Congruential generators on pseudorandom numbers

Tran The Vinh and Pavel Varbanets

I. I. Mechnikov Odessa National University, Ukraine varb@sana.od.ua

Let p be a prime number, $m > 1$ be a positive integer. Consider the following recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{p^m}, (a, b \in \mathbb{Z}), \tag{1}$$

where $\overline{y}_n$ is a multiplicative inversive modulo p^m for y_n if $(y_n, p) = 1$. The parameters a, b, y_0 we called the multiplier, shift and initial value, respectively.

In the works of Eichenauer, Lehn, Topuzoğlu, Niederreiter, Shparlinski, Grothe, Emmerih ets were proved that the inversive congruential generator (1) produces the sequence $\{x_n\}$, $x_n = y_n/p^m$, $n = 0, 1, 2, \ldots$, which passes s-dimensional serial tests on equidistribution and statistical independence for $s = 1, 2, 3, 4$ if the defined conditions on relative parameters a, b, y_0 are accomplishable.

It was proved that this generator is extremely useful for Quasi-Monte Carlo type application. The sequences of PRN's can be used for the cryptographic applications. Now the initial value y_0 and the constants a and b are assumed to be secret key, and then we use the output of the generator (1) as a stream cipher.

In our talk we consider two generalizations of the generator (1):

$$y_{n+1} \equiv a\overline{y}_n + b + cy_0 \pmod{p^m}, \tag{2}$$

where $m \geq 3$ be positive integer; $a, b, c \in \mathbb{Z}_{p^m}$, $(a, p) = 1$, $b \equiv c \equiv 0 \pmod{p}$.

That generator we call the linear-inversive generator.

The following type of generator over the sequence of pseudorandom numbers connect with the norm units in the ring of residues modulo p^n over $\mathbb{Z}[i]$.

Let $u + iv \in \mathbb{Z}[i]$ be the generated element of the cyclic group

$$E_\ell := \{\omega \in \mathbb{Z}[i] \mid (\omega, p) = 1,\ N(\omega) \equiv \pm 1 \pmod{p^m}\},\ \ell = 1, \ldots, m.$$

We have

$$\#E_\ell = \begin{cases} 2(p+1)p^{\ell-1} & if \quad p \equiv 3 \pmod 4, \\ 2(p-1)p^{\ell-1} & if \quad p \equiv 1 \pmod 4. \end{cases}$$

We define the congruential generator

$$z_n \equiv \Im(u+iv)^n \cdot (\Re(u+iv)^n)^{-1} \pmod{p^m},\ n = 0, 1, 2, \ldots.$$

The main goal of our investigation is the construction of representations of y_n (or z_n) as the polynomials on initial value y_0 (or $u_0 + iv_0$) and number n. Using these representations we study the special exponential sums on the sequences of pseudorandom numbers $\{y_n\}$ (or $\{z_n\}$)

$$S = \sum_{n=0}^{N-1} e^{2\pi i h x_n / p^m} \ for\ x_n = y_n\ or\ x_n = z_n,\ h \in \mathbb{Z}$$

and then prove that the sequence $\{y_n/p^m\}$ ($\{z_n/p^m\}$) satisfies by requirements of equidistribution and unpredictability.

Our results generalize the investigations provided by Eichenauer, Niederreiter, Shparlinskii, S. Varbanets etc.