3. 未来100年を進む私が目指すもの

3-1　22世紀の情報理論

Information Theory in the Twenty-second Century

渡辺　峻

1. は　じ　め　に

筆者が情報理論に初めて出会ったのは東京工業大学在籍時の学部の講義であった．データ圧縮や通信路符号化といった工学的な問題が，エントロピーや相互情報量といった数学的な量で簡明に記述される様に感動を覚え興味を持った．卒業研究を実施するための研究室配属では，情報理論の研究を行っていた植松・松本研究室を志望し配属された．その当時は将来研究者になるとまでは想像していなかったが，徐々に情報理論の魅力にのめり込み，気が付けば10数年の間夢中になって研究を続けていた．

情報理論の魅力は何なのだろうか．ある人は数学的美しさと答えるかもしれない．また，ある人は工学的な問題へ重要な示唆を与えることだと答えるかもしれない．もちろんこういったことは情報理論の魅力ではあるが，筆者が一番魅力に感じているのは，情報理論の研究成果は永い間廃れないことである．これは日進月歩で新しい技術が出現する工学分野では異例なことである．100年後の世界がどのようになっているのかは到底想像できるものではないが，情報理論は何らかの形で残り続けているはずである．

さて，本稿では筆者のこれまでの研究遍歴を紹介し，情報理論の今後について筆者の私見を述べたい．それを通じて，情報理論の魅力が伝われば幸いである(注1)．

(注1)　情報理論史の概説については文献(1)を参照．

渡辺　峻　正員　東京農工大学工学部情報工学科
E-mail　shunwata@cc.tuat.ac.jp
Shun WATANABE, Member (Faculty of Engineering, Tokyo University of Agriculture and Technology, Koganei-shi, 184-8588 Japan).
電子情報通信学会誌　Vol.100 No.6 pp.468-473 2017年6月

2. これまでの研究遍歴

本章では筆者のこれまでの研究遍歴について述べる．また，これまでの研究キャリアの中で出会った研究者から受けた影響についても触れる．

2.1　学生時代

前述のように，学部4年時に植松・松本研究室に配属された．研究室に配属されてしばらくたったある日，卒業研究のテーマを決めるためのゼミが開催された．記憶によると，先生方から四つほどテーマが提示された．その中の一つが松本先生から提示された量子暗号に関するテーマであった．当時，量子暗号については新聞の科学記事でキーワードを見聞きしたことがあるだけでほとんど何も知らなかったが，「量子」と「暗号」が掛け合わさった妖しさに魅力を感じ，このテーマを卒業研究として選ぶことにした．

量子暗号（量子鍵配送）とは，送受信者間で秘密鍵を共有するためのプロトコルで，ランダムに発生させたビット列を光子の偏向に変調させて送る．その過程でもし盗聴者がいたとしても，量子力学の原理に基づき情報の漏えい量を推定できるのが特徴である．そして，情報漏えい量が十分に少ないときは，伝送したビット列に対してディジタルな情報処理を施すことで，安全な秘密鍵を共有することができる．量子暗号は最初の光子を伝送する部分以外はほとんどディジタルな情報処理である．特に，盗聴情報量の推定や秘密鍵生成の手続きは情報理論の守備範囲である．そのような視点から研究を進めていくことで，従来より高い鍵生成レートを有するプロトコルを提案することができ，幾つかの成果を上げることができた(2)～(4)．

このような次第で学生時代は松本先生指導の下，量子暗号やそれに関連する情報理論的セキュリティの研究を

主に行っていた．量子暗号の研究を始めたきっかけは偶然であったが，学生のうちに量子情報理論に関する基礎的な知識を身に付けることができたのは，その後の研究キャリアにおいて非常に重要なことであったと思う．文献(5)で林先生（名古屋大学・シンガポール国立大学）が述べているように，量子情報理論の知見は，通常の情報理論の研究をする際にも大きなアドバンテージとなるからである．量子暗号の研究をしていたため，林先生とも学生時代から交流があった．そのことがきっかけで，後に有限長解析等について共同研究をさせて頂き様々なことを学んだ．

2.2 徳島大学にて

博士号取得後は，徳島大学に助教として着任した．当時徳島大学では，大濱先生（現電気通信大学）により情報通信講座が運営されていた．

情報理論における符号化定理の研究は，通信システムにおいてある通信レートの符号が存在することを証明する符号化順定理と，ある通信レート以上の符号は存在しないことを証明する符号化逆定理に大別することができる．多くの場合，「存在する」ことを証明するより「存在しない」ことを証明する方が困難であり，未解決問題は逆定理が証明できずに未解決となっていることが多い．そのような中，大濱先生は困難なマルチユーザ情報理論における符号化逆定理の研究に熱心に打ち込まれていた．その影響もあり，筆者も次第に逆定理の研究に興味を持っていった．

ここで，徳島大学にいた頃に行ったマルチユーザ情報理論の研究を一つ紹介したい．マルチメディアコンテンツ配信等の普及により，多数の受信者に対して効率的にデータを送る問題は非常に重要になってきている．特に，動画像の送信において，あるフレームを符号化する際に前のフレームを受信側で補助情報として参照する分散符号化テクニックが注目を集めている．情報理論において，多数の受信者がいる分散符号化の研究は歴史が長く，Heegard と Berger によって 1985 年に始められた[6]．彼らの研究によって，多数の受信者の間にある種の順序構造を有するモデル（劣化形と呼ばれる）においては，最適な符号化法が明らかにされていたものの，順序構造を有しない一般的なモデルは長い間未解決問題であった．筆者はこの問題の解決の糸口を探るために，順序構造を有しない典型的な場合として，データが二つの統計的に独立なベクトルから成る特殊な場合に取り組み，最適な符号化法を明らかにした[7]．この問題でも困難なのはやはり逆定理の証明であった．この研究を通じて，逆定理を示す大変さ並びに面白さを実感できたように思う．

2.3 メリーランド大学にて

2013 年春から約 2 年間，日本学術振興会の海外特別研究員制度を使って米国，メリーランド大学に滞在した．現地でのホストは Prakash Narayan 先生にお願いした．Narayan 先生は情報理論において幅広く研究されているが，特に情報理論的セキュリティを精力的に研究されており，筆者の興味とマッチしたためである．

Narayan 先生のグループは博士課程の学生が二人いるだけだったため，滞在中はディスカッションに多くの時間を取って頂くことができた．密度の濃い研究をするために，学生は一度に二人までしか採らないと決めているそうである．研究グループの大所帯化が進んでいる米国では珍しいことだと思われる．

メリーランド大学滞在中は当時 Narayan 先生の学生だった Himanshu Tyagi 博士（現 Indian Institute of Science, Bangalore）と意気投合し，様々な共同研究を行った．そのうちの一つでは，後述の符号化問題を仮説検定に対応させる方法により（3.2 参照），マルチパーティの秘密鍵共有問題に対して，非漸近的な逆定理のバウンドを導出することに成功した[8]．また，その結果を応用することで，暗号理論で活発に研究されている秘匿計算（Oblivious Transfer や Bit Commitment）に対しても，非漸近的なバウンドを出すことができた．

Tyagi 博士との親交は互いに帰国した後も続き，インドを訪問する機会も何度かあった．インド訪問はカルチャーギャップにより驚きの連続であったが，非常に楽しいものであった．

2.4 東京農工大学にて

米国から帰国した後，東京農工大学へ異動することとなった．最近は，後述の関数計算の問題（3.2 参照）やマルチユーザ情報理論における有限長解析並びに二次オーダ解析に興味を持って取り組んでいる．

従来の情報理論では遅延を許容し十分に長いブロック長で符号化した際の通信システムの漸近的な性能解析を行うことが多かったが，最近は有限のブロック長での性能解析が盛んに行われるようになってきている[9],[10]．例えば通信路符号化において，高い信頼性で送ることができるメッセージのビット数は，通信路容量を C としたとき漸近的に $nC+o(n)$ のような振舞いをすることはよく知られている．二次オーダ解析とは，許容する誤り確率 ε に対して $nC-\sqrt{nV}\,\mathrm{Q}^{-1}(\varepsilon)+o(\sqrt{n})$ のように(注2)，$\sqrt{n}$ の係数まで求める解析手法であり，有限長性能の良い近似値を与えることから注目を集めている．（有限長解析や二次オーダ解析の詳細については，例えば文献(11)を参照．）

(注 2)　ここで，$\mathrm{Q}(t)$ は標準ガウス確率変数の裾確率．

さて，マルチユーザ情報理論の符号化問題には解析を難しくする二つの要因がある．一つは，マルチユーザネットワークにおいて特殊な符号化法を使うことに起因する補助確率変数の存在である．もう一つは，分散符号化に起因する確率変数間のマルコフ連鎖の条件である．まずは一つ目の困難性を解決するために，筆者は Gray-Wyner ネットワークと呼ばれる問題に取り組み，最適な二次オーダのレート領域を導出することに成功した[12]．二つの困難性が混在する問題に対する解決の見通しは立っていないものの，難しさの要因が何なのか少しずつ分かってきた．これについては 3.3 で述べる．

3. 今後の展望

本章では，情報理論において今後 100 年の間に発展すべき重要な研究の方向性を紹介し，その展望を述べる．既に述べたように，情報理論における未解決な符号化問題の多くは逆定理の困難性に起因することが多いため，以下で紹介するのは逆定理の証明手法に関するものに偏ってしまった．しかしながら，順定理における重要な研究がないわけではない．これは誌面の都合並びに筆者の浅学によるものである．

3.1 Single Letter Characterization

Shannon によって示された通信路符号化定理は，与えられた通信路 $W(y|x)$ に対して通信路容量 $C(W)$ が，入力分布を P_X としたときの入出力間の相互情報量 $I(X \wedge Y)$ を用いて[注3]，

$$C(W)=\max_{P_X} I(X \wedge Y) \qquad (1)$$

のように通信路を“1 回”使用した際の最大相互情報量として表現できることを述べている．さて，この定理はなぜ有用なのだろうか．もし，

$$C(W)=\lim_{n\to\infty} \frac{1}{n} \max_{P_{X^n}} I(X^n \wedge Y^n) \qquad (2)$$

のように，通信路を“n 回”使用した際の最大相互情報量の極限として表現されているだけだったとしたらどうだろうか．情報理論では通称，式(1)のような表現は Single Letter Characterization（SLC），式(2)のような表現は Multi Letter Characterization（MLC）と呼ばれる．前者はブロック長 n によらない計算量で通信路容量を計算することができるのに対し，後者を計算するにはブロック長 n を大きくしながら入力分布に関する最適化問題を解く必要がある．つまり，符号を設計するための指針であるはずの通信路容量を計算するために，符号を実際に作る並の労力が必要になってしまうわけである．このような理由により，情報理論では SLC を求めることが極めて重要な課題となる．

さて，情報理論の問題では逆定理において MLC から SLC を求めるのが困難であることが多い．特にマルチユーザ情報理論の問題では，エントロピーの連鎖則等を極めて技巧的に利用することで SLC は導出される．また，2.4 で述べたように，マルチユーザネットワーク特有の補助確率変数をいかに導入するかが困難になる．現在知られている SLC の方法は問題（対象とする通信システム）ごとに経験則に基づき場当たり的に提案されているものがほとんどである．したがって，現在未解決である通信システムの限界を求めるには，よりシステマティックな SLC の導出法の発展が望まれる[注4]．また，既に漸近的な限界が求まっている通信システムに対しても，有限長解析並びに二次オーダ解析を考える際には，既存の SLC の議論は使えないことが多く，SLC の方法を抜本的に見直す必要があるかもしれない．

SLC の導出法を探求することの他分野への波及効果についても触れておきたい．例えば，計算機科学における communication complexity の分野で活発に研究されている直和問題が挙げられる．直和問題では，「ある関数を分散計算するために必要な通信量」に対して，「同じ関数を n 回まとめて計算するための通信量」が n に応じてどのようなオーダで増加するかといったことを考える．そのような問題を解くためのツールとして近年，information complexity と呼ばれる手法が提案されている[15]．計算機科学の文献では余り明確には述べられていないが，この手法は情報理論の SLC の考え方に類似のものである[注5]．また，最近は hypercontractivity 係数のテンソル性と SLC の関係も報告されている[19]．今後，情報理論の分野で開発された SLC の導出法が情報理論にとどまらず，他の多くの分野へ展開されることを期待したい．

3.2 Reduction

Reduction（帰着）とは計算量理論や暗号理論で使われる用語で，あるタスク P を解くためのアルゴリズム A が与えられたとき，別のタスク Q を解くためのアルゴリズム B を A から（効率的に）構築できるならば，「タスク Q はタスク P に reduction される」といった言

(注3) 相互情報量は $I(X;Y)$ のように表記されることが多いが[13]，相互情報量は対称性 $I(X;Y)=I(Y;X)$ を満たすことから，Csiszár 教授をはじめとするヨーロッパの情報理論研究者の間では $I(X \wedge Y)$ のような表記法が使われている[14]．最近は筆者も Narayan 先生の勧めでこちらの表記法を使用するようにしている．

(注4) このような問題意識は徳島大学にいた頃に大濱先生から教わった．

(注5) 特に，amortized communication complexity と information complexity の等価性を導いている手法は[16]，正に SLC の導出法そのものである[17],[18]．

い方をする．このような考え方は計算量理論における NP 完全性の証明や，暗号理論における安全性証明等に頻繁に使われる．例えば，一方向性関数の存在を仮定し構成した擬似乱数生成器の安全性を議論する際には(注6)，生成した擬似乱数を真性乱数と識別するアルゴリズムがあったとしたら，一方向性関数の逆像を計算するアルゴリズムを構築できてしまうといった論法で証明する．

上述のような reduction の考え方は，情報理論において逆定理を示す際にもしばしば有効になる．ある（符号化）問題 P の符号を用いて別の問題 Q の符号が構成できたとしよう．つまり，問題 Q の方が問題 P よりある意味で簡単であると言えたとしよう．すると，適当な尺度の対応付けを行うことで，問題 P の限界を問題 Q の限界で抑えることができる．このような論法で最も成功を収めているものの例としては，通信路符号化における meta converse 法が挙げられる(注7)．Meta converse 法では，通信路符号化（問題 P）を統計学における仮説検定（問題 Q）に関連付けることで逆定理を導く．与えられた通信路符号化のための符号を用いて，実際の通信路と，通信路容量が 0 である仮想的に与えられた通信路との検定を行うのである．ここで，問題 Q として解析が容易なもの（少なくとも問題 P よりは解析がしやすい問題）を選ぶことがポイントである．2.3 で述べた秘密鍵共有のバウンドも同様な論法で導出されている．また，このような論法は，複数回繰り返すことも有効である．例えば，先の論文（8）では，秘匿計算の問題におけるプロトコルが存在したとしたら，秘密鍵共有のプロトコルを構築することができ，その鍵共有プロトコルから仮説検定法が構築できるといった二段構えの reduction によって，秘匿計算のバウンドを導出している．

Reduction の考え方が有効な他の問題としては，分散関数計算の問題が挙げられる．この問題では，観測データを分散符号化によって通信することで，復号器側で観測データの関数値を計算することを目的とする．関数計算の問題では復号器で観測データそのものを復元する必要がないため（関数の値域は 1 bit だけの場合もある），通常の符号化問題において逆定理を示すためのテクニックはほとんど役に立たない．特に，Ahlswede-Csizsár によって示された sensitive な関数族に対する結果は証明が非常に難解で(20)，後に El Gamal による平易な証明が示されていたものの(21)，理解するのに非常に苦労した．この問題は 2014 年頃から興味を持ち始め，葛岡博士（和歌山大学）と共同で研究を開始した(22)．そしてようやく最近になって，ある種の構造を有する関数族に対しては，Slepian-Wolf 符号化（問題 Q）から関数計算（問題 P）への reduction を示すことで，非常に直感的で簡明な証明を与えることができた(23)．

以上幾つか例示してきたように，reduction は逆定理を示す際に非常に有効な考え方である．このような方法では reduction の段階は操作的な議論なため，情報理論でよく考えられる定常無記憶性等を仮定せずに行えるという利点もある(注8)．今後このような方法はますます重要になってくるのではないだろうか．本節の冒頭で述べたように，reduction は計算機科学や暗号理論で頻繁に使われる考え方である．したがって，それらの分野からアイデアを取り入れることで，情報理論のテクニックは更に発展することが期待できる．その一方で，情報理論で発展したテクニックを他の分野の問題に適用してみるのも面白い．

3.3 Isoperimetric 問題

Isoperimetric 問題（等周問題）とは，「面積が一定の下で周囲の長さが最小になる閉曲線は何か」といった古代から考えられていた幾何学の問題で，円が最適解になることはよく知られている(注9)．情報理論でもこのような極値問題はしばしば登場する．ここではそのような問題の中から，筆者が最近興味を持っているものを一つ紹介したい．

通信路 $W(y|x)$ を反転確率が p の二元対称通信路とする．与えられた入力集合 $\mathcal{A}_n \subseteq \{0,1\}^n$ に対して，できるだけ小さな出力集合 $\mathcal{B}_n \subseteq \{0,1\}^n$ によって，任意の $x^n \in \mathcal{A}_n$ を通信路 W^n で送った際に高確率で受容できるようにしたい．そこで，与えられた $0 \leq \varepsilon < 1$ に対して，$\mathcal{A}_n$ の W^n による image size として

$$g_{W^n}(\mathcal{A}_n, \varepsilon) := \min\left\{ |\mathcal{B}_n| : \sum_{y^n \in \mathcal{B}_n} W^n(y^n|x^n) \geq 1-\varepsilon, \quad \forall x^n \in \mathcal{A}_n \right\} \tag{3}$$

のように定義する．このとき，入力集合のサイズが一定の下で image size $g_{W^n}(\mathcal{A}_n, \varepsilon)$ はどのように表現できるのだろうか．このような問題は image size characterization と呼ばれ(14)(注10)，マルチユーザ情報理論における符号化問題の強逆定理を示すための道具として導入された(25)(注11)．漸近的な振舞いについては解決済みで，与えられた $0 < r < 1$ に対して，入力集合が

$$\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{A}_n| \geq r \tag{4}$$

（注 6） 一方向性関数とは，簡単に計算することができるが，逆関数の計算が非常に困難な関数を指す．例えば，二つの素数の積を計算するのは容易であるが，合成数を素因数分解するのは困難であると考えられている．

（注 7） Meta converse の詳細や発展の歴史については文献（5）を参照．

（注 8） 定常無記憶性等を仮定せずに一般的な符号化定理を導出する手法としては情報スペクトル的方法がある(24)．実際，前述の meta converse 法は情報スペクトル的方法から派生したものである．

（注 9） もちろん多次元版も考えることができ，超球が解となる．

（注 10） ここでは議論を簡単にするため，二元対称通信路に限ったが，image size characterization はより一般の通信路に対しても定式化できる．

というレート制約を満たす下で，image size は

$$\liminf_{n\to\infty}\frac{1}{n}\log g_{W^n}(\mathcal{A}_n,\varepsilon)\geq h(h^{-1}(r)*p),\quad \forall 0<\varepsilon<1 \tag{5}$$

のような不等式を満たすことが知られている．ただし，$h(\cdot)$ と $h^{-1}(\cdot)$ は二元エントロピー関数とその逆関数，$a*b=a(1-b)+b(1-a)$ は二元畳込みである．また，式(5)の不等式は，入力集合 $\mathcal{A}_n$ として半径 $nh^{-1}(r)$ の n 次元ハミング球 $\mathcal{H}_n(nh^{-1}(r))$ に取ることで等号が達成される．ここで，$\frac{1}{n}\log|\mathcal{A}_n|$ を $\mathcal{A}_n$ の面積，$\frac{1}{n}\log g_{W^n}(\mathcal{A}_n,\varepsilon)$ を $\mathcal{A}_n$ の周囲の長さとみなすと，上記の結果は通信路の image size に関する isoperimetric 問題と考えることもできる．

上記の image size characterization 問題をより精密な形で解くことができれば，マルチユーザ情報理論における符号化問題に対して，より精密な解析を行えるのではないかと考え，筆者はこの問題に興味を持った．この問題は isoperimetric 問題の一種と考えると，式(5)のような漸近的な場合だけでなく，有限の n に対してもハミング球が最小の image size を持つのではないかと予想したくなる．仮に全ての n では成り立たないとしても，$\frac{1}{n}\log|\mathcal{A}_n|\geq r$ が各 n で満たされているとき，

$$\begin{aligned}&\liminf_{n\to\infty}\frac{1}{\sqrt{n}}(\log g_{W^n}(\mathcal{A}_n,\varepsilon)-nh(h^{-1}(r)*p))\\&\geq\lim_{n\to\infty}\frac{1}{\sqrt{n}}(\log g_{W^n}(\mathcal{H}_n(nh^{-1}(r)),\varepsilon)-nh(h^{-1}(r)*p))\end{aligned} \tag{6}$$

のような二次オーダの isoperimetric 不等式は成り立つのではないだろうか．

Isoperimetric 問題はもっともらしい主張にもかかわらず証明が困難なのが常である．式(6)を証明するためにいろいろな手を試してみたが，今のところ証明の見通しは立っていない．式(5)を証明する際には，blowing-up 補題と呼ばれる measure concentration[28]のテクニックが重要な役割を果たすが，式(6)を証明するには不十分なようである．したがって，マルチユーザ情報理論における精密な解析を行うには，blowing-up 補題に代わる新しいテクニックの発展が望まれる．

式(6)の成否は明らかではないものの，組合せ論において以下のような類似の結果が知られている．二元対称通信路の代わりに，通信路 $W^n(y^n|x^n)$ では t 個以下の任意の誤り（反転）が起きるとしよう．そして，$x^n\in\mathcal{A}_n$ を送ったとき，出力を必ず受容できるように $\mathcal{B}_n$ を取りたいとする．すると，image size $g_{W^n}(\mathcal{A}_n,0)$ は $\mathcal{A}_n$ に含まれるベクトルとハミング距離が高々 t 以下のベクトルを全て集めた集合 $\Gamma^t(\mathcal{A}_n)$ のサイズになる．このとき，$|\mathcal{A}_n|\geq|\mathcal{H}_n(d)|$ の下で，

$$\begin{aligned}|\Gamma^t(\mathcal{A}_n)|&\geq|\Gamma^t(\mathcal{H}_n(d))|\\&=|\mathcal{H}_n(d+t)|\end{aligned} \tag{7}$$

が成り立つ．この結果は Harper の vertex isoperimetric 不等式と呼ばれている(注12)．

タイプの理論をはじめとし，情報理論において組合せ論的な方法が有効なことはよく知られている．その一方で，情報理論で発展した手法が組合せ論においても有効であるといった結果も報告されている[26),(27)]．例えば，前述の不等式(7)の edge 版である Harper の edge isoperimetric 不等式は，結合エントロピー間の不等式である Han の不等式を使うと容易に示すことができる（文献(28)4.4 節）．今後は，情報理論と組合せ論はますます交流が盛んになっていくのではないだろうか．

4. お わ り に

Shannon によって始められた符号化定理を示すといった方向の研究は，今後も情報理論の一つの柱であり続けるであろう．しかしながら，情報理論の研究はそのようなものに限られるわけではない．3. で見たように情報理論は分野の中で閉じているわけではなく，時にはアイデアを輸入し，時にはアイデアを輸出しながら発展してきたわけである．今後は情報理論で育まれた議論を更に洗練し，他の分野に応用していくといった，テクニックとしての情報理論もますます重要になるのではないだろうか．

冒頭でも述べたように，情報理論は 100 年後も何らかの形で残り続けているはずである．それがどのような形であるか，今はまだ分からない．情報理論の将来は，今現在を生きる研究者たちの手によって創られていくからである．筆者もそのような研究者たちの一人として，22 世紀の情報理論に少しでも影響を残せるよう日々精進していく所存である．

（注 11） 情報理論における通常の逆定理（弱逆定理とも呼ばれる）では，例えば通信路符号化問題の場合，通信路容量より高い通信レートで漸近的に誤り確率が 0 に収束するような符号化法は存在しないことを証明する．一方，強逆定理では，通信路容量より高い通信レートを有する任意の符号化法は，漸近的に誤り確率が 1 に収束することを証明する．誤りを少し許容したとしても通信路容量より高いレートでは通信できないという意味で，後者は前者より強い主張になっている．

（注 12） 組合せ論において isoperimetric 問題はグラフ上の問題として扱われることが多く，edge isoperimetric 問題と vertex isoperimetric 問題に区別される．

文　　献

（1） 植松友彦，“情報理論，”電子情報通信学会 100 年史，基礎・境界，電子情報通信学会，2017.

（2） S. Watanabe, R. Matsumoto, and T. Uyematsu, “Noise tolerance of the BB84 protocol with random privacy amplification,” International Journal of Quantum Information, vol. 4, no. 6, pp. 935-946, Dec. 2006.

（3） S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, “Key rate of quantum key distribution with hashed two-way classical communication,” Phys. Rev. A, At. Mol. Opt. Phys., vol. 76, no. 3, p. 032312, Sept. 2007.

（4） S. Watanabe, R. Matsumoto, and T. Uyematsu, “Tomography increases key rates of quantum-key-distribution protocols,” Phys. Rev. A, At. Mol. Opt. Phys., vol. 78, no. 4, p. 042316, Oct. 2008.

（5） 林　正人，“情報理論における量子情報理論の役割―非可換拡張を超えて―，”信学 FR 誌，vol. 10, no. 1, pp. 4-13, July 2016.

（6） C. Heegard and T. Berger, “Rate distortion when side-information may be absent,” IEEE Trans. Inf. Theory, vol. 31, no. 6, pp. 727-734, Nov. 1985.

（7） S. Watanabe, “The rate-distortion function for product of two sources with side-information at decoders,” IEEE Trans. Inf. Theory, vol. 59, no. 9, pp. 5678-5691, Sept. 2013.

（8） H. Tyagi and S. Watanabe, “Converses for secret key agreement and secure computing,” IEEE Trans. Inf. Theory, vol. 61, no. 9, pp. 4809-4827, Sept. 2015.

（9） M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” IEEE Trans. Inf. Theory, vol. 55, no. 11, pp. 4947-4966, Nov. 2009.

（10） Y. Polyanskiy, H.V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2307-2359, May 2010.

（11） 林　正人，“情報スペクトルによる二次オーダーの情報理論―一次漸近論を超えて―，”信学 FR 誌 , vol. 6, no. 1, pp. 12-25, July 2012.

（12） S. Watanabe, “Second-order region for Gray-Wyner network,” IEEE Trans. Inf. Theory, vol. 63, no. 2, pp. 1006-1018, Feb. 2017.

（13） T.M. Cover and J.A. Thomas, Elements of Information Theory, Wiley-Interscience, 2006.

（14） I. Csiszár and J. Körner, Information Theory : Coding Theorems for Discrete Memoryless Systems, Cambridge University Press, 2011.

（15） B. Barak, M. Braverman, X. Chen, and A. Rao, “How to compress interactive communication,” SIAM J. Comput., vol. 42, no. 3, pp. 1327-1363, June 2013.

（16） M. Braverman and A. Rao, “Information equals amortized communication,” IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 6058-6069, Oct. 2014.

（17） N. Ma and P. Ishwar, “Some results on distributed source coding for interactive function computation,” IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 6180-6195, Sept. 2011.

（18） A.H. Kaspi, “Two-way source coding with a fidelity criterion,” IEEE Trans. Inf. Theory, vol. 31, no. 6, pp. 735-740, Nov. 1985.

（19） S. Beigi and A. Gohari, “On the duality of additivity and tensorization,” arXiv : 1502.00827.

（20） R. Ahlswede and I. Csiszár, “To get a bit of information may be as hard as to get full information,” IEEE Trans. Inf. Theory, vol. 27, no. 4, pp. 398-408, July 1981.

（21） A.E. Gamal, “A simple proof of the Ahlswede-Csiszár one-bit theorem,” IEEE Trans. Inf. Theory, vol. 29, no. 6, pp. 931-933, Nov. 1983.

（22） S. Kuzuoka and S. Watanabe, “A dichotomy of functions in distributed coding : An information spectral approach,” IEEE Trans. Inf. Theory, vol. 61, no. 9, pp. 5028-5041, Sept. 2015.

（23） S. Kuzuoka and S. Watanabe, “On distributed computing for functions with certain structures,” arXiv : 1602.08204.

（24） T.-S. Han, Information-Spectrum Methods in Information Theory, Springer, 2003.

（25） R. Ahlswede, P. Gác, and J. Körner, “Bounds on conditional probabilities with applications in multi-user communication,” Z. Wahrscheinlichkeitstheor. verwandte Geb. , vol. 34, pp. 157-177, 1976.

（26） R. Ahlswede and N. Cai, “General edge-isoperimetric inequalities, Part I : Information-theoretic methods,” Eur. J. Comb., vol. 18, no. 4, pp. 355-372, 1997.

（27） J. Radhakrishnan, “Entropy and counting,” IIT Kharagpur Golden Jubilee Volume, 2001.

（28） S. Boucheron, G. Lugosi, and P. Massart, Concentration Inequalities : A Nonasymptotic Theory of Independence, Oxford University Press, 2013.

（平成 28 年 12 月 27 日受付　平成 29 年 2 月 6 日最終受付）

渡辺　峻（正員）

平 17 東工大・工・情報卒．平 19 同大学院修士課程了，平 21 同大学院博士課程了．同年，徳島大助教．平 25～27 学術振興会海外特別研究院，メリーランド大客員助教．現在，東京農工大・工・情報・准教授．多端子情報理論，量子情報理論の研究に従事．博士（学術）．平 22 年度本会論文賞受賞．現在，IEEE IT Trans. 編集委員に従事．