1 Research Plan

The purpose of this research is to develop and analyze new methods of pseudorandom sequence generation based on structures from abstract algebra such as algebraic number fields, algebraic function fields, and completions of rings in $p$-adic topologies. This work would benefit greatly from interaction with researchers with expertise in these and related fields.

Pseudorandom sequences are essential tools in a wide variety of information technology applications. Binary pseudorandom sequences are used as spreading codes in spread spectrum communications, including code-division multiple access systems [14] such as digital cellular telephones and GPS signals; for frequency-hopping in radar and radio systems for protection against jamming [28]; as randomizing keys in stream cipher (private key) cryptosystems [17]; as pseudo-noise generators to mask communications [4] from eavesdroppers and jammers; and as codewords in error correcting codes. Pseudorandom sequences of large numbers are a key ingredient in large simulations and other quasi-Monte Carlo (QMC) applications such as reactor design, oil well exploration, radiation cancer therapy, traffic flow, pricing of financial instruments, and VLSI design [11].

Linear feedback shift registers (LFSRs) of various types are commonly used for the generation of pseudorandom sequences for many of these applications because they are fast, easy to implement in hardware, and have excellent randomness properties. They have been studied intensively for over forty years [12] (principally using the Galois theory of finite fields). Their usefulness does not appear to have any end in sight.

While LFSRs are weak cryptographically, over the years many techniques have been developed for the synthesis of more secure pseudorandom sequences using LFSRs [6, 10, 12, 13, 23, 26, 30]. Nevertheless, the underlying linear structure of LFSR sequences tends to leave them vulnerable to attack (e.g., by algebraic cryptanalysis and correlation attacks).

Despite forty years of research, no fundamentally new architecture for feedback shift registers had been developed and successfully analyzed until the discovery (by Goresky and Klapper [15, 16] in the context of cryptography, and independently by Marsaglia, Couture and L’Ecuyer
[18, 8] in the context of quasi-Monte Carlo simulation) of “feedback-with carry” shift registers (FCSRs). They are also related to Blum, Blum, and Shub’s pseudo-random number generator [5]. In the time since their appearance, FCSR generators have been incorporated into reference books and textbooks [9, 24, 20, 3], and have been studied by various researchers [1, 2, 8, 19, 21, 22, 25, 27]. They have been implemented in a number of standard software packages. Pseudorandom sequences generated by FCSRs have many desirable properties for applications to spread spectrum communications, error correcting codes, cryptology, and quasi-Monte Carlo simulation. However they are very different from LFSR sequences and their analysis involves a completely different collection of mathematical tools: where the analysis of LFSR sequences depends on power series over finite fields, the analysis of FCSR sequences depends on $p$-adic numbers and algebraic number fields. Many of the basic properties of FCSR/MWC sequences have been explored and determined, while a whole zoo of related algebraic feedback shift register (AFSR) pseudorandom sequence generators has been discovered, whose analysis often requires modern sophisticated mathematical techniques. Their analysis depends on $I$-adic rings of various sorts and involves interesting and often hard questions in number theory (for example, Minkowski’s method of analyzing number fields via integer lattices in Euclidean space plays a role in understanding the periodicity of AFSR sequences). My goal of finding and studying AFSR sequences with good pseudorandomness properties would benefit greatly from interaction with various mathematicians at the Institute for Advanced Study.

My research over the 2006-2007 academic year will address a number of new, innovative issues concerning FCSR sequences, their generalizations, and applications. The main research goals of the proposed project are the following, in collaboration with Mark Goresky.

1. The development of cryptographically secure stream ciphers which incorporate FCSR and AFSR sequences.
2. The solution of the “register synthesis problem”, an essential step in understanding the security of a large class of stream ciphers.
3. The development of high speed FCSR-MWC generators with good statistical properties for use in pseudo Monte Carlo methods, and the introduction of new algebraic techniques for the analysis of these generators.
4. The identification of new classes of AFSR sequences with good randomness properties for use in pseudo Monte Carlo applications.
5. The development of new block and convolutional error correcting codes obtained by replacing LFSR and power series constructions by AFSRs and generalizations of power series.
6. The completion of a comprehensive book on abstract algebra and its application to sequence design and analysis.
References


2 List of Andrew Klapper’s Publications

Most publications are available from http://www.cs.uky.edu/~klapper/papers.html

2.1 Refereed Journal Articles and Book Chapters


2.2 Refereed Conferences


2.3 Unrefereed and Invited Conferences


