S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

*Том 11, стр. 18–25 (2014)* УДК 519.214
MSC 60F05

# CONVERGENCE RATE ESTIMATORS FOR THE NUMBER OF ONES IN OUTCOME SEQUENCE OF MCV GENERATOR WITH $m$-DEPENDENT REGISTERS ITEMS

N.M. MEZHENNAYA

Abstract. This paper is focused on studying properties of the number of ones $\xi_r$ in outcome sequence of MCV generator with $r$ registers over $GF(2)$. We concern on the case when generator outcome sequence has length close to the cycle length and registers filled with $m$-dependent binary random variables. Exact expressions for mean and variance of $\xi_r$ are given. We derive estimate in uniform metric between cumulative distribution functions of the standardized number of ones in MCV generator outcome sequence and product of $r$ independent standard normal random variables. The estimate allows to prove limit theorem for $\xi_r$ when number $r$ is fixed. We also estimate distance (in uniform metric) between the cumulative distribution function of normalized $\xi_r$ and log-normal distribution law. This result allows to prove a normal-type limit theorem for $r \to \infty$.

**Keywords:** MCV generator, normal-type limit theorem, uniform distance estimate, m-dependent random variables.

## 1. Introduction

MCV generator ([1]) consists of $r$ shift registers with relatively prime lengths $m_1, \ldots, m_r$ over residue ring modulo $M$. Let $(X_0^{(i)}, \ldots, X_{m_i-1}^{(i)})$ be the $i$-th register fill, $i = 1, \ldots, r$. Outcome sequence of the generator is constructed by rule

$$Z_t = X_{t(m_1)}^{(1)} + \ldots + X_{t(m_r)}^{(r)} \bmod M,\ t = 0, 1, 2, \ldots, \tag{1}$$

Mezhennaya, N.M., Convergence rate estimators for the number of ones in outcome sequence of MCV generator with $m$-dependent registers items.

The work is supported by RFBR (grant 14-01-00318A).
*Received November, 18, 2013, published January, 30, 2014.*

there $t(n) = t \bmod n$. Sequence $\{Z_t\}$ is repeating with period length $T = m_1 \dots m_r$.

Let items $(X_0^{(i)}, \dots, X_{m_i-1}^{(i)})$ in $i$-th register be independent random variables with values in the set $A_M = \{0, 1, \dots, M-1\}$, $i = 1, \dots, r$,. It was shown [1] that MCV generator outcome sequence with length order less than $T$ (about $\sqrt{T}$ and less) has properties common to the equiprobable random sequences when registers filled with equiprobable random variables. For the sequence with length close to $T$ this is not true.

Normal-type limit theorems for the number of ones in MCV generator outcome sequence were deduced in paper [2]. These results show that MCV generator outcome sequence with length equal to the period length $T$ significantly differs from the equiprobable random sequence. In this paper we show that this property holds true then items in registers are finitely dependent.

## 2. Main results

In present paper we consider the MCV generator with registers filled with $m$-dependent binary random variables ([3], chapter XIX). Let $X_0^{(i)}, \dots, X_{m_i-1}^{(i)}$ be binary random variables such that

$$\mathbf{P}\{X_j^{(i)} = 1\} = 1/2,\ j = 0, 1, \dots, m_i. \tag{2}$$

Suppose that the random variables $X_0^{(i)}, \dots, X_{m_i-1}^{(i)}$ are circle-wise $m$-dependent, i. e. for any $a, b, p, q \in \mathbb{Z}$, $a < b$, random vectors $(X_{(a-p)(m_i)}^{(i)}, \dots, X_{a(m_i)}^{(i)})$ and $(X_{b(m_i)}^{(i)}, \dots, X_{(b+q)(m_i)}^{(i)})$ are independent when $(b-a) \bmod m_i > m$ and $(a-b-q-p) \bmod m_i > m$. It is reasonable to suppose that $m < \min\{m_1, \dots, m_r\} - 1$.

Let random vectors $X^{(1)}, \dots, X^{(r)}$ be mutually independent.

We consider MCV generator with outcome sequence (1). We denote by $\xi_r$ the number of ones in sequence (1) with length $T = m_1 \dots m_r$. Let $S_i$ be the number of ones in vector $X^{(i)}, i = 1, \dots, r$. It was shown in [2] that

$$m_1 \dots m_r - 2\xi_r = (m_1 - 2S_1) \dots (m_r - 2S_r) \tag{3}$$

Equality (3) implies that the distribution of random variable $m_1 \dots m_r - 2\xi_r$ coincides with the distribution of product of $r$ centered independent random variables (compare with [2], theorem 1).

**Theorem 1.** *Suppose the random vectors $X^{(i)}, i = 1, \dots, r,\ r \geqslant 2$, are mutually independent, for every $i = 1, \dots, r$ $X_0^{(i)}, \dots, X_{m_i-1}^{(i)}$ are circle-wise $m$-dependent binary random variables which satisfy (2), $m < \min\{m_1, \dots, m_r\} - 1$. Then*

$$\mathbf{E}\xi_r = \frac{m_1 \dots m_r}{2}, \tag{4}$$

$$\mathbf{D}\xi_r = 4^{r-1} \prod_{i=1}^{r} \left( m_i \left( \frac{1}{4} - \frac{m}{2} \right) + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} \mathbf{P}\{X_{j_1}^{(i)} = X_{(j_1+k) \bmod m_i}^{(i)} = 1\} \right). \tag{5}$$

Remark 1. If random variables in the sets $X^{(i)}, i = 1, \dots, r$, are pairwise independent then formula (5) coincides with the analogous formula in paper [2].

If for all $i$ distributios of the random variables $X_0^{(i)}, X_1^{(i)}, \dots, X_{m_i-1}^{(i)}$ is cycle shift invariant then instead of (5) we can write

$$\mathbf{D}\xi_r = 4^{r-1}\prod_{i=1}^{r} m_i\sigma_i,$$

$$\sigma_i = m_i\left(\frac{1}{4} + 2\sum_{k=1}^{m}\mathbf{P}\{X_0^{(i)} = X_k^{(i)} = 1\} - \frac{m}{2}\right),\ i = 1, \dots, r.$$

We suppose that $\tilde{\xi}_r = \left(\frac{m_1\dots m_r}{2} - \xi_r\right)(\mathbf{D}\xi_r)^{-1/2}$. Let us denote by $F_X$ the cumulative distribution function of random variable $X$, $\Phi$ the cumulative distribution function of standard normal law, $\Phi_r$ the cumulative distribution function of product of $r$ independent standard normal random variables. Let

$$d(U, V) = \sup_{x\in\mathbb{R}} |U(x) - V(x)|$$

be the distance in uniform metric between the cumulative distribution functions $U$ and $V$ on real line.

**Theorem 2.** *Let hypothesis of theorem* 1 *be held. Suppose the numbers $m_1, \dots, m_r$ are relatively prime odd numbers, the distribution of random variables $X_0^{(i)}$, $X_1^{(i)}, \dots, X_{m_i-1}^{(i)}$ is cycle shift invariant for any $i$. Then*

$$d(F_{\tilde{\xi}_r}, \Phi_r) \leqslant C(2m+1)^2\sum_{j=1}^{r}\frac{1}{\sqrt{m_j}\sigma_j^{3/2}}, \tag{6}$$

*where $C = 32(1+\sqrt{6}) \leq 110,4$.*

Remark 2. The order of estimate (6) for $m = const$ is the same as order of estimate for $m = 0$ derived in theorem 2 of paper [2].

**Corollary 1.** *Let hypothesis of theorem* 2 *be held. If number $r$ is fixed, $m_1, \dots, m_r \to \infty$ and parameter $m$ varies in a such way that $\frac{m^2}{\min\limits_{1\leq j\leq r}\{\sqrt{m_j}\}} \to 0$ then for any $x \in \mathbb{R}$*

$$F_{\tilde{\xi}_r}(x) \to \Phi_r(x).$$

We assume that

$$a = \frac{2}{\sqrt{2\pi}}\int_0^{+\infty}\ln x\, e^{-x^2/2}dx \approx -0,6352, \tag{7}$$

$$b = \frac{2}{\sqrt{2\pi}}\int_0^{+\infty}\ln^2 x\, e^{-x^2/2}dx \approx 1,6372, \tag{8}$$

$$c = \frac{2}{\sqrt{2\pi}}\int_0^{+\infty}|\ln x - a|^3 e^{-x^2/2}dx \approx 2,9607, \tag{9}$$

$$\sigma^2 = b - a^2 \approx 1,2337. \tag{10}$$

It is clear from (7)-(10) that if random variable $\eta$ has standard normal law then $a = \mathbf{E}\ln|\eta|$, $\sigma^2 = \mathbf{D}\ln|\eta|$, $c = \mathbf{E}|\ln|\eta| - a|^3$.

We also set

$$\tilde{\zeta}_r = e^{-\frac{a}{\sigma}\sqrt{r}}\left|\tilde{\xi}_r\right|^{\frac{1}{\sigma\sqrt{r}}},$$

$$\Upsilon(x) = \frac{1}{\sqrt{2\pi}}\int\limits_0^x \frac{1}{y}e^{-\ln^2 y/2}dy.$$

As it seen from the last definition $\Upsilon(x)$ is the cumulative distribution function of standard log-normal law.

**Theorem 3.** *Let hypothesis of theorem* 2 *be held. Then*

$$d\left(F_{\tilde{\zeta}_r}, \Upsilon\right) \leq 2C(2m+1)^2\sum_{j=1}^{r}\frac{1}{\sqrt{m_j}\sigma_j^{3/2}} + C_{BE}\frac{c}{\sigma^3\sqrt{r}}, \tag{11}$$

*where $C_{BE}$ is a constant from Berry—Esseen inequality for identically distributed summands.*

Remark 3. In paper [4] it was shown that $C_{BE} \leq 0,48$.

**Corollary 2.** *Let hypothesis of theorem* 2 *be held. Then for any $x \in \mathbb{R}$*

$$\left|F_{\tilde{\xi}_r}(x) - \frac{1}{2}\left(1 + sign(x)\Phi\left(\frac{\ln|x|}{\sigma\sqrt{r}} - \frac{a}{\sigma}\sqrt{r}\right)\right)\right| \leqslant$$

$$\leqslant C(2m+1)^2\sum_{j=1}^{r}\frac{1}{\sqrt{m_j}\sigma_j^{3/2}} + C_{BE}\frac{c}{2\sigma^3\sqrt{r}}.$$

**Corollary 3.** *Let hypothesis of theorem* 2 *be held. If $r, m_1, \ldots, m_r \to \infty$ such that $m^2\sum\limits_{j=1}^{r} m_j^{-1/2} \to 0$ then for any $\frac{1}{2} < \alpha < 1$*

$$\mathbf{P}\left\{\xi_r < \frac{m_1\ldots m_r}{2} + e^{ar+u_{2\alpha-1}\sigma\sqrt{r}}\prod_{i=1}^{r} m_i\sigma_i\right\} \to \alpha,$$

$$\mathbf{P}\left\{\xi_r < \frac{m_1\ldots m_r}{2} - e^{ar+u_{2\alpha-1}\sigma\sqrt{r}}\prod_{i=1}^{r} m_i\sigma_i\right\} \to 1-\alpha,$$

*where $u_{2\alpha-1}$ is $(2\alpha-1)$-quantile of standard normal law.*

## 3. Proofs

Proof of theorem 1. We first calculate mean of the random variable $\xi_r$. Since $S_i = \sum\limits_{j=0}^{m_i-1} X_j^{(i)}$ and all random variables $X_0^{(i)}, \ldots, X_{m_i-1}^{(i)}$ have the same one-dimensional distribution laws equation (2) implies

$$\mathbf{E}S_i = \sum_{j=0}^{m_i-1}\mathbf{E}X_j^{(i)} = m_i\mathbf{E}X_1^{(i)} = m_i\mathbf{P}\{X_1^{(i)} = 1\} = \frac{m_i}{2}.$$

Applying expectation operator to (3) and using independence of random vectors $X^{(i)} = (X_0^{(i)}, \ldots, X_{m_i-1}^{(i)}), i = 1, \ldots, r$, we derive that

$$\mathbf{E}(m_1\ldots m_r - 2\xi_r) = \mathbf{E}(m_1 - 2S_1)\ldots\mathbf{E}(m_r - 2S_r) = 0.$$

This involves formula (4).

Now we compute the variance

$$\mathbf{D}S_i = \mathbf{D}\left(\sum_{j=0}^{m_i-1} X_j^{(i)}\right) = \sum_{j=0}^{m_i-1} \mathbf{D}X_j^{(i)} + 2 \sum_{0\leqslant j_1<j_2\leqslant m_i-1} \operatorname{cov}(X_{j_1}^{(i)}, X_{j_2}^{(i)}) =$$

$$= m_i \mathbf{D}X_1^{(i)} + 2 \sum_{0\leqslant j_1<j_2\leqslant m_i-1} \left(\mathbf{E}X_{j_1}^{(i)}X_{j_2}^{(i)} - \mathbf{E}X_{j_1}^{(i)}\mathbf{E}X_{j_2}^{(i)}\right) =$$

$$= \frac{m_i}{4} + 2 \sum_{\substack{0\leqslant j_1\leqslant m_i-1,\\ 0<j_2-j_1\leqslant m}} \left(\mathbf{P}\{X_{j_1}^{(i)} = X_{j_2}^{(i)} = 1\} - \frac{1}{4}\right) =$$

$$= \frac{m_i}{4} + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} \left(\mathbf{P}\{X_{j_1}^{(i)} = X_{(j_1+k) mod\, m_i}^{(i)} = 1\} - \frac{1}{4}\right) =$$

$$= m_i \left(\frac{1}{4} - \frac{m}{2}\right) + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} \mathbf{P}\{X_{j_1}^{(i)} = X_{(j_1+k) mod\, m_i}^{(i)} = 1\}. \tag{12}$$

From (4) and (12) we develop

$$\mathbf{D}\xi_r = \mathbf{E}\Big(\xi_r - \frac{m_1 \dots m_r}{2}\Big)^2 = \frac{1}{4}\mathbf{E}(2\xi_r - m_1 \dots m_r)^2 =$$

$$= \frac{1}{4}\mathbf{E}(m_1 - 2S_1)^2 \dots \mathbf{E}(m_r - 2S_r)^2 =$$

$$= 4^{r-1}\mathbf{D}S_1 \dots \mathbf{D}S_r =$$

$$= 4^{r-1} \prod_{i=1}^{r} \left(m_i \left(\frac{1}{4} - \frac{m}{2}\right) + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} \mathbf{P}\{X_{j_1}^{(i)} = X_{(j_1+k) mod\, m_i}^{(i)} = 1\}\right).$$

The theorem is proved.

Proof of theorem 2. Denote

$$\tilde{S}_i = (\mathbf{D}S_i)^{-1/2}(S_i - \mathbf{E}S_i) = \frac{S_i - \frac{m_i}{2}}{\sqrt{m_i\sigma_i}}.$$

It follows from (3) that

$$\frac{m_1 \dots m_r}{2} - \xi_r = 2^{r-1} \prod_{i=1}^{r} \Big(\frac{m_i}{2} - S_i\Big).$$

Substituting (5) into the last formula we obtain that

$$\tilde{\xi}_r = (\mathbf{D}\xi_r)^{-1/2} \left(\frac{m_1 \dots m_r}{2} - \xi_r\right) = \frac{2^{r-1} \prod\limits_{i=1}^{r} \left(\frac{m_i}{2} - S_i\right)}{2^{r-1} \prod\limits_{i=1}^{r} \sqrt{m_i\sigma_i}} =$$

$$= \prod_{i=1}^{r} \frac{\frac{m_i}{2} - S_i}{\sqrt{m_i\sigma_i}} = \prod_{i=1}^{r} \tilde{S}_i. \tag{13}$$

We set $\zeta_r = \ln|\xi_r|$, $\varsigma_j = \ln|\tilde{S}_j|$, $j = 1, \dots, r$. Then (13) implies

$$\zeta_r = \sum_{j=1}^{r} \varsigma_j. \tag{14}$$

Since the random variables $\varsigma_1, \ldots, \varsigma_r$ are independent we find out

$$F_{\zeta_r} = F_{\varsigma_1} * \ldots * F_{\varsigma_r},$$

where sign $*$ is used to designate convolution.

Suppose that random variables $\eta_1, \ldots, \eta_r$ are independent and each has standard normal distribution law,

$$\delta_i = \ln|\eta_i|,\ i = 1, \ldots, r. \tag{15}$$

From the last definitions and formula (14) we derive estimate

$$d\left(F_{\zeta_r}, F_{\sum\limits_{j=1}^{r}\delta_j}\right) = d\left(F_{\varsigma_1} * \ldots * F_{\varsigma_r}, F_{\delta_1} * \ldots * F_{\delta_r}\right) \leqslant$$

$$\leqslant d\left(F_{\varsigma_1} * \ldots * F_{\varsigma_r}, F_{\delta_1} * F_{\varsigma_2} * \ldots * F_{\varsigma_r}\right) + d\left(F_{\delta_1} * F_{\varsigma_2} * \ldots * F_{\varsigma_r}, F_{\delta_1} * \ldots * F_{\delta_r}\right).$$

For any cumulative distribution functions $U, V, W$ we have the inequality $d(U * W, V * W) \leqslant d(U, V)$. Thus

$$d\left(F_{\zeta_r}, F_{\sum\limits_{j=1}^{r}\delta_j}\right) \leqslant d\left(F_{\varsigma_1}, F_{\delta_1}\right) + d\left(F_{\varsigma_2} * \ldots * F_{\varsigma_r}, F_{\delta_2} * \ldots * F_{\delta_r}\right) \leqslant$$

$$\leqslant d\left(F_{\varsigma_1}, F_{\delta_1}\right) + d\left(F_{\varsigma_2}, F_{\delta_2}\right) + d\left(F_{\varsigma_3} * \ldots * F_{\varsigma_r}, F_{\delta_3} * \ldots * F_{\delta_r}\right) \leqslant \ldots \leqslant$$

$$\leqslant \sum_{j=1}^{r} d\left(F_{\varsigma_j}, F_{\delta_j}\right). \tag{16}$$

If random variables $X$ and $Y$ have symmetric about zero distributions then

$$F_{|X|}(x) = 2F_X(x) - 1,\ x \geqslant 0,\ F_{|X|}(x) = 0,\ x < 0, \tag{17}$$

$$d(F_{\ln|X|}, F_{\ln|Y|}) = \sup_{x\in\mathbb{R}} \left|F_{\ln|X|}(x) - F_{\ln|Y|}(x)\right| = \sup_{x\in\mathbb{R}} \left|F_{|X|}(e^x) - F_{|Y|}(e^x)\right| =$$

$$= \sup_{y\geq 0} \left|F_{|X|}(y) - F_{|Y|}(y)\right| = \sup_{y\in\mathbb{R}} |2F_X(y) - 2F_Y(y)| = 2d\left(F_X, F_Y\right). \tag{18}$$

Equations (17), (18) and properties of the random variables $\tilde{S}_i$ imply that

$$d\left(F_{\varsigma_j}, F_{\delta_j}\right) = d\left(F_{\ln|\tilde{S}_i|}, F_{\ln|\eta_j|}\right) = 2d\left(F_{\tilde{S}_i}, \Phi\right). \tag{19}$$

Later we estimate the right side of the last inequality using next result.

**Lemma 1.** *Let conditions of theorem* 2 *be held. Then*

$$d\left(F_{\tilde{S}_i}, \Phi\right) \leqslant \frac{C(2m+1)^2}{\sqrt{m_i}(\sigma_i)^{3/2}}. \tag{20}$$

From formulas (16), (19) and (20) we develop

$$d\left(F_{\zeta_r}, F_{\sum\limits_{j=1}^{r}\delta_j}\right) \leq 2\sum_{j=1}^{r} d\left(F_{\tilde{S}_j}, \Phi\right) \leq 2C(2m+1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m_j}\sigma_j^{3/2}}. \tag{21}$$

The last inequality and formula (18) give

$$2d\left(F_{\xi_r}, \Phi_r\right) = d\left(F_{\ln|\xi_r|}, F_{\sum\limits_{j=1}^{r}\delta_j}\right) = d\left(F_{\zeta_r}, F_{\sum\limits_{j=1}^{r}\delta_j}\right) \leq$$

$$\leq 2C(2m+1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m_j}\sigma_j^{3/2}}.$$

Estimate (6) comes from the last inequality. The theorem is proved.

Proof of theorem 3. Since

$$d\left(F_{\tilde{\zeta}_r}, \Upsilon\right) = d\left(F_{\ln\tilde{\zeta}_r}, \Phi\right),$$

$$\ln\tilde{\zeta}_r = \frac{1}{\sigma\sqrt{r}}\left(ln|\tilde{\xi}_r| - ra\right) = \frac{1}{\sigma\sqrt{r}}\left(\zeta_r - ra\right),$$

from equality (14) we have

$$\ln\tilde{\zeta}_r = \sum_{i=1}^{r} \tilde{\varsigma}_i, \tilde{\varsigma}_i = \frac{\varsigma_i - a}{\sigma\sqrt{r}}.$$

Thus

$$d\left(F_{\tilde{\zeta}_r}, \Upsilon\right) = d\left(F_{\sum\limits_{i=1}^{r}\tilde{\varsigma}_i}, \Phi\right) \leqslant d\left(F_{\sum\limits_{i=1}^{r}\tilde{\varsigma}_i}, F_{\sum\limits_{i=1}^{r}\tilde{\delta}_i}\right) + d\left(F_{\sum\limits_{i=1}^{r}\tilde{\delta}_i}, \Phi\right), \tag{22}$$

where $\tilde{\delta}_i = \frac{\delta_i - a}{\sigma\sqrt{r}}$, the random variables $\delta_i$ defined by (15). Consider the first summand in right side of inequality (22). For any random variables $Z_1$, $Z_2$ and any $a > 0, b \in \mathbb{R}$

$$d\left(F_{aZ_1+b}, F_{aZ_2+b}\right) = \sup_{x\in\mathbb{R}} |F_{aZ_1+b}(x) - F_{aZ_2+b}(x)| =$$

$$= \sup_{x\in\mathbb{R}} \left|F_{Z_1}\left(\frac{x-b}{a}\right) - F_{Z_2}\left(\frac{x-b}{a}\right)\right| =$$

$$= \sup_{y\in\mathbb{R}} |F_{Z_1}(y) - F_{Z_2}(y)| = d\left(F_{Z_1}, F_{Z_2}\right).$$

Hence

$$d\left(F_{\sum\limits_{i=1}^{r}\tilde{\varsigma}_i}, F_{\sum\limits_{i=1}^{r}\tilde{\delta}_i}\right) = d\left(F_{\sum\limits_{i=1}^{r}\varsigma_i}, F_{\sum\limits_{i=1}^{r}\delta_i}\right) = d\left(F_{\zeta_r}, F_{\sum\limits_{i=1}^{r}\delta_i}\right)$$

Then formula (22) implies

$$d\left(F_{\sum\limits_{i=1}^{r}\tilde{\varsigma}_i}, F_{\sum\limits_{i=1}^{r}\tilde{\delta}_i}\right) \leqslant 2C(2m+1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m_j}\sigma_j^{3/2}}. \tag{23}$$

We use Berry—Esseen inequality (see, e.g., [5]) for the second summand in the right side of (22)

$$d\left(F_{\sum\limits_{i=1}^{r}\tilde{\delta}_i}, \Phi\right) \leq C_{BE}\frac{E|\delta_i|^3}{\sqrt{r}(D\delta_i)^{3/2}} = C_{BE}\frac{c}{\sigma^3\sqrt{r}}. \tag{24}$$

(formulas (7)—(10)), $C_{BE} \leqslant 0,48$ ([4]). Plugging (23) and (24) into (22) we derive (11). The theorem is proved.

Proof of lemma 1. For convergence rate estimation of the cumulative distribution function of random variable $\tilde{S}_i$ to normal law cumulative distribution function we use the next result of paper [6]. Let $\{\xi_v\}_{v\in V}$ be a system of random variables with dependency graph $G = (V, E)$, where $V$ and $E \subseteq V \times V$ are the sets of

graph vertices and graph edges respectively. If there exists a constant $B$ such that $\mathbf{P}\{|\xi_v - \mathbf{E}\xi_v| \le B\} = 1$ for any $v \in V$ then

$$\left|\mathbf{P}\left\{\frac{W - \mathbf{E}W}{\sqrt{\mathbf{D}W}} < x\right\} - \Phi(x)\right| \le 32(1+\sqrt{6})|V|D^2B^3(\mathbf{D}W)^{-3/2}, \tag{25}$$

where $W = \sum\limits_{v\in V}\xi_v$, $D$ is a maximal vertex degree in graph $G$.

We now consider a system of random indicators $X^{(i)}$. Its components $X^{(i)}_{j_1}$ and $X^{(i)}_{j_2}$ are dependent if $|j_1 - j_2| \le m$. Thus, maximal vertex degree in dependency graph corresponding to the system $X^{(i)}$ is $D \le 2m+1$. As $B$ can be set equal to 1 for random indicators formula (25) implies

$$\left|\mathbf{P}\left\{\tilde{S}_i < x\right\} - \Phi(x)\right| \leqslant 32(1+\sqrt{6})m_i(2m+1)^2(\mathbf{D}S_i)^{-3/2} \leqslant$$

$$\le \frac{32(1+\sqrt{6})m_i(2m+1)^2}{(m_i\sigma_i)^{3/2}} = \frac{32(1+\sqrt{6})(2m+1)^2}{\sqrt{m_i}(\sigma_i)^{3/2}}.$$

The lemma is proved.

Proofs of corollary 2 and 3 are very similar to that of corollary 3 and 4 of paper [2]. So they are not presented here.

Author is grateful to referee for helpful comments and suggestions on an earlier version of the paper.

## References

[1] Pohl P., *Description of MCV, a pseudo-random number generator* // Scand. Actuarial J. **1** (1976), 1–14. MR0474695

[2] Mezhennaya N.M., Mikhailov V.G. *Estimators and limit theorems for the number of ones in MCV generator outcome sequence* // Mathematical Aspects of Cryptography, **5**:1 (2014) (in russian).

[3] Ibragimov I.A., Linnik Yu.V. *Independent and stationary related variables*. Moscow: Nauka, 1965, 524 p. MR0202176

[4] Tyurin I.S. *An improvement of the residual in the Lyapunov theorem* // Teor. Veroyatnost. i Primenen., **56**:4 (2011), 808–811.

[5] Shiryaev A.N. *Probability*. Moscow: Nauka, 1980, 576 pp. MR0609521

[6] Baldi P., Rinott Y. *On normal approximations of distributions in terms of dependency graph* // Ann. Probab., **17**:4 (1989), 1646–1650. MR1048950

Natalia Mikhailovna Mezhennaya
Bauman Moscow State University,
2-nd Baumanskaya st., 5
105005, Moscow, Russia
*E-mail address*: natalia.mezhennaya@gmail.com