

# 世界をORする視線 (20)

## 第I部 通信・デジタル技術の発展

### (3) コンピュータの発展：コンピュータ科学の 数学的基礎 (続き 7)

住田 潮

(注：本稿は前回からの続きであるので、文献リストは継続し、新たに必要となる分を追加する)

前回、シャノンの第一基本定理 (情報源符号化定理) を証明し、確率変数  $X$  によって記述される情報に対し、一意的に復元可能な語頭符号によって、エントロピー  $H(X)$  bit と  $H(X) + 1$  bit の間まで送信量を圧縮することが可能であることを示した。本稿では、そのような符号化が実際どのようにして実現できるのか、いくつかの手法を具体的に紹介する。

情報源の符号化と符号語長に関する記法を復習しておく。メッセージを表わす記号の集合を  $S$ 、その要素  $x \in S$  に有限な 0-1 の列を割り当てる写像  $C: S \rightarrow B^\infty$  を符号、その値  $C(x)$  を記号  $x$  の符号語、その長さを符号語長と呼び、 $l_C(x) = |C(x)|$  で表わす。 $S$  上の確率変数  $X$  が確率分布  $P(x)$  をもつとき、 $X$  に対応する符号  $C$  の平均符号語長  $L_C(X)$  は

$$L_C(X) = \sum_{x \in S} P(x) l_C(x)$$

で与えられる。 $C$  の逆像  $C^{-1}: B^\infty \rightarrow S$  が存在するとき、 $y = C(x)$  に対して  $x = C^{-1}(y)$  を  $y$  の  $x$  への復元と呼ぶ。

情報源の生成するメッセージとは、 $S$  に属する記号を有限個並べて生成される系列であり、 $\mathbf{x} = [x_1, \dots, x_n] \in S^n$  に対応する符号列を  $C(\mathbf{x}) = C(x_1) \dots C(x_n) \in B^\infty$  と書く。どの符号値も、ほかの符号値の先頭部分と一致しない符号を語頭符号と呼ぶ。語頭符号は、ルート・ノードから出発し、0-1 の分

岐を繰り返すことによって、すべての符号をリーフ・ノードにもつ 2 分木構造として表現することが可能であり、一意的に復元可能な符号となる。 $S$  上で定義される語頭符号の集合を  $HC(S)$  で表わす。

#### 1. シャノン符号

1948 年、情報と通信に関する記念碑的論文「The Mathematical Theory of Communication (通信の数学的理論)」の中でシャノンが提唱した符号化の方法は、 $-\log_2 P(x)$  の値を切り上げて整数化し符号語長を定めるというものであった。すなわち、符号  $C_S$  を

$$l_{C_S}(x) = \lceil -\log_2 P(x) \rceil \quad (1.1)$$

によって定義すると、連載第 19 回で示したように、

$$H(X) \leq L_{C_S}(X) < H(X) + 1 \quad (1.2)$$

が成立することを証明したのである。ここでは、この定理を、以下の具体例によって検証してみる。

表 1 から、平均符号語長とエントロピーを求めると、小数点 3 桁までを有効数字として、

$$\begin{aligned} L_{C_S}(X) &= \frac{1}{3} \times 2 + \frac{1}{6} (3 \times 3) + \frac{1}{12} (4 \times 2) = \frac{17}{6} \\ &= 2.833 \\ H(X) &= \frac{1}{3} \times 1.585 + \frac{1}{6} (2.585 \times 3) + \frac{1}{12} (3.585 \times 2) \\ &= 2.418 \end{aligned}$$

となるので、

$$\begin{aligned} H(X) = 2.418 &\leq L_{C_S}(X) = 2.833 \\ &< H(X) + 1 = 3.418 \end{aligned}$$

が成立していることがわかる。表 1 をもとに、 $C_S$  の具体例として語頭符号を生成してみると、図 1 の 2 分

すみた うしお  
筑波大学名誉教授

〒305-8573 茨城県つくば市天王台 1-1-1

表 1 シヤノン符号

| 記号<br>$x$ | 生起確率 $P(x)$ | $-\log_2 P(x)$ | $l_{C_S}(x)$ |
|-----------|-------------|----------------|--------------|
| $a$       | 1/3         | 1.585          | 2            |
| $b$       | 1/6         | 2.585          | 3            |
| $c$       | 1/6         | 2.585          | 3            |
| $d$       | 1/12        | 3.585          | 4            |
| $e$       | 1/6         | 2.585          | 3            |
| $f$       | 1/12        | 3.585          | 4            |

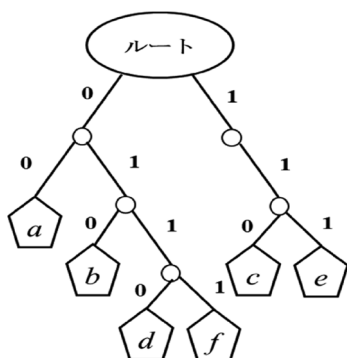


図 1 シヤノン符号  $C_S$  の 2 分木表現

木のようになる。その結果を、表 2 にまとめておく。

## 2. ファノ符号

シャノンとほぼ同時期に、独自の符号化アルゴリズムを提唱したのはファノ (Robert Mario Fano) [69] である。その概要は以下のとおりである [70]。

- (1) 記号  $x$  を  $P(x)$  の降順に並べる
- (2) 記号グループを、それぞれのグループの  $P(x)$  の和が可能な限り等しくなるように、2 分割する
- (3) 大きい方のグループに属する記号の最後の数字を 0 に、もう一方のグループに属する記号の最後の数字に 1 を割り当てる (第 1 回目の分割では、最初の数字に充当する)
- (4) 分割されたグループが二つ以上の記号をもつならば、(2)~(3) を繰り返す
- (5) すべてのグループが一つの記号で構成されたとき、アルゴリズムを終了する

前出の例に対してファノ符号を適用して生成される符号を  $C_F$  とすると、表 3 のようになる。図 2 に示すようにファノ符号も語頭符号として 2 分木で表現できる。

表 3 から、例題のファノ符号の平均符号語長を求めると、

表 2 シヤノン符号  $C_S$  の符号例

| 記号 $x$ | 語頭符号 $C_S$ |
|--------|------------|
| $a$    | 00         |
| $b$    | 010        |
| $c$    | 110        |
| $d$    | 0110       |
| $e$    | 111        |
| $f$    | 0111       |

表 3 例題のファノ符号

| 記号 $x$ | $P(x)$ | 第 1 分割 | 第 2 分割 | 第 3 分割 | 最終符号 $C_F$ |
|--------|--------|--------|--------|--------|------------|
| $a$    | 1/3    | 0      | 0      |        | 00         |
| $b$    | 1/6    | 0      | 1      |        | 01         |
| $c$    | 1/6    | 1      | 0      | 0      | 100        |
| $e$    | 1/6    | 1      | 0      | 1      | 101        |
| $d$    | 1/12   | 1      | 1      | 0      | 110        |
| $f$    | 1/12   | 1      | 1      | 1      | 111        |

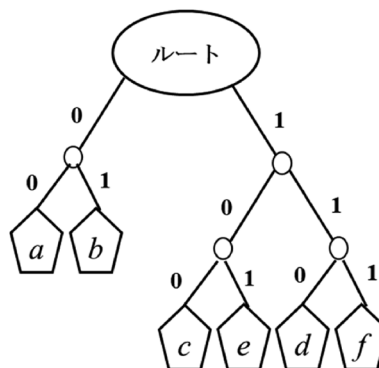


図 2 例題のファノ符号の 2 分木表現

$$L_{C_F}(X) = \frac{1}{3} \times 2 + \frac{1}{6} (2 + 3 \times 2) + \frac{1}{12} (3 \times 2) = \frac{5}{2} = 2.5$$

となる。もちろん、エントロピー  $H(X) = 2.418$  より大きいのが、シャノン符号の平均符号語長  $L_{C_S}(X) = 2.833$  より 0.333 bit 圧縮している。

ファノ [69] は 1917 年、イタリアのトリノで生まれた。1939 年、トリノ工科大学を卒業したが、ムッソリーニ (Benito Mussolini) が制定した反ユダヤ法を逃れてアメリカへ移民として渡った。1941 年、MIT で電気工学専門の学士号を取得後、同大学の放射能研究所の職員として働いた。第 2 次世界大戦後、MIT の博士課程に進み、1947 年、博士号を取得、そのまま電気工学科の教員となった。マイクロ波、情報理論、コンピュータ科学の分野で先駆的な研究を行い、前述の符号化アルゴリズムは、1949 年 MIT の Technical

Report として発表された。

情報理論の分野では、シャノン符号を「シャノン-ファノ符号」として言及することが多い。明らかに二つの符号化方法論は異なっており、それぞれが独立的に開発された。にもかかわらず同一視されることになった理由の一つは、シャノンが1948年の自分の論文の中でファノの符号化法を紹介し、「非常に似ている」と言及していることにあると思われる。当時、シャノンはベル研究所に在籍しており、ファノはMITの教員となっていたが、シャノンは何らかの研究交流を通して、論文発表前のファノの符号化法を知っていたことになる。Wikipedia [70]によれば、シャノンの符号化法をシャノン-ファノ符号として言及する研究者群と、ファノの符号化法をシャノン-ファノ符号として言及する研究者群とが混在しているようである。研究者の世界においては、珍しい現象ではある。

### 3. ハフマン符号

シャノン符号もファノ符号も、平均符号語長の下限值であるエントロピーとの差を1bitの範囲で収める語頭符号を生成する点で優れているといえるが、最小語頭符号

$$C_X^* = \operatorname{argmin}_{C \in HC(S)} \left\{ L_C(X) = \sum_{x \in S} P(x) l_C(x) \right\} \quad (3.1)$$

を実現することを保証する訳ではない。このギャップを埋めるべく、平均符号語長が最小語頭符号となる符号の生成アルゴリズムを確立したのがデイビット・ハフマン (David Albert Huffman)[71]である。1952年に発表されたこの方式は、ハフマン符号と呼ばれているが、ここでは  $C_H$  で表わすことにする。

ハフマンは1925年、オハイオ州に生まれた。アメリカのコンピュータ科学の先駆者であり、折り紙を数学的に体系化した業績でも知られている。1944年、オハイオ州立大学を電気工学専攻で卒業、すぐに海軍士官となり、そこで終戦を挟む2年間を過ごした。その後、オハイオ州立大学に戻り、1949年に修士号を得てからMITの博士課程に進学。1953年、“The Synthesis of Sequential Switching Circuits (連結回路の合成)”という題名の学位論文によって博士号を取得し、MITの教員となった。ハフマン符号に関する論文は、博士学生であった1952年に発表した。本人は学位論文の方が重要な貢献であると考えていたようである。1967年、カリフォルニア大学サンタ・クルーズ校に移り、Computer Science Department の設立に貢献、

1970年から1973年まで学科長を務めた。IEEE から多くのメダルを授与され、1994年に退職、1999年、サンタ・クルーズで74歳の生涯を閉じた。

ハフマン符号の生成アルゴリズムは、次の定理で示す、最小語頭符号  $C_X^*$  が満たすべき四つの条件に基礎を置いている。なお、自明の場合を排除して  $|S| \geq 2$  を仮定する。このとき、2分木で親ノードを共有する二つのノードを兄弟ノードと呼ぶことにする。

#### 定理 3.1

$C_X^*$  を式 (3.1) で定まる最小語頭符号とし、それを2分木で表わしたとき、任意の節点から伸びる左側の枝に0、右側の枝に1を割り当てるものとする。このとき、以下の命題が成立する。

- (a)  $P(x) > P(y) \Rightarrow l_{C_X^*}(x) \leq l_{C_X^*}(y)$
- (b)  $C_X^*$  を2分木で表わしたとき、リーフ・ノード以外の内部節点からは、必ず2本の枝が伸びている。
- (c) 以下の条件を満たす  $x_{min:1}$  と  $x_{min:2}$  が存在する。
  - (1)  $\min_{z \in S} \{P(z)\}$  が一意に定まるときは、 $x_{min:1} = \operatorname{argmin}_{z \in S} \{P(z)\}$ 、二つ以上の記号で実現される場合は、その中で最も大きな深度をもつ記号を  $x_{min:1}$  とする。このとき、 $x_{min:1}$  は  $x \in S$  全体で最も大きな深度を実現する。
  - (2) 最小語頭符号が存在して、 $x_{min:1}$  の兄弟ノード  $x_{min:2}$  を、 $x_{min:2} = \operatorname{argmin}_{z \in S \setminus \{x_{min:1}\}} \{P(z)\}$  を満たすようにすることができる。
  - (3)  $l_{C_X^*}(x_{min:1}) = l_{C_X^*}(x_{min:2})$
  - (4)  $C_X^*(x_{min:1})$  と  $C_X^*(x_{min:2})$  は、最後の桁の数字のみが異なる。

#### [証明]

$C_X^*$  の符号語に現れる記号  $x$  と  $y$  を交換することで得られる符号を  $\hat{C}_X$  とする。もし  $l_{C_X^*}(x) > l_{C_X^*}(y)$  であるとすると、

$$\begin{aligned} L_{C_X^*}(X) - L_{\hat{C}_X}(X) &= P(x)l_{C_X^*}(x) + P(y)l_{C_X^*}(y) - P(x)l_{\hat{C}_X}(y) \\ &\quad - P(y)l_{\hat{C}_X}(x) \\ &= \{P(x) - P(y)\} \{l_{C_X^*}(x) - l_{C_X^*}(y)\} > 0 \end{aligned}$$

となり、これは  $C_X^*$  の最小性に矛盾するので (a) が証明された。

次に、2分木の内部節点が存在し、そこから1本だけ枝が伸びていると仮定する。その枝を切断し、その内部節点を到達点とする枝と入れ替えると、すべてのリーフ・ノードはリーフ・ノードとして保たれるので、

結果として得られる 2 分木もまた語頭符号に対応する。

この操作により、切断された部分木に属するリーフ・ノードに対応する符号語の符号語長は 1 bit だけ短くなるので、 $C_X^*$  の最小性に反し、(b) が示された。

(c) に関しては、(1) の手続きによって定まる  $x_{min:1}$  が  $x \in S$  全体で最も大きな深度を実現しないと仮定しよう。このとき、最も大きな深度を実現するノードを  $y$  とする。明らかに、 $l_{C_X^*}(y) > l_{C_X^*}(x_{min:1})$  が成立する。一方、 $x_{min:1}$  の定め方から、 $P(y) > P(x_{min:1})$  であり、(a) より  $l_{C_X^*}(y) \leq l_{C_X^*}(x_{min:1})$  となり、これは矛盾である。したがって、 $x_{min:1}$  は  $x \in S$  上で最大深度を実現することになり、(1) が証明された。

$|S| \geq 2$  の仮定と (b) より、 $x_{min:1}$  は必ず兄弟ノード  $w$  をもつ。もし  $P(w) = \arg \min_{z \in S \setminus \{x_{min:1}\}} \{P(z)\}$  であれば、 $w = x_{min:2}$  とすれば (2) を満たす。一方、 $y \in S$  が存在して  $P(y) = \arg \min_{z \in S \setminus \{x_{min:1}\}} \{P(z)\} < P(w)$  を満たすとする、(a) より、 $l_{C_X^*}(y) \geq l_{C_X^*}(w)$  が成立する。 $l_{C_X^*}(y) > l_{C_X^*}(x_{min:2})$  であれば、 $y$  と  $x_{min:2}$  を入れ替えた符号  $\hat{C}_X^*$  に対し、 $L_{\hat{C}_X^*}(X) < L_{C_X^*}(X)$  となる。明らかに  $\hat{C}_X^*$  は語頭符号であるので、これは  $C_X^*$  が最小語頭符号であることに矛盾する。よって、 $l_{C_X^*}(y) = l_{C_X^*}(x_{min:2})$  が成立し、 $L_{\hat{C}_X^*}(X) = L_{C_X^*}(X)$  となる。すなわち、 $\hat{C}_X^*$  も最小語頭符号であり、 $y = x_{min:2}$  とすることで (2) が示された。(3) と (4) は、 $X_{min:1}$  と  $x_{min:2}$  が兄弟ノードであることから、ただちに結論される。□

記号集合を  $S$  とし、 $S$  上で定義される確率変数  $X$  とその確率分布  $P(x) = P[X = x]$  が与えられたとき、定理 3.1 に基づき、 $C_X^*$  を実現するハフマン符号の生成アルゴリズムを、以下のように記述することができる。

#### ハフマン符号 $C_H$ の生成アルゴリズム

- [1]  $S$  の要素を  $P(x_i) \geq P(x_{i+1}), i = 1, \dots, N-1$ , を満たすように  $x_1, \dots, x_{N-1}, x_N$  と並べ替える
- [2]  $k \leftarrow 1; M \leftarrow N; x_i(0) \leftarrow x_i, i = 1, \dots, N$
- [3] LOOP:  $x_i(k) \leftarrow x_i(k-1), i = 1, \dots, M-2; \{x_{M-1}(k-1), x_M(k-1)\}$  を新しい記号  $x_{M-1}(k)$  に置き換える
- [4]  $P(x_i(k)) = P(x_i(k-1)), i = 1, \dots, M-2; P(x_{M-1}(k)) = P(x_{M-1}(k-1)) + P(x_M(k-1))$
- [5]  $\{x_1(k), \dots, x_{M-1}(k)\}$  を  $P(x_i(k)) \geq P(x_{i+1}(k))$  となるように並べ替え、左側から番

号を  $\{x_1(k+1), \dots, x_{M-1}(k+1)\}$  と付け替える

- [6]  $M \leftarrow M-1; k \leftarrow k+2$
- [7]  $M > 2$  であれば LOOP へ
- [8] 以上の操作に対応する 2 分木を作成、内部節点から伸びる二つの枝の左側に 0、右側に 1 を付与して語頭符号  $C_H$  を生成する

#### 定理 3.2 ハフマン符号 $C_H$ の最小性

ハフマン符号  $C_H$  は、 $C_H = C_X^*$  を満たす。

[証明]

$|S|$  に関する帰納法で証明する。二つの要素をもつ  $S(2)$  を考え、この上で定義される確率変数を  $X(2)$ 、その確率分布を  $P(x|2) = P[X(2) = x]$  と書く。一般性を失うことなく  $S(2) = \{x_1, x_2\}, P(x_1|2) \geq P(x_2|2)$  と仮定できる。このとき、生成可能なハフマン符号は以下の 2 通りのみである。

| 記号 $x$ | $C_{H:1}$ | $C_{H:2}$ |
|--------|-----------|-----------|
| $x_1$  | 0         | 1         |
| $x_2$  | 1         | 0         |

明らかに、 $L_{C_{H:1}}(X(2)) = L_{C_{H:2}}(X(2)) = 1 \times P(x_1|2) + 1 \times P(x_2|2) = 1 = L_{C_{X(2)}^*}(X(2))$  が成立し、 $C_{H:1}$  と  $C_{H:2}$  はともに最小平均符号語長を実現する。

今、 $N-1$  個の要素からなる  $S(N-1)$  を考え、この上で定義される確率変数  $X(N-1)$  の確率分布  $P(x|N-1)$  が与えられたとき、そこから生成される任意のハフマン符号が、 $S(N-1)$  で定義される語頭符号集合  $HC(S(N-1))$  上で最小平均符号語長を実現すると仮定する。ここで、 $N$  個の要素からなる  $S(N)$  を考え、この上で定義される確率変数  $X(N)$  が確率分布  $P(x|N)$  をもつとする。 $S(N)$  の要素を  $x_1, \dots, x_{N-1}, x_N$  と並べ替え、 $P(x_i|N) \geq P(x_{i+1}|N), i = 1, \dots, N-1$ , を満たすようにする。 $S(N-1) = \{x_2, \dots, x_{N-1}, x_N\}$  とし、この上で定義される確率変数  $X(N-1)$  の確率分布を  $P(x|N-1) = P(x|N) / \{1 - P(x_1|N)\}$  と定義する。すると帰納法の仮定より、これから生成されるハフマン符号  $C_H(N-1)$  は  $S(N-1)$  で定義される語頭符号集合  $HC(S(N-1))$  上で最小平均符号語長を実現する。すなわち、

$$\begin{aligned}
C_H(N-1) &= C_{X(N-1)}^* \\
&= \arg \min_{C \in HC(S(N-1))} \left\{ L_C(X) \right. \\
&\quad \left. = \sum_{x \in S(N-1)} P(x|N-1) l_C(x) \right\} \\
&= \arg \min_{C \in HC(S(N-1))} \left\{ L_C(X) \times \{1 - P(x_1|N)\} \right\} \\
&= \sum_{x \in S(N-1)} P(x|N) l_C(x) \left. \right\}
\end{aligned}$$

ハフマン符号生成アルゴリズムを適用した際の  $C_H(N-1)$  の最終形は、深度 1 の 2 分木となっている。

$P(x_1|N) \geq 1/2$  であれば  $x_1$  の右側、そうでない場合は左側に  $C_H(N-1)$  をおくと深度 2 の 2 分木が構成され、これにハフマン符号生成アルゴリズムを適用すると 1 ステップで収束する。すると、最終的に、 $L_{C_H(N)}(X(N)) = 1 \times P(x_1|N) + \{1 + L_{C_H(N-1)}(X(N-1))\} \{1 - P(x_1|N)\} = L_{C_H(N)}^*(X(N))$  となり、最後の結合を含めて生成されたハフマン符号  $C_H(N)$  は、 $HC(S(N))$  上で最小平均符号語長を実現することになり、定理が証明された。□

表 1 に与えられた例題に、ハフマン符号生成アルゴリズムを適用してみる。

| 記号 $x$ | $a$ | $b$ | $c$ | $d$  | $e$ | $f$  |
|--------|-----|-----|-----|------|-----|------|
| $P(x)$ | 1/3 | 1/6 | 1/6 | 1/12 | 1/6 | 1/12 |

これを、生成確率の降順に並べ替える。

| 記号 $x$ | $a$ | $b$ | $c$ | $e$ | $d$  | $f$  |
|--------|-----|-----|-----|-----|------|------|
| $P(x)$ | 1/3 | 1/6 | 1/6 | 1/6 | 1/12 | 1/12 |

並べ替えた後、左側から  $x_1(0) \sim x_6(0)$  と番号を付け替える。  $M = N = 6$  である。

| 記号 $x$ | $x_1(0)$ | $x_2(0)$ | $x_3(0)$ | $x_4(0)$ | $x_5(0)$ | $x_6(0)$ |
|--------|----------|----------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/6      | 1/6      | 1/6      | 1/12     | 1/12     |

$x_i(1) \leftarrow x_i(0), i = 1, \dots, 4, \{x_5(0), x_6(0)\}$  を新たに  $x_5(1)$  と設定し、 $P(x_5(1)) = P(x_5(0)) + P(x_6(0)) = 1/12 + 1/12 = 1/6$  とする。

| 記号 $x$ | $x_1(1)$ | $x_2(1)$ | $x_3(1)$ | $x_4(1)$ | $x_5(1)$ |
|--------|----------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/6      | 1/6      | 1/6      | 1/6      |

これを改めて降順に並べ替え、番号を付け替えるが、この例ではたまたま  $P(x_5(1)) = 1/6$  が最小値となったので、 $x_i(2) \leftarrow x_i(1), i = 1, \dots, 5$  となる。

| 記号 $x$ | $x_1(2)$ | $x_2(2)$ | $x_3(2)$ | $x_4(2)$ | $x_5(2)$ |
|--------|----------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/6      | 1/6      | 1/6      | 1/6      |

$M = 5, x_i(3) \leftarrow x_i(2), i = 1, \dots, 3, \{x_4(2), x_5(2)\}$  を  $x_4(3)$  と設定し、 $P(x_4(3)) = 1/6 + 1/6 = 1/3$  とする。

| 記号 $x$ | $x_1(3)$ | $x_2(3)$ | $x_3(3)$ | $x_4(3)$ |
|--------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/6      | 1/6      | 1/3      |

これを降順に並べ替えて、

| 記号 $x$ | $x_1(3)$ | $x_4(3)$ | $x_2(3)$ | $x_3(3)$ |
|--------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/3      | 1/6      | 1/6      |

改めて番号を  $x_i(4), i = 1, \dots, 4$  として付け替える。

| 記号 $x$ | $x_1(4)$ | $x_2(4)$ | $x_3(4)$ | $x_4(4)$ |
|--------|----------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/3      | 1/6      | 1/6      |

$M = 4, x_i(5) \leftarrow x_i(4), i = 1, 2, \{x_3(4), x_4(4)\}$  を  $x_3(5)$  と設定し、 $P(x_3(5)) = 1/6 + 1/6 = 1/3$  とする。

| 記号 $x$ | $x_1(5)$ | $x_2(5)$ | $x_3(5)$ |
|--------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/3      | 1/3      |

この場合も  $P(x_3(5))$  は最小値なので順番は変わらず、 $x_i(6) \leftarrow x_i(5), i = 1, 2, 3$  となる。

| 記号 $x$ | $x_1(6)$ | $x_2(6)$ | $x_3(6)$ |
|--------|----------|----------|----------|
| $P(x)$ | 1/3      | 1/3      | 1/3      |

$M = 3, x_1(7) \leftarrow x_1(6), x_2(7) \leftarrow \{x_2(6), x_3(6)\}$  と設定し、 $P(x_2(7)) = 1/3 + 1/3 = 2/3$  とする。

| 記号 $x$ | $x_1(7)$ | $x_2(7)$ |
|--------|----------|----------|
| $P(x)$ | 1/3      | 2/3      |

これを降順に並べ替えて、

| 記号 $x$ | $x_2(7)$ | $x_1(7)$ |
|--------|----------|----------|
| $P(x)$ | 2/3      | 1/3      |

改めて番号を付け替えると

| 記号 $x$ | $x_1(8)$ | $x_2(8)$ |
|--------|----------|----------|
| $P(x)$ | 2/3      | 1/3      |

を得る。ここで、 $M = 2$  となって、アルゴリズムは収束する。

以上の操作の結果を 2 分木で表わしたものを図 3、対応するハフマン符号の具体例を表 4 に示す。

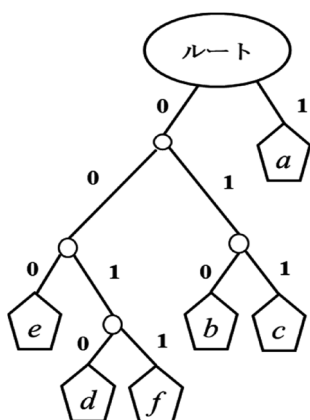


図3 例題のハフマン符号の2分木表現

表4 例題のハフマン符号

| 記号 $x$ | $P(x)$ | $C_H(x)$ |
|--------|--------|----------|
| $a$    | $1/3$  | 1        |
| $b$    | $1/6$  | 010      |
| $c$    | $1/6$  | 011      |
| $e$    | $1/6$  | 000      |
| $d$    | $1/12$ | 0010     |
| $f$    | $1/12$ | 0011     |

表4から、例題のハフマン符号の平均符号語長を求めると、

$$L_{CH}(X) = \frac{1}{3} \times 1 + \frac{1}{6} (3 \times 3) + \frac{1}{12} (4 \times 2) = \frac{5}{2} = 2.5$$

となる。これをエントロピー、シャノン符号、ファノ符号と比べてみると、

$$\begin{aligned} H(X) &= 2.418 < L_{CH}(X) = L_{CF}(X) \\ &= 2.5 < L_{CS}(X) \\ &= 2.833 \end{aligned}$$

となっている。ファノ符号の2分木表現である図2を見てみると定理3.1の条件を満たしており、この場合は偶然、ファノ符号はハフマン符号となっている。ハフマン符号は一意的ではないことを示す例である。シャノン符号の2分木表現である図1を見てみると、深度1で1を割り振られた内部節点が定理3.1(b)を満たしておらず、ハフマン符号とはなっていない。

#### 4. LZ符号

シャノン符号、ファノ符号、ハフマン符号は、すべて、 $\mathcal{S}$ 上で定義される確率変数  $X$  の確率分布  $P(x) = P[X = x]$  をあらかじめ求めてからでないと生成することができない。これは大規模なデータ送信を行う際には、極めて不便である。この難題を初めて克服したの

はイスラエルの Technion-Israel Institute of Technology の2人の研究者エイブラハム・レンペル (Abraham Lempel) [72] と ジェイコブ・ジヴ (Jacob Ziv) [73] である。1977年の共著論文 [74] で、2人は増分分解と呼ばれる概念を導入し、送信される記号列を順次、部分列に分解し、得られた部分列を符号語に対応させることにより、確率分布  $P(x)$  を前提知識とすることなくデータ圧縮を実現する手法を開発した。この手法の正式名称は、学界の慣例に従えば論文著者の順番に従って Ziv-Lempel 符号であり、当初はそれを省略して LZ 符号と呼ばれていた。しかし、ある著名なコンピュータ科学者が自分の論文の中で間違えて LZ 符号として紹介したため、その後、LZ 符号の呼称が定着してしまった。2人は1977年の論文に改良を加え、後述するエントロピーへの収束を証明する数学的な解析を付加した論文を1978年に発表 [75]、現在は、前者を LZ77、後者を LZ78 と呼ぶことが一般化している。

ここでは、まず、LZ78 符号を生成するアルゴリズムの中核部分をサブアルゴリズムとして紹介する。入力として必要なのは、送信されるべき符号列  $\underline{s} = (x_1, \dots, x_{N-1}, x_N)$  のみである。出力は、サブアルゴリズムが  $K(N)$  個の部分列を生成したとして、各部分列について、 $(i(k), x(k)), k = 1, \dots, K(N)$  のペアである。ここで、 $i(k)$  は、 $k$  番目の部分列の最後の1bitを除いた部分がそれまでの部分列に現れていれば、その部分列の番号 ( $1 \leq i(k) \leq k-1$ )、現れていなければ  $i(k) = 0$  とする。また、 $x(k)$  は  $k$  番目に生成された分解部分列の最後尾の記号を表す。

記法を簡便化するため、ベクトル  $\underline{w}$  の先頭から  $n$  個の要素を取り出したベクトルを  $\underline{w}_{\uparrow n}$ 、先頭から  $n$  個の要素を取り除いたベクトルを  $\underline{w}_{\downarrow n}$  で表す。また、 $|\underline{w}|$  で  $\underline{w}$  の要素の数を表す。

#### LZ78 符号生成のサブアルゴリズム

- [1]  $\underline{s}(1) \leftarrow (x_2, \dots, x_{N-1}, x_N); L_{SUV}(1) \leftarrow (x_1); i(1) \leftarrow 0; x(1) \leftarrow x_1; k \leftarrow 1$
- [2] LOOP:  $k \leftarrow k + 1$
- [3] 任意の長さの  $\underline{s}(k-1)$  の先頭部分列が、すべての  $j \in \{1, \dots, k-1\}$  に対して  $L_{SUV}(j)$  と一致しなければ、 $i(k) \leftarrow 0; x(k) \leftarrow L_{SUV}(k) \leftarrow \underline{s}_{\uparrow 1}(k-1); \underline{s}(k) \leftarrow \underline{s}_{\downarrow 1}(k-1)$
- [4] ある  $j \in \{1, \dots, k-1\}$  が存在して、 $\underline{s}(k-1)$  の先頭からのある最長部分列が、 $L_{SUV}(j)$  と一致すれば、 $i(k) \leftarrow j; L_{SUV}(k) \leftarrow \underline{s}_{\uparrow(|L_{SUV}(j)|+1)}(k-1);$

表 5 LZ78 符号生成サブアルゴリズムの例

| 増分分解                      | 辞書          |        | 送信符号列         |               |
|---------------------------|-------------|--------|---------------|---------------|
|                           | 分解部分列<br>番号 | 分解部分列  | 分解部分列<br>接続番号 | 分解部分列<br>最終記号 |
| abcacbaaccbac             | 0           | $\phi$ |               |               |
| a, bcacbaaccbac           | 1           | a      | 0             | a             |
| a, b, cacbaaccbac         | 2           | b      | 0             | b             |
| a, b, c, acbaaccbac       | 3           | c      | 0             | c             |
| a, b, c, ac, baaccbac     | 4           | ac     | 1             | c             |
| a, b, c, ac, ba, accbac   | 5           | ba     | 2             | a             |
| a, b, c, ac, ba, acc, bac | 6           | acc    | 4             | c             |
| a, b, c, ac, ba, acc, bac | 7           | bac    | 5             | c             |

$$\hat{s}(k-1) \leftarrow \underline{s}_{\downarrow(L_{SUUV}(j))}(k-1);$$

$$x(k) \leftarrow \hat{s}_{\uparrow 1}(k-1); \underline{s}(k) \leftarrow \hat{s}_{\downarrow 1}(k-1)$$

[5]  $\underline{s}(k)$  に要素が残っていれば LOOP へ、残っていないければ終了

以下、 $\underline{s} = (\text{abcacbaaccbac})$  という記号列の送信を例にとって、LZ78 符号の生成サブアルゴリズムを走らせた結果を表 5 に纏めてある。第 1 列目は  $\underline{s}, (L_{SUUV}(1), \dots, L_{SUUV}(k), \underline{s}(k)), k = 1, \dots, K(N) = 7$  を示し、増分分解の状態推移を表している。第 2 列目が  $k$ 、第 3 列目は分解部分列  $L_{SUUV}(k)$ 、最後の 2 列で出力  $(i(k), x(k))$  を与えている。たとえば、 $k = 6$  を見てみると、 $\underline{s}(5) = (\text{accbac})$  に対して、先頭の 2 記号 (ac) が  $L_{SUUV}(4)$  と一致するので、次の記号 c を語尾に加えて  $L_{SUUV}(6) = (\text{acc})$  とし、 $\underline{s}(5)$  からこれを取り除いて  $\underline{s}(6) = (\text{bac})$ 、出力は、 $(i(6), x(6)) = (4, c)$  となる。

出力された  $(i(k), x(k)), k = 1, \dots, K(N)$  を受信すれば、元の記号列  $\underline{s}$  が復元できることは明らかであり、これらのペアを 0-1 表示に変換したものが、実際に送信される圧縮データを構成する。 $i(k) \in \{0, 1, \dots, k-1\}$  であり、 $x(k)$  は  $\underline{s}$  の要素の一つであるから、それぞれを 2 進数表示に変換する際に必要となる桁数は、 $\lceil \log_2 k \rceil$  と  $\lceil \log_2 |\underline{s}| \rceil = \lceil \log_2 N \rceil$  である。したがって、 $L_{SUUV}(k)$  を圧縮化した後のデータの長さを  $L_{0-1}(k)$  とすると、

$$L_{0-1}(k) = \lceil \log_2 k \rceil + \lceil \log_2 N \rceil \quad (4.1)$$

が成立する。これより、 $\underline{s} = (x_1, \dots, x_{N-1}, x_N)$  全体の圧縮データの長さ  $L_{0-1}(x_1, \dots, x_{N-1}, x_N)$  は、

$$L_{0-1}(x_1, \dots, x_{N-1}, x_N) = \sum_{k=1}^{K(N)} \lceil \log_2 k \rceil + K(N) \times \lceil \log_2 N \rceil \quad (4.2)$$

で与えられる。式 (4.2) は  $\underline{s} = (x_1, \dots, x_{N-1}, x_N)$  が

与えられたときに機械的に定まり、以下で議論する裏側に隠された確率的構造に一切、関係しない。それが LZ78 符号の特徴である。

$S$  で定義される離散的確率過程  $X_t, t = 1, 2, \dots$  に対し、 $x_t$  を  $X_t$  の実現値とする。 $P(x_1, \dots, x_{N-1}, x_N) = P[X_1 = x_1, \dots, X_{N-1} = x_{N-1}, X_N = x_N]$  とすると、対応するエントロピー  $H(X_1, \dots, X_{N-1}, X_N)$  は、

$$H(X_1, \dots, X_{N-1}, X_N) = - \sum_{(x_1, \dots, x_{N-1}, x_N) \in S^N} P(x_1, \dots, x_{N-1}, x_N) \times \log_2 P(x_1, \dots, x_{N-1}, x_N) \quad (4.3)$$

で与えられる。

$S$  で定義される離散的確率過程  $X_t, t = 1, 2, \dots$  が互いに独立で同じ確率分布  $Q(x) = P[X = x]$  をもつとする。このとき、

$$H(X) = \lim_{N \rightarrow \infty} \frac{1}{N} H(X_1, \dots, X_{N-1}, X_N) \quad (4.4)$$

が存在する。この条件下で、Ziv と Lempel は共著論文 [75] で以下の定理を証明した。証明は難しくはないが、必要とされる前提知識が拡がるので、ここでは省略する。

#### 定理 4.1 LZ78 符号の最小性

$S$  で定義される離散的確率過程  $X_t, t = 1, 2, \dots$  が互いに独立で同じ確率分布  $Q(x) = P[X = x]$  をもつとき、式 (4.2) と式 (4.4) に関し、

$$H(X) = \lim_{N \rightarrow \infty} \frac{1}{N} L_{0-1}(x_1, \dots, x_{N-1}, x_N)$$

が成立する。

定理 4.1 は、送信される記号列が十分に長いとき、LZ78 符号の 1 符号当たりの符号語長は、データ圧縮

率の下限値であるエントロピー  $H(X)$  bit に限りなく近づくことを主張している。文献 [75] 以降、多くの研究者によって改良が加えられ、現在、ほとんどの大規模データ送信が、ここから派生したデータ圧縮技術に基づいて行われている。また、通信システムのマルチメディア化に伴い、音声データ、画像データに関しても統計学を駆使したそれぞれに固有のデータ圧縮技術が開発されているが、思想的には Ziv と Lempel の発想を受け継いでいるといえよう。ここまで、シャノンの第一基本定理（情報源符号化定理）を出発点として、ノイズや通信誤作動が発生しないことを前提に、通信効率化を目指すデータ圧縮理論の展開を見てきた。言葉を換えると、これらは効率的なデータ通信を実現するための「データ表現」の体系に過ぎないといえる。実際の通信効率を評価するためには、情報伝送の限界を示す通信路容量が問題となる。この方面の扉を開いたのもシャノンで、1948 年に発表した第一基本定理と同じ論文の中で、第二基本定理（通信路符号化定理）を確立した。次号では、この定理を解説する。

## 5. 閑話休題

何人かの読者からメールを戴いた。その趣旨はおおむね共通で、「連載は面白いので読んでいますが、一体、何時になったら『現在』に辿り着くのですか？」というものであった。これはもっともな疑問で、ペースが遅すぎるといって読者の苛立ちを表わしていると思われる。筆者としては、連載を通して実現したいと願っている意図を優先させた結果、このような進み具合になっている、というのが正直な本音である。ここで、連載の意図を改めて述べることは、読者の苛立ちを多少なりとも和らげるかも知れないと思ひ立ち、この閑話休題を書いている。

情報技術が深化・拡散し、社会生活のあらゆる局面で陰に陽に関わるようになって来ている現在、OR 研究者はもとより、できるだけ多くの人々が、人間的感覚をもって情報技術に接することができるようになることが、これからの社会にとって極めて重要である。情報技術に対し、普通感覚で物申すことのできる人々が多数を占めることにより、情報技術の暴走を未然に防ぐ本質的な抑止力が準備されるからである。この面で大きく貢献したものとして、NHK の「プロジェクト X」や派生的に出版された「電子立国日本」、フジテレビの「ほこ・たて」などの例を挙げることができるが、これらは離散的で単発であった。歴史的な時間軸に沿って技術革新を俯瞰することにより、現在の情報

技術の裏にある「人間の手触り」を伝えること、これが連載執筆の最大の目的である。あえて、「コンピュータ科学の数学的基礎」を含めた所以でもある。

連載の構造は「No.1 連載を始めるにあたって」で述べたように、3 部構成になっている。第 1 部は、電信電話網が社会的基盤として形成された時代からインターネットの普及までを、技術革新の側面から振り返ることにある。この期間の特徴は、革命的な技術革新は数多くあったものの、既存技術の影響力が及ぶ範囲を連続的に拡大してきたことにある。言葉を換えると、既存技術の発展経路から外挿的に捉えられる形で技術革新が進み、それに伴う社会的変化もまた、既存の慣性力を拡大する形で連続的に進んできたといえよう。

第 2 部では、DX (Digital Transformation) 化を契機とする変容を体系的に捉える試みに挑戦する。この時代の特徴は、ハードウェアとソフトウェアの組み合わせの技術革新が、多様かつ大規模に、また質的にも深く、百花繚乱的に展開されつつある点に見出される。社会的には、既存システムの慣性力を突き抜ける変容が相当程度のスピードを以て胚胎されつつあり、それが顕現する際には、対応することが手遅れになるような事態が想定される。たとえば、モノ造りやサービス産業を支える Value Chain において、新しい連鎖が突然出現したり、また、既存の連鎖が突然、消滅してしまうというような事態が起こり得る。戦略的には、胚胎しつつある変化の先を見据え、将来、そこで自社はどのような場所を占めたいのかを「ありたい姿」として構想し、そこへ至るべく近未来的に実現すべき「あるべき姿」を措定、さらに現在から出発してそこへ向かう行動計画を確立・実践するという、3 段階構造からなる“Backcasting Approach”が重要となる。

第 3 部では、北米・EU・日本を含むアジアの先進地域からなる 3 局体制を比較分析するための共通尺度として社会システム・モデルを素描し、直接金融 vs. 間接金融という金融システムの違いに着目して、3 局体制の差異を通時的・共時的に論じる予定である。

世界を OR するための視線を獲得するためには、第 2 部の本質に象徴される現在の課題を意識しつつ、第 1 部で議論を進めている技術革新の歴史に立ち戻り、その時点での悪銭苦闘の本質から現在を照射することが重要である。今までの議論から、一つだけ例を挙げてみる。

近年、モノ製品を販売していた製造業が、その製品の中にサービスを含め、それを商品として販売し利潤を上げようとする新たなビジネス・モデルが出現してい



る。こうした現象は「モノからコトへのシフト」という標語で語られることが多いが（たとえば文献 [76]）、言葉を換えると、製品を売切るのではなく、その効用を継続的に販売するともいえよう。このビジネス・モデルの主要な戦略的意図としては、

- ① 顧客の資金負担を軽減し、購買意欲を促す
- ② Market segmentation が進む中、ますます多品種少量化する顧客ニーズに対し、迅速かつ効率的に対応する

を挙げることができる。

このビジネス・モデルは新しいものではなく、古くは家庭への菓の置き売りを開発した江戸時代の富山の菓売りまでさかのぼるが、連載第 10 回で述べたように、19 世紀のアメリカでも優れた靴の縫製機の量産体制を開発したゴードン・マッケイ (Gordon McKay) がいる。南北戦争が勃発し、ブーツの需要が飛躍的に伸びることを見抜いたマッケイは、彼の製造する靴の縫製機を販売せずに無料で貸し出し、その機械で製造・販売される靴のそれぞれから些少な歩合を得るというビジネス・モデルを導入した。すなわち、靴の縫製機を製品として売切ることせず、『靴を縫製する』という効用を販売するビジネス・モデルを開発したのである。これが見事に当たり、1876 年には歩合収入だけで年間 500,000 ドルを超えるまでに成長し、巨万の富を築いた。

その後も、ベル電話会社の受話器、Xerox のコピー機など、このビジネス・モデルを散見することができるが、どの場合も、「効用を提供する企業と、効用を享受しそれに対して料金を支払う顧客とが同意できる形で、効用を計量化するシステム」が確立されている。マッケイのモデルでは、リースされた縫製機で製造される 1 足の靴が効用の基本単位であり、ベル電話会社の場合は、登録された送信元と受信先の電話番号によって距離を測り、回線の接続時間を通話時間として記録することで、透明性のある効用測定システムを整備した。Xerox 社の場合は、多大な開発資金を投じてコピー枚数を正確に記録する計数器を開発したことにより、コピーの枚数が増えれば単価が安くなるという階段構造をもつ価格体系の導入を可能にした。

このビジネス・モデルが広く普及することがなかった最大の理由は、そうした評価システムを用意することが極めて困難であったことにある。近年、「モノからコトへのシフト」として急速に拡大した背景には、MPU (Micro Processing Unit) の普及によりインターネットへの接続が多様化し、さまざまな分野において、顧

客の効用測定を正確に行う手段が比較的容易に準備できるようになったことがある。連載第 10 回では、これを技術革新の法則 (13) として、以下のようにまとめている。

技術革新の法則 (13) 効用販売型ビジネス・モデルの有効性：以下の条件が満たされるとき、技術革新の成果を効用販売型ビジネス・モデルとして展開することは有効である

- ① 必要資本投資を、継続的な資金の流れとして回収することに耐えられるだけの資本力を有する
- ② 提供される効用の市場規模が十分に大きく、また、そのライフ・サイクルが十分に長い
- ③ 効用の計量化を実現するシステムが用意され、かつ、その監視コストが低い

「モノからコトへのシフト」のルーツは、実は遙か昔から存在したのであり、それを成立せしめるに必要な条件が多様な分野で整ったことにより、現在、急速な拡大を見せているという理解こそが、世界を OR するための視線に繋がる。連載の構想は膨大で、完結までにはまだまだ時間を要する。編集部の皆さんの理解を得ながら、可能な限り健康を保ち、何とか完結させたいと強く願っているが、一方、人生はすべからく未完である。万一、志半ばで中断を余儀なくされたとしても、そこまでに織り込んだ技術革新の法則を通して、読者諸氏が世界を OR するための視線を自ら獲得することに役立つよう心掛けたいと思っている。

謝辞 連載を通して、常に、編集委員長ならびに機関誌編集事務局の方々には極めて丁寧な推敲を賜り、幾つもの誤りを訂正して戴き、心より感謝申し上げます。特に今回は、定理 3.1 の証明の不備を御指摘いただいたうえに解決の方向性まで御提示下さった編集委員長に対し、感謝の念で一杯です。改めて、心より御礼申し上げます。

#### 参考文献

- [1] H. Goldstine, The Computer from Pascal to von Neumann, Princeton University Press, 1972. (末包良太, 米口肇, 犬伏茂之訳, 『復刊 計算機の歴史—パスカルからノイマンまで—』, 共立出版, 2016.)
- [2] S. McCartney, The Triumphs and Tragedies of the World's First Computer, Walker, 1999. (日暮雅通訳, 『エニアック—世界最初のコンピュータ開発秘話—』, パーソナルメディア, 2001.)
- [3] 坂村健, 『痛快! コンピュータ学』, 集英社, 1999 (文庫版 2002).

- [4] 竹内伸, 『実物でたどるコンピュータの歴史—石ころからリングへ—』, 東京理科大学出版センター(編), 東京書籍, 2012.
- [5] 小田徹, 『コンピュータ開発のはてしない物語—起源から驚きの近未来まで—』, 技術評論社, 2016.
- [6] Wikipedia, Francois Viète, [https://en.wikipedia.org/wiki/Francois\\_Viète](https://en.wikipedia.org/wiki/Francois_Viète) (2021年12月14日閲覧)
- [7] E. T. Bell, *Men of Mathematics Volume 1*, Simon & Schuster, 1937. (田中勇・銀林浩訳, 『数学をつくった人びと上』, 東京図書, 1976.)
- [8] Wikipedia, René Descartes, [https://en.wikipedia.org/wiki/René\\_Descartes](https://en.wikipedia.org/wiki/René_Descartes) (2021年12月21日閲覧)
- [9] E. T. Bell, *Men of Mathematics Volume 2*, Simon & Schuster, 1937. (田中勇・銀林浩訳, 『数学をつくった人びと下』, 東京図書, 1976.)
- [10] Wikipedia, George Boole, [https://en.wikipedia.org/wiki/George\\_Boole](https://en.wikipedia.org/wiki/George_Boole) (2021年12月14日閲覧)
- [11] P. J. Nahin, *The Logician and the Engineer: How George Boole and Claude Shannon Created the Information Age*, Princeton University Press, 2012. (松浦俊輔訳, 『0と1の話—ブール代数とシャノン理論—』, 青土社, 2013.)
- [12] J. Soni and R. Goodman, *A Mind at Play: How Claude Shannon Invented the Information Age*, Simon & Schuster, 2017. (小坂恵理訳, 『クロード・シャノン—情報時代を発明した男—』, 筑摩書房, 2019.)
- [13] Wikipedia, Claude Shannon, [https://en.wikipedia.org/wiki/Claude\\_Shannon](https://en.wikipedia.org/wiki/Claude_Shannon) (2021年12月20日閲覧)
- [14] Wikipedia, Alan Turing, [https://en.wikipedia.org/wiki/Alan\\_Turing](https://en.wikipedia.org/wiki/Alan_Turing) (2021年12月20日閲覧)
- [15] B. J. Copeland, *Turing: Pioneer of the Information Age*, Oxford University Press, 2012. (服部桂訳, 『チューリング—情報時代のバイオニアー—』, NTT出版, 2013.)
- [16] A. Hodges, *Alan Turing: The Enigma*, Princeton University Press, 2014. (土屋俊・土屋希和子訳, 『エニグマ—アラン・チューリング伝—』, 勁草書房, 2015.)
- [17] 高岡詠子, 『チューリングの計算理論入門—チューリング・マシンからコンピュータへ—』, 講談社, 2014.
- [18] Wikipedia, Galileo Galilei, [https://en.wikipedia.org/wiki/Galileo\\_Galilei](https://en.wikipedia.org/wiki/Galileo_Galilei) (2021年12月21日閲覧)
- [19] Wikipedia, Nicolaus Copernicus, [https://en.wikipedia.org/wiki/Nicolaus\\_Copernicus](https://en.wikipedia.org/wiki/Nicolaus_Copernicus) (2021年12月21日閲覧)
- [20] Wikipedia, Marin Mersenne, [https://en.wikipedia.org/wiki/Marin\\_Mersenne](https://en.wikipedia.org/wiki/Marin_Mersenne) (2021年12月21日閲覧)
- [21] Wikipedia, Isaac Beeckman, [https://en.wikipedia.org/wiki/Isaac\\_Beeckman](https://en.wikipedia.org/wiki/Isaac_Beeckman) (2022年1月2日閲覧)
- [22] Wikipedia, Adrien Baillet, [https://en.wikipedia.org/wiki/Adrien\\_Baillet](https://en.wikipedia.org/wiki/Adrien_Baillet) (2022年1月2日閲覧)
- [23] Wikipedia, Elisabeth of the Palatinate, [https://en.wikipedia.org/wiki/Elisabeth\\_of\\_the\\_Palatinate](https://en.wikipedia.org/wiki/Elisabeth_of_the_Palatinate) (2022年1月2日閲覧)
- [24] Wikipedia, エリーザベト・フォン・デア・プファルツ (1618-1680), [https://ja.wikipedia.org/wiki/エリーザベト・フォン・デア・プファルツ\\_\(1618-1680\)](https://ja.wikipedia.org/wiki/エリーザベト・フォン・デア・プファルツ_(1618-1680)) (2022年1月2日閲覧)
- [25] 有賀暢迪, “合理力学の一例としての衝突理論 1720–1730年”, 科学哲学科学史研究, **6**, pp. 17–37, 2012.
- [26] Wikipedia, ソディの6球連鎖, <https://ja.wikipedia.org/wiki/ソディの6球連鎖> (2022年1月4日閲覧)
- [27] Wikipedia, Thordod Gosset, [https://en.wikipedia.org/wiki/Thorold\\_Gosset](https://en.wikipedia.org/wiki/Thorold_Gosset) (2022年1月4日閲覧)
- [28] 寒川町ガイド, <https://samukawaguide.blogspot.com/2019/12/6.html> (2022年1月4日閲覧)
- [29] Wikipedia, Gottfried Wilhelm Leibniz, [https://en.wikipedia.org/wiki/Gottfried\\_Wilhelm\\_Leibniz](https://en.wikipedia.org/wiki/Gottfried_Wilhelm_Leibniz) (2022年1月4日閲覧)
- [30] Wikipedia, Christina, Queen of Sweden, [https://en.wikipedia.org/wiki/Christina,\\_Queen\\_of\\_Sweden](https://en.wikipedia.org/wiki/Christina,_Queen_of_Sweden) (2022年1月4日閲覧)
- [31] Wikipedia, Isaac Newton, [https://en.wikipedia.org/wiki/Isaac\\_Newton](https://en.wikipedia.org/wiki/Isaac_Newton) (2022年1月4日閲覧)
- [32] 向井茂, “不変式の話,” 数学セミナー連載, 2005年12月号, 2006年1, 2, 4月号.
- [33] 日本医学会ホームページ, <https://jams.med.or.jp/news/013.html> (2022年2月4日閲覧)
- [34] Wikipedia, Vannevar Bush, [https://en.wikipedia.org/wiki/Vannevar\\_Bush](https://en.wikipedia.org/wiki/Vannevar_Bush) (2022年2月25日閲覧)
- [35] Britanica, William-Thomson-Baron-Kelvin, <https://www.britannica.com/biography/William-Thomson-Baron-Kelvin> (2022年3月6日閲覧)
- [36] Wikipedia, Hannibal Ford, [https://en.wikipedia.org/wiki/Hannibal\\_Ford](https://en.wikipedia.org/wiki/Hannibal_Ford) (2022年3月6日閲覧)
- [37] Wikipedia, Joseph Fourier, [https://en.wikipedia.org/wiki/Joseph\\_Fourier](https://en.wikipedia.org/wiki/Joseph_Fourier) (2022年3月6日閲覧)
- [38] Wikipedia, ユトランド沖海戦, <https://ja.wikipedia.org/wiki/ユトランド沖海戦> (2022年3月6日閲覧)
- [39] Wikipedia, Mark I Fire Control Computer, [https://en.wikipedia.org/wiki/Mark\\_I\\_Fire\\_Control\\_Computer](https://en.wikipedia.org/wiki/Mark_I_Fire_Control_Computer) (2022年3月7日閲覧)
- [40] Wikipedia, Bell Labs, [https://en.wikipedia.org/wiki/Bell\\_Labs](https://en.wikipedia.org/wiki/Bell_Labs) (2022年4月7日閲覧)
- [41] Wikipedia, Thornton Carle Fry, [https://en.wikipedia.org/wiki/Thornton\\_Carle\\_Fry](https://en.wikipedia.org/wiki/Thornton_Carle_Fry) (2022年4月7日閲覧)
- [42] Wikipedia, Schön scandal, [https://en.wikipedia.org/wiki/Schön\\_scandal](https://en.wikipedia.org/wiki/Schön_scandal) (2022年4月7日閲覧)
- [43] Wikipedia, ヘンドリック・シェーン, <https://ja.wikipedia.org/wiki/ヘンドリック・シェーン> (2022年4月7日閲覧)
- [44] Wikipedia, ジョン・フォン・ノイマン, <https://ja.wikipedia.org/wiki/ジョン・フォン・ノイマン> (2022年4月29日閲覧)
- [45] Wikipedia, ヘルマン・ワイル, <https://ja.wikipedia.org/wiki/ヘルマン・ワイル> (2022年4月29日閲覧)
- [46] Wikipedia, 第二次世界大戦, <https://ja.wikipedia.org/wiki/第二次世界大戦> (2022年5月31日閲覧)
- [47] Wikipedia, フランクリン・ルーズベルト, <https://ja.wikipedia.org/wiki/フランクリン・ルーズベルト> (2022年4月30日閲覧)
- [48] Wikipedia, ウォーレン・ウィーバー, <https://ja.wikipedia.org/wiki/ウォーレン・ウィーバー> (2022年5月3日閲覧)
- [49] Wikipedia, ジェイムス・コナント, <https://ja.wikipedia.org/wiki/ジェイムス・コナント> (2022年5月3日閲覧)
- [50] Wikipedia, ロバート・オッペンハイマー, <https://ja.wikipedia.org/wiki/ロバート・オッペンハイマー> (2022年5月3日閲覧)
- [51] Wikipedia, Homer Dudley, [https://en.wikipedia.org/wiki/Homer\\_Dudley](https://en.wikipedia.org/wiki/Homer_Dudley) (2022年4月7日閲覧)
- [52] Wikipedia, SIGSALY, <https://ja.wikipedia.org/wiki/SIGSALY> (2022年5月31日閲覧)
- [53] Wikipedia, ワンタイムパッド, <https://ja.wikipedia.org/wiki/ワンタイムパッド> (2022年5月3日閲覧)
- [54] 釜賀一夫, 藤原邦樹, 吉村昭, “座談会日本陸軍暗号はなぜ破られなかったか,” 歴史と人物—太平洋戦争シリーズ—, 昭和60年冬号, 1985.
- [55] Wikipedia, Harry Nyquist, [https://en.wikipedia.org/wiki/Harry\\_Nyquist](https://en.wikipedia.org/wiki/Harry_Nyquist)

- org/wiki/Harry\_Nyquist (2022年5月7日閲覧)
- [56] Wikipedia, Ralph Hartley, [https://en.wikipedia.org/wiki/Ralph\\_Hartley](https://en.wikipedia.org/wiki/Ralph_Hartley) (2022年5月7日閲覧)
- [57] Wikipedia, ニコラ・レオナルド・サディ・カルノー, <https://ja.wikipedia.org/wiki/ニコラ・レオナルド・サディ・カルノー> (2022年6月6日閲覧)
- [58] Wikipedia, ジェームズ・プレスコット・ジュール, <https://ja.wikipedia.org/wiki/ジェームズ・プレスコット・ジュール> (2022年6月6日閲覧)
- [59] Wikipedia, ユリウス・ロベルト・フォン・マイヤー, <https://ja.wikipedia.org/wiki/ユリウス・ロベルト・フォン・マイヤー> (2022年6月6日閲覧)
- [60] Wikipedia, ヘルマン・フォン・ヘルムホルツ, <https://ja.wikipedia.org/wiki/ヘルマン・フォン・ヘルムホルツ> (2022年6月6日閲覧)
- [61] Wikipedia, ルドルフ・クラウジウス, <https://ja.wikipedia.org/wiki/ルドルフ・クラウジウス> (2022年6月6日閲覧)
- [62] Wikipedia, ジェームズ・クラーク・マクスウェル, <https://ja.wikipedia.org/wiki/ジェームズ・クラーク・マクスウェル> (2022年6月6日閲覧)
- [63] Wikipedia, ルートヴィッヒ・ボルツマン, <https://ja.wikipedia.org/wiki/ルートヴィッヒ・ボルツマン> (2022年6月6日閲覧)
- [64] Wikipedia, エントロピー, <https://ja.wikipedia.org/wiki/エントロピー> (2022年6月6日閲覧)
- [65] Wikipedia, カルノーの定理\_(熱力学), [https://ja.wikipedia.org/wiki/カルノーの定理\\_\(熱力学\)](https://ja.wikipedia.org/wiki/カルノーの定理_(熱力学)) (2022年6月7日閲覧)
- [66] Wikipedia, ウィラード・ギブズ, <https://ja.wikipedia.org/wiki/ウィラード・ギブズ> (2022年6月7日閲覧)
- [67] 植松友彦, 『イラストで学ぶ情報理論の考え方』, 講談社, 2012.
- [68] Wikipedia, アルフレッド・ヴェイル, <https://ja.wikipedia.org/wiki/アルフレッド・ヴェイル> (2022年6月7日閲覧)
- [69] Wikipedia, Robert Fano, [https://en.wikipedia.org/wiki/Robert\\_Fano](https://en.wikipedia.org/wiki/Robert_Fano) (2022年8月4日閲覧)
- [70] Wikipedia, Shannon-Fano coding, [https://en.wikipedia.org/wiki/Shannon-Fano\\_coding](https://en.wikipedia.org/wiki/Shannon-Fano_coding) (2022年8月4日閲覧)
- [71] Wikipedia, David A. Huffman, [https://en.wikipedia.org/wiki/David\\_A.\\_Huffman](https://en.wikipedia.org/wiki/David_A._Huffman) (2022年8月4日閲覧)
- [72] Wikipedia, Abraham Lempel, [https://en.wikipedia.org/wiki/Abraham\\_Lempel](https://en.wikipedia.org/wiki/Abraham_Lempel) (2022年8月4日閲覧)
- [73] Wikipedia, Jacob Ziv, [https://en.wikipedia.org/wiki/Jacob\\_Ziv](https://en.wikipedia.org/wiki/Jacob_Ziv) (2022年8月4日閲覧)
- [74] J. Ziv and A. Lempel, "A Universal Algorithm for Sequential Data Compression," *IEEE Transactions on Information Theory*, **23**, pp 337–343, 1977.
- [75] J. Ziv and A. Lempel, "Compression of Individual Sequences via Variable-Rate Coding," *IEEE Transactions on Information Theory*, **24**, pp 530–536, 1978.
- [76] 正嶋宏一, 高木重定, 折口壮志, 鶴田祥一郎, 鈴木徹也, "モノからコトへ—新たなる循環経済の形成—," 日本LCA学会誌, **14**, pp. 173–177, 2018.