項式をパリティ検査多項式 $H(x)$ とする符号は $(2^m - 1, m, 2^{m-1})$ 符号である．これを**最大長系列符号（M 系列符号）**と呼ぶ． □

（証明） 全ゼロ以外のすべての符号語は $G(x) = \frac{x^n-1}{H(x)}$，$\deg G(x) = n - m$ となる $G(x)$ を生成多項式とする長さ $n = 2^m - 1$ の符号が最大長系列符号である†．よって，$G(x), xG(x), x^2G(x), \cdots, x^{m-1}G(x)$ を基底とする．符号語は全ゼロ多項式と $G(x), xG(x), x^2G(x), \cdots, x^{n-2}G(x) \bmod x^n - 1$ で表されるから非ゼロの符号語の重みはすべて等しい．ところが，長さ $2^m - 1$ の非ゼロの最大長系列符号の符号語には任意の連続した長さ m のパターンはすべて異なり $2^m - 1$ 個ある‡．長さ m のパターン数は 2^m 個あり，したがって $GF(2)$ の元はこの中に $m2^m$ 個，この内 1 の数は $\frac{1}{2}m2^m = m2^{m-1}$ である．非ゼロの最大長系列符号には全ゼロパターンはないから 0 の数は $m(2^{m-1} - 1)$ である．この数は m 倍重複して数えているから 1 の数，すなわち，非ゼロの符号語の重みは 2^{m-1} である‼． □

非ゼロの任意の 1 つの符号語を繰返し並べた系列は $2^m - 1$ を周期とする**M 系列**で，0,1 が疑似的にランダムに生起し，**PN**(psudo noise) **系列**とも呼ばれる．

［**例 2.5.9** ］$m = 3$ とする．$H(x)$ が式 (2.5.27.a) の右辺で与えられる $(7, 3, 4)$ 最大長系列符号は，その生成多項式 $G(x)$ が

$$G(x) = \frac{x^7 - 1}{H(x)} = 1 + x^2 + x^3 + x^4, \tag{2.5.35}$$

† したがって，Hamming 符号のナル空間である．

‡ $H(x)$ を係数とする長さ m の線形フィードバックシフトレジスタの初期値を非ゼロとする．このとき生成される系列 $v_0, v_1, \cdots, v_{n-1}, v_0, v_1, \cdots, v_{m-2}$ からとり出した任意の連続した長さ m のパターンはすべて異なる．なぜならば，周期が $2^m - 1$，レジスタのとり得るパターンの数が $2^m - 1$ であるから，全ゼロでない状態を除き 1 周期後にもとにもどるからである．最大長周期系列（M 系列）の名はここからきている．

‼ 最大長系列符号は式 (q.3.2.1) の Pltokin の上界式を等式で満たす．

より，$2^m = 8$ 個の符号語は

$$\boldsymbol{v}_0 = 0000000, \quad \boldsymbol{v}_1 = 1011100,$$
$$\boldsymbol{v}_2 = 0101110, \quad \boldsymbol{v}_3 = 0010111,$$
$$\boldsymbol{v}_4 = 1001011, \quad \boldsymbol{v}_5 = 1100101,$$
$$\boldsymbol{v}_6 = 1110010, \quad \boldsymbol{v}_7 = 0111001,$$

である†. □

演習問題

[**問 2.1**] 定理 2.1.5 を証明せよ.

[**問 2.2**] 系 2.1.1 を証明せよ.

[**問 2.3**] 符号語の生起確率が等しいとき，最尤復号法は復号誤り確率を最小にすることを示せ.

[**問 2.4**] 2 つのベクトル $\boldsymbol{w}_1, \boldsymbol{w}_2$ が同一のシンドロームをもつことと，これらが同一のコセットに属することは等価であることを示せ.

[**問 2.5**] 定理 2.4.1 を証明せよ.

[**問 2.6**] 2 つの線形符号 (n_1, k_1, d_1) 符号と (n_2, k_2, d_2) 符号をそれぞれ行と列に 2 次元的に配列して得られる (n_0, k_0, d_0) **積符号** (product code) は，$n_0 = n_1 n_2$, $k_0 = k_1 k_2$, $d_0 = d_1 d_2$, であることを示せ.

[**問 2.7**] (n, k, d) 巡回符号のパリティ検査行列 H は式 (2.5.22) で与えられることを示せ.

[**問 2.8**] 定理 2.5.4 を証明せよ.

[**問 2.9**] $n = 7$ の M 系列を示せ.

† 最大長系列符号は**等距離符号**である.

[問 2.10] 誤り確率 ε, $0 \leq \varepsilon < 0.5$, の 2 元対称通信路において，符号長 $n = 2\ell + 1$（ℓ:正整数）の反復符号を用いるとき，**復号誤り確率** $P(\varepsilon)$ を求めよ.

3
誤り訂正能力の限界

ここでは，符号の誤り訂正能力の上界と下界を示す．

3.1 Hamming の上界式

もし $d \geq 2t+1$ ならば，この符号はすべての t 個以下の誤りパターンを訂正できる．M 個の符号語のそれぞれに対し t 個またはそれ以下の誤りパターンの数は

$$1 + \left(\begin{array}{c} n \\ 1 \end{array} \right) + \left(\begin{array}{c} n \\ 2 \end{array} \right) + \cdots + \left(\begin{array}{c} n \\ t \end{array} \right),$$

であるから

$$M \sum_{i=0}^{t} \left(\begin{array}{c} n \\ i \end{array} \right) \leq 2^n, \tag{3.1.1}$$

でなければならない．いま，$M = 2^k$ とすると次の定理が得られる．

［**定理 3.1.1** ］**(Hamming の限界式)** 2 元 $(n, k, 2t+1)$ 線形符号は次式を満足する．

$$n - k \geq \log_2 [\sum_{i=0}^{t} \left(\begin{array}{c} n \\ i \end{array} \right)]. \tag{3.1.2}$$

□

$n \to \infty$ としたときの漸近式として

$$1 - \frac{k}{n} \geq H_b(\frac{t}{n}), \tag{3.1.3}$$

を得る．ここで

$$\lim_{n\to\infty}\frac{1}{n}\log_2[\sum_{i=0}^{j}\left(\begin{array}{c} n \\ i \end{array}\right)] = H_b(\frac{j}{n}), \quad j < \frac{n}{2}, \tag{3.1.4}$$

$$H_b(x) = -x\log_2 x - (1-x)\log_2(1-x),$$

$$0 \le x \le 1, \tag{3.1.5}$$

を用いた [Pet61].

［**定義 3.1.1** ］**(完全符号)** もし式 (3.1.2) の等式が成り立つ符号が存在すれば，その符号を**完全符号** (perfect code) と呼ぶ. □

次の 3 つの線形符号は，完全符号として知られている†.

(1) 反復符号（例 1.2.2），ただし符号長 n は奇数

(2) Hamming 符号（定理 2.2.1）

(3) $(23, 12, 7)$ Golay 符号 [Gol49]（定理 2.3.1）

3.2 Varshamov-Gilbert の下界式

定理 2.1.7 を用いてパリティ検査行列を構成してみる．もし $d-1$ 個以下の列ベクトルの線形結合が非ゼロですべて異なる‡ような行列が見つかれば，これをパリティ検査行列とする符号は，(n, k, d) 符号である．どのような条件であれば，このようなパリティ検査行列が作れるか考えよう．

まず，長さ $n-k$ の非ゼロ列ベクトルを考える．第 j ステップ，$j = 1, 2, \cdots, n$, で $d-2$ 個以下の列ベクトルが線形独立であるような行列 $H_j = [\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_{j-1}]$, $\boldsymbol{h}_0 = \phi$, が既に得られているとする．$j = 1$ では任意の非ゼロベクトルを選べばよい．これを $\boldsymbol{h}_1$ とする．$j = 2$ では，$\boldsymbol{h}_1$ と異なる非ゼロベクトルを選びこれを $\boldsymbol{h}_2$, $\boldsymbol{h}_2 \neq \boldsymbol{h}_1$, とする．$j = 3$ では $\boldsymbol{h}_1, \boldsymbol{h}_2$ と線形独立となる非ゼロベクトル $\boldsymbol{h}_3$ を選ぶ．すなわち，$\boldsymbol{h}_2 \neq \boldsymbol{h}_1$, $\boldsymbol{h}_3 \neq \boldsymbol{h}_2$, $\boldsymbol{h}_3 \neq \boldsymbol{h}_1 + \boldsymbol{h}_2$ である．一般に第 j ステップでは $\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_{j-1}$ の任意の $d-2$ 個の線形結合 $c_1\boldsymbol{h}_1 + c_2\boldsymbol{h}_2 + \cdots + c_{j-1}\boldsymbol{h}_{j-1}$, $c_i \in \{0, 1\}$, $i = 1, 2, \cdots, j-1$, が $\boldsymbol{h}_j$ に等しくならないように選べば，$\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_j$ の任意の $d-1$ 個以下の線形結合は非ゼロである．列ベクトル $\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_{j-1}$ の任意の $d-2$ 個以下の線形

† 極めて特殊な場合として，$(n, n, 1)$ 符号，$(n, 0)$ 符号を加えることがある.

‡ $d-1$ 個以下の列ベクトルが線形独立.

結合によって得られるベクトルの数が，長さ $n-k$ のすべての非ゼロベクトルの数より小さければもう 1 つの列ベクトル $\boldsymbol{h}_j$ を選ぶことができる．すなわち

$$\left(\begin{array}{c} j-1 \\ 1 \end{array}\right)+\left(\begin{array}{c} j-1 \\ 2 \end{array}\right)+\cdots+\left(\begin{array}{c} j-1 \\ d-2 \end{array}\right)<2^{n-k}-1, \quad (3.2.1)$$

のとき，もう 1 つのベクトル $\boldsymbol{h}_j$ をつけ加えることができる．ここで，式 (3.2.1) を満足する j の最大値を n とすると

$$\left(\begin{array}{c} n \\ 1 \end{array}\right)+\left(\begin{array}{c} n \\ 2 \end{array}\right)+\cdots+\left(\begin{array}{c} n \\ d-2 \end{array}\right)\geq 2^{n-k}-1, \quad (3.2.2)$$

を満足する (n,k,d) 符号が存在する．式 (3.2.2) は符号長 n，情報記号数 k の符号で達成できる最小距離 d の下界を与える．

［定理 3.2.1 ］(Varshamov-Gilbert(V-G) の限界式) 次式を満足する 2 元 (n,k,d) 線形符号を構成することが可能である．

$$n-k\leq \log_2[\sum_{i=0}^{d-2}\left(\begin{array}{c} n \\ i \end{array}\right)]. \quad (3.2.3)$$

□

$n\to\infty$ においては

$$H_b(\frac{d-2}{n-1})\simeq H_b(\frac{d}{n}), \quad (3.2.4)$$

が成り立つから，式 (3.1.3) と同様に次式が成り立つ．

$$1-\frac{k}{n}\leq H_b(\frac{d}{n}). \quad (3.2.5)$$

定理 3.1.1 の式 (3.1.2) は符号語から半径 t の超球が互いに交らないで全空間 B^n をうめつくすような符号語の数 $M=2^k$ の限界を与える必要条件である．一方，式 (3.2.1) は (n,k,d) 符号が必ず実現し得ることを保証する M の限界を考える十分条件であり必要条件ではないことに注意する．$d=3$，すなわち $t=1$ とすると，式 (3.1.2) より $2^{n-k}\geq 1+n$，同時に式 (3.2.2) より $2^{n-k}-1\leq n$ が成り立つ．したがって，$n=2^{n-k}-1$ は $t=1$ に対する必要十分条件である†．

符号長 $n\to\infty$ の限界式を図 3.2.1 に示す．ここで，$\delta(r)=\lim_{n\to\infty}\frac{d}{n}$, $r=\frac{k}{n}$, を**漸近的距離比** (asynptotic distance ratio) という．また，$H_b^{-1}(\cdot)$ は式 (3.1.5) で定義した 2 元エントロピー関数 $H_b(\cdot)$ の逆関数である．

† Hamming 符号は式 (2.2.1.a)，式 (2.2.1.b) より等式が成り立つ．

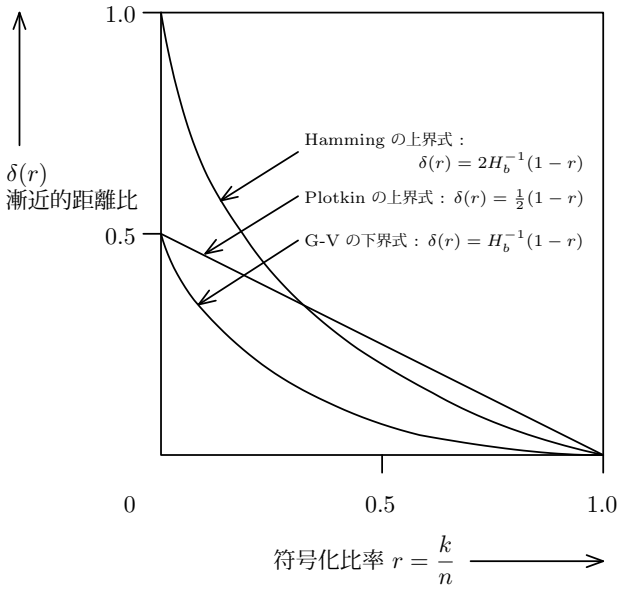


図 3.2.1: 2 元符号の最小距離（漸近的距離比）の限界 [Pet61]

図 3.2.1 より $n \to \infty$ において V-G 下界式を満足する符号が存在することになるが，現在代数的符号化によりそのような符号はまだ知られていない．$n \to \infty$ で　$r \neq 0$ に対し $\delta \neq 0$ となる唯一の符号として Justesen 符号（後述）が知られているが V-G 下界式にはるかに及ばない．ただし，符号長 n が有限では V-G 下界式を越える符号を構成することができる．例えば，$n \leq 10^3$ 程度の BCH 符号（後述）には，V-G 下界式を上まわる符号が多数存在する．

演習問題

[問 3.1] 式 (3.1.4) を導け．

[問 3.2] (Plotkin の上界式) q 元線形 (n, k, d) 符号は次式を満足することを示せ†.

$$d \leq \frac{nq^{k-1}(q-1)}{q^k - 1}. \tag{q.3.2.1}$$

[問 3.3] (Singlton の上界式) q 元線形 (n, k, d) 符号は次式を満足することを示せ.

$$d \leq n + 1 - k. \tag{q.3.3.1}$$

† 非線形符号にも適用できる.

4
抽象代数の基礎

前章まで，主として行列を用いて符号構成，およびその性質について述べてきた．実は既に，表 2.1.1 で Galois 体 $GF(2)$ を用い，また巡回符号の節でもイデアルを説明している．ここでは新しい符号を導き，さらに詳しく論じるために，若干の数学的準備を行う．

4.1 群，環および体

［**定義 4.1.1** ］**(群** (group)**)** 群 $\mathcal{G}$ は次の 4 つの性質を満足する任意の 2 つの元の演算 $*$ をもつ集合である．

G1. $^{\forall}a, b \in \mathcal{G}$ ならば　　$a * b \in \mathcal{G}$.

G2. (結合則) $^{\forall}a, b, c \in \mathcal{G}$ ならば　　$a * (b * c) = (a * b) * c$.

G3. (恒等元) $^{\forall}a \in \mathcal{G}$ に対し　　$^{\exists}e \in \mathcal{G},\ a * e = e * a = a$.

G4. (逆　元) $^{\forall}a \in \mathcal{G}$ に対し　　$^{\exists}b \in \mathcal{G},\ a * b = b * a = e$.

□

［**注 4.1.1** ］

(1) $\mathcal{G}$ の元の数を群の**位数** (order) といい，位数が有限のとき**有限群** (finite group) という．

(2) $^{\forall}a, b \in \mathcal{G}$ に対し，$a * b = b * a$（可換則）が成り立つとき**可換群** (commutative group)，または **Abel 群** (Abelian group) という．

(3) 可換群のとき通常 $*$ を $+$（加法）で表わし**加法群** (additive group) という．このとき，**恒等元**は 0（**ゼロ元**），a の**逆元**は $-a$ で表わす．

(4) 演算 $*$ が $\cdot$（乗法）のとき**乗法群** (multiplicative group) という．このとき，**恒等元**は 1（**単位元**），a の**逆元**は a^{-1} で表わす．可換則は成立しなくてもよい．

(5) $\mathcal{S} \subset \mathcal{G}$ となる群 $\mathcal{S}$ を $\mathcal{G}$ の**部分群**という．$^{\forall}a, b \in \mathcal{S}$ ならば $a * b \in \mathcal{S}$ である．このとき，$\mathcal{G}$ を $\mathcal{S}$ で表 4.1.1 のように展開することが可能である．$\mathcal{G}$ の元は表に唯一回現われる．また，$\mathcal{S}$ の位数（元の数）は $\mathcal{G}$ の位数を割り切る．

表 4.1.1: 群の展開表

$\mathcal{S}$	$s_1 = 1$	s_2	$\cdots$	s_n
$g_1\mathcal{S}$	$g_1 * s_1 = g_1$	$g_1 * s_2$	$\cdots$	$g_1 * s_n$
$g_2\mathcal{S}$	$g_2 * s_1 = g_2$	$g_2 * s_2$	$\cdots$	$g_2 * s_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$g_m\mathcal{S}$	$g_m * s_1 = g_m$	$g_m * s_2$	$\cdots$	$g_m * s_n$

(6) $\mathcal{S} \subset \mathcal{G}$ となる $\mathcal{G}$ の部分群 $\mathcal{S}$ において，$^{\forall}g \in \mathcal{G}$, $^{\forall}s \in \mathcal{S}$ に対し $g^{-1}sg \in \mathcal{S}$ ならば $\mathcal{S}$ を**正規部分群** (normal subgroup) という．よって可換群の部分群は正規部分群である．

□

［**例 4.1.1** ］**無限群** (infinite group)

(1) すべての実数（有理数，複素数）の集合 $\mathcal{R}$ $(\mathcal{Q}, \mathcal{C})$ は通常の加法に関し群をなす．

(2) すべての正および負の整数と 0 の集合 $\mathcal{Z}$ は加法に関し群をなす．

(3) 0 を除くすべての実数（有理数，複素数）の集合 $\mathcal{R}$ $(\mathcal{Q}, \mathcal{C})$ は乗法に関し群をなす．

(4) n 次正則行列は，行列の加法に対し可換群であるが，行列の乗法に関し非可換群をなす．

□

［**例 4.1.2** ］**有限群** (finite group)

(1) $\mathcal{Z}_p = \{0, 1, 2, \cdots, p-1\}$ とする．0 を除く $\mathcal{Z}_p$ は p を法とする乗法群をなす．ただし，p は任意の素数とする．また，これは可換群である．

(2) 唯一の（単位）元 e の集合 $\{e\}$ は群をなす．

(3) $\mathcal{Z}_r$ は r を法とする加法群をなす．ここで，ある整数 r で割った余りの等しい組 $\{0\}, \{1\}, \{2\}, \cdots, \{r-1\}$ を**剰余類** (residue class) という．特に，$\mathcal{Z}_2 = \{0, 1\}$ の演算は表 2.1.1 の $+$ で与えられる．

(4) $\mathcal{S}$ が $\mathcal{G}$ の正規部分群のときコセットの集合は群をなす．例えば，$\mathcal{Z}$ の素数 p による**剰余類**は加法群をなす（表 4.1.2 参照）．

(5) 1 の n 乗根 $\rho_j = e^{i(2\pi j/n)} = \cos(2\pi j/n) + i\sin(2\pi j/n)$, $j = 0, 1, 2, \cdots, n-1$ は乗法群をなす．また，これは可換群である．ここで，$i = \sqrt{-1}$ である．

$p = 3$ のとき

$$\{0\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\},$$

$$\{1\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\},$$

$$\{2\} = \{\cdots, -4, -1, 2, 5, 8, \cdots\}.$$

$+$	$\{0\}$	$\{1\}$	$\{2\}$
$\{0\}$	$\{0\}$	$\{1\}$	$\{2\}$
$\{1\}$	$\{1\}$	$\{2\}$	$\{0\}$
$\{2\}$	$\{2\}$	$\{0\}$	$\{1\}$

表 4.1.2: 加法群の例

□

［**定理 4.1.1** ］恒等元および各元の逆元はそれぞれ唯一つ存在する． □

（証明） 加法群を仮定する．2 つの零元 0 と $0'$ が存在するとき，G3 より

$$0 = 0 + 0' = 0' + 0 = 0',$$

となり $0 = 0'$ である．同様にある元 $a \in \mathcal{G}$ に対し 2 つの逆元 $-a, (-a)'$ が存在するとき，G4 より

$$-a = 0 + (-a) = (-a)' + a + (-a) = (-a)' + 0 = (-a)',$$

となり $-a = (-a)'$ である．乗法群も同様である． □

［**定義 4.1.2** ］**(環** (ring)**)** 環 $\mathcal{R}$ は，次の 4 つの性質を満足する 2 つの演算，加法 $+$ および乗法 $\cdot$ をもつ集合である．

R1. $\mathcal{R}$ は加法群である．

R2. $^\forall a, b \in \mathcal{R}$ ならば $\quad a \cdot b \in \mathcal{R}.$

R3. (結合則) $^\forall a, b, c \in \mathcal{R}$ ならば $\quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$

R4. (分配則) $^\forall a, b, c \in \mathcal{R}$ ならば $\quad a \cdot (b + c) = a \cdot b + a \cdot c,$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

□

［**注 4.1.2** ］$a \cdot b = b \cdot a$ のとき**可換環** (commutative ring) という． □

［**例 4.1.3** ］

(1) すべての実数（有理数，複素数） $\mathcal{R}$ $(\mathcal{Q}, \mathcal{C})$ の集合は通常の加法，乗法に関し環をなす．

(2) $\mathcal{Z}$ は加法，乗法に関し環をなす．これを**整数環** (integer ring) という．

(3) 整数係数の不定元 x の多項式 $a(x)$ の集合は可換環をなす．単位元は $a(x) = 1$ である．

(4) 整数または実数を要素とする行列は行列の加法，乗法に関し非可換環をなす．単位元は単位行列である．

□

［**例 4.1.4** ］

(1) 唯一つの（ゼロ）元 0 の集合 $\{0\}$ は次の演算に関し環をなす．

$$0 + 0 = 0,\ 0 \cdot 0 = 0.$$

(2) $\mathcal{Z}_2 = \{0, 1\}$ は次の演算に関し環をなす．

1) $0 + 0 = 1 + 1 = 0,\ 0 + 1 = 1 + 0 = 1,$
$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1.$

2) $0 + 0 = 1 + 1 = 0,\ 0 + 1 = 1 + 0 = 1,$
$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 1 \cdot 1 = 0.$

(3) $\mathcal{Z}_r = \{0, 1, 2, \cdots, r-1\}$ は r を法とする加法，乗法に関し環をなす．これを**剰余類環** (residue class ring) という．

□

［**定義 4.1.3** ］**(イデアル** (ideal)**)** $\mathcal{I} \subset \mathcal{R}$ となるイデアル $\mathcal{I}$ は次の性質をもつ集合である．

I1. $\mathcal{I}$ は $\mathcal{R}$ の加法に関する部分群である．

I2. $^\forall a \in \mathcal{I},\ ^\forall r \in \mathcal{R}$ ならば，$a \cdot r \in \mathcal{I},\ r \cdot a \in \mathcal{I}$.

□

［**注 4.1.3** ］

(1) 注 4.1.1 (5) において部分群 $\mathcal{S}$ は $a \in \mathcal{S}$ かつ $b \in \mathcal{S}$ のとき，$a * b \in \mathcal{S}$，イデアル $\mathcal{I}$ は $a \in \mathcal{I}$ または $b \in \mathcal{I}$ のとき，$a \cdot b \in \mathcal{I}$ である．表 4.1.2 と同様，$\mathcal{R}$ を $\mathcal{I}$ で展開できる．

(2) 整数環のある部分集合がイデアルであるための必要十分条件は，$v \in \mathcal{I}$ が $\mathcal{I}$ の正の最小の元 g の倍数でなければならない（演習問題 [問 4.1] 参照）．多項式環も同様である．

□

［例 4.1.5 ］

(1) 剰余類を元とする集合は環をなす．これを**剰余類環** (residue class ring) という．例 4.1.2 (4) において $\{0\}$ はイデアルである．

(2) 注 4.1.3 (2) より**巡回符号**はイデアルの性質をもつ．すなわち，$x^n - 1$ を法とする多項式環の剰余類環のイデアルが巡回符号である．

□

［**定義 4.1.4** ］**(体** (field)**)** 体 $\mathcal{F}$ は次の 3 つの性質を満足する 2 つの演算，加法 $+$ および乗法 $\cdot$ をもつ集合である．

F1. $\mathcal{F}$ は加法群である．

F2. $^\forall a, b \in \mathcal{F}$ ならば，$a \cdot b \in \mathcal{F}$．また，非ゼロ元は乗法のもとに可換群をなす†．

F3. (分配則) $^\forall a, b, c \in \mathcal{F}$ ならば，$a \cdot (b + c) = a \cdot b + a \cdot c$,
$(b + c) \cdot a = b \cdot a + c \cdot a$.

□

［注 4.1.4 ］

(1) 単位元をもち，すべての非ゼロ元が乗法に関し逆元をもつ可換環が体である‡．非可換のとき**斜体**という．

(2) 整数 r を法とする整数環は r が素数のとき体をなす（演習問題 [問 4.3] 参照）．

□

［例 4.1.6 ］

(1) すべての実数（有理数，複素数） $\mathcal{R}$ $(\mathcal{Q}, \mathcal{C})$ の集合は通常の加法，乗法に関し体をなす．

(2) すべての整数の集合は体ではない‡‡．

□

［例 4.1.7 ］

† 任意の $a, b \in \mathcal{F}$ に対し $ax = b$ を満足する $x \in \mathcal{F}$ が一意に存在する．

‡ 環においては加減乗の 3 つの演算は可能であるが，乗法の逆元が定義されていないから一般に除算はできない．体においては 4 則演算が可能となる．

‡‡ 1 以外の元に乗法に関する逆元が存在しない．

(1) $\mathcal{Z}_p$ は p を法とする加法，乗法に関し体をなす．ただし，p は素数である．これを**剰余類体** (residue class field) という．p が素数でないときは体にはならない．例えば，4 を法とする乗法では $2 \times 2 = 0$ となり 0 でない数をかけて 0 となる．また $2 \times 1 = 2$, $3 \times 2 = 2$ となり 2 の逆元が 2 つ存在する（演習問題 [問 4.2] 参照）．

(2) $\mathcal{Z}_2 = \{0, 1\}$ は体をなす．その演算を表 2.1.1 に示す．G3 よりゼロ元 0，F2 より単位元 1 をもつ位数の最も小さい体である．

□

［**定義 4.1.5** ］**(Galois** 体 (Galois field)，有限体 (finite field)，素体 (prime field)**)** p 個の元からなる体を Galois 体といい，$GF(p)$ で表わす．ここで，p は素数である．また，p を Galois 体の**標数** (characteristic) とよぶ†. □

［**例 4.1.8** ］例 4.1.7(1) は $GF(p)$ である．$p = 3$ の演算を表 4.1.3 に示す. □

表 4.1.3: $GF(3)$ の演算

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

4.2 Galois 体

$GF(p)$ 上の m 次の多項式 $P(x)$ を次式のように与える．

$$P(x) = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_1 x + f_0, \tag{4.2.1}$$

$$f_m \neq 0,\ f_i \in GF(p),\ i = 0, 1, 2, \cdots, m,$$

ここで，$f_m = 1$ のときこの多項式を**モニック多項式** (monic polynomial) という．注 4.1.4 (2) と同様に，次の定理が得られる（演習問題 [問 4.3] 参照）．

［**定理 4.2.1** ］$m - 1$ 次の多項式 $P(x)$ を法とする $GF(p)$ 上の多項式環は $P(x)$ が**既約** (irreducible) のとき体をなす††. □

† 後に示すように，Galois 体の位数は必ず標数 p のべき乗である．

†† $P(x)$ が $m - 1$ 次以下，$m \geq 1$, の任意の多項式で割り切れないとき，$P(x)$ を**既約多項式**という．

［**例 4.2.1** ］実数体上の既約多項式 $P(x) = x^2 + 1$ を法とする実係数の多項式環を考える．x を含む剰余類を $\{x\} = i$, $i^2 = -1$, とすると，$P(i) = 0$ であるから剰余類体の要素は $a + bi$, $a, b \in \Re$ で与えられる．このように $x^2 + 1$ は実数体上では既約であるが複素数体上では可約で $x^2 + 1 = (x + i)(x - i)$ と因数分解される． □

［**例 4.2.2** ］$GF(2)$ 上の多項式 $P(x) = x^2+1$ を法とする剰余類環 $\{\{0\}, \{1\}, \{x\}, \{x+1\}\}$ は $x^2 + 1 = (x + 1)(x + 1)$ となり可約であるから体をなさない†． □

$P(x)$ は $GF(p)$ では根をもたないが，p^m 個の元からなる体を考えれば根をもつ．そこで，p^m 個の元をもつ Galois 体に拡張する．

［**定義 4.2.1** ］**(拡大体** (extended field)**)** $GF(p)$ を**基礎体** (ground field) とするとき，$P(x)$ から導かれる $GF(p^m)$ を m 次の**拡大体**と呼ぶ．ここで，$P(x)$ は $GF(p)$ 上の次数 m の既約多項式である．また，Galois 体の元の数 p^m を**位数** (order) という． □

［**例 4.2.3** ］$GF(2)$ 上の既約多項式 $P(x) = x^2 + x + 1$ から導かれる拡大体 $GF(2^2)$ を考える．明らかに

$$P(x) = 0 \mod P(x), \tag{4.2.2}$$

より根，すなわち剰余類 $\{x\} = \alpha$ は $P(\alpha) = 0$ を満足する．$\{0, 1\} \in GF(2)$ に α を付加して多項式の剰余類環からなる $GF(2^2)$ の元は

$$\{0, 1, \alpha, 1 + \alpha\} \in GF(2^2), \tag{4.2.3}$$

$\alpha^2 + \alpha + 1 = 0$ より，式 (4.2.3) または

$$\{0, 1, \alpha, \alpha^2\} \in GF(2^2), \tag{4.2.4}$$

となる．表 4.2.1 に $GF(2^2)$ の演算を示す．これは体をなしていることがわかる． □

表 4.2.1: $GF(2^2)$ の演算

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

† $\{x + 1\}\{x + 1\} = 0$ となるから非ゼロの 2 つの元を乗じて 0 となる．

Galois 体には必ず 0 と 1 を元として含む．$GF(p)$ の元は素数 p を法とする整数の剰余類環 $\{0\},\{1\},\cdots,\{p-1\}$ で定義できる．通常，これらの元を単に $0,1,\cdots,p-1$ で表す．位数が p の Galois 体は，p を法とする整数の剰余類環と同型である．すなわち，位数が素数 p の 2 つの Galois 体は，両者の元の対応が一意にきまる†．例 4.1.7 (1) に指摘した通り，$\alpha\to 2,\ \alpha^2\to 3$ として $\mathcal{Z}_4$ で 4 を法とした演算は体にならない．そこで，定理 4.2.1 より $GF(p)$ 上の m 次の既約多項式 $P(x)$ を用いて，位数 $q=p^m$ の拡大体を構成する‡．

［**定理 4.2.2** ］位数 q が素数のべき乗のときに限り，Galois 体 $GF(q)$ が存在する． □

［**定理 4.2.3** ］標数 p の Galois 体 $GF(q),\ q=p^m$, において，$\alpha,\beta\in GF(q)$ に対し次式が成り立つ．

$$(\alpha+\beta)^p=\alpha^p+\beta^p. \tag{4.2.5}$$

□

（証明） 式 (4.2.5) を 2 項展開する．

$$(\alpha+\beta)^p=\alpha^p+\left(\begin{array}{c}p\\1\end{array}\right)\alpha^{p-1}\beta+\cdots+\beta^p. \tag{4.2.6}$$

係数 $\left(\begin{array}{c}p\\i\end{array}\right)$, $1\le i\le p-1$, は p を因数としてもつ．よって，$GF(p)$ において $p=0$ より，式 (4.2.5) が成り立つ． □

［**定義 4.2.2** ］$\alpha\in GF(p^m),\ \alpha\neq 0$, に対し，$m(\alpha)=0$ となる $GF(p)$ 上の最高次の係数が 1 のモニック多項式を考える．その中で最小次数の多項式を元 α の**最小多項式** (minimal polynomial) という． □

［**定理 4.2.4** ］最小多項式 $m(x)$ は

(i) $GF(p)$ 上で既約多項式である．

(ii) その次数は m 以下である．

---

† Galois 体の元 $0,1$ 以外を $\alpha,\beta,\gamma,\cdots$ と表しても $2,3,\cdots,p-1$ と表しても，名前のつけ方を除けばすべて同一である．すなわち，位数が素数 p の Galois 体 $GF(p)$ は p を法とする算法以外に存在しない．

‡ 基礎体を $GF(q)$ とすれば，同様に m' 次の $GF(q)$ 上の既約多項式を用いて $GF(q^{m'})$ を構成することができる．

□

（証明） (i) $m(x)$ が既約でなく $m(x)=m_1(x)m_2(x)$ とすると $m_1(\alpha)=0$ または $m_2(\alpha)=0$ となり $m(x)$ より次数の小さな $m_1(x)$，または $m_2(x)$ が存在し矛盾する．したがって，$m(x)$ は既約である．
(ii) 次数 m の多項式 $f(x)$ の剰余類環は，m 次元ベクトル空間をなす．すなわち，多項式 $r(x)$ のスカラー $a\in GF(p)$ による乗算を $a\{r(x)\}=\{ar(x)\}$ で定義すれば，剰余類環はベクトル空間の公理をすべて満たす．$\{1\},\{x\},\{x^2\},\cdots,\{x^{m-1}\}$ は m 次元空間を張るから任意の剰余類は次数 m 未満の多項式により表わされ

$$\{a_0+a_1x+\cdots+a_{m-1}x^{m-1}\}$$

$$=a_0\{1\}+a_1\{x\}+\cdots+a_{m-1}\{x^{m-1}\},\tag{4.2.7}$$

となる．上式が 0 となるのは，$a_0=a_1=\cdots=a_{m-1}=0$ のときを除き $f(x)$ で割り切れるときに限るが，これは不可能である．よって，m 次以下の多項式 $m(x)$ が存在し $m(\alpha)=0$ となる．このことは，$m+1$ 個の $1,\alpha,\alpha^2,\cdots,\alpha^m$ を考えると必ず線形従属となり，すべて 0 ではない $f_0,f_1,\cdots,f_m\in GF(p)$ に対し

$$f_0+f_1\alpha+\cdots+f_m\alpha^m=0,\tag{4.2.8}$$

から少くとも

$$f(x)=f_0+f_1x+\cdots+f_mx^m,\tag{4.2.9}$$

が存在し，$f(\alpha)=0$ でなければならない．したがって，$m(x)$ の次数は m 以下である． □

［**定理 4.2.5** ］$GF(p)$ 上の多項式 $f(x)$ に対し $f(\alpha)=0,\ \alpha\in GF(p^m)$, ならば $m(x)|f(x)$ である． □

（証明） Euclid の互除法を用いて $m(x)\not|f(x)$ ならば

$$f(x)=q(x)m(x)+r(x),\quad \deg m(x)>\deg r(x),\tag{4.2.10}$$

である．ここで，$x=\alpha$ とすれば $r(\alpha)=0$ でなければならない．これは $m(x)$ が最小多項式であるという仮定に反する． □

位数が有限の**乗法群** (multiplicative group) $\mathcal{G}$ とは $g\in\mathcal{G},\ g\neq 0$, のとき，$g^2\in\mathcal{G},g^3\in\mathcal{G},\cdots,g^e=1,\ e>0$, となる群で，最小の整数 e を位数という．したがって，$1,g,g^2,\cdots,g^{e-1}$ は乗法群をなし，g^i の逆元 $(g^i)^{-1}=g^{e-i}\in\mathcal{G}$ である．さらに，$\mathcal{G}$ に属するすべての元が $g\in\mathcal{G}$ のべき乗で表わされるとき $\mathcal{G}$ を**巡回群** (cyclic group) といい g を**原始元** (primitive element) という．また，巡回群の位数は原始元の位数に等しい†．

† ただし，原始元は 1 つに限らない（演習問題 [問 4.5] 参照）．

いま，Galois 体 $GF(p^m)$ の非ゼロ元を α を用いて表そう．$\{x^i\} = \alpha^i$ であるから $\alpha^i \in GF(p^m)$ である．$GF(p^m)$ の元は有限個であるから，$^\exists i,\ \alpha^i = \alpha^j,\ i > j$, となる．したがって，$\alpha^{i-j} = 1$ となるから，$\alpha^e = 1$ となる最小の正整数を e とすれば e は α の位数であり，$\alpha^0 = 1, \alpha^1, \alpha^2, \cdots, \alpha^{e-1}$, はすべて異なり巡回群をなす．ここで，$\alpha$ が原始元のとき $e = p^m - 1$ である†．したがって，素数 p を標数とする Galois 体 $GF(p^m)$ の非ゼロ元は巡回群でその位数は $p^m - 1$ である．

［**定理 4.2.6** ］次式は $GF(p^m)$ のすべての元を根としてもつ．

$$x^{p^m} - x = 0. \tag{4.2.11}$$

□

（証明） $q = p^m$ とする．$x^q - x = x(x^{q-1} - 1)$ であるから $GF(q)$ の $q-1$ 個の非ゼロ元は $x^{q-1} - 1 = 0$ の根であり，これら非ゼロ元は乗法群をなす††．$GF(q)$ の各元の位数は $q-1$ を割り切らねばならず，したがって $q-1$ 個の元は $x^{q-1} = 1$ の根である．一方，次数は $q-1$ であるから，高々 $q-1$ 個の根しかなく，したがって，これらがすべての元である†††．□

次に，後に必要となる結論を定理として示しておく．

［**定理 4.2.7** ］$P(x)$ を $GF(q)$ 上の m 次の既約多項式とし，その 1 つの根を $\beta \in GF(q^m)$ とする．このとき，$P(x)$ は相異なる m 個の根 $\beta, \beta^q, \beta^{q^2}, \cdots, \beta^{q^{m-1}}$ をもつ．□

（証明） $[P(x)]^q = P(x^q)$ であるから（演習問題 [問 4.4] 参照），$\beta^q, \beta^{q^2}, \cdots, \beta^{q^m}$ が根となることは明らかである．いま，$m > i > j$ とし $\beta^{q^i} = \beta^{q^j}$ と仮定する．$\beta = \beta^{q^m} = (\beta^{q^i})^{q^{m-i}} = (\beta^{q^j})^{q^{m-i}} = \beta^{q^{m+j-i}}$ から $\beta^{q^{m+j-i}-1} = 1$ となり $e|q^m - 1,\ e|q^{m'} - 1,\ m' < m$ である．ここで，e は β の位数である．これは，$P(x)$

† α の位数 e は，$P(x)|(x^e - 1)$ となる最小の正整数 e に一致する．これを $P(x)$ の**周期** (period) という．周期が $p^m - 1$ に等しいものが**原始多項式**である（式 (2.5.32) 参照）．原始多項式は $GF(p^m)$ の原始元を根としてもつ．

†† $\alpha \in GF(q)$ とすれば，他の非ゼロの元は $\alpha^i,\ i = 2, 3, \cdots, q-1$, である．$\alpha$ の位数は $q-1$ であるから $x = \alpha^i$ は $x^{q-1} = 1$ を満たす．

††† $GF(p^m)$ は $GF(p)$ をその部分集合として含むが $x^p - x = 0$ の根は p 個しか存在せず，それらが $GF(p)$ の元である．よって，$x^{p^m} - x = (x^p - x)A(x)$ と表わされる．以上から位数 $q = p^m$ の $GF(q)$ において，$\prod_{i=1}^{n}(x - \rho^i) = x^n - 1$ となる．ただし，ρ が位数 n すなわち $\rho^n = 1$ を満たす最小の n のとき，ρ を 1 の原始 n 乗根 (primitive n-th root of unity) とよぶ．$n = q - 1$ としたものが式 (4.2.11) である．$GF(q)$ の元 α の位数が $q-1$ ならば，α は $GF(q)$ の原始元である．

が $GF(q)$ 上の m 次の既約多項式であることに矛盾する．したがって，これらの根はすべて異なる． □

4.2.1 Galois 体の元のべき表現

$GF(p)$ の元を係数とする m 次の原始多項式 $F(x)$ の根を α とする．先に述べたように，$GF(p^m)$ の非ゼロ元はすべてある原始元 α のべき乗で表わされ，位数 p^m-1 の巡回的な乗法群をなす．すなわち

$$\{0, 1, \alpha, \alpha^2, \cdots, \alpha^{p^m-2}\} = GF(p^m), \tag{4.2.12}$$

である．ここで，$\alpha^{p^m-1} = 1$ である．これを**べき表現**という．

4.2.2 Galois 体の元のベクトル表現

$GF(p)$ 上の m 次の原始多項式 $P(x)$ の根を α とする．$GF(p^m)$ は $P(x)$ を法とする多項式の剰余類環であるから，$P(x)$ の根を $\alpha = \{x\}$ とすれば $GF(p^m)$ の元は，$1, \alpha = \{x\}, \alpha^2 = \{x^2\}, \cdots, \alpha^{m-1} = \{x^{m-1}\}$ の線形結合で表される（定理 4.2.4 (ii) 参照）．これは，次式のように $m-1$ 次の多項式で表わされる．

$$\begin{aligned} &c_{m-1}\{x^{m-1}\} + c_{m-2}\{x^{m-2}\} + \cdots + c_1\{x\} + c_0 \\ &= c_{m-1}\alpha^{m-1} + c_{m-2}\alpha^{m-2} + \cdots + c_1\alpha + c_0, \end{aligned} \tag{4.2.13}$$

$$c_i \in GF(p),\ i = 0, 1, \cdots, m-1.$$

したがって

$$(c_{m-1}, c_{m-2}, \cdots, c_1, c_0) \in GF(p^m), \tag{4.2.14}$$

と表わされる．これを**ベクトル表現**といい，$\{\alpha^{m-1}, \alpha^{m-2}, \cdots, 1\}$ を多項式基底 (polynomial basis) という．

［**例 4.2.4** ］$p = 2,\ m = 3$ とし α の最小多項式 $m(x) = x^3 + x + 1$ とする．$GF(2^3)$ の元は表 4.2.2 のように $GF(2)$ の長さ 3 のベクトルに展開できる． □

演習問題

表 4.2.2: $GF(2^3)$ の元

べき表現	多項式表現			ベクトル表現		
0				0	0	0
1			1	0	0	1
α		α		0	1	0
α^2	α^2			1	0	0
α^3		α	$+1$	0	1	1
α^4	α^2	$+\alpha$		1	1	0
α^5	α^2	$+\alpha$	$+1$	1	1	1
α^6	α^2		$+1$	1	0	1

[問 4.1] 整数環のある部分集合がイデアル $\mathfrak{I}$ であるための必要十分条件は，$s \in \mathfrak{I}$ が $\mathfrak{I}$ の最小の元 r の倍数でなければならないことを示せ．

[問 4.2] 4 を法とする加法と乗法を示せ．また，これが体の公理を満たさないことを示せ．4 つの元からなる集合 $\{0, 1, a, b\}$ が体となる加法と乗法の例を示せ．

[問 4.3] 整数 r を法とする整数環が体をなすための必要十分条件は r が素数であることである．これを証明せよ．

[問 4.4] $GF(2)$ の x の任意の多項式を $a(x)$ とする．次式が成り立つことを示せ†．

$$[a(x)]^2 = a(x^2).$$

[問 4.5] $\{1, 2, 3, 4\} = GF(5)\backslash 0$ よりなる乗法群 $\mathcal{G}$ の原始元を求めよ．

[問 4.6] 例 4.2.4 において原始元を示せ．また，$f(x) = x^3 + x^2 + 1$ としたときはどうか．

[問 4.7] $GF(q)$ 上において $x^c - 1 | x^n - 1$, $n \geq c$, であるための必要十分条件は $c|n$ であることを証明せよ．

† 一般に，$GF(q)$ 上の多項式 $a(x)$ について，$[a(x)]^q = a(x^q)$ が成り立つ．

5
BCH 符号と RS 符号

BCH 符号はその発見者 R.C.Bose, D.K.Ray-Chaudhuri, A.Hocquenghem の 3 人の名前の頭文字をとって名づけられた．優れた能力を持ち，かつ広範囲のパラメータ値に対し定義されたランダム誤り訂正符号の代表的なものである．ここでは，一般に $GF(q)$ 上の符号を考える．ただし，q は素数のべき乗である．

5.1 巡回符号

第 4 章で述べた準備をもとに，再び巡回符号をとりあげ補足し，BCH 符号を導く．

$GF(q)$ 上の m 次の生成多項式 $G(x)$ は，m 個の根 $\alpha_1, \alpha_2, \cdots, \alpha_m$ をもつ．すなわち，α_i の最小多項式を $m_i(x)$ とすると

$$G(x) = \mathrm{LCM}[m_1(x), m_2(x), \cdots, m_m(x)], \tag{5.1.1}$$

である．一方，式 (2.5.5) の符号語 $v(x)$ は $G(x)|v(x)$ であるから，s 個の根 $\alpha_1, \alpha_2, \cdots, \alpha_s$, $s \leq m$, をもつものとする†．このとき

$$v(\alpha_i) = 0, \quad i = 1, 2, \cdots, s, \tag{5.1.2}$$

$$G(x) = \mathrm{LCM}[m_1(x), m_2(x), \cdots, m_s(x)], \tag{5.1.3}$$

さらに，$m_i(x)$ の周期を n_i とするとき

$$\mathrm{LCM}(n_1, n_2, \cdots, n_s)|n, \tag{5.1.4}$$

† 通常，$v(x)$ に対しては $G(x)$ の一部の根が与えられる．例 5.1.1 では $1, \alpha$ のみを与えている．BCH 符号なども同様である．なお，α_i を M_i 重にもつとき $G(x)$ に $[m_i(x)]^{M_i}$ を含ませればよい．

でなければならない（演習問題 [問 4.7] 参照）†．以上より，次の定理を得る．

［**定理 5.1.1** ］$GF(q)$ 上の m 次の多項式 $G(x)$ で生成される式 (5.1.2) の巡回符号のパリティ検査行列 H は次式で与えられる．

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_s & \alpha_s^2 & \cdots & \alpha_s^{n-1} \end{bmatrix}. \tag{5.1.5}$$

□

（証明）式 (5.1.2) の $\boldsymbol{s}$ 個の連立方程式を $\boldsymbol{v}H^{\mathrm{T}} = 0$ とすれば明らか． □

ここで，$G(x)$ を既約多項式に分解し，それぞれより 1 つずつ根を選ぶ．ここで，分解された次数 m_i の最小多項式 $m_i(x)$ の根 α_i は，$GF(q)$ 上で長さ m_i のベクトルである．また，定理 4.2.7 に示した通り，$\alpha_i \neq \alpha_j$ であっても，$m_i(x)$ が α_j の根をもてば $m_j(x)$ は不要である††．

［**例 5.1.1** ］次式で与えられる $G(x) = 0$ の根は $1, \alpha, \alpha^2, \alpha^4$ である．

$$G(x) = (1+x)(1+x+x^3). \tag{5.1.6}$$

いま，$1, \alpha$ を選べば，表 4.2.2 より

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

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}, \tag{5.1.7}$$

となる． □

一般に，2 元 Hamming 符号のパリティ検査行列 H は次のようにして与えられる．$GF(2^m)$ の原始元 α を用い，その最小多項式 $m_1(x)$ を生成多項式とする．このとき

$$H = [1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}], \tag{5.1.8}$$

† $G(x) | x^n - 1$ であるから $\alpha_1, \alpha_2, \cdots, \alpha_s$ は $x^n - 1$ の根である．したがって α_i の周期 $n_i | n$.

†† $G(x)$ を既約多項式に分解し，各々から 1 つずつ根を選べば $\sum m_i = \deg G(x)$ である．その結果，パリティ検査行列 H は $[\deg G(x)] \times n$ の行列で与えられる．

で，各列は $GF(2^m)$ の非ゼロの 2^m-1 個の元からなる．α^j は $GF(2)$ 上で長さ m のベクトルである．

誤り（系列）多項式 (error polynomial) を $e(x)=e_0+e_1x+\cdots+e_{n-1}x^{n-1}$ としたとき，式 (5.1.8) で与えられるパリティ検査行列より，シンドローム $\boldsymbol{s}=\boldsymbol{e}H^{\mathrm{T}}$ は

$$\sum_{i=0}^{n-1} e_i\alpha^i = w(\alpha), \tag{5.1.9}$$

ただし

$$w(x)=w_0+w_1x+w_2x^2+\cdots+w_{n-1}x^{n-1}, \tag{5.1.10}$$

を与える．ここで，$w(x)$ は**受信（系列）多項式** (received polynomial) である．式 (5.1.9) より α^i の i は系列の位置で，$e_i\neq 0$ ならば第 $i+1$ 番目の位置に誤りが生じたことを示す．また α^i の係数 e_i は誤り数値を示す．

巡回 Hamming 符号は，$GF(2^m)$ 上の原始元 α を根とする最小多項式を生成多項式とする符号で $d=3$ である．いま，最小距離 d を大きくするために符号語多項式が満足する根の数を増加させる．もし，α^2 を追加すると $m_1(x)$ は既に根として α^2 をもつから，巡回 Hamming 符号と同一である．すなわち，符号語を $v(x)$ とするとき

$$v(\alpha)=0, \tag{5.1.11.a}$$

$$v(\alpha^2)=0, \tag{5.1.11.b}$$

となり

$$H_1=[1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{n-1}], \tag{5.1.12.a}$$

$$H_2=[1,\alpha^2,\alpha^4,\alpha^6,\cdots,\alpha^{2(n-1)}], \tag{5.1.12.b}$$

は同じパリティ検査行列を与える．

［**例 5.1.2** ］$m=3$ とし $(7,4,3)$ Hamming 符号を考える．$G(x)=x^3+x+1$ と

すると

$$H_1 = \begin{bmatrix} 1001011 \\ 0101110 \\ 0010111 \end{bmatrix}. \tag{5.1.13.a}$$

$$H_2 = \begin{bmatrix} 1001011 \\ 0010111 \\ 0111001 \end{bmatrix}. \tag{5.1.13.b}$$

となり，実際

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}, \tag{5.1.14}$$

としても任意の 2 行が線形独立でしかなく，$d = 3$ である． □

次に，α, α^2 に加え α^3 を追加する．すなわち

$$H_3 = [1, \alpha^3, \alpha^6, \alpha^9, \cdots, \alpha^{3(n-1)}]. \tag{5.1.15}$$

とし

$$H = \begin{bmatrix} H_1 \\ H_3 \end{bmatrix}, \tag{5.1.16}$$

(5.1.17)

とする．いま，H_1 より得られるシンドロームを S_1，H_3 より得られるシンドロームを S_3 とすると

$$\boldsymbol{S} = [S_1, S_3], \tag{5.1.18}$$

は次のように $t = 2$ 個の誤りを訂正できる．2 つの誤りが生起したとし，その誤り位置の未知数を，$A, B \in \{0, 1, \cdots, n-1\}$ とする．

$$S_1 = \alpha^A + \alpha^B, \tag{5.1.19.a}$$

$$S_3 = \alpha^{3A} + \alpha^{3B}. \tag{5.1.19.b}$$

上式より

$$\alpha^A \cdot \alpha^B = (S_1)^2 + \frac{S_3}{S_1}, \tag{5.1.20}$$

を得る．式 (5.1.19.a)，式 (5.1.20) より，α^A, α^B は

$$z^2 + S_1 z + (S_1)^2 + \frac{S_3}{S_1} = 0, \tag{5.1.21}$$

の根として求められる．同様に誤りが 1 個のときは

$$z + S_1 = 0, \tag{5.1.22}$$

の根となる．ただし，$(S_1)^3 = S_3$ である．

以上より，巡回符号の生成多項式の根を追加することより最小距離を増加させることができることがわかる．これを一般に，$\alpha, \alpha^2, \cdots, \alpha^{2t}$ となる連続する根をもつ生成多項式を選ぶことにより BCH 符号が導かれる．

5.2 BCH 符号

BCH 符号は生成多項式 $G(x)$ もしくは生成行列 G，或いはパリティ検査行列 H のいずれかにより定義される．

[定理 5.2.1] α を $GF(q^m)$ の元とする．生成多項式 $G(x)$ が $\alpha^{d_0}, \alpha^{d_0+1}, \cdots, \alpha^{d_0+d-2}$ を根としてもつ q 元 BCH 符号の最小距離は少なくとも d である．□

(証明) 式 (5.1.5) において根 $\alpha_1, \alpha_2, \cdots, \alpha_s$ が題意を満たす根で与えられるとき，そのパリティ検査は式 (5.2.11) のように与えられる†．この行列の任意の $d-1$ 個の相異なる列で作られる次式の行列式 D を考える．

$$D = \begin{vmatrix} (\alpha^{d_0})^{j_1} & (\alpha^{d_0})^{j_2} & \cdots & (\alpha^{d_0})^{j_{d-1}} \\ (\alpha^{d_0+1})^{j_1} & (\alpha^{d_0+1})^{j_2} & \cdots & (\alpha^{d_0+1})^{j_{d-1}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{d_0+d-2})^{j_1} & (\alpha^{d_0+d-2})^{j_2} & \cdots & (\alpha^{d_0+d-2})^{j_{d-1}} \end{vmatrix} \tag{5.2.1}$$

$$= \alpha^{d_0(j_1+j_2+\cdots+j_{d-1})} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{d-1}} \\ \vdots & \vdots & & \vdots \\ (\alpha^{j_1})^{d-2} & (\alpha^{j_2})^{d-2} & \cdots & (\alpha^{j_{d-1}})^{d-2} \end{vmatrix}. \tag{5.2.2}$$

ここで，次式 **Vandermonde の行列式**

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_s \\ x_1^2 & x_2^2 & \cdots & x_s^2 \\ \vdots & \vdots & & \vdots \\ x_1^{s-1} & x_2^{s-1} & \cdots & x_s^{s-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j), \tag{5.2.3}$$

† 定理 5.2.3 参照.

から†，式 (5.2.1) の任意の 2 つの列が同じでなければ $D \neq 0$，よって式 (5.2.11) のパリティ検査行列の任意の $d-1$ またはそれ以下の列の和は非ゼロ，すなわち $GF(q)$ 上で線形独立である．この結果，定理 2.1.7 を q 元符号に拡張すれば最小距離は少なくとも d 以上である‡．□

最も簡単かつ重要な q 元 BCH 符号は $GF(q^m)$ の原始元を α とし，$d_0 = 1,\ d = 2t+1$ とするとき，符号語多項式が

$$\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t}, \tag{5.2.4}$$

を根としてもち t 個の誤りが訂正できる．このように，原始元の連続するべき乗を根とするような $G(x)$ を求めることが必要である．$\alpha, \alpha^2, \cdots, \alpha^{d-1}$ の最小多項式をそれぞれ $m_1(x), m_2(x), \cdots, m_{d-1}(x)$ とするとき

$$G(x) = \mathrm{LCM}[m_1(x), m_2(x), \cdots, m_{d-1}(x)], \tag{5.2.5}$$

で与えられる．特に，2 元 BCH 符号においては任意の偶数乗の根 α^{i_e} はある奇数 i_o の最小多項式 $m_{i_o}(x)$ の根に含まれるから卌

$$G(x) = \mathrm{LCM}[m_1(x), m_3(x), \cdots, m_{d-2}(x)], \tag{5.2.6}$$

である．定理 4.2.4 より $\deg m_i(x) \leq m$，ゆえに $\deg G(x) \leq mt,\ d-1 = 2t$ である．

［**定理 5.2.2** ］次式を満足する 2 元 (n, k, d)（原始）BCH 符号が存在する．

$$n = 2^m - 1, \tag{5.2.7.a}$$

$$n - k \leq mt, \tag{5.2.7.b}$$

$$d = 2t + 1. \tag{5.2.7.c}$$

□

一般に，符号長 $n = q^m - 1$ の BCH 符号を**原始 BCH 符号** (primitive BCH code) と呼ぶ．

---

† もし $x_i = x_j$ なら両辺は共に 0 であるから $(x_i - x_j)$ を因数としてもつ．両辺は同じ次数でなければならないから，左辺の対角要素の積 $1 \cdot x_2 \cdot x_3^2 \cdots x_s^{s-1}$ より右辺の定数は 1 であることがわかる．

‡ 連続根をもてば $D \neq 0$ であるから，これは d 以上の最小距離をもつための十分条件である．

卌 例えば，α^2, α^4 は $m_1(x)$，α^6 は $m_3(x)$，α^8 は $m_1(x)$，α^{10} は $m_5(x)$ のそれぞれの根である．一般にある整数 j により，$i_e = i_o \times 2^j,\ i_o < i_e,$ で表される．

式 (5.2.7.a) ∼ 式 (5.2.7.c) のパラメータは，図 3.2.1 において $d/n \to 0,\ n \to \infty$ ではあるが，$n \leq 1000$ では V-G 下界式を越える [Pet61].

いま，符号語多項式を $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$ とする．$\alpha, \alpha^2, \cdots, \alpha^{2t}$ を根としてもつから

$$\begin{aligned} v(\alpha^i) &= v_0 + v_1\alpha^i + v_2\alpha^{2i} + \cdots + v_{n-1}\alpha^{(n-1)i} \\ &= 0, \quad i = 1, 2, \cdots, 2t, \end{aligned} \tag{5.2.8}$$

すなわち

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \cdots & \alpha^{2t(n-1)} \end{bmatrix}. \tag{5.2.9}$$

とおくと

$$(v_0, v_1, \cdots, v_{n-1})H^{\mathrm{T}} = 0. \tag{5.2.10}$$

一般に，次の定理が与えられる．

［**定理 5.2.3** ］**(BCH 符号)** q 元 (n, k, d) BCH 符号のパリティ検査行列 H は次式で与えられる．

$$H = \begin{bmatrix} 1 & \alpha^{d_0} & (\alpha^{d_0})^2 & \cdots & (\alpha^{d_0})^{n-1} \\ 1 & \alpha^{d_0+1} & (\alpha^{d_0+1})^2 & \cdots & (\alpha^{d_0+1})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d_0+d-2} & (\alpha^{d_0+d-2})^2 & \cdots & (\alpha^{d_0+d-2})^{n-1} \end{bmatrix}. \tag{5.2.11}$$

□

なお，$\alpha^{d_0-1}, \alpha^{d_0+d-1}$ を根としてもたないとき，この d を特に BCH 符号の **設計距離** (designed distance) ということがある．

［**例 5.2.1** ］$t = 1$ とするとき，Hamming 符号は m 次の原始多項式 $m_1(x)$ を生成多項式とする符号である．したがって，パリティ検査行列 H は，α を $m_1(x)$ の原始元とするとき，$m_1(x)$ は α, α^2 を根としてもつから

$$H = [1, \alpha, \cdots, \alpha^{n-1}], \tag{5.2.12}$$

で与えられる．例えば，2 元 $(15, 11, 3)$ Hamming 符号は，α を $m_1(x) = x^4 + x + 1$ の根とするとき，次式で与えられる．

$$H = \begin{bmatrix} 100010011010111 \\ 010011010111100 \\ 001001101011110 \\ 000100110101111 \end{bmatrix}. \tag{5.2.13}$$

□

［**例 5.2.2** ］$t = 2$ とする．2 元 $(15, 7, 5)$ 原始 BCH 符号を構成する．$GF(2^4)$ の原始元を α とすると

$$m_1(x) = x^4 + x + 1, \tag{5.2.14.a}$$

$$m_3(x) = x^4 + x^3 + x^2 + x + 1, \tag{5.2.14.b}$$

より $m_1(x)$ は $\alpha, \alpha^2, \alpha^4, \alpha^8$ を，$m_3(x)$ は $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ をもつ．連続した 4 個の根 $\alpha, \alpha^2, \alpha^3, \alpha^4$ をもつ生成多項式 $G(x)$ は

$$\begin{aligned} G(x) &= \mathrm{LCM}[m_1(x), m_3(x)] \\ &= m_1(x) \cdot m_3(x) \\ &= x^8 + x^7 + x^6 + x^4 + 1, \end{aligned} \tag{5.2.15}$$

となる．このとき，パリティ検査行列 H は

$$H = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}, \tag{5.2.16}$$

すなわち，式 (2.1.15) で与えられる． □

5.3 RS 符号

RS 符号 [RS60] †は，その能力が優れており，復号法の開発にともない注目されている符号の 1 つである．理論的ばかりでなく実用的にも優れ，連接符号 [For66] の外部符号に用いられる他，バースト誤り訂正にも有効である．

$GF(q)$ 上 , $q > 2$, の非 2 元 (n, k, d) BCH 符号は，次のパラメータをもつ．

$$n = q^m - 1, \tag{5.3.1.a}$$

$$n - k \leq 2mt, \tag{5.3.1.b}$$

$$d = 2t + 1. \tag{5.3.1.c}$$

† 有本 [Ari61] により独立に RS 符号に相当する符号の構成法と復号法が発見されている．

RS 符号は BCH 符号において，$m=1$, $n=q-1$ とおいた特別なパラメータの $GF(q)$ 上の符号である．RS 符号の生成多項式 $G(x)$ は $GF(q)$ の原始元を α とすると，$\alpha, \alpha^2, \cdots, \alpha^{d-1}$ を根としてもつ．この結果，次の定理が得られる．

［**定理 5.3.1** ］$GF(q)$ 上 , $q>2$, の (n,k,d) RS 符号は

$$n = q-1, \tag{5.3.2.a}$$

$$0 < k \leq q-1, \tag{5.3.2.b}$$

$$d = n-k+1, \tag{5.3.2.c}$$

を満足する．ここで，生成多項式 $G(x)$ は

$$G(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1}), \quad \alpha \in GF(q), \tag{5.3.3}$$

で与えられる． □

［**定義 5.3.1** ］(n,k,d) 符号において

$$d = n-k+1, \tag{5.3.4}$$

を満たす符号を**最大距離分離** (maximum distance separable : MDS) **符号**という†. □

RS 符号は最大距離分離符号である．すなわち，同一の最小距離の符号の中で，最小の検査記号数となる優れた符号である．RS 符号のパリティ検査行列 H は

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d-1} & \alpha^{(d-1)2} & \cdots & \alpha^{(d-1)(n-1)} \end{bmatrix}. \tag{5.3.5}$$

で与えられる．ここで，$\alpha \in GF(q)$ である．RS 符号は，符号語の記号と原始元 α が共に同一の拡大体 $GF(q)$ の元であるのが特徴である．

［**例 5.3.1** ］$GF(4)$ 上の $(3,2,2)$ RS 符号を構成する．$\alpha^2+\alpha+1=0$, $\alpha^2=\beta$ とし

$$\{0, 1, \alpha, \beta\} = GF(4),$$

† Singlton の上界式 (q.3.3.1) を等式で満たす.

で表わす.

$$G(x) = x - \alpha, \tag{5.3.6}$$

であり，符号語は次の通りである.

$$\begin{array}{cccc} 000 & 1\alpha 0 & \beta 0\alpha & \beta\alpha 1 \\ 01\alpha & \alpha\beta 0 & 10\beta & 111 \\ 0\alpha\beta & \beta 10 & 1\beta\alpha & \alpha\alpha\alpha \\ 0\beta 1 & \alpha 01 & \alpha 1\beta & \beta\beta\beta \end{array}$$

□

［**定理 5.3.2** ］符号長 n の RS 符号を考える．誤りのみを訂正，または消失と誤りの両者を訂正するとき，その復号化に必要な計算労力（論理演算回数）は $O(n \log_2^4 n)$ で与えられる． □

（証明） 略 [Jus72][Hir96]. □

$GF(q)$ 上 , $q = 2^m$, の RS 符号は m ビットを 1 バイトとするバイト誤り訂正符号と考えることができる．それぞれの m ビットをさらに符号化したものが連接符号である [For66][KK80][Hir96].

［**定義 5.3.2** ］**(連接符号)** kK 個の q 元記号を $GF(q^K)$ 上で (n, k, d) 外部符号化し†，さらに n 個，$n \leq q^K - 1$, の q^K 元記号を，それぞれ $GF(q)$ 上で (N, K, D) 内部符号化する．これを連接して得られる (n_0, k_0, d_0) 符号を連接符号と呼ぶ．ここで

$$\begin{aligned} n_0 &= nN, \\ k_0 &= kK, \\ d_0 &\geq dD. \end{aligned} \tag{5.3.7}$$

ただし，q は素数のべき乗である． □

連接符号は図 5.3.1 のように 2 段の符号化過程をもつ.

［**例 5.3.2** ］図 5.3.2 に外部符号を $GF(2^4)$ 上の $(15, 11, 5)$ RS 符号，内部符号を $GF(2)$ 上の $(7, 4, 3)$ Hamming 符号とする 2 元 $(105, 44, 15)$ 連接符号の符号語の例を示す．ここで，外部符号は $P(x) = x^4 + x + 1$ の根を α とするとき，生成

† 外部符号には通常 RS 符号を用いる.

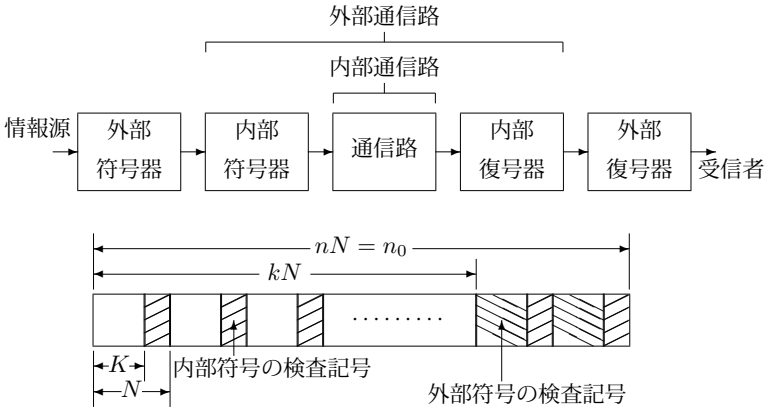


図 5.3.1: 連接符号の符号化復号化過程と符号語

多項式 $g(x) = x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10}$ で生成され，内部符号は生成多項式 $G(x) = x^3 + x + 1$ で生成されるものとする．また，例では情報記号列を 10 進数で $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ とする．このとき，$(15, 11, 5)$ RS 符号の符号語 $(0, \alpha^0, \alpha^1, \alpha^4, \alpha^2, \alpha^8, \alpha^5, \alpha^{10}, \alpha^3, \alpha^{14}, \alpha^9, \alpha^6, \alpha^{11}, \alpha^3, \alpha^4)$ で与えられる．図中縦方向左側 4 列は $GF(2^4)$ 上の RS 外部符号を，横方向 15 行は Hamming 内部符号を示している． □

連接符号を用いて，構成的で漸近的に能率の良い†，現在知られている唯一の代数的符号が **Justesen 符号** [Jus72] である．

［**定義 5.3.3** ］**(Justesen 符号)** kK 個の 2 元情報記号を $GF(2^K)$ 上で (n, k) RS 外部符号化する．ここで，$n = 2^K - 1$ である．次いで，n 個の 2^K 元記号をランダムシフト符号による Wozencraft の $2^K - 1$ 個の集合の相異なる符号に写像し，それぞれ $GF(2)$ 上の $(N, N/2)$ 符号化する．$(N, N/2)$ 符号の検査記号の ℓ 個の記号を除いて得られる $(N - \ell, N/2)$ 削除符号を内部符号とする．ここで，$0 \le \ell < N/2 = K$ である．これらを連接して得られる線形 (n_0, k_0) 符号を Justesen 符号と呼ぶ．ただし，$n_0 = n(2K - \ell)$, $k_0 = kK$ である． □

［**定理 5.3.3** ］2 元 (n_0, k_0, d_0) Justesen 符号の漸近的距離比 $\delta_J(r_0)$ は次式

† 漸近的に能率の良い符号とは， $r > 0$ で $\lim_{n\to\infty} \frac{d}{n} > 0$ の性質を指す．

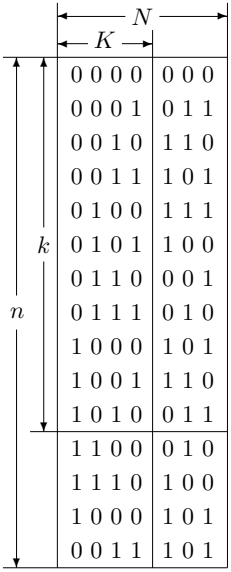


図 5.3.2: 2 元 $(105, 44, 15)$ 連接符号の符号語の例

を満足する．

$$\delta_J(r_0) = \lim_{n_0\to\infty} \inf(d_0/n_0)$$
$$\geq \max_{1/2\leq R<1} (1 - \frac{r_0}{R}) H_b^{-1}(1-R), \tag{5.3.8}$$

$H_b(\cdot)$ は式 (3.1.5) で与えた 2 元エントロピー関数，$0 < \frac{k_0}{n_0} = r_0 < 1$ である．

□

（証明） 略 [Jus72][Hir96]. □

演習問題

[問 5.1] $GF(2^6)$ の原始元を α とする．$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ を根にもつ $GF(2)$ 上の符号のパラメータを求めよ．ただし，原始多項式は $m_1(x) = x^6 + x + 1$ で与えられる．

[問 5.2] $GF(2)$ 上の原始多項式 $m_1(x) = x^3 + x + 1$ の根を α とする．

(1) $GF(2^3)$ のすべての元のべき表現とベクトル表現を示せ.

(2) 原始元 α を根としてもつ Hamming 符号のパリティ検査行列 H_1 を示せ.

(3) $G(x) = (x+1)m_1(x)$ を生成多項式とする巡回符号のパリティ検査行列 H_2 を示せ.

(4) $G(x)$ で生成される巡回符号のパラメータ n, k, d を示せ†.

(5) $G(x)$ で生成される巡回符号のバースト誤り検出能力を示せ. ただし, バースト長は 7 以下とする.

[**問 5.3**] $GF(2)$ 上の原始多項式 $m_1(x) = x^4 + x + 1$ の根を α とする.

(1) $GF(2^4)$ のすべての元のべき表現とベクトル表現を示せ.

(2) 原始元 α を根としてもつ Hamming 符号のパリティ検査行列 H_1 を示せ.

(3) α^3 を根としてもつ最小多項式 $m_3(x) = x^4 + x^3 + x^2 + x + 1$ により (n, k, d) BCH 符号を構成したとき, パラメータ n, k, d を求めよ.

(4) この BCH 符号のパリティ検査行列 H_2 を示せ.

† 情報点の 1 つを検査点とし, 全記号に対する偶数パリティをとる.

6
代数的復号法

復号法には最尤復号を実行する**確率的復号** (probabilitic decoding[For66]) **法**と，符号化の代数的構造を利用し，シンドロームを用いて代数的演算を実行する**代数的復号** (algebraic decoding) **法**がある．前者は指数的な演算回数，例えば $O(2^{nr})$ を必要とするが，後者は代数的な演算回数，例えば，2 元 BCH 符号は $O(n\log_2^2 n)$ で実現できる．ここで，n は符号長を示す．

6.1 復号手順

$GF(q)$ 上の (n,k,d) 符号の復号手順は次の通りである．

1. **シンドローム計算**：受信系列より**シンドローム多項式** (syndrome polynomial) $S(z)$ を計算する．
2. **基本方程式**：$S(z)$ より，**誤り位置多項式** (error locator polynomial) $\sigma(z)$，**誤り数値多項式** (error evaluator polynomial) $\eta(z)$ を与え，適当な多項式 $\phi(z)$ を用いて，次の**基本方程式** (key equation) を解く．

$$\sigma(z)S(z)+\phi(z)z^{2t}=\eta(z). \tag{6.1.1}$$

式 (6.1.1) から，$\sigma(z),\eta(z)$ を求める．ただし，$t=\lfloor\frac{d-1}{2}\rfloor$ である．

3. **誤り位置計算**：$\sigma(z)$ より，その根 α^i を求め，誤り位置を求める．
4. **誤り数値計算**：$\sigma(z)$ の形式的微分をほどこした多項式 $\sigma'(z)$ と $\eta(z)$ より，非零の誤り数値を求める．

5.1 で $t=2$ の場合を示したように，t が小さい場合は $\sigma(z)$ を比較的簡単な形で表わすことができる．しかし，t が大きくなると基本方程式を解くことが大変となる．復号アルゴリズムには，**Peterson アルゴリズム**，**Berlekamp-Massey**

アルゴリズム，Euclid アルゴリズム [SKHN75][KK80]，Welch-Berlekamp アルゴリズム，スペクトル技法を用いた復号法などがある．ここでは広範な符号の復号法を与える Euclid アルゴリズムについて述べる．Euclid アルゴリズムは，整数の最大公約数を求める Euclid 互除法を基本とし，これを多項式に適用し基本方程式を解くものである．

［Euclid **アルゴリズム**］

$GF(q)$ 上の符号語 $\boldsymbol{v} = (v_0, v_1, \cdots, v_{n-1})$ を $GF(q^m)$ 上の有理式表現することにより，**Goppa 符号**と同様に符号語 $\boldsymbol{v}$ が

$$\boldsymbol{v} \to \sum_{i=0}^{n-1} \frac{v_i}{z - \alpha_i} = 0 \quad \mod g(z), \tag{6.1.2}$$

を満足する広いクラスの符号の復号法を考える．ここで，$\alpha_i,\ i = 0, 1, \cdots, n-1,$ は $GF(q^m)$ の元から多項式 $g(z)$ の根を除いた部分集合の元，$g(z)$ は $GF(q^m)$ 上の多項式である．なお，$g(z) = z^{2t}$ とすれば $\{\boldsymbol{v}\}$ は最小距離 $2t+1$ の BCH 符号である．

ここでは，$GF(q)$ 上の $(n, k, 2t+1)$ BCH 符号を考える．**送信符号語多項式**を $v(x)$，**受信系列多項式**を $w(x)$，**誤り系列多項式**を $e(x)$ とする．ここで

$$v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1}, \tag{6.1.3.a}$$

$$w(x) = w_0 + w_1 x + w_2 x^2 + \cdots + w_{n-1} x^{n-1}, \tag{6.1.3.b}$$

$$e(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{n-1} x^{n-1}, \tag{6.1.3.c}$$

$$v_i, w_i, e_i \in GF(q),\ i = 0, 1, 2, \cdots, n-1,$$

と表わす．明らかに

$$w(x) = v(x) + e(x), \tag{6.1.4}$$

である．ここで，$e_i \neq 0$ となる誤り位置 i の集合を $\mathcal{E}$ で表わす．簡単のためパリティ検査行列 H は，定理 5.2.3 で $d_0 = 1$，すなわち式 (5.2.9) で与えられるものとする．

1. **シンドローム多項式**

シンドローム $S_1, S_2, \cdots, S_{2t}$ は

$$\begin{aligned} S_j &= w(\alpha^j) \\ &= e(\alpha^j), \quad j = 1, 2, \cdots, 2t, \end{aligned} \tag{6.1.5}$$

で与えられる．いま，t 個以下の誤り位置を

$$\{i_1, i_2, \cdots, i_s\} = \mathcal{E}, \quad s \leq t, \tag{6.1.6}$$

とする．

$$\begin{aligned} S_j &= e_{i_1}(\alpha^j)^{i_1} + e_{i_2}(\alpha^j)^{i_2} + \cdots + e_{i_s}(\alpha^j)^{i_s} \\ &= \sum_{i \in \mathcal{E}} e_i(\alpha^j)^i, \end{aligned} \tag{6.1.7}$$

であるから

$$S(z) = S_1 + S_2 z + \cdots + S_{2t} z^{2t-1}, \tag{6.1.8}$$

とおくと

$$S(z) = \sum_{i \in \mathcal{E}} \frac{e_i \alpha^i}{1 - \alpha^i z} \mod z^{2t}, \tag{6.1.9}$$

である．なぜならば

$$\begin{aligned} S(z) &= \sum_{j=1}^{2t} S_j z^{j-1} \\ &= \sum_{j=1}^{2t} \sum_{i \in \mathcal{E}} e_i (\alpha^j)^i z^{j-1} \\ &= \sum_{i \in \mathcal{E}} e_i \sum_{j=1}^{2t} (\alpha^i)^j z^{j-1} \pmod{z^{2t}}, \end{aligned} \tag{6.1.10}$$

と表すことができるからである．ここで

$$\frac{\alpha^i}{1 - \alpha^i z} = \sum_{j=1}^{\infty} (\alpha^i)^j z^{j-1}, \tag{6.1.11}$$

を用いた．

2. **基本方程式**

式 (6.1.9) の両辺に

$$\sigma(z) = \prod_{i \in \mathcal{E}} (1 - \alpha^i z), \tag{6.1.12}$$

を乗ずると

$$\sigma(z) S(z) = \eta(z) \mod z^{2t}, \tag{6.1.13}$$

を得る†．ここで

$$\eta(z) = \sum_{i \in \mathcal{E}} e_i \alpha^i \prod_{\ell \neq i} (1 - \alpha^\ell z), \tag{6.1.14}$$

である．式 (6.1.13) は関数 $\phi(z)$ を用いて，式 (6.1.1) となる．ここで，式 (6.1.12)，式 (6.1.13) より，明らかに

$$t \geq \deg \sigma(z) > \deg \eta(z) \tag{6.1.15}$$

である．Euclid 互除法は式 (6.1.15) を用いて，$g(z) = z^{2t}$ と $S(z)$ との最大公約多項式を求めるとき，剰余多項式はその次数が初めて $t-1$ 以下になったとき停止すれば，式 (6.1.1) の $\sigma(z)$ の解を与える．

一般に 2 つの整数 $M > N$ に対し，Euclid 互除法は，

$$\begin{aligned} M &= Q_1 N + r_1, \quad N > r_1, \\ N &= Q_2 r_1 + r_2, \quad r_1 > r_2, \\ r_1 &= Q_3 r_2 + r_3, \quad r_2 > r_3, \\ &\vdots \\ r_{n-1} &= Q_{n+1} r_n + 0, \end{aligned} \tag{6.1.16}$$

とするとき

$$\mathrm{GCD}(M, N) = r_n, \tag{6.1.17}$$

である．

［**例 6.1.1** ］整数 $33019, 10947$ の最大公約数を Euclid 互除法により求める．

$$\begin{aligned} 33019 &= 3 \times 10947 + 178, \\ 10947 &= 61 \times 178 + 89, \\ 178 &= 2 \times 89 + 0, \end{aligned}$$

より

$$\mathrm{GCD}(33019, 10947) = 89.$$

□

† 誤り訂正は，結局式 (6.1.13) の $\sigma(z), \eta(z)$ を求める問題であるから，これを**基本方程式**とよぶ場合がある．

［**定理 6.1.1** ］$r_{-1}(z) = z^{2t}$, $r_0(z) = S(z)$ とおく．GCD$[r_{-1}(z), r_0(z)]$ を求める多項式の Euclid 互除法

$$r_{i-2}(z) = q_i(z) r_{i-1}(z) + r_i(z),$$

$$\deg r_{i-2}(z) = \deg q_i(z) + \deg r_{i-1}(z), \tag{6.1.18}$$

$$\deg r_{i-1}(z) > \deg r_i(z), \quad i = 1, 2, \cdots,$$

を実行する．$\deg r_i(z) \leq t-1$ のとき，これを停止する．このとき

$$\sigma(z) = \gamma a_h(z), \tag{6.1.19.a}$$

$$\eta(z) = (-1)^h \gamma r_h(z), \tag{6.1.19.b}$$

で与えられる．ただし，γ は $\sigma(0) = 1$ とするための係数であり，$a_h(z)$ は

$$a_j(z) = q_j(z) a_{j-1}(z) + a_{j-2}(z), \tag{6.1.20}$$

$$j = 1, 2, \cdots, h,$$

で与えられる．ここで，$a_{-1}(z) = 0$, $a_0(z) = 1$ である． □

3. **誤り位置計算**

   式 (6.1.19.a) で得られた $\sigma(z)$ により，$\sigma(\alpha^i) = 0$ となる $\alpha^i \in GF(q^m)$ を求め，誤り位置 $i \in \mathcal{E}$ を求める†.

   2 元 BCH 符号の場合，$e_i \in \{0, 1\}$ であるから，これで復号は完了する．

4. **誤り数値計算**

   非 2 元 BCH 符号のとき，誤り e_i の値を求める必要がある．これは，$i \in \mathcal{E}$ に対し

$$e_i = -\frac{\eta(\alpha^i)}{\sigma'(\alpha^i)}, \tag{6.1.21}$$

   で与えられる [Forney アルゴリズム].

［**定理 6.1.2** ］Euclid 復号法による復号アルゴリズムの計算労力は $O(t^2)$ で与えられる． □

（証明） 略 [KK80]. □

† $\sigma(z)$ に $z = \alpha^i$, $i = 0, 1, \cdots, n-1$, を順次代入し，$\sigma(\alpha^i) = 0$ となる i を求める．これを，Chien 探索という．

［**例 6.1.2** ］2 元 $(15, 5, 7)$ BCH 符号を考える．$GF(2^4)$ の原始元 α を $GF(2)$ 上の $z^4 + z + 1$ の根とする．非ゼロの元は表 6.1.1 のように与えられる．ここで，$\alpha^{15} = 1$ である．簡単のため符号語 $\boldsymbol{v} = 00\cdots0$, 受信系列 $\boldsymbol{w} = 010010100000000$ とする．したがって，$\boldsymbol{e} = \boldsymbol{w}$ である．

表 6.1.1: $GF(2^4)$ の非ゼロ元

	α^3	α^2	α	1
α^0	0	0	0	1
α^1	0	0	1	0
α^2	0	1	0	0
α^3	1	0	0	0
α^4	0	0	1	1
α^5	0	1	1	0
α^6	1	1	0	0
α^7	1	0	1	1
α^8	0	1	0	1
α^9	1	0	1	0
α^{10}	0	1	1	1
α^{11}	1	1	1	0
α^{12}	1	1	1	1
α^{13}	1	1	0	1
α^{14}	1	0	0	1

さて，シンドロームは

$$\begin{aligned} S_1 &= \alpha + \alpha^4 + \alpha^6 = \alpha^{13}, \\ S_2 &= S_1^2 = \alpha^{26} = \alpha^{11}, \\ S_3 &= \alpha^3 + \alpha^{12} + \alpha^{18} = \alpha^{12}, \\ S_4 &= S_2^2 = \alpha^{22} = \alpha^7, \\ S_5 &= \alpha^5 + \alpha^{20} + \alpha^{30} = 1, \\ S_6 &= S_3^2 = \alpha^{24} = \alpha^9. \end{aligned} \tag{6.1.22}$$

したがって

$$S(z) = \alpha^{13} + \alpha^{11} z + \alpha^{12} z^2 + \alpha^7 z^3 + z^4 + \alpha^9 z^5, \tag{6.1.23}$$

である．次に，$g(z) = z^6$ と $S(z)$ の最大公約数を求めるため Euclid 互除法を適用する．

$$\begin{aligned} z^6 &= (\alpha^6 z + \alpha^{12})S(z) + r_1(z), \\ S(z) &= \alpha^8 z r_1(z) + r_2(z), \\ r_1(z) &= (\alpha^{13} z + \alpha^{13}) r_2(z) + r_3(z). \end{aligned} \tag{6.1.24}$$

ここで

$$\begin{aligned} r_1(z) &= \alpha z^4 + \alpha^7 z^3 + \alpha^{11} z^2 + \alpha^5 z + \alpha^{10}, \\ r_2(z) &= \alpha^3 z^3 + \alpha z^2 + \alpha^5 z + \alpha^{13}, \\ r_3(z) &= \alpha^{12} z^2 + \alpha^{14}, \\ \deg r_3(z) &= 2 \leq t - 1, \end{aligned} \tag{6.1.25}$$

であるから，ここで停止する．一方

$$\begin{aligned} a_{-1}(z) &= 0, \\ a_0(z) &= 1, \end{aligned}$$

とおき

$$\begin{aligned} a_1(z) &= (\alpha^6 z + \alpha^{12}) + 0, \\ a_2(z) &= \alpha^8 z a_1(z) + 1 \\ &= \alpha^{14} z^2 + \alpha^5 z + 1, \\ a_3(z) &= (\alpha^{13} z + \alpha^{13}) a_2(z) + a_1(z) \\ &= \alpha^{12} z^3 + \alpha^{10} z^2 + \alpha^{14} z + \alpha, \end{aligned} \tag{6.1.26}$$

より

$$\sigma(z) = \alpha^{11} z^3 + \alpha^9 z^2 + \alpha^{13} z + 1, \tag{6.1.27}$$

を得る．$\sigma(z) = 0$ を解いて，$z = \alpha^9, \alpha^{11}, \alpha^{14}$ を得る．$\alpha^i - z = \alpha^i(1 - \alpha^{-i} z)$ より，それぞれ $\alpha^{-6}, \alpha^{-4}, \alpha^{-1}$ を用いて誤り位置 $\mathcal{E} = \{1, 4, 6\}$ となる．これは $\boldsymbol{e} = \boldsymbol{w}$ を示す． □

6.2 スペクトル技法を用いた符号化復号化

Fourier 変換による符号化復号化の表現 [Bla83] につき簡単に述べる．長さ n のベクトル $\boldsymbol{v}$ を考える．

$$\boldsymbol{v} = (v_0, v_1, \cdots, v_{n-1}), \quad v_i \in GF(q), \tag{6.2.1}$$

この離散 Fourier 変換 $\boldsymbol{f}$ を

$$\boldsymbol{f} = (f_0, f_1, \cdots, f_{n-1}), \quad f_j \in GF(q^m), \tag{6.2.2}$$

とするとき

$$f_j = \sum_{i=0}^{n-1} v_i \alpha^{ij}, \quad j = 0, 1, 2, \cdots, n-1, \tag{6.2.3}$$

で定義される．ここで，α は 1 の原始 n 乗根である．このとき，逆 Fourier 変換が存在し

$$v_i = \frac{1}{n} \sum_{i=0}^{n-1} f_j \alpha^{-ij}, \quad i = 0, 1, 2, \cdots, n-1, \tag{6.2.4}$$

である．

v_i も f_j も同一の体 $GF(q)$ から選んだものが RS 符号である．符号語は $2t$ 個の特定のスペクトル $f_i^* = 0$ とする条件の下に，逆 Fourier 変換して得られたベクトル $\boldsymbol{v}$ の集合として定義される．同様に，復号化は誤り訂正能力以下の誤りベクトルのスペクトルが受信系列を Fourier 変換して得られる．これが $2t$ 個のシンドロームであり，$f_i^* = 0$ と定めた条件より誤りベクトルを求めることができる．

演習問題

[問 6.1] Euclid アルゴリズムの C 言語によるソースプログラムを作れ．ただし，$q = 2$, $n \leq 64$, とする．

[問 6.2] 2 元 $(15, 5, 7)$ BCH 符号を考える．

(1) 生成多項式 $G(x)$ の例を示せ．

(2) 情報系列多項式 $u(x) = 1 + x^2 + x^4$ のとき，符号語多項式 $v(x)$ を求めよ．

(3) 誤り系列多項式 $e_1(x) = 1 + x^6 + x^7$, $e_2(x) = 1 + x^7 + x^9 + x^{12}$ のとき，それぞれ誤り訂正を行え．

7
誤り訂正符号，誤り検出符号の応用例

誤り訂正符号，誤り検出符号は LSI の発達と共に広く用いられる様になった．特に

1. データ伝送機器，宇宙・衛星通信システム，移動通信システム，
2. 計算機の主記憶装置，補助記憶装置，
3. ディジタルオーディオ・ビデオ機器，

などに多くの適用例がある．

7.1 通信システム用符号

コンピューネットワークアーキテクチャの下層レイヤであるデータリンクレベルにおける HDLC 手順には生成多項式

$$G(x) = x^{16} + x^{12} + x^5 + 1, \tag{7.1.1}$$

の **CRC**(cyclic redundancy check) **符号**が誤り検出符号として用いられている．この符号は $b \leq 16$ の単一集中バースト誤り，2 ビットおよび奇数ビット誤りをすべて検出する．

自動車無線などの移動通信システムにはバースト誤り訂正符号として $(43, 31)$ BCH 符号が，PCM 音声放送用衛星通信システムにはランダム誤り訂正符号として $(63, 56)$ BCH 符号が，また文字放送システムには $(272, 190)$ 短縮差集合巡回符号が用いられている．いずれも誤り訂正装置を簡単化する必要がある．

本文では述べなかったが，たたみ込み符号を用いたものも実用化されている．宇宙通信システムでは内部符号をたたみ込み符号とし，$(255, 233)$ RS 外部符号による連接符号が用いられている．

7.2 計算機記憶装置用符号

2 元 $(2^m, 2^m - m - 1, 4)$ 拡大 Hamming 符号は，（半導体）主記憶装置に**単一誤り訂正二重誤り検出** (single error correcting/double error detecting : SEC/DED) **符号**として大型計算機に広く用いられている．通常，主記憶装置は 1 語長 k を 8 ビット（= 1 バイト）の整数倍で構成することが多いから，拡大 Hamming 符号を短縮して用いる．すなわち，情報記号部の先頭 s ビットを 0 とみなし，(n, k, d) 符号から $(n - s, k - s, d)$ 符号を得る．通常

(22,16,4) 符号,
(39,32,4) 符号,
(72,64,4) 符号,

などが用いられる．次に，(22,16,4) 符号を例にとって符号化復号化過程を示そう．このための符号器・復号器は専用 LSI として既に市販されている†．このような LSI では記憶装置アクセスメモリの高速性が要求されるため，高速組合せ論理回路を用いており，また大きい符号長の符号器・復号器を作るのに，

† たとえば，AMD 社製 Am2960 などである．

LSI を縦続接続することにより容易に実現できる．この LSI の生成行列 G は

$$G = [I_{16}, P], \tag{7.2.1}$$

$$P = \begin{bmatrix} 011100 \\ 110100 \\ 110010 \\ 100010 \\ 011010 \\ 100110 \\ 010110 \\ 001110 \\ 110001 \\ 101001 \\ 011001 \\ 100101 \\ 010101 \\ 001101 \\ 100011 \\ 001011 \end{bmatrix}, \tag{7.2.2}$$

で与えられる [AMD79]．この符号のパリティ検査行列 H は式 (2.1.5) より容易に求められる．例 2.1.4，例 2.2.1 で示したようにシンドロームは誤り訂正に関する情報を持つから，表 7.2.1 のように誤り訂正表としてあらかじめ計算しておくことが可能である．

主記憶装置には，Hamming 符号のようにランダム誤り訂正符号が用いられる．一方，補助記憶装置では記憶媒体の性格上，磁性面の傷などが連続した誤りを生じさせることが多く，通常バースト誤り訂正符号が用いられる．

表 7.2.1: シンドロームによる誤り訂正手順 [AMD79]

			s_6	0	1	0	1	0	1	0	1
			s_5	0	0	1	1	0	0	1	1
s_1	s_2	s_3	s_4	0	0	0	0	1	1	1	1
0	0	0		$*$	22	21	T	20	T	T	M
0	0	1		19	T	T	16	T	14	9	T
0	1	0		18	T	T	M	T	13	7	T
0	1	1		T	11	5	T	1	T	T	M
1	0	0		17	T	T	15	T	12	6	T
1	0	1		T	10	4	T	M	T	T	M
1	1	0		T	8	3	T	2	T	T	M
1	1	1		M	T	T	M	T	M	M	T

$*$ − no errors detected.

Number − the location of the single bit-in-error.

T − two errors detected.

M − three or more errors detected.

$\boldsymbol{s} = (s_1, s_2, \cdots, s_6)$.

磁気ディスク装置では

$$n \leq 585442,$$

$$n - k = 56,$$

$$\begin{aligned} G(x) = (x^{22}+1)&(x^{11}+x^7+x^6+x+1) \\ &\cdot(x^{11}+x^9+x^7+x^6+x^5+x+1) \\ &\cdot(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6 \\ &\quad +x^5+x^4+x^3+x^2+x+1), \end{aligned} \tag{7.2.3}$$

などのバースト誤り訂正符号が用いられている．この符号は $b \leq 11$ [bits] の単一集中バースト誤りを訂正できる†．磁気テープ記憶装置では，トラック走行方向に $GF(2^8)$ 上の $(8, 7, 2)$ Reed-Solomon 符号を用い，さらにトラック垂直方向に $(9, 8, 2)$ 符号を用いている．

† この符号器・復号器として AMD 社製 AmZ8065 専用 LSI がある．

図 7.3.1: 誤り訂正アルゴリズム用 LSI の例（三菱電機（株）提供）

7.3 ディジタルオーディオ，ビデオ機器用符号

CD(compact disk) などオーディオ用光ディスク装置にはランダム誤りとバースト誤りが混在し 2 重化 RS 符号が用いられ，10^{-7} 以下の誤り確率を達成している．また，DAT(digital audio tape) には RS 積符号が用いられている．ビデオ用 VTR(video tape recoder) にも RS 積符号が用いられ，2.46 ～ 227 [Mbits/sec] という高速伝送速度で，10^{-7} 程度の誤り確率を達成している．

図 7.3.1 に，6 で述べた Euclid アルゴリズムを実行する LSI の例を示す．光ディスク装置，DVD(digital versatile disk)，ディジタル TV 用などのための RS 符号誤り訂正（消失も含む）を 160Mbps の高速で実行する．符号長 $n \leq 255$ バイト，パリティ検査記号数 $n-k \leq 16$ バイトの符号に対応する．シンドローム計算，Euclid アルゴリズム計算，Chien 探索の 3 パイプライン方式により高速処理を可能としている．図 7.3.1 の写真のように，外形 100 ピンのパッケージに収められている．

略解・ヒント

第 1 章の略解・ヒント

[解 1.1] まず，$D_H(\boldsymbol{v}_m, \boldsymbol{v}_{m'})$ と $d_H(v_{mi}, v_{m'i})$ の大小関係が対応していることを述べる．$d_H(\cdot,\cdot)$ の非負性，対称性は明らか．三角不等式は $v_{mi} = v_{m'i}$ と $v_{mi} \neq v_{m'i}$ に分けて示す†．

[解 1.2] 誤り検出可能なことは受信系列が符号語にならないこと，誤り訂正可能なことは t 個以下の誤りを訂正して受信系列から唯一つの符号語が得られることを示す．

[解 1.3] 解 1.2 と同様，復号方法を示す．

第 2 章の略解・ヒント

[解 2.1] $W_H(\boldsymbol{e}) = \ell$ のとき，$W_H(\boldsymbol{c}_i) = \ell$, $^{\exists}\hat{m}$, $\boldsymbol{w} \to \boldsymbol{v}_{\hat{m}}$ となり正しく復号される．

[解 2.2] $\boldsymbol{e} = \boldsymbol{c}_i$, $\boldsymbol{v}_{\hat{m}} = \boldsymbol{w} + \boldsymbol{c}_i$ とすれば最小距離復号を実行している．

[解 2.3] 最大事後確率復号法が平均復号誤り確率を最小にする．Bayes 規則を用いて符号語の生起確率が等しいとき最尤復号法が事後確率を最大にしていることを示す．

[解 2.4] $\boldsymbol{w}_1 H^{\mathrm{T}} = \boldsymbol{w}_2 H^{\mathrm{T}}$ のとき $\boldsymbol{w}_1 + \boldsymbol{w}_2 = \boldsymbol{v}_m \in \mathcal{C}$ から，$^{\exists}\boldsymbol{v}_{m'} \in \mathcal{C}$, $\boldsymbol{w}_1 = \boldsymbol{c}_i + \boldsymbol{v}_{m'}$, $\boldsymbol{w}_2 = \boldsymbol{v}_m + \boldsymbol{w}_1$ より $\boldsymbol{w}_2 = \boldsymbol{c}_i + \boldsymbol{v}_{m'} + \boldsymbol{v}_m$，したがって $\boldsymbol{w}_2$ のコセットリーダも $\boldsymbol{c}_i$ となる．

[解 2.5] $2^{m-r-1} - 1$ 個以下の誤りを訂正し，2^{m-r-1} 個の誤りを検出できることを用いる．そのために，r 段の多数決論理復号法を適用する．

[解 2.6] $n_0 = n_1 n_2$, $k_0 = k_1 k_2$, であることは明らか．k_0 の情報記号のうち第 i 行第 j 列，$i \leq k_1$, $j \leq k_2$, が非ゼロとすると，第 i 行には少なくとも d_1 個の非ゼロの要素があり，そのそれぞれに d_2 個の非ゼロの要素がある．よって，$d_0 = d_1 d_2$.

[解 2.7] GH^{T} の第 (i,j) 成分を直接計算する．

---

† $v_{mi}, v_{m'i}, v_{m''i}$ の等式関係を 6 つ (または 8 つ) の場合に分けて示してもよい．

[解 2.8] $v(x) \in \mathcal{C}$ と $v'(x) = x^n v(1/x)$ をそれぞれ $G(x), H'(x)$ が割り切る.

[解 2.9] $H(x) = 1 + x^2 + x^3$ のとき 101110, および $H(x) = 1 + x + x^3$ のとき 1110100.

[解 2.10] $\ell + 1$ 個以上の誤りが生じたとき復号誤りとなる.

第 3 章の略解・ヒント

[解 3.1] $n!$ に対する Stirling の公式を用いる.

[解 3.2] q 元線形 (n, k) 符号の重みの総和 $W \leq nq^{k-1}(q-1)$ を導く.

[解 3.3] k 個の情報記号のうち $k-1$ 個がゼロ, 残り 1 個が非ゼロの符号語を考える.

第 4 章の略解・ヒント

[解 4.1] Euclid の互除法を用いて r と s の最大公約数 $g = ar + bs \in \mathfrak{I}$ から $g = r$ を導く.

[解 4.2] 4 を法とする演算では $2 \cdot 2 = 0$ となり, 体をなさない. 例えば, $P(x) = 1+x+x^2$ の剰余類 $\{x\} = \alpha$ とするとき, $\{0, 1, a, b\} = \{0, 1, \alpha, \alpha^2\}$ は体をなす.

[解 4.3] $r = ab$ (合成数) と仮定し矛盾することを導く.

[解 4.4] $a(x)$ を与えこれを 2 乗する. $GF(2)$ では $1^2 = 1,\ 0^2 = 0,\ 1 + 1 = 0$ となることを用いる.

[解 4.5] 原始元は $2, 3$ である.

[解 4.6] α の他 $\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ は原始元である.

[解 4.7] $x^c - 1 | x^{jc} - 1$ であるから, $n = jc + i,\ i < c$ と仮定し Euclid の互除法を適

用する．$x^i-1|x^{jc}-1$ となり仮定に矛盾する．よって $i=0$.

第 5 章の略解・ヒント

[解 5.1] $G(x)=(x^6+x^4+x^2+x+1)(x^3+x^2+1)$，2 元 $(21,12,5)$ 符号が得られる．

[解 5.2] (1) 表 4.2.2 参照．(2) $H_1=[1\ \alpha\ \alpha^2\ \cdots\ \alpha^6]$. (3) $H_2=\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \alpha & \alpha^2 & \cdots & \alpha^6\end{bmatrix}$. (4) $(7,3,4)$ 符号．(5) バースト長を b，見逃し誤り率を P_d とする．$b\le 4$ のとき $P_d=0$，$b=5$ のとき $P_d=2^{-3}$，$b>5$ のとき $P_d=2^{-4}$.

[解 5.3] (1) 表 6.1.1 参照．(2) $H_1=[1\ \alpha\ \alpha^2\ \cdots\ \alpha^{14}]$. (3) $(15,7,5)$ 符号．(4) $H_2=\begin{bmatrix}1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14}\\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12}\end{bmatrix}$.

第 6 章の略解・ヒント

[解 6.1] 略.

[解 6.2] (1) $G(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$. (2) $v(x)=x^{14}+x^9+x^7+x^4+x^3+x+1$. (3) $e_1(x)$ のとき，シンドローム S_j, $j=1,2,\cdots,6$, は

$$S_j=w(\alpha^j)=e(\alpha^j),\quad j=1,2,\cdots,6, \tag{a.3.2.1}$$

である．したがってシンドローム多項式 $S(z)$ は

$$\begin{aligned}S(z)&=S_1+S_2z+S_3z^2+\cdots+S_6z^5\\&=\alpha^5+\alpha^{10}z+\alpha^8z^2+\alpha^5z^3+\alpha^5z^4+\alpha z^5,\end{aligned} \tag{a.3.2.2}$$

となる．$r_{-1}(z)=z^{2t}$, $r_0(z)=S(z)$ とし，Euclid 復号法を行うと

$$r_{i-2}(z)=q_i(z)r_{i-1}(z)+r_i(z), \tag{a.3.2.3}$$

より

$$q_1(z) = \alpha^3 + \alpha^{14}z,$$
$$r_1(z) = \alpha^8 + \alpha^{11}z + \alpha^2 z^2 + \alpha^{11}z^3 + \alpha^5 z^4,$$
$$q_2(z) = \alpha^8 + \alpha^{11}z,$$
$$r_2(z) = \alpha^2 + \alpha^{10}z + \alpha^{14}z^2 + \alpha^3 z^3$$
$$q_3(z) = \alpha^3 + \alpha^2 z,$$
$$r_3(z) = \alpha^4 + \alpha^{12}z^2,$$
$$\deg(r_3(z)) \leq t - 1, \tag{a.3.2.4}$$

となる．また $a_{-1}(z) = 0,\ a_0(z) = 1$ とし

$$a_i(z) = q_i(z)a_{i-1}(z) + a_{i-2}(z), \tag{a.3.2.5}$$

より

$$a_1(z) = \alpha^3 + \alpha^{14}z,$$
$$a_2(z) = \alpha^{12} + \alpha z + \alpha^{10}z^2,$$
$$a_3(z) = \alpha^{14} + \alpha^4 z + \alpha^8 z^2 + \alpha^{12}z^3, \tag{a.3.2.6}$$

である．したがって誤り位置多項式 $\sigma(z)$ は

$$\sigma(z) = \frac{1}{\alpha^{14}}a_3(z) = 1 + \alpha^5 z + \alpha^9 z^2 + \alpha^{13}z^3, \tag{a.3.2.7}$$

となり，これを Chien 探索することにより $\sigma(1) = \sigma(\alpha^8) = \sigma(\alpha^9) = 0$ が得られる．したがって $\mathcal{E} = \{0, 6, 7\}$ となり，$e_1(x)$ を得ることができる．

$e_2(x)$ のときは訂正能力以上の誤りが生じているため $\mathcal{E} = \{2, 8, 11\}$ となり，正しく訂正できない．

参 考 文 献

[AMD79] “Am 2960 Fast error detection and correcting for memories,” *The Am 2960 family data book*, pp.2/312-2/327, AMD Inc., CA. 1979.

[AMD80] “Am 2960 Boots memory reliability,” *AMD Tech.Rep.*, Jan 1980.

[Ari61] 有本卓, “*p* 元群符号系の符号化，復号化法と誤りの訂正機構, ” 情報処理, Vol.2, No.6, pp.320-325, Nov. 1961.

[Ber68] E.R.Berlekamp, *Algebraic coding theory*, NY: McGraw-Hill Book Co., 1968.

[Ber80] E.R.Berlekamp, “The technology of error-correcting codes,” *Proc. IEEE*, Vol.68, pp.564-593, May 1980.

[Bha83] V.K.Bhargava, “Forward error correction schemes for digital communications,” *IEEE Comm. Magazine*, pp.11-19, Jan 1983.

[Bla83] R.E.Blahut, *Theory and practice of error control coding*, MA: Addison-Wesley Publishing Co., 1983.

[EK96] 江藤良純, 金子敏信監修, 誤り訂正符号とその応用, オーム社, 1996.

[For66] G.D.Forney,Jr., *Concatenated codes*, MA: The M.I.T.Press, 1966.

[Gol49] M.J.E.Golay, “Note on digital coding,” *Proc.IRE*, Vol.37, p.657, June 1949.

[Ham50] R.W.Hamming, “Error detecting and error correcting codes,” *Bell syst. Tech.J.*, Vol.29, pp.147-160, Apr. 1950.

[Hil86] R.Hill, *A first course in coding theory*, Oxford: Clarendon Press, 1986.

[Hir96] 平澤茂一, 情報理論，培風館, 1996.

[Hir00] 平澤茂一, 情報理論入門，培風館, 2000.

[HN99] 平澤茂一, 西島利尚，符号理論入門，培風館, 1999.

[Ima90] 今井秀樹, 符号理論, コロナ社, 1990.

[Jus72] J.Justesen, “A class of constractive asymptotically good algebraic codes,” *IEEE Trans. Inform. Theory*, vol.IT-18, pp.652-656, Sept. 1972.

[KK80] 笠原正雄, 嵩忠雄, 今井秀樹, 阪田省二郎, 平澤茂一, 杉山康夫, 後藤宗弘, 有本卓, “特集 符号理論,” 数理科学, No.210. 1980.

[KTII75] 嵩忠雄, 都倉信樹, 岩垂好裕, 稲垣康雄, 符号理論, コロナ社, 1975.

[LC83] S.Lin and D.J.Costello,Jr., *Error control coding*, Englewood Cliffs, New Jersey: Prentice-Hall Inc., 1983.

[Lin70] S.Lin, *An introduction to error-correcting codes*, Englewood Cliffs, New Jersey: Prentice-Hall Inc., 1970.

[MHI82] 宮川洋, 原島博, 今井秀樹, 情報と符号の理論, 岩波講座情報科学 4, 岩波書店, 1982.

[MII73] 宮川洋, 岩垂好裕, 今井秀樹, 符号理論, 昭晃堂, 1973.

[MS77] F.J.MacWilliams and N.J.A.Sloane, *The theory of error-correcting codes*, Amsterdam: North-Holland Publishing Co., 1977.

[Mul54] D.E.Muller, “Application of Boolean algebra to switching circuit design and error detection,” *IRE Trans. Electron. Comput.*, vol.EC-3, pp.6-12, Sept. 1954.

[Pet61] W.W.Peterson, *Error correcting codes*, 1st Ed. MA: The M.I.T.Press, 1961.

[PW72] W.W.Peterson and E.J.Weldon,Jr., *Error correcting codes*, 2nd Ed. MA: The M.I.T.Press, 1972.

[Ree54] I.S.Reed, “A class of multiple-error-correcting codes and the decoding scheme,” *IRE Trans*, *PGIT-4*, pp.38-49, 1954.

[RS60] I.S.Reed and G.Solomon, “Polynomial codes over certain finite fields,” *J. Soc. Ind. Appl. Math.*, vol.8, pp.300-304, June 1960.

[Sha48] C.E.Shannon, “A mathematical theory of communication,” *Bell syst. Tech.J.*, Vol.27, pp.379-423, July 1948.

[SKHN75] Y.Sugiyama, M.Kasahara, S.Hirasawa and T.Namekawa, “A

method for solving key equations for decoding Goppa codes," *Infom. Contr.* vol.27, pp.87-99, Jan. 1975.

[Slo75] N.J.A.Sloane, *A short course on error correcting codes*, 3rd Printing, CISM Courses and Lectures No.188, Udline, Italy, 1975.

主な記号表

記号	意味
$\mathcal{A} \cup \mathcal{B}$	集合 $\mathcal{A}$ と $\mathcal{B}$ の和集合
$\mathcal{A} \cap \mathcal{B}$	集合 $\mathcal{A}$ と $\mathcal{B}$ の積集合
$\mathcal{A}^{\mathrm{C}}$	集合 $\mathcal{A}$ の補集合
$\mathcal{A} \setminus \mathcal{B}$	集合 $\mathcal{B}$ を除く集合 $\mathcal{A}$
$\mathcal{A} \supset \mathcal{B}$	集合 $\mathcal{A}$ は集合 $\mathcal{B}$ を含む
$^{\forall}a \in \mathcal{A}$	全称記号 (集合 $\mathcal{A}$ の任意の要素 a に対し)
$^{\exists}a \in \mathcal{A}$	存在記号 (集合 $\mathcal{A}$ の要素 a が存在する)
sup	上限 (l.u.b.,supremum)
inf	下限 (g.l.b.,infimum)
$\simeq$	漸近的に等しい
$\fallingdotseq$	近似的に等しい
$o(f(x))$	Landau の記号: $g(x) = o(f(x))$ とは $\lim_{x\to\infty} \dfrac{g(x)}{f(x)} = 0,$
$O(f(x))$	Landau の記号: $g(x) = O(f(x))$ とは $^{\exists}A(\neq 0),\ \lvert g(x)\rvert \le A\lvert f(x)\rvert,\ (x \to \infty)$
$n!$	階乗 $(= n(n-1)\cdots 2\cdot 1,$ ただし $0! = 1)$
$\binom{n}{r}$	組合せ $\left(= \frac{n!}{r!(n-r)!}\right)$
$\det[A]$	行列 A の行列式
A^{T}	行列 A の転置行列
$\boldsymbol{a}^{\mathrm{T}}$	ベクトル $\boldsymbol{a}$ の転置ベクトル
$\lvert a\rvert$	a の絶対値
$(\cdot,\cdot)$	開区間, $(a,b) = \{x; a < x < b\}$
$[\cdot,\cdot]$	閉区間, $[a,b] = \{x; a \le x \le b\}$
max	最大値
min	最小値
lim	極限
$\mathrm{mod}(\cdot)$	法
$\lfloor x \rfloor$	x より小さいか等しい (x を越えない) 最大の整数
$\lceil x \rceil$	x より大さいか等しい (x を越える) 最小の整数
ϕ	空集合 (empty set)
$P(E)$	事象 E の確率
$D_H(\cdot,\cdot)$	ベクトル間の Hamming 距離
$d_H(\cdot,\cdot)$	要素間の Hamming 距離
$W_H(\cdot)$	ベクトルの Hamming 重み
$w_H(\cdot)$	要素の Hamming 重み

主な記号表

記号	意味
$\mathrm{LCM}(\cdot,\cdot,\cdots,\cdot)$	最小公倍数
$\mathrm{GCD}(\cdot,\cdot,\cdots,\cdot)$	最大公約数
$\deg(\cdot)$	次数
$M \mid N (M \not\mid N)$	M は N を割り切る（割り切らない）

主な記号表

記号	意味
$\mathcal{G}$	群
$\mathcal{R}$	環
$\mathcal{I}$	イデアル
$\mathcal{F}$	体
$GF(\cdot)$	Galois 体
$\mathcal{N}$	自然数
$\mathcal{Z}$	整数
$\mathcal{R}$	実数
$\mathcal{C}$	複素数
$\mathcal{Q}$	有理数
$\mathcal{B} = \{0, 1\}$	2 元記号
$H_b(\cdot)$	2 元エントロピー関数 (対数の底は 2)

主な変数名表

記号	意味
n	符号長
k	情報記号数
d	最小距離
t	誤り訂正個数
r	符号化比率 $r = \frac{k}{n}$
$\delta(r)$	漸近的距離比，$\delta = \lim_{n\to\infty} \frac{d}{n}$，$r = \frac{k}{n}$
ε	2 元対称通信路の誤り確率
p	素数
q	素数のべき乗，$q = p^m$ （m は正整数）
$\alpha \in GF(p^m)$	$GF(p)$ 上の既約多項式の根，$q = p^m$
$\boldsymbol{u}$	情報記号系列（ベクトル）$\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$
$\boldsymbol{v}$	符号語，符号系列（ベクトル）$\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$
$\boldsymbol{w}$	受信系列（ベクトル）$\boldsymbol{w} = (w_1, w_2, \cdots, w_n)$
$\boldsymbol{e}$	誤り系列（ベクトル），誤りパターン $\boldsymbol{e} = (e_1, e_2, \cdots, e_n)$
$u(x)$	情報記号多項式 $u(x) = u_0 + u_1 x + \cdots + u_{k-1}x^{k-1}$
$v(x)$	符号語多項式 $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$
$w(x)$	受信系列多項式 $w(x) = w_0 + w_1 x + \cdots + w_{n-1}x^{n-1}$
$e(x)$	誤り系列多項式 $e(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$
G	生成行列
H	パリティ検査行列
$G(x)$	生成多項式
$H(x)$	パリティ検査多項式
$P(x)$	既約多項式
$F(x)$	原始多項式
$m(x)$	最小多項式
$m_i(x)$	α_i を根とする最小多項式，$\alpha_i \in GF(q)$
$\sigma(z)$	誤り位置多項式
$\eta(z)$	誤り数値多項式
$S(z)$	シンドローム多項式
x, z	不定元
$\mathcal{E}$	誤り位置の集合

（注）多くの変数名は従来の習慣に従った.

索　引

A
低密度パリティ検査符号

低密度パリティ検査 (Low density parity check:LDPC) **符号**は, 1963 年 R.G.Gallaer [Gal63] により提案された符号のクラスである．Gallager は情報理論の分野で知られ，特にランダム符号化による符号化定理を明快に証明している†．この考え方は，LDPC 符号のパリティ検査行列集合や Justesen 符号 [Jus72] の内部符号に見られる．LDPC 符号はパリティ検査行列で定義されるから，勿論線形符号である．LDPC 符号の提案は古いが，ランダム符号の考え方‡を巧みに用い，しかも当初から復号法に重点を置いている‡‡．その意味で，性能の良い符号より，むしろ復号が容易な符号と位置づけられる．

LDPC 符号は符号長 n が十分大きいときに良い性能を示す‡‡‡．n を大としなければならないことは，当然復号に要する計算量 $\chi(n)$ が大となる．本資料で議論した BCH 符号などは，第 6 章の復号アルゴリズムで $O(d^2)$，$O(n\log_2 n)$ 程度の計算量で良いが，符号性能 $d/n \to 0 (n \to \infty)$（定理 5.2.2 参照）となってしまう．そのような視点から見ると，LDPC 符号は $\chi(n) = O(n)$ 程度に押さえ，$n \to \infty$ で符号性能を劣化させず程々の $d/n \nrightarrow 0 (n \to \infty)$ を持つ．したがって，$P(\mathcal{E}) \to 0 (n \to \infty)$ を達成する．勿論，理想的なランダム符号化‡‡‡‡と最尤復号法による性能（ただし，符号の存在のみ）には及ばない．

以上の結果，LDPC 符号は Shannon limit の近傍の性能を実現することが出来る．同様な性質を持つ数少ない非ランダム符号として知られる**繰り返し符号** (iterated codes)・**連接符号** (concatenated codes) は明快に定義され符号の探索に n の代数的オーダの計算量で可能であるのに比べ，LDPC 符号は，はるかに計算量がかかる．しかし，ランダ

---

† Shannon によるランダム符号化は符号語をランダムに生成するのに対し，Gallager は符号（化）をランダムに生成している [Hir00].

‡ 代数的構成法よりランダム符号化に条件を付けた確率的構成法と見ることが出来る．

‡‡ 本資料では代数的構成法による良い性能を持った符号化に力点があり，復号法は符号化の結果として成り立つ条件を用いて実行される．勿論，LDPC 符号でも両者は対であり別々に考えることは出来ない．ただし，最尤復号法では符号化の構造を考慮しない．

‡‡‡ 符号化定理が示す通り，多くの符号は復号誤り確率 $P(\mathcal{E})$ が n と共に指数的に 0 に収束する．LDPC 符号の $P(\mathcal{E})$ の上界は，十分小さな誤り確率 $\mathcal{E}$ の 2 元対称通信路で，ある条件の下に $\sqrt{n}$ と共に指数的に 0 に収束することが示されている [Gal63].

‡‡‡‡ パリティ検査行列 H のハミング重み $W_H(H) = O(n^2)$ である．

ム符号化ほどではない.

なお，LDPC 符号は非 2 元符号も構成できるが，ここでは 2 元符号を仮定する．また，LDPC 符号には確率的な議論が必要であるが，本資料の性格上主として代数的な記述に止める．各章と同様，符号長 n，情報記号数 k，生成行列 G，パリティ検査行列 H など特に断わらない限り同一の記号を用いる．

A.1 符号化法

A.1.1 パリティ検査行列

LDPC 符号はその名の通り，パリティ検査行列 $H = [h_{ij}]$ の非 0 要素が少ない（ハミング重みが小さな，疎な）符号のクラスと定義される．

［**定義 A.1.1** ］(正則 LDPC 符号) m 行 n 列 $(m < n)$ のパリティ検査行列 $H_{\rm reg} = [h_{ij}]$ の行ベクトル表現，列ベクトル表現をそれぞれ式 (A.1.2),(A.1.3) とする．

$$H_{\rm reg} = \left[\ h_{ij}\ \right] \tag{A.1.1}$$

$$= \begin{bmatrix} \boldsymbol{h}_{r1} \\ \boldsymbol{h}_{r2} \\ \vdots \\ \boldsymbol{h}_{rm} \end{bmatrix} \tag{A.1.2}$$

$$= \left[\ \boldsymbol{h}_{c1}^{\rm T},\quad \boldsymbol{h}_{c2}^{\rm T},\quad \cdots\quad ,\boldsymbol{h}_{cn}^{\rm T}\ \right] \tag{A.1.3}$$

ここで

$$\begin{aligned} \forall i\quad &: W_H(\boldsymbol{h}_{ri}) = w_r\quad (i = 1, 2, \cdots, m), \\ \forall j\quad &: W_H(\boldsymbol{h}_{cj}) = w_c\quad (j = 1, 2, \cdots, n) \end{aligned} \tag{A.1.4}$$

ただし，$w_c \ll m (w_r \ll n)$ のとき，$H_{\rm reg}$ で定義される符号を (n, w_c, w_r) **正則 LDPC 符号**という． □

通常，$w_c = O(1)$ である．また，$W_H(H) = O(n)$ であり，極端に $w_c \ll m$ と選ぶと符号性能の劣化することが知られている．ただし，行列 A のハミング重みを $W_H(A)$ で表す．$w_c n = w_r m$ が成り立つから，(n, w_c, w_r) 正則 LDPC 符号の**符号化比率** r は次式で与えられる†.

$$r \geq 1 - \frac{w_c}{w_r} \tag{A.1.5}$$

† 不等号は $\mathrm{rank}(H) < m$ のため.

［**定義 A.1.2** ］**(Gallager 型正則 LDPC 符号)** 式 (A.1.1) の $H_{\rm reg}$ を w_c 個の部分行列 $H_{r1}, H_{r2}, \cdots, H_{rw_c}$ に分解する．

$$H_{r1} = \begin{bmatrix} 111\cdots1 & & 0 \\ 0 & 111\cdots1 & 0 \\ & \vdots & \\ 0 & & 111\cdots1 \end{bmatrix} \tag{A.1.6}$$

で与えられ，$H_{r2}, H_{r3}, \cdots, H_{rw_c}$ は H_{r1} の列置換で与えられるパリティ検査行列 $H_{\rm Gal}$ で定義される符号を (n, w_c, w_r)**Gallager 型正則 LDPC 符号**という． □

ここで，部分行列を決める列置換は互いに独立な乱数を用いるものと仮定する．

［**例 A.1.1** ］$n = 15$，$w_c = 3$，$w_r = 2$，$m = 10$，$r \geq 1 - (2/3) = 1/3$ の $(15, 3, 2)$ 正則 LDPC 符号

$$H_{\rm reg} = \left[\begin{array}{ccc:ccc:ccc:ccc:ccc} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1 \\ \hdashline 1&0&0&0&0&1&0&0&0&0&1&0&0&0&0 \\ 0&1&0&0&0&0&1&0&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&0&1&0&0&0&0&1&0&0 \\ 0&0&0&1&0&0&0&0&1&0&0&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0&1&0&0&0&0&1 \end{array}\right] \tag{A.1.7}$$

このパリティ検査行列は，H_{c1} の列置換を下記の規則的な置換行列によって H_{c2} を生成している．

$$\begin{bmatrix} 1&2&3&4&5&6&7&8&9&10&11&12&13&14&15 \\ 1&4&7&10&13&2&5&8&11&14&3&6&9&12&15 \end{bmatrix}$$

その結果，$H_{\rm reg}$ の列ベクトルは全て異なり 2 個の列ベクトルは線形独立である，定理 2.1.7 より最小距離 $d \geq 3$ である． □

［**例 A.1.2** ］**((15,3,2)Gallgaer 型正則 LDPC 符号)** [例 A.1.1] で，乱数による列置換を用いて Gallgaer 型正則 LDPC 符号の $H_{\rm Gal}$ を生成する．列置換の置換行列をランダムに選ぶ．その結果、例えば

$$\begin{bmatrix} 1&2&3&4&5&6&7&8&9&10&11&12&13&14&15 \\ 12&8&10&4&2&6&1&3&7&5&9&13&15&14&11 \end{bmatrix}$$

で与えるとき

$$H_{\mathrm{reg}} = \left[\begin{array}{ccc:ccc:ccc:ccc:ccc} 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&1&1&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\ \hdashline 0&0&0&0&1&0&1&1&0&0&0&0&0&0&0\\ 0&0&0&1&0&1&0&0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\ 1&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&1&1&1&0 \end{array}\right] \tag{A.1.8}$$

明らかに，$h_{c7} = h_{c8}, h_{c13} = h_{c14}$ であり，$d \geq 1$ である． □

Gallager は復号性能を向上させるため，内径の大きい 2 部グラフを乱数を用いて生成するよう工夫している [Gal63].

なお，式 (A.1.4) のいづれか一方が成り立たない（重みが一定ではない）とき，**非正則 LDPC 符号**という．非正則 LDPC 符号に良い性能を持った符号が存在することが知られている [Mac99].

一般に符号長 n が比較的小さい場合は，ランダムに生成されたパリティ検査行列から復号性能の良い符号を選び出す必要がある．n が大きい場合，ランダムに生成されたパリティ検査行列のほとんど全てが同一の性能を持つ．したがって，n が大きくなるに従い，良い符号の選別の必要性は減少する．

A.1.2 生成行列

パリティ検査行列で定義される LDPC 符号は復号の計算量の点で優れるが，符号化の計算量に問題がないわけではない．巡回符号・擬巡回符号に基づいて構成的に与えられる LDPC 符号は，本文中 2.5 に述べた生成多項式により容易に符号化出来る．しかし，一般にパリティ検査行列 H で与えられた符号を生成するためには，定理 2.1.3 などを用いて $GH^{\mathrm{T}} = 0$ となる生成行列 G を求める必要がある．これは，m 元 1 次連立方程式を解く（例えば，ガウスの消去法）ことになり $O(n^3)$ の計算量を要する．さらに，これにより求められた生成行列 G は一般に疎な行列ではなくなり，$W_H(G) = O(n^2)$ から符号語の生成に $O(n^2)$ の計算量がかかることになる†.

† 組織符号の場合，右上三角をゼロ（すなわち，下三角行列）としたような疎なパリティ検査行列を与え，簡単に符号化することが出来る（付録演習問題 [1] 参照）．この場合，生成行列を用いることなく情報記号から順次検査記号求めることが出来る．なお，与えられ LDPC 符号のパリティ検査行列をガウスの消去法で右上三角をゼロに変換しても，得られたパリティ検査行列は疎な行列とは限らないことに注意.

A.1.3 最小距離

A.2 復号法

A.2.1 最大事後確率復号法

(1) ブロック単位の最大事後確率復号法

（ブロック単位の）復号誤り確率 $P(\mathcal{E})$ を最小とする復号法は**最大事後確率** (maximum a posterior:MAP) **復号法**である．この復号法は，符号語を $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_M$，受信語を $\boldsymbol{w}$ とするとき，復号器は

$$\boldsymbol{w} \to \boldsymbol{v}_{\hat{m}} | [\max_{1 \le m \le M} P(\boldsymbol{v}_m|\boldsymbol{w}) = P(\boldsymbol{v}_{\hat{m}}|\boldsymbol{w})] \tag{A.2.1}$$

を実行する [Hir96]．式 (1.2.7) で示した**最尤復号法**は右辺後半の条件式の事後確率 $P(\boldsymbol{v}_m|\boldsymbol{w})$ が尤度 $P(\boldsymbol{w}|\boldsymbol{v}_m)$ となっていることが異なる．しかし，Bayes 規則により，符号語の生起確率 $P(\boldsymbol{v}_m)$ が m によらず一定，$P(\boldsymbol{v}_m) = 1/M, m = 1, 2, \cdots, M$ のとき，最大化操作は等価である．したがって，m によらず $P(\boldsymbol{v}_m) = 1/M$ のとき，最尤復号は $P(\mathcal{E})$ を最小にする．

(2) シンボル単位の最大事後確率復号法

符号長が比較的小さいブロック符号の場合，通常（ブロック単位の）復号誤り確率 $P(\mathcal{E})$ で評価する．しかし，ブロック符号とは構造の異なるトレリス符号や符号長の大きい LDPC 符号・ターボ符号の場合，（シンボル単位の）復号誤り確率 $P(e)$ で評価することが多い．シンボル単位の最大事後確率復号法はシンボル単位の復号誤り確率を最小にする．この復号法は，$\boldsymbol{v}_m = (v_{m1}, v_{m2}, \cdots, v_{mn}), \boldsymbol{w} = (w_1, w_2, \cdots, w_n)$ とすると

$$w_i \to \hat{v}_i | [\max_{v_i} P(v_i|\boldsymbol{w}) = P(\hat{v}_i|\boldsymbol{w})], i = 1, 2, \cdots, n, \tag{A.2.2}$$

である．ただし，ここでは 2 元符号を仮定しているから，$v_i, \hat{v}_i \in \{0, 1\}$ である．上式右辺の条件式は

$$P(v_i|\boldsymbol{w}) = \sum_{1 \le m \le M, v_{mi} = v_i} P(\boldsymbol{v}_m|\boldsymbol{w}), v_i \in \{0, 1\} \tag{A.2.3}$$

により計算される．上式より，シンボル単位の事後確率 $P(v_i|\boldsymbol{w})$ を求めるには全ての符号語について周辺確率を計算する必要がある．すなわち

$$P(v_i = 0|\boldsymbol{w}) = \sum_{1 \le m \le M, v_{m_i} = 0} P(\boldsymbol{v}_m|\boldsymbol{w}) \tag{A.2.4.a}$$

$$P(v_i = 1|\boldsymbol{w}) = \sum_{1 \le m \le M, v_{m_i} = 1} P(\boldsymbol{v}_m|\boldsymbol{w}) \tag{A.2.4.b}$$

である．

A.2.2 条件付独立

式 (A.2.4.a),(A.2.4.b) で与えられる周辺確率の計算は，M 個の符号語で $v_{mi} = 0$（または，$v_{mi} = 1$）となる符号語全ての和をとらねばならず，指数オーダの計算量が必要である．しかし幸い実問題では，確率変数間に条件付独立が仮定できる場合が多い．LDPC 符号もその様な条件が成り立つ†．その結果，周辺確率の計算量を小さくできる．これを実行する方法が，後に述べる sum-product:SP) アルゴリズムである．

n 個の確率変数（事象‡）を $V_1, V_2, \cdots, V_n$ とする．一般に n 変数の同時確率（結合確率）$P(V_1, V_2, \cdots, V_n)(\geq 0)$ は，次式のように展開‡‡できる．

$$P(V_1, V_2, \cdots, V_n) =$$

$$P(V_1)P(V_2|V_1)P(V_3|V_1, V_2)\cdots P(V_n|V_1, V_2, \cdots, V_{n-1}) \tag{A.2.5}$$

ここで，n 個の事象 $V_1, V_2, \cdots, V_n$ の生起が互いに独立のとき，次式が成り立つ．

$$P(V_1, V_2, \cdots, V_n)$$

$$= P(V_1)P(V_2)P(V_3)\cdots P(V_n) \tag{A.2.6}$$

いま簡単のため 3 つの確率変数を考え，これらを X, Y, Z とする．次式が成り立つとき，X と Y は**独立**であるという．

$$P(X|Y) = P(X) \tag{A.2.7}$$

同様に次式が成り立つとき，X と Y は Z の下に**条件付き独立**であるという．

$$P(X|Y, Z) = P(X|Z) \tag{A.2.8}$$

式 (A.2.8) を図 A.2.1 のように表す．

A.2.3 ベイジアンネットワーク

ベイジアンネットワーク†(Bayesian network:BN)[Pea88] は同時確率における確率変数間の依存関係を表す**非巡回有向グラフ** (direct acyclic graph:DAG) である．図

† むしろパリティ検査行列を低密度にし，条件付独立性を利用して復号を容易にしていると言うことが出来る．

‡ 正確には，m 個の互いに素な事象 $E_1, E_2, \cdots, E_m$ に対し，事象 E_i が生起したとき値 x をとる偶然量 X が確率変数である．例えば，サイコロを投げたとき目が i である事象を $E_i (i = 1, 2, \cdots, 6)$ とし，同時に 2 つのサイコロを投げたとき事象 E_i, E_j が生起したとする．目の和 $x = i + j$ をとる X が確率変数で，$X = 2, X = 3, X = 4, \cdots, X = 12$ となる確率がそれぞれ $P(X = 2) = 1/36, P(X = 3) = 2/36, P(X = 4) = 3/36, \cdots, P(X = 12) = 1/36$ である．ここでは $n = m$ で，m 個の事象が n 個の確率変数 $V_1, V_2, \cdots, V_n$ に 1 対 1 に対応しているために混乱はない．

‡‡ これを**チェーン則という．**

† 確率推論の分野では**信念ネットワーク** (belief network:BN) とも呼ばれる [IEICE99]．ノードは命題を示し，アークは命題間の依存関係を示す．

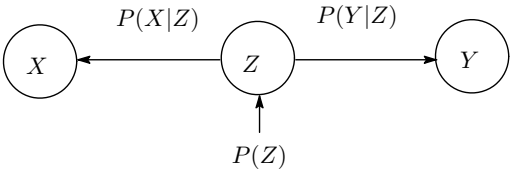


図 A.2.1: 確率変数 X と Y は Z の下に条件付き独立

A.2.1 に示した通り，ノードに確率変数，親ノードから子ノードへの有向アークに子ノードの条件付親ノードの確率を対応させる．その結果，条件付独立の確率構造を単純なグラフで示すことが出来る．論理的 (logical) に，あるいは仮説 (hypothesis)，仮定 (assumption) により，確率変数間に条件付独立性が成り立つとき，コンパクトにデータ構造を表現することが出来る．

［**例 A.2.1** ］次式の BN を図 A.2.2 に示す．

$$(1)\quad P(V_1,V_2,V_3,V_4,V_5)$$
$$= P(V_1)P(V_2|V_1)P(V_3|V_1,V_2)P(V_4|V_1,V_2,V_3)P(V_5|V_1,V_2,V_3,V_4) \tag{A.2.9}$$

$$(2)\quad P(V_1,V_2,V_3,V_4,V_5)$$
$$= P(V_1)P(V_2|V_1)P(V_3|V_2)P(V_4|V_3)P(V_5|V_4) \tag{A.2.10}$$

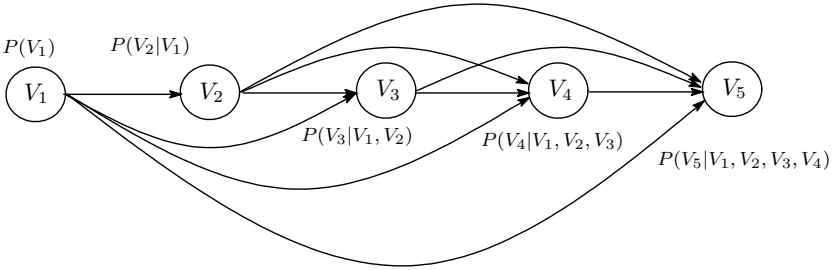
$$(3)\quad P(V_1,V_2,V_3,V_4,V_5)$$
$$= P(V_1)P(V_2|V_1)P(V_3|V_1)P(V_4|V_2,V_3)P(V_5|V_2) \tag{A.2.11}$$

A.2.4 Sum-product 復号法

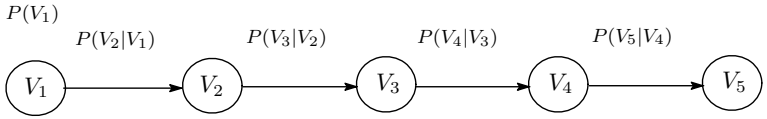
ベイジアンネットワークはノードにより確率変数を，アークにより確率変数間の依存関係を示す†．一般にノードが変数を示し，アークに変数間の関数を記述したグラフが**ファクターグラフ**であり，関数もノードで示す．前者を**変数ノード**といい丸で示すし，後者を**関数ノード**といい四角で示すことにする．変数 V_i と V_j が関数関係 $f(V_i,V_j)$ を持つとき，図 A.2.3 のように表す．

これを用いて LDPC 符号の復号を考えよう．m 行 n 列のパリティ検査行列 $H=[h_{ij}]$ が与えられると，そのファクターグラフは n 個の変数ノード，m 個の関数ノード（検査ノード）を持つ．符号語のシンボル V_j を変数ノード（符号ノード），パリティ検査行

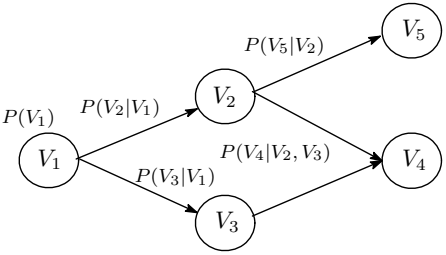
† 必ずしもアークに条件付確率を付与する必要はない．



(1) 式 (A.2.9)



(2) 式 (A.2.10)



(3) 式 (A.2.11)

図 A.2.2: 式 (A.2.9) − (A.2.11) のベイジアンネットワーク

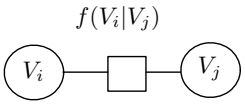


図 A.2.3: ファクターグラフ

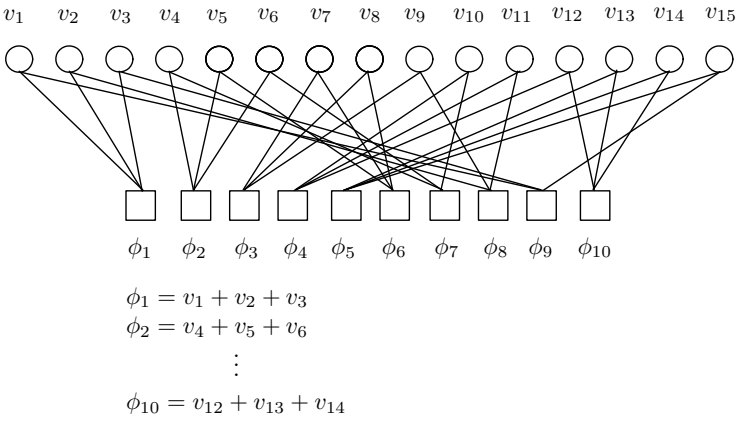


図 A.2.4: 式 (A.1.8) のタナーグラフ

列の条件 ϕ_i（シンドロームが 0 となるパリティ検査方程式）を関数ノードとするとき，**タナーグラフ**という．タナーグラフは，$h_{ij} = 1$ のとき，v_j と ϕ_i の間にアークを持ち，変数ノード間，関数ノード間にはアークは存在しない．

タナーグラフ上で有向グラフの順方向へ変数ノードと関数ノード間で交互に局所計算結果をメッセージとして伝播させることにより，周辺事後確率の計算を実行アルゴリズムが **sum-product アルゴリズム**である．変数ノードでは，関数ノードから送られてきたメッセージの（送り先の関数ノードからきたメッセージを除いて）積を計算し送り先の関数ノードに戻す．関数ノードでは，変数ノードから送られてきたメッセージの（送り先の変数ノードからきたメッセージを除いて）積和を計算し送り先に返す．このアルゴリズムはグラフにループがないとき，正確な周辺事後確率を計算する[††]

[Sum-product アルゴリズム]

[††] 多くの場合，ループが存在する．このとき，sum-product アルゴリズムは正確な計算をする保障はない．しかし，短いループを含まない場合，良い近似を与えることが知られている．ただし，メッセージ伝播はグラフ上の全ての関数ノードからアークのある全ての変数ノードにメッセージを伝播させ，続いて全ての変数ノードからアークのある全ての関数ノードにメッセージを伝播させ，これを繰り返す並列アルゴリズムを仮定する．

A.3 復号誤り確率

A.3.1 確率的復号法

A.3.2 シンボル単位の復号誤り確率の評価

演習問題

[**問 A.1**] 情報記号列 $\boldsymbol{u} = (u_1, u_2, \cdots, u_k)$ が与えられたとき, $m \times n (m < n, m = n-k)$ のパリティ検査行列 $H = [h_{ij}]$ を用いて組織符号の符号語 $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$ を生成せよ．ただし，$H = [h_{ij}]$ の $(m-1) \times (m-1)$ 右上三角はゼロであるとする．

参 考 文 献

[Gal63] R. G. Gallger, *Low-density parity-check codes*, MA:The M.I.T. Press, 1963.

[Hir96] 平澤茂一，情報理論，培風館，東京，1996 年.

[IEICE99] 電子情報通信学会編，電子情報通信ハンドブック，オーム社，東京，1999 年.

[Mac99] D.J.MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol.45, pp.399-431, 1999.

[Mat05] 松嶋敏泰，"ターボ符号・LDPC 符号とその復号法の概要，"信学誌，vol.88, no.4, pp.244-248, 2005 年 4 月.

[Pea88] J. Pearl, *Probabilistic reasoning in intelligent systems: Networks of plausible inference*, (2nd Ed.) CA:Morgan Kaufmann Publishers, Inc.,1997.

[Wad02] 和田山正，低密度パリティ検査符号とその復号法，トリケップス，2002 年.

略解・ヒント

[解 A.1] 組織符号であるから，$v_1 = u_1, v_2 = u_2, \cdots, v_k = u_k$ である．$\boldsymbol{v}H^{\mathrm{T}} = 0$ より

$$\begin{aligned} \sum_{i=1}^{k} v_i h_{1i} + v_{k+1} &= 0, \\ \sum_{i=1}^{k+1} v_i h_{2i} + v_{k+2} &= 0, \\ &\vdots \\ \sum_{i=1}^{n-1} v_i h_{ki} + v_n &= 0, \end{aligned} \tag{A.a.1}$$

が成り立つ．式 (A.a.1) の第 1 式から v_{k+1} を求め，これを第 2 式に代入し v_{k+2} を求める．これを順次第 3 式，第 4 式と繰り返すと全てのパリティ検査記号 $v_{k+1}, v_{k+2}, \cdots, v_n$ が求められる．例えば

$$\begin{aligned} \boldsymbol{u} &= (u_1, u_2, u_3, u_4) \\ &= (v_1, v_2, v_3, v_4), \end{aligned} \tag{A.a.2}$$

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \tag{A.a.3}$$

のとき，次式が成り立つ．

$v_1+v_2+v_4+v_5 = 0$ から，$v_5 = v_1+v_2+v_4$，これを次式に代入し $v_3+v_5+v_6 = 0$ から，$v_6 = v_3+v_5$，これを次式に代入し $v_2+v_3+v_5+v_6+v_7 = 0$ から，$v_7 = v_2+v_3+v_5+v_6$ と順次求まり，符号語 $\boldsymbol{v} = (v_1, v_2, \cdots, v_7)$ が得られる．