OP&PM SURVEYS
ON APPLIED AND INDUSTRIAL
Volume 25 MATHEMATICS Issue 1
2018

III INTERNATIONAL BALTIC SYMPOSIUM ON APPLIED AND INDUSTRIAL MATHEMATICS

N. M. Mezhennaya, **V. G. Mikhailov** (Moscow, Bauman Moscow State Technical University, Steklov Mathematical Institute of Russian Academy of Sciences). **Limit theorem for number of ones in extended Pohl generator outcome sequence.**

We consider the generator consisted of r cyclic shift registers without feedback with coprime lengths $m_1,\dots,m_r$ under residue ring modulo 2. Let $(x_0^{(j)},x_1^{(j)},\dots,x_{m_j-1}^{(j)})$, $j=1,2,\dots,r$, be the vectors of registers cells fillings. Elements of generator outcome sequence are formed by the formula

$$z_t = f\bigl(x^{(1)}_{t(m_1)}, x^{(2)}_{t(m_2)},\dots,x^{(r)}_{t(m_r)}\bigr),\quad t=0,1,2,\dots, \tag{1}$$

where f is a Boolean function of r variables and $t(m)=t \mod m$.

If $f(y_1,y_2,\dots,y_r)=y_1\oplus y_2\oplus\ldots\oplus y_r$, where $\oplus$ is the operation of addition modulo 2 (XOR), the generator was considered in [1] and is called *Pohl generator*. The generator of the form (1) with arbitrary Boolean function f essentially depending on its all r arguments we designate as *extended* Pohl generator.

The generator outcome sequence is purely periodical and has the period (possibly not minimal) of length $L=m_1m_2\cdots m_r$. So when the properties of the number of ones is investigated we consider the segment $(z_0,z_1,\dots,z_{L-1})$, which is called *cycle* of outcome sequence.

Let ξ be the number of ones in the cycle of outcome sequence of generator (1). We use the notations $W_f(u)$, $u\in\{0,1\}^r$, for Walsh–Hadamard transform of function f in point u and $wt(f)$ for weight of function f (see [2]). Let $u_{(j)}\in\{0,1\}^r$ be the vector in which the jth element is one and the remaining elements are zeros.

Theorem. *Let extended Pohl generator with coprime registers lengths $m_1<\cdots<m_r$ be given by Boolean function f, the numbers $x_k^{(j)}$, $k=0,1,\dots,m_j-1$, $j=1,2,\dots,r$, be random, mutually independent and uniformly distributed on the set $\{0,1\}$.*

If $m_1,m_2,\dots,m_r\to\infty$ in such a way that

$$\bigl(W_f(u_{(1)})+W_f(u_{(2)})+\cdots+W_f(u_{(r)})\bigr)^2>0,$$

then the random variable

$$\left(\sum_{j=1}^{r}\frac{1}{4\,m_j}\bigl(W_f(u_{(j)})\bigr)^2\right)^{-1/2}\left(\frac{2^r\xi}{m_1m_2\cdots m_r}-w\,t(f)\right)$$

has standard normal limiting distribution.

Remark 1. If $m_1/m_j\to\rho_j^2\in[0,1]$, $j=1,2,\dots,r$, conclusion of the theorem equivalent to the statement that the random variable

$$\sqrt{m_1}\left(\frac{2^r\xi}{m_1m_2\cdots m_r}-w\,t(f)\right)$$

has (in limit) normal distribution with zero mean and variance

$$\frac{1}{4}\sum_{j=1}^{r}\rho_j^2\left(W_f(u_{(j)})\right)^2>0.$$

Remark 2. It can be shown that if conditions of the theorem are fulfilled for function f, then these conditions are also fulfilled for function $f\oplus 1$.

Remark 3. Asymptotic properties of the distribution of the number of ones in outcome sequence of ordinary Pohl generator are significantly different from those which are described above. The conditions of our theorem can not be fulfilled for ordinary Pohl generator with equiprobable registers fillings. In this case ξ (under appropriate standardization) has the limiting distribution which is equal to the distribution of the product of r independent standard normally distributed random variables (see [3]). In [4] it was shown that normal distribution is a limiting distribution for ξ when Pohl generator registers are filled with segments of un-equiprobable Bernoulli sequence.

REFERENCES

1. *Pohl P.* Description of MCV, a pseudo-random number generator. — Scand. Actuar. J., 1976, №1, p. 1–14.
2. *Logachev O. A.*, *Sal'nikov A. A.*, *Smyshlyaev S. V.*, *Yashchenko V. V.* Bulevy funkcii v teorii kodirovaniya i kriptologii [Boolean functions in the theory of coding and cryptology]. M.: MTsNMO, 2004, 470 p. (In Russian.)
3. *Mezhennaya N. M.*, *Mikhailov V. G.* On the distribution of the number of ones in the output sequence of the MCV-generator over $GF(2)$. — Math. Aspects Cryptogr., 2013, v. 4, № 4, p. 95–107. (in Russian.)
4. *Mezhennaya N. M.* On distribution of number of ones in binary multicycle sequence. — Appl. Discr. Math., 2015, №1(27), p. 69–77.