Для каждого t, $1 \le t \le L$ вычисляем:

Функция перехода состояний F.

1. $i_t = i_t + 1 (\mathrm{mod}\, n)$,
2. $j_t = j_{t-1} + s_{t-1}[i_t] (\mathrm{mod}\, n)$,
3. переставляем $s_t[i_t]$ и $s_t[j_t]$.

Функция выхода f.

$z_t = s_t[(s_t[i_t] + s_t[j_t]) \bmod n]$.

3.2. Свойства выходной последовательности генератора RC4

Предложение 3.1. Если начальное состояние криптосхемы $S_0, i_0 = k (\mathrm{mod}\, n), j_0 = k + 1 (\mathrm{mod}\, n)$, причем $S_0[(k+1) \bmod n] = 1$, тогда криптосхема вернется в то же состояние через n $(n - 1)$ шагов.

Доказательство. Вычислим следующее состояние криптосхемы: $i_1 = i_0 + 1 = k + 1 (\mathrm{mod}\, n)$,

$j_1 = (j_0 + S_0[i_1]) \bmod n = (k + 1 + S_0[(k+1)]) \bmod n) \bmod n = (k+2) \bmod n$,

$S_1[j_1] = S_0[i_1] = S_0[(k+1) \bmod n] = 1$, $S_1[i_1] = S_0[j_1] = S_0[(k+2) \bmod n]$. Т. е. получили состояние, которое отличается от (S_0, i_0, j_0) тем, что $k' = k + 1$ и $S_1[k' \bmod n] = S_0[(k'+1) \bmod n] = 1$. Заметим, что через n шагов криптосхема вернется в состояние (S_n, i_0, j_0), где S_n – такая подстановка, что $S_n[(k+1) \bmod n] = 1$, $S_n[k \bmod n] = S_0[(k+2) \bmod n]$ и для $\forall l \in \mathrm{Z}$, $l \ne k, k + 1 (\mathrm{mod}\, n)$ $S_n[l \bmod n] = S_0[(l-1) \bmod n]$, т. е. за n шагов k-ый элемент сдвигается на две позиции влево, а остальные элементы подстановки сдвигаются на одну позицию вправо. Таким образом, для того, чтобы все элементы подстановки вернулись на свои места, потребуется $n - 1$ серия из n шагов. Т. е. получили, что через n $(n - 1)$ шагов криптосхема вернется в исходное состояние.

Литература

1. *Jovan Dj. Golic, Mahmoud Salmasizadeh, Ed Dawson* Fast Correlation Attacks on the Summation Generator // Journal of Cryptology, vol 13, pp. 245–262, 2000.

ИССЛЕДОВАНИЕ СВОЙСТВ УСТОЙЧИВЫХ ЗАКОНОВ РАСПРЕДЕЛЕНИЯ И ИХ КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

Л. Э. Гаджиева

1. Введение

В настоящее время для исследования различных экономических и финансовых моделей достаточно часто применяется вероятностный под-

ход. Наиболее подходящей стохастической моделью для многих практических приложений является класс устойчивых распределений Леви. Несмотря на то, что их использование влечет за собой существенные аналитические трудности, устойчивые распределения являются одними из наиболее важных. Это связано с тем, что если существуют предельные распределения нормированных независимых одинаково распределенных случайных величин, то они будут устойчивыми. Наиболее исследованным в классе устойчивых распределений является нормальное.

2. Понятие устойчивых распределений

Самым простым и удобным способом определения устойчивой случайной величины является задание ее характеристической функции.

Для того чтобы случайная величина ξ была устойчивой (пишут $\xi \sim S_\alpha(\sigma,\beta,\mu)$), необходимо и достаточно, чтобы ее характеристическая функция $\psi_\xi(t)$ допускала представление

$$\ln \psi_\xi(t) = \begin{cases} -\sigma^\alpha |t|^\alpha (1 - i\beta sign(t) tg\frac{\alpha\pi}{2}) + i\mu t, \alpha \neq 1 \\ -\sigma |t| (1 + i\beta \frac{2}{\pi} sign(t) \ln|t|) + i\mu t, \alpha = 1 \end{cases}, \quad (1)$$

где $a \in (0,2]$, $\sigma \geq 0$, $\beta \in [-1,1]$ и $\mu \in \mathbb{R}$.

Параметр сдвига μ показывает насколько сдвинуто распределение влево или вправо. Параметр масштаба σ сжимает или растягивает распределение вокруг μ. Индекс устойчивости $a \in (0,2]$. Когда $a = 2$ мы имеем распределение Гаусса с математическим ожиданием μ и дисперсией $2\sigma^2$. В общем случае α – устойчивая случайная величина имеет конечный момент порядка p только если $p < \alpha$. Четвертый параметр β называют параметром ассиметрии. Если β отрицательное, то распределение скошено влево, если положительное, – вправо. Если $\beta = 0$, то распределение симметрично. При α стремящемся к 2, β теряет свой эффект перекоса и распределение стремится к симметричному гауссовскому.

Сложность проблемы генерирования устойчивых случайных величин состоит в том, что вид характеристической функции не позволяет получить аналитического выражения ни для обратной функции распределения, ни для плотности распределения. Исключение составляют частные случаи устойчивых распределений – распределение Гаусса ($S_2(\sigma,0,\mu) = N(\mu, 2\sigma^2)$), Коши ($S_1(\sigma,0,\mu)$) и Леви ($S_{1/2}(\sigma,1,\mu)$,

$S_{1/2}(\sigma,-1,\mu)$), для которых применимы обычные методы моделирования. Во всех остальных случаях, чтобы получить плотность распределения, необходимо использовать численное интегрирование. Такой метод требует много машинного времени и влечет за собой погрешность, связанную с численным интегрированием.

Далее получено выражение устойчивой случайной величины через равномерно распределенную и экспоненциальную случайные величины [1, с. 55] с моделированием которых не возникает существенных проблем.

3. Основные способы параметризации устойчивых законов. Связь между параметрами

Есть несколько различных способов параметризации устойчивых законов. Хотя все они и эквивалентны, их существование оправдано тем, что каждый из них, обладая своими преимуществами и недостатками, оказывается удобным для решения какой-либо конкретной проблемы.

Золотарев в [2] вводит следующий способ параметризации устойчивых случайных величин, который называет «парамеризацией (B)»:

$$\ln\psi_{\xi(t)} = \lambda\left(it\gamma - |t|^{\alpha}\,\omega_B(t,\alpha,\beta)\right), \tag{2}$$

где $\omega_B(t,a,\beta) = \begin{cases} \exp(-i\frac{\pi}{2}\beta K(\alpha)sign(t)), \alpha \neq 1 \\ \frac{\pi}{2} + i\beta\ln|t|\,sign(t), \alpha = 1 \end{cases}$, $K(\alpha) = \alpha - 1 + sign(1-\alpha)$.

Параметры связаны с представлением (1) следующим образом:

Если $\alpha \neq 1$, то

$$\beta = ctg(\frac{\pi\alpha}{2})tg(\frac{\pi}{2}\beta_B K(\alpha)),\ \mu = \lambda_B\gamma_B,\ \sigma^{\alpha} = \lambda_B\cos(\frac{\pi}{2}\beta_B K(\alpha)). \tag{3}$$

Если $\alpha = 1$, то

$$\beta = \beta_B,\ \mu = \lambda_B\gamma_B,\ \sigma = \frac{\pi}{2}\lambda_B. \tag{4}$$

В данном случае индекс B употребляется, чтобы указать на то, что параметры соответствуют «параметризации (B)».

4. Вид функции распределения устойчивых случайных величин

Золотарев, работая с «параметризацией (B)», вывел в [2] вид функции распределения для устойчивых законов в случае $\lambda_B = 1$, $\gamma_B = 0$. Используя полученную в предыдущем пункте связь между параметрами

можно показать, что функция распределения при нашей параметризации (1) имеет следующий вид.

1. $\alpha \neq 1,\ x > 0$

$$F(x,\alpha,\beta) = 1 - \frac{(1+\varepsilon(\alpha))}{4}(1+\frac{2}{\pi}C_{\alpha,\beta}) +$$

$$+\frac{\varepsilon(\alpha)}{\pi}\int_{-C_{\alpha,\beta}}^{\pi/2} \exp(-x^{\frac{\alpha}{\alpha-1}}u_\alpha(\gamma,C_{\alpha,\beta}))d\gamma, \qquad (5)$$

2. $\alpha = 1,\ \beta > 0$

$$F(x,1,\beta) = \frac{1}{\pi}\int_{-\pi/2}^{\pi/2} \exp(-e^{\frac{x}{\beta}\frac{\pi}{2}}u_1(\gamma,\beta))d\gamma, \qquad (6)$$

где $C_{\alpha,\beta} = \frac{arctg(\beta tg(\pi\alpha/2))}{\alpha}$, $D_{\alpha,\beta} = (\cos(arctg(\beta tg\frac{\pi\alpha}{2})))^{-\frac{1}{\alpha}}$,

$$u_\alpha(\gamma,C_{\alpha,\beta}) = (D_{\alpha,\beta}\frac{\sin\alpha(\gamma+C_{\alpha,\beta})}{\cos\gamma})^{\frac{\alpha}{1-\alpha}}\frac{\cos(\gamma-\alpha(\gamma+C_{\alpha,\beta}))}{\cos\gamma},$$

$$u_1(\gamma,\beta) = \frac{\pi/2+\beta\gamma}{\pi/2\cos\gamma}\exp(\frac{1}{\beta}(\frac{\pi}{2}+\beta\gamma)tg\gamma).$$

Если $\alpha \neq 1, x < 0$ или $\alpha = 1, \beta_B < 0$, тогда, используя равенство

$$F(-x,\alpha,\beta) + F(x,\alpha,\beta) = 1, \qquad (7)$$

можем найти функцию распределения и для таких случайных величин.

Теорема. Пусть V – случайная величина, которая равномерно распределена на $(-\frac{\pi}{2},\frac{\pi}{2})$, а W – независимая от V экспоненциально распределенная случайная величина с $EW = 1$, тогда случайная величина X, заданная следующими формулами

1. $\alpha \neq 1$

$$X = D_{\alpha,\beta}\frac{\sin\alpha(V+C_{\alpha,\beta})}{(\cos V)^{1/\alpha}}(\frac{\cos(V-\alpha(V+C_{\alpha,\beta}))}{W})^{\frac{1-\alpha}{\alpha}}, \qquad (8)$$

2. $\alpha = 1$

$$X = \frac{2}{\pi}\left[(\frac{\pi}{2} + \beta V)tgV - \beta \ln(\frac{\pi/2 W \cos V}{\pi/2 + \beta V}) \right], \quad (9)$$

где $C_{\alpha,\beta} = \frac{arctg(\beta tg(\pi\alpha/2))}{\alpha}$, $D_{\alpha,\beta} = (\cos(arctg(\beta tg\frac{\pi\alpha}{2})))^{-\frac{1}{\alpha}}$ является устойчивой с $\sigma = 1$, $\mu = 0$ ($X \sim S_\alpha(1,\beta,0)$).

Теорема дает формулы для генерирования устойчивой случайной величины с $\sigma = 1$, $\mu = 0$ ($X \sim S_\alpha(1,\beta,0)$). Используя следующее свойство, которое вытекает из вида характеристической функции, можем сгенерировать устойчивую случайную величину для всех допустимых значений параметров.

Если $X \sim S_\alpha(1,\beta,0)$ и

$$Y = \begin{cases} \sigma X + \mu, \alpha \neq 1 \\ \sigma X + \frac{2}{\pi}\beta\sigma \ln\sigma + \mu, \alpha = 1 \end{cases}, \quad (10)$$

то случайная величина Y является устойчивой с $\sigma \neq 1$, $\mu \neq 0$ ($Y \sim S_\alpha(\sigma,\beta,\mu)$).

Литература

1. *Aleksander Janicki, Adam Izydorczyk*. Komputerowe metody w modelowaniu stochastycznym // WNT, Warszawa. 2001
2. *Золотарев В. М*. Одномерные устойчивые распределения // М.: Наука. 1983.

ПРОГНОЗИРОВАНИЯ AR-ВРЕМЕННЫХ РЯДОВ ПРИ НАЛИЧИИ «ПРОПУСКОВ»

А. С. Гурин

Введение

Авторегрессионные временные ряды часто используются для математического моделирования, статистического анализа данных, прогнозирования временных рядов, в теории принятия статистических решений [1–3]. На практике временные ряды, как правило, наблюдаются при наличии «пропусков» [4; 5]. Методы, используемые в литературе для прогнозирования авторегрессионных временных рядов при наличии «пропусков», являются, как правило, эвристическими, трудными для анализа и для них не изучены их асимптотические свойства. В настоящей работе