ロバスト符号化

山本 博資
(東京大学 複雑理工学専攻)
Hirosuke@ieee.org

1　はじめに

情報を通信路[1]を通して送るとき，**効率よく，高品質で，安全に**伝送きることが望まれる．通信路では送信量に比例してコストがかかることから，同じ情報を送る場合でも，できるだけコンパクトに圧縮して送る必要がある．また，無線通信路を始めとしてどのような通信路も，不可避的に雑音が存在し，受信情報には誤りが含まれる可能性がある．高品質な情報伝送を実現するためには，そのような誤りを訂正できる技術が必要となる．また，無線通信路やインターネットのような公開通信路では，送信されている情報を第３者が容易に知ることができる．情報の安全性を守るためには，そのような公開通信路を通して伝送する場合でも，情報の漏洩や改ざんに対して安全である必要がある．

これらの要求を満たすものとして符号化技術が存在し，その各々の要求に対して，次の符号化技術が対応している．

(A) 情報源符号化：データ圧縮を実現するための符号化

(B) 通信路符号化：誤り訂正を実現するための符号化

(C) 暗号化：情報セキュリティを実現するための符号化

本稿では，これらの符号化におけるロバスト性を考察する．

[1]光磁気ディスクなどの記憶媒体も一種の通信路と考えることができる．

2　符号化のロバスト性

2.1　情報源符号化

情報源系列 $x^n = x_1x_2\cdots x_n$ が確率分布 $P(x^n)$ に従って生起するとき，その圧縮限界は次式で定義されるエントロピーレート $H(\boldsymbol{X})$ で与えられる．

$$H(\boldsymbol{X}) \equiv \lim_{n\to\infty} \frac{1}{n} \sum_{x^n} P(x^n) \log \frac{1}{P(x^n)} \qquad (1)$$

また，復号時にひずみを許す圧縮の場合には，いわゆるレートひずみ関数 $R(D)$ で圧縮限界が与えられる．

情報源符号は，符号の構成に情報源の確率を陽に利用するエントロピー符号化と，情報源の確率を陽に用いないユニバーサル符号化とに分類できる．エントロピー符号化に分類される符号には，Huffman 符号,Tunstall 符号, 算術符号などがあり，圧縮限界であるエントロピーレート $H(\boldsymbol{X})$ までの圧縮が可能である．しかし，エントロピー符号化では，符号の構成に用いた確率モデル $Q(X^n)$ と，実際のデータ系列の確率 $P(X^n)$ が異なっているとき，圧縮性能にダイバージェンス $D(P\|Q)$ 分のロスが生じ，確率分布の変動に対するロバスト性が弱い．

これに対して，ユニバーサル符号は，情報源の確率構造を陽に利用しないため，広い情報源クラスに対してロバストに圧縮限界のエントロピーレート $H(\boldsymbol{X})$ まで圧縮できる特長を持つ．

ユニバーサル符号の研究は 1966 年に始まり [1, 2, 3]，現在まで非常に多数の符号が提案されている．それらは，辞書法, ソート法, 文法法, 確率のユニバーサル推定＋エントロピー符号化に大きく分類できる [4, 5].

ユニバーサル符号は，符号化アルゴリズムに確率を陽に利用していないため，その圧縮性能を理論的に解析することは一般に難しい場合が多い．もっとも簡単なユニバーサル符号の 1 つとして，MTF(move-to-front) 法がある [6]．MTF 法は，ワープロの日本語変換などでもよく用いられている手法であり，出現した文字をリストの先頭に移動させる方法である．符号化は出現した文字が現時点のリストの何番目に存在するかを示す整数値に符号化する．例えば，文字のアルファベット $\mathcal{X}$ が $\mathcal{X} = \{amoty\}$ のとき，文字列 yamamoto は次のように符号化される．

リスト	データ系列	符号語
$amoty$	y	5
$yamot$	a	2
$aymot$	m	3
$mayot$	a	2
$amyot$	m	2
$mayot$	o	4
$omayt$	t	5
$tomay$	o	2

整数値は，さらに正整数のユニバーサル符号 [7] やエントロピー符号化を用いて 2 値系列に符号化される．この MTF 法の圧縮性能は，出現したシンボルを先頭に移動させるという非定常な動作のため，理論解析が困難であったが，我々の研究 [8] により，その圧縮性能が詳しく解析された．その結果，MTF が圧縮限界であるエントロピーレート $H(\boldsymbol{X})$ を達成できるのは，データ系列が 1 次マルコフ情報源系列で，次の形をした確率を持つ場合だけであることが明らかとなった．

$$
\begin{aligned}
& P(x_i|x_1, x_2, \cdots, x_{i-1}) \\
&= P(x_i|x_{i-1}) \\
&= \begin{cases} 1-(|\mathcal{X}|-1)q, & \text{if } x_i = x_{i-1} \\ q, & \text{otherwise} \end{cases}
\end{aligned}
$$

2.2 通信路符号化

遷移確率 $P(y|x)$ を持つ通信路を通して情報を伝送するとき，情報の伝送レート R が次式で与えられる通信路容量 C より小さければ，符号語長 n を十分長くすることにより，任意に小さい誤り確率を達成できる．

$$C = \inf_X I(X;Y) \tag{2}$$

しかし，式 (2) の通信路容量は，符号語をランダムに生成するランダム符号化により達成できるが，ランダム符号化では復号処理に，符号語長 n の指数オーダのメモリ量や計算量が必要となるため実用的ではない．そのため，符号に線形性を持たせることにより，復号時のメモリ量や計算量が実用的なレベルで実現できる線形符号が用いられている．

離散的な通信路としては，入出力シンボルアルッファベッとが $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ で，遷移確率が次式で与えられる 2 値対称通信路 (BSC, binary symmetric channel) がよく用いられる．

$$P(y|x) = \begin{cases} 1-q, & \text{if } y = x \\ q, & \text{if } y \neq x \end{cases} \tag{3}$$

また，連続的な通信路としては，通信路の入力 X と出力 Y がガウス雑音 Z により $Y = X + Z$ と関係づけられている加法的ガウス雑音通信路 (AGC, additive Gaussian channel) が重要である．

これらの通信路に対してさまざまな符号が提案され詳しく研究されているが [9]，一般に，与えられた復号誤り率 P_e を達成するためには，BSC のビット誤り率 q や AGC のガウス雑音の分散 σ_z^2 が大きくなるにつれて，符号語長 n を大きくしなければならない．逆に言えば，符号語長 n を大きくすると，q や σ_z^2 の変動に対して，ロバストな誤り訂正が可能となる．しかし，n が大きくなるにつれて，復号器の複雑さが増加するため，一般にはあまり大きくできない．

多くの線形符号では，n が大きくなるにつれて誤り復号率 P_e を小さくできるが，符号化レート R もゼロに近づくため，効率よく伝送できない欠点があった．これに対して，代数幾何符号では，n を大きくしても，レート R を大きく保った符号が構成できることが知られている [9]．また，低密度パリティ検査 (LDPC, low density parity check) 符号 [10] やターボ符号 (turbo code)[11]

では，ビット単位で近似的に事後確率最小復号を行うことができ，比較的大きな q や σ_z^2 に対しても性能のよい復号誤り率 P_e を実現できるようになって来ている．今後，これらの符号に対する研究がさらに進むことにより，通信路符号のロバスト性がより向上するものと思われる．

2.3 暗号化

情報セキュリティを実現する暗号システムは，大きく分けて計算量的な安全性に基づく方式と，情報量的な安全性に基づく方式に分類できる [12]．前者は，素因数分解の困難さや離散対数問題の困難さに基づいて作られており，暗号を解読するのに必要な計算時間が非常に大きいことに安全性の根拠を置いている．これに対して後者は，秘密鍵などの秘密情報量に基づく安全性であり，どのような計算機を用いてもその秘密情報量分の安全性を保つことができる特長を持つ．

RSA 暗号を始めとして，計算量的な安全性に基づく多くの暗号システムが実用化されているが，量子コンピュータや，インターネットを介した超並列計算により，その安全性が将来に渡って安全である保証がない．これに対して，情報量的な安全性に基づく暗号システムは，計算機などの科学技術の発展によらず，秘密情報量分の安全性を未来永劫に渡って保証することができ，情報セキュリティのロバスト性から考えてより望ましいシステムである．このような観点から，2005 年 10 月には，情報量的な安全性に基づく暗号に関する国際ワークショップ（IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security) が開催されている．

我々の研究室では，世界に先駆けて，情報量的な安全性に基づく暗号システムに関してさまざまな研究を行ってきた [13, 14]．次節では，最近得られた成果の一つを紹介する [15].

3 盗聴通信路に対する多重符号化

3.1 盗聴通信路

雑音のある通信路を通して Alice から正規の受信者 Bob に情報を送るとき，敵である Eve がその通信を盗聴する．Alice から Bob への主通信路と Alice から Eve への盗聴通信路の雑音特性が異なることを利用して，秘密鍵を全く使わずに，Eve に対して情報量的に完全に安全に情報を送る符号化問題を盗聴通信路（wiretap channel）に対する符号化問題という．

盗聴通信路に対する符号化問題は 1975 年に Wyner[16] により導入され，まず degraded broadcast channel 形の盗聴通信路に対して符号化定理が示された．次に，一般の broadcast channel について，Csiszár と Körner[17] により，Bob への主通信路が Eve への盗聴通信路よりも雑音が小さい場合に対して符号化定理が証明された．また，Eve への盗聴通信路が Bob への主通信路より雑音が小さい場合でも，Alice と Bob の間で公開通信路が利用可能であれば，その盗聴通信路と公開通信路の両方を用いることにより，安全に情報共有が行えることが示されている [18]．これらの議論は，通信路が定常性を持つ条件の下でなされてきた．これに対し，定常性を仮定しない一般情報源/一般通信路に対する符号化定理は，情報スペクトル理論 [19] として研究され，さまざまな符号化に対する性能限界が明らかにされている．この情報スペクトル理論において，Han と Verdú[20] は通信路 resolvability 問題を提案した．これは，目標となる分布を通信路の出力分布で近似するためには，どれだけのサイズの一様乱数を符号化して通信路に入力すればよいかを考える問題である．Devetak[21] は，量子通信路において盗聴を防ぐ符号化に stochastic encoder（確率的符号器）を導入した．さらに Hayashi[22] はこの stochastic encoder を用いる符号化法を通信路 resolvability 問題と対応させ，盗聴通信路符号化定理に対する一般的な証明手法を与えている．

盗聴通信路を通して安全に送信できる情報量は秘密保持通信路容量（secrecy capacity）C_S で与えられるが，一般に C_S は通常の通信路容

量 C に比べて小さい値となる．以下では，無駄になっている容量 $C - C_S$ を有効に利用するために，複数の互いに独立な情報を多重に符号化することを考える．その結果，トータルの情報伝送量として通信路容量を達成し，かつ伝送する各情報ごとに個別に完全な安全性が達成できることを示す．

3.2 多重符号化による情報伝送

盗聴通信路を通して情報を盗聴者に知られることなく，どれだけの情報量を安全に送ることができるかを考える．Alice が送信する通信路の入力アルファベットを $\mathcal{X}$，Bob，Eve が受信する通信路の出力アルファベットをそれぞれ $\mathcal{Y}, \mathcal{Z}$ とする．用いる通信路やその入出力は情報スペクトル理論 [19] の意味での一般通信路/一般情報源とする．Alice–Bob 間の主通信路を $\mathbf{W}$，Alice から Eve への盗聴通信路を $\mathbf{V}$ とし，Alice の入力を $\mathbf{X}$，Bob と Eve への出力をそれぞれ $\mathbf{Y}$，$\mathbf{Z}$ とする．ここでは盗聴通信路に比べ，主通信路の方が雑音が小さい場合を考える．相互情報量で表すと，$\underline{I}(P_{\mathbf{X}}, W^n) > \overline{I}(P_{\mathbf{X}}, V^n)$ となる $P_{\mathbf{X}}$ が存在する場合を考える[2]．Alice から Bob に伝送したい S 個の互いに確率的に独立な情報を $K_1, K_2, \ldots, K_S$ とし，各 s, $1 \le s \le S$ に対して，そのアルファベットを $\mathcal{K}_s = \{1, 2, \cdots, M_s\}$，各アルファベットサイズを $M_s = |\mathcal{K}_s|$ とする．また各 K_s は $\mathcal{K}_s$ 上で一様分布をするものとする．全体のメッセージ空間は $\mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_S$ となる．この通信における目標は，Eve に対しては，個々のメッセージについて全く情報を漏らさないという個別の完全な安全性を達成し，Bob へはすべてのメッセージを誤りなく伝送することである．

メッセージ $(K_1, K_2, \cdots, K_S)$ は符号器 φ_n によって符号語 X^n に符号化されて送信されるが，ここで φ_n としては一般に stochastic encoder も許すものとする．正規の受信者である Bob は，受信した情報 Y^n から復号器 ψ_n によって各情報 K_s の復号を行う．例えば情報 K_s について復号を行う場合，M_s 個の互いに排反な復号領域 $\mathcal{D}_1^s, \ldots, \mathcal{D}_{M_s}^s$ を定めておき，受信した Y^n が $Y^n \in \mathcal{D}_k^s$, $k \in \mathcal{K}_s$ のとき，復号メッセージを $\widehat{K_s} = k$ とする．

この符号を $\mathcal{C}_n(\{M_1, \cdots, M_S\}, \varphi_n, \psi_n)$ と書き，この符号の性能を 3 つの観点から評価する．

1. 各情報 K_s の符号化レート $\frac{1}{n}\log M_s$.
2. 各情報 K_s に対する Bob の平均復号誤り確率.

$$\varepsilon_n^s(\mathcal{C}_n) \equiv \frac{1}{M_s}\sum_{k=1}^{M_s} Q_k^s W^n(\overline{\mathcal{D}_k^s}) \qquad (4)$$

ここで Q_k^s は，情報 $K_s = k$ を送信するときに，$K_{s'}, s' \neq s$ の値や stochastic encoder により X^n が確率的に定まることによる X^n の確率分布であり，$Q_k^s W^n(y^n)$ はそのときの出力 Y^n の確率分布である．また $\overline{\mathcal{D}_k^s}$ は $\mathcal{D}_k^s$ の補集合を示す．

3. Eve が受信する盗聴通信路出力 Z^n と各情報 K_s との間の相互情報量:

$$I_n^s(\mathcal{C}_n) \equiv \frac{1}{n} I(K_s; Z^n) \qquad (5)$$

また，Eve がメッセージ K_s をどの程度識別できるかを示す別の指標として，$I_n^s(\mathcal{C}_n)$ の代わりに，各メッセージ K_s ごとで，$K_s = k$ と $K_s = k'$ の出力分布間の平均変動距離を用いることもできる．

$$d_n^s(\mathcal{C}_n) \equiv \frac{1}{M_s(M_s-1)}\sum_{k' \neq k} ||Q_{k'}^s V^n - Q_k^s V^n||_1 \qquad (6)$$

各メッセージ K_s の情報が，Eve に漏れないようにするためには，式 (5)(6) を小さく抑えればよい．なぜなら，式 (5) を任意に小さい $\varepsilon > 0$ で抑えることができれば，

$$\frac{1}{n}H(K_s|Z^n) = \frac{1}{n}[H(K_s) - I(K_s; Z^n)] \ge \frac{1}{n}H(K_s) - \varepsilon \approx \frac{1}{n}H(K_s) \qquad (7)$$

[2] $\underline{I}(P_{\mathbf{X}}, W^n), \overline{I}(P_{\mathbf{X}}, V^n)$ は，相互情報量スペクトル上限と下限である．詳しくは [19] を参照．

が成り立ち，K_s と Z^n が確率的にほぼ独立となる．つまり Eve は Z^n を受信しても K_s の情報が全く得られないことがわかる．また，式 (6) が小さく抑えられていれば，直感的には Eve が通信路出力 Z^n を観測しても Z^n の確率分布 $Q_k^s V^n$ が k に依存しないため，$K_s = k$ について情報が全く得られないことを意味する．

各情報 K_s を Eve に漏らさずに Bob に正しく伝送するとき，レート R_s, $s = 1, 2, \cdots, S$ が達成可能であることを次のように定義する．

定義 1 式 (8)–(11) を満たす符号の列 $\mathcal{C}_n$ が存在するとき，レート R_s, $s = 1, 2, \cdots, S$ は $I_n^s(\mathcal{C}_n)$ の意味で達成可能である．また，式 (8)–(10)(12) を満たす符号の列 $\mathcal{C}_n$ が存在するとき，$d_n^s(\mathcal{C}_n)$ の意味で達成可能である．

$$\liminf_{n\to\infty} \frac{1}{n} \sum_{s'=1}^{S} \log M_n^{s'} \geq R_{total} \tag{8}$$

$$\liminf_{n\to\infty} \frac{1}{n} \sum_{s'=1, s'\neq s}^{S} \log M_n^{s'} \leq R_{total} - R_s \quad s = 1, 2, \cdots, S \tag{9}$$

$$\lim_{n\to\infty} \varepsilon_n^s(\mathcal{C}_n) = 0, \ s = 1, 2, \cdots, S \tag{10}$$

$$\lim_{n\to\infty} I_n^s(\mathcal{C}_n) = 0, \ s = 1, 2, \cdots, S \tag{11}$$

$$\lim_{n\to\infty} d_n^s(\mathcal{C}_n) = 0, \ s = 1, 2, \cdots, S \tag{12}$$

ここで，R_{total} は次式で定義される．

$$R_{total} = \sum_{s=1}^{S} R_s \tag{13}$$

定義 2 deterministic encoder を用いた $I_n^s(\mathcal{C}_n)$ および $d_n^s(\mathcal{C}_n)$ の意味で達成可能な R_s, $s = 1, 2, \cdots, S$ の集合を，それぞれ $\mathcal{R}_{\rm det}^I(S)$, $\mathcal{R}_{\rm det}^d(S)$ で表す．また，stochastic encoder を用いて，$I_n^s(\mathcal{C}_n)$ および $d_n^s(\mathcal{C}_n)$ の意味で達成可能な R_s, $s = 1, 2, \cdots, S$ の集合を，それぞれ $\mathcal{R}_{\rm sto}^I(S)$, $\mathcal{R}_{\rm sto}^d(S)$ で表す．

このとき，明らかに次式が成り立つ．

$$\mathcal{R}_{\rm det}^I(S) \subseteq \mathcal{R}_{\rm sto}^I(S), \ \mathcal{R}_{\rm det}^d(S) \subseteq \mathcal{R}_{\rm sto}^d(S)$$

これらの領域 $\mathcal{R}_*^*(S)$ を求めるために，次のような領域 $\mathcal{R}_1(S)$ と $\mathcal{R}_2(S)$ を考える．

定義 3

$$\begin{aligned}\mathcal{R}_1(S) = &\{(R_1, R_2, \cdots, R_S) : \text{式 (14)(15) を} \\ &\text{満たす入力分布 } P_{\mathbf{X}} \text{ が存在する } \} \\ &R_{total} \leq \underline{I}(P_{\mathbf{X}}, \mathbf{W}) \qquad (14) \\ &R_{total} - R_s \geq \overline{I}(P_{\mathbf{X}}, \mathbf{V}), \\ &\qquad s = 1, 2, \cdots, S \qquad (15)\end{aligned}$$

定義 4

$$\begin{aligned}\mathcal{R}_2(S) = &\{(R_1, R_2, \cdots, R_S) : \text{式 (16)(17) を} \\ &\text{満たす入力分布 } P_{\widetilde{\mathbf{X}}} \text{ および通信路 } \mathbf{U} \\ &\text{が存在する } \} \\ &R_{total} \leq \underline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UW}) \qquad (16) \\ &R_{total} - R_s \geq \overline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UV}), \\ &\qquad s = 1, 2, \cdots, S \qquad (17)\end{aligned}$$

ここで，$\widetilde{\mathcal{X}}$ は任意の有限アルファベットとし，$\mathbf{U}$ は $\widetilde{\mathcal{X}}$ から $\mathcal{X}$ への仮想通信路であり，$P_{\widetilde{\mathbf{X}}}$ は $\widetilde{\mathcal{X}}$ 上の確率分布である．また，$\mathbf{UW}$ と $\mathbf{UV}$ は，それぞれ $\widetilde{\mathcal{X}} \to \mathcal{X} \to \mathcal{Y}$ および $\widetilde{\mathcal{X}} \to \mathcal{X} \to \mathcal{Z}$ の合成通信路の遷移確率分布である．

定理 5 $S \geq 2$ に対して次式が成り立つ．

$$\mathcal{R}_{\rm det}^I(S) \supseteq \mathcal{R}_1(S), \quad \mathcal{R}_{\rm det}^d(S) \supseteq \mathcal{R}_1(S) \tag{18}$$

定理 6 $S \geq 2$ に対して次式が成り立つ．

$$\mathcal{R}_{\rm sto}^I(S) \supseteq \mathcal{R}_2(S), \quad \mathcal{R}_{\rm sto}^d(S) \supseteq \mathcal{R}_2(S) \tag{19}$$

(定理 5 および 6 の証明は，[15] に示されている．)

注 7 式 (14)(15) および式 (16)(17) より，各 R_s は定理 5,6 の各々において，それぞれ次式を満たさなければならない．

$$R_s \leq \underline{I}(P_{\mathbf{X}}, \mathbf{W}) - \overline{I}(P_{\mathbf{X}}, \mathbf{V}) \tag{20}$$

$$R_s \leq \underline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UW}) - \overline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UV}) \tag{21}$$

注 8 定理 6 において $S = 1$ の場合も式 (19) が成り立つ．したがって，$R_1 = \underline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UW})$, $0 = \overline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UV})$ が達成可能となり，[22] より秘密保持通信路容量 C_S に対して次式が成り立つ．

$$\begin{aligned} C_S &= \sup_{P_{\widetilde{\mathbf{X}}}, \mathbf{U}: \overline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UV})=0} \underline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UW}) \\ &= \sup_{P_{\widetilde{\mathbf{X}}}, \mathbf{U}} \left[\underline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UW}) - \overline{I}(P_{\widetilde{\mathbf{X}}}, \mathbf{UV}) \right] \end{aligned} \quad (22)$$

注 9 通信路容量 C に対して $C = \sup_{P_{\mathbf{X}}} \underline{I}(P_{\mathbf{X}}, \mathbf{W})$ を達成する分布を $P^*_{\mathbf{X}}$ とすると，$\mathcal{R}_1(S)$ よりトータルのレート R_{total} として通信路容量 C を達成できる．このとき，情報の個数 S は次式を満たさなければならない．

$$S > \left\lceil \frac{\underline{I}(P^*_{\mathbf{X}}, \mathbf{W})}{\underline{I}(P^*_{\mathbf{X}}, \mathbf{W}) - \overline{I}(P^*_{\mathbf{X}}, \mathbf{V})} \right\rceil \quad (23)$$

4 今後の展望と課題

本稿では，符号化を情報源符号化, 通信路符号化, 暗号化に分類して，ロバスト性について考察を行った．特に，情報源符号化におけるユニバーサル符号，通信路符号化における LDPC 符号やターボ符号，暗号化における情報量的安全性に基づく暗号などが，ロバスト性が強いことを紹介した．

上記のロバスト性は，符号のロバスト性であるが，符号の特性を解析する理論手法のロバスト性も必要となる．従来の情報理論的な解析では，確率モデルとして，定常性やエルゴード性を仮定することが多く，また解析手法が，無記憶過程，マルコ過程，定常過程，エルゴード過程などで異なっているため，符号の性能が，データや通信路の確率モデルの特性によるものか，符号自身の特性によるものかが，明確に分離されていなかった．

これに対して，Han-Verdú[20] に始まる情報スペクトル理論 [19] では，情報源や通信路に一切の仮定を置かない完全な一般情報減/一般通信路を取り扱うことができる．その結果，符号化操作の本質と，情報源や通信路などの確率過程の本質が分離でき，より見通しのよい理論展開を行うことが可能である．第 3 節で述べた「盗聴通信路に対する多重符号化」でも，情報スペクトル理論を用いることにより，見通しのよい一般的な証明が可能となっている [15]．また，最適な FV 符号の漸近特性に関して，情報スペクトル理論的な解析を行い，その特性を明らかにしている [23]．

今後の課題として，情報源符号化, 通信路符号化, 暗号化などで使われる個別の符号ごとに，解決すべきさまざまな問題が残されているが，それら以外に，基礎理論として得られた研究成果の幾つかが，まだ十分に応用に結びついていない問題点がある．今後，符号の実用的な応用に最新の基礎理論成果を結びつけて行くことが大きな課題の一つである．

参考文献

[1] B.M.Fitingof, “Optimal Coding in the Case of Unknown and Changing Message Statistics,” *Probl. Inform. Transm.*, vol.2, no.2, pp.3-11 (in Russian), pp.1-7 (English Trans.), 1966.

[2] T.J.Lynch, “Sequence Time Coding for Data Compression,” *Proc.IEEE*, vol.54, pp.1490-1491, Oct. 1966.

[3] L.D.Davisson, “Comments on ’Sequence Time Coding for Data Compression’,” *Proc. IEEE*, vol.54, p.2010, Dec. 1966.

[4] 山本博資, “データ圧縮における最新アルゴリズム [I] ー無ひずみデータ圧縮アルゴリズムの変遷ー,” 電子情報通信学会誌, vol.86, no.2, pp.120-126, Feb. 2003

[5] 山本博資, “情報源符号化手法の広がり”, 数理科学「特集, 符号化理論の新時代, 情報･通信技術を支える数理」, vol.42, no.11, pp.13-18, Nov. 2004

[6] J.L.Bentley, D.D.Sleator, R.E.Tarjan, and V.K.Wei, “A Locally Adaptive Compres-

sion Scheme," *Commun. ACM*, vol.29, no.4, pp.320-330, April 1986.

[7] 山本博資, "データ圧縮と正整数のユニバーサル表現," 情報理論とその応用学会編, "現代情報源符号化　無歪みデータ圧縮", 第４章, 培風館, 1998

[8] M. Arimura and H.Yamamoto, "Asymptotic redundancy of the MTF scheme for stationary ergodic sources," *IEEE Trans. on Inform. Theory*, vol.51, no.11, pp.3742-3752, Nov. 2005

[9] V.S.Press and W.C.Huffman (ed.), "Handbook of coding theory," volumes I and II, North-Holland, 1998

[10] 和田山正, "低密度パリティ検査符号とその復号法," トリケップス, 2002

[11] 荻原春生, "ターボ符号の基礎," トリケップス, 1999

[12] 岡本, 山本, "現代暗号," 産業図書, 1997

[13] H.Yamamoto, "Information theory in cryptology", *IEICE Trans.*, vol.E74, no.9, pp.2456-2464, Sep. 1991

[14] H.Yamamoto, "Rate-distortion theory for the Shannon cipher system", *IEEE Trans. on Inform. Theory*, vol.43, no.3, pp.827-835, May 1997

[15] D.Kobayashi, H.Yamamoto, T.Ogawa, "Secure multiplex coding to attain the channel capacity in wiretap channels," (submitted to *IEEE Trans. on Inform. Theory*)

[16] A. D. Wyner, "The wire-tap channel," *Bell System Technical Jounal,* vol. 54, no. 8, pp. 1355–1387, 1975.

[17] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory,* vol. IT-24, no. 3, pp. 339–348, May 1989.

[18] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory,* vol. 39, no. 3, pp. 733–742, May 1993.

[19] T. S. Han, "Information-spectrum methods in information theory," Springer-Verlag, 2003.

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

[21] I. Devetak, "The private classical information capacity and quantum information capacity of a quantum channels," *IEEE Trans. Inform. Theory*, vol.51, no.1, pp.44–55, Jan. 2005.

[22] M. Hayashi, "General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel," (submitted to *IEEE Trans. Infrom. Theory.*)

[23] H.Koga and H.Yamamoto, "Asymptotic properties on the codeword lengths of optimal FV codes for general sources", *IEEE Trans. on Inform. Theory*, vol.51, no.4, pp.1546-1555, April 2005