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 \( \mathbb{GF}(2) \). 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

\[
Z_t = X_{t(m_1)}^{(1)} + \ldots + X_{t(m_r)}^{(r)} \mod M, \quad t = 0, 1, 2, \ldots
\]

Mezhennaya, N.M., Convergence rate estimators for the number of ones in outcome sequence of MCV generator with \( m \)-dependent registers items.
© 2014 Mezhennaya N.M.
The work is supported by RFBR (grant 14-01-00318A).
Received November, 18, 2013, published January, 30, 2014.
there \( t(n) = t \mod n \). Sequence \( \{Z_t\} \) is repeating with period length \( T = m_1 \ldots m_r \).

Let items \((X_0^{(i)}, \ldots, X_{m_i-1}^{(i)})\) in \( i \)-th register be independent random variables with values in the set \( A_M = \{0, 1, \ldots, M - 1\}, \ i = 1, \ldots, r \). 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 \( X_0^{(i)}, \ldots, X_{m_i-1}^{(i)} \) be binary random variables such that

\[
P[X_j^{(i)} = 1] = 1/2, \ j = 0, 1, \ldots, m_i. \tag{2}
\]

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

Let random vectors \( X^{(i)}, \ldots, X^{(r)} \) 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 \( T = m_1 \ldots m_r \). Let \( S_i \) be the number of ones in vector \( X^{(i)}, i = 1, \ldots, r \). It was shown in [2] that

\[
m_1 \ldots m_r - 2\xi_r = (m_1 - 2S_1) \ldots (m_r - 2S_r) \tag{3}
\]

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

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

\[
E\xi_r = \frac{m_1 \ldots m_r}{2}, \tag{4}
\]

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

Remark 1. If random variables in the sets \( X^{(i)}, i = 1, \ldots, r, \) are pairwise independent then formula (5) coincides with the analogous formula in paper [2].
If for all distributions of the random variables \(X^{(i)}_0, X^{(i)}_1, \ldots, X^{(i)}_{m_i-1}\) is cycle shift invariant then instead of (5) we can write

\[ D_{\xi} = 4^{r-1} \prod_{i=1}^{m_i} \sigma_i, \]

\[ \sigma_i = m_i \left( \frac{1}{4} + 2 \sum_{k=1}^{m_i} \mathbb{P}\{X^{(i)}_k = X^{(i)}_1 = 1\} - \frac{m_i}{2} \right), \quad i = 1, \ldots, r. \]

We suppose that \(\tilde{\xi}_r = (m_1 \cdots m_r - \xi_r) (D_{\xi} r)^{-1/2}\). Let us denote by \(F_X\) 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 \(m_1, \ldots, m_r\) are relatively prime odd numbers, the distribution of random variables \(X^{(i)}_0, X^{(i)}_1, \ldots, X^{(i)}_{m_i-1}\) is cycle shift invariant for any \(i\). Then

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

where \(C = 32(1 + \sqrt{6}) \leq 110.4\).

Remark 2. The order of estimate (6) for \(m = \text{const}\) 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, \(m_1, \ldots, m_r \to \infty\) and parameter \(m\) varies in a such way that \(m_i^2 \geq \frac{\sqrt{m_j}}{100} \to 0\) then for any \(x \in \mathbb{R}\)

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

We assume that

\[ a = \frac{2}{\sqrt{2\pi}} \int_{0}^{+\infty} \ln x e^{-x^2/2} dx \approx -0.6352, \]

\[ b = \frac{2}{\sqrt{2\pi}} \int_{0}^{+\infty} \ln^2 x e^{-x^2/2} dx \approx 1.6372, \]

\[ c = \frac{2}{\sqrt{2\pi}} \int_{0}^{+\infty} |\ln x - a|^3 e^{-x^2/2} dx \approx 2.9607, \]

\[ \sigma^2 = b - a^2 \approx 1.2337. \]

It is clear from (7)-(10) that if random variable \(\eta\) has standard normal law then

\[ a = \mathbb{E} \ln |\eta|, \quad \sigma^2 = \mathbb{D} \ln |\eta|, \quad c = \mathbb{E} |\ln |\eta| - a|^3. \]
We also set
\[ \tilde{\zeta}_r = e^{-a\sigma\sqrt{r}} \tilde{\xi}_r \approx e^{-a\sigma/\sqrt{r}} \Theta, \]
\[ \Upsilon(x) = \frac{1}{\sqrt{2\pi}} \int_0^x \frac{1}{y} e^{-\ln^2(y)/2} dy. \]

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
\[ d \left( \tilde{F}_{\tilde{\zeta}}, \Upsilon \right) \leq 2C(2m + 1)^2 \sum_{j=1}^r \frac{1}{\sqrt{m_j\sigma_j^3}} + \frac{C_{BE} c}{\sigma^3\sqrt{r}}, \]
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 \( x \in \mathbb{R} \)
\[ \left| \tilde{F}_{\tilde{\xi}}(x) - \frac{1}{2} \left( 1 + \text{sign}(x) \Phi \left( \frac{\ln|x|}{\sigma} - \frac{a}{\sigma}\sqrt{r} \right) \right) \right| \leq \]
\[ \leq C(2m + 1)^2 \sum_{j=1}^r \frac{1}{\sqrt{m_j\sigma_j^3}} + \frac{C_{BE} c}{2\sigma^3\sqrt{r}}. \]

**Corollary 3.** Let hypothesis of theorem 2 be held. If \( r, m_1, \ldots, m_r \to \infty \) such that
\[ m^2 \sum_{j=1}^r m_j^{-1/2} \to 0 \]
then for any \( \frac{1}{2} < \alpha < 1 \)
\[ P \left\{ \xi_r < \frac{m_1 \cdots m_r}{2} + e^{ar + u_{2\alpha - 1} \sigma\sqrt{r}} \prod_{i=1}^r m_i \sigma_i \right\} \to \alpha, \]
\[ P \left\{ \xi_r < \frac{m_1 \cdots m_r}{2} - e^{ar + u_{2\alpha - 1} \sigma\sqrt{r}} \prod_{i=1}^r m_i \sigma_i \right\} \to 1 - \alpha, \]
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 \( S_i = \sum_{j=0}^{m_i - 1} X_{j}^{(i)} \) and all random variables \( X_0^{(i)}, \ldots, X_{m_i - 1}^{(i)} \) have the same one-dimensional distribution laws equation (2) implies
\[ E(S_i) = \sum_{j=0}^{m_i - 1} E(X_{j}^{(i)}) = m_i E(X_1^{(i)}) = m_i P(X_1^{(i)} = 1) = \frac{m_i}{2}. \]

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
\[ E(m_1 \cdots m_r - 2\xi_r) = E(m_1 - 2S_1) \cdots E(m_r - 2S_r) = 0. \]
This involves formula (4).
Now we compute the variance

\[ DS_i = D \left( \sum_{j=0}^{m_i-1} X_j^{(i)} \right) = \sum_{j=0}^{m_i-1} DX_j^{(i)} + 2 \sum_{0 \leq j_1 < j_2 \leq m_i-1} \text{cov}(X_{j_1}^{(i)}, X_{j_2}^{(i)}) = \]

\[ = m_i DX_1^{(i)} + 2 \sum_{0 \leq j_1 < j_2 \leq m_i-1} \left( E X_{j_1}^{(i)} X_{j_2}^{(i)} - E X_{j_1}^{(i)} E X_{j_2}^{(i)} \right) = \]

\[ = \frac{m_i}{4} + 2 \sum_{0 \leq j_1 \leq m_i-1, \ 0 < j_2-j_1 \leq m} \left( P\{X_{j_1}^{(i)} = X_{j_2}^{(i)} = 1\} - \frac{1}{4} \right) = \]

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

(12) \[ = m_i \left( \frac{1}{4} - \frac{m}{22} \right) + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} P\{X_{j_1}^{(i)} = X_{(j_1+k) \mod m_i}^{(i)} = 1\}. \]

From (4) and (12) we develop

\[ D \xi_r = E \left( \xi_r - \frac{m_1 \ldots m_r}{2} \right)^2 = \frac{1}{4} E (2 \xi_r - m_1 \ldots m_r)^2 = \]

\[ = \frac{1}{4} E (m_1 - 2 S_1)^2 \ldots E (m_r - 2 S_r)^2 = \]

\[ = 4^{r-1} DS_1 \ldots DS_r = \]

\[ = 4^{r-1} \prod_{i=1}^{r} \left( m_i \left( \frac{1}{4} - \frac{m}{22} \right) + 2 \sum_{j_1=0}^{m_i-1} \sum_{k=1}^{m} P\{X_{j_1}^{(i)} = X_{(j_1+k) \mod m_i}^{(i)} = 1\} \right). \]

The theorem is proved.

Proof of theorem 2. Denote

\[ \hat{S}_i = (DS_i)^{-1/2} (S_i - ES_i) = \frac{S_i - m_i}{\sqrt{m_i} \sigma_i}. \]

It follows from (3) that

\[ \frac{m_1 \ldots m_r}{2} - \xi_r = 2^{r-1} \prod_{i=1}^{r} \left( \frac{m_i}{2} - S_i \right). \]

Substituting (5) into the last formula we obtain that

\[ \hat{\xi}_r = (DS_r)^{-1/2} \left( \frac{m_1 \ldots m_r}{2} - \xi_r \right) = \frac{2^{r-1} \prod_{i=1}^{r} \left( \frac{m_i}{2} - S_i \right)}{2^{r-1} \prod_{i=1}^{r} \sqrt{m_i} \sigma_i} = \]

(13) \[ = \prod_{i=1}^{r} \frac{m_i}{\sqrt{m_i} \sigma_i} = \prod_{i=1}^{r} \hat{S}_i. \]

We set \( \zeta_r = \ln |\xi_r|, \ldots, \zeta_j = \ln |\hat{S}_j|, \ j = 1, \ldots, r. \) Then (13) implies

(14) \[ \zeta_r = \sum_{j=1}^{r} \zeta_j. \]
Since the random variables $\zeta_1, \ldots, \zeta_r$ are independent we find out

$$F_{\zeta_i} = F_{\zeta_1} * \ldots * F_{\zeta_r},$$

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,

$$\delta_i = \ln |\eta_i|, \ i = 1, \ldots, r.$$  \hspace{1cm} (15)

From the last definitions and formula (14) we derive estimate $\delta_i (15)$ normal distribution law, where sign $\leq$ is used to designate convolution.

$$F \leq \sum_{j=1}^{r} \delta_j,$$  \hspace{1cm} (16)

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

$$d \left( \sum_{j=1}^{r} \delta_j \right) \leq d \left( \sum_{j=1}^{r} \delta_j \right) = \sum_{j=1}^{r} d \left( F_{\zeta_j}, F_{\delta_j} \right).$$

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

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

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

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

$$d \left( F_{|\eta_i|}, F_{|\eta_i|} \right) = d \left( F_{|\eta_i|}, F_{|\eta_i|} \right) = 2d \left( F_{\bar{\zeta}_i}, \Phi \right).$$

Later we estimate the right side of the last inequality using next result.  \hspace{1cm} \textbf{Lemma 1.} Let conditions of theorem 2 be held. Then

$$d \left( F_{\bar{\zeta}_i}, \Phi \right) \leq \frac{C(2m + 1)^2}{\sqrt{m \sigma_i^2}}.$$

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

$$d \left( \sum_{j=1}^{r} \delta_j \right) \leq 2 \sum_{j=1}^{r} d \left( F_{\bar{\zeta}_j}, \Phi \right) \leq 2C(2m + 1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m \sigma_j^2}}.$$

The last inequality and formula (18) give

$$2d \left( F_{\bar{\zeta}_i}, \Phi \right) = d \left( F_{|\eta_i|}, F_{\sum_{j=1}^{r} \delta_j} \right) = d \left( F_{\zeta_i}, F_{\sum_{j=1}^{r} \delta_j} \right) \leq$$
\[ \leq 2C(2m + 1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m_j} \sigma_j^{3/2}}. \]

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

Proof of theorem 3. Since
\[ d\left(F_{\hat{\zeta}_r}, \Upsilon\right) = d\left(F_{\ln \hat{\zeta}_r}, \Phi\right), \]
\[ \ln \hat{\zeta}_r = \frac{1}{\sigma \sqrt{r}} \left(\ln|\hat{\xi}_r| - ra\right) = \frac{1}{\sigma \sqrt{r}} \left(\zeta_r - ra\right), \]
from equality (14) we have
\[ \ln \hat{\zeta}_r = \sum_{i=1}^{r} \tilde{\varsigma}_i, \tilde{\varsigma}_i = \varsigma_i - a \sigma \sqrt{r}. \]

Thus
\[ (22) \quad d\left(F_{\hat{\zeta}_r}, \Upsilon\right) = d\left(F_{\sum_{i=1}^{r} \tilde{\varsigma}_i}, \sum_{i=1}^{r} \tilde{\delta}_i\right) \leq d\left(F_{\sum_{i=1}^{r} \varsigma_i}, \sum_{i=1}^{r} \delta_i\right) + d\left(F_{\sum_{i=1}^{r} \delta_i}, \Phi\right), \]
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
\[ d\left(F_{\sum_{i=1}^{r} \varsigma_i}, \sum_{i=1}^{r} \delta_i\right) = d\left(F_{\sum_{i=1}^{r} \tilde{\varsigma}_i}, \sum_{i=1}^{r} \tilde{\delta}_i\right) \]
Then formula (22) implies
\[ (23) \quad d\left(F_{\sum_{i=1}^{r} \tilde{\varsigma}_i}, \sum_{i=1}^{r} \tilde{\delta}_i\right) \leq 2C(2m + 1)^2 \sum_{j=1}^{r} \frac{1}{\sqrt{m_j} \sigma_j^{3/2}}. \]

We use Berry–Esseen inequality (see, e.g., [5]) for the second summand in the right side of (22)
\[ (24) \quad d\left(F_{\sum_{i=1}^{r} \tilde{\delta}_i}, \Phi\right) \leq C_{BE} \frac{E[|\delta_i|^3]}{\sqrt{r}(D\delta_i)^{3/2}} = C_{BE} \frac{c}{\sigma \sqrt{r}}. \]
(formulas (7)–(10)), \( C_{BE} \leq 0, 48 \) ([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

$$P\left\{ |\xi - E\xi| \leq B \right\} = 1 \text{ for any } v \in V$$

then

$$P\left\{ \left| \frac{W - EW}{\sqrt{DV}} - x \right| - \Phi(x) \right\} \leq 32(1 + \sqrt{6})|V|D^2B^3(DW)^{-3/2},$$

where $W = \sum_{v \in V} \xi_v$, $D$ 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 $|j_1 - j_2| \leq m$. Thus, maximal vertex degree in dependency graph corresponding to the system $X^{(i)}$ is $D \leq 2m + 1$. As $B$ can be set equal to 1 for random indicators formula (25) implies

$$P\left\{ S_i < x \right\} - \Phi(x) \leq 32(1 + \sqrt{6})m_i(2m + 1)^2(D_i)^{-3/2} \leq$$

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

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


NATALIA MIKHAILOVNA MEZHENNYA
BAUMAN MOSCOW STATE UNIVERSITY,
2-nd Baumanskaya st., 5
105005, Moscow, RUSSIA
E-mail address: natalia.mezhennaya@gmail.com