

ま え が き

本書は、通信理論の解説書である。ここでいう通信とは、距離あるいは時間の隔たりを越えて情報を伝達/交換することを指す。東京から大阪の友人に電話やメールをしたり、映像や音楽を記録メディアに記録し、あとで観賞したりするのは、距離ならびに時間を越えた通信の例である。

例えば、人間の発する声/言葉などの情報を即時に遠方まで運ぶには、声などをそれが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。

電気通信においては、人や計算機などが発する情報を距離的あるいは時間的に隔たった宛先(相手)へ届けるため、送信機などと呼ばれる装置によって情報を加工して光(電磁波)や電気信号に変換し、通信路(自由空間や光ファイバケーブルや記録媒体など)を通して、宛先(受信側)へ伝達する。受信側では、受信機などと呼ばれる装置によって、受信された電気信号から人や計算機が発した元の情報を復元することになる。このとき、いずれの通信路においても

(a) 物理的な障害(雑音、帯域制限、歪など)、(b) 人為的な妨害などが存在するため、送信された信号がそのまま形を変えずに受信側に現れることはない。したがって、これらの妨害を克服して、情報をいかに、

(1) 「正確」、かつ (2) 速く(大量に)、そして (3) 安全に
伝えるか、が通信工学の課題となる^{†1}。通信理論の目的は、上記の(1)、(2)、(3)を最大限実現する通信方式の解明にある。

まず情報を「速く」あるいは「大量に」という要請であるが、これに答えるためには、そもそも情報はどう測られるべきかを知らなくてはならない。その答えは2章に述べられている。

^{†1} 「正確」であることは大前提である。不正確な情報をいくら速く送っても意味がない。

すると次には、情報表現の冗長性が問題になる。一つのことを1回話しても、3回話しても、相手に伝わる本質的な情報の量は変わらないと考えられる。3回話すのは無駄で1回話せば十分ということである。自然言語などは普通多くの無駄を含む。このような無駄(冗長性)を除くと、情報はどこまで短く簡潔に表現できるであろうか? 「情報圧縮の限界」と「その限界を達成する方法」が3章、4章に述べられている。

次に、与えられた通信路を通して、情報を伝達しようとしたとき、誤りなく伝達できる情報量の限界が問題になる。上に述べたように、通信路には雑音などの妨害が存在する。このとき、その雑音の性質や大きさにより、各通信路は「通信路容量」と呼ばれる、通信路固有の特徴量 C を持つことが示される(5章)。ここで、 k シンボルで表される情報に $n - k$ 個の冗長シンボルを付け加え、 n シンボルの符号語に変換して通信路に送出するとする。すると、情報伝達のスピード $R := k/n$ が $R < C$ を満たすならば、冗長シンボルを「うまく」選ぶことにより、この通信路を通して誤りなく情報を伝達できることが示される。この事実は通信路符号化定理として知られ、通信理論の最も重要な結果の一つである(6章)。近年この情報伝達速度の限界(通信路容量)を達成する具体的な符号の有力な候補としてLDPC符号が注目されている。本書ではその入門的な解説をやや丁寧に述べるようにした(6章)。

最後に、悪意のない単なるミスを含む人為的な妨害による情報の変化などを排して情報を安全に通信することが要請される。このための技術が「セキュリティ技術」であり、その中心に「暗号技術」がある。これに関する入門的解説を述べたのが8章である。

さて、本書を著すにあたっては次の点に留意した。必要な予備知識はできるだけ少ないこと、しかし証明などは省かず本書だけで完結して読み切れること、である。具体的には、予備知識としては大学入学程度の数学的基礎だけを仮定し、残りは本書を読み進むことによって理解できるよう、一通りの証明は漏らさないように心掛けた。そのため、いくつかの章に付録という形で、必要な数学的基礎事項をまとめている。

本書の内容は、基本的にシャノン (C.E. Shannon) によって提唱された「通信の数学的理論 (A Mathematical Theory of Communication)」(巻末の参考文献 1)) に述べられた内容である。日本では、この内容の書物は「情報理論」ということが多い。しかし本書では原点に立ち返るという意味でも、また内容をよりの確に表す意味でも「通信理論」とすることが適切と考えた。また記述に関しても、できるだけ原典に近い記述を心掛けるように努めた。科学技術を切り開いてきた先人達の考え方に触れることは、自らが新しい発見をしていく際の助けになるであろうと考えたからである。

講義のテキストとして使用されるときには、多少具体的な例を付け加えて説明いただくとよいように考える。学生はこれにより、話の概要を理解し、その後このテキストを読み返すことで、数学的/理論的内容まで理解を進めることができるようになると期待される。

世の中に通信理論 (情報理論) に関する名著/良書は少なくない。したがって、本書にどれほどの存在意義があるかについては疑問が残らないわけではないが、上に述べた点において、内容/記述法において多少の特色はあるものとする。本書が、通信理論を学ぼうとする学生諸君にとって、何らかの意味でお役に立つことができれば、著者にとって望外の喜びである。

最後に、原稿に目を通して多くの貴重な指摘とコメントをいただいた、神奈川県大学野崎隆之博士に感謝する。また辛抱強く原稿を待つて下さったコロナ社に感謝する。

平成 26 年 7 月

坂庭好一，笠井健太

目 次

1. 通信理論の概要

1.1 通信の目的とモデル	1
1.2 通信理論の概要と本書の構成	3
1.3 付録：確率の初歩	6
1.3.1 テイラー展開とロピタルの定理	7
1.3.2 確率空間	8
1.3.3 確率変数と平均	9
1.3.4 特性関数	13
1.3.5 中心極限定理	14
章末問題	16

2. 情報源のモデルと情報量

2.1 情報源のモデル	17
2.2 情報の尺度	21
2.2.1 情報の大小と加法性	22
2.2.2 情報の尺度	23
2.3 平均情報量 (エントロピー)	25
章末問題	28

3. 情報源符号化定理

3.1 情報源符号	29
3.1.1 符号化と復号化	29
3.1.2 符号の例	30
3.2 クラフト・マクミランの定理	32
3.2.1 符号化 (情報表現の変換)	33
3.2.2 クラフト・マクミランの定理	37
3.3 情報源符号化定理	40
3.3.1 情報源の拡大	41
3.3.2 情報源符号化定理	41
章末問題	44

4. 代表的な情報源符号

4.1 情報源符号の機能	45
4.2 2元ハフマン符号	46
4.2.1 2元ハフマン符号の例	46
4.2.2 2元ハフマン符号の構成法	48
4.2.3 ハフマン符号の性質	50
4.2.4 多元ハフマン符号	55
4.3 イライアス符号	56
4.4 イライアス符号を用いたユニバーサル符号	67
4.5 ジブ・レンベル符号	74
4.5.1 増分分解	75
4.5.2 符号化	76

4.5.3 復号化	77
4.5.4 漸近的最良性	79
4.6 ワイル符号	86
4.7 付録：凸関数といくつかの不等式	90
章末問題	93

5. 通信路モデルと通信路容量

5.1 通信路のモデル	94
5.1.1 通信システムの実例	94
5.1.2 一般の離散無記憶通信路	97
5.1.3 伝達情報量 (相互情報量)	99
5.2 通信路容量	102
5.2.1 数学的準備	102
5.2.2 通信路容量	105
5.2.3 基本的な通信路の通信路容量	109
章末問題	116

6. 通信路符号化定理

6.1 情報伝達の例と通信路符号化定理	117
6.2 最大事後確率復号法と最尤復号法	118
6.3 (順)符号化定理	124
6.3.1 通信システムのモデルと (順)符号化定理	124
6.3.2 誤り確率の上界	125
6.3.3 ギャラガー関数とその性質	130
6.3.4 符号化定理の証明	132

6.4	逆符号化定理	134
6.4.1	弱い逆符号化定理	135
6.4.2	強い逆符号化定理	138
6.5	簡単な誤り訂正符号	142
6.5.1	有 限 体	143
6.5.2	距離, 重みと限界距離復号法	143
6.5.3	加法的通信路と限界距離復号	145
6.5.4	単一誤り訂正符号 (ハミング符号)	146
6.6	低密度パリティ検査 (LDPC) 符号	148
6.6.1	LDPC 符号と Sum-Product アルゴリズム	148
6.6.2	2 元消失通信路 (BEC) における性能評価	163
	章 末 問 題	175

7. 連続情報と連続通信路

7.1	連続情報源と連続通信路	176
7.2	アナログ信号からデジタル信号へ	177
7.3	連続標本値のエントロピー	181
7.3.1	連続標本値のエントロピー	181
7.3.2	多次元エントロピー	183
7.4	帯域制限 AWGN 通信路の通信路容量	184
7.4.1	帯域制限 AWGN 通信路	184
7.4.2	帯域制限 AWGN 通信路の伝達情報量	187
7.4.3	帯域制限 AWGN 通信路の通信路容量	188
7.4.4	離散的通信路との比較	191
7.4.5	通信路符号化定理 (再掲)	193
7.5	付録: 電力スペクトル密度と白色雑音	194

7.5.1 相 関 関 数	194
7.5.2 電力スペクトル密度	194
章 末 問 題	197

8. 情報セキュリティの基礎 — 暗号理論の初歩 —

8.1 暗号の考え方と共通鍵暗号系	198
8.1.1 暗号システム	198
8.1.2 共通鍵暗号の代表例	199
8.2 公開鍵暗号系	202
8.2.1 公開鍵暗号系の基本構成	203
8.2.2 公開鍵暗号系の成立条件	204
8.2.3 デジタル署名 (認証) の改良	205
8.3 公開鍵暗号成立の根拠	206
8.3.1 素因数分解と離散対数	207
8.3.2 素数判定アルゴリズム	208
8.4 公開鍵暗号系の具体例 (I) : RSA 暗号	209
8.5 公開鍵暗号系の具体例 (II) : ラビン暗号	211
8.5.1 2次多項式の求解 — ラビン暗号の復号 —	212
8.5.2 ラビン暗号の構成	215
8.6 公開鍵暗号系の具体例 (III) : 逆数暗号	216
8.7 公開鍵暗号系の具体例 (IV) : エルガマル暗号	219
8.8 付録 : 初等整数論の基礎	220
8.8.1 群 , 体 , 環	220
8.8.2 整 数	221
8.8.3 多 項 式	222
8.8.4 ユークリッドの互除法	223

8.8.5 中国人の剰余定理	225
8.8.6 オイラーの関数とフェルマの小定理	228
8.8.7 有 限 群	229
8.8.8 有 限 体	230
8.8.9 平 方 剰 余	232
8.8.10 ソロベイ・ストラッセンの素数判定法	238
章 末 問 題	240
引用・参考文献	241
索 引	246

1

通信理論の概要

1.1 通信の目的とモデル

〔1.1.1〕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、アメリカからテレビ中継したりすることが挙げられる。このような距離を越えた通信においては、即時（リアルタイム）性が要求されることが多い。一方、CD（Compact Disc）に録音された音楽を鑑賞したり、DVD（Digital Versatile 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^{†1}。

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きた通信のやり方は対面し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からである。したがって、距離を克服して通信を行うには、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。

〔1.1.2〕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宛先（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

^{†1} 時間を越えた通信（記録）では、情報の誤りが心配されても問い合わせできないことが多い。したがって、特に正確性に対する要求の強いことが考えられる。

2 1. 通信理論の概要

路(自由空間や光ファイバケーブルや記録媒体など)を通して、受信側へ伝達する。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 1.1 のように書くことができる。通信は双方向が基本であるが、図 1.1 はその片方を記述していることになる。また、多数が会議を行うような通信も考えられるが、その場合も図 1.1 が基本の構成要素である。

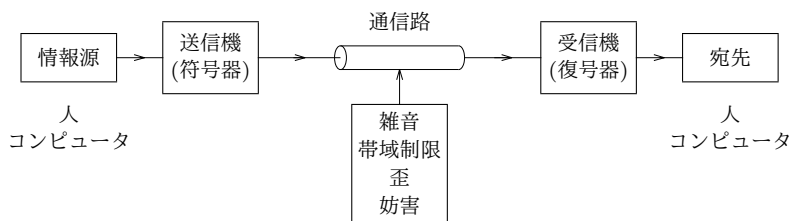


図 1.1 電気通信のモデル

さて、図 1.1 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 など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
が存在する。したがって、これらの障害や妨害を克服して、情報をいかに、

(1) 「正確」、かつ (2) 速く (大量に)、そして (3) 安全に
伝えるか、が通信工学の課題となる^{†1}。

^{†1} 情報は「正確」であることが大前提である。不正確 (デタラメ) な情報をいくら (速く、安全に) 送っても意味がない。

1.2 通信理論の概要と本書の構成

前節最後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しょうか？その概要は次のようにまとめられる。(この結果のすべてが本質的にシャノン (C.E. Shannon) の貢献^{1),2)} によっている。また巻末に示すように多くの優れたテキストが存在する^{3)~9),11)~19)}。

【1.2.1】 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、人の話や文章を考えてみよう。人の話や文章は、文字 (シンボル) の集合 $A := \{a_1, a_2, \dots, a_M\}$ ^{†1} から発せられる文字 (シンボル) の系列 $x_1 x_2 \dots$ ($x_i \in A$) と捉えることができる。このとき、情報の測り方に関する検討を行うと、2章に述べるように、各文字の情報は $-\log_2 p(a_i)$ [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、 $p(a_i)$ は文字 (シンボル) a_i が発生する確率である。

【1.2.2】 次に、与えられた情報の表現に無駄がないかどうか問題になる。例えば人の言葉 (自然言語) は多分に「冗長」である^{†2}。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、情報はどこまで簡潔に表現できるのであろうか？

表現の簡潔さを、情報表現に必要な「文字列の (平均的) 長さ」で測ることにすると、その下限は平均情報量 (あるいはエントロピー)

$$H(A) := \sum_{i=1}^M -p(a_i) \log p(a_i) \quad (1.1)$$

^{†1} A は、英語ならば $A := \{a, b, \dots, z, \sqcup\}$ 、日本語ならば $A := \{\text{あ, い, う, \dots, ん}\}$ で与えられるアルファベットである。

^{†2} この冗長さのために、多少「話」を聞き漏らしても、意味を取り違えることを少なくできている。人間同士の会話では、この冗長さは有効に機能していると考えられる。

で与えられることが示される^{†1}。逆に $H(A)$ に限りなく近い長さの簡潔な表現が可能なることも導かれる。表現を簡潔にする操作は情報源符号化または情報圧縮、データ圧縮などと呼ばれ、情報を記録したり、伝達したりするとき、事前になすべき重要な操作となる。情報圧縮の限界が式 (1.1) によって与えられることは 3 章で、またその限界を達成すべく考案された圧縮アルゴリズムについては 4 章に述べる。

〔1.2.3〕 その次には、(簡潔に表現された) 情報を、(1) 遠く離れた場所へ送信してそれを受信したり、(2) 記録してそれを再生したり、することが行われる。このとき、受信したり再生したりした情報は、一般にもとの情報とは異なる。この原因の第一に挙げられるのが、雑音と呼ばれる物理的障害である。

〔5.1.1〕 で見るように、実際に広く用いられている通信方式として、情報を 2 値 (正, 負のパルスや $\{0, 1\}$) の系列によって表現し、それを伝送したり、記録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 1.2 に示すような通信路モデル (遷移図) によって表すことができる^{†2}。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。

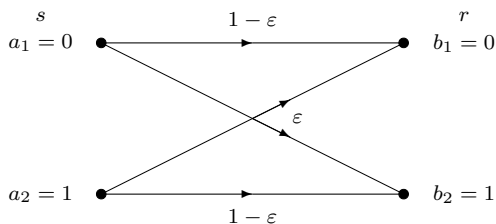


図 1.2 2 元対称通信路 (BSC)

^{†1} 記号「:=」は定義を表す。 $A := B$ は「 A は B で定義される」ことを表す。

^{†2} 図 1.2 において、送信シンボル s ならびに受信シンボル r は、共に 2 値のシンボル $a_1 = 0, a_2 = 1$ ならびに $b_1 = 0, b_2 = 1$ をとるとしている。

〔1.2.4〕 さて，図 1.2 に示したような通信路を通して，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) が受信されたとしよう．(これ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．通信が行われた後を考えると，受信側ではシンボル b_j が受信されている．したがって，送信シンボル a_i の情報量は， $-\log_2 p_s(a_i)$ [ビット] から， $-\log_2 p_{s|r}(a_i|b_j)$ [ビット] に変化していることになる．($p_{s|r}(a_i|b_j)$ は条件付き確率．〔1.3.6〕 参照)．送信シンボル a_i に関するこの情報量の変化分

$$I(a_i; b_j) := -\log_2 p_s(a_i) - [-\log_2 p_{s|r}(a_i|b_j)] \quad (1.2)$$

が， a_i が送信されて 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 (伝達情報量と呼ぶ) と解釈することができる．

〔1.2.5〕 情報源の平均情報量 (エントロピー) を考えたのと同様に，(1 シンボル当たりの) 伝達情報量 $I(a_i; b_j)$ を，(図 1.2 の) 通信システム全体にわたって平均した量

$$I(A; B) := E[I(a_i; b_j)] = \sum_i \sum_j p_{s,r}(a_i, b_j) I(a_i; b_j) \quad (1.3)$$

を考える (平均伝達情報量と呼ぶ)．そして，この平均伝達情報量 $I(A, B)$ を，送信シンボルの出現確率 $\{p(a_i)\}_i$ に関して最大化した値を

$$C := \max_{\{p(a_i)\}_i} I(A; B) \quad (1.4)$$

とおく． C は，通信路 $\{p_{r|s}(b_j|a_i)\}_{i,j}$ だけで決まる，通信路固有の量で，通信路容量と呼ばれる．図 1.2 の BSC の通信路容量は

$$C = 1 - \mathcal{H}_2(\varepsilon), \quad \mathcal{H}_2(x) := -x \log_2 x - (1-x) \log_2(1-x) \quad (1.5)$$

で与えられることが示される．通信路容量については，5 章，7 章で述べる．(5 章では，いわゆる離散無記憶通信路について，また 7 章では，物理的実体である連続通信路について述べている)．

[1.2.6] 与えられた (図 1.2 の) 2 元通信路を通して, 情報を (できるだけ) 誤りなく伝達するために, k シンボルで表される情報 (c_1, c_2, \dots, c_k) に $n - k$ 個の冗長シンボル (c_{k+1}, \dots, c_n) を付け加え, 長さ n の 2 元符号語

$$\mathbf{c} = (c_1, c_2, \dots, c_k, c_{k+1}, \dots, c_n), \quad c_i \in \{0, 1\} \quad (1.6)$$

に変換して通信路に送出するものとする. (この操作を通信路符号化と呼ぶ).

このとき, 通信路容量 C は, その通信路を使って誤りなく伝達できる情報伝達速度の最大値を与える. すなわち, 概ね次の関係が成り立つ:

定理: 誤りのない情報伝達を実現する式 (1.6) の形式の符号が存在するための必要十分条件は, 「情報伝達速度 $R := k/n$ が $R < C$ を満たす」ことである.

この定理は通信路符号化定理と呼ばれ, 通信理論の最も重要な結果の一つである. これに関する, より一般的な議論は, 6 章に述べられる.

[1.2.7] 最後に, 人為的な妨害などを排して情報を安全に通信する技術が残されている. 残念ながら, 世の中には悪事を企む不逞の輩ふてい やから もおり, 情報の盗聴や改竄かいざんなどに備えなければならない. また, 現代のネットワーク社会では, 悪意のない単なる「ミス」によっても情報が変化し, 結果において, 悪意による情報操作と変わらない影響を及ぼす可能性もある. このような, 情報に対する人為的妨害から情報を保護する技術が「セキュリティ技術」であり, その中心に「暗号技術」がある. これに関する入門的解説を述べたのが 8 章である.

1.3 付録: 確率の初歩

ここでは, 本書の内容を理解する上で基本的である, 確率の初歩と (ガウス雑音の根拠を与える) 中心極限定理などについて簡単にまとめている.

1.3.1 テイラー展開とロピタルの定理

補題〔1.3.1〕テイラー展開^{†1}： $f(x)$ を、一つの区間 $I \subseteq \mathbb{R}$ (実数全体の集合) で m 回連続微分可能な関数とする。すると、 $a < b$ ($a, b \in I$) を固定したとき、

$$f(b) = \sum_{k=0}^{m-1} \frac{f^{(k)}(a)}{k!} (b-a)^k + \frac{f^{(m)}(c)}{m!} (b-a)^m \quad (1.7)$$

を満たす実数 $c \in (a, b)$ が存在する。ただし、 $f^{(k)}(x)$ は $f(x)$ の k 階微分を表す。
($a > b$ の場合もまったく同様に式 (1.7) が成立する)。

(証明) 与えられた $f(x)$ ならびに a, b に対して、 K_m を

$$f(b) = \sum_{k=0}^{m-1} \frac{f^{(k)}(a)}{k!} (b-a)^k + K_m (b-a)^m$$

が成り立つように定める (常に可能)。そして、 $a \leq t \leq b$ として、

$$F(t) := f(b) - \sum_{k=0}^{m-1} \frac{f^{(k)}(t)}{k!} (b-t)^k - K_m (b-t)^m$$

とおく。すると、 $F(b) = 0$ 、 $F(a) = f(b) - f(b) = 0$ が成り立つ。したがって、ロールの定理⁴⁵⁾ ^{†2} により、 $c \in (a, b)$ が存在して、 $F'(c) = 0$ が成立する。ここで、実際に $F'(t)$ を計算すれば、

$$F'(c) = -\frac{f^{(m)}(c)}{(m-1)!} (b-c)^{m-1} + mK_m (b-c)^{m-1}$$

が得られ、 $K_m = \frac{f^{(m)}(c)}{m!}$ となって、式 (1.7) が成立する。

補題〔1.3.2〕ロピタルの定理： m 回連続微分可能な関数 $f(x)$ 、 $g(x)$ があり、 $f(a) = \dots = f^{(m-1)}(a) = 0$ 、 $g(a) = \dots = g^{(m-1)}(a) = 0$ 、 $g^{(m)}(a) \neq 0$ であるとする。すると、下記が成立する^{†3}：

$$\lim_{b \rightarrow a} \frac{f(b)}{g(b)} = \frac{f^{(m)}(a)}{g^{(m)}(a)} \quad (1.8)$$

(証明) 式 (1.7) より直ちに得られる。

^{†1} テイラーの定理とも呼ばれる。また、 $a = 0$ のときには、マクローリン展開と呼ばれる。

^{†2} 片かつこ”・)” で示した番号は、巻末の引用・参考文献の番号を表す。

^{†3} ロピタルの定理は、 $f(a) = g(a) = 0$ である関数の比 $\lim_{b \rightarrow a} f(b)/g(b)$ の簡便な計算法を与える。 $f(a) = g(a) = \pm\infty$ の場合にも同様の結果が成立する。

索引

- 【2】**
- 2 元消失通信路 (BEC) [Binary Erasure Channel] 96
 - 2 元対称通信路 (BSC) [Binary Symmetric Channel] 4, 94, 95
 - 2 元入力 AWGN 通信路 [binary input AWGN channel] 191
 - 2 元無記憶対称通信路 [binary memoryless symmetric channel] 96
-

【A】

- AES [Advanced data Encryption Standard] 201
- AWGN 通信路 [Additive White Gaussian Noise channel] 185

【B】

- Belief Propagation 復号法 [Belief Propagation decoding] 156
- Berry-Esseén の定理 [Berry-Esseén theorem] 15

【D】

- DES [Data Encryption Standard] 201
- DSA [Digital Signature Algorithm] 209, 219

- 【K】**
- Kullback-Leibler 情報量 [Kullback-Leibler information] 27

【M】

- MAP 復号法 [Maximum A Posteriori probability decoding] 121
- ML 復号法 [Maximum Likelihood decoding] 123

【R】

- RSA 暗号 [RSA cryptosystem] 209

【S】

- SSH [Secure SHell] 209
- Sum-Product アルゴリズム [Sum-Product algorithm] 152, 156, 161

【Z】

- Z 通信路 [Z-channel] 96
 - ZL 符号 [Ziv-Lempel code] 74
-

【あ】

- アナログ情報 [analog information] 176
- アナログ信号 [analog signal] 176
- 余り [remainder] 221

- 誤り訂正符号 [error correcting code] 142
- アルファベット [alphabet] 17
- 暗号 [cryptography, cryptogram, code, cipher] 198
- 暗号化 [encryption, coding] 199
- 暗号化鍵 [encryption key] 203
- 暗号文 [cipher text] 199

【い】

- イエンゼンの不等式 [Jensen's inequality] 90
- 位数 [order] 229
- 一意に復号可能 [uniquely decodable] 31, 33
- 一方方向ハッシュ関数 [one way hash function] 206
- イライアス符号 [Elias code] 57
- 因数定理 [factor theorem] 223

- インパルス応答 [impulse response] 195

【え】

- 枝 [edge] 34
- エルガマル暗号 [ElGamal cryptography] 219
- エルガマル署名 [ElGamal signature] 219
- エントロピー [entropy] 3, 26, 182

【お】

オイラーの関数 [Euler's function] 228
 オイラーの基準 [Euler's criterion] 232
 凹関数 [concave function] 90
 重み [weight] 144

【か】

解読 [decipher, decode, decrypt] 199
 ガウス雑音 [Gaussian noise] 95
 ガウス信号 [Gaussian signal] 182
 ガウスの補題 [lemma of Gauss] 233
 ガウス分布 [Gaussian distribution] 14
 ガウス変数 [Gaussian random variable] 186
 可換群 [commutative group] 220
 可換律 [commutativity] 221
 鍵 [key] 199
 鍵共有プロトコル [key sharing protocol] 220
 鍵の配送 [key delivery (key distribution)] 201
 拡大情報源 [extended source] 41
 拡大体 [extention field] 231
 確率 [probability] 8
 確率過程 [stochastic process] 194
 確率空間 [probability space] 8
 確率の公理 [axioms of probability system] 8
 (確率) 分布関数 [probability distribution function] 9
 確率ベクトル [probability vector] 102

確率変数 [random variable] 9
 確率密度関数 [probability density function] 10
 確率モデル [probabilistic model] 17
 加群 [additive group] 144, 221
 加法群 [additive group] 144, 221
 加法的通信路 [additive channel] 145
 加法的白色ガウス雑音通信路 [additive white Gaussian noise channel] 185
 可約 [reducible] 223
 環 [ring] 221
 換字暗号 [substitution cipher] 199
 完全符号 [perfect code] 146
 環同型 [ring isomorphism] 227

【き】

木 [tree] 35
 期待値 [expectation] 11
 既約 [irreducible] 223
 逆元 [inverse] 221
 既約多項式 [irreducible polynomial] 143
 ギャラガー関数 [Gallager function] 130
 ギャラガーの上界 [Gallager's upper bound] 126
 行重み [row weight] 150
 共通鍵暗号システム [common key cryptosystem] 199
 共分散行列 [covariance matrix] 186
 距離 [distance] 144
 近傍グラフ [neighborhood graph] 150

【く】

空間計算量 [space complexity] 45
 空事象 [empty event] 8
 グラフ [graph] 34
 クラフト・マクミランの定理 [Kraft-McMillan's theorem] 37
 クラフトの不等式 [Kraft's inequality] 37
 群 [group] 220

【け】

計算量 [computational complexity] 45
 結合確率分布関数 [joint probability distribution function] 9
 結合確率変数 [joint random variable] 9
 結合確率密度関数 [joint probability density function] 10
 結合事象 [joint event] 8
 結合弱定常 [jointly weakly stationary] 194
 結合律 [associativity] 220
 限界距離復号法 [bounded distance decoding] 145
 原始元 [primitive element] 229

【こ】

公開鍵暗号系 [public key cryptosystem] 202
 広義定常 [wide-sense stationary] 194
 合成数 [composite number] 222
 合同 [congruent, congruence] 226
 公倍数 [common multiple] 222

公約数 [common divisor] 222
 公約多項式 [common divisor] 223
 コーシーの定理 [Cauchy's theorem] 230
 語頭 [prefix] 34, 75
 語頭符号 [prefix code] 34
 根 [root] 223
 コンパクト符号 [compact code] 50
 コンマ符号 [comma code] 31

【さ】
 最小公倍数 [least common multiple] 209, 222
 最小ハミング重み [minimum Hamming weight] 144
 最小ハミング距離 [minimum Hamming distance] 144
 最大公約数 [greatest common divisor] 209, 222
 最大公約多項式 [greatest common divisor] 223
 最大事後確率復号法 [maximum a posteriori probability decoding] 121
 最適復号器 [optimum decoder] 120
 最適復号領域 [optimum decoding region] 120
 最尤復号法 [maximum likelihood decoding] 123
 雑音 [noise] 4, 95
 算術符号 [arithmetic code] 57

【し】
 シーザー暗号 [Caesar cipher] 199
 時間計算量 [time complexity] 45
 自己相関 [auto-correlation] 194
 事象 [event] 8
 次数 [degree] 150, 222

実数体 [field of real numbers] 143
 ジブ・レンベル符号 [Ziv-Lempel code] 74
 ジブの不等式 [Ziv's inequality] 83
 写像 [mapping] 29
 シヤノン・ファノ符号 [Shannon-Fano code] 39, 46
 シヤノンの補題 [Shannon's lemma] 26
 周辺確率 [marginal probability] 9
 受信機 [receiver] 2
 巡回群 [cyclic group] 229
 準指数関数 [subexponential] 207
 瞬時符号 [instantaneous code] 31, 34
 商 [quotient] 221
 条件付き確率 [conditional probability] 8
 冗長 [redundant] 29
 冗長シンボル [redundant symbol] 146
 情報圧縮 [information compression] 4
 乗法群 [multiplicative group] 221
 情報源 [information/message source] 17
 情報源符号化 [source coding] 4, 29
 情報源符号化定理 [source coding theorem] 40, 42
 情報シンボル [information symbol] 146
 情報伝達速度 [information transfer rate] 6, 124
 剰余系 [residue class system] 226
 剰余環類 [residue class ring] 226

剰余類群 [residue class group] 226, 229
 信号 [signal] 176
 信号対雑音比 [signal to noise ratio] 189
 シンドローム [syndrome] 147
 真部分集合 [proper subset] 35
 シンボル [symbol] 17
 信頼性関数 [reliability function] 130

【す】

スキャナー [scanner] 86
 ストリーム暗号 [stream cipher] 199

【せ】

正規部分群 [normal subgroup] 229
 正規分布 [normal distribution] 14, 15
 整除の関係 [division algorithm] 221, 223
 生成 [generate] 229
 生成行列 [generator matrix] 147
 生成元 [generator] 219, 229
 正則 LDPC 符号 [regular LDPC code] 150
 正則パリティ検査行列 [regular parity check matrix] 150
 静的符号化 [static coding] 45
 セグメント [segment] 74, 75
 節点 [vertex, node] 34
 零元 [zero] 221
 遷移確率 [transition probability] 97, 125
 遷移行列 [transition matrix] 98
 漸近的最良性 [asymptotically optimum] 66
 線形時不変システム [linear time-invariant system] 195

線形量子化 [linear quantization] 179
 全事象 [whole event] 8
【そ】
 素因数分解 [prime factorization] 207
 相互情報量 [mutual information] 100, 187
 相互相関 [cross-correlation] 194
 送信機 [transmitter] 1
 増分分解 [incremental parsing] 75
 疎行列 [sparse matrix] 150
 素数 [prime number] 143, 222
 素体 [prime field] 230
 ソロベイ・ストラッセンの素数判定法 [Solovay-Strassen's primality test] 238
【た】
 体 [field] 143, 221
 帯域制限信号 [bandlimited signal] 178
 対称 [symmetric] 109
 対称通信路 [symmetric channel] 109
 ダイバージェンス [divergence] 27
 互いに素 [mutually disjoint] 8
 多項式 [polynomial] 222
 多次元エントロピー [multi-dimensional entropy] 183
 多次元条件付きエントロピー [multi dimensional conditional entropy] 183
 畳み込み [convolution] 13
 タナーグラフ [Tanner graph] 149
 単位元 [identity] 220
 単一誤り訂正符号 [single er-

ror correcting code] 146
 単純閉路 [simple loop] 35
 単純マルコフ情報源 [simple Markov source] 20
 端点 (葉) [end node (leaf)] 35
 単連結 [simply connected] 35
【ち】
 チェックノード [check node] 149
 チェビシエフの不等式 [Chebyshev's inequality] 12
 置換 [permutation] 109
 中国人の剰余定理 [Chinese remainder theorem] 227
 中心極限定理 [central limit theorem] 15, 95
 超関数 [distribution] 9
 頂点 [vertex, node] 34
【つ】
 通信 [communication] 1
 通信路 [communication channel] 2
 通信路「逆」符号化定理 [converse coding theorem] 118
 通信路行列 [channel matrix] 98
 通信路符号化 [channel coding] 6
 通信路符号化定理 [channel coding theorem] 6, 118, 125, 193
 通信路容量 [channel capacity] 5, 106, 188
【て】
 デジタル情報 [digital information] 176
 デジタル署名 [digital signature] 205
 デジタル信号 [digital signal] 176

低密度パリティ検査符号 [LDPC (Low-Density Parity-Check) code] 150
 テイラー展開 [Taylor expansion] 7
 テイラーの定理 [Taylor's theorem] 7
 データ圧縮 [data compression] 4
 データ圧縮符号 [data compression code] 45
 適応符号化 [adaptive coding] 45
 電気通信 [electrical communication] 1
 伝達情報量 [transinformation] 5, 100, 187
 転置暗号 [transposition (permutation) cipher] 200
 電力スペクトル密度 [power spectral density] 195, 196
【と】
 (統計的に) 独立 [statistically independent] 8, 10
 同値関係 [equivalence relation] 226
 等長符号 [fixed length code] 31
 動的符号化 [dynamic coding] 45
 特異符号 [singular code] 31
 特性関数 [characteristic function] 13
 独立情報源 [independent source] 18
 独立同一分布 [i.i.d. independent and identically distributed] 15, 189
 独立分解 [independent decomposition] 79
 上に凸な関数 [concave function] 90
 凸関数 [convex function] 90

- 下に凸な関数 [convex function] 90
 凸集合 [convex set] 90
- 【な行】**
- 内挿 [interpolation] 178
 内挿関数 [interpolation function] 178
 認証子 [authenticator] 206
 根 [root] 35
 ノード [node] 34
- 【は】**
- バーナム暗号 [Vernam cipher] 200
 白色ガウス雑音 [white Gaussian noise] 184
 白色雑音 [white noise] 196
 パス [path] 35
 ハッシュ関数 [hash function] 206
 ハフマン符号 [Huffman code] 46
 ハミング重み [Hamming weight] 144
 ハミング距離 [Hamming distance] 144
 ハミング符号 [Hamming code] 146
 パリティ検査行列 [parity check matrix] 146
- 【ひ】**
- 非瞬時符号 [non-instantaneous code] 32
 歪 [distortion] 30
 非線形量子化 [nonlinear quantization] 179
 ビット誤り率 [bit error rate] 4, 95
 標準偏差 [standard deviation] 12
 標本化定理 [sampling theorem] 178
- 標本化 [sampling] 177, 178
 標本化間隔 [sampling interval] 178
 標本化関数 [sampling function] 178
 標本化周波数 [sampling frequency] 178
 標本値 [sampled value] 178
 平文 (ひらぶん) [plain text] 198
 平文化 [decipher, decode, decrypt] 199
 平文復元によるデジタル署名 [digital signature by plain text recovery] 205
- 【ふ】**
- ファクシミリ [facsimile] 86
 フィルタ [filter] 195
 フーリエ変換 [Fourier transform] 13
 フェルマテスト [Fermat test] 208
 フェルマの小定理 [Fermat's theorem] 228, 229
 不規則過程 [stochastic process] 194
 不規則信号 [random process] 194
 不規則変数 [random variable] 9
 復号 [decipher, decode, decrypt] 199
 復号閾値 [decoding threshold] 169
 復号化 [decoding] 29
 復号化鍵 [decryption key] 203
 復号器 [decoder] 2, 29
 復号木 [decoding tree] 150
 復号領域 [decoding region] 119
 複雑度 [complexity] 79
 複素数体 [field of complex numbers] 143
- 負元 [negative element] 221
 符号 [code] 29
 符号化 [coding] 29
 符号化率 [coding rate] 124
 符号器 [encoder] 1, 29
 符号器アルファベット [encoder alphabet] 29
 符号語 [codeword] 29
 符号長 [code length] 146
 符号の木 [code tree] 35
 不等長符号 [variable length code] 31
 不動点 [fixed point] 169
 部分群 [subgroup] 229
 ブロック暗号 [block cipher] 199
 ブロック符号 [block code] 124
 分割 [partition] 119
 分散 [variance] 12
 分配律 [distributive law] 221
 分布関数 [distribution function] 9
- 【へ】**
- 平均 [mean, average] 11
 平均に関する基本定理 [fundamental theorem of expectation] 11
 平均値の定理 [mean value theorem] 91
 平均伝達情報量 [mean transinformation] 5, 100
 平均電力 [average power] 194
 平均符号長 [average code length] 32
 バイズの定理 [Bayes' theorem] 9
 平方剰余 [quadratic residue] 213, 232
 平方非剰余 [quadratic non-residue] 213, 232
 閉路 [loop, cycle, circuit] 35
 辺 [arc, edge] 34

平均情報量 [entropy] 3, 26
 変数ノード [variable node] 149

【ほ】

補間 [interpolation] 178

【ま】

マクローリン展開 [Maclaurin expansion] 7
 マルコフ情報源 [Markov source] 19

【み】

道 [path] 35
 密度発展法 [density evolution] 172

【む】

無記憶 [memoryless] 96, 97, 125
 無記憶情報源 [memoryless source] 18
 無条件に安全 [unconditionally secure] 201
 無相関 [no correlation] 194
 無歪圧縮 [distortionless compression] 30

【め】

メッセージ [message] 157
 メッセージパッシングアルゴリズム [message passing algorithm] 156

【も】

モーメント [moment] 12
 モニック多項式 [monic polynomial] 223

【や】

ヤコビの記号 [Jacobi's sym-

bol] 217, 236

【ゆ】

ユークリッドアルゴリズム [Euclidean algorithm] 223
 ユークリッドの互除法 [Euclidean algorithm] 223
 有限群 [finite group] 229
 有限体 [finite field] 143, 230
 有理数体 [field of rational numbers] 143
 ユニバーサル符号 [universal code] 67

【よ】

余事象 [complement event] 8

【ら】

ラグランジュの定理 [Lagrange's theorem] 229
 ラメの定理 [Lamé's theorem] 224
 ラン [run] 86
 ランダウの記号 [Landau symbol] 152
 ランダム符号化 [random coding] 127
 ランレンクス符号 [run length code] 86

【り】

離散情報 [discrete information] 176
 離散信号 [discrete signal] 176
 離散対数 [discrete logarithm] 207
 離散無記憶通信路 [discrete memoryless channel] 5, 97
 量子化 [quantization] 177, 179
 量子化誤差 [quantization error] 180

量子化雑音 [quantization noise] 180
 量子化ステップ幅 [quantization step size] 180
 量子化歪み [quantization distortion] 180
 量子化ビット数 [number of quantization bits] 180

【る】

ルート [root] 35
 ルジャンドルの記号 [Legendre's symbol] 216, 232

【れ】

レート歪理論 [rate distortion theory] 30
 列重み [column weight] 150
 連結 [connected] 35
 連続情報 [continuous information] 176
 連続信号 [continuous signal] 176
 連続通信路 [continuous channel] 5, 176

【ろ】

ロールの定理 [Rolle's theorem] 7
 ロピタルの定理 [l'Hôpital's rule] 7

【わ】

ワイル符号 [Wyle code] 86
 和事象 [union event] 8
 割り切る [divisible] 222, 223
 ワンショット符号化 [one-shot coding] 67
 ワンタイムパッド [one time pad] 201

— 著者略歴 —

坂庭 好一（さかにわ こういち）
1972年 東京工業大学工学部電子工学科卒業
1974年 東京工業大学大学院修士課程修了
（電子工学専攻）
1977年 東京工業大学大学院博士課程修了
（電子工学専攻）
工学博士
1977年 東京工業大学助手
1983年 東京工業大学助教授
1991年 東京工業大学教授
2014年 東京工業大学名誉教授

笠井 健太（かさい けんた）
2001年 東京工業大学工学部情報工学科卒業
2003年 東京工業大学大学院修士課程修了
（集積システム専攻）
2006年 東京工業大学大学院博士課程修了
（集積システム専攻）
博士（学術）
2006年 東京工業大学助手
2007年 東京工業大学助教
2012年 東京工業大学准教授
現在に至る

通信理論入門

Introduction to Communication Theory

© Kohichi Sakaniwa, Kenta Kasai 2014

2014年9月22日 初版第1刷発行

検印省略

著者 坂庭 好一
笠井 健太
発行者 株式会社 コロナ社
代表者 牛来真也
印刷所 三美印刷株式会社

112-0011 東京都文京区千石 4-46-10

発行所 株式会社 コロナ社

CORONA PUBLISHING CO., LTD.

Tokyo Japan

振替 00140-8-14844・電話(03)3941-3131(代)

ホームページ <http://www.coronasha.co.jp>

ISBN 978-4-339-02464-7 (金) (製本：愛千製本所)

Printed in Japan



本書のコピー、スキャン、デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられております。購入者以外の第三者による本書の電子データ化及び電子書籍化は、いかなる場合も認めておりません。

落丁・乱丁本はお取替えいたします