連載

世界をORする視線 (22)
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9）

住田　潮

（註：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）

1.　シャノンの第二基本定理の本質

シャノンが第二基本定理（通信路符号化定理）を示す以前は，誤通信受諾確率 E_ε を小さくするためには，伝送速度を小さくする必要があると考えられていた．たとえば，2 元対象通信路を通して 0 か 1 の送信を行うとき，同じ信号を奇数回送信し，受信側は送信された記号を多数決で判定することを考える．1 回だけ送信すれば $E_{\varepsilon:1}=\varepsilon$ である．3 回送って多数決で送信された信号を判定するとすれば，$E_{\varepsilon:3}$ は 2 回以上誤送信する確率で与えられるので，$E_{\varepsilon:3}=\varepsilon^3+3\varepsilon^2(1-\varepsilon)=\varepsilon^2(3-2\varepsilon)$ となる．この曲線は単調増加であり，$\varepsilon=0$ で $E_{0:3}=0$，$\varepsilon=1$ で $E_{1:3}=1$，$E_{(1/2):3}=1/2$ で変曲点をもつ．さらに，$0<\varepsilon<1/2$ で凸関数となって $E_{\varepsilon:3}<\varepsilon$ が成立し，$1/2<\varepsilon<1$ では凹関数となり $\varepsilon<E_{\varepsilon:3}$ が成立する．$1/2<\varepsilon$ の場合は 0 と 1 を反転させればよいので，結局，$E_{\varepsilon:3}<E_{\varepsilon:1}$ となることがわかる．一般的には，$n=1,2,\cdots$ に対して $2n-1$ 回送信し，結果を多数決で判定することにすれば，$E_{\varepsilon:2n-1}$ は n を大きくすることで任意に小さくできる．しかし，当然，一つの記号の送信に要する時間は増加し，その逆数としての単位時間当りに伝送できる記号の数 $1/(2n-1)$ も減少し，伝送速度は小さくなる．

シャノンが示したのは，復号誤り率とトレードオフの関係にあるのは，それまで常識とされてきた「単位時間当たりに伝送できる記号の数」ではなく，「符号化とその解読に要する計算量」であることであった．すなわち，伝送速度が，通信路に固有の量である通信路容量の範囲内にあれば，前回，Parity Bit の例で見たように，符号化における符号長を長くして複雑化することにより，伝送速度を小さくすることなく復号誤り率をいくらでも小さくできることを示したのである．本稿では引き続き，基本的に文献 [67] に沿って，この第二基本定理を解説する．定理を構造的に理解するため，まず，基本モデルを構成するいくつかの定義を与える．

2.　通信路と通信路容量

送信側における情報源の符号化は，入力記号集合 A の元 $x\in A$ に対し，何らかの仕組みで有限な 0-1 の列を割り当てることに相当する．結果として得られる符号を $C(x)$，その長さを $l_C(x)=|C(x)|$ と表わした．A 上の確率変数 X とその確率分布 P_X が与えられたとき，符号化の目指すのは，復元可能な符号の集合である語頭符号の集合 $HC(A)$ の範囲で，平均符号長　$L_C(X)=\sum_{x\in A}P_X(x)l_C(x)$ を最小にする符号を見出すことにあった．

これに対し，受信側の観点からは，上述の手続きで得られる符号に必要なビットを追加することにより，通信路で生じる誤送信の影響を軽減し，送受信者の間で生じる齟齬を小さくするという意味で，信頼度の高い通信を実現することが重要になる．前号で，送信符号に誤送信を回復させるための符号を冗長的に付加することにより，復号誤り率を減少させることができることを，Parity Bit，Block Parity Bits，ハミング符号などの具体例によって示した．より一般的な枠組でこの問題を数学モデルとして定式化するためには，ま

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

ず，通信路を正確に定義することが必要となる．

入力記号の集合 A 上の離散確率変数を X，その確率分布の集合を $\mathcal{D}(A)$ で表わし，その要素を $P_X \in \mathcal{D}(A)$ と書くことにする．すなわち，$x \in A$ に対し，$P_X(x) = P[X = x]$ である．同様に，出力記号集合 B 上の離散確率変数を Y，その確率分布の集合を $\mathcal{D}(B)$ で表わし，その要素を $P_Y \in \mathcal{D}(B)$ と書く．このとき，通信路の数学的特性は「$P_X \in \mathcal{D}(A)$ が与えられたとき，$P_Y \in \mathcal{D}(B)$ を決定する仕組み」によって定まると解釈できる．この仕組みが，過去の入力列に依存せず，そのときの入力 $x \in A$ のみに依存して定まるとき，この通信路をマルコフ（無記憶）通信路と呼ぶ．本稿では特に断らない限り，マルコフ通信路のみを対称とする．

通信路がマルコフ性を満たすとき，「$P_X \in \mathcal{D}(A)$ が与えられたとき，$P_Y \in \mathcal{D}(B)$ を決定する仕組み」は，条件付き確率

$$P_{Y|X}(y|x) = P[Y = y|X = x] \tag{2.1}$$

によって表わされる．すなわち，$(x, y) \in A \times B$ に対して $P_X(x)$ と $P_{Y|X}(y|x)$ が与えられると，X と Y の同時確率 $P_{XY}(x, y) = P[X = x, Y = y]$ が

$$P_{XY}(x, y) = P_{Y|X}(y|x) P_X(x) \tag{2.2}$$

によって定まり，

$$P_Y(y) = \sum_{x \in A} P_{XY}(x, y) \tag{2.3}$$

が求まることになる．以上より，通信路を次のように定義する．

定義 2.1　通信路

入力記号集合 A 上の離散確率変数 X とその確率分布 $P_X \in \mathcal{D}(A)$ が与えられたとする．$x \in A$ に対し，ある送信路を通して送信することで得られる出力記号 $y \in B$ が条件付き確率 $P_{Y|X}(y|x)$ で定まるとき，この送信路を離散的通信路と呼ぶ．x を行，y を列 とする $|A| \times |B|$ のマルコフ行列 $\boldsymbol{P}_{Y|X} = [P_{Y|X}(y|x)]$ を通信路行列と呼ぶ．

前号で議論した，二つの基本的な通信路の例を思いだそう．図 1 に示す通信路は，$A_1 = B_1 = \{0, 1\}$ に対し，0，1 いずれを送信しても確率 ε $(0 < \varepsilon < 1)$ で誤送信が発生する 2 元対称通信路である．誤送信された結果を誤って正しいものとして受諾してしまう確率

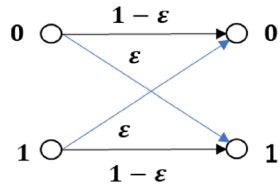

図 1　$A_1 = B_1 = \{0, 1\}$

表 1　図 1 の例に対する $\boldsymbol{P}_{Y|X}$

	0	1
0	$1-\varepsilon$	ε
1	ε	$1-\varepsilon$

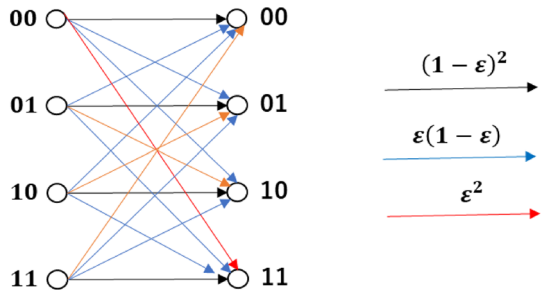

図 2　$A_2 = B_2 = \{00, 01, 10, 11\}$

表 2　図 2 の例に対する $\boldsymbol{P}_{Y|X}$

	00	01	10	11
00	$(1-\varepsilon)^2$	$\varepsilon(1-\varepsilon)$	$\varepsilon(1-\varepsilon)$	ε^2
01	$\varepsilon(1-\varepsilon)$	$(1-\varepsilon)^2$	ε^2	$\varepsilon(1-\varepsilon)$
10	$\varepsilon(1-\varepsilon)$	ε^2	$(1-\varepsilon)^2$	$\varepsilon(1-\varepsilon)$
11	ε^2	$\varepsilon(1-\varepsilon)$	$\varepsilon(1-\varepsilon)$	$(1-\varepsilon)^2$

は $E_{\varepsilon:1} = \varepsilon$ で与えられる．2 元対称通信路の通信路行列を，表 1 に示しておく．

さらに，2 元対称通信路を用いて，$A_2 = \{00, 01, 10, 11\}$，$B_2 = \{00, 01, 10, 11\}$ として送信を行う場合を考える．図 2 に示すように，送信された符号が正しく復元される確率は $(1-\varepsilon)^2$ となり，誤送信受諾率は $E_\varepsilon = 1 - (1-\varepsilon)^2 = \varepsilon(2-\varepsilon)$ で与えられる．この例に対する通信路行列は，表 2 のようになる．

連載第 19 回で，二つの確率分布 $P(x)$ と $Q(x)$ が与えられたとき，相対エントロピー

$$H(P||Q) = \sum_{x \in \Omega} P(x) \log_2 \frac{P(x)}{Q(x)} \tag{2.4}$$

が，「$P(x)$ を $Q(x)$ と誤判断して符号化を行った際，その平均符号語長は本来のそれからどれだけ乖離するか」を測る指標と解釈できることを示した．さらに，こ

の考え方を，$\Omega_1 \times \Omega_2$ 上で定義される二つの離散確率変数 X と Y の独立性を測る目的に適用し，相互情報量 $I(X;Y)$ を

$$I(X;Y) = H(P_{XY}||P_X P_Y)$$
$$= \sum_{x\in\Omega_1}\sum_{y\in\Omega_2} P_{XY}(x,y)\log_2\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)} \quad (2.5)$$

と定義し，さらに

$$I(X;Y) = H(Y) - H(Y|X) \quad (2.6)$$

が成立することを証明した．ここで，$H(Y)$ は Y のエントロピー，$H(Y|X)$ は X に対する Y の条件付きエントロピーを表わし，それぞれ，

$$H(Y) = -\sum_{y\in\Omega_2} P_Y(y)\log_2 P_Y(y) \quad (2.7)$$

$$H(Y|X) = -\sum_{x\in\Omega_1}\sum_{y\in\Omega_2} P_{XY}(x,y)\log_2 P_{Y|X}(y|x) \quad (2.8)$$

によって与えられることを思い出しておこう．

条件付き確率 $P_{Y|X}(y|x)$ をもつ通信路の通信路容量 C_0 は，この相互情報量 $I(X;Y)$ の $P_X \in \mathcal{D}(A)$ 上での最大値として，次のように定義される．

定義 2.2　通信路容量

入力記号集合を A，出力記号集合を B とする．$|A|\times|B|$ の通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ をもつ通信路に対し，

$$C_0 = \max_{P_X\in\mathcal{D}(A)}\left[I(X;Y)\right] \quad (2.9)$$

を，この通信路の通信路容量と呼ぶ．

送信符号に誤送信を回復させるための符号を付加することにより，復号誤り率をいくらでも減少させることができるという条件の下で，通信路容量は「通信路を 1 回使うたびに送信できる最大ビット数」という操作的な意味をもっている．

図 1 の 2 元対称通信路について，通信路容量を求めてみよう．

定理 2.3　2 元対称通信路の通信路容量

2 元対称通信路を考え，

$$h(\varepsilon) = -\{(1-\varepsilon)\log_2(1-\varepsilon) + \varepsilon\log_2\varepsilon\} \quad (2.10)$$

とおくと，その通信容量は

$$C_0 = 1 - h(\varepsilon)$$

で与えられる．

[証明]

式 (2.8) より，

$$H(Y|X) = -\sum_{x=0}^{1}\sum_{y=0}^{1} P_{XY}(x,y)\log_2 P_{Y|X}(y|x)$$
$$= -\sum_{x=0}^{1}\sum_{y=0}^{1} P_{Y|X}(y|x)P_X(x)\log_2 P_{Y|X}(y|x)$$
$$= -\sum_{x=0}^{1} P_X(x)\sum_{y=0}^{1} P_{Y|X}(y|x)\log_2 P_{Y|X}(y|x)$$
$$= -P_X(0)\{(1-\varepsilon)\log_2(1-\varepsilon) + \varepsilon\log_2\varepsilon\}$$
$$\quad -P_X(1)\{\varepsilon\log_2\varepsilon + (1-\varepsilon)\log_2(1-\varepsilon)\}$$

を得る．したがって，$H(Y|X) = \{P_X(0)+P_X(1)\}h(\varepsilon) = h(\varepsilon)$ が成立し，式 (2.6) より，

$$I(X;Y) = H(Y) - h(\varepsilon) \quad (2.11)$$

が結論される．

式 (2.10) より，明らかに $h(\varepsilon)$ は二つの元から成る集合上で定義される確率変数のエントロピーであり，連載第 18 回の図 3 に示したように，狭義の凹関数で $\varepsilon = 1/2$ で最大値 1 を取る．Y は $B_1 = \{0,1\}$ 上の確率変数であり，$P_Y(0) = \alpha, P_Y(1) = 1-\alpha, 0 \le \alpha \le 1$ とおくと，式 (2.7) から，$H(Y) = h(\alpha) \le 1$ となる．したがって，式 (2.11) より，$I(X;Y) \le 1 - h(\varepsilon)$ が成立し，

$$C_0 = \max_{P_X\in\mathcal{D}(A)}\left[I(X;Y)\right] \le 1 - h(\varepsilon) \quad (2.12)$$

となることがわかる．

一方，X が $P_X(0) = P_X(1) = 1/2$ という一様分布に従う場合，式 (2.2)，(2.3) より，

$$P_Y(1) = P_{Y|X}(1|0)P_X(0) + P_{Y|X}(1|1)P_X(1)$$
$$= \frac{1}{2}\varepsilon + \frac{1}{2}(1-\varepsilon) = \frac{1}{2}$$

が求まる．これより，$P_Y(0) = 1 - P_Y(1) = 1/2$ となり，Y も一様分布に従うので，この Y に対して $H(Y) = h(1/2) = 1$ が成立する．このとき，式 (2.11) から，

$$C_0 = \max_{P_X\in\mathcal{D}(A)}\left[H(Y)\right] - h(\varepsilon) \ge 1 - h(\varepsilon) \quad (2.13)$$

となり，不等式 (2.12) と (2.13) から，

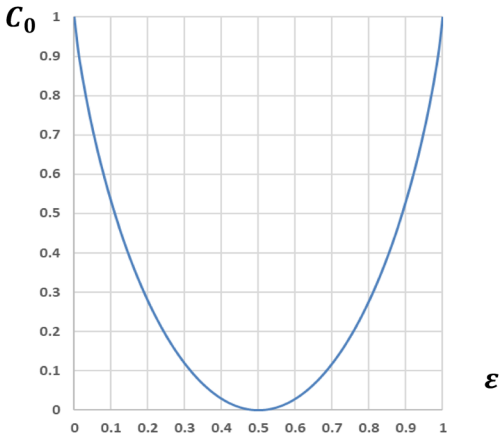

図 3　2 元対称通信路の通信路容量

$$C_0 = 1 - h(\varepsilon)$$

が結論される．□

図 3 に，2 元対称通信路の通信路容量 C_0 をグラフで示す．誤通信の確率 ε が 1/2 の場合は，送信の正誤が完全にランダムになり，通信路容量は 0 である．ε が 1/2 の値を取るまでは C_0 は単調に減少する．ε が 1/2 を超えると再び上昇するが，これは受信符号集合 $B_1 = \{0, 1\}$ が二つの値のみを含むため，ε が 1/2 の値を超えた場合は，0 と 1 を反転させることによって，正誤の判断を得ることができるからで，C_0 のグラフが $\varepsilon = 1/2$ の縦軸を中心に，線対称となっている所以である．

3.　対称通信路の通信路容量

通信路は，入力記号 $x \in A$ が与えられたときに出力記号 $y \in B$ を定める仕組みによって特徴付けられ，数学的には，入力記号の確率分布 $P_X \in \mathcal{D}(A)$ と通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ によって記述されることを見てきた．このとき，通信路容量 C_0 を，$P_X \in \mathcal{D}(A)$ を変化させたときの相互情報量 $I(X;Y)$ の最大値として定義した．したがって，通信路容量を求める問題は多変数最適化問題として定式化され，一般的にはこれを解くことは容易ではない．本節では，この最大化問題を簡単に解くことができるばかりでなく，応用上も重要である対称通信路を論じる．

いま，$i, j \in \{1, 2, \ldots, N\}$ に対して，

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

と定義したとき，行列 $\boldsymbol{I}_N = [\delta_{ij}]$ は単位行列と呼ばれる $N \times N$ 行列で，行列の積に関して単位元となる．すなわち，任意のベクトル $\boldsymbol{x} \in \mathbb{R}^N$ に対して，$\boldsymbol{I}_N \boldsymbol{x} = \boldsymbol{x}, \boldsymbol{x}^{\boldsymbol{T}} \boldsymbol{I}_N = \boldsymbol{x}^{\boldsymbol{T}}$ が成立する．ここで，単位行列の行あるいは列を並べ替えて得られる行列の集合

$$\mathcal{W}_N = \left\{ \boldsymbol{W}_N = [w_{ij}] : \sum_{i=1}^{N} w_{ij} = 1, \sum_{j=1}^{N} w_{ij} = 1, w_{ij} = 0 \ or \ 1 \right\}$$

を考える．このとき，$\boldsymbol{I}_N$ の行ベクトルを並べ替えて $\boldsymbol{W}_N \in \mathcal{W}_N$ が得られたとすると，$\boldsymbol{W}_N \boldsymbol{x}$ は同じ順番で $\boldsymbol{x}$ を並べ替えた列ベクトルとなる．この行列 $\boldsymbol{W}_N \in \mathcal{W}_N$ は $\boldsymbol{I}_N$ の列ベクトルを並べ替えても得られるが，このとき，$\boldsymbol{x}^{\boldsymbol{T}} \boldsymbol{W}_N$ はその順番で $\boldsymbol{x}$ を並べ替えた行ベクトルとなる．以下の例では，$\boldsymbol{W}_3$ は $\boldsymbol{I}_3$ の行ベクトルを $[3, 1, 2]$，列ベクトルを $[2, 3, 1]$ の順番で並べ替えることにより得られる．

$$\boldsymbol{W}_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

これに対し，ベクトル $[a\ b\ c]^{\boldsymbol{T}}$ の積を施すと，行ベクトルと列ベクトルの入れ替え順が，それぞれ，

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} c \\ a \\ b \end{bmatrix};$$

$$[a\ b\ c] \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = [b\ c\ a]$$

のように移されることがわかる．

定義 3.1　対称通信路

入力記号集合 A，出力記号集合 B，$|A| \times |B|$ の通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ をもつ通信路を考え，$\boldsymbol{P}_{Y|X}$ の第 i 行を $\boldsymbol{P}_{Y|X:i\cdot}$，第 j 列を $\boldsymbol{P}_{Y|X:\cdot j}$ と書くことにする．

(a) 任意の $i \in \{1, 2, \cdots, |A|\}$ に対して $\boldsymbol{W}_{|B|:i} \in \mathcal{W}_{|B|}$ が存在して，$\boldsymbol{P}_{Y|X:1\cdot} \boldsymbol{W}_{|B|:i} = \boldsymbol{P}_{Y|X:i\cdot}$ が

成立するとき，この通信路を入力対称通信路と呼ぶ．

(b) 任意の $j \in \{1,2,\cdots,|B|\}$ に対して $\boldsymbol{W}_{|B|:j} \in \mathcal{W}_{|B|}$ が存在して，$\boldsymbol{W}_{|B|:j}\boldsymbol{P}_{Y|X:1} = \boldsymbol{P}_{Y|X:j}$ が成立するとき，この通信路を出力対称通信路と呼ぶ．

(c) 通信路が入力対称通信路であり，かつ出力対称通信路でもあるとき，この通信路を狭義の対称通信路と呼ぶ．

通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ の各行が最初の行の並べ替えとなっているのが入力対称通信路であり，各列が最初の列の並べ替えとなっていれば出力対称通信路，それらが同時に成立しているのが狭義の対称通信路である．

入力対称通信路の例：$\boldsymbol{P}_{Y|X} = \begin{bmatrix} a & b & c \\ c & b & a \end{bmatrix}$

出力対称通信路の例：$\boldsymbol{P}_{Y|X} = \begin{bmatrix} a & b \\ b & c \\ c & a \end{bmatrix}$

狭義の対称通信路の例：$\boldsymbol{P}_{Y|X} = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$

図 2 の例は，表 2 からわかるように，狭義の対称通信路となっている．

通信路の対称性が，通信路容量 C_0 の計算を容易にすることを示そう．まず，一つの補題を証明する．

補題 3.2

入力記号集合 A，出力記号集合 B，通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ をもつ通信路が入力対称通信路であるとき，$H(Y|X=x)$ は $x \in A$ に対して同じ値を取る．すなわち，A の最初の記号を x_1 とすると，すべての $x_i \in A$ に対して，ある関数 g が存在して，

$$H(Y|X=x_i) = g(x_1) \tag{3.1}$$

が成立する．

[証明]

$\hat{\boldsymbol{P}}_{Y|X} = \left[-P_{Y|X}(y|x)\log_2 P_{Y|X}(y|x)\right]$ とおき，その第 i 行と第 j 列をそれぞれ $\hat{\boldsymbol{P}}_{Y|X:i\cdot}$,$\hat{\boldsymbol{P}}_{Y|X:\cdot j}$ と書くことにする．定義 3.1(a) から，明らかにすべての $x_i \in A$ に対して，$\hat{\boldsymbol{P}}_{Y|X:1\cdot}\boldsymbol{W}_{|B|:i} = \hat{\boldsymbol{P}}_{Y|X:i\cdot}$ が成立する．ここで，$\mathbf{1}^{\boldsymbol{T}} = [1\ 1\ \ldots\ 1], g(x_1) = \hat{\boldsymbol{P}}_{Y|X:1\cdot}\mathbf{1}$ とおくと，$\boldsymbol{W}_{|B|:i}\mathbf{1} = \mathbf{1}$ に注意して，

$$H(Y|X=x_i) = -\sum_{y\in B} P_{Y|X}(y|x_i)\log_2 P_{Y|X}(y|x_i)$$
$$= \hat{\boldsymbol{P}}_{Y|X:i\cdot}\mathbf{1} = \hat{\boldsymbol{P}}_{Y|X:1\cdot}\boldsymbol{W}_{|B|:i}\mathbf{1} = \hat{\boldsymbol{P}}_{Y|X:1\cdot}\mathbf{1} = g(x_1)$$

となり，補題が証明された．□

定理 3.3

入力記号集合 A，出力記号集合 B，通信路行列 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ をもつ通信路を考える．

(a) この通信路が入力対称通信路のとき，補題 3.2 の $g(x_1)$ と通信路容量 C_0 に対し，

$$C_0 = \max_{P_X\in\mathcal{D}(A)}[H(Y)] - g(x_1) \tag{3.2}$$

が成立する．

(b) さらに，狭義の対称通信路である場合は，

$$C_0 = \log_2|B| - g(x_1) \tag{3.3}$$

が成立する．

[証明]

補題 3.2 より，

$$H(Y|X) = -\sum_{x\in A} P_X(x)\,H(Y|X=x)$$
$$= g(x_1)\sum_{x\in A} P_X(x) = g(x_1)$$

となることがわかる．式 (2.6) より，$I(X;Y) = H(Y) - H(Y|X) = H(Y) - g(x_1)$ が成立し，定義 2.2 から 定義 3.3(a) が証明される．

$H(Y)$ は Y のエントロピーであり，連載第 18 回定理 5.1 より，$\max_{P_Y\in\mathcal{D}(B)}[H(Y)] = \log_2|B|$ となり，その最大値は Y が一様分布の場合に達成される．ここで，X が一様分布に従うとすると，

$$P_Y(y_j) = \sum_{i=1}^{|A|} P_{Y|X}(y_j|x_i)\,P_X(x_i)$$
$$= \frac{1}{|A|}\sum_{i=1}^{|A|} P_{Y|X}(y_j|x_i)$$

が成立する．通信路が狭義の対称通信路であれば，出力対称通信路でもあるので，$\mathbf{1}^{\boldsymbol{T}}\boldsymbol{W}_{|B|:j} = \mathbf{1}^{\boldsymbol{T}}$ に注意すると

$$\sum_{i=1}^{|A|} P_{Y|X}(y_j|x_i) = \mathbf{1}^{\boldsymbol{T}}\boldsymbol{P}_{Y|X:j} = \mathbf{1}^{\boldsymbol{T}}\boldsymbol{W}_{|B|:j}\boldsymbol{P}_{Y|X:1}$$
$$= \mathbf{1}^{\boldsymbol{T}}\boldsymbol{P}_{Y|X:1}$$

となり，$\sum_{i=1}^{|A|} P_{Y|X}(y_j|x_i)$ は j に依存しない一定値を取り，Y もまた一様分布となる．したがって，$\max_{P_X \in \mathcal{D}(A)} [H(Y)] = \log|B|$ となり，(b) が成立する．□

図 2 に示された例の通信路容量を，表 2 に与えられた通信路行列から求めてみる．

定理 3.4

図 2 に示された例の通信路容量は，

$$C_0 = 2\{1 - h(\varepsilon)\}$$

によって与えられる．

[証明]

表 2 に与えられた通信路行列より，

$$\begin{aligned} H(Y|X = x_i) &= -\sum_{y \in B} P_{Y|X}(y|x_i) \log_2 P_{Y|X}(y|x_i) \\ &= -\sum_{y \in B} P_{Y|X}(y|00) \log_2 P_{Y|X}(y|00) \\ &= -\left\{(1-\varepsilon)^2 \log_2 (1-\varepsilon)^2 \right. \\ &\quad \left. + 2\varepsilon(1-\varepsilon) \log_2 \varepsilon(1-\varepsilon) + \varepsilon^2 \log_2 \varepsilon^2 \right\} \end{aligned}$$

となる．これを整理し，式 (2.10) で与えられた $h(\varepsilon)$ を用いると，

$$H(Y|X = x_i) = g(x_1) = 2h(\varepsilon)$$

となることがわかる．これと定理 3.3 (b) より，

$$\begin{aligned} C_0 &= \log_2 |B| - g(x_1) \\ &= \log_2 4 - 2h(\varepsilon) = 2\{1 - h(\varepsilon)\} \end{aligned}$$

を得る．□

定理 2.3 より，2 元対称通信路の場合に比べて，通信路容量が 2 倍になっていることがわかる．

4. 通信路符号と第二基本定理

通信路符号化の目的は，送信符号に誤送信を回復させるための符号を冗長的に付加することにより，復号誤り率を減少させることにある．

定義 4.1　通信路符号と伝送速度

(a) 入力記号集合 A の要素から構成される長さ n の系列の集合 A^n の部分集合 $C_{L:n} \subset A^n$ を通信路符号と呼ぶ．このとき，n を符号長，$x \in C_{L:n}$ を符号語，$|C_{L:n}|$ を符号数と呼ぶ．

(b) 符号長 n の通信路符号 $C_{L:n}$ の伝送速度 $R_{L:n}$ を

$$R_{L:n} = \frac{1}{n} \log_2 |C_{L:n}|$$

と定義する．

$C_{L:n}$ 上で定義される離散的確率変数の集合を $\mathcal{D}_{L:n}$，$X \in \mathcal{D}_{L:n}$ の確率分布を P_X，そのエントロピーを $H(X)$ とすると，連載第 18 回定理 5.1 より，

$$\max_{P_X \in \mathcal{D}_{L:n}} [H(X)] = \log_2 |C_{L:n}|$$

が成立し，その最大値は P_X が一様分布の場合，すなわち，すべての $x \in C_{L:n}$ に対して $P_X(x) = 1/|C_{L:n}|$ が成立するときに実現される．このことから，伝送速度 $R_{L:n}$は，誤通信が全く発生せず，P_X が一様分布のとき，通信路に一つの通信路符号を送ったときに伝送できるエントロピーの平均を表わしている．もちろん，この値は，誤通信が発生する可能性があり，P_X が任意の離散的確率分布である場合の上界となっている．

通信路容量 C_0 は，送信側の確率変数と受信側の確率変数の間の相対エントロピーの最大値であり，両者間の条件付き確率分布で表わされる通信路の特性のみによって決定される．一方，伝送速度 $R_{L:n}$ は，通信線の特性とは無関係に，通信路符号化のメカニズムによってのみ定まる量である．通信路符号化が通信線の容量の範囲で設計されなければならないという意味で，

$$R_{L:n} < C_0 \tag{4.1}$$

という制約を満たすことが要請される．

入力記号集合を A，出力記号集合を B，符号長を n とすると，A の要素から構成される長さ n の系列の集合 A^n に対し，B^n を受信空間と呼ぶ．部分集合 $C_{L:n} \subset A^n$ は通信路符号化された後に送信される入力信号の集合を意味し，その送信結果は B^n に属することになる．

通信路符号化の概念図を図 4 に示す．$C_{L:n}$ から B^n への写像 $\boldsymbol{P}_{Y|X} = \left[P_{Y|X}(y|x)\right]$ は送信線の特性によってのみ定まり，通信路符号化とは関係しない．A^n の中から，$C_{L:n} = \{w_1, w_2, \ldots, w_M\}$ を選び出す作業が通信路符号化に対応する．シャノンが構想した通信路符号化は，冗長性を表現する n を十分に大きく取れば，可能な限り $P_{Y|X}(D_i|w_i)$ を大きく取りつつ，

$$\bigcap_{i=1}^{M} \mathcal{D}_i = \phi \tag{4.2}$$

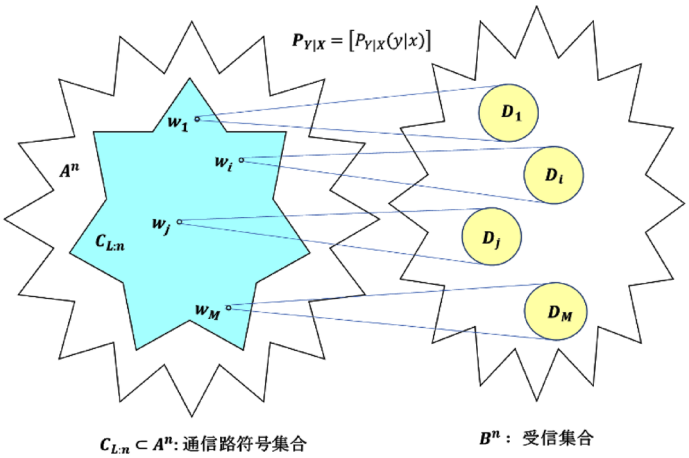

図 4　通信路符号化の概念図

を満たすように $\{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_M\}$ を構成する，$C_{L:n} = \{w_1, w_2, \ldots, w_M\}$ が決定できるというものであった．この方式によって誤通信を検出・訂正する仕組みは，以下のようにまとめられる．

① 符号語 $w_i \in C_{L:n} \subset A^n, i = 1, \ldots, M$ を送信したとき，送信結果 $\boldsymbol{y}_i \in B^n$ が複合領域 $\mathcal{D}_i \subset B^n$ に帰属すれば，$y_i \neq w_i$ であったとしても送信された通信路符号は w_i であると判断する．

② $\boldsymbol{y_i} \notin \mathcal{D}_i$ の場合には，誤通信が発生したと判断する．

シャノンの構想を実現するためには，

(a) 可能な限り $P_{Y|X}(D_i|w_i)$ を大きく取りつつ，$\cap_{i=1}^{M} \mathcal{D}_i = \phi$ を満たすように $\{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_M\}$ を構成できる $C_{L:n} = \{w_1, w_2, \ldots, w_M\}$ の決定方式を確立すること

(b) $\boldsymbol{w_i} \in C_{L:n}$ の受信結果 $\boldsymbol{y}_i \in B^n$ に対し，$\boldsymbol{y_i} \in \mathcal{D}_i$ が成立するか否かを判定するアルゴリズムを確立すること

が必要である．前号で紹介した，t 個の通信誤差を検出・訂正できる一般化されたハフマン法は，これを解決する一例となっている．

以上を，もう少し数式を用いて表現してみよう．入力記号集合 A，出力記号集合 B に対し，$C_{L:n} \subset A^n$ 上の離散確率変数を X，その受信結果を表わす B^n 上の離散確率変数を Y とする．いま，$x \in A^n$ を送信して $y \in B^n$ を受信する条件付き確率 $P_{Y|X}(y|x)$ をもつ通信路を通して，$w_i \in C_{L:n}, i = 1, \ldots, M$ を送信することを考える．このとき，受信結果が受諾される確率は，

$$P_{Accept:X}(w_i) = \sum_{\boldsymbol{y} \in \mathcal{D}_i} P_{Y|X}(\boldsymbol{y}|w_i) \qquad (4.3)$$

となり，その期待値は，

$$P_{Accept} = \sum_{i=1}^{M} P_X(w_i) P_{Accept:X}(w_i)$$

となる．よって，式 (4.3) から，

$$P_{Accept} = \sum_{i=1}^{M} P_X(w_i) \sum_{y \in \mathcal{D}_i} P_{Y|X}(y|w_i) \qquad (4.4)$$

が成立する．これより，復号誤り率，すなわち受信された通信路符号が誤通信となる確率 P_{Reject} は，

$$\begin{aligned} P_{Reject} &= 1 - P_{Accept} \\ &= \sum_{i=1}^{M} P_X(w_i) \sum_{y \notin \mathcal{D}_i} P_{Y|X}(y|w_i) \end{aligned} \qquad (4.5)$$

によって与えられる．すべての通信路符号の送信される確率が等しいとき，すなわち X が一様分布にしたがうとき，式 (4.4)，(4.5) は，

$$P_{Accept} = \frac{1}{M} \sum_{i=1}^{M} \sum_{y \in \mathcal{D}_i} P_{Y|X}(y|w_i)$$

$$P_{Reject} = \frac{1}{M} \sum_{i=1}^{M} \sum_{y \notin \mathcal{D}_i} P_{Y|X}(y|w_i)$$

となる．

シャノンが証明したのは，通信路容量を超えない伝送速度であれば，いくらでも精度よく通信できるような通信路符号法があり，逆に，通信容量を超える伝送速度であれば，そのような通信路符号法は存在しない

という事実である．この第 2 基本定理（通信路符号化定理）は，次のようにまとめられる．

定理 4.2　第二基本定理（通信路符号化定理）

通信路容量 C_0 をもつ通信路に対し，長さ n の通信路符号の伝送速度 $R_{L:n}$ が $R_{L:n} < C_0$ を満たすように符号化されるとする．このとき，任意の $\varepsilon > 0$ に対して，

$$P_{Reject} < \varepsilon$$

を満たす符号 $C_{L:n}$ が存在する．また，$R_{L:n} > C_0$ であれば，ある $\delta > 0$ が存在して，どのような通信路符号に対しても

$$P_{Reject} > \delta$$

となる．

この定理の前半部分のシャノンの証明は，受信空間から独立な無作為復元抽出を n 回繰り返すことにより n 個の符号語を選ぶランダム符号化法に基づいている．このランダム符号化によって作られる符号 $C_{L:n}$ の復号誤り率の期待値 P_{Reject} を求め，通信路容量 C_0 と伝送速度 $R_{L:n}$ が $R_{L:n} < C_0$ を満たすとき，符号長 n を $n \to \infty$ とすれば，$P_{Reject} \to 0$ となることを示した．定理の後半部分は，通信路容量と伝送速度の定義から背理法で導くことができる．

シャノンの証明は難解であるが，文献 [67] では，$P_{Reject} \to 0$ となるような符号列 $C_{L:n}$ を実際に構成する Ash [79] による証明を紹介しており，こちらはわかりやすい．興味のある読者は，文献 [78] と併せて参照されたい．

シャノンは，「情報」という言葉が専門的な論文から飛び出して時代の名称となるまでを生きた．1948 年のシャノンの論文は，数十年後に Scientific American 誌によって「情報時代のマグナカルタ」と呼ばれた [12].

次回は，情報理論を確立した後も充実した人生を送った「その後のシャノン」を追うことにする．

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―石ころからリンゴへ―』，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 Viéte, https://enwikipedia.org/wiki/Francois_Viéte（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（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（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（2021 年 12 月 20 日閲覧）

[14] Wikipedia, 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―情報時代のパイオニア―』，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（2021 年 12 月 21 日閲覧）

[19] Wikipedia, 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（2021 年 12 月 21 日閲覧）

[21] Wikipedia, 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（2022 年 1 月 2 日閲覧）

[23] Wikipedia, 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)（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, 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/Gottf_ried_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（2022 年 1 月 4 日閲覧）
[31] Wikipedia, 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（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（2022 年 3 月 6 日閲覧）
[37] Wikipedia, 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（2022 年 3 月 7 日閲覧）
[40] Wikipedia, 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（2022 年 4 月 7 日閲覧）
[42] Wikipedia, 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（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（2022 年 5 月 7 日閲覧）
[56] Wikipedia, Ralph Hartley, https://en.wikipedia.org/wiki/Ralph_Hartley（2022 年 5 月 7 日閲覧）
[57] Wikipedia，ニコラ・レオナール・サディ・カルノー，https://ja.wikipedia.org/wiki/ニコラ・レオナール・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)（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（2022 年 8 月 4 日閲覧）
[70] Wikipedia, 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（2022 年 8 月 4 日閲覧）
[72] Wikipedia, 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（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] 正畠宏一，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.
[77] Wikipedia, Richard Hammin, https://en.wikipedia.org/wiki/Richard_Hamming（2022 年 12 月 20 日閲覧）
[78] 植松友彦，『代数系と符号理論』，コロナ社，2010.
[79] R. B. Ash, *Information Theory*, John Wiley & Sons, 1965.