

ДВА КРИТЕРИЯ ДЛЯ ПРОВЕРКИ СЛОЖНОЙ ГИПОТЕЗЫ О ПАРАМЕТРАХ БИНАРНОЙ ЦЕПИ МАРКОВА

А. Л. Костевич, А. С. Шмуратко

*Научно-исследовательский институт
прикладных проблем математики и информатики БГУ
Минск, Беларусь
E-mail: shmuratko@bsu.by*

Для бинарной последовательности рассматривается сложная нулевая гипотеза, соответствующая «небольшому» отклонению последовательности от модели независимых симметричных испытаний Бернулли и описываемая стационарной цепью Маркова первого порядка (с двумя параметрами). В работе предлагаются два критерия для проверки параметров указанной цепи Маркова. Исследуются свойства предложенных критериев как при нулевой гипотезе, так и в определенном классе альтернатив.

Ключевые слова: бинарная цепь Маркова, сложная гипотеза.

ПОСТАНОВКА ЗАДАЧИ

Пусть имеется выходная последовательность некоторого источника бинарных данных:

$$X_1, X_2, \dots, X_n, \quad X_i \in \{0, 1\}. \quad (1)$$

Для применения в области защиты информации, имитационного моделирования и т.п. этот источник стремятся сделать таким, чтобы порождаемая им последовательность была «как можно ближе» к чисто случайной, т.е. к последовательности независимых, равномерно распределенных на множестве $\{0, 1\}$ величин. Свойства источника в этом случае исключают явно «большие» отклонения порождаемой последовательности от чисто случайной; остаются, таким образом, «небольшие» отклонения. По своему типу это могут быть отклонения как от независимости, так и от равномерности. В результате совокупность наших предположений относительно последовательности (1) можно сформулировать следующим образом [1]:

- 1) зависимость между битами последовательности (1) ограничивается тем, что очередной бит зависит не от всех предыдущих, а только от последнего бита;
- 2) распределение каждого бита близко к равномерному;
- 3) кроме того, будем предполагать, что средние характеристики выходной последовательности источника (математическое среднее, ковариация на фиксированном лаге) не меняются во времени.

Сформулированные предположения приводят нас к следующей математической модели последовательности (1): X_1, X_2, \dots, X_n – стационарная цепь Маркова первого поряд-

ка со стационарным распределением π и матрицей вероятностей одношаговых переходов P следующего вида:

$$M: \quad \pi = \left(\frac{1}{2} - \varepsilon \quad \frac{1}{2} + \varepsilon \right), \quad P = \begin{pmatrix} \frac{1}{2} - \varepsilon_0 & \frac{1}{2} + \varepsilon_0 \\ \frac{1}{2} + \varepsilon_1 & \frac{1}{2} - \varepsilon_1 \end{pmatrix}.$$

В силу стационарности величины ε , ε_0 и ε_1 оказываются связанными следующим соотношением:

$$\varepsilon = \frac{1}{2} \frac{\varepsilon_0 - \varepsilon_1}{1 + \varepsilon_0 + \varepsilon_1}.$$

Таким образом, модель M однозначно определяется двумя параметрами: ε_0 и ε_1 .

Из сказанного выше следует, что относительно последовательности (1), в предположении, что для неё справедлива модель M , нам нужно проверить нулевую гипотезу о «небольших» отклонениях, то есть гипотезу вида:

$$H_0: |\varepsilon_0| \leq \varepsilon, \quad |\varepsilon_1| \leq \varepsilon, \quad (2)$$

где границу ε будем считать заданной. Требуется построить набор критериев для проверки гипотезы H_0 против разумно выбранной альтернативной гипотезы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Прежде всего, зададимся вопросом: какие критерии выбрать? Для этого заметим, что в модели M можно выделить два «крайних» случая, при которых достигается граница ($|\varepsilon_0| = |\varepsilon_1| = \varepsilon$) нулевой гипотезы. Эти два случая соответствуют двум вышеупомянутым типам отклонений от модели чистой случайности и описываются следующими частными случаями модели M :

$$M_1: \quad \pi = (1-p \quad p), \quad P = \begin{pmatrix} 1-p & p \\ 1-p & p \end{pmatrix}; \quad M_2: \quad \pi = \left(\frac{1}{2} \quad \frac{1}{2} \right), \quad P = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Теперь заметим, что если бы вместо модели M имела место более простая модель M_1 , то для проверки нулевой гипотезы вида $\left| p - \frac{1}{2} \right| \leq \varepsilon$ против альтернативы $\left| p - \frac{1}{2} \right| > \varepsilon$ равномерно наиболее мощный несмещенный критерий – это критерий знаков (или монобит), основанный на количестве единиц в последовательности (1). Если же принять модель M_2 , то для проверки той же нулевой гипотезы против той же альтернативы равномерно наиболее мощный несмещенный критерий – это критерий знакоперемен, основанный на количестве перемен знака (вида 01 ил 10) в последовательности (1).

По этой причине два указанных критерия и были нами включены в предлагаемый набор критериев для проверки нулевой гипотезы H_0 вида (2). В качестве альтернативы пока будем рассматривать альтернативу общего вида: $H_1 = \overline{H_0}$. Функцию мощности критерия при фиксированной гипотезе $H = H(\varepsilon_0, \varepsilon_1)$ будем обозначать через $\beta(H)$ либо $\beta(\varepsilon_0, \varepsilon_1)$.

Приведем описание критериев и их свойства как при нулевой гипотезе H_0 , так и для определенного класса альтернатив.

1. Критерий знаков.

Критерий основан на количестве единиц в последовательности (1). Статистика критерия

$$S_n = \sum_{i=1}^n X_i.$$

Критерий знаков имеет вид:

$$\text{принимается} \begin{cases} H_0 : \text{если } \Delta \leq S_n \leq n - \Delta; \\ H_1 : \text{в противном случае.} \end{cases}$$

Порог Δ равен

$$\Delta = \left[n \left(\frac{1}{2} - \varepsilon_* \right) - q \sqrt{n} \sqrt{\frac{1}{4} - \varepsilon_*^2} \right].$$

Здесь $[\cdot]$ – целая часть числа сверху, $q = \Phi^{-1} \left(1 - \frac{\alpha}{2} \right)$ – квантиль стандартного нормального распределения, α – требуемый уровень значимости критерия.

Теорема 1 даёт уровень значимости критерия, теорема 2 – поведение функции мощности критерия в различных областях значений параметров ε_0 и ε_1 .

Теорема 1. Пусть выполнены условия:

$$\varepsilon_* < \frac{1}{4} \quad \text{и} \quad \sqrt{n} > q \frac{1 + 4\varepsilon_*^2}{\sqrt{1 - 4\varepsilon_*^2}}.$$

Тогда уровень значимости критерия знаков лежит в интервале $\left(\frac{\alpha}{2}, \alpha \right]$:

$$\sup_{H \in \Pi_n} \beta(H) \in \left(\frac{\alpha}{2}, \alpha \right]$$

(с точностью до используемой в расчетах нормальной аппроксимации).

Замечание 1. Условия теоремы 1 не являются ограничительными для приложений.

Замечание 2. При $\varepsilon_* = 0$ (модель чистой случайности) уровень значимости критерия знаков равен α . При $\varepsilon_* \neq 0$ можно ожидать, что с ростом n уровень значимости приближается к $\alpha/2$.

Теорема 2. Пусть имеет место гипотеза $H = H(\varepsilon_0, \varepsilon_1) \in M$. Тогда справедливы следующие асимптотические свойства критерия знаков.

1) Если $|\varepsilon| < \varepsilon_*$, то для любого $\delta > 0$ существует такое N , что для всех $n \geq N$

$$\beta(\varepsilon_0, \varepsilon_1) \leq e^{-n \left(\ln \frac{1}{1-\alpha} - \delta \right)}.$$

2) Если $|\varepsilon| > \varepsilon_*$, то для любого $\varepsilon' \in (\varepsilon_*, |\varepsilon|)$ и любого $\delta > 0$ существует такое N , что для всех $n \geq N$

$$1 - \beta(\varepsilon_0, \varepsilon_1) \leq e^{-n \left(\ln \frac{1}{1-\alpha'} - \delta \right)}.$$

Здесь

$$a = a(\varepsilon_0, \varepsilon_1, \varepsilon_*) = \left(\sqrt{(0.5 + \varepsilon_*)(0.5 + \varepsilon_{\min})} - \sqrt{(0.5 - \varepsilon_*)(0.5 + \varepsilon_{\max})} \right),$$

$$a' = a(\varepsilon_0, \varepsilon_1, \varepsilon'_*), \quad \varepsilon_{\min} = \min\{\varepsilon_0, \varepsilon_1\}, \quad \varepsilon_{\max} = \max\{\varepsilon_0, \varepsilon_1\}.$$

2. Критерий знакоперемен.

Для того чтобы исследовать только зависимость между соседними символами, для критерия знакоперемен вместо двухпараметрической модели M мы рассматриваем более узкую – однопараметрическую – модель M_2 , приведенную выше. В случае двухпараметрической модели M расчет параметров критерия знакоперемен является затруднительным.

Для удобства и единообразия будем вместо вероятности p в определении модели M_2 использовать отклонение ε вероятности p от 0.5: $p = 0.5 + \varepsilon$. Таким образом, модель M_2 определяется одним параметром – ε . Нулевая гипотеза в этом случае будет иметь вид: $H'_0: |\varepsilon| \leq \varepsilon_*$, альтернатива: $H'_1: |\varepsilon| > \varepsilon_*$. Мы используем штрих, чтобы указать на то, что рассматривается более узкая модель.

Критерий знакоперемен основан на количестве перемен знака в последовательности (1). *Переменной знака* называется всякая переменная значения в последовательности бит: с 0 на 1 или обратно, с 1 на 0. Статистика критерия

$$S_n = \sum_{i=1}^{n-1} I(X_i \neq X_{i+1}).$$

Заметим, что S_n в рамках модели M_2 имеет биномиальное распределение с параметрами $(n-1, 0.5 + \varepsilon)$. Отсюда естественным образом получается структура критерия и все его свойства как при H'_0 , так и при H'_1 .

Итак, критерий знакоперемен имеет вид:

$$\text{принимается} \begin{cases} H'_0: \text{если } \Delta \leq S_n \leq n-1-\Delta; \\ H'_1: \text{в противном случае.} \end{cases}$$

Порог Δ равен

$$\Delta = \max \left\{ d \in N : \Phi \left(\frac{d - m_1}{\sigma} \right) + \Phi \left(\frac{d - m_2}{\sigma} \right) \leq \alpha \right\}. \quad (3)$$

Здесь α – требуемый уровень значимости критерия,

$$m_1 = (n-1) \left(\frac{1}{2} + \varepsilon_* \right), \quad m_2 = (n-1) \left(\frac{1}{2} - \varepsilon_* \right), \quad \sigma = \sqrt{n-1} \sqrt{\frac{1}{4} - \varepsilon_*^2}.$$

Отметим, что время нахождения порога из соотношения (3) имеет порядок $O(\log_2 n)$. Можно было бы использовать точное (биномиальное) распределение для нахождения порога Δ , однако нам будет удобнее оперировать соотношением (3).

Две следующие теоремы аналогичны теоремам 1 и 2.

Теорема 3. Критерий знакоперемен имеет уровень значимости α :

$$\sup_{H \in H'_0} \beta(H) \leq \alpha$$

(с точностью до используемой в расчетах нормальной аппроксимации).

Теорема 4. Функция мощности $\beta(\varepsilon)$ критерия имеет минимум в точке $\varepsilon = 0$ и монотонно возрастает с ростом $|\varepsilon|$. Кроме того, справедливы следующие неравенства:

1) Если $|\varepsilon| < \varepsilon_*$, то при $n \rightarrow \infty$

$$\beta(\varepsilon) \leq e^{-2n((\varepsilon_0 - |\varepsilon|)^2 + O(n^{-1/2}))}$$

2) Если $|\varepsilon| > \varepsilon_*$, то при $n \rightarrow \infty$

$$1 - \beta(\varepsilon) \leq e^{-2n((\varepsilon_0 + |\varepsilon|)^2 + O(n^{-1/2}))}$$

ДОКАЗАТЕЛЬСТВА

Доказательство теоремы 1. Пусть имеет место гипотеза $H \in H_0$. Согласно центральной предельной теореме для цепи Маркова [2, теорема 19.1.1] нормированная статистика S_n имеет асимптотическое стандартное нормальное распределение:

$$\frac{S_n - \sum_{i=1}^n EX_i}{\sigma\sqrt{n}} \rightarrow N(0,1), \quad n \rightarrow \infty.$$

Здесь $EX_i = 0.5 + \varepsilon$ и

$$\sigma^2 = DX_1 + 2 \sum_{i \geq 1} \text{cov}(X_1, X_{i+1}) = \frac{1}{4} \frac{(1+2\varepsilon_0)(1+2\varepsilon_1)(1-\varepsilon_0-\varepsilon_1)}{(1+\varepsilon_0+\varepsilon_1)^3}.$$

Тогда уровень значимости критерия знаков можно представить в следующем виде:

$$\beta(H) = P(S_n < \Delta) + P(S_n > n - \Delta) \approx \Phi\left(\frac{\Delta - n(0.5 + \varepsilon)}{\sigma\sqrt{n}}\right) + \Phi\left(\frac{\Delta - n(0.5 - \varepsilon)}{\sigma\sqrt{n}}\right).$$

Найти супремум $\beta(H)$ по всем $H \in H_0$ оказывается трудно, поэтому мы воспользуемся очевидной оценкой сверху:

$$\sup_{H \in H_0} \beta(H) \leq \sup_{H \in H_0} \Phi\left(\frac{\Delta - n(0.5 + \varepsilon)}{\sigma\sqrt{n}}\right) + \sup_{H \in H_0} \Phi\left(\frac{\Delta - n(0.5 - \varepsilon)}{\sigma\sqrt{n}}\right).$$

Использование этой оценки, к сожалению, может снизить действительный размер критерия до $\alpha/2$, что и отражено в формулировке теоремы. Далее, поскольку каждой гипотезе $H = H(\varepsilon_0, \varepsilon_1) \in H_0$ можно поставить в соответствие гипотезу $H' = H(\varepsilon_1, \varepsilon_0) \in H_0$ и при этом величинам ε и σ из H будут соответствовать величины $-\varepsilon$ и σ из H' , получаем, что супремумы в последнем выражении равны между собой. Так что порог Δ можно искать из соотношения:

$$2 \sup_{H \in H_0} \Phi\left(\frac{\Delta - n(0.5 - \varepsilon)}{\sigma\sqrt{n}}\right) = \alpha,$$

которое равносильно следующему:

$$\Delta = \frac{1}{2} \left(n - \sqrt{n} \sup_{H \in H_0} (2\varepsilon\sqrt{n} + 2g\sigma) \right). \quad (4)$$

Лемма 1. Пусть выполнено первое из условий теоремы 1. Тогда функция $\sigma = \sigma(\varepsilon_0, \varepsilon_1)$ убывает по ε_0 и по ε_1 , а функция $\varepsilon = \varepsilon(\varepsilon_0, \varepsilon_1)$ возрастает по ε_0 и убывает по ε_1 .

Доказательство леммы получается взятием производных.

Из леммы 1 следует, что нужно положить $\varepsilon_1 = -\varepsilon_0$, что в дальнейшем мы и считаем выполненным. Тогда задача сводится к максимизации функции одной переменной. Введем для этой функции отдельное обозначение:

$$f(x) = \sqrt{n} \frac{x + \varepsilon_0}{1 + x - \varepsilon_0} + q \sqrt{\frac{(1 + 2x)(1 - 2\varepsilon_0)(1 - x + \varepsilon_0)}{(1 + x - \varepsilon_0)^3}}.$$

Лемма 2. Пусть выполнены условия теоремы 1. Тогда функция $f(x)$ является возрастающей на отрезке $-\varepsilon_0 \leq x \leq \varepsilon_0$.

Доказательство леммы 2 носит технический характер и поэтому здесь опускается. (Доказательство основано на последовательном взятии и изучении производных $f(x)$.)

Из леммы 2 следует, что

$$\sup_{|x| \leq \varepsilon_0} f(x) = f(\varepsilon_0) = 2\varepsilon_0 \sqrt{n} + q \sqrt{1 - 4\varepsilon_0^2}.$$

Подставляя это в соотношение (4), получаем искомый порог Δ . Теорема 1 доказана.

Доказательство теоремы 2. Воспользуемся теорией больших уклонений для цепи Маркова [3, глава IV].

Вначале рассмотрим случай, когда $|\varepsilon| < \varepsilon_0$. Используя определение порога Δ , имеем следующую оценку для функции мощности:

$$\beta(\varepsilon_0, \varepsilon_1) \leq P(S_n \leq n(0.5 - \varepsilon_0)) + P(S_n \geq n(0.5 + \varepsilon_0)) = P(L_n \in \tilde{A}).$$

Здесь

$$L_n = (L_n(0), L_n(1)) = \left(\frac{1}{n} \sum_{i=1}^n I(X_i = 0), \frac{1}{n} \sum_{i=1}^n I(X_i = 1) \right) -$$

эмпирическое распределение выборки X_1, X_2, \dots, X_n , а множество \tilde{A} имеет вид:

$$\tilde{A} = \{(1-p, p) : p \leq 0.5 - \varepsilon_0 \text{ или } p \geq 0.5 + \varepsilon_0\}.$$

Вместо двумерного множества \tilde{A} , которое описывается одним параметром p , нам будет удобнее оперировать соответствующим одномерным множеством

$$A = \{p : p \leq 0.5 - \varepsilon_0 \text{ или } p \geq 0.5 + \varepsilon_0\}.$$

Основным инструментом доказательства теоремы 2 служит следующая теорема.

Теорема 5 [3, теоремы IV.6, IV.7]. Пусть имеется стационарная бинарная цепь Маркова, описываемая моделью M . И пусть \tilde{S} — произвольное замкнутое подмножество множества $\{(1-p, p) : p \in [0, 1]\}$. Тогда для вероятности больших уклонений справедливо следующее неравенство:

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \ln P(L_n \in \tilde{S}) \leq -I(\tilde{S}),$$

где функция скорости $I(\tilde{S})$ имеет вид:

$$I(\tilde{S}) = I(S) = \inf_{p \in \tilde{S}} \sup_{x > 0} \left(-(1-p) \ln \left(1 + p_{01} \left(\frac{1}{x} - 1 \right) \right) - p \ln(1 + p_{10}(x-1)) \right) = \inf_{p \in \tilde{S}} \sup_{x > 0} f(p, x).$$

Здесь для краткости мы обозначили через p_{ij} элементы матрицы переходных вероятностей: $p_{ij} = P(X_{t+1} = j | X_t = i)$. Через S обозначено, как и ранее, сокращение двумерного множества \tilde{S} до одномерного: $p \in S \Leftrightarrow (1-p, p) \in \tilde{S}$.

Таким образом, нам остается оценить сверху величину $-I(A)$. Используя неравенство $(1-p)(-\ln x) + p(-\ln y) \geq -\ln((1-p)x + py)$ (для $x, y > 0, p \in [0, 1]$), имеем:

$$f(p, x) \geq -\ln\left((1-p)\left(1 + p_{01}\left(\frac{1}{x} - 1\right)\right) + p(1 + p_{10}(x-1))\right) = -\ln f_1(p, x).$$

Поэтому

$$I(A) = \inf_{p \in A} \sup_{x > 0} f(p, x) \geq -\ln \sup_{p \in A} \inf_{x > 0} f_1(p, x).$$

Нетрудно показать, что $\inf_{x > 0} f_1(p, x) = 1 - \left(\sqrt{(1-p)p_{01}} - \sqrt{p_{10}p}\right)^2 = f_1(p)$ и, далее, что при $|\varepsilon| < \varepsilon_0$, $\sup_{p \in A} f_1(p) = \max\{f_1(0.5 - \varepsilon_0), f_1(0.5 + \varepsilon_0)\} = 1 - a$, где величина a определена в формулировке теоремы 2. Отсюда получаем первое утверждение теоремы.

Случай $|\varepsilon| > \varepsilon_0$ рассматривается аналогично. Выберем произвольное $\varepsilon' \in (\varepsilon_0, |\varepsilon|)$. Тогда для достаточно больших n имеем оценки:

$$1 - \beta(\varepsilon_0, \varepsilon_1) \leq P(n(0.5 - \varepsilon') \leq S_n \leq n(0.5 + \varepsilon')) = P(L_n \in \tilde{B}).$$

Здесь $B = [0.5 - \varepsilon', 0.5 + \varepsilon']$. В случае $|\varepsilon| > \varepsilon_0$ получаем, что $\sup_{p \in A} f_1(p) = \max\{f_1(0.5 - \varepsilon'), f_1(0.5 + \varepsilon')\} = 1 - a'$. Теорема 2 доказана.

Доказательство теоремы 3 следует из того, что в рамках модели M_2 статистика S_n имеет биномиальное распределение с параметрами $(n-1, 0.5 + \varepsilon)$. Поэтому супремум $\beta(H)$ по всем $H \in H'_0$ достигается при $\varepsilon = \pm \varepsilon_0$ и равен (после использования нормальной аппроксимации)

$$\beta(\varepsilon_0) \approx \Phi\left(\frac{\Delta - m_1}{\sigma}\right) + \Phi\left(\frac{\Delta - m_2}{\sigma}\right).$$

(Определения величин m_1, m_2 и σ см. выше в описании критерия знакоперемен.) Отсюда получаем соотношение (3) для порога Δ критерия. Теорема 3 доказана.

Доказательство теоремы 4. Свойство монотонности функции $\beta(\varepsilon)$ следует из свойств биномиального распределения. Как известно, для биномиальных (с параметрами (n, p)) вероятностей справедливо следующее представление через функцию бета-распределения:

$$P(S_n \geq \Delta) = I_p(\Delta, n - \Delta + 1) = \frac{1}{B(\Delta, n - \Delta + 1)} \int_0^p x^{\Delta-1} (1-x)^{n-\Delta} dx,$$

где $B(\Delta, n - \Delta + 1) = \int_0^1 x^{\Delta-1} (1-x)^{n-\Delta} dx$. Выражая функцию мощности $\beta(\varepsilon)$ через интегралы

I_p и исследуя производную $\beta(\varepsilon)$, получим искомую монотонность.

Пусть $|\varepsilon| < \varepsilon_0$. Для оценки вероятностей больших отклонений биномиального распределения воспользуемся неравенством, полученным Хёфдинггом, которое мы цитируем по книге [4] (см. неравенство 8 на с. 76). Если X_1, X_2, \dots, X_n — независимые бинарные случайные величины, то для любого $x > 0$

$$P(S_n - ES_n \geq nx) \leq e^{-2nx^2}.$$

Поэтому для $\beta(\varepsilon)$ получим следующую оценку:

$$\beta(\varepsilon) \leq e^{-2nx^2} + e^{-2ny^2}, \quad (5)$$

где $x = \frac{\Delta - m + 1}{n}$ и $y = \frac{n - \Delta - m}{n}$, а $m = (n-1)(0.5 + \varepsilon)$.

Из определения порога Δ (3) можно получить следующие границы для Δ :

$$m_2 - q_2\sigma \leq \Delta \leq m_2 - q_1\sigma,$$

где квантили $q_1 = \Phi^{-1}(1 - \alpha)$, $q_2 = \Phi^{-1}\left(1 - \frac{\alpha}{2}\right)$. Подставляя верхнюю оценку для Δ в x и y

(заметим, что $x < 0$, $y > 0$), из (5) получим первое утверждение теоремы.

Пусть теперь $\varepsilon > \varepsilon_0$. Имеем: $1 - \beta(\varepsilon) \leq P(S_n \leq n - 1 - \Delta)$. Применяя неравенство Хёфдинга и, далее, нижнюю оценку для Δ , получим часть второго утверждения теоремы.

Совершенно аналогично рассматривается случай, когда $\varepsilon < -\varepsilon_0$.

Теорема 4 доказана.

ЛИТЕРАТУРА

1. Application Notes and Interpretation of the Scheme 31: Functionality classes and evaluation methodology for physical random number generators. AIS 31, Version 3.1. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, Germany, 25 Sept. 2001. 38 p.

2. *Ибрагимов, И. А.* Независимые и стационарно связанные величины / И.А. Ибрагимов, Ю.В. Линник. М.: Наука, 1965. 524 с.

3. *Hollander, F. den.* Large deviations / F. den Hollander. American Mathematical Society, 2000. 142 p.

4. *Петров, В.В.* Суммы независимых случайных величин / В.В. Петров. М.: Наука. 1972. 416 с.