Slepian-Wolf符号化問題に関する研究動向

- 佐藤創先生のご退職に寄せて-

Recent Development on Slepian-Wolf Coding Problem

ネットワーク情報学部　野村亮
School of Network and Information　Ryo Nomura

Keywords: Information Theory, Source Coding, Slepian-Wolf Coding

1　はじめに

著者が初めて佐藤創先生の名前を知ったのは，大学院生時代に韓太舜先生（当時専修大, 現情報通信研究機構 (NICT)）と佐藤先生との共同研究である "Feedback Codes with Uniformly Bounded Codeword Length and Zero-Error Capacities"[1] という論文を読んだのが最初と思う．この論文の掲載された IEEE Transaction on Information Theory という雑誌は情報理論界で世界的かつ最も "権威"のある雑誌とされており，必然掲載基準も非常に厳しい．情報理論の研究者にとってこの雑誌に論文が掲載されることは世界的な研究者として認められたことを意味し，スポーツの世界で言えばワールドカップ，オリンピックに出場するのと等しい価値を持っていると言えるだろう．当時の専修大学における情報理論研究のレベルの高さがうかがい知れる．

さて，日本の情報理論研究の一端は 2012 年で第 35 回を数える「情報理論とその応用シンポジウム」（第 7 回までは情報理論とその応用研究会研究討論会という名称）が支えてきた．同シンポジウムは年に一回（温泉地で）開催されるので第 1 回の研究討論会は実に 34 年前のことである．当時の予稿集を紐解けば今では情報理論界の大御所の名前が散見されるが，佐藤創先生の名前も第 4 回から登場する．第 4 回の討論会では "多重情報源に対する可変長符号化について" [2] というタイトルで，第 5 回の討論会では "補助情報源を持つ誤りなし可変長符号化について" [3] というタイトルで発表されている．どちらも複数の相関を持った情報源から出力されるデータを個別に圧縮する問題，いわゆる相関を持った情報源に対する情報源符号化問題の一つである．相関を持った情報源に対する情報源符号化問題は，1973 年に発表された Slepian と Wolf の共著論文 "Noiseless coding of correlated information sources" [4] に端を発する．同論文は IEEE Information Theory Society の論文賞を受賞した論文であり，多数のユーザが関わる多元情報理論と呼ばれる分野の幕開けを告げたものである．今でこそセンサネットワーク，MIMO 通信など幅広い分野の基礎となり，実用の観点からの重要性も認められている多元情報理論であるが，当時はどこに応用できるともわからない，数学としては面白いが実用性がないと批判されていたとも聞く．佐藤創先生はこのような背景の中で前述の通りいち早くこの分野の研究に取り組んでおり，その先見の明に驚かされる．

Slepian と Wolf の提案した問題設定は Slepian-Wolf 符号化システム，Slepian-Wolf 符号化問題等と呼ばれ現在でもなお重要な研究対象の一つである．本稿では，Slepian-Wolf 符号化システムの問題設定から現在の研究成果まで概観したい．

2　Slepian-Wolf 符号化システム

本章では，Slepian-Wolf 符号化システムを定義する．Slepian-Wolf 符号化システムは互いに相関を有する二つのデータ列を別々に圧縮符号化する場合を対象としている．よくある例としては，映像の RGB の出力を別々に符号化する．あるいはある事象をそれぞれ別の場所にある二つのカメラで観測し，そのデータを別々にセンターに送るなどである．後者の場合二つのカメラで別の場所から測定しているのでデータ自体は異なったものである．しかし，それぞれのデータには強い相関性があると考えられる．二つのデータを別々に圧縮する際にこの相関性を利用することにより，圧縮利得を稼ぐことができるというのが

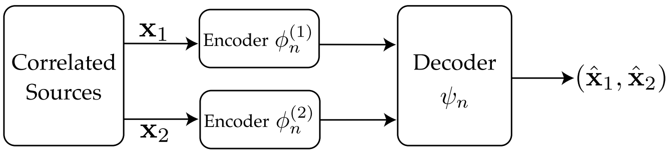

図 1　Slepian-Wolf 符号化システム

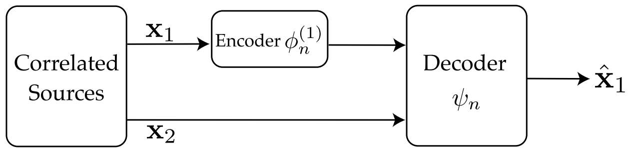

図 2　補助情報を伴う符号化システム

Slepian と Wolf の主張である．以降この問題を数理モデル化した上で考えていく．

2.1　相関を有する情報源

情報理論では圧縮対象のデータ列を確率変数とし，その確率変数列の集合を情報源と呼び

$$\mathbf{X} = \left\{ X^n = (X_1^{(n)}, X_2^{(n)}, \cdots, X_n^{(n)}) \right\}_{n=1}^{\infty}$$

と表す．X^n は集合 $\mathcal{X}$(情報源アルファベットと呼ぶ) の直積 $\mathcal{X}^n$ の中に値を取る確率変数でその確率分布を P_{X^n} と書く．情報理論の分野では P_{X^n} に対して，様々な確率分布を仮定するが，本稿では一般情報源と定常無記憶情報源（i.i.d. 情報源）を取り扱う．一般情報源とは，定常性やエルゴード性を仮定しないだけでなく次式で表される整合性条件すら仮定しない極めて一般的な情報源である [5].

$$X_i^{(m)} \equiv X_i^{(n)} \quad (i = 1, 2, \cdots, m; m < n). \tag{1}$$

前述のように Slepian-Wolf 符号化システムでは二つの相関を有するデータ列を考えるので相関を有する二つの一般情報源 $(\mathbf{X}_1, \mathbf{X}_2) = \{(X_1^n, X_2^n)\}_{n=1}^{\infty}$ を考えることになる．$\mathcal{X}_1$ と $\mathcal{X}_2$ をそれぞれの情報源アルファベットとする．$\mathcal{X}_1$ と $\mathcal{X}_2$ は，一般的に加算無限集合としておく．なお，$\mathbf{x}_j = x_{j1}, x_{j2}, \cdots, x_{jn}$ を確率変数 X_j^n $(j = 1, 2)$ の実現値とし，$(\mathbf{x}_1, \mathbf{x}_2)$ の出現確率を $P_{X_1^n X_2^n}(\mathbf{x}_1, \mathbf{x}_2)$ と書く．

特に，この情報源ペアが定常無記憶性を有するとき，i.i.d. 情報源と呼び，次のように書くことができる．

$$P_{X_1^n X_2^n}(\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} P_{X_1 X_2}(x_{1i}, x_{2i}).$$

2.2　Slepian-Wolf 符号化システム

上で与えられる二つの情報源からの出力をそれぞれ別々に（圧縮）符号化したのちに同じ受信機へ送信，受信側はこれら二つのデータをそれぞれ復元（復号）することを考える（図 1）．

二つの符号化器は二つの写像 $\phi_n^{(1)}$, $\phi_n^{(2)}$，復号化も写像 ψ_n と考えることができる．ここで二つの符号化器は，情報源の同時確率分布 $P_{X_1^n X_2^n}$ は知っているが，実際にどのデータ列が出力されたかについては自分に入ってくるものしか分からないとする．すなわち相手の圧縮対象データ列を観測できない状況である．なお，この問題設定の特別な場合として図 2 のように片方の情報源からの出力 $X_2^n = \mathbf{x}_2$ は確実に復元できる状況を考えることができる．この場合，$\mathbf{x}_2$ は $\mathbf{x}_1$ を特定するための補助的なものと考えるわけである．この問題は補助情報を伴う情報源符号化，補助情報源を持つ符号化等と呼ばれる．[3] はこちらの問題を主に取り扱っている．

Slepian-Wolf 符号化システムは符号化方式の違いにより大きく二種類に分類できる．それぞれ固定長情報源符号化と可変長情報源符号化と呼ぶ．

2.2.1　固定長情報源符号化

各符号化器 $\phi_n^{(i)}(i = 1, 2)$ に対して整数の集合 $\mathcal{M}_n^{(i)} = \{1, 2, \cdots, M_n^{(i)}\}$ を用意しておき，情報源からの出力を $\mathcal{M}_n^{(i)}$ のいずれかに変換する．すなわち，符号化器は

$$\phi_n^{(1)} : \mathcal{X}_1^n \to \mathcal{M}_n^{(1)}, \quad \phi_n^{(2)} : \mathcal{X}_2^n \to \mathcal{M}_n^{(2)}$$

のような写像と定義できる．ある情報源からの出力 $\mathbf{x}_1$ に対する符号化器の出力 $\phi_n^{(1)}(\mathbf{x}_1)$ は $\mathbf{x}_1$ に対する符号語と呼ばれる．

受信側は二つの符号語 $\left(\phi_n^{(1)}(\mathbf{x}_1), \phi_n^{(2)}(\mathbf{x}_2)\right)$ を受け取り，元々の情報源系列 $\mathbf{x}_1, \mathbf{x}_2$ の復元を試みる（これを復号化という）．復号化器 ψ_n は次で定義される．

$$\psi_n : \mathcal{M}_n^{(1)} \times \mathcal{M}_n^{(2)} \to \mathcal{X}_1^n \times \mathcal{X}_2^n.$$

注意 2.1 この符号化が固定長情報源符号化と呼ばれる理由は次の通りである．例えば符号化器 $\phi_n^{(1)}$ により変換された $j \in \{1, 2, \cdots, M_n^{(1)}\}$ を送信するために，必要な文字の集合 $\mathcal{U}_1$（これを符号アルファベットと呼ぶ）を考えると

$$\lceil \log_{|\mathcal{U}_1|} M_n^{(1)} \rceil$$

の長さを持った $\mathcal{U}$ の文字列に変換してやれば良いことが分かる．ここで $\lceil y \rceil$ とは y 以上の最小の整数を意味する．

例えば，$\mathcal{U}_1 = \{0, 1\}$ を考えると $\lceil \log_2 M_n^{(1)} \rceil$ ビット必要となる．別の言い方をすれば情報源からの出力を全て

$\lceil \log_{|\mathcal{U}|} M_n^{(1)} \rceil$ の長さで送信することになる．これが本符号化方式を固定長情報源符号化と呼ぶ所以である．なお，煩雑さを避けるために

$$\lceil \log_{|\mathcal{U}_1|} M_n^{(1)} \rceil \approx \log_{|\mathcal{U}_1|} M_n^{(1)}$$

として考えることが多い．

さて固定長情報源符号化においては

$$M_n^{(1)} < |\mathcal{X}_1^n|, \quad M_n^{(2)} < |\mathcal{X}_2^n|$$

なる状況を考える．なぜならば $M_n^{(1)} \geq |\mathcal{X}_1^n|$ であれば $\mathbf{x}_1$ を圧縮したことにならないからである．しかしながらこの状況では復号化器で完全に元の系列を復元できる保証はない．元の系列の復元に失敗する事象を“誤り”と呼ぶ．固定長情報源符号化ではこの誤りの生じる確率（誤り確率）をなるべく小さくする必要がある．上の議論から $M_n^{(1)}, M_n^{(2)}$ が大きければ大きいほど誤り確率は小さくできそうなことが直感的に分かる．実際 $M_n^{(1)} = |\mathcal{X}_1^n|, \quad M_n^{(2)} = |\mathcal{X}_2^n|$ とすれば誤り無しで送信できる．ただし全く圧縮しない．

一方で圧縮効率を上げるためには $M_n^{(1)}, M_n^{(2)}$ を小さくすれば良いわけである（注意 2.1 参照）．

まとめると固定長情報源符号化の問題とは，誤り確率の観点から $M_n^{(1)}, M_n^{(2)}$ を大きくしたい一方で圧縮率の観点からは $M_n^{(1)}, M_n^{(2)}$ を小さくしたいという二律背反の問題を対象としている．

2.2.2 可変長情報源符号化

可変長情報源符号化とは符号化後の長さ（符号語長）が圧縮対象のデータ列に依存して変化する符号化方式である．形式的に言えば，各符号アルファベットを $\mathcal{U}_i (i = 1, 2)$ としたとき

$$\phi_n^{(1)} : \mathcal{X}_1^n \to \mathcal{U}_1^* \quad \phi_n^{(2)} : \mathcal{X}_2^n \to \mathcal{U}_2^*$$

とする符号化のことである．ここで $\mathcal{U}_i^*$ は $\mathcal{U}_i$ のすべての有限文字列の集合を表す（ただし長さ 0 の文字列 Λ は含まない）．復号化器は

$$\psi_n : \mathcal{U}_1^* \times \mathcal{U}_2^* \to \mathcal{X}_1^n \times \mathcal{X}_2^n.$$

となる．この場合，通常は誤り確率を任意の n に対して 0 にする符号化器，復号化器を作成することを対象とする．（これを 0 誤りと呼ぶ．）

Slepian-Wolf 符号化システムにおける 0 誤り可変長情報源符号化の解析は困難であまり進んでいない．本稿でも主に固定長情報源符号化を対象とする．

3 定常無記憶情報源に対する結果

3.1 達成可能領域の評価

上で述べたように固定長情報源符号化を考えた場合，符号語のサイズ $M_n^{(1)}, M_n^{(2)}$ と誤り確率はトレードオフである．そこで十分長いデータ列に対して誤り確率

$$\varepsilon_n = \Pr\{(X_1^n, X_2^n) \neq \psi_n(\phi_n^{(1)}(X_1^n), \phi_n^{(2)}(X_2^n))\}.$$

を任意に小さくできるという制約を考え，この制約のもとで $\log M_n^{(1)}, \log M_n^{(2)}$ をどこまで小さくできるかという問題を考える．$M_n^{(1)}, M_n^{(2)}$ でなく $\log M_n^{(1)}, \log M_n^{(2)}$ を考えるのは符号化後の長さ（符号長）を考えるからである（注意 2.1）．

この問題を初めて考えたのが他ならぬ Slepian と Wolf であり，次の様に定式化される．ここで符号語のサイズがそれぞれ $M_n^{(1)}, M_n^{(2)}$ のとき誤り確率が ε_n となる符号化器，復号化器のセットを $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号と呼ぶことにする．

定義 3.1 次を満たす $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号が存在するとき，レートペア (R_1, R_2) を達成可能と呼ぶ．

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n^{(1)} \leq R_1, \ \limsup_{n\to\infty} \frac{1}{n} \log M_n^{(2)} \leq R_2$$
$$\lim_{n\to\infty} \varepsilon_n = 0.$$

我々が興味があるのはどのようなレートペア (R_1, R_2) であれば達成可能であるかということである:

定義 3.2 (達成可能領域)

$$R(\mathbf{X}_1, \mathbf{X}_2) = \{(R_1, R_2) | (R_1, R_2) \text{ は達成可能 }\}.$$

Slepian と Wolf の得た結果は次の通りである．

定理 3.1 (Slepian and Wolf [4]) 任意の有限アルファベットを持つ定常無記憶情報源に対して次が成り立つ．

$$\begin{aligned} &R(\mathbf{X}_1, \mathbf{X}_2) \\ &= \{(R_1, R_2) \,|\, R_1 \geq H(X_1|X_2), R_2 \geq H(X_2|X_1), \\ &\quad R_1 + R_2 \geq H(X_1X_2)\}. \end{aligned}$$

ここで $H(X_1|X_2)$ と $H(X_2|X_1)$ は条件付きエントロピー，$H(X_1X_2)$ は同時エントロピーと呼ばれ下記で定義される情報源の性質を表す量である．

$$\begin{aligned} &H(X_1|X_2) \\ &= \sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{X}_1^n\times\mathcal{X}_2^n} P_{X_1X_2}(\mathbf{x}_1, \mathbf{x}_2) \log \frac{1}{P_{X_1|X_2}(\mathbf{x}_1|\mathbf{x}_2)}, \end{aligned}$$

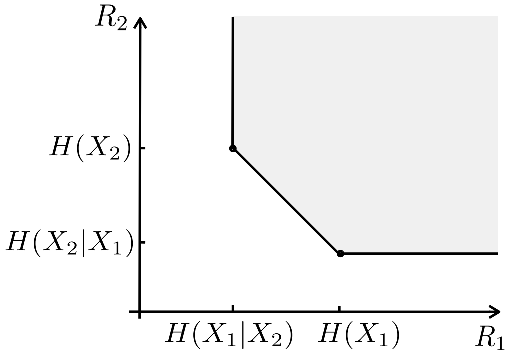

図 3　達成可能領域

$$H(X_2|X_1) = \sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{X}_1^n\times\mathcal{X}_2^n} P_{X_1X_2}(\mathbf{x}_1,\mathbf{x}_2)\log\frac{1}{P_{X_2|X_1}(\mathbf{x}_2|\mathbf{x}_1)},$$

$$H(X_1X_2) = \sum_{(\mathbf{x}_1,\mathbf{x}_2)\in\mathcal{X}_1^n\times\mathcal{X}_2^n} P_{X_1X_2}(\mathbf{x}_1,\mathbf{x}_2)\log\frac{1}{P_{X_1X_2}(\mathbf{x}_1\mathbf{x}_2)}.$$

この領域は 2 次元平面上で多角形をなす（図 3 参照）.

この結果の証明は非常に難解であったが，後に Cover によってその簡潔な証明が与えられた [6]. さらに Cover は同論文で情報源を任意のエルゴード情報源まで拡張している.

3.2　誤り指数の評価 - 信頼性関数

定理 3.1 により $(R_1, R_2) \in R(\mathbf{X}_1, \mathbf{X}_2)$ を満たすレートペアであれば，漸近的に誤り確率が 0 になることがわかる．しかし誤り確率が 0 に近づく速度を教えてはくれない．この問題と類似の問題は情報理論の通信路符号化問題においても生じる．Gallager [7] は通信路符号化問題において，誤り確率が 0 になる速度を符号長の関数で表した．この関数は指数を用いた式で表されこの指数部は信頼性関数と呼ばれる.

Slepian-Wolf 符号化システムにおいては，Koshelev [8] が Gallager の手法を用いて誤り指数を導出している.．Koshelev は次の定理を情報理論で有名な手法のランダム符号化を使って証明した．まず

$$E_1(s) \equiv -\log\sum_{x_2\in\mathcal{X}_2}\left(\sum_{x_1\in\mathcal{X}_1}P_{X_1X_2}(x_1,x_2)^{\frac{1}{1+s}}\right)^{1+s}$$

$$E_2(s) \equiv -\log\sum_{x_1\in\mathcal{X}_1}\left(\sum_{x_2\in\mathcal{X}_2}P_{X_1X_2}(x_1,x_2)^{\frac{1}{1+s}}\right)^{1+s}$$

$$E_3(s) \equiv -\log\left(\sum_{(x_1,x_2)\in\mathcal{X}_1\times\mathcal{X}_2}P_{X_1X_2}(x_1,x_2)^{\frac{1}{1+s}}\right)^{1+s},$$

とする．このとき次が成り立つ:

定理 3.2 (Koshelev [8])
$R_1 = \frac{1}{n}\log M_n^{(1)}$, $R_2 = \frac{1}{n}\log M_n^{(2)}$, とすると次を満たす $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号が存在する.

$$\begin{aligned}\varepsilon_n \le \min_{0\le s\le 1}\Big(&\exp\left[-n\left(R_1 s - E_1(s)\right)\right]\\ &+\exp[-n\left(R_2 s - E_2(s)\right)]\\ &+[-n\left(\left(R_1+R_2\right)s - E_3(s)\right)]\Big).\end{aligned}$$

この結果は Nomura and Han [9] により若干強められている．詳しくは [9, Section V] を参照されたい.

4　一般情報源に対する結果

4.1　ε-達成可能領域

前述の通り，一般情報源とは情報源の整合性条件すら仮定しない極めて一般的な情報源である．1990 年代に入り，Han and Verdú [10] によって提唱された一般情報源に対する一連の解析は当初一対一通信に対して行われていたが，その後 Slepian-Wolf 符号化システムのような多対一通信に対しても適用されるようになった.

まず必要な用語としてエントロピースペクトル上限を定義する*1:

$$\overline{H}(\mathbf{X}_1|\mathbf{X}_2) \equiv \text{p-}\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{P_{X_1^n|X_2^n}(X_1^n|X_2^n)},$$
$$\overline{H}(\mathbf{X}_2|\mathbf{X}_1) \equiv \text{p-}\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{P_{X_2^n|X_1^n}(X_2^n|X_1^n)},$$
$$\overline{H}(\mathbf{X}_1\mathbf{X}_2) \equiv \text{p-}\limsup_{n\to\infty}\frac{1}{n}\log\frac{1}{P_{X_1^nX_2^n}(X_1^nX_2^n)}.$$

実は定常無記憶情報源を考えれば次の関係が成り立つことは明らかであるので，この量は従来の条件付きエントロピーなどを一般化した概念といえる.

$$\overline{H}(\mathbf{X}_1|\mathbf{X}_2) = H(X_1|X_2),\quad \overline{H}(\mathbf{X}_2|\mathbf{X}_1) = H(X_2|X_1),$$
$$\overline{H}(\mathbf{X}_1\mathbf{X}_2) = H(X_1X_2).$$

これらの量は Slepian-Wolf 符号化システムに限らず一般情報源等に関する解析を進める上で重要な役割を果たす.

*1 For any sequence $\{Z_n\}_{n=1}^\infty$ of real-valued random variables, we define the limit superior in probability of $\{Z_n\}_{n=1}^\infty$ by $\text{p-}\limsup_{n\to\infty} Z_n = \inf\{\beta|\lim_{n\to\infty}\Pr\{Z_n>\beta\}=0\}$ (cf. [5]) .

最初に相関を有する一般情報源に対する符号化定理を導出したのは Miyake and Kanaya [11] である:

定理 4.1 (Miyake and Kanaya [11]) 有限アルファベットを持つ任意の一般情報源に対して次が成り立つ.

$$R(\mathbf{X}_1, \mathbf{X}_2) = \{(R_1, R_2) \,|\, R_1 \geq \overline{H}(\mathbf{X}_1|\mathbf{X}_2), \\ R_2 \geq \overline{H}(\mathbf{X}_2|\mathbf{X}_1), R_1 + R_2 \geq \overline{H}(\mathbf{X}_1\mathbf{X}_2).\}.$$

この結果は定理 3.1 の非常な一般化となっている.

さて，今までは誤り確率が漸近的に 0 になるレートペアの条件を議論してきた．ここで，条件を緩くして微少な誤りは許容できる場合を考えてみよう．この場合，従来よりも圧縮できる，すなわちレートペアを小さく出来ることが期待できる．次のような達成可能性を考えよう．ただし ε は $0 \leq \epsilon < 1$ とする.

定義 4.1 次を満たす $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号が存在するとき，レートペア (R_1, R_2) を ε-達成可能と呼ぶ.

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n^{(1)} \leq R_1,\ \limsup_{n\to\infty} \frac{1}{n} \log M_n^{(2)} \leq R_2$$

$$\limsup_{n\to\infty} \varepsilon_n \leq \varepsilon.$$

さらに定義 3.1 と同様に領域を定義する.

定義 4.2 (ε-達成可能領域)

$$R(\varepsilon|\mathbf{X}_1, \mathbf{X}_2) = \{(R_1, R_2) | (R_1, R_2) \text{ は } \varepsilon\text{-達成可能 }\}.$$

上の定義から明らかに

$$R(0|\mathbf{X}_1, \mathbf{X}_2) = R(\mathbf{X}_1, \mathbf{X}_2)$$

が成り立つことに注意しよう.

この領域は Han [5] によって加算無限アルファベットを持つ一般情報源に対して特定された．まず次のような関数 $F_n(R_1, R_2)$ を定義する:

$$F_n(R_1, R_2) = \Pr\left\{ \frac{1}{n} \log \frac{1}{P_{X_1^n|X_2^n}(X_1^n|X_2^n)} \geq R_1 \right. \\ \text{or } \frac{1}{n} \log \frac{1}{P_{X_2^n|X_1^n}(X_2^n|X_1^n)} \geq R_2 \\ \left. \text{or } \frac{1}{n} \log \frac{1}{P_{X_1^n X_2^n}(X_1^n X_2^n)} \geq R_1 + R_2 \right\},$$

定理 4.2 (Han [5]) 加算無限アルファベットを持つ任意の一般情報源に対して次が成り立つ.

$$R(\varepsilon|\mathbf{X}_1, \mathbf{X}_2) \\ = \mathrm{Cl}\left(\left\{ (R_1, R_2) \,\middle|\, \limsup_{n\to\infty} F_n(R_1, R_2) \leq \varepsilon \right\} \right),$$

ここで $\mathrm{Cl}(\cdot)$ は閉包操作を表す.

この定理において $\varepsilon = 0$ とし，情報源を定常無記憶情報源とすると定理 3.1 を導くことができる.

4.2 強逆定理

定理 4.2 は一般情報源に対する極めて広い結果であるが，上の結果を定常無記憶情報源に対して適用するとどうだろうか．$\varepsilon = 0$ とした場合，定理 3.1 が導けることは述べたが，ε $(0 < \varepsilon < 1)$ という微少な誤りを許すとレート領域は広がるであろうか．この問いに対する答えも Han [5] によってもたらされた．まず強逆性という概念を定義する.

定義 4.3 $(R_1, R_2) \notin R(0|\mathbf{X}_1, \mathbf{X}_2)$ であるような任意の (R_1, R_2) を考えると,

$$\limsup_{n\to\infty} \frac{1}{n} \log M_n^{(1)} \leq R_1,\ \limsup_{n\to\infty} \frac{1}{n} \log M_n^{(2)} \leq R_2$$

であるどのような $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号に対しても

$$\lim_{n\to\infty} \varepsilon_n = 1,$$

が成り立つとき，この情報源 $(\mathbf{X}_1, \mathbf{X}_2)$ は強逆性を満たすという.

強逆性とは情報源の性質であることに注意したい.

強逆性を持つ情報源に対しては漸近的な意味では誤り確率が 0 もしくは 1 以外とりえない，すなわち最適な符号を用いたとして，漸近的には，全て誤るか全て正しく復号できるかどちらかしか取りえないという著しい性質が成り立つことを示している．強逆性を考察するためにエントロピースペクトル上限と双対な量であるエントロピースペクトル下限を定義する:

$$\underline{H}(\mathbf{X}_1|\mathbf{X}_2) \equiv \text{p-}\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{P_{X_1^n|X_2^n}(X_1^n|X_2^n)},$$

$$\underline{H}(\mathbf{X}_2|\mathbf{X}_1) \equiv \text{p-}\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{P_{X_2^n|X_1^n}(X_2^n|X_1^n)},$$

$$\underline{H}(\mathbf{X}_1\mathbf{X}_2) \equiv \text{p-}\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{P_{X_1^n X_2^n}(X_1^n X_2^n)}.$$

定理 4.3 (Han [5]) 強逆性が成立するための必要十分条件は

- $\overline{H}(\mathbf{X}_1\mathbf{X}_2) > \overline{H}(\mathbf{X}_1|\mathbf{X}_2) + \overline{H}(\mathbf{X}_2|\mathbf{X}_1)$ が成立するとき:
$$\overline{H}(\mathbf{X}_1|\mathbf{X}_2) = \underline{H}(\mathbf{X}_1|\mathbf{X}_2),\ \overline{H}(\mathbf{X}_2|\mathbf{X}_1) = \underline{H}(\mathbf{X}_2|\mathbf{X}_1),$$
$$\overline{H}(\mathbf{X}_1\mathbf{X}_2) = \underline{H}(\mathbf{X}_1|\mathbf{X}_2),$$
- $\overline{H}(\mathbf{X}_1\mathbf{X}_2) \le \overline{H}(\mathbf{X}_1|\mathbf{X}_2) + \overline{H}(\mathbf{X}_2|\mathbf{X}_1)$ が成立するとき:
$$\overline{H}(\mathbf{X}_1|\mathbf{X}_2) = \underline{H}(\mathbf{X}_1|\mathbf{X}_2),\ \overline{H}(\mathbf{X}_2|\mathbf{X}_1) = \underline{H}(\mathbf{X}_2|\mathbf{X}_1),$$

が成り立つことである．

定常無記憶情報源は

$$\overline{H}(\mathbf{X}_1|\mathbf{X}_2) = \underline{H}(\mathbf{X}_1|\mathbf{X}_2) = H(X_1|X_2),$$
$$\overline{H}(\mathbf{X}_2|\mathbf{X}_1) = \underline{H}(\mathbf{X}_2|\mathbf{X}_1) = H(X_2|X_1),$$
$$\overline{H}(\mathbf{X}_1\mathbf{X}_2) = \underline{H}(\mathbf{X}_1|\mathbf{X}_2) = H(X_1X_2),$$

となるので強逆性を有することがわかる．

5　2次の達成可能領域に関する結果

5.1　2次の達成可能領域

定常無記憶情報源は強逆性を有するので，$(R_1, R_2) \in R(0|\mathbf{X}_1, \mathbf{X}_2)$ が成立するか否かで，漸近的には誤り確率は 0 または 1 となる．また $(R_1, R_2) \in R(0|\mathbf{X}_1, \mathbf{X}_2)$ となる場合に誤り確率が 0 に近付く速度の上界は定理 3.2 によって求められる．次に我々が興味を持つのは，符号長 n についてのより細かい評価である．従来の考えでは符号語のサイズ $M_n^{(1)}, M_n^{(2)}$ に対して

$$\frac{1}{n}\log M_n^{(1)},\ \frac{1}{n}\log M_n^{(2)}$$

という量の上極限を考えているがこれは

$$\log M_n^{(1)} + o(n),\ \log M_n^{(2)} + o(n)$$

を考えていることに相当する．この $o(n)$ の項をより精密に評価するために

$$\frac{1}{\sqrt{n}}\log M_n^{(1)},\ \frac{1}{\sqrt{n}}\log M_n^{(2)}$$

という量を考えてみよう．このような立場で達成可能性を議論する研究は従来から行われていたが ([12, 13])，通信路符号化を対象とした Hayashi [14] の論文と Polyanskiy et al. [15] の論文が 2010 年の IEEE Information Theory Society の Paper Award を同時受賞したことにより一躍脚光を浴びることとなった．この考え方は，有限長解析や 2 次の漸近解析などと呼ばれ，現在様々な問題に適用されている ([16, 17, 18, 19, 20])，この立場での Slepian-Wolf 符号化システムに対する研究は，Tan and Kosut [21] や Nomura and Han [9, 22] により行われている．ここでは [22] の結果を紹介する．

定義 5.1 a_1, a_2, ε が与えられたもとで，次式を満たす $\left(n, M_n^{(1)}, M_n^{(2)}, \varepsilon_n\right)$ 符号が存在するとき，(L_1, L_2) を (a_1, a_2, ε)-達成可能と呼ぶ．

$$\limsup_{n\to\infty}\frac{1}{\sqrt{n}}\log\frac{M_n^{(1)}}{e^{na_1}} \le L_1,\ \limsup_{n\to\infty}\frac{1}{\sqrt{n}}\log\frac{M_n^{(2)}}{e^{na_2}} \le L_2$$

$$\limsup_{n\to\infty}\varepsilon_n \le \varepsilon.$$

さらに定義 3.1 と同様に領域を定義する．

定義 5.2 ((a_1, a_2, ε)–達成可能領域)

$$\begin{aligned}&L(a_1, a_2, \varepsilon|\mathbf{X}_1, \mathbf{X}_2)\\ &\quad = \{(R_1, R_2)|(R_1, R_2)\ \text{は}\ (a_1, a_2, \varepsilon)\text{-達成可能}\ \}.\end{aligned}$$

(a_1, a_2, ε)-達成可能領域は，2 次の達成可能領域などと呼ばれるが，このとき従来の ε-達成可能領域（定義 4.2）は 1 次の達成可能領域と呼ばれることが多い．

注意 5.1 a_1, a_2 は通常 1 次の 0-達成可能領域の境界を考える．それ以外の点の 2 次領域を考えることは意味を持たないからである (cf. 注意 5.2)．例えば，$a_1 = H(X_1|X_2)$ とすると

$$\begin{aligned}\frac{1}{\sqrt{n}}\log\frac{M_n^{(1)}}{e^{na_1}} &= \frac{1}{\sqrt{n}}\log\frac{M_n^{(1)}}{e^{nH(X_1|X_2)}}\\ &= \frac{\log M_n^{(1)} - nH(X_1|X_2)}{\sqrt{n}},\end{aligned}$$

と書けることに注意しよう．すなわち 2 次の達成可能性とは符号長と最適な 1 次達成可能レートとの差を $\sqrt{n}$ の項まで評価しようとするものである．

5.2　一般情報源に対する (a_1, a_2, ε)-達成可能領域

本節では一般情報源に対する (a_1, a_2, ε)-達成可能領域を述べる．以降一般情報源は加算無限アルファベットを許す

ものとする．まず関数 $F_n(L_1,L_2|a_1,a_2)$ を定義する．

$$\begin{aligned}
&F_n(L_1,L_2|a_1,a_2)\\
&=\Pr\left\{\frac{-\log P_{X_1^n|X_2^n}(X_1^n|X_2^n)-na_1}{\sqrt{n}}\ge L_1\right.\\
&\quad\text{or}\quad\frac{-\log P_{X_2^n|X_1^n}(X_2^n|X_1^n)-na_2}{\sqrt{n}}\ge L_2\\
&\quad\text{or}\quad\left.\frac{-\log P_{X_1^nX_2^n}(X_1^nX_2^n)-n\,(a_1+a_2)}{\sqrt{n}}\ge L_1+L_2\right\},
\end{aligned}$$

さらに

$$\begin{aligned}
&\overline{F}_n(L_1,L_2|a_1,a_2)\\
&\equiv 1-F_n(L_1,L_2|a_1,a_2)\\
&=\Pr\left\{\frac{-\log P_{X_1^n|X_2^n}(X_1^n|X_2^n)-na_1}{\sqrt{n}}<L_1,\right.\\
&\qquad\frac{-\log P_{X_2^n|X_1^n}(X_2^n|X_1^n)-na_2}{\sqrt{n}}<L_2,\\
&\qquad\left.\frac{-\log P_{X_1^nX_2^n}(X_1^nX_2^n)-n\,(a_1+a_2)}{\sqrt{n}}<L_1+L_2\right\},
\end{aligned}$$

とする．このとき次の定理が成り立つ．

定理 5.1 (Nomura and Han [22]) 任意の一般情報源に対して (a_1,a_2,ε)-達成可能領域は次で与えられる．

$$\begin{aligned}
&L(a_1,a_2,\varepsilon|\mathbf{X}_1,\mathbf{X}_2)\\
&=\mathrm{Cl}\Big(\Big\{(L_1,L_2)\Big|\limsup_{n\to\infty}F_n(L_1,L_2|a_1,a_2)\le\varepsilon\Big\}\Big)\\
&=\mathrm{Cl}\Big(\Big\{(L_1,L_2)\Big|\liminf_{n\to\infty}\overline{F}_n(L_1,L_2|a_1,a_2)\ge 1-\varepsilon\Big\}\Big)
\end{aligned}$$

この結果は定理 4.2 を精密化した定理と考えることができる．実際関数 $F_n(L_1,L_2|a_1,a_2)$ は定理 4.2 に登場する関数 $F_n(R_1,R_2)$ と類似した形式であることが確認できる．一方，次節で考えるように定常無記憶情報源などを考える時には $F_n(L_1,L_2|a_1,a_2)$ でなくそれと双対な $\overline{F}_n(L_1,L_2|a_1,a_2)$ を考えた方が都合が良い．これは関数 $\overline{F}_n(L_1,L_2|a_1,a_2)$ が多次元の累積分布関数を表すためである．

5.3 定常無記憶情報源に対する (a_1,a_2,ε)-達成可能領域

この節では定常無記憶情報源を考える．定常無記憶情報源の場合，(a_1,a_2) は次の 3 つに場合分けできることが $R(0|\mathbf{X}_1,\mathbf{X}_2)$ より分かる．

Case I (Corner Points):

$$a_1=H(X_1|X_2)\quad\text{and}\quad a_2=H(X_2);$$

$$a_1=H(X_1)\quad\text{and}\quad a_2=H(X_2|X_1),$$

Case II (Non-Corner Points): For $0<\forall\lambda<1$,

$$\begin{aligned}
a_1&=\lambda H(X_1)+(1-\lambda)H(X_1|X_2),\\
a_2&=(1-\lambda)H(X_2)+\lambda H(X_2|X_1),
\end{aligned}$$

Case III (Full Side Points):

$$a_1=H(X_1|X_2)\quad\text{and}\quad a_2>H(X_2);$$

$$a_1>H(X_1)\quad\text{and}\quad a_2=H(X_2|X_1).$$

注意 5.2 (a_1,a_2) が 1 次達成可能領域の内部にある場合，$L(a_1,a_2,\varepsilon|\mathbf{X}_1,\mathbf{X}_2)=\mathbb{R}^2$ であることが容易に確かめられる．同様に 1 次達成可能領域の外部にある場合，$L(a_1,a_2,\varepsilon|\mathbf{X}_1,\mathbf{X}_2)$ は空集合 $\emptyset$ となる．

(a_1,a_2,ε)-達成可能領域を述べるために必要な関数を定義しよう．

$$\begin{aligned}
&\Phi(T_1,T_2,T_3)\\
&\equiv\lim_{n\to\infty}\Pr\left\{\frac{-\log P_{X_1^n|X_2^n}(X_1^n|X_2^n)-nH(X_1|X_2)}{\sqrt{n}}<T_1,\right.\\
&\qquad\frac{-\log P_{X_2^n|X_1^n}(X_2^n|X_1^n)-nH(X_2|X_1)}{\sqrt{n}}<T_2,\\
&\qquad\left.\frac{-\log P_{X_1^nX_2^n}(X_1^nX_2^n)-nH(X_1X_2)}{\sqrt{n}}<T_1+T_2\right\},
\end{aligned}$$

とする．このとき多次元中心極限定理 [23, 24] より

$$\begin{aligned}
\Phi(T_1,T_2,T_3)&=\int_{-\infty}^{T_1}dy_1\int_{-\infty}^{T_2}dy_2\int_{-\infty}^{T_3}dy_3\\
&\quad\times\frac{1}{(\sqrt{2\pi})^3\sqrt{\det\Sigma}}\exp\left(-\frac{1}{2}\mathbf{y}\Sigma^{-1}\mathbf{y}^{\mathrm{T}}\right),
\end{aligned}$$

となる．ここで $\mathbf{y}=(y_1,y_2,y_3)$ は 3 次元ベクトル，$\Sigma=(\sigma_{ij}^2)$ $(i,j=1,2,3)$ は次で与えられる分散共分散行列となる．

$$\sigma_{ij}^2=\sum_{x_1\in\mathcal{X}_1}\sum_{x_2\in\mathcal{X}_2}P_{X_1X_2}(x_1,x_2)z_i(x_1,x_2)z_j(x_1,x_2),$$

ただし

$$z_1(x_1,x_2)=-\log P_{X_1|X_2}(x_1|x_2)-H(X_1|X_2),$$

$$z_2(x_1,x_2)=-\log P_{X_2|X_1}(x_2|x_1)-H(X_2|X_1),$$

$$z_3(x_1,x_2)=-\log P_{X_1X_2}(x_1,x_2)-H(X_1X_2),$$

である．さらに $\Phi(T_1,T_2,T_3)$ の周辺分布関数 $\Phi_{13}(T_1,T_3)$, $\Phi_3(T_3)$ を次の様に定義する．

$$\Phi_{13}(T_1,T_3)\equiv\lim_{T_2\to\infty}\Phi(T_1,T_2,T_3),$$

$$\Phi_3(T_3)\equiv\lim_{T_1,T_2\to\infty}\Phi(T_1,T_2,T_3).$$

定理 5.2 (Nomura and Han [22]) 任意の定常無記憶情報源に対して次が成立する．

Case I $a_1 = H(X_1|X_2)$ and $a_2 = H(X_2)$ (without loss of generality):

$$L(a_1, a_2, \varepsilon|\mathbf{X}_1, \mathbf{X}_2) \\ = \{(L_1, L_2)\,|\Phi_{13}\,(L_1, L_1 + L_2) \geq 1 - \varepsilon\}.$$

Case II (for all $0 < \lambda < 1$):

$$L(a_1, a_2, \varepsilon|\mathbf{X}_1, \mathbf{X}_2) = \{(L_1, L_2)\,|\Phi_3\,(L_1{+}L_2) \geq 1 - \varepsilon\}.$$

Case III $a_1 = H(X_1|X_2)$ and $a_2 > H(X_2)$ (without loss of generality):

$$L(a_1, a_2, \varepsilon|\mathbf{X}_1, \mathbf{X}_2) = \{(L_1, L_2)\,|\Phi_1\,(L_1) \geq 1{-}\varepsilon\}.$$

注意 5.3 ここで $\Phi_3\,(L_1{+}L_2)$ と $\Phi_1\,(L_1)$ は 1 次元正規分布の累積分布関数であることに注意しよう．すなわち

$$\Phi_3\,(L_1 + L_2) = \int_{-\infty}^{L_1+L_2} \frac{1}{\sqrt{2\pi}\sigma_{33}} \exp\left(-\frac{y_3^2}{2\sigma_{33}^2}\right) dy_3,$$

$$\Phi_1\,(L_1) = \int_{-\infty}^{L_1} \frac{1}{\sqrt{2\pi}\sigma_{11}} \exp\left(-\frac{y_1^2}{2\sigma_{11}^2}\right) dy_1,$$

である．一方

$$\Phi_{13}\,(L_1, L_1{+}L_2) = \int_{-\infty}^{L_1} dy_1 \int_{-\infty}^{L_1+L_2} dy_3 \\ \times \frac{1}{2\pi\sqrt{\det \Sigma_{13}}} \exp\left(-\frac{1}{2}\mathbf{y}_{13}\Sigma_{13}^{-1}\mathbf{y}_{13}^T\right),$$

は次の共分散行列を持つ 2 次元正規分布の累積分布関数となる．

$$\Sigma_{13} = \begin{pmatrix} \sigma_{11}^2 & \sigma_{13}^2 \\ \sigma_{31}^2 & \sigma_{33}^2 \end{pmatrix}.$$

文献 [9] では上記 3 種類の場合分けを統一的に表現した結果も述べられている．

6 おわりに

本稿では，Slepian-Wolf 符号化システムにおける研究結果を概観した．あくまで著者の視点であるが，Slepian-Wolf 符号化システムが登場した 1973 年から 40 年間，固定長情報源符号化においてはいくつかの重要な結果が得られたと思われる．一方，本稿で取り扱わなかった 0 誤りを対象とする可変長情報源符号化についてはその困難さ故か研究にあまり進展がないように思える．可変長情報源符号化において

- 0 誤り達成可能領域
- 最適な符号の構成法

などの課題が難しいことは 1981 年に佐藤先生が既に指摘している [2]．近年 Koulgi et al. [25] により，Slepian-Wolf 符号化システムの特別な場合である補助情報つき情報源符号化における最適な符号の構成問題が NP-困難であることが示され，また Yan and Berger [26] により同符号化において，最適な符号構成における部分問題も NP-完全であることが報告されている．この事実は佐藤先生の考察が正しかったことを示しているように著者には思える．ついでながら述べさせてもらうと [26] では佐藤先生の研究成果である [27] を参考文献として挙げている．1982 年の研究成果が 2006 年の研究成果の参考となるのは基礎研究であるということだけでなく，それが深い考察に基づいているからであろう．改めて佐藤先生の洞察力に驚嘆するとともに，著者も基礎研究に携わる者の一人としてその精神を引き継ぎ，後の時代に多少なりとも参考となる “深い”研究を進めたいと考える次第である．しかしこのように書くと「目的が違うんじゃない？」と佐藤先生に言われそうである．そう我々は今自分が面白いと思える対象について深く考察することが第一で，後の評価はその時代の人間が決めることでしょうと．これこそが極道の心意気，前述の韓太舜先生の言葉を引用すれば，“それでベストを尽くしたあとは思い煩うことは何もない、ただ天命に任せればよいではないか。このような信条こそが『極道』すなわち『道を極める』ことに人生を掛けた者達の心意気というものであろう” [28]．学問の道を極めることに人生を捧げた佐藤創先生のこれからのご活躍を祈念して本稿を終わりたい．

参考文献

[1] T. S. Han and H. Sato, “Feedback codes with uniformly bounded codeword length and zero-error capacities,” *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 655–660, 1991.

[2] 佐藤創, 星守, “多重情報源に対する可変長符号化について,” 情報理論とその応用研究会第四回研究討論会資料, pp. 308–312, 1981.

[3] 佐藤創, 星守, “補助情報源を持つ誤りなし可変長符号化について,” 情報理論とその応用研究会第五回研究討論会資料, pp. 393–398, 1982.

[4] D. Slepian and J.K. Wolf, “Noiseless coding of

correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[5] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer, New York, 2003.

[6] T. M. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 226–228, 1975.

[7] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.

[8] V. N. Koshelev, "On a problem of separate coding of two dependent sources," *Problems of Information Transmission*, vol. 13, no. 1, pp. 18–22, 1977.

[9] R. Nomura and T. S. Han, "Second-order Slepian-Wolf coding theorems for mixed sources," arXiv: 1207.2505, 2012.

[10] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, 1993.

[11] S. Miyake and F. Kanaya, "Coding theorems on correlated general sources,' *IEICE Trans. Fundamentals*, vol. E78-A, no. 9, pp. 1063–1070, 1995.

[12] I. Kontoyiannis, "Second-order noiseless source coding theorems," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1339–1341, 1997.

[13] V. Strassen, "Asymptotische abshätzungen in Shannon's informations theorie," in *Trans. 3rd Prague Conf. Inf. Theory*, pp. 687–723, 1962.

[14] M. Hayashi, "Information spectrum approach to second-order coding rate in channel coding," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4947–4966, 2009.

[15] Y. Polyanskiy, H. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[16] M. Hayashi, "Second-order asymptotics in fixed-length source coding and intrinsic randomness," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4619–4637, 2008.

[17] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Strongly secure privacy amplification cannot be obtained by encoder of Slepian-Wolf code," *IEICE Trans. Fundamentals*, vol. E93-A, no. 9, pp. 1650–1659, 2010.

[18] R. Nomura and T. S. Han, "Second-order resolvability, intrinsic randomness, and fixed-length source coding for mixed sources: information spectrum approach," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 1–16, 2013.

[19] V. Kostina and S. Verdú, "Fixed-length lossy compression in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3309–3338, 2012.

[20] V. Kostina and S. Verdú, "Lossy joint source-channel coding in the finite blocklength regime," in *Proc. 2012 IEEE International Symposium on Information Theory*, pp. 1553–1557, 2012.

[21] V. Y. F. Tan and O. Kosut, "The dispersion of Slepian-Wolf coding," in *Proc. 2012 IEEE International Symposium on Information Theory*, pp. 920–924, 2012.

[22] R. Nomura and T. S. Han, "Second-order Slepian-Wolf source coding theorems," 第 35 回情報理論とその応用シンポジウム予稿集, pp.356-361, 2012.

[23] V. Bentkus, "On the dependence of the berry-esseen bound on dimension," *J. Stat. Planning and Inference*, vol. 113, no. 2, pp. 385–402, 2003.

[24] P. Billingsley, *Probability and Measure*. Wiley, 1995.

[25] P. Koulgi, E. Tuncel, S.L. Regunathan and K. Rose, "On zero-error source coding with decoder side information," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 99–111, 2003.

[26] Y. O. Yan and T. Berger, "Zero-error instantaneous coding of correlated sources with length constraints is NP-complete," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1705–1708, 2006.

[27] H. Sato, "On the instantaneous code for multiple information sources," in *Proc. 1982 IEEE International Symposium on Information Theory*, p. 103, 1982.

[28] 韓太舜, "極道としての学問," 情報理論とその応用学会ニューズレター, no. 23, pp. 3–6, 1996.