**ИНФОРМАТИКА**

**2008** **июль-сентябрь** **№ 3**

*УДК 681.32:519.2*

**А.Н. Ярмола**

# ОБ ОБНАРУЖЕНИИ КВАЗИПЕРИОДОВ В БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

*Разрабатываются новые методы и алгоритмы статистического обнаружения квазипериодов в бинарных последовательностях. Исследуется состоятельность предложенных методов оценивания квазипериода, находятся оценки числа наблюдений, достаточного для эффективного использования разработанных алгоритмов. Представляются оценки вычислительной сложности алгоритмов и результаты численных экспериментов.*

## Введение

Генераторы псевдослучайных последовательностей (ПСП) применяются в системах защиты информации [1]. Одним из основных требований к генераторам ПСП является большое значение периода выходной последовательности генератора, однако важным является и структура периода выходной последовательности. В работах [2, 3] были предложены методы обнаружения закономерностей в выходной последовательности $\{x_t\}$ генератора ПСП в случае, если ее можно представить в виде $x_t = y_t \oplus \gamma_t$, где $\{y_t\}$ – выходная последовательность линейного регистра сдвига с обратной связью, полином обратной связи которого считается известным, $\{\gamma_t\}$ – последовательность независимых одинаково распределенных случайных величин (н.о.р.с.в.) Бернулли, $\mathbf{P}\{\gamma_t = 1\} < 0{,}5$. Данная работа продолжает исследования [2, 3] для случая, когда ограничение линейности на последовательность $\{y_t\}$ отсутствует.

В настоящей работе предлагаются методы и алгоритмы, позволяющие выявлять следующую структуру периода выходной последовательности – последовательность на периоде можно разбить на несколько малоразличающихся между собой и равных по длительности частей. Длительность этих частей назовем квазипериодом $T^*$. Такая структура выходной последовательности генератора ПСП означает, что можно построить аппроксимацию наблюдаемой последовательности вида $x_t = y_t \oplus \gamma_t$, где $\{y_t\}$ – выходная последовательность некоторого более простого (не обязательно линейного) детерминированного генератора с периодом $T^*$.

Достоинством предлагаемых методов обнаружения квазипериода в бинарной последовательности является возможность их применения в отсутствие какой-либо априорной информации о внутренней структуре генератора ПСП.

## 1. Задача распознавания моделей VBAR и VBR

Пусть $x_t = A = \{0,1\}$ – бинарная периодическая последовательность, период которой равен $T^0 = m^* T^*$, и $X^* = (x_1, \ldots, x_{T^0})$ можно представить в виде $m^*$ фрагментов длительности $T^*$:

$$X^* = (X^{(1)}, \ldots, X^{(m^*)}), \tag{1}$$

где $X^{(i)} = (x_{(i-1)T^*+1}, \ldots, x_{iT^*})$, $i = 1, \ldots, m^*$, причем векторы $\{X^{(i)}\}$ «мало отличаются» друг от друга. Рассмотрим задачу обнаружения последовательностей с такой структурой и оценивания величины квазипериода $T^*$.

Для обнаружения последовательностей вида (1) введем следующие две модели дискретных временных рядов (ДВР).

Модель векторной бинарной авторегрессии (VBAR):

$$X^{(i)} = X^{(i-1)} \oplus \Gamma^{(i)},\ i = 2, \ldots, m^*, \tag{2}$$

где $X^{(1)}$ – случайный вектор с равномерным на $A^{T^*}$ распределением вероятностей, $\{\Gamma^{(i)}, i=2,\dots,m^*\}$ – независимые одинаково распределенные случайные векторы.

Модель векторной бинарной регрессии (VBR) задается стохастическим уравнением

$$X^{(i)} = X^{(0)} \oplus \Gamma^{(i)},\ i=1,\dots,m^*, \tag{3}$$

где $X^{(0)}$ – случайный вектор с равномерным на $A^{T^*}$ распределением вероятностей, $\{\Gamma^{(i)}, i=1,\dots,m^*\}$ – независимые одинаково распределенные случайные векторы, $X^{(0)}$ неизвестен.

Везде далее будем предполагать, что $\Gamma^{(i)} = (\gamma_1^{(i)},\dots,\gamma_{T^*}^{(i)})$, $\{\gamma_j^{(i)},\ i=1,\dots,m^*,\ j=1,\dots,T^*\}$ – н.о.р.с.в. Бернулли, $\mathbf{P}=\{\gamma_j^{(i)}=1\}=\varepsilon\neq 1/2$.

Сформулируем задачу обнаружения квазипериода. По наблюдаемому участку последовательности $X=(x_1,\dots,x_n)$ длительности $n<T^0$ необходимо проверить гипотезу $H_0$: $x_t$ является равномерно распределенной случайной последовательностью (РРСП) [1] против альтернативы $H_1$: имеет место модель (1). Заметим, что гипотезу $H_1$ можно представить в виде $H_1=\bigcup_{T^*=2}^{\infty} H_{1,T^*}$, где гипотеза $H_{1,T^*}$: имеет место модель (1) с квазипериодом $T^*$.

Пусть $2\le T\le \lfloor n/2\rfloor$, тогда наблюдения $X=(x_1,\dots,x_n)$ можно представить в виде

$$X=(X^{(1)},\dots,X^{(m)},X^{(m+1)}),\ m=\lfloor n/T\rfloor,$$

где $X^{(i)}=(x_{(i-1)T+1},\dots,x_{iT})$, $i=1,\dots,m$, $X^{(m+1)}=(x_{mT+1},\dots,x_n)$.

Для проверки гипотез $H_0$, $H_1$ будем использовать статистики

$$Z_1(T)=\frac{1}{m-1}\sum_{i=2}^{m}\mathrm{wt}(X^{(i)}\oplus X^{(i-1)}),\ m=\lfloor n/T\rfloor,\ 2\le T_-\le T\le T_+\le\lfloor n/2\rfloor; \tag{4}$$

$$Z_2(T)=\min_{X^{(0)}\in A^T}\frac{1}{m}\sum_{i=1}^{m}\mathrm{wt}(X^{(i)}\oplus X^{(0)}),\ m=\lfloor n/T\rfloor,\ 2\le T_-\le T\le T_+\le\lfloor n/2\rfloor, \tag{5}$$

где $\mathrm{wt}(a)$ – вес Хэмминга бинарного вектора $a$; $T_-, T_+$ – некоторые априорно заданные границы для возможной величины квазипериода.

***Лемма 1.*** Статистика $Z_2(T)$ допускает эквивалентное (5) представление:

$$Z_2(T)=\frac{1}{m}\sum_{j=1}^{T}Z_{2,j}, \tag{6}$$

где $Z_{2,j}=\min\{\sum_{i=1}^{m}x_{(i-1)T+j}, m-\sum_{i=1}^{m}x_{(i-1)T+j}\}$.

Доказательство. Заметим, что

$$Z_2(T)=\frac{1}{m}\min_{(x_1^{(0)},\dots,x_T^{(0)})\in A^T}\sum_{i=1}^{m}\sum_{j=1}^{T}(x_{(i-1)T+j}\oplus x_j^{(0)})=\frac{1}{m}\sum_{j=1}^{T}\min_{x_j^{(0)}\in A}\sum_{i=1}^{m}(x_{(i-1)T+j}\oplus x_j^{(0)}).$$

Полученное соотношение и приводит к формуле (6). Отметим также, что минимум достигается при $X^{(0)}=(x_1^{(0)},\dots,x_{T^*}^{(0)})$, где

$$x_j^{(0)}=\mathbf{I}\{\sum_{i=1}^{m}x_{(i-1)T+j}>m/2\},\ j=1,\dots,T^*. \tag{7}$$

Здесь $\mathbf{I}\{a\}\in\{0,1\}$ – индикаторная функция события $a$.

Следующие две теоремы поясняют выбор статистик $Z_1$, $Z_2$.

***Теорема 1.*** *Пусть* $X=(x_1,\ldots,x_n)$ *– наблюдаемый фрагмент последовательности, определенной моделью VBAR (2), и* $T^*$ *известно, тогда оценка максимального правдоподобия (ОМП) параметра* $\varepsilon$ *имеет вид*

$$\widehat{\varepsilon}=(T^*)^{-1}Z_1(T^*).$$

Доказательство. Логарифмическая функция правдоподобия (ЛФП)

$$l_{\mathrm{VBAR}}(\varepsilon)=-T^*\ln 2+\sum_{j=2}^{m}\ln \mathrm{C}_{T^*}^{\mathrm{wt}(X^{(j)}\oplus X^{(j-1)})}+(m-1)\Big(Z_1(T^*)\ln\varepsilon+(T^*-Z_1(T^*))\ln(1-\varepsilon)\Big).$$

Решая задачу $l_{\mathrm{VBAR}}(\varepsilon)\to\max\limits_{\varepsilon\in[0,1]}$, приходим к утверждению теоремы. ■

***Теорема 2.*** *Пусть* $X=(x_1,\ldots,x_n)$ *– наблюдаемый фрагмент последовательности, определенной моделью VBR (3), и* $T^*$ *известно, тогда ОМП параметров* $\varepsilon$, $X^{(0)}$ *имеет вид*

$$\widehat{\varepsilon}=(T^*)^{-1}Z_2(T^*),$$

*а* $\widehat{X}^{(0)}$ *определяется по формуле (7).*

Доказательство. Заметим, что ЛФП может быть записана в виде

$$l_{\mathrm{VBR}}(\varepsilon,X^{(0)})=-T^*\ln 2+\sum_{j=1}^{m}\ln \mathrm{C}_{T^*}^{\mathrm{wt}(X^{(j)}\oplus X^{(0)})}+m\Big(Z_2(T^*,X^{(0)})\ln\varepsilon+(T^*-Z_2(T^*,X^{(0)}))\ln(1-\varepsilon)\Big),$$

где $Z_2(T^*,X^{(0)})=\sum_{j=1}^{m}\mathrm{wt}(X^{(j)}\oplus X^{(0)})/m$. Максимизируем вначале $l_{\mathrm{VBR}}$ по $\varepsilon$ и получаем $\widehat{\varepsilon}(X^{(0)})=Z_2(T^*,X^{(0)})/T^*$. Подставляем полученное значение $\varepsilon$ в формулу для ЛФП:

$$l_{VBR}(X^{(0)})=-T^*(\ln 2+m\ln T^*)+\sum_{j=1}^{m}\ln \mathrm{C}_{T^*}^{\mathrm{wt}(X^{(j)}\oplus X^{(0)})}+$$
$$+m(T^*-Z_2(T^*,X^{(0)}))\ln(T^*-Z_2(T^*,X^{(0)}))+mZ_2(T^*,X^{(0)})\ln Z_2(T^*,X^{(0)}).$$

Рассмотрим задачу $l_{\mathrm{VBR}}(X^{(0)})\to\max\limits_{X^{(0)}\in A^{T^*}}$. Зафиксируем все элементы вектора $X^{(0)}$, кроме $j$-го. Так как справедливо равенство

$$\sum_{j=1}^{m}\ln \mathrm{C}_{T^*}^{\mathrm{wt}(X^{(j)}\oplus X^{(0)})}=\ln\left(\frac{(T!)^m(mZ_2(T^*,X^{(0)}))!(mT^*-mZ_2(T^*,X^{(0)}))!}{(mT)!\prod_{j=1}^{m}\mathrm{wt}(X^{(j)}\oplus X^{(0)})!\prod_{j=1}^{m}(T^*-\mathrm{wt}(X^{(j)}\oplus X^{(0)}))!}\right),$$

то максимум ЛФП по $j$-му элементу вектора $X^{(0)}$ будет достигаться при $x_j^{(0)}=\mathbf{I}\{\sum_{i=1}^{m}x_{(i-1)T+j}>m/2\}$. ■

### 2. Вероятностные свойства статистик $Z_1$, $Z_2$

Сформулируем вначале результаты, позволяющие найти распределение вероятностей статистик $Z_1, Z_2$ в случае гипотезы $H_0$.

***Лемма 2.*** Если справедлива гипотеза $H_0$, то для любого $T$ и любых различных $1\le i,j\le m$

$$L\{\mathrm{wt}(X^{(i)}\oplus X^{(j)})\}=Bi(T,1/2),$$

где $L\{\eta\}$ – закон распределения вероятностей случайной величины $\eta$; $Bi(n, \alpha)$ – биномиальный закон распределения вероятностей с параметрами $n, \alpha$.

Доказательство. Обозначим $Y = X^{(i)} \oplus X^{(j)}$. Очевидно, что в случае гипотезы $H_0$ вектор $Y$ имеет равномерное на $A^T$ распределение вероятностей. Следовательно, случайная величина $\mathrm{wt}(Y)$ имеет биномиальное распределение с параметрами $T$ и 1/2. ■

***Лемма 3.*** Если справедлива гипотеза $H_0$, то для любого $T$ и различных $1 \le i, j, j' \le m$, случайные величины $\mathrm{wt}(X^{(i)} \oplus X^{(j)})$ и $\mathrm{wt}(X^{(i)} \oplus X^{(j')})$ независимы, однако случайные величины $\{\mathrm{wt}(X^{(i)} \oplus X^{(j)}),\ \mathrm{wt}(X^{(i)} \oplus X^{(j')}),\ \mathrm{wt}(X^{(j)} \oplus X^{(j')})\}$ зависимы в совокупности, причем

$$\mathbf{P}\{\mathrm{wt}(X^{(i)} \oplus X^{(j)}) = r_{ij}, \mathrm{wt}(X^{(i)} \oplus X^{(j')}) = r_{ij'}, \mathrm{wt}(X^{(j)} \oplus X^{(j')}) = r_{jj'}\} =$$
$$= \mathbf{I}\{\alpha \in \mathrm{N}\}\mathbf{I}\{r_{ij} \ge \alpha, r_{ij'} \ge \alpha\}\mathbf{I}\{r_{ij} + r_{ij'} + r_{jj'} \le 2T\}\frac{1}{2^{2T}}\frac{T!}{\alpha!(r_{ij} - \alpha)!(r_{ij'} - \alpha)!(r_{ij} + r_{ij'} - \alpha)!},$$

где $\alpha = (r_{ij} + r_{ij'} - r_{jj'})/2$.

Доказательство. Видно, что в условиях леммы

$$\mathbf{P}\{\mathrm{wt}(X^{(i)} \oplus X^{(j)}) = a, \mathrm{wt}(X^{(i)} \oplus X^{(j)}) = b\} = 2^{-2T},\ a, b \in A^T,$$

и случайные величины $X^{(i)} \oplus X^{(j)}$, $X^{(i)} \oplus X^{(j')}$ независимы. Следовательно, случайные величины $\mathrm{wt}(X^{(i)} \oplus X^{(j)})$, $\mathrm{wt}(X^{(i)} \oplus X^{(j')})$ независимы как борелевские функции независимых случайных величин [4]. Заметим, что

$$\mathbf{P}\{\mathrm{wt}(X^{(i)} \oplus X^{(j)}) = a, \mathrm{wt}(X^{(i)} \oplus X^{(j)}) = b, \mathrm{wt}(X^{(j)} \oplus X^{(j')}) = c\} = 2^{-2T}\mathbf{I}\{a \oplus b = c\},\ a, b, c \in A^T.$$

Из последнего равенства следует, что

$$\mathbf{P}\{\mathrm{wt}(X^{(i)} \oplus X^{(j)}) = r_{ij}, \mathrm{wt}(X^{(i)} \oplus X^{(j')}) = r_{ij'}, \mathrm{wt}(X^{(j)} \oplus X^{(j')}) = r_{jj'}\} =$$
$$= 2^{-2T}\sum_{a,b \in A^T}\mathbf{I}\{\mathrm{wt}(a) = r_{ij}, \mathrm{wt}(b) = r_{ij'}, \mathrm{wt}(a \oplus b) = r_{jj'}\}.$$

Вычисляя сумму в полученном соотношении, приходим к утверждению леммы. ■

***Следствие 1.*** *Если справедлива гипотеза $H_0$, то для любого $T$ случайные величины $\{\mathrm{wt}(X^{(2)} \oplus X^{(1)}),\ \mathrm{wt}(X^{(3)} \oplus X^{(2)}),\ldots,\ \mathrm{wt}(X^{(m)} \oplus X^{(m-1)})\}$ независимы в совокупности.*

***Лемма 4.*** Если справедлива гипотеза $H_0$, то для любого $T$ случайные величины $\{Z_{2,j},\ j = 1,\ldots,T\}$ независимы и их распределение имеет вид

$$\mathbf{P}\{Z_{2,j} = r \mid H_0\} = \begin{cases} 2^{-m+1}\mathrm{C}_m^r, & 0 \le r < m/2, \\ 2^{-m}\mathrm{C}_m^r, & r = m/2, \\ 0, & r > m/2. \end{cases} \qquad (8)$$

Доказательство. Случайные величины $\{Z_{2,j}\}$ независимы как борелевские функции независимых случайных величин [4]. Очевидно, что в случае гипотезы $H_0$ случайная величина $y_j = \sum_{i=1}^{m} x_{(i-1)T+j}$ имеет биномиальное распределение вероятностей с параметрами $m$ и 0,5. Учитывая, что $Z_{2,j} = \min\{y_j, m - y_j\}$, приходим к формуле (8). ■

***Теорема 3.*** *Если справедлива гипотеза $H_0$, то*

$$L\{(m-1)Z_1(T) \mid H_0\} = Bi((m-1)T, 1/2),\ 2 \le T \le \lfloor n/2 \rfloor; \qquad (9)$$

$$\mathbf{E}\{mZ_2(T)\,|\,H_0\} = T\mu_{Z2}(m),\ \mathbf{D}\{mZ_2(T)\,|\,H_0\} = T\sigma^2_{Z2}(m),\ 2 \le T \le \lfloor n/2 \rfloor, \tag{10}$$

*где* $\mu_{Z2,\varepsilon}(m)$, $\sigma^2_{Z2}(m)$ *– математическое ожидание и дисперсия случайной величины с распределением вероятностей (8). Более того, при* $T \to \infty$ *имеет место асимптотика:*

$$T^{-1}Z_2(T) \xrightarrow{\mathbf{P}=1} \mu_{Z2}(m)/m. \tag{11}$$

Доказательство. Утверждение (9) вытекает из следствия 1 и леммы 2. Утверждение (10) следует из независимости случайных величин $x_1,\ldots,x_n$ и леммы 3. Сходимость (11) вытекает из леммы 1 на основании леммы 3. ■

***Лемма 5.*** Если справедлива гипотеза $H_0$, $T_1 < T_2$ и $T_2 \ne kT_1$, то справедливы асимптотические выражения для коэффициентов корреляции

$$\mathbf{Corr}\{Z_1(T_1), Z_1(T_2)\} = 0;$$

$$\mathbf{Corr}\{Z_2(T_1), Z_2(T_2)\} \xrightarrow[n\to\infty]{} 0.$$

Доказательство. Докажем вначале первое утверждение леммы. Обозначим $m_i = \lfloor n/T_i \rfloor$, $i = 1,2$. В силу определения статистики $Z_1$ (4) получаем

$$\mathbf{E}\{Z_1(T_1)Z_1(T_2)\} = \frac{1}{(m_1-1)(m_2-1)} \sum_{i=2}^{m_1}\sum_{j=1}^{T_1}\sum_{l=2}^{m_2}\sum_{k=1}^{T_2} \mathbf{E}\{(x_{(i-1)T_1+j} \oplus x_{(i-2)T_1+j})(x_{(l-1)T_2+k} \oplus x_{(l-1)T_2+k})\}, \tag{12}$$

так как $(y_1 \oplus y_2)(y_3 \oplus y_4) = y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 - 2(y_1y_3y_4 + y_2y_3y_4 + y_1y_2y_3 + y_1y_2y_4) + 4y_1y_2y_3y_4$, и при $T_1$, $T_2$, удовлетворяющих условию леммы:

$$\mathbf{E}\{x_{(i-a)T_1+j}x_{(l-b)T_2+k}\} = (1 + \mathbf{I}\{(i-a)T_1 + j = (l-b)T_2 + k\})/4, \quad a,b = 1,2;$$

$$\mathbf{E}\{x_{(i-1)T_1+j}x_{(i-2)T_1+j}x_{(l-b)T_2+k}\} = (1 + \mathbf{I}\{\exists a \in \{1,2\} : (i-a)T_1 + j = (l-b)T_2 + k\})/8, \quad b = 1,2;$$

$$\mathbf{E}\{x_{(i-1)T_1+j}x_{(i-2)T_1+j}x_{(l-1)T_2+k}x_{(l-2)T_2+k}\} = (1 + \mathbf{I}\{\exists a,b \in \{1,2\} : (i-a)T_1 + j = (l-b)T_2 + k\})/16.$$

Подставляя соотношения для математических ожиданий в (12), находим $\mathbf{E}\{Z_1(T_1)Z_1(T_2)\} = T_1T_2/4$, следовательно, $\mathbf{Corr}\{Z_1(T_1), Z_1(T_2)\} = 0$.

Для доказательства второго утверждения леммы 5 способом, аналогичным примененному ранее, можно установить, что $\mathbf{E}\{Z_2(T_1), Z_2(T_2)\} = T_1T_2(0,25 + O(h(m_{\min})))$, где $m_{\min} = \min\{m_1, m_2\}$, $h(m) = 2^{-m}\mathrm{C}_m^{m/2}\mathbf{I}\{m \text{ четно}\} + 2^{-m+1}\mathrm{C}_{m-1}^{(m-1)/2}\mathbf{I}\{m \text{ нечетно}\}$. Учитывая, что $\mathbf{E}\{Z_2(T)\} = T(0,5 + h(m))$, $\mathbf{D}\{Z_2(T)\} = T\mathbf{D}\{Z_{2,j}(T)\} \ge 0,25m^{-2}T$,

$$\left|\mathbf{Corr}\{Z_2(T_1), Z_2(T_2)\}\right| = \left|\frac{\mathbf{E}\{Z_2(T_1), Z_2(T_2)\} - \mathbf{E}\{Z_2(T_1)\}\mathbf{E}\{Z_2(T_2)\}}{\sqrt{\mathbf{D}\{Z_2(T_1)\}\mathbf{D}\{Z_2(T_2)\}}}\right| \ge \sqrt{T_1T_2}\,m_1m_2O(h(m_{\min})) \xrightarrow[n\to\infty]{} 0. \blacksquare$$

Исследуем теперь свойства статистик $Z_1, Z_2$ в случае гипотезы $H_1$.

***Теорема 4.*** *Если имеет место одна из моделей VBAR, VBR и справедлива гипотеза* $H_{1,T^*}$, *то при* $T \ne kT^*$

$$\mathbf{E}\{Z_1(T) \mid E\{Z_1(T) \mid H_{1,T^*}\} = T/2\}, \tag{13}$$

*однако* $L\{(m-1)Z_1(T) \mid H_{1,T^*}\} \ne Bi((m-1)T, 1/2)$.

Доказательство. Докажем утверждение теоремы в случае модели VBAR. Заметим, что

$$\mathbf{E}\{Z_1(T) \mid H_{1,T^*}\} = \frac{1}{m-1}\sum_{i=1}^{m}\mathbf{E}\{X^{(i)} \oplus X^{(i-1)}\}.$$

Обозначим $Y = X^{(i)} \oplus X^{(i-1)}$, $i = 2,\ldots,m$, $Y = (y_1,\ldots,y_T)$. Если $T = kT^* + r$, $r \neq 0$, и справедлива гипотеза $H_{1,T^*}$, то вектор $Y$ можно представить в виде $y_j = x_{1+((i-1)T+j) \bmod T^*} \oplus$ $\oplus x_{1+((i-2)T+j) \bmod T^*} \oplus \gamma_{(i-1)T+j}$, $j = 1,\ldots,T$, причем для всех $j$ справедливо $1+((i-1)T+j) \bmod T^* \neq$ $\neq 1+(iT+j) \bmod T^*$. Следовательно, каждый из элементов вектора $Y$ принимает значение 1 с вероятностью 0,5. Таким образом,

$$\mathbf{E}\{\mathrm{wt}(Y)\} = \sum_{a \in A^T} \mathrm{wt}(a)\mathbf{P}\{Y = a\} = \sum_{a=(a_1,\ldots,a_T) \in A^T} (a_1 + \ldots + a_T)\mathbf{P}\{Y = a\} = \sum_{j=1}^{T}\sum_{a_j \in A} a_j \mathbf{P}\{y_j = a_j\} = T/2.$$

Из полученного равенства следует соотношение (13). В случае модели VBR формула (13) доказывается аналогично. ■

***Теорема 5.*** *Если имеет место модель VBAR и справедлива гипотеза* $H_{1,T^*}$, *то при* $T=kT^*$

$$L\{(m-1)Z_1(T) \mid H_{1,T^*}\} \neq Bi((m-1)T, \varepsilon)). \tag{14}$$

Доказательство. Обозначим $Y^{(i)} = (y_1^{(i)},\ldots,y_T^{(i)}) = X^{(i)} \oplus X^{(i-1)}$, $i = 2,\ldots,m$. Очевидно, что в случае модели VBAR и гипотезы $H_{1,T^*}$ при $T = kT^*$ элементы вектора $Y^{(i)}$ можно представить в виде $y_j^{(i)} = \gamma_{1+r}^{(ik+s)}$, где $j = sT^* + r$. Таким образом, элементы вектора $Y^{(i)}$ независимы и векторы $Y^{(2)},\ldots,Y^{(m)}$ независимы. Отсюда и следует утверждение теоремы. ■

***Лемма 5.*** Если имеет место модель *VBR* и справедлива гипотеза $H_{1,T^*}$, то при $T = kT^*$, $j \neq j' \bmod (T^*)^2$ величины $Z_{2,j}$, $Z_{2,j'}$ независимы, и при $j = 1,\ldots,T$ распределение $Z_{2j}$ имеет вид

$$\mathbf{P}\{Z_{2,j} = r \mid H_{1,T^*}\} = \begin{cases} \mathrm{C}_m^r(\varepsilon_*^r(1-\varepsilon_*)^{m-r} + \varepsilon_*^{m-r}(1-\varepsilon_*)^r), 0 \le r < m/2, \\ \varepsilon_*^r(1-\varepsilon_*)^{m-r}\mathrm{C}_m^r, r = m/2, \\ 0, r > m/2, \end{cases} \tag{15}$$

где $\varepsilon^* = 2\varepsilon(1-\varepsilon)$.

Доказательство. Заметим, что в условиях леммы случайная величина $Z_{2,j}$, $j=sT^*+r$, есть борелевская функция от случайных величин $x_{1+r}^{(0)}, \gamma_{1+r}^{(s)}, \gamma_{1+r}^{(T^*+s)},\ldots,\gamma_{1+r}^{((m-1)T^*+s)}$. Таким образом, если $j \neq j' \bmod (T^*)^2$, случайные величины $Z_{2,j}$, $Z_{2,j'}$ независимы [4]. Распределение случайной величины $Z_{2,j}$ находится аналогично лемме 3. ■

Отметим, что поскольку $n < m^*T^*$, то при $m^* < T^*$ статистика $Z_2$ при $T=kT^*$ является суммой попарно независимых одинаково распределенных случайных величин.

***Теорема 5.*** *Если имеет место модель VBR и справедлива гипотеза* $H_{1,T^*}$, *то при* $T=kT^*$

$$\mathbf{E}\{Z_1(T) \mid H_{1,T^*}\} = T\varepsilon(1-\varepsilon); \tag{16}$$

$$\mathbf{E}\{mZ_2(T) \mid H_{1,T^*}\} = T\mu_{Z2,\varepsilon}(m), \ \mathbf{D}\{mZ_2(T) \mid H_{1,T^*}\} = T\sigma_{Z2,\varepsilon}^2(m), \tag{17}$$

*где* $\mu_{Z2,\varepsilon}(m)$, $\sigma^2_{Z2,\varepsilon}(m)$ *– математическое ожидание и дисперсия случайной величины с распределением вероятностей (15). Более того, если* $T^*\to\infty$, *то*

$$(T^*)^{-1}Z(T^*)\xrightarrow{\mathbf{P}=1}\mu_{Z2,\varepsilon}(m)/m.$$

Доказательство. Обозначим $Y^{(i)}=(y_1^{(i)},\ldots,y_T^{(i)})=X^{(i)}\oplus X^{(i-1)}$, $i=1,\ldots,m$. Очевидно, что в случае модели VBR и гипотезы $H_{1,T^*}$ при $T=kT^*$ элементы вектора $Y^{(i)}$ можно представить в виде $y_j^{(i)}=\gamma_{1+r}^{((i-1)k+s)}\oplus\gamma_{1+r}^{(ik+s)}$, где $j=sT^*+r$. Отсюда и следует соотношение (16). Формула (17) справедлива в силу леммы 4 на основании леммы 1. ■

Доказанные свойства статистик $Z_1$, $Z_2$ позволяют построить алгоритмы оценки величины квазипериода и проверки гипотезы о наличии в последовательности квазипериода.

### 3. Идентификация моделей *VBR*, *VBAR*

Рассмотрим задачу статистического оценивания квазипериода $T^*$ по наблюдениям $X=(x_1,\ldots,x_n)$ длительности *n*. Построим оценки, используя статистики $Z_1$, $Z_2$ и установленные в разд. 2 их свойства:

$$\widehat{T}_{Z1}=\arg\max_{T_-\le T\le T_+}|T^{-1}(Z_1^0(T)-0,5)|,\ \widehat{T}_{Z2}=\arg\max_{T_-\le T\le T_+}|T^{-1}(Z_1^0(T)-\mu_{Z2}(m))|. \qquad (18)$$

Исследуем свойства предложенных оценок. Докажем вспомогательное утверждение.

***Лемма 7.*** Если для последовательностей случайных величин $\eta_{1,n},\ldots,\eta_{k,n}\in\mathbf{R}$, определенных на вероятностном пространстве $(\Omega,F,\mathbf{P})$, при $n\to\infty$ имеет место сходимость $\eta_{i,n}\xrightarrow{\mathbf{P}}0$, $i=1,\ldots,k-1$, $\eta_{k,n}\xrightarrow{\mathbf{P}}\alpha\ne0$, то для случайной величины $r_n=\arg\max|\eta_{i,n}|$ выполнено $\mathbf{P}\{r_n=k\}\xrightarrow[n\to\infty]{}1$.

Доказательство. Рассмотрим множества $A_{i,n}(\delta)=\{\omega\in\Omega:|\eta_{i,n}|<\delta\}$, $i=1,\ldots,k-1$, $A_{k,n}(\delta)=\{\omega\in\Omega:|\eta_{i,n}-\alpha|<\delta\}$. В силу определения сходимости по вероятности [4] выполнено: для любого $\delta>0$ $\rho_{i,n}(\delta)=1-\mathbf{P}\{A_{i,n}(\delta)\}\xrightarrow[n\to\infty]{}0$. Положим $\delta^*=|\alpha|/4$. Очевидно, что на множестве $A_n=\bigcap_{i=1}^k A_{i,n}(\delta^*)$ случайная величина $r_n$ принимает значение *k*. Следовательно,

$$P\{r_n=k\}\ge P\{A_n^*\}=1-P\{\overline{A}_n^*\}\ge1-\sum_{i=1}^k\rho_{i,n}(\delta^*).$$

Из полученной оценки и следует утверждение леммы. ■

***Теорема 6.*** *Если* $X=(x_1,\ldots,x_n)$ *– фрагмент последовательности, определяемой моделью VBAR (2), а* $T_-,T_+$ *таковы, что существует единственное* $k\in\mathbf{N}$, $T_-\le kT^*\le T_+$, *то имеет место сходимость* $\mathbf{P}\{\widehat{T}_{Z1}=kT^*\}\xrightarrow[n\to\infty]{}1$.

Доказательство. Из теорем 3, 4 следует, что $(kT^*)^{-1}(Z_1^0(kT^*)-0,5)\xrightarrow{\mathbf{P}=1}\varepsilon-0,5\ne0$, а при $T\ne kT^*$ $T^{-1}(Z_1^0(T)-0,5)\xrightarrow{\mathbf{P}}0$. Поэтому утверждение теоремы следует из леммы 7. ■

Аналогично доказывается следующая теорема.

***Теорема 7.*** *Если* $X=(x_1,\ldots,x_n)$ *– фрагмент последовательности, определяемой моделью VBR (3),* $T_-,T_+$ *таковы, что существует единственное* $k\in\mathbf{N}$, $T_-\le kT^*\le T_+$, *то имеет место сходимость* $\mathbf{P}\{\widehat{T}_{Z2}=kT^*\}\xrightarrow[n\to\infty]{}1$.

Таким образом, при выполнении условия {существует единственное $k\in\mathbf{N}$, $T_- \le kT^* \le T_+$} статистики (18) являются состоятельными оценками квазипериода. Заметим, что если $K = \{k \in \mathbf{N}, T_- \le kT^* \le T_+\}$, то аналогично доказательству леммы 5 и теоремы 6 можно показать:

$$P\{\widehat{T}_{ZS} \in K\} \xrightarrow[n\to\infty]{} 1,\ S=1,\ 2.$$

Построим на основе статистик $Z_1$, $Z_2$ статистические тесты проверки гипотезы $H_0$. Для проверки гипотезы $H_0$ будем использовать статистики

$$\widehat{T}^0_{Z1} = \arg\max_{T_-\le T\le T_+} |Z^0_1(T)|,\ \ Z^0_1(T) = \frac{2(m-1)Z_1(T) - (m-1)T}{\sqrt{(m-1)T}}; \tag{19}$$

$$\widehat{T}^0_{Z2} = \arg\max_{T_-\le T\le T_+} |Z^0_2(T)|,\ \ Z^0_2(T) = \frac{mZ_2(T) - T\mu_{Z2}}{\sqrt{T\sigma^2_{Z2}}}. \tag{20}$$

В силу леммы 4, при истинной гипотезе $H_0$ и $T_+ \le 2T_-$, статистики $Z^0_S(T_1)$, $Z^0_S(T_2)$ при $T_1 \ne T_2$ для любого $S$=1, 2 асимптотически некоррелированы, а в силу теоремы 3 статистика $Z^0_S(T)$ при $T_- \le T \le T_+$ имеет асимптотическое стандартное нормальное распределение вероятностей. Для построения статистических тестов потребуется вспомогательное утверждение.

***Теорема 8.*** *Если распределение вероятностей случайного вектора* $\vec{\eta} = (\eta_1,...,\eta_k) \in \mathbf{R}^k$ *является абсолютно непрерывным с плотностью* $p_\eta(y)$, $y\in\mathbf{R}^k$, *то распределение вероятностей случайной величины* $r = \arg\max\limits_{1\le j\le k} |\eta_j|$ *имеет вид*

$$\mathrm{P}\{r=j\} = \int_{-\infty}^{\infty} F_j(z)\mathrm{d}z, \qquad j=1,...,k; \tag{21}$$

$$F_j(z) = \int_{-|z|}^{|z|} ... \int_{-|z|}^{|z|} p_{\vec{\eta}}(y_1,...,y_{j-1},z,y_{j+1},...,y_k)\mathrm{d}y_1...\mathrm{d}y_{j-1}\mathrm{d}y_{j+1}...\mathrm{d}y_k,\ j=1,...,k,$$

*а плотность распределения вероятностей случайной величины* $\xi = \eta_r$

$$p_\xi(z) = \sum_{j=1}^{k} F_j(z), \qquad z\in\mathbf{R}. \tag{22}$$

Доказательство. Докажем вначале первое утверждение теоремы. Событие $\{r=j\}$ означает, что для любого $i\ne j$ $|\eta_1| < |\eta_k|$, поэтому

$$\{r=j\} = \left\{\vec{\eta}\in\mathbf{R}^k \mid \forall i\ne j \quad -|\eta_j| < \eta_i < |\eta_j|\right\}.$$

Из полученного представления и следует формула (18). Заметим, что

$$\mathbf{P}\{\xi \le z\} = \sum_{j=1}^{k} \mathbf{P}\{\xi \le z, r=j\} = \sum_{j=1}^{k} \mathbf{P}\{\eta_r \le z, r=j\}. \tag{23}$$

Очевидно, что $\{\eta_r \le z, r=j\} = \left\{\vec{\eta}\in\mathbf{R}^k \mid \eta_j \le z, \forall i\ne j, |\eta_i| < |\eta_j|\right\}$. Поэтому $\mathbf{P}\{\eta_r \le z, r=j\} = \int_{-\infty}^{z} F_j(x)\mathrm{d}x$. Подставляя полученное соотношение в (23), приходим к (21). ■

***Следствие 2.*** *Если* $\eta_1,...,\eta_k \in \mathbf{R}$ *– независимые случайные величины со стандартным нормальным законом распределения вероятностей, то для случайных величин r, ξ, определенных в теореме 7, выполнено*

$$\mathrm{P}\{r = j\} = k^{-1}, j = 1,...,k; \tag{24}$$

$$p_\xi(z) = kp_0(z)\left|2\Phi(z) - 1\right|^{k-1}, z \in \mathbf{R}, \tag{25}$$

*где $p_0(z)$ – плотность стандартного нормального распределения; $\Phi(z)$ – функция распределения вероятностей.*

Доказательство. Достаточно подставить в формулы (21), (22) плотность стандартного нормального распределения вероятностей. ■

***Следствие 3.*** *Пусть имеет место гипотеза $H_0$ и $T_+ \le 2T_-$, тогда, если статистики $\{Z_S^0(T), T = T_-,...,T_+\}$ при любом S=1, 2 асимптотически независимы,*

$$\mathrm{P}\{\widehat{T}_{ZS}^0 = j\} \xrightarrow[n\to\infty]{} \frac{1}{T_+ - T_- + 1}, j = T_-,...,T_+, S = 1,2; \tag{26}$$

$$L\{Z_S^0(\widehat{T}_{ZS}^0)\} \xrightarrow[n\to\infty]{} p_\xi, S = 1,2. \tag{27}$$

Следствие 3 позволяет построить статистический тест, имеющий (при $n\to\infty$) асимптотический размер $\alpha$:

$$d_S(X, T_-, T_+) = \begin{cases} H_0, \text{åñëè } |Z_S^0(\widehat{T}_{ZS})| \le \Delta_{\alpha/2}; \\ H_1, \text{åñëè íà÷å}, \end{cases} \tag{28}$$

где $S \in \{1, 2\}$, $\Delta_\beta$ – квантиль уровня $\beta$ распределения вероятностей, определенного формулой (25). В табл. 1 приведены значения $\Delta_{\alpha/2}$ при различных $\alpha$ и $T_+ - T_- + 1$.

Таблица 1

Значения величины $\Delta_{\alpha/2}$

| $T_+ - T_- + 1$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ |
|---|---|---|---|---|---|
| $\alpha = 0{,}05$ | 4,049 | 4,559 | 5,021 | 5,446 | 5,844 |
| $\alpha = 0{,}1$ | 3,877 | 4,405 | 4,881 | 5,317 | 5,721 |

Оценим мощность предложенных тестов. Рассмотрим вначале тест на основе статистики $Z_1$. Для мощности теста справедливо

$$\omega = \mathbf{P}\{d_1(X) = H_1 \mid H_1\} =$$
$$= \mathbf{P}\{\widehat{T} = T^* \mid H_1\}\mathbf{P}\{|Z_{Z1}^0(T^*)| > \Delta_{\alpha/2} \mid H_1\} + \mathbf{P}\{\widehat{T} \ne T^* \mid H_1\}\mathbf{P}\{d_1(X) = H_1 \mid H_1, \widehat{T} \ne T^*\}.$$

Поскольку в силу теоремы 6 при $n \to \infty$ имеет место асимптотика: $\mathbf{P}\{\widehat{T} = T^* \mid H_1\} = 1 - o(n)$, то $\omega = \mathbf{P}\{|Z_{Z1}^0(T^*)| > \Delta_{\alpha/2} \mid H_1\} + o(n)$. На основании теоремы 5 и теоремы Муавра – Лапласса [4] получаем, что в качестве оценки функции распределения случайной величины $Z_{Z1}^0(T^*)$ можно использовать функцию распределения нормального закона распределения вероятностей с математическим ожиданием $\sqrt{(m-1)T^*}(2\varepsilon - 1)$ и дисперсией $4\varepsilon(1-\varepsilon)$. Следовательно,

$$\omega \approx 1-\Phi\left(\frac{-\sqrt{(m-1)T^*}(2\varepsilon-1)+\Delta_{\alpha/2}}{2\sqrt{\varepsilon(1-\varepsilon)}}\right)+\Phi\left(\frac{-\sqrt{(m-1)T^*}(2\varepsilon-1)-\Delta_{\alpha/2}}{2\sqrt{\varepsilon(1-\varepsilon)}}\right). \quad (29)$$

В табл. 2 приведены наименьшие значения $n$, при которых оценка мощности (29) теста (28) превышает 0,999 для теста на основе статистики $Z_1^0$ при $\alpha$=0,05, $T_+ - T_- + 1 = 10^6$. Из табл. 2 следует, что объем данных, необходимых для эффективного проведения теста, в большей степени определяется величиной $|\varepsilon - 0{,}5|$, чем $T^*$.

Аналогичным образом для мощности теста на основе статистики $Z_2^0$ можно получить

$$\omega \approx 1-\Phi\left((-\sqrt{T^*/\sigma^2_{Z2}(m)}(\mu_{Z2,\varepsilon}(m)-\mu_{Z2}(m))+\Delta_{\alpha/2})/\sqrt{\sigma^2_{Z2,\varepsilon}(m)/\sigma^2_{Z2}(m)}\right)+$$
$$+\Phi\left((-\sqrt{T^*/\sigma^2_{Z2}(m)}(\mu_{Z2,\varepsilon}(m)-\mu_{Z2}(m))-\Delta_{\alpha/2})/\sqrt{\sigma^2_{Z2,\varepsilon}(m)/\sigma^2_{Z2}(m)}\right). \quad (30)$$

В табл. 3 приведены наименьшие значения $n$, при которых оценка мощности (30) теста (28) превышает 0,999 для теста на основе статистики $Z_2^0$ при $\alpha$=0,05, $T_+ - T_- + 1 = 10^6$. Отметим, что для эффективного проведения теста на основе статистики $Z_1^0$ требуется значительно меньше наблюдений, чем для теста на основе статистики $Z_2^0$.

Таблица 2

Оценка числа наблюдений для использования теста на основе статистики $Z_1^0(T)$

| $T^*$ | $2^{10}$ | $2^{13}$ | $2^{15}$ | $2^{17}$ | $2^{20}$ |
|---|---|---|---|---|---|
| $\|\varepsilon-0{,}5\|=0{,}05$ | $2^{13,17}$ | $2^{14}$ | $2^{16}$ | $2^{18}$ | $2^{21}$ |
| $\|\varepsilon-0{,}5\|=0{,}01$ | $2^{14,17}$ | $2^{17,59}$ | $2^{17,81}$ | $2^{18,59}$ | $2^{21}$ |
| $\|\varepsilon-0{,}5\|=0{,}001$ | $2^{24,12}$ | $2^{24,12}$ | $2^{24,12}$ | $2^{24,13}$ | $2^{24,25}$ |

Таблица 3

Оценка числа наблюдений для использования теста на основе статистики $Z_2^0(T)$

| $T^*$ | $2^{10}$ | $2^{13}$ | $2^{15}$ | $2^{17}$ | $2^{20}$ |
|---|---|---|---|---|---|
| $\|\varepsilon-0{,}5\|=0{,}05$ | $2^{14,89}$ | $2^{16,91}$ | $2^{18,17}$ | $2^{19,59}$ | $2^{22}$ |
| $\|\varepsilon-0{,}5\|=0{,}01$ | $2^{17,84}$ | $2^{19,84}$ | $2^{21,21}$ | $2^{22,49}$ | $2^{24,52}$ |
| $\|\varepsilon-0{,}5\|=0{,}001$ | $2^{22,28}$ | $2^{24,25}$ | $2^{25,57}$ | $2^{26,91}$ | $2^{28,91}$ |

**4. Алгоритм оценивания квазипериода**

Полученные ранее результаты позволяют построить алгоритм оценивания квазипериода. Входными данными алгоритма являются $X=(x_1,\ldots,x_n)$ – наблюдаемый фрагмент двоичной последовательности и величина $T_+ \le n/2$ – некоторое максимально возможное значение величины квазипериода.

1. Полагаем $T_- = \lfloor T_+/2 \rfloor + 1$.

2. При выбранных $T_-, T_+$ по наблюдениям $X$ проверяем гипотезу $H_0$, используя тест (23).

3. Если принимается гипотеза $H_0$, то алгоритм заканчивает работу с результатом «квазипериод отсутствует».

4. Если принимается гипотеза $H_1$, находим оценку величины квазипериода $\widehat{T}$.

5. Если $\widehat{T}$ – простое число, то алгоритм заканчивает работу с результатом «квазипериод равен $\widehat{T}$».

6. Если $\widehat{T}$ – составное число, то находим $T^1$ – наибольший делитель $\widehat{T}$ – и выполняем алгоритм рекурсивно, положив $T_+ = T^1$.

7. Если вызванный рекурсивно алгоритм закончил работу с результатом «квазипериод отсутствует», то алгоритм заканчивает работу с результатом «квазипериод равен $\widehat{T}$ ».

8. Если иначе, то результатом работы алгоритма является результат вызванного рекурсивно алгоритма.

Заметим, что вычислительная сложность этого алгоритма есть $O(nT_+ \log_{T^*}(n))$.

### 5. Результаты численных экспериментов

В разд. 3 для нахождения асимптотического ($n\to\infty$) распределения статистик (19), (20), которое необходимо для построения статистического теста, было использовано предположение о том, что статистики $\{ Z_S^0(T), T = T_-,\ldots,T_+ \}$ при $S$=1, 2 в случае гипотезы $H_0$ асимптотически независимы. Для подтверждения этого предположения был проведен ряд экспериментов. Методом Монте-Карло оценивалось распределение вероятностей статистик $Z_S^0(\widehat{T}_{ZS}^0)$, $S$=1, 2. В качестве исходных данных для экспериментов использовались «истинно случайные» последовательности [5]. Гистограмма распределения статистики $Z_1^0(\widehat{T}_{Z1}^0)$ (рис. 1) построена по 5000 фрагментам длительности $n = 3000$ при $T_- = 500$, $T_+ = 1000$. Гистограмма распределения вероятностей статистики $Z_2^0(\widehat{T}_{Z2}^0)$ (рис. 2) построена по 5000 фрагментам длительности $n = 6000$. На обоих рисунках для сравнения приведен график теоретической плотности распределения вероятностей. Как видно из рис. 1 и 2, результаты численных экспериментов подтверждают предположение об асимптотической независимости.

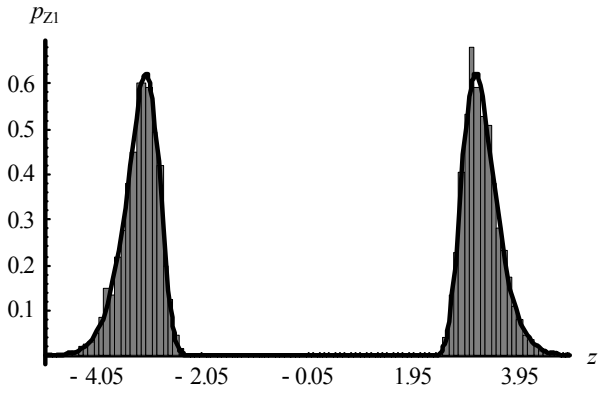


Рис. 1. Гистограмма распределения вероятностей статистики $Z_1^0(\widehat{T}_{Z1}^0)$ в случае гипотезы $H_0$ и теоретическое распределение вероятностей в случае гипотезы $H_0$

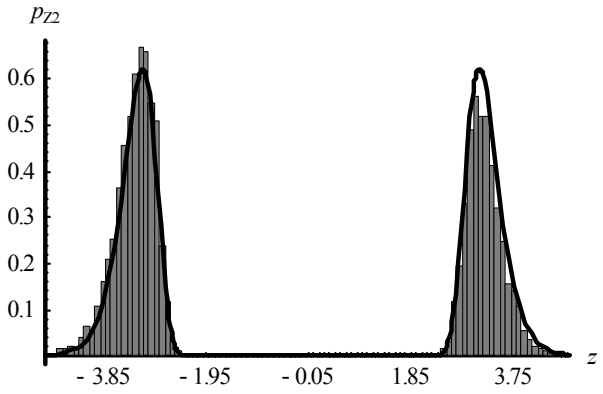


Рис. 2. Гистограмма распределения вероятностей статистики $Z_2^0(\widehat{T}_{Z2}^0)$ в случае гипотезы $H_0$ и теоретическое распределение вероятностей в случае гипотезы $H_0$

Гистограмма распределения вероятностей статистики $Z_1^0(T)$ (рис. 3) построена по 5000 фрагментам длительности $n=12000$ при $T_-=500$, $T_+=1000$ в случае, когда наблюдаемая последовательность описывается моделью VBAR (2) при $T^*=800$, $\varepsilon=0,48$. Для сравнения на рисунке также приведен график теоретической плотности распределения вероятностей статистики в случае гипотезы $H_0$. Рис. 3 подтверждает высокую эффективность предложенных статистических тестов. На рис. 4 показана оценка мощности теста в зависимости от длительности наблюдаемой последовательности при $T^*=800$, $\varepsilon=0,48$, $T_-=500$, $T_+=1000$.

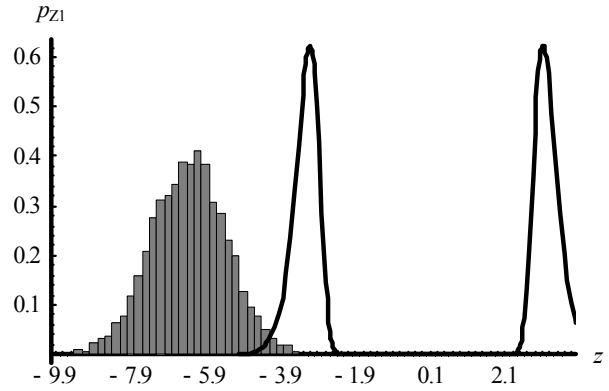


Рис. 3. Гистограмма распределения вероятностей статистики $Z_1^0(\bar{T}_{Z1}^0)$ в случае гипотезы $H_1$ и теоретическое распределение вероятностей в случае гипотезы $H_0$

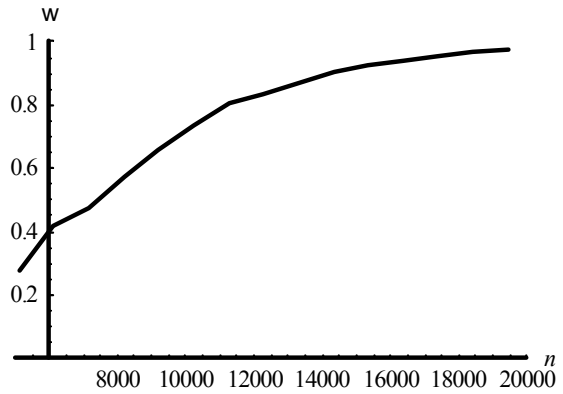


Рис. 4. Оценка мощности теста на основе статистки $Z_1$

**Заключение**

Для моделей VBR и VBAR построены методы статистического оценивания параметров и тесты проверки гипотезы о наличии в последовательности квазипериода, исследованы свойства предложенных оценок и даны оценки мощности построенных тестов. Разработаны новые методы обнаружения квазипериодов в бинарных последовательностях, сделаны оценки вычислительной сложности предложенных методов. Особенностью новых методов является возможность их использования в отсутствие какой-либо информации о генераторе, породившем наблюдаемую последовательность.

Работа поддержана Государственной программой фундаментальных исследований «Математические модели» (проект ММ-24).

**Список литературы**

1. Математические и компьютерные основы криптологии / Ю.С. Харин [и др.]. – Минск: Новое знание, 2003.

2. Zeng, K. On the Linear Syndrome Method in Cryptoanalysis / K. Zeng, M. Huang // Proc. of the Int. Cryptology Conf. on Advances in Cryptology. – Santa Barbara, USA, 1988. – P. 469–478.

3. Zeng, K. On the Linear Consistency Test (LCT) in Cryptanalysis with Applications / K. Zeng, C.-H. Yang, T.R.N. Rao // Proc. of the Int. Cryptology Conf. on Advances in Cryptology. – Santa Barbara, USA, 1989. – P. 164–174.

4. Боровков, А.А. Теория вероятностей / А.А. Боровков. – М.: Наука, 1986.

5. Marsaglia, G. The Marsaglia Random Number CDROM / G. Marsaglia. – Supercomputer Computations Research Institute and Department of Statistics, Florida State University, 1995.

**Поступила 29.04.2008**

*Научно-исследовательский институт*
*прикладных проблем математики и информатики,*
*Минск, пр. Независимости, 4*
*e-mail: and_yarmola@tut.by*

**A.N. Yarmola**

## DETECTION OF QUASI PERIODS IN BINARY SEQUENCES

New methods and algorithms of quasi period detection in binary sequences are proposed. Properties of the new methods are investigated. Estimates of algorithm computational complexity and results of computational experiments are presented.