

情報理論とその応用学会ニューズレター

第9回シンポジウムに向けて

情報理論とその応用学会主催の第9回シンポジウムは、すでにご案内のとおり、10月29日(水)から31日(金)までの3日間にわたって、名勝の地赤倉温泉(ホテル太閣)で開催されますが、そのための準備は長岡技科大の丸林 元先生(実行委員長)を始めとする諸先生方の御努力により着々と進められ今や最後の詰め段階に入っています。現在時点での参加申し込み者数は260名、発表論文数は147件です。この様子からすると来るシンポジウムの成功はすでに”当確”といったところでしょう。

ここでその詳細は省き、一部を紹介致しましょう。まず、特別講演についてですが、これは情報理論とその応用の技術的最先端のみに捕らわれない自由な立場から、隣接分野あるいは全く隣接していない諸分野から面白い刺激のお話を伺うという主旨で数年前から恒例化したものですが、今回のシンポジウムでは次ぎの三人の先生方をお願い致しました。

甘利俊一：情報幾何学

喜安善一：情報理論研究事はじめ(仮題)

川上正光：ブラックホールプロフェッサー
撲滅論—知的謀反のすすめ—

また、これも恒例のワークショップについてですが、第1回シンポジウム(1978年)以来、夕食後のリラックスした雰囲気の中で、全国から参加された方々の自己紹介や分野毎の現状と将来展望に関する意見交換などを通じて参加者間の親睦や研究上の接触を深める上で大きな役割を果たし続け、最近では、大方の参加者がお互いに知己の間柄といった雰囲気になってきましたので、今年は趣向を少しかえて、本来の意味での”ワーク”ショップにしてみようということになりました。各

分野の第一線で活躍している若年の研究者に話題を提供していただき、それを種に参加者全員が自由な議論を楽しみながら新知識を—自分は勉強しないで一居ながらにして仕入れさせていこうという悪巧みですが、遠慮は無用、談論風発、百家争鳴、話題提供者が逆に話題を提供されたり、参加者同志が勝手に議論に熱中してそちらに興味が移ってしまったり、など想像するだにわくわくするような研究討論の新形態を創造してみませんか。このようなわけで、今回は、次の先生方に話題提供者という名の”いけにえ”になって頂くことになりました。どのワークショップに参加するかは全く個人の自由です。

話題及びその提供者

”公開鍵暗号系” 黒沢(東工大)、松本(横国大)

”光通信理論” 広田(相工大)、中川(慶大)

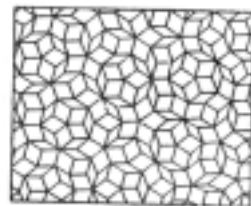
”LDPモデル—データ圧縮の新しい可能性” 小林(阪大)

”2次元 Berlekamp- Massey アルゴリズムについて” 阪田(豊橋技科大)

”カオス、情報、ARモデル” 大石(早大)、相沢(早大)

”確率過程と信号処理” 長岡(東京工科大)

なお、シンポジウムに問するお問い合わせは長岡技大電気系(TEL:0258-46-6000)の萩原先生または太刀川先生の方をお願い致します。(編集より)



ペンローズタイル貼り(小田 泰・サイエンス9月号・1986より)

佐藤 洋（電通大）

前回のニューズレターに堀内先生が「学会」という同好会がいいという短文を書いておられたが、情報理論の「同好会」が東京地区ですでに7、8年間続いていることをこの機会に報告しPRとしたい。

この会の名前は「情報理論研究会」である。慣習のみで成り立つ研究会で、参加、発表は全く任意である。研究テーマは情報理論的なものならなんでもよい。この頃は二か月に一回程土曜の午後電通大で開くことが多い。参加希望者には開催通知を出す。このところ幹事は私と川端勉氏である。テーマはどちらかということとシャノン理論的なものが多い。

この会の誕生は、昭和53年11月に神戸で開かれた「情報理論とその応用研究会」の前後と記憶している。その頃相模工大におられた韓太舜先生から熱心なお話しがあって、東京地区でもシャノン理論を中心に同好者が集まることとしたのが始まりである。その頃、東京地区でもシャノン理論の研究者は少なく、研究者間の連絡もなかったのも、この会のできた意義は大きかったと思う。多くの若手研究者が、この会で刺激を受けて研究を育てて行ったと思う。また、外国のシャノン理論家、Berger さん、中国の章さんなどにもこの会に来て頂いた。

この研究会の特長を三つ程述べておこう。その第一は、シャノン理論的ということからお分かり頂けるかと思うが、応用的というより基礎的な研究に関心が強い。第二にはその自由な雰囲気である。諸演者の話の途中で自由に割りこみがかかり、時によっては討論が延々と続き、新しい研究の示唆がえられることが、しばしばある。その三は始めに書いたように、極めて同好会的であり、組織もはっきりしない（組織能力が欠如している）。それでいて、この会がつぶれもしないで長らく続いているのは、いろいろよいところがあるのだろうと、幹事を続ける気にもなるわけである。御関心の向きは、幹事に連絡を頂けば、案内を差し上げます。

小倉 久直（京工繊大）

点過程(point process)の名を初めて耳（目？）にされる方も多いでしょうが、ランダム点(random points)といえ意味は分かると思います。点過程は情報、通信以外でも、例えば持ち時間、神経パルス、伝染病、植物群落、天体物理、統計物理などに関連して古くから工学、物理、生物、医学などの話題でありましたが、確率過程の目ざましい進歩や応用に比べると点過程は地味な目立たない分野と思われ研究者の数も多くありませんでした。この方面に英国系の研究者の多いことは興味のあることです。しかし最近では点過程の関与する現象が多く観測され、モデル化が要求され、この方面に研究の銚先を向ける必要性が高まって来ています。去る7月11、12日の両日に開催しました第1回の「確率過程とその応用」時限研究会ではテーマとして「点過程」をとりあげました。ニューズレター編集者から何かを書けとの御依頼ですので少し紹介してみます。点過程は「確率過程とその応用」の中でも境界領域に属します。数学をはじめ通信、情報、数理、経済、生物、医学などいろいろな方面の先生方が集まり、十分時間をかけて研究紹介、討論などを行いました。掲げたテーマの性格から、模索的な、問題提起的な何かを要求する雰囲気の伴う面白い研究会だったと思います。内容は点過程のレビューの後、山本氏（東北大）の神経インパルス系列のマルコフ性、八名氏（法政大）のシナプスの高頻度ランダムパルスの生起頻度の推定、武者氏（東工大）による微弱光のフォトカウンティングにおけるゆらぎ解析の報告がなされました。これらは生体および物理系で観測される点過程の統計的な時系列解析を取り扱い、種々の提案と問題提起を行っています。加納氏（横浜国大、経済）からは経済学への応用を意図した点過程を含む系のカルマンフィルタの研究紹介がありました。加納氏は点過程で著名な、Coxのもとで研究された方です。ついで佐藤氏（電通大）はポアソン点過程の情報縮約理論の問題点をのべられました。この研究は昨年の情報理論とその応用シンポジウムでも報告されましたが、

点過程の立場からは種々の問題提起を含んだ新しいテーマへの糸口といえます。杉山氏は再生過程の問題点とマルコフ再生過程モデルによる符号列スペクトルについて報告されています。これらのテーマからは点過程の統計時系列解析、点過程の情報理論、点過程の数学解析などの方向に研究を向けるべきであることが示唆されます。現在は、第1の統計の時系列解析が先行している印象をうけます。第3の問題に至っては確率過程のそれに匹敵するものは殆どない状態です。点過程は確率過程の一つの変種でありながら確率過程とは違い、いわゆる関数ではないために関数(?)解析に相当するものが確立されていない未開拓な分野のように思われます。したがって、点過程は今後も再々テーマとして取り上げる必要のある多くの問題を抱えています。情報理論とその応用学会の先生方の関心をひくことが出来れば幸いです。

光通信理論研究会

広田 修 (相模工大)

編集より何か書けと命令が下ったので、昨年11月1日に発足した光通信理論研究会の紹介をさせていただこうと思います。

発足以来、光通信理論とは一体何だとかよく質問を受けます。別にこれといった定義があるわけではありませんが、光を通信の媒体とする通信システムの設計理論およびその基礎(物理、数学)と言えます。筆者は ”情報” という言葉はあまり好きではないので通信としました。電気にしろ光にしろ、通信理論は通信デバイスとその動作原理を支える物理学から最適設計理論構築のための基礎数学まで、その全てを範ちゅうとする通信の基礎理論であることは何人にも疑いのないところでしょう。

では、光と電気(電波)とでは何が違うのでしょうか。まず、通信デバイスの基礎となる物理学が古典物理から量子物理へ移ります。これは通信の質を劣化させる雑音が熱雑音から量子雑音に移ることを意味します。量子雑音は Gauss 加法性雑音とは限りませんので、

(Gauss 加法性でない方が多い) この雑音を解析する数学を整備する必要があります。これには関数解析が必要不可欠となります。雑音理論が関数解析ならそれに対処する最適理論も関数解析となり、これらが量子通信理論の母体となります。量子通信理論は全くの未完成といって良いのです。”理論がなくてもデバイスは働く”これが世の常です。最近の光デバイスの開発には目覚ましいものがあります。システム家は早急それらを用いて通信システムを実現せねばなりません。現段階では、量子雑音理論と最適理論を分離して雑音を古典モデルに移し、それに従来の通信理論を適用するしかありません。これは半古典通信理論と呼ばれます。このような研究も工学にとっては極めて重要なものです。したがって、当研究会はデバイスの動作原理からヒルベルト空間論まで光通信を目的とするものなら全て受け入れるわけです。

けし粒のような存在ですが、一生懸命やっております。本学会の御協力を心より期待しております。世話役は次の通りです。

広田 修 (相工大)
高原 幹夫 (山梨大)
中川 正雄 (慶応大)

情報理論シンポジウムに参加して

小林 欣吾 (阪大)

ヨーロッパにおける情報理論研究の指導的立場にある3人の大御所、すなわち、R.Ahlsweide, J.H.van Lint と J.Massey らがオーガナイザーとなって、本年5月11日から5月17日にかけて、西ドイツの黒い森として有名なシュバルツバルトのどまん中にあるオーベルボルファッハという、本当にひなびた、のどかな田舎村で研究会が開催された。ここにある数学研究所では、30人~50人位を1週間単位で籠りきりにして、ほとんど通年、とっかえひっかえ、数学関係のシンポジウムが行われている。今回は、多元情報理論、符号理論、暗号理論に関する最新のトピックスの発表と熱心な討論がもたれた。参加者は、

16ヶ国45人で、37件の発表があった。わが国からは、専修大学 韓太舜 教授 と小生が出席した。発表の内訳は、多元情報理論を中心とした Shannon 理論に関するもの18件、符号理論に関するもの15件、暗号理論に関するもの4件であった。シンポジウムはいたって informal で、プログラムなどは、前日の夜、オーガナイザーが次の日の発表者を募ってあるくといった風でした。発表することは強制されているわけでないのだけれど、発表したくてうずうずしている人ばかりなので、オーガナイザーには楽そうにも思えた。朝は9時から始まり、12時半に午前の部が終わり昼食となる。午後は、4時から6時半頃まで討論が続く。長い昼休みと夕食の後の憩いのひとときには、研究内容からんだ情報やアイデアのやりとりがおこなわれる。そこで severe な駆け引きが水面下で進行しているのが解るようになるのは会議も終わりに近づいたころでした。昼食と夕食は、毎回名札が shuffle されて、普通ではとても隣に座ることなどはばれる大家と同じテーブルを囲むこともしばしばで、そこでは、研究とは離れた話題を通して彼等の人柄を知ることができる。また、中日のある夜には、8~9人が次々に前に出て、彼等が現在抱えていて、すぐには解けない問題を提起して、参加者の意見を聞くといった催しもおこなわれた。もちろん、本気で解きたい種類の問題はそうはやすやすとそんな場面で提示することはないのだけれど、どんなことに関心があるのかを知るのに都合はよい。そのうちの何問かに対しては、翌日までに答えを与える賢い人がいるのには、またまた、感心させられた。さらに、国際会議ではよくあることだが、好き者が、掲示板に初等幾何学のちょっと気のきいた練習問題を懸賞付で出したりして楽しんでいる。16日の午後には、3人のオーガナイザーが、old timers と名うって、それぞれの得意とする分野の重厚な講演をおこない、これからの情報理論の研究動向に多くの示唆を与えた。

この研究会の際だった特徴は、単に数学的厳格さだけを追いもとめるだけでなく、他分野の中心的话题への情報理論の立場からの接近が試みられており、それによって情報理論の適用範囲を広げていこうとする努力がみられたことであろう。たとえば、Korner と Marton は graph entropy と呼ばれる新しい道

具立てで、計算機科学の重要問題の一つである完全ハッシュ法に挑んでいるし、韓は、統計学の仮説検定問題を多元情報理論の視点から一般化を試みている。ここで、注目を浴びた発表と、筆者のかたよった興味からめぼしいものをいくつか拾いあげておこう。Ahlswe de と Dueck は、雑音を伴う通信路を通して情報伝送を考えるに際し、従来の通報誤りを、ずっと緩和してしまった状況で定義される同定容量(identification capacity)は、ほぼ、 2^c (c は Shannon の意味での従来の通信路容量)となることを論証した。彼等の仕事は、情報理論に、また、新しい概念を持ち込むことになり、理論の適用領域を拡大することにつながる。Csisar は、jammer がコスト制限をうける場合の arbitrarily varying channel の容量について考察した。Ahlswe de and Kaspi と小生は、blackwell が考えた trapdoor channel を一般化した permuting channel を多元情報理論の視点からとらえていくつかの結論を得ている。Schalkwijk は二方向通信路に関する発表をおこない、van der Meulen は非対称多重アクセス通信路を通して、相関のある情報源を伝送する問題について話した。Zhang は、多元情報圧縮に関わる Multiple description のいくつかの結果をしめした。Costa は、干渉通信路について、Willems は、ある種のユニバーサル情報圧縮法について、Heegard は、constrained channel の (d,k) 符号のスペクトルについて議論した。Ericson は、重み一定の符号の漸近的性質について、Zinoviev and Zyablov は連接符号について、Wan は Berlekamp-Massey と Euclid 算法の関係を論じた発表をおこなった。Calderbank は符号理論のデザイン理論への応用に関して、Niederreiter は符号理論の暗号理論への応用について話題を提供した。Simmons と Schnorr は署名法について議論を展開した。確率過程に関係しては、Marton が相関のある情報源の弱漸近同型性についてのある結果を提示した

この研究所に着くと、各人シャワー付のゆったりした個室をあてがわれ、しかし、鍵は渡されない。泥棒など絶対に人ってこないほどの片田舎なのだ。そんな心配より、そこに集まった研究者の交流こそ大切と考えてのことらしい。別棟のセミナー棟も46時中鍵はかかっていない。夜いつでも、気がむいたとき、入ることができるのだ。しかも、そこに

ある図書室には、世界中の数学関係の雑誌は、ほとんど、すべて網羅してある。まったく、いたれりつくせりなのである。もちろん、コピーもセルフサービスで自由にとれる。休憩時には、コーヒー、紅茶、ジュース、コーラ、ビール、ワインどれでも冷蔵庫をあければ、十分のストックが用意されている。そばに置いてあるメモ用紙にチェックして、自分の消化したぶんだけは後払いとなる。ともかく、こんな研究所を産んだヨーロッパの文化に対応するものを、この成り金日本が持つことができるのだろうかという思いが日本に帰ってからずっと拭い切れないのはどうしてなのだろうか。

1986年符号理論とその応用ワークショップ (WCTA86) 報告

企画理事 今井 秀樹 (横浜国大)
企画幹事 河野 隆二 (東洋大)

日時： 昭和61年8月
25日(月) 10:00~18:30
26日(火) 9:00~12:00
場所： 横浜通信会館
合同開催：1986年暗号と情報セキュリティワークショップ (WCIS86) -
暗号と情報セキュリティ研究会 (代表、
今井 秀樹) 及び電子通信学会情報セキュリティ時限専門委員会 (委員長、辻井
重男) 主催
参加者： 156名
大学関係 78名 (内、学生49名)
企業、公共研究機関 78名

情報理論とその応用学会が昭和61年1月に発足してから最初の記念すべきワークショップが横浜港近くの官庁街にある横浜通信会館で開催された。合同開催であったこともあるが、当初の予想を大幅に上回る総計156名、1日平均約120名の参加者が一会場に集合し連日、盛んな質疑応答が交わされた。

両ワークショップとも招待講演であり本学会主催のワークショップは、符号理論とその各分野への応用に関して10名の専門家によ

るサーベイと解説を中心にし、入門から最新の応用に関する講演が行われた。

各講演の内容及び議論の対象となった話題について、簡単にまとめると次の通りである。

WCTA86-1 山田 隆弘 (宇宙研)
「二重符号化方式とその応用」

二重符号化方式の中で代表的な積符号、連接符号とそれを一般化して得られる一般化連接符号、修正符号について統一的な解説がなされた。また、これらの深宇宙通信への適用、2次元巡回符号との関連について、議論が行われた。

WCTA86-2 山岸 篤弘 (三菱)
「BCH符号とRS符号の符号化/復号化LSI」

最近、広く応用されているBCH符号及びRS符号の符号化復号化を実現する専用LSIについて、開発動向と開発上の問題点等について解かり易く説明がなされ、DSP、マイクロプロセッサによる構成との比較等に関する議論が行われた。

WCTA86-3 杉山 康夫 (摂南大)
「Goppa符号とその復号法その1」

本講演では、次の講演と合わせて、BCH符号やスリヴァスタヴァ符号等を含む広いクラスの符号であるGoppa符号について、特に復号の定式化、アルゴリズムのバリエーションや制御理論などとの関係について解説された。

WCTA86-4 今村 恭己 (佐賀大)
「Goppa符号とその復号法その2」

特に、Berlekamp-Masseyアルゴリズムの考え方の解り易い説明と、Euclidアルゴリズムや連分数法との関連の解説が行われた。その後、前の講演と合わせて質疑討論が行われ、代数幾何に基づく符号、多次元への拡張、V-G限界式を満たす符号の割合などに関して多くの議論がなされた。

WCTA86-5 藤原 英二 (NTT)
「符号理論と計算機」

計算機に於ける記憶装置と論理回路の高信頼化のための誤り訂正符号の応用について具体例を混じえた説明が行われた。特に、Ma

ss Memoryへの応用について、活発な討論が行われた。

WCTA86-6 平田 康夫, 安田 豊
(KDD)

「符号理論と衛星通信」インテルサットSCPC, TDMA/DSI、IBSシステムやインマルサットシステムに適用される誤り訂正符号について、解説が行われ、符号化利得による評価、符号化多値変調方式、逐次復号法などに関する多くの意見が交わされた。また、安田氏のインマルサットにおける体験やBerlekampのサイクロトロミックス社などの最新の情報について語られた。

WCTA86-7 鈴木 隆敏 (赤井)
「符号理論とオーディオ」

デジタルオーディオの発展における誤り訂正符号の役割と変遷について、PCMアダプタから、DAT、CD-ROMに至るまで各システム毎に標準化の問題点と共に系統的な解説が行われた。そして、衛星通信の場合との評価基準の相違や、訂正と補正の割合などに関する討論が行われた。

WCTA86-8 河野 隆二 (東洋大)
「擬似雑音符号系列とその応用」

擬似雑音系列(PN)系列の代表的な応用と主なクラスのPN系列に関する解説が行われ、デシメーションの考え方による線形帰還フィードバックシフトレジスタ系列の統一的な説明やGMW系列に代表される非線形フィードフォワード論理操作を含むPN系列についての解説に対し質疑応答が行われた。

WCTA86-9 中村 勝洋 (日電)、
大村 一宏 (UCLA)

「有限体での乗算・除算及び、べき乗演算について」

誤り訂正符号や暗号の実現において重要な有限体上での演算を回路構成上で効率的に実現するための手法についての最近の成果が説明された。特に、正規基底などの基底を用いた要素ベクトルの表現に基づく演算法について議論された。

WCTA86-10 田中 初一 (神戸大)
「符号理論と暗号系」
同日午後から合同開催されたワークショップ

プとの関連を考慮し、符号理論と暗号系の共通点、相違点や符号理論の暗号系への寄与などについて、解り易い包括的な解説が行われ、両ワークショップの橋渡しの役割を果たした。

同会場において、引き続いて開催された1986年暗号と情報セキュリティワークショップは、特に、若手の研究者を中心に最近の研究報告が行われ、白熱した討論が続いた。つぎに、各講演について、簡単に内容を報告する。

WCIS86-1 神竹 孝至、川村 信一
(東芝)「ICカードとセキュリティ」

- ・ICカードのセキュリティ機能
- ・カード発行時のセキュリティ
- ・取引証明

WCIS86-2 高島 洋一、松本 勉、
今井 秀樹 (横国大)「ジャンケンとコイン投げ」

- ・ネットワーク上でのジャンケンとコイン投げ実現
- ・確率的な問題、暗号的な問題、計算量的な問題
- ・RSA暗号系を利用したジャンケン

WCIS86-3 太田 和夫 (NTT)
「RSAマスタ鍵による同報通信における安全性」

- ・同報暗号通信での安全性の要件(同報データの秘密性、宛先集合の確認、同報データの同一性の確認)

WCIS86-4 鳥居 直哉、東 充宏、
秋山 良太 (富士通研)「RSA分割計算処理の一検討」

- ・高速指数計算法
- ・剰余計算の分割処理とパイプライン処理
- ・512ビットRSA暗号化処理速度200~300 kbps

WCIS86-5 伊東 利哉、オン・ティチャイ、辻井 重男(東工大)「正規基底を用いたGF(2^t)における逆元的高速算法」

- ・GF(2^t)上で構成される公開鍵暗号系的高速暗号化/復号化の実現
- ・正規基底を用いたGF(2^t)上の逆元的高速算法

WCIS86-6 岡本 栄司、中村 勝洋
(日電)「暗号用乱数発生器について」
・数学上の困難な問題に安全性の保証を帰着
させた乱数の発生方式
・暗号用乱数の Unpredictability

WCIS86-7 植松 友彦、稲葉 和生、
坂庭 好一(東工大)「RSA暗号系の拡張
とその計算量に関する一考察」
・代数的整数に対して定義されるRSA暗号
系(一般的拡張)
・最大乗算回数の軽減と暗号系の強度の低下

WCIS86-8 森井 昌克 笠原 正雄
(阪大)「中国人剰余定理を用いた公開鍵暗
号系について」
・ナップザック問題を利用した公開鍵暗号系
とその解読法
・中国人剰余定理を用いた公開鍵暗号系の多
項式環上の構成

WCIS86-9 黒沢 馨、伊東 利哉、竹
内 正士(東工大)「素因数分解の困難さと
同等の強さを有する逆数を利用した公開鍵暗
号」
・素因数分解ができなければ破れない公開鍵
暗号
・暗号文に対して平文は一つ決定される

WCIS86-10 松本 勉、今井 秀
樹(横国大)「第三の鍵共有方式」
・個別に暗号鍵を共有する方式、PKDS、
に続く第三の鍵共有方式
・総エンティティ数が多い大規模ネットワ
ークにおける実用的な鍵共有方式
・ランダム符号を用いた実現

WCIS86-11 宮口 庄司 (NTT)
「高速データ暗号アルゴリズムFEALのf
関数と安全性」
・f関数のデータランダム化特性(DES対
FEAL)
・マイクロプロセサのアセンブラプログラム
による暗号化速度150kbpsの達成

WCIS86-12 館林 誠 (松下)「
CRYPTO86参加報告」
・DESの性質(2件)

- ・素因数分解の並列処理(3件)
- ・暗号ハードウェア(3件)
- ・公開鍵暗号、乱数発生、署名(8件)
- ・秘密分散法(2件)
- ・ソフトウェアシステム(3件)
- ・暗号プロトコールとzero-knowledge proofs(8件)
- ・ソフトウェア保護、確率的暗号系など(5件)

以上の両ワークショップの更に詳しい内容に
ついては、講演論文集の在庫を、二冊一組と
して3000円で販売しております。ご希望
の方は下記までご連絡下さい。

〒350 川越市鯨井中野台2100
東洋大学工学部電気工学科
河野隆二

Phone (0492) 31-1211

内線320、332

Fax (0492) 33-1855

編集後記

ニューズレターNo. 2をお届けします。
今年は、学会発足一年目ということもあって、
ニューズレター発行については準備不足の感
も否めませんでした。編集についても明確な
方針といったものはまだありません。これは
今後の課題ですが、むしろこのまま形式に捕
らわれない自由な編集をしてゆくのも面白い
のではないのでしょうか。会員諸氏の自発的な
寄稿を歓迎します。(編集：韓太舜、川端勉)

情報理論とその応用学会事務局

吹田市山田丘2-1 (〒565)

大阪大学工学部通信工学科

佐藤 正志 06-877-5111