Novel Application of Collatz-like Sequences to Cryptographically Secure Pseudo-Random Number Generation

Chen, James

In the digital age, more and more data needs to be transmitted securely, making cryptographic functions increasingly important. At the basis of all cryptographic functions is a pseudo-random bit generator, which takes in a seed and returns a generated bitstring which ``looks'' random. A function which may satsify this property of randomness is the Collatz function, which takes a positive integer input n and outputs 3n+1 if n is odd and n/2 if n is even. We extend this function to a generalized Collatz function, which again takes a positive integer input n, outputting (mn+d)/2 if n is odd and n/2 if n is even, where m and d are odd positive integers. The objective of this project is to introduce a class of pseudo-random bit generators based off of Collatz-like functions. We first propose a simple Collatz generator, which returns the least significant bit of the output of the Collatz function, iterated on a seed value. This entropy of this generator is analyzed using the Diehard battery of statistical tests, allowing specific characteristics and patterns to be identified. We then analyze the cryptographic security of the generator with respect to known number theory problems to determine its computational complexity. We then propose an improvement to the simple Collatz generator, which shrinks its bits to increase security. The self-shrinking Collatz generator provides increased cryptographic complexity over the simple Collatz generator for large seed values.

Awards Won:
Mu Alpha Theta, National High School and Two-Year College Mathematics Honor Society: Third Award of $1,000.