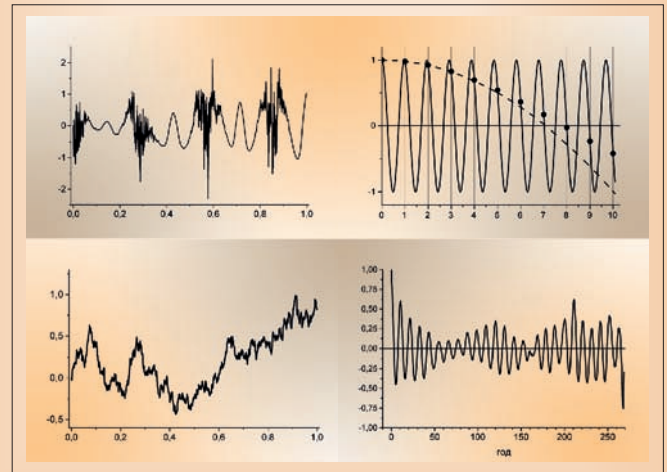


С. М. Пригарин

ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ МНОГОМЕРНЫХ ГАУССОВСКИХ РАСПРЕДЕЛЕНИЙ



ISBN 978-5-4437-0782-2



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Механико-математический факультет
Кафедра вычислительной математики

С. М. Пригарин

Численное моделирование многомерных гауссовских распределений

Учебное пособие

НОВОСИБИРСК
2018

УДК 519.6; 519.2
ББК 22.19; 22.17
П 754

Рецензент:
д-р физ.-мат. наук *В. А. Огородников*

Пригарин, С. М.
П 754 Численное моделирование многомерных гауссовских распределений : учеб. пособие / С. М. Пригарин ; Новосиб. гос. ун-т. — Новосибирск : ИПЦ НГУ, 2018. — 84 с.

ISBN 978-5-4437-0782-2

В пособии излагаются общие методы численного моделирования гауссовских векторов, которые используются при компьютерном моделировании разнообразных случайных процессов и явлений. Пособие будет полезно студентам, аспирантам и слушателям ФПК, изучающим методы Монте-Карло, а также специалистам по статистическому моделированию.

УДК 519.6; 519.2
ББК 22.19; 22.17

ISBN 978-5-4437-0782-2

© Новосибирский государственный университет, 2018
© Пригарин С. М., 2018

Оглавление

Предисловие	5
Список обозначений	6
Глава 1. Гауссовские распределения	7
1.1. Нормальные случайные величины	7
1.2. Гауссовские векторы	7
1.3. Условные гауссовские распределения	13
1.4. Гауссовские решения линейных систем	15
1.5. Распределение гауссовского вектора в правой части совместной линейной системы уравнений	21
Глава 2. Численное моделирование гауссовских распределений	24
2.1. Моделирование нормальных случайных величин	24
2.2. Общие методы моделирования гауссовских случайных векторов	29
2.2.1. Квадратный корень из корреляционной матрицы	29
2.2.2. Моделирование на основе разложения Холецкого	31
Глава 3. Примеры моделирования	35
3.1. Моделирование гауссовского вектора с равноправны- ми компонентами	35
3.2. О моделировании гауссовских векторов стационарного типа	36
3.3. Мультифрактальное броуновское движение	46
Приложение А. Сведения из теории матриц	51
А.1. Положительно определенные матрицы	51
А.2. Скелетное разложение матрицы	52
А.3. Псевдообратные матрицы	52
А.4. Системы линейных уравнений	55
А.5. Полярное разложение матрицы	57

Приложение Б. О моделировании случайных чисел	58
Б.1. Источники случайных чисел	58
Б.2. О мультипликативных датчиках	63
Б.3. Тексты процедур на Паскале	67
Литература	73
Предметный указатель	81

Предисловие

Методы численного моделирования случайных величин, процессов и полей – это обширный раздел теории методов Монте-Карло (статистического моделирования). В данном пособии излагаются общие методы численного моделирования гауссовских векторов, которые используются при компьютерном моделировании разнообразных случайных процессов и явлений. В первой главе даются общие определения и описываются свойства гауссовских распределений, рассматриваются соотношения для условных распределений и гауссовских решений линейных систем алгебраических уравнений. Вторая глава посвящена общим методам численного моделирования гауссовских векторов на основе факторизации корреляционных матриц. Здесь обсуждаются различные варианты численных алгоритмов с использованием разложения Холецкого, разбирается случай вырожденной корреляционной матрицы. В третьей главе рассматриваются примеры моделирования эвкоррелированных гауссовских векторов, векторов стационарного типа и случайных процессов мультифрактального броуновского движения. Основной материал дополнен приложениями, в которых излагаются сведения из теории матриц и приводится информация об источниках случайных чисел на ЭВМ.

Предполагается, что читатель знаком с основами линейной алгебры и теории вероятностей. Для самостоятельной работы предлагаются упражнения. В пособии использованы материалы специального курса лекций, который читается автором в Новосибирском государственном университете для студентов старших курсов, специализирующихся на кафедре вычислительной математики механико-математического факультета.

Пособие предназначено для студентов высших учебных заведений и аспирантов, изучающих методы Монте-Карло. Оно будет полезно также широкому кругу специалистов по статистическому моделированию.

Список обозначений

A^+	– псевдообратная матрица;
A^T	– транспонирование матрицы A ;
A^*	– сопряженная матрица;
\mathbb{C}	– множество комплексных чисел;
$D\xi$	– дисперсия случайной величины ξ ;
$\det(A)$	– детерминант матрицы A ;
$\dim_B(A)$	– клеточная размерность множества A ;
$\dim_H(A)$	– хаусдорфова размерность множества A ;
$\dim(X)$	– размерность пространства X ;
$\Gamma(z)$	– гамма-функция;
I	– единичная матрица;
$\text{Image}(A)$	– образ оператора A ;
$\text{Ker}(A)$	– ядро оператора (матрицы) A ;
$M\xi$	– математическое ожидание случайной величины ξ ;
$\text{Pr}(A)$	– проектор на множество A ;
\mathbb{R}	– множество вещественных чисел;
$\text{rang}(A)$	– ранг матрицы A ;
$\text{Re } z, \text{Im } z$	– вещественная и мнимая части числа z ;
$\text{tr}(A)$	– след матрицы A ;
$\langle a, b \rangle$	– скалярное произведение векторов a и b .

Глава 1

Гауссовские распределения

В этой главе приводятся сведения о гауссовских распределениях.

1.1. Нормальные случайные величины

Случайная величина ξ называется *гауссовской* (или *нормальной*), если ее распределение является абсолютно непрерывным с плотностью вида

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(x-m)^2}{2\sigma^2}\right], \quad x \in \mathbb{R}. \quad (1.1.1)$$

Для гауссовской случайной величины ξ часто используется обозначение $\xi \sim N(m, \sigma^2)$. При этом

$$\begin{aligned} \mathbf{M}\xi &= m, \quad \mathbf{D}\xi = \sigma^2, \\ \mathbf{M}\xi^2 &= m^2 + \sigma^2, \quad \mathbf{M}\xi^3 = m(3\sigma^2 + m^2), \\ \mathbf{M}(\xi - \mathbf{M}\xi)^4 &= 3\sigma^4. \end{aligned}$$

Характеристическая функция гауссовского распределения записывается в виде

$$\mathbf{M}e^{i\lambda\xi} = \exp\left(i\lambda m - \frac{\sigma^2\lambda^2}{2}\right), \quad \lambda \in \mathbb{R}.$$

Гауссовскую случайную величину с нулевым средним и единичной дисперсией, $\xi \sim N(0, 1)$, называют *стандартной нормальной*.

1.2. Гауссовские векторы

Случайный вектор $\xi = (\xi_1, \dots, \xi_n)^T$ называется гауссовским (или нормальным), если для его характеристической функции выполнено

$$\mathbf{M}e^{i\langle\lambda, \xi\rangle} = \exp\left(i\langle\lambda, m\rangle - \langle\lambda, R\lambda\rangle/2\right), \quad \lambda \in \mathbb{R}^n,$$

где $\langle \cdot, \cdot \rangle$ — скалярное произведение в \mathbb{R}^n . При этом вектор m является математическим ожиданием,

$$m = \mathbf{M}\xi = (\mathbf{M}\xi_1, \dots, \mathbf{M}\xi_n)^T,$$

а матрица R — корреляционной матрицей вектора ξ :

$$R = \mathbf{M}(\xi - m)(\xi - m)^T = [\mathbf{M}(\xi_i - m_i)(\xi_j - m_j)].$$

Запись $\xi \sim N(m, R)$ будет использоваться для обозначения того, что случайный вектор ξ является гауссовским со средним m и корреляционной матрицей R .

Если матрица R невырождена, то гауссовское распределение имеет плотность в \mathbb{R}^n :

$$f(x) = [\det(2\pi R)]^{-1/2} \exp\left[-\frac{\langle(x-m), R^{-1}(x-m)\rangle}{2}\right], \quad x \in \mathbb{R}^n.$$

Определение гауссовского вектора в общем случае дается в терминах характеристической функции, а не через плотность распределения, так как если корреляционная матрица R является вырожденной, то плотность в \mathbb{R}^n не существует, и распределение сосредоточено на множестве меньшей размерности $m + R(\mathbb{R}^n)$.

Корреляционная матрица $[R_{ij}] = [\mathbf{M}(\xi_i - m_i)(\xi_j - m_j)]$ произвольного случайного вектора (в том числе и гауссовского) обладает свойством *положительной определенности*, т. е. для любых комплексных чисел c_i , $i = 1, \dots, n$, выполнено

$$\sum_{i=1}^n \sum_{j=1}^n \bar{c}_i c_j R_{ij} \geq 0. \quad (1.2.1)$$

(Согласно этому определению мы допускаем вырожденность положительно определенной матрицы.) Это следует из очевидного равенства

$$\sum_{i=1}^n \sum_{j=1}^n \bar{c}_i c_j R_{ij} = \mathbf{M} \left| \sum_{i=1}^n c_i (\xi_i - m_i) \right|^2.$$

С другой стороны, любая положительно определенная матрица может выступать в роли корреляционной для некоторого гауссовского распределения.

Замечание (об определениях положительной определенности). В терминах скалярного произведения

$$\langle a, b \rangle = \sum_{i=1}^n \bar{a}_i b_i$$

положительная определенность (1.2.1) эквивалентна тому, что

$$\langle c, Rc \rangle \geq 0, \quad \forall c \in \mathbb{C}^n. \quad (1.2.2)$$

Если выполнено

$$\langle c, Rc \rangle > 0, \quad \forall 0 \neq c \in \mathbb{C}^n, \quad (1.2.3)$$

то будем говорить о *строгой положительной определенности* матрицы R . Строгая положительная определенность эквивалентна положительной определенности и невырожденности. Заметим, что для обозначения свойства (1.2.2) в литературе часто используются термины «неотрицательная определенность» или «положительная полуопределенность», а для свойства (1.2.3) используется термин «положительная определенность».

Замечание (о вещественных и комплексных положительно определенных матрицах). Свойство (1.2.1), (1.2.2) гарантирует эрмитовость (самосопряженность) $R = R^*$ комплексной матрицы и симметричность $R = R^T$ вещественной матрицы (см. по этому поводу п. VI.4 на стр. 218 в [41]). Если вместо (1.2.1), (1.2.2) рассмотреть свойство положительной определенности над полем вещественных чисел

$$\langle c, Rc \rangle \geq 0, \quad \forall c \in \mathbb{R}^n, \quad (1.2.4)$$

то симметричность вещественной матрицы R из этого свойства не следует. В качестве примера можно привести

$$R = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \quad a > 0.$$

Для этой несимметричной матрицы выполнено (1.2.4). Более того, свойство (1.2.4) сохраняется, если к матрице R прибавить любую кососимметричную матрицу S , $S_{ij} = -S_{ji}$, так как для нее выполнено (см. п. 10.61 в [10]):

$$\langle c, Sc \rangle = 0, \quad \forall c \in \mathbb{R}^n. \quad (1.2.5)$$

Упражнение 1.1. Докажите следующее утверждение: если для вещественной симметричной матрицы R выполнено свойство (1.2.4), то для этой матрицы выполнено и свойство (1.2.2).

Для корреляционных матриц можно доказать:

$$R_{ii} \geq 0, \quad R_{ij} = R_{ji}, \quad (1.2.6)$$

$$R_{ij}^2 \leq R_{ii} R_{jj}, \quad (1.2.7)$$

$$|R_{ik} - R_{jk}|^2 \leq R_{kk} [R_{ii} + R_{jj} - 2R_{ij}]. \quad (1.2.8)$$

Упражнение 1.2. (а) Докажите свойства корреляционной функции (1.2.6)-(1.2.8). Для доказательства (1.2.8) воспользуйтесь положительной определенностью (1.2.1) матрицы

$$\begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{bmatrix}$$

и возьмите $c_1 = \sqrt{R_{33}}$, $c_2 = -c_1$, $c_3 = (R_{23} - R_{13})/\sqrt{R_{33}}$ (см. [12] на стр. 242 и [14] на стр. 248).

(б) Предположим, что квадратные матрицы R^1 и R^2 одинаковой размерности с элементами R_{nm}^1 и R_{nm}^2 являются положительно определенными. Докажите, что матрица R с элементами $R_{nm} = R_{nm}^1 R_{nm}^2$ тоже будет положительно определенной.

Упражнение 1.3. (а) Докажите, что необходимыми и достаточными условиями существования трехмерного гауссовского вектора с нормированной корреляционной матрицей

$$\begin{bmatrix} 1 & r_1 & r_2 \\ r_1 & 1 & r_1 \\ r_2 & r_1 & 1 \end{bmatrix} \quad (1.2.9)$$

являются условия

$$r_1 \in [-1, 1], \quad r_2 \in [-1 + 2r_1^2, 1]. \quad (1.2.10)$$

(б) Найдите необходимые и достаточные условия положительной определенности корреляционной матрицы

$$\begin{bmatrix} 1 & r_1 & r_2 \\ r_1 & 1 & r_3 \\ r_2 & r_3 & 1 \end{bmatrix}.$$

Как выглядит в трехмерном пространстве множество значений (r_1, r_2, r_3) , обеспечивающих положительную определенность?

(в) Докажите, что положительная определенность $n \times n$ -матрицы с единицей на главной диагонали и одим и тем же значением r вне главной диагонали

$$\begin{bmatrix} 1 & r & \dots & r \\ r & 1 & \dots & r \\ \dots & \dots & \dots & \dots \\ r & r & \dots & 1 \end{bmatrix} \quad (1.2.11)$$

эквивалентна тому, что

$$r \in [-1/(n-1), 1]. \quad (1.2.12)$$

Для доказательства необходимости неравенства (1.2.12) воспользуйтесь тем, что $\mathbf{D}(\xi_1 + \dots + \xi_n) \geq 0$, где (ξ_1, \dots, ξ_n) — случайный вектор с корреляционной матрицей (1.2.11). Изучите работу [58], где доказываются более общие результаты.

Гауссовские распределения обладают следующими свойствами: из некоррелируемости гауссовских величин следует их независимость; наилучшее среднееквадратическое приближение гауссовской величины гауссовским семейством оказывается линейным; линейное преобразование гауссовского вектора также имеет гауссовское распределение. В частности, выполнено

Утверждение 1.1. Если $\eta = A\xi + b$ и $\xi \sim N(m, R)$, то $\eta \sim N(Am + b, ARA^T)$.

Гауссовское распределение обладает «наибольшей неопределенностью» среди всех непрерывных распределений с конечными двумя первыми моментами. Если сформулировать более строго, то среди всех n -мерных распределений, плотность которых мы будем обозначать через $f(x_1, \dots, x_n)$, с фиксированным математическим ожиданием и заданной корреляционной матрицей наибольшее значение *дифференциальной энтропии*

$$-\int \dots \int f(x_1, \dots, x_n) \log f(x_1, \dots, x_n) dx_1 \dots dx_n$$

достигается для гауссовского распределения (см., например, [43, 64]). Дифференциальная энтропия n -мерного гауссовского вектора $\xi \sim N(m, R)$ равна $\frac{1}{2} \log[(2\pi e)^n \det(R)]$.

Упражнение 1.4. Докажите следующие утверждения (см., например, [8]).

(а) Точками перегиба плотности вероятности (1.1.1) являются точки $m \pm \sigma$.

(б) Если ξ_1, ξ_2 — нормальные случайные величины с нулевым средним, то случайная величина $\xi_1 \xi_2 / \sqrt{\xi_1^2 + \xi_2^2}$ имеет нормальное распределение. Если, кроме этого, дисперсии случайных величин совпадают, то случайная величина $(\xi_1^2 - \xi_2^2) / (\xi_1^2 + \xi_2^2)$ является гауссовской. Найдите выражения для средних и дисперсий соответствующих распределений.

Гауссовское распределение фигурирует в качестве предела в центральных предельных теоремах (ЦПТ). Одна из формулировок ЦПТ приведена ниже.

Теорема 1.1 (центральная предельная теорема). Пусть ξ_k , $k = 1, 2, \dots$, — независимые одинаково распределенные случайные величины с нулевым средним и дисперсией σ^2 . Тогда последовательность случайных величин

$$\frac{1}{\sqrt{n}} \sum_{k=1}^n \xi_k$$

слабо сходится к нормальной случайной величине с нулевым средним и дисперсией σ^2 .

ЦПТ для случайных векторов представлена, например, в [13] гл. 1, § 2.

1.3. Условные гауссовские распределения

Представим, что гауссовский вектор ξ размерности n (для краткости далее мы будем писать $\xi \in \mathbb{R}^n$) с математическим ожиданием m и корреляционной матрицей R состоит из двух компонент размерности j и k :

$$\xi = (\xi_1, \xi_2)^T, \quad \xi_1 \in \mathbb{R}^j, \quad \xi_2 \in \mathbb{R}^k, \quad j + k = n.$$

Тогда вектор средних и корреляционную матрицу можно представить в виде

$$m = (m_1, m_2)^T, \quad m_1 \in \mathbb{R}^j, \quad m_2 \in \mathbb{R}^k,$$

$$R = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix},$$

где m_i — математические ожидания, R_{ii} — корреляционные матрицы векторов ξ_i , $i = 1, 2$, а R_{12} — взаимные корреляционные матрицы векторов ξ_1 и ξ_2 .

Предположим теперь, что известно значение вектора $\xi_2 = x$.

Теорема 1.2 (условные гауссовские распределения). Распределение вектора ξ_1 при условии $\xi_2 = x$ является гауссовским с математическим ожиданием

$$m(x) = m_1 + R_{12}R_{22}^{-1}(x - m_2) \quad (1.3.1)$$

и корреляционной матрицей

$$R_{1|2} = R_{11} - R_{12}R_{22}^{-1}R_{21}. \quad (1.3.2)$$

Если матрица R_{22} вырождена и

$$\xi_2 = x \in m_2 + R_{22}(\mathbb{R}^k), \quad (1.3.3)$$

то формулы для условного среднего и корреляционной матрицы примут вид

$$m(x) = m_1 + R_{12}R_{22}^+(x - m_2), \quad (1.3.4)$$

$$R_{1|2} = R_{11} - R_{12}R_{22}^+R_{21}, \quad (1.3.5)$$

где R_{22}^+ — псевдообратная к матрице R_{22} . Если же x не принадлежит носителю распределения ξ_2 , т. е. $x \notin m_2 + R_{22}(\mathbb{R}^k)$, то эти формулы дают значения математического ожидания и корреляционной матрицы гауссовского распределения ξ_1 при условии, что $\|\xi_2 - x\|$ принимает минимальное значение.

Доказательство теоремы для невырожденной матрицы R_{22} можно найти, например, в учебнике [14] (гл. 6, § 6). По поводу доказательств формул (1.3.4), (1.3.5) см. [1].

Упражнение 1.5. (а) Запрограммируйте алгоритм численного моделирования гауссовского вектора ξ_1 при условии минимума $\|\xi_2 - x\|$. Для псевдообращения корреляционной матрицы воспользуйтесь рекуррентными формулами из [1], с. 193.

(б) Выпишите формулы для моделирования трехмерного гауссовского вектора (ξ_1, ξ_2, ξ_3) с заданными средними значениями и корреляционной матрицей с использованием условного распределения ξ_2 при фиксированном ξ_1 и условного распределения ξ_3 при фиксированных значениях ξ_1, ξ_2 . Используйте формулу для обратной матрицы

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - cb} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

(в) Выпишите формулу для моделирования значения винеровского процесса $w(x)$ в точке $c \in (a, b)$ при фиксированных значениях винеровского процесса в точках a и b . При $c = (a+b)/2$ сравните полученные выражения с алгоритмом из [20], с. 93. Указание: покажите, что условное распределение $w(c)$ при условии $w(a)=w_a$, $w(b) = w_b$ является гауссовским с математическим ожиданием

$$\frac{b-c}{b-a}w_a + \frac{c-a}{b-a}w_b$$

и дисперсией

$$\frac{(b-c)(c-a)}{b-a}.$$

1.4. Гауссовские решения линейных систем

Предположим, что о гауссовском случайном векторе $\xi \sim N(m, R)$ имеется дополнительная информация: вектор является решением (недоопределенной) системы линейных алгебраических уравнений $A\xi = b$. Посмотрим, как эта дополнительная информация повлияет на распределение вектора ξ .

Лемма 1.1. Пусть ξ — гауссовский случайный вектор размерности k с математическим ожиданием m и невырожденной корреляционной матрицей R ; A — прямоугольная $l \times k$ -матрица, $0 < l \leq k$, $\text{rang}(A) = l$ (т. е. A — матрица полного ранга); b — вектор размерности l . Тогда условное распределение вектора ξ при условии $A\xi = b$ будет гауссовским с математическим ожиданием

$$m + RA^T(ARA^T)^{-1}(b - Am) \quad (1.4.1)$$

и корреляционной матрицей

$$R - RA^T(ARA^T)^{-1}AR. \quad (1.4.2)$$

Доказательство. Формулы (1.4.1), (1.4.2) следуют (см. теорему 1.2) из того, что случайный вектор $(\xi, A\xi)^T$ является гауссовским с математическим ожиданием $(m, Am)^T$ и корреляционной матрицей

$$\begin{bmatrix} R & RA^T \\ AR & ARA^T \end{bmatrix}.$$

Остается заметить, что квадратная $l \times l$ -матрица ARA^T невырождена, так как ее ранг совпадает с ее размерностью:

$$\text{rang}(ARA^T) = \text{rang}(A\sqrt{R}\sqrt{R}A^T) = \text{rang}(A\sqrt{R}) = \text{rang}(A) = l.$$

Здесь мы воспользовались тем, что $\text{rang}(B) = \text{rang}(BB^*)$, и тем, что ранг прямоугольной матрицы не изменяется при умножении на невырожденную квадратную матрицу (см., например, [10, 24]). \square

Замечание. Если матрица A в условиях леммы 1.1 является квадратной, то линейная система является определенной и гауссовское решение является вырожденным, $\xi \sim N(A^{-1}b, 0)$.

Пример А. Рассмотрим гауссовский двумерный случайный вектор $(\xi_1, \xi_2)^T$ с нулевым математическим ожиданием и корреляционной матрицей

$$\begin{bmatrix} r_1 & r \\ r & r_2 \end{bmatrix}.$$

Условное распределение вектора $(\xi_1, \xi_2)^T$ при $\xi_1 + \xi_2 = b$ является гауссовским с математическим ожиданием

$$cb \begin{bmatrix} r_1 + r \\ r + r_2 \end{bmatrix}$$

и корреляционной матрицей

$$c \begin{bmatrix} d & -d \\ -d & d \end{bmatrix},$$

где $c = 1/(r_1 + 2r + r_2)$, $d = r_1 r_2 - r^2$. Отсюда получаем следующие формулы для численного моделирования:

$$\xi_1 = \left(\frac{r_1 r_2 - r^2}{r_1 + 2r + r_2} \right)^{1/2} \varepsilon + \frac{r_1 + r}{r_1 + 2r + r_2} b, \quad (1.4.3)$$

$$\xi_2 = b - \xi_1.$$

Здесь ε — стандартная нормальная случайная величина.

Пример Б. Воспользовавшись выражением (1.4.3), легко получить формулы моделирования независимых гауссовских случайных величин ξ_1, \dots, ξ_n с нулевым средним и дисперсиями $\sigma_1^2, \dots, \sigma_n^2$ при условии $\xi_1 + \dots + \xi_n = b$:

$$\xi_1 = \left(\frac{\sigma_2^2 + \dots + \sigma_n^2}{\sigma_1^2 + \dots + \sigma_n^2} \right)^{1/2} \sigma_1 \varepsilon_1 + \frac{\sigma_1^2}{\sigma_1^2 + \dots + \sigma_n^2} b,$$

$$\xi_2 = \left(\frac{\sigma_3^2 + \dots + \sigma_n^2}{\sigma_2^2 + \dots + \sigma_n^2} \right)^{1/2} \sigma_2 \varepsilon_2 + \frac{\sigma_2^2}{\sigma_2^2 + \dots + \sigma_n^2} (b - \xi_1),$$

$$\xi_3 = \left(\frac{\sigma_4^2 + \dots + \sigma_n^2}{\sigma_3^2 + \dots + \sigma_n^2} \right)^{1/2} \sigma_3 \varepsilon_3 + \frac{\sigma_3^2}{\sigma_3^2 + \dots + \sigma_n^2} (b - \xi_1 - \xi_2),$$

$$\dots$$

$$\xi_{n-1} = \left(\frac{\sigma_n^2}{\sigma_{n-1}^2 + \sigma_n^2} \right)^{1/2} \sigma_{n-1} \varepsilon_{n-1} + \frac{\sigma_{n-1}^2}{\sigma_{n-1}^2 + \sigma_n^2} (b - \xi_1 - \dots - \xi_{n-2}),$$

$$\xi_n = b - \xi_1 - \xi_2 - \dots - \xi_{n-1}.$$

Здесь $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}$ — независимые стандартные нормальные случайные величины.

Рассмотрим теперь более общую ситуацию. Мы не будем требовать, чтобы A была матрицей полного ранга, и откажемся от условия невырожденности корреляционной матрицы R гауссовского вектора ξ .

Лемма 1.2 (гауссовское решение линейной системы). *Предположим, что система линейных алгебраических уравнений $Ax = b$ совместна.*

А. Пусть ξ — гауссовский случайный вектор с математическим ожиданием m и корреляционной матрицей R такой, что $b - Am \in AR(\mathbb{R}^k)$. Тогда условное распределение вектора ξ при условии $A\xi = b$ будет гауссовским с математическим ожиданием

$$\begin{aligned} \mu &= m + R^{1/2}(AR^{1/2})^+(b - Am) \\ &= m + RA^T(ARA^T)^+(b - Am) \end{aligned} \quad (1.4.4)$$

и корреляционной матрицей

$$B = R - R^{1/2}(AR^{1/2})^+AR = R - RA^T(ARA^T)^+AR. \quad (1.4.5)$$

Б. Если ξ — вектор из независимых стандартных нормальных случайных величин, то формулы для математического ожидания и корреляционной матрицы (1.4.4), (1.4.5) гауссовского решения $A\xi = b$ примут вид

$$\mu = A^+b, \quad (1.4.6)$$

$$B = I - A^+A. \quad (1.4.7)$$

Замечания. (а) Через A^+ здесь и далее обозначается псевдообратная матрица к матрице A . (б) Условие $b - Am \in AR(\mathbb{R}^k)$ означает, что вектор b принадлежит образу носителя распределения гауссовского вектора ξ при преобразовании A .

Приведем **доказательство леммы 1.2**, опирающееся на лемму 1.1 и скелетное разложение матрицы (о скелетном разложении см., например, п. 6.42 в [10] и [50], а также приложение А.2).

Докажем пункт Б. Пусть A — прямоугольная матрица размером $l \times k$ ранга r . Рассмотрим ее скелетное разложение:

$$A = A_1 A_2,$$

где A_1 и A_2 — матрицы ранга r и размеров $l \times r$ и $r \times k$ соответственно. Случайный вектор $\xi_1 = A_2 \xi$ размерности r удовлетворяет уравнению $A_1 \xi_1 = b$. Из условия леммы следует, что система $A_1 \xi_1 = b$ совместна и, значит, эквивалентна системе $A_1^T A_1 \xi_1 = A_1^T b$. Матрица $A_1^T A_1$ как $r \times r$ -матрица ранга r является невырожденной и

$$\xi_1 = (A_1^T A_1)^{-1} A_1^T b = A_1^+ b.$$

Таким образом, условие

$$A\xi = b$$

равносильно

$$A_2 \xi = A_1^+ b,$$

и можно воспользоваться леммой 1.1:

$$\mu = A_2^+ A_1^+ b = A^+ b,$$

$$B = I - A_2^+ A_2 = I - A^+ A.$$

Последнее равенство очевидно:

$$A^+ A = A_2^+ A_1^+ A_1 A_2 = A_2^+ (A_1^T A_1)^{-1} A_1^T A_1 A_2 = A_2^+ A_2.$$

Пункт Б леммы 1.2 доказан.

Для доказательства пункта А представим вектор ξ в виде

$$\xi = Q\varepsilon + m,$$

где ε — вектор из независимых стандартных нормальных случайных величин, $QQ^* = R$. Условие $A\xi = A(Q\varepsilon + m) = b$ дает

$$AQ\varepsilon = b - Am. \quad (1.4.8)$$

Эта система совместна, если $b - Am \in AR(\mathbb{R}^k)$. Применяя пункт Б леммы к гауссовскому вектору ε , получим, что среднее и корреляционная матрица распределения вектора ε при условии (1.4.8) имеют вид

$$\mu_\varepsilon = (AQ)^+(b - Am),$$

$$B_\varepsilon = I - (AQ)^+(AQ),$$

и, значит, условное распределение вектора $\xi = Q\varepsilon + m$ имеет математическое ожидание

$$\mu = Q\mu_\varepsilon + m = m + Q(AQ)^+(b - Am)$$

и корреляционную матрицу

$$B = QB_\varepsilon Q^* = R - Q(AQ)^+(AQ)Q^* = R - Q(AQ)^+ AR.$$

Положив $Q = R^{1/2}$ и учитывая равенство (см., например, [1], с. 36)

$$H^+ = H^T(HH^T)^+, \quad (1.4.9)$$

получим (1.4.4), (1.4.5). Лемма 1.2 доказана. \square

Лемма 1.3. Пусть ξ — вектор из независимых стандартных нормальных случайных величин. Тогда условное распределение вектора ξ при условии, что ξ является псевдорешением системы линейных алгебраических уравнений $A\xi = b$, будет гауссовским с математическим ожиданием (1.4.6) и корреляционной матрицей (1.4.7): $\mu = A^+ b$, $B = I - A^+ A$.

Лемма 1.3 является простым следствием п. Б леммы 1.2. Действительно, все псевдорешения уравнения $A\xi = b$ и только они являются решениями совместной линейной системы уравнений $A^T A\xi = A^T b$. Учитывая свойство псевдообращения матрицы (1.4.9), получим требуемое. \square

Гауссовские решения систем линейных уравнений использовались в [33, 34, 86, 87] для построения условных спектральных моделей гауссовских полей, которые в свою очередь применялись для численного моделирования гигантских морских волнубийц [25, 88, 89].

1.5. Распределение гауссовского вектора в правой части совместной линейной системы уравнений

Предположим, что известны математическое ожидание и корреляционная матрица n -мерного гауссовского вектора $\xi \sim N(m, R)$. Предположим также, что задана некоторая матрица A , содержащая n строк, и имеется дополнительная информация, которая состоит в том, что существует решение линейной системы с матрицей A и вектором ξ в качестве правой части. Следующее утверждение отвечает на вопрос, как дополнительная информация отражается на распределении случайного вектора ξ .

Лемма 1.4. Пусть $x \in \mathbb{R}^k$, A — $n \times k$ -матрица, ξ — n -мерный гауссовский случайный вектор с математическим ожиданием m и корреляционной матрицей R .

1. Рассмотрим проектор P на ядро матрицы A^T :

$$P = I - AA^+ = Pr(\text{Ker}(A^T)).$$

Условие

$$Pt \in PR(\mathbb{R}^n) \quad (1.5.1)$$

является необходимым и достаточным для существования векторов $y \in R(\mathbb{R}^n) + t$, принадлежащих носителю распределения $\xi \sim N(m, R)$, для которых система $Ax = y$ совместна.

2. Предположим, что (1.5.1) выполнено. Распределение вектора ξ при условии, что существует решение системы $Ax = \xi$, будет гауссовским с математическим ожиданием Qt и корреляционной матрицей QR , где

$$Q = I - RP(PR^+P) = I - R^{1/2}(PR^{1/2})^+P. \quad (1.5.2)$$

3. Уравнение $Ax = \xi$ однозначно определяет распределение вектора x тогда и только тогда, когда выполнено условие (1.5.1) и условие

$$\text{rang}(A) = k \quad (u, \text{ значит, } n \geq k). \quad (1.5.3)$$

При этом вектор $x = A^+\xi$ будет распределен по гауссовскому закону со средним A^+Qt и корреляционной матрицей $A^+QR(A^+)^T$.

Доказательство. 1. Совместность системы $Ax = y$ равносильна тому, что $y \perp \text{Ker}(A^T)$. Так как проектор на ядро A^T представляется в виде $P = I - AA^+$ (соответствующие сведения можно найти, например, в [10], § 6), то совместность линейной системы эквивалентна равенству $Pu = 0$. Предположим теперь, что вектор y принадлежит носителю гауссовского распределения $N(m, R)$. Тогда y можно представить в виде суммы $m + z$, где $z \in R(\mathbb{R}^n)$. Нетрудно убедиться, что существование $z \in R(\mathbb{R}^n)$ таких, что выполнено равенство $P(m + z) = 0$ означает (1.5.1).

2. По условию леммы $\xi \sim N(m, R)$. Условие (1.5.1) означает, что для некоторых выборочных значений ξ система $Ax = \xi$ будет совместной. Информация о том, что существует решение x системы $Ax = \xi$ равносильна тому, что $(I - AA^+)\xi = P\xi = 0$ (см. приложение А.4). Остается воспользоваться частью А леммы 1.2. Формулы (1.4.4), (1.4.5) дадут выражения Qt и QR соответственно для математического ожидания и корреляционной матрицы условного распределения ξ .

3. Предположим, что выполнено (1.5.1) и (1.5.3). Условие (1.5.1) означает, что имеется непустое множество векторов y из носителя гауссовского распределения $N(m, R)$, для которых система $Ax = y$ является совместной. (Из пункта 2 леммы следует, что это множество можно представить в виде $\{y \in Qm + QR(\mathbb{R}^n)\}$, где Q определено формулой (1.5.2)). Условие (1.5.3) гарантирует однозначную разрешимость системы $Ax = y$. Решение определяется выражениями $A^T Ax = A^T y$, $x = (A^T A)^{-1} A^T y = A^+ y$. Таким образом, $x = A^+ \xi$, где, как мы знаем из п. 2, $\xi \sim N(Qm, QR)$. Отсюда следует, что распределение вектора x однозначно определено и оно является гауссовским со средним A^+Qt и корреляционной матрицей $A^+QR(A^+)^T$,

т. е. $x \sim N(A^+Qm, A^+QR(A^+)^T)$. В одну сторону утверждение п. 3 леммы доказано.

Отметим, что здесь мы воспользовались следующими известными утверждениями о матрицах и линейных системах (см., например, [10], шп. 6.19, 6.36, 6.46):

- совместная система имеет единственное решение тогда и только тогда, когда ранг матрицы системы равен числу неизвестных;

- если система $Ax = y$ совместна, то она эквивалентна системе $A^T Ax = A^T y$;

- если A является $n \times k$ -матрицей и $n \geq k$, то

$$A^+ = (A^T A)^{-1} A^T.$$

В обратную сторону п. 3 леммы доказывается элементарно. То, что распределение вектора x определяется однозначно, подразумевает существование решений для некоторых $y \in m + R(\mathbb{R}^n)$ и их единственность. Таким образом, должно выполняться (1.5.1) и (1.5.3). \square

Лемма 1.4 использовалась в работах [34, 38, 71, 87] при исследовании краевых задач для линейных стохастических дифференциальных уравнений.

Глава 2

Численное моделирование гауссовских распределений

2.1. Моделирование нормальных случайных величин

Для моделирования пары независимых гауссовских случайных величин $\varepsilon_1, \varepsilon_2$ с нулевым средним и единичной дисперсией можно воспользоваться формулами

$$a_1 = \cos(2\pi\alpha_2), \quad a_2 = \sin(2\pi\alpha_2), \quad (2.1.1)$$

$$R = (-2 \ln \alpha_1)^{1/2}, \quad (2.1.2)$$

$$\varepsilon_1 = Ra_1, \quad \varepsilon_2 = Ra_2, \quad (2.1.3)$$

где α_1, α_2 – независимые случайные величины, равномерно распределенные на отрезке $(0, 1)$. Этот метод моделирования называют методом Бокса – Мюллера (см. [60, 81, 82]), а его обоснование можно найти, например, в [9, 30].

Ниже приводится текст процедуры, написанной на паскале и реализующей метод Бокса – Мюллера:

```
{*
  Simulation of a standard Gaussian random variable
*}
Function GaussRN: Real;
Const GaussRNconst:integer=1;  GaussRNtmp:real=0;
var  R,Fi: real;
Begin
  if GaussRNconst>0 then
  begin
    R:=sqrt(-2*ln(Random));
    Fi:=2*PI*Random;
    GaussRNtmp:=R*cos(Fi);
```

```

GaussRN:=R*sin(Fi);
GaussRNconst:=-GaussRNconst;
end
else
begin
  GaussRN:=GaussRNtmp;
  GaussRNconst:=-GaussRNconst;
end;
End;

```

Случайный вектор (a_1, a_2) является изотропным на единичной окружности с центром в нуле, т. е. равномерно распределен на окружности. Для его моделирования можно использовать метод исключения:

- 1) $a_1 = 1 - 2\beta_1, \quad a_2 = 1 - 2\beta_2, \quad d = a_1^2 + a_2^2;$
- 2) если $d > 1$, то возвращаемся на 1, иначе
 $c = 1/\sqrt{d}, \quad a_1 = ca_1, \quad a_2 = ca_2.$

Здесь β_1, β_2 – независимые случайные величины, равномерно распределенные на интервале $(0, 1)$. В те времена, когда вычисление тригонометрических функций на компьютерах было существенно более трудоемким, метод исключения был заметно быстрее, чем моделирование по формулам (2.1.1). Соответствующую модификацию метода Бокса – Мюллера иногда называют полярным методом.

Упражнение 2.1. Сравните быстродействие моделирования двумерного изотропного вектора методом исключения и по формулам (2.1.1) на современных компьютерах для разных генераторов псевдослучайных чисел из приложения Б.

Упражнение 2.2. Докажите, что $(\xi_1, \dots, \xi_n)^T \sim N(0, I)$ тогда и только тогда, когда

$$\xi_k = Xa_k, \quad k = 1, \dots, n. \quad (2.1.4)$$

Здесь (a_1, \dots, a_n) – изотропный случайный вектор (единичной длины) в n -мерном пространстве, X – независимая от этого вектора случайная величина с χ -распределением Пирсона, I – единичная $n \times n$ -матрица. Для доказательства воспользуйтесь формулой для плотности p_η случайного вектора $\eta = f(\xi)$, полученного взаимно однозначным преобразованием f вектора ξ с плотностью p_ξ :

$$\eta = f(\xi), \quad \eta = (\eta_1, \dots, \eta_n) = (f_1(\xi_1), \dots, f_n(\xi_n)),$$

$$\xi = g(\eta), \quad \xi = (\xi_1, \dots, \xi_n) = (g_1(\eta_1), \dots, g_n(\eta_n)).$$

$$p_\eta(y_1, \dots, y_n) = p_\xi(g(y_1, \dots, y_n)) |J_g(y_1, \dots, y_n)|,$$

где $g = f^{-1}$, J_g – якобиан обратного преобразования:

$$J_g = \begin{vmatrix} \frac{\partial g_1}{\partial y_1} & \frac{\partial g_1}{\partial y_2} & \cdots & \frac{\partial g_1}{\partial y_n} \\ \frac{\partial g_2}{\partial y_1} & \frac{\partial g_2}{\partial y_2} & \cdots & \frac{\partial g_2}{\partial y_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial g_n}{\partial y_1} & \frac{\partial g_n}{\partial y_2} & \cdots & \frac{\partial g_n}{\partial y_n} \end{vmatrix}.$$

(Точные формулировки утверждений о плотности вероятностей преобразования случайных векторов можно найти в [22, 23, 80].)

Напомним, что χ -распределение Пирсона с n степенями свободы имеет плотность

$$\frac{1}{2^{n/2-1}\Gamma(n/2)} x^{n-1} \exp(-\frac{x^2}{2}), \quad x > 0, \quad (2.1.5)$$

где $n > 0$ и необязательно целое. Математическое ожидание определяется выражением

$$m_\chi = \sqrt{2} \frac{\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n}{2})},$$

а дисперсия равна $n - m_\chi^2$. При целых n математическое ожидание можно представить в виде

$$m_\chi = \begin{cases} \frac{(n-1)!!}{(n-2)!!} \sqrt{\pi/2}, & n - \text{четное,} \\ \frac{(n-1)!!}{(n-2)!!} \sqrt{2/\pi}, & n - \text{нечетное.} \end{cases}$$

Здесь двойной факториал $k!!$ обозначает произведение всех натуральных чисел от 1 до k , имеющих ту же четность, что и значение k .

Упражнение 2.3. Из выражения (2.1.5) для плотности χ -распределения получите выражение

$$\frac{1}{2^{n/2}\Gamma(n/2)} x^{n/2-1} \exp(-\frac{x}{2}), \quad x > 0. \quad (2.1.6)$$

для плотности χ^2 -распределения. Найдите математическое ожидание и дисперсию для распределения χ^2 с n степенями свободы.

Упражнение 2.4. Докажите, что изотропный вектор (a, b, c) на трехмерной сфере единичного радиуса можно моделировать по формулам

$$c = 2\alpha_1 - 1, \quad a = \sqrt{1 - c^2} \cos 2\pi\alpha_2, \quad b = \sqrt{1 - c^2} \sin 2\pi\alpha_2,$$

где α_1, α_2 – независимые случайные величины, равномерно распределенные на интервале $(0, 1)$.

Упражнение 2.5. Найдите эффективные формулы для моделирования изотропного вектора (a_1, \dots, a_n) на единичной сфере четной размерности n . Если такие формулы удастся найти, то изучите возможность моделирования вектора $(\xi_1, \dots, \xi_n)^T \sim N(0, I)$ по формулам (2.1.4). Заметим, что случайную величину с χ -распределением Пирсона при четных n можно моделировать по формуле (см., например, [8])

$$\sqrt{-2 \ln \left(\prod_{i=1}^{n/2} \alpha_i \right)}.$$

Здесь α_i – независимые случайные величины, равномерно распределенные на интервале $(0, 1)$. Изучите работы, в которых рассматривается проблема моделирования многомерного изотропного случайного вектора (см., в частности, [73]).

Приближенные методы моделирования стандартных нормальных случайных величин можно построить на основе ЦПТ (см. теорему 1.1), рассматривая суммы независимых одинаково распределенных случайных величин η :

$$\omega_n = \frac{1}{\sqrt{n\mathbf{D}\eta}} \left(\sum_{i=1}^n \eta_i - n\mathbf{M}\eta \right). \quad (2.1.7)$$

Например, если в качестве η взять случайную величину α , равномерно распределенную на $(0, 1)$ ($\mathbf{M}\alpha = 0.5$, $\mathbf{D}\alpha = 1/12$), то для $n = 12$ получим формулу

$$\sum_{i=1}^{12} \alpha_i - 6,$$

которую можно использовать для приближенного моделирования стандартной нормальной величины. Однако приближенными формулами следует пользоваться с осторожностью, учитывая специфику решаемой задачи и особенности приближенного распределения.

Замечание. Множество других приближенных методов можно найти, например в [15]. В частности, там приводятся следующие формулы приближенного моделирования гауссовских случайных величин с нулевым средним и единичной дисперсией:

$$\varepsilon(\omega_n) = \omega_n + \frac{1}{20n} (\omega_n^3 - 3\omega_n),$$

$$\varepsilon(\omega_n) = \omega_n - \frac{41}{13440n^2} (\omega_n^5 - 10\omega_n^3 + 15\omega_n). \quad (2.1.8)$$

где ω_n моделируются согласно (2.1.7). Утверждается, что случайные величины $\varepsilon(\omega_n)$ являются асимптотически нормальными с более высоким порядком сходимости, чем в ЦПТ, а формула (2.1.8) дает хорошее приближение уже при $n = 2$.

2.2. Общие методы моделирования гауссовских случайных векторов

Если $\xi = A\varepsilon$ – линейное преобразование гауссовского вектора ε с нулевым средним и корреляционной матрицей R_ε , то вектор ξ будет гауссовским с нулевым средним и корреляционной матрицей $R = AR_\varepsilon A^T$. Этот факт используется для моделирования гауссовских векторов: пусть ε – вектор из независимых стандартных нормальных величин ($R_\varepsilon = I$ – единичная матрица), и известно представление $R = AA^T$, тогда гауссовский вектор ξ с математическим ожиданием m и корреляционной матрицей R можно моделировать по формуле $\xi = A\varepsilon + m$.

2.2.1. Квадратный корень из корреляционной матрицы

Если $R = AA^T$, и $A = A^T$ – симметричная положительно определенная матрица, то A является *квадратным корнем* корреляционной матрицы R , $A = R^{1/2}$. Для любой положительно определенной матрицы R существует единственный квадратный корень A , $R = AA$. Строгая положительная определенность R эквивалентна строгой положительной определенности A . Матрицу A можно приближенно вычислять с помощью рекуррентной процедуры

$$A_0 = 0, \quad A_{k+1} = A_k + (2\|R\|_2^{1/2})^{-1}(R - A_k^2) \quad (2.2.1)$$

(см., например, задачу 567 в [21] и п. 104 в [42]). Здесь $\|R\|_2$ обозначает спектральную норму матрицы R , индуцированную

евклидовой нормой векторов. Так как R положительно определенная, то ее спектральная норма совпадает с максимальным собственным числом (спектральным радиусом). Вместо $\|R\|_2$ в формуле (2.2.1) можно брать заведомо большее число. Например, можно использовать норму Фробениуса $\|R\|_E$, которую называют также евклидовой матричной нормой:

$$\|R\|_E = \sqrt{\sum_i \sum_j R_{ij}^2} = \sqrt{\text{tr}(R^2)} = \sqrt{\sum_i \lambda_i^2(R)} \geq \|R\|_2.$$

Здесь $\lambda_i^2(R)$ – собственные числа матрицы R , а tr обозначает след матрицы.

Кроме того, матрица A может быть найдена по формуле

$$A = W(D)^{1/2}W^T, \quad (2.2.2)$$

где D – диагональная матрица с собственными числами матрицы R по диагонали, а W – матрица, столбцы которой состоят из собственных векторов матрицы R ,

$$R = WDW^T. \quad (2.2.3)$$

Замечание. Соответствующие результаты о представлении (2.2.3) для симметричных матриц и представлении (2.2.2) для квадратного корня положительно определенной матрицы можно найти в учебниках по теории матриц (см., например, [24]). Представление (2.2.3) является частным случаем *сингулярного разложения*, которое для произвольной прямоугольной матрицы B запишется в виде

$$B = WDV,$$

где столбцы матрицы W образуют ортонормированный базис из собственных векторов матрицы BB^T , столбцы матрицы V образуют ортонормированный базис из собственных векторов матрицы $B^T B$, а D – диагональная матрица с сингулярными числами матрицы B на диагонали (сингулярные числа – это неотрицательные значения квадратных корней общих собственных чисел матриц BB^T и $B^T B$).

Упражнение 2.6. Докажите, что если симметричная $n \times n$ -матрица A имеет вид

$$\begin{bmatrix} a_0 & a & \dots & a \\ a & a_0 & \dots & a \\ \dots & \dots & \dots & \dots \\ a & a & \dots & a_0 \end{bmatrix}, \quad (2.2.4)$$

то для матрицы $R = A^2$ выполнено

$$R = \begin{bmatrix} r_0 & r & \dots & r \\ r & r_0 & \dots & r \\ \dots & \dots & \dots & \dots \\ r & r & \dots & r_0 \end{bmatrix}, \quad (2.2.5)$$

где

$$\begin{aligned} r_0 &= a_0^2 + (n-1)a^2, \\ r &= 2aa_0 + (n-2)a^2. \end{aligned} \quad (2.2.6)$$

Найдите все решения системы уравнений (2.2.6) относительно неизвестных a_0, a . Убедитесь, что решениями, в частности, являются

$$a = [-\sqrt{r_0 - r} \pm \sqrt{r_0 + (n-1)r}]/n, \quad a_0 = \sqrt{r_0 - r} + a.$$

Выясните, какое решение дает положительно определенную матрицу A .

2.2.2. Моделирование на основе разложения Холецкого

Потребуем теперь, чтобы A была нижней треугольной матрицей. Это приведет к известным рекуррентным формулам на элементы матрицы A_{rt} (см., например, [20]):

$$\begin{aligned} A_{11} &= (R_{11})^{1/2}, \\ A_{rt} &= \left(R_{rt} - \sum_{k=1}^{t-1} A_{rk}A_{tk} \right) / A_{tt}, \quad t = 1, \dots, r-1, \end{aligned} \quad (2.2.7)$$

$$A_{rr} = \left(R_{rr} - \sum_{t=1}^{r-1} A_{rt}^2 \right)^{1/2}, \quad r = 2, \dots, n.$$

Представление (симметричной) положительно определенной матрицы R в виде произведения AA^T , где A – нижняя треугольная, называют *разложением Холецкого* (в отечественной литературе используется также термин «метод квадратного корня»). Если матрица R строго положительно определена (т. е. положительно определена и невырождена), то существует единственное разложение Холецкого $R = AA^T$ с нижней треугольной матрицей A , диагональные элементы которой (строго) положительны, см. теорему 4.2.5 в [16, 72].

Вычисления элементов нижней треугольной матрицы A по формулам (2.2.7) можно проводить, начиная с верхнего левого угла, по строкам (алгоритм Холецкого – Банашевича) или по столбцам (алгоритм Холецкого – Краута). Строгая положительная определенность матрицы R гарантирует положительность выражения $R_{rr} - \sum_{t=1}^{r-1} A_{rt}^2$ в (2.2.7).

Алгоритм Холецкого – Банашевича.

```
A[1,1]:=sqrt(R[1,1]);

for r:=2 to n do
begin
  for t:=1 to r-1 do
  begin
    tmp:=0.0;
    for k:=1 to t-1 do tmp:=tmp+A[r,k]*A[t,k];
    A[r,t]:=(R[r,t]-tmp)/A[t,t];
  end;
  tmp:=0.0;
  for k:=1 to r-1 do tmp:=tmp+sqrt(A[r,k]);
  A[r,r]:=sqrt(R[r,r]-tmp);
end;
```

Разложение Холецкого можно применять и для вырожденных положительно определенных матриц (см., например, [16, 72, 76]). В частности, известно [76], что для (вырожденной) положительно определенной матрицы R найдется нижняя треугольная матрица A с неотрицательными элементами на диагонали такая, что $R = AA^T$.

Некоторые значения A_{tt} в разложении Холецкого $R = AA^T$ для вырожденной $n \times n$ -матрицы R принимают нулевые значения. Это означает, что компонента ξ_t случайного вектора $\xi = A\varepsilon$, где $\xi \sim N(0, R)$, $\varepsilon \sim N(0, I)$, линейно зависит от предыдущих компонент ξ_1, \dots, ξ_{t-1} и $\varepsilon_1, \dots, \varepsilon_{t-1}$. Следовательно, можно выбрать такое линейное преобразование $\xi = A\varepsilon$ с нижней треугольной матрицей A , что случайная величина ε_t вообще не будет использоваться этим линейным преобразованием, т. е. $A_{rt} = 0$ при $r \geq t$. Таким образом, естественная модификация метода Холецкого (2.2.7) для вырожденных матриц состоит в следующем:

$$\text{если } A_{tt} = 0, \text{ то } A_{rt} = 0, \quad r = t + 1, \dots, n. \quad (2.2.8)$$

Предположим теперь, что матрица \hat{A} состоит из ненулевых столбцов матрицы A . Матрица \hat{A} будет прямоугольной с n строками и $\text{rang}(R) = \text{rang}(A) = \text{rang}(\hat{A})$ столбцами. Тогда гауссовский случайный вектор $\xi \sim N(0, R)$ можно моделировать по формуле $\xi = \hat{A}\hat{\varepsilon}$, где $\hat{\varepsilon}$ – вектор размерности $\text{rang}(R)$, состоящий из независимых стандартных нормальных случайных величин.

Замечание. В работе [51] на стр. 27 описывается модификация алгоритма Холецкого – Банашевича для вырожденных матриц, в которой сразу формируется матрица \hat{A} .

Ниже приведен алгоритм Холецкого – Краута для вырожденных матриц из [16, 72].

Алгоритм Холецкого – Краута (здесь элементы нижней треугольной матрицы A записываются на соответствующие места исходной матрицы R).

```

for t:=1 to n do
  if R[t,t]>0 then
    begin
      R[t,t]:=sqrt(R[t,t]);

      for r:=t+1 to n do R[r,t]:=R[r,t]/R[t,t];

      for k:=t+1 to n do for m:=k to n do
        R[m,k]:=R[m,k] - R[m,t]R[k,t];
    end;

```

Упражнение 2.7. (а) Покажите, что выше приведенный алгоритм Холецкого – Краута порождает нижнюю треугольную матрицу, удовлетворяющую условию (2.2.8).

(б) Разработайте модификации алгоритмов Холецкого – Банашевича и Холецкого – Краута, которые вычисляют непосредственно матрицу \hat{A} .

(в) Предложите свои модификации разложения Холецкого для вырожденных матриц, отличные от (2.2.8).

Упражнение 2.8. (а) Проверьте следующее утверждение: разложение вещественной симметричной положительно определенной матрицы $R = AA^T$ определяется однозначно с точностью до ортогонального оператора: $R = AA^T = AU(AU)^T$, $UU^T = I$. Используйте полярное разложение матриц (см. приложение А.5).

(б) Предложите свой метод разложения $R = AA^T$, отличный от рассмотренных выше. Запрограммируйте алгоритмы моделирования гауссовского вектора с заданными вектором средних значений и корреляционной матрицей, используя различные способы разложения корреляционной матрицы. Сравните быстродействие алгоритмов.

Глава 3

Примеры моделирования

Ниже мы кратко рассмотрим несколько примеров моделирования гауссовских многомерных распределений.

3.1. Моделирование гауссовского вектора с равноправными компонентами

Рассмотрим более подробно методы моделирования гауссовского вектора ξ с нулевым средним и корреляционной матрицей

$$R = \begin{bmatrix} 1 & r & \dots & r \\ r & 1 & \dots & r \\ \dots & \dots & \dots & \dots \\ r & r & \dots & 1 \end{bmatrix} = (1-r)I + rE. \quad (3.1.1)$$

Здесь I – единичная матрица, E – матрица, все элементы которой равны единице. Матрицу R называют *эквикорреляционной*, а соответствующие случайные векторы (необязательно гауссовские) – *эквикоррелированными*. Случайный вектор, распределение которого не зависит от порядка его компонент, естественно называть вектором с *равноправными* компонентами. Используется также термин «перестановочно-симметричный вектор» [96]. Очевидно, что гауссовский эквикоррелированный случайный вектор с нулевым средним имеет равноправные компоненты.

Положительная определенность матрицы (3.1.1) равносильна условию [58, 96]

$$r \in [-1/(n-1), 1]. \quad (3.1.2)$$

При $r > 0$ случайный гауссовский вектор $\xi = (\xi_1, \dots, \xi_n)$ можно моделировать по формуле

$$\xi_i = (1-r)^{1/2}\varepsilon_i - r^{1/2}\varepsilon_0, \quad (3.1.3)$$

где ε_i , $i = 0, 1, 2, \dots, n$ – независимые стандартные нормальные случайные величины.

Собственные числа и векторы $(n \times n)$ -матрицы (3.1.1) имеют вид [96]:

$$\lambda_1 = 1 + (n-1)r, \quad (3.1.4)$$

$$w_1 = (1, \dots, 1)^T / \sqrt{n}, \quad (3.1.5)$$

$$\lambda_i = 1 - r, \quad i = 2, \dots, n, \quad (3.1.6)$$

$$w_2 = (1, -1, 0, \dots, 0)^T / \sqrt{2},$$

$$w_3 = (1, 1, -2, \dots, 0)^T / \sqrt{6},$$

$$\dots$$

$$w_n = (1, \dots, 1, -(n-1))^T / \sqrt{n(n-1)}. \quad (3.1.7)$$

Детерминант матрицы R выражается формулой

$$\det(R) = [1 + (n-1)r][1 - r]^{n-1}. \quad (3.1.8)$$

Упражнение 3.1. (а) Разработайте алгоритм моделирования гауссовского вектора $\xi \sim N(0, R)$ с корреляционной матрицей (3.1.1), используя представление $\xi = \sqrt{R}\varepsilon$, $\varepsilon \sim N(0, I)$ и выражения, полученные, для \sqrt{R} на основе (3.1.4)-(3.1.7) (см. пункт 2.2.1).

(б) Найдите разложение Холецкого для матрицы (3.1.1).

Результаты численного моделирования эквикоррелированных гауссовских случайных векторов (по 200 компонент) с нулевым средним представлены на рис. 3.1

3.2. О моделировании гауссовских векторов стационарного типа

В этом параграфе мы кратко остановимся на проблеме моделирования гауссовских векторов стационарного типа. Под

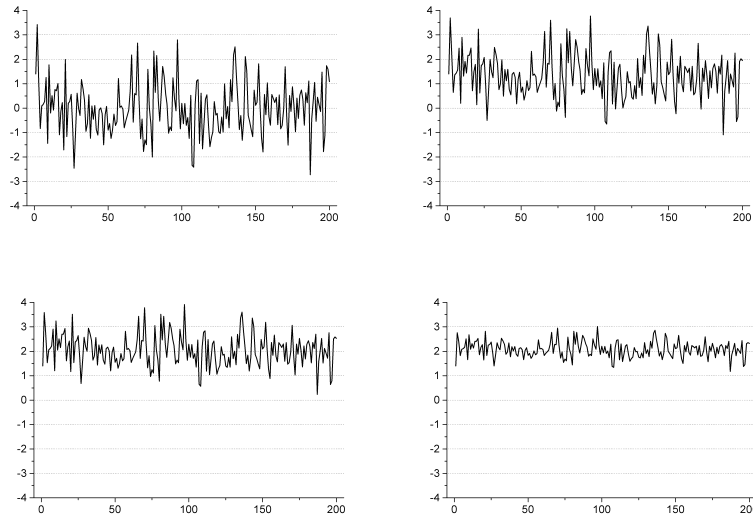


Рис. 3.1. Реализации гауссовских эквикоррелированных случайных векторов с нулевым средним для $r = -1/199$ (слева сверху), $r = 0.3$ (справа сверху), $r = 0.6$ (слева внизу), $r = 0.9$ (справа внизу). Реализации моделировались с помощью разложения Холецкого и одной (для всех четырех векторов) выборки независимых стандартных нормальных случайных величин

случайным вектором стационарного типа мы будем понимать «кусоч» стационарной последовательности или, как еще говорят, стационарного *временного ряда*. Приведем соответствующие определения.

Случайную последовательность $x(n)$, $n = \dots, -1, 0, 1, \dots$, называют *стационарной в узком смысле* (или сильно стационарной), если ее конечномерные распределения совпадают с конечномерными распределениями последовательности $x(n + m)$ для любого целого m .

Случайная последовательность является *стационарной в широком смысле* (или слабо стационарной), если ее математи-

ческое ожидание является константой, $\mathbf{M}x(n) = \text{const}$, а корреляционная функция

$$K_x(n_1, n_2) = \mathbf{M}[x(n_1) - \mathbf{M}x(n_1)][x(n_2) - \mathbf{M}x(n_2)]$$

зависит лишь от разницы $n_2 - n_1$. Корреляционную функцию стационарного процесса мы будем обозначать той же буквой, подразумевая теперь

$$K_x(n) = \mathbf{M}[x(m) - \mathbf{M}x(m)][x(n + m) - \mathbf{M}x(n + m)].$$

Очевидно, что в общем случае из сильной стационарности следует слабая стационарность, а для гауссовских последовательностей оба определения эквивалентны.

Свойства (1.2.6)-(1.2.8) для стационарной последовательности запишутся в виде

$$(1) \quad K_x(0) \geq 0, \tag{3.2.1}$$

$$(2) \quad K_x(n) = \overline{K_x(-n)}, \tag{3.2.2}$$

$$(3) \quad |K_x(n)| \leq K_x(0), \tag{3.2.3}$$

$$(4) \quad |K_x(n_3 - n_1) - K_x(n_3 - n_2)|^2 \leq 2K_x(0)[K_x(0) - \text{Re } K_x(n_2 - n_1)]. \tag{3.2.4}$$

Приведем еще одно свойство корреляционной функции стационарного процесса, которое было отмечено, в частности, в работах [39, 40] и монографии [35]:

$$K_x(0) - \text{Re } K_x(j) \leq j^2 [K_x(0) - \text{Re } K_x(1)], \quad j = 1, 2, \dots \tag{3.2.5}$$

Для большей наглядности неравенство (3.2.5) перепишем в следующем виде

$$\text{Re } K_x(j) \geq K_x(0) - j^2 [K_x(0) - \text{Re } K_x(1)], \quad j = 1, 2, \dots \tag{3.2.6}$$

Смысл этого неравенства для вещественных корреляционных функций состоит в следующем. Рассмотрим график произвольной вещественной корреляционной функции $K_x(n)$ и параболу,

проходящую через точки $(0, K_x(0)), (1, K_x(1)), (-1, K_x(1))$. Тогда точки $(j, K_x(j))$ для любого целого j расположены не ниже этой параболы (см. пример на рис. 3.2).

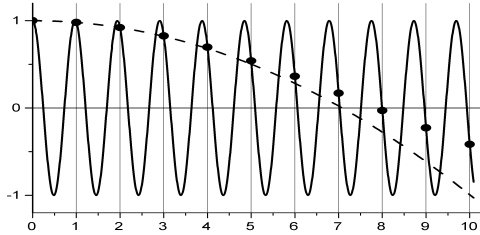


Рис. 3.2. Иллюстрация свойства (3.2.5), (3.2.6) для корреляционной функции $K_x(j) = \cos(Aj)$, $A = 2\pi + 0.2$: $\cos(Aj) \geq 1 - j^2[1 - \cos(A)]$

Упражнение 3.2. (а) Докажите неравенства (3.2.5), (3.2.6). Воспользуйтесь тождеством

$$x(j) - x(0) = \sum_{k=1}^j [x(k) - x(k-1)]$$

и вытекающим из него неравенством

$$\mathbf{M}|x(j) - x(0)|^2 \leq j^2 \mathbf{M}|x(1) - x(0)|^2.$$

(б) Докажите следующее утверждение: для произвольной корреляционной функции стационарного процесса выполнено

$$\begin{aligned} & \operatorname{Re} K_x(j-1) - 2 \operatorname{Re} K_x(j) + \operatorname{Re} K_x(j+1) \\ & \leq 2j^2 [K_x(0) - 2 \operatorname{Re} K_x(1) + \operatorname{Re} K_x(2)] - \\ & 2[K_x(0) - \operatorname{Re} K_x(1)] + j^2 [K_x(0) - \operatorname{Re} K_x(2)], \quad j = 1, 2, \dots \end{aligned} \quad (3.2.7)$$

Воспользуйтесь равенством

$$\begin{aligned} & \sum_{k=1}^j [x(k+1) - 2x(k) + x(k-1)] \\ & = x(j+1) - x(j) - x(1) + x(0). \end{aligned}$$

Дайте наглядную интерпретацию свойства (3.2.7).

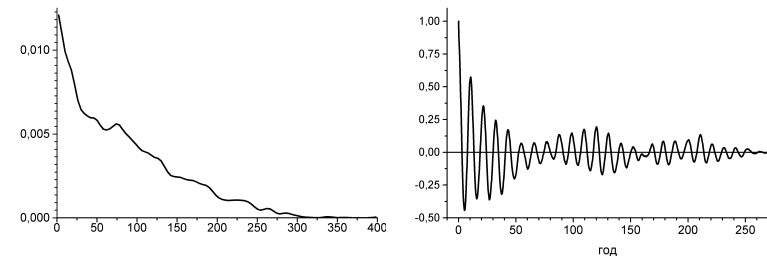
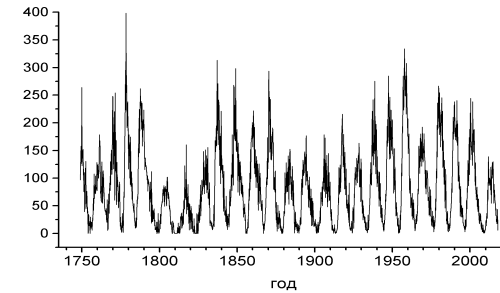


Рис. 3.3. Случайная последовательность среднемесячных чисел Вольфа (вверху), характеризующих солнечную активность за период с января 1749 г. по декабрь 2017 г., оценки плотности одномерного распределения (внизу слева) и нормированной корреляционной функции (внизу справа) последовательности чисел Вольфа

В качестве примера стационарной последовательности приведем график солнечной активности за 269 лет. На рис. 3.3 представлены 3228 среднемесячных чисел Вольфа (см. [95]), характеризующих солнечную активность за период с января 1749

г. по декабрь 2017 г., а также оценки нормированной корреляционной функции и плотности одномерного распределения рассматриваемой случайной последовательности. Обратите внимание, что локальные максимумы корреляционной функции соответствуют периодам солнечной активности, приблизительно равным 11, 120 и 210 лет.

Случайная последовательность чисел Вольфа не является гауссовской (одномерное распределение больше похоже на экспоненциальное). Если известна корреляционная функция и одномерное распределение стационарного случайного процесса, то для его моделирования можно применить достаточно универсальный метод, основанный на нелинейном преобразовании гауссовского процесса. Описание метода можно найти в [34], а некоторые его применения, в том числе для численного моделирования временных рядов сетевого трафика и стохастической структуры полей атмосферной облачности, представлены в работах [31, 36, 37, 90, 91]. Рис. 3.4 демонстрирует использование этого метода для моделирования временного ряда, имитирующего солнечную активность. На предварительном этапе (см. рис. 3.4 слева) моделируется гауссовский вектор стационарного типа с корреляционной функцией, близкой к той, которая изображена на рис. 3.3, а затем (см. рис. 3.4 справа) с помощью нелинейного преобразования вычисляется негауссовская случайная последовательность с требуемой плотностью одномерного распределения (как на рис. 3.3).

Очевидно, что корреляционная матрица случайного вектора стационарного типа имеет вид

$$\begin{bmatrix} R(0) & R(1) & \dots & R(N-2) & R(N-1) \\ R(1) & R(0) & \dots & R(N-3) & R(N-2) \\ \dots & \dots & \dots & \dots & \dots \\ R(N-2) & R(N-3) & \dots & R(0) & R(1) \\ R(N-1) & R(N-2) & \dots & R(1) & R(0) \end{bmatrix}, \quad (3.2.8)$$

т. е. является симметричной *теплицевой* матрицей (матрицей Тёплица называется «диагонально-постоянная» матрица, для

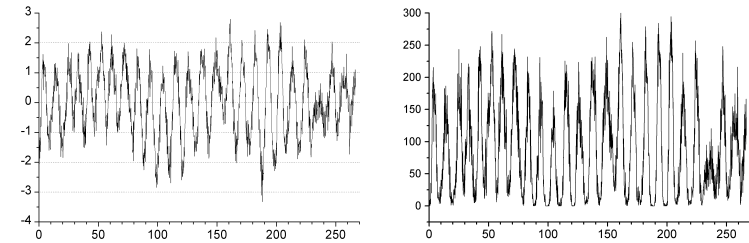


Рис. 3.4. Стохастическая имитация временного ряда, представленного на рис. 3.3: реализация вспомогательного гауссовского вектора (слева) и негауссовская последовательность (справа), которая имеет требуемую корреляционную функцию и одномерное распределение

которой выполнено $R_{ij} = R_{i-1,j-1}$). Для моделирования гауссовских векторов стационарного типа можно применять общие методы, рассмотренные во второй главе. Однако специальные методы, которые мы не рассматриваем в данном пособии, позволяют проводить моделирование более эффективно. Ниже даны ссылки на работы, которые помогут при изучении методов моделирования гауссовских векторов с учетом свойства стационарности.

1. Для разложения Холецкого корреляционной матрицы в общем случае требуется $O(N^3)$ арифметических операций с плавающей точкой. В литературе можно встретить утверждение о том, что нет более быстрых алгоритмов для теплицевых корреляционных матриц (см., например, [74] и [75] стр.347). Однако быстрые модификации разложения Холецкого с числом операций $O(N^2)$ для корреляционных матриц стационарного вида (3.2.8) существуют, см. [44] на стр. 18 и [94].
2. Другой известный подход к моделированию случайных векторов состоит в моделировании каждого следующего элемента $x(n)$ по условному распределению, зависящему

от уже имеющихся элементов $x(1), \dots, x(n-1)$. При этом для моделирования стационарного гауссовского вектора используются соотношения вида

$$x(n) = \sum_{k=1}^{n-1} b_k^{(n)} x(n-k) + c_n \varepsilon_n,$$

где ε_n – независимые стандартные нормальные величины. Коэффициенты $b_k^{(n)}$, c_n удовлетворяют уравнениям Юла – Уокера

$$R(n) = \sum_{k=1}^{n-1} b_k^{(n)} R(n-k),$$

$$R(0) = c_n^2 + \sum_{k=1}^{n-1} b_k^{(n)} R(k).$$

Для нахождения коэффициентов $b_k^{(n)}$ и c_n используется рекурсивный алгоритм Левинсона – Дурбина, который требует $O(N^2)$ арифметических операций с плавающей точкой и по сути осуществляет разложение Холецкого матрицы обратной к корреляционной матрице (3.2.8), см. [26, 74, 83]

3. Наиболее быстрыми методами моделирования гауссовских векторов стационарного типа считаются методы на основе быстрого преобразования Фурье. Такие методы требуют $O(N \log N)$ арифметических операций с плавающей точкой. На первом этапе последовательность корреляций

$$R(0), \dots, R(N-2), R(N-1)$$

расширяется, например, следующим образом:

$$R(0), \dots, R(N-2), R(N-1), R(N-2), \dots, R(1). \quad (3.2.9)$$

К этой расширенной последовательности применяется быстрое преобразование Фурье, и вычисляется «спектр».

Затем корни квадратные значений этого спектра покомпонентно умножаются на независимые стандартные нормальные величины. К полученной гауссовской последовательности с независимыми элементами применяется обратное преобразование Фурье, и половина получившегося вектора используется в качестве результата моделирования (более подробно см. [65, 74] и гл. 11 в [56]). Важно, чтобы корреляционная матрица

$$\begin{bmatrix} R(0) & R(1) & \dots & R(2) & R(1) \\ R(1) & R(0) & \dots & R(3) & R(2) \\ \dots & \dots & \dots & \dots & \dots \\ R(2) & R(3) & \dots & R(0) & R(1) \\ R(1) & R(2) & \dots & R(1) & R(0) \end{bmatrix} \quad (3.2.10)$$

для расширенного корреляционного вектора (3.2.9) сохранила свойство положительной определенности. Симметричная теплицева матрица (3.2.10) является *циркулянттом*. Циркулянттом (циркулянтной матрицей) называют матрицу вида

$$\begin{bmatrix} c_0 & c_{n-1} & \dots & c_2 & c_1 \\ c_1 & c_0 & \dots & c_3 & c_2 \\ \dots & \dots & \dots & \dots & \dots \\ c_{n-2} & c_{n-3} & \dots & c_0 & c_{n-1} \\ c_{n-1} & c_{n-2} & \dots & c_1 & c_0 \end{bmatrix}.$$

Процедуру расширения корреляционной матрицы (3.2.8) до циркулянта в англоязычной литературе называют «circulant embedding». Алгоритмы на основе быстрых преобразований Фурье с успехом применяют и для моделирования однородных гауссовских полей [61, 66, 67, 97].

Отметим, что известные схемы авторегрессии и скользящего среднего позволяют моделировать гауссовские вектора стационарного типа неограниченной длины (см., например, [17, 34, 47, 49]).

Замечание (об оценке корреляционной функции стационарной последовательности). Предположим для простоты, что случайная последовательность $x(n)$ имеет нулевое математическое ожидание и единичную дисперсию. Корреляционную функцию $R(n) = \mathbf{M}x(k+n)x(k)$, $n = 0, \dots, N-1$, по одной реализации $x(k)$, $k = 1, \dots, N$, можно оценить по формулам

$$R'(n) = \frac{1}{N-n} \sum_{k=1}^{N-n} x(k+n)x(k), \quad n = 0, \dots, N-1. \quad (3.2.11)$$

Оценка $R'(n)$ будет несмещенной для $R(n)$ и, очевидно, что ее «качество» становится хуже при больших n . Кроме того, матрица

$$\begin{bmatrix} R'(0) & R'(1) & \dots & R'(M) \\ R'(1) & R'(0) & \dots & R'(M-1) \\ \dots & \dots & \dots & \dots \\ R'(M) & R'(M-1) & \dots & R'(0) \end{bmatrix}$$

может оказаться не положительно определенной. Поэтому вместо оценки (3.2.11) часто используется смещенная оценка

$$\begin{aligned} R^*(n) &= \frac{N-|n|}{N} R'(n) = \\ &= \frac{1}{N} \sum_{k=1}^{N-n} x(k+n)x(k), \quad n = 0, \dots, N-1. \end{aligned} \quad (3.2.12)$$

Оценка (3.2.12), в частности, обладает тем замечательным свойством, что соответствующая корреляционная матрица

$$\begin{bmatrix} R^*(0) & R^*(1) & \dots & R^*(N-1) \\ R^*(1) & R^*(0) & \dots & R^*(N-2) \\ \dots & \dots & \dots & \dots \\ R^*(N-1) & R^*(N-2) & \dots & R^*(0) \end{bmatrix}$$

всегда будет положительно определенной (см., например, [52] на стр. 75 и 238). По этому поводу в работе [70] на стр. 42

отмечается, что именно оценки вида (3.2.12) используются по умолчанию в большинстве пакетов прикладных программ для анализа временных рядов, так как на практике эти оценки оказываются предпочтительнее оценок (3.2.11).

На рис. 3.3 представлена оценка нормированной корреляционной функции, полученная именно по формулам (3.2.12). Для сравнения оценка (3.2.11) для той же выборки представлена на рис. 3.5.

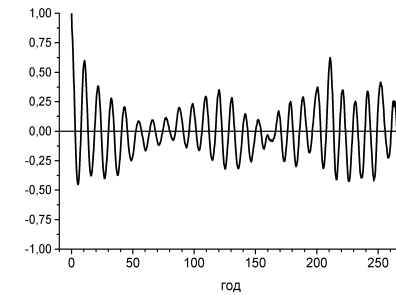


Рис. 3.5. Другая оценка нормированной корреляционной функции последовательности среднемесячных чисел Вольфа. В отличие от рис. 3.3, где использовалась формула (3.2.12), здесь использовалась формула (3.2.11)

3.3. Мультифрактальное броуновское движение

Винеровский процесс играет существенную роль в теории случайных процессов и ее многочисленных приложениях. Процессы мультифрактального броуновского движения являются интересными обобщениями винеровского процесса. Они также находят широкое применение в различных областях благодаря своим фрактальным свойствам. Определения и примеры моделирования таких процессов представлены ниже.

Гауссовский случайный процесс $w(t)$, $t > 0$, называется *дробным* или *фрактальным броуновским движением* с пока-

затем Хёрста H , если его математическое ожидание равно нулю, а корреляционная функция определяется выражением

$$R(t, s) = \mathbf{M}w(t)w(s) = \frac{\sigma^2}{2}(|t|^\alpha + |s|^\alpha - |t-s|^\alpha), \quad \alpha = 2H. \quad (3.3.1)$$

Доказательство положительной определенности корреляционной функции и дополнительную информацию о дробном броуновском движении можно найти, например, в [93].

Очевидно, что для дробного броуновского движения выполнено $\mathbf{D}w(t) = \sigma^2|t|^\alpha$. Если $\sigma = 1$, то дробное броуновское движение называют стандартным. При $\alpha = 1$, $H = 0.5$ получаем «обыкновенное» броуновское движение (винеровский процесс):

$$R(t, s) = \mathbf{M}w(t)w(s) = \frac{\sigma^2}{2}(|t| + |s| - |t-s|) = \sigma^2 \min(t, s). \quad (3.3.2)$$

Семейство процессов дробного броуновского движения впервые было рассмотрено в работе [77], а в работе [78] было показано, что это единственное семейство гауссовских самоподобных процессов со стационарными приращениями. Свойства самоподобия процессов $w(t)$ и $y_h(t) = w(t+h) - w(t)$ можно записать в виде

$$w(ct) \sim c^{\alpha/2}w(t), \quad y_{ch}(ct) \sim c^{\alpha/2}y_h(t),$$

где c – положительная константа, а символ \sim означает, что случайные процессы имеют одинаковые конечномерные распределения.

Результаты численного моделирования дробного броуновского движения на интервале $[0, 1]$ с шагом 0.001 представлены на рис. 3.6.

Хаусдорфова размерность дробного броуновского движения с показателем Хёрста H равна $2 - H = 2 - \alpha/2$ (см. [54]). Т. е. на любом участке траектории график случайной функции имеет эту размерность. Размерность мультифрактального броуновского движения может меняться в зависимости от участка траектории.

Предположим, что функция $H : [0, +\infty) \rightarrow (0, 1)$ является непрерывной по Гёльдеру. Гауссовский случайный процесс

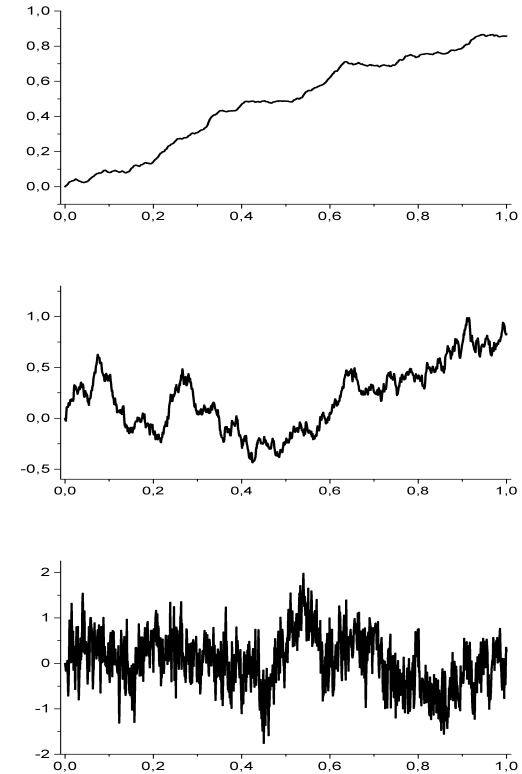


Рис. 3.6. Траектории дробного броуновского движения с фрактальной размерностью 1.1 (вверху), 1.5 (в середине) и 1.9 (внизу)

$w(t)$, $t > 0$, с нулевым средним называется мультифрактальным броуновским движением, если его корреляционная функция имеет вид (см., например, [57, 62])

$$R(t, s) = \mathbf{M}w(t)w(s) = \sigma^2 \frac{C(H(t), H(s))}{2} \times \left(|t|^{H(t)+H(s)} + |s|^{H(t)+H(s)} - |t-s|^{H(t)+H(s)} \right), \quad (3.3.3)$$

где

$$C(G, H) = \frac{\sqrt{\Gamma(2G+1)\Gamma(2H+1)\sin(\pi G)\sin(\pi H)}}{\Gamma(G+H+1)\sin(\frac{\pi(G+H)}{2})}. \quad (3.3.4)$$

Эквивалентное представление функции C имеет вид [62]

$$C(G, H) = \frac{I(\frac{G+H}{2})}{\sqrt{I(G)I(H)}}, \quad (3.3.5)$$

где

$$I(H) = \begin{cases} \frac{\Gamma(1-2H)}{H} \sin\{\frac{\pi}{2}(1-2H)\}, & H \in (0, 0.5), \\ \pi, & H = 0.5, \\ \frac{\Gamma(2(1-H))}{H(2H-1)} \sin\{\frac{\pi}{2}(2H-1)\}, & H \in (0.5, 1). \end{cases}$$

Функция C обладает свойством $C(H, H) = 1$. Таким образом, $\mathbf{D}w(t) = |t|^{2H(t)}$. Траектории мультифрактального броуновского движения являются непрерывными (с вероятностью 1), а для размерности Хаусдорфа \dim_H и клеточной размерности \dim_B графика мультифрактального броуновского движения выполнено (см., например, [85]):

$$\dim_H\{w(t), t \in [a, b]\} = \dim_B\{w(t), t \in [a, b]\} = 2 - \min_{t \in [a, b]} H(t). \quad (3.3.6)$$

О размерности Хаусдорфа и клеточной размерности см., например, [69].

Примеры моделирования траекторий мультифрактального броуновского движения на интервале $[0, 1]$ с шагом 0.001 приведены на рис. 3.7

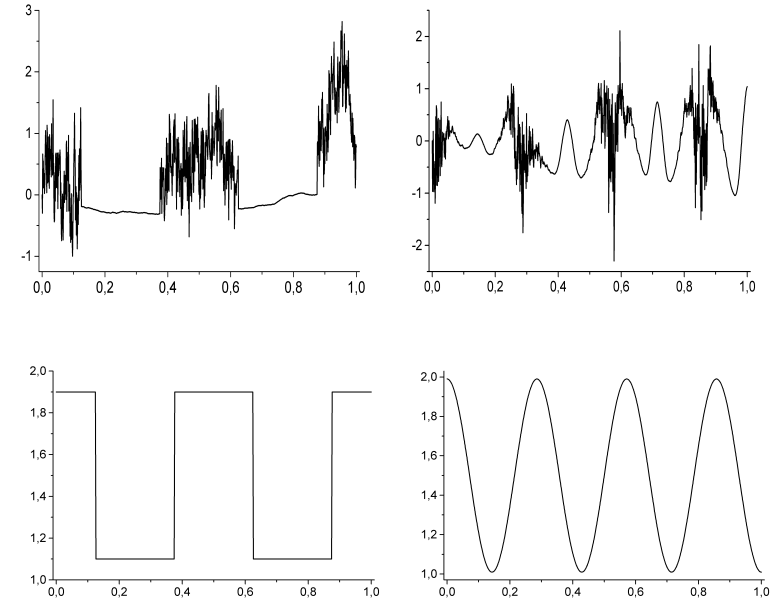


Рис. 3.7. Траектории мультифрактального броуновского движения $w(t)$ (вверху) и графики локальной размерности $\dim w(t) = 2 - H(t)$ (внизу) для функции $H(t)$ (слева), принимающей значения 0.9 на множестве $[0.125, 0.325] \cup [0.625, 0.875]$ и 0.1 вне его, и для функции $H(t) = 0.5 - 0.49 \cos(7\pi t)$ (справа)

Приложение А

Сведения из теории матриц

Ниже представлены дополнительные сведения, которые будут полезными при изучении основного материала нашего пособия.

А.1. Положительно определенные матрицы

Доказательства следующих утверждений о (комплекснозначных) положительно определенных матрицах (1.2.1) можно найти в монографии [59].

(1) Матрица является положительно определенной тогда и только тогда, когда она самосопряженная и ее собственные числа неотрицательны. Строгая положительная определенность означает строгую положительность собственных чисел.

(2) Матрица является положительно определенной тогда и только тогда, когда она самосопряженная и ее главные миноры неотрицательны. Строгая положительная определенность означает строгую положительность главных миноров.

(3) Матрица R является положительно определенной тогда и только тогда, когда $R = A^*A$ для некоторой матрицы A . Строгая положительная определенность равносильна невырожденности матрицы A .

(4) Матрица R является положительно определенной тогда и только тогда, когда $R = A^*A$ для некоторой верхней треугольной матрицы A (разложение Холецкого). Строгая положительная определенность равносильна невырожденности матрицы A . Матрицу A можно выбрать таким образом, что все ее диагональные элементы будут неотрицательны (такая матрица A единственна, если R – строго положительно определена).

(5) Матрица R является положительно определенной тогда и только тогда, когда $R = A^2$ для некоторой положитель-

но определенной матрицы A . Такая матрица A единственна (ее называют квадратным корнем R). Строгая положительная определенность R равносильна строгой положительной определенности A .

(6) Положительная определенность $n \times n$ -матрицы R с элементами R_{ij} равносильна тому, что найдется n комплексных n -мерных векторов d_1, \dots, d_n , $d_i \in \mathbb{C}^n$, таких, что

$$R_{ij} = \langle d_i, d_j \rangle.$$

Строгая положительная определенность равносильна линейной независимости векторов d_1, \dots, d_n .

А.2. Скелетное разложение матрицы

Для произвольной $n \times m$ -матрицы A ранга r найдутся $n \times r$ -матрица A_1 ранга r и $r \times m$ -матрица A_2 ранга r такие, что

$$A = A_1 A_2. \quad (\text{A.2.1})$$

Представление (A.2.1) называется скелетным разложением матрицы A [10, 11]. Матрицы A_1 , A_2 являются так называемыми матрицами полного ранга. Можно построить множество скелетных разложений:

$$A = A_1 A_2 = (A_1 X)(X^{-1} A_2),$$

где X – невырожденная $r \times r$ -матрица. В качестве матрицы A_2 можно взять матрицу, состоящую из r линейно независимых строк A . Тогда $A_1 = AA_2^+ = AA_2^T(A_2A_2^T)^{-1}$.

А.3. Псевдообратные матрицы

Для прямоугольной матрицы A со скелетным разложением $A = A_1 A_2$ псевдообратная матрица A^+ к матрице A определяется по формуле

$$A^+ = A_2^*(A_2A_2^*)^{-1}(A_1^*A_1)^{-1}A_1^*. \quad (\text{A.3.1})$$

Для любой матрицы псевдообратная к ней существует и единственна. Для $n \times r$ -матрицы B полного ранга $r \leq n$ выполнено

$$B^+ = (B^*B)^{-1}B^*,$$

а для $r \times m$ -матрицы C полного ранга $r \leq m$ выполнено

$$C^+ = C^*(CC^*)^{-1}.$$

Таким образом, (A.3.1) можно записать в виде

$$A^+ = A_2^+A_1^+. \quad (\text{A.3.2})$$

Псевдообратную матрицу можно определить с помощью равенств

$$A^+ = \lim_{\delta \rightarrow 0} (A^*A + \delta I)^{-1}A^* = \lim_{\delta \rightarrow 0} A^*(A^*A + \delta I)^{-1}.$$

Для квадратной невырожденной матрицы псевдообратная матрица совпадает с обратной.

Верны следующие равенства

$$\begin{aligned} (A^+)^+ &= A, & (A^*)^+ &= (A^+)^*, \\ (A^+A)^* &= A^+A, & (AA^+)^* &= AA^+, \\ (A^+A)^2 &= A^+A, & (AA^+)^2 &= AA^+, \\ A^+AA^+ &= A^+. \end{aligned}$$

Ядро и образ матриц A^+ , A^* совпадают. Напомним, что ядро $\text{Ker}(A)$ матрицы A – это множество векторов x , для которых $Ax = 0$. Образом $\text{Image}(A)$ матрицы A называется множество векторов y , для которых $y = Ax$ хотя бы для одного вектора x . Размерность образа – это ранг матрицы: $\text{rang}(A) = \dim(\text{Image}(A))$. Размерность ядра $\text{Ker}(A)$ называют дефектом матрицы A . Выполнены соотношения

$$\text{rang}(A) = \text{rang}(A^*), \quad \dim(\text{Ker}(A)) = \dim(\text{Ker}(A^*)),$$

$$\text{Ker}(A^*) = (\text{Image}(A))^\perp, \quad \text{Ker}(A) = (\text{Image}(A^*))^\perp,$$

$$\text{Ker}(A^*A) = \text{Ker}(A), \quad \text{Ker}(AA^*) = \text{Ker}(A^*),$$

$$\text{Image}(A^*A) = \text{Image}(A^*), \quad \text{Image}(AA^*) = \text{Image}(A).$$

Матрица AA^+ является проектором на $\text{Image}(A)$, а матрица A^+A – проектором на $\text{Image}(A^*)$:

$$AA^+ = \text{Pr}(\text{Image}(A)), \quad A^+A = \text{Pr}(\text{Image}(A^*)),$$

$$I - AA^+ = \text{Pr}(\text{Ker}(A^*)), \quad I - A^+A = \text{Pr}(\text{Ker}(A)).$$

Если вещественная матрица A является квадратной и симметричной, то ее можно представить в виде

$$A = \sum \lambda_j x_j x_j^T, \quad (\text{A.3.3})$$

где λ_j – собственные числа, а x_j – собственные вектора матрицы A , которые образуют ортонормированный базис,

$$Ax_j = \lambda_j x_j.$$

Псевдообратная матрица в этом случае запишется в виде

$$A^+ = \sum \lambda_j^+ x_j x_j^T, \quad (\text{A.3.4})$$

где $\lambda_j^+ = 1/\lambda_j$, если $\lambda_j \neq 0$, и $\lambda_j^+ = 0$ в противном случае.

Для симметричной матрицы A выполнено

$$A^+A = AA^+, \quad (A^\alpha)^+ = (A^+)^{\alpha}.$$

Свойство $A^+A = AA^+$ выполнено и для *нормальных* матриц (т. е., когда $A^T A = AA^T$).

Условия, при которых выполняется $(AB)^+ = B^+A^+$, и другую полезную информацию о псевдообратных матрицах можно найти в работах [1, 10, 11].

А.4. Системы линейных уравнений

Рассмотрим систему линейных (алгебраических) уравнений $Ax = y$. Эта система является *совместной* (существует хотя бы одно решение системы) тогда и только тогда, когда ранг матрицы A равен рангу *расширенной* матрицы, полученной добавлением справа столбца y (*теорема Кронекера – Капелли*).

Однородная система $Ax = 0$ совместна для любой матрицы A . Множество решений однородной системы $Ax = 0$, $A : X \rightarrow Y$ образует подпространство размерности $\dim(X) - \text{rang}(A)$ в пространстве X .

Условие $\dim(X) = \text{rang}(A)$ равносильно тому, что однородная система $Ax = 0$ имеет только нулевое решение. Если при этом система $Ax = y$ совместна, т. е. $y \in \text{Image}(A)$, то существует единственное решение системы $Ax = y$.

Существование единственного решения линейной системы $Ax = y$ с квадратной матрицей A равносильно невырожденности матрицы A . При этом $x = A^{-1}y$. Компоненты единственного решения $x = (x_k)^T$ можно вычислить по *формулам Крамера*

$$x_k = d_k/d,$$

где d – детерминант матрицы A , а d_k – детерминанты полученные заменой k -го столбца матрицы A на вектор y .

Система линейных уравнений $Ax = y$ имеет решение для любых y тогда и только тогда, когда сопряженная однородная система $A^*v = 0$ имеет только нулевое решение $v = 0$ (это вариант формулировки *альтернативы Фредгольма*).

Существование решений системы $Ax = y$, $y \neq 0$, равносильно тому, что вектор y ортогонален всем решениям v сопряженной однородной системы $A^*v = 0$ (*теорема Фредгольма*). Кратко это утверждение можно записать в виде $\text{Ker}(A^*) = (\text{Image}(A))^\perp$ или в виде

$$y \in \text{Im}(A) \iff y \perp \text{Ker}(A^*) \iff (I - AA^+)y = 0.$$

В пространстве всех решений совместной системы $Ax = y$ выделяют (единственное) *нормальное* решение x_0 , которое характеризуется одним из следующих (эквивалентных) свойств:

- среди всех решений нормальное решение является единственным, для которого выполнено $x_0 \in \text{Image}(A^*) = (\text{Ker}(A))^\perp$;
- среди всех решений x нормальное решение имеет минимальную длину $|x_0| = \min_x |x|$;
- $x_0 = A^+y$.

Система уравнений

$$A^*Ax = A^*y \tag{А.4.1}$$

называется *нормальной* (т. к. матрица A^*A – нормальная) и всегда является совместной (для любых матриц A и векторов y). Всегда совместной является и система

$$Ax = AA^+y \tag{А.4.2}$$

(напомним, что AA^+ – это проектор на $\text{Image}(A)$). Если система $Ax = y$ совместна, то она эквивалентна как системе (А.4.1), так и системе (А.4.2). Для несовместных линейных систем $Ax = y$ вводят понятие псевдорешений. *Псевдорешения* \tilde{x} несовместной системы $Ax = y$ характеризуются следующими (эквивалентными) свойствами:

- множество псевдорешений \tilde{x} системы $Ax = y$ совпадает с множеством решений системы (А.4.1) и с множеством решений (А.4.2);
- множество псевдорешений системы $Ax = y$ – это множество всех векторов \tilde{x} , для которых невязка $A\tilde{x} - y$ ортогональна $\text{Image}(A)$;
- множество псевдорешений системы $Ax = y$ – это множество всех векторов \tilde{x} , для которых достигается минимум длины невязки: $|A\tilde{x} - y| = \min_x |Ax - y|$.

Среди всех псевдорешений \tilde{x} линейной системы $Ax = y$ выделяют (единственное) *нормальное псевдорешение* \tilde{x}_0 , для которого выполнено одно из следующих (эквивалентных) утверждений:

- вектор нормального псевдорешения \tilde{x}_0 имеет минимальную длину среди всех псевдорешений;
- $\tilde{x}_0 \perp \text{Ker}(A)$;
- $\tilde{x}_0 = A^+y$.

Для более подробного изучения соответствующего материала можно рекомендовать книги [6, 10].

А.5. Полярное разложение матрицы

Любую комплексную квадратную матрицу A (вещественную) можно представить в виде произведения положительно определенной эрмитовой (симметричной) матрицы $H = H^*$ ($H = H^T$) на унитарную (ортогональную) матрицу U , $U^*U = UU^* = I$ ($U^T U = U U^T = I$). Представление $A = HU$ является аналогом представления комплексного числа $z = |z|e^{i\varphi}$ и называется *полярным разложением* матрицы A . Матрица H в полярном разложении определяется единственным образом из соотношения $H^2 = AA^*$. Если матрица A невырождена, то H также невырождена, и полярное разложение единственно: $U = H^{-1}A$. Более подробно о полярном разложении см. [7, 11, 32].

Приложение Б

О моделировании случайных чисел

В данном приложении кратко обсуждается проблема получения случайных чисел на компьютере и рассматривается один из способов программной реализации алгоритма Лемера.

Б.1. Источники случайных чисел

Случайно или закономерно, но так уж исторически сложилось, что в основе компьютерных вычислений методом Монте-Карло лежит моделирование случайных величин, равномерно распределенных на интервале $(0, 1)$. Все другие случайные величины и процессы, промежуточные и окончательные результаты вычислений методом Монте-Карло — это, по сути, преобразования независимых равномерно распределенных случайных величин (*случайных чисел*). Обычно выделяют три способа получения случайных чисел на компьютере: генераторы псевдослучайных чисел, физические датчики (аппаратные генераторы) и таблицы случайных чисел.

Генератор псевдослучайных чисел — это детерминированный алгоритм моделирования последовательности чисел, свойства которых близки к свойствам случайных величин, равномерно распределенных на промежутке $(0, 1)$. Именно этот способ получения случайных чисел применяется для статистического моделирования наиболее часто. Встроенные датчики случайных чисел, которые используются при вызове стандартных подпрограмм типа RANDOM или RAND на Паскале, Фортране, Си и других языках программирования — это генераторы псевдослучайных чисел. При проведении серьезных расчетов желательно изучить информацию о встроенном датчике (которая далеко не всегда оказывается легко доступной), а еще лучше воспользоваться каким-либо широко известным датчиком, хорошо себя зарекомендовавшим (программные реализа-

ции датчиков нетрудно найти в сети Интернет, в том числе и на странице автора <http://osmf.sccc.ru/~smp>).

Каким же образом детерминированные алгоритмы позволяют моделировать случайность? В качестве наглядного примера часто приводят алгоритм середины квадратов, предложенный одним из основателей метода Монте-Карло Джоном фон Нейманом. Пример соответствующей последовательности псевдослучайных чисел α_n приведен ниже:

$$\begin{aligned} x_1^2 &= 97[5353]76, & x_2 &= 5353, & \alpha_2 &= 0.5353, \\ x_3^2 &= 28[6546]09, & x_3 &= 6546, & \alpha_3 &= 0.6546, \quad \dots \end{aligned}$$

Квадратные скобки здесь поясняют, что в качестве следующего числа x_{n+1} берутся четыре цифры из середины квадрата предыдущего числа x_n . Конечно, для вычислений в настоящее время таким датчиком никто не пользуется (проанализируйте самостоятельно недостатки этого алгоритма), однако он служит хорошей иллюстрацией. Отметим, что перед моделированием псевдослучайной последовательности необходимо задать *начальное состояние генератора* (в английском языке для этого используется специальный термин «seed»). В данном примере это число x_1 . Для встроенных датчиков для задания начального состояния генератора используется специальная процедура. На Турбо Паскале это, например, процедура RANDOMIZE, которая формирует начальное состояние, обращаясь к системному таймеру. Если процедура RANDOMIZE в программе не вызывается, то встроенный датчик псевдослучайных чисел будет моделировать одну и ту же последовательность при каждом запуске программы. В то же время вызывать процедуру RANDOMIZE в программе более одного раза нецелесообразно, так как хорошие статистические свойства обеспечиваются именно последовательным моделированием псевдослучайных чисел. Предположим, что RANDOMIZE вызывается в цикле:

```
FOR I:=1 TO N DO
BEGIN
```

```
RANDOMIZE; A[I]:=RANDOM; ...
END;
```

В этом случае хорошие статистические свойства последовательности $A[I]$ совершенно не гарантированы! Правильно будет:

```
RANDOMIZE; ...
FOR I:=1 TO N DO
BEGIN
  A[I]:=RANDOM; ...
END;
```

Одним из наиболее популярных алгоритмов моделирования последовательностей псевдослучайных чисел α_j , равномерно распределенных на отрезке $(0, 1)$, является «мультипликативный генератор»:

$$\alpha_j = C * n_j, \quad n_{j+1} = (n_j * L) \bmod M, \quad C = M^{-1}. \quad (\text{Б.1.1})$$

Здесь n_j , L и M — натуральные числа, $n_j \in \{1, \dots, M-1\}$, а $x \bmod M$ — остаток от деления x на M . Другие названия этого метода: *линейный конгруэнтный генератор*, *метод вычетов*, *метод сравнений*, *алгоритм Лемера* (Р. Н. Lehmer, 1948). Проблема выбора параметров генератора (модуля M и множителя L) весьма нетривиальна. Среди специалистов хорошо известен случай, когда мультипликативный генератор, рекомендованный специалистами фирмы IBM и входящий в стандартное математическое обеспечение, в последующем был забракован (см., например, [45]).

Важной характеристикой псевдослучайного генератора является его период, после которого последовательность повторяется заново. Желательно, чтобы период на несколько порядков превышал длину псевдослучайной последовательности, используемой в алгоритме. Нужно иметь в виду, что генераторы, которые устраивали специалистов лет десять назад, для современных вычислений могут оказаться непригодными из-за недостаточной длины периода.

Приведем рекомендацию Г. А. Михайлова по выбору параметров мультипликативного генератора [28]:

$$M = 2^m, \quad L = 5^{2p+1}, \quad p = \max\{q \in \mathbb{N} : 5^{2q+1} < M\}. \quad (\text{Б.1.2})$$

Период такого датчика равен 2^{m-2} .

В последнее время широкое распространение получил генератор «вихрь Мерсенна» (Mersenne twister), разработанный в 1997 году японскими учеными Мамото Мацумото и Такудзи Нисимура [79]. Генератор обеспечивает равномерное распределение генерируемых псевдослучайных чисел в 623 измерениях и имеет огромный период, равный $2^{19937} - 1$. Утверждается, что «вихрь Мерсенна» в два-три раза быстрее линейных конгруэнтных генераторов.

Кроме методов Монте-Карло областью применения псевдослучайных чисел является криптография. Простой и эффективный алгоритм шифрования последовательности бит x_i состоит в следующем:

$$y_i = x_i \text{ XOR } b_i.$$

Здесь XOR — операция исключающего «или» (сложение по модулю 2), b_i — псевдослучайная последовательность бит. Декодирование происходит аналогичным образом:

$$x_i = y_i \text{ XOR } b_i.$$

Ключом для декодирования служит начальное состояние псевдослучайной последовательности, использованной при шифровании. К криптографическим генераторам псевдослучайных чисел предъявляются дополнительные требования криптостойкости, а сами алгоритмы обычно засекречены.

Что касается физических датчиков, то производители соревнуются в создании быстрых, компактных и статистически устойчивых аппаратных генераторов. На новостной ленте февраля 2008 года можно найти следующее сообщение: «Исследователи из японской корпорации Toshiba сконструировали

самый быстрый в мире аппаратный генератор случайных чисел. Устройство, реализованное в виде микросхемы площадью в 1200 квадратных микрон, способно генерировать данные со скоростью до 2 мегабит в секунду». Более того, почти все крупные производители микрочипов поставляют аппаратные генераторы случайных чисел. В частности, аппаратные генераторы встроены в чипсеты INTEL и AMD. Работа таких устройств основана на различных физических процессах (тепловой шум, фотоэлектрический эффект и др.). Основная проблема, которую вынуждены решать разработчики физических датчиков, это стабильность генерации случайных чисел во времени. Для повышения стабильности и улучшения характеристик используется дополнительная алгоритмическая коррекция случайных чисел. Согласно [63] современные аппаратные генераторы могут моделировать гигабиты случайных чисел в секунду.

В криптографии аппаратные датчики случайных чисел используют для формирования надежных ключей шифрования и электронной цифровой подписи.

Так или иначе, обнаружив аппаратный генератор в своем персональном компьютере или приобретя соответствующую электронную плату, можно организовать вычисления с использованием физического датчика. Однако физический датчик, скорее всего, окажется значительно медленнее программного моделирования псевдослучайных чисел. Кроме того, за «истинную случайность» придется заплатить отсутствием возможности воспроизвести вычисления и неуверенностью в качестве случайных чисел. Конечно, можно запомнить последовательность случайных чисел, полученных физическим датчиком, проконтролировать ее статистические свойства и затем использовать в алгоритмах Монте-Карло. Таким образом, мы приходим к идее использования таблиц случайных чисел.

Самая большая из опубликованных таблиц случайных чисел [53] была получена с помощью физического датчика, а точнее с помощью электронной рулетки. На практике использование таблиц случайных чисел для вычислений методом

Монте-Карло малоэффективно, так как требуются значительный объем памяти для хранения чисел и большое время доступа, если числа хранятся на внешнем носителе.

Таким образом, основным способом получения случайных чисел для вычислений методом Монте-Карло являются генераторы псевдослучайных чисел, в алгоритмах которых нет ничего случайного. Часто приводят высказывание Роберта Кавью: «The generation of random numbers is too important to be left to chance» («Генерация случайных чисел слишком важна, чтобы оставлять ее на волю случая»). В то же время, как отмечал И. М. Соболев (см. [46] на стр. 19), «общей теории псевдослучайных чисел в настоящее время нет».

Более подробные сведения о моделировании псевдослучайных чисел, а также случайных величин, процессов и полей можно найти в обширной литературе (см., например, [9, 15, 19, 20, 27–30, 34, 46, 48, 84, 87, 92]). Отдельно упомянем книгу [29], где обсуждаются особенности реализации мультипликативных генераторов для параллельных вычислений.

Б.2. О мультипликативных датчиках

В данном пункте рассматриваются особенности реализации мультипликативных датчиков псевдослучайных чисел (Б.1.1) на языках программирования высокого уровня.

Ниже представлены следующие процедуры, написанные на Паскале и реализующие мультипликативный метод:

`RAND_1`: $M = 2^{40}$, $L = 5^{17}$ [20].

`RAND_2`: $M = 2^{55}$, $L = 48\ 044\ 648\ 058\ 128\ 333$ [2].

`RAND_3`: $M = 2^{70}$, $L = 5^{29}$.

Процедура `RAND_4` реализует суммирование по модулю 1 трех мультипликативных генераторов [4]:

$$a_j = C_1 * n_j^1 + C_2 * n_j^2 + C_3 * n_j^3 \pmod{1},$$

$$n_{j+1}^k = n_j^k * L_1 \pmod{M_k}, \quad C_k = M_k^{-1},$$

$$L_1 = 1\ 528, \quad M_1 = 1\ 400\ 159, \quad L_2 = 1\ 356, \quad M_2 = 1\ 500\ 419,$$

$$L_3 = 1\ 856, \quad M_3 = 1\ 001\ 003.$$

Процедура `RAND_5` реализует суммирование по модулю 1 пяти мультипликативных генераторов.

Результаты тестирования некоторых мультипликативных и смешанных конгруэнтных генераторов приведены в [2]. Там же найден ряд множителей, оптимальных с точки зрения функционально-корреляционных характеристик. При выборе множителя в процедуре `RAND_3` была использована рекомендация (Б.1.2).

Для того, чтобы мультипликативная псевдослучайная последовательность обладала наибольшим возможным периодом, множитель должен выбираться специальным образом.

Теорема Б.1 (см., например, [18]). *Максимальная длина периода последовательности (Б.1.1) при $M = 2^m$, $m \geq 3$, равна 2^{m-2} и достигается для всех нечетных p_0 , если остаток от деления L на 8 равен 3 или 5.*

Согласно работе [3] в вычислительном алгоритме не рекомендуется использовать более чем $P^{2/3}$ чисел псевдослучайной последовательности, где P — период последовательности.

Кратко остановимся на особенностях программной реализации процедур `RAND_1`-`RAND_5`.

В процедурах `RAND_1`-`RAND_3` фактически реализовано умножение «в столбик» для целых чисел в системе счисления по основанию 2^{14} :

$$\begin{array}{rcccccc}
 & * & a_n & \dots & a_3 & a_2 & a_1 \\
 & & \hline
 & & b_n & \dots & b_3 & b_2 & b_1 \\
 + & c_{1,n+1} & c_{1,n} & \dots & c_{1,3} & c_{1,2} & c_{1,1} \\
 + & c_{2,n+1} & c_{2,n} & \dots & c_{2,2} & c_{2,1} & \\
 & \dots & \dots & \dots & \dots & \dots & \dots \\
 + & c_{n,n+1} & \dots & \dots & c_{n,1} & & \\
 \hline
 & a'_{2n} & \dots & a'_n & \dots & a'_3 & a'_2 & a'_1,
 \end{array}$$

где a_i, b_i, c_{ij} — «цифры» соответствующей системы счисления.

В процедурах RAND_1–RAND_3 для увеличения быстродействия используются специальные операции с целыми числами:

$$C \bmod 2^k = C \text{ and}(2^k - 1), \quad C \text{ div } 2^k = C \text{ shr } k.$$

Здесь and — операция побитового умножения, а shr — операция побитового сдвига вправо. Создавать более быстродействующие реализации алгоритмов позволяет программирование на низком уровне (ассемблер, машинные коды).

Алгоритм, реализованный в процедурах RAND_1–RAND_3, легко настраивается для любого модуля вида $M=2^m$ и произвольного множителя L . Константы b_1, \dots, b_n в этих процедурах представляют разложение множителя L в системе счисления по основанию 2^k , $k \leq 14$:

$$L = b_1 + b_2 2^k + b_3 2^{2k} + \dots + b_n 2^{(n-1)k},$$

n — число цифр в разложении. Система счисления по основанию 2^k , $k = 14$, может быть использована в данном алгоритме при $m \leq 98$, $n \leq 7$ (при $n > 7$ возникнут переполнения за диапазон LONGINT; для $k = 13$ допустимы значения $n \leq 31$).

В процедурах RAND_4, RAND_5 используется суммирование по модулю 1 псевдослучайных чисел, полученных несколькими мультипликативными генераторами [4]. В качестве модулей этих мультипликативных генераторов используются числа Смита (различные для разных генераторов), а в качестве множителей первообразные корни чисел Смита. В работе [4] числом Смита называется простое число, представимое в виде $2P + 1$, где P также простое. Целое число L называется первообразным корнем простого числа M , если $1 < L < M$ и наименьшая степень k , для которой выполнено $L^k \bmod M = 1$, равна $M - 1$.

Период такой мультипликативной последовательности равен соответствующему числу Смита, уменьшенному на единицу. Период датчика, в котором числа, полученные несколькими различными мультипликативными генераторами, суммируются по модулю 1, равен произведению периодов суммируемых генераторов. Использование такой методики позволяет

конструировать генераторы с практически неограниченным периодом. Кроме того, суммирование по модулю 1 дает псевдослучайную последовательность с улучшенными статистическими свойствами [5, 55].

Замечание. Датчики псевдослучайных чисел, реализованные на языках программирования высокого уровня, значительно уступают по быстродействию датчикам, реализованным на машинно-ориентированных языках. Однако во многих случаях генерация случайных чисел не является критическим моментом в вычислительных алгоритмах и составляет лишь небольшую долю в общем объеме вычислений. В этой ситуации использование датчиков, написанных на языках высокого уровня, может оказаться более предпочтительным из соображений универсальности и переносимости программ.

Упражнение Б.1. (а) Найдите остаток от деления 5^p на 8 для различных значений p .

(б) Запрограммируйте алгоритмы моделирования псевдослучайных чисел по мультипликативному алгоритму (Б.1.1) со следующими параметрами:

- а) $M = 1400423$, $L = 1499$ [4] (покажите, что в данном случае M является числом Смита, а L — его первообразный корень);
- б) $M = 2^{31}$, $L = 5^{13}$ [45];
- в) $M = 2^{42}$, $L = 5^{17}$ [15, 46];
- г) $M = 2^{47}$, $L = 5^{15}$, $n_0 = 2001$ ($P = 2^{45} \approx 3.52 \cdot 10^{13}$, $P^{2/3} \approx 1.07 \cdot 10^9$) [48];
- д) $M = 2^{48}$, $L = 5^{19}$ (этот датчик используется в пакете MCNP — «A General Monte Carlo N-Particle transport code»);
- е) $M = 2^{55}$, $L = 14\,312\,160\,467\,264\,461$ [2];
- ж) $M = 2^{54}$, 2^{55} , 2^{56} , $L = 5^{23}$;
- з) $M = 2^{98}$, множитель L выберите по правилу (Б.1.2);

- и) $M = 2^{128}$, множитель L выберите по правилу (Б.1.2);
 к) $M = 2^{128}$, $L = 5^K \bmod 2^{128}$, $K = 100109$ [68].

Определите периоды этих датчиков.

(в) Изучите принцип, заложенный в «вещественной» реализации мультипликативного генератора в процедуре `RAND_1r`. Какие условия должны выполняться для корректной работы алгоритма, использованного в этой процедуре? Сравните быстроедействие «вещественной» реализации алгоритма с быстрымдействием «целочисленной» процедуры `RAND_1`.

Б.3. Тексты процедур на Паскале

Приведенные ниже генераторы псевдослучайных чисел, а также другие генераторы на Паскале, Фортране и Си можно найти в Интернете по адресу <http://osmf.sccc.ru/~smp>.

```
{
  Subject: Demo program for different
           generators of pseudo-random numbers
  Language: Turbo Pascal for IBM PC
}

{$A+,B-,D-,E+,F-,G+,I+,L-,N+,O-,P-,Q-,R+,S+,T-,V-,X+}
{$M 16384,0,655360}
PROGRAM RND_TEST;

{-----
  Мультипликативный датчик псевдослучайных чисел
  M = 2**40, L = 5**17 = 762 939 453 125
  (период 2**38 = 274 877 906 944)
  -----
  Начальные значения: 1<=a1<=16383, 0<=a2<=16383,
                      0<=a3<=4095, a1 - нечетное !
}
function RAND_1: real;
const {40=14+14+12}
  a1:longint=1; a2:longint=0; a3:longint=0;
```

```
  b1:longint=11973; b2:longint=2800; b3:longint=2842;
  x1=1.0/4096.0; x2=x1/16384.0; x3=x2/16384.0;
var c11, c12, c13, c21, c22, c31: longint;
    d1, d2, d3: longint;
begin
  c11 := b1*a1; c12 := b1*a2; c13 := b1*a3;
  c21 := b2*a1; c22 := b2*a2;
  c31 := b3*a1;
  d1 := c11;
  d2 := c21 + c12 + (d1 shr 14);
  d3 := c31 + c22 + c13 + (d2 shr 14);
  a1:=d1 and 16383; a2:=d2 and 16383; a3:=d3 and 4095;
{ для стандартного паскаля:
  d2 := c21 + c12 + (d1 div 16384);
  d3 := c31 + c22 + c13 + (d2 div 16384);
  a1:=d1 mod 16384; a2:=d2 mod 16384; a3:=d3 mod 4096;
}
  RAND_1 := a3*x1 + a2*x2 + a1*x3;
END;

{-----
  Мультипликативный датчик псевдослучайных чисел
  M = 2**55, L = 48 044 648 058 128 333
  (период 2**53 = 9 007 199 254 740 992)
  -----
  Начальные значения: 1<=a1<=16383, 0<=a2<=16383,
                      0<=a3<=16383, 0<=a4<=8191, a1 - нечетное !
}
function RAND_2: real;
const {55=14+14+14+13}
  a1:longint=1; a2:longint=0; a3:longint=0;
                                     a4:longint=0;

  b1: longint=1997; b2: longint=4980;
  b3: longint=1445; b4: longint=10924;
  x1 = 1.0/8192.0; x2 = x1/16384.0;
  x3 = x2/16384.0; x4 = x3/16384.0;
var c11,c12,c13,c14,c21,c22,c23,c31,c32,c41: longint;
    d1,d2,d3,d4: longint;
begin
```

```

c11:=b1*a1; c12:=b1*a2; c13:=b1*a3; c14:=b1*a4;
c21:=b2*a1; c22:=b2*a2; c23:=b2*a3;
c31:=b3*a1; c32:=b3*a2;
c41:=b4*a1;
d1 := c11;
d2 := c21 + c12 + (d1 shr 14);
d3 := c31 + c22 + c13 + (d2 shr 14);
d4 := c41 + c32 + c23 + c14 + (d3 shr 14);
a1:=d1 and 16383; a2:=d2 and 16383;
a3:=d3 and 16383; a4:=d4 and 8191;
RAND_2 := a4*x1 + a3*x2 + a2*x3 + a1*x4;
end;

{-----
Мультипликативный датчик псевдослучайных чисел
M = 2**70, L = 5**29 = 186 264 514 923 095 703 125
(период 2 68 = 295 147 905 179 352 825 856)
-----
Начальные значения: 0 <= a1,a2,a3,a4,a5 <= 16383,
a1 - нечетное !
}
function RAND_3: real;
const {70=14*5}
a1:longint=1; a2:longint=0; a3:longint=0;
a4:longint=0; a5:longint=0;
b1:longint=15957; b2:longint=11842; b3:longint=5942;
b4:longint=15391; b5:longint=2584;
x1=1.0/16384.0; x2=x1/16384.0; x3=x2/16384.0;
x4=x3/16384.0; x5=x4/16384.0;
var c11,c12,c13,c14,c15,c21,c22,c23,c24,
c31,c32,c33,c41,c42,c51: longint;
d1,d2,d3,d4,d5: longint;
begin
c11:=b1*a1; c12:=b1*a2; c13:=b1*a3; c14:=b1*a4;
c15:=b1*a5;
c21:=b2*a1; c22:=b2*a2; c23:=b2*a3; c24:=b2*a4;
c31:=b3*a1; c32:=b3*a2; c33:=b3*a3;
c41:=b4*a1; c42:=b4*a2;
c51:=b5*a1;

```

```

d1 := c11;
d2 := c21 + c12 + (d1 shr 14);
d3 := c31 + c22 + c13 + (d2 shr 14);
d4 := c41 + c32 + c23 + c14 + (d3 shr 14);
d5 := c51 + c42 + c33 + c24 + c15 + (d4 shr 14);
a1:=d1 and 16383; a2:=d2 and 16383;
a3:=d3 and 16383; a4:=d4 and 16383;
a5:=d5 and 16383;
RAND_3 := a5*x1 + a4*x2 + a3*x3 + a2*x4 + a1*x5;
end;

{-----
Датчик М.В. Антипова
(период 1400158*1500418*1001002=2.10292729e+18)
-----
Начальные значения: 1 <= n1 <= 1400158,
1 <= n2 <= 1500418,
1 <= n3 <= 1001002
}
function RAND_4: real;
const n1:longint=1; n2:longint=1; n3:longint=1;
const c1=1.0/1400159; c2=1.0/1500419; c3=1.0/1001003;
var R: real;
begin
n1 := (n1*1528) mod 1400159;
n2 := (n2*1356) mod 1500419;
n3 := (n3*1856) mod 1001003;
R := n1 * c1 + n2 * c2 + n3 * c3;
RAND_4 := frac(R);
end;

{-----
Датчик М.В. Антипова
(период 27000706*24001798*21000982*
*15001606*10000222=2.0417656605e+36)
-----
Начальные значения: 1 <= n1 <= 27000706,
1 <= n2 <= 24001798,
1 <= n3 <= 21000982,

```

```

        1 <= n4 <= 15001606,
        1 <= n5 <= 10000222
    }
FUNCTION Rand_5: double;
Function DMOD(x,y:double):double;
Begin
    DMOD:=x-y*int(x/y);
End;
const n1:double=1; n2:double=1; n3:double=1;
      n4:double=1; n5:double=1;
const c1:double=1.0/27000707;
      c2:double=1.0/24001799;
      c3:double=1.0/21000983;
      c4:double=1.0/15001607;
      c5:double=1.0/10000223;
var R: double;
begin
    n1 := DMOD(n1*6173, 27000707);
    n2 := DMOD(n2*7853, 24001799);
    n3 := DMOD(n3*10330, 21000983);
    n4 := DMOD(n4*20203, 15001607);
    n5 := DMOD(n5*45773, 10000223);
    R := n1*c1 + n2*c2 + n3*c3 + n4*c4 + n5*c5;
    RAND_5 := frac(R);
end;

{-----
Multiplicative generator with module 2**40
and multiplier 5**17 = 762 939 453 125
(cycle length 2**38 = 274 877 906 944)

"Real-valued" realization
-----
Initial values: 0 <= A1,A2 <= 1048575, A1 must be odd !
Here we set: A1=1, A2=0
}
function Rand_1r: double;
const {40=20+20}

```

```

a1:double=1; a2:double=0;
b1: double=798405; b2: double=727595;
x1=1.0/1048576; x2=x1/1048576;
var c11, c12, c21, d1, d2: double;

Function DMOD(x,y:double):double;
Begin DMOD:=x-y*int(x/y); End;

begin
    c11 := b1*a1; c12 := b1*a2; c21 := b2*a1;
    d1 := c11; d2 := c21 + c12 + int(d1*x1);
    a1:= DMOD(d1,1048576); a2:=DMOD(d2,1048576);
    Rand_1r := a2*x1 + a1*x2;
END;

{}
var test, code: integer; i: longint; x: double;
BEGIN {PROGRAM}
    val(paramstr(1), test, code);
    case test of
1: for i:=1 to 1000000 do x := Rand_1;
2: for i:=1 to 1000000 do x := Rand_2;
3: for i:=1 to 1000000 do x := Rand_3;
4: for i:=1 to 1000000 do x := Rand_4;
5: for i:=1 to 1000000 do x := Rand_5;
6: for i:=1 to 1000000 do x := Rand_2r;
else for i:=1 to 1000000 do x := Random;
}
    {
        Встроенный датчик Турбо-Паскаля версии 6.0:
        Random = abs(n(j) / 2^31),
        n(j) = [134775813*n(j-1)+1+2^31] mod 2^32 - 2^31
    }
    end;
    writeln(x);
END.

```

Литература

1. Алберт А. Регрессия, псевдоинверсия и рекуррентное оценивание. М.: Наука, 1977.
2. Антипов М. В. Оценка и выбор генератора псевдослучайных чисел для заданного класса задач. Новосибирск, 1985. 18 с. (Препринт / АН СССР. Сиб. отд-ние. ВЦ; 554).
3. Антипов М. В. Ограничения в вычислительных методах Монте-Карло при использовании псевдослучайных чисел // Теория и приложения статистического моделирования. Новосибирск, 1989. С. 3–9.
4. Антипов М. В. Системы генераторов псевдослучайных чисел для персональных компьютеров. Новосибирск, 1990. 27 с. (Препринт / АН СССР. Сиб. отд-ние. ВЦ; 910).
5. Антипов М. В., Михайлов Г. А. Оценки неравномерности распределений конгруэнтных сумм случайных величин // Докл. РАН. 1996. Т. 347, № 1. С. 23–26.
6. Беклемишев В. Д. Дополнительные главы линейной алгебры. М.: Наука, 1983.
7. Беклемишев В. Д. Курс аналитической геометрии и линейной алгебры. М.: Физматлит, 2009.
8. Вадзинский Р. Н. Справочник по вероятностным распределениям. М.: Наука, 2001.
9. Винклер Г. Анализ изображений, случайные поля и методы Монте-Карло на цепях Маркова. Новосибирск: ГЕО, 2008.
10. Воеводин В. В., Кузнецов Ю. А. Матрицы и вычисления. М.: Наука, 1984.
11. Гантмахер Ф. Р. Теория матриц. М.: Физматлит, 2004.
12. Гихман И. И., Скороход А. В. Теория случайных процессов. Т. 1. М.: Наука, 1971.
13. Гихман И. И., Скороход А. В. Введение в теорию случайных процессов. М.: Наука, 1977.
14. Гихман И. И., Скороход А. В., Ядренко М. И. Теория вероятностей и математическая статистика. Киев: Вища школа, 1979.
15. Голенко Д. И. Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах. М.: Наука, 1965.
16. Голуб Дж., Ван Лоан Ч. Матричные вычисления. М.: Мир, 1999.
17. Дуброва Т. А. Статистические методы прогнозирования. М.: ЮНИТИ-ДАНА, 2003.
18. Ермаков С. М. Метод Монте-Карло и смежные вопросы. М.: Наука, 1971.
19. Ермаков С. М. Метод Монте-Карло в вычислительной математике: вводный курс. СПб.: Невский диалект, 2009.
20. Ермаков С. М., Михайлов Г. А. Статистическое моделирование. М.: Наука, 1982.
21. Кириллов А. А., Гвишиани А. Д. Теоремы и задачи функционального анализа. М.: Наука, 1979.
22. Коваленко И. Н., Филиппова А. А. Теории вероятностей и математическая статистика. М.: Высш. школа, 1982.
23. Королюк В. С., Портенко Н. И., Скороход А. В., Турбин А. Ф. Справочник по теории вероятностей и математической статистике. М.: Наука, 1985.
24. Ланкастер П. Теория матриц. М.: Наука, 1982.
25. Литвенко К. В., Пригарин С. М. Численные стохастические модели поверхности морского волнения и гигантских океанических волн // Сибирский журнал вычислительной математики. 2014. Т. 17, № 4. С. 349–361.
26. Марченко А. С., Огородников В. А. Моделирование гауссовских последовательностей большой длины с заданной корреляционной структурой // Журн. вычислит. математики и мат. физики. 1984. Т. 24. С. 1514–1519.
27. Михайлов Г. А. Некоторые вопросы теории методов Монте-Карло. Новосибирск: Наука, 1974.
28. Михайлов Г. А. Оптимизация весовых методов Монте-Карло. М.: Наука, 1987.
29. Михайлов Г. А. Весовые алгоритмы статистического моделирования. Новосибирск: Изд-во ИВМиМГ СО РАН, 2003.

30. Михайлов Г. А., Войтишек А. В. Численное статистическое моделирование. Методы Монте-Карло. М.: Академия, 2006.
31. Огородников В. А., Пригарин С. М., Родионов А. С. Квазигавссовская модель сетевого трафика // Автоматика и телемеханика. 2010. № 3. С. 117–130.
32. Прасолов В. В. Задачи и теоремы линейной алгебры. М.: Наука, 2008.
33. Пригарин С. М. Условные спектральные модели гауссовских однородных полей. Новосибирск, 1997. 19 с. (Препринт/РАН. Сибирское отделение, ВЦ; № 1098).
34. Пригарин С. М. Методы численного моделирования случайных процессов и полей. Новосибирск: Изд. ИВМиМГ СО РАН, 2005.
35. Пригарин С. М. Модели случайных процессов и полей в методах Монте-Карло. Saarbruecken: Palmarium Academic Publishing, 2014.
36. Пригарин С. М., Маршак А. Л. Численная имитационная модель разорванной облачности адаптированная к результатам наблюдений // Оптика атмосферы и океана. 2005. Т. 18, № 3. С. 256–263.
37. Пригарин С. М., Маршак А. Л. Численное моделирование векторных полубинарных однородных случайных полей и имитация разорванной облачности // Сибирский журнал вычислительной математики. 2008. Т. 11, № 3. С. 347–356.
38. Пригарин С. М., Федченко Н. В. Решение краевых задач для линейных систем стохастических дифференциальных уравнений // Сибирский журн. вычисл. мат. 2004. Т. 7, № 4. С. 301–318.
39. Пригарин С. М., Хан К., Винклер Г. Дисперсионная размерность случайных последовательностей и ее применение // Сибирский журн. вычисл. мат. 2009. Т. 12, № 4. С. 435–448.
40. Пригарин С. М., Хан К., Винклер Г. Оценка фрактальной размерности случайных полей на основе анализа дисперсии вращений // Сибирский журн. вычисл. мат. 2011. Т. 14, № 1. С. 91–102.
41. Рид М., Саймон Б. Методы современной математической физики. Т.1. Функциональный анализ. М.: Мир, 1977.

42. Рисс Ф., Сёкефальви-Надь Б. Лекции по функциональному анализу. М.: Мир, 1979.
43. Сборник задач по теории вероятностей, математической статистике и теории случайных функций / Под ред. А. А. Свешникова. М.: Наука, 1970.
44. Сверхбольшие интегральные схемы и современная обработка сигналов / Под ред. С. Гуна, Х. Уайтхауса, Т. Кайлата. М.: Мир, 1989.
45. Соболев И. М. Метод Монте-Карло. М.: Наука, 1985.
46. Соболев И. М. Численные методы Монте-Карло. М.: Наука, 1973.
47. Тараскин А. Ф. Статистический анализ временных рядов авторегрессии и скользящего среднего. Самара: Самар. гос. аэрокосм. ун-т., 1998.
48. Франк-Каменецкий А. Д. Моделирование траекторий нейтронов при расчете реакторов методом Монте-Карло. М.: Атомиздат, 1978.
49. Хеннан Э. Многомерные временные ряды. М.: Мир, 1974.
50. Цехан О. Б. Матричный анализ. М.: ФОРУМ, 2012.
51. Шалыгин А. С., Палагин Ю. И. Прикладные методы статистического моделирования. Л.: Машиностроение, 1986.
52. Яглом А. М. Корреляционная теория стационарных случайных функций. Л.: Гидрометеиздат, 1981.
53. A Million Random Digits with 100000 Normal Deviates. Glenkoe, Ill.: Free Press, 1955.
54. Adler R. J. The Geometry of Random Fields. N. Y.: Wiley, 1981.
55. Antipov M. V., Mikhailov G. A. On the improvement in random number generators by using a modulo 1 sum // Rus. J. Numer. Anal. and Math. Modell. 1996. Vol. 11, № 2. P. 93–111.
56. Asmussen S., Glynn P. W., Stochastic Simulation: Algorithms and Analysis. N. Y.: Springer, 2007.
57. Ayache A., Cohen S., Levy Vehel J. // The covariance structure of multifractional Brownian motion, with application to long range dependence. 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing. Istanbul, 2000. P. 3810–3813.

58. Baba K., Shibata R. Multiplicative correlations // *Annals of the Institute of Statistical Mathematics*. 2006. Vol. 58, № 2. P. 311–326.
59. Bhatia R. *Positive Definite Matrices*. Princeton, N. J.: Princeton University Press, 2007.
60. Box G. E. P., Muller M. E. A note on the generation of random normal deviates // *Ann. Math. Statist.* 1958. Vol. 29. P. 610–611.
61. Chan G., Wood A. An Algorithm for Simulating Stationary Gaussian Random Fields // *Journal of the Royal Statistical Society*. 1997. Vol. 46, No. 1. P. 171–181.
62. Chan G., Wood A. Simulation of multifractional Brownian motion // *Proceedings in Computational Statistics (13th Symposium, Bristol, Great Britain)*. 1998. P. 233–238.
63. Comparison of hardware random number generators [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Comparison_of_hardware_random_number_generators (дата обращения 31 января 2018).
64. Cover T. M., Thomas J. A. *Elements of Information Theory* (second edition). N. Y.: Wiley & Sons, New York, 2006.
65. Davies R. B., Harte D. S. Tests for Hurst effect // *Biometrika*, 1987. V. 74. P. 95–101.
66. Dietrich C. R., Newsam G. N. A fast and exact method for multidimensional Gaussian stochastic simulations // *Water Resources Research*. 1993. Vol. 29. P. 2861–2869.
67. Dietrich C. R., Newsam G. N. Fast and exact simulation of stationary Gaussian processes through circulant embedding of the covariance matrix // *SIAM Journal on Scientific Computing*. 1997. Vol. 18. P. 1088–1107.
68. Dyadkin I. G., Hamilton K. G. A study of 128-bit multipliers for congruential pseudorandom number generators // *Computer Physics Communications*. 2000. Vol. 125. P. 239–258.
69. Falconer K. *Fractal Geometry*. N. Y.: Wiley, 2003.
70. Fan, J. and Yao, Q. *Nonlinear Time Series: Nonparametric and Parametric Methods*. N. Y.: Springer-Verlag, 2003.
71. Fedchenko N. V., Prigarin S. M. Boundary value problems for linear stochastic differential equations // *Rus. J. Numer. Anal. Math. Modell.* 2004. Vol. 19, № 6. P. 467–553.

72. Golub G. H., Van Loan C. F. *Matrix Computations*. Baltimore: The Johns Hopkins University Press, 1996.
73. Harman R., Lacko V. On decompositional algorithms for uniform sampling from n-spheres and n-balls // *Journal of Multivariate Analysis*. Vol. 101 (2010). P. 2297–2304.
74. Hauser M., Hörmann W. *The Generation of Stationary Gaussian Time Series*. Preprint Series / Department of Applied Statistics and Data Processing, 17. Department of Statistics and Mathematics, Vienna: University of Economics and Business, 1997.
75. Hörmann W., Leydold J., Deringer G. *Automatic Non-Uniform Random Variate Generation*. Berlin: Springer-Verlag, 2004.
76. Higham N. J. Analysis of the Cholesky decomposition of a semi-definite matrix. // *Reliable Numerical Computation* / M. G. Cox and S. J. Hammarling, editors. Oxford University Press, 1990, P. 161–185.
77. Kolmogorov A. N. Wienersche Spiralen und einige andere interessante Kurven im Hilbertschen Raum // *Доклады Акад. наук СССР*. 1940. Т. 26. № 2. С. 115–118.
78. Mandelbrot B. B., Ness J. W. V. Fractional Brownian motions, fractional noises and applications // *SIAM Rev.* 1968. Vol. 10. P. 422–437.
79. Matsumoto M., Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudorandom number generator // *ACM Trans. on Modeling and Computer Simulations*. 1998. Vol. 8, № 1. P. 3–30.
80. Mood A. M., Graybill F. A., Boes D. C., *Introduction to the Theory of Statistics*. Singapore: McGraw-Hill, 1974.
81. Müller M. E. An inverse method for the generation of random normal deviates on large-scale computers // *Math. Tables Other Aids Comp.* 1958. Vol. 12. P. 167–174.
82. Müller M. E. A comparison of methods for generating normal deviates on digital computers // *J. Assoc. Comp. Mach.* 1959. Vol. 6 P. 376–383.
83. Musicus B. R. *Levinson and Fast Choleski Algorithms for Toeplitz and Almost Toeplitz Matrices*. RLE Technical report No. 538,

- Research Laboratory of Electronics, Massachusetts Institute of Technology, 1988.
84. Ogorodnikov V. A., Prigarin S. M. Numerical Modelling of Random Processes and Fields: Algorithms and Applications. Utrecht: VSP, 1996.
 85. Peltier R., Levy Vehel J. Multifractional Brownian motion: definition and preliminary results. INRIA research report No. 2645, 1995.
 86. Prigarin S. M. Conditional spectral models of Gaussian homogeneous fields // Rus. J. Numer. Anal. and Math. Modell. 1998. Vol. 13, № 1. P. 57–68.
 87. Prigarin S. M. Spectral Models of Random Fields in Monte Carlo Methods. Utrecht: VSP, 2001.
 88. Prigarin S. M., Litvenko K. V. Numerical simulation of the sea surface and extreme ocean waves with stochastic spectral models // Proceedings of the AMSA-2011 International Workshop "Applied Methods of Statistical Analysis. Simulations and Statistical Inference" (20–22 September, 2011, Novosibirsk, Russia). Novosibirsk: Publishing house of NSTU, 2011, P. 394–402
 89. Prigarin S. M., Litvenko K. V. Conditional spectral models of extreme ocean waves // Rus. J. Numer. Anal. and Math. Modell. 2012. Vol. 27, № 3. P. 289–302.
 90. Prigarin S. M., Marshak A. L. A simple stochastic model for generating broken cloud optical depth and cloud top height fields // J. Atmospheric Sci. 2009. Vol. 66, № 1. P. 92–104.
 91. Prigarin S. M., Martin A., Winkler G., Simulation of binary random fields with Gaussian numerical models // Monte Carlo Methods and Applications. 2010. Vol. 16, Iss. 2. P. 129–142.
 92. Ripley B. D. Stochastic Simulation. N. Y.: Willey, 1987.
 93. Samorodnitsky G., Taqqu M. S. Stable non-Gaussian Random Processes: Stochastic Models with Infinite Variance. New York: Chapman & Hall, 1994.
 94. Stewart M. Cholesky factorization of semi-definite Toeplitz matrices // Lin. Alg. Appl. 1997. V. 254, P. 497–526.

95. Sunspot Number [Электронный ресурс]. URL: <http://www.sidc.be/silso/datafiles> (дата обращения 23 января 2018).
96. Tong Y. L. The Multivariate Normal Distribution. N. Y.: Springer-Verlag, 1990.
97. Wood A., Chan G. Simulation of stationary Gaussian processes in $[0, 1]^d$ // Journal of Computational and Graphical Statistics. 1994. Vol. 3. P. 409–432.

Предметный указатель

алгоритм Левинсона – Дурбина (Levinson–Durbin recursion), 43

алгоритм Холецкого – Банашевича (Cholesky–Banachiewicz algorithm), 32

алгоритм Холецкого – Краута (Cholesky–Crout algorithm), 32

альтернатива Фредгольма (Fredholm alternative), 55

аппаратный генератор случайных чисел (hardware random number generator), 62

винеровский процесс (Wiener process), 15, 47

гауссовский вектор (Gaussian vector), 8

гауссовское распределение (Gaussian distribution), 7

генератор «вихрь Мерсенна» (Mersenne twister), 61

генератор псевдослучайных чисел (pseudorandom number generator), 58

дробное броуновское движение (fractional Brownian motion), 47

квадратный корень матрицы (square root of a matrix), 29

матрица Тёплица (Toeplitz matrix, diagonal-constant matrix), 42

метод Бокса – Мюллера (Box–Muller transform), 24

мультипликативный генератор псевдослучайных чисел (linear congruential generator), 60, 64

мультифрактальное броуновское движение (multifractional Brownian motion), 49

начальное состояние генератора псевдослучайных чисел (seed), 59

нормальная матрица (normal matrix), 54

нормальная система (normal system), 56

нормальное псевдорешение (normal pseudo-solution), 57

нормальное решение (normal solution), 56

ортогональная матрица (orthogonal matrix), 57

показатель Хёрста (Hurst exponent), 47

положительно определенная матрица (positive definite matrix), 8, 51

полярное разложение (polar decomposition), 57

псевдообратная матрица (pseudoinverse), 53

псевдорешение (pseudo-solution), 56

разложение Холецкого (Cholesky decomposition), 32, 42

расширенная матрица (augmented matrix), 55

сильно стационарная случайная последовательность (strictly stationary random sequence), 37

сингулярное разложение (singular-value decomposition), 30

сингулярные числа (singular values), 30

скелетное разложение матрицы (skeleton decomposition), 18, 52

слабо стационарная случайная последовательность (weakly stationary random sequence), 38

случайный вектор с равноправными компонентами (exchangeable random variables), 35

случайный перестановочно-симметричный вектор (permutation-symmetric random vector), 35

совместная система линейных уравнений (consistent linear system), 55

таблица случайных чисел (random number table), 63

теорема Кронекера – Капелли (Kronecker–Capelli theorem), 55

теорема Фредгольма (Fredholm’s theorem), 55

унитарная матрица (unitary matrix), 57

уравнения Юла – Уокера (Yule–Walker equations), 43

условное гауссовское распределение (conditional Gaussian distribution), 15, 17

формулы Крамера (Cramer’s rule), 55

циркулянт (circulant matrix), 44

циркулянтное вложение (circulant embedding), 44

эввикоррелированный вектор (equicorrelated vector), 35

эввикорреляционная матрица (equicorrelated matrix), 35

Учебное издание

Пригарин Сергей Михайлович

Численное моделирование многомерных
гауссовских распределений

Учебное пособие

Редактор: *Скворцова А. А.*
Обложка *Неклюдовой Е. В.*

Подписано в печать 07.05.2018 г.
Формат $60 \times 84^{1/16}$. Гарнитура Computer Modern.
Уч.-изд. л. 4,9. Усл. печ. л. 5,3. Тираж 45 экз. Заказ № 96

Издательско-полиграфический центр НГУ
630090, Новосибирск, ул. Пирогова, 2