abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Linear feedback shift registers (or, equivalently, linear recurrences) have been studied in one form or another for at least 75 years. They have found a
Myriad of applications in communications, cryptography, random number generation, and other areas. A decade or so ago we began to study arithmetic (or
With carry'') analogues of LFSRs, called feedback with carry shift registers (or FCSRs) or multiply with carry generators. FCSRs are based on the
algebra of the integers and N-adic numbers where LFSRs are based on the algebra of polynomials and power series. Many basic properties of FCSRs have been mapped out, and various applications have begun to emerge (cryptanalysis, stream cipher design, quasi-Monte Carlo).

More recently, we have considered more general sequence generators, call algebraic feedback shift registers (or AFSRs), based on general algebraic rings and their pi-adic completions. Much less is known about these sequence generators. For example, we know how to solve the register synthesis problem for LFSRs (via the Berlekamp-Massey algorithm) and FCSRs, but only in special cases for general AFSRs.

This talk will be a survey of these topics, requiring no prior knowledge of the area. I will review the basic properties of LFSRs and survey the current state of our knowledge of FCSRs and AFSRs. I will describe basic properties, special cases when we know statistical properties, when there is
a register synthesis algorithm, and perhaps other topics such as arithmetic analogues of correlation functions.