目次

第 1 章　情報の数量的認識 3
1.1　自己情報量 . . . 3
1.2　エントロピー . . . 3
1.2.1　１変数の場合 . . . 4
1.2.2　多変数の場合 . . . 4
1.2.3　相対エントロピー . . . 4
1.3　関手としてのエントロピー . . . 5
1.4　二進数と対数関数 . . . 5

第 2 章　情報源のモデル 6
2.1　情報源の定義 . . . 6
2.2　Markov 情報源 . . . 6
2.3　情報源のエントロピー . . . 6
2.4　エントロピーと平均符号長 . . . 6
2.5　Shannon-Fano 符号 . . . 7
2.6　拡大情報源と積のエントロピー . . . 7
2.7　Shannon の第一定理 . . . 7

第 3 章　情報源符号化 8
3.1　符号化 . . . 8
3.2　一意復号可能性 . . . 8
3.3　瞬時符号 . . . 9
3.3.1　語頭符号 . . . 9
3.3.2　木と構成法 . . . 9
3.3.3　Kraft の不等式 . . . 9
3.4　網羅性 . . . 10

第 4 章　最適符号 11
4.1　最適符号の定義と存在 . . . 11
4.2　２元 Huffman 符号 . . . 11
4.3　２元 Huffman 符号の最適性 . . . 11
4.4　拡大情報源 . . . 12

第 5 章　情報通信路 13
5.1　記法と定義 . . . 13
5.2　システムエントロピー . . . 13
5.3　通信路に関するシャノンの第一基本定理 . . . 13
5.4　相互情報量 . . . 14
5.5　通信路容量 . . . 14

第 6 章 信頼できない通信路の利用 15
6.1 決定則 . . . 15
6.2 信頼性を高める例 . . . 15
6.3 Hamming 距離 . . . 15
6.4 Shannon の基本定理 . . . 15
6.5 Shannon の基本定理の逆 . . . 16

第 7 章 誤り訂正符号 17
7.1 枠組みと線型符号 . . . 17
7.2 符号の例 . . . 17
7.3 最小距離 . . . 18
7.4 ハミングの球充填限界式 . . . 18
7.5 Gilbert-Varshamov 限界 . . . 18
7.6 Hadamard 符号 . . . 19

第 8 章 線型符号 20
8.1 線型符号の行列表現 . . . 20
8.1.1 生成行列 . . . 20
8.1.2 パリティ検査行列 . . . 20
8.2 線型符号の同値性 . . . 20
8.3 線型符号の最小距離 . . . 21
8.4 Hamming 符号 . . . 21
8.5 Golay 符号 . . . 21
8.6 標準配列 . . . 21
8.7 シンドローム復号 . . . 21
8.8 巡回符号 . . . 22
8.8.1 定義 . . . 22
8.8.2 生成多項式 . . . 22

第 9 章 暗号 23
9.1 RSA . . . 23
9.2 Diffie-Hellman の鍵交換 . . . 23
9.3 ElGamal 暗号 . . . 24

参考文献 25

第 1 章

情報の数量的認識

情報とは，「確率分布の変化」として形式化する．確率的な現象が確定的な現象となるとき，確定に必要な分だけの情報の流入が起こった，とする．

1.1 自己情報量

情報量の形式化の仕方から，対数の登場は必然であった

確率 1/6 の事象（を確定させるのに必要な）の情報量は，確率 1/2 と 1/3 との情報量の和に等しく合ってほしい（ある事象が段階的に起こったとして，経路に依存しないでほしいので）．これより，測度の値 $[0,1]$ 上の乗法を $\mathbb{R}_{\geq 0}$ 上の加法に変換する群同型として $-\log$ が必要とされる（事象が連続して起こる際，確率は積だが情報量は和で増えてほしいため）．なお，これを情報の単調性と加法性と呼ぶが，これに加えて正規化条件の 3 公理を満たす関数は対数関数に限る（群同型は 1 つ）．

記法 1.1.1. 離散集合上の積分作用素は行列積である．そこで，アルファベット A とその上の確率分布 P の組 (A,P) を，

$$\begin{pmatrix} A \\ P \end{pmatrix} = \begin{Bmatrix} a_1 & a_2 & \cdots & a_n \\ p_1 & p_2 & \cdots & p_n \end{Bmatrix}$$

と表す．

定義 1.1.2 ((self) information)**.** $I : [0,1] \to \mathbb{R}_{\geq 0}$ を，$I(p) := -\log_2 p$ bit と定める．これを**（自己）情報量**という．

要諦 1.1.3. まず，自己情報量とは，確率に対する対応である．よって，測度 $P : \Omega \to [0,1]$ に合成すべき関数 $[0,1] \to \mathbb{R}_{\geq 0}$ を得たことになる．不符号は，確率が $[0,1]$ の間で正規化されるがための形式である．

1.2 エントロピー

確率に対して，群準同型 $I := -\log_2$ bit を合成したものは，新たな測度となる（もはや確率測度ではないが）．これが情報量の総合計・エントロピーである．確率変数のエントロピー：情報量の定める測度に関する積分である．複数の確率変数について，

(1) 条件付きエントロピー：情報量の定める測度に関する条件付き期待値．直感的には，「Y が起こったことはわかっているとして，X がわかったときに得られる情報量」．
(2) 結合エントロピー：X かつ Y が起こったときの情報量．エントロピーの連鎖律 $H(X,Y) = H(Y) + H(X|Y)$ が成り立つ．
(3) さらに，$I(X;Y) := H(X) - H(X|Y)$ を相互情報量といい，「Y が起きたことは，X に対してどれくらい示唆するか？」を表す．これが 0 のとき，X, Y が独立であることに同値．
(4) 相対エントロピー：情報量の差の期待値であるが，これが何故か非負性を持つ．そこで，三角不等式を満たさない擬距離として用いる．

1.2.1　1 変数の場合

A 上に自己情報量が定める測度に関する確率変数の積分 (期待値) をエントロピーという．その確率変数の実現値を知った際に得られる情報量の期待値である．

定義 1.2.1 (entropy)**.** $H : \mathrm{Meas}(A, \mathbb{R}) \to \mathbb{R}_{\geq 0}$（実は $\mathrm{Im}\, H \subset [0, \log \alpha]$）を，自己情報量 $I(p)$ を新たな測度としてその上の積分作用素 $H(X) := -\sum_{i=1}^{n} p_i \log p_i = E_p[-\log p(X)]$ bit と定める．これを確率変数の**エントロピー**という．

例 1.2.2 (binary entropy function)**.** 特に $|A| = 2$ であるとき，$H(X) = -p \log p - (1-p)\log(1-p)$ は p の関数である．これを**2 元エントロピー関数**という．これは $p = 1/2$ で最大値 1 bit，$p = 0, 1$ で最小値 0 bit を取る．

1.2.2　多変数の場合

条件付き確率についての自己エントロピーの期待値となる．

定義 1.2.3 (conditional entropy)**.** $X, Y \in \mathrm{Meas}(A, \mathbb{R})$ とする．

(1) $H(X|Y=y) := -\sum_{x \in \mathbb{R}} p(x|y) \log p(x|y)$，$H(X|Y) := \sum_{y \in \mathbb{R}} p(y) H(X|Y=y)$ と定める．これを**条件付きエントロピー**という．

(2) Bayes の定理より，$H(X|Y) = E_{p_{X,Y}}[-\log p(X|Y)]$ であることを確認できる．

定義 1.2.4 (joint entropy)**.** $X, Y \in \mathrm{Meas}(A, \mathbb{R})$ とする．結合確率 $p(X, Y)$ について，

$$H(X, Y) := -\sum_{x \in \mathbb{R}} \sum_{y \in \mathbb{R}} p(x, y) \log p(x, y) = E_{p_{X,Y}}[-\log p(X, Y)]$$

と定める．これを**結合エントロピー**または同時エントロピーという．

補題 1.2.5 (chain rule of entropy)**.** $H(X, Y) = H(Y) + H(X|Y)$.

要諦 1.2.6. $|A \cup B| = |B| + |A \setminus B|$ はこの特殊な例である．X, Y が独立のとき，$H(X, Y) = H(X) + H(Y)$．これは $|X \cup Y| = |X| + |Y|$ $(X \cap Y = \emptyset)$ を含む．

定義 1.2.7 (mutual information)**.** $I(X; Y) := H(X) - H(X|Y)$ を**相互情報量**という．

補題 1.2.8.

(1) 相互情報量 $I(X; Y)$ は非負である．

(2) $I(X; Y) = 0$ と，X, Y が独立であることは同値．

(3) 結合エントロピー $H(X, Y)$ は対称である．

(4) 相互情報量 $I(X; Y)$ は対称である．

(5) $I(X; Y) = \sum_{x,y \in \mathbb{R}} p(x, y) \log \dfrac{p(x, y)}{p(x)p(y)} = E_{p_{X,Y}}\left[\log \dfrac{p(X, Y)}{p(X)p(Y)}\right]$ は相互情報量を特徴付ける．

1.2.3　相対エントロピー

エントロピーの差の期待値を相対エントロピーという．非負性しか満たさないが，$P(A)$ 上の距離としても使う．

定義 1.2.9 (relative entropy / divergnce)**.** アルファベット A 上の確率分布 $p, q \in P(A)$ の**相対エントロピー**または**発散**とは，

$$D(p||q) = \sum_{x \in A} p(x) \log \frac{p(x)}{q(x)} = E_p\left[\log \frac{p(X)}{q(X)}\right]$$

で定まる.

命題 1.2.10 (相対エントロピーの非負性)**.**

(1) 任意の確率分布 $(x_i), (y_i)$ について，$\sum_{i=1}^{q} x_i \log_r \frac{1}{x_i} \leq \sum_{i=1}^{q} x_i \log_r \frac{1}{y_i}$.

(2) $D(p||q) \geq 0$ であり，等号成立は $p = q$ のとき.

命題 1.2.11 (エントロピーの上限)**.** $|A| =: \alpha \in \mathbb{N}$ とする．$H(X) \leq \log \alpha$ が成り立ち，等号成立は $X \sim U(A)$ の場合.

要諦 1.2.12. デルタ分布によって最小値，一様分布によって最大値を取るのがエントロピー $H : \mathrm{Meas}(A, \mathbb{R}) \to [0, \log \alpha]$ となる.

1.3　関手としてのエントロピー

John Baez, Tobias Fritz and Tom Leinster 2011[a]

[a] https://ncatlab.org/johnbaez/show/Entropy+as+a+functor

1.4　二進数と対数関数

エントロピーの特徴付け

初等超越関数 log の使用が特徴的である．これは乗法と加法の間の群準同型として導入したが，bit の単位からわかるように，文字数としても特徴付けられるのがエントロピーの well-definedness であった．これを考察する.

命題 1.4.1. 正整数 x の 2 進数表記における桁数 $l_2(x)$ は，$l_2(x) = \lfloor \log x \rfloor + 1$ と表される.

第 2 章

情報源のモデル

前章では確率変数の情報量を定義した．（情報源アルファベット上の）確率変数の列 (確率過程) とその上の制約の組 $(X_i)_{i\in\mathbb{N}}$ を**情報源**という．

2.1 情報源の定義

定義 2.1.1 (memoryless information source, Markov source)**.**

(1) 情報源 $(X_i)_{i\in\mathbb{N}}$ が Markov 連鎖であるとき，**記憶のない情報源**または **i.i.d. 情報源**という．
(2) Markov 性が直前の有限個の記号に限定されていて，それ以前の記号列からは影響を受けない情報源を**（m-重）Markov 情報源**という．特に $m = 1$ の場合は**単純**であるという．

2.2 Markov 情報源

記憶を持つ情報源のうち，ある種の有限性を持つのが Markov 情報源である．主な問題は定常分布を知ることであるが，これは遷移確率行列の定める力学系の極限を求める問題である．特に重要な atom として，エルゴード情報源を考える．

定義 2.2.1 (state transition diagram)**.** m 重 Markov 情報源について，状態空間 A^m 上の遷移として捉えたものを，**状態遷移図**または **Shannon** 線図という．

要諦 2.2.2. このような捉え方によって，$m = 1$ として一般性は失われない．

2.3 情報源のエントロピー

定義 2.3.1. 情報源の出力 1 記号当たりの情報量の期待値を**情報源のエントロピー**といい，$H_r(S)$ で表す．

例 2.3.2.

(1) 記憶のない情報源のエントロピーは任意の i について $H(X_i)$ である．
(2) Markov 情報源のエントロピーは，各状態の出力分布のエントロピーを，定常分布に関して積分したものを言う．

2.4 エントロピーと平均符号長

定理 2.4.1. 情報源 S の一意復号可能な r-元符号 C について，$L(C) \geq H_r(S)$ が成り立つ．

要諦 2.4.2. $H_r(S)$ は，S から発信されるシンボルの持つ自己情報量の期待値である．C が一意復号可能ならば，この情報量が保存されているはずである．

系 2.4.3. S を生起確率 (p_i) の情報源とする．

(1) 一意復号可能な r 元符号 $\mathcal{C}$ で，$L(C) = H_r(S)$ を満たすものが存在する．
(2) $\exists_{e_i \in \mathbb{Z}_{\leq 0}}\ p_i = r^{e_i}$．

定義 2.4.4. 情報源 S の r 元符号 C について，$\eta := \dfrac{H_r(S)}{L(C)}$ を**効率**といい，$0 \leq \eta \leq 1$ を満たす．$\overline{\eta} := 1 - \eta$ を**冗長性**という．

2.5　Shannon-Fano 符号

Huffman 符号は平均符号長の計算が複雑である．一方で，Shannon-Fano 符号は最適に近いことが保証されている上に，平均符号長の評価も容易である．

定義 2.5.1. $l_i := \lfloor \log_r(1/p_i) \rfloor$ は Kraft の不等式を満たすので，これが定める瞬時符号が存在する．これを **Shannon-Fano 符号**という．

命題 2.5.2. $H_r(S) \leq L(C) \leq 1 + H_r(S)$.

2.6　拡大情報源と積のエントロピー

定理 2.6.1. S を任意の情報源とする．$H_r(S^n) = nH_r(S)$ が成り立つ．

定理 2.6.2. 独立な情報源 $S, \mathcal{T}$ について，$H_r(S \times \mathcal{T}) = H_r(S) + H_r(\mathcal{T})$.

2.7　Shannon の第一定理

定理 2.7.1 (Noiseless Coding Theorem (Shannon 48))**.** 任意の $\epsilon > 0$ に対して，十分大きな $n \in \mathbb{N}$ が存在して，S^n を符号化することによって，情報源 S の一意復号可能な r 元符号 C であって，平均符号長がエントロピー $H_r(S)$ に対して，$L(C) - H_r(S) < \epsilon$ を満たす．

第 3 章

情報源符号化

情報源（の出力）系列を効率よく符号化する，データ圧縮の問題を扱う．48 の Shannon の論文は，Weiner の確率論の方法を用いて，データ圧縮の方法を議論し，符号化の問題から情報理論を創始した．ここではまず，容易で，曖昧さのない復号が存在する符号の構成を考える．

3.1 符号化

記法 3.1.1.

(1) $T^* = \cup_{n\geq 0}[T]^n, T^+ := \cup_{n>0}[T]^n$.
(2) $C := \mathrm{Im}\, C$ と混用する．

定義 3.1.2 (coding, non-singular, decoding, uniquely decodable)**.**

(1) アルファベット A, B について，写像 $f : A \to B^+$ を**符号**，値 $f(a) \in B^+$ を**符号語**という．始域アルファベットを**情報源アルファベット**，終域を生成するアルファベットを**符号アルファベット**という．
(2) f が単射であるとき，**正則符号**という．以降正則符号のみを考える．
(3) f の延長 $f^* : A^* \to B^*$ の逆写像を求めることを**復号**という．逆写像が B^* の全域で定まるとき，すなわち，f^* が単射であるとき**一意復号可能**であるという．

注 3.1.3. 符号アルファベットは主に通信路の技術に依るので，A, B は応用上も別物である．$|B|$ を基数 (radix) といい，多くの例では $r = 2$ である．モールス信号は空白を含めて $r = 3$ の例である．

例 3.1.4.

(1) ASCII (American Standard Code for Information Interchange) は二元符号で，$f(A) \subset B^7$ を満たす 7 ビットの符号化である．
(2) A に線形順序があり，隣接する符号語の Hamming 距離が 1 になるような二元符号を **Gray 符号**という．
(3) バーコードや受験番号，ISBN の最後の桁は誤り訂正符号となっている．ISBN はハイフンを除いて長さ 10 の $\mathbb{Z}_{11}$ 上の符号語で，$a_1 0$ は $a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \mod 11$ を満たすように定まっている．これは，単一誤りと，2 つの記号の置換を検出できる，人為エラーに特化された符号である．

定義 3.1.5.

(1) $L : \mathrm{Map}(S, T^+) \to \mathbb{R}$ を，関数 $|C^*(X_n)| : S \to \mathbb{N}$ の期待値として定める．これを**平均符号長**という．

3.2 一意復号可能性

定理 3.2.1. C は単射とする．Im C に含まれる符号語の長さが全て同じならば，C は一意復号可能である．このとき，C を長さ l の**ブロック符号**であるという．

定義 3.2.2. $C_0 := \mathrm{Im}\, C, C_n := \{w \in T^+ \mid \exists_{u \in \mathrm{Im}\, C, v \in C_{n-1}}\ uw = v \vee vw = u\}$ と帰納的に定める．$C_\infty := \cup_{n=1}^{\infty} C_n$ とする．

注 3.2.3. $C_1 = \{w \in T^+ \mid \exists_{u,v \in C}\ uw = v\}$ となる．

定理 3.2.4 (Sardinas, Patterson 53)**.** 次の 2 条件は同値.

(1) C は一意復号可能.
(2) $C \cap C_\infty = \emptyset$.

定理 3.2.5 (McMillan 56)**.** 次の 2 条件は同値.

(1) 符号長が $l_1, \cdots, l_q$ である一意復号可能な r 元符号 C が存在する.
(2) $\sum_{i=1}^{q} \frac{1}{r^{l_i}} \leq 1$.

3.3　瞬時符号

瞬時符号とは，語頭符号である．これが存在するための条件は，Kraft の不等式によって特徴づけることができる．組み合わせ論的な本質は，木構造である．

3.3.1　語頭符号

定義 3.3.1 (instantaneously decodable codee)**.**

(1) 符号 C が**瞬時復号可能な符号**であるとは，任意の符号語列 $t \in T^+$ に対して，t で始まる全ての符号列が，その後の符号に依らず，一意に復号されることをいう.
(2) 符号 C が**語頭符号**であるとは，どの符号語も，他の符号語の語頭には来ないことをいう：$\forall_{w_i \in \mathrm{Im}\, C}\ \forall_{w \in T^*}\ \forall_{w_j \in \mathrm{Im}\, C}\ i \neq j \Rightarrow w_j \neq w_i w$．すなわち，$C_1 = \emptyset$.

定理 3.3.2. 次の 2 条件は同値.

(1) 誤頭符号である.
(2) 瞬時符号である.

3.3.2　木と構成法

議論 3.3.3. T^* は自然な包含関係に関して r 元根付き木の構造を持ち，ϵ を根とする．この木の頂点集合 $(\epsilon\ \notin) C$ が，性質 $\forall_{x,y \in C}\ x \neq y \Rightarrow x \wedge y = \epsilon$ を満たすとき，C は瞬時符号である.

3.3.3　Kraft の不等式

定理 3.3.4 (Kraft 49)**.** 次の 2 条件は同値.

(1) 符号長が $l_1, \cdots, l_q$ であるような r 元瞬時符号 C が存在する.
(2) $\sum_{i=1}^{q} \frac{1}{r^{l_i}} \leq 1$.

要諦 3.3.5. 符号長が l であるとは，木構造の中の頂点としては高さ l に存在することを表す．これは，高さ $h(> l)$ の頂点 r^h 個のうち，r^{h-l} 個を使用不可とする．これを根に引き戻して考えると，$\frac{1}{r_i^l}$ の和が 1 を超えると，どのようにうまく選ぼうと瞬時符号は構成できないことがわかる.

系 3.3.6. 次の 2 条件は同値.

(1) 符号長が $l_1, \cdots, l_q$ の r 元瞬時符号が存在する.
(2) 符号長が $l_1, \cdots, l_q$ の r 元一意復号可能な符号が存在する.

3.4 網羅性

一番効率よく符号を作るには, $\sum_{i=1}^{q} \frac{1}{r^{l_i}} = 1$ を狙いたい. これを捉える概念が存在する.

定義 3.4.1 (exhaustive). $\exists_{n\in\mathbb{N}}\ \forall_{w\in T^+}\ |w| > n \Rightarrow [\exists_{w_0\in \mathrm{Im}\, C}\ \exists_{w_1\in T^*}\ w_0 w_1 = w]$ を満たすとき, C を**網羅的**であるという.

定理 3.4.2. 次の 2 条件は同値.

(1) 符号長が $l_1, \cdots, l_q$ であるような r 元網羅的符号 C が存在する.
(2) $\sum_{i=1}^{q} \frac{1}{r^{l_i}} \geq 1$.

第 4 章

最適符号

良い符号とは，ある程度は符号語が長くなければならないことを組み合わせ論的に観察し，２つの不等式の形で結果を得た．そこで，その制約の中でも，平均符号長 $L(C)$ がなるべき短い符号の構成方法を考える．

4.1 最適符号の定義と存在

定義 4.1.1 (optimal code / compact code)**.** 平均符号長 $L : \mathrm{Map}(S, T^+) \to \mathbb{R}$ を最小にする r 元瞬時符号を**最適符号**または**コンパクト符号**という．

補題 4.1.2 (定義の well-defined 性)**.** 情報源 S と整数 r について，S の一意復号可能な r 元符号 C の平均符号長 $L(C)$ の値域は，S の r 元瞬時符号 C の平均符号長 $L(C)$ の値域に一致する．

定理 4.1.3. 任意の情報源 S と整数 $r \geq 2$ について，最適な r 元符号が存在する．

4.2 ２元 Huffman 符号

符号アルファベットを $\{0,1\}$ とする．Huffman 52 の理論．生起確率に基づいて，符号を定める．

定義 4.2.1 (reduced source)**.**

(1) 情報源 S の値域を $\{s_1, \cdots, s_q\}$ とし，それぞれの生起確率を $p_1 \geq \cdots \geq p_q$ とする．新たなシンボル $s' := s_{q-1} \vee s_q$ を定め，**縮退情報源** S' を構成する．

(2) ２つの情報源の間に，写像 $\Phi : \{S'\text{の符号 }\} \to \{S\text{ の符号 }\}$ を構成する．S' の符号 C に対して，符号 C' は，$\{s_1, \cdots, s_{q-2}\}$ 上では同じだが，s_{q-1} を $w'0$，s_q を $w'1$ に対応させることとする．

(3) 縮退情報源を取る操作を $q-1$ 回繰り返すと，値域が一点集合の情報源となる．この自明な符号 $C^{(q-1)}$ の値域を $\{\epsilon\}$ とし（これは明らかに瞬時符号），Φ の値を $q-1$ 回とることで，**Huffman 符号** C を得る．

補題 4.2.2. Φ は瞬時符号を保つ．すなわち，C' が瞬時符号ならば，C も瞬時符号である．

［証明］. 瞬時符号は語頭符号であることから従う． ■

要諦 4.2.3. 一意復元可能性は失われかねないが，瞬時符号ならうまくいく．絶妙．

4.3 ２元 Huffman 符号の最適性

定義 4.3.1 (sibling)**.** ２つの２元符号語 w_1, w_2 が，ある符号語 $x \in T^*$ が存在して $x0, x1$ とあらわせるとき，w_1, w_2 は**兄弟**であるという．

補題 4.3.2. 任意の情報源 S は，符号長が最も長い２つの符号語が兄弟であるような２元最適符号 D を持つ．

定理 4.3.3. C が情報源 S の 2 元 Huffman 符号ならば，最適符号である．

4.4　拡大情報源

よりマクロな構造に注目し，情報源アルファベットをうまく取り直すことで，生起確率が高い特定の列を符号化すると，さらに平均符号長を小さくすることが出来る．

第 5 章

情報通信路

雑音の多い／信頼性の低い通信路を介してメッセージを届ける情報源.

エントロピーは情報量の平均であったが，これが「字数」に対応づくことは，ある種「情報量」の概念の well-definedness をあらわす．エントロピーはこちらを定義として採用することも出来る.

5.1 記法と定義

定義 5.1.1 (channel)**.** 情報源 $\mathcal{A}, \mathcal{B}$ について，それぞれのアルファベットを $\{a_1, \cdots, a_r\}, \{b_1, \cdots, b_s\}$ とする.

(1) それぞれのアルファベットの間の写像 Γ を**情報通信路**という.
(2) 各成分を $P_{ij} := P(b = b_j | a = a_i)$ とする行列を，**通信路行列**という.

例 5.1.2 (binary symmetric channel, binary erasure channel)**.**

(1) $A = B = 2$ で，シンボルに依らず成功・失敗確率が一様であるとき，**二元対称通信路**という.
(2) $A = 2, B = 2 \cup \{?\}$ であるとき，**二元消失通信路**という.

定義 5.1.3. Γ, Γ' を通信路とする.

(1) 和 $\Gamma + \Gamma'$ とは，入力アルファベット $A \sqcup A'$ と出力アルファベット $B \sqcup B'$ について，通信路行列を直和 $M \oplus M'$ とする通信路である.
(2) 積 $\Gamma \times \Gamma$ とは，入力アルファベット $A \times A'$ と出力アルファベット $B \times B'$ について，通信路行列を Kronecker 積 $M \otimes M'$ とする通信路である.
(3) 積 Γ^n を，n **次拡大**という.
(4) 合成 $\Gamma \circ \Gamma'$ とは，入力アルファベット A と出力アルファベット B' について，通信路行列を積 MM' とする通信路である．これを通信路の**カスケード**という.

5.2 システムエントロピー

$H(\mathcal{A}), H(\mathcal{B}), H(\mathcal{A}|\mathcal{B}), H(\mathcal{B}|\mathcal{A}), H(\mathcal{A}, \mathcal{B})$ をシステムエントロピーという.

議論 5.2.1 (equivocation)**.** 条件付きエントロピー $H(\mathcal{A}|b_i)$ の積分 $H(\mathcal{A}|\mathcal{B})$ を**あいまい度**という.

5.3 通信路に関するシャノンの第一基本定理

定理 5.3.1. 通信路の出力 $\mathcal{B}$ が既知ならば，任意の $\epsilon > 0$ に対して，十分大きな $n \in \mathbb{N}$ が存在して，$\mathcal{A}^n$ を符号化することによって，入力 $\mathcal{A}$ の一意復号可能で，$L(C) - H(\mathcal{A}|\mathcal{B}) < \epsilon$ を満たす符号化が存在する.

5.4 相互情報量

議論 5.4.1. 相互情報量 $I(\mathcal{A},\mathcal{B}) := H(\mathcal{A}) - H(\mathcal{A}|\mathcal{B})$ は次の 3 通りの解釈がある.

(1) $\mathcal{B}$ を知ることで解消する $\mathcal{A}$ についての不確かさの総量.
(2) $\mathcal{B}$ によって伝送される $\mathcal{A}$ についての情報量の総量.
(3) $\mathcal{A}$ に対する符号語に含まれるシンボルで，$\mathcal{B}$ の符号語に出てくるものの平均個数.

要諦 5.4.2 (数え上げ測度の例)**.** $|A \cap B| = |A| - |A \setminus B|$ における左辺が相互情報量と見れる.

5.5 通信路容量

定義 5.5.1 (capacity)**.** 通信路 $\Gamma : A \to B$ の**容量**を，$I(\mathcal{A},\mathcal{B})$ の最大値と定める.

定理 5.5.2.

(1) $\mathcal{P} := \left\{ p \in \mathbb{R}^r \mid p_i \geq 0, \sum_i p_i = 1 \right\}$ はコンパクト.
(2) $\mathcal{I}$ は，入力確率分布 $(p_i) \in \mathcal{P}$ の連続関数である.
(3) 任意の通信路について，容量が存在する.

第 6 章

信頼できない通信路の利用

Bravo と Victor のように，互いに十分異なる符号語を使えば，符号語に含まれるシンボルのいくつかが不正確な場合でも，受信側が混乱する可能性は低いというアイデアが Shannon の定理に含まれている．このように，情報理論は存在性を保証するが，実際の構成とアルゴリズムに対する考察は符号理論の範疇である．

6.1 決定則

定義 6.1.1.

(1) 関数 $\Delta : B \to A$ を**決定則**という．$\Delta(b_j) = a_{j^*}$ とあらわす．
(2) 正しい決定則を用いて，送信元のアルファベットを求めることを**復号**という．
(3) 正しく復号される確率 $P_C = \sum_j q_j P(a = a_{j^*} | b = b_j)$ を最大にする決定則を**理想的観測者規則**という．
(4) 一方で，確率 $P(a = a_{j^*} | b = b_j)$ が不可知であることも多い．その場合は，前向き確率 P_{ij}（通信路についての知識）のみが判断基準となり，$\forall_i\ P_{j^*j} \geq P_{ij}$ を満たす決定則を**最尤法**という．

6.2 信頼性を高める例

例 6.2.1 (binary repetition code, majority decoding)**.** 同じ入力を n 回繰り返すとする．そこで，届いた符号語のうち，一番多いシンボルを採用して復号する．これを，r 元**反復符号** R_n という．この代償は，伝送速度が遅くなることである（n 倍の時間がかかるはず）．これを伝送レートという概念で測る．$|R_n| = r$ なので，伝送レートは $R = \dfrac{\log_r(r)}{n} = 1/n$ である．

定義 6.2.2 (transmission rate)**.** 符号 $C \subset [A]^n$ の**伝送レート**とは，

$$R := \frac{\log_r |C|}{n}$$

である．

補題 6.2.3. $0 \leq R \leq 1$.

6.3 Hamming 距離

最尤法は，反復符号については Hamming 距離の言葉によって特徴づけられ，これを**最近傍復号**という．

6.4 Shannon の基本定理

定理 6.4.1. Γ を通信路容量 $C > 0$ の通信路とする．任意の $\delta, \epsilon > 0$ について，十分大きな $N \in \mathbb{N}$ が存在して，任意の $n \geq N$ について，$C - \epsilon \leq R < C$ を満たし，誤り確率が $P_E < \delta$ となる決定則を持つような，長さ n で伝送レート R の符号 C が存在する．

系 6.4.2.

(1) Γ を $P > 1/2$ となる二元対称通信路とすると，Γ の容量は $C = 1 - H(P) > 0$ となる．
(2) 任意の $\delta, \epsilon > 0$ について，十分大きな $n \in \mathbb{N}$ が存在して，伝送レート R が $C - \epsilon \leq R < C$ を満たし，最近傍復号が誤り確率 $P_E < \delta$ を与えるような符号 $C \subset 2^n$ が存在する．

6.5 Shannon の基本定理の逆

定理 6.5.1 (Fano bound)**.** Γ を通信路，r 元入力を $\mathcal{A}$，出力を $\mathcal{B}$ とする．Γ に対する任意の決定則 Δ の誤り確率 P_E は，次を満たす：

$$H(\mathcal{A}|\mathcal{B}) \leq H(P_E) + P_E[\log(r-1)].$$

系 6.5.2. 通信路容量 C について，任意の $C' > C$ について，Shannon の定理は成り立たない．すなわち，C は任意の精度での伝送を可能にするためのレートの上限である．

第 7 章

誤り訂正符号

なるべく高い伝送レート R と，低い誤り率 P_E を兼ね備えた符号 C の構成法を考える．以降は符号理論であり，構成論であるが，その時の主要な道具が代数であり，特に線形代数である．

7.1 枠組みと線型符号

記法 7.1.1.

(1) 通信路はアルファベットを $\mathbb{F} := A = B$ として一般性を失わない．
(2) すべての符号語は等しい長さ n を持つとする（ブロック符号）．これは Shannon の定理による帰結．
(3) 任意の有限体は，p 群であり，$\mathbb{Z}/p^n\mathbb{Z}$ と表せる．

定義 7.1.2.

(1) $C \subset \mathbb{F}^n$ が線型部分空間であるとき，C を**線型符号**または**群符号**という．
(2) $k := \dim C$ のとき，これを線型 $[n, k]$ 符号という．

補題 7.1.3. 線型 $[n, k]$ 符号の伝送レートは $R = k/n$ と表せる．

要諦 7.1.4. 情報は k 成分に乗せて，残りは誤り訂正に使われる，という比率である．

7.2 符号の例

例 7.2.1 (repetition code)**.** $\mathbb{F}$ 上の反復符号 R_n は，$\mathbb{F}^n$ 内の一次元の線型符号で，符号語 $11\cdots1$ によって張られる空間となる．誤り率が十分小さい時，最近傍復号によって誤りが訂正される．しかし，伝送レートは悪く，$R = 1/n$.

例 7.2.2 (parity-check code)**.** **パリティ検査符号** P_n とは，

$$P_n := \left\{ (u_i) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} u_i = 1 \right\}$$

によって定まる $n-1$ 次元の線型符号で，u_n を検査桁とする．伝送レートは優秀だが，誤り訂正は不可能で，検出も穴がある．

例 7.2.3 (binary Hamming code (47))**.** 2 元ハミング符号 H_7 は，長さ $n = 7$ の $\mathbb{F}_2$ 上の 4 次元の線型符号である．Bell 研究所の Hamming によって開発された．長さ 4 の 2 元記号列 $a_1a_2a_3a_4$ を，7 桁で符号化する．u_3, u_5, u_6, u_7 に写し，残りの u_1, u_2, u_4 は誤り訂正桁である．単一の誤りが修正可能．

例 7.2.4 (extended code)**.** 長さ n の体 $\mathbb{F}$ 上の符号 C に対して，**拡大符号** $\overline{C}$ とは，追加の桁を $\sum_{i=1}^{n+1} u_i = 0$ となるように選ぶことで，濃度の変わらない長さ $n+1$ の符号のことである．C が線型ならば，$\overline{C}$ も線型．

例 7.2.5 (punctured code)**.** 長さ n の符号 C に対して，**パンクチャド符号** C° とは，定めた桁数 $i \in [n]$ に対して，シンボル u_i を各符号語 $u_1 \cdots u_n \in C$ から取り除くことで定義される．

7.3　最小距離

誤り訂正の精度を上げる技法

最近傍復号を行うにあたって，符号の最小距離は大きければ大きいほど精度が高い．長さ n，符号語濃度 M，最小距離 d の符号を (n,M,d)-符号という．d に対して，$t := \left\lfloor \dfrac{d-1}{2} \right\rfloor$ ビット以内の誤りを正確に訂正できる．

補題 7.3.1. C が線型符号のとき，最小距離は $d = \min\{d(v,0) \geq 0 \mid v \in C, v \neq 0\}$.

要諦 7.3.2. $w(v) := d(v,0)$ を **(Hamming) 重み**という．Hamming 距離が定めるノルムである．

定義 7.3.3. 符号 C が t **重誤り訂正**であるとは，最大 t 桁の誤りまでは（誤りが距離 t 以下であるときは），常に正しく訂正されることをいう．

注 7.3.4. 一方で，最小距離 d の符号は，$d-1$ 個の誤りを検出する．

定義 7.3.5. ベクトル $e := v - u$ を**誤りパターン**という．

定理 7.3.6. 最小距離 d の符号 C について，

(1) t 個の誤りを訂正する．
(2) $d \geq 2t+1$ を満たす．

7.4　ハミングの球充填限界式

符号語 u に復号される範囲は，球 $S_t(u)$ である．誤り訂正の精度は，この球の大きさに単調増加し，伝送レートは，球の総数に単調増加する．$M := |C|$ の上界を与える．

定理 7.4.1 (Hamming's sphere-packing bound)**.** C を q 元 t 重誤り訂正符号で，長さが n の M 個の符号語からなるとする．このとき，

$$M\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{t}(q-1)^t\right) \leq q^n.$$

要諦 7.4.2. この条件を満たす符号を**完全**符号という．これは，交わらない球 $S_t(u)$ が C を埋め尽くす条件と同値である．

7.5　Gilbert-Varshamov 限界

長さ n，最小距離 d に対して，符合語の数 M の最大値を $A_q(n,d)$ とすると，この下限を与える．

定理 7.5.1 (Gilbert-Varshamov bound)**.** $q \geq 2$ かつ $n \geq d \geq 1$ ならば，

$$A_q(n,d)\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{d-1}(q-1)^{d-1}\right) \geq q^n$$

命題 7.5.2 (singleton の限界式, MDS : maximum distance separable code)**.** $\mathbb{F}_q$ 上の符号が長さ n，最小距離 d，濃度 M であるとする．

$$\log_q M \leq n - d + 1.$$

等号を成立させるときの符号を，**最大距離分離符号**という．

7.6　Hadamard 符号

符号の構成の中でも，Hadamard 行列から構成できるクラスがある．

定理 7.6.1 (Hadamard)**.**

(1) $|h_{ij}| \leq 1$ を満たす行列 $H = (h_{ij})$ の行列式について，$|\det H| \leq n^{n/2}$ が成り立つ．
(2) 等号成立条件は，$h_{ij} = \pm 1$ かつ H の任意の 2 つの異なる行は直交するとき．これを満たす行列を **Hadamard 行列**という．

注 7.6.2. $h_{ij} = \pm 1$ は，各行が長さ $\sqrt{n}$ であることを含意する $r_i \cdot r_i = n$．$HH^T = nI_n$ である．これより，$(\det H)^2 = n^n$ がすぐに従う．

補題 7.6.3. Hadamard 行列 H に対し，$H' := \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ は $2n$ 次元の Hadamard 行列である．

系 7.6.4 (Sylvester matrix)**.** 任意の $m \in \mathbb{N}$ について，2^m 次元の Hadamard 行列が存在する．

［証明］. $H := (1)$ は 1 次の Hadamard 行列である．これに対して補題を繰り返し適用すれば，帰納法より従う．この算譜で構成される Hadamard 行列を Sylvester 行列という． ■

命題 7.6.5.

(1) Hadamard 行列の次数 $n > 1$ は偶数である．
(2) Hadamard 行列の次数 $n > 2$ は 4 の倍数である．

注 7.6.6. すべての 4 の倍数について，その次数の Hadamard 行列が存在するかは未解決．

定理 7.6.7 (Hadamard code)**.** H を n 次元 Hadamard 行列とする．最小距離 $d = n/2$ で，符号語濃度が $M = 2n$ であるような長さ n の 2 元符号を，各行ベクトルの $\pm$ 計 $2n$ 個を，-1 を 0 とみなして定める．

歴史 7.6.8. $n = 32$ のものが，1969 年の火星探査機マリナーからの写真伝送に使われた．

命題 7.6.9. 長さ n の Hadamard 符号の伝送レートは，$R = \dfrac{\log_2(2n)}{n} = \dfrac{1 + \log_2 n}{n} \xrightarrow{n\to\infty} 0.$

第 8 章

線型符号

線型符号は最小距離の計算が簡単であることをみた．また，最尤復号が最近傍復号となり，誤り訂正の計算の枠組みも最小距離の言葉で統一的である．ここで，線型符号を統一的に扱う枠組みを鳥瞰する．

8.1 線型符号の行列表現

8.1.1 生成行列

線型符号化は，生成行列 G を用いて $x = uG$ と表せる．

定義 8.1.1. k 行 n 列の行列 G の各行が C の基底からなるとき，k 次元線型符号 C の**生成行列**という．

要諦 8.1.2. この行列 G が定める線型同型 $\mathbb{F}^k \to \mathbb{F}^n$ が，情報源からの符号化を定めるとみなせる．

例 8.1.3. 反復符号 R_n は $G = (1\ 1\ \cdots\ 1)$ によって生成される．

8.1.2 パリティ検査行列

$HG^T = O$ を満たす行列をパリティ検査行列という．行ベクトルが線型符号を生成する行列を生成行列としたが，行ベクトルが C の直交補空間を生成する行列をパリティ検査行列という．

定義 8.1.4. 線型符号 C が，c 個の一次方程式 $vH^T = 0$ で規定されるとき，これらを**パリティ検査方程式**といい，係数行列 H を**パリティ検査行列**という．

定義 8.1.5. H を生成行列とみなして得る符号を，元の符号 C の**双対符号** D という．

補題 8.1.6. $D = C^{\perp}$.

8.2 線型符号の同値性

線型符号の統一論

線型符号の分類を行う．代表元は組織符号が選ばれる．組織符号 $G = (I_k|P)$ の I_k を情報ビット，P をパリティ検査ビットという．$H = (G^T|I_{n-k})$ となる．

定義 8.2.1 (equivalent, systematic code form)**.**

(1) 生成行列が相似な 2 つの線型符号を，**同値**であるという．
(2) ある行列 P について，$G = (I_k|P)$ と表せるとき，G を**組織符号形式**であるという．

要諦 8.2.2. 定義上，行の置換は符号を変えない．列の置換は，部分空間を変えるかもしれないが，シンボルの順序が変わるだけで，基本的な特性量は変わらない．その同値類の代表元は，各 $a_1 \cdots a_k \in [\mathbb{F}]^k$ をそのまま情報桁に写し取り，検査桁が aP で定義される符号である．

補題 8.2.3. 組織符号形式 $G = (I_k|P)$ のパリティ検査符号は $H = (-P^T|I_{n-k})$ である．

8.3 線型符号の最小距離

線型符号の最小距離は，

$$d = \min\{w(v) = d(v,0) \in \mathbb{R}_{\geq 0} \mid v \in C, v \neq 0\}$$

であったが，パリティ検査行列の言葉で特徴づけることが出来る．

定理 8.3.1. C を最小距離 d の線型符号とし，H を C のパリティ検査符号とする．このとき，d は H の一次従属な列の数の最小数となる．

要諦 8.3.2. $Hx^T = 0$ は $\sum_i x_i h_i = 0$ だが，これは $x_i = 1$ なる i について，列ベクトル h_i を足したもの．すなわち，これらの h_i が一次従属であることを表す．すなわち，一次従属な列ベクトル h_i の最小個数は，1 の最小個数に一致する．

8.4 Hamming 符号

定義 8.4.1. パリティ検査行列 H の列ベクトルとして，零ベクトル以外のすべての列ベクトルを取って得られる組織符号を，**Hamming 符号**という．

例 8.4.2. $n = 6, k = 3$ とする．

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

がパリティ検査行列となり，主座な 3×4 行列が P^T に当たる．生成行列は

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

となる．最小距離は 3 で，$t = \lfloor (3-1)/2 \rfloor = 1$ ビット誤り訂正符号となる．

定義 8.4.3. Hamming 符号に，さらにパリティビット $p := x_1 + \cdots + x_k \mod 2$ を加えて得る $y = (x\ p)$ からなる符号を，**拡大 Hamming 符号**という．符号の Hamming 重みが偶数になるが，最小重みは小さくならない．よって，$n = 6, k = 3$ のとき，最小重みは 4 になる．最近傍復号により，単一誤りの訂正と二重誤りの検出が可能になる．

8.5 Golay 符号

8.6 標準配列

8.7 シンドローム復号

線型符号が定めるシンドローム $s^T = Hy^T$ を求め，これからコセットリーダー e が求まれば，$y - e = x$ である．

議論 8.7.1 (線型符号の最尤復号)**.** 符号語 $x \in C$ に対して，誤りパターン $e = y - x$ は $Hy^T = He^T$ を満たす．よって，入力と出力の組 (x, y) について次の 3 条件は同値．

(1) $d(x,y)$ が最小.
(2) $w(e)$ が $\{e = y - x \mid x \in C\}$ で最小.
(3) $w(e)$ が $\left\{e \in V \mid He^T = Hy^T\right\}$ で最小.

定義 8.7.2.

(1) $s^T := Hy^T$ を**シンドローム**という.
(2) $\left\{e \in V \mid He^T = Hy^T\right\}$ を**コセット**という.
(3) $\arg\min\left\{w(e) \geq 0 \mid He^T = Hy^T\right\}$ を**コセットリーダー**という.

8.8 巡回符号

剰余環 $\mathbb{F}/(z^n - 1)$ のイデアルとみなせる線型符号を，巡回符号という.

8.8.1 定義

定義 8.8.1.

(1) 線型符号 C の任意の符号語 $x = (x_1, \cdots, x_n)$ の巡回シフト $(x_n, x_1, \cdots, x_{n-1})$ も C の符号語であるとき，C を**巡回符号**という.
(2) C の符号語を多項式 $f(z) = \sum_{i=1}^{n} x_i z^{n-i} \in \mathbb{Z}_2[z]/(z^n - 1)$ と同一視すると，z 倍準同型が巡回シフトに対応する.

命題 8.8.2.

(1) 巡回符号 C に対応する符号多項式の集合は，剰余環 $\mathbb{Z}_2[z]/(z^n - 1)$ のイデアルに対応する.
(2) 環 $Z_2[Z]/(z^n - 1)$ は単項イデアル整域である.

8.8.2 生成多項式

定義 8.8.3. 巡回符号 C を生成する多項式 $g \in \mathbb{Z}_2[z]/(z^n - 1)$ を**生成多項式**という.

補題 8.8.4. g は，$C \setminus \{0\}$ の中で次数が最小の多項式になる.

定理 8.8.5. 生成多項式 g は $z^n - 1$ を割り切る.

定理 8.8.6. 巡回符号 C のパリティ検査多項式 h は，以下を満たす：$f \in C \Leftrightarrow h(z)f(z) \equiv 0 \mod z^n - 1$.

第 9 章

暗号

信頼できないのは通信路の性質だけでなく，通信路の傍受である可能性もある．

9.1 RSA

Rivest-Shamir-Adleman 暗号 (78) は，「戻し方が簡単にはわからない Cieser 暗号」となる．このように暗号化と復号化の鍵が異なる暗号を，**公開鍵暗号**という．RSA は位数が秘密鍵を知らないと／ $n = pq$ の因数分解が出来ないと不明な群 $(\mathbb{Z}/\varphi(n)\mathbb{Z})^*$ によってこれを実現している．

定理 9.1.1 (Euler)**.** 任意の正整数 m に対して，$\gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$.

定義 9.1.2.

(1) Alice は素数 p,q を選び，$n := pq$ と，$1 < e < \phi(n) = (p-1)(q-1)$ かつ $\gcd(e,\phi(n)) = 1$ を満たす整数 e とを公開鍵とし，$d := e^{-1} \mod \phi(n)$ を秘密鍵とする．
(2) Bob は平文 $m \in (\mathbb{Z}/n\mathbb{Z})^*$ を送るとき，暗号文 $c := m^e \mod n$ を送信する．
(3) Alice は $m = c^d \mod n$ を計算することで復号できる．

要諦 9.1.3. 平文・暗号文の空間 $(\mathbb{Z}/n\mathbb{Z})^*$ と，その乗数の空間 $(\mathbb{Z}/\varphi(n)\mathbb{Z})^*$ とがある．十分大きな $n := pq$ について，$e < |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ を用意すると，$e \in (\mathbb{Z}/\phi(n)\mathbb{Z})^*$ の逆元はなかなか判らない．n を p,q に因数分解できないと，Euler 関数 $d := e^{-1} \mod \phi(n)$ の計算の仕様もない（２つの素数を使うメカニズムはここにある）．すると，「戻し方が判らない Cieser 暗号」のようになる．戻る原理は Euler の定理 $m = (m^e)^d = m^{k\varphi(n)+1} = m \mod n$ による．

例 9.1.4 (discrete logarithm)**.** 一般に，巡回群 $G = \langle\alpha\rangle$ について，$\forall_{\beta\in G}\ \exists_{n\in\mathbb{N}}\ \alpha^n = \beta$ であるが，$n = \log_\alpha \beta$ を求める問題を離散対数問題という．これが計算困難であるから，離散群の指数をいじる方針が立つ．

9.2 Diffie-Hellman の鍵交換

RSA が（素因数分解をするか）離散対数問題を解かねばならないのと同様なメカニズムで，安全に暗号鍵を共有する方法 (76)．すべての公開鍵と秘密鍵の内１つを得ることで簡単に破られる．

定義 9.2.1.

(1) Alice と Bob は素数 p と原子根 $g \in \mathbb{F}_p$ を定めて共有する．
(2) 整数 a,b を，Alice と Bob がそれぞれ定め，秘密鍵とする．
(3) Alice が $g^a \mod p$ を Bob に送信し，Bob は $g^b \mod p$ を Alice に送信する．すると，２人の間のみで $g^{ab} \mod p$ の値が秘密裏に共有される．

9.3　ElGamal 暗号

実際に Diffie-Hellman の鍵交換を用いた暗号化法 (85).

定義 9.3.1.

(1) Alice が素数 p と原子根 $g \in \mathbb{F}_p$ を定め，整数 $0 < a < p-2$ を用意し，$h := g^a \mod p$ と併せて，3-組 (h, g, p) を Bob に共有する.
(2) Bob は同様に $0 < b < p-2$ を定め，共有された秘密鍵 $s := h^b \mod p$ を定める．平文 $m \in \mathbb{F}_p^\times$ の暗号化を $c := ms$ として行い，これを $g^b \mod p$ と共に送信する.
(3) Alice も $(g^b)^a = s$ を得るので，$s^{-1} \in \mathbb{F}_p$ を Euclid の互除法によって計算し，これを用いて復号する.

要諦 9.3.2. 今回は体の元なので，逆元の計算は簡単である代わりに，秘密鍵 a, b の取得が困難になる.

参考文献

[1] 横尾英俊『情報理論の基礎』
[2] 甘利俊一『情報理論』
[3] Claude E. Shannon "A mathematical Theory of Communication" (1948)