Transitive piecewise polynomial transformations over primary residue rings and some statistical properties of the generated sequences

Vasin Anton,
Lipina Tatiana

JSC «Aktiv-Soft»

Iteration of polynomial transformations

Applications:

- nonlinear arithmetic pseudorandom sequence generators;
- nonlinear components and blocks in stream ciphers (e.g., Achterbahn, Bleep64, Fountain, Grain, Trivium);
- polynomial-based blocks in cipher systems (e.g., the WG family, AEAD-cipher WAGE).

Desirable properties of output sequences:

- large **periods** and ranks (combinatorial-algebraic approach);
- high algorithmic complexity (algorithmic approach);
- indistinguishability from an ideal random sequence by a polynomial probabilistic algorithm (computational complexity approach);
- good **statistical properties** (statistical approach).

Transitive polynomial transformations

Maximal period T of a polynomial generator:

- over a finite field $GF(q)$: $T = q$;
- over a residue ring $\mathbb{Z}_{p^n}$: $T = p^n$ (Anashin V.S., Larin M.V.);
- over other Galois rings $GR(q^n, p^n)$ (Anashin V.S., Ermilov D.M., Kozlitin O.A., Larin M.V.):

$$T = q(q-1)p^{n-2} < q^n = |R|.$$

Piecewise polynomial functions over Galois rings

- Let R be a Galois ring $GR(q^n, p^n)$;
- for $x = p^l\hat{x}$, where $\hat{x} \in R^*$, $0 \le l \le n$, $F(x) = f_0 + f_1 x + \ldots + f_d x^d \in R[x]$ define

$$\phi_F(x) = \phi_F(p^l\hat{x}) = f_0 + p^l(f_1\hat{x} + \ldots + f_d\hat{x}^d).$$

- $x_0, x_1 = \phi_F(x_0), \ldots, x_{m+1} = \phi_F(x_m), \ldots, x_0 \in R$, — piecewise polynomial sequence;
- for $x' \in pR$ define the set $\mathrm{Orb}(x') = \{x', \phi_F(x'), \ldots, \phi_F^{q-1}(x')\}$,
- consider the sequence $x_0 = 0, x_1 = \phi_F(x_0), \ldots, x_{m+1} = \phi_F(x_m), \ldots$, let $\mathcal{B}(\phi_F) = \overline{x_{q-1}} + pR$.

Piecewise polynomial functions over Galois rings

Let ϕ_F be a permutation over R, $\bar{\phi}_F$ — full-cycle permutation over $GF(q)$, π — full-cycle permutation over pR, $x \in \mathrm{Orb}(x')$. Define the function $\Phi_{F,\pi} \colon R \to R$ as:

$$\Phi_{F,\pi}(x) = \begin{cases} \phi_F(x), \text{ если } x \notin \mathcal{B}(\phi_F); \\ \pi(x'), \text{ если } x \in \mathcal{B}(\phi_F). \end{cases}$$

The period of a sequence, generated by the function $\Phi_{F,\pi}$, equals $|R|$.
Question: in what cases can we set $\pi(x') = \phi_F(x)$, $x \in \mathrm{Orb}(x')$, that is $\Phi_{F,\pi}(x) = \phi_F(x)$?

Transitivity of piecewise polynomial functions

In what cases is the function ϕ_F a full-cycle permutation over R?

- Let $R = \mathbb{Z}_{2^n}$;
- $\phi(2^l \hat{x}) = 2^l a \hat{x}^{e-1} + b$ is a piecewise inversive function, where e is the exponent of R;
- $\{\phi^i(x_0)\}_{i=0}^{\infty}$, $x_0 \in R$, — piecewise inversive sequence.

Theorem (J. Eichenauer-Herrmann, H. Grothe)

A piecewise inversive sequence over $\mathbb{Z}_{2^n}$ has period 2^n iff $a \equiv_4 1$ u $b \equiv_2 1$.

Transitivity of piecewise polynomial functions

Let

$$d' = \begin{cases} d, & d \equiv 1 \mod 2, \\ d-1, & d \equiv 0 \mod 2. \end{cases}$$

Theorem

A piecewise polynomial function ϕ_F is transitive over $\mathbb{Z}_{2^n}$ for any $n \geq 1$ iff the following relations hold:

1. $f_0 \equiv 1 \mod 2$;
2. $f_1 + f_3 + \ldots + f_{d'} \equiv 1 \mod 4$;
3. $f_2 + f_4 + \ldots + f_{2\lfloor \frac{d}{2} \rfloor} \equiv 0 \mod 4$.

Piecewise power functions

Corollary

A piecewise power function $\phi_F(2^l\hat{x}) = 2^l a\hat{x}^d + b$ *is transitive over* $\mathbb{Z}_{2^n}$ *for any* $n \geq 1$ *iff* d *is odd,* $a \equiv_4 1$, $b \equiv_2 1$.

Theorem (M.V. Larin)

A polynomial $F(x) = \sum_{k\geq 0} f_k x^k \in \mathbb{Z}[x]$ *is transitive modulo* 2^n *for any* $n \geq 1$ *iff the following relations hold:*

1. $f_3 + f_5 + \ldots \equiv_4 2f_2$;
2. $f_4 + f_6 + \ldots \equiv_4 f_1 + f_2 - 1$;
3. $f_1 \equiv_2 1$;
4. $f_0 \equiv_2 1$.

In particular, $f_1 \equiv_2 1$, therefore, full-cycle binomials can only be of the first degree.

Discrepancy

Definition

The discrepancy D_l of a segment $x_0, \ldots, x_{l-1}$ of a sequence $\{x_i\}_{i=0}^{\infty} \in [0,1)^{\infty}$ is defined by

$$D_l(x_0, \ldots, x_{l-1}) = \sup_{0<\alpha\leq 1} \left| \frac{N([0,\alpha), l)}{l} - \alpha \right|,$$

where $N([0,\alpha), l) = |\{x_n \in [0,\alpha) \mid 0 \leq n \leq l-1\}|$.

For a sequence of i.i.d. random variables uniformly distributed on $[0,1)$, as $l \to \infty$ we have

$$D_l = O(l^{-1/2}(\log\log l)^{1/2}).$$

Discrepancy of piecewise polynomial sequences

- $R = \mathbb{Z}_q$, $q = p^n$, $p > 2$;
- $\{x_i\}_{i=0}^{\infty}$ — piecewise polynomial sequence of period q over R;
- $P = \left\{ \frac{x_i}{q} \right\}_{i=0}^{\infty}$;
- $V(R) = \frac{4}{\pi^2} n \ln p + \frac{4}{5}$.

Theorem

Let ϕ_F be a transitive piecewise polynomial function over R, and $d \geq 2$, $(d, p) = 1$. Then for l, such that $1 \leq l \leq q$, we have

$$D_l(P) < \frac{1}{q} + 3V(R) p^{-\frac{1}{2s}} l^{-\frac{1}{2}} q^{\frac{1}{2}},$$

where $s = d^{\sqrt{\frac{3}{2}p+1}}$.

Comparison of the asymptotics of estimates

- piecewise polynomial sequence over $\mathbb{Z}_q$ as $q \to \infty$, $p, d, l = O(q)$:

$$D_l = O(l^{-1/2} q^{1/2} p^{-\frac{1}{2s}} \log q), \ s = d^{\sqrt{\frac{3}{2}p+1}};$$

- polynomial generator over $\mathbb{Z}_q$ as $q \to \infty$, $l = O(q)$ (E. El-Mahassni, A. Winterhof):

$$D_l = O(l^{-1/2} q^{1/2} \log\log\log q \cdot (\log\log q)^{-1/2});$$

- polynomial generator over $GF(p)$ as $p \to \infty$, $l = O(p)$ (H. Niederreiter, I.E. Shparlinski):

$$D_l = O(l^{-1/2} p^{1/2} \log\log p \cdot \log^{-1/2} p).$$

Autocorrelation coefficients

Definition

Autocorrelation coefficients of a sequence $\{x_i\}_{i=0}^{\infty}$, *where* $x_i = \phi_F^i(x_0)$, $x_0 \in R$, *are complex numbers, defined as*

$$A_{\phi_F}(l, s, g) = \sum_{i=0}^{l-1} e^{2\pi i \frac{g(x_i - x_{i+s})}{q}}.$$

The smaller the value of $|A_{\phi_F}(l, s, g)|$, the more «uncorrelated» segments

$$(x_0, \ldots, x_{l-1}) \text{ and } (x_s, \ldots, x_{l+s-1})$$

are between each other.

Autocorrelation coefficients of piecewise polynomial sequences

Theorem

Let ϕ_F be a transitive piecewise polynomial function over R, and $d \geq 2$, $(d,p) = 1$. Then for $h = \frac{q}{(q,g)}$ we have

$$|A_{\phi_F}(q,s,g)| < 4,41h^{-\frac{1}{d^s}}q + 2sp^{-1}q.$$

This estimate is nontrivial for small values of the shift $s < \frac{p}{2}$ and the generating polynomial degree d: $d^s < \frac{1}{\log_h 4,41}$.

Thank you for your attention!