計　算　機　科　学　7

2025 年度版

はじめに

通信に関する重要な数学的理論で双璧をなすのは, 「符号理論」と「暗号理論」である. 前者は過酷な条件の中をいかに正確かつ円滑に通信を行ふかに関はる理論であり, 後者は, 傍受された通信内容の解読をいかにして防ぐかといふ安全性の問題に関はる理論である. 本講義では, 専ら前者を扱ふ.

符号理論とは, 途中に noise(ノイズ) が入る状況下において, 信号を送ることによる通信を行ふ場合に, それをいかに正確に効率的に実行させるかを考案する分野である.

本講義では, 線形代数学で学んだことをふんだんに使ふ. 特に, 行基本変形, 簡約化, vector 空間, 基, 部分空間, 次元, 核 (Ker), 像 (Im) など. これらについては [O] を参照されたい.

本書の大部分は, 平松豊一氏による [Hi] に沿つてゐて, その内容を本講義用に整理したものである. 現在のところ, 多くの問題は, 同書のものをそのまま採用してゐる.

符号理論と数論の関係で興味深いのは自己双対符号と呼ばれるもので, これは自己双対格子なるものを与へる. この格子に theta 級数を付随させるとき, 双対格子の theta 級数は元の格子の theta 級数から modular 変換で得られるから, 自己双対格子から保型形式が得られる. この辺りはいづれ追加したいと思ふ.

文　献

[D] 代数学 1, 2019, 名城大学 数学教室

[O] 線形代数学, 2019, 名城大学 数学教室

[Hi] 平松 豊一 著 : 応用代数学, 1997, 裳華房

[Hu] K. Huber : Codes over Gaussian integers, IEEE, Trans, IT,. 40(1994) 207 - 216

[Im] 今井 秀樹 著 : 符号理論, 電子情報通信学会, 1990

[Iy] 彌永 昌吉, 有馬 哲, 浅枝 陽 著 : 詳解 代数入門, 1990, 東京図書

[MS] MacWilliams, F.J., Slone, N.J.A : The Theory of Error-Correcting Codes, 1977, North-Holland

記号や言葉の約束　この講義録では, 慣例に従ひ $\mathbb{Z}$ で整数環, $\mathbb{Q}$ で有理数体, $\mathbb{R}$ で実数体, $\mathbb{R}^+$ で正の実数全体, $\mathbb{C}$ で複素数体, $\mathbb{F}_q$ で q 元体 (q は 1 つの素数の冪) を表す. 特に $\mathbb{F}_2 = \{0,\ 1\}$ とする. また x の多項式 $f(x)$ に対し $f(x) = 0$ の根（あるいは解）を単に $f(x)$ の根（あるいは解）と呼ぶことが多い.

体 $\mathbf{K}$ と $k \in \mathbb{N}$ に対し

$$\mathbf{K}^{-k} = \mathrm{Mat}(1, k, \mathbf{K}) \text{（行 vectors）}, \quad \mathbf{K}^{k} = \mathrm{Mat}(k, 1, \mathbf{K}) \text{（列 vectors）}$$

と記すものと約束する.

単位行列は I, または次数 n を明示して I_n で表す. 成分を $\mathbf{K}$ に持つ n 次正則行列の全体が行列の積に関してなす群（一般線型群）を

$$\mathrm{GL}(n, \mathbf{K})$$

と記す. n 次置換行列（つまり単位行列 I_n の行（或いは列）を自由に入れ替へてできる行列）の全体は $\mathrm{GL}(n, \mathbf{K})$ の部分群であるが, これを（$\mathbf{K}$ は省いて）

$$\mathrm{W}(n)$$

と記す.

目 次

1. 誤り訂正符号の基礎

1.1. 符号理論とは

Digital 通信 system では, 通信しやうとする k bit の情報に m bit の誤り検査 bit を付加し, $n = k + m$ bit の符号語を構成して通信する. n をその符号語の長さ または 符号長 といふ. 例へば, 1 bit の data をそのまま送るのでは, 誤りが心配なので, 同じものを 3 回繰り返して送ることにする. 0 に対しては $[0\ 0\ 0]$, 1 に対しては $[1\ 1\ 1]$ を bit 列として送る. これを符号長 3 の繰り返し符号といふ. ここで, bit 列の 2 番目に誤りが起き, $[0\ 1\ 0]$ を受けたとする. これは, あり得ない bit 列だから誤りが起きたことがわかる. 送つたものが $[0\ 0\ 0]$ か $[1\ 1\ 1]$ かを判断する場合, たいていの人は $[0\ 0\ 0]$ と判断するであろう. かうして, 2 bit 目の誤りは訂正されることになる. このやうに, 受けた bit 列をあり得る bit 列の中の「らしい」もので置き換へることによつて, 通信が完了する. この最後の段階を復号といふ. 起きやすい誤りに対し常に訂正ができて, その方法も簡単であるやうに工夫するのが符号理論である. しかし, 上で述べた方法はあまりに安直であつて非効率的である. 現代は非常に巧妙な方法が知られてゐる. それは現代数学の様々な知見を総合して得られたものである. それをこの講義を通して伝へていきたい.

2 進法とその演算 ここで, 2 元体 $\mathbb{F}_2 = \{0, 1\}$ を思ひ出しておく. これは 2 の剰余系 とも呼ばれる. 「代数学 1」では $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ と書いてゐた.

符号の効率 以下に 2 種類の通信（「繰り返し符号」と「$(4, 7)$ 符号」）を説明し, これらの効率を比較してみる.

例 1.1. 使用できる単語は

$$[0\ 0\ 0],\ [0\ 0\ 1],\ \cdots,\ [1\ 1\ 1]$$

の 8 個だけとして, 送信はこれを 3 回づつ繰り返して行なふこととする.

例 1.2. まづ, 始めに空間

$$V = \left\{ [\, a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\,] \,\middle|\, a_j \in \mathbb{F}_2,\ 1 \leqq j \leqq 7 \right\}$$

を考へる. V は $\mathbb{F}_2$ 上の 7 次元 vector 空間である. つまり通常の 2 次元空間 $\mathbb{R}^2$ や 3 次元空間 $\mathbb{R}^3$ と同様の性質を持つ. 具体的には和, 差, scalar 倍, 内積の演算ができる.
さて, いま, 行列

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

を考へる. これは 2 進法の 1 〜 7, つまり

$$1 = 001_{(2)},\quad 2 = 010_{(2)},\quad 3 = 011_{(2)},\quad 4 = 100_{(2)},\quad 5 = 101_{(2)},\quad 6 = 110_{(2)},\quad 7 = 111_{(2)}$$

を列 vectors にして, 左から並べたものに他ならない. さて, 我々は,

$$\mathscr{G} = \left\{ \boldsymbol{x} \in V \,\middle|\, \boldsymbol{x}\,{}^t H = \boldsymbol{0} \right\}$$

を単語として用意する. その理由はあとでわかる. さて, $\mathscr{G}$ の要素を具体的に表示するために, 線形代数で学んだ簡約化（掃き出し法）を使ふ.

H の簡約化は, 第 1 行と第 3 行を入れ換へるだけで終はり,

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

となる. よつて, $H{}^t\boldsymbol{x} = \mathbf{0}$ の解は

$${}^t\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = x_3 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_5 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_6 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + x_7 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

ここで

$$x_3 = c_1, \quad x_5 = c_2, \quad x_6 = c_3, \quad x_7 = c_4, \quad \boldsymbol{c} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix}$$

とおくと上の解は

$${}^t\boldsymbol{x} = G\boldsymbol{c}, \quad \text{但し} \quad G = \begin{bmatrix} 1\,1\,0\,1 \\ 1\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,1\,1 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix}$$

となる. よつて

$$\mathscr{G} = \left\{ \boldsymbol{x} \in V \,\middle|\, \boldsymbol{x}\,{}^tH = \mathbf{0} \right\} = \left\{ {}^t\boldsymbol{c}\,{}^tG \,\middle|\, \boldsymbol{c} \in {\mathbb{F}_2}^4 \right\}.$$

問 1.3. $\mathscr{G}$ の要素の個数はいくつか.

問 1.4. $[1\,1\,1\,1\,1\,1\,0]$ は $\mathscr{G}$ の要素であるか. 理由をつけて答へよ.

誤り訂正の仕組み さて, もし $\boldsymbol{y}\,{}^tH \neq 0$ となれば, もちろん, 単語 $\boldsymbol{y}$ に error が含まれてゐる. いま, 情報源（送信者）が単語 $\boldsymbol{x}$ を送信したとし, それに noise が加はつて, 第 i 成分の値が逆転してしまつたとする. つまり, 受信機に届いたのは

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}_i$$

である. ただし, ここで $\boldsymbol{e}_i$ は第 i 成分のみが 1 で他の成分はすべて 0 であるやうな vector である. たとへば $\boldsymbol{e}_2 = [0\,1\,0\,0\,0\,0\,0]$ である. さて, このとき受信側で $H{}^t\boldsymbol{y}$ を計算してみる：

$$H{}^t\boldsymbol{y} = H({}^t\boldsymbol{x} + {}^t\boldsymbol{e}_i) = H{}^t\boldsymbol{x} + H{}^t\boldsymbol{e}_i = \mathbf{0} + H{}^t\boldsymbol{e}_i = H{}^t\boldsymbol{e}_i$$

となる. これは H の第 i 列に他ならない. ところが実は H の第 i 列は i の 2 進法表示に他ならないので, $\boldsymbol{y}$ から i がいくつなのかがわかり, $\boldsymbol{e}_i$ が noise とわかるので, 送信者が送つたものは $\boldsymbol{y}$ でなくて $\boldsymbol{x} = \boldsymbol{y} - \boldsymbol{e}_i$ であることがわかるのである. 以上では, noise の影響は各単語 につき, 高々 1 箇所であるとの仮定の話である.

問 1.5. 上の 1.2 の方法で, 信号 $\boldsymbol{y} = [0\,1\,1\,1\,0\,1\,0]$ が届いたとする. noise は高々 1 箇所にしか入らなかつたと仮定して, 送信された単語を求めよ.

まとめ 以上のまとめとして, 1.1 と 1.2 の効率を比較してみやう. いま noise が, 0 と 1 を逆転させる確率を p $(0 < p < \frac{1}{2})$ とする

例 1.1 の場合. ここでは 3-bit word を 3 回づつ繰り返して送信するものとしよう. このときは error が唯 1 つであれば誤りを完全に正すことができるので, 誤りを正せない場合といふのは 2 つ以上の errors が起こる場合である. いま, 単語 1 つを 1 回送信して, 少くとも 1 回の誤りを生じる確率は $p' = 1 - (1-p)^3$ である. よつて, 3 回送信して, 正しい信号を復元できない確率は P_1 は

$$P_1 = 1 - (1-p')^3 - 3p'(1-p')^2$$

である. 例へば $p = 0.01$ であれば

$$P_1 = 0.0025940\cdots$$

である. この場合の送信効率は

$$E_1 = \frac{3}{9} = 0.333\cdots$$

である.

例 1.2 の場合. このときも error が唯 1 つであれば誤りを完全に正すことができ, 誤りを正せない場合といふのは 2 つ以上の errors が起こる場合である. その確率は

$$P_2 = 1 - (1-p)^7 - 7p(1-p)^6$$

である. 例へば $p = 0.01$ のときは

$$P_2 = 0.00203\cdots$$

となる. またこの方法では元々 4-bit word だつた $\boldsymbol{c}$ を 7-bit word にして $\boldsymbol{x}$ として, 送信するので, 効率 E_2 は

$$E_2 = \frac{4}{7} = 0.57\cdots$$

である.

結論. 1.2 の方法が 1.1 よりすぐれてゐる.

1.2. 通信系の model

符号理論で取り扱ふのは, digital 化された情報である. 以下, その様な情報の流れを分解してみる.

情報源 通信において, 情報の発生源や, それを digital 化する部分を含めて 情報源 といふ. 送りたい情報を 0, 1 の bit 列 (情報 bit 列 ともいふ) として発生させる.

符号器 符号器は情報 bit 列を k bit ごとの block に区切つて扱ふ. これを 通報 といひ, $\boldsymbol{i} = [\, i_1 \ \cdots \ i_k \,]$ で表す. 符号器では, 通報 $\boldsymbol{i}$ に対応した n bit ($n > k$) の bit 列 $\boldsymbol{w} = [\, x_1 \ \cdots \ x_n \,]$ が出力される. ここで n を 符号長, k を 情報 bit 数, w を 符号語, この操作を 符号化 といふ. 符号長 n, 情報 bit 数 k の符号を (n, k) 符号 といふ. 通報の種類が全部で $M = 2^k$ 個あるので, 対応する符号語も M 種類ある. この符号語の全体 $C = \{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_m\}$ を 符号 (code) と呼ぶ.

$$R = \frac{k}{n}$$

を 符号化率 といふ. R は符号の能率を表す量の 1 つであり, この値が大きいほど望ましい.

通信路 通信路は, 送信語 $\boldsymbol{w} = [\, x_1 \ \cdots \ x_n \,]$ が入力されると, n bit の受信語 $\boldsymbol{y} = [\, y_1 \ \cdots \ y_n \,]$ を出力する. 通信媒体に雑音等の影響がなければ送信語 w と同じものが出力されるが, 実際はある確率で異なつたものが受信される. 各 bit の誤りを e_i とし, $\boldsymbol{e} = (e_1 \cdots e_n)$ とおくと

$$\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{e}. \tag{1.6}$$

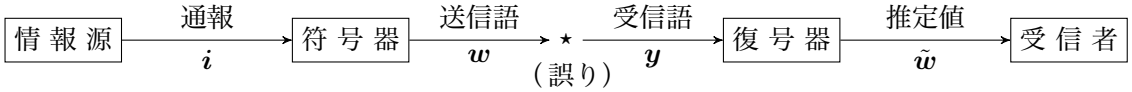
このとき $\boldsymbol{e}$ を 誤り pattern といふ.

復号器 復号器では, $\boldsymbol{y}$ をもとにいづれの符号語が送信されたかを推定し, 送信語 $\boldsymbol{w}$ の推定値 $\tilde{\boldsymbol{w}}$ を得る. このとき $\boldsymbol{w}$ が $\tilde{\boldsymbol{w}}$ に 復号 されたといふ. 誤り pattern $\boldsymbol{e}$ に関する (1.6) 式の計算は bit ごとに mod 2 などで行ふ. 例へば, 送信語 $\boldsymbol{w} = [\, 0\ 1\ 1\ 0 \,]$ を送つたとする. 通信路で 1 bit 目が誤り, $\boldsymbol{y} = [\, 1\ 1\ 1\ 0 \,]$ を受信したとする. これは (1.6) 式の誤り pattern が $\boldsymbol{e} = [\, 1\ 0\ 0\ 0 \,]$ である場合に相当する:

$$[\, 1\ 1\ 1\ 0 \,] = [\, 0\ 1\ 1\ 0 \,] + [\, 1\ 0\ 0\ 0 \,].$$

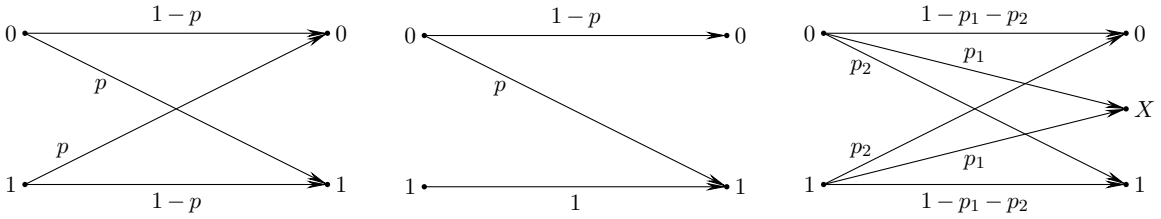
いままでは, 符号語は 0, 1 より強る bit 列であり, 2 元符号といふ. 一般には, q 種類の記号からなる記号列でよい. この場合, q 元符号 といふ. この q 種類の記号は q 元体 の元が使はれることが多い. その場合, q は素数の冪である.

以上の流れを図にまとめておく.



1.3. 通信路の model

通信路で起きる誤りでは, random 誤りが大切である. random 誤り とは, 送信した個々の bit に独立に発生する誤りのことである. 例へば, 宇宙通信における宇宙線等で生じる noise による誤りは random 誤りである. random 誤りの通信路は bit ごとに同一で, たとへば次の (a)〜(c) の様な model がある.



(a) 2 元対称通信路　(b) 2 元非対称通信路　(c) 2 元消失通信路

2 元対称通信路　0 を送出したときも 1 を送出したときも同じ確率 $1-p$ で正しく受信され, 確率 p で 0 は 1 に, 1 は 0 に誤る. この p を 誤生起確率 と呼ぶことにする. 実用的な場面を考へて, この note では, 誤生起確率は常に $0 \leqq p < \frac{1}{2}$ とする. これは符号理論で想定する代表的通信路である.

2 元非対称通信路　これは, 1 は常に正しく受信されるが, 0 は誤つて 1 になることがある（或いはその逆の）通信路である.

2 元消失通信路　これの通信路出力は, 0, 1, X の 3 通りの記号になり得る. 送信された 0, 1 は通信媒体の中では, 例へば pulse の ある/なし の信号波形である. 受信側で ある/なし を 0, 1 に判別するが, 通信媒体で被つた雑音によつて無理に判断して誤るより, その bit は不明 X として扱つた方がよい場合があるこのやうなときの通信路の model である.

1.4. 符号の種類

通信路で生じた誤りを訂正することを目的とした, ここまでに述べた符号を 誤り訂正符号 といふ. 他に, 誤りの検出のみを目的とする 誤り検出符号 がある.

両者をまとめて 誤り制御符号 と呼ぶこともある. 2 つの符号に本質的差はなく, 使はれ方に違ひがあるのみである. 従つて, 符号の種類としては, 次の 3 つが考へられる :

(1) 受信側でまづ誤りを検出し, その後その誤りを符号の能力によつて訂正する;
(2) 検出だけに止めておき, 送信側に data の再送を要求する;
(3) 検出の後, data の性質を利用し他の正常な data から誤つた data の正しい値を推測する.

さて, random 誤り訂正符号の能力は, 訂正可能な誤りの個数 t で評価される. t が大きい符号が良い符号である. 一般に, 誤り訂止能力が高いと符号化率 R は低い. また, R を一定にしたとき, 符号長 n が長いほど復号誤り率は小さくなる.

符号が block 単位で独立に通報と符号語を対応させてゐるとき, block 符号 といひ, 過去の block も関つて現時点の符号語が決まる逐次的な対応であるとき, 畳み込み符号 といふ. block 符号は, それが以降で述べる様な仕方で, 線形の方程式にもとづいて定義されるとき, 線形符号 といふ. これはまた, 巡回符号 と 非巡回符号 に分類される. 後者の中には, 代数幾何符号 が含まれる.

2. 線形符号

2.1. 符号の一般的な定義

前節では, 符号の仕組みを荒く説明したが, この節以降では, 厳密な定義にもとづいて説明していく. そのために, まづ, つぎの定義をおく.

定義 2.1. 一般に体 $\mathbf{K}$ と $n \in \mathbb{N}$ が与へられたとき, 部分集合

$$C \subset \mathbf{K}^{-n}$$

を 符号 と呼ぶ. 符号 C の要素を 符号語 と呼ぶ.

注意 2.2. 前節で述べた符号は 2 つの文字 $\{0,\ 1\}$ だけで構成されてゐたから, わざわざ, ここで, 一般の体を持ち出す理由を説明すべきであらう. しかし, この note を最後まで読まれれば, その答は自ずと明らかになる. ここでは, 実用的な便宜や, 使ひ易い理論を展開するためには, ともかく vector 空間の中に符号を設定すべきである, とのみ述べておく. ただし, 実用上は基礎の体 $\mathbf{K}$ として, 有限体を採るのが普通である.

2.2. 線形符号と検査行列

符号を構成するに際し, 符号語がばらばらに離れてゐることが望ましいのであるが, そこに規則性がなければ余り実用的ではない. つまり, ある種の規則性をもつ符号が大切である. その 1 つとして線形符号がある. この note では, 線形符号に焦点を当てる. そのために使ふ線型代数学の理論を含めて, この節でまとめておく.

ここでも $\mathbf{K}$ は一般に体を表はす. Vector 空間 $\mathbf{K}^{-n}$ の任意の部分空間 W は, 基を指定して記述できるが, 解空間としても記述できる. しかも, これらの記述の仕方は双対の関係にあることを説明する.

命題 2.3. Vector 空間 $\mathbf{K}^{-n}$ の任意の部分空間 W を考へる. $\dim W = r$ とする. もちろん $0 \leqq r \leqq n$ である. このとき, 次のことが成り立つ :

(1) （基による表記）W の 1 つの基を $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_r \in \mathbf{K}^{-n}$ とし,

$$A = \begin{bmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \vdots \\ \boldsymbol{a}_r \end{bmatrix} \in \mathrm{Mat}(r, n, \mathbf{K})$$

とおくと,

$$W = \{\, \boldsymbol{c}A \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

である.

(2) （解空間としての表記）$H \in \mathrm{Mat}(n-r, n, \mathbf{K})$ が存在して

$$W = \{\, {}^t\boldsymbol{x} \,|\, H\boldsymbol{x} = \boldsymbol{0}_{n-r} \,\}$$

と書ける.

(3) （まとめて）以上から

$$W = \{\, {}^t\boldsymbol{x} \in \mathbf{K}^{-n} \,|\, H\boldsymbol{x} = \boldsymbol{0}_{n-r} \,\} = \{\, \boldsymbol{c}A \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

である.

証明 (1) は基の生成性を述べてゐるに過ぎない. (2) の証明は, 以下に述べる 2.5 から自ずと浮び上がるであらう. (3) は (1) と (2) を併記しただけである. □

定義 2.4. 行列 $A = [\, a_{ij} \,] \in \mathrm{Mat}(m, n, \mathbf{K})$ について

$$A^{\curvearrowright} = [\, a_{m-i+1, n-j+1} \,]$$

と記し, これを A の反転行列と呼ぶことにする. もちろん $(A^{\curvearrowright})^{\curvearrowright} = A$ である. また, $B \in \mathrm{Mat}(m, n, \mathbf{K})$ について, $B^{\curvearrowright}$ が簡約行列であるとき, B を反転簡約行列と呼ぶ. さらに A の簡約化が B のとき, $B^{\curvearrowright}$ を A の反転簡約化と呼ぶ.

例 2.5. 次の 2 本の vectors で生成される $\mathbf{Q}^{-6}$ の部分空間（$(6,2)$ 符号）を W とする：

$$\boldsymbol{a}_1 = [\ 9\ \ 0\ \ 8\ \ 3\ -2\ -1\ ],$$
$$\boldsymbol{a}_2 = [-8\ \ 7\ \ 3\ -5\ \ 8\ \ 4\ ].$$

これらを並べた行列を

$$A = \begin{bmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \end{bmatrix} = \begin{bmatrix} 9 & 0 & 8 & 3 & -2 & -1 \\ -8 & 7 & 3 & -5 & 8 & 4 \end{bmatrix}$$

とおく. このとき

$$W = \{\, \boldsymbol{c}\, A \,|\, \boldsymbol{c} \in \mathbb{Q}^{-2} \,\}$$

である. さて 2.3 にいふ行列 H を求めるために, 行列 A を反転簡約化する. 結果は

$$B = \begin{bmatrix} 4 & 1 & 5 & 1 & 0 & 0 \\ 3 & 3 & 7 & 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{bmatrix}$$

となる. B の行 vectors の生成する部分空間は A のそれと一致するから,

$$W = \{\, \boldsymbol{c}\, B \,|\, \boldsymbol{c} \in \mathbb{Q}^{-2} \,\}$$

でもある. 行 vectors だと見辛いので, 列 vectors に直して

$${}^tW = \{\, c_1\, {}^t\boldsymbol{b}_1 + c_2\, {}^t\boldsymbol{b}_2 \,|\, c_1,\ c_2 \in \mathbb{Q} \,\} = \left\{ c_1 \begin{bmatrix} 4 \\ 1 \\ 5 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 3 \\ 3 \\ 7 \\ 0 \\ 2 \\ 1 \end{bmatrix} \,\middle|\, c_1,\ c_2 \in \mathbb{Q} \right\}$$

を解空間に持つ様な方程式は

$$H\boldsymbol{x} = \mathbf{0}, \quad \text{但し } H = \begin{bmatrix} 1 & 0 & 0 & -4 & 0 & -3 \\ 0 & 1 & 0 & -1 & 0 & -3 \\ 0 & 0 & 1 & -5 & 0 & -7 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{bmatrix}.$$

以上から

$$W = \{\, \boldsymbol{c}A \,|\, \boldsymbol{c} \in \mathbb{Q}^{-2} \,\} = \{\, \boldsymbol{c}B \,|\, \boldsymbol{c} \in \mathbb{Q}^{-2} \,\} = \{\, {}^t\boldsymbol{x} \in \mathbb{Q}^{-6} \,|\, H\boldsymbol{x} = \mathbf{0} \,\}.$$

問 2.6. $\mathbb{Q}^{-6}$ の vectors

$$\left.\begin{aligned} \boldsymbol{a}_1 &= [\ 6\ \ 0\ -5\ -3\ \ 3\ \ 1\ ], \\ \boldsymbol{a}_2 &= [\ 8\ \ 1\ -4\ \ 0\ \ 6\ \ 2\ ], \\ \boldsymbol{a}_3 &= [-8\ \ 1\ \ 7\ \ 1\ -9\ -3\ ] \end{aligned}\right\} \quad \text{からなる行列 } A = \begin{bmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \boldsymbol{a}_3 \end{bmatrix}$$

について,

$$W = \{\, \boldsymbol{c}\, A \,|\, \boldsymbol{c} \in \mathbb{Q}^{-3} \,\}\ (\subset \mathbb{Q}^{-6})$$

とおく. このとき $W = \{\, {}^t\boldsymbol{x} \,|\, H\boldsymbol{x} = \mathbf{0}_3 \,\}$ となる簡約行列 H を求めよ.

定義 2.7. 行列 H が簡約行列のとき, 連立 1 次方程式

$$H\boldsymbol{x} = \mathbf{0}$$

を 簡約方程式 と呼ぶことにする.

命題 2.8. 2.3 を計算手順に即して述べれば次の様になる.

(1) 2.3 の記号での A の反転簡約化を B とすれば, A の列 vectors で $\mathbf{K}$ 上に生成される部分空間 $W \subset \mathbf{K}^{-n}$ は

$$W = \{\, \boldsymbol{c}B \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\} = \{\, \boldsymbol{c}A \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

と書かれる. このとき簡約行列 $H \in \mathrm{Mat}(n-r, n, \mathbf{K})$ が一意的に存在して,

$$W = \{\, {}^t\boldsymbol{x} \in \mathbf{K}^{-n} \,|\, H\boldsymbol{x} = \mathbf{0}_{n-r} \,\}$$

と表される. 即ち, いかなる部分空間 W も簡約方程式の解空間として表される. 行列 H は上の手順で機械的に求められる.

(2) さらに, この主張のうち“反転簡約化”と“簡約化”を相互におきかへた主張も成り立つ.

また, 明らかに, 次の様に 2.3 の双対が成り立つ（2.11 を参照）.

命題 2.9. （2.3 の双対） 2.8 の記号のもとで, A の反転簡約化を B する. このとき

$$\{\, \boldsymbol{x}H \,|\, \boldsymbol{x} \in \mathbf{K}^{-(n-r)} \,\} = \{\, {}^t\boldsymbol{c} \in \mathbf{K}^{-n} \,|\, B\boldsymbol{c} = \mathbf{0}_r \,\} = \{\, {}^t\boldsymbol{c} \in \mathbf{K}^{-n} \,|\, A\boldsymbol{c} = \mathbf{0}_r \,\} \,(=: W^{\perp}).$$

証明 B の反転置行列を係数行列とする斉次型方程式の解が, まさしく, H の反転置行列の列 vectors を基とする部分空間になつてゐる. 主張はそのことから, 直ちにわかる. □

次の命題は容易に証明できる.

命題 2.10. 部分空間 $W \subset \mathbf{K}^{-n}$ の 直交補空間

$$W^{\perp} = \{\, \boldsymbol{u} \in \mathbf{K}^{-n} \,|\, \boldsymbol{u}\,{}^t\boldsymbol{w} = 0 \text{ for } \forall \boldsymbol{w} \in W \,\}$$

は $\mathbf{K}^{-n}$ の部分空間である. いま $\dim W = r$ として, W の 1 組の基を縦に並べた行列を $A \in \mathrm{Mat}(r, n, \mathbf{K})$ とおくと,

$$W = \{\, \boldsymbol{c}\,A \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}, \qquad W^{\perp} = \{\, {}^t\boldsymbol{x} \,|\, A\,\boldsymbol{x} = \mathbf{0}_r \,\}.$$

上の 2.10 は, 先の記号で, B と H の役割りを入れ替へることと W を $W^{\perp}$ に取り替へることが完全に対応してゐることを示してゐる.

問 2.11. （2.9 の確認） 2.5 の行列 H を

$$H = \begin{bmatrix} 1 & 0 & 0 & -4 & 0 & -3 \\ 0 & 1 & 0 & -1 & 0 & -3 \\ 0 & 0 & 1 & -5 & 0 & -7 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \boldsymbol{h}_3 \\ \boldsymbol{h}_4 \end{bmatrix}$$

と書いて, $\boldsymbol{h}_1$, $\boldsymbol{h}_2$, $\boldsymbol{h}_3$, $\boldsymbol{h}_4$ の張る部分空間を W' とする :

$$W' = \{\, \boldsymbol{c}\,H \,|\, \boldsymbol{c} \in \mathbb{Q}^{-4} \,\} = \mathbb{Q}\,\boldsymbol{h}_1 + \mathbb{Q}\,\boldsymbol{h}_2 + \mathbb{Q}\,\boldsymbol{h}_3 + \mathbb{Q}\,\boldsymbol{h}_4 \;(\subset \mathbb{Q}^{-6}).$$

このとき $W' = \{\, {}^t\boldsymbol{x} \,|\, B\boldsymbol{x} = \mathbf{0}_2 \,\}$ となる反転簡約行列 B を求めよ.

命題 2.12. 部分空間 $W \subset \mathbf{K}^{-n}$ の直交補空間 $W^{\perp}$ について,

$$\dim W + \dim W^{\perp} = n$$

が成り立つ. $W^{\perp}$ は W の双対(そうつい)空間とも呼ばれる.

証明 $\dim W = r$ とする. W の基を 1 組定め, それらを行 vectors として並べた行列を $A \in \mathrm{Mat}(r, n, \mathbf{K})$ とする. このとき

$$W^{\perp} = \{\, \boldsymbol{u} \mid A\, {}^t\boldsymbol{u} = \mathbf{0}_r \,\} \subset \mathbf{K}^{-n}$$

である. $W' \subset \mathbf{K}^{-r}$ を ${}^tA$ の行 vectors の生成する空間とする. このとき, 線形写像

$${}^tT_A : \mathbf{K}^{-n} \longrightarrow W', \quad \boldsymbol{u} \longmapsto \boldsymbol{u}\, {}^tA$$

について,

$$\mathrm{rank}({}^tT_A) = \dim W' = \mathrm{rank}({}^tA) = \mathrm{rank}(A) = r = \dim W,$$
$$n - r = \mathrm{null}({}^tT_A) = \dim W^{\perp}$$

であるから[1] 主張の等式を得る. □

符号理論の立場から以下の定義をしておくべきであらう.

定義 2.13. 線形符号 $C \subset \mathbf{K}^{-n}$ について, $C^{\perp} \subset \mathbf{K}^{-n}$ を C の双対(そうつい)符号と呼ぶ.

双対符号の例は次節の 2.26 で述べる.

注意 2.14. **(重要)** たとへば $\mathbf{K} = \mathbb{R}$ のときは,

$$\mathbf{K}^{-n} \times \mathbf{K}^{-n} \longrightarrow \mathbf{K}, \quad (\boldsymbol{u}, \boldsymbol{w}) \longmapsto \boldsymbol{u}{}^t\boldsymbol{w}$$

は内積の公理を満たす. 特に

$$\boldsymbol{u}\, {}^t\boldsymbol{u} = 0 \Longleftrightarrow \boldsymbol{u} = \mathbf{0} \tag{2.15}$$

である. しかし, 一般には (2.15) は成り立たない. 我々は $\mathbf{K}$ として有限体を考へることが多いが, その場合, この性質は満たされないことに注意せよ. 従つて $\mathbf{K} = \mathbb{R}$ のときは, 上の記号で

$$W^{\perp} \cap W = \{\, \mathbf{0} \,\}, \quad W^{\perp} \oplus W = \mathbf{K}^{-n} \quad (\text{但し } \mathbf{K} = \mathbb{R} \text{ のとき})$$

であるが, $\mathbf{K}$ が有限体のときは

$$W^{\perp} = W$$

さへ, 成り立つことがある (自己双対符号). しかもこの場合は特に重要である.

問 2.16. 2.14 の記号で $\mathbf{K} = \mathbb{F}_5$, $n = 3$ のときに $\boldsymbol{u} \neq \mathbf{0}$ にも拘らず $\boldsymbol{u}\, {}^t\boldsymbol{u} = 0$ である様な例を具体的に挙げよ.

[1] これは「線形代数 3」で学んだ次元定理に他ならない.

ここまでに登場した概念を符号理論の言葉として整理しておく.

定義 - 命題 2.17. ここまでに登場した概念を以下の様に名付ける :

(1) $\mathbf{K}^{-n}$ の部分空間 W を一般に線形符号とも呼ぶ. 特に, $\dim W = r$ のとき, W を (n,r) 線形符号, あるいは単に (n,r) 符号と呼ぶ.

(2) $\mathbf{K}^{-n}$ の線形符号 W （$\dim W = r$） について

$$W = \{\, \boldsymbol{c}G \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

となる（簡約行列とは限らない）行列 $G \in \mathrm{Mat}(r,n,\mathbf{K})$ を W の生成行列と呼ぶ.

(3) 一般に $r \leqq n$ で, 行列 $G \in \mathrm{Mat}(r,n,\mathbf{K})$ が $\mathrm{rank}\, G = r$ を満たすとき,

$$\{\, {}^t\boldsymbol{x} \in \mathbf{K}^{-n} \,|\, H\boldsymbol{x} = \mathbf{0}_{n-r} \,\} = \{\, \boldsymbol{c}G \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

を満たす（簡約行列とは限らない）行列 $H \in \mathrm{Mat}(n-r,n,\mathbf{K})$ を G の双対(そうつい)行列と呼ぶ. このとき $\mathrm{rank}\, H = n-r$ であり, 逆に, G は H の双対行列である. このとき, 言ふまでもなく

$$H\,{}^tG = O \in \mathrm{Mat}(n-r,r,\mathbf{K})$$

である.

(4) $\mathbf{K}^{-n}$ の線形符号 W （$\dim W = r$） について

$$W = \{\, {}^t\boldsymbol{x} \in \mathbf{K}^{-n} \,|\, H\boldsymbol{x} = \mathbf{0}_{n-r} \,\}$$

となる（簡約行列とは限らない）行列 $H \in \mathrm{Mat}(n-r,n,\mathbf{K})$ を W の検査行列（または parity 行列）と呼ぶ. 検査行列の階数はその行数と同一にしておくのが普通である（余計な検査は不要なので）.

(5) 上の記号の下で, W から得られる簡約行列 H を W の簡約検査行列[2)]と呼ぶ.

(6) 一般に $\mathbf{K}^{-n}$ 内の線形符号 W に対して

$$W^{\perp} = \{\, \boldsymbol{v} \in \mathbf{K}^{-n} \,|\, \boldsymbol{u}\,{}^t\boldsymbol{v} = 0 \text{ for } \forall \boldsymbol{u} \in W \,\}$$

とおき, これを W の双対符号と呼ぶ. 上の $W = \{\, \boldsymbol{c}G \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$ について

$$W^{\perp} = \{\, \boldsymbol{x}\,H \,|\, \boldsymbol{x} \in \mathbf{K}^{-(n-r)} \,\} = \{\, {}^t\boldsymbol{x} \in \mathbf{K}^{-n} \,|\, G\boldsymbol{x} = \mathbf{0}_r \,\}$$

となる.

以後, $\mathbf{K}^{-n}$ の部分空間を表す記号としては, 線形符号（linear code）の呼び名にちなんで, W よりも C を使用することが多い. 次の小節以降で, 上記のことを例で説明する.

ここで, 1.1 節と 1.2 節で定義した術語を再定義しておく.

定義 2.18. 生成行列 $G \in \mathrm{Mat}(r,n,\mathbf{K})$ を指定された線形符号 $C \subset \mathbf{K}^{-n}$ について,

$$C = \{\, \boldsymbol{c}G \,|\, \boldsymbol{c} \in \mathbf{K}^{-r} \,\}$$

であるが, $\boldsymbol{c}$ から $\boldsymbol{c}G$ を作ることを $\boldsymbol{c}$ を符号化するといふ. この意味で $\mathbf{K}^{-r}$ の元を単語と呼ぶことがある.

[2)] この講義のみにおける言葉.

定義 2.19. 生成行列 $G \in \mathrm{Mat}(r,n,\mathbf{K})$ を持つ線形符号 $C \subset \mathbf{K}^{-n}$ において，$\boldsymbol{cG}$ から $\boldsymbol{c} \in \mathbf{K}^{-r}$ を求めること（符号化の逆）を 元語化[3] と呼ぶことにする．

例題 2.20. 行列

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \in \mathrm{Mat}(4,7,\mathbb{F}_2)$$

を生成行列とする線形符号 C について $[\,1\,0\,1\,0\,0\,0\,1\,]$ を元語化せよ．

解答 題意から

$$[\,x_1\ x_2\ x_3\ x_4\,]G = [\,1\,0\,1\,0\,0\,0\,1\,]$$

つまり

$$ {}^tG \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad (=\boldsymbol{b}\ \text{とおく})$$

を解けばよい．$[\,{}^tG\ \ \boldsymbol{b}\,]$ を簡約化すると

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

より求める単語は $[\,x_1\ x_2\ x_3\ x_4\,] = [\,1\,1\,0\,1\,]$ である． □

演 習 問 題

2.21. 次の各符号 C_1, C_2, C_3 は $\mathbb{F}_2$ 上の線形符号である．これらの符号の生成行列と検査行列, 次元を求めよ．

(1) $C_1 = \{\,[\,0\,0\,0\,0\,0\,0\,]$, $[\,0\,0\,1\,0\,1\,1\,]$, $[\,0\,1\,0\,1\,0\,1\,]$, $[\,0\,1\,1\,1\,1\,0\,]$,
$[\,1\,0\,0\,1\,1\,0\,]$, $[\,1\,0\,1\,1\,0\,1\,]$, $[\,1\,1\,0\,0\,1\,1\,]$, $[\,1\,1\,1\,0\,0\,0\,]\,\}$.

(2) $C_2 = \{\,[\,0\,0\,0\,0\,0\,0\,0\,0\,]$, $[\,0\,1\,1\,0\,1\,1\,1\,1\,]$, $[\,1\,1\,0\,1\,1\,0\,0\,0\,]$, $[\,1\,1\,1\,1\,1\,1\,0\,1\,]$,
$[\,1\,0\,0\,1\,0\,0\,1\,0\,]$, $[\,0\,0\,1\,0\,0\,1\,0\,1\,]$, $[\,0\,1\,0\,0\,1\,0\,1\,0\,]$, $[\,1\,0\,1\,1\,0\,1\,1\,1\,]\,\}$.

(3) $C_3 = \{\,[\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,]$, $[\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,]$,
$[\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,]$, $[\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,]\,\}$.

[3] この講義のみにおける言葉．

2.3. 線形符号のさらなる例, 線形符号の同値

ここでは, さらに線形符号の例を述べる.

例 2.22. 単一 parity 検出符号. Vector 空間 $\mathbb{F}_2{}^{-4}$ の部分空間

$$C = \{\, [\, x_1\ x_2\ x_3\ x_4\,] \,|\, x_1 + x_2 + x_3 + x_4 = 0 \,\} \subset \mathbb{F}_2{}^{-4} \tag{2.23}$$

を (4, 3) 符号 と呼ぶ. 通報 $[\, x_1\ x_2\ x_3\,]$ が符号語

$$[\, x_1\ \ x_2\ \ x_3\ \ -x_1 - x_2 - x_3\,]$$

に対応してゐる. 通報とそれに対応する符号語は表 2.24 の様になる. ここで, 符号語はどれも語中の 1 の個数が偶数になつてゐて, 1 の個数が奇数のものはないことに注意されたい. 従つて, 復号器では受信語中の 1 の個数が偶数か否かを判断すれば, すべての 1 bit の誤りは検出できる. この様に, 符号語の 1 および 0 の個数の偶奇を一定にしてある様な符号を, 単一 parity 検査符号 といふ.

通報 i	符号語 w
$x_1\ x_2\ x_3$	$x_1\ x_2\ x_3\ x_4$
0 0 0	0 0 0 0
0 0 1	0 0 1 1
0 1 0	0 1 0 1
0 1 1	0 1 1 0
1 0 0	1 0 0 1
1 0 1	1 0 1 0
1 1 0	1 1 0 0
1 1 1	1 1 1 1

表 2.24

例 2.25. (7, 4) Hamming 符号. 1.2 で扱つた符号をもう一度, 取り上げる. ここでは, 検査符号 H から始める :

$$H = \begin{bmatrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{bmatrix} \in \mathrm{Mat}(3, 7, \mathbb{F}_2).$$

H を検査行列とする符号を C とせよ. 即ち, vector 空間 $\mathbb{F}_2{}^{-7}$ の中で,

$$C = \left\{\, \boldsymbol{x} = [\, x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7\,] \;\middle|\; H^t\boldsymbol{x} = \boldsymbol{0} \,\right\} \subset \mathbb{F}_2{}^{-4}$$

なる部分空間 (つまり線形符号) を考へる. そもそも, 行列 H は簡約行列である. 従つて, 直ちに解空間 C を基で記述できて,

$$C = \left\{ \boldsymbol{x} \;\middle|\; {}^t\boldsymbol{x} = x_3 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_5 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_6 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + x_7 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix},\ x_3,\ x_5,\ x_6,\ x_7 \in \mathbb{F}_2 \right\}$$

である. x_3, x_5, x_6, x_7 を任意に与へれば, 他の x_1, x_2, x_4 が上の式から定まる. つまり, この連立方程式の解空間は $\mathbb{F}_2$ 上 4 次元なので, 解は $2^4 = 16$ 個ある : この符号語は, 全部で $2^4 = 16$ 個ある : この線形符号を (7, 4) Hamming 符号 といふ.

例 2.26. 上の (7, 4)-Hamming 符号 C に対し,

$$H = \begin{bmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \boldsymbol{h}_3 \end{bmatrix} = \begin{bmatrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{bmatrix}$$

で $\boldsymbol{h}_1, \boldsymbol{h}_2, \boldsymbol{h}_3$ を定めれば, C の双対符号は

$$C^\perp = \mathbb{F}_2\boldsymbol{h}_1 + \mathbb{F}_2\boldsymbol{h}_2 + \mathbb{F}_2\boldsymbol{h}_3$$

となる. $C^\perp$ は (7, 3) 符号である.

注意 2.27. G を (n,r) 線形符号 C の 1 つの生成行列とする. このとき $\operatorname{rank} G = r$ である. 簡単のために $G \in \mathrm{Mat}(r,n,\mathbf{K})$ とする. このとき, $R \in \mathrm{GL}(r,\mathbf{K})$, と置換行列 $S \in \mathrm{W}(n)$ が存在して,

$$RGS = [\, I_r \; G_1 \,]$$

の形にできる. この様に, $r \leqq n$ に対して, 右端の $r \times r$ の部分が単位行列である様な (r,n) 型行列を 被約台形型 と呼ぶことにする. 今の場合, $\{\, \boldsymbol{u}G \,|\, \boldsymbol{u} \in \mathbf{K}^{-r} \,\} = \{\, \boldsymbol{u}RG \,|\, \boldsymbol{u} \in \mathbf{K}^{-r} \,\}$ が成立するから, G から生成される符号と RG で生成される符号は同一である. これは, C の基底 (G の行 vectors) を取り換へただけである. さらに,

$$\{\, \boldsymbol{u}RGS \,|\, \boldsymbol{u} \in \mathbf{K}^{-r} \,\} = \{\, \boldsymbol{u}GS \,|\, \boldsymbol{u} \in \mathbf{K}^{-r} \,\}.$$

これは, もとの符号語の n 個の座標の順序を S の列 vectors に従つて変更したものにあたる. 入れ替へた

この様な座標の変換で互ひに移り合ふ 2 種類の符号を同値とみなす関係を定義する. 即ち, 次の様に定義する.

定義 2.28. C, C' を体 $\mathbf{K}$ 上の 2 つの (n,r) 線形符号とし, それぞれの生成行列を G, G' とする. もし,

$$G' = RGS$$

となる $R \in \mathrm{GL}(r,\mathbf{K})$ および $S \in \mathrm{W}(n)$ が存在するならば, C と C' は 同値 であるといはれる. 容易にわかることであるが, この関係は同値関係である.

注意 2.29. 2 つの線形符号 $C \subset \mathbf{K}^{-m}$ と $C' \subset \mathbf{K}^{-m}$ に対して m と n が異るときは, C と C' が vector 空間として同型であつても, 誤り訂正能力が異る場合もある. しかし, 同値な符号については, 次節で述べる“最小距離”が等しいゆゑ, それらの誤り訂正能力は同一である. また, 互ひに同値な 2 つの線形符号の生成行列は, 行の基本変形と列の入れ替へで同一の被約台形型に移る.

例 2.30. を生成行列とする線形符号 C は

$$C = \{\, \boldsymbol{u}G \,|\, \boldsymbol{u} \in {\mathbb{F}_2}^{-3} \,\} = \{[0\,0\,0\,0\,0], [1\,1\,0\,0\,0], [1\,1\,1\,0\,1], [0\,0\,1\,0\,1],$$
$$[1\,1\,1\,1\,0], [0\,0\,1\,1\,0], [1\,1\,0\,1\,1], [0\,0\,0\,1\,1]\}.$$

ここで, $R = \begin{bmatrix} 1&0&0 \\ 1&1&0 \\ 0&0&1 \end{bmatrix}$, $S = \begin{bmatrix} 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \\ 0&0&1&0&0 \\ 0&1&0&0&0 \end{bmatrix}$ とするとき

$$G' = RGS = \left[\begin{array}{ccc|cc} 1&0&0&1&0 \\ 0&1&0&0&1 \\ 0&0&1&0&1 \end{array}\right] = [\, I_3 \; G_1 \,].$$

従つて,

$$C' = \{\, \boldsymbol{u}G \,|\, \boldsymbol{u} \in {\mathbb{F}_2}^{-3} \,\} = \{[00000], [10010], [01001], [00101],$$
$$[11011], [10111], [01100], [11100]\}.$$

C と C' は, 巡回置換 $\sigma = (2\,4\,3\,5)$ で成分位置を変換させた $C^\sigma = C'$ と互ひに同値である.

問 2.31. 2.25 の $(7,4)$ Hamming 符号 C について, 次の問に答へよ.

(1) C の生成行列 A を記せ.

(2) 2^4 個の符号語をすべて書き出せ.

(3) C は 行列

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

を生成行列とする符号 $D \in {\mathbb{F}_2}^{-7}$ と同値であることを示せ. その際, $B = RAS$ となる $R \in \mathrm{GL}(4, \mathbb{F}_2)$, $S \in \mathrm{W}(7)$ も記せ.

注意 2.32. 線形符号では, 符号語の成分の順序を入れ換へることにより, 検査行列 H を $[P\ I]$ の形で表現する場合がある. この場合, P の部分を 通報 bit と呼び, I の部分を 検査 bit を呼ぶ. この様に, 通報 bit と 検査 bit の位置が前後に区別されてゐる符号を 組織符号 (systematic code) と呼ぶことがある. しかし, これは本質的な事柄ではないので, この講義では以降触れない.

例 2.33. 自己双対符号. 特に, $C^\perp = C$ となる符号 C は 自己双対符号 と呼ばれ, 一般的に効率の良い符号であつて, 深い研究がなされてゐる. これはまた, 高次元 Euclid 空間における 球体の高密度充填 の理論と表裏の関係にある.

自己双対符号を与へる検査行列（この場合は生成行列と一致する）を 2 つ述べておく :

$$H = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right] \in \mathrm{Mat}(4, 8, \mathbb{F}_2), \qquad K = \left[\begin{array}{cc|cc} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 5 \end{array}\right] \in \mathrm{Mat}(2, 4, \mathbb{F}_7)$$

は, 自己双対な検査行列である.

問 2.34. 上の 2 つの検査行列 H, K について, 対応する符号の生成行列を（反転置簡約行列の形で）求め, それを簡約化することで, これらが実際に自己双対符号であることを示せ.

演 習 問 題

2.35. α を $x^2 + x + 1 \in \mathbb{F}_2[x]$ の 1 つの根とする. $\mathbb{F}_4$ 上の検査行列

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ \alpha & \alpha^2 & 0 & 1 \end{bmatrix}$$

をもつ $(4,2)$ 符号 $C \subset {\mathbb{F}_4}^4$ の符号語をすべて求めよ.

3. 符号と距離

3.1. 距離

Gauss 符号 に
中. 再度の check

以下の様に, 一般の線形空間に対して距離の公理をおく :

命題 3.1. 線形空間 V のに対して, 函数

$$d : V \times V \longrightarrow \mathbb{R}^+ \text{（正の実数全体）},$$

が与へられて次の 4 つの性質を持つとする :

M1. $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x} + \boldsymbol{w}, \boldsymbol{y} + \boldsymbol{w})$. 特に $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x} - \boldsymbol{y}, \boldsymbol{0})$.
M2. $d(\boldsymbol{x}, \boldsymbol{y}) = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{y}$.
M3. $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.
M4. $d(\boldsymbol{x}, \boldsymbol{y}) \leqq d(\boldsymbol{x}, \boldsymbol{z}) + d(\boldsymbol{z}, \boldsymbol{y})$.

このとき, V に 距離（または 距離函数） d が定義されてゐるといふ.

以下で, 具体的な距離について述べる. 従つて, これらの公理を満たす距離が存在する.

3.2. Hamming 距離

先に 2.14 で述べたことは, 有限体 $\mathbf{K}$ 上の vector 空間においては, $\mathbb{R}$ 上の場合とは異なり, 内積によつて距離を導入することができないことを意味する. 有限体 $\mathbf{K}$ 上の vector 空間における自然な距離の一つとして, Hamming 距離と呼ばれるものがあり, これが符号理論の目的に適合する.

定義 3.2. 符号 C を含む全空間 $\mathbf{K}^{-n}$ に対して, 函数 $d : \mathbf{K}^{-n} \times \mathbf{K}^{-n} \longrightarrow \mathbb{N}$ を

$$d(\boldsymbol{x}, \boldsymbol{y}) = \#\{\, i \,|\, x_i \neq y_i \,\}$$

で定める. 但し, $\boldsymbol{x} = [\, x_1 \ \cdots \ x_n \,]$, $\boldsymbol{y} = [\, y_1 \ \cdots \ y_n \,]$ である. これを C の Hamming 距離[4)]と称する. 即ち $\boldsymbol{x}, \boldsymbol{y}$ の相異なる成分の数が $\boldsymbol{u}$ と $\boldsymbol{v}$ の Hamming 距離 $d(\boldsymbol{u}, \boldsymbol{v})$ である.

次の小節で述べる様に, Hamming 距離は, 符号に対する距離として重要なものの一つである.

問 3.3. 次の 2 つの bit 列の Hamming 距離はいくらか.

$$[\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,],$$
$$[\,0\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,].$$

命題 3.4. $\mathbf{K}^{-n}$ の Hamming 距離 d は次の性質を持つ.

- **H1.** $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x} + \boldsymbol{w}, \boldsymbol{y} + \boldsymbol{w})$. 特に $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{x} - \boldsymbol{y}, \boldsymbol{0})$.
- **H2.** $d(\boldsymbol{x}, \boldsymbol{y}) = 0 \ \Leftrightarrow \ \boldsymbol{x} = \boldsymbol{y}$.
- **H3.** $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.
- **H4.** $d(\boldsymbol{x}, \boldsymbol{y}) \leqq d(\boldsymbol{x}, \boldsymbol{z}) + d(\boldsymbol{z}, \boldsymbol{y})$.
- **H5.** $\lambda \in \mathbf{K}^{\times}$ ならば $d(\lambda\boldsymbol{x}, \lambda\boldsymbol{y}) = d(\boldsymbol{x}, \boldsymbol{y})$. 特に $d(-\boldsymbol{x}, -\boldsymbol{y}) = d(\boldsymbol{x}, \boldsymbol{y})$.

証明 **H4** 以外は明らかである. **H4** を示す. いま,

$$\boldsymbol{x} = (x_1 \ \cdots \ x_n), \quad \boldsymbol{y} = (y_1 \ \cdots \ y_n), \quad \boldsymbol{z} = (z_1 \ \cdots \ z_n) \quad (\, x_1,\ y_i,\ z_i \in \mathbf{K}\,)$$

とおく, 第 i 成分に関して, $x_i = y_i$ のときは $x_i = y_i = z_i$ または $x_i = y_i \neq z_i$ であり, $x_i \neq y_i$ のときは $x_i = z_i \neq y_i$, $x_i \neq z_i = y_i$, $x_i \neq z_i$ かつ $y_i \neq z_i$ であるかの 3 つ場合のいづれかである. これらのどの場合でも, 左辺へと右辺の Hamming 距離への寄与は等しいか, 右辺が 1 だけ多い. これをすべての成分で考慮すれば, 与式が成り立つことは明らかである. □

[4)] 米国の数学者 Richard Wesley Hamming (1915 年 2 月 11 日 ～ 1998 年 1 月 7 日) により発明された符号 (Hamming 符号) に由来する.

3.3. 最尤復号法と Hamming 距離

ここでは, 通信といふ言葉を確率の概念を用いて定式化し, それについて, 最も自然な誤りの生じ方を想定する. このとき Hamming 距離の近さは, 自然な確率的な近さ（最尤(ゆう)性）と一致することを説明する.

定義 3.5. $C \subset \mathbf{K}^{-n}$ を符号とし, $0 < p < \frac{1}{2}$ を固定する. 一般には p は小さい. 符号語 $\boldsymbol{w}$ を送信し, $\boldsymbol{y}$ を受信する確率, 即ち, 写像

$$P : C \times \mathbf{K}^{-n} \longrightarrow [\,0,\,1\,], \quad (\boldsymbol{w},\,\boldsymbol{y}) \longmapsto P(\boldsymbol{w}|\boldsymbol{y})$$

が与へられてゐるとする. このとき, 組 (C, P) を 通信 と呼ぶ.
さらに, いま, この確率 $P(\boldsymbol{w}|\boldsymbol{y})$ が $d = d(\boldsymbol{y}, \boldsymbol{w})$ のみに依存してゐて,

$$P(\boldsymbol{w}|\boldsymbol{y}) = p^d(1-p)^{n-d}$$

となつてゐるとき, (C, P) を random 誤り通信 と称する. また, このとき p を random 誤り通信 (C, P) の 誤り生起率 といふ.

通信路は 5 page の図の (a) の様であるとして, $(4, 3)$ 符号（2.22 を参照）

$$C = \{\, \boldsymbol{x} \in {\mathbb{F}_2}^4 \,|\, x_1 + x_2 + x_3 + x_4 = 0 \,\}$$

を考へる. いま誤り生起率が p であるとし, 受信語として, $\boldsymbol{y} = [\,0\ 1\ 0\ 0\,]$ が得られたとする. 例へば, 2 つの符号語 $\boldsymbol{w}_1 = [\,0\ 0\ 0\ 0\,]$, $\boldsymbol{w}_2 = [\,1\ 1\ 1\ 1\,]$ のそれぞれが送られた確率は,

$$P(\boldsymbol{w}_1|\boldsymbol{y}) = (1-p)^3 p, \quad P(\boldsymbol{w}_2|\boldsymbol{y}) = (1-p)p^3$$

である. もちろん $P(\ |\ )$ は $|$ の後の条件のもとで $|$ の前の事柄が起きる条件付き確率を表す. p は通常 10^{-1}〜10^{-10} 程度である. 明らかに, 異つてゐる bit 数の少ない前者の方が確率が高いから, $\boldsymbol{w} = \boldsymbol{w}_1$ のときが $P(\boldsymbol{y}|\boldsymbol{w})$ が最も小さくなる. ちなみに, $p = 10^{-2}$ とすると

$$P(\boldsymbol{w}_1|\boldsymbol{y}) \doteqdot 10^{-2}, \quad P(\boldsymbol{w}_2|\boldsymbol{y}) \doteqdot 10^{-6}.$$

従つて, 受信語 $\boldsymbol{y}$ が複号されるべき「最も正しさうな」符号語は $\boldsymbol{w}_1$ ではないと判断されるべきである. 明らかに「最も正しさうな」符号は $[\,1\ 1\ 0\ 0\,]$, $[\,0\ 0\ 0\ 0\,]$, $[\,0\ 1\ 1\ 0\,]$, $[\,0\ 1\ 0\ 1\,]$ の 4 つである.

定義 3.6. 一般に, 受信語 $\boldsymbol{y}$ と対応する有り得べきすべての送信語 $\boldsymbol{w}_1, \cdots, \boldsymbol{w}_M$ に対し条件付き確率 $P(\boldsymbol{w}_i|\boldsymbol{y})$ $(i = 1, \cdots, M)$ を計算し, 最も値の大きい符号語に復号する方法を 最尤(ゆう)復号法 といふ.

注意 3.7. (1) 上の考察からわかる通り, 最尤復号法は, 受取る可能性のある受信語との距離が最小である様な符号語が, 常に唯 1 つであれば, その符号語に復号ができる. このことについては, 次の 4.2 節で解説する.
(2) 最尤復号法は, 復号誤り率が最も小さくなる復号法であるが, M が大きいときは実用的でない.

例 3.8. $C \subset \mathbb{F}_2{}^5$ なる符号があつたとして, $\boldsymbol{y} = [1\ 0\ 1\ 0\ 0] \in \mathbb{F}_2{}^5$ と $\boldsymbol{w}_1 = [1\ 1\ 1\ 0\ 0]$, $\boldsymbol{w}_2 = [0\ 1\ 1\ 1\ 1] \in C$ に対し,

$$d(\boldsymbol{y}, \boldsymbol{w}_1) = 1, \quad d(\boldsymbol{y}, \boldsymbol{w}_2) = 4.$$

ここで, $\boldsymbol{y}$ を受信語, $\boldsymbol{w}_1$, $\boldsymbol{w}_2$ を送信語と考へると,

$$P(\boldsymbol{w}_1 \,|\, \boldsymbol{y}) = (1-p)^4 p, \quad P(\boldsymbol{w}_2 \,|\, \boldsymbol{y}) = (1-p)p^4.$$

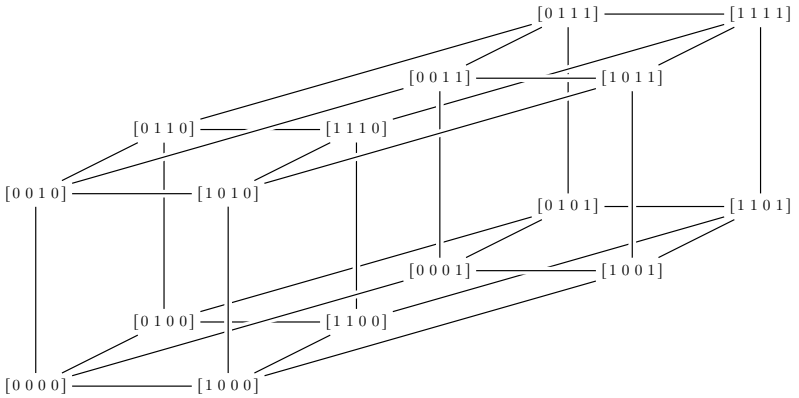
実際の通信では $0 \leqq p < \frac{1}{2}$ ゆゑ, 前者が大きく $\boldsymbol{w}_1$ の方が $\boldsymbol{y}$ に似てゐる. 従つて Hamming 距離の小さいことと条件付き確率の大きいことが対応し, 「最も正しさうな」符号語を選ぶ手順の数量化が得られた.

この例からもわかるやうに, 2 元対称通信路での最尤復号法は, Hamming 距離が一番近い符号語に復号することに他ならない. この意味で 最小距離復号法 ともいふ. 次に, bit 列の非零の bit 数を, $\boldsymbol{u}$ の Hamming 重さ といひ, $\mathrm{wt}(\boldsymbol{u})$ と書く. 線形符号で, (1.6) 式 : $\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{e}$ が成立するとき,

$$d(\boldsymbol{y}, \boldsymbol{w}) = \mathrm{wt}(\boldsymbol{y} - \boldsymbol{w}) = \mathrm{wt}(\boldsymbol{e}).$$

すなはち, 送信語 $\boldsymbol{w}$ 受信語 $\boldsymbol{y}$ の距離は誤り pattern $\boldsymbol{e}$ の重さに等しい.

下の図は $\mathbb{F}_2{}^{-4}$ において Hamming 距離が 1 である符号語の間のみ線分で結んだものである.



定義 3.9. 距離 d が与へられた符号 $C \subset \mathbf{K}^{-n}$ に対して,

$$d(C) = \min\{\, d(\boldsymbol{w}, \boldsymbol{w}') \,|\, \boldsymbol{w},\ \boldsymbol{w}' \in C \text{ かつ } \boldsymbol{w} \neq \boldsymbol{w}' \,\}$$

を C の 最小距離 といふ.

命題 3.10. C を線形符号とする. 最小距離 $d(C)$ は符号語の最小重さと一致する :

$$d(C) = \min\{\, \mathrm{wt}(\boldsymbol{w}) \,|\, \boldsymbol{w} \in C,\ \boldsymbol{w} \neq \boldsymbol{0} \,\}.$$

証明 最小距離を与へる符号語の組 $\boldsymbol{w}_1$, $\boldsymbol{w}_2$ をとれ. 即ち $d(C) = d(\boldsymbol{w}_1, \boldsymbol{w}_2)$ とする. このとき $\boldsymbol{w} = \boldsymbol{w}_2 - \boldsymbol{w}_1\ (\neq \boldsymbol{0})$ とおけば $d(C) = \mathrm{wt}(\boldsymbol{w})$ であるから

$$d(C) \geqq \min\{\, \mathrm{wt}(\boldsymbol{w}) \,|\, \boldsymbol{w} \in C,\ \boldsymbol{w} \neq \boldsymbol{0} \,\}.$$

一方, 任意の $\boldsymbol{w} \in C$ について $\mathrm{wt}(\boldsymbol{w}) = d(\boldsymbol{w}, \boldsymbol{0})$ であるから

$$d(C) \leqq \min\{\, \mathrm{wt}(\boldsymbol{w}) \,|\, \boldsymbol{w} \in C,\ \boldsymbol{w} \neq \boldsymbol{0} \,\}.$$

よつて主張は証明された. □

演 習 問 題

3.11. 次の 8 個の符号語をもつ $\mathbb{F}_2$ 上の符号について, Hamming 距離に関しての最小距離 d をめよ.

$$[0\,0\,0\,0\,0\,0\,0],\ [1\,0\,0\,1\,1\,1\,0],\ [1\,1\,1\,0\,1\,0\,0],$$
$$[0\,1\,0\,0\,1\,1\,1],\ [0\,1\,1\,1\,0\,1\,0],\ [1\,0\,1\,0\,0\,1\,1],$$
$$[0\,0\,1\,1\,1\,0\,1],\ [1\,1\,0\,1\,0\,0\,1].$$

4. 誤り訂正と復号の理論

4.1. 誤りの検出と誤り訂正の原理

距離が与へられた符号 $C \subset \mathbf{K}^{-n}$ に対して,

$$d(C) = \min\{\, d(\boldsymbol{w}, \boldsymbol{w}') \mid \boldsymbol{w},\ \boldsymbol{w}' \in C \text{ かつ } \boldsymbol{w} \neq \boldsymbol{w}' \,\}$$

を C の最小距離と呼ぶのであつた. また

$$U_t(\boldsymbol{w}) = \{\, \boldsymbol{w}' \mid d(\boldsymbol{w}, \boldsymbol{w}') \leqq t \,\}$$

を, 中心 $\boldsymbol{w}$, 半径 t の 小球 といふ. 各符号語を中心とする半径 t の小球たちは,

$$d(C) \geqq 2t + 1 \tag{4.1}$$

が成り立つていれば, 共通部分をもたない. この状況で, 送信語として $\boldsymbol{w}$ を送り, t 箇所以下の誤りを生じて $\boldsymbol{y}$ を受信したとする :

$$\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{e}, \quad \mathrm{wt}(\boldsymbol{e}) \leqq t.$$

このとき, $\boldsymbol{y}$ に一番近い符号語は $\boldsymbol{w}$ であるから, 受信側で $\boldsymbol{y}$ を $\boldsymbol{w}$ に復号するならばこの誤りは訂正される. この様な, 復号ができる符号を t 重誤り訂正符号 といふ. このやうに, 符号語間の距離が十分離れてゐることが誤り訂正のできるための条件である. (4.1) 式をみたす t を選び, t 箇所以下の誤りのみ訂正の対象にする復号法を, 限界距離復号法 といふ.

$t > 1$ の場合の t 重誤り訂正符号は重要であるが, その例を述べるのは手間が掛かるので, ずつと後の方（7.1 節や 7.3 節など）で述べる.

誤り検出の原理

送信語 $\boldsymbol{w}$, に対し, k 箇所以下の誤りが加わり受信語 $\boldsymbol{y}$ になつたとする. $\boldsymbol{y}$ は $\boldsymbol{w}$ を中心とする半径 k の小球内にある. そこで,

$$d \geqq k + 1$$

ならば, その小球の中に他の符号語はなく, $\boldsymbol{y}$ が他の符号語と一致することはない. 従つて, 誤りとして検出できる. しかし, 訂正は必ずしもできない. また, k を越える個数の誤りが生じて, ほかの符号語と一致してしまつた場合は, 誤りの検出もできず, 見逃し誤りとなる. 通信の分野では, 誤り検出符号は古くから用ゐられてゐる.

4.2. 誤り訂正の基礎

誤り訂正同時検出の原理

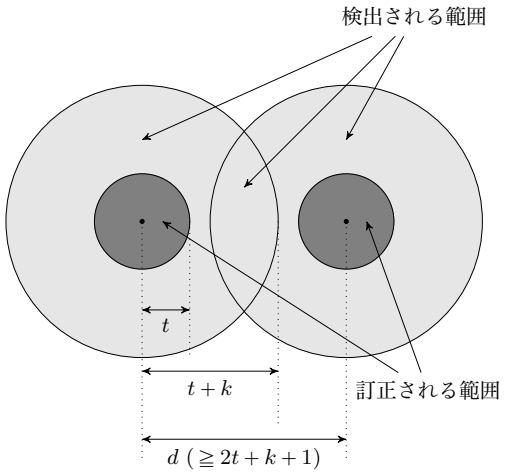
少ない誤りに対しては訂正を, 多い誤りに対しては検出する場合を考へる. すなはち, t 重の誤りまでは訂正し, ぞれ以上 $t+k$ 重までの誤りは検出する場合を考へる. 各符号語 $\boldsymbol{w}_i$ を中心とする半径 t の小球内の受信語は, 中心の符号語に復号される. この小球を訂正領域といふ.

$t+k$ 重までの誤りが加はり受信語 $\boldsymbol{y}$ を得たとき, その誤りが検出されるためには $\boldsymbol{y}$ が他の符号語の訂正領域になければよい. すなはち, 各符号語を中心とする半径 $t+k$ の小球が他の符号語を中心とする半径 t の小球と重複部をもたなければよい. 以上のことは, 次の様にまとめられる.

定理 4.2. 符号 C の最小距離 $d=d(C)$ について, 不等式

$$d \geqq 2t+k+1$$

をみたす t, k に対しては, t 重誤りを訂正し, 同時に $(t+k)$ 重誤りを検出することができる.



例 4.3. $d(C)=5$ の符号 C により random 誤り通信を構成する場合, 誤り生起率 p の大きさに応じて, 次の 3 通りの中から, 最善の処理を選ぶことになる ;
(1) 2 重誤り訂正 $(t=2, k=0)$,
(2) 1 誤り訂正かつ 2 重誤り検出 $(t=1, k=2)$,
(3) 4 重誤り検出 $(t=0, k=4)$.
つまり, p の大きさに応じて, 最小距離 $d(C)$ を, 訂正能力と検出能力にいかに配分するかによつて使ひ方が決まるとも言へる.

4.3. 線形符号の復号法

ここでは線形符号の送信誤りを自動的に復号する方法を述べる. 基本的な idea を一言で述べると次の様になる.

原理的には, 受信語 $\boldsymbol{y}\in\mathbf{K}^{-n}$ と Hamming 距離に関して $\boldsymbol{y}$ に最も近い符号 $\boldsymbol{w}\in C$ を送信語であらうと推測しそれを, 復号語と見做す. しかし, 実用上は, 送信語 $\boldsymbol{w}$ と受信語 $\boldsymbol{y}$ の差（誤り pattern）$\boldsymbol{e}$ の内, 起きやすいものについては, その syndrome $\boldsymbol{r}=H\,{}^t\boldsymbol{e}\in\mathbf{K}^{-n}$ とが 1 対 1 に対応する様にしておいて, 瞬時に $\boldsymbol{r}$ から $\boldsymbol{e}$ を見付けて, $\boldsymbol{w}=\boldsymbol{y}-\boldsymbol{e}$ を復号する様に仕組む.

Syndrome の定義を述べる.

定義 4.4. 検査行列 H をもつ線形符号 C, および, 受信語 $\boldsymbol{y}$ に対し,

$$\boldsymbol{s}=H\,{}^t\boldsymbol{y}$$

を $\boldsymbol{y}$ の syndrome[5] といふ. $\boldsymbol{y}$ の送信語が $\boldsymbol{w}\in C$ であつたとし, 誤り pattern を $\boldsymbol{e}=\boldsymbol{y}-\boldsymbol{w}$ と書くと, $H\,{}^t\boldsymbol{w}=\boldsymbol{0}$ であるから,

$$\boldsymbol{s}=H\,{}^t\boldsymbol{y}=H\,{}^t(\boldsymbol{w}+\boldsymbol{e})=H\,{}^t\boldsymbol{e}.$$

従つて, syndrome $\boldsymbol{s}$ は送信語 $\boldsymbol{w}$ にはよらず, 誤り pattern $\boldsymbol{e}$ のみによつて決まる.

注意 4.5. Syndromes は検査行列 H の選び方には依存する.

例 4.6. $(7,4)$ **Hamming 符号の復号**.
$(7,4)$ Hamming 符号を考へる. 送信語 $\boldsymbol{w}=[\,x_1\ \cdots\ x_7\,]$ に対し, 受信語を $\boldsymbol{y}=[\,y_1\ \cdots\ y_7\,]$, 誤り pattern を $\boldsymbol{e}=[\,e_1\ \cdots\ e_7\,]$ とすると, syndrome $\boldsymbol{s}$ は,

$$\boldsymbol{s}=\begin{bmatrix}s_1\\s_2\\s_3\end{bmatrix}=H\begin{bmatrix}e_1\\\vdots\\e_7\end{bmatrix},\quad \text{但し } H=\begin{bmatrix}0\,0\,0\,1\,1\,1\,1\\0\,1\,1\,0\,0\,1\,1\\1\,0\,1\,0\,1\,0\,1\end{bmatrix}.$$

いま, x_1 に誤りが生じたとすると,

$$e_1=1,\quad e_2=\cdots=e_7=0.$$

従つて,

$$s_1=s_2=0,\ s_3=1.$$

同様にして, 1 箇所だけの誤り pattern の全体については, それらの誤りの発生位置と syndrome $\boldsymbol{s}$ が 1 対 1 に対応する (右の表参照). よつて, 誤りが事実上, 高々 1 箇所しか起きない様な場合には, 受信語 $\boldsymbol{y}$ に対し, $H\,{}^t\boldsymbol{y}$ を計算して syndrome $\boldsymbol{s}$ を求めれば, 誤りの発生位置がわかり訂正できる. もちろん, 2 箇所以上の誤りについては, この様な 1 対 1 の対応はない（表の最下 2 段）.

誤り位置	s_1	s_2	s_3
x_1	0	0	1
x_2	0	1	0
x_3	0	1	1
x_4	1	0	0
x_5	1	0	1
x_6	1	1	0
x_7	1	1	1
x_1 と x_2	0	1	1
x_5 と x_6	0	1	1

[5] もし $\boldsymbol{s}\neq\boldsymbol{0}$ であつたならば, $\boldsymbol{y}$ に誤りが含まれてゐることが確実で, その兆候（syndrome）を $\boldsymbol{s}$ が捉へてゐるから, その様に呼ぶのだと思はれる.

一般に, t 重誤り訂正符号の場合, 異なる t 個以下の誤りは異なる syndrome に対応する. つまり, Hamming 重さ t 以下の誤り pattern の集合を

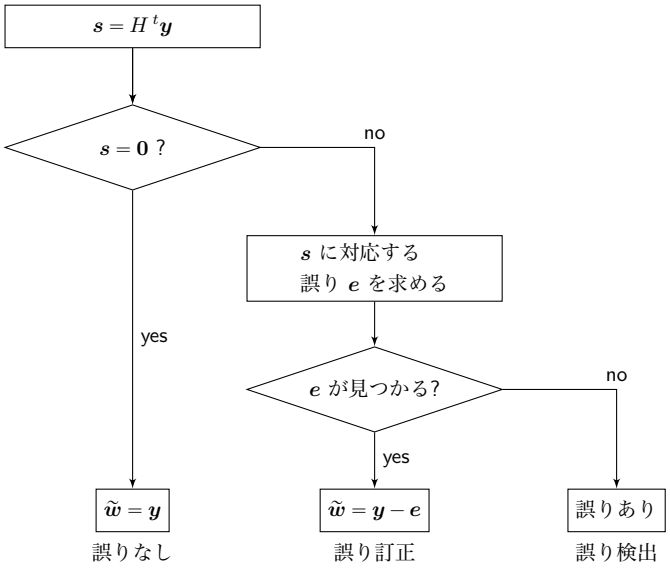
$$E = \{\, \boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \cdots,\ \boldsymbol{e}_L \,\}$$

とすれば, これらに対応する syndrome $\boldsymbol{s}_i = H\,{}^t\boldsymbol{e}_i$ はすべて異つてゐるのである. 従つて, 復号器では, 受信語から syndrome s を計算し, $\boldsymbol{s} = \boldsymbol{0}$ なら誤りなし, $\boldsymbol{s} \neq \boldsymbol{0}$ のときは, $\boldsymbol{s}$ が誤り pattern $\boldsymbol{e}_i$ に対応する syndrome $\boldsymbol{s}_i$ とすると, 誤り $\boldsymbol{e}_i$ が発生したものとして送信語の推定値

$$\widetilde{\boldsymbol{w}} = \boldsymbol{y} - \boldsymbol{e}_i$$

を得る. s が E のどの元とも対応しないときは, 誤りの発生を検出するのみとする.

次の図は, 誤り訂正の flow chart である.



次に, 復号法を代数学の言葉で記述しておく. $C \subset \mathbf{K}^{-n}$ を (n, r) 線形符号とする. C は $(\#\mathbf{K})^r$ 個の符号語を含む. $\mathbf{K}^{-n}$ は Abel 群で, C はその部分群である. そこで, C を法とする $\mathbf{K}^{-n}$ の剰余類分解

$$\mathbf{K}^{-n}/C$$

を考へる. $\mathbf{K}^{-n} \ni \boldsymbol{e}$ を代表元とする剰余類は $\boldsymbol{e} + C$ と表せる. $\mathbf{K}^{-n}/C$ は次の基本的性質をもつ (「代数学 1」参照):

(1) 各類は C と同数個の元を含む;
(2) 任意の 2 つの類は共通部分がないか一致する;
(3) $\mathbf{K}^{-n}$ は剰余類全部の合併集合である;
(4) 剰余類は全部で $(\#\mathbf{K})^{n-r}$ 個ある.

ここで, $\mathbf{K}^{-n}/C \ni K$ の代表元 $\boldsymbol{e}$ を選び

$$K = \boldsymbol{e} + C$$

と表す. この $\boldsymbol{e}$ を K の coset leader[6] と呼ぶ.
通常, 誤り patterns の全体は, その部分集合になつてゐる.

[6] 代数学の言葉では代表元 (representative) である.

いま, coset leaders の全体を

$$\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_L\} \quad (\boldsymbol{e}_i \neq \boldsymbol{0})$$

とする. ここで, $L = (\#\mathbf{K})^{n-r} - 1$ である.

$$C = \{\boldsymbol{w}_1, \cdots, \boldsymbol{w}_M\} \quad (\boldsymbol{w}_1 = \boldsymbol{0},\ M = (\#\mathbf{K})^r)$$

と書くとき, C の 標準配列 とは下記の表うち左の $(L+1) \times M$ の部分のことをいふ.

C	$\boldsymbol{0}\,(=\boldsymbol{w}_1)$	$\boldsymbol{w}_2$	$\cdots$	$\boldsymbol{w}_M$	syndrome
$\boldsymbol{e}_1 + C$	$\boldsymbol{e}_1$	$\boldsymbol{e}_1 + \boldsymbol{w}_2$	$\cdots$	$\boldsymbol{e}_1 + \boldsymbol{w}_M$	$H\,{}^t\boldsymbol{e}_1$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$\boldsymbol{e}_L + C$	$\boldsymbol{e}_L$	$\boldsymbol{e}_L + \boldsymbol{w}_2$	$\cdots$	$\boldsymbol{e}_L + \boldsymbol{w}_M$	$H\,{}^t\boldsymbol{e}_L$

一般には, 標準配列は幾通りもあることに注意せよ.

例 4.7. $(4,2)$ 符号. 検査行列 $H = \begin{bmatrix} 1&0&1&0 \\ 0&1&1&1 \end{bmatrix} \in \mathrm{Mat}(2,4,\mathbb{F}_2)$ から定まる

$$C = \{[0\ 0\ 0\ 0],\ [1\ 1\ 1\ 0],\ [1\ 0\ 1\ 1],\ [0\ 1\ 0\ 1]\}$$

を $(4,2)$ 符号 と呼ぶ. 下の表は C の標準配列の例である. 右端はそれぞれの syndrome を示す.

0 0 0 0	1 1 1 0	1 0 1 1	0 1 0 1	${}^t[0\ 0]$
0 0 0 1	1 1 1 1	1 0 1 0	0 1 0 0	${}^t[0\ 1]$
0 0 1 0	1 1 0 0	1 0 0 1	0 1 1 0	${}^t[1\ 1]$
1 0 0 0	0 1 1 0	0 0 1 1	1 1 0 1	${}^t[1\ 0]$

最左列に $[0\ 1\ 0\ 0]$ がないが, これは, 第 2 行の最右列にあるので, この標準配列においては $[0\ 1\ 0\ 0]$ が誤り pattern に含まれない. 従つて, これは 1 重誤り訂正さへできない符号である. この表が, 3 つの誤り patterns （左端）から, 上で説明した様に構成されてゐることを確かめられたい.

問 4.8. $G = \begin{bmatrix} 1&0&0&1&1&1 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{bmatrix} \in \mathrm{Mat}(3,6,\mathbb{F}_2)$ を生成行列とする線形符号 $C \subset {\mathbb{F}_2}^{-6}$ において, 誤り patterns に, 成分の 1 箇所のみが 1 となるものの全体を含む様な C の標準配列を 1 つ作成せよ. さらに, 各類の syndromes を右端に記入せよ.

さて, coset leaders が復号化の上でどのやうな役割をもつのか. 以下で述べる 4.10 がこれに答へる. その前に 1 つ補題を用意する.

補題 4.9. (n,r) 線形符号 $C \subset \mathbf{K}^{-n}$ の剰余類 $\mathbf{K}^{-n}/C$ から syndrome の全体 $S \subset \mathbf{K}^r$ への次の写像は全単射である:

$$\mathbf{K}^{-n}/C \longrightarrow S, \quad \boldsymbol{e} + C \longmapsto H^t\boldsymbol{e}.$$

証明 $\mathbf{K}^{-n}/C$ の各元 $\boldsymbol{e} + C$ の任意の元 $\boldsymbol{e} + \boldsymbol{w}$ $(\boldsymbol{w} \in C)$ に対し,

$$H\,{}^t(\boldsymbol{e} + \boldsymbol{w}) = H\,({}^t\boldsymbol{e} + {}^t\boldsymbol{w}) = H\,{}^t\boldsymbol{e} + H\,{}^t\boldsymbol{w} = H\,{}^t\boldsymbol{e}.$$

次に $\boldsymbol{e}_i$, $\boldsymbol{e}_j$ を 2 つの類の coset leaders とする. もし, $H\,{}^t\boldsymbol{e}_i = H\,{}^t\boldsymbol{e}_j$ ならば, $H\,{}^t(\boldsymbol{e}_i - \boldsymbol{e}_j) = 0$. 従つて $\boldsymbol{e}_i - \boldsymbol{e}_j \in C$ であり $\boldsymbol{e}_i + C = \boldsymbol{e}_j + C$. つまり類が異なれば syndrome も異なる. □

定理 4.10. 線形符号 $C \subset \mathbf{K}^{-n}$ による剰余類 $\mathbf{K}^{-n}/C$ の各類に Hamming 重さ最小の元が 1 つづつしかないのであれば, それらを標準配列の coset leaders として, 線形符号の最小距離復号法が実現される.

証明 受信語を $\boldsymbol{y}$ とする. $\boldsymbol{y}$ の属する類における重さ最小の元を $\boldsymbol{e}$ とせよ. つまり,

$$\boldsymbol{w}_0 := \boldsymbol{y} - \boldsymbol{e} \in C$$

である. このとき, $\boldsymbol{y}$ とあらゆる $\boldsymbol{w} \in C$ との距離の中で, $d(\boldsymbol{y}, \boldsymbol{w})$ が最小となるのは, $\boldsymbol{w} = \boldsymbol{w}_0$ のときに限ることが次の様にわかる. 実際, すべての $\boldsymbol{w}$ $(\neq \boldsymbol{w}_0)$ に対して, $\boldsymbol{e} + \boldsymbol{w}$ と $\boldsymbol{e}$ は同じ類に入り, また, その類の中では $\boldsymbol{e}$ だけが, 最小の重さ ($\mathrm{wt}(\boldsymbol{e}) = d(\boldsymbol{e}, \boldsymbol{0})$) を与へるのであるから, 3.4 を使つて, 任意の $\boldsymbol{w}$ について,

$$\begin{aligned} d(\boldsymbol{y}, \boldsymbol{w}) &= d(\boldsymbol{w}_0 + \boldsymbol{e}, \boldsymbol{w}) = d(\boldsymbol{e} + \boldsymbol{w}_0 - \boldsymbol{w}, \boldsymbol{0}) \quad (\because 3.4, \mathbf{H1}) \\ &> d(\boldsymbol{e}, \boldsymbol{0}) = d(\boldsymbol{e} + \boldsymbol{w}_0, \boldsymbol{w}_0) \quad (\because 3.4, \mathbf{H1}) \\ &= d(\boldsymbol{y}, \boldsymbol{w}_0). \end{aligned}$$

途中の不等号は $\boldsymbol{e} + \boldsymbol{w}_0 - \boldsymbol{w}$ が $\boldsymbol{e}$ と同一の類の元であつて, $\boldsymbol{e}$ とは異なるからである. 4.9 より, $\boldsymbol{y}$ に対応する syndrome $\boldsymbol{y}^t H$ から, 一意的に類 $\boldsymbol{e} + C$ が定まるが, ここでは, その中の重さが最小の唯一の元として $\boldsymbol{e}$ 自身が得られるから, 結局, 受信語 $\boldsymbol{y}$ に対し, 最小の Hamming 距離にある $\boldsymbol{w}_0 \in C$ は, C の検査行列 H を使つて,

$$\text{syndrome} \quad \boldsymbol{y}^t H \longmapsto \boldsymbol{e} \longmapsto \boldsymbol{w}_0 = \boldsymbol{y} - \boldsymbol{e}$$

として得られる. □

上の結果を, まとめれば次の様に最小距離復号法が実行される :

各類 $\boldsymbol{e} + C$ に Hamming 重さ最小の元が 1 つづつしかないときの復号法 :
(1) 受信語 $\boldsymbol{y}$ に対し, syndrome $H\,{}^t\boldsymbol{y} = \boldsymbol{s}$ を計算する.
(2) syndrome と誤り pattern の対応表より, $\boldsymbol{s}$ に対応する誤り pattern $\boldsymbol{e}$ を求める.
(3) $\boldsymbol{y} - \boldsymbol{e}$ が送信語である.

注意 4.11. 例へば, $n = 30$ のとき 2^{30} 個の元の表の記憶装置が必要になる. syndrome を組み合はせれば, 記憶容量はもつと少なくてすむ :
実際, $C \in {\mathbb{F}_2}^{-30} = V$ を線形符号とし, $\dim C = r$ であれば, syndrome （つまり剰余類 V/C の代表元）の個数は $2^{30}/2^r = 2^{30-r}$ なので, 記憶に必要なのは, 標準配列の第 1 行と第 1 列と syndromes なので $2^r + 2 \times 2^{30-r}$ bit であるから, 2^{30} よりずつと少ない. もし $r = 15$ なら $2^{30} = 1073741824 > 98304 = 2^{15} + 2 \times 2^{30-15}$ となり, 随分と違ふ.

5. 最小重さと検査行列

この節では, 線形符号の最小距離のもつ意味を説明する.

線形符号 C の（Hamming）最小距離 $d(C)$ は, 非零の符号語の Hamming 重さの最小値に等しいのであつた（3.10 を参照）. さて, 線形符号 $C \subset \mathbf{K}^{-n}$ の検査行列 H を列 vectors を使って

$$H = [\, \boldsymbol{h}_1 \ \cdots \ \boldsymbol{h}_n \,]$$

と表すとき, $\boldsymbol{u} = [\, u_1 \ \cdots \ u_n \,]$ が符号語であるためには,

$$u_1 \boldsymbol{h}_1 + \cdots + u_n \boldsymbol{h}_n = \boldsymbol{0}$$

をみたすことが必要十分である. Hamming 距離でなくても同様か.
このとき, 次の定理が成り立つ.

定理 5.1. 距離が与へられた線形符号 $C \subset \mathbf{K}^{-n}$ について, 次の様な C の検査行列 H が存在するとき, かつ, その時に限り $d(C) = d$ である： H の任意の $d-1$ 個の列 vectors が 1 次独立で, d 個の列 vectors で 1 次従属なものが存在する.

証明 以下では検査行列を $H = [\, \boldsymbol{h}_1 \ \cdots \ \boldsymbol{h}_n \,]$ とおく.
（前半）$\{\, \boldsymbol{h}_{i_1}, \ \cdots, \ \boldsymbol{h}_{i_d} \,\}$ は $\mathbf{K}$ 上 1 次従属とする. すなはち, 全部は 0 でない $\mathbf{K}$ の元 c_{i_1}, $\cdots$, c_{i_d} があつて

$$c_{i_1} \boldsymbol{h}_{i_1} + \cdots + c_{i_d} \boldsymbol{h}_{i_d} = \boldsymbol{0}.$$

一方, 任意の $d-1$ 個の列は 1 次独立だから, すべての c_{i_j} $(j = 1, \cdots, d)$ が 0 でない. そこで, c_{i_j} $(j = 1, \cdots, d)$ 以外をすべて 0 とした n 次元 vector

$$\boldsymbol{c} = [\, c_1 \ \cdots \ c_n \,]$$

を考へる. これは, C に属する符号語で, $\mathrm{wt}(\boldsymbol{c}) = d$ である. さらに, 重さが $d-1$ 以下の vector は符号語になり得ない. 従つて, C の最小距離は d である.
（後半）もしも, $\mathbf{K}$ 上 1 次従属な組

$$\{\, \boldsymbol{h}_{i_1}, \ \cdots, \ \boldsymbol{h}_{i_{d-1}} \,\}$$

があつたとすると, 全部は 0 でない $\mathbf{K}$ の元 $a_{i_1}, \cdots, a_{i_{d-1}}$ があつて

$$a_{i_1} \boldsymbol{h}_{i_1} + \cdots + a_{i_{d-1}} \boldsymbol{h}_{i_{d-1}} = \boldsymbol{0}.$$

i_j $(1 \leqq j \leqq d-1)$ 番目が a_{i_j} で, 他はすべて 0 の n 次元の行 vector を $\boldsymbol{a}$ とするとき, $H\,{}^t\boldsymbol{a} = \boldsymbol{0}$ だから $\boldsymbol{a} \in C$. しかし, $\boldsymbol{a}$ の重さ $\mathrm{wt}(\boldsymbol{a}) \leqslant d-1$ で, これは d の最小性に反する.
次に, $\boldsymbol{c} = [\, c_1 \ \cdots \ c_n \,]$ を重さ d の C の元とする. 成分のうち 0 でないものが d 個あるゆゑ, それらを

$$c_{i_1}, \ \cdots, \ c_{i_d}$$

とする. このとき, $H\,{}^t\boldsymbol{c} = \boldsymbol{0}$ だから

$$c_1 \boldsymbol{h}_{i_1} + \cdots + c_{i_d} \boldsymbol{h}_{i_d} = \boldsymbol{0}.$$

従つて, $\{\boldsymbol{h}_{i_1}, \ \cdots, \ \boldsymbol{h}_{i_d}\}$ は 1 次従属である. □

最後に, 線形符号 C の最小距離 $d(C)$ と syndrome による復号の関係を述べる. まづ, 検出の方は $d(C)-1$ 重誤りまで可能であつた. 次に,

$$d(C) \geqq 2t+1$$

となる t を 1 つ固定する. いま $\boldsymbol{e}_i$, $\boldsymbol{e}_j$ を相異なる 2 つの t 重以下の誤り patterns とし, $\boldsymbol{s}_i$, $\boldsymbol{s}_j$ をこれらに対応する syndrome とする:

$$\mathrm{wt}(\boldsymbol{e}_i) \leqq t, \quad \mathrm{wt}(\boldsymbol{e}_j) \leqq t, \quad \boldsymbol{s}_i = H\,{}^t\boldsymbol{e}_i, \quad \boldsymbol{s}_j = H\,{}^t\boldsymbol{e}_j.$$

ここで $\boldsymbol{u} = \boldsymbol{e}_i - \boldsymbol{e}_j$ とおくと, $\boldsymbol{u} \neq \boldsymbol{0}$ で,

$$\mathrm{wt}(\boldsymbol{u}) \leqq \mathrm{wt}(\boldsymbol{e}_i) + \mathrm{wt}(\boldsymbol{e}_j) \leqq 2t < d(C).$$

従つて, $\boldsymbol{u}$ は符号語でない. ゆゑに, $H\,{}^t\boldsymbol{u} \neq \boldsymbol{0}$ である. 一方,

$$H\,{}^t\boldsymbol{u} = H\,{}^t\boldsymbol{e}_i - H\,{}^t\boldsymbol{e}_j = \boldsymbol{s}_i - \boldsymbol{s}_j.$$

よつて, $\boldsymbol{s}_i \neq \boldsymbol{s}_j$. 従つて, 誤り pattern と syndrome は 1 対 1 に対応し (4.9 も参照), 4.2 で述べた通り, t 重誤りの復号が可能であることが再確認された.

ここで, 簡単な線形符号の一般な形について, その能力を見ておく.

例 5.2. 単一 parity 検査符号. $H = [\underbrace{1 \ \cdots \ 1}_{n\text{ 個}}] \in \mathrm{Mat}(1, n, \mathbb{F}_2)$ を検査行列とする $(n, n-1)$ 符号 C は, 方程式

$$x_1 + \cdots + x_n = 0 \mod 2$$

で定義される. $d(C) = 2$ ゆゑ, 単一誤り検出符号である.

例 5.3. 一般 Hamming 符号. 1 から $2^m - 1$ までの整数を m bit の 2 進数で表し, それらを列 vectors とした行列を検査行列 H とする符号 C を考へる. これの階数は m である.

$$H = \begin{bmatrix} 0\,0\,0 \cdots 1\,1 \\ 0\,0\,0 \cdots 1\,1 \\ \vdots\,\vdots\,\vdots \quad \vdots\,\vdots \\ 0\,1\,1 \cdots 1\,1 \\ 1\,0\,1 \cdots 0\,1 \end{bmatrix} \in \mathrm{Mat}(m, 2^m - 1, \mathbb{F}_2).$$

すべての列 vectors が異つてゐるから, どの 2 列も 1 次独立で, $\boldsymbol{h}_1 + \boldsymbol{h}_2 + \boldsymbol{h}_3 = \boldsymbol{0}$ だから, 1 次従属な 3 列がある. ゆゑに, 定理 4.10 から $d(C) = 3$. 従つてこれは, 単一誤り訂正可能な $(2^m - 1,\ 2^m - m - 1)$ 符号である. $m = 3$ のときが, $(7, 4)$ Hamming 符号である.

例 5.4. 拡大 Hamming 符号. 上の 5.3 の H に, 次の様に 1 番下の行と最後の 1 列が付加された行列

$$\widetilde{H} = \begin{bmatrix} 0\,0\,0 \cdots 1\,0 \\ \vdots\,\vdots\,\vdots \quad \vdots\,\vdots \\ 0\,1\,1 \cdots 1\,0 \\ 1\,0\,1 \cdots 1\,0 \\ 1\,1\,1 \cdots 1\,1 \end{bmatrix} \in \mathrm{Mat}(m+1, 2^m, \mathbb{F}_2)$$

を考へる. これの階数は $m+1$ である. $\widetilde{H}$ を検査行列とする符号 $\widetilde{C}$ は $d(\widetilde{C}) = 4$ なる $(2^m,\ 2^m - m - 1)$ 符号で, 1 誤り訂正かつ 2 重誤り検出符号である.

問 5.5. 上の 5.4 において, $d(\widetilde{C}) = 4$ である理由を詳しく述べよ.

演 習 問 題

5.6. $\mathbb{F}_3$ 上の検査行列 H が

$$H = \begin{bmatrix} 0\,1\,1\,2 \\ 1\,0\,2\,2 \end{bmatrix}$$

で与へられた線形符号 C に対し, 次の (1) 〜 (3) に答へよ.

(1) C の最小距離 d を求めよ.

(2) C の生成行列 G および C の符号語をすべて求めよ.

(3) C の標準配列と対応する syndrome を求めよ.

5.7. $\mathbb{F}_{2^2} = \mathbb{F}_2[\alpha] = \{0,\ 1,\ \alpha,\ 1+\alpha\}$（但し $\alpha^2 = 1+\alpha$）上の検査行列

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

で定義される線形符号 C に対し,

(1) C の最小距離 $d(C)$ を求めよ.

(2) C が 1 誤り訂正符号であることを示せ.

(3) C の生成行列を反転簡約化の形で求めよ.

(4) 通報 $[\alpha\ \ 1]$ を符号化せよ.

(5) C が 1 誤り符号であることを踏まへて, 受信語 $[1{+}\alpha\ \ 0\ \ 1\ \ 1{+}\alpha]$ を復号せよ.

6. 巡回符号

6.1. n 対称群の $\mathbf{K}^{-n}$ の作用

群の 作用[7] については既知とする. n 次対称群 を $\mathfrak{S}_n$ で表す. 但し, ここでは $\mathfrak{S}_n$ は $\{0,\ 1,\ 2,\ \cdots,\ n-1\}$ の置換（の全体）とする. このとき

$$\gamma \in \mathfrak{S}_n,\quad \boldsymbol{x} = [\,x_0\ x_1\ \cdots\ x_{n-1}\,] \in \mathbf{K}^{-n}$$

について $\boldsymbol{x}^\gamma$ を γ に応じて, 成分の位置を変更したものと定める :

$$\boldsymbol{x}^\gamma = [\,x_{\gamma^{-1}(0)}\ x_{\gamma^{-1}(1)}\ \cdots\ x_{\gamma^{-1}(n-1)}\,].$$

例へば $\gamma = (1,2,3)$ のとき $[3,-2,5]^\gamma = [5,3,-2]$ である. これにより $(\boldsymbol{x},\,\gamma) \longmapsto \boldsymbol{x}^\gamma$ は $\mathfrak{S}_n$ の $\mathbf{K}^{-n}$ への作用を定める.

問 6.1. 上の定義が $\mathfrak{S}_n$ の $\mathbf{K}^{-n}$ への作用を与へることを確かめよ.

以後, $\sigma = \sigma_n$ は専ら特別な 巡回置換

$$\sigma = \sigma_n = (\,0\ \ 1\ \ \cdots\ \ n{-}1\ \ n{-}2\,) \in \mathfrak{S}_n$$

を表すものとする. 従つて

$$\boldsymbol{x}^\sigma = [\,x_{n-1}\ x_0\ x_1\ \cdots\ x_{n-2}\,] \tag{6.2}$$

また $\gamma \in \mathfrak{S}_n$ と部分集合 $C \in \mathbf{K}^{-n}$ に対し, C^γ を次の様に定める :

$$C^\gamma = \{\,\boldsymbol{c}^\gamma \,|\, \boldsymbol{c} \in C\,\}.$$

6.2. 巡回符号

巡回符号を定義する. 巡回符号は豊かな代数的構造をもつ.

定義 6.3. (1) 線形符号 $C \in \mathbf{K}^{-n}$ が,

$$C^\sigma = C \quad (\,\sigma = \sigma_n\,)$$

をみたすとき, C は 巡回符号 と呼ばれる.

(2) Vector $\boldsymbol{a} = [\,a_0\ a_1\ \cdots\ a_{n-1}\,] \in \mathbf{K}^{-n}$ に対し,

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbf{K}[x]$$

を対応させ, これを vector $\boldsymbol{a}$ の多項式表現といひ $f(x) = \mathrm{rep}(\boldsymbol{c}, x)$ と書くことにする.

例 6.4. いま

$$C = \{\,[0\,0\,0\,0],\ [0\,1\,0\,1],\ [1\,0\,1\,0],\ [1\,1\,1\,1]\,\} = \mathbb{F}_2\cdot[0\,1\,0\,1] + \mathbb{F}_2\cdot[1\,0\,1\,0] \subset {\mathbb{F}_2}^{-4}$$

とおくと, これは巡回符号である. $\dim C = 2$.

例 6.5. また,

$$C = \{\,[0\,0\,0],\ [0\,1\,2],\ [1\,2\,0],\ [2\,0\,1],\ \cdots\} = \mathbb{F}_3\cdot[0\,1\,2] + \mathbb{F}_3\cdot[1\,2\,0] \subset {\mathbb{F}_3}^{-3}$$

とおくと, これは巡回符号である. $\dim C = 2$.

---

[7] 群 G の集合 X への 作用 とは, 次の 2 つの性質 **A1**, **A2** を持つ写像 $X \times G \to X$, $(x,g) \mapsto x^g$ のことである : **A1** 任意の $x \in G$ について $x^{1_G} = x$; **A2** 任意の $x \in G$, 任意の $g, h \in G$ について $(x^g)^h = x^{hg}$. 「代数学 5 及び 6」の text の §26 も参照されたい.

定理 6.6. 線形符号 $C \subset \mathbf{K}^{-n}$ が巡回符号であるためには, C の元の多項式表現を代表元とする $\mathbf{K}[x]/(x^n-1)$ 内の剰余類からなる集合 $J = J(C)$ が $\mathbf{K}[x]/(x^n-1)$ の ideal となることが必要十分である.

証明 x^n-1 は n 次式だから, 剰余環 $\mathbf{K}[x]/(x^n-1)$ の各剰余類の代表元として $n-1$ 次以下の多項式が唯一つ含まれる. 即ち $n-1$ 次式

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$$

の剰余類を $f(x)+(x^n-1)$ で表すとき,

$$\begin{aligned} \mathrm{rep}(\ ,x) : \mathbf{K}^{-n} &\longrightarrow \mathbf{K}[x]/(x^n-1), \\ \boldsymbol{a} = [\,a_0\ a_1\ \cdots\ a_{n-1}\,] &\longmapsto \mathrm{rep}(\boldsymbol{a},x)+(x^n-1) \end{aligned}$$

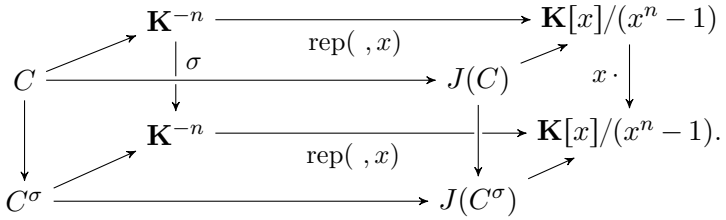
なる対応によつて $\mathbf{K}^{-n}$ と $\mathbf{K}[x]/(x^n-1)$ とが 1 対 1 に対応する. もつと詳しく, 両者は $\mathbf{K}$ 上の vector 空間として同型である. ここで

$$\begin{aligned} xf(x) &= a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n \\ &= a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}(x^n-1) \end{aligned}$$

であるから,

$$\mathrm{rep}(\boldsymbol{a}^\sigma, x) + (x^n-1) = x\,\mathrm{rep}(\boldsymbol{a},x) + (x^n-1) \tag{6.7}$$

が成り立つ. これは次の図式が可換であるといふことである :



ここで (6.7) を繰り返へせば, $\nu = 0,\ 1,\ \cdots$ に対し

$$\mathrm{rep}(\boldsymbol{a}^{\sigma^\nu}, x) + (x^n-1) = x^\nu\,\mathrm{rep}(\boldsymbol{a},x) + (x^n-1).$$

(必要性) $f(x)+(x^n-1) \in J$ を任意にとる. ある $\boldsymbol{c} \in C$ により $f(x) = \mathrm{rep}(\boldsymbol{c},x)$ と書ける. C が巡回符号であるから, $\nu = 0,\ 1,\ 2,\ \cdots$ について $\boldsymbol{c}^\nu \in C$ であるから (6.7) により

$$x^\nu f(x) + (x^n-1) = \mathrm{rep}(\boldsymbol{c}^{\sigma^\nu}, x) + (x^n-1) \in J.$$

C は線形符号なので, J は $\mathbf{K}[x]/(x^n-1)$ の $\mathbf{K}$ 上の vector 空間としての部分空間であり, 任意の $p(x) \in \mathbf{K}[x]$ は x^ν $(\nu = 1,\ 2,\ \cdots)$ の $\mathbf{K}$ 上の線形和なので,

$$\big(p(x)+(x^n-1)\big)\big(f(x)+(x^n-1)\big) = p(x)f(x) + (x^n-1) \in J.$$

よつて, J は $\mathbf{K}[x]/(x^n-1)$ の ideal である.
(十分性) 符号語 $\boldsymbol{c} \in C$ の多項式表現 $\mathrm{rep}(\boldsymbol{c},x)$ について $\mathrm{rep}(\boldsymbol{c},x)+(x^n-1) \in J$ であるが, J は $\mathbf{K}[x]/(x^n-1)$ の ideal であるから (6.7) を使つて

$$\begin{aligned} J \ni \big(x+(x^n-1)\big)\big(\mathrm{rep}(\boldsymbol{c},x)+(x^n-1)\big) \\ = x\,\mathrm{rep}(\boldsymbol{c},x) + (x^n-1) = \mathrm{rep}(\boldsymbol{c}^\sigma, x) + (x^n-1). \end{aligned}$$

ゆゑに J の定義により $\boldsymbol{c}^\sigma \in C$. よつて C は巡回符号である. □

さて, 巡回符号の構成に関しては次の定理が基礎になる.

定理 6.8. 単項 ideal 整域（PID）の（ideal による）剰余環は単項 ideal 環（一般には整域でなくなる）である. 特に, 環 $\mathbf{K}[x]/(x^n-1)$ は単項 ideal 環である. それゆゑ, 巡回符号 C に対して, $J(C)$ は $g(x)|(x^n-1)$ なる, ある $g(x)\in\mathbf{K}[x]$ により $J(C)=g(x)\mathbf{K}[x]/(x^n-1)$ と書かれる. このとき,

$$\dim C = n-\deg g$$

で, $g(x)$ は C の生成多項式と呼ばれる.

証明 ここでは, 第 2 の主張のみ証明しておけば十分であらう. いま I を $\mathbf{K}[x]/(x^n-1)$ の任意の ideal とせよ. I の $\mathbf{K}[x]$ への引き戻しを $\tilde{I}$ と記す. $\tilde{I}$ が $\mathbf{K}[x]$ の ideal であることは容易にわかる. もちろん $\tilde{I}\supset(x^n-1)$ であるが, $\mathbf{K}[x]$ が単項 ideal 整域（PID）であるから, ある $g(x)\in\mathbf{K}[x]$ によつて $\tilde{I}=(g(x))$ と書かれる. このとき $g(x)|(x^n-1)$ を満たす. つまり,

$$I = g(x)\,\mathbf{K}[x]/(x^n-1)$$

となつてゐて, これは単項 ideal である. いま, $\deg g = n-k$ とおくと, 明らかに $J(C)=\{\,\varphi(x)g(x)\,|\,\deg\varphi\leqslant k-1\,\}$ であるから, $J(C)$ の $\mathbf{K}$ 上の基底として,

$$\{\,g(x),\ xg(x),\ \cdots,\ x^{k-1}g(x)\,\}$$

がとれる. 実際, これらは $J(C)$ を $\mathbf{K}$ 上生成するし, 1 次独立であることも簡単にわかるから, $\dim C = k = n-\deg g$ である. □

注意 6.9. 上の証明の記号の下で, I から $\tilde{I}$ の生成元を求めるには次の様にすればよい. 即ち, $\mathbf{K}[x]$ は Euclid 環であることに注意すると, I の生成集合（有限個とする）がわかつてゐれば, 互除法により, $\tilde{I}$ の生成元を求めることができる. 実際, $I=(g_1(x),\cdots g_m(x))\subset\mathbf{K}[x]/(x^n-1)$ に対して, $\mathbf{K}[x]$ において

$$g(x)=\gcd(g_1(x),\cdots g_m(x),\,x^n-1)$$

を互除法で求めることができるが, このとき $g(x)|(x^n-1)$ で $\tilde{I}=(g(x))$ である.

例 6.10. $f(x)=1+x+x^5$ とし, $I=f(x)\,\mathbb{F}_2[x]/(x^{12}-1)$ を考へる. このとき, 互除法を使つて, $\mathbb{F}_2[x]$ において $\gcd(f(x),x^{12}-1)=1+x+x^2$ がわかる. 従つて,

$$\tilde{I}=(1+x+x^2)\subset\mathbb{F}_2[x]$$

であり, $I=J(C)$ となる巡回符号 C は

$$\begin{aligned}C=\{&[0\,0\,0\,0\,0\,\cdots\,0],\ [1\,1\,1\,0\,0\,\cdots\,0],\ [0\,1\,1\,1\,0\,\cdots\,0],\\ &\cdots,\ [0\,\cdots 0\,1\,1\,1],\ [1\,0\,\cdots 0\,1\,1],\ [1\,1\,0\,\cdots 0\,1]\}\subset{\mathbb{F}_2}^{-12}\end{aligned}$$

で $\dim C=9$ であることは, 以下の説明で示される.

生成行列と検査行列 巡回符号 C について, 上の様に $g(x)|(x^n-1)$ なる $g(x)\in\mathbf{K}[x]$ により, $J(C)=g(x)\,\mathbf{K}[x]/(x^n-1)$ となつてゐるとする. $\deg g\leqslant n-1$ だから,

$$g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}\quad(g_{n-k}\neq 0)$$

とする. 上の 6.8 の証明で述べた通り, $J(C)$ の $\mathbf{K}$ 上の基底として,

$$\{\,g(x),\ xg(x),\ \cdots,\ x^{k-1}g(x)\,\}$$

がとれるから, 基底の各多項式を vectors に表現して, C の生成行列 G を得る :

$$G=\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \ddots & & & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}\in\mathrm{Mat}(k,n,\mathbf{K}). \tag{6.11}$$

ここで $g_{n-k}\neq 0$ ゆゑ $\operatorname{rank}G=k$ なので, $\dim C=k$ でなくてはならない. 上の記号で

$$h(x)=\frac{x^n-1}{g(x)}=h_0+h_1x+\cdots+h_kx^k$$

とおき, H を次のやうに定義する :

$$H=\begin{bmatrix} & & & h_k & \cdots & h_1 & h_0 \\ & & h_k & \cdots & h_1 & h_0 & \\ & \iddots & & & \iddots & & \\ h_k & \cdots & h_1 & h_0 & & & \\ & & & & & & \end{bmatrix}\in\mathrm{Mat}(n-k,n,\mathbf{K}). \tag{6.12}$$

このとき, $H\,{}^tG=O$ が成り立つ. 実際, G の第 j 行と H の第 i 行の内積は, $h(x)g(x)=x^n-1$ の $\mathbf{K}[x]/(x^n-1)$ での $x^{n-i-j+1}$ の係数に一致するが, それは 0 である. また $h(x)g(x)=x^n-1$ の x^n の係数は $1=h_kg_{n-k}$ で, 定数項 は $h_0g_0=-1$ ゆゑ, h_k, h_0, g_0 は（もちろん g_{n-k} も）0 でない. 従つて, $\operatorname{rank}H=n-k$ である. よつて, H は C の検査行列になる.

問 6.13. どんな巡回符号 C も, $\mathbf{0}$ でないある $\boldsymbol{c}\in C$ から σ の作用を繰り返して得られる符号語で生成される. 即ち, 巡回符号 $C\subset\mathbf{K}^{-n}$ が $\dim C=k$ とすれば

$$C=\langle\,\boldsymbol{c}^{\sigma^j}\mid 0\leqslant j\leqslant k-1\,\rangle=\mathbf{K}\,\boldsymbol{c}+\mathbf{K}\,\boldsymbol{c}^{\sigma}+\mathbf{K}\,\boldsymbol{c}^{\sigma^2}+\cdots+\mathbf{K}\,\boldsymbol{c}^{\sigma^{k-1}}$$

と書ける. これを示せ. (Hint : (6.11) の G の第 1 行が $\boldsymbol{c}$ である.)

問 6.14. (6.11) の H と (6.12) の G について, $H\,{}^tG=O$ を確かめよ.

定義 - 命題 6.15. 多項式 $g(x)\in\mathbf{K}[x]$ が x^n-1 を割り切り, $\ell<n$ をみたすすべての ℓ に対して $x^\ell-1$ は割り切らないとき, n を $g(x)$ の周期といふ. 体 $\mathbf{K}$ が有限体であれば, いかなる $g(x)\in\mathbf{K}[x]$ も（有限の）周期を有する.

証明 （ここでは「代数学 1」の定理 13.5 や「代数学 5 及び 6」の §17 は既知としてゐる.）$\mathbf{K}$ が q 元体 $\mathbb{F}_q$ （q はある素数 p の冪）であるとし, $\deg g(x)=m$ とする. $g(x)$ が $\mathbf{K}$ 上既約であれば, $g(x)$ の最小分解体は $\mathbb{F}_{q^m}$ （$\mathbb{F}_q$ の m 次拡大）である. ${\mathbb{F}_q}^\times$ は q^m-1 次巡回群（「代数学 1」, 定理 13.5）であるから, $g(x)=0$ の根は $x^{q^m-1}-1=0$ の根である. どちらも分離的な多項式なので, $g(x)|(x^{q^m-1}-1)$ である. $g(x)$ が既約でない場合は, 次の様にすればよい. $g_1(x)$ と $g_2(x)$ が互ひに素であつて, $g_1(x)|(x^{n_1}-1)$ で $g_2(x)|(x^{n_2}-1)$ とする. $(x^{n_1}-1)|(x^{n_1n_2}-1)$, $(x^{n_2}-1)|(x^{n_1n_2}-1)$ であるから,

$$g_1(x)g_2(x)|(x^{n_1n_2}-1)$$

である. また, 重根を持つ場合は, p の適当な冪乗 p^M をとり, $(x^{q^m-1}-1)$ の p^M 乗

$$(x^{q^m-1}-1)^{p^M}=x^{(q^m-1)p^M}-1 \qquad \text{（標数が } p \text{ であることに注意）}$$

を考へればよい. 以上により, 任意の $g(x)$ に対して, $n\in\mathbb{N}$ が存在して $g(x)|x^n-1$ である. その様な最小の n が存在することは明らかである. □

例 6.16. $(7,4)$ 巡回符号をとりあげる. $g(x)=1+x+x^3\in\mathbb{F}_2[x]$ は $\mathbb{F}_2$ 上で既約である. 従つてこれの周期は $2^3-1=7$ である（以下の 6.17）. この $g(x)$ を生成多項式とする巡回符号 C の多項式表現 $J(C)$ の基底 $\{\,g(x),\,xg(x),\,x^2g(x),\,x^3g(x)\,\}$ の vectors による表現から得られる C の生成行列 G は

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

C の各元の多項式表現は,

$$J(C)=g(x)\,\mathbb{F}_2[x]/(x^7-1)=\mathbb{F}_2\,g(x)+\mathbb{F}_2\,g(x)x+\mathbb{F}_2\,g(x)x^2+\mathbb{F}_2\,g(x)x^3.$$

最後に, この巡回符号 C が $(7,4)$ Hamming 符号と同値であることもわかる.

問 6.17. 例 6.16 の巡回符号 C について, 次の問に答へよ.

(1) $g(x)\,|\,(x^7-1)$ を示すと同時に $h(x)=\dfrac{x^7-1}{g(x)}\in\mathbb{F}_2[x]$ を求めよ.
(2) C の検査行列 $H\in\mathrm{Mat}(3,7,\mathbb{F}_2)$ を (6.12) の様に求めよ.
(3) C が $(7,4)$ Hamming 符号と同値であることを確かめよ.

注意 6.18. 通常は $g(x)$ が周期 n の生成多項式で $n|N$ ならば 6.6 より, $J(C)\subset\mathbf{K}[x]/(x^N-1)$ なる巡回符号が存在するが, 実用上は, 生成多項式 $g(x)$ は $\mathbf{K}[x]/(x^n-1)$ の元とするのが普通である. さらに 6.8 に基き, n が $g(x)$ の周期であらうとなからうと, $g(x)|(x^n-1)$ である限り,

$$h(x)=\frac{x^n-1}{g(x)}$$

を C の <u>検査多項式</u> と呼ぶ.

命題 6.19. 巡回符号の双対符号は巡回符号である.

証明 $g(x)$ と $h(x)$ の役割りが完全に入れ代はるだけなので, ほとんど明らかである. □

例 6.20. $J(C)=(x-1)\mathbb{F}_2[x]/(x^n-1)$ なる C 巡回符号を考へる.

$$J(C)=\{\,1-x,\ x-x^2,\ x^2-x^3,\ \cdots,\ x^{n-2}-x^{n-1}\,\}$$

であり, 生成行列 G は

$$G=\begin{bmatrix}1&1&0&0&\cdots&0&0&0&0\\0&1&1&0&\cdots&0&0&0&0\\0&0&1&1&\cdots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\cdots&0&1&1&0\\0&0&0&0&\cdots&0&0&1&1\end{bmatrix}\in\mathrm{Mat}(n-1,n,\mathbb{F}_2).$$

また検査多項式は $h(x)=\dfrac{x^n-1}{x-1}=1+x+x^2+\cdots+x^{n-1}$ なので, 検査行列 H は

$$H=[\,1\ 1\ \cdots 1\,]\in\mathrm{Mat}(1,n,\mathbb{F}_2).$$

ゆゑに 5.1（の証明）により, 最小距離は $d(C)=2$ である.

例題 6.21. 環 $\mathbb{F}_3[x]/(x^{11}-1)$ の ideals をすべて求めよ.
解答 $x^{11}-1$ を $\mathbb{F}_3[x]$ で因数分解すれば

$$x^{11}-1=(2+x)(2+2x+x^2+2x^3+x^5)(2+x^2+2x^3+x^4+x^5).$$

よつて,

$$0,\ \ 1,\ \ 2+x,\ \ 2+2x+x^2+2x^3+x^5,\ \ 2+x^2+2x^3+x^4+x^5$$

のそれぞれを生成元とする 5 つの ideals と, 後ろの 3 つうち異なる 2 つを選んで掛けたものを含めた合計 8 個が求めるすべてである. □

例題 6.22. 次の行列 G を生成行列とする線形符号は巡回符号であるか :

$$G=\begin{bmatrix}1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\end{bmatrix}\in \mathrm{Mat}(3,5,\mathbb{F}_2).$$

解答 巡回符号であるならば $(1+x^2)|(x^5-1)$ であるが, 除法を実行すれば, 余り $1+x$ を得る. ゆゑに, これは巡回符号を与へない. 実際, $[10100]+[01010]=[11110]$ を σ^{-1} で写した $[11101]$ を 3 つの列 vectors の 1 次結合で表すことはできない. □

例題 6.23. 次の行列 G を生成行列とする線形符号は巡回符号であるか :

$$G=\begin{bmatrix}2&2&1&2&0&1&0&0&0&0&0\\0&2&2&1&2&0&1&0&0&0&0\\0&0&2&2&1&2&0&1&0&0&0\\0&0&0&2&2&1&2&0&1&0&0\\0&0&0&0&2&2&1&2&0&1&0\\0&0&0&0&0&2&2&1&2&0&1\end{bmatrix}\in \mathrm{Mat}(6,11,\mathbb{F}_3).$$

解答 行列 G から読みとれる多項式 $g(x)=2+2x+x^2+2x^3+x^5$ について $g(x)|(x^{11}-1)$ であれば, これは $g(x)$ を生成多項式とする巡回符号であるが, 実際, 除法を実行すれば, $(x^{11}-1)/(2+2x+x^2+2x^3+x^5)=1+2x+2x^2+2x^3+x^4+x^6$ となり, 割り切れるから, これは巡回符号を与へる.
補足として, 例へば, 第 1 列と第 2 列の和 $[2\,1\,0\,0\,2\,1\,1\,0\,0\,0\,0]$ を σ^{-1} で写したものは

$$[1\,0\,0\,2\,1\,1\,0\,0\,0\,0\,2]=2\boldsymbol{g}_0+\boldsymbol{g}_1+\boldsymbol{g}_2+2\boldsymbol{g}_3+2\boldsymbol{g}_5 \tag{6.24}$$

となる. 但し $\boldsymbol{g}_i$ は G の第 $(i+1)$ 列を表す. これの計算は次の通り. 符号語を σ^{-1} で写すことは x^{10} を掛けることに他ならないから, $x^{10}(g(x)+x\,g(x))$ を $g(x),\, x\,g(x),\ \cdots,\ x^5g(x)$ の 1 次結合で表はせばよい.

$$h(x)=\frac{x^{11}-1}{g(x)}=1+2x+2x^2+2x^3+x^4+x^6\quad\text{(検査多項式)}$$
$$x^{10}=h(x)(2+x+2x^2+x^4)+1+x+x^2+2x^3+2x^5\quad(x^{10}\text{ の }h(x)\text{ による除算})$$

以下は $(x^{11}-1)$ を法としての計算である :

$$\begin{aligned}x^{10}(g(x)+x\,g(x))&=x^{10}\,g(x)+x^{11}\,g(x)=x^{10}\,g(x)+g(x)\\&=(1+x+x^2+2x^3+2x^5)g(x)+g(x)\\&=(2+x+x^2+2x^3+2x^5)g(x).\end{aligned}$$

これの係数から (6.24) が得られる. □

例 6.25. $f(x)=1+x^3+x^{63}$ について $I=f(x)\,\mathbb{F}_2[x]/(x^{127}-1)$ を考へる. まづ

$$\gcd(f(x),\ x^{127}-1)=1+x+x^7\quad(=g(x)\ \text{とおく})$$

であるから, 自然な写像 $\mathbb{F}_2[x]\to\mathbb{F}_2[x]/(x^{127}-1)$ に関する I の引き戻し $\tilde{I}$ は $\tilde{I}=(g(x))$ である. 一方, $g(x)$ の周期が 127 であることは pari/gp 等で確認できる. $f(x)\in\mathbb{F}_2[x]/(x^{127}-1)$ を生成多項式とする符号を C とする. C の検査多項式は

$$\begin{aligned}h(x)=\frac{x^{127}-1}{g(x)}=1&+x+x^2+x^3+x^4+x^5+x^6+x^8+x^{10}+x^{12}+x^{15}+x^{16}+x^{19}\\&+x^{20}+x^{21}+x^{23}+x^{24}+x^{25}+x^{27}+x^{30}+x^{32}+x^{33}+x^{37}+x^{38}\\&+x^{40}+x^{41}+x^{42}+x^{43}+x^{45}+x^{46}+x^{48}+x^{50}+x^{51}+x^{53}+x^{54}\\&+x^{57}+x^{60}+x^{64}+x^{65}+x^{66}+x^{71}+x^{73}+x^{74}+x^{75}+x^{76}+x^{77}\\&+x^{80}+x^{82}+x^{84}+x^{85}+x^{86}+x^{89}+x^{90}+x^{92}+x^{96}+x^{99}+x^{100}\\&+x^{101}+x^{102}+x^{106}+x^{108}+x^{113}+x^{114}+x^{120}\end{aligned}$$

である. 以上で $J(C)=I$ となる巡回符号 $C\subset\mathbb{K}^{-127}$ が得られた. その次元は $\dim C=\deg h(x)=120$ である. C の最小距離（Hamming 重みの最小値）d は $d\leqslant 5$ であることは pari/GP によつて確かめた. 実際 $d=5$ である様に思はれる（check する方法はないか）.

問 6.26. $\mathbb{F}_3[x]/(x^{13}-1)$ の ideals を全て求めよ.
（ここでは pari/GP, paridroid（など computer）による計算を行つてよい.）

問 6.27. $g(x)=1+x^2+x^5+x^6\in\mathbb{F}_3[x]$ は周期 13 の多項式である.[8)]
これの生成する巡回符号 $C\subset{\mathbb{F}_3}^{-13}$, 即ち

$$\mathbb{F}_3\,g(x)+\mathbb{F}_3\,xg(x)+\cdots+\mathbb{F}_3\,x^6g(x)$$

の係数を昇冪の順に拾つてできる ${\mathbb{F}_3}^{-13}$ 内の vectors の全体のなす部分空間, について以下に答へよ.
(1) C の検査多項式 $h(x)$ を求めよ.
(2) $\boldsymbol{u}=[1\,2\,0\,0\,1\,2\,0\,1\,1\,0\,2\,1\,1]$ は符号語であるか否か. 理由を付けて答えよ.
(3) $\boldsymbol{v}=[2\,2\,0\,0\,1\,2\,0\,1\,1\,0\,2\,1\,1]$ は符号語であるか否か. 理由を付けて答えよ.
(4) C の生成行列 G を (6.11) の様に定め, それを

$$G=\begin{bmatrix}\boldsymbol{g}_0\\ \boldsymbol{g}_1\\ \vdots\\ \boldsymbol{g}_6\end{bmatrix}\tag{6.28}$$

とおく. このとき $\boldsymbol{g}_1+{\boldsymbol{g}_3}^{\sigma^2}$ を $\boldsymbol{g}_0,\cdots,\boldsymbol{g}_6$ の 1 次結合で表せ.

演 習 問 題

6.29. $f(x)=1+x^2+x^3+x^4\in\mathbb{F}_2[x]$ で生成される $(9,4)$ 符号 $C\subset{\mathbb{F}_2}^{-9}$ の生成行列と検査行列を求めよ. また, $[1\,1\,0\,1\,1\,0\,1\,1\,1]$ が符号語であるかどうかを, 検査行列を用ゐて決定せよ.

[8)] つまり $g(x)\,|\,x^n-1$ となる最小の自然数 n は 13.

6.3. 巡回符号の構成

理論上の構成法. いま C を周期 n 生成多項式 $g(x)\in\mathbf{K}[x]$ に対応する巡回符号とし, $\deg g = n-k$ とする. 即ち $J(C)=g(x)\,\mathbf{K}[x]/(x^n-1)$ であるとする. このもとで, k bit の情報列 $\boldsymbol{a}=[\,a_0\ a_1\ \cdots\ a_{k-1}\,]$ を符号化するには,

$$(a_0+a_1x+\cdots+a_{k-1}x^{k-1})\,g(x)$$

の係数を拾ひ出せばよい. しかし, 実用上は例 6.30 の次に説明する方法が取られる.

例 6.30. 6.16 の巡回符号（$(7,4)$ Hamming 符号）について, $\boldsymbol{a}=[\,1\ 0\ 1\ 1\,]$ の符号化は, その多項式表現 $a(x)=1+x^2+x^3$ と $g(x)$ の積

$$a(x)g(x)=(1+x^2+x^3)(1+x+x^3)=1+x+x^2+x^3+x^4+x^5+x^6$$

の係数から $[\,1\,1\,1\,1\,1\,1\,1\,]$ となる. 実際, 6.16 の G について, $\boldsymbol{a}G=[\,1\,1\,1\,1\,1\,1\,1\,]$ である.

実用を考慮した構成法. 実用のためには組織符号（2.32 を見よ.）の形にしたいので, 以下の様な工夫をする. ここでも上で述べた, 周期 n の生成多項式 $g(x)\in\mathbf{K}[x]$ から得られる $J(C)=g(x)\,\mathbf{K}[x]$ なる巡回符号 C を考へる. まづ,

$$a(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$$

とおく. これを $\boldsymbol{a}=[\,a_0\ a_1\ a_2\ \cdots\ a_{k-1}\,]$ の情報多項式ともいふ. ここで,

$$x^{n-k}a(x)=a_0x^{n-k}+a_1x^{n-k+1}+\cdots+a_{k-1}x^{n-1}$$

を $g(x)$ で割り, 余り $r(x)$ を求め,

$$-r(x)=c_0+c_1x+\cdots+c_{n-k-1}x^{n-k-1}$$

とおく. さらに, $u(x)$ を次で定義する :

$$\begin{aligned}u(x)&=x^{n-k}a(x)-r(x)\\&=c_0+c_1x+\cdots+c_{n-k-1}x^{n-k-1}+a_0x^{n-k}+a_1x^{n-k+1}+\cdots+a_{k-1}x^{n-1}.\end{aligned}$$

$u(x)$ は $g(x)$ で割り切れるから符号多項式, つまり $u(x)\in J(C)$. そこで $\boldsymbol{a}$ に対応する符号語を

$$\boldsymbol{c}=[\,c_0\ c_1\ \cdots\ c_{n-k-1}\ a_0\ \cdots\ a_{k-1}\,]$$

と定めればよい. これは, 右側に k bit の情報列が付いた形をしてゐる. この様に, 使用する任意の情報列がそのまま, それに対応する符号語の一部（通常は右詰め）になつてゐるとき, その符号を組織符号と呼ぶのであつた.

例 6.31. $g(x)=x^3+x+1\in\mathbb{F}_2[x]$ を生成多項式とする $(7,4)$ 巡回 Hamming 符号の符号化をしてみる. 例へば, 情報列 $[\,1011\,]$ を符号化する.

$$a(x)=1+x^2+x^3,\quad x^3a(x)=x^3+x^5+x^6.$$

$x^3a(x)$ を $g(x)$ で割つた余り $r(x)=1$. 従つて,

$$u(x)=x^3a(x)+1=1+x^3+x^5+x^6.$$
$$\therefore\ \boldsymbol{c}=[\,1\,0\,0\,|\,1\,0\,1\,1\,].$$

この例からもわかるやうに, 符号化のためには多項式の割り算が必要である. 割り算回路には (直列型) shift register（シフトレジスタ）が使はれる. これにより, 比較的容易に符号器, 復号器が構成できる.

6.4. Shift register

基本的な演算素子として, 2 を法とする加算器（2 元加算器）や単位時間遅延素子 D （略して D 素子 と呼ぶ）などがある. D は, $\mathbb{F}_2$ の元を入力に対しては 1 bit のみの記憶素子であるが, 一般の $\mathbb{F}_q$ の元を入力に対しては q 種類以上の値を記憶できるものとする. 巡回符号 C の次元を k としたとき, 大まかに云つて k 個の D 素子を直列につないだ基本回路を shift register（シフトレジスタ）といふ. これの利用方法を以下に例で説明する[9].

例 6.32. 例 6.31 では $n=7$, $k=4$ で, 生成多項式は $g(x)=1+x+x^3$, 検査多項式は

$$h(x)=\frac{x^7-1}{1+x+x^3}=1+x+x^2+x^4\ \in\mathbb{F}_2[x]$$

である. 一般に, 多項式

$$f(x)=f_0+f_1x+f_2x^2+\cdots+f_5x^5+f_6x^6\in\mathbb{F}_2[x]/(x^7-1)$$

について, $\mathbb{F}_2[x]/(x^7-1)$ において $f(x)h(x)=0$ であることは, 生成行列 (6.11) と検査行列 (6.12) について (6.12) の直後に述べた関係 $H^tG=O$ と同値である. つまり $h(x)$ の係数を降冪順に成分とする vector $\boldsymbol{h}=[\,1\ 0\ 1\ 1\ 1\,]$ と $f(x)$ の係数を昇冪順に並べた vector $\boldsymbol{f}=[\,f_0\ f_1\ \cdots f_5\ f_6\,]$ の任意の連続した 5 項からなる vector との内積がどれも 0 であることと $\boldsymbol{f}\in C$ であることが同値である. 以上をまとめると $\mathbb{F}_2[x]/(x^7-1)$ において,

$$\begin{aligned} f(x)\in J(C)&\iff f(x)h(x)=0\\ &\iff f_j+f_{j+2}+f_{j+3}+f_{j+4}=0\ \ (0\leqslant\forall j\leqslant 2)\\ &\iff f_j=-f_{j+2}-f_{j+3}-f_{j+4}\ \ (0\leqslant\forall j\leqslant 2). \end{aligned}\tag{6.33}$$

このことより, f_3, f_4, f_5, f_6 が任意に与へられたとき, 残りの f_0, f_1, f_2 を $\boldsymbol{f}\in C$ となる様に与へることができて, しかもその様な $\boldsymbol{f}$ は唯一つであることがわかる.

以上の事実を利用すると, 6.30 で述べた組織符号の構成を以下の様に実装することができる. 即ち, 与へられた情報多項式

$$a(x)=a_0+a_1x+a_2x^2+a_3x^3\in\mathbb{F}_2[x]$$

について $-r(x)=c_0+c_1x+c_2x^2$ を見付けて

$$\begin{gathered} -r(x)+x^3\,a(x)=c_0+c_1x+c_2x^2+a_0x^3+a_1x^4+a_2x^5+a_3x^6\\ \in g(x)\,\mathbb{F}_2[x]/(x^7-1),\\ [\,c_0\ c_1\ c_2\ a_0\ a_1\ a_2\ a_3\,]\in C \end{gathered}$$

となる様にすることができる. ここで上の $f(x)$ として $-r(x)+x^3\,a(x)$ をとれば,

$$\begin{aligned} c_2&=\quad\ a_1+a_2+a_3,\\ c_1&=\quad a_0+a_1+a_2,\\ c_0&=c_2+a_0+a_1 \end{aligned}\tag{6.34}$$

として c_2, c_1, c_0 が計算される.

[9] [Im], §5.2.4 に基く.

以上の方法を 6.31 の場合に実装すると次の様になる. 4 個の単位時間遅延素子 D 素子と 2 個の 2 元加算器を使つた以下の回路（shift register）を用意する.

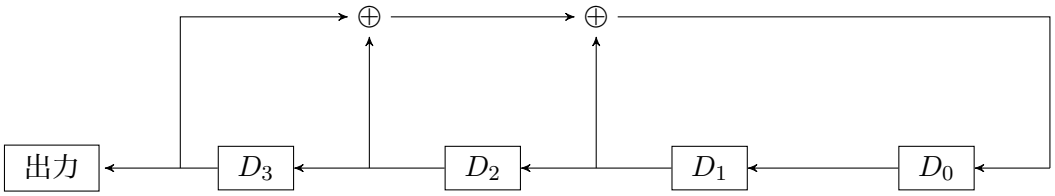


図 6.35 Shift register

これを使つて,

$$a(x) = a_0 + a_1x + a_2x^2 + a_3x^3 = 1 + x^2 + x^3$$

に対応する情報列 $[1\,0\,1\,1]$ の符号化を実行すると以下の様になる. まづ, shift register D_3, D_2, D_1, D_0, の内容をすべて 0 にする. そしてこれらのそれぞれに a_3, a_2, a_1, a_0 を同期させて入力する. いま D_3, D_2, D_1, D_0 の記憶をそれぞれ d_3, d_2, d_1, d_0 としたとき,

$$d_3,\ d_2,\ d_1,\ d_0 \longrightarrow d_2,\ d_1,\ d_0,\ d_1 + d_2 + d_3$$

といふ手順を繰り返へし行ひつつ D_3 の記憶を出力させていく. その結果, 下表の出力欄の最下行の左欄を逆順に並べて, 情報列 $[1\,0\,1\,1]$ の符号化 $[1\,0\,0|1\,0\,1\,1]$ が得られる.

D_3 からの出力							D_3	D_2	D_1	D_0	時間
							1	1	0	1	0
						1	1	0	1	0	1
					1	1	0	1	0	0	2
				1	1	0	1	0	0	1	3
			1	1	0	1	0	0	1	1	4
		1	1	0	1	0	0	1	1	1	5
	1	1	0	1	0	0	1	1	1	0	6
1	1	0	1	0	0	1	1	1	0	1	7

表 6.36 Shift register

得られた $[1\,0\,0|1\,0\,1\,1]$ の左側の $[1\,0\,0]$ は $-r(x)$ の係数を昇冪順に並べたものになつてゐて, $r(x) = 1$ を得る.

問 6.37. 6.16 の $(7, 4)$ 巡回符号 C に関して以下に答へよ.

(1) 6.31 とその直前で説明した手順に沿つて多項式

$$a(x) = x + x^2 + x^3 \in \mathbb{F}_2[x]/(x^7 - 1)$$

を情報多項式とする $\boldsymbol{a} = [0\,1\,1\,1] \in {\mathbb{F}_2}^{-4}$ の符号化を組織符号の形で符号化せよ. その際, 6.36 と同様な表も作成せよ.

(2) 上の (1) で得られた組織符号を $[c_0\ c_1\ c_2\,|0\ 1\ 1\ 1]$ としたとき, $x^3a(x)$ を生成多項式 $g(x) = 1 + x + x^3$ によつて除した余りが $r(x) = c_0 + c_1x + c_2x^2$ であることを直接計算で確かめよ.

演 習 問 題

6.38. 多項式 $g(x) = 2 + 2x + 2x^3 + x^4 \in \mathbb{F}_3[x]$ の周期は 8 である. これを既知とした上で $\mathbb{F}_3[x]/(x^8 - 1)$ の ideal $g(x)\,\mathbb{F}_3[x]/(x^8 - 1)$ に対応する巡回置換 $C \subset {\mathbb{F}_3}^{-8}$ について答へよ.

(1) 検査多項式 $h(x) = (x^8 - 1)/g(x)$ を求めよ.

(2) 多項式 $f(x) = f_0 + f_1\,x + f_2\,x^2 + \cdots + f_6\,x^6 + f_7\,x^7 \in \mathbb{F}_3[x]$ が $J(C)$ に属すことと同値な (6.33) に相当する $\{f_j \mid j = 0, \cdots, 7\}$ の関係式（漸化式）を作れ.

(3) 多項式

$$a(x) = 1 + 2x + 2x^3 \in \mathbb{F}_3[x]$$

に対し $x^{8-4}\,a(x) = x^4\,a(x)$ を $g(x)$ で除した余り $r(x)$ を 6.32 の方法で求めよ. その際に表 6.36 と同様な表を作成しつつ計算せよ. 表で計算されるのは $r(x)$ の係数ではなく $-r(x)$ の係数であることに注意せよ.

6.5. 巡回符号の復号

巡回符号 $C \subset \mathbf{K}^{-n}$ （$\dim C = k$）において, 送信した符号語 $\boldsymbol{w} \in C$ に誤り $\boldsymbol{e}$ が生じ, 受信語 $\boldsymbol{y} \in \mathbf{K}^{-n}$ が受信されたとする：

$$\boldsymbol{y} = \boldsymbol{w} + \boldsymbol{e}.$$

そこで, $\boldsymbol{y}$, $\boldsymbol{w}$, $\boldsymbol{e}$ をそれぞれ多項式表現して, $y(x)$, $w(x)$, $e(x)$ とすると,

$$y(x) = w(x) + e(x).$$

巡回符号 C の生成多項式を $g(x)$ とすると, $g(x)|w(x)$ ゆゑ $y(x)$, $e(x)$ を $g(x)$ で割つた余りは一致する. それを $s(x)$ とする. 従つて, $s(x)$ は $e(x)$ のみで決まり, これも C の syndrome（または syndrome 多項式）といふ. よつて, 誤り多項式 $e(x)$ を syndrome $s(x)$ から求めるには, 両者が 1 対 1 に対応してゐることが必要である.

例 6.39. もし, $g(x)$ の周期が n で $J(C) = g(x)\mathbb{F}_2[x]/(x^n - 1)$ となつてゐれば, 1 箇所だけの誤り多項式 $e(x)$ と syndrome $s(x)$ は 1 対 1 に対応する. 実際 $0 \leqq i < j \leqq n-1$ なる i, j について $g(x)|(x^j - x^i)$ であれば $g(x)|(x^{j-i} - 1)$ となり矛盾である.
しかし, 基礎の体が $\mathbb{F}_2$ でないと, さうならない場合が存在する. 下記の 6.41 を見よ.

例 6.40. 例 6.16 で与へた $g(x) = x^3 + x + 1$ を生成多項式とする $(7, 4)$ 巡回 Hamming 符号の復号を上の立場から考へる. 1 個の誤りを表す多項式は, x^i $(i = 0, 1, \cdots, 6)$ の 7 種類である. これらを $g(x)$ で割つた余り $s(x)$ を求めると次の表のやうになる：

$e(x)$	1	x	x^2	x^3	x^4	x^5	x^6
$s(x)$	1	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$

これより, syndrome $s(x)$ と $e(x)$ が 1 対 1 に対応してゐることがわかる. 従つて, 受信語 $y(x)$ を $g(x)$ で割つて syndrome $s(x)$ を求め, 対応する誤り多項式を知り, 送信語 $w(x)$ を特定できる.

以上のことと 4.6 で述べた syndrome とを比較してみられたい.

例題 6.41. $g(x) = 2 + x + x^2 \in \mathbb{F}_3[x]$ は周期 8 の多項式である.
（つまり $g(x)|x^n - 1$ なる最小の $n \in \mathbb{N}$ は 8）.
これの生成する巡回符号 $C \subset {\mathbb{F}_3}^{-8}$ について以下に答へよ.
(1) C の検査多項式 $h(x)$ を求めよ.
(2) $\boldsymbol{u} = [\,2\ 2\ 2\ 0\ 2\ 0\ 1\ 2\,]$ は符号語であるか否か. 理由を付けて答えよ.
(3) 各 $e(x) \in \{1, 2,\ x,\ 2x \cdots,\ x^7,\ 2x^7\}$ の $g(x)$ による余り（syndromes）$s(x)$ を求め, 6.40 にある様な表を作成せよ. その表から何が言へるか.

解答 (1) $h(x) = (x^8 - 1)/g(x) = 1 + x + 2x^2 + 2x^4 + 2x^5 + x^6$.
(2) $\mathrm{rep}(\boldsymbol{u}, x)\, g(x) = 2x^5 + 2x^4 + x^2 + 2x + 1$ であるから, 符号語である.
(3) 表は以下の通り：

$e(x)$	1	2	x	$2x$	x^2	$2x^2$	x^3	$2x^3$	x^4	$2x^4$	x^5	$2x^5$	x^6	$2x^6$	x^7	$2x^7$
$s(x)$	1	2	x	$2x$	$1+2x$	$2+x$	$2+2x$	$1+x$	2	1	$2x$	x	$1+2x$	$2+x$	$1+x$	$2+2x$

たとへば受信語 $\boldsymbol{v} = [\,2\ 2\ 2\ 0\ 2\ 2\ 2\ 1\,]$ について, $v(x) = \mathrm{rep}(\boldsymbol{v}, x)$ とすると, $v(x) = g(x)(x^5 + x^4 + 2x^3 + x^2 + x + 2) + 1 + x$ である. $\boldsymbol{v}$ の誤りを $\boldsymbol{e}$ とするとき, これが 1 誤りと仮定しても $\mathrm{rep}(\boldsymbol{e}, x)$ は $2x^3$ であるか x^7 であるかを判定できない. □

7. BCH 符号

この節では, Hocquenghem[10] (1959), Bose-Chaudhuri[11] (1960) によつて独立に発見された符号（BCH 符号）について解説する. 有限体が有効に使はれる.

7.1. 2 重誤り訂正 BCH 符号

2 重誤り訂正可能な符号がいかに構成されるかをみる.

定義 7.1. (1) $\mathbf{K}$ が有限体のとき, $\mathbf{K}^\times = \mathbf{K} - \{0\}$ は乗法に関して群をなすが, これは巡回群である[12]. その（群としての）生成元を $\mathbf{K}^\times$ の原始根と呼ぶ.
(2) $m \in \mathbb{N}$ と素数 $p \in \mathbb{N}$ が与へられたとせよ. m 次既約多項式 $f(x) \in \mathbb{F}_p[x]$ の周期が $p^m - 1$ であるとき, $f(x)$ を原始根多項式と呼ぶ.

注意 7.2. $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$ であつても $f(x) = \mathrm{irr}(\alpha, \mathbb{F}_p, x)$ [13] は原始根多項式とは限らない（「代数学 5 及び 6」, p.41, 17.6）. 例へば $p = m = 3$ のとき

$$x^3 + 2x + 1, \quad x^3 + x^2 + 2x + 1, \quad x^3 + 2x^2 + 1, \quad x^3 + 2x^2 + x + 1$$

は, どれも原始根多項式（つまり周期が $3^3 - 1 = 26$）である. 一方,

$$x^3 + 2x + 2, \quad x^3 + x^2 + 2, \quad x^3 + x^2 + x + 2, \quad x^3 + 2x^2 + 2x + 2$$

はいづれも $\mathbb{F}_3$ 上の既約多項式であるが, $x^{13} - 1$ の約数になつてゐて, 原始根多項式ではない.

命題 7.3. $m \in \mathbb{N}$ と素数 $p \in \mathbb{N}$ が与へられたとし, $f(x) \in \mathbb{F}_p[x]$ は m 次既約多項式であるとせよ. $f(x)$ が原始根多項式であるためには, $f(x)$ の任意の根 α が $(\mathbb{F}_{p^m})^\times$ の原始根であることが必要十分である.

証明 $f(x)$ は monic として示せば十分なので, さうしておく.
（必要性）$f(x)$ が原始根多項式であるのは,

$$f(x) \mid (x^M - 1) \quad (1 \leqslant M < p^m - 1)$$

が成り立つことであるが, $f(x)$ の既約性から, このとき $f(x)$ の任意の根 α について, $f(x) = \mathrm{irr}(\alpha, x, \mathbb{F}_p)$ である. ゆゑに「代数学 5 及び 6」, 5.8(3) より

$$\alpha^M \neq 1 \quad (1 \leqslant M < p^m - 1).$$

（十分性）もし, $1 \leqslant M < p^m - 1$ なるある M について

$$f(x) \mid (x^M - 1)$$

であれば $f(x)$ の任意の根 α について

$$\alpha^M = 1$$

となつてしまふ. □

[10] Alexis Hocquenghem （1908 年 1 月 14 日 〜 1990 年 4 月 17 日）は仏国の数学者.
[11] Raj Chandra Bose （1901 年 1 月 19 日 〜 1987 年 10 月 31 日）と Dwijendra Kumar Ray-Chaudhuri (1933 年 11 月 1 日 〜) は米国の数学者.
[12]「代数学 1」, 13.5 参照.
[13] 記号 $\mathrm{irr}(\alpha, x, \mathbf{K})$ は α の体 $\mathbf{K}$ 上の（文字 x に関する）最小多項式で「代数学 5 及び 6」の記法である.

BCH 符号の構成. 素数 p を固定する. m 次原始根多項式 $g(x)\in\mathbb{F}_p[x]$ を生成多項式とする巡回符号を C とする. 以下 $n=p^m-1$ と記す. $g(x)$ の根の 1 つ α を固定する. $n-1$ 次以下の多項式 $u(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in\mathbb{F}_p[x]$ について

$$g(x)|u(x) \iff u(\alpha)=0 \iff a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=0$$

である. よつて, 検査行列 H は次で与へられる :

$$H=[\,1\ \alpha\ \cdots\ \alpha^{n-1}\,]\in \mathrm{Mat}(1,\,n,\,\mathbb{F}_p(\alpha))\quad (\,n=p^m-1\,).$$

いま $\boldsymbol{h}_{i-1}\in{\mathbb{F}_p}^m$ を, x^{i-1} を $g(x)$ で割つた余り $h_{i-1}(x)$ を情報多項式とする符号語とし,

$$\widetilde{H}=[\,\boldsymbol{h}_0\ \boldsymbol{h}_1\ \cdots\ \boldsymbol{h}_{n-1}\,]\in \mathrm{Mat}(m,\,n,\,\mathbb{F}_p)\quad (\,n=p^m-1\,)$$

とすれば, α は $m-1$ 次以下の多項式の根ではないから, $\boldsymbol{a}=[\,a_0\ a_1\ \cdots\ a_{n-1}\,]$ について

$$\begin{aligned} a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=0 &\iff a_0h_0(\alpha)+a_1h_1(\alpha)+\cdots+a_{n-1}h_{n-1}(\alpha)=0\\ &\iff a_0h_0(x)+a_1h_1(x)+\cdots+a_{n-1}h_{n-1}(x)=0\\ &\iff \widetilde{H}\,{}^t\boldsymbol{a}=\boldsymbol{0}\end{aligned}$$

が成り立つ. 今後は $\widetilde{H}$ も H で表すことにする. 混乱は生じないであらう. この様に構成した巡回符号の呼称を定義をしておく.

定義 7.4. p を素数とする. m 次原始根多項式 $g(x)\in\mathbb{F}_p[x]$ (従つて周期 p^m-1) を生成多項式とする巡回符号 $C\subset{\mathbb{F}_p}^{-(p^m-1)}$ を $(p^m-1,\,p^m-1-m)$ Hamming 符号 と呼ぶ.

以下では, $(p^m-1,\,p^m-1-m)$ Hamming 符号 の誤り訂正の仕組みについて述べる. 説明を具体的にするため, $p=2$, $m=4$ として, 次の多項式 $g(x)\in\mathbb{F}_2[x]$ を生成多項式とする巡回符号 C について考へる : $g(x)=x^4+x+1$.

問 7.5. 上の $g(x)$ の周期が $n=2^m-1=15$ であり, $\dim C=11$ であることを確かめよ.

さて, $g(x)$ の根 α から得られる検査行列 H の各成分を $\mathbb{F}_2$ 上で vectors に表現すれば,

$$H=\begin{bmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \end{bmatrix}. \tag{7.6}$$

この (15, 11) 符号は以下の様にして 2 重誤り訂正ができる符号に拡張できる. 送信語 $\boldsymbol{w}\in{\mathbb{F}_2}^{-15}$ に対する受信語を $\boldsymbol{y}\in{\mathbb{F}_2}^{-15}$ とし, それぞれの多項式表現を $w(x)$, $y(x)$, 誤り pattern 多項式 $e(x)=y(x)-w(x)$ と記す. たとへば, $\boldsymbol{y}$ の第 i 成分のみに誤りがあるとすると

$$e(x)=x^{i-1}$$

である. この場合に

$$s=y(\alpha)=w(\alpha)+e(\alpha)=e(\alpha)=\alpha^{i-1}$$

を $\boldsymbol{y}$ の syndrome とも呼ぶ. Syndrome s から $s=\alpha^{i-1}$ なる i が計算されれば, すぐに i 番目の bit が誤つてゐることがわかる. i 番目の bit の位置を α^{i-1} の位置などと呼ぶことにし, α^{i-1} を受信語の第 i 成分に対応する 誤り locator といふ. 復号とは, syndrome から未知の誤りの位置に対応する誤り locators を推定することである.

1 誤り訂正. 上に述べた様に, 誤りが 1 箇所だけの場合は, 予め, 誤り位置 i と誤り locator α^{i-1} の対応表を用意しておけば, syndrome s から i が得られる.

2 誤り訂正. 次に, α^i と α^j 番目の 2 箇所に誤りが起きたとすると, 誤り pattern 多項式と syndrome は,

$$e(x) = x^i + x^j, \quad s = \alpha^i + \alpha^j.$$

この式より, α^i と α^j を確定することはできない. 独立な方程式が 2 つ必要である. 未知数 α^i, α^j を含み, $y(x)$ から計算される別の syndrome が必要である. そこで, $g(x)$ とは異る最小多項式を持つ様な元, 例へば α^3 に対応する符号も考へることにする. ここで $g(x)$ の根は α, α^2, α^4, α^8 （これは「代数学 5 及び 6」, 17.3(3) からわかる）であることに注意せよ. α^3 のみたす $\mathbb{F}_2$ 上既約で monic[14] な多項式（α^3 の最小多項式）は,

$$f_3(x) = x^4 + x^3 + x^2 + x + 1 \tag{7.7}$$

で与へられる（次 page 参照）. 従つて, α と α^3 を根にもつ符号の生成多項式は

$$\begin{aligned} \hat{g}(x) &= \mathrm{LCM}(g(x),\, f_3(x)) \\ &= g(x) f_3(x) = x^8 + x^7 + x^6 + x^4 + 1 \end{aligned} \tag{7.8}$$

で与へられる. ここで, LCM は最小公倍多項式を表す. $g(x)$, $f_3(x)$ の周期はそれぞれ 15, 5 だから, $\hat{g}(x)$ の周期 n は, $n = \mathrm{LCM}(15,\, 5) = 15$ で与へられる. よつて, この $\hat{g}(x)$ を生成多項式とする巡回符号 $\hat{C}$ の符号長は 15 である. また, 情報 bit 数（つまり $\dim \hat{C}$）r は,

$$r = n - \deg \hat{g} = 7.$$

以上より, 2 重誤り訂正符号 $(15, 7)$ が得られた. ここで, 生成多項式 $\hat{g}(x)$ は α, α^2, α^4, α^8, α^3, α^6, α^9, α^{12} を根に持つので, この場合の検査行列 $\hat{H}$ は

$$\hat{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 \cdots \alpha^5 & \cdots \alpha^{10} & \cdots \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 \cdots 1 & \cdots 1 & \cdots \alpha^{12} \end{bmatrix}$$

である. そして, その復号は, この場合の syndrome

$$s_1 = y(\alpha) = \alpha^i + \alpha^j, \quad s_3 = y(\alpha^3) = (\alpha^i)^3 + (\alpha^j)^3 \tag{7.9}$$

を解いて誤り locator α^i, α^j を求め $i+1$, $j+1$ 番目の bits の誤りを訂正すればよい.

この様に構成される線形符号を 2 重誤り訂正 BCH 符号といふ. 一般の t 重誤り訂正 BCH 符号については §7.3 で述べる.

注意 7.10. $m \geqq 2$ とする. 一般に, $(\mathbb{F}_{2^m})^\times$ の原始根 α について $g(x) = \mathrm{irr}\,(\alpha, x, \mathbb{F}_2)$ は原始根多項式である. もちろん次数は m. 従つて $g(x)$ の根の全体は $\{\, \alpha^{2^i} \mid 0 \leqslant i \leqslant m-1 \,\}$ であり, α の位数は $2^m - 1$ なので, α^3 は $g(x)$ の根ではない. このことから, この場合（$m = 4$ と限らなくても）でも α および α^3 を根にもつ符号として, 2 重誤り訂正符号が得られる. 即ち, $f_3(x) = \mathrm{irr}\,(\alpha^3, x, \mathbb{F}_2)$ とするとき, $\hat{g}(x) = g(x)\, f_3(x)$ を生成多項式とする $2^m - 1$ bit の巡回符号が得られる. この符号も 2 重誤り訂正 BCH 符号と呼ばれる.

問 7.11. 7.10 の $\deg f_3(x)$ および $\hat{g}(x)$ の周期を調べよ.

[14] 最高次係数が 1 である様な多項式を monic と呼ぶ.

与へられた元の最小多項式の求め方. ここで, 上で述べた記号の下, つまり α を $g(x)$ の根とするとき, (7.7) に記した α^3 の最小多項式 $f_3(x)$ の求め方を説明する. まづ,

$$(\alpha^3)^2=\alpha^6,\ (\alpha^6)^2=\alpha^{12},\ (\alpha^{12})^2=\alpha^{24}=\alpha^9,\ (\alpha^9)^2=\alpha^{18}=\alpha^3$$

だから, $\mathrm{irr}\,(\alpha^3,x,\mathbb{F}_2)$ のその他の根は α^6, α^9, α^{12} である. よつて

$$\begin{aligned}\mathrm{irr}\,(\alpha^3,x,\mathbb{F}_2)&=(x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})\\&=\{x^2+(\alpha^3+\alpha^6)x+\alpha^9\}\{x^2+(\alpha^9+\alpha^{12})x+\alpha^{21}\}\\&=x^4+x^3+x^2+x+1=f_3(x)\end{aligned}$$

となる.

演 習 問 題

7.12. $x^2+x+2\in\mathbb{F}_3[x]$ の 1 つの根を α として, α^2 の最小多項式を求めよ.

7.13. α を $\alpha^5=1+\alpha^2$ をみたす $\mathbb{F}_{2^5}$ の元とすると, α は $\mathbb{F}_{2^5}$ の原始根となる. このことを既知として, α^3 を根にもつ $\mathbb{F}_2$ 上の既約多項式を求めよ.

7.2. 誤り locator

引き続き, 前節の符号 C について考察する. (7.9) で得られたこの符号の syndrome s_1, s_3 から誤り locator α^i, α^j を求める手段を考へる.

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

をみたす α^i, α^j を求める. α^i, α^j を根にもつ

$$\begin{aligned} \sigma(z) &= (1-\alpha^i z)(1-\alpha^j z) \\ &= 1 + \sigma_1 z + \sigma_2 z^2 \quad (\in \mathbb{F}_{2^4}[x]) \end{aligned}$$

を考へる. $\sigma(z)$ を誤り位置多項式といふ. s_1, s_3 から $\sigma(z)$ が求まればよい.

$$\begin{aligned} \sigma_1 &= -(\alpha^i + \alpha^j) = -s_1 = s_1, \\ {s_1}^3 &= (\alpha^i + \alpha^j)^3 \\ &= (\alpha^i)^3 + (\alpha^j)^3 + \alpha^i \cdot \alpha^j(\alpha^i + \alpha^j) \\ &= s_3 + s_1 \alpha^i \alpha^j = s_3 + s_1 \sigma_2. \end{aligned}$$

よつて

$$\sigma_2 = \alpha^i \alpha^j = \frac{{s_1}^3 + s_3}{s_1}.$$

従つて, 2 次方程式

$$\sigma(z) = 0$$

を解けばよい. ここでは標数が 2 の体を扱つてゐるので, 通常の根の公式は使えない. ここでは, α^j $(j = 0, 1, \cdots, 14)$ を順次代入して根を求める[15].

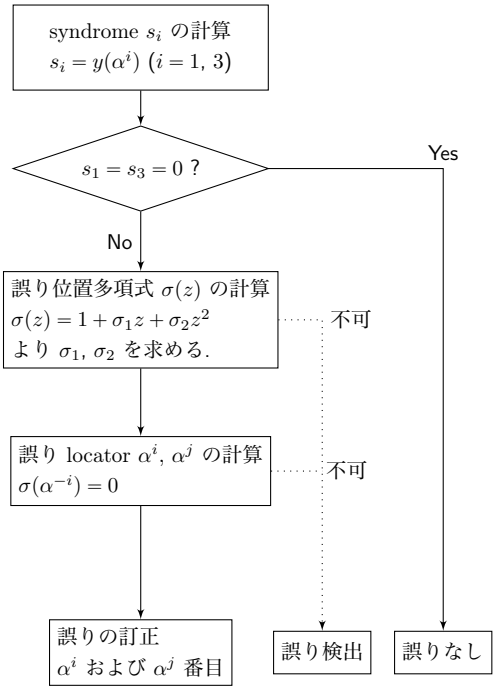


図 7.14 2 重誤り訂正 BCH 符号の復号手順

例題 7.15. 上で考察した 2 重誤り訂正 BCH $(15, 7)$ 符号 C で, 受信語

$$\boldsymbol{y} = [\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,]$$

の誤りを訂正せよ.

解答 受信語 y の多項式表現は

$$y(x) = x^2 + x^3 + x^7 + x^9 + x^{10}.$$

このとき

$$\begin{aligned} s_1 &= y(\alpha) = \alpha^2 + \alpha^3 + \alpha^7 + \alpha^9 + \alpha^{10}. \\ \alpha^{10} &= \alpha^6(\alpha^4 + \alpha + 1) + \alpha^7 + \alpha^6 \\ &= \alpha^6(\alpha^4 + \alpha + 1) + \alpha^3(\alpha^4 + \alpha + 1) + \alpha^4 + \alpha^3 + \alpha^6, \\ \alpha^9 &= \alpha^5(\alpha^4 + \alpha + 1) + \alpha^6 + \alpha^5 \\ &= \alpha^5(\alpha^4 + \alpha + 1) + \alpha^6 + \alpha(\alpha^4 + \alpha + 1) + \alpha^2 + \alpha, \\ \alpha^7 &= \alpha^3(\alpha^4 + \alpha + 1) + \alpha^4 + \alpha^3. \end{aligned}$$

[15] より理論的な解法はないのか.

従つて,

$$s_1 = \alpha^3 + \alpha.$$

ここで, $(\alpha^4)^2 + \alpha^2 + 1 = (\alpha^4 + \alpha + 1)^2 = 0$ を使えば,

$$s_1 = \alpha^3 + \alpha = \alpha^9.$$

同様にして, ,

$$s_3 = y(\alpha^3) = \alpha^2.$$

従つて

$$\begin{aligned}\sigma(z) &= 1 + \alpha^9 z + \frac{\alpha^{27} + \alpha^2}{\alpha^9} z^2 \\ &= 1 + \alpha^9 z + \alpha^{13} z^2 \\ &= 1 + (\alpha + \alpha^3) z + (\alpha^3 + \alpha^2 + 1) z^2\end{aligned}$$

$\sigma(z)$ に, $z = 1, \alpha^1, \alpha^2, \cdots$ を順次代入して, 2 つの根

$$z = \alpha^4,\ \alpha^{13}$$

を得る. 従つて, α^4, α^{13} 番目の位置で誤りが生じてゐることがわかり

$$\boldsymbol{w} = [0\,0\,1\,1\,\underline{1}\,0\,0\,1\,0\,1\,1\,0\,0\,\underline{1}\,0]$$

と送信語が得られた. □

演 習 問 題

7.16. 上で考察した 2 重誤り訂正 BCH $(15, 7)$ 符号 C, 即ち, 前節の (7.8) に現れた多項式

$$\hat{g}(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_2[x]$$

で生成される 2 重誤り訂正 BCH 符号で, 受信語

$$\boldsymbol{y} = [1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1]$$

の誤りを訂正せよ.

7.17. 前問の 2 重誤り訂正 BCH 符号 C について, 受信多項式

$$y(x) = x^2 + x^4 + x^8 + x^9 + x^{10} \in \mathbb{F}_2[x]$$

を復号せよ.

7.3. $t>2$ 場合

次に $t>2$ とし, t 重誤り訂正符号を構成する. $(\mathbb{F}_{2^m})^\times$ の原始根 α を固定する. t 個の元

$$\alpha,\ \alpha^3,\ \alpha^5,\ \cdots,\ \alpha^{2t-1}$$

(但し, $2t-1<2^m-1$) のすべてを根にもつ次数最小の monic 多項式 $\hat{g}(x)\in\mathbb{F}_2[x]$ は

$$\hat{g}(x)=\mathrm{LCM}(f_1(x),\, f_3(x),\, \cdots,\, f_{2t-1}(x))$$

で与へられる. 但し, $f_i(x)=\mathrm{irr}\,(\alpha^i,x,\mathbb{F}_2)$ $(i=1,\,3,\,5,\,\cdots,\,2t-1)$ である. $\hat{g}(x)$ の周期は $n=2^m-1$ である. なぜなら, 各 i について $f_i(x)\,|\,(x^n-1)$ であり, $f_1(x)$ の周期は n であるから. それゆゑ $\hat{g}(x)$ を生成多項式とする n bit の巡回符号が得られる. これを 2 元 BCH 符号[16] と呼ぶ. この巡回符号を $\hat{C}$ とする. $\mathbb{F}_{2^m}/\mathbb{F}_2$ は m 次拡大で, $\mathbb{F}_2(\alpha^i)$ は $\mathbb{F}_{2^m}$ の部分体であるから, $\deg f_i(x)\leqslant m$ である (「代数学 5 及び 6」, 5.10(2)). ゆゑに $\deg\hat{g}(x)\leqslant mt$ であり, $\hat{C}$ の情報 bit 数 (つまり $\dim\hat{C}$) r は $r=n-\deg\hat{g}$ $(\geqq n-mt)$ である. $\hat{C}$ の最小距離 d は, $d\geqq 2t+1$ をみたすことを以下の 7.18 で述べる. この状況で, $2t+1$ を BCH 符号の 設計距離 といふ. さて $\hat{C}$ の検査行列を求めやう. $\hat{g}(x)$ は少なくとも $2t$ 個の根

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

を持つ. 実際, まづ $\hat{g}(\alpha)=0$ だから, $\hat{g}(\alpha^2)=\hat{g}(\alpha)^2=0$ となる. 従つて, α^{2^k} $(k\in\mathbb{N})$ も根になる. また α^3 も根であるので, $\alpha^{3\times 2^k}$ も根である. 以下同様に見ていくとき, $2t$ 以下のどんな自然数も“$2t$ 未満の正の奇数”$\times 2^k$ と書けることに注意すれば, 以下の様に検査行列を得る.

符号語 $\boldsymbol{w}=[\,c_0\ c_1\ \cdots\ c_n\,]\in\hat{C}$ の多項式表現 $w(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ が与へられたとき, $w(\alpha^i)=0$ $(\,i=1,\cdots,\ 2\,t\,)$ だから

$$w(\alpha^i)=c_0+c_1\alpha^i+\cdots+c_{n-1}(\alpha^i)^{n-1}=0\quad(\,1\leqslant i\leqslant 2t\,)$$

が成り立つ. 逆に, この $2t$ 本の式がすべて成立するならば, $\hat{g}(x)$ の定義から $\hat{g}(x)\,|\,w(x)$ でなければならない. 以上から, 符号語 $\boldsymbol{w}=[c_0\ c_1\ \cdots\ c_{n-1}]$ に対して上式を書き直すことによつて, 次の検査行列 H を得る:

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

定理 7.18. 上の状況で, 不等式 $d\geqq 2t+1$ が成立する.

証明 上の H の任意の $2t$ 列からなる行列式 $\neq 0$ が示されて, それら $2t$ 列は 1 次独立になり, 5.1 により, $d\geqq 2t+1$ がいへる. 実際, H の任意の $2t$ 列からなる行列式[17]について,

$$|H|=\begin{vmatrix}\alpha^{i_1}&\alpha^{i_2}&\cdots&\alpha^{i_{2t}}\\(\alpha^{i_1})^2&(\alpha^{i_2})^2&\cdots&(\alpha^{i_{2t}})^2\\\vdots&\vdots&&\vdots\\(\alpha^{i_1})^{2t}&(\alpha^{i_2})^{2t}&\cdots&(\alpha^{i_{2t}})^{2t}\end{vmatrix}=\alpha^{i_1+i_2+\cdots+i_{2t}}\prod_{1\leqslant h<k\leqslant 2t}(\alpha^{i_k}-\alpha^{i_h})\neq 0$$

となり結論を得る. □

7.18 と 4.2 より, 符号 C が t $(t>2)$ 重誤り訂正符号であることがわかる.

[16] “2 元”の 2 は $\mathbb{F}_2$ を基礎体にしてゐることを意味する. 7.21 も参照されたい.
[17] この形の行列式は Vandermonde の行列式と呼ばれる.

注意 7.19. $t>2$ の場合にも, 上記 $w(x)$ の係数を送信されたときの受信語 $\boldsymbol{y}$ を係数として定まる多項式を $y(x)$ と書けば, t 個からなる組

$$y(\alpha),\ y(\alpha^3),\ y(\alpha^5),\ \cdots,\ y(\alpha^{2t-1})$$

がこの通信の syndromes と呼ばれるべきものである. これらの syndromes から誤り位置を決めるのは $t=2$ のときよりはるかに複雑になる. この場合の復号法については, 文献 [Im] を参照.

例 7.20. $n=4$, $m=2^4-1=15$ のときに $t=3,4,5$ に対し, t 重誤り訂正 BCH 符号の生成多項式を求めてみる. この場合, α を $f_1(x)=x^4+x+1$ の根とするとき, (7.7) において α^3 は

$$f_3(x)=x^4+x^3+x^2+x+1$$

の根であると述べて, そのことを §7.1 の最後のところで確認したのであつた. それにより $\hat{g}(x)=\mathrm{LCM}(f_1(x),\, f_3(x))$ を求めたのであつた. 他の場合でも $f_i(x)=\mathrm{irr}\,(\alpha^i,\mathbb{F}_2,x)$ を用ゐて, 以下の様にして生成多項式 $\hat{f}(x)$ を求めることができる :

$t=3$ のとき : $\hat{f}(x)=\mathrm{LCM}(f_1,\, f_3,\, f_5)=x^{10}+x^8+x^5+x^4+x^2+x+1.$

$t=4$ のとき : $\hat{f}(x)=\mathrm{LCM}(f_1,\, f_3,\, f_5,\, f_7)=f_1\,f_3\,f_5\,f_7=\dfrac{x^{15}+1}{x+1}=\displaystyle\sum_{i=0}^{14}x^i.$

$t=5$ のとき : $\hat{f}(x)=\mathrm{LCM}(f_1,\, f_3,\, f_5,\, f_7,\, f_9)=\displaystyle\sum_{i=0}^{14}x^i$ $\quad(\,f_9=f_3\ \text{より}\,).$

注意 7.21. p を奇素数とし, $q>1$ は p の冪であるとする. また, $n=q^m-1$ $(m\in\mathbb{N})$ とし, α を 1 の原始 n 乗根とする. 整数 ℓ と $h<n$ を固定する. $\ell=0$ または 1 とすることが多い. α の連続する $h-1$ 個の冪乗の列

$$\alpha^{\ell},\ \alpha^{\ell+1},\ \cdots,\ \alpha^{\ell+h-2}\quad(\,h<n\,)$$

を根にもつ $\mathbb{F}_q$ 上の次数最小の monic 多項式 $G(x)$, つまり

$$G(x)=\mathrm{LCM}(f_\ell(x),\, f_{\ell+1}(x),\, \cdots,\, f_{\ell+h-2}(x)\,)$$
$$(\,\text{但し}\ f_i(x)=\mathrm{irr}\,(\alpha^i,\,\mathbb{F}_q,\,x)\,)$$

を生成多項式とする符号長 n の巡回符号 $\hat{C}$ は, q 元 BCH 符号と呼ばれる. 特に, $m=1$ の場合は Reed-Solomon 符号 と呼ばれる. $\hat{C}$ の最小距離 $d=d(\hat{C})$ は $d\geqq h$ を満たす. これについての詳細は [Im], §7.1 または [MS], Chapters 7 〜 9 を見られたい.

問 7.22. 上の 7.20 における計算の過程において $\mathrm{irr}\,(\alpha^3,x,\mathbb{F}_2)=f_3(x)$,

$$\mathrm{irr}\,(\alpha^5,x,\mathbb{F}_2)=f_5(x),\quad \mathrm{irr}\,(\alpha^7,x,\mathbb{F}_2)=f_7(x)$$

の計算の細部を記述せよ.

問 7.23. $t=3,5,7$ についての上の 7.20 における $f_i(x)$ $(i=1,3,5,7)$ から $\hat{f}(x)$ を得る計算を `pari/GP` 等を利用して確かめよ.

8. 付録

8.1. Pari/GP の基本的な使用法

Pari/GP を PC や Mac に install する方法 : とりあへず, 使用するには

http://pari.math.u-bordeaux.fr/index.ja.html

の左にある “Download”のところから, binary を intall すればよい. (Source file からの install も可能である)

Anrdoid の smartphone については paridroid を install すれば使へる.

iPhone については SageMath を install すれば, それに含まれてゐる.

SageMath で使用する場合は 'gp: 命令' と入力して Evaluate の Key を押せばよい.

例題 8.1. (**整数を法とした多項式の除法**) 多項式

$$g(x) = 1 + x + 2x^2 + x^3 + x^5, \quad f(x) = 1 + 2x + x^{10} + x^{100} \in \mathbb{F}_3[x]$$

について, Pari/GP を利用して, $f(x)$ を $g(x)$ で割つた余り $r(x)$ ($\deg r(x) \leqslant 4$) を求めよ.

解答 単純に

```
> Mod(g,f)
```

として, 計算すると, 巨大な係数を持つ $r(x)$ が Mod($r(x)$,$g(x)$) の形で表示される. $\mathbb{F}_3$ 係数で求めたいので

```
> Mod(Mod(g,f),3)
%1 = Mod(Mod(1, 3)*x^3 + Mod(1, 3)*x^2 + Mod(1, 3)*x + Mod(2, 3),
    x^5 + x^3 + 2*x^2 + x + 1)
```

とすればよい. 結果に Mod(,$g(x)$) が付くので, これを外したければ,

```
> lift(Mod(Mod(g,f),3))
%2 = Mod(1, 3)*x^3 + Mod(1, 3)*x^2 + Mod(1, 3)*x + Mod(2, 3)
```

とすればよい. さらに, 結果の係数に一々付いてゐる Mod(,3) を外したければ

```
> lift(lift(Mod(Mod(g,f),3)))
%3 = x^3 + x^2 + x + 2
```

とできる. 通常, 符号理論では多項式は昇冪順で扱ふので,

```
> lift(lift(Mod(Mod(g,f),3)))+O(x^5)
%4 = 2 + x + x^2 + x^3 + O(x^5)
```

とする方法がよいかも知れない. □

例題 8.2. （**因数分解の方法**） $x^{12}-1$ を $\mathbb{F}_2$ 上で因数分解せよ.

解答 次の様に入力すればよい.

```
> A=factor(Mod(x^12-1,2))
%5 =
[                Mod(1, 2)*x + Mod(1, 2) 4]
[Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2) 4]
```

とする. ここで各行の右の数字は重複度を表す. つまり, この 2 つの因子がどちらも 4 乗冪で現れることを意味してゐる. 欲しい因子を取り出すには（これらを行列と受け止めて）

```
> A[2,1]                    \\ ( (2,1) 成分を意味する )
%6 = Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2)
```

などとする.

```
> lift(lift(A[2,1]))+O(x^3)
%7 = 1 + x + x^2 + O(x^3)
```

等は上に述べた通りである. □

例題 8.3. （**最大公約数**, **最小公倍数**） 3 つの多項式 x^3+1, x^2+x+1, $x^4+x+1 \in \mathbb{F}_2[x]$ の最小公倍数を求めよ.

解答 次の様に入力すればよい.

```
> lift(lcm(lcm(Mod(x^3+1,2),Mod(x^2+x+1,2)),Mod(x^4+x+1,2)))+O(x^9)
%8 = 1 + x + x^3 + x^7 + O(x^9)
```

これより最小公倍数 $1+x+x^3+x^7$ を得る. □

8.2. MacWilliams の恒等式

自己双対的な符号は保型形式の理論などと結びつく. その際に, 最も重要な道具が, ここに述べる MacWilliams の公式である.

C を有限体 $\mathbb{F}_q$ 上の (n,k) 線形符号とし,

$$A_i = \#\{\, \boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) = i \,\} \quad (0 \leqslant i \leqslant n)$$

とおく. $\{A_0,\ A_1,\ \cdots,\ A_n\}$ を C の 重さ分布 といふ. このとき, 文字 x, y の多項式

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

を C の 重さ母函数 または 重さ分布多項式 といふ.

定理 8.4. (MacWilliams[18]) 次の等式が成立する :

$$W_{C^\perp}(x,y) = \frac{1}{|C|}\, W_C(x+(q-1)y, x-y).$$

ここでは簡単のため $q=2$ のときのみ証明する. 読者には, 一般の場合の証明を試みられたい. 証明には, 補題を 2 つ使ふ.

補題 8.5. $\boldsymbol{u} \in {\mathbb{F}_2}^{-n}$ に対し,

$$\sum_{\boldsymbol{v} \in {\mathbb{F}_2}^{-n}} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} = \begin{cases} 2^n & (\,\boldsymbol{u} = \boldsymbol{0}\,) \\ 0 & (\,\boldsymbol{u} \neq \boldsymbol{0}\,). \end{cases}$$

証明 $\boldsymbol{u} = \boldsymbol{0}$ のときは明らかであるから, $\boldsymbol{u} \neq \boldsymbol{0}$ とする. このとき, $\boldsymbol{u} = [\, u_1\ \cdots\ u_n\,]$ で $u_n \neq 0$ としてよい. いま $\boldsymbol{v} = [\, v_1\ \cdots\ v_n\,]$ として,

$$\boldsymbol{u}\,{}^t\boldsymbol{v} = u_1v_1 + \cdots + u_{n-1}v_{n-1} + v_n.$$

ここで

$$v_n = u_1v_1 + \cdots + u_{n-1}v_{n-1} \qquad \text{のとき,} \quad \boldsymbol{u}\,{}^t\boldsymbol{v} = 0,$$
$$v_n = u_1v_1 + \cdots + u_{n-1}v_{n-1} + 1 \quad \text{のとき,} \quad \boldsymbol{u}\,{}^t\boldsymbol{v} = 1.$$

従つて,

$$\#\{\, \boldsymbol{v} \in {\mathbb{F}_2}^{-n} \mid \boldsymbol{u}\,{}^t\boldsymbol{v} = 0 \,\} = \#\{\, \boldsymbol{v} \in {\mathbb{F}_2}^{-n} \mid \boldsymbol{u}\,{}^t\boldsymbol{v} = 1 \,\}.$$

よつて, $u \neq 0$ のとき

$$\sum_{v \in {\mathbb{F}_2}^{-n}} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} = 0$$

となる. □

[18] Florence Jessie MacWilliams, 英国の女性数学者 (1917 年 4 月 4 日 〜 1990 年 5 月 27 日).

補題 8.6. $\boldsymbol{u} \in {\mathbb{F}_2}^{-n}$ に対し,

$$\sum_{\boldsymbol{v}\in C} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} = \begin{cases} |C| & (\boldsymbol{u} \in C^\perp) \\ 0 & (\boldsymbol{u} \notin C^\perp). \end{cases}$$

証明 $\boldsymbol{u} \in C^\perp$ なら, C の任意の元 v に対し, $\boldsymbol{u}\,{}^t\boldsymbol{v} = 0$. よつて, この場合は成立する. $\boldsymbol{u} \notin C^\perp$ とする. $\mathbb{F}_2$ 上では, C と同値な符号で検査行列 H と生成行列 G

$$H = [P\ I_{n-k}] \in \mathrm{Mat}(n-k, k, \mathbb{F}_2), \quad G = [I_k\ {}^tP] \in \mathrm{Mat}(k, n, \mathbb{F}_2)$$

を持つものがある. 但し $P \in \mathrm{Mat}(n-k, k, \mathbb{F}_2)$. 実際

$$H\,{}^tG = P + P = O.$$

C をその様な線形符号に取り換へても問題ないので, さうする. $\boldsymbol{u}$, $\boldsymbol{v}$ の前半の k bit からなる vectors をそれぞれ $\boldsymbol{u}_1$, $\boldsymbol{v}_1$ と書く. そして, $\boldsymbol{u} = [\,\boldsymbol{u}_1\ \boldsymbol{u}_2\,]$, $\boldsymbol{v} = [\,\boldsymbol{v}_1\ \boldsymbol{v}_2\,]$ とおく. このとき,

$$0 = \boldsymbol{v}\,{}^tH = [\,\boldsymbol{v}_1\ \boldsymbol{v}_2\,] \begin{bmatrix} {}^tP \\ I_{n-k} \end{bmatrix} = \boldsymbol{v}_1\,{}^tP + \boldsymbol{v}_2.$$

よつて,

$$\boldsymbol{v}_2 = \boldsymbol{v}_1\,{}^tP.$$

この式から $\boldsymbol{v}$ が C を走るとき, $\boldsymbol{v}_1$ が ${\mathbb{F}_2}^{-k}$ 全体を走つて, その各々の $\boldsymbol{v}_1$ に $\boldsymbol{v}_2 = \boldsymbol{v}_1{}^tP$ が定まつてゐるだけだといふことに注意せよ. このとき,

$$\boldsymbol{u}\,{}^t\boldsymbol{v} = \boldsymbol{u}_1\,{}^t\boldsymbol{v}_1 + \boldsymbol{u}_2\,{}^t\boldsymbol{v}_2 = \boldsymbol{u}_1\,{}^t\boldsymbol{v}_1 + \boldsymbol{u}_2\,{}^t(\boldsymbol{v}_1\,{}^tP) = (\boldsymbol{u}_1 + \boldsymbol{u}_2P)\,{}^t\boldsymbol{v}_1.$$

ここで, $\boldsymbol{w} = \boldsymbol{u}_1 + \boldsymbol{u}_2P$ とおくと, $\boldsymbol{u}\,{}^t\boldsymbol{v} = \boldsymbol{w}\,{}^t\boldsymbol{v}_1$ で,

$$\boldsymbol{w} = \boldsymbol{u} \begin{bmatrix} I_k \\ P \end{bmatrix} = \boldsymbol{u}\,{}^tG.$$

$\boldsymbol{u} \notin C^\perp$ だから, $\boldsymbol{w} \neq 0$. 従つて, 8.5 より

$$\sum_{\boldsymbol{v}\in C} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} = \sum_{\boldsymbol{v}_1 \in {\mathbb{F}_2}^{-k}} (-1)^{\boldsymbol{w}\,{}^t\boldsymbol{v}_1} = 0.$$

となる. □

証明 定理の証明 まづ,

$$W_C(x,y) = \sum_{\boldsymbol{v}\in C} x^{n-\mathrm{wt}(\boldsymbol{v})} y^{\mathrm{wt}(\boldsymbol{v})} = \sum_{\boldsymbol{v}=[v_1\cdots v_n]\in C} \prod_{i=1}^{n} x^{1-v_i} y^{v_i}.$$

$$\begin{aligned} |C|\, W_{C^\perp}(x,y) &= |C| \sum_{\boldsymbol{u}\in C^\perp} x^{n-\mathrm{wt}(\boldsymbol{u})} y^{\mathrm{wt}(\boldsymbol{u})} \\ &= \sum_{\boldsymbol{u}=[u_1\cdots u_n]\in {\mathbb{F}_2}^{-n}} \sum_{\boldsymbol{v}\in C} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} \prod_{i=1}^{n} x^{1-u_i} y^{u_i} \quad (\text{補題 8.6 より}) \\ &= \sum_{\boldsymbol{v}\in C} \sum_{\boldsymbol{u}=[u_1\cdots u_n]\in {\mathbb{F}_2}^{-n}} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} \prod_{i=1}^{n} x^{1-u_i} y^{u_i}. \end{aligned}$$

ここで, $\sum_{u_i\in\mathbb{F}_2} (-1)^{u_i v_i} x^{1-u_i} y^{u_i} = x + (-1)^{v_i} y$ を使つて,

$$|C|\, W_{C^\perp}(x,y) = \sum_{\boldsymbol{v}\in C} \sum_{\substack{\boldsymbol{u}=[u_1\cdots u_{n-1}]\\ \in {\mathbb{F}_2}^{-(n-1)}}} \prod_{i=1}^{n-1} (-1)^{\boldsymbol{u}\,{}^t\boldsymbol{v}} x^{1-u_i} y^{u_i} (x + (-1)^{v_n} y).$$

これを繰り返し, 結局

$$|C|\, W_{C^\perp}(x,y) = \sum_{\boldsymbol{v}\in C} \prod_{i=1}^{n} (x + (-1)^{v_i} y).$$

ここで, $v_i = 0$, $v_i = 1$ の部分を別々にまとめると,

$$|C|\, W_{C^\perp}(x,y) = \sum_{\boldsymbol{v}\in C} (x+y)^{n-\mathrm{wt}(\boldsymbol{v})} (x-y)^{\mathrm{wt}(\boldsymbol{v})} = W_C(x+y, x-y).$$

□

例題 8.7. 重さ母函数

$$W_C(x,y) = x^5 + x^4 y + 2x^3 y^2 + 2x^2 y^3 + x y^4 + y^5$$

をもつ $\mathbb{F}_2$ 上の線形符号 C を構成せよ.

解答 求める符号を C とし, まづ $C^\perp$ の重さ母函数を求めると,

$$W_{C^\perp}(x,y) = |C|^{-1} W_C(x+y, x-y) = x^5 + 2x^3 y^2 + x y^4.$$

これより, $C^\perp$ は重さ 0, 2, 4 の符号語をそれぞれ 1, 2, 1 個づつもつ. 従つて, $C^\perp$ は

$$\{[00000],\ [11000],\ [00110],\ [11110]\}$$

か, またはこれと同値な符号である. 従つて, $C^\perp$ の生成行列 H として

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

がとれて, C はこれを検査行列とする符号である. よつて, C は 2.30 で与へた符号かそれと同値な符号になる. □

8.3. 符号の限界式

符号長 n と訂正能力 t を与へたとき, 符号語数の限界を求める. 以下, 有限体 $\mathbf{K}$ 上の (n,k) 線形符号 $C \subset \mathbf{K}^{-n}$ について考へる.

Hamming の限界式. 線形符号 $C \subset {\mathbb{F}_2}^{-n}$ において, Hamming 距離を考へる. 一つの $\boldsymbol{w} \in C$ に対し, $\boldsymbol{w}$ と k 箇所で異なる長さ n の元の総数は $\binom{n}{k}$ である. 従つて, ある 1 つの符号語 $\boldsymbol{w}$ から Hamming 距離が t 以内にある $\mathbf{K}^{-n}$ の元の総数は, $\boldsymbol{w}$ も含めて,

$$N = \sum_{k=0}^{t} \binom{n}{k}$$

である. 訂正能力が t だから, 1 つの符号語から Hamming 距離が t 以内にある記号系列が, 他の符号語から Hamming 距離が t 以内にある vector に等しくなることはない. 従つて, 作り得る符号語の総数を M とするとき,

$$MN \leqslant q^{-n}.$$

ここで q は基礎の体 $\mathbf{K}$ の元の個数である. これを Hamming の限界式 といふ. 等号が成立するときは, 各符号語を中心とする半径 t の小球で受信空間が埋めつくされることになり, t 重誤り訂正符号としては最も効率のよい符号になる. これを 完全符号 といふ.

Singleton 限界. 一般の距離を与へられた (n,k) 線形符号 C の最小距離を d とするとき,

$$d + k \leqslant n + 1$$

が成立する. これを Singleton (シングルトン) 限界[19] といふ. 実際, C の検査行列 H は $(n-k) \times n$ 行列だから, H の $(n-k+1)$ 列は 1 次従属である. 従つて, 5.1 より

$$d \leqslant n - k + 1.$$

この不等式で, 等号の成立する符号を 最大距離分離符号 (MDS 符号[20]) といふ. 2 元符号には, 等号の成立する符号は存在しないことが知られてゐる. また, MDS 符号の重さ分布は容易に求まる.

[19] Richard Collom Singleton (1928 年 2 月 21 日 ____ 生まれ, 2007 年 4 月 8 日 California 州没)
[20] maximum distance separable codes.

8.4. Gauss 整数上の符号構成 ([Hu])

p を素数とし, 簡単のため $p \equiv 1 \bmod 4$ とする. このとき, p は Gauss 整数環 $\mathbb{Z}[i]$ 内で

$$p = \pi\overline{\pi} = a^2 + b^2 \quad (a,\ b \in \mathbb{Z})$$

と分解する. ここで, $\pi = a + bi$, $\overline{\pi} = a - bi$ である.

$$\mathscr{G}_\pi = \mathbb{Z}[i]/(\pi)$$

とおく. ここで, (π) は複素素数 π で生成される素 ideal を表す. 自然な準同型写像

$$\mu : \mathbb{Z}[i] \longrightarrow \mathscr{G}_\pi, \quad \xi \longmapsto \xi \bmod \pi$$

により, 剰余体 $\mathscr{G}_\pi$ は $\mathbb{F}_p$ と同型である.

$\gamma \in \mathscr{G}_\pi$ に対して, $\gamma' \equiv \gamma \bmod \pi$ なる γ' 全体の中で, γ' の実部の絶対値と虚部の絶対値の和の最小値を γ の重さと定め

$$\mathrm{wt}_{\mathrm{M}}(\gamma) = \min\{\, |\mathrm{Re}\,\gamma'| + |\mathrm{Im}\,\gamma'| \,;\, \gamma' \in \mathbb{Z}[i],\ \gamma' \equiv \gamma \bmod \pi \,\}$$

と書く. これを γ の Mannheim 重さ と称する. さらに 2 元 $\alpha,\ \beta \in \mathscr{G}_\pi$ に対して, $\beta - \alpha$ の重さを α と β の Mannheim 距離 と称し,

$$d_{\mathrm{M}}(\alpha, \beta) = \mathrm{wt}_{\mathrm{M}}(\gamma)$$

と書く. これをもとにして, 各 vector $\boldsymbol{c} = [\, c_0 \ c_1 \ \cdots \ c_{n-1} \,] \in \mathscr{G}_\pi{}^{-n}$ の Mannheim 重さ[21] $\mathrm{wt}_{\mathrm{M}}(\boldsymbol{c})$ を

$$\mathrm{wt}_{\mathrm{M}}(\boldsymbol{c}) = \sum_{j=0}^{n-1} \mathrm{wt}_{\mathrm{M}}(c_j)$$

で定義する. さらに, $\mathscr{G}_\pi$ 上の 2 つの n 次元 vectors $x,\ y$ に対し,

$$d_{\mathrm{M}}(\boldsymbol{x},\ \boldsymbol{y}) = \mathrm{wt}_{\mathrm{M}}(\boldsymbol{x} - \boldsymbol{y})$$

で $x,\ y$ の Mannheim 距離 を定義する. d_{M} は距離の公理をみたす.

問 8.8. d_{M} が実際に 3.1 の距離の公理 **M1** ～ **M4** ををみたすことを示せ.

例 8.9. $p = 13 \equiv 1 \bmod 4$, $\pi = 3 + 2i$ とする. $\alpha = 3 + 4i$, $\beta = 1 + i$ のとき, $\beta - \alpha = 2 + 2i \equiv 1 \bmod \pi$ より, $d_{\mathrm{M}}(\alpha, \beta) = 2$ となる. 図 8.10 において α' は α を $-\pi$ 移動したものである.

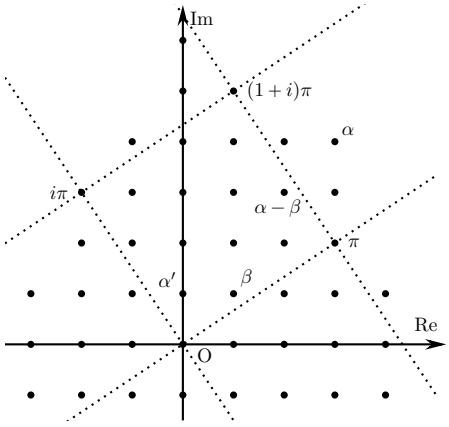


図 8.10 $\mathbb{Z}[i]/(\pi)$ の代表元

[21] 独国の都市 Mannheim の Mannheim 城から北北東に広がる市街地の道路が碁盤の目の様になつてをり, $\mathscr{G}_\pi$ の代表系が複素数平面上になす模様が, この都市の地図において道路の交叉点の全体に似てゐることから名付けられたらしい.

さて, 以下で Mannheim 1 重誤り訂正符号 を構成する.

α を位数 $p-1$ の $\mathscr{G}_\pi$ の元とし, $n=\frac{p-1}{4}$ とおく. 検査行列 H が

$$H=[\,1\ \alpha\ \cdots\ \alpha^{n-1}\,]\in \mathrm{Mat}(1,n-1,\mathscr{G}_\pi)$$

で与へられる $\mathscr{G}_\pi$ 上の $(n,n-1)$ 線形符号を C とする. これの生成行列 G は

$$G=\begin{bmatrix} -\alpha & 1 & 0 & \cdots & 0 & 0\\ -\alpha^2 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ -\alpha^{n-1} & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}\in \mathrm{Mat}(n-1,n,\mathscr{G}_\pi)$$

で与へられる. 以下では混乱を避けるため, 全空間の任意の元 $\boldsymbol{v}\in\mathscr{G}_\pi{}^{-n}$ の成分を左から, 第 0 成分, 第 1 成分, $\cdots$, 第 $n-1$ 成分, と呼ぶことにする.

問 8.11. 上記の状況で, 実際に G が線形符号 C の生成行列であることを確かめよ.
(Hint: $\mathrm{rank}\,G=n-1$ であることと $G^tH=O$ を確かめよ.)

G の任意の 2 列は $\mathscr{G}_\pi$ 上 1 次独立なので, 5.1 から, Mannheim 重さに関しての C の最小重さ $d_{\mathrm{M}}(C)$ は $d_{\mathrm{M}}(C)\geqq 3$ だから, C は 1 誤り (もちろん Mannhaim 重さに関して) 訂正が可能である.

以下, C での復号を考へる. まづ, 誤り patterns は

$$\boldsymbol{e}=[\,0\ \cdots\ 0\ \underset{\text{第 } j \text{ 成分}}{e_j}\ 0\ \cdots\ 0\,]\in\mathscr{G}_\pi{}^{-n},\quad (e_j\in\{\pm1,\ \pm i\}) \tag{8.12}$$

である. このとき, これらの syndromes $H\,{}^t\boldsymbol{e}$ は互ひに異なる. 従つて, 復号が可能である.

問 8.13. 上記 $4n$ 個の誤り patterns の syndromes $H\,{}^t\boldsymbol{e}$ が互ひに異なることを示せ.
(H を上記の様に定義した理由がここにある.)
(Hint: どの syndrome も $\varepsilon\alpha^j$ $(\varepsilon\in\{\pm1,\pm i\},\ j\in\{0,\cdots,n-1\})$ の形であることを示せ.)

復号の手順. 上の状況において, 送信語 $\boldsymbol{c}$ に対し, $\boldsymbol{r}=\boldsymbol{c}+\boldsymbol{e}$ を受信したとすると,

$$H\,{}^t\boldsymbol{r}=H\,{}^t\boldsymbol{e}=s\in\mathbb{Z}[i]$$

に対応する誤り pattern $\boldsymbol{e}$ を求め $\boldsymbol{c}=\boldsymbol{r}-\boldsymbol{e}$ と復号される. 具体的には, まづ, s に対応する $\mathscr{G}_\pi$ の元は α^ℓ $(\ell\in\{0,\cdots,p-2\})$ と書ける. このとき, 誤り locator は

$$\bar{\ell}\equiv\ell\ \bmod n\ (=\log_\alpha s\ \bmod n),\quad (\bar{\ell}\in\{0,\cdots,n-1\})$$

で与へられ, $\alpha^{\ell-\bar{\ell}}\in\{\pm1,\pm i\}$ であつて, これを ε と書けば,

$$s=\varepsilon\alpha^{\bar{\ell}}$$

である. これより直ちに, $\boldsymbol{e}$ が

$$\boldsymbol{e}=[\,0,\cdots,0,\ \underset{\text{第 } \bar{\ell} \text{ 成分}}{\varepsilon},\ 0,\cdots,0\,]$$

であるとわかる.

例題 8.14. $p=13\equiv 1 \bmod 4$, $\pi=3+2i$ のとき, 以下の問に答へよ.
(1) 上記の記号で以下の様になることを示せ:
$\alpha=1+i$, $n=\frac{p-1}{4}=3$, $\alpha^3=-2+2i\equiv -i \bmod \pi$ であり,

$$H=\begin{bmatrix}1 & 1+i & 2i\end{bmatrix}\in \mathrm{Mat}(1,3,\mathscr{G}_\pi),\quad G=\begin{bmatrix}-1-i & 1 & 0\\ -2i & 0 & 1\end{bmatrix}.$$

(2) 受信語 $\boldsymbol{r}=\begin{bmatrix}1+i & i & -1+i\end{bmatrix}$ を復号せよ.

解答 (1) の解答は容易なので省略する.
(2) については, まづ

$$s=H\,{}^t\boldsymbol{r}=-2=\alpha^{11},\quad \ell=11,\quad \overline{\ell}=2.$$

従つて,

$$s\alpha^{-2}=\alpha^9=i,\quad \boldsymbol{e}=\begin{bmatrix}0 & 0 & i\end{bmatrix}.$$

よつて,

$$\boldsymbol{c}=\boldsymbol{r}-\boldsymbol{e}=\begin{bmatrix}1+i & i & -1\end{bmatrix}$$

である. □

演 習 問 題

8.15. $p=17$, $\pi=1+4i$ に対する Gauss 符号 C について答へよ. 但し $\alpha=1+i$ とする.
(1) 巡回群 $\mathscr{G}_\pi{}^\times$ における α の位数は 16 であることを示せ.
(2) この節の説明に沿つて, 検査行列 H と生成行列 G を書き下せ.
(3) C が 1 誤り訂正が可能であることを利用して,

$$\boldsymbol{r}=\begin{bmatrix}1-i & 2i & 3-i & 1+2i\end{bmatrix}$$

を復号せよ.

索 引