A Survey on Recursive Nonlinear Pseudorandom Number Generators

Arne Winterhof

Austrian Academy of Sciences
Johann Radon Institute for Computational and Applied Mathematics
Linz

MCQMC 2012
Pseudorandom Numbers

Numbers which are generated by a deterministic algorithm and 'look random' are called pseudorandom.

Desirable 'randomness properties' depend on the application!

cryptography:
unpredictability $\rightarrow$ high linear complexity

numerical integration (Monte Carlo):
uniform distribution $\rightarrow$ low discrepancy
A pseudorandom number generator is a sequence \((s_n)\) over a finite field \(\mathbb{F}_q\) (or residue class ring \(\mathbb{Z}_m\)). Here we consider only \(\mathbb{F}_p\) with \(p\) prime.

We derive pseudorandom numbers in \(\mathbb{Z}\) or in \([0, 1)\) in the following way:
Identify \(\mathbb{F}_p\) with \(\{0, 1, \ldots, p - 1\}\).

\[x_n = s_n/p \in [0, 1)\]
Part I: Predictability, Linear Complexity, and Lattice Structure
Linear Complexity

The linear complexity $L(s_n)$ of a periodic sequence $(s_n)$ over $\mathbb{F}_p$ is the smallest positive integer $L$ such that there are constants $c_0, \ldots, c_{L-1} \in \mathbb{F}_p$ with

$$s_{n+L} = c_{L-1}s_{n+L-1} + \ldots + c_0s_n, \quad n \geq 0.$$ 

For a positive integer $N$ the $N$th linear complexity $L(s_n, N)$ of a sequence $(s_n)$ over $\mathbb{F}_p$ is the smallest positive integer $L$ such that there are constants $c_0, \ldots, c_{L-1} \in \mathbb{F}_p$ satisfying

$$s_{n+L} = c_{L-1}s_{n+L-1} + \ldots + c_0s_n,$$

$$0 \leq n \leq N - L - 1.$$
Linear Pseudorandom Number Generators

\[ a, b, x_0 \in \mathbb{F}_p, \ a \neq 0 \]

\[ x_{n+1} = ax_n + b, \quad n \geq 0 \]

- predictable \((L(x_n) \leq 2)\)
(Recursive) Nonlinear Pseudorandom Number Generators

\[ f \in \mathbb{F}_p[X], \ 2 \leq \deg(f) \leq p - 1, \ x_0 \in \mathbb{F}_p \]

\[ x_{n+1} = f(x_n), \quad n \geq 0 \]

(purely) periodic with period \( t \leq p \)
Lower Bound on the Linear Complexity Profile

Gutierrez/Shparlinski/W. 2003:
The linear complexity profile of a nonlinear sequence \((x_n)\) defined by

\[ x_{n+1} = f(x_n), \quad n = 0, 1, \ldots, \]

with a polynomial \(f \in \mathbb{F}_p[X]\) of degree \(d \geq 2\), purely periodic with period \(t\), satisfies

\[ L(x_n, N) \geq \min \{ \lceil \log_d (N - \lfloor \log_d N \rfloor) \rceil, \lfloor \log_d t \rfloor \}. \]

Reason for weak result: The degrees in the sequence of iteration of \(f\)

\[ f_0(X) = X, \quad f_{k+1}(X) = f(f_k(X)), \quad k \geq 0 \]

grow exponentially.
\[ \sum_{l=0}^{L} c_l x_{n+l} = 0, \quad 0 \leq n \leq N - L - 1, \quad c_L = -1 \]

\[ F(X) = \sum_{l=0}^{L} c_l f_l(X) \] of degree \( d^L \) has at least \( \min\{N - L, t\} \) zeros.

\[ d^L \geq \min\{N - L, t\} \]
Inversive Generators

\[ a, b, y_0 \in \mathbb{F}_p, \ a \neq 0 \]

\[ y_{n+1} = a y_n^{p-2} + b = \begin{cases} ay_n^{-1} + b, & y_n \neq 0, \\ b, & y_n = 0. \end{cases} \]

Gutierrez/Shparlinski/W. 2003:

\[ L(y_n, N) \geq \min \left\{ \left\lceil \frac{N - 1}{3} \right\rceil, \left\lfloor \frac{t - 1}{2} \right\rfloor \right\} \]

Reason for better result:

\[ f(X) = \frac{bX + a}{X}, \quad f_j(X) = \frac{a_jX + b_j}{c_jX + d} \]

(still predictable and not suitable for cryptography but for MC)
Power Generator

\[ f(X) = X^e \]

Griffin/Shparlinski, 2000:

\[ L(p_n, N) \geq \min \left\{ \frac{N^2}{4(p-1)}, \frac{t^2}{p-1} \right\}, \quad N \geq 1. \]

Reason for better result: \[ f_k(X) = X^{e^k} \mod p-1 \]
Dickson generator

\[ D_e(x + x^{-1}) = x^e + x^{-e}, \quad x \in \mathbb{F}_{p^2} \]

\[ u_{n+1} = D_e(u_n), \quad n \geq 0, \]

with some initial value \( u_0 \) and \( e \geq 2 \).

Aly/W. 2006:

\[ L(u_n, N) \geq \frac{\min\{N^2, 4t^2\}}{16(p + 1)} - (p + 1)^{1/2} \]
Other nice nonlinear generators

Redéi generator, Meidl/W. 2007
multivariate polynomials, Topuzoğlu/W. 2005: nonlinear and
inversive generators of order $m$
polynomial systems, Ostafe/Shparlinski/W. 2010
polynomials with low $p$-weight degree, Ibeas/W. 2010
Marsaglia’s Lattice test, 1972

\( (\eta_n) \) T-periodic sequence over \( \mathbb{F}_p \)

For \( s \geq 1 \) we say that \( (\eta_n) \) passes the \( s \)-dimensional lattice test if the vectors \( \{u_n - u_0 : 1 \leq n < T\} \) span \( \mathbb{F}_p^s \), where

\[
u_n = (\eta_n, \eta_{n+1}, \ldots, \eta_{n+s-1}), \quad 0 \leq n < T.
\]

\[
S(\eta_n) = \max \{ s : \langle u_n - u_0, 1 \leq n < T \rangle = \mathbb{F}_p^s \}
\]
Niederreiter/W. 2002: \( L(\eta_n) = S(\eta_n) \) or \( = S(\eta_n) + 1 \)

Dorfer/W. 2003: Lattice test for parts of the period, \( S(\eta_n, N) \)
We have either

\[
S(\eta_n, N) = \min(L(\eta_n, N), N + 1 - L(\eta_n, N))
\]

or

\[
S(\eta_n, N) = \min(L(\eta_n, N), N + 1 - L(\eta_n, N)) - 1.
\]
Little is known about lattice tests with arbitrary lags, i.e., vectors \((x_{n+d_0}, x_{n+d_1}, \ldots, x_{n+d_{s-1}}) \in \mathbb{F}_p^s\) with \(0 \leq d_0 < d_1 < \ldots < d_{s-1}\).

modified inversive generator, Niederreiter/W. 2007
some explicit nonlinear generators, Pirsic/W. 2010, Chen/Ostafe/W. 2010
Part II: Uniform Distribution and Discrepancy
Discrepancy

\[ \Gamma = \left\{ (\gamma_{n,0}, \ldots, \gamma_{n,s-1})_{n=1}^N \right\} \]

sequence of \( N \) points in the \( s \)-dimensional unit interval \([0, 1)^s\)

\[ \Delta(\Gamma) = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|, \]

where \( T_\Gamma(B) \) is the number of points of \( \Gamma \) inside the box

\[ B = [\alpha_0, \beta_0) \times \cdots \times [\alpha_{s-1}, \beta_{s-1}) \subseteq [0, 1)^s \]

and the supremum is taken over all such boxes.
Erdős-Turan-Koksma inequality (from discrepancy to exponential sums)

\[ \Delta(\Gamma) \leq \left( \frac{3}{2} \right)^s \left( \frac{2}{H+1} + \frac{1}{N} \sum_{0 < |a| \leq H} \prod_{j=0}^{s-1} \frac{1}{\max\{|a_j|, 1\}} \left| \Sigma_N^{(s)}(\Gamma, a) \right| \right), \]

where

\[ \Sigma_N^{(s)}(\Gamma, a) = \sum_{n=1}^{N} \exp \left( 2\pi i \sum_{j=0}^{s-1} a_j \gamma_{n,j} \right) \]

and the outer sum is taken over all integer vectors

\[ a = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s \setminus \{0\} \] with \[ |a| = \max_{j=0,\ldots,s-1} |a_j| \leq H. \]
Nonlinear Pseudorandom Numbers

\[ f \in \mathbb{F}_p[X], \ 2 \leq \deg(f) \leq p - 1, \ x_0 \in \mathbb{F}_p \]

\[ x_{n+1} = f(x_n), \quad n \geq 0 \]

\[ S_N(a) = \sum_{n=0}^{N-1} \psi(ax_n), \quad a \neq 0, \]

where \( \psi(x) = \exp(2\pi ix/p) \) is the additive canonical character of \( \mathbb{F}_p \).
Niederreiter/Shparlinski 1999:

\[ S_N(a) = O \left( N^{1/2} p^{1/2} \log(d)^{1/2} \log(p)^{-1/2} \right), \quad a \neq 0 \]

(improvement, Niederreiter/W. 2008)

Main idea of proof:
Reduction to Weil-bound:

\[ \left| \sum_{x \in \mathbb{F}_p} \psi(F(x)) \right| \leq (\deg(F) - 1)p^{1/2} \]

Here:

\[ F(X) = \sum a_i f_{k_i}(X) \]

Exponential degree growth when iterating \( f(X) \) is the reason for the weakness of these bounds. (Cf. linear complexity bounds.)
Improvements for Special Nonlinear Generators

inversive generators: Niederreiter/Shparlinski 2001

\[ D_N = O(N^{-1/2} p^{1/4} \log^s(p)) \]

power generator: Friedlander/Shparlinski 2001
Dickson generator: Gomez/Gutierrez/Shparlinski 2006
Redéi generator: Gutierrez/W. 2007
polynomial systems: Ostafe/Shparlinski since 2009
low \( p \)-weight degree: Ibeas/W. 2010
under construction
Linz opera house will open 2013
Thank you for your attention.