第 9 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：愛媛大学（現地/オンライン）
開催期間：2023 年 9 月 11 日（月）～12 日（火）
実行委員長　小寺雄太（岡山大学）

2023 年 9 月 11 日（月）から 12 日（火）の 2 日間、第 9 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（FFTPRSWS 2023）を開催しました。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（ISTA)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持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、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す。

第 6 回目(2020 年度)および第 7 回（2021 年度）は、世界的に流行した新型コロナウイルス感染症へ配慮し、全面オンラインでの開催となりましたが、第 8 回目から感染状況に応じて完全にオンライン開催とすることをお断りしたうえで、九州情報大学の博多駅東サテライトキャンパスで 1 日のみの現地で開催しました。

今回のワークショップではより現地での開催規模を大きくし、従前どおりのスケジュールでの実施を目指し、1 泊 2 日での開催としつつ、遠方の方もご参加いただきやすいようにオンラインでの同時接続も行いました。開催場所は愛媛大学の原本博史先生にご尽力いただき、教室設備を無償で使用させていただきました。この場をお借りして謝意を申し上げます。

さて、肝心のワークショップですが、13 名（一般 7 名、学生 6 名）の参加があり、9 件の一般講演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。

発表者と発表題目は以下の通りです（敬称略)。

一般講演 1）藤井　博希（北九州市立大学）
「2 つの整数上のロジスティック写像を用いた疑似乱数生成法の提案」

一般講演 2）斉藤　朝輝（公立はこだて未来大学）
「代数的整数の一様集合の算術的独立性」

一般講演 3）武内　友希（岡山大学）
「トレースと平方剰余判定を用いた擬似乱数生成器に一様分布を保障するためのパラメータに関する考察」

一般講演 4）原本　博史（愛媛大学）

「NIST SP800-22 の二重検定におけるサンプルサイズに関する研究」

一般講演 5）藤原　光樹（岡山大学）

「Wold 型 RO-Based RNG における D-FF のクロック同期の乱数列への影響と XOR ゲートへの不定値入力での挙動の検証」

一般講演 6）宮﨑　武（九州情報大学）

「迷路法によって生成される系列の種類数の理論的解析に関する一考察」

一般講演 7）石田　哲郎（岡山大学）

「行列演算による NTRU 方程式の解法に関する考察」

一般講演 8）林　夏生（北九州市立大学）

「CAPTCHA への逆画像検索攻撃を対象とする織物フィルタの耐性評価に関する研究」

一般講演 9）高市 康平（北九州市立大学）

「動的同期カオスベースランダム科技を用いたストリーミングデータ用暗号システム」

参加者同士で忌憚のない活発な議論や交流の場を設けることができた有意義なワークショップとなりました。

なお、今回でも前回と同様に予稿集を発行し、参加者各位へは印刷物および PDF として配布いたしました。

図 1. 発表の様子