ПОСТРОЕНИЕ ОДНОЭТАПНОЙ ПРОЦЕДУРЫ МНОЖЕСТВЕННОЙ ПРОВЕРКИ ГИПОТЕЗ СО «СВИДЕТЕЛЕМ»

Костевич А. Л., Милованова И. С., БГУ, Минск

Введение

В различных практических задачах требуется одновременное применение набора статистических критериев для проверки нулевых гипотез, например, в криптографии, медицине [1] и др. Для этого используются процедуры множественной проверки гипотез, среди которых можно выделить одноэтапные процедуры, для которых показатель $FWER$ (вероятность ошибки хотя бы одного критерия при истинной нулевой гипотезе) не превосходит заданного значения. Общепринятым способом [2] контроля $FWER$ является выбор малых уровней значимости для каждого критерия, так как большие значения приводят к увеличению числа ложных тревог. Однако при большом числе критериев такой подход приводит к снижению мощности процедур [2]. В данной статье предлагается процедура, основанная на другом принципе контроля $FWER$ — использовании части критериев набора в качестве «свидетелей» для отсева ложных тревог.

Математическая модель

Пусть имеется m пар критериев $(C_1^{(1)}, C_1^{(2)}),\ldots,\ (C_m^{(1)}, C_m^{(2)})$ для проверки нулевой гипотезы $\mathbf{H}_0$ против альтернатив $\mathbf{H}_{1,1},\ldots,\mathbf{H}_{1,m}$ соответственно. Будем полагать, что решения критериев $C_i^{(1)},\ C_i^{(2)},\ i=\overline{1,m}$ на большей части выборочного пространства совпадают, но они не являются эквивалентными в том смысле, что на некоторых выборках они принимают различные решения.

Предложим процедуру проверки $\mathbf{H}_0$, состоящую из двух этапов.

<u>Этап 1</u> состоит в проверке $\mathbf{H}_0$ с помощью критериев $\{C_i^{(1)}\},\ i=\overline{1,m}$ на уровне значимости α_1. Обозначим $J^{(1)}$ — множество индексов критериев, отвергнувших гипотезу $\mathbf{H}_0$ на данном этапе.

<u>Этап 2</u> состоит в уточнении множества принятых альтернатив $J^{(1)}$ с целью отсева ложных тревог критериев первого этапа с помощью проверки $\mathbf{H}_0$ критериями-«свидетелями» $\{C_i^{(2)}\},\ i\in J^{(1)}$ на уровне значимости α_2. Пусть $J^{(2)}$ — множество индексов критериев, отвергнувших $\mathbf{H}_0$ на втором этапе.

Определим итоговое решение процедуры:

$$\text{принимается гипотеза} \begin{cases} \mathbf{H}_0, \text{если } J^{(1)}=\varnothing \text{ или } J^{(2)}=\varnothing, \\ \mathbf{H}_1=\mathbf{H}_{1,1}\cup\ldots\cup\mathbf{H}_{1,m}, \text{иначе.} \end{cases} \tag{1}$$

Задача данной работы состоит в исследовании вероятности ошибки первого рода (показателя $FWER$) $\alpha^*=\mathbf{P}\{\text{принять}\,\mathbf{H}_1\,|\,\mathbf{H}_0\ \text{истинна}\}$ процедуры (1) в зависимости от уровней значимости α_1,α_2 критериев следующего вида:

$$C_i^{(j)}\ \text{принимает гипотезу} \begin{cases} \mathbf{H}_0, \text{если } \dot{s}_i^{(j)}=\left|\dfrac{s_i^{(j)}-\mu_i^{(j)}}{\sigma_i^{(j)}}\right|\le\Delta_j=\Phi^{-1}(1-\alpha_j/2), \\ \mathbf{H}_{1,i}, \text{иначе,} \end{cases} \tag{2}$$

где статистики $\{s_i^{(j)}\}$ критериев $\{C_i^{(j)}\}$ при истинной гипотезе $\mathbf{H}_0$ имеют нормальное распределение с параметрами $\mu_i^{(j)}, \sigma_i^{(j)2}$, а совместное распределение статистик $\left(s_i^{(1)}, s_i^{(2)}\right)$ является двумерным нормальным распределением, $corr\left(s_i^{(1)}, s_i^{(2)}\right) = \rho_i$, $i = \overline{1, m}$, $j = 1{,}2$.

Исследование вероятности ошибки первого рода

Оценим вероятность ошибки первого рода α^* процедуры (1).

Теорема. *Для вероятности ошибки первого рода (показателя $FWER$) α^* процедуры (1) с критериями (2) справедливо следующее утверждение:*

$$\alpha^* \le \alpha_+(\alpha_1, \alpha_2) = \sum_{i=1}^{m} \left[\alpha_1 + \alpha_2 - 1 + \int_{-\Delta_1}^{\Delta_1} \int_{-\Delta_2}^{\Delta_2} p(x, y \mid \rho_i) dxdy \right], \tag{3}$$

где $p(\cdot, \cdot \mid \rho_i)$ — совместная плотность распределения статистик $\left(\dot{s}_i^{(1)}, \dot{s}_i^{(2)}\right)$.

Для верхней границы справедливо также следующее разложение в ряд:

$$\alpha_+(\alpha_1, \alpha_2) = \sum_{i=1}^{m} \left[\alpha_1 \alpha_2 + \sum_{k=1}^{+\infty} \frac{4 p^{(2k-1)}(\Delta_1(\alpha_1)) p^{(2k-1)}(\Delta_2(\alpha_2))}{(2k)!} \rho_i^{2k} \right], \tag{4}$$

где $p^{(k)}(\Delta)$ — k-я производная плотности стандартного нормального распределения в точке Δ.

Доказательство основано на использовании неравенства Бонферрони. ■

Свойство. *Функция $\alpha_+(\alpha_1, \alpha_2)$ при фиксированном значении одного аргумента убывает по второму аргументу.*

Разложение (4) удобно использовать для вычисления α_+ на практике. Найденная верхняя граница (3) может быть использована для нахождения уровней α_1 и α_2 по заданному уровню значимости α всей процедуры. Свойство монотонности позволяет находить методом половинного деления уровень значимости одного этапа процедуры при фиксированных значениях уровней значимости другого этапа и всей процедуры.

Вычислительный эксперимент

Для исследования эффективности построенной процедуры проводились численные эксперименты для проверки гипотезы $\mathbf{H}_0 : \{X_t\}$ — независимые, одинаково распределенные с.в., $\mathbf{P}\{X_t = 1\} = \mathbf{P}\{X_t = 0\} = 0.5$ по выборке X объема n. На первом этапе применялось 8 критериев шаблонов $h_1^{(i)} h_2^{(i)} h_3^{(i)}$ длины 3 по непересекающимся интервалам со статистиками $s_i^{(1)} = \sum_{j=1}^{[n/3]} \mathbf{1}\left\{X_{3j-2} = h_1^{(i)}, \ldots, X_{3j} = h_3^{(i)}\right\}$, $i = \overline{1, m}$. В качестве критериев–«свидетелей» использовались критерии шаблонов по пересекающимся интервалам, $s_i^{(2)} = \sum_{j=1}^{n-2} \mathbf{1}\left\{X_j = h_1^{(i)}, \ldots, X_{j+2} = h_3^{(i)}\right\}$. Пары критериев $C_i^{(1)}$, $C_i^{(2)}$, относящиеся к одинаковым шаблонам, не являются эквивалентными, т.к. $|\rho_i| \ne 1$, $i = \overline{1, 8}$. Для значений $\alpha_1 = 0.01$, $\alpha_2 = 0.02$ согласно (3) было найдено теоретическое значение $\alpha_+ = 0.019428$. На рис. 1 приведены экспериментальные значения α^* процедуры (1) (сплошная тонкая линия) в зависимости от длины выборки n. Как видно, значение α_+, попадает в 95%-й доверительный интервал (пунктир).

Вторая серия экспериментов (рис. 2) проводилась для сравнения мощности процедуры (1) (сплошная линия) с процедурой Бонферрони (длинный пунктир), построенной по критериям шаблонов длины 3 по непересекающимся интервалам. Индивидуальный уровень значимости процедуры Бонферрони выбирался согласно [1] равным $\alpha_c = 0.019428/8 = 0.0024285$. Как видно, процедура Бонферрони проигрывает по мощности построенной двухэтапной процедуре на альтернативе $\mathbf{H}_1 : \mathbf{P}\{X_t = 1\} = 0.53$.

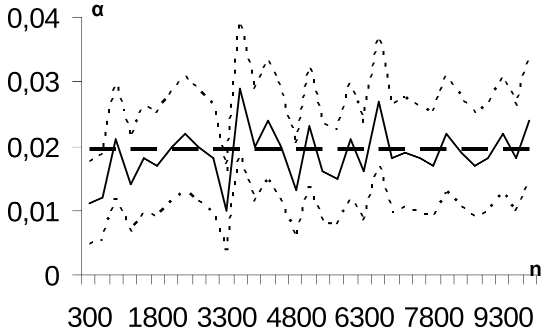

Рис. 1. Оценка вероятности ошибки первого рода построенной процедуры

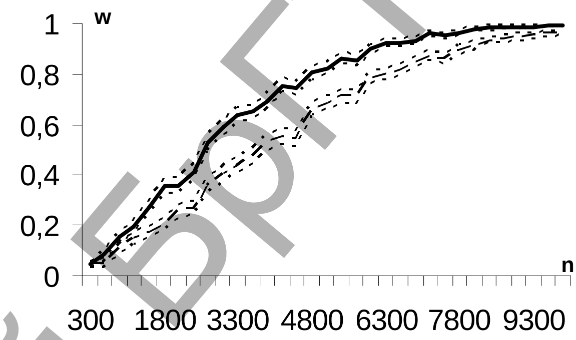

Рис. 2. Сравнение мощности построенной процедуры и процедуры Бонферрони

Литература

1. Aickin M., Gensler H. Adjusting for Multiple Testing When Reporting Research Results: The Bonferroni vs Holm Methods // Public Health Briefs, 1996, v.86, №5.
2. Lehmann E. L., Romano J. P. Generalizations of the familywise error rate // Annals of Statistics, 2005, v. 33, № 3, P. 1138-1154.

ПОСТРОЕНИЕ КРИТЕРИЯ СОГЛАСИЯ ДЛЯ ЦЕПЕЙ МАРКОВА БОЛЬШОЙ СВЯЗНОСТИ

Костевич А. Л., Шилкин А.В., БГУ, Минск

Введение

Многие задачи криптографии, например генерация ключей, предварительный анализ стойкости криптографических примитивов, требуют применения статистических критериев для обнаружения отклонений от модели независимых симметричных испытаний Бернулли. Одной из важных моделей отклонений является наличие марковской зависимости большого порядка связности *L*=32, 64, 128 и алфавитом мощности *N*. Применение классических методов выявления марковской зависимости [1] является невозможным ввиду большого числа параметров $N^L(N-1)$.

В данной статье предлагается подход к построению критерия согласия о значении матрицы вероятностей одношаговых переходов цепи Маркова большой связности, основанный на замене задачи проверки гипотезы согласия задачей прогнозирования реализации цепи Маркова. Работоспособность предлагаемого подхода иллюстрируется на примере MTD–модели цепи Маркова большой связности [2].