В. А. Ватутин, О близости распределения некоторой случайной величины к равновероятному распределению, *Матем. вопр. криптогр.*, 2023, том 14, выпуск 1, 5–14

DOI: 10.4213/mvk427

**МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ**
**2023 Т. 14 № 1 С. 5–14**

УДК 519.213 DOI https://doi.org/10.4213/mvk427

# О близости распределения некоторой случайной величины к равновероятному распределению

**В. А. Ватутин**

*Математический институт им В.А. Стеклова Российской академии наук, Москва*

*Получено* 12.V.2022

**Аннотация.** Пусть $b \geqslant 2$ и $N$ – натуральные числа, $X_0, X_1, \ldots, X_{n-1}$ – неоднородная последовательность независимых случайных величин, принимающих значения $0, 1, \ldots, b-1$,

$$Y_n = X_0 + bX_1 + \ldots + X_{n-2}b^{n-2} + X_{n-1}b^{n-1}$$

и

$$Z_n = Y_n \bmod N.$$

В предположении, что числа $b$ и $N$ взаимно просты, оценивается близость распределения случайной величины $Z_n$ к равновероятному распределению на множестве $\{0, 1, \ldots, N-1\}$.

**Ключевые слова:** преобразования случайных величин, приведение по модулю, равновероятные распределения, расстояния между распределениями

## On the closeness of distribution of some random variable to the equiprobable one

**V. A. Vatutin**

*Steklov Mathematical Institute of Russian Academy of Sciences, Moscow*

**Abstract.** Let $b \geqslant 2$ and $N$ be natural numbers, $X_0, X_1, \ldots, X_{n-1}$ be nonhomogeneous sequence of independent random variables taking values $0, 1, \ldots, b-1$,

$$Y_n = X_0 + bX_1 + \ldots + X_{n-2}b^{n-2} + X_{n-1}b^{n-1}$$

and

$$Z_n = Y_n \bmod N.$$

We estimate the closeness of distribution of random variable $Z_n$ to the uniform distribution on $\{0, 1, \ldots, N-1\}$ in the case when $b$ and $N$ are mutually prime.

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 1, pp. 5–14 (Russian)

**Keywords:** transformations of random variables, modulo reduction, equiprobable distributions, distances between distributions

Пусть $X_0, X_1, \ldots, X_{n-1}$ – неоднородная последовательность независимых случайных величин со значениями в множестве $\{0, 1, \ldots, b-1\}$ и распределениями, задаваемыми соотношениями

$$\mathbf{P}\left(X_i = t\right) = p_{it}, \quad t = 0, 1, \ldots, b-1, \ i = 0, 1, \ldots, n-1.$$

Свяжем с этой последовательностью неотрицательное целое число

$$Y_n = X_0 + X_1 b + \ldots + X_{n-2} b^{n-2} + X_{n-1} b^{n-1}. \tag{1}$$

Пусть далее $N < b^n$ – натуральное число, а

$$Z_n = Y_n \bmod N. \tag{2}$$

Наша цель — изучить вероятностные свойства случайной величины $Z_n$, точнее, нас будет интересовать ответ на вопрос: при каких значениях чисел $b$ и $N$ распределение $Z_n$ близко к равновероятному?

Задача, рассматриваемая в данной работе, тесно связана с проблемой моделирования знака $\varkappa$, имеющего равновероятное распределение на множестве $\{0, 1, \ldots, q-1\}$, исходя из случайной последовательности $\gamma = \{\gamma_n, n \geqslant 1\}$ независимых знаков, распределенных не обязательно равновероятно на множестве $\{0, 1, \ldots, p-1\}$ (см. в этой связи основополагающую работу фон Неймана [2], а также статью Ф. М. Малышева [1] и ссылки в ней). В анализируемой нами ситуации случайная величина $Y_n$ (аналог величины $\gamma_n$ из работы [1]) также имеет неравновероятное распределение, хотя некоторые знаки в наборе $(X_0, X_1, \ldots, X_{n-1})$ распределены равновероятно на множестве $\{0, 1, \ldots, b-1\}$. Поскольку кроме преобразования (2) никаких других операций над случайной величиной $Y_n$ производиться не будет, то в качестве основной характеристики распределения случайной величины $Z_n$ будет служить параметр

$$\Delta_N(n) = \max_{0 \leqslant k \leqslant N-1} \left| \mathbf{P}\left(Z_n = k\right) - \frac{1}{N} \right|,$$

отражающий близость распределения $Z_n$ к равновероятному распределению на множестве $\{0, 1, \ldots, N-1\}$.

В данной работе мы получим оценки сверху величины $\Delta_N(n)$, накладывая на пару чисел $(b, N)$ некоторые ограничения. А именно, будем

предполагать, что числа $b$ и $N$ взаимно просты и $N < b^n$. Обозначим через $[x]$ целую часть числа $x$ и запишем число $H = [b^n/N]$ в виде

$$H = \left[\frac{b^n}{N}\right] = rb^m + s, \tag{3}$$

где $m$, $r$ и $s$ – целые числа, причем $1 \leqslant r \leqslant b$, а $|s| < b^m/2$. Отметим, что

$$rb^m + s \leqslant \frac{b^n}{N} < rb^m + s + 1$$

и, следовательно,

$$\left|\frac{1}{N} - \frac{r}{b^{n-m}}\right| \leqslant \frac{|s|+1}{b^n}. \tag{4}$$

Для $k = 0, 1, \ldots, N-1$ обозначим

$$\mathcal{A}_k := \left\{0 \leqslant j \leqslant H : k + jN \leqslant b^n - 1\right\}.$$

В силу определения величины $H$ для любого $j \in \mathcal{A}_k$ имеем

$$0 \leqslant j \leqslant \frac{b^n}{N} - \frac{k+1}{N} = H + \theta - \frac{k+1}{N},$$

где $\theta \in [0, 1)$. Таким образом, либо $\mathcal{A}_k = \{0, 1, \ldots, H-1\}$, либо $\mathcal{A}_k = \{0, 1, \ldots, H\}$. Пусть, далее,

$$\mathcal{B}_k(r, s) := \mathcal{A}_k \setminus \{0, 1, \ldots, rb^m - 1\},$$

если $s$ в представлении (3) неотрицательно, и

$$\mathcal{C}_k(r, s) := \{0, 1, \ldots, rb^m - 1\} \setminus \mathcal{A}_k,$$

если $s$ в представлении (3) отрицательно. Обозначая $|\mathcal{D}|$ мощность множества $\mathcal{D}$, имеем

$$|\mathcal{B}_k(r, s)| = |\mathcal{A}_k| - rb^m \leqslant H + 1 - rb^m \leqslant s + 1, \quad s > 0, \tag{5}$$

и

$$|\mathcal{C}_k(r, s)| = rb^m - |\mathcal{A}_k| \leqslant rb^m - H + 1 \leqslant 1 - s = 1 + |s|. \tag{6}$$

В формулируемой ниже лемме предполагаем, что случайные величины $X_i, i \in [m, n-1]$, т. е. старшие разряды числа $Y_n$ в его представлении (1) в $b$-ичной системе, имеют равномерное распределение на множестве $\{0, 1, \ldots, b-1\}$.

**Лемма 1.** *Если случайные величины* $X_0, X_1, \ldots, X_{n-1}$ *независимы, причем*

$$\mathbf{P}\left(X_i = t\right) = \frac{1}{b} \quad \textit{для } t = 0, 1, \ldots, b-1, \quad i = m, m+1, \ldots, n-1, \tag{7}$$

*то при* $s \geqslant 0$

$$\mathbf{P}\left(Z_n = k\right) = \frac{r}{b^{n-m}} + \frac{1}{b^{n-m}} \sum_{j \in \mathcal{B}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right), \tag{8}$$

*а при* $s < 0$

$$\mathbf{P}\left(Z_n = k\right) = \frac{r}{b^{n-m}} - \frac{1}{b^{n-m}} \sum_{j \in \mathcal{C}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right). \tag{9}$$

*Доказательство*. Зафиксируем число $k \in \{0, 1, \ldots, N-1\}$ и для $j \in \{0, 1, \ldots, H\}$ положим

$$k_j := \left[\frac{k + Nj}{b^m}\right].$$

Тогда для некоторого набора

$$(\zeta_0, \ldots, \zeta_{m-1}) \in \{0, 1, \ldots, b-1\}^m,$$

зависящего от $k$ и $j$, справедливо представление

$$\begin{aligned} k + Nj &= (k + Nj) \mod b^m + k_j b^m \\ &= \zeta_0 + \zeta_1 b + \ldots + \zeta_{m-2} b^{m-2} + \zeta_{m-1} b^{m-1} + k_j b^m \\ &=: Y_m + k_j b^m. \end{aligned}$$

Отсюда следует, что $b$-ичное разложение числа $k + jN \leqslant b^n - 1$ имеет вид

$$\begin{aligned} k + jN &= Y_m + k_j b^m \\ &= Y_m + \zeta_m b^m + \zeta_{m+1} b^{m+1} + \ldots + \zeta_{n-2} b^{n-2} + \zeta_{n-1} b^{n-1}, \end{aligned}$$

где

$$(\zeta_0, \ldots, \zeta_{m-1}, \zeta_m, \ldots, \zeta_{n-1}) \in \{0, 1, \ldots, b-1\}^n$$

– некоторый набор, зависящий от $k$ и $j$.

Если $j \in \mathcal{A}_k$, то в силу условия (7)

$$\begin{aligned}\mathbf{P}\left(Y_n = k + jN\right) &= \mathbf{P}((X_0, X_1, \ldots, X_{n-1}) = (\zeta_0, \zeta_1, \ldots, \zeta_{n-1})) \\ &= \frac{1}{b^{n-m}}\mathbf{P}((X_0, X_1, \ldots, X_{m-1}) = (\zeta_0, \zeta_1, \ldots, \zeta_{m-1})) \\ &= \frac{1}{b^{n-m}}\mathbf{P}(Y_m = (k + Nj\ ) \bmod b^m). \end{aligned} \tag{10}$$

Следовательно,

$$\begin{aligned}\mathbf{P}\left(Z_n = k\right) &= \sum_{j \in \mathcal{A}_k} \mathbf{P}\left(Y_n = k + jN\right) \\ &= \frac{1}{b^{n-m}} \sum_{j \in \mathcal{A}_k} \mathbf{P}(Y_m = (k + Nj) \bmod b^m). \end{aligned} \tag{11}$$

Рассмотрим сначала случай $H = rb^m + s, s \geqslant 0$. Тогда

$$\begin{aligned}\sum_{j \in \mathcal{A}_k} \mathbf{P}\left(Y_m = (k + Nj) \bmod b^m\right) = &\sum_{0 \leqslant j \leqslant rb^m - 1} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right) \\ &+ \sum_{j \in \mathcal{B}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \bmod b^m\right). \end{aligned} \tag{12}$$

Ясно, что для любого $y \in \{0, 1, \ldots, r-1\}$

$$\begin{aligned}\sum_{yb^m \leqslant j \leqslant (y+1)b^m - 1} &\mathbf{P}\left(Y_m = (k + Nj) \bmod b^m\right) \\ &= \sum_{0 \leqslant q \leqslant b^m - 1} \mathbf{P}\left(Y_m = (k + Nq) \mod b^m\right). \end{aligned}$$

Следовательно,

$$\begin{aligned}\sum_{0 \leqslant j \leqslant rb^m - 1} &\mathbf{P}\left(Y_m = (k + Nj) \bmod b^m\right) \\ &= \sum_{y=0}^{r-1} \sum_{yb^m \leqslant j \leqslant (y+1)b^m - 1} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right) \\ &= r \sum_{0 \leqslant q \leqslant b^m - 1} \mathbf{P}\left(Y_m = (k + Nq) \bmod b^m\right). \end{aligned} \tag{13}$$

Поскольку числа $N$ и $b$ взаимно просты, то множество

$$\mathcal{D}_k := \{(k + Nq) \mod b^m,\ q = 0, 1, \ldots, b^m - 1\}$$

совпадает с множеством

$$\mathcal{D}_0 := \{(Nq) \mod b^m,\ q = 0, 1, \ldots, b^m - 1\} = \{0, 1, \ldots, b^m - 1\}.$$

Поэтому для любого допустимого значения $k$

$$\begin{aligned}\sum_{0\leqslant q\leqslant b^m-1} \mathbf{P}\left(Y_m = (k + Nq) \mod b^m\right) \\ = \sum_{0\leqslant q\leqslant b^m-1} \mathbf{P}\left(Y_m = Nq \mod b^m\right) \\ = \sum_{0\leqslant q\leqslant b^m-1} \mathbf{P}\left(Y_m = q\right) = 1. \qquad (14)\end{aligned}$$

Объединяя соотношения (11)–(14), приходим к (8).

Случай $H = rb^m + s, s < 0$, исследуется таким же способом:

$$\begin{aligned}\mathbf{P}\left(Z_n = k\right) &= \frac{1}{b^{n-m}} \sum_{j\in\mathcal{A}_k} \mathbf{P}(Y_m = (k + Nj\ ) \mod b^m) \\ &= \frac{1}{b^{n-m}} \sum_{0\leqslant j\leqslant rb^m-1} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right) \\ &- \frac{1}{b^{n-m}} \sum_{j\in\mathcal{C}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right) \\ &= \frac{r}{b^{n-m}} - \frac{1}{b^{n-m}} \sum_{j\in\mathcal{C}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right), \qquad (15)\end{aligned}$$

что доказывает (9).

Лемма 1 доказана. □

**Замечание 1.** Легко проверить, что при доказательстве соотношений (14) независимость случайных величин $X_0, \ldots, X_{m-1}$ не использовалась. Таким образом, заключение леммы 1 остается верным в ситуации, когда набор как угодно зависимых между собой случайных величин $X_0, \ldots, X_{m-1}$ не зависит от набора независимых случайных величин $X_m, \ldots, X_{n-1}$, каждая из которых имеет равномерное распределение на множестве $\{0, 1, \ldots, b - 1\}$.

Пусть

$$h_i = \max_{0\leqslant t\leqslant b-1} p_{it}, \quad i = 0, 1, \ldots, m - 1.$$

**Теорема 1.** *Если случайные величины $X_0, X_1, \ldots, X_{n-1}$ независимы, выполнено условие* (7)*, числа $b$ и $N$ взаимно просты и $H = rb^m + s$, то*

$$\Delta_N(n) = \max_{0\leqslant k\leqslant N-1}\left|\mathbf{P}\left(Z_n = k\right) - \frac{1}{N}\right| \leqslant \frac{|s|+1}{b^n} + \frac{|s|+1}{b^{n-m}}\prod_{i=0}^{m-1} h_i.$$

*Доказательство*. Пусть $s \geqslant 0$. Используя соотношения (8) и обращаясь к (4) и (5), заключаем, что

$$\begin{aligned}
\Delta_N(n) &= \max_{0\leqslant k\leqslant N-1}\left|\mathbf{P}\left(Z_n = k\right) - \frac{1}{N}\right| \\
&\leqslant \left|\frac{r}{b^{n-m}} - \frac{1}{N}\right| + \max_{0\leqslant k\leqslant N-1}\left|\mathbf{P}\left(Z_n = k\right) - \frac{r}{b^{n-m}}\right| \\
&\leqslant \frac{s+1}{b^n} + \frac{1}{b^{n-m}}\max_{0\leqslant k\leqslant N-1}\left(\sum_{j\in\mathcal{B}_k(r,s)}\mathbf{P}\left(Y_m = (k+Nj) \bmod b^m\right)\right) \\
&\leqslant \frac{s+1}{b^n} + \frac{s+1}{b^{n-m}}\max_{0\leqslant k\leqslant N-1, j\in\mathcal{B}_k(r,s)}\mathbf{P}\left(Y_m = (k+Nj) \bmod b^m\right) \\
&\leqslant \frac{s+1}{b^n} + \frac{s+1}{b^{n-m}}\prod_{i=0}^{m-1} h_i, \qquad (16)
\end{aligned}$$

что доказывает теорему для случая $s \geqslant 0$.

При $s < 0$, опираясь на (4), (6) и (9), имеем

$$\begin{aligned}
\Delta_N(n) &= \max_{0\leqslant k\leqslant N-1}\left|\mathbf{P}\left(Z_n = k\right) - \frac{1}{N}\right| \\
&\leqslant \left|\frac{r}{b^{n-m}} - \frac{1}{N}\right| + \max_{0\leqslant k\leqslant N-1}\left|\mathbf{P}\left(Z_n = k\right) - \frac{r}{b^{n-m}}\right| \\
&\leqslant \frac{|s|+1}{b^n} + \frac{|s|}{b^{n-m}}\max_{0\leqslant k\leqslant N-1, j\in\mathcal{C}_k(r,s)}\mathbf{P}\left(Y_m = (k+Nj) \bmod b^m\right) \\
&\leqslant \frac{|s|+1}{b^n} + \frac{|s|+1}{b^{n-m}}\prod_{i=0}^{m-1} h_i.
\end{aligned}$$

Теорема 1 доказана. □

Конечно, условие

$$\mathbf{P}\left(X_i = t\right) = \frac{1}{b}, \quad t = 0, 1, \ldots, b-1$$

при $i = m, m+1, \ldots, n-1$ является весьма ограничительным. Рассмотрим более общую ситуацию. С этой целью введем обозначение

$$g_i := \min_{0 \leqslant t \leqslant b-1} p_{it}, \quad i = 0, 1, \ldots, n-1.$$

**Теорема 2.** *Пусть случайные величины $X_0, X_1, \ldots, X_{n-1}$ независимы, числа $b$ и $N$ взаимно просты и $H = rb^m + s$. Предположим, что для некоторых чисел $\varepsilon_1 \in (0,1)$ и $\varepsilon_2 > 0$ справедливы неравенства*

$$\frac{1-\varepsilon_1}{b^{n-m}} \leqslant \prod_{i=m}^{n-1} g_i \leqslant \prod_{i=m}^{n-1} h_i \leqslant \frac{1+\varepsilon_2}{b^{n-m}} \tag{17}$$

*и, кроме того, для некоторого $\delta > 0$ справедлива оценка*

$$\prod_{i=0}^{m-1} h_i \leqslant \frac{1+\delta}{b^m}. \tag{18}$$

*Тогда при $s \geqslant 0$*

$$\begin{aligned} \left| \mathbf{P}\left(Z_n = k\right) - \frac{1}{N} \right| &\leqslant \frac{s+1}{b^n} \\ &+ \frac{1}{b^{n-m}} \max\left\{ r\varepsilon_2 + \frac{(1+\varepsilon_2)(s+1)(1+\delta)}{b^m}, r\varepsilon_1 \right\}, \end{aligned}$$

*а при $s < 0$*

$$\begin{aligned} \left| \mathbf{P}\left(Z_n = k\right) - \frac{1}{N} \right| &\leqslant \frac{|s|+1}{b^n} \\ &+ \frac{1}{b^{n-m}} \max\left\{ r\varepsilon_1 + \frac{(1+\varepsilon_1)|s|(1+\delta)}{b^m}, r\varepsilon_2 \right\}. \end{aligned}$$

*Доказательство*. По аналогии с (10) и (11) при $k + jN < b^n$ имеем

$$\begin{aligned} \mathbf{P}\left(Y_n = k + jN\right) &= \mathbf{P}((X_0, X_1, \ldots, X_{n-1}) = (\zeta_0, \zeta_1, \ldots, \zeta_{n-1})) \\ &= \mathbf{P}((X_m, \ldots, X_{n-1}) = (\zeta_m, , \ldots, \zeta_{n-1}))\, \mathbf{P}(Y_m = (k + Nj) \mod b^m) \\ &\leqslant \left( \prod_{i=m}^{n-1} h_i \right) \mathbf{P}(Y_m = (k + Nj) \mod b^m) \\ &\leqslant \frac{1+\varepsilon_2}{b^{n-m}} \mathbf{P}(Y_m = (k + Nj) \mod b^m) \end{aligned}$$

и

$$\begin{aligned}\mathbf{P}\left(Y_n = k + jN\right) &\geqslant \left(\prod_{i=m}^{n-1} g_i\right) \mathbf{P}(Y_m = (k + Nj) \mod b^m) \\ &\geqslant \frac{1-\varepsilon_1}{b^{n-m}} \mathbf{P}(Y_m = (k + Nj) \mod b^m).\end{aligned}$$

Отсюда следует, что при $s \geqslant 0$

$$\begin{aligned}\mathbf{P}\left(Z_n = k\right) &= \sum_{0 \leqslant j \leqslant rb^m - 1} \mathbf{P}\left(Y_n = k + jN\right) \\ &+ \sum_{j \in \mathcal{B}_k(r,s)} \mathbf{P}\left(Y_n = (k + Nj) \mod b^m\right) \\ &\leqslant \frac{(1+\varepsilon_2)}{b^{n-m}} \sum_{0 \leqslant j \leqslant rb^m - 1} \mathbf{P}\left(Y_m = k + jN\right) \\ &+ \frac{(1+\varepsilon_2)}{b^{n-m}} \sum_{j \in \mathcal{B}_k(r,s)} \mathbf{P}\left(Y_m = (k + Nj) \mod b^m\right) \\ &\leqslant \frac{(1+\varepsilon_2)}{b^{n-m}} \left(r + (s+1) \prod_{i=0}^{m-1} h_i\right) \\ &\leqslant \frac{(1+\varepsilon_2)}{b^{n-m}} \left(r + \frac{(s+1)\,(1+\delta)}{b^m}\right)\end{aligned}$$

и

$$\begin{aligned}\mathbf{P}\left(Z_n = k\right) &\geqslant \sum_{0 \leqslant j \leqslant rb^m - 1} \mathbf{P}\left(Y_n = k + jN\right) \\ &\geqslant \frac{(1-\varepsilon_1)}{b^{n-m}} \sum_{0 \leqslant j \leqslant rb^m - 1} \mathbf{P}\left(Y_m = k + jN\right) \\ &= \frac{r\,(1-\varepsilon_1)}{b^{n-m}}.\end{aligned}$$

Эти неравенства в сочетании с оценкой (4) влекут первое утверждение теоремы 2.

При $s<0$ имеем

$$\begin{aligned}\mathbf{P}\left(Z_n=k\right) &= \sum_{0\leqslant j\leqslant \mathcal{A}_k}\mathbf{P}\left(Y_n=k+jN\right)\\ &\leqslant \sum_{0\leqslant j\leqslant rb^m-1}\mathbf{P}\left(Y_n=k+jN\right)\\ &\leqslant \prod_{i=m}^{n-1}h_i\sum_{0\leqslant j\leqslant rb^m-1}\mathbf{P}\left(Y_m=k+jN\right)\leqslant\frac{(1+\varepsilon_2)\,r}{b^{n-m}}\end{aligned}$$

и

$$\begin{aligned}\mathbf{P}\left(Z_n=k\right) &= \sum_{0\leqslant j\leqslant rb^m-1}\mathbf{P}\left(Y_n=k+jN\right)\\ &\quad-\sum_{j\in\mathcal{C}_k(r,s)}\mathbf{P}\left(Y_n=(k+Nj)\mod b^m\right)\\ &\geqslant \prod_{i=m}^{n-1}g_i\sum_{0\leqslant j\leqslant rb^m-1}\mathbf{P}\left(Y_m=k+jN\right)\\ &\quad-\prod_{i=m}^{n-1}h_i\sum_{j\in\mathcal{C}_k(r,s)}\mathbf{P}\left(Y_m=(k+Nj)\mod b^m\right)\\ &\geqslant \frac{(1-\varepsilon_1)}{b^{n-m}}r-\frac{1+\varepsilon_2}{b^{n-m}}\,|s|\prod_{i=0}^{m-1}h_i\\ &\geqslant \frac{(1-\varepsilon_1)}{b^{n-m}}r-\frac{|s|\,(1+\varepsilon_2)(1+\delta)}{b^{n-m}}.\end{aligned}$$

Эти неравенства и оценка (4) подтверждают справедливость второго утверждения теоремы 2.

□

**Замечание 2.** Из вида оценок, установленных в теоремах 1 и 2, следует, что распределение случайной величины $Z_n$ будет наиболее близко к равновероятному, если в представлении (3) параметр $|s|$ будет мал.

## Список литературы

[1] Малышев Ф. М., "Моделирование равномерного распределения, устойчивое к неравновероятности исходных знаков", *Дискретная математика*, **17**:4 (2005), 72–80.

[2] Neumann J. von, "Various techniques used in connection with random digits", *John von Neumann, Collected Works*, **V**, MacMillan, New York, 1963, 768–770.