

SITA 情報理論とその応用学会ニューズレター

理想暗号を求めて 8 年(私の Key Paper)	田中 初一
情報理論研究(日本)のあけぼのーその 2	有本 卓
SITA'93 報告	武部 幹
ワークショップ「変動現象の力学系モデル」報告	佐藤俊輔
国際会議のお知らせ	
IEEE ISSSTA'94	中川 正雄
QCM'94	広田 修
博士論文要旨	
情報源符号化の幾何学的小および確率論的研究	川端 勉
電子メールの有効利用	編集理事
情報理論とその応用学会 1993 年度総会報告	事務局
平成 5 年度第 2 回理事会議事録	事務局

理想暗号を求めて 8 年

ー私の Key Paperー

田中初一(神戸大)

先日、金沢で開催されました SITA'93 のオープニング・パーティの席上、編集理事の橋本猛先生から“ニューズレターの新しい企画として「私の Key Paper」という読みものを掲載することになったのですが如何でしょうか？”と御相談がございまして、お酒の勢いで軽率に“それは大変面白い企画ですね”と賛辞を表わしたのが運の分かれ道、自分が最初の原稿を執筆するはめになりました。この新しい企画を成功させなければならない、という大変な重責を感じております。

研究テーマの選定に少なからず影響を与えた私の“Key Paper”は、Crypto'84 で発表された Adi Shamir 著の論文“Identity-Based Cryptosystems and Signature

Schemes”であります。また、この論文は私の暗号研究の歴史の中で思い出の多い論文でもあります。1985 年の春先、当時大阪大学工学部の通信工学科に在籍されておられた笠原正雄先生（現在京都工芸繊維大学教授）に“関西に何か非公式な暗号の研究会を作りませんか？符号理論の次は暗号が重要になると思うのですが…”と御相談申し上げまして“Crypto 関西”という全く非公式な研究会が発足することになり、月一回のペースで大阪大学で暗号理論の勉強会を始めました。因みにこの“Crypto 関西”という素晴らしい名前の名付け親は、三菱電機に勤務されております符号理論の大家、井上徹氏であります。上掲の Shamir の論文は、Crypto 関西で私がみなさんに紹介した思い出

の深い論文であります。まずこの論文の歴史的背景から紹介しましょう。1976年にDiffieとHellmanにより、極めて画期的な公開鍵暗号系の概念が提案され、2年後の1978年にはその概念の実現法として有名なRSA暗号が提案されました。また1985年にはElGamal公開鍵暗号系が提案され、世は正に現代暗号の研究の春、とりわけ公開鍵暗号系が隆盛をきわめた時代でありました。Shamirの論文は公開鍵を個人の名前や住所、電話番号などの固有情報で置き換えることにより、公開鍵暗号系の公開鍵リストをも排除し、郵便型の通信を可能にするという夢のような理想的な暗号系の概念を提案したものであります。ID情報に基づく署名法の実現法については、Shamir自身がこの論文の中で素晴らしい実現法を提案しておりますが、ID情報に基づく暗号系の実現法については何の提案もなく、また実現できるかどうかとも明らかではありません。しかし画期的なID暗号の基本概念が実に魅惑的に記述されており、今すぐにでも素晴らしい理想的な暗号系が実現できそうな気がして、読み進むにつれて読者をずるずるとその基本概念の中に引き込んで行きます。たとえば、原論文中に次のような読者の研究心を奮い立たせる大変興味深い一節があります。

“This situation is reminiscent of the 1976 period, when public key cryptosystems were defined and their potential applications were investigated even though the the first concrete implementations were published only in 1978…”

1976年は公開鍵暗号系の概念が提案された年を示し、1978年はその概念の実現法として有名なRSA暗号が提案された年を示しているようです。私はこの素晴らしいID暗号の概念に魅惑され、実現法の研究へと駆り立てられました。1985年の紅葉の美しい季節のことです。翌1986年7月、“ID情報に基づく暗号系の一実現法”(信学技法IT86-38)と題して最初の研究成果を報告致しました。しかし残念ながら、NECの岡本栄司氏(現在、北陸先端大教授)と横浜国大の松本勉助教授によりアタックされ、結託という手段によりセンタ秘密を露呈させるという見事なアタックの前に最初のアイディアは一瞬のうちに崩れ去りました。その時、はじめて“結託”というアタックの強力さとその恐ろしさが身にしました。何もかも消えてしまったとき、日本で最初の研究であったというささやかな誇りと必ず結託に対しても安全な実現法を提案す

るという決意のみが残りました。その後、岡本栄司氏を中心とするNECグループおよび今井秀樹教授、松本勉助教授のグループによってID暗号の研究成果が報告されました。前者の研究は、後にID情報で認証機能を付与した公開鍵配送方式であることが判明し、真にID暗号ではないことが判明しました。後者の研究はKPSと名付けられLSIにより実現システムを作成されましたが、既に1982年にBlomにより類似の鍵共有法が提案されていることが分かり、研究会等の席で議論になったことは記憶に新しいところです。その後、辻井重男教授を中心とする東工大のグループおよび館林誠氏を中心とする松下電器のグループがID暗号の研究に参入され、少し遅れて笠原正雄教授を中心とする京都工繊大のグループが研究を始められました。このようにID暗号の研究者数が急激に増加し、それに応じて研究成果の報告も増加し、ID暗号の研究に関しては世界をリードするまでになりました。また東京理科大で開催されました「1987年暗号と情報セキュリティワークショップ」ではID暗号に関するパネル討論が企画され、活発な討論が繰り広げられ、幾多の新しい知見が得られました。しかし、暗号技術は“両刃の剣”でございまして、アタックのテクニックも急激に進歩し、結託に基づく各種の強力なアタック、ユークリッドアタック、ベキ積アタックなどによりほとんど全ての実現法がアタックされ、ユーザ数を制限したり、秘密情報が読み出されないモジュールを使用するというような制限条件を付けない限り、いずれの実現法も安全な実現法にはなりません。その結果、ID暗号の安全な実現法は存在しないのではないか、存在しないことを証明できないか、などの悲観論が大勢を占めるようになり、いつの間にかShamirにより提案された素晴らしい魅力的な基本概念を実現する真のID暗号を構築するという意気込みが薄れて行きました。そして、結託しきい値が高ければ実用上問題はない、という考え方に基づき結託しきい値の高さをその実現法の良さの評価に用いられるようになったのです。いわゆるID暗号の“冬の時代”を迎え、多数の研究者がこの研究に魅力をなくし、手を引いてしまいました。これは1989年から1991年頃の出来ごとであります。その後ID暗号の研究を続けているのは、辻井教授、笠原教授及び私の僅か3グループ(3人といってもよいかな)になってしまいました。さて、このようにID暗号の研究が冬の時代に入り、暗号理論の大家から“離散

対数にトラップが埋め込めない限り、真の ID 暗号の実現法は存在しないように思う”、“制限条件を付けて、その条件毎に ID 暗号の実現法をまとめられたらどうか”、“真に安全な ID 暗号は存在しないのではないか”など悲観的な意見が圧倒的に多い中、私は長年続けてきた ID 暗号の研究を諦めるべきかどうか、本当に悩みました。ID 暗号の研究を始めてから 7 年が経過し、本当に無駄な時間を浪費したなあ、という自己嫌悪の念でいっぱいになりました。その反面、安全な ID 暗号の簡潔な実現法の魅力も捨てきれませんでした。私の心の中で葛藤が始まったのです。その時、ふと頭の中に“冬来れば春遠からじ..”という一節が浮かび、もう一度だけ真の ID 暗号の実現法の研究に挑戦してみよう、と思いました。ただし、もう一度 ID 暗号の基本概念に戻り、ID 暗号が保有すべき条件・構造を徹底的に再検討すると共に、これまでに提案された多数の実現法がなぜブレイクされたのか、その根本原因を再確認して、それらの問題点を排除するにはどのような構造にすればよいのか、を考えていくという方向で研究を続けていくことに致しました。これまでに提案された結託しきい値のある ID 暗号を私は第一世代の ID 暗号と名付けています。それは結託しきい値のない真に Shamir の基本概念を実現する第二世代の ID 暗号の存在を確信しているからです。これからの ID 暗号の研究は第二世代の ID 暗号系を目指すべきであると思っています。それは単なる妄想ではなく、現代暗号の進歩の歴史すなわち公開鍵暗号系の進歩と ID 暗号の進歩をアナロジーして得られた結果であります。最近、海外の暗号研究者も ID 暗号の素晴らしさに魅惑されて、研究を始めているようです。彼らが本格的に研究を始めると、たちまち多くの研究成果が報告され、RSA 暗号系に匹敵するような計算量的安全性に基づく素晴らしい ID 暗号系の実現法が、世界のどこかで発表されるかも知れない。最近、やっと長い間私の脳裏を悩ませた自己嫌悪感と悲観的な考え方が薄れて、何か RSA 暗号に匹敵するような計算量的安全性に基づく真の ID 暗号が存在するようになってきて ID 暗号時代到来の“あけぼの”がほのかに見

えるような気がしております。

このように何らの研究成果を得ることもなく、ひたすら理想の暗号という“夢”を追い続けた 8 年間ではございましたが、以前の研究生生活では決して得られなかった貴重な教訓を得ることができました。まず、研究の対象としている問題に関連した諸知識が整理され、その問題の核心部分の本質のみが悩みのキャンパスに明確に浮かび上がるようになったとき、はじめてその解への素晴らしいアイデアが誘発されるということです。おそらく皆様方も経験をお持ちのことと思いますが、就寝前にビールでも飲んで何もかも忘れて眠り込み、夜中の 3 時か 4 時頃に目を覚ますと、急に前の日に考えていた問題の核心部分がくっきりと悩みのキャンパスに描かれ、同時にその解も与えられる、という大変面白い経験を致しました。これは寝ている中に前の日に考えていた色々な情報が整理されて雑音が消去され、問題の核心部分のみが悩みに浮かび上がるという不思議な現象であると思います。つぎに、研究における独創性の重みについての認識が変わりました。研究によって新しい知見を得るために費やす努力を 100 と致しますと、その研究成果を模倣したり破壊するためには 10 の努力で十分であり、それを“論評”するに要する努力は僅か 1 で十分である。すなわち、真に創造性を発揮することの偉大さと重要性を身をもって知りました。また、この ID 暗号の研究を通じて、“A simple result is the best”という本当の意味が何となく分かるようになりました。最後に、化学技術の研究とは直接の関係はないのですが、研究発表とそれに対する反応から“人の心”が読み取れる、という人間くさい一面を垣間見たような気が致します。

Shamir の論文に魅惑され、理想暗号の“夢”を追い求めた 8 年間の精神的葛藤の道程を、恥も外聞も考えずに紹介させて頂きましたが、過ぎ去った自分の研究生生活について、くどくどと Complain するのは研究者の終エンを意味するのもかも知れない。

情報理論研究(日本)のあけぼの—その2(完結)

有本 卓(東大)

1968年に阪大基礎工学部に移った時、招いて頂き、所属したのは機械工学科だったので、専門としては機械制御の研究をやらねばならないことになっていたし、実際、研究は機械系の制御に向けて走り出していた。情報理論の勉強を本格的に始めてのは1969年の学園紛争で大学に行けなくなり、暇な時間が出来たときであった。1967年頃、日本では、シャノンの定義したエントロピーやハフマン符号に基づく情報源符号化の意義は判るが、通信路符号化の方は何を行っているのか良く判らないという定評があった。数学者を含む秀才たちの集まったある私的な研究会でも本質的には理解が進まなかった、という話しも伝わって聞こえていた。数学的な証明がsophisticatedで理解出来なかったというだけでなく、誤り訂正の符号化によって系列を冗長にしていけば誤り率が改善できるようになるのは当たり前のようなのに、証明が数学的に難しくなるのはどうしてだろう、等々と言われていた。1969年、自分自身でファノの教科書から、Gallagerの論文[10]へと読み進んだとき、定理の数学的証明がきっちり呑み込めましたが、更に、通信路符号化定理の心はむしろ、冗長性の割合は一定にしたまま（伝送速度を犠牲にしないで）、符号器を複雑にするだけでいくらかでも誤り率が改善できるという統計物理的現象にあることを知り、感銘を覚えるとともに、工学的手段の存在と限界が理路整然と決まる数理的構造に美しさすら感じたのである。学園紛争で研究室に通えなかった期間はわずかであったが、この時以来、二つの研究分野を抱えることになってしまった。

1975年の夏、機会を得て、ブタペストのハンガリー科学アカデミー数学研究所に1ヶ月滞在するとともに、ここが主催する情報理論コロキウムに参加した。筆者にとっては、情報理論で外国の研究者と顔合せをする初めての機会であった。論文を通じて筆者の方もハンガリー学派の研究を知っていたとはいえ、それは切れ端であった。共産圏にありながら、彼らは孤立することなく理論の目標と発展のプロセスを実に丹念に追い、世界的にコミュニケーションして研究を進めていることに感嘆させられた。研究所には傑出した力を持つ何人かの研究者がよって集まって議論し、創

造の力が凝集するように触れ、一人一人が孤立し、知的刺激の機会が少ないままでは、日本の情報理論の研究は結局は大したことになるどころか立ち上がりさえ出来ないのではないかと、考えるようになった。1976年10月、IEEE主催の情報理論シンポジウムはコーネル大学であった。その前に三菱電機(株)の杉山康男氏(故人)から電話があり、イサカ(Ithaca)では同じ宿に申し込むことにした。コーネル大のこのシンポジウムの日本からの実質的参加者は筆者と杉山氏だけであった。他に、プログラムには小倉久直氏(現京大教授)の名前もあったように記憶(記憶違いかも知れない)しているが、会えなかった。もっとも、杉山氏と筆者がIEEEの情報理論シンポジウムに参加したのはこのときが初めてであり、それ以前のシンポジウムには嵩教授を始め、笠原正雄氏(当時阪大、現京都工芸繊維大教授)や何人かの方々が参加されていた。しかし、1970年代の当時、日本はすでに先進国の仲間に入り、半導体関連やコンピュータ、制御工学、パターン認識の関連分野の国際会議では日本からの研究者はすでに相当数であった。ここに、日本の科学技術界が目先の研究テーマにしか取り組まない体質が見て取れるが、コーネル大キャンパスのホテルで杉山氏とは、毎晩、何百人の中に日本からたった2人の参加者しかいない現状をなんとかするにはどうしたら良いか、等と話し合った。

杉山氏は、同僚の平沢茂一氏(現早稲田大学教授)とともに阪大の滑川・笠原研究室に派遣されたが、そこでBCH符号やGoppa符号の復号法にユークリッド互助法があり得ることを発見し、1976年当時、世界的に注目され出していた。笠原氏は賛意を表すだけでなく、すぐに準備にとりかかろうと提案し、こうして筆者と平沢、杉山の4人が集まって相談にかかった。滑川、嵩両教授には積極的に支持していただけたよう了解をとりつけた。候補地に出向き、予備折衝も重ねた。阪大は豊中と吹田にキャンパスが分かれていたが、三菱電機(伊丹市)から杉山氏は車を運転してこれ、筆者は良く便乗して工学部の笠原氏のもとに出向き、夜遅くまで、計画を練ったものである。泊まり込みのスタイル、ワークショップ等の考え方もその中で

決まった。こうして、1977 年第一回の「情報理論とその応用」シンポジウムを神戸氏の六甲荘で開催することが出来たのである。学会組織の枠をはみ出して、同好の志が集まり泊まり込んでインテシブな議論をする研究会はそれまで例が少なく、我々はともかく手答えを感じた。

第二回、三回と進める時、当時の電子通信学会の重鎮にいかに認知してもらうか、が課題になった。当時の東大工学部滝保夫教授（故人）と宮川洋教授（故人）に我々の目的と計画について詳細な説明を試みんとし、長文の手紙をしたためたのもこの頃である。ともかく、我々が企画したシンポジウムは、その後、電子情報通信学会の研究会や専門委員会のあり方にも影響を与えたのではないかと推察している。他方、笠原氏と筆者とで日本学術振興会の短期招へい教授の申し込みを行い、当時アクティブに研究していた研究者を外国から次々と（T. Berger, G.M. Gray, R. Blahut）呼んだ。当時、杉山氏は 10 人近く乗せられる車を運転していて、外国人研究者が家族ぐるみでレジデンスから研究会場へ、談話会へ、レストランへ、と移動できたのは杉山氏のおかげであった。何事もスムーズに計画が進んだのも、あのワゴン車のおかげであった。今も懐かしくあの頃の光景が思い浮かぶ。機械工学科にあって、筆者の研究室では 1/2 に近いエネルギーが情報理論とその応用の研究に向けられていくようになっていたし、阪大の他のグループの研究活動もそれぞれ活発であった。こうして、阪大における情報理論関係のポテンシャルが最も上がった時期に IEEE の ISIT シンポジウムを 1988 年神戸のポートアイランドで開催することができたのである。もっとも ISIT を開くに至るまで、紆余曲折はあった。1970 年前後、嵩教授の符号理論に関する仕事はすでに世界的に認められていたが、その関係で ISIT を日本で開けるかどうか打診があったそうである。しかし、日本の情報工学分野の有力教授の中で耳を貸してくれる人は当時誰もいなかった、と聞いている。

しかし、1980 年代に入っても、情報科学の中で情報理論はそれほど注目を浴びることはなかったように思う。音声や文字、パターン、画像の認識と理解、AI と認知科学、ニューラルネット等々と流行を追っかける方が成果が上がりやすいし、華やかに思われていた。情報理論をやってい

ると見向きもされないという状況は 1980 年代に入っても続いていた。1985 年 11 月に第 1 回の京都賞の基礎科学部門はシャノン(C. E. Shannon)に贈られた。これを記念してワークショップを開くことが企画されたが、この時、情報理論の当時最も活躍し、業績のあった研究者にスピーカーになってもらうよう推薦していたが、京都大学の当時有名な S 教授が全く情報理論と関係ない研究テーマをもった自分の弟子にいつのまにか差し換えてしまう、ということでもない出来事があった。司会者として指名されていた筆者もいつに間にか降ろされていた。もちろん、シャノンに会い、話しをすることができた上に、シャノンが 1960 年代に作ったチェスの駒を動かすロボットを 8mm のフィルムを見ることができ、そしてジャグリングに興味を抱いた話しを聞いて、筆者のもう一つの専門とも一致することを知って感慨は一塩のものではあったが。

昔、情報伝送はデジタル方式(電信、手旗、カンテラ)であった。電話やラジオ、テレビのおかげで情報伝送はアナログ方式が主流になったが、エレクトロニクスの技術発展のおかげでビット系列の自由自在なる加工が可能になると、デジタル伝送がむしろ中心となる時代が来た。ここに、別々に議論を進めてきた情報理論と符号理論は、新しい観点では統合されて同じ枠組の中で論じられようとしている[11]。変調と検波を中心としたアナログ伝送からビット系列の加工や変換(符号化)と波形設計を中心としたデジタル伝送の時代がやってきたのである。理論で性能を予測し、ほぼそれに近い性能を実現できる筋道を作らねばならない時、その様な研究がフットライトを浴びる時代になってきたのである。

参考文献

- [10] R. G. Gallager, A simple derivation of the coding theorem and some applications, IEEE Trans. on Information Theory, Vol.IT-11, No.1, pp.3-18, (1965).
- [11] R. E. Blahut, Digital Transmission of Information, Addison-Wesley, New York, (1990)

S I T A '93 報告

S I T A ' 93 実行委員長 武部 幹 (金沢大)

第 16 回情報理論とその応用シンポジウム(SITA'93)は 1993 年 10 月 19 日(火)より 22 日(金)までの 4 日間に渡って金沢市のシディモンドホテルで開かれた。参加者は 277 名(国内 269 名, 海外 8 名)で 45%は学生であった。発表件数(予稿集掲載件数)は 170 件で,セッション総数は 45 件,発表は 5 セッション並列に行なわれた。世界的な景気後退のせいか海外からの参加者はあまり多くなかったが,国内の留学生が多数参加された。また英語論文は 48 件に達し,当シンポジウムの国際化が着実に進みつつあるのが感じられた。

2 日目の午後に特別講演が 3 件行なわれた。 電気通

信大学の韓太舜教授による“乱数発生と同定符号”,金沢大学医学部加藤聖教授による“神経網膜における情報処理機構”ならびに北陸先端科学技術大学院大学の Magnus Halldorsson 助教授による“オンライン・アルゴリズム”であった。また同日夜は 4 つの興味深いテーマについてワークショップが遅くまで続けられた。

今回は 23 社に上る賛助会員からの会費と,地元石川県,金沢市からの補助金によりシンポジウムの準備と運営を円滑に行なうことが出来た。また種々のご支援を頂いた会員の皆様に実行委員会を代表して謝意を表したい。

国際会議のお知らせ

IEEE Third International Symposium on Spread Spectrum Techniques & Applications

昨年(1992)11 月に横浜で開かれた同名のシンポジウム(第 2 回目)も皆さまの御支援のお蔭で無事終了いたしました。参加者 268 名と単一のテーマのシンポジウムとしては多くの方に御参加いただき実行委員会として皆様に感謝いたします。さて早いもので 2 年に一度のこのシンポジウムも第 3 回目の開催が近くなりましたので下記のように御報告いたします。

記

日程	: 7 月 4 日から 6 日, 1994 年
場所	: フィンランド国, オウル市(Oulu)オウル大学
論文原稿締切	: 11 月 15 日, 1993
実行委員長	: P. Leppanen (University of Oulu)
プログラム委員長	: S. Glisic (University of Oulu)

ただし, この報告がなされている時には既に締め切られていると思います。

＜このシンポジウムの前には＞

1994 年は情報通信関連の主要な国際会議がスカンジナビア諸国で開かれます。IEEE VTC(Vehicular Technology Conference), ノルディックセミナー(移動通信関係), IEEE ISIT(International Symposium on Information Theory)がこのシンポジウムの開かれる前月の6月にスカンジナビア諸国で開かれ、特に本学会と関係の深い ISIT94 は6月 27 日から7月 1 日までノールウェイのトロンハイムで開かれますので、ISIT94 と ISSSTA94 にぜひともシリーズで御参加ください。

＜フィンランドそしてオウル大学＞

フィンランドと言えばサンタクロースとムーミン、そしてサウナの国、歴史的にはロシアからの独立の精神を交響曲にした作曲家シベリウスの国として我々日本人にはなじみの国ですが、他のスカンジナビア諸国と同様に移動通信の分野では高い技術力を持っています。特にこの国の NOKIA は世界的に有名な通信機メーカーですし、森と湖の多いこの国の人々は自然を楽しむために移動通信を頻繁に利用します。

首都のヘルシンキはこの国の最も南に位置し、オウル市はヘルシンキから北へ飛行機で1時間あまりでこの国のほぼ中央に位置します。オウル大学を訪問した際にこの大学の Leppanen 教授によれば、世界の中で最北の大学で、

少なくともスペクトル拡散通信を研究する大学の中では最北であるとの冗談をとばしていました。オウル大学では1985 年頃からスペクトル拡散の研究がなされ、現在 Leppanen 教授と Glisic 教授の二人の指導者によるチームで広い範囲にわたり研究が精力的になされています。

＜フィンランドはヨーロッパの一国＞

ヨーロッパと言えば一まとめに考えがちところが我々にはありますが、ドイツやフランスとはまた違った感覚がこの国にはあります。ドイツやフランスには過去の歴史の流れから、どうしても国策としての産業とか、産業のための産業といった部分が残っていますが、この国を訪問して、フィンランドでは個人生活を楽しむための産業、消費者中心の産業といった面がより徹底されているような気がしました。現在の日本は戦後最大の不況に遭遇し、それを切り抜けるには我々の生活上の価値観の変化が必要であり、そうした意味でも一度は訪問したい国と言えます。

＜連絡先＞

実行委員長: Prof. Pentti Leppanen
University of Oulu, Department of EE
Linnanmaa S1, SF-90570 Oulu, Finland
E-mail: pentti.leppanen@ee.oulu.fi
Fax: 358 81 5532845

中川 正雄(慶應義塾大学)

2nd International Workshop
on
Quantum Communication and Measurement

日時: 1994 年 7 月 11 日(月)から 16 日(土)

場所 Mathematics Department, University of Nottingham
University Park, Nottingham NG7 2RD, UK

内容

- | | |
|--|---|
| ○ Mathematical foundations of quantum communications | ○ Quantum noise and output stochastic processes |
| ○ Quantum measurement and dynamical reduction theory | ○ Causality, filtering and control in quantum systems |
| ○ Squeezed states and nonclassical light | ○ New quantum optical phenomena and effects |
| ○ Proposed experiments for quantum communications | ○ Devices for quantum communication systems |

定員 約 100 名

参加申し込み・参加費払い込み方法等は下記にお問い合わせ下さい

連絡先 194 東京都町田市玉川学園 6-1-1
玉川大学量子通信研究施設 広田修
電話 0427-39-8442 Fax 0427-39-8858

広田 修(玉川大学)

博士論文要旨

Geometric and Stochastic Theories of Source
Coding
(情報源符号化の幾何学的小よび確率論的研究)
東京大学 川端 勉(電通大情報工学科)

情報源符号化は、情報理論の一分野であり、データ圧縮システムの設計指針を与える役割を担っている。情報源符号化の基本問題として、情報源の数え上げ、確率的情報源の誤りなし符号化、および確率的情報源の忠実度規範付き符号化をあげることができる。本論文では、それら各々の問題に属する未解決問題を、第二章以下の三つの章でとりあげ、解決する。

第二章では、確率的情報源の忠実度規範付き符号化に属する問題として、自己相似集合に対するレートひずみ関数の理論を構築する。ユークリッド空間 R^k 上に確率分布 μ があるとき、その直積として R^k に値をとる独立定常情報源が定まる。この情報源に対するレートひずみ関数を考える。ただし、復号は同じ R^k 内で行うものとし、ひずみ尺度としてユークリッド距離の $r > 0$ 乗をとるものとする。一般にレートひずみ関数 $R(D)$ は、相互情報量の制約条件つき極小化問題として定式化できる。しかしながら、一般にそれを厳密に解くことは困難である。数値的に評価する方法はあるが、 μ として離散的でない一般の確率分布をとると、その結果を見通しよく評価してゆくのは

難しい．その一方， μ がルベーグ測度に関して絶対連続な密度を有する場合には極限值 $\lim_{n \rightarrow \infty} -rR(D)/\log D$ がユークリッド空間の次元 k に等しくなることが知られている．では， μ がルベーグ分解におけるクラス Φ_2 に属する場合，すなわち非離散的であってかつルベーグ測度に関して絶対連続な密度を有しない場合はどうだろうか？本章では， μ の台 S として，近年人々の興味を引いているフラクタル集合をとった場合， $R(D)$ を特徴づける問題，さらに，上述の極限値を求める問題などを考察する．

結果の一部を述べる． S としては自己相似集合，すなわち S が自分自身の互いに素な相似像の和になっているものとする．各相似像を与える相似変換を $W_i, i \in M$ ，対応する W_i のスケールを α_i と表記する． S に属する任意の点 x を出発点として，次の手順を考える．まず，定義から x を含む唯一の相似像 $W_{b_1}S$ ， $b_1 \in M$ が決まる．そこで， x を $W_{b_1}^{-1}$ で拡大すると再び S の点に移る．この点を再び出発点と考える．この操作を繰り返すことにより， M に値をとる列 $\{b_i\}_{i=1}^{\infty}$ が一意に決まる．そうすると，写像 $b(x) = \{b_i\}_{i=1}^{\infty}$ により S 上の確率分布 μ は M^{∞} に値をとる確率過程 μ^* に変換される． μ として μ^* が定常かつエルゴートのであるようなものと考えたと μ^* のエントロピーレート $H_{\infty}(\mu^*)$ ，期待対数縮小率 $E_{\mu^*}[-\log \alpha_{b_1}]$ などの諸量が定義できる．このとき，次の結果を得る： S の各成分がお互いに正の距離だけ離れているような自己相似集合 S について，上述の極限値は $H_{\infty}(\mu^*) / (\text{期待対数縮小率})$ に等しい．また， μ^* が定常かつエルゴートのであるような範囲内で， μ を変えて前述の値の上限をとったものは， S のハウスドルフ次元に等しい．さらに，この事実を参考にする，ユークリッド空間の任意のコンパクト集合 S の新しい次元，すなわちレート歪み次元を定義できる．以上の結果は $R(D)$ の高レートにおける漸近的性質であるが，低レートにおける評価も可能である．特に， μ として，いわゆるカントル測度を少し一般化した α -カントル測度にとった場合について，実際に符号化を行ったり，またよく知られた $R(D)$ の双対表現を一般確率分布に拡張した補題などを用いたりすることにより， $R(D)$ に対する上下界を求める．

第三章では，確率的情報源の誤りなし符号化に関連した問題として，漸近的最良性を有しかつ計算量的性能がよいことで有名な Lempel-Ziv 分解アルゴリズムの新しい設計と解析を行なう． $A = \{a_1, \dots, a_m\}$ を情報源アルファベットとし，空列を λ と表す．半無限列 $x \in A^{\infty}$ を左から

有限部分列の列 $\mathbf{w}_1, \mathbf{w}_2, \dots$ に分解する仕方のなかで，特に $t \geq 0$ について再帰的に， $\mathbf{w}_{t+1}$ を $\lambda, \mathbf{w}_1, \dots, \mathbf{w}_t$ のどの要素とも異なるものの中で最も短い部分列とする仕方を Lempel-Ziv 分解という．情報源系列の符号化復号化は，分解毎にその候補のなかで実際の分解部分列を番号づけることに他ならない．本章ではまず，そのような番号づけをなるべく系統的に行えるようデータ構造を工夫した，簡単に性能のよい符号化復号化の実現法を与える．

次に，Lempel-Ziv 分解法の性能解析を行う．この特徴は圧縮率を厳密に評価する点である．いま固定した番号 t_0 までの分解部分列のあらゆる組合せは $\Pi_{i=1}^{t_0} \{(m-1)t+1\}$ 通りある．従って，この総数の対数と $\sum_{i=1}^{t_0} (\mathbf{w}_i \text{ の長さ})$ の期待値との比が圧縮率を与える．情報源を独立定常過程と仮定すると，この分母の期待値を与える厳密式が得られる．この解析を基礎にして，独立定常過程の漸近解析が可能となり，可変長固定長符号としてみたときの，新しい符号化定理が得られる．

さらに，上述の厳密解析の発想は，ユニフィラマルコフ過程における，状態依存型 Lempel-Ziv 分解アルゴリズムの新しい漸近解析も可能とする．証明では，Donsker の不変原理等の確率解析を応用する．

第四章では，情報源の数え上げの問題を考える．著者は，構造を持つ集合の数え上げも情報源符号化の問題として認識している．本章では，エネルギー制約があり，ブロック同期をするスイッチ系のモデルとして，スイッチ集合族による一様なスイッチ系という概念を定義し，その数え上げの問題などを議論する．そこでの数理的問題は，以下に述べるアレイ符号に関する問題に等価である．

サイズが $n \times m$ で各要素が 0 または 1 の二値行列を考えよう．縦に見ると 1 の要素数が k で一定であり，横に見ると 1 の要素数が常に偶数になっているような行列はいくつあり，それを数え上げるにはどうすれば良いか？本章では，この種の問題にアプローチするための基本原理として，スピン確率変数を用いた組合せ論的補題を与える．それを用いて上の行列の総数を求める問題を解き，具体的に番号づけシステムを構成し，さらにその計算量を考察する．

さらに，縦の列が，一般の非線形制約，例えば線形符号の最小重み部分等，をとる場合を考える．この場合行列の総数の詳細な漸近式が得られる．厳密な数え上げは一般的には困難ではあるが，縦ベクトルが属する非線形符号が対称

な構造を有する場合、問題を解決する一般的な方針がある。これを述べ、それがうまくゆく例をいくつか示す。

行列に課した制約は利用可能である。例えば、多重に課した偶パリティ性はリピータでの簡単な同期検査に使え。また、行列に誤りが生じたとき、誤り制御が可能である。この問題を、最初に示した重み一定符号の場合について考察する。誤りの型としては、二つのものを考える。一つは、単一列の誤り、もう一つは単一行の誤りである。この両者について、それぞれ次の二通りの最適な誤り訂正法を与える。一つは確定的訂正法、すなわち確実に誤りが訂正できるときしか成功と見なさない方法であり、もう一つはランダム訂正法、すなわち確定的でなくてもあらゆる訂正の可能性を網羅する方法である。以上すべての場合について誤り訂正確率を定式化し、行列のサイズが大きい場合におけるそれらの漸近的振舞いを議論する。ただし、誤り訂正確率とは、ある固定した誤りパターンに関して、あらゆる可能な信号の母集団からのランダムな選択に対して、その信号が誤り訂正できる確率と定義している。

情報源符号化において、著者が特徴的であると考えてき

た方法論は、情報源が確率的であれ非確率的であれ、まずその幾何学的構造を調べ、それを利用して情報源を一様構造に埋め込むことにより、その中で数えあげアルゴリズムを構成するというものである。この方法によると、アルゴリズムが単純で無駄なく設計でき、性能解析も自然にゆき、それもほとんど最適に近いものとなる。上の三章で展開した理論は、一見異質で相互の関係が薄いように見えるが、それらは皆、この方法論に基づいている。

電子メールの有効利用

現在会員の約 1/3 の方が電子メールアドレスと学会に登録しておられ、この電子メールを用いて学会からのお知らせやシンポジウム・ワークショップに関する情報の good timing な配布を行ないたいという意見が理事会に出ております。(今回の理事会議事録参照)しかし、電子メール連絡網を役立つように完備するためには、もっと多くの会員の方に電子メールアドレスを登録して頂く必要があり

ます。電子メールアドレスの登録法については担当者間で準備が進められておりますので近い内に電子メールアドレス登録の御案内があると思いますが、電子メール利用可能な環境におられましたらぜひアドレス取得などの御用意をお願いします、

橋本 猛

情報理論とその応用学会 1993 年度総会報告

平成 5 年 10 月 21 日(木)16 時 30 分より金沢市「金沢シティモントホテル」(SITA'93 会場)にて、情報理論とその応用学会 1993 年度総会が実施された。議事次第は次の通りであり、議事 2～12 についてはすべて承認された。

1. 会長挨拶(嵩忠雄会長より)
2. 1992 年度事業報告・収支決算報告
3. SITA'92 決算報告
4. ISITA'92 最終および決算報告
5. 1993 年度事業中間報告・収支中間報告
6. SITA'93 中間報告
7. 1994 年度事業計画・収支予算案
8. SITA'94 開催計画
9. ISITA'94 開催計画
10. 会則の一部変更
11. 1994 年度役員承認の件
12. その他(SITA'91 決算報告を含む)

また総会に先だって 1994 年度役員の選挙が実施され、1994 年度役員構成は下記の通りとなった。なお今総会で会則の一部変更が承認されたのにもない会長の任期は 1 年となる。

1994 年度役員

	氏名	所属	
会長	有本 卓	東京大学	新任
副会長	笠原 正雄	京都工芸繊維大学	留任
	平沢 茂一	早稲田大学	新任
理事			
(無任所)	中村 勝洋	日本電気	留任
	小倉 久直	京都大学	新任
(庶務)	金谷 文夫	NTT	留任
	山本 博資	東京大学	新任
(会計)	金子 敏信	東京理科大学	留任
	村上 篤道	三菱電機	新任
(編集)	橋本 猛	電気通信大学	留任
	今村 恭己	九州工業大学	新任
(企画)	佐藤 俊輔	大阪大学	留任
	古賀 敬一郎	KDD	新任
監事	今井 秀樹	東京大学	留任
	丸林 元	長岡技術科学大学	新任

情報理論とその応用学会理事会議事録

平成 5 年度第二回

1. **日時** : 1993 年 7 月 23 日(金)15:30～18:00

2. **場所** : NTT 横須賀研究センタ 10 階会議室

3. **出席者** :

会長 : 嵩(奈良先端大)
 副会長 : 田崎(愛媛大), 笠原(京都工繊大)
 理事 : 広田(玉川大), 金谷(NTT), 津田(富士通), 吉田(京大), 橋本(電通大), 高崎(日立)
 監事 : 松嶋(早大), 平沢(代理)
 評議員 : 岡本(北陸先端大), 坂庭(東工大), 鈴木(沖電気), 武部(金沢大), 中川(慶大), 広崎(日電), 森(慶大), 山内(三菱)

幹事 : 河野(横国大), 藤原(阪大), 山崎(玉川大), 三宅(NTT), 笹瀬(慶大), 山本(東大), 鈴木(中央大)

4. **配布資料** :

H5-2-1 : 平成 5 年度情報理論とその応用学会役員名簿
 H5-2-2 : SITA'93 準備状況
 H5-2-3 : 企画関係報告事項
 H5-2-4 : 会計関連の状況
 H5-2-5 : ISITA'94 Call For Papers
 H5-2-6 : 情報理論とその応用学会会則(抜粋)
 H5-2-7 : 庶務関連の資料

H5-2-8 : 2nd International Workshop on Quantum Communication and Measurement 開催のお知らせ

H5-2-9 : IEEE ISSSTA'94 Call For Papers

H5-2-10 : 入会申込者および賛助会員入会申し込み団体

H5-2-11 : ニュースレター No. 15 案

H5-2-12 : ITW-93 報告資料

会費徴収の進み具合についての報告がなされた。

5.5 ISITA'94 準備状況報告(資料 H5-2-5)

中川実行委員より諸経費の見積りを含め準備状況に関して説明がなされた。

5.6 会則一部変更の件(資料 H5-2-6)

嵩会長より、会長任期を1年とし再任なしとすること、ならびに評議員および幹事の任期は引続き3期を越えてはならないとするよう会則を一部変更する旨の提案がなされた。議論の結果これらを総会に図ることが承認された。

5.7 庶務関係報告(資料 H5-2-7)

金谷理事より JICST への資料寄贈の件および老朽化したパソコン廃棄の件について説明がなされ承認された。これに関連してシンポジウム予稿集の無料配布の範囲をどうするかが再び議論され、賛助会員および国会図書館は含めるが大学は除くこととなった。

5.8 2nd International Workshop on Quantum Communication and Measurement (資料 H5-2-8)

広田理事より案内の紹介がなされた。

5.9 IEEE ISSSTA'94 の案内の件(資料 H5-2-9)

河野幹事より案内の紹介がなされた。

5.10 1993 年度入会申し込み承認の件(資料 H5-2-10)

金谷理事より 1993 年 2 月 2 日以降 7 月 23 日現在までの入会申込者および賛助会員申し込み団体について説明がなされ入会が承認された。このとき学生の新入会員が少ないことが問題となった。これについては、SITA の会場で入会手続きを可能にすることと、アドバンスプログラム送付時に入会申し込み用紙を同封することが提案され、SITA'93 から実施することとなった。

5.11 ニュースレターNo. 15 の件(資料 H5-2-11)

橋本理事よりニュースレター案の説明がなされ承認された。また IEEE IT ニュースレターの巻頭論文のようなものを各々の専門分野の

5. 議事要約:

5.1 前回議事録(案)の承認(資料は事前配布)
原案通り承認された。

5.2 SITA'93 準備状況(資料 H5-2-2-)

武部実行委員長および岡本実行委員より日程、場所、応募状況および特別講演等に関する説明がなされた。さらに、予稿集は 350 部印刷し一部を大学等に無償配布することにしたらどうかという提案が実行委員長よりなされたが、無料配布の範囲については資料 H5-2-7 との関連で再議論することとなった。

5.3 企画関連報告(資料 H5-2-3)

山本幹事より当日行なわれた講演見学会の報告がなされた。また、高崎理事より講演会共同主催および講師旅費援助の提案が行なわれた。これに関連し、他学会と共同主催の講演会、研究会、ワークショップにおける講師旅費援助の可否について種々議論がなされた。その結果、今回の提案は特例として承認するが、今後は年度事業計画として了承を受けたものに限ることとし、また援助額の基準については企画および会計理事間で協議することとなった。一方、マイクロタスクフォースおよび会員連絡システムの電子メール化推進の提案もなされた。これについては、電子メールの連絡網をより完備なものにするため、次回発行のニュースレターで電子メールへの登録を呼びかけることが提案され承認された。

5.4 会計関連報告(資料 H5-2-4)

津田理事より SITA'93 および ISITA'94 の準備金に関する説明がなされ承認された。また

人に書いてもらうことが提案されたが、これについては企画担当の間で検討を続けることとなった。

5.12 ITW-93 報告(資料 H5-2-12)

河野幹事よりワークショップの開催報告がなされた。

5.13 SITA'94 について

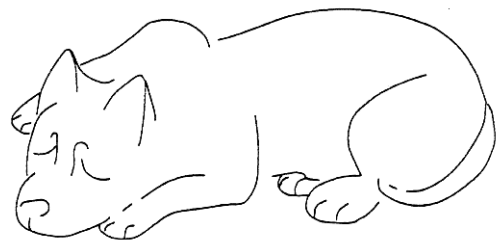
嵩会長より SITA'94 計画に関しては、広島大学に開催を打診し前向きの回答が得られていること、また、時期は 12 月頃の予定となることが報告され承認された。これをうけて嵩会長より広島大学に対して正式に開催計画の立案を依頼することとなった。

5.14 その他

- (a) 信学会の SITA 特集号を毎年ある部数だけ本学会で買い上げてはどうか、という意見が出た。具体的方法に関し種々議論されたが、予算の出所の問題があるので引続き

会計理事に検討をお願いすることとなった。

- (b) 次回理事会は SITA'93 初日(10/19)のオープニングパーティー終了後に開催されることとなった。またこれに関連して金谷理事より各担当理事へ、1993 年度通常総会資料原案を 9 月末日までに準備して頂きたい旨の依頼がなされた。



編集後記

編集理事になって二回目のニューズレターです。今回は平成5年度ニューズレターの三つめということで今度こそは予定通り年内に—と—but、やはり遅れてしまいました。与えられたメ切を守るのさえ難しいのに自分で決めたメ切を守るのはなお難しい...

さて、前回に引続き「情報理論のあけぼの—その2」を掲載しました。こちらの後半部には私もその多大勢の一人としての思い出があり、「ああ、あの時は」と今更ながらに思い起こされます。

思い起こすといえば、今回の巻頭記事の田中 初一氏のエッセーも氏の多方面の活動を知る一人としてなるほどと

思われます。田中氏も文中に書かれているように、このエッセーはシリーズとして幾人かの方々に御自分の研究の中に思い起こされる論文などを中心として過去-現在-未来について自由に書いて頂こうというものです。次回は「他人の論文に面白いものはない」と(酒を飲んだ上で)豪語された嵩氏です。とすれば何を書いて頂けるのか、興味シンシンです。

さて、ニューズレター編集部(?)では皆様からの企画をお待ちしています。今度はこの様な記事を書いて欲しい、などの御意見をお寄せ下さい。(猛)

投稿募集

ニューズレターの内容を充実し定期刊行化を更に進めるために投稿および企画を募集しております。投稿や新しい記事の企画、お問い合わせ、御意見などは下記の編集担当者迄お寄せ下さい。

吉田 進(編集理事)

〒606-01 京都市左京区吉田本町
京都大学工学部電子工学科
Tel. 075-753-5317(直通)
Fax. 075-753-4982
E-mail yoshida@kuee.kyoto-u.ac.jp

橋本 猛(編集理事)

〒182 調布市調布が丘 1-5-1
電気通信大学電子工学科
Tel. 0424-83-2161, ext. 3331
Fax. 0424-80-3801
E-mail hasimoto@liszt.ee.uec.ac.jp

内匠 逸(編集幹事)

〒466 名古屋市昭和区御器所町
名古屋工業大学知能情報システム学科
Tel. 052-732-2111, ext. 2850
Fax. 052-733-6589
E-mail takumi@ics.nitech.ac.jp

笹瀬 巖(編集幹事)

〒223 横浜市港北区日吉 3-14-1
慶應義塾大学理工学部電気工学科
Tel. 045-563-1141, ext. 3376
Fax. 045-563-2773
E-mail sasase@mori.elec.keio.ac.jp

情報理論とその応用学会事務局

〒238-03 神奈川県横須賀市武 1-2356
NTT 伝送システム研究所 金谷特別研究室
Tel. 0468-59-3030 Fax. 0468-59-3388 E-mail sita@nttsd.ntt.jp