有限体理論とその擬似乱数系列応用ワークショップ開催報告
開催日：平成 27 年 8 月 27,28 日
場所：草津温泉（群馬県）

岡山大学　野上保之

平成 27 年 8 月 27,28 日に群馬県は草津温泉にて「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」を開催いたしましたので報告をいたします。

私が情報理論とその応用シンポジウム（SITA）に参加をするようになって、はや 20 年が経ちます。その間、有限体理論をベースにした種々のテーマに興味をもってきましたが、最近は縁あって擬似乱数系列について研究をしています。ふと SITA や ISITA、IWSDA など系列に関する国内外の会議、また論文誌での発表を見渡しますと、SITA シンポジウムでよくお会いする方々が、とてもアクティブに最前線で活躍していることに気がつきます。そして自然と、そのような皆様とここ数年、色んな場面でお話をしたり、議論をしたり、さらには共同で研究を進める機会も増えてまいりました。

私もそうですが、有限体理論を深掘りしながら研究を進めている方々は、研究テーマや、着眼点、その進め方などがマニアックであることが少なくありません。個人的にはとても興味があって進めていても、それを周辺研究者にも共感してもらえるか不安に思いながら進めている研究もあると思います。「系列」というキーワードに焦点を絞りながら、そのような研究活動の一端をお互いに披露し、楽しさを共有し、十分に時間をとってより深く議論したいという意見が集まり、本ワークショップが企画されました。

そのようにして、「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」が開催される運びとなり、関係の方々とその開催地について話をしていると、自ずと温泉という言葉がでてまいります。期せずして、私の故郷が草津温泉ということもあり、その開催地は草津温泉になりました。メインの会場を湯畑（右下写真）のふもとにある老舗旅館の日新館としつつも、ここではセッション用のスペースをとることはせず、草津町役場の研修室をセッション会場とするという異例な実施になりましたが、これも本企画ワークショップの一つの思い出になりそうです。

写真：草津温泉湯畑（日新館はこの斜め向かい）

さて、会場が草津温泉ということで、必ずしも交通の便が良くないため、初日は午後 3 時から、2 日目もお昼には終了するというスケジュールで開催いたしました。

初日は、信州大学の杉村立夫先生による基調講演ではじまり、杉村先生のこれまでの研究テーマについてじっくり紹介をいただきました。先生の教え子としてその側で一緒に研究させていただいた私としては、ご講演の中の円周等分既約多項式や Zech 対数表の研究の話がとても懐かしく感じられましたが、何より杉村先生の「研究を楽しむ」という言葉、改めて自分自身の教え子にも同じように伝えてゆきたいと思いました。続いて、長野高専の小林先生が偶既約多項式に関する発表をされました。有限体上で与えられる既約多項式は、その特性などから種々の分類ができますが、ご発表では次数が偶数である項のみからなる偶既約多項式の数、構成法、低次の既約多項式との関連、そして偶既約多項式の根を用いた効率のよい拡大体演算の構成法への応用について紹介がありました。とりわけ暗号の分野において、そのような演算の効率化が活きてきそうです。初日の最後は、九工大の荒木先生の発表で、整数上で定義されるロジスティック写像について、初期値に対する鋭敏性に基づく乱数生成への応用、これを定義するコントロールパラメータと初期値の設定による周期や（生成される系列が描く）ループ構造との関係、またその系列を用いたセキュリティ応用について紹介がありました。初期値などパラメータの設定による系列の振舞いが明確になることで、様々なアプリケーションへの応用が議論できるのだと思います。初日のセッションを終え、本来の会場である日新館にて懇親会を開き、引き続いて客室にてお酒なども交えながら遅くまで議論がつづきました。日新館は私の同級生の旅館でもあるので、その辺りは気兼ねなく、（私は日新館に宿泊をしていないのですが）旅館の露天風呂にも入らせていただきました。

本ワークショップ 2 日目は、北九州市大の宮崎先生と上原先生のご研究で、素体上で定義されるロジスティック写像についての発表からはじまりました。前日の荒木先生のご発表では整数上で定義されたロジスティック写像を考えていましたが、これを素体上で考えた場合に、幾らかの特徴が浮かび上がってきます。宮崎先生の発表では、標数としての素数の選び方と最大周期の関係、得られる系列の乱数性の NIST 検定報告、そして異なる 2 つの系列ループ間での自己準同型写像の存在などの紹介がありました。これに続いて、株式会社光電製作所の土屋さんの発表では、その素体上のロジスティック写像に対して、コントロールパラメータを 4 に限定し、長周期が期待される初期値集合をルジャンドル記号で特徴づけ、生成される系列の取りうる最大周期について双曲線構造を導入した証明を紹介されました。そして、長周期をとるための初期値の設定について、さらには得られる系列の線形複雑度およびそのプロファイルについての報告もありました。この辺りは、今後さらに深く掘り下げられてゆくものと楽しみにしています。そして本ワークショップの最後

の発表になりますが、私は原始多項式とべき乗剰余記号を用いた多値擬似乱数系列の生成について報告をいたしました。もとより M 系列やルジャンドル系列がよく知られていますが、これらを組合せて得られる系列について、その周期や周期自己相関特性、線形複雑度の特徴を紹介いたしました。ターゲットをセキュリティ応用とした場合、理論的に明確にその辺りの振る舞いが示せることは意義があります。その着眼点や理論的な証明方法については、上原先生や土屋さんからたくさんのご指導とアドバイスをいただきました。

以上、開催報告になります。

私の個人的な感想ですが、それぞれが独立した研究のように見えながらも、互いの報告を聞くことによって、その一部一部が重なりあい、それぞれのより深い理解へとつながり、時間を気にせずに議論をすることで、何かがぼんやり特異点のように炙りだされます。 今回のワークショップで炙りだされた「何か」の一つは、Dickson 多項式でした。そのような不思議なものをそれぞれが持ち帰り、研究をさらに深掘りし、研究がいっそう進展してゆくことを願っております。皆さん、研究を楽しみましょう！