

# マルチメディア情報符号化の 基礎と応用

— 情報伝達の効率化と信頼性の確保 —

杉浦 彰彦

岡村 好庸 共著

小暮 悟

コロナ社

# ま え が き

近年の情報通信技術はすさまじいスピードで進化している。スマートフォンに代表される通信機器が普及し、身のまわりでマルチメディア情報通信を利用しない日はない。本書は、工学・情報系の大学生・高専生に対して、マルチメディア情報通信で利用されている技術要素と基礎原理をわかりやすく解説するものである。

マルチメディア情報通信の基礎となる情報数学や、情報理論、符号理論といった理論系の科目を長年にわたり担当し、基礎や理論に対する理解こそが新しい技術やブレイクスルーを産んでいると実感している。一方で、最新技術と基礎原理をつなげる教科書が多くない点についても痛切に感じている。そこで、本書は基礎と応用を結び付ける教科書として執筆することにした。

本書の半分は、情報理論や符号理論の基礎となる数学や理論について岡村先生と小暮先生に担当していただき、杉浦が応用との関係性を前半で述べることで、基礎と応用の結び付きをもたせる構成をとっている。これまで大学生や高専生に講義をしてきた経験から、身のまわりでどう利用されているか知ったうえで基礎を学ぶことの有用性は高いものと信じ、本書の執筆を進めた。

本書では、初学者の理解を促すために、基礎部分では例題など具体的な記述を多くし、応用部分では実用例や例え話などを多く盛りこみ、基礎と応用のつながりが見えやすくなるように工夫した。また、読者の理解を促すことを優先し、簡素化した例などを挙げて解説し、例外などの説明は省略している。同じ理由で極端な比喩表現なども取り入れているが、見苦しい点があったなら御容赦願いたい。

また本書では、実用化されている音声や画像の符号化方式について、規格化の経緯や基礎原理の説明を中心に述べている。マルチメディア情報通信の規格

化は、周辺技術や利用形態により日々変化してしまいが、基礎的な考え方には普遍的な部分も多く、新携帯電話方式に代表される新たな通信に適したアプリケーションを考えるうえでもおおいに役に立つと考えている。

また、マルチメディア情報処理は、通信分野に限らず、さまざまな方面で活用されている。例えば、医学の分野では遠隔医療診断支援や在宅ケアシステムなど、教育分野では遠隔教育やeラーニングなど、職場ではテレワークやテレビ会議など、分野・応用例は数えきれない。本書は、マルチメディア情報通信技術を活用する皆様にも、符号化方式の特性や限界などを熟知してもらい、応用・開発をスムーズに進めていただくのにも役立てていただければと願っている。

2020年9月

杉浦 彰彦

# 目 次

## 1. 情報のための数学基礎

1.1 情報理論と集合・確率	1
1.1.1 集合表現	1
1.1.2 事象と確率概念	4
1.1.3 確率変数の平均と分散	7
1.1.4 結合確率	8
1.1.5 条件付確率	11
1.2 行列	14
1.2.1 和と積	16
1.2.2 逆行列	17
1.2.3 対角化および固有値, 固有方程式	18
1.3 ガロア体	22
1.3.1 群	22
1.3.2 環と体	24
1.3.3 ガロア体と素体	25
1.3.4 ガロア体の拡大体	28

## 2. 情報に関する諸量

2.1 情報の伝達	34
2.2 情報量	35

2.3 平均情報量 (エントロピー) .....	38
2.3.1 エントロピー .....	38
2.3.2 シャノンの補助定理 .....	41
2.3.3 エントロピー関数 .....	42
2.3.4 冗 長 度 .....	43
2.3.5 結合エントロピー .....	43
2.3.6 条件付エントロピー .....	44
2.3.7 エントロピーの性質 .....	45
2.4 相 互 情 報 量 .....	47

### 3. 情報源と符号化

3.1 情報源とエントロピー .....	55
3.2 記憶のない情報源 (無記憶情報源) .....	57
3.3 記憶のある情報源 (マルコフ情報源) .....	62
3.3.1 シャノンダイアグラムと遷移確率行列 .....	63
3.3.2 状態の存在確率に変化しない場合 (定常状態) .....	64
3.3.3 初期時点後の状態確率分布 .....	65
3.3.4 エントロピー計算 .....	66
3.4 単純マルコフ情報源 .....	69
3.4.1 情報源のモデル .....	69
3.4.2 定 常 状 態 .....	74
3.4.3 極 限 状 態 .....	75
3.4.4 エントロピー .....	78
3.4.5 出力パターン .....	80
3.5 情報源符号化 .....	81
3.5.1 情報伝送速度と通信路容量 .....	82

3.5.2	クラフトの不等式	82
3.5.3	第一符号化定理	84
3.5.4	ブロック符号	85
3.5.5	一意復号可能な符号	85
3.5.6	クラフト・マクミランの不等式	86
3.5.7	平均符号長の下限と情報源符号化定理	88
3.6	情報源符号化法	91
3.6.1	シャノンの符号化	92
3.6.2	ハフマンの符号化	93
3.6.3	ハフマン符号構成法	95
3.6.4	ハフマンブロック符号	98
3.6.5	ランレングスハフマン符号	101

## 4. 通信路と情報量

4.1	通信モデルと伝達情報量	106
4.1.1	ビット誤り率	106
4.1.2	通信モデル	108
4.1.3	情報量伝達	110
4.2	通信路容量と通信路符号化定理	119
4.2.1	通信路容量	119
4.2.2	誤り率の改善	120
4.2.3	通信路符号化定理	122
4.3	加法的通信路	128
4.3.1	記憶のない加法的通信路	131
4.3.2	BSCにおける誤りの統計的性質	136
4.3.3	記憶のある加法的通信路	139

4.3.4 誤り訂正符号化	141
4.4 非加法的通信路とモンティ・ホール問題	148

## 5. 符号理論

5.1 誤り訂正符号	153
5.2 線形符号	155
5.3 巡回符号	161
5.4 BCH 符号	164
5.5 リード・ソロモン符号 (RS 符号)	170
5.6 畳み込み符号	176
5.7 接続符号とターボ符号	181
5.8 暗号への応用	183
5.8.1 暗号と鍵	183
5.8.2 ヒル暗号	184
5.8.3 RSA 暗号	186

## 6. マルチメディア符号化の基礎

6.1 符号化の基礎	188
6.2 標本化と量子化	189
6.3 可逆圧縮と非可逆圧縮	192
6.4 波形符号化	193
6.4.1 線形 PCM	194
6.4.2 ベクトル量子化	194
6.5 周波数変換と符号化	195
6.5.1 相関とスペクトル	195

6.5.2	周波数変換と画像符号化	197
6.5.3	量子化による情報圧縮	199

## 7. 音声・オーディオの符号化

7.1	音声の特性	202
7.1.1	音声信号の振幅	203
7.1.2	音声信号のスペクトル成分	203
7.1.3	音声の生成モデル	204
7.2	音声の符号化	205
7.2.1	線形予測分析法	206
7.2.2	偏相関分析法	206
7.2.3	生成源符号化の応用	207
7.3	オーディオ符号化	208
7.3.1	人間の聴覚の特性	208
7.3.2	MPEG1 Audio	209

## 8. 画像・映像

8.1	画像・映像の特性	212
8.1.1	画像・映像情報	212
8.1.2	画像・映像符号化の原理	214
8.1.3	画像・映像符号化の考え方	216
8.1.4	冗長度削減	217
8.1.5	量子化	218
8.1.6	2進符号化	219
8.2	静止画像の圧縮	219
8.3	準動画の圧縮	224



8.4 映像の圧縮	227
8.4.1 MPEGの概要	227
8.4.2 MPEG1	229
8.4.3 MPEG2	233
8.4.4 MPEG4	235
8.4.5 MPEG2システム	237
引用・参考文献	239
索引	240

# 2

## 情報に関する諸量

世の中には、多くのありふれた事象と、たまに遭遇する珍しい事象とが存在する。平日に電車で通勤している社会人は、ほとんどの平日において自身の乗る電車は通常運行しているだろう。しかし、たまに機器トラブルなどでいつも乗車している電車が定時に出発しない状況に遭遇することがある。このように、「ありふれた」や「たまに、まれに」という状況を数学的に捉える枠組みとして情報量という概念がある。情報量は、いわば、得られた情報がどれだけ驚愕に値するかを示す指標である。また、情報量の期待値を計算することで、事象の生起確率がどれだけ偏っているのか知ることができる。

本章では、情報量の定義に加えて、情報量にまつわる各種概念・諸量についても示す。

### 2.1 情報の伝達

情報理論で用いられる諸量について詳解する。ここでは、情報の伝達を例に諸量の意味するところについても説明する。まず情報理論で用いられる諸量の中で、最も基本的な情報量について考えてみる。1章で述べたとおり、情報理論では対象とする事象の生起確率に応じた諸量を定義している。すなわち、当たり前の事象では小さくなり、めったに起こらない事象では大きくなるような関係性をもつ必要がある。例えば、細工のされていないサイコロを例にとると、6面のサイコロを振って“1”が出るという事象と、100面ダイスを振って“1”以外が出る事象では、前者のほうが情報量が高いような関数が望ましい。つまり、

生起確率が大きいほど小さく、生起確率が小さいほど大きくなるような、生起確率に対して単調減少をするような関数であることが望ましい。また、二つ以上の事象があった場合、それらの事象が独立であったなら、事象が多いほど情報も多くなるため、加法的性質をもった関数である必要がある。この二つの条件をもち合わせた関数として代表的なものが対数関数である。情報理論でも対数関数を用いて、基本的な情報の量を定義している。

さらに情報理論では、さまざまな事象を情報の源（情報源）として扱う。特に対象とする事象の発生する確率（生起確率）が情報理論では重要な要素となるため、情報源を事象と生起確率を上下に並べた形で次式のように記載する。これは情報源  $X$  の中に要素が  $n$  個あり、それぞれの要素  $S_i$  の生起確率が  $P_i$  であることを示している。

$$X = \begin{pmatrix} S_1 & S_2 & \cdots & S_n \\ P_1 & P_2 & \cdots & P_n \end{pmatrix}, \quad \sum_{i=1}^n P_i = 1, P_i \geq 0 \quad (2.1)$$

## 2.2 情 報 量

情報理論で用いられる諸量の中でも、最も基礎的なものが情報量である。情報量は式 (2.2) により示され、2.1 節で述べたとおり、生起確率に対して単調減少であること (図 2.1) と、加法的性質の特性とをもち合わせている。ここでは、これら二つの特性を中心に、情報量の特性について詳解する。

$$I = K \log_a \frac{1}{p}, \quad K > 0, a > 1 \quad (2.2)$$

また、ここでは 0 と 1 の 2 種類のシンボル（ビット）で事象を表現するデジタル（1/0）で情報量を定義するので、対数関数の底の部分  $a$  は 2 になっている。また、 $K$  は通常 1 とするため、情報量は次式で計算できる。

$$I(p) = -\log_2 p \quad [\text{ビット}] \quad (2.3)$$

単位は [ビット] である。[ビット] という単位は 2 進数 1 桁を表す場合に

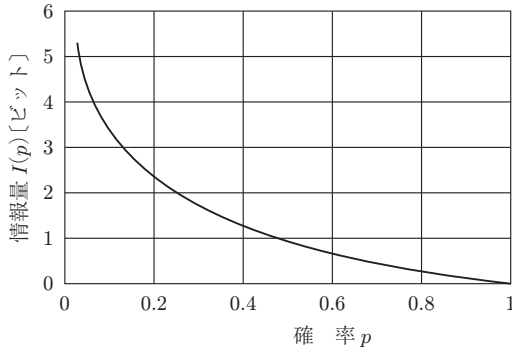


図 2.1 情報量  $I(p)$  は  $p$  の単調減少関数である

も用いられている。この情報量は、 $p = 1/2$  のとき  $I(1/2) = 1$  であり、確率  $(1/2)$  の事象が生じたとき 1 ビットの情報が伝達されたと決めている。例として、サイコロを振ったとき 1 の目が出た場合、伝達された情報量は

$$I(1/6) = -\log_2(1/6) = 2.585 \text{ ビット} \quad (2.4)$$

と計算することができ、また、100 面ダイスを振ってみたとき 1 の目以外が出た場合の伝達情報量は

$$I(0.99) = -\log_2 0.99 = 0.0145 \text{ ビット} \quad (2.5)$$

と求めることができる。このようにして定義された情報量では、起こることが確実な事象 ( $p = 1$ ) が生起しても  $I(1) = 0$  であり、情報の伝達はないが、起こるはずのない事象が起こった場合 ( $p = 0$ ) は、 $I(0) = \infty$  となり、無限大の情報量が伝達されたことになる。すなわち、ビックリしたことが大きいほど多量の情報が伝達されたといえる。

事象  $A$  が生起する確率  $p_A$  と事象  $B$  が生起する確率  $p_B$  が独立な場合、情報量はつぎの性質を満たす。

$$I(p_{APB}) = I(p_A) + I(p_B) \quad (2.6)$$

これは独立事象  $A$  と独立事象  $B$  が起こったとき、伝達された情報量は個々の情報量の和と考えると、独立事象  $A$  と独立事象  $B$  の一体化した事象（生起確率は個々の確率の積）と考えると、伝達された情報量は同じであることを表す。5 円玉と 100 円玉のコイン投げを行い、5 円玉と 100 円玉がともに表となった場合、個々の事象は確率  $(1/2)$  で生じるので、伝達された情報量の和は

$$I(1/2) + I(1/2) = 2 \text{ ビット} \quad (2.7)$$

また、ともに表となる確率は  $(1/4)$  なので、伝達された情報量は

$$I(1/4) = 2 \text{ ビット} \quad (2.8)$$

と 2 通りの方法で計算することができ、同じ結果を与える。見て結果を知る代わりに、つぎのような質問により結果を知ることもできる。「5 円玉は表ですか。」答えは yes でも no でも 5 円玉の表裏を判断することができる。つぎに、「100 円玉は表ですか。」同様に yes でも no でも 100 円玉の表裏を判断することができる。すなわち、質問をする前は見えていないためコインの表裏はあいまいであったが、2 回の質問の答えから完全にコインの表裏の情報を得たといえる。この質問の回数が情報量であると考えて、2 ビットの情報が伝達されたといってもよい。ただし、これは確率  $(1/2)$  で生起する事象に対して質問が二者択一でなされた場合に限られることに注意する。以後、特に必要と思われる場合を除いて、単位をいちいち表示しないが、特に断らない限り情報量の単位は [ビット] である。

整理すると、情報量には図 2.2 に示す性質がある。

非負性：	$I(p) \geq 0$
加法性：	$I(pq) = I(p) + I(q)$
正規性：	$I\left(\frac{1}{2}\right) = 1$
単調減少：	$p_1 < p_2 \rightarrow I(p_1) > I(p_2)$

図 2.2 情報量の性質

**例題 2.1** 情報源から 0 が出力される確率が 0.75 のとき、0 が出力された場合に伝達された情報量はいくらか。

**【解答】** 0.415

◇

**例題 2.2** 情報量を

$$I(p) = -\log_{10} p \quad [\text{ハートレー}]$$

と定義することもある。1 ハートレーは何ビットか。単位として [ハートレー] 以外に [ディット] や [デシット] も用いられている。また、自然対数を用いて

$$I(p) = -\log_e p \quad [\text{ナット}]$$

と定義することもできる。1 ナットは何ビットか。

**【解答】** 1 ハートレー = 3.322 ビット, 1 ナット = 1.443 ビット

◇

## 2.3 平均情報量（エントロピー）

### 2.3.1 エントロピー

一つの事象について、その生起確率から情報量が求められるが、多くの事象が存在する場合には、それら集合（事象）全体での平均的な情報量を平均情報量で表すことができる。平均情報量  $H$  は次式で示されるように、情報量に生起確率を乗じて足し合わせた形で表現され、ちょうど情報量の期待値の形で求めることができる。

$$H = -\sum_{i=1}^n P_i \log_2 P_i \quad (2.9)$$

特性が似ていることから、熱力学（物理）におけるエントロピーにちなんで、

# 索引

**【あ行】**

あいまいエントロピー	117
あいまい度	117
アナログ信号	188
アナログ-デジタル変換	189
誤り検出	142
誤り訂正	142, 153
誤り訂正符号	153
暗号化	183
一意復号可能な符号	83
1次エントロピー	56
1次従属	158
1次独立	158
異方性パラメータ	72
動きベクトル量	225
動き補償予測	225
エントロピー	39
エントロピー関数	42
音源	204
音声生成モデル	204

**【か行】**

ガウス雑音	107
可逆圧縮(符号化)	192
確率変数	7
加法的通信路	129
画面群構造	230
ガロア体	25
環	24
記憶のある情報源	62
記憶のない情報源	57
期待値	7
基底	157
基底関数	196
基本周波数	203

逆行列	18
逆フーリエ変換	196
共通鍵	183
行ベクトル	14
行列	14
行列式	18
空事象	3
クラフトの不等式	83
クラフト・マクミランの不等式	87
群	22
結合エントロピー	43
結合確率	8
検査記号	143
原始 $n$ 乗根	26
公開鍵	183
勾配法	226
固定長符号化	83
固有値	19
固有ベクトル	19

**【さ行】**

最小(ハミング)距離	142
最尤復号法	135
差事象	3
雑音エントロピー	117
散布度	117
サンプリング	189
サンプリング定理	189
ジグザグスキャン	223
次元	158
自己相関	195
自己同型写像	22
事象	3
シャノンダイアグラム	63
シャノンの符号化	92

シャノンの不等式	46
シャノンの補助定理	41
集合	1
巡回符号	161
瞬時符号	83
条件付エントロピー	44
条件付確率	11
状態遷移図	63
冗長度	43
情報圧縮	192
情報誤り	154
情報記号	143
情報源符号化	81
情報伝送速度	82
情報量	35
スペクトル	196
生成源符号化	205
正方行列	15
積事象	3
線形符号	155
線形予測分析法	206
線形量子化	218
線形PCM	194
全事象	3
相関値	195
相関パラメータ	72
相関法	226
相互情報量	47
相互相関	195
組織符号	155

**【た行】**

体	24
第一符号化定理	84
対角行列	19
タイムベース処理	228

多重化処理	228	パルス符号化	194	マルコフ情報源	62
畳み込み符号	153	非可逆圧縮 (符号化)	192	丸め誤差	190
ターボ符号	182	非瞬時符号	83	モールス符号	4
単位行列	18	非線形量子化	218	モンティ・ホール問題	148
単純マルコフ情報源	69	ビタビ復号	179		
調音	204	ビット	4	<b>【や行】</b>	
直交変換符号化	217	ビット誤り	106	余事象	3
直交ミラーフィルタ	209	ビット誤り率	106	予測符号化	217
通信路記号	111	非等長符号	83		
通信路行列	108	標準偏差	8	<b>【ら行】</b>	
通信路線図	112	標本化	189	ランダム誤り	154
通信路符号化	81	標本化周期	189	ランレングス	193
通信路容量	82	標本化定理	189	ランレングスハフマン符号	101
デジタル信号	189	フィルタリング	189	リード・ソロモン符号	
適応差分 PCM	210	フォルマント	203		154, 170
同期処理	228	符号化	189	量子化	190
等長符号	83	符号語	143	量子化係数	199
等ラウドネス曲線	208	符号の木	86	量子化雑音	191
特性方程式	19	部分集合	2	量子化テーブル	200
独立	47	フーリエ変換	196	量子化特性	231
		ブロックノイズ	223	量子化ひずみ	190
<b>【な行】</b>		ブロック符号	153	量子化マトリックス	231
2元対称通信路	133	分散	7	列ベクトル	14
		平均情報量	38	ロスレス方式	223
<b>【は行】</b>		ベクトル量子化	194		
ハイブリッド符号化	217	変形離散コサイン変換	209	<b>【わ行】</b>	
バースト誤り	154	偏相関分析法	207	和事象	3
ハフマンの符号化	93				
ハミング距離	142	<b>【ま行】</b>			
パリティ検査	142	マスキング効果	208		

---

		GOP	230	MP3	210
<b>【A, B, D】</b>		H.264	227	<b>【P, Q, R, S】</b>	
ADPCM	210	LDPC 符号	182	PNG	224
A-D 変換	189			QMF	209
BCH 符号	164	<b>【M】</b>		RS 符号	154
BSC	133	MC	231	RSA 暗号	186
D-A (デジタル-アナログ)		MDCT	209	SN 比	153, 191
変換処理	189	MPEG1	209, 229		
		MPEG1 Audio	209		
<b>【G, H, L】</b>		MPEG2	233		
GIF	224	MPEG4	235		



— 著者略歴 —

杉浦 彰彦 (すぎうら あきひこ)	岡村 好庸 (おかむら よしのぶ)
1988年 東京農工大学工学部応用物理学卒業	1973年 神戸大学理学部物理学卒業
1997年 東京大学大学院工学系研究科博士 (工学) 取得 (電子情報工学専攻)	1981年 ニューヨーク州立大学大学院物理学研究科博士課程修了, Ph.D. (物理学)
2007年 静岡大学教授	2003年 宇部工業高等専門学校教授
現在に至る	2014年 宇部工業高等専門学校退職

小暮 悟 (こぐれ さとる)

1997年 豊橋技術科学大学工学部情報工学課程卒業
2002年 豊橋技術科学大学大学院工学研究科博士課程修了 (電子・情報工学専攻), 博士 (工学)
2017年 静岡大学准教授
現在に至る

## マルチメディア情報符号化の基礎と応用

— 情報伝達の効率化と信頼性の確保 —

Introduction to Multimedia Information Encoding and The Application

— Efficiency of Communication and Securing of Reliability —

© Akihiko Sugiura, Yoshinobu Okamura, Satoru Kogure 2020

2020年10月23日 初版第1刷発行



検印省略

著者 杉浦 彰彦  
岡村 好庸  
小暮 悟  
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  
製本所 有限会社 愛千製本所

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 <https://www.coronasha.co.jp>

ISBN 978-4-339-02913-0 C3055 Printed in Japan

(新宅)



< 出版者著作権管理機構 委託出版物 >

本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は、そのつど事前に、出版者著作権管理機構 (電話 03-5244-5088, FAX 03-5244-5089, e-mail: info@jcopy.or.jp) の許諾を得てください。

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います。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いません。落丁・乱丁はお取替えいたします。