СТАТИСТИЧЕСКОЕ ПОСТРОЕНИЕ ДАТЧИКОВ БАЗОВОЙ СЛУЧАЙНОЙ ВЕЛИЧИНЫ НА ОСНОВЕ ФЛУКТУАЦИЙ ФИЗИЧЕСКИХ СИСТЕМ

Сосинович Е. С., Жук Е. Е.
Кафедра математического моделирования и анализа данных, Белорусский государственный университет
Минск, Республика Беларусь
E-mail: fpm.sosinovi@bsu.by, zhukee@mail.ru

В данной работе излагаются особенности физических датчиков базовых случаных величин и методы их построения. Предложен метод построения датчиков на основе реализации любой слуйчайной величины путем функционального преобразования. Исследована эффективность предложенного метода, а также приведен пример реализации функционального преобразования на реальнных данных.

Введение

Проблема имитационного статистического моделирования случайной величины ξ с заданной функцией распределения вероятностей $F_\xi(x)$ сводится к проблеме моделирования базовой случайной величины (БСВ) α, равномерно распределенной на отрезке $[0,1]$. Датчик БСВ – устройство, позволяющее по запросу получать реализацию случайной величины (СВ) или несколько независимых реализаций. Выделяют несколько типов датчиков: табличный, физический и программный. Физический датчик БСВ – специальное радиоэлектронное устройство, являющееся приставкой к ЭВМ. Он состоит из источника флуктуационного шума, значение которого является некоторой СВ [1]. Основным преимущетсвом физического датчика БСВ является его криптографическая стойкость за счет невозможности повторения некоторой ранее полученной реализации. Для построения датчика БСВ, обладающего улучшенными вероятностными свойствами, предлагается подвергать выборку-реализацию произвольной СВ ξ функциональному преобразованию на основе эмпирической функции распределения (ЭФР). Эффект от такого преобразования исследуется при помощи стандартного набора тестов Д. Кнута: критериев согласия с функцией распределения (критерии Колмогорова и Пирсона), тестов «совпадение моментов» и «ковариация» [1].

I. Функциональное преобразование

Приведем функциональное преобразование, позволяющее построить датчик БСВ на основе реализации произвольной СВ.

Базования случайная величина α, равномерно распределенная на $[0,1]$, имеет функцию распределения:

$$F_\alpha(x) = \begin{cases} 0, & x \le 0, \\ x, & 0 < x < 1, \\ 1, & x \ge 1, \end{cases}$$

математическое ожидание $E\{\alpha\} = \frac{1}{2}$ и дисперсию $D\{\alpha\} = \frac{1}{12}$.

Установлен следующий факт [2,3]. Если существует обратная $F_\xi^{-1}(\cdot)$ функции распределения $F_\xi(\cdot)$ некоторой случайной величины ξ, то БСВ α можно смоделировать следующим образом: $\alpha = F_\xi(\xi)$, так как

$$F_\alpha(x) = P(\alpha \le x) = P(F_\xi(\xi) \le x) = \\ = P(\xi \le F_\xi^{-1}(x)) = F_\xi(F_\xi^{-1}(x)) = x.$$

Пусть имеется выборка-реализация $\Xi = \{\xi_1, ..., \xi_n\}$ СВ ξ. По ней строим ЭФР:

$$\hat{F}_\xi(x) = \frac{1}{n}\sum_{t=1}^{n} I(x - \xi_t), x \in \mathbf{R}, \\ I(x) = \begin{cases} 1, & x \ge 0, \\ 0, & x < 0, \end{cases} \quad (1)$$

в качестве статистической оценки неизвестной функции распределения $F_\xi(\cdot)$.

Таким образом, посредством функционального преобразования элементов исходной последовательности Ξ на основе ЭФР (1) получаем реализацию $X = (x_1, ..., x_n)$ БСВ, где $x_i = \hat{F}_\xi(\xi_i)$, $i = \overline{1,n}$.

II. Исследование эффективности

Проверим эффективность преобразования на основе ЭФР (1) с помощью набора тестов Д. Кнута. В тестах Колмагорова и Пирсона относительно последовательности X проверяется гипотеза согласия с равномерным распределением вероятностей $H_0 : F_x(\cdot) \equiv F_\alpha(\cdot)$ против альтернативы $H_1 = \overline{H_0} : \exists x \in \mathbf{R} : F_x(x) \ne F_\alpha(x)$. Тесты строятся при малом уровне значимости $\epsilon \in (0,1)$, представляются через P-значение $P(X,n) \in [0,1]$ и имеют вид:

$$\begin{cases} \text{принимается } H_0, P(X,n) \ge \epsilon, \\ \text{принимается } H_1, P(X,n) < \epsilon. \end{cases}$$

В [2] было установлено, что для критериев Колмагорова, Пирсона и «совпадения моментов»[1] P-значения будут иметь вид соответственно:

- $P(X,n) = 1 - K(1/\sqrt{n})$ для критерия Колмагорова, где $K(z) = 1 - 2\sum\limits_{j=1}^{\infty}(-1)^{j-1}e^{-2j^2z^2}, z \ge 0$ – функция распределения Колмагорова.
- $P(X,n) = 1 - F_{\chi^2_{k-1}}(\chi^2)$ для χ^2-критерия Пирсона, где $k \ge 2$ – число ячеек одинаковой

длины, на которые разбивается отрезок $[0,1]$, $F_{\chi^2_{k-1}}(\cdot)$ – функция χ^2-распределения с $k-1$ степенями свободы, $\chi^2 = \sum\limits_{i=1}^{k} \frac{(n_i - \frac{n}{k})}{\frac{n}{k}}$ – χ^2-статистика, n_i – число элементов преобразованной последовательности, попавших в i-тую ячейку.

- $P(X,n) = 2(1 - \Phi(\sqrt{12n}|\overline{x} - \frac{1}{2}|))$, $P(X,n) = 2(1 - \Phi(6\sqrt{2(n-1)}|s_x^2 - \frac{1}{12}|))$ для гипотез относительно математического ожидания μ_x и дисперсии σ_x^2 соответсвенно для теста «совпадение моментов», где $\Phi(z) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{z} e^{-\frac{\omega^2}{2}} d\omega$ – функция распределения стандартного нормального закона, $\overline{x} = \frac{1}{n}\sum\limits_{t=1}^{n} x_t$ – оценка для μ_x, $s_x^2 = \frac{1}{n-1}\sum\limits_{t=1}^{n}(x_t - \overline{x})^2$ – оценка для σ_x^2.

Установлено [2], что приведенные выше P-значения: $P(X,n) \to 1, n \to \infty$. Следовательно, всегда можно добиться принятия гипотезы H_0.

Для теста «ковариация» справедлив следующий факт [3]:

$E\{x_t\} = \frac{1}{2} + \frac{1}{2n}, D\{x_t\} = Cov\{x_t, x_t\} = \frac{1}{12} - \frac{1}{12n^2}, Cov\{x_t, x_k\} = \frac{1}{12n} - \frac{1}{12n^2}$,
что соответсвует БСВ при $n \to \infty$.

Можно предположить, что зависимость между элементами преобразованной последовательности можно «ослабить», если преобразованию на основе ЭФР $\hat{F}_\xi(\cdot)$, построенной по последовательности $\Xi = \{\xi_1, ...\xi_n\}$, подвергать так называемые «вновь поступающие» значения $\Xi_n^m = \{\xi_{n+1}, ..., \xi_{n+m}\}$. Как было установлено в [3], относительно такого преобразования уже нельзя утверждать, что тесты Колмогорова, Пирсона и «совпадение моментов» будут «заведомо проходить». Следовательно, преимущесвто преобразования «вновь поступающих» значений не оправдалось.

III. Вычислительный эксперимент

Применим предложенное преобразование к реальным данным для построения датчика БСВ по реализации нормально распределенной СВ.

Для проверки свойств преобразования используются ежедневные значения атмосферного давления на уровне метеостанции в Минске за 01.05.2015 – 22.04.2019. Установлено, что данная последовательность $\Xi = \{\xi_1, ..., \xi_n\}$ подчиняется нормальному закону.

Построим две последовательности БСВ: $X^{(1)}$ и $X^{(2)}$. $X^{(1)}$ получим путем применения преобразования на основе ЭФР (1), построенной по Ξ, ко всей выборке Ξ. Для построения $X^{(2)}$ разобьем исходную последовательность на две части: $\Xi = \left(\Xi_0^{[\frac{n}{2}]}, \Xi_{[\frac{n}{2}]}^n\right)$, по выборке $\Xi_0^{[\frac{n}{2}]}$ построим ЭФР (1) и применим ее для преобразования выборки $\Xi_{[\frac{n}{2}]}^n$.

Результаты проверки эффективности предложенных преобразований с помощью набора тестов Д. Кнута представлены в Таблице 1.

Заключение

Результаты тестирования позволяют сделать вывод, что построенная с помощью предложенного преобразования последовательность действительно может служить базовой случайной величиной. Таким образом, данное функциональное преобразование позволяет моделировать датчик БСВ на основе произвольной последовательности СВ. Если входная последовательность пополняется «вновь поступающими» значениями, то их целесообразно присоединять к предыдущим и подвергать все доступные на данный момент значения преобразованию.

Преимуществом такого построения датчика БСВ является осутствие в нем детерминированного алгоритма. Это позволяет утверждать, что такой датчик защищен от взлома, так как СВ, использующаяся для построения датчика, не является псевдослучайной.

Список литературы

1. Харин, Ю. С. Практикум на ЭВМ по математической статичтике: Для мат. спец. ун-тов / Ю. С. Харин, М. Д. Степанова. – Мн. : изд-во «Университетское», 1987. – 304 с.
2. Жук Е. Е. Улучшение статистических свойств датчиков БСВ на основе эмпирической функции распределения / Е. Е. Жук // Весці НАН Беларусі. Сер. фіз.–мат. навук. – 2008. – №3. – С. 4–10
3. Жук Е. Е. Исследование ковариационных свойств псевдослучайных последовательностей, преобразованных на основе эмпирической функции распределения // Весці НАН Беларусі. Сер. фіз.–мат. навук. – 2010. – №2. – С. 18-22

Таблица 1 – Результаты экспериментального подтверждения эффективности

Выборка	Обьем, n	Кр. Пирсона, $p-value$	Кр. Колмогорова, $p-value$	Величина $\lvert\overline{x} - \frac{1}{2}\rvert$	Величина $\lvert s_x^2 - \frac{1}{12}\rvert$
$X^{(1)}$	1452	1	0.9217	0.002869605	2.430142e-05
$X^{(2)}$	726	1	0.4057	0.004454766	5.063509e-05