STEVE WANG, Carleton University

A matrix approach to the period of a nonlinear congruential pseudorandom sequences over finite fields

We study the period of a nonlinear congruential pseudorandom sequence $\bar{a} = \{a_0, a_1, a_2, ...\}$ generated by $a_n = f^{(n)}(a_0)$ with initial value a_0, where f is a permutation polynomial over a finite field. We explain the connection between the period of the sequence and the order of an associated matrix $A(f)$ defined by the powers of $f(x)$. We also explore the connection between the rank of $A(f)$ and the cardinality of the value set of f.