On upper bounds for periods of PCG sequences over Galois rings

Ermilov D.M.

TVP Laboratories

Polynomial congruential generator

(PCG) over the ring R is a machine with the states sequence $\{x_i\}$, $i = 0, 1, \ldots$. The elements x_i are defined by conditions:

$$x_{i+1} = f(x_i),$$

where $x_0 \in R$, and $f(x) \in R[x]$.

Let R be **Galois ring** of cardinality q^n and characteristic p^n, $R = GR(q^n, p^n)$, $q = p^m$. There is an isomorphism $R \cong \mathbb{Z}_{p^n}[x]/f(x)$, $\deg(f) = m$, f – Galois Polynom.

There is no **full cycle** polynomial transformation over Galois ring $R = GR(q^n, p^n)$, $q \neq p$ and $n > 1$.

PCG sequence over R achieve the **largest period** $q(q-1)p^{n-2}$.

The **linear congruential generator (LCG)** over R is a PCG with the states sequence $\{x_i\}$ of elements defined by relation $x_{i+1} = ax_i + b$, $a, b \in R$.

LCG sequence over $\mathbb{Z}_m$ achieve the largest period m.

What is the largest period of the LCG sequence over R?

Let $G_{f,R}$ be the graph of bijective transformation of the ring R assigned by polynomial $f(x) \in R[x]$.

Statement 1.

The length of cycle in graph $G_{ax+b,R}$, $ax + b \in R[x]$ is at most $(q-1)p^{n-1}$.

By definition $J = pR$ and $R_i = R/J^i$, $i \in \overline{1,n}$ ($R_1 \cong GF(q)$).

Theorem 1. ($p \neq 2$)

There is a cycle of length $(q-1)p^{n-1}$ in the graph $G_{ax+b,R}$, $p \neq 2$ iff

1. $a \equiv a_0 \pmod{J}$, where a_0 is a *primitive element* of the field R_1;
2. $a \in R \setminus \Gamma(R)$, where $\Gamma(R) = \{r \in R | \, r^q = r\}$.

Theorem 2. ($p = 2$)

There is a cycle of length $(2^m-1)2^{n-1}$ in the graph $G_{ax+b,R}$, $p = 2$ iff

1. $a \equiv a_0 \pmod{J}$, where a_0 – *primitive element* of the field R_1;
2. $a \in R \setminus \Gamma(R)$;
3. $a^{2^m-1}r + b(1 + a + \cdots + a^{2^m-2}) \not\equiv 3e \pmod{J^2}$, $r \in R$.

Consider the Galois ring $R = GR(2^{3*3}, 2^3) = \mathbb{Z}_8[y]_{/y^3+y+1}$.
Consider the polynomial $f(x) \in R[x]$:

$$f(x) = (4, 3, 3)x + (1, 1, 2).$$

The cyclic structure of $G_{f,R}$ is equals $[14^{32}, 7^8, 1^1]$ and the bound from the theorem 2 is not achieved.

Quadratic congruential generator

The **quadratic congruential generator (QCG)** over R is a PCG with the states sequence $\{x_i\}$ of elements defined by relation $x_{i+1} = ax_i^2 + bx_i + c$, a, b and $c \in R$.

Statement 2.

Let $f(x) = ax^2 + bx + c \in R[x]$ be a bijective polynom over R. The length of cycle in graph $G_{f(x),R}$ is at most $(q-1)p^{n-1}$.