第 6 回誤り訂正符号のワークショップ開催報告

開催場所：山口県山口市　セントコア山口

開催期間：2017 年 9 月 6 日(水) ~ 9 月 8 日(金)

第 6 回誤り訂正符号のワークショップ実行委員長

安永 憲司（金沢大学）

2017 年 9 月 6 日(水)から 7 日(木)にかけて山口県山口市湯田温泉のセントコア山口にて、第 6 回誤り訂正符号のワークショップを開催致しました。本ワークショップは、情報理論とその応用サブソサイエティが主催するワークショップとして開催され、9 月 8 日(金)には情報理論研究会を併催致しました。

誤り訂正符号のワークショップは、最近は毎年開催しており、開催時期も昨年と同様、私立大学の夏休み期間を考慮し、9 月上旬としました。

今回の開催にあたっては、当初会場・宿泊先として予約していた宿が開催の 3 ヶ月前になって急遽使用できなくなるというトラブルが発生致しました。併催の情報理論研究会の関係者の皆様等、各所にご心配をおかけしましたが、野崎先生（山口大学）を始めとする実行委員の皆様の迅速な対応により、代替の開催会場を見つけることができました。開催会場と宿泊先を同じにすることは叶いませんでしたが、結果として、非常によい会場で開催することができたと思っております。

本ワークショップは、誤り訂正符号とその関連分野に関するものであり、一般講演の他にワークショップ企画を用意し、深く掘り下げた議論を行う場の提供を目指しております。今年は、１つ１つの講演の内容をじっくりと味わうことを狙い、ワークショップ企画による講演の数を減らしてみました。その結果、入門講演 2 件、一般講演 5 件、国際会議開催報告 1 件、コードコンペ結果発表 1 件、未解決問題セッション講演 2 件が行われました。コードコンペは、昨年初めて企画されたプログラミングコンペを受け継いだ企画です。また、未解決問題セッションは、参加申し込みを締め切った後に、参加者向けに募集を行い、開催しました。

会場のセントコア山口

会場内の様子

開催のプログラムは以下の通りです。

入門講演

・小柴 健史（早稲田大学） Secure Message Transmission : 可能性と限界

・岩本 貢（電気通信大学） 情報理論的安全性：さまざまな視点から

一般講演

・福本 真也（名古屋工業大学） ニューラルネットワークを用いた非正則 LDPC 符号に対する Normalized Min-Sum 復号法

・中原 悠太（早稲田大学） 富士山型空間結合符号の重み分布

・森田 啓義（電気通信大学） 二重最近傍誤り訂正符号の復号アルゴリズム

・廣友 雅徳（佐賀大学） LDPC 符号を用いたゼロ知識証明型認証方式

・Ryutaroh Matsumoto (Nagoya University) Two Gilbert-Varshamov Type Existential Bounds for Asymmetric Quantum Error-Correcting Codes

国際会議参加報告

・眞田 亜紀子（電気通信大学） ISIT2017 参加報告

企画セッション

・コードコンペ結果発表

未解決問題セッション

・松本 隆太郎（名古屋大学） 所与のアクセス構造を持つ秘密分散法を与える線形符号対の直接的な構成

・安永 憲司（金沢大学） 擬似ランダムな符号の構成

以下では、開催内容について簡単に振り返ってみたいと思います。

入門講演では、2 件ともに暗号よりの講演を用意しました。1 件目は小柴先生（早稲田大学）による、Secure Message Transmission に関する講演でした。送信者と受信者の間に n 本の通信路があり、そのうちの t 本が敵対者に盗聴・改竄されたとしてもメッセージを正しく安全に送信するための技術です。秘密分散法に近い技術ですが、送受信者間で複数回やり取りが可能であり、異なる技術です。小柴先生には、研究背景と問題設定、不可能性に関する基本的な結果等、入門講演にふさわしい講演を行って頂けました。秘匿性と信頼性を同時に実現する通信技術として、SITA コミュニティにおいてもっと注目されても良い技術だと感じました。

入門講演の 2 件目は、岩本先生（電気通信大学）による情報理論的安全性に関する講演でした。Shannon により導入されたいわゆる完全秘匿性は、多くの方がよく理解されている安全性概念です。しかし、それを少し拡張した場合、それがどのような意味で安全性を保証しているのか、たちまちわからなくなってしまいます。岩本先生には、安全性の定義のある種の難しさを非常に丁寧に、かつ独自の観点からご説明頂けました。誤り訂正符号を研究する上では秘匿性なんて無縁だと感じる方もいるかと思

いますが、秘密分散を始め様々な概念が登場した現在では、避けることも難しいと感じます。その場合、どのような意味で秘匿したといえるのか自信を持って答えつつ、しかしそれは難しい問いであるという自覚も持ちたいと感じました。

一般講演については、個々の講演に対する報告は控えますが、ニューラルネットワーク・LDPC 符号・空間結合符号・最近傍誤り訂正・ゼロ知識証明・量子誤り訂正符号・Gilbert-Varshamov 限界という様々なトピックが登場し、誤り訂正符号とその関連分野の広さを感じました。

国際会議参加報告では、今年 Aachen で開催された ISIT 2017 の報告を眞田先生（電気通信大学）に行って頂きました。ISIT 会期中に参加報告のお願いするという手順の悪い依頼をお引き受けいただいた眞田先生に、あらためて感謝申し上げます。

未解決問題セッションは、形式的すぎない形で議論できる場を提供したいという狙いで設けました。また、通常の講演だと新しい成果がないと発表しにくいため、そのような敷居のないセッションとして未解決問題セッションとしました。松本先生（名古屋大学）より、ある意味で古典的な問題に対する未解決問題をご提示頂きました。符号を構成してその性質を調べることは一般的に簡単ではないですが、それとは逆に、ある性質をもつように符号を構成するというのはもっと難しい問題だと改めて感じました。あまり進展のないテーマですので、参加者の誰かがブレークスルーを起こすことを期待したいです。最後に、私から、符号語が擬似ランダムであることの利点ならびにそのような符号に関する未解決問題の紹介を行いました。暗号技術を直接的に誤り訂正に活かそうという話であり、最後も暗号色の強い話で、今年のワークショップを締めました。

最後に、企画セッションであるコードコンペについて述べたいと思います。これは、昨年開催されたプログラミングコンペを受け継いだ企画です。今年の課題は、よいパラメータをもつ削除訂正符号を見つけるというものでした。具体的には、以下の条件を満たす符号を見つけることです。

1. t 個の削除を訂正できる 2 元符号であり、符号語の長さはすべて等しい
2. 符号長 N と符号語数 M に関して、N×M が 50000 以下である
3. 符号化レートが大きい符号である

上記に関し、t = 2, 4, 8 の 3 部門を設け、さらに、それぞれに一般符号部門と線形符号部門を設けました。

コードコンペの課題の狙いとしては、まず、最近注目を集めつつある削除・挿入訂正符号に興味を持ってもらいたいという点があります。その上で今回の課題ですが、訂正する削除数 t を固定して符号化レートの大きい符号を構成しようとするため、符号長が大きい方が、符号長に対する削除割合が小さくなり有利です。しかし、符号長が大きいと全数探索的な方法は時間がかかります。そのため、探索の精度と時間のトレードオフを考慮する必要がある課題となっています。N×M が 50000 以下という制限は、提出された符号の訂正可能な削除数を短時間で確認できるようにするためです。また、線形符号部門を設けた理由ですが、削除訂正可能な線形符号としては、(t+1)回繰り返し符号が t 削除訂正できるということがよく知られていますが、それ以外のよい方法が知られていないため、繰り返し符号を越える

線形符号の提案を密かに期待して設定しました。(t+1)回繰り返し符号だと符号化レートは符号長に関係なく 1/(t+1)です。

コンペへの参加者数ですが、一般符号部門の t = 2 に 5 名、t = 4 に 3 名、t = 8 に 2 名、線形符号部門には t = 2, 4, 8 いずれも 1 名となりました。線形符号部門は、出題者でもある実行委員長だけが符号を提出することとなり、また提出された符号も (t+1)回繰り返し符号でしたので、新たな発見には至りませんでした。

一般符号の各部門について優れた符号を提出された方を表彰し、ワークショップにおいて簡単な講演を行っていただきました。受賞者並びに提出された符号のパラメータは以下の通りです。(敬称略)

t = 2 部門：石松 佑太（名古屋工業大学）中野 貴文（名古屋工業大学）

符号長 N = 21, 符号語数 M = 2380, 符号化レート 0.534131

t = 4 部門：中野 貴文（名古屋工業大学）

符号長 N = 30, 符号語数 M = 1666, 符号化レート 0.356739

t = 8 部門：Justin Kong（千葉大学）

符号長 N = 50, 符号語数 M = 289, 符号化レート 0.163499

いずれも学生の受賞となりました。3 名に講演を行っていただきましたが、皆異なるアプローチで問題に取り組んでおり、大変興味深かったです。

今回のコードコンペは、出題者も正解を知らない中での実施となりましたが、優れた符号が複数提出され、企画としてはなかなか良かったかと思っております。とある大学の研究室では、研究室の学生間で事前コンペを開催し、その優秀者にワークショップへの参加権を付与するという方法でコードコンペを活用していたようです。ワークショップ企画のこのような活用は大変嬉しいことでした。手間のかかりすぎないお手頃な課題の設定というのはなかなか難しいですが、今後もこのような企画を続けることができればと思っております。