



情報理論とその応用学会ニュースレター

私が出会った本 金子敏信 (東京理科大学)
 シヤノン理論ワークショップ開催報告 植松友彦 (東京工業大学)
 2007 年度第 3 回理事会報告
 2007 年度総会報告
 ニュースレター原稿募集

私が出会った本

金子敏信 (東京理科大学)



金子敏信 (東京理科大学)

私の研究は、誤り訂正符号でスタートしたので、出会った本で、記憶に残っているものをあげるならば、宮川洋、岩垂好裕、今井秀樹著「符号理論」(昭晃堂)と W.Wesley Peterson 著 “ERROR-CORRECTING CODES” (The MIT Press) である。両方とも、符号理論の教科書であり、群、環、体などの離散数学の知識を含め、線形符号、巡回符号、BCH 符号や RS 符号、そして、たたみ込み符号 (Peterson の本では Recurrent code) まで解説している。

修士 1 年の時に、東京大学出版会の Reprint 版として Peterson の本を購入した。私には難しく感じられ、なぜこんなに難しい数学の勉強をする必要があるのかわからないまま、表面的に 7 割ほど、読破した。工学系の人間であり、離散数学の講義を受けたことのない人間にとっては、“符号理論は、数式で綺麗に表現している” 程度の感想である。

その後、宮川の符号理論が出、500 ページ以上の厚さに驚き“誤り訂正符号は、こんなに沢山の種類がある” などと思いながら拾い読みをした。それは、広い範囲の誤り訂正符号を網羅し、その後出版された Peterson の “ERROR-CORRECTING CODES -2nd Edition-” (The MIT Press) と共に、私にとり、バイブルである。現在の専門は、暗号理論であるが、この分野で符号理論の知識が役に立ち、今でも、符号理論の本を開くと、“暗号のこの分野に使えるのでは？” などと思う知識に出会うことがある。その時点で解らなくても、とにかく本を読み通せば、後日、役に立つ知識が頭の中に入ってくるものである。

私の現在の専門において、出会った本を紹介する。E.Biham, A. Shamir 著 “Differential Cryptanalysis of DES-like Cryptosystems” である。差分攻撃と呼ばれる手法で、共通鍵暗号 DES が、選択平文攻撃で 2^{47} 組の平文・暗号文対を使って解読できると 1990 年に示した、Biham の博士論文である。選択平文攻撃は、攻撃者が意図的に選んだ平文に対応する暗号文を手に入れて行う攻撃である。

DES の唯一の非線形要素は S-box であり、6 ビット入力 4 ビット出力のテーブルで与えられる関数である。Biham は、それを計算機解析し、入力差分が、その出力差分に高い確率で伝播するものを選び、そ

れを接続し DES の暗号化関数において伝播する差分の連なり（差分パス）を見だし、DES の解読アルゴリズムとしている。図を用い、差分パスが解りやすく示されているが、“解読とは、ここまで丹念にやる作業である”との感想を持った。

その翌年 1991 年に、私は、共通鍵暗号 FEAL-4 を既知平文攻撃で 24 組の平文・暗号文対を使い、PC で解読した。解読所要時間は 14 秒である。既知平文攻撃は、ランダムに与えた平文・暗号文対を使って行う攻撃である。FEAL の唯一の非線形関数は、S 関数と呼ばれる算術加算であり、その入出力差分の関

係をビット単位の関係式として表現し、その式を暗号系全体で接続することにより、差分を係数とする方程式を導出し、既知平文による攻撃を可能としている。昔、出会った本の感想、「数式にすると綺麗である」「解読とは、丹念に調べる作業である」が心の隅に残っていて、この研究に影響したと考えている。

最後に、情報理論とその応用学会の（特に若手の）研究者に、“ともかく本を読む”事を勧めたい。7 割程度の理解でも、頭の隅に残っていて、その後の研究に役立つと思う。

シャノン理論ワークショップ開催報告

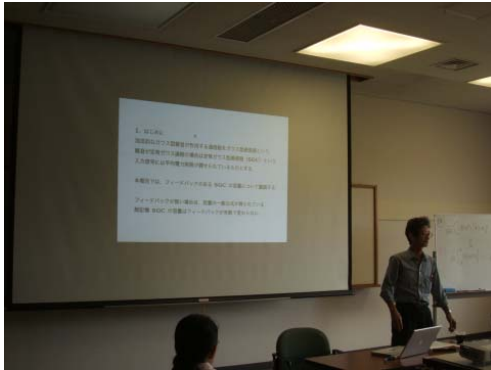
植松友彦 (東京工業大学)

第 5 回シャノン理論ワークショップは、9 月 6 日から 8 日にかけて修善寺のラフォーレ修善寺にて開催された。不便な場所での開催が続いていたこともあり、本年は関東や関西から新幹線で容易にアクセスできる修善寺温泉を選択した。しかし、ワークショップ当日の伊豆半島は、夜半に台風 9 号が通過するという状況にあり、午後になると暴風雨が強まり、外に居ると傘があっても全身ずぶぬれの状態になり、主催者として参加者 21 名全員の無事到着を祈るばかりであった。本ワークショップに初回から皆勤だった韓先生は、当日キャンセルの連絡があったことをホテルのフロントから聞き、君子危うきに近寄らずの心で台風に恐れをなしたかと思ったが、後日、風邪をひいて体調を崩されたことを知った。



ラフォーレ修善寺ホテル

今回のワークショップは 6 日午後に 1 セッション、7 日に 4 セッションの計 5 セッションが行われた。6 日のセッション LDPC 符号と接続符号では、NTT の三宅先生らによる LDPC 行列を用いたユニバーサル通信路符号化、電通大の Kurkoski 先生らによる LDPC 符号の復号についての密度発展法、法政大の西島先生らによる接続符号の見逃し誤り確率の計 3 件の発表があった。7 日の午前には、カオスのセッションでは九大の香田先生らの AD 変換とカオスの関係、記録符号化と通信路符号化のセッションでは、愛知江南短大の井原先生のフィードバックのあるガウス通信路の容量問題、および岐阜大の鎌部先生による 2 次元記録符号化法の拘束条件についての発表があった。7 日の午後には、情報源符号化の 2 セッションが行われ、前半は和歌山大の葛岡先生による多端子情報源符号化問題に関する 2 つの発表、後半は千葉大の須鎗先生による Tsallis エントロピーと一般符号木の関係、九大の竹内先生らによる木情報源と状態遷移関数の関係についての 2 件の発表が行われた。



セッションの様子

最後に台風の直撃について述べる，6日の夜，施設内をバスで移動して，別棟にあるバンケット会場で洋食のコースを味わった後，2次会と称して幹事部屋に集まり酒を飲んでいると，風の音も強くなり，窓はガタガタ揺れ始め，いよいよ台風が近づいてき

たなと思った．10時を過ぎたころ，なんとホテルは停電の間に包まれた．さすが台風直撃のダメージと感心していたら，停電は5分程度で復旧した．その後，台風のパワーに再度乾杯して2次会を続けたが，夜半になっても停電以外に何も起きなかったので寝てしまった．翌日の朝には雨も止み，昼には雲が切れ，夕方には風も止んで，7日の夜は，全員タオルを持って懇親会に出かけ，和室で和食を楽しんだ後，そのまま隣の建屋にある外風呂に浸かり，ワークショップで疲れた頭を休めると共に，台風から無事だったことにほっとしたのであった．

次回もまた SITA では行くことのない温泉地にて開催予定である．シャノン理論とその周辺分野に関連する多くの方々の参加を心から期待しております．

2007 年度第 3 回理事会報告

情報理論とその応用学会

2007 年度第 3 回理事会

2007 年 11 月 28 日 (水) 12:00 ~ 14:30

於 宝生苑「アイリス」の間

議事

1. 会長挨拶
2. 2007 年度第 2 回理事会議事録確認
3. 2007 年通常総会について
4. 2006(会計) 年度決算報告および監査報告
5. ISITA2006 決算報告および監査報告
6. 2007(会計) 年度予算案および収支中間報告
7. SITA からの開催補助を伴う WS の審議について
8. 2007 年度事業中間報告および 2008 年度事業

計画

9. 2007 年度ニューズレター発行状況および 2008 年度発行計画
10. SITA2007 開催報告
11. SITA2008 開催計画
12. ISITA2008 準備状況報告
13. IEEE Explore の件について
14. ISITA2010 開催地について
15. 2008 年度役員候補について
16. 細則変更案について
17. 入退会者について
18. その他
 - (a) 学会休会について
 - (b) SITA 皆勤賞に対する支出について

2007 年度総会報告

情報理論とその応用学会

2007 年度 通常総会

2007 年 11 月 29 日 (木) 16:00 ~ 16:40

於 宝生苑 「アイリス」の間

議事

- | | |
|-----------------------------|----------------------------|
| 1. 会長挨拶 | 5. ISITA2006 収支決算報告および監査報告 |
| 2. 2006 年度事業報告 | 6. 2007 年度事業中間報告 |
| 3. 2006(会計) 年度収支決算報告および監査報告 | 7. 2007(会計) 年度予算案および収支中間報告 |
| 4. SITA2006 収支決算報告および監査報告 | 8. SITA2007 開催報告 |
| | 9. 2008 年度事業計画 |
| | 10. SITA2008 開催計画 |
| | 11. ISITA2008 開催について |
| | 12. 2008 年度役員選挙 |
| | 13. 名誉会員の推薦について (報告) |
| | 14. その他 |

ニュースレター原稿募集

ニュースレター編集担当では、会員の皆様からの原稿をお待ちしております。研究会やワークショップなどの call for papers や国際会議などの参加報告、会員の声など、気軽に投稿して下さい。

今年は、あと 4 回のニュースレターの発行を予定しております。原稿の締切は 2 月末ですが、随時投

稿を受け付けており、原稿を頂いた時点での最近号に掲載する予定です。原稿は、できるだけ $\text{\LaTeX}$ のソースファイルが望ましいですが、その他の形式でも受け付けます。写真などの掲載も歓迎します。詳細は、巻末の編集理事・幹事にお尋ね下さい。

編集後記

原稿の執筆を快くお引き受け下さいました皆様に心よりお礼を申し上げます。皆様のご協力とご理解のお蔭で、無事任期中に 4 回のニュースレターを発行することができました。さて、最後に、ある方から画期的な発見を教えていただいたので、この場をお借りして皆様にお伝えいたします。2 送信者 1 受信者の $Y = X_1 + X_2 + N$ で表わされるガウス型多

重アクセス通信路を考えます。このとき $E[X_1^2] = 1$ かつ $X_1 = X_2$ とすると送信電力は $1 + 1 = 2$ ですが、受信電力は $E[(X_1 + X_2)^2] = 4$ になり、電力を増幅できるんだそうです。最近の原油価格高騰による不景気を緩和するためにこの発見が役に立つかも知れません・・・。(植松，松本)

編集担当者

植松友彦 (編集理事)

〒152-8552 東京都目黒区大岡山 2-12-1

東京工業大学大学院理工学研究科集積システム専攻

Tel. 03-5734-3243

Fax. 03-5734-2905

E-mail: uematsu@it.ss.titech.ac.jp

杉村立夫 (編集理事)

〒380-8553 長野県長野市若里 4-17-1

信州大学工学部電気電子工学科

Tel. 026-269-5237

Fax. 026-269-5220

E-mail: tsugimu@gipwc.shinshu-u.ac.jp

松本隆太郎 (編集幹事)

〒152-8552 東京都目黒区大岡山 2-12-1

東京工業大学大学院理工学研究科集積システム専攻

Tel. 03-5734-3864

Fax. 03-5734-2905

E-mail: ryutaroh@it.ss.titech.ac.jp

西新 幹彦 (編集幹事)

〒380-8553 長野市若里 4-17-1

信州大学工学部電気電子工学科

Tel. 026-269-5249

Fax. 026-269-5220

E-mail: mikihiko@shinshu-u.ac.jp

情報理論とその応用学会事務局

〒305-8573 茨城県つくば市天王台 1-1-1

筑波大学大学院 システム情報工学研究科 知能機能システム専攻

古賀 弘樹 気付

Tel: 029-853-6476

Fax: 029-853-6471

E-mail: sita-office@sita.gr.jp

URL: <http://www.sita.gr.jp/>