New Results on the Linear Complexity of Nonlinear Pseudorandom Number Generators

Hassan Aly, Wilfried Meidl, Arne Winterhof

The *linear complexity profile* of a sequence (s_n) over the finite field $\mathbb{F}_p$ is the function $L(s_n, N)$ defined for every positive integer N, as the least order L of a linear recurrence relation over $\mathbb{F}_p$

$$s_{n+L} = c_{L-1}s_{n+L-1} + \ldots + c_0 s_n, \quad 0 \le n \le N - L - 1,$$

satisfied by the first N elements of (s_n). The value $L(s_n) = \sup_{N \ge 1} L(s_n, N)$ is called the *linear complexity* of the sequence (s_n). Linear complexity and linear complexity profile are valuable measures for unpredictability and thus suitability in cryptography. Generators with low linear complexity are also shown to be unsuitable for some applications using quasi-Monte Carlo methods.

Given a rational function $f(X)$ over $\mathbb{F}_p$ the *nonlinear congruential pseudorandom number generator* (u_n) is defined by the recurrence relation

$$u_{n+1} = f(u_n), \quad n \ge 0,$$

with some initial value $u_0 \in \mathbb{F}_p$. Obviously, the sequence (u_n) is eventually periodic with some period $t \le p$. We may assume that it is purely periodic. In the case that $f(X)$ is a polynomial of degree $d \ge 2$ we have the lower bound

$$L(u_n, N) \ge \min\left\{\log_d(N - \lfloor \log_d N \rfloor), \log_d t\right\}, \quad N \ge 2,$$

on the linear complexity profile of a nonlinear congruential pseudorandom number generator with a general polynomial $f(X)$ of degree $d \ge 2$. For some special classes of functions $f(X)$ much better results were proven:

1. Binomials of the form

$$f(X) = aX^{p-2} + b, \quad a, b \in \mathbb{F}_p,\ a \ne 0;$$

2. Monomials

$$f(X) = X^e, \quad e \ge 2;$$

3. The family of *Dickson polynomials* $D_e(X) \in \mathbb{F}_p[X]$ defined by the recurrence relation

$$D_e(X) = XD_{e-1}(X) - D_{e-2}(X), \quad e = 2, 3, \ldots,$$

with initial values $D_0(X) = 2, \quad D_1(X) = X$;

4. Rédei functions defined as follows.

Suppose that $r(X) = X^2 - \alpha X - \beta \in \mathbb{F}_p[X]$ is an irreducible quadratic polynomial with the two different roots ξ and $\zeta = \xi^p$ in $\mathbb{F}_{p^2}$. We consider the unique polynomials $g_e(X), h_e(X) \in \mathbb{F}_p[X]$ defined by the equation $(X + \xi)^e = g_e(X) + h_e(X)\xi$. The *Rédei function* $f_e(X)$ of degree e is then given by

$$f_e(X) = \frac{g_e(X)}{h_e(X)}.$$