平成24年度 前学期

電気学第一 講義ノート

「通信の基礎」

坂庭 好一

東京工業大学 大学院理工学研究科

集積システム専攻

目　　次

0. 通信理論の概要

1. 情報源のモデルと情報量

2. 誤り訂正符号

0 通信理論の概要

0.1 通信の目的とシステムモデル

〔0.1.1〕通信の目的は，距離的あるいは時間的な隔たりを越えて情報を交換することにある．距離的な隔たりを越えた通信の具体例としては，東京から大阪へ電話を掛けたり，アメリカから US オープンをテレビ中継したりすることがある．このような距離を越えた通信においては，通常即時 (リアル・タイム) 性が要求される．一方，CD (Compact Disc) に録音された音楽を鑑賞したり，DVD (Digital Video Disc) や BD (Blu-ray Disc) に記録された映画やテレビ番組を見たりするのは，時間を越えた通信の例である．

最も基本的な音声による通信を考えてみよう．大昔から人間が行って来た通信のやり方は面と向かって話をすることである．しかし，この方法では遠く離れた相手と話をすることはできない．音は距離が隔たるにつれて大きく減衰するため，遠くまで到達しない．従って，距離を克服して通信を行なうには，人間の発する情報を即時に遠くまで伝達可能な物理量に変換して伝達する必要がある．この条件を満たしてくれたのがいわゆる**電気通信**である．

〔0.1.2〕電気通信においては人やコンピュータなどが発する情報を距離的あるいは時間的に隔たった所 (相手) へ届けるため，**送信機**あるいは**符号器**と呼ばれる装置によって情報を加工した後，光 (電磁波) や電気信号に変換し，**通信路**である自由空間や光ファイバ・ケーブルや記録媒体を通して，受信側へ伝達する．

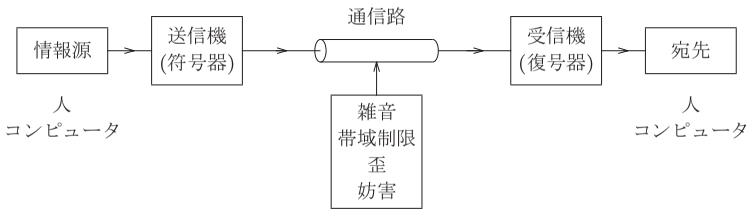

図 0.1　電気通信のモデル

受信側では，**受信機**あるいは**復号器**と呼ばれる装置によって，受信信号を人やコンピュータが発したもとの情報に戻すことになる．これを図示すると**図 0.1** のように書くことができる．通信は多者間，双方向であるが，**図 0.1** は基本要素である，2 者間，片方向を記述していることになる．

図 0.1 において通信路と記した部分は，空間伝搬路であったり，光ファイバやメタリック・ケーブルであったり，CD，DVD，BD 等の記録媒体であったりする．いずれの通信路においても幸か不幸か送信された情報がそのままの形で受信されることはない．通信路には，

(1) 物理的な障害 (雑音，帯域制限，歪など)，(2) 人為的な妨害

等が存在する．従って，これらの障害を克服して情報を如何に，

(1) 速く (大量に) かつ正確に，そして (2) 安全に伝えるか，

が通信工学の課題となる．

0.2 通信理論の概要

上に述べた通信工学の課題は，現在どのように解決されているのであろうか？その概要は次のようにまとめられる．

〔0.2.1〕まず情報を「速く」あるいは「大量に」という要請であるが，それにはそもそも情報はどう測られるべきかが問題になる．情報の測り方が決まらなければ，「速く」も「大量に」も議論できない．

情報の例として，人が話をする場合を考えてみよう．人の話は，ことばの集合 $A := \{a_1, a_2, \ldots, a_M\}$ から，ことばの系列 $a_i a_j \cdots a_k$ を発することと捉えることが出来る．このとき，情報の測り方に関する検討を行なうと，情報は $-\log_2 p(a_i)$ [ビット] のように測るのが妥当であることが導かれる．ただし，$p(a_i)$ はことば (情報) a_i が発生する確率である．これについては，本講義ノートの第 1 章に述べる．

〔0.2.2〕 次に，与えられた情報の表現に無駄がないかが問題になる．例えば人の話 (自然言語) は多分に「冗長性」を含んでいる．逆にいうと，話の本質的な内容 (情報の量) は変えることなく，もっと簡潔に表現できるのである．では，情報は何処まで簡潔に表現できるのであろうか？

表現の簡潔さを「ことばの系列の (平均的) 長さ」で測ることにすると，その限界は**平均情報量 (エントロピー)**

$$H(A) := \sum_{i=1}^{M} -p(a_i) \log p(a_i) \tag{0.1}$$

で与えられ，逆に $H(A)$ に限りなく近い簡潔な表現が可能であることが導かれる．このような操作は**情報圧縮**または**データ圧縮**と呼ばれ，情報を記録したり，伝達したりするときに，事前に為すべき重要な操作となる．なお，$M = 2$ のとき，$p(a_1) =: x$，$p(a_2) = 1 - x$ とし，式 (0.1) の $H(A)$ を x の関数として $\mathcal{H}_2(x)$ と表すと，$\mathcal{H}_2(x)$ の形は**図 1.2** (p.13) のように与えられる．

〔0.2.3〕 その次には，(簡潔に表現された) 情報を，(1) 記録してそれを再生したり，(2) 遠く離れた場所へ送信してそれを受信したり，することが行われる．このとき，再生したり受信したりした情報は，一般にもとの情報と同じではない．それは主として雑音と呼ばれる妨害要因による．

実際に広く用いられている方式として，情報を 2 値 (正，負のパルスや $\{0, 1\}$) の系列によって表現し，それを記録したり，送信したりする方式がある．このとき，上に述べた**雑音**の影響は，**図 0.2** に示すような遷移図として書かれる．

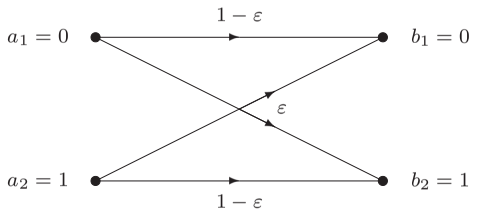

図 0.2 2 元対称通信路 (BSC).

この通信路モデルは **2 元対称通信路 (BSC)** と呼ばれ，ε は**ビット誤り率**と呼ばれる．

〔0.2.4〕 (一シンボル当たりの) 伝達情報量： さて，**図 0.2** に示した通信路を通して，送信シンボル一つ (a_i とする) を送信して，受信シンボル一つ (b_j とする) が受信される，という機能が通信の基本機能である．このとき，この通信によって，どれだけの情報が伝えられたのであろうか？

通信が行なわれる前，送信シンボル a_i の持っていた情報量は，$-\log_2 p_s(a_i)$ [ビット] であった．通信が行なわれた後を考えると，受信側では受信シンボル b_j が受信され，送信シンボル a_i の持っていた情報量は，$-\log_2 p_s(a_i)$ [ビット] から，$-\log_2 p_{s|r}(a_i|b_j)$ [ビット] に変化している．($p_{s|r}(a_i|b_j)$ は条件付き確率を表す)．送信シンボル a_i に関するこの情報量の変化分，

$$I(a_i; b_j) := -\log_2 p_s(a_i) - [-\log_2 p_{s|r}(a_i|b_j)] \tag{0.2}$$

は，a_i を送信して b_j が受信されたという『通信』によって送信側から受信側へ伝達された情報量と解釈することが出来る．

〔0.2.5〕 (一シンボル当たりの) 平均伝達情報量 $I(A; B)$： 情報源のエントロピー (平均情報量) を考えたのと同様に，伝達情報量 $I(a_i; b_j)$ の (**図 0.2** の) 通信システム全体に関する平均

$$I(A; B) := E\left[I(a_i; b_j)\right] = \sum_i \sum_j p_{s,r}(a_i, b_j) I(a_i; b_j) \tag{0.3}$$

を考え，さらに，$I(A,B)$ を送信シンボルの出現確率 $\{p(a_i)\}_i$ を変化させた最大値

$$C := \max_{\{p(a_i)\}} I(A;B) \tag{0.4}$$

を考える．C は，通信路 $\{p_{r|s}(b_j|a_i)\}$ だけで定まる，通信路固有の量で，**通信路容量**と呼ばれる．**図 0.2** の BSC の通信路容量は

$$C = 1 - \mathcal{H}_2 n(\varepsilon) \tag{0.5}$$

で与えられる．

通信路容量 C は，その通信路を使って伝達できる情報の量 (速度) を定める基本的な量であり，次の定理が成り立つ．(次は分かり易さのために，BSC に対して (大雑把な不正確な表現で) 述べているが，一般の通信路に対して (厳密な形で) 成立する)．

定理〔0.2.6〕 通信路容量が C である 2 元対称通信路 (**図 0.2**) を通して，$L := 2^k$ 個の情報シンボルの一つひとつを，$n-k$ 個の冗長シンボルを付け加えて長さ n の 2 元符号語に変換して伝達するものとする．すなわち，

$$\boldsymbol{c} = (c_1, c_2, \ldots, c_k, c_{k+1}, \ldots, c_n), \quad c_i \in \{0,1\} \tag{0.6}$$

のように，情報を表す $(c_1, c_2, \ldots, c_k)$ に対して，冗長シンボル $(c_{k+1}, \ldots, c_n)$ を付け加えた符号語を伝送する．

このとき，**情報伝達速度**「$R := k/n$」に対して，『$R < C$』であることが，情報を誤りなく伝達できるための必要十分条件である． □

この定理は**通信路符号化定理**と呼ばれる．この定理の実現を目指す技術が，第 2 章に述べる，誤り訂正符号である．

〔0.2.7〕 最後に，人為的な妨害などに抗して情報を安全に通信する技術であるが，これは「セキュリティ技術」と呼ばれ，その中心に「暗号技術」がある [6]．

1 情報源のモデルと情報量

1.1 情報源のモデル

〔1.1.1〕 図 1.1 に示すように，**情報源**は有限個の**シンボル**からなる**アルファベット**を有し，一定の**確率モデル**に従ってシンボルを発生するものとする．

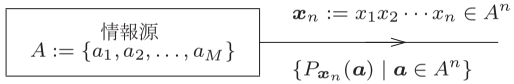

図 1.1 情報源モデル

以下に，このような確率モデルを自然言語に対して想定した場合について，例を考えてみよう．

例〔1.1.2〕 自然言語 (英語) のシミュレーション [3]：簡単のため，英語のアルファベットが，$A = \{a, b, c, \ldots, z, \sqcup\}$ で与えられる 27 文字 (シンボル) からなるものとする．

(i) すべてのシンボルが等確率 $(1/27)$ で独立に発生するとした場合：

$\{a, b, c, \ldots, z, \sqcup\}$ の各文字を書いたカードを各一枚ずつ箱の中に入れ，よくかき回して一枚取り出し，カードに書かれた文字を記録する．取り出したカードを箱に戻し，再びよくかき回してカードを取り出し，書かれた文字を記録する．この操作を繰り返すと，例えば，**表 1.1** に示すような文字列が得られる．

表 1.1 英語文字列の近似 (i) (等確率，独立生起)

xpoml␣rxkhrjffjuj␣zlpwcfwkcyj
ffjeyvkcqsghyd␣qpaamkbzaacibzlhjqd

(ii) 英語アルファベットの出現確率を考慮した場合：当然のことながら英語における各文字の出現確率は同じではない．一つの調査の結果を**表 1.2** に示す (例えば一冊の本に現れる，各文字の頻度を調べればこのような結果が得られる)．スペース (␣) の出現頻度が最も高く，1/5 に近い．これから，英語の単語は平均的に 4〜5 文字からなることが分かる．

シンボルの発生確率が**表 1.2** で，各文字は独立に生起するような情報源をシミュレートするには，$\{a, b, c, \ldots, z, ␣\}$ の各文字を書いたカードを**表 1.2** で与えられる頻度に比例した枚数 (例えば，スペースを 1859 枚，a を 642 枚，...) 用意し，箱の中に入れてよくかき回し，取り出した一枚のカードの文字を記録するといった，(i) と同様の操作を繰り返せば良い．すると，例えば**表 1.3** に示すような文字列が得られる．まだ不十分であるが，**表 1.1** に比べれば単語の長さなど，実際の英語に近い文字列が得られているといえよう．

(iii) さらに，実際の英語では各文字の生起は独立ではない．一つの文字が現

表 1.2 英語のアルファベットの生起確率

文字	生起確率	順位	文字	生起確率	順位
␣	0.1859	1	n	0.0574	7
a	0.0642	4	o	0.0632	5
b	0.0127	21	p	0.0152	19
c	0.0218	14	q	0.0008	25
d	0.0317	12	r	0.0484	9
e	0.1031	2	s	0.0514	8
f	0.0208	15	t	0.0766	3
g	0.0152	19	u	0.0228	13
h	0.0467	10	v	0.0083	22
i	0.0575	6	w	0.0175	17
j	0.0008	25	x	0.0013	24
k	0.0049	23	y	0.0164	18
l	0.0321	11	z	0.0005	27
m	0.0198	16			

表 1.3 英語文字列の近似 (ii) (独立，確率は**表 1.2**)

ocro␣hli␣rgwr␣nmielwis␣eu␣ll␣nbnesebya
th␣eei␣alhenhttpa␣oobttva␣nah␣brl

れたとき，それに続く文字の生起確率は文字によって大きく違う．例えば，英語では，the，this，that，these，those などの単語が頻繁に現れ，逆に tq··· のような単語は殆んど見られない．従って，$x_{n-1} = \mathrm{t}$ のとき，$x_n = \mathrm{h}$ である確率は**表 1.2** の値 (0.0467) より遥かに大きく，一方，$x_n = \mathrm{q}$ である確率は**表 1.2** の値 (0.0008) よりさらに小さいと想像される．このように，**条件付き確率**

$$p(x_n|x_{n-1}) \ : \ x_{n-1}, x_n \in A_0 := A \cup \{\emptyset\}$$

までもが与えられる情報源モデル[†1]を考えることにより，より精度良く英語をシミュレートできると考えられる．このような情報源を (単純) **マルコフ情報源**という． この考え方は，条件となる文字列が一般に k 文字である場合

$$p(x_n|x_{n-k}\cdots x_{n-1}) \ : \ x_{n-i} \in A_0 := A \cup \{\emptyset\}, \ i = 0, 1, \ldots, k$$

に拡張できる ($(k$ 重) **マルコフ情報源**)．**表 1.4** の (a)，(b) に $k = 1$ および $k = 2$ としたマルコフ情報源によって得られる文字列の例を示している．

1.2 情報の尺度

前節では，情報源が確率的モデルによって (近似的に) 記述できることを見た．本節では，情報源が確率的モデルで記述できるとき，情報がどのように測られるべきかを論じる[†2]．

---

†1 文字列の始まりを記述するために，空文字 $\emptyset$ を導入している．$x_n \in A$ に対し，$p(x_n|x_{n-1} = \emptyset)$ は**表 1.2** で与えられる確率とし，任意の $x_{n-1} \in A_0$ に対して $p(x_n = \emptyset|x_{n-1}) = 0$ と約束する．

†2 以下では簡単のため，各文字の生起が独立なモデルで解析を行なうが，マルコフモデルを用いても結果は同じであることに注意しておく．

表 1.4 英語文字列の近似 (iii) (マルコフ情報源)

(a) 単純マルコフ情報源

on␣ie␣antsoutinys␣are␣inctore␣st␣be␣s␣deamy
achin␣d␣ilonasive␣tucoowe␣at␣teasonare␣fuso
tizin␣andy␣tobe␣seace␣ctisbe

(b) 2 重マルコフ情報源

in␣no␣ist␣lat␣whey␣cratict␣froure␣birs␣grocid
pondenome␣of␣demonstures␣of␣the␣reptagin
is␣regoactiona␣of␣cre

1.2.1 情報の大小と加法性

〔1.2.1〕 ニュースの例 [4] : 次の 2 つのニュース

A : 夏至の 6 月 21 日，東京は雨でした.

B : 夏至の 6 月 21 日，東京は雪でした.

があったとして，どちらのニュースの情報が大きいかを考えてみよう．梅雨の 6 月後半，東京が雨ということは，聞かなくても十分予想できる．一方，夏に入ったこの時期に東京に雪が降ったとすれば，これは驚きである．「情報量」という意味では，A の情報に比べて B の情報が大きい，と言えると考えられる．すなわち，ニュースの情報源を確率モデルで捉えれば，

「A の確率 $>$ B の確率」 $\Rightarrow$ 「A の情報 $<$ B の情報」

が成立することになる．すなわち，情報量を確率 p の関数として，$I(p)$ で表すことにすれば，

$$p_1 < p_2 \Rightarrow I(p_1) > I(p_2) \tag{1.1}$$

が成立することになる．

〔1.2.2〕 次に, 6 月 21 日の東京とニューヨークの天気を考えてみよう．その日，

A : 東京は雨， **B** : ニューヨークは晴れ

であったとしよう．東京とニューヨークは遠く離れており，その天気は無関係 (独立) であると考えられる．すなわち,「A : 東京が雨」の確率 $p(A)$,「B : ニューヨークが晴れ」の確率 $p(B)$ と，「東京が雨」かつ「ニューヨークが晴れ」の確率 $p(A \cap B)$ に関して，

$$p(A \cap B) = p(A)p(B) \tag{1.2}$$

が成立する．

ところで,「東京が雨」かつ「ニューヨークが晴れ」であることを知ることは,「東京が雨」で「ニューヨークが晴れ」であることを別々に知った場合と，得られる情報に関して何も変わらない．このことを情報量 $I(p)$ によって表せば,

$$I(p(A)p(B)) = I(p(A)) + I(p(B)) \tag{1.3}$$

が成立することになる．

〔1.2.3〕 (トランプ) カードの特定 : カードにおいて，52 枚のカードから一枚を引いたとき，それが「ハートである確率」は 1/4,「Queen である確率」は 1/13,「ハートの Queen である確率」は 1/52，などである．また，引いたカードが「ハートである」ことと「Queen である」こととは独立である．

このとき，カードが「ハートの Queen」であることを知ったときに得られる情報量 $I(1/52)$ は，カードが「ハート」であることを知ったときに得られる情報量 $I(1/4)$ とカードが「Queen」であることを知ったときに得られる情報量 $I(1/13)$ との和に等しく，式 (1.3) の関係

$$I(1/52) = I((1/4)(1/13)) = I(1/4) + I(1/13)$$

が成立する．

1.2.2 情 報 の 尺 度

前節で，情報の尺度 $I(p)$ が満たすべき条件として，式 (1.1)，(1.3) が得られた．情報の尺度 $I(p)$ は，これらの条件から一意に決まる．

定理〔1.2.4〕 $I(x)$ $(0 < x \leqq 1)$ を

$$\text{(i) } I(xy) = I(x) + I(y), \quad \text{(ii) } I(x) < I(y) \text{ if } x > y \tag{1.4}$$

を満たす「微分可能」な関数とする．すると，$I(x)$ は

$$I(x) = -K \log x, \quad K > 0 \tag{1.5}$$

で与えられる．($I(x)$ を「連続」な関数としても結果は変わらない [3]).

(証明) **(1)** 式 (1.4) の第一式において $x = y = 1$ とおけば,

$$I(1) = I(1) + I(1) \quad \therefore\ I(1) = 0.$$

(2) $I(x)$ は微分可能であるから，式 (1.4) の第一式の両辺を x で微分すれば，$yI'(xy) = I'(x)$．ここで，$x = 1$ とすれば，$yI'(y) = I'(1)$．すなわち,

$$I'(x) = \frac{1}{x} I'(1)$$

が成立する．(文字を y から x に変更している).

(3) 従って，$k := I'(1)$ とおいて両辺を積分すれば,

$$I(x) = \int \frac{k}{x} dx = k \log_e x + C$$

が得られる．ただし，C は積分定数である．ここで $I(1) = 0$ に注意すれば，$C = 0$ が得られる．すなわち,

$$I(x) = k \log_e x. \tag{1.6}$$

最後に, 式 (1.4) の第二式の条件より, 式 (1.6) の定数 $k = -K$ は “負” $(K > 0)$ でなければならないことが導かれる.

〔1.2.5〕 上記の定理により，情報の測り方は，本質的に式 (1.5) で与えられることが明らかとなった．あとは，式 (1.5) において，定数 K と対数の底をどう

選ぶかである．これは，長さをメートルで測るのかヤードで測るのか，あるいは重さをキログラムで測るのかポンドで測るのかといった類の議論である.

情報の単位としては,

(1) $K = 1$, 対数の底 $= 2 \Rightarrow I(p) = -\log_2 p$ [bit]

(2) $K = 1$, 対数の底 $= e \Rightarrow I(p) = -\log_e p$ [nat]

が良く使われる．特に，実用上はビット (bit) が，また理論解析などではナット (nat) が良く使われる.

1.3 平均情報量 (エントロピー)

〔1.3.1〕 以上により，情報源 $A = \{a_1, a_2, \ldots, a_M\}$ から一つのシンボル a_i が出てきたとき，その情報量は，$I[p(a_i)] = -\log_2 p(a_i)$ [bit/symbol] で与えられる，とすることの妥当性が示された.

一方，情報源 A 全体を論じる必要が屡々生じる．そのとき最も良く取り扱われる量は，各シンボルの情報量の情報源 A 全体に関する平均

$$H(A) := \sum_{a_i \in A} p(a_i) I[p(a_i)] = -\sum_{i=1}^{M} p(a_i) \log_2 p(a_i) \tag{1.7}$$

である．式 (1.7) の $H(A)$ は，情報源 A の**平均情報量**あるいは**エントロピー**と呼ばれる．$M = 2$ のとき，$p(a_1) =: x$, $p(a_2) = 1 - x$ とし，式 (1.7) の $H(A)$ を x の関数として

$$\mathcal{H}_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \tag{1.8}$$

と表すと，エントロピー $\mathcal{H}_2(x)$ の形状は，**図 1.2** のように与えられる.

エントロピー $H(A)$ が情報圧縮の限界を与えることは，〔0.2.2〕に述べたとおりである.

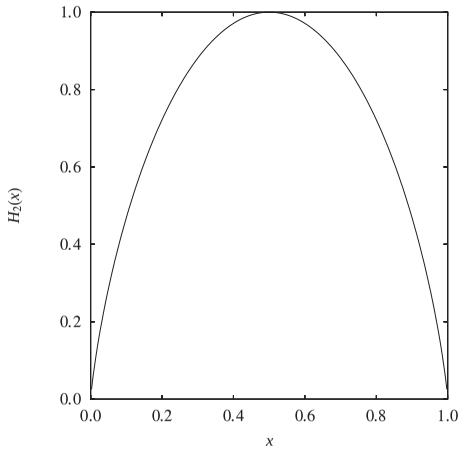

図 1.2 エントロピー関数 $\mathcal{H}_2(x)$ の形状.

章 末 問 題

1.1 次の関数方程式を解け (条件を満足する関数 $f(x)$ を求めよ). ただし関数 $f(x)$ は微分可能と仮定して良い.

(1) $f(x+y) = f(x) + f(y)$
(2) $f(x+y) = f(x)f(y)$
(3) $f(x+y) = f(x) + f(y) + f(x)f(y)$
(4) $f(xy) = f(x) + f(y)$
(5) $f(xy) = f(x)f(y)$
(6) $f(xy) = f(x) + f(y) + f(x)f(y)$

1.2 〔1.3.1〕に述べたエントロピー $\mathcal{H}_2(x)$ (式 (1.8)) の形状が, **図 1.2** のように与えられることを確認せよ.

2 誤り訂正符号

本章では通信システムや計算機システムの多くの場面で広く使われている「誤り訂正符号」について概説する. その数学的基礎は「有限体」にある. そして有限体の基礎になっているのが「ユークリッドの互除法」である. 有限体は計算機システムにおいて誤差のない計算手段を提供するものであり, その応用は誤り訂正符号に限られない.

2.1 有 限 体

2.1.1 体

〔2.1.1〕体とは, 簡単にいうと, 足し算, 引き算, 掛け算, 割り算の『四則演算ができる数の集合』のことである. 有理数体, 実数体, 複素数体などは我々が良く知っている (と思っている) 体の例である.

〔2.1.2〕 上に四則演算といったが, もう少し正確にいうと, 基本的な演算は足し算 (加算ともいう) と掛け算 (乗算ともいう) の 2 種類である.

体には, その任意の要素 a に対して $a + a' = 0$ となる要素 a' の存在が要請されている. この要素 a' を通常 $-a$ と表し, 足し算

$$b + a' = b + (-a)$$

を $b - a$ と書いて, "b から a を引く (引き算する)" といっている訳である.

同様に, 体には "0" を除く任意の要素 a に対して $a \times a' = 1$ となる要素 a'

の存在が要請されている．この要素 a' を通常 a^{-1} あるいは $1/a$ と表し，掛け算

$$b \times a' = b \times a^{-1} = b \times (1/a)$$

を b/a と書いて，“b を a で割る (割り算する)” といっている訳である．

従って，『四則演算のできる数の集合』といった体は，

『任意の a に対して $-a$ が存在し，また任意の $a\ (\neq 0)$ に対して a^{-1} が存在して，足し算，掛け算が自由にできる数の集合』

であるとするのが，より正確な表現である．

以上に述べた体の定義をややフォーマルに表現すると以下のようになる．

〔2.1.3〕群：　集合 G の任意の要素 x, y に対して，2 項演算 $x * y (\in G)$ が定義され，次の条件 (G-1) から (G-3) を満たすとき，G を**群**という．以上に加えて条件 (G-4) も満たすとき，G を**可換群**という．

(G-1)　**結合律** $x * (y * z) = (x * y) * z$ が成立する．

(G-2)　**単位元**と呼ばれる特別の元 $e \in G$ が存在して，任意の $x \in G$ に対して，$x * e = e * x = x$ が成立する．

(G-3)　任意の $x \in G$ に対して，**逆元**と呼ばれる $y \in G$ が存在して，$x * y = y * x = e$ が成立する．

(G-4)　**可換律** $x * y = y * x$ が成立する．　□

演算が加法 $+$ である群においては，単位元 e を**零元**と呼んで 0_G などと表し，逆元 x^{-1} を**負元**と呼んで $-x$ と表すことが多い．

また，演算が乗算 $\cdot$ である群においては，単位元 e を 1_G などと表す．

〔2.1.4〕体：　集合 $\mathbb{F}$ の任意の要素 x, y に対して，“和” $x + y (\in \mathbb{F})$ と “積” $xy (\in \mathbb{F})$ が定義され，次の条件を満たすとき，$\mathbb{F}$ を**体**という．

(F-1)　$\mathbb{F}$ は加法 $(+)$ に関して “可換群” を成す．

(F-2)　$\mathbb{F}^\times := \mathbb{F} \setminus \{0_\mathbb{F}\}$ とするとき，$\mathbb{F}^\times$ は乗法に関して “可換群” を成す．

(F-3)　**分配律**，すなわち，$\forall x, y, z \in \mathbb{F}$ に対して，

$$x(y + z) = xy + xz, \quad (x + y)z = xz + yz$$

が成り立つ．　□

2.1.2 整　数

〔2.1.5〕 整数の集合を $\mathbb{Z}$，自然数の集合を $\mathbb{N}$ で表す．すなわち，$\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$，$\mathbb{N} := \{1, 2, \ldots\}$．整数や自然数の基本的性質については既知とする．

〔2.1.6〕 (整数に関する) **整除の関係**：　$n, m \in \mathbb{Z}, m > 0$ とすると，

$$n = qm + r, \quad 0 \leqq r < m \tag{2.1}$$

を満たす整数 q, r が一意に定まる (数直線を認めれば自明)．式 (2.1) において，q を**商**，r を**余り**という．また，n を m で割った余り r を，次の記号で表す：

$$\langle n \rangle_m . \tag{2.2}$$

〔2.1.7〕 式 (2.1) において，$r = 0$ のとき，m は n を**割り切る**といい，

$$m | n \quad (\Leftrightarrow n = qm,\ q \in \mathbb{Z})$$

と書く．特に，0 はすべての整数で割り切れる $(0 = 0m + 0)$．また，1 はすべての整数を割り切る $(n = n \times 1 + 0)$.

〔2.1.8〕公約数と最大公約数：$a, b \in \mathbb{Z}$ が与えられ，$d > 0$ が，$d | a$ 且つ $d | b$ を満たすならば，d を a と b の**公約数**という．

さらに，a と b の任意の公約数 $d' (> 0)$ に対して，$d' | d$ が成立するとき，$d (> 0)$ は，a と b の**最大公約数**と呼ばれ，$\gcd(a, b)$ で表される．

〔2.1.9〕素数：　$p\ (\geqq 1) \in \mathbb{Z}$ が，任意の $n \in \mathbb{Z}$ に対して，

“$n | p \Rightarrow n = 1$ or $n = p$”　(p と 1 だけが約数)

を満たすとき，p は**素数**と呼ばれ，そうでなければ**合成数**と呼ばれる．

2.1.3 ユークリッドの互除法

〔2.1.10〕ユークリッドの互除法：　2つの整数 r_0 と r_1 の最大公約数は，整除の関係式 (2.1) に基づいて以下のように求められる．

与えられた $r_0, r_1 \in \mathbb{Z}\ (r_1 > 0)$ に対して，r_0 を r_1 で割った商を q_1，余りを r_2 とする．次に，r_1 を r_2 で割り，商を q_2，余りを r_3 とする．以下同様の操作を繰り返す．このとき，$r_1 > r_2 > r_3 > \cdots$ であるので，有限の $k \in \mathbb{N}$ において，$r_{k+1} = 0$ が成立する．すなわち，

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, && r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && r_3 < r_2 \\
&\vdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, && r_k < r_{k-1} \\
r_{k-1} &= q_k r_k + r_{k+1}, && r_{k+1} = 0
\end{aligned}$$

が成立する．このとき，r_k が r_0 と r_1 の最大公約数である．

(証明)　互除法のアルゴリズムを行列表現すれば，

$$\begin{aligned}
\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} \\
&= \cdots = \left\{ \prod_{i=1}^{k} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \right\} \begin{pmatrix} r_k \\ 0 \end{pmatrix}. \qquad (2.3)
\end{aligned}$$

よって，$\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \prod_{i=1}^{k} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ とおけば，a, b, c, d は整数で

$$r_0 = a r_k, \quad r_1 = c r_k.$$

すなわち，r_k は r_0 と r_1 の公約数である．

一方，簡単に分かるように $\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ であるから，式 (2.3) より

$$\begin{pmatrix} r_k \\ 0 \end{pmatrix} = \left\{ \prod_{i=k}^{1} \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \right\} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

が得られ[†1]，$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \prod_{i=k}^{1} \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ とおけば，a', b', c', d' は整数で

$$r_k = a' r_0 + b' r_1. \qquad (2.4)$$

ここで，d を r_0 と r_1 の公約数，すなわち，$r_0 = d d_0$，$r_1 = d d_1$ とすれば，

$$r_k = a' d d_0 + b' d d_1 = d(a' d_0 + b' d_1)$$

が得られ，$d | r_k$ が成立する．よって，r_k は最大公約数である．

系〔2.1.11〕式 (2.4) より，

$$\exists x, y \in \mathbb{Z}, \quad ax + by = \gcd(a, b) \qquad (2.5)$$

が成立する．特に，次の重要な関係が成立する：

$$\gcd(a, b) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z},\ ax + by = 1. \qquad (2.6)$$

(証明)　式 (2.6) の証明：$\Rightarrow$) 式 (2.5) より自明．　$\Leftarrow$) 条件式の左辺 $(ax + by)$ は $\gcd(a, b)$ で割り切れるが，右辺はそれが 1 であることを表している．　□

2.1.4 有限体 (素体)

〔2.1.12〕要素数が有限の体を**有限体**という．有限体の要素数は素数 $p\ (\geqq 2)$ の冪乗

$$|\mathbb{F}| = p^n \qquad (2.7)$$

であることが知られている．特に，要素数が素数である有限体を**素体**という．

[†1]　積の順序に注意．$\prod_{i=1}^{k} a_i = a_1 a_2 \cdots a_k$，$\prod_{i=k}^{1} a_i = a_k a_{k-1} \cdots a_1$ である．

〔**2.1.13**〕$p\ (\geqq 2)$ を素数として，

$$\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\} \tag{2.8}$$

とおき，$x, y \in \mathbb{F}_p$ の和 $(\oplus)$ と積 $(*)$ を

$$x \oplus y := \langle x + y \rangle_p, \quad x * y := \langle xy \rangle_p \tag{2.9}$$

で定義する．すると，$\mathbb{F}_p(\oplus, *)$ は要素数が p の素体となる．

(証明) 体の他の条件が満たされることは容易に確かめられるので，乗法に関する逆元の存在だけを示す．

$a \in \mathbb{F}_p^{\times} := \mathbb{F}_p \setminus \{0\}$ とすると，$\gcd(a, p) = 1$ に注意すれば，式 (2.5) より，整数 x, y が存在して

$$ax + py = \gcd(a, p) = 1.$$

このとき明らかに $p \nmid x$ であり，両辺でそれぞれ p で割った余りを取れば，$\mathbb{F}_p(\oplus, *)$ における a の逆元が $\langle x \rangle_p$ で与えられることは直ちに分かる． □

〔**2.1.14**〕素体の例として，$\mathbb{F}_2$ と $\mathbb{F}_3$ の演算規則を**表 2.1**，**表 2.2** に示す．

表 2.1　$\mathbb{F}_2 = \{0, 1\}$ における演算

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

表 2.2　$\mathbb{F}_3 = \{0, 1, 2\}$ における演算

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

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.1.5 拡　大　体

〔**2.1.15**〕$\mathbb{F}_p$ を要素数が p の素体とし，$f(x)$ を $\mathbb{F}_p$ 係数の n 次**既約多項式** (因数分解の出来ない，次数 n の多項式) とする．このとき，

$$\mathbb{F} := \left\{ \sum_{i=0}^{n-1} a_i x^i \;\middle|\; a_i \in \mathbb{F}_p \right\} \tag{2.10}$$

とおき，$g(x), h(x) \in \mathbb{F}$ の和 $(\oplus)$ と積 $(*)$ を

$$\left.\begin{aligned} g(x) \oplus h(x) &:= \langle g(x) + h(x) \rangle_{f(x)}, \\ g(x) * h(x) &:= \langle g(x)h(x) \rangle_{f(x)} \end{aligned}\right\} \tag{2.11}$$

で定義すれば，$\mathbb{F}(\oplus, *)$ は要素数が p^n の有限体となる．

(証明) 多項式は整数と同様の代数的性質を持っており，整除の関係，ユークリッドの互除法が成立する．そのため，本質的に素体 $\mathbb{F}_p$ の場合と同様の議論が展開できる．すなわち，$a(x) \in \mathbb{F}^{\times} := \mathbb{F} \setminus \{0\}$ とすると，$f(x)$ が既約多項式であることから $\gcd(a(x), f(x)) = 1$ が成立し，式 (2.5) より整数の場合と同様に $a(x)$ の逆元 $(\in \mathbb{F}(\oplus, *)\ )$ の存在が示される． □

〔**2.1.16**〕詳細は割愛するが，有限体は本質的に式 (2.10) に与えた形のものですべてである．最も簡単な例として，$\mathbb{F}_2$ 係数の 2 次既約多項式 $f(x) = x^2 + x + 1$ によって構成される 2 次の拡大体 $\mathbb{F}_{2^2}$ の演算規則の表を**表 2.3** に示している．

〔**2.1.17**〕補足であるが，複素数体は実数体の 2 次の拡大体である．通常既約多項式としては $f(x) = x^2 + 1$ をとるが，本質的には判別式が負の，実係数 2 次多項式であれば何でも良い．また，『代数学の基本定理 (Gauss)』から導かれ

表 2.3　$\mathbb{F}_{2^2} = \{0, 1, x, 1 + x\}$ における演算

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

るように，実係数既約多項式の次数は高々 2 次である．これから，実数体の拡大体は複素数体だけであることが分かる．これに対して，有限体ではすべての次数 (自然数) の拡大体が存在する．

2.2 誤り訂正符号

通信路で生じる誤りを訂正し，より信頼性の高い通信を行う技術として**誤り訂正符号**がある．ここでは最も簡単な例として，**ハミング符号**について概説する．より一般的な誤り訂正符号である **BCH 符号**などについては，[4, 5] などを参照されたい．誤り訂正符号の基礎となるのが，上に述べた「有限体」である．誤り訂正符号は，有限体の上に構築される実用性と理論的美しさを備えた技術といえる．

2.2.1 ハミング符号

〔2.2.1〕ハミング符号は，k ビットの**情報ビット**に $n-k$ ビットの**冗長ビット**を付け加えて構成される**符号長** n の**単一誤り訂正符号**である．

次の例は，ハミング [7,4] 符号と呼ばれる符号で

$$H = \left(\begin{array}{ccc:cccc} 1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1 \end{array}\right) = (I, P) \tag{2.12}$$

で与えられる行列 (**パリティ検査行列**と呼ばれる) に対して，符号 $\mathcal{C}$ (符号語 $\boldsymbol{c}$ の集合) は，

$$\mathcal{C} = \{\boldsymbol{c} = (c_0, c_1, \ldots, c_6) \mid \boldsymbol{c}H^T = \boldsymbol{0}, c_i \in \mathbb{F}_2\} \tag{2.13}$$

として定義される[†1]．ただし，H^T は行列 H の転置を表す．行列の掛け算の規則等は通常通りであるが，$\mathbb{F}_2$ は 0 と 1 の 2 要素だけから成る**有限体** (式 (2.8) で $p = 2$ の場合) を表し，演算の結果は “2 で割った余り” を考える ($\bmod 2$ による演算ともいう)．

[†1] 一般に 2 元ハミング符号は，長さ m の非零の 2 列元ベクトルすべてを並べて得られるパリティ検査行列 H によって定義される．従って，そのパラメタは「$n = 2^m - 1$, $k = n - m, (m = 2, 3, \ldots)$」で与えられる．式 (2.12) は $m = 3$ の場合である．

〔2.2.2〕 式 (2.12)，(2.13) で与えられるハミング [7,4] 符号は，

$$H = (I, P),\ \boldsymbol{c} = (\boldsymbol{p}, \boldsymbol{i}),\ \boldsymbol{p} = (p_0, p_1, p_2),\ \boldsymbol{i} = (i_0, i_1, i_2, i_3) \tag{2.14}$$

とおくと，

$$\begin{aligned} &\boldsymbol{c}H^T = (\boldsymbol{p}, \boldsymbol{i})\begin{pmatrix} I \\ P^T \end{pmatrix} = \boldsymbol{p} + \boldsymbol{i}P^T = \boldsymbol{0}, \\ &\therefore)\ \boldsymbol{p} = -\boldsymbol{i}P^T,\ \text{即ち},\ \boldsymbol{c} = \boldsymbol{i}(-P^T, I) =: \boldsymbol{i}G \end{aligned} \tag{2.15}$$

のように表すこともできる．このとき，$G := (-P^T, I)$ を**生成行列**という．式 (2.12) の H に対応する生成行列は

$$G = (-P^T, I) = \left(\begin{array}{ccc:cccc} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 1&1&1&0&0&1&0 \\ 1&0&1&0&0&0&1 \end{array}\right) \tag{2.16}$$

のようになる ($\mathbb{F}_2$ では $-1 = 1$ であることに注意)．

〔2.2.3〕 式 (2.15)，(2.16) より，例えば，情報 $\boldsymbol{i} = (1111)$ に対する符号語は，$\boldsymbol{c} = \boldsymbol{i}G = (1111111)$ で与えられる．今，この符号語が送信されて，第 1 ビット目の 1 が 0 に誤り，受信語 $\boldsymbol{r} = (0111111)$ が受信されたとしよう．このとき，誤り訂正の操作は以下のように行われる．

まず，**シンドローム**と呼ばれる $\boldsymbol{s} := \boldsymbol{r}H^T$ を計算する．この結果は，今考えている例の場合，$\boldsymbol{s} = (100)$ となり，パリティ検査行列 H の “第 1 列目” と一

致する．この結果から，復号器は受信語 $\boldsymbol{r}$ の“第 1 ビット”目が誤っていたと判断し，次のように訂正を行なう：

$$\boldsymbol{r} = (0111111) \to (11111111).$$

〔2.2.4〕 この誤り訂正のメカニズムをより一般的に見れば，例えば符号語第 1 ビット目の誤りは，送信語 $\boldsymbol{c}$ に誤りベクトル $\boldsymbol{e} = (1000000)$ が加わって，$\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ が受信されると表現できる．このとき，シンドローム $\boldsymbol{s}$ は

$$\boldsymbol{s} = \boldsymbol{r}H^T = \boldsymbol{c}H^T + \boldsymbol{e}H^T = \boldsymbol{e}H^T$$

となる (符号の定義式 (2.13) より $\boldsymbol{c}H^T = \boldsymbol{0}$ であることに注意)．従って，誤りベクトル $\boldsymbol{e}$ が $\boldsymbol{0}$ であれば (誤りがなければ) シンドロームは $\boldsymbol{0}$ となり，第 k ビット目に誤りがあれば H^T の第 k 行目 (H の第 k 列目の転置) がシンドローム $\boldsymbol{s}$ として得られる．パリティ検査行列 H はすべての列ベクトルが異なっているため，誤りが 1 個以下ならばどのビットに誤りが生じたかを特定できるのである．

章 末 問 題

2.1 $\mathbb{F}_2$ 係数の多項式 $f(x) = x^2 + x + 1$ が既約であることを示せ．

2.2 **表 2.2**，**表 2.3** に示した演算規則が正しいことを確認せよ．

2.3 最も簡単な 2 元「単一誤り訂正」符号：パリティ検査行列が $H = \begin{pmatrix} 1\,0\,1 \\ 0\,1\,1 \end{pmatrix}$ で与えられる 2 元線形符号を考える．(p. **21** 脚注 **1** で，$m = 2$ の場合)．

(1) 生成行列が $G = (111)$ で与えられることを示せ．このとき，符号語は $\boldsymbol{c}_0 = (0)G = (000)$，$\boldsymbol{c}_1 = (1)G = (111)$ の 2 つ (だけ) で与えられ，明らかに「単一誤り訂正」符号となる．(この符号は，その符号語の形から「繰り返し符号」と呼ばれる)．

(2) 一般に，符号長 $n = 2t + 1$ の「繰り返し符号」は，t 個までの誤りを訂正可能である．これを示せ．

引用・参考文献

1) C.E. Shannon: “A Mathematical Theory of Communication,” *Bell System Tech. J.*, vol.27 pp.397–423, 623–656, 1948

2) C.E. Shannon, W. Weaver: *The Mathematical Theory of Communication*, Univ. of Illinois Press, 1949 (邦訳 : (1) 長谷川淳，井上光洋「コミュニケーションの数学的理論」，明治図書，1969; (2) 植松友彦「通信の数学的理論」，ちくま学芸文庫， 2009)

3) 宮川 洋: 情報理論, コロナ社，1979

4) 宮川 洋，原島 博，今井 秀樹: 情報と符号の理論，岩波講座情報科学 4，岩波書店，1983

5) 坂庭好一，渋谷智治: 代数系と符号理論入門，コロナ社，2010

6) 黒澤 馨，尾形わかは: 現代暗号の基礎数理，電子情報通信学会編，コロナ社，2004

索　　引