第 4 回有限体理論とその擬似乱数系列生成への応用ワークショップ開催報告

開催場所：萩・明倫学舎（山口県萩市）

開催期間：2018 年 8 月 27 日（月）～28 日（火）

実行委員長　松元隆博（山口大学）

2018 年 8 月 27 日（月）から 28 日（火）の 2 日間、第 4 回有限体理論とその擬似乱数系列生成への応用ワークショップ（FFTPRSWS2018）を山口県萩市の萩・明倫学舎にて開催しました。このワークショップは、情報理論とその応用シンポジウム（SITA）あるいは、International Symposium on Information Theory and Its Applications (ISITA) などにおいて、 日頃より、有限体理論とその擬似乱数系列生成への応用に関連する研究の成果発表をしている研究者、またそのようなテーマに興味をもっている研究者が一堂に会し、日々の研究活動の中で得られた成果の報告をはじめ、疑問に思っている事柄、あるいは個人的な興味から深く掘り下げているテーマなどを、十分な時間をかけてお互いに紹介し、共有し、密な議論を展開するための場を提供することを意図したワークショップで、2015 年 8 月に群馬県吾妻郡草津町（草津温泉）で第 1 回目が開催され、その後、2016 年 9 月に大分県由布市（由布院温泉）、2017 年 10 月に北海道旭川市にて開催されてきました。

第 4 回目にあたる FFTPRSWS2018 は、開催する平成 30 年(2018 年)が明治元年(1868 年)からちょうど 150 年になる節目の年であることから、長州藩 36 万石の城下町であり、世界遺産（明治日本の産業革命遺産）を有する萩で開催することにしました。私事ですが、山口大学に勤めて 20 年になりますが、萩で学会が開かれたことを聞いたことが無く、珍しいこともあり選定しました。また、会場の萩・明倫学舎は享保 3 年(1718 年)に創設された長州藩の藩校明倫館の跡地に建っており、現在観光の起点になっている場所です。この明倫館では吉田松陰や楫取素彦(小田村伊之助)も教鞭をとり、高杉晋作や木戸孝允(桂小五郎)も通いました。また、施設内の有備館は文久 2 年(1862 年)に萩を訪れた坂本龍馬が剣術の試合をしたと言われています。

肝心のワークショップですが、14 名（一般 11 名、学生 3 名）の参加があり、1 件の招待講演と 7 件の一般講演の合計 8 件の発表がありました。いずれの発表においても、熱心かつ有意義なディスカッションが行われました。

なお、発表者と発表題目は下記の通りです（敬称略）。

招待講演）松藤信哉(山口大学)

「Bent 型 ZCZ 符号の構成法」

一般講演 1）小寺雄太(岡山大学)

「検索可能暗号への暗号理論的擬似乱数生成器の活用に関する考察」

一般講演 2）武田祐樹(岡山大学)

「線形複雑度が可変な擬似乱数系列の生成法」

一般講演 3）土屋和由(光電製作所)

「半 l 系列における記号の出現度数の対称性」

一般講演 4) 上原聡(北九州市立大学)

「Zm 上のアダマール型行列の要素表現に関する一考察」

一般講演 5) 宮崎武(北九州市立大学)

「擬似乱数生成器のための二次合同系列の周期による分類に関する一考察」

一般講演 6) 村岡英之(九州工業大学)

「整数上のテント写像とロジスティック写像におけるビット毎の 0/1 の出現確率」

一般講演 7) 小嶋徹也(東京工業高等専門学校)

「有限体上のアダマール型行列とその展望」

上記の発表の時間以外でも、休憩時間や同会場の萩暦で開催した懇親会を通じて、研究者間の交流を深めることができ、有意義なワークショップとなりました。

なお、今回からの新しい試みとして、これまで予稿集を発行せず、発表だけ行っていましたが、今回から予稿集を発行しました。予算削減と効率化のために、予稿集は電子データのみとし、発表者はワークショップ HP からダウンロード、出席者は会場で USB メモリから PC にコピーしてもらうことで配布しました。

最後に、本ワークショップを開催するにあたり、情報理論とその応用サブソサイエティから助成を頂きましたことに感謝申し上げます。

図 1. 発表風景

図 2. 萩・明倫学舎外観