

信州大学工学部

学士論文

雑音のない一般通信路符号化におけるコスト制約付き
通信路容量について

指導教員 西新 幹彦 准教授

学科 電子情報システム工学科
学籍番号 20T2156C
氏名 村岡 和奏

2024 年 4 月 29 日

目次

1	はじめに	1
2	先行研究	1
2.1	定常無記憶情報源のコスト付き固定長符号化	1
2.2	コスト制約付き通信路符号化	2
3	復号誤りが漸近的にゼロになる雑音のない一般通信路のコスト制約付き通信路 容量	5
4	まとめ	12
	謝辞	12
	参考文献	12
	付録 A 補題の証明	13

1 はじめに

インターネットやモバイル通信は急速な発展を遂げ、日本だけでなく、世界中で生活インフラの基盤となっている。さらなる進展に伴い、通信の高速化、大容量化、高信頼化などの需要に応えるべく進歩を続ける技術の一つに通信システムがあげられる。通信システムとは符号語の送受信によって情報を伝えるシステムであり、目的によって二つの符号化に分けられる。一つ目が情報をより効率良く符号化し、小さいデータで情報を送る情報源符号化である。二つ目が誤りをできるだけ小さくし、通信の信頼性の向上を達成する通信路符号化である。

本研究では通信路符号化の問題を考える。通信路符号化問題では情報の送り手と受け手の存在を前提とし、送り手が送ったメッセージを受け手が正しく受け取るために必要な伝送レートや復号誤り確率を求める。そのように通信をする際、すなわち、符号シンボルが通信路を通る際、一般にコストがかかる。具体的には、情報を伝達するための電力や受信までの時間がコストとされ、かかるコストは形式的にはコスト関数によって表される。その上で、符号シンボルの通信コストに上限を設け、その制約内での最適な符号化、および、符号化定理を求める問題をコスト制約付き通信路符号化問題と呼ぶ。コスト付き符号化問題は符号長のコストへの単なる一般化になっているだけでなく、情報源符号化の周辺の種々の問題に登場することが分かっている [2]。また、雑音のある通信路の符号化や符号化定理も先行研究により解明されており [1]、雑音のない通信路においてもコスト付き符号化問題として定理が示されている [2]。

本研究では雑音のない場合の符号化定理を証明した。雑音がない場合は雑音がある場合の特別な場合なので、成立する定理自体は自明である。本研究の狙いは、雑音がないという条件を使って定理を証明することによって、雑音のない場合の良い符号の構成方法に関して知見を得ることである。

2 先行研究

はじめに本研究の先行研究となる様々な条件における符号化について復習する。本論文で扱う底の明記されていない対数は自然対数である。

2.1 定常無記憶情報源のコスト付き固定長符号化

本研究で扱うのは通信路符号化の問題であるが、雑音のない通信路の問題は情報源符号化の問題と関連が深い。よってこの節では、コスト付き情報源符号化に関してすでに知られていることを確認する。

定常無記憶情報源とは $X_1, X_2, \dots$ が独立で同一の分布に従うような確率過程 $(X_1, X_2, \dots)$

のことである。各 $n = 1, 2, \dots$ に対して、整数の集合 $\mathcal{M}_n = \{1, 2, \dots, M_n\}$ を定めておく、長さ n の出力 $\mathbf{x} \in \mathcal{X}^n$ を集合 $\mathcal{M}_n$ のいずれかの要素に変換する操作を符号化といい、この変換を表す写像 $\varphi_n : \mathcal{X}^n \rightarrow \mathcal{M}_n$ を符号化関数という。ここで、 $\varphi_n(\mathbf{x})$ は $\mathbf{x}$ の符号語と呼ばれている。次に、符号語 $m = \varphi_n(\mathbf{x})$ を受け取った受信者はこれからもとの出力系列 $\mathbf{x}$ を復元しようとする。この操作を復号化といい、この変換を表す写像 $\psi_n : \mathcal{M}_n \rightarrow \mathcal{X}^n$ を復号化関数という。ここで復号された結果は必ずしも元の情報源系列に一致しなくともよい。そのとき情報源からの長さ n の系列を確率変数 $X^n = (X_1, \dots, X_n)$ とおき

$$\varepsilon_n \triangleq \Pr\{X^n \neq \psi_n(\varphi_n(X^n))\} \quad (1)$$

を誤り確率と呼ぶ。復号誤りが起こると精度の高い通信ではなくなるため、誤り確率 ε_n は小さければ小さいほどよいが、そのためには符号語数 M_n がある程度大きくなければならない。そこで、その大きさを定量的に表す量を定義する必要がある。それを表す量として

$$r_n \triangleq \frac{1}{n} \log M_n \quad (2)$$

を考え符号化レートと呼ぶ [1]。この符号化レートが小さければ小さいほど通信効率が良くなり、高速な通信が可能になるが、すると誤り確率が大きくなってしまうという相反関係にある。

ここにさらに、コストの概念を導入する。一般に、 $n = 1, 2, \dots$ に対して、写像 $c_n : \mathcal{X}^n \rightarrow \mathbb{R}$ が与えられているとし、

$$\mathbf{c} = \{c_n\}_{n=1}^{\infty} \quad (3)$$

とおく。ただし、 $\mathbb{R}$ は実数全体の集合を表す。このとき、 $\mathbf{x} \in \mathcal{X}^n$ に対して $c_n(\mathbf{x})$ を $\mathbf{x}$ のコストと呼び、 $\frac{1}{n}c_n(\mathbf{x})$ を 1 文字当りの $\mathbf{x}$ のコストという。ここで、コスト t で送信可能な系列の総数を $N(t)$ によって表し、単位コストあたりに送信できるビット数をコスト容量とし、

$$\alpha_c \triangleq \lim_{t \rightarrow \infty} \frac{\log_2 N(t)}{t} \quad (4)$$

と定義する。定常無記憶情報源がエントロピー H を有するとき、任意の $\varepsilon > 0$ に対し、単位記号当たりの平均コストが $H/\alpha_c + \varepsilon$ 以下になるように情報源からの出力系列を符号化することが可能である。また逆に、単位記号当たりの平均コストを H/α_c より真に小さくするように情報源からの出力系列を符号化することは不可能である [2]。

2.2 コスト制約付き通信路符号化

この節ではコスト制約付き通信路符号化問題の基本について確認する。まず、定常無記憶通信路における符号化について述べる。通信路の入出力アルファベットをそれぞれ $\mathcal{X}, \mathcal{Y}$ とす

る。通信路は条件付き確率の組 $\{W(y|x)\}_{x \in \mathcal{X}, y \in \mathcal{Y}}$ によって表される。すなわち

$$\sum_{y \in \mathcal{Y}} W(y|x) = 1 \quad (\forall x \in \mathcal{X}) \quad (5)$$

を満たす。

入力系列

$$\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathcal{X}^n \quad (6)$$

が与えられたとき出力系列

$$\mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathcal{Y}^n \quad (7)$$

の出現する条件付確率 $W^n(\mathbf{y}|\mathbf{x})$ が

$$W^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n W(y_i|x_i) \quad (8)$$

で与えられる通信路のことを定常無記憶通信路と呼ぶ。伝送すべきメッセージの集合を $\mathcal{M}_n = \{1, 2, \dots, M_n\}$ としたとき、それらを長さ n の通信路入力に変換する写像 $\varphi_n: \mathcal{M}_n \rightarrow \mathcal{X}^n$ を符号化関数と呼ぶ。ここで通信路の受信側では、あらかじめ定めておいた $\mathcal{Y}^n$ の分割

$$\mathcal{Y}^n = \psi_n^{-1}(1) \cup \dots \cup \psi_n^{-1}(M_n) \quad (\psi_n^{-1}(i) \cap \psi_n^{-1}(j) = \emptyset \text{ for } i \neq j) \quad (9)$$

に基づいて、受信語 $\mathbf{y}$ が $\mathbf{y} \in \psi_n^{-1}(m)$ ならば $m \in \mathcal{M}_n$ が送信されてきたものと判定する。ここで、

$$r_n = \frac{1}{n} \log M_n \quad (10)$$

は通信路 1 回当りの伝送情報量を表し符号化レートと呼ばれる。また、通信路符号化における復号の誤り確率 ε_n は

$$\varepsilon_n \triangleq \frac{1}{M_n} \sum_{m=1}^{M_n} W^n(\psi_n^{-1}(m)^c | \varphi_n(m)) \quad (11)$$

と定義される。通信路符号化問題は通常、誤り確率を漸近的にゼロにするような符号器と復号器の組が存在するという条件のもとで符号化レートを最大限どこまで大きく出来るかという形で定式化される。そこで次のように定義する。

定義 1 任意の非負実数 R に対し、レート R が達成可能とは

$$\lim_{n \rightarrow \infty} \varepsilon_n = 0 \quad (12)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R \quad (13)$$

を満たすような符号の列 $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ が存在することである。

定義 2 (通信路容量)

$$C(W) \triangleq \sup\{R \mid R \text{ が達成可能}\}. \quad (14)$$

確率変数 X, Y に対して $I(X; Y)$ を

$$I(X; Y) \triangleq \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P_{XY}(x, y) \log \frac{P_{Y|X}(y|x)}{P_Y(y)} \quad (15)$$

と定義し、 X と Y の間の相互情報量と呼ぶ。相互情報量を用いて、通信路容量は

定理 1

$$C(W) = \sup_X I(X; Y) \quad (16)$$

で与えられる [1].

次に、通信路を定常無記憶とは限らない一般の通信路に拡張したときの符号化を考える。そのために一般の通信路を次のように定義する。すなわち、 W^n を各 $n = 1, 2, \dots$ に対して

$$\sum_{y \in \mathcal{Y}^n} W^n(y|x) = 1 \quad (\forall x \in \mathcal{X}^n) \quad (17)$$

を満たすものとする。それらの系列 $\mathbf{W} = \{W^n\}_{n=1}^{\infty}$ を一般通信路と呼ぶ。

定義 3

$$\underline{I}(\mathbf{X}; \mathbf{Y}) \triangleq \text{p-}\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{W^n(Y^n|X^n)}{P_{Y^n}(Y^n)} \quad (18)$$

ここで、実数値確率変数列 $\{Z_n\}_{n=1}^{\infty}$ に対して

$$\text{p-}\liminf_{n \rightarrow \infty} Z_n \triangleq \sup\{\beta \mid \lim_{n \rightarrow \infty} \Pr\{Z_n \leq \beta\} = 0\} \quad (19)$$

とし、確率的下極限という。

定理 2 任意の通信路 $\mathbf{W}$ に対して、その通信路容量 $C(\mathbf{W})$ は

$$C(\mathbf{W}) = \sup_{\mathbf{X}} \underline{I}(\mathbf{X}; \mathbf{Y}) \quad (20)$$

で与えられる [1]. ここで $\sup_{\mathbf{X}}$ はすべての入力過程 $\mathbf{X}$ にわたる上限を表す。

ここでさらに符号化のコストについて考える。前節の式 (3) で導入したのと同様のコストをここでも導入する。ここではコストは符号語に対して定義される。そのもとで、すべての $n = 1, 2, \dots$ に対してすべての符号語が

$$\frac{1}{n} c_n(\varphi_n(m)) \leq \Gamma \quad (m = 1, 2, \dots, M_n) \quad (21)$$

を満たすような符号を考える。ただし、 Γ は与えられた定数であり、この形の条件をコスト制約 Γ と呼ぶ。

コスト制約付きの通信路符号化問題はコスト制約のない通信路符号化問題と同様に定義できる。

定義 4 非負実数 R, Γ に対し、レート R が Γ -達成可能とは

$$\lim_{n \rightarrow \infty} \varepsilon_n = 0 \quad (22)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R \quad (23)$$

$$\frac{1}{n} c_n(\varphi_n(m)) \leq \Gamma \quad (\forall n \in \mathbb{N}, m = 1, 2, \dots, M_n) \quad (24)$$

を満たすような符号の列 $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ が存在することである。

定義 5 Γ に対して

$$C_s(\Gamma|W) \triangleq \sup\{R | R \text{ が } \Gamma\text{-達成可能}\} \quad (25)$$

を Γ -通信路容量と呼ぶ

Γ -通信路容量の数学的表現のため、

$$\mathcal{X}^n(\Gamma) = \left\{ \mathbf{x} \in \mathcal{X}^n \mid \frac{1}{n} c_n(\mathbf{x}) \leq \Gamma \right\} \quad (26)$$

とにおいて、すべての $n = 1, 2, \dots$ に対して

$$\Pr\{X^n \in \mathcal{X}^n(\Gamma)\} = 1 \quad (27)$$

を満たす入力過程 $\mathbf{X} = \{X^n\}_{n=1}^\infty$ の全体を S_Γ で表すと、定理 2 に対応する次の定理を得る。

定理 3 通信路 W の Γ -通信路容量 $C_s(\Gamma|W)$ は

$$C_s(\Gamma|W) = \sup_{\mathbf{X} \in S_\Gamma} \underline{I}(\mathbf{X}; \mathbf{Y}) \quad (28)$$

で与えられる [1]。ただし、 $\mathbf{Y}$ は $\mathbf{X}$ を入力過程とする通信路 W の出力過程を表す。

3 復号誤りが漸近的にゼロになる雑音のない一般通信路のコスト制約付き通信路容量

本論文の本題として、雑音のない一般通信路を考える。つまり、出力 Y は入力 X に等しい。しかし、符号器と復号器による誤りは許容する。従って、誤り確率 ε_n は

$$\varepsilon_n \triangleq \Pr\{X^n \neq \psi_n(\varphi_n(X^n))\} \quad (29)$$

と定義される．ここで，雑音のない通信路における Γ -達成可能を，2 章と同じく以下のように定義する．

定義 6 非負実数 R, Γ に対し，レート R が Γ -達成可能とは

$$\lim_{n \rightarrow \infty} \varepsilon_n = 0 \quad (30)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R \quad (31)$$

$$\Pr \left\{ \frac{1}{n} c_n(\varphi_n(U_{M_n})) \leq \Gamma \right\} = 1 \quad (32)$$

を満たすような符号の列 $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ が存在することである．

Γ -通信路容量は定義 5 に従って定義するが，通信路に雑音がないので単に $C(\Gamma)$ と表すことにする．

定理 3 は通信路に雑音がない場合も成り立つことから， $\mathbf{X} = \mathbf{Y}$ ならば，定義 3 は

$$\underline{I}(\mathbf{X}; \mathbf{X}) = \text{p-}\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{W^n(X^n | X^n)}{P_{X^n}(X^n)} \quad (33)$$

となり，ここで一般通信路の定義

$$W^n(\mathbf{y} | \mathbf{x}) \triangleq \Pr\{Y^n = \mathbf{y} | X^n = \mathbf{x}\} \quad (\mathbf{x} \in \mathcal{X}, \mathbf{y} \in \mathcal{Y}) \quad (34)$$

より

$$W^n(\mathbf{x} | \mathbf{x}) = \Pr\{X^n = \mathbf{x} | X^n = \mathbf{x}\} \quad (35)$$

$$= 1 \quad (36)$$

となることから

$$\underline{I}(\mathbf{X}; \mathbf{X}) = \text{p-}\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \quad (37)$$

であるが，ここで

$$\underline{H}(\mathbf{X}) \triangleq \text{p-}\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \quad (38)$$

を用いて

$$\underline{I}(\mathbf{X}; \mathbf{X}) = \underline{H}(\mathbf{X}) \quad (39)$$

と書き換えることができる．

これにより，以下の定理が直ちに得られる．

定理 5 Γ -通信路容量 $C(\Gamma)$ は

$$C(\Gamma) = \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\} = 1} \underline{H}(\mathbf{X}) \quad (40)$$

で与えられる.

以下では通信路に雑音がないことを使って定理 5 の証明をする.

[証明]

1) Direct part:

まず, すべての n に対して

$$\Pr\left\{\frac{1}{n}c_n(X^n) \leq \Gamma\right\} = 1 \quad (41)$$

であるような任意の情報源 $\mathbf{X}$ を考える. 次にこの $\mathbf{X}$ に対して,

$$R < \underline{H}(\mathbf{X}) \quad (42)$$

なる任意の R を考える. このとき, ある $\gamma > 0$ に対して,

$$R = \underline{H}(\mathbf{X}) - 2\gamma \quad (43)$$

が成り立つ. この R が Γ -達成可能であることを示す. 準備として

$$\mathcal{T}_n \triangleq \left\{ \mathbf{x} \in \mathcal{X}^n \left| \frac{1}{n} \log \frac{1}{P_{X^n}(\mathbf{x})} > \underline{H}(\mathbf{X}) - \gamma \right. \right\} \quad (44)$$

を定める. $M_n \triangleq e^{nR} = e^{H(\mathbf{X})-2\gamma}$ とおき, $\bar{\varphi}_n(1), \bar{\varphi}_n(2), \dots, \bar{\varphi}_n(M_n) \in \mathcal{X}^n$ を互いに独立に分布 P_{X^n} に従って発生させる. この $\bar{\varphi}_n$ が符号器となる. 次に復号器を定める. 復号器 $\bar{\psi}_n$ は $\mathbf{x} \in \mathcal{X}^n$ を受け取ったとき,

$$\bar{\varphi}_n(m) = \mathbf{x} \quad (45)$$

となるような $m \in \mathcal{M}_n$ がただ一つのとき, $\bar{\psi}_n(\mathbf{x}) = m$ とし, それ以外は誤りとみなす. $m \in \mathcal{M}_n$ が正しく伝わるためには受信語 $\bar{\varphi}_n(m)$ がどの $m' \neq m$ に対しても $\bar{\varphi}_n(m') \neq \bar{\varphi}_n(m)$ であればよい. ここで, 事象 $E(m)$ を

$$E(m) \triangleq \{ \text{ある } m' \neq m \text{ に対して } \bar{\varphi}_n(m') = \bar{\varphi}_n(m) \} \quad (46)$$

と定める. すると, メッセージ m を送信したときの復号誤り確率 $\bar{\varepsilon}_n(m)$ は

$$\bar{\varepsilon}_n(m) = \Pr\{E(m)\} \quad (47)$$

$$= \Pr\{E(m) \text{ かつ } \bar{\varphi}_n(m) \notin \mathcal{T}_n\} + \Pr\{E(m) \text{ かつ } \bar{\varphi}_n(m) \in \mathcal{T}_n\} \quad (48)$$

と表される.

ここで第 2 項は

$$\Pr\{E(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\} \quad (49)$$

$$= \Pr\{\{\text{ある } m' \neq m \text{ に対して } \bar{\varphi}_n(m') = \bar{\varphi}_n(m)\} \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\} \quad (50)$$

$$= \Pr\{\text{ある } m' \neq m \text{ に対して } \{\bar{\varphi}_n(m') = \bar{\varphi}_n(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\}\} \quad (51)$$

$$= \Pr\left\{\bigcup_{m' \neq m} \{\bar{\varphi}_n(m') = \bar{\varphi}_n(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\}\right\} \quad (52)$$

$$\leq \sum_{m' \neq m} \Pr\{\bar{\varphi}_n(m') = \bar{\varphi}_n(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\} \quad (53)$$

であり, 和の中は

$$\Pr\{\bar{\varphi}_n(m') = \bar{\varphi}_n(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n\} \quad (54)$$

$$= \sum_{\mathbf{x}} \Pr\{\bar{\varphi}_n(m') = \bar{\varphi}_n(m) \text{ か } \bar{\varphi}_n(m) \in \mathcal{T}_n \text{ か } \bar{\varphi}_n(m) = \mathbf{x}\} \quad (55)$$

$$= \sum_{\mathbf{x}} \Pr\{\bar{\varphi}_n(m') = \mathbf{x}\} \cdot \Pr\{\bar{\varphi}_n(m) \in \mathcal{T}_n \text{ か } \bar{\varphi}_n(m) = \mathbf{x}\} \quad (56)$$

$$= \sum_{\mathbf{x}} \Pr\{X^n = \mathbf{x}\} \cdot \Pr\{X^n \in \mathcal{T}_n \text{ か } X^n = \mathbf{x}\} \quad (57)$$

$$= \sum_{\mathbf{x}} P_{X^n}(\mathbf{x}) \cdot \Pr\{\mathbf{x} \in \mathcal{T}_n \text{ か } X^n = \mathbf{x}\} \quad (58)$$

$$= \sum_{\mathbf{x}} P_{X^n}(\mathbf{x}) \cdot \Pr\{X^n = \mathbf{x}\} \cdot \mathbb{1}\{\mathbf{x} \in \mathcal{T}_n\} \quad (59)$$

$$= \sum_{\mathbf{x} \in \mathcal{T}_n} P_{X^n}(\mathbf{x}) \cdot P_{X^n}(\mathbf{x}) \quad (60)$$

と書き換えることができる. そこで, $\mathbf{x} \in \mathcal{T}_n$ より,

$$\frac{1}{n} \log \frac{1}{P_{X^n}(\mathbf{x})} > \underline{H}(\mathbf{X}) - \gamma \quad (61)$$

$$\log \frac{1}{P_{X^n}(\mathbf{x})} > n(\underline{H}(\mathbf{X}) - \gamma) \quad (62)$$

$$\frac{1}{P_{X^n}(\mathbf{x})} > e^{n(\underline{H}(\mathbf{X}) - \gamma)} \quad (63)$$

$$P_{X^n}(\mathbf{x}) < e^{-n(\underline{H}(\mathbf{X}) - \gamma)} \quad (64)$$

であり, これを 式 (60) に代入すると,

$$\sum_{\mathbf{x} \in \mathcal{T}_n} P_{X^n}(\mathbf{x}) \cdot P_{X^n}(\mathbf{x}) < \sum_{\mathbf{x} \in \mathcal{T}_n} P_{X^n}(\mathbf{x}) \cdot e^{-n(\underline{H}(\mathbf{X}) - \gamma)} \quad (65)$$

$$\leq 1 \cdot e^{-n(\underline{H}(\mathbf{X}) - \gamma)} \quad (66)$$

となる．これにより式 (48) は

$$\bar{\varepsilon}_n(m) \leq \Pr\{\bar{\varphi}_n(m) \notin \mathcal{T}_n\} + \sum_{m' \neq m} e^{-n(\underline{H}(\mathbf{X})-\gamma)} \quad (67)$$

$$= \Pr\{X^n \notin \mathcal{T}_n\} + (M_n - 1)e^{-n(\underline{H}(\mathbf{X})-\gamma)} \quad (68)$$

$$< \Pr\{X^n \notin \mathcal{T}_n\} + M_n e^{-n(\underline{H}(\mathbf{X})-\gamma)} \quad (69)$$

$$= \Pr\{X^n \notin \mathcal{T}_n\} + e^{n(\underline{H}(\mathbf{X})-2\gamma)-n(\underline{H}(\mathbf{X})-\gamma)} \quad (70)$$

$$= \Pr\{X^n \notin \mathcal{T}_n\} + e^{-n\gamma} \quad (71)$$

となる．ここで $\bar{\varepsilon}_n(m)$ は $m \in \mathcal{M}_n$ に依存しない値で上から押さえられるため，平均復号誤り確率 $\bar{\varepsilon}_n$ は

$$\lim_{n \rightarrow \infty} \bar{\varepsilon}_n = \lim_{n \rightarrow \infty} \frac{1}{M_n} \sum_{m=1}^{M_n} \bar{\varepsilon}_n(m) \quad (72)$$

$$\leq \lim_{n \rightarrow \infty} (\Pr\{X^n \notin \mathcal{T}_n\} + e^{-n\gamma}) \quad (73)$$

$$= 0 \quad (74)$$

となる．ただし式 (74) では大数の法則 [1] を用いた．

一方符号語のコストは

$$\Pr\left\{\frac{1}{n}c_n(\bar{\varphi}_n(U_{M_n})) \leq \Gamma\right\} = \sum_{m=1}^{M_n} \Pr\left\{\frac{1}{n}c_n(\bar{\varphi}_n(U_{M_n})) \leq \Gamma, U_{M_n} = m\right\} \quad (75)$$

$$= \sum_{m=1}^{M_n} \Pr\left\{\frac{1}{n}c_n(\bar{\varphi}_n(m)) \leq \Gamma, U_{M_n} = m\right\} \quad (76)$$

$$= \sum_{m=1}^{M_n} \Pr\left\{\frac{1}{n}c_n(\bar{\varphi}_n(m)) \leq \Gamma\right\} \cdot \Pr\{U_{M_n} = m\} \quad (77)$$

$$= \frac{1}{M_n} \sum_m \Pr\left\{\frac{1}{n}c_n(X^n) \leq \Gamma\right\} \quad (78)$$

$$= 1 \quad (79)$$

より，ここで発生させた符号は必ずコスト制約（式 (32)）を満たす．ここで U_M は M 以下の自然数上に一様に分布する確率変数とする．

ところが， $\bar{\varepsilon}_n$ はランダム符号のすべてにわたる平均値であったので，誤り確率 ε_n が $\varepsilon_n \leq \bar{\varepsilon}_n$ となるようなランダムでない符号 (φ_n, ψ_n) が少なくとも 1 つ存在する．

ここで (φ_n, ψ_n) の符号化レートは

$$\frac{1}{n} \log M_n = \frac{1}{n} \log e^{nR} \quad (80)$$

$$= R \quad (81)$$

であり、式 (74), 式 (79) より, この符号 (φ_n, ψ_n) は

$$\lim_{n \rightarrow \infty} \varepsilon_n = 0 \quad (82)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R \quad (83)$$

$$\Pr \left\{ \frac{1}{n} c_n(\bar{\varphi}_n(U_{M_n})) \leq \Gamma \right\} = 1 \quad (84)$$

を満たす. よってレート R は Γ -達成可能である. このことから, $C(\Gamma) \geq R = \underline{H}(\mathbf{X}) - 2\gamma$ が成り立つが, $\mathbf{X}$ は式 (41) を満たす任意の情報源であったので,

$$C(\Gamma) \geq \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) - 2\gamma \quad (85)$$

が成り立つ. ここで $\gamma > 0$ は任意だったことに注意すれば,

$$C(\Gamma) \geq \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) \quad (86)$$

が得られる.

2) Converse part:

背理法によって

$$C(\Gamma) \leq \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) \quad (87)$$

を示す. そこで

$$R = \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) + 3\gamma \quad (88)$$

が Γ 達成可能であるとして矛盾を導く. ただし, $\gamma > 0$ は任意に小さい定数である.

R が Γ -達成可能であるから,

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log M_n \geq R \quad (89)$$

$$\lim_{n \rightarrow \infty} \varepsilon_n = 0 \quad (90)$$

$$\Pr \left\{ \frac{1}{n} c_n(\varphi_n(U_{M_n})) \leq \Gamma \right\} = 1 \quad (91)$$

なる符号の列 $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ が存在することになる.

そこで, $X^n = \varphi_n(U_{M_n})$ とすれば, 付録 A にある補題により

$$\varepsilon_n \geq \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \frac{1}{n} \log M_n - \gamma \right\} - e^{-n\gamma} \quad (92)$$

である。一方、式 (89) より

$$\frac{1}{n} \log M_n \geq R - \gamma \quad (\forall n \geq n_0) \quad (93)$$

が得られ、これを式 (92) に代入すると

$$\varepsilon_n \geq \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq R - 2\gamma \right\} - e^{-n\gamma} \quad (\forall n \geq n_0) \quad (94)$$

となる。ここで式 (88) より

$$R - 2\gamma = \sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) + \gamma \quad (95)$$

であるが、今考えている $X^n = \varphi_n(U_{M_n})$ は式 (91) を満たすので

$$\sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X}) + \gamma \geq \underline{H}(\mathbf{X}) + \gamma \quad (96)$$

となる。したがって式 (94) は

$$\varepsilon_n \geq \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \underline{H}(\mathbf{X}) + \gamma \right\} - e^{-n\gamma} \quad (97)$$

となる。ここで $\underline{H}(\mathbf{X})$ の定義は

$$\underline{H}(\mathbf{X}) \triangleq \text{p-}\liminf_{n \rightarrow \infty} \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \quad (98)$$

$$\triangleq \sup \left\{ \beta \mid \lim_{n \rightarrow \infty} \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \beta \right\} = 0 \right\} \quad (99)$$

である。したがって $\alpha = \underline{H}(\mathbf{X}) + \gamma$ を用いて

$$\lim_{n \rightarrow \infty} \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \alpha \right\} \neq 0 \quad (100)$$

$$\limsup_{n \rightarrow \infty} \Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \alpha \right\} > \exists \delta > 0 \quad (101)$$

$$\Pr \left\{ \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \alpha \right\} > \delta > 0 \quad (\exists n \geq \forall n_0) \quad (102)$$

となることから式 (97) は

$$\varepsilon_n \geq \delta - e^{-n\gamma} \quad (103)$$

となる。つまり式 (103) となる n が可算無限個存在することから、 $\varepsilon_n \rightarrow 0 (n \rightarrow \infty)$ とはなれない。これは式 (90) に矛盾する。よって、達成可能なレート R は $\sup_{\mathbf{X}: \Pr\{\frac{1}{n} c_n(X^n) \leq \Gamma\}=1} \underline{H}(\mathbf{X})$ より大きくなれない。□

4 まとめ

本研究では、雑音のない一般通信路の固定長通信路符号化におけるコスト制約付き通信路容量の証明をした。

雑音がないことから送り手が送った符号シンボルが誤ることなく受け手に届くということを再定義し、証明を進めるなかで、雑音のない通信路は雑音のある通信路の特別な条件であるため、同じ証明で導けると考えたが、雑音のない通信路の特別な証明が必要だった。

今後は本研究で定義した補題で用いた証明方法を活用して、雑音のない一般通信路の可変長通信路符号化におけるコスト制約付き通信路容量を考え、固定長通信路符号化との関係を考察するとともに、情報源符号化と通信路符号化の関係にも検討していきたい。

謝辞

本研究を進めるにあたり、丁寧なご指導を頂いた西新幹彦准教授に感謝の意を表する。

参考文献

- [1] 韓太舜, 情報理論における情報スペクトル的方法, 培風館, 1998.
- [2] 植松友彦, 「情報源のコスト付き符号化とその応用」, 電子情報通信学会, 論文誌, no.5, pp.558–590, May 2004.

付録 A 補題の証明

ここでは次の補題を証明する.

補題 符号 $\varphi_n(\mathcal{M}_n)$ 上の一様分布に従う確率変数を X^n とし, 各 $n = 1, 2, \dots$ に対して

$$\varepsilon_n \geq \Pr\left\{\frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} \leq \frac{1}{n} \log M_n - \gamma\right\} - e^{-n\gamma} \quad (104)$$

が成立する.

[証明] 証明を始めるにあたり

$$L_n \triangleq \left\{\mathbf{x} \left| \frac{1}{n} \log \frac{1}{P_{X^n}(\mathbf{x})} \leq \frac{1}{n} \log M_n - \gamma \right.\right\} \quad (105)$$

とおく. これらを用いると, 式 (104) は

$$\varepsilon_n \geq \Pr\{X^n \in L_n\} - e^{-n\gamma} \quad (106)$$

と書き換えられる. これを示すために, 正しく復号されるメッセージの集合を $D = \{m \in \mathcal{M}_n | \psi_n(\varphi_n(m)) = m\}$ とすると,

$$\Pr\{X^n \in L_n\} = \sum_{m=1}^{M_n} \Pr\{X^n \in L_n, U_{M_n} = m\} \quad (107)$$

$$= \sum_{m=1}^{M_n} \Pr\{\varphi_n(U_{M_n}) \in L_n, U_{M_n} = m\} \quad (108)$$

$$= \sum_{m=1}^{M_n} \Pr\{\varphi_n(m) \in L_n, U_{M_n} = m\} \quad (109)$$

$$= \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n\} \cdot \Pr\{U_{M_n} = m\} \quad (110)$$

$$= \frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n\} \quad (111)$$

$$= \frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \notin D\} + \frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} \quad (112)$$

となる．ここで，第1項は，

$$\frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \notin D\} \leq \frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{m \notin D\} \quad (113)$$

$$= \frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\psi_n(\varphi_n(m)) \neq m\} \quad (114)$$

$$= \varepsilon_n \quad (115)$$

となる．また，第2項は，

$$\frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} = \sum_{m=1}^{M_n} \frac{1}{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} \quad (116)$$

となる．ここで $\mathbf{x} \in L_n$ のとき

$$\frac{1}{n} \log \frac{1}{P_{X^n}(\mathbf{x})} \leq \frac{1}{n} \log M_n - \gamma \quad (117)$$

$$\log \frac{1}{P_{X^n}(\mathbf{x})} \leq \log M_n - n\gamma \quad (118)$$

$$\log \frac{1}{P_{X^n}(\mathbf{x}) \cdot M_n} \leq -n\gamma \quad (119)$$

$$\frac{1}{P_{X^n}(\mathbf{x}) \cdot M_n} \leq e^{-n\gamma} \quad (120)$$

$$\frac{1}{M_n} \leq P_{X^n}(\mathbf{x}) \cdot e^{-n\gamma} \quad (121)$$

であるが， $\varphi_n(m) \in L_n$ なので

$$\frac{1}{M_n} \leq P_{X^n}(\varphi_n(m)) \cdot e^{-n\gamma} \quad (122)$$

である．よって，式(116)は

$$\frac{1}{M_n} \sum_{m=1}^{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} = \sum_{m=1}^{M_n} \frac{1}{M_n} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} \quad (123)$$

$$\leq \sum_{m=1}^{M_n} P_{X^n}(\varphi_n(m)) e^{-n\gamma} \mathbb{1}\{\varphi_n(m) \in L_n, m \in D\} \quad (124)$$

$$\leq e^{-n\gamma} \sum_{m=1}^{M_n} P_{X^n}(\varphi_n(m)) \mathbb{1}\{m \in D\} \quad (125)$$

$$= e^{-n\gamma} \sum_{m \in D} P_{X^n}(\varphi_n(m)) \quad (126)$$

$$\leq e^{-n\gamma} \quad (127)$$

となる．ただし最後の不等式は， $m \in D$ に対して $\varphi_n(m)$ はすべて異なるためである．したがって

$$\Pr\{X^n \in L_n\} \leq \varepsilon_n + e^{-n\gamma} \quad (128)$$

となる．よって式 (104) が示された．□