Санкт-Петербургский государственный университет
Прикладная математика и информатика
Статистическое моделирование

Бзикадзе Андрей Важевич

# Статистические свойства некоторых процедур сжатия данных

Выпуская квалификационная работа

Научный руководитель:
к. ф.-м. н., доцент В. В. Некруткин
Рецензент:
исследователь Е. А. Советкин

Санкт-Петербург
2017

Saint Petersburg State University
Applied Mathematics and Computer Science
Statistical Modelling

Bzikadze Andrey

# Statistical properties of some data compression procedures

Graduation Project

Scientific Supervisor:
Associate Professor V. V. Nekrutkin, PhD

Reviewer:
Researcher E. A. Sovetkin

Saint Petersburg
2017

# Оглавление

# Введение

Рассмотрим нулевую гипотезу о независимости и равномерной распределенности некоторого набора дискретных случайных величин, имеющих одинаковый носитель. Эта стандартная статистическая задача возникает, в частности, при проверке свойств генераторов псевдослучайных чисел (в дальнейшем — ГСЧ), которые используются повсеместно, начиная от решения задач с помощью метода Монте-Карло, вплоть до задач криптографии. «Качество» ГСЧ, определяемое их статистическими свойствами, оказывает существенное влияние, например, на результаты применения метода Монте-Карло.

Для проверки этих свойств существует несколько батарей тестов, среди которых наиболее известные: система, разработанная NIST [1], в основном предназначенная для криптографических генераторов, система под названием «Die Hard» [2], а также достаточно развитая и подробно документированная батарея «TestU01» [3].

В 2004 году появилась статья [4], в которой рассматривается новый тест для проверки свойств ГСЧ, названный «Book Stack». В основе теста лежит одноименное преобразование, предложенное в 1980 году в статье [5], применение которого заключалось в описании простой и наглядной процедуры сжатия информации. В англоязычной литературе более распространено название «Move-to-Front» [6]. Алгоритм приобрел достаточно широкую популярность и ныне используется в некоторых утилитах для сжатия данных — в основном как один из промежуточных шагов (см., например, [7]). После [4] было опубликовано еще несколько статей [8]–[15], так или иначе касающихся теста «Book Stack». В статье [11] теми же авторами предложен другой тест для проверки свойств ГСЧ, названный «Order»-тест.

Суть «Book Stack»- и «Order»-преобразований, лежащих в основе соответствующих тестов, заключается в том, что на вход алгоритмов подается набор случайных величин $\{\eta_i\}_{i\geqslant 1}$, принимающих значения во множестве $\{1, 2, \ldots, S\}$ и (при выполнении нулевой гипотезы) независимых и равномерно распределенных на этом множестве (будем кратко обозначать такое распределение $\mathrm{U}_S$). Результатом является новый набор случайных величин $\{\xi_i\}_{i\geqslant 1}$, которые при выполнении нулевой гипотезы обладают теми же свойствами, что и $\{\eta_i\}_{i\geqslant 1}$ (формальное описание «Book Stack»- и «Order»-преобразований дано в разделах 1.2 и 3.1 соответственно).

Авторами было предложено использовать «Book Stack»- и «Order»-преобразования

для проверки свойств ГСЧ. Стиль тестирования — побитовый, то есть рассматриваются отдельные двоичные биты (или их группы) псевдослучайных чисел, вырабатываемые ГСЧ, которые проверяются на равномерную распределенность на соответствующем множестве. Поэтому стандартным выбором $S$ является некоторая степень двойки.

С формальной точки зрения проверяется гипотеза $\mathbb{H}_0$, заключающаяся в том, что последовательность $\{\eta_i\}_{i\geqslant 1}$ является последовательностью независимых случайных величин, причем $\mathbb{P}(\eta_i = k) = 1/S$ при $1 \leqslant k \leqslant S$. Проверка осуществляется с помощью стандартного критерия $\chi^2$, причем в случае больших $S$ производится приемлемая группировка. Суть «Book Stack»- и «Order»-теста согласно статье [4], однако, состоит в том, что критерий $\chi^2$ применяется не к исходным случайным величинам $\{\eta_i\}_{i\geqslant 1}$, а к преобразованным $\{\xi_i\}_{i\geqslant 1}$, причем с той же степенью свободы. При этом утверждается, что «более вероятные буквы будут в среднем иметь более высокие частоты встречаемости» (см., например, [15]).

Таким образом, можно рассматривать два критерия: $\chi^2$, примененный к исходному набору $\{\eta_i\}_{i\geqslant 1}$, и $\chi^2$ — к преобразованному с помощью «Book Stack» или «Order» набору $\{\xi_i\}_{i\geqslant 1}$. Авторами неявно утверждается, что «Order»- и «Book Stack»-преобразования увеличивают мощность критерия, хотя теоретические и экспериментальные результаты, подтверждающие этот факт, в названных статьях отсутствуют, равно как не обсуждается и выбор альтернатив, относительно которых мощность должна потенциально увеличиваться. Более того, утверждается, что предложенные тесты улавливают отклонения от «случайности» даже для тех генераторов, которые выдерживают проверку некоторыми лучше изученными и более распространенными тестами.

В [14] приводятся результаты применения «Book Stack»-теста к линейным конгруэнтным генераторам (в дальнейшем — ЛКГ), рекомендованным в [16]. Утверждается, что это лучшие генераторы в классе ЛКГ, отбор происходил на основе так называемого спектрального теста (рассматривается в [17]). Каждый генератор, который был рассмотрен, в итоге отвергнут при применении «Book Stack».

В [11] рассматриваются результаты применения «Order»-теста к ЛКГ. После двойного тестирования не отвергнут только один мультипликативный генератор со следующими параметрами: модуль = 18776556235061 и период = $2^{48}$.

В [18] рассматриваются некоторые генераторы, которые рекомендуются для практического применения (например Вихрь Мерсенна [19], который один из немногих вы-

держивает проверку «Book Stack»-тестом). В [12] «Book Stack» применяется к криптографическим генераторам.

В литературе (например в [8], [9] и [10]) также присутствует обсуждение программных реализаций алгоритма. В частности, в [8] приводится ссылка на компьютерную реализацию с описанием функциональности и краткой документацией. Обзор эффективных реализаций «Book Stack»-преобразования, а также реализаций в открытом доступе с описанием их достоинств и недостатков см. в [20].

Со статистической точки зрения задача заключается в сравнении мощностей критерия $\chi^2$, примененного к исходному набору $\{\eta_i\}_{i\geqslant 1}$, и $\chi^2$ — к преобразованному с помощью «Book Stack»- или «Order»-преобразования набору $\{\xi_i\}_{i\geqslant 1}$. Для доказательства корректности тестов необходимо доказать, что случайные величины $\{\xi_i\}_{i\geqslant 1}$ независимы и равномерно распределены на множестве $\mathbb{S}$ тогда и только тогда, когда этими же свойствами обладают случайные величины $\{\eta_i\}_{i\geqslant 1}$. Поскольку в цитированных статьях доказательство этого факта (а также ссылка на него) отсутствует, для «Book Stack»-теста доказательство было проведено в [20] и в [21]. Для «Order»-теста корректность следует из результатов, полученных в данной работе (подробнее в Главе 3).

Нельзя говорить о сравнении мощностей критериев без выбора определенной альтернативной гипотезы. В рамках выпускной квалификационной работы бакалавра [20] и в [21] для «Book Stack» теста было проведено исследование альтернативной гипотезы, заключающейся в том, что случайные величины $\{\eta_i\}_{i\geqslant 1}$ являются независимыми и одинаково, но не равномерно, распределенными. Было показано, что относительно такого выбора альтернативной гипотезы мощность критерия «после» преобразования «Book Stack», как правило, является асимптотически меньшей, чем мощность критерия «до» преобразования. В [21] для проверки нулевой гипотезы $\mathbb{H}_0$ помимо критерия $\chi^2$ было предложено использовать критерий отношения правдоподобия. Удалось доказать, что относительно той же альтернативы мощность такого критерия «после» «Book Stack»-преобразования всегда является асимптотически меньшей, чем мощность критерия «до». Доказательство основывается на соотношении предельных распределений исходной последовательности $\{\eta_i\}_{i\geqslant 1}$ и преобразованной — $\{\xi_i\}_{i\geqslant 1}$.

Задачей данной работы является изучение поведения «Book Stack»-теста против альтернативы, заключающейся в том, что исходные случайные величины $\{\eta_i\}_{i\geqslant 1}$ образуют эргодическую однородную марковскую цепь со стационарным равномерным рас-

пределением. Удается показать, что против такой альтернативы критерий $\chi^2$ до преобразования «Book Stack» оказывается несостоятельным, в то время как при некоторых ограничениях такой же критерий «после» преобразования является состоятельным. Заметим, что доказательство вновь основывается на сравнении предельных распределений исходной последовательности $\{\eta_i\}_{i\geqslant 1}$ и преобразованной — $\{\xi_i\}_{i\geqslant 1}$.

В работе также получено обобщение «Book Stack»-преобразования, для которого сохраняются многие теоретико-вероятностные результаты. В предположении, что исходные случайные величины $\{\eta_i\}_{i\geqslant 1}$ образуют однородную марковскую цепь, удовлетворяющую некоторым свойствам, доказано наличие предельного распределения у преобразованных случайных величин $\{\xi_i\}_{i\geqslant 1}$, сходимость частот к которому обеспечивается Законом Больших Чисел. Более того, доказана Центральная Предельная Теорема для частот исходных и преобразованных случайных величин. Для (стандартного) «Book Stack»-преобразования такие результаты получены в предположении эргодичности марковской цепи $\{\eta_i\}_{i\geqslant 1}$. Для обобщений «Book Stack»-преобразования те же результаты получены при положительности всех переходных вероятностей марковской цепи $\{\eta_i\}_{i\geqslant 1}$.

В работе также изучаются свойства «Order»-теста. Удается доказать, что для любого критерия для проверки $\mathbb{H}_0$, такого что его статистика зависит только от частот выборки и инвариантна относительно их перестановок, статистики «до» и «после» «Order»-преобразования совпадают. С связи с этим применение «Order»-теста против любой альтернативной гипотезы вряд ли является оправданным.

Общая структура работы следующая. В Главе 1 приводится описание семейства преобразований, являющихся обобщением преобразования «Book Stack», а также вводятся основные обозначения. В Главе 2 рассматривается ситуация, состоящая в том, что входная последовательность $\{\eta_i\}_{i\geqslant 1}$ образует однородную марковскую цепь: в разделе 2.1 дано описание преобразования всей «стопки книг» марковской цепью, в разделе 2.2 найдено стационарное распределение выходной последовательности $\{\xi_i\}_{i\geqslant 1}$, сходимость к которому обеспечивается Законом Больших Чисел, в разделе 2.3 рассматриваются результаты, относящиеся к ЦПТ частот «входной» и «выходной» последовательности, а в разделе 2.4 производится сравнение предельных распределений входной и выходной последовательности. В Главе 3 рассматривается «Order»-преобразование и «Order»-тест: в разделе 3.1 приводится описание лежащего в основе теста «Order»-преобразования, а также вводятся основные обозначения, в разделе 3.2 обоснована бесперспективность

применения «Order»-теста, в разделе 3.3 произведено сравнение предельных распределений частот «входной» и «выходной» последовательностей.

# Глава 1

# Семейство «Book Stack»-подобных преобразований

## 1.1. Описание общей схемы преобразования

Рассмотрим формальное описание общей схемы «Book Stack»-подобного преобразования. «На вход» подается последовательность, вообще говоря, случайных величин $\{\eta_i\}_{i\geqslant 1}$, принимающих значения во множестве $\mathbb{S} \stackrel{\text{def}}{=} \{1, 2, \ldots, S\}$. Обозначим $\mathfrak{S}_S$ — множество всевозможных перестановок чисел от 1 до $S$, причем перестановки упорядочены лексикографически. Рассмотрим некоторое отображение $f\colon \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$, задающее «Book Stack»-подобное преобразование.

Введем последовательность векторов $\{\Xi_n \in \mathfrak{S}_S\}_{n\geqslant 0}$ так, что для $i \geqslant 1$

$$\Xi_i = f(\Xi_{i-1}, \eta_i), \tag{1.1.1}$$

а $\Xi_0$ — вообще говоря, случайный вектор, принимающий значения во множестве перестановок $\mathfrak{S}_S$. Конечно, все компоненты вектора $\Xi_i$ (для всех $i \geqslant 0$) различны.

Наконец, для всех $i \geqslant 1$ введем «выходную» последовательность$\{\xi_i\}_{i\geqslant 1}$, где $\xi_i \in \mathbb{S}$ определяется как решение уравнения

$$\eta_i = \Xi_{i-1}[\xi_i], \tag{1.1.2}$$

где $\Xi_i = (\Xi_i[1], \Xi_i[2], \ldots, \Xi_i[S])^{\mathrm{T}}$. Заметим, что для всех $i \geqslant 1$ решение уравнения (1.1.2) существует и единственно, так как $\Xi_{i-1}$ является некоторой перестановкой чисел $1, 2, \ldots, S$, а $\eta_i \in \mathbb{S}$.

Таким образом, «Book Stack»-подобному преобразованию «на вход» подается последовательность случайных величин $\{\eta_i\}_{i\geqslant 1}$, а «на выходе» имеется последовательность случайных величин $\{\xi_i\}_{i\geqslant 1}$, которая определяется отображением $f$, вектором $\Xi_0$ и «входной» последовательностью $\{\eta_i\}_{i\geqslant 1}$.

Нам понадобятся несколько определений, характеризующих условия, в дальнейшем накладываемые на отображение $f$.

**Определение 1.1.1.** Пусть $X, Y$ — некоторые множества. Отображение $g\colon X \times Y \to X$ будем называть *инъективным по второй компоненте*, если $g(x_1, y_1) \neq g(x_2, y_2)$ для любых неравных $y_1, y_2 \in Y$ и любых $x_1, x_2 \in X$.

Введем удобное сокращенное обозначение. Пусть $g\colon X \times Y \to X$ и пусть $\mathcal{Y} = (y_1, \ldots, y_n, \ldots)$, $y_i \in Y$. Для $j$-й декартовой степени множества $Y$ введем обозначение $Y^j$ (для всех $j \geqslant 1$). Обозначим $Y_j = (y_1, \ldots, y_j)$ для всех $j \geqslant 1$ и введем отображения $g^{(j)} : X \times Y^j \to X$ следующим образом: для любого $x \in X$ положим $g^{(1)}(x, Y_1) = g^{(1)}(x, y_1) = g(x, y_1)$ при $j = 1$ и

$$g^{(j)}(x, Y_j) = g\Big(g^{(j-1)}(x, Y_{j-1}), y_j\Big) \tag{1.1.3}$$

при $j > 1$.

**Определение 1.1.2.** Пусть $X$, $Y$ — некоторые множества. Рассмотрим отображение $g\colon X \times Y \to X$. Будем говорить, что отображение $g$ *$n$-связно по первому аргументу* (или просто *$n$-связно*), если для любых $x_1, x_2 \in X$ существует такое $Y_n = Y_n(x_1, x_2) \in Y^n$, что $g^{(n)}(x_1, Y_n) = x_2$.

Если отображение $g$ является $n$-связным при некотором $n$, то оно называется *конечно-связным. Порядком связности* конечно-связного отображения является минимальное $n$, при котором отображение является $n$-связным.

Вернемся к описанию «Book Stack»-подобного преобразования. По-прежнему, рассматриваем отображение $f : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$. Обозначим для любого $\alpha \in \mathfrak{S}_S$

$$\mathrm{C}_\alpha^{\mathfrak{S}_S} = \{\beta \,|\, \text{существует } k\colon f(\beta, k) = \alpha\}, \tag{1.1.4}$$

$$\mathrm{C}_\alpha^{S} = \{k \,|\, \text{ существует } \beta : f(\beta, k) = \alpha\}. \tag{1.1.5}$$

По определению $\mathrm{C}_\alpha^{\mathfrak{S}_S} \subset \mathfrak{S}_S$, а $\mathrm{C}_\alpha^{S} \subset \mathbb{S}$.

**Лемма 1.1.1.** *Рассмотрим отображение $f : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ и выберем произвольное $\alpha \in \mathfrak{S}_S$. Тогда*

*1. Если $f$ — конечно-связно, то множества $\mathrm{C}_\alpha^{\mathfrak{S}_S}$ и $\mathrm{C}_\alpha^{S}$ непусты.*

*2. Если $f$ — инъективно по второй компоненте, то множество $\mathrm{C}_\alpha^{S}$ либо пусто, либо состоит из одного элемента.*

*3. Если $f$ одновременно удовлетворяет пунктам 1 и 2, то $\mathrm{C}_\alpha^{S}$ состоит ровно из одного элемента.*

*Доказательство.* 1. Зафиксируем $\beta \in \mathfrak{S}_S$. Обозначим $n$ — порядок связности отображения $f$. Тогда существует $\overline{k}_n = (k_1, k_2, \ldots, k_n) \in \mathbb{S}^n$ такое, что $f^{(n)}(\beta, \overline{k}_n) = \alpha$. Если

$n = 1$, то $f(\beta, k_1) = \alpha$, а значит $\beta \in \mathrm{C}_\alpha^{\mathfrak{S}_S}$ и $k_1 \in \mathrm{C}_\alpha^S$ и утверждение доказано. В противном случае обозначим $\overline{k}_{n-1} = (k_1, k_2, \dots k_{n-1})$. Тогда $f^{(n-1)}(\beta, \overline{k}_{n-1}) \in \mathrm{C}_\alpha^{\mathfrak{S}_S}$, а $k_n \in \mathrm{C}_\alpha^S$.

2. Очевидно следует из определения 1.1.1.

3. Следует из п.1 и п.2. □

**Замечание 1.1.1.** В дальнейшем всегда предполагается, что отображение $f : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ — конечно-связно и инъективно по второй компоненте. В связи с п.3 Леммы 1.1.1, будем отождествлять множество $\mathrm{C}_\alpha^S$ и его единственный элемент.

Введем несколько дополнительных обозначений.

Пусть $\overline{\ell} = (\ell_0, \dots, \ell_j, \dots)$ и $\overline{k} = (k_0, \dots, k_j, \dots)$ — бесконечные последовательности с $\ell_j, k_j \in \mathbb{S}$. Обозначим $\overline{\ell}_m = (\ell_0, \dots, \ell_m)$, $\overline{k}_m = (k_0, \dots, k_m) \in \mathbb{S}^{m+1}$ для любого $m \geqslant 0$ и положим

$$\mathcal{F}_m(\overline{\ell}, \overline{k}) = \left\{\alpha \in \mathfrak{S}_S \,|\, \alpha_{\ell_0} = k_0 \text{ и } f^{(j)}(\alpha, \overline{k}_{j-1})[\ell_j] = k_j \;\text{ при } j \in 1 : m\right\}. \tag{1.1.6}$$

В случае $m = 0$ обозначим $\ell = \ell_0$ и $k = k_0$, тогда

$$\mathcal{F}_0(\ell, k) = \{\alpha \in \mathfrak{S}_S \,|\, \alpha_\ell = k\}. \tag{1.1.7}$$

## 1.2. Описание стандартного «Book Stack»-преобразования

Частным случаем описанной в предыдущем разделе общей схемы является так называемое (стандартное) «Book Stack»-преобразование. Отображение $f : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ для него определяется следующим образом. Для любого $x \in \mathbb{S}$ и любой перестановки $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_S) \in \mathfrak{S}_S$ обозначим $i_0 = i_0(\alpha, x)$ такой индекс, что $\alpha_{i_0} = x$. Тогда

$$f(\alpha, x)[i] \stackrel{\text{def}}{=} \begin{cases} x & \text{при } i = 1, \\ \alpha_i & \text{при } i > i_0, \\ \alpha_{i-1} & \text{при } 1 < i \leqslant i_0. \end{cases} \tag{1.2.1}$$

Нетрудно проверить, что $f$ является инъективным по второй компоненте и $S$-связным. Заметим, что $\mathrm{C}_\alpha^S = \{\alpha_1\}$ для любой перестановки $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_S) \in \mathfrak{S}_S$, где $\mathrm{C}_\alpha^S$ введено в (1.1.5).

Приведем теперь неформальное описание преобразования «Book Stack», которое лежит в основе рассматриваемого ниже алгоритма. Рассмотрим множество $\mathbb{S}$, как некоторый набор «книг», которые лежат в стопке («Book Stack») в каком-то начальном порядке. Можно для наглядности считать, что $1, \dots, S$ — это названия книг.

Само преобразование состоит в том, что из стопки некоторым образом выбирается (по названию) книга и кладется наверх. Так делается $n$ раз. Более формально, есть некоторая последовательность величин $\eta_i$, принимающих значения в множестве $\mathbb{S}$, о которых всегда в дальнейшем будем говорить, как о названиях книг.

Пусть после $(i-1)$-й итерации порядок книг в стопке оказался $(b_1, b_2 \ldots, b_S)$. Найдем тот номер $\xi_i$, при котором $\eta_i = b_{\xi_i}$. Иначе говоря, найдем $\xi_i$ — порядковый номер в стопке книги $\eta_i$ (затем эта книга перекладывается наверх, и процедура повторяется с заменой $\eta_i$ на $\eta_{i+1}$).

Результат $n$-кратного преобразования «Book Stack» — это последовательность положений $\xi_1, \xi_2 \ldots, \xi_n$ в стопке выбранных книг. При фиксированном начальном положении книг эта последовательность, конечно, определяется последовательностью $\eta_i$.

Обозначим начальное состояние стопки $(b_1, b_2, \ldots, b_S)$, где $b_i \in \mathbb{S}$, и сформулируем общее алгоритмическое описание «Book Stack»-преобразования.

### Общее алгоритмическое описание «Book Stack»-преобразования

**Входные данные**: $n$, $S$, $(b_1, b_2 \ldots, b_S)$, $(\eta_1, \eta_2 \ldots, \eta_n)$. **Результат**: $(\xi_1, \xi_2 \ldots, \xi_n)$.

**1.** (*Цикл по шагам Book Stack*) For $i = 1$ to $n$ do

- (*Инициализация*) $j \leftarrow 1$;
- (*Поиск места выбранной книги*) While $(b_j \neq \eta_i)$ do $(j \leftarrow j + 1)$; $\xi_i \leftarrow j$;
- (*Формирование новой стопки*) $b_1, \ldots b_{j-1} \to b_2, \ldots b_j$; $b_1 \leftarrow \eta_i$.

**2.** (*Завершение работы*) STOP.

# Глава 2

# «Book Stack»-тест при отклонении от независимости: однородная марковская цепь

Предположим, что «входная» последовательность «Book Stack»-подобного преобразования $\{\eta_i\}_{i\geqslant 1}$ образует однородную марковскую цепь (в дальнейшем ОМЦ). Как хорошо известно (см., например, [22]), для эргодических ОМЦ (в дальнейшем ЭОМЦ) существует единственное стационарное распределение, сходимость частот ЭОМЦ к которому обеспечивается Законом Больших Чисел (в дальнейшем ЗБЧ). При этом, согласно [23], в тех же предположениях выполняется многомерная Центральная Предельная Теорема (в дальнейшем ЦПТ) для частот цепи. В этом разделе доказывается, что если ОМЦ $\{\eta_i\}_{i\geqslant 1}$ является эргодической, то для «Book Stack»-преобразования, определенного в разделе 1.2, «выходная» последовательность $\{\xi_i\}_{i\geqslant 1}$ имеет некоторое предельное распределение, причем выполняется соответствующие ЗБЧ и многомерная ЦПТ для частот этой последовательности. Если же ОМЦ $\{\eta_i\}_{i\geqslant 1}$, обладает переходной матрицей с положительными переходными вероятностями, то те же результаты сохраняются для произвольного инъективного по второй компоненте и конечного-связного отображения.

## 2.1. «Стопка книг» как марковская цепь

Целью данного раздела является изучение марковских свойств последовательности состояний «стопки книг» $\{\Xi_i\}_{i=1}^{\infty}$, введенной в (1.1.1), а также отыскание условий, которые обеспечивают существование стационарного распределения у этой последовательности. Предположим, что выполнены следующие условия:

a) последовательность $\{\eta_n\}_{n\geqslant 1}$ является ОМЦ с фазовым пространством $\mathbb{S}$, переходной матрицей $\mathbf{P}^{(\eta)} = (p_{ij})$ и начальным распределением $\left(p_1^{(1)}, p_2^{(1)}, \ldots, p_S^{(1)}\right)$,

b) случайный вектор $\Xi_0 \in \mathfrak{S}_S$, имеющий распределение $\left(\pi^{(0)}_{1,2,\ldots,S}, \ldots, \pi^{(0)}_{S,S-1,\ldots,1}\right)$, и марковская цепь $\{\eta_n\}_{n\geqslant 1}$ независимы.

Начнем с общего случая, когда отображение $f$ является конечно-связным и инъективным по второй компоненте.

**Предложение 2.1.1.** *1. Если отображение $f\colon \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ является конечно-связ-*

*ным и инъективным по второй компоненте, то последовательность* $\{\Xi_i\}_{i=1}^{\infty}$, *введенная в* (1.1.1), *образует ОМЦ с фазовым пространством* $\mathfrak{S}_S$, *начальным распределением*

$$\mathbb{P}(\Xi_1 = \alpha) = p^{(1)}_{\mathrm{C}^S_\alpha} \sum_{\beta \in \mathrm{C}^{\mathfrak{S}_S}_\alpha} \pi^{(0)}_\beta, \quad \alpha \in \mathfrak{S}_S, \tag{2.1.1}$$

*и матрицей переходных вероятностей* $\mathbf{P}^{(\Xi)} = \left(p^{(\Xi)}_{\alpha\beta}\right)$, *где для* $\alpha, \beta \in \mathfrak{S}_S$

$$p^{(\Xi)}_{\alpha\beta} = \begin{cases} p_{\mathrm{C}^S_\alpha, \mathrm{C}^S_\beta} & \text{при } \alpha \in \mathrm{C}^{\mathfrak{S}_S}_\beta, \\ 0 & \text{иначе}, \end{cases} \tag{2.1.2}$$

*а множества* $\mathrm{C}^{\mathfrak{S}_S}_\alpha$ *и* $\mathrm{C}^S_\alpha$ *введены в* (1.1.4) *и* (1.1.5) *соответственно.*

*2. Если дополнительно потребовать, чтобы* $p_{ij} > 0$ *для всех* $i$ *и* $j$, *то марковская цепь* $\{\Xi_n\}_{n \geqslant 1}$ *окажется эргодической.*

*Доказательство.* 1. По п.3 Леммы 1.1.1 для любой перестановки $\alpha \in \mathfrak{S}_S$ множество $\mathrm{C}^S_\alpha$ состоит ровно из одного элемента. Для любого $n \geqslant 1$ и любых перестановок $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathfrak{S}_S$ рассмотрим вероятность $\mathbb{P}(\Xi_1 = \alpha_1, \ldots, \Xi_n = \alpha_n)$. Нужно доказать, что

$$\mathbb{P}(\Xi_1 = \alpha_1, \ldots, \Xi_n = \alpha_n) = \left( p^{(1)}_{\mathrm{C}^S_{\alpha_1}} \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \pi^{(0)}_{\alpha_0} \right) p^{(\Xi)}_{\alpha_1\alpha_2} \ldots p^{(\Xi)}_{\alpha_{n-1}\alpha_n}. \tag{2.1.3}$$

Если найдется такое $i \in 2 : n$, что $\alpha_{i-1} \notin \mathrm{C}^{\mathfrak{S}_S}_{\alpha_i}$, то $p^{(\Xi)}_{\alpha_{i-1}\alpha_i} = 0$ и поэтому левая часть (2.1.3) равна нулю и совпадает с правой. Если же $\alpha_{i-1} \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_i}$ для всех $i$, то ввиду инъективности по второй компоненте отображения $f$ события $\{f(\alpha_{i-1}, \eta_i) = \alpha_i\}$ и $\{\eta_i = \mathrm{C}^S_{\alpha_i}\}$ совпадают. Следовательно,

$$\begin{aligned}
\mathbb{P}(\Xi_1 = \alpha_1, \ldots, \Xi_n = \alpha_n) &= \sum_{\alpha_0 \in \mathfrak{S}_S} \mathbb{P}(\Xi_0 = \alpha_0, \Xi_1 = \alpha_1, \ldots, \Xi_n = \alpha_n) = \\
&= \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \mathbb{P}(\Xi_0 = \alpha_0, \Xi_1 = \alpha_1, \ldots, \Xi_n = \alpha_n) = \\
&= \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \mathbb{P}(\Xi_0 = \alpha_0, f(\Xi_0, \eta_1) = \alpha_1, \ldots, f(\Xi_{n-1}, \eta_n) = \alpha_n) = \\
&= \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \mathbb{P}\left(\Xi_0 = \alpha_0, \eta_1 = \mathrm{C}^S_{\alpha_1}, \ldots, \eta_n = \mathrm{C}^S_{\alpha_n}\right) = \\
&= \mathbb{P}\left(\eta_1 = \mathrm{C}^S_{\alpha_1}, \ldots, \eta_n = \mathrm{C}^S_{\alpha_1}\right) \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \mathbb{P}\left(\Xi_0 = \alpha_0\right) = \\
&= p^{(1)}_{\mathrm{C}^S_{\alpha_1}} p_{\mathrm{C}^S_{\alpha_1}\mathrm{C}^S_{\alpha_2}} \ldots p_{\mathrm{C}^S_{\alpha_{n-1}}\mathrm{C}^S_{\alpha_n}} \sum_{\alpha_0 \in \mathrm{C}^{\mathfrak{S}_S}_{\alpha_1}} \pi^{(0)}_{\alpha_0},
\end{aligned}$$

то есть согласно определению $p^{(\Xi)}_{\alpha\beta}$ в (2.1.2) равенство (2.1.3) снова имеет место.

2. Пусть теперь $p_{ij} > 0$ для всех $i$ и $j$. Для того, чтобы конечная ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ была эргодической, достаточно существование такой степени $k$, что матрица $\left(\mathbf{P}^{(\Xi)}\right)^k$ имеет все положительные элементы. Очевидно, что достаточно возвести матрицу $\mathbf{P}^{(\Xi)}$ в степень равную порядку связности отображения $f$. □

Хорошо известен следующий результат (см., например, [22]).

**Предложение 2.1.2.** *Пусть выполнены условия второго пункта Предложения 2.1.1. Тогда*

*1. У ОМЦ $\{\Xi_n\}_{n\geqslant 1}$ имеется стационарное распределение $(\pi_\alpha, \alpha \in \mathfrak{S}_S)$ со всеми положительными вероятностями.*

*2. Для любого начального распределения $\{\Xi_n\}_{n\geqslant 1}$ (т.е. согласно первому пункту Предложения 2.1.1 для любых $\mathcal{L}(\eta_1)$ и $\mathcal{L}(\Xi_0)$) при $n \to \infty$*

$$\mathbb{P}(\Xi_n = \alpha \,|\, \Xi_1 = \beta) \to \pi_\alpha,$$
$$\mathbb{P}(\Xi_n = \alpha) \to \pi_\alpha,$$

*для всех $\alpha$, $\beta \in \mathfrak{S}_S$.*

*При этом существует такое $\rho \in [0; 1)$ и $C > 0$, что для всех $\alpha$, $\beta \in \mathfrak{S}_S$*

$$\left|\mathbb{P}(\Xi_n = \alpha \,|\, \Xi_1 = \beta) - \pi_\alpha\right| \leqslant C\rho^n. \tag{2.1.4}$$

Таким образом, для произвольного «Book Stack»-подобного преобразования положительность всех вероятностей перехода $p_{ij}$ «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$ является достаточным условием для существования стационарного распределения у ОМЦ $\{\Xi_i\}_{i\geqslant 1}$. Оказывается, что для преобразования «Book Stack», введенного в разделе 1.2, условие можно ослабить, а именно потребовать лишь эргодичности ОМЦ $\{\Xi_i\}_{i\geqslant 1}$. Прежде, чем сформулировать строгий результат, необходимо доказать вспомогательную лемму.

**Лемма 2.1.1.** *Рассмотрим $f$ — преобразование «Book Stack», определенное в разделе 1.2. Пусть $\alpha \in \mathfrak{S}_S$ и $X_m = (x_1, x_2, \ldots, x_m)^{\mathrm{T}} \in \mathbb{S}^m$. При этом среди $\{x_i\}_{i=1}^m$ ровно $k \leqslant S$ различных элементов. Обозначим $\beta = f^{(m)}(\alpha, X_m) \in \mathfrak{S}_S$. Тогда $\beta[1:k]$ состоит только из компонент вектора $X_m$. Причем порядок компонент в $\beta[1:k]$ однозначно определяется вектором $X_m$.*

*Доказательство.* Индукция по $k$. База при $k = 1$ и $m \geqslant 1$ очевидна. Пусть утверждение верно для $k$ и любого $m \geqslant k$ и пусть теперь среди $\{x_i\}_{i=1}^m$ ровно $k+1 \leqslant S$ различных элементов, при этом $m \geqslant k+1$. Выберем такое $t \in 1 : m$, что среди $\{x_i\}_{i=1}^t$ ровно $k$ различных элементов. Обозначим $\gamma = f^{(t)}\left(\alpha, (x_1, x_2, \ldots, x_t)^{\mathrm{T}}\right)$. Тогда по индукционному предположению $\gamma[1 : k]$ состоит из элементов $\{x_i\}_{i=1}^t$, причем порядок компонент в $\gamma[1 : k]$ однозначно определяется набором $\{x_i\}_{i=1}^t$. По базе индукции, примененной к $\gamma$, и определению отображения $f$ имеем $\beta[1] = x_{t+1} = x_{t+2} = \ldots = x_m$, поэтому $\beta = f(\gamma, x_{t+1})$. Заметим, что по индукционному предположению $\gamma[i] \neq x_{t+1} = x_m$ для любого $i \in 1 : k$. По определению отображения $f$ имеем, что $\beta[2 : (k+1)] = \gamma[1 : k]$, откуда следует требуемое. □

**Следствие 2.1.1.** В обозначениях Леммы 2.1.1 перестановка $\beta$ при $k = S$ не зависит от выбора $\alpha$.

**Предложение 2.1.3.** *Пусть $f$ — стандартное «Book Stack»-преобразование, определенное в разделе 1.2 и пусть «входная» ОМЦ $\{\eta_n\}_{n\geqslant 1}$ — эргодическая. Тогда $\{\Xi_n\}_{n\geqslant 1}$ образует ОМЦ и имеет ровно один непериодический эргодический класс и, быть может, несколько несущественных состояний.*

*Доказательство.* В первом пункте Предложения 2.1.1 показано, что $\{\Xi_n\}_{n\geqslant 1}$ образует ОМЦ для любого инъективного по второй компоненте и конечно-связного и, в частности, для стандартного «Book Stack»-преобразования.

Сначала докажем единственность эргодического класса ОМЦ $\{\Xi_i\}_{i=1}^\infty$. Из эргодичности «входной» ОМЦ $\{\eta_i\}_{i\geqslant 1}$ следует существование траектории $\{x_i\}_{i=0}^m \in \mathbb{S}^m$ с положительными вероятностями переходов, такой что $x_0 = x_m$ и среди $\{x_i\}_{i=0}^m$ есть все элементы множества $\mathbb{S}$. Для дальнейшего обозначим $X_m = (x_1, x_2, \ldots, x_m)^{\mathrm{T}}$.

Рассмотрим произвольную перестановку $\alpha \in \mathfrak{S}_S$. В силу эргодичности «входной» ОМЦ $\{\eta_i\}_{i\geqslant 1}$ существует траектория положительной вероятности $Y_\ell \in \mathbb{S}^\ell$ с $Y_\ell[\ell] = x_0$ и $p_{\alpha[1]Y_\ell[1]} > 0$. Обозначим $\beta = f^{(\ell)}(\alpha, Y_\ell)$. Ясно, что $\beta[1] = x_0$.

Теперь определим $\gamma = f^{(m)}(\beta, X_m)$. Ясно, что $\gamma[1] = x_m = x_0$. По Следствию 2.1.1 $\gamma$ не зависит от выбранной перестановки $\beta$ (и, следовательно, $\alpha$) и полностью определяется последовательностью $\{x_i\}_{i=0}^m$.

Таким образом, построена перестановка $\gamma \in \mathfrak{S}_S$, являющаяся достижимой из любой другой перестановки $\alpha \in \mathfrak{S}_S$. Из этого мгновенно следует единственность эргодического класса ОМЦ $\{\Xi_i\}_{i=1}^\infty$.

Теперь докажем непериодичность единственного эргодического класса ОМЦ $\{\Xi_i\}_{i=1}^{\infty}$. Для любого непустого множества $A \subset \mathbb{N}$ обозначим $\gcd(A)$ — наибольший общий делитель элементов множества $A$. По условию $\gcd(n \,|\, p_{ii}(n) > 0) = 1$ для любого $i \in 1 : S$. Требуется показать, что $\gcd\left(n \,\middle|\, p_{\alpha\alpha}^{(\Xi)}(n) > 0\right) = 1$ для любого существенного $\alpha \in \mathfrak{S}_S$.

Фиксируем существенное $\alpha \in \mathfrak{S}_S$. Обозначим $\overline{\alpha} = \alpha[1]$. Заметим, что для некоторого $n \geqslant S$ существует траектория положительной вероятности $X_n = (x_1, x_2, \ldots, x_n)^{\mathrm{T}} \in \mathbb{S}^n$, такая что $\alpha = f^{(n)}(\alpha, X_n)$, $p_{\overline{\alpha}x_1} > 0$ и при этом среди компонент $X_n$ встречаются все элементы $\mathbb{S}$. Действительно, из доказательства единственности эргодического класса следует, что существует траектория положительной вероятности, удовлетворяющая указанным свойствам, но «приходящая» в некоторое $\gamma$, а по предположению $\alpha$ является существенным состоянием.

Рассмотрим теперь любое такое $\ell$, что $p_{\overline{\alpha}\overline{\alpha}}(\ell) > 0$ и траекторию положительной вероятности $Y_\ell = (y_1, y_2, \ldots y_\ell)^{\mathrm{T}} \in \mathbb{S}^\ell$, с $y_\ell = \overline{\alpha}$ и $p_{\overline{\alpha}y_1} > 0$. Положим $\beta = f^{(\ell)}(\alpha, Y_\ell)$. Заметим, что, вообще говоря, $\beta \neq \alpha$. Однако, по Следствию 2.1.1 $f^{(n)}(\beta, X_n) = \alpha$, причем $p_{\beta[1]x_1} > 0$, так как $\beta[1] = y_\ell = \overline{\alpha}$, а $p_{x_i x_{i+1}} > 0$ для всех $1 \leqslant i < n$ по построению $X_n$.

Обозначим теперь $Z_{n,\ell} = Z(X_n, Y_\ell) = (y_1, y_2, \ldots, y_\ell, x_1, x_2, \ldots, x_n)^{\mathrm{T}} \in \mathbb{S}^{\ell+n}$. Ясно, что $f^{(n+\ell)}(\alpha, Z_{n,\ell}) = \alpha$, причем вероятности всех переходов положительны. Таким образом, для $n$ и такого $\ell$, что $p_{\overline{\alpha}\overline{\alpha}}(\ell) > 0$, выполнено неравенство

$$p_{\alpha\alpha}^{(\Xi)}(n + \ell) > 0. \tag{2.1.5}$$

Покажем, что

$$\gcd\left(n + \ell \,\middle|\, p_{\overline{\alpha}\overline{\alpha}}(\ell) > 0, \ell \in \mathbb{N}\right) = 1. \tag{2.1.6}$$

Из этого по (2.1.5) будет следовать, что $\gcd\left(n + \ell \,\middle|\, p_{\alpha\alpha}^{(\Xi)}(n + \ell) > 0, \ell \in \mathbb{N}\right) = 1$. А, значит, будет доказано, что и $\gcd\left(\ell \in \mathbb{N} \,\middle|\, p_{\alpha\alpha}^{(\Xi)}(\ell) > 0\right) = 1$.

Итак, доказываем (2.1.6). Обозначим

$$\mathcal{L} = \{\ell \in \mathbb{N} \,|\, p_{\overline{\alpha}\overline{\alpha}}(\ell) > 0\}.$$

По условию

$$\gcd(\mathcal{L}) = 1.$$

Если $1 \in \mathcal{L}$, то (2.1.6) очевидно и утверждение Предложения доказано. Пусть $1 \notin \mathcal{L}$. Выберем $t \in \mathbb{N}$ так, что $(\min \mathcal{L})^t > n + m_0$, где $m_0$ — такая минимальная степень,

что $\left(\mathbf{P}^{(\eta)}\right)^{m_0}$ имеет все положительные элементы. Из равенства Чепмена-Колмогорова и определения множества $\mathcal{L}$ мгновенно следует, что $p_{\overline{\alpha}\alpha}\left(\ell^t\right) > 0$ для всех $\ell \in \mathcal{L}$ и, конечно, $\gcd\left(\ell^t \,|\, \ell \in \mathcal{L}\right) = 1$. Следовательно, т.к. $\ell^t - n > m_0$, то $p_{\overline{\alpha}\alpha}(\ell^t - n) > 0$ для любого $\ell \in \mathcal{L}$. Обозначим $\overline{\mathcal{L}} = \{\ell^t - n \,|\, \ell \in \mathcal{L}\}$.

Таким образом, существует такое множество $\overline{\mathcal{L}} \subset \mathbb{N}$, что $p_{\overline{\alpha}\alpha}(\overline{\ell}) > 0$ для всех $\overline{\ell} \in \overline{\mathcal{L}}$ и

$$\gcd\left(n + \overline{\ell} \,|\, \overline{\ell} \in \overline{\mathcal{L}}\right) = 1.$$

Из этого следует (2.1.6), а значит $\gcd\left(\ell \in \mathbb{N} \,|\, p^{(\Xi)}_{\alpha\alpha}(\ell) > 0\right) = 1$. □

**Замечание 2.1.1.** Из второго пункта Предложения 2.1.1 следует, что при $p_{ij} > 0$ для всех $i, j \in \mathbb{S}$, несущественных состояний нет.

**Пример 2.1.1.** Для того, чтобы показать, как устроены несущественные состояния, приведем следующий пример. Пусть $S = 3$ и все $p_{ij} > 0$ кроме $p_{23}$ и $p_{33}$. В таком случае «входная» ОМЦ $\{\eta_i\}_{i\geqslant 1}$ является эргодической. В то же время, так как при $i > 0$

$$\mathbb{P}\left(\Xi_i = (3, 2, 1)^{\mathrm{T}}\right) = 0,$$

то состояние $(3, 2, 1)^{\mathrm{T}}$ ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ является несущественным.

Результат Предложения 2.1.3 отличается от результата второго пункта Предложения 2.1.1 лишь возможностью наличия у $\{\Xi_i\}_{i=1}^{\infty}$ нескольких несущественных состояний. Как известно, конечная ОМЦ «покидает» в пределе несущественные состояния. В связи с этим естественно ожидать выполнение аналога Предложения 2.1.2. Как мы увидим, такой аналог, действительно, имеет место. Для того, чтобы в этом убедится, потребуется следующая теорема.

**Теорема 2.1.1.** *Пусть последовательность $\beta_1, \beta_2, \ldots, \beta_n, \ldots$ является ОМЦ с конечным фазовым пространством $X$, обладает ровно одним непереодическим эргодическим классом и, быть может, несколькими несущественными состояниями. Для любого $x \in X$ и каждого $n \geqslant 1$ определим*

$$\tau_x(n) = \mathbb{I}_x(\beta_1) + \ldots + \mathbb{I}_x(\beta_n).$$

*Тогда*

*1. ОМЦ $\{\beta_n\}_{n\geqslant 1}$ имеет единственное стационарное распределение $\pi = (\pi_x)_{x\in X}$. При этом $\pi_x = 0$ тогда и только тогда, когда $x \in X$ является несущественным состоянием.*

*2. Для любого начального распределения ОМЦ* $\{\beta_n\}_{n\geqslant 1}$ *имеет место сходимость*

$$\mathbb{P}(\beta_n = x \,|\, \beta_1 = x_0) \to \pi_x$$

*для всех* $x$, $x_0 \in X$. *Причем существует* $\rho \in [0;1)$ *и* $C > 0$ *такое, что для всех* $x$, $x_0 \in X$

$$\left|\mathbb{P}(\beta_n = x \,|\, \beta_1 = x_0) - \pi_x\right| \leqslant C\rho^n. \tag{2.1.7}$$

*3. Для всех* $x \in X$ *имеет место сходимость*

$$\frac{\tau_x(n)}{n} \to \pi_x$$

*почти всюду.*

*Доказательство.* Первый пункт следует из [24, Гл. VIII, §6, Теорема 2].

Из [25, Гл. 12, §5, Теорема 1] следует, что произвольного начального распределения ОМЦ $\{\beta_n\}_{n\geqslant 1}$ и для всех $x, x_0 \in X$ существуют пределы

$$\lim_{n\to\infty} \mathbb{P}(\beta_n = x \,|\, \beta_1 = x_0),$$

независящие от начального распределения и состояния $x_0$.

Из [24, Гл. VIII, §6, Теорема 1] следует, что эти пределы совпадают с единственным стационарным распределением:

$$\lim_{n\to\infty} \mathbb{P}(\beta_n = x \,|\, \beta_1 = x_0) = \pi_x$$

для всех $x, x_0 \in X$ и любого начального распределения ОМЦ $\{\beta_n\}_{n\geqslant 1}$.

Для несущественного состояния $x \in X$ (2.1.7) следует из доказательства [25, Гл. 12, §5, Теорема 1]. Для существенных состояний $x$ тот же результат, а также третий пункт Теоремы следует из [26, Гл. 1, §1.9 Пример 1.9.9]. □

Непосредственное применение Теоремы 2.1.1 к ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ дает следующий результат.

**Предложение 2.1.4.** *В условиях Предложения 2.1.3 у ОМЦ* $\{\Xi_n\}_{n\geqslant 1}$ *имеется стационарное распределение* $(\pi_\alpha, \alpha \in \mathfrak{S}_S)$, *причем нулевые вероятности соответствуют несущественным состояниям (и только им). Свойства стационарного распределения* $(\pi_\alpha, \alpha \in \mathfrak{S}_S)$, *установленные в пункте 2 Предложения 2.1.2, полностью сохраняются.*

Таким образом, найдены условия, накладываемые на «входную» ОМЦ $\{\eta_i\}_{i=1}^{\infty}$, являющиеся достаточными для существования стационарного распределения ОМЦ $\{\Xi_n\}_{n\geqslant 1}$. Для произвольного «Book Stack»-подобного преобразования условия — это положительность всех вероятностей перехода, а для стандартного «Book Stack»-преобразования достаточно более слабого условия — эргодичности цепи.

В дальнейшем стационарное распределение марковской цепи $\{\Xi_n\}_{n\geqslant 1}$ всегда будет обозначаться

$$(\pi_{1,2,\ldots,S},\ldots,\pi_{S,S-1,\ldots,1})\,. \tag{2.1.8}$$

## 2.2. Закон Больших Чисел для частот выходной последовательности

Цель данного раздела заключается в изучении свойств сходимости по вероятности частот «выходной» последовательности $\{\xi_i\}_{i=1}^{\infty}$, введенной в (1.1.2), к неким предельным вероятностям. Как и раньше, предполагаем, что входная последовательность $\{\eta_i\}_{i\geqslant 1}$ образует ОМЦ с матрицей переходных вероятностей $\mathbf{P}^{(\eta)} = (p_{ij})$. Мы предполагаем также, что вектор $\Xi_0$ и ОМЦ $\{\eta_i\}_{i\geqslant 1}$ независимы.

В предыдущем разделе исследовались различные условия, обеспечивающие существование и единственность стационарного распределения ОМЦ $\{\Xi_n\}_{n\geqslant 1}$, введеной в (1.1.1). В этом разделе доказывается, что в таких же условиях имеет место ЗБЧ для «выходной» последовательности $\{\xi_n\}_{n\geqslant 1}$.

Прежде всего нам потребуется следующая лемма, в которой исследуются марковские свойства последовательности пар $\{(\Xi_n,\eta_{n+1})\}_{n\geqslant 0}$. Как мы увидим, они во многом аналогичны марковским свойствам ОМЦ $\{\Xi_i\}_{i\geqslant 1}$. По-прежнему будем обозначать $\left(\pi^{(0)}_{1,2,\ldots,S},\ldots,\pi^{(0)}_{S,S-1,\ldots,1}\right)$ и $\left(p_1^{(1)},\ldots,p_S^{(1)}\right)$ распределения $\Xi_0$ и $\eta_1$ соответственно. Также будем обозначать $(\pi_{1,2,\ldots,S},\ldots,\pi_{S,S-1,\ldots,1})$ — стационарное распределение ОМЦ $\{\Xi_i\}_{i\geqslant 1}$.

**Лемма 2.2.1.** *1. Если отображение $f\colon \mathfrak{S}_S\times\mathbb{S}\to\mathfrak{S}_S$ является инъективным по второй компоненте и конечно-связным, то последовательность пар $\{(\Xi_n,\eta_{n+1})\}_{n\geqslant 0}$ образует ОМЦ с фазовым пространством $\mathfrak{S}_S\times\mathbb{S}$, начальным распределением, для всех $(\alpha,k)\in\mathfrak{S}_S\times\mathbb{S}$ задаваемым вероятностями*

$$\mathbb{P}\big((\Xi_0,\eta_1)=(\alpha,k)\big)=\pi^{(0)}_{\alpha}p^{(1)}_k,$$

*и переходной матрицей* $\mathbf{P}^{(\Xi,\eta)} = \left(p^{(\Xi,\eta)}_{\alpha i \beta j}\right)$, *где*

$$p^{(\Xi,\eta)}_{\alpha i \beta j} = p^{(\Xi,\eta)}_{(\alpha,i),(\beta,j)} = \begin{cases} p_{ij} & \text{при } f(\alpha,i) = \beta, \\ 0 & \text{иначе.} \end{cases} \tag{2.2.1}$$

*2. Если в условиях п.1 дополнительно потребовать, чтобы* $p_{ij} > 0$ *для всех* $i, j \in \mathbb{S}$, *то ОМЦ* $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$ *является эргодической.*

*3. Если отображение* $f\colon \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ *— стандартное «Book Stack»-преобразование, определенное в разделе 1.2, а «входная» последовательность образует ЭОМЦ, то последовательность пар* $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$ *образует ОМЦ, которая обладает одним непереодическим эргодическим классом и, быть может, несколькими несущественными состояниями.*

*4. В предположении п.2 или 3 стационарное распределение ОМЦ* $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$ *задается вероятностями вида*

$$\pi^{(\Xi,\eta)}_{(\alpha,k)} = \pi_\alpha p_{\mathrm{C}^S_\alpha k}, \tag{2.2.2}$$

*где множество* $\mathrm{C}^S_\alpha$ *введено в* (1.1.5), $\alpha \in \mathfrak{S}_S$ *и* $k \in \mathbb{S}$.

*5. В предположении п.2 или 3 для любого начального распределения ОМЦ* $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$ *и для любых* $\alpha, \beta \in \mathfrak{S}_S$ *и всех* $k, r \in \mathbb{S}$ *при* $n \to \infty$

$$\mathbb{P}\big(\,(\Xi_n, \eta_{n+1}) = (\alpha, k) \,\big|\, (\Xi_0, \eta_1) = (\beta, r)\big) \to \pi_\alpha p_{\mathrm{C}^S_\alpha k},$$
$$\mathbb{P}\big(\,(\Xi_n, \eta_{n+1}) = (\alpha, k)\big) \to \pi_\alpha p_{\mathrm{C}^S_\alpha k}.$$

*Причем существует такое* $\rho \in [0, 1)$ *и* $C > 0$, *что для любых* $\alpha, \beta \in \mathfrak{S}_S$ *и всех* $k, r \in \mathbb{S}$

$$\left|\mathbb{P}\big(\,(\Xi_n, \eta_{n+1}) = (\alpha, k) \,\big|\, (\Xi_0, \eta_1)) = (\beta, r)\big) - \pi_\alpha p_{\mathrm{C}^S_\alpha, k}\right| \leqslant C\rho^n.$$

*Доказательство.* 1. Для любых $n \geqslant 1$, $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathfrak{S}_S$ и $k_1, k_2, \ldots, k_n \in \mathbb{S}$ рассмотрим вероятность

$$\mathbb{P}\big((\Xi_0, \eta_1) = (\alpha_0, k_1), (\Xi_1, \eta_2) = (\alpha_1, k_2), \ldots, (\Xi_{n-1}, \eta_n) = (\alpha_{n-1}, k_n)\big).$$

Если найдется такой $i \in 1 : (n-1)$, что $f(\alpha_{i-1}, k_i) \neq \alpha_i$ (то есть $k_i \neq \mathrm{C}^S_{\alpha_i}$ или $\alpha_{i-1} \notin \mathrm{C}^{\mathfrak{S}_S}_{\alpha_i}$),

то эта вероятность равна 0. Рассмотрим оставшийся случай.

$$\begin{gathered}\mathbb{P}\big((\Xi_0,\eta_1)=(\alpha_0,k_1),(\Xi_1,\eta_2)=(\alpha_1,k_2),\dots,(\Xi_{n-1},\eta_n)=(\alpha_{n-1},k_n)\big)=\\ =\mathbb{P}\left((\Xi_0,\eta_1)=\left(\alpha_0,\mathrm{C}^S_{\alpha_1}\right),(\Xi_1,\eta_2)=\left(\alpha_1,\mathrm{C}^S_{\alpha_2}\right),\dots,(\Xi_{n-1},\eta_n)=(\alpha_{n-1},k_n)\right)=\\ =\mathbb{P}\left(\Xi_0=\alpha_0,\eta_1=\mathrm{C}^S_{\alpha_1},\eta_2=\mathrm{C}^S_{\alpha_2},\dots,\eta_{n-1}=\mathrm{C}^S_{\alpha_{n-1}},\eta_n=k_n\right)=\\ =\mathbb{P}\left(\Xi_0=\alpha_0\right)\mathbb{P}(\eta_1=\mathrm{C}^S_{\alpha_1},\eta_2=\mathrm{C}^S_{\alpha_2},\dots,\eta_{n-1}=\mathrm{C}^S_{\alpha_{n-1}},\eta_n=k_n)=\\ =\pi^{(0)}_{\alpha_0}p^{(1)}_{\mathrm{C}^S_{\alpha_1}}p_{\mathrm{C}^S_{\alpha_1}\mathrm{C}^S_{\alpha_2}}\dots p_{\mathrm{C}^S_{\alpha_{n-1}}k_n}.\end{gathered}$$

Заметим, что при $n=1$

$$\mathbb{P}\big((\Xi_0,\eta_1)=(\alpha_0,k_1)\big)=\pi^{(0)}_{\alpha_0}p^{(1)}_{k_1}.$$

2. Доказательство абсолютно аналогично доказательству второго пункта Предложения 2.1.1.

3. Схема доказательства совпадает со схемой доказательства Предложения 2.1.3. Сначала докажем единственность эргодического класса.

Из доказательства Предложения 2.1.3 следует такое утверждение об ОМЦ $\{\Xi_i\}_{i\geqslant 1}$: существует $\gamma\in\mathfrak{S}_S$, достижимая из любой другой перестановки $\alpha\in\mathfrak{S}_S$. Выберем такое число $\ell\in\mathbb{S}$, что $p_{\gamma[1]\ell}>0$. Рассмотрим любое $(\alpha,k)\in\mathfrak{S}_S\times\mathbb{S}$, такое что $p_{\alpha[1]k}>0$. Ясно, что из $f(\alpha,k)\in\mathfrak{S}_S$ достижима перестановка $\gamma$. Таким образом, из $(\alpha,k)$ с $p_{\alpha[1]k}>0$ достижимо состояние $(\gamma,\ell)$. Для того, чтобы в этом убедиться, достаточно рассмотреть (2.2.1).

Если же $p_{\alpha[1]k}=0$, то неравенство

$$\mathbb{P}((\Xi_n,\eta_{n+1})=(\alpha,k))>0$$

возможно только при $n=0$. Действительно, при $n>0$

$$\mathbb{P}((\Xi_n,\eta_{n+1})=(\alpha,k))\leqslant p_{\alpha[1]k}=0. \tag{2.2.3}$$

Далее

$$\mathbb{P}\big(\Xi_1=f(\alpha,k)\,|\,(\Xi_0,\eta_1)=(\alpha,k)\big)=1.$$

Следовательно, из любого $(\alpha,k)$ достижимо состояние $(\gamma,\ell)$. Единственность эргодического класса для ОМЦ $\{(\Xi_n,\eta_{n+1})\}_{n\geqslant 0}$ доказана.

Докажем теперь непериодичность единственного эргодического класса ОМЦ $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$. Рассмотрим произвольное существенное состояние $(\alpha, k) \in \mathfrak{S}_S \times \mathbb{S}$. Согласно (2.2.3) $p_{\alpha[1]k} > 0$. Обозначим $\beta = f(\alpha, k)$. Нужно показать, что

$$\gcd\left(n \,\middle|\, p^{(\Xi,\eta)}_{\alpha k \alpha k}(n) > 0\right) = 1.$$

Построим траекторию положительной вероятности ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ из состояния $\alpha$ в себя. Для этого сначала построим две вспомогательные траектории положительной вероятности. Первая из этих траекторий «начинается» из состояния $\beta$ и «заканчивается» в нем же. Траектория задается вектором $X_n = (x_1, x_2, \ldots, x_n) \in \mathfrak{S}_S^n$, таким что $x_1 = x_n = \beta$. Вторая траектория «начинается» из состояния $\beta$ и «заканчивается» в состоянии $\alpha$. Зафиксируем любое такое $\ell \in \mathbb{N}$, что $p^{(\Xi)}_{\beta\alpha}(\ell) > 0$ и рассмотрим следующий вектор, задающий траекторию: $Y_\ell = (y_1, y_2, \ldots, y_\ell) \in \mathfrak{S}_S^\ell$, такой что $y_1 = \beta$ и $y_\ell = \alpha$.

Таким образом, мы имеем траекторию ОМЦ $\{\Xi_n\}_{n\geqslant 1}$ длины $n+\ell$, «начинающуюся» в состоянии $\alpha$ и «заканчивающуюся» в нем же:

$$Z_{n,\ell} = (\alpha, x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{\ell-1}, y_\ell) = (\alpha, \beta, x_2, \ldots, x_{n-1}, \beta, y_2, \ldots, y_{\ell-1}, \alpha) \in \mathbb{S}^{n+\ell}.$$

Обозначим $\overline{n}_\ell = n + \ell$. Конечно, $Z_{n,\ell}$ — траектория положительной вероятности.

Заметим, что траектории $Z_{n,\ell}$ для ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ однозначно соответствует траектория ОМЦ $\{(\Xi_n, \eta_{n+1})\}_{n\geqslant 0}$, состоящая из последовательности состояний

$$\Big[(\alpha, k), (\beta, x_2[1]), (x_2, x_3[1]), \ldots, (x_{n-1}, \beta[1]),$$
$$(\beta, y_2[1]), (y_2, y_3[1]), \ldots, (y_{\ell-1}, \alpha[1]), (\alpha, k)\Big] \in (\mathfrak{S}_S \times \mathbb{S})^{\ell+n}.$$

При этом вероятности всех переходов по такой траектории положительны по (2.2.1).

Аналогично доказательству Предложения 2.1.3 получаем, что

$$\gcd\Big(n + \ell \,\Big|\, p^{(\Xi)}_{\alpha\alpha}(\ell) > 0, n \in \mathbb{N}\Big) = 1.$$

Из этого так же, как и в доказательстве Предложения 2.1.3, заключаем, что

$$\gcd\Big(n + \ell \,\Big|\, p^{(\Xi,\eta)}_{\alpha k \alpha k}(n + \ell) > 0, n \in \mathbb{N}\Big) = 1.$$

Следовательно,

$$\gcd\Big(n \,\Big|\, p^{(\Xi,\eta)}_{\alpha k \alpha k}(n) > 0, n \in \mathbb{N}\Big) = 1.$$

В силу произвольности выбора существенного состояния $(\alpha, k)$ утверждение полностью доказано.

4. Для любых $\alpha \in \mathfrak{S}_S$ и $k \in \mathbb{S}$, используя Предложение 2.1.2 в рамках п.2 и Предложение 2.1.4 в рамках п.3, получаем

$$\mathbb{P}\big((\Xi_n, \eta_{n+1}) = (\alpha, k)\big) = \mathbb{P}(\eta_{n+1} = k \,|\, \Xi_n = \alpha)\mathbb{P}(\Xi_n = \alpha) =$$
$$= \mathbb{P}(\Xi_{n+1} = f(\alpha, k) \,|\, \Xi_n = \alpha)\mathbb{P}(\Xi_n = \alpha) \underset{n\to+\infty}{\to} p_{\mathrm{C}^S_\alpha k}\pi_\alpha.$$

5. В предположении пункта 2 результат является хорошо известным. В предположении пункта 3 результат следует из Теоремы 2.1.1.

Лемма доказана. □

Перейдем к доказательству непосредственно Закона Больших Чисел для частот последовательности $\{\xi_i\}_{i\geqslant 1}$. Для этого обозначим

$$\tau_k = \tau_k(n) = \mathbb{I}_k(\xi_1) + \ldots + \mathbb{I}_k(\xi_n),$$

где $\mathbb{I}_A$ — индикатор множества $A$ и $1 \leqslant k \leqslant S$. Кроме того, положим для любого $1 \leqslant k \leqslant S$

$$s_k \overset{\text{def}}{=} \sum_{j=1}^{S} \sum_{\substack{\alpha\in\mathfrak{S}_S \\ \alpha[k]=j}} \pi_\alpha p_{\mathrm{C}^S_\alpha, j}. \tag{2.2.4}$$

**Теорема 2.2.1.** *Пусть $\eta_n$ и $\Xi_0$ независимы для любого $n \geqslant 1$. Для того, чтобы при $n \to \infty$ для любого $\mathcal{L}(\Xi_0)$ и любого $1 \leqslant k \leqslant S$*

$$\mathbb{P}(\xi_i = k) \to s_k, \tag{2.2.5}$$
$$\frac{\tau_k}{n} \xrightarrow{\mathbb{P}} s_k, \tag{2.2.6}$$

*достаточно выполнения одного из следующих условий:*

1. *$f$ — инъективное по второй компоненте и конечно-связное отображение, а переходные вероятности $p_{ij}$ положительны для всех $i$, $j$;*
2. *$f$ — стандартное «Book Stack»-преобразование, определенное в разделе 1.2, и «входная» последовательность $\{\eta_n\}_{n\geqslant 1}$ — ЭОМЦ.*

*Доказательство.* Доказательство при предположениях обоих пунктов абсолютно одинаково, разница лишь в ссылках на разные пункты Леммы 2.2.1. По первому пункту

Леммы 2.2.1 для предположений обоих пунктов последовательность $\{(\Xi_i, \eta_{i+1})\}_{i\geqslant 0}$ образует ОМЦ. Фазовое пространство — $\mathfrak{S}_S \times \mathbb{S}$, матрица переходных вероятностей — $\mathbf{P}^{(\Xi,\eta)} = \left(p^{(\Xi,\eta)}_{\alpha i \beta j}\right)$, определенная в (2.2.1).

В случае предположений пункта 1 согласно второму пункту Леммы 2.2.1 ОМЦ $\{(\Xi_i, \eta_{i+1})\}_{i\geqslant 0}$ является эргодической. В случае предположений пункта 2 согласно третьему пункту Леммы 2.2.1 ОМЦ $\{(\Xi_i, \eta_{i+1})\}_{i\geqslant 0}$ обладает одним непериодическим эргодическим классом и, быть может, несколькими несущественными состояниями.

По пункту 4 Леммы 2.2.1 для предположений обоих пунктов стационарное распределение $\{(\Xi_i, \eta_{i+1})\}_{i\geqslant 0}$ задается вероятностями $\pi^{(\Xi,\eta)}_{(\alpha,k)} = \pi_\alpha p_{\mathrm{C}^S_\alpha k}$, где $\alpha \in \mathfrak{S}_S$ и $k \in \mathbb{S}$, где множество $\mathrm{C}^S_\alpha$ введено в (1.1.5).

По пункту 5 Леммы 2.2.1 для предположений обоих пунктов имеет место геометрическая скорость сходимость к стационарному распределению, а именно для любых $\alpha, \beta \in \mathfrak{S}_S$ и $i, j \in \mathbb{S}$ верно, что

$$\left|p^{(\Xi,\eta)}_{\alpha i \beta j}(n) - \pi_\alpha p_{\mathrm{C}^S_\alpha i}\right| \leqslant c\rho^n, \tag{2.2.7}$$

где $0 \leqslant \rho < 1$.

Как всегда, из этого следует, что для любого $k \geqslant 1$

$$\left|\mathbb{P}\big((\Xi_k, \eta_{k+1}) = (\alpha, i)\big) - \pi_\alpha p_{\mathrm{C}^S_\alpha i}\right| \leqslant c\rho^k. \tag{2.2.8}$$

Используя (2.2.7) и (2.2.8), оценим сверху величину

$$\left|\mathbb{P}\big((\Xi_i, \eta_{i+1}) = (\alpha, t), (\Xi_j, \eta_{j+1}) = (\beta, r)\big) - \pi_\alpha p_{\mathrm{C}^S_\alpha t}\pi_\beta p_{\mathrm{C}^S_\beta r}\right|$$

для любых $t, r \in \mathfrak{S}_S$ и $1 \leqslant i < j$:

$$\begin{gathered}
\left|\mathbb{P}\big((\Xi_i, \eta_{i+1}) = (\alpha, t), (\Xi_j, \eta_{j+1}) = (\beta, r)\big) - \pi_\alpha p_{\mathrm{C}^S_\alpha t}\pi_\beta p_{\mathrm{C}^S_\beta r}\right| = \\
= \left|\mathbb{P}\big((\Xi_i, \eta_{i+1}) = (\alpha, t)\big)\mathbb{P}\big((\Xi_j, \eta_{j+1}) = (\beta, r) \,|\, (\Xi_i, \eta_{i+1}) = (\alpha, t)\big) - \pi_\alpha p_{\mathrm{C}^S_\alpha t}\pi_\beta p_{\mathrm{C}^S_\beta r}\right| = \\
= \left|\left(\pi_\alpha p_{\mathrm{C}^S_\alpha t} + \mathrm{O}(\rho^i)\right)\left(\pi_\beta p_{\mathrm{C}^S_\beta r} + \mathrm{O}(\rho^{j-i})\right) - \pi_\alpha p_{\mathrm{C}^S_\alpha t}\pi_\beta p_{\mathrm{C}^S_\beta r}\right| = \\
= \begin{cases} \mathrm{O}(\rho^i) & \text{при } 2i \leqslant j, \\ \mathrm{O}(\rho^{j-i}) & \text{при } 2i > j, \end{cases}
\end{gathered} \tag{2.2.9}$$

причем константа, описывающая $\mathrm{O}(\rho^{\cdot})$, не зависит от $i, j$.

Фиксируем $j \in 1 : S$ и тогда для любого $i \geqslant 2$ получаем

$$\mathbb{P}(\xi_i = j) = \sum_{k,\alpha} \mathbb{P}(\xi_i = j \,|\, \eta_i = k, \Xi_{i-1} = \alpha)\mathbb{P}(\eta_i = k, \Xi_{i-1} = \alpha).$$

По определению множества $\mathcal{F}_0$, введенном в (1.1.7),

$$\mathbb{P}\big(\xi_i = j \,\big|\, \eta_i = k, \Xi_{i-1} = \alpha\big) = \begin{cases} 1 & \text{при } \ \alpha \in \mathcal{F}_0(j,k), \\ 0 & \text{иначе.} \end{cases}$$

Таким образом, для фиксированного $j \in 1:S$ и любого $i \geqslant 2$

$$\mathbb{I}_j(\xi_i) = \sum_{k=1}^{S} \sum_{\substack{\alpha \in \mathfrak{S}_S \\ \alpha[j]=k}} \mathbb{I}_{(\alpha,k)}(\Xi_{i-1}, \eta_i).$$

Отсюда, переходя к математическим ожиданиям и учитывая (2.2.8),

$$\begin{aligned} \mathbb{E}\mathbb{I}_j(\xi_i) = \sum_{k,\alpha} \mathbb{E}\mathbb{I}_{(\alpha,k)}(\Xi_{i-1}, \eta_i) = \sum_{k,\alpha} \mathbb{P}(\Xi_{i-1} = \alpha, \eta_i = k) = \\ = \sum_{k,\alpha} \pi_\alpha p_{\mathrm{C}^S_\alpha, k} + \mathrm{O}\left(\rho^{i-1}\right) \underset{i \to +\infty}{\to} s_j. \end{aligned} \tag{2.2.10}$$

Таким образом, справедливость (2.2.5) установлена.

Покажем, что

$$\mathbb{E}(\tau_k/n - s_k)^2 = \frac{1}{n^2}\mathbb{E}\left(\sum_{i=1}^{n}(\mathbb{I}_k(\xi_i) - s_k)\right)^2 \to 0, \tag{2.2.11}$$

откуда с помощью стандартного неравенства Чебышева будет следовать (2.2.6).

Фиксируем произвольное $k \in 1:S$, тогда

$$\begin{aligned} \mathbb{E}\left(\sum_{i=1}^{n}(\mathbb{I}_k(\xi_i) - s_k)\right)^2 = \mathbb{E}\left(\sum_{i=1}^{n}(\mathbb{I}_k(\xi_i) - s_k)\right)\left(\sum_{j=1}^{n}(\mathbb{I}_k(\xi_j) - s_k)\right) = \\ = \sum_{i,j=1}^{n}\left(\mathbb{E}\,\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j) - s_k\mathbb{E}\,\mathbb{I}_k(\xi_j) - s_k\mathbb{E}\,\mathbb{I}_k(\xi_i) + s_k^2\right) = \\ = \sum_{i,j=1}^{n}\left(\mathbb{E}\,\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j) - s_k^2 + \mathrm{O}(\rho^{\min\{i,j\}-1})\right), \end{aligned} \tag{2.2.12}$$

где последнее равенство (а также равенство $\mathbb{E}\mathbb{I}_k^2(\xi_i) = \mathbb{E}\mathbb{I}_k(\xi_i) = s_k + \mathrm{O}(\rho^{i-1})$) следует из (2.2.10).

Заметим, что фактически остается вычислить $\mathbb{E}\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j)$ для $i < j$. Пусть $2i \leqslant j$,

тогда

$$\mathbb{E}\,\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j) = \mathbb{E}\left(\sum_{r=1}^{S}\sum_{\substack{\alpha\in\mathfrak{S}_S\\ \alpha[k]=r}}\mathbb{I}_{(\alpha,r)}(\Xi_{i-1},\eta_i)\right)\left(\sum_{t=1}^{S}\sum_{\substack{\beta\in\mathfrak{S}_S\\ \beta[k]=t}}\mathbb{I}_{(\beta,t)}(\Xi_{j-1},\eta_j)\right) =$$

$$= \sum_{r,t,\alpha,\beta}\mathbb{E}\,\mathbb{I}_{(\alpha,r)}(\Xi_{i-1},\eta_i)\mathbb{I}_{(\beta,t)}(\Xi_{j-1},\eta_j) = \sum_{r,t,\alpha,\beta}\mathbb{P}(\Xi_{i-1}=\alpha,\eta_i=r,\Xi_{j-1}=\beta,\eta_j=t) =$$

$$= \sum_{r,t,\alpha,\beta}\pi_\alpha p_{\mathrm{C}^S_\alpha r}\pi_\beta p_{\mathrm{C}^S_\beta t} + \mathrm{O}(\rho^{i-1}) = s_k^2 + \mathrm{O}(\rho^{i-1}). \tag{2.2.13}$$

В случае $i<j<2i$ в последней приведенной выкладке произойдет замена $\mathrm{O}(\rho^{i-1})$ на $\mathrm{O}(\rho^{j-i})$, что мгновенно следует из (2.2.9).

С помощью только что полученных промежуточных результатов продолжим оценивание (2.2.12):

$$\sum_{i,j=1}^{n}\left(\mathbb{E}\,\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j) - s_k^2\right) =$$

$$= n(s_k - s_k^2) + \sum_{i=1}^{n}\mathrm{O}(\rho^{i-1}) + 2\sum_{2i\leqslant j}\left(\mathrm{O}(\rho^{i-1})\right) + 2\sum_{i<j<2i}\left(\mathrm{O}(\rho^{j-i})\right), \tag{2.2.14}$$

Покажем, асимптотика правой части в (2.2.14) равна $\mathrm{O}(n)$.

$$\left|\sum_{i=1}^{n}\mathrm{O}(\rho^{i-1})\right| \leqslant \rho^{-1}C\sum_{i=1}^{n}\rho^i \leqslant \frac{C}{\rho(1-\rho)} = \mathrm{O}(1). \tag{2.2.15}$$

Из этого мгновенно следует оценка следующего слагаемого:

$$\left|\sum_{2i\leqslant j}\left(\mathrm{O}(\rho^{i-1})\right)\right| \leqslant \rho^{-1}C\sum_{2i\leqslant j}\rho^i = \rho^{-1}C\sum_{j=2}^{n}\sum_{i=1}^{\lfloor j/2\rfloor}\rho^i \leqslant \frac{nC}{\rho(1-\rho)} = \mathrm{O}(n).$$

Осталось разобраться с последним слагаемым в (2.2.14).

$$\left|\sum_{i<j<2i}\left(\mathrm{O}(\rho^{j-i})\right)\right| \leqslant \left|\sum_{i<j}\mathrm{O}(\rho^{j-i})\right| \leq C\sum_{i<j}\rho^{j-i} = C\sum_{j=2}^{n}\sum_{i=1}^{j-1}\rho^{j-i} = C\sum_{j=2}^{n}\sum_{i=1}^{j-1}\rho^i =$$

$$= C\rho\left(\frac{\rho^n-1}{(1-\rho)^2} + n\frac{1}{1-\rho}\right) = \mathrm{O}(n).$$

Это означает, что (2.2.14) перепишется в виде: $\sum_{i,j=1}^{n}\left(\mathbb{E}\,\mathbb{I}_k(\xi_i)\mathbb{I}_k(\xi_j) - s_k^2\right) = \mathrm{O}(n)$. Применяя последнее равенство к (2.2.12) заключаем, что $\mathbb{E}(\tau_k/n - s_k)^2 = \mathrm{O}(n^{-1}) \to 0$. Ссылка на стандартное неравенство Чебышева завершает доказательство теоремы. $\square$

## 2.3. Центральные Предельные Теоремы для частот входной и выходной последовательностей

Как и раньше, предполагаем, что входная последовательность $\{\eta_i\}_{i\geqslant 1}$ образует ОМЦ с матрицей переходных вероятностей $\mathbf{P}^{(\eta)} = (p_{ij})$. Мы предполагаем также, что вектор $\Xi_0$ и ОМЦ $\{\eta_i\}_{i\geqslant 1}$ независимы.

В разделе 2.1 были сформулированы условия, обеспечивающие существование и единственность стационарного распределения ОМЦ $\{\Xi_n\}_{n\geqslant 1}$, введеной в (1.1.1). В предыдущем разделе исследовались свойства сходимости по вероятности частот «входной» и «выходной» последовательности к соответствующим предельным распределениям в рамках рассматриваемых предположений. Для «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$ такая сходимость является хорошо известной (см., например, [22]), а для «выходной» последовательности $\{\xi_i\}_{i\geqslant 1}$, введенной в (1.1.2), была показана в Теореме 2.2.1. В этом разделе показано, что можно доказать не только ЗБЧ, но и ЦПТ для частот обеих последовательностей.

Рассмотрим отображение $f : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$ и до конца этого раздела предположим, что выполнено одно из следующих условий:

1. $f$ — инъективное по второй компоненте и конечно-связное отображение, а переходные вероятности $p_{ij}$ положительны для всех $i$, $j$;

2. $f$ — стандартное «Book Stack»-преобразование, определенное в разделе 1.2, и «входная» ОМЦ $\{\eta_n\}_{n\geqslant 1}$ — эргодическая.

Обозначим $\mathbf{p}^{(\infty)} = \left(p_1^{(\infty)}, p_2^{(\infty)}, \ldots, p_S^{(\infty)}\right)^{\mathrm{T}}$ — стационарное распределение последовательности $\{\eta_n\}_{n\geqslant 1}$.

Для векторов частот «входной» и «выходной» последовательности мы будем использовать обозначения

$$\tau_n^{(\eta)} = \left(\tau_{1,n}^{(\eta)}, \ldots \tau_{S,n}^{(\eta)}\right)^{\mathrm{T}}, \quad \tau_n^{(\xi)} = \left(\tau_{1,n}^{(\xi)}, \ldots \tau_{S,n}^{(\xi)}\right)^{\mathrm{T}} \tag{2.3.1}$$

для любого $n \geqslant 1$, где для каждого $k \in 1 : S$

$$\tau_{k,n}^{(\eta)} = \sum_{i=1}^{n} \mathbb{I}(\eta_i = k), \quad \tau_{k,n}^{(\xi)} = \sum_{i=1}^{n} \mathbb{I}(\xi_i = k).$$

Прежде всего нам потребуется многомерная ЦПТ для марковских цепей с произвольным пространством состояний и дискретным временем. Доказательство этой теоремы приведено в [23, Глава 3, §2].

**Теорема 2.3.1.** *Пусть $X$ — некоторое множество, а $F_X$ — $\sigma$-алгебра его подмножеств. Рассмотрим $\zeta_1, \zeta_2, \ldots, \zeta_n, \ldots$ — ОМЦ с множеством состояний $X$ и переходной функцией $p : X \times F_X$. Для любого $n > 0$ обозначим $p^{(n)}$ — переходную функцию за $n$ шагов. Предположим, что существует $k_0 > 0$*

$$\sup_{\substack{x_1,x_2\in X\\ A\in F_X}} \left|p^{(k_0)}(x_1, A) - p^{(k_0)}(x_2, A)\right| < 1. \tag{2.3.2}$$

*Обозначим $\pi$ — стационарное распределение ОМЦ $\{\zeta_i\}_{i\geqslant 1}$. Рассмотрим $d$-мерное отображение $h : X \to \mathbb{R}^d$, $h = (h_1, h_2, \ldots, h_d)^{\mathrm{T}}$, предполагая, что все координатные функции $h_i$ — $F_X$-измеримы. Тогда при $n \to \infty$ имеет место следующая сходимость:*

$$\mathcal{L}\left(\sqrt{n}\left(\frac{1}{n}\sum_{i=1}^{n} h(\zeta_i) - \mathbb{E}_\pi h(\zeta_1)\right)\right) \Rightarrow \mathcal{N}(\mathbf{0}, \Sigma_\zeta), \tag{2.3.3}$$

*где $\Sigma_\zeta$ — матрица размеров $d \times d$ со следующими компонентами для всех $1 \leqslant i, j \leqslant d$*

$$\begin{gathered}
\left(\Sigma_\zeta\right)_{ij} = \\
= \mathbb{E}_\pi\Big[\big(h_i(\zeta_1) - \mathbb{E}_\pi h_i(\zeta_1)\big)\big(h_j(\zeta_1) - \mathbb{E}_\pi h_j(\zeta_1)\big)\Big] + \\
+ \sum_{r=1}^{\infty} \mathbb{E}_\pi\Big[\big(h_i(\zeta_1) - \mathbb{E}_\pi h_i(\zeta_1)\big)\big(h_j(\zeta_{r+1}) - \mathbb{E}_\pi h_j(\zeta_{r+1})\big)\Big] + \\
+ \sum_{r=1}^{\infty} \mathbb{E}_\pi\Big[\big(h_j(\zeta_1) - \mathbb{E}_\pi h_j(\zeta_1)\big)\big(h_i(\zeta_{r+1}) - \mathbb{E}_\pi h_i(\zeta_{r+1})\big)\Big].
\end{gathered} \tag{2.3.4}$$

**Следствие 2.3.1.** Пусть $\zeta_1, \zeta_2, \ldots, \zeta_n, \ldots$ — ОМЦ с конечным пространством состояний. Тогда для выполнения ЦПТ 2.3.1 достаточно, чтобы $\{\zeta_i\}_{i\geqslant 1}$ обладала одним непериодическим эргодическим классом и, может быть, несколькими несущественными состояниями. В частности, достаточно, чтобы $\{\zeta_i\}_{i\geqslant 1}$ была эргодической.

Перейдем к формулировке и доказательству ЦПТ для частот «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$. Введем вспомогательные обозначения:

$$a_{k,\ell}^{(\eta)} = \begin{cases} p_k^{(\infty)}\left(1 - p_k^{(\infty)}\right) & \text{при } \ k = \ell, \\ -p_k^{(\infty)} p_\ell^{(\infty)} & \text{при } \ k \neq \ell. \end{cases} \tag{2.3.5}$$

$$b_{k,\ell}^{(\eta)} = \sum_{r=1}^{\infty}\left(p_{k,\ell}(r) - p_\ell^{(\infty)}\right) p_k^{(\infty)}. \tag{2.3.6}$$

для всех $k, \ell \in \mathbb{S}$.

**Лемма 2.3.1.** *Величины $b_{k,\ell}^{(\eta)}$ конечны для всех $k, \ell \in \mathbb{S}$. Более того, верна следующая равномерная оценка:*

$$|b_{k,\ell}^{(\eta)}| \leqslant \frac{C_\eta \rho_\eta}{1-\rho_\eta}, \tag{2.3.7}$$

*где $C_\eta, \rho_\eta$ зависят только от переходных вероятностей $\{p_{ij}\}$ и $C_\eta > 0$ и $\rho_\eta \in [0;1)$.*

*Доказательство.* Так как $\{\eta_i\}_{i\geqslant 1}$ образует ЭОМЦ, то существуют такие $C_\eta > 0$ и $\rho_\eta \in [0;1)$, что

$$\left| p_{k,\ell}(r) - p_\ell^{(\infty)} \right| \leqslant C_\eta \rho_\eta^r.$$

Ссылка на формулу суммы геометрической прогрессии завершает доказательство. □

**Теорема 2.3.2.** *Для векторов $\tau_n^{(\eta)}$, определенных в (2.3.1), имеет место следующая асимптотическая сходимость*

$$\mathcal{L}\Big(\sqrt{n}\big(\tau_n^{(\eta)}/n - \mathbf{p}^{(\infty)}\big)\Big) \Rightarrow \mathcal{N}\left(0, \Sigma_\eta\right), \tag{2.3.8}$$

*где матрица $\Sigma_\eta$ размеров $S \times S$ и имеет компоненты*

$$(\Sigma_\eta)_{k,\ell} = a_{k,\ell}^{(\eta)} + b_{k,\ell}^{(\eta)} + b_{\ell,k}^{(\eta)}. \tag{2.3.9}$$

*Более того, равномерно по всем $k, \ell \in \mathbb{S}$ справедлива следующая оценка:*

$$a_{k,\ell}^{(\eta)} - \frac{2C_\eta\rho_\eta}{1-\rho_\eta} \leqslant (\Sigma_\eta)_{k,\ell} \leqslant a_{k,\ell}^{(\eta)} + \frac{2C_\eta\rho_\eta}{1-\rho_\eta}. \tag{2.3.10}$$

*для некоторых констант $\rho_\eta \in [0;1)$ и $C_\eta > 0$, зависящих только от переходных вероятностей $\{p_{ij}\}$.*

*Доказательство.* Для доказательства воспользуемся Теоремой 2.3.1. Вычисления всех математических ожиданий происходят, как это требуется в Теореме 2.3.1, в предположении, что ОМЦ $\{\eta_n\}_{n\geqslant 1}$ является стационарной. Сначала докажем наличие сходимости (2.3.8). Рассмотрим такое $h : \mathbb{S} \to \mathbb{R}^S$, что $h(k) = e_k$ для любого $k \in \mathbb{S}$, где $e_k$ — $k$-й единичный орт. Тогда сходимость (2.3.8) следует из ЦПТ 2.3.1 с выбором такого $h$. Действительно, $\sum_{i=1}^n h(\eta_i) = \tau_n^{(\eta)}$, а $\mathbb{E}h(\eta_i) = \mathbf{p}^{(\infty)}$.

Осталось вычислить компоненты ковариационной матрицы $\Sigma_\eta$ по формулам (2.3.4). Заметим, что $h_k(\eta_i) = \mathbb{I}_k(\eta_i)$ и, следовательно, $\mathbb{E}h_k(\eta_i) = s_k$ для каждого $k \in \mathbb{S}$ и любого $i \geqslant 1$. Начнем с первого слагаемого. Ясно, что для любых $k, \ell \in \mathbb{S}$

$$\mathbb{E}\Big[\left(\mathbb{I}_k(\eta_1) - p_k^{(\infty)}\right)\left(\mathbb{I}_\ell(\eta_1) - p_\ell^{(\infty)}\right)\Big] = a_{k,\ell}^{(\eta)}, \tag{2.3.11}$$

где $a^{(\eta)}_{k,\ell}$ введено в (2.3.5).

Далее для любого $r \geqslant 1$ и любых $k, \ell \in \mathbb{S}$:

$$\mathbb{E}h_k(\eta_1)h_\ell(\eta_{r+1}) = \mathbb{P}(\eta_1 = k)\mathbb{P}(\eta_{r+1} = \ell \,|\, \eta_1 = k) =$$
$$= p_k^{(\infty)} \left( p_\ell^{(\infty)} + p_{k,\ell}(r) - p_\ell^{(\infty)} \right) = p_k^{(\infty)} p_\ell^{(\infty)} + \left( p_{k,\ell}(r) - p_\ell^{(\infty)} \right) p_k^{(\infty)}.$$

Следовательно,

$$\sum_{r=1}^{\infty} \mathbb{E}\Big[ \left( h_k(\eta_1) - p_k^{(\infty)} \right) \left( h_\ell(\eta_{r+1}) - p_\ell^{(\infty)} \right) \Big] = b^{(\eta)}_{k,\ell}.$$

Оценка (2.3.10) следует из Леммы 2.3.1. □

Перейдем к доказательству ЦПТ для частот «выходной» последовательности $\{\xi_i\}_{i\geqslant 1}$. Стационарное распределение ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ обозначим $(\pi_\alpha)_{\alpha\in\mathfrak{S}_S}$. Для любых $k, \ell \in \mathbb{S}$ введем обозначения:

$$a^{(\xi)}_{k,\ell} = \begin{cases} s_k(1 - s_k), & \text{при} \quad k = \ell, \\ -s_k s_\ell, & \text{при} \quad k \neq \ell. \end{cases} \tag{2.3.12}$$

$$b^{(\xi)}_{k,\ell} = \sum_{r=1}^{\infty} \sum_{q,t\in\mathbb{S}} \sum_{\substack{\alpha,\beta\in\mathfrak{S}_S \\ \alpha_k = t \\ \beta_\ell = q}} \pi_\alpha p_{\mathrm{C}^S_\alpha, t} \left( p^{(\Xi,\eta)}_{\alpha t \beta q}(r) - \pi_\beta p_{\mathrm{C}^S_\beta, q} \right), \tag{2.3.13}$$

где $p^{(\Xi,\eta)}_{\alpha t\beta q}$ введено в (2.2.1), $\mathrm{C}^S_\alpha$ — в (1.1.5) а $s_k$ — в (2.2.4).

**Лемма 2.3.2.** *Пусть выполнены условия пункта 2 или 3 Леммы 2.2.1. Введенные величины $b^{(\xi)}_{k,\ell}$ конечны для всех $k, \ell \in \mathbb{S}$ и, более того, верна следующая равномерная на $k, \ell \in \mathbb{S}$ оценка:*

$$|b^{(\xi)}_{k,\ell}| \leqslant \frac{C_{\Xi,\eta}\rho_{\Xi,\eta} S!}{1 - \rho_{\Xi,\eta}} \tag{2.3.14}$$

*для некоторых констант $C_{\Xi,\eta}, \rho_{\Xi,\eta} \geqslant 0$, $\rho_{\Xi,\eta} < 1$ и $C_{\Xi,\eta} \leqslant 1$, зависящих только от переходных вероятностей $\{p_{ij}\}$.*

*Доказательство.* Доказательство аналогично Лемме 2.3.1. Действительно, достаточно сослаться на пункт 5 Леммы 2.2.1. □

Обозначим $\mathbf{s} = (s_1, \ldots, s_S)^{\mathrm{T}}$ — вектор предельных вероятностей для «выходной» последовательности $\{\xi_i\}_{i\geqslant 1}$.

**Теорема 2.3.3.** *Имеет место следующая асимптотическая сходимость*

$$\mathcal{L}\left(\sqrt{n}\left(\tau_n^{(\xi)}/n - \mathbf{s}\right)\right) \Rightarrow \mathcal{N}\left(0, \Sigma_\xi\right), \tag{2.3.15}$$

*где матрица* $\Sigma_\xi$ *размеров* $S \times S$ *имеет компоненты*

$$\left(\Sigma_\xi\right)_{k,\ell} = a_{k,\ell}^{(\xi)} + b_{k,\ell}^{(\xi)} + b_{\ell,k}^{(\xi)}, \tag{2.3.16}$$

*а* $s_k$ *для всех* $k \in \mathbb{S}$ *введены в* (2.2.4). *При этом равномерно по всем* $k, \ell \in \mathbb{S}$ *верна следующая оценка:*

$$a_{k,\ell}^{(\xi)} - \frac{2C_{\Xi,\eta}\rho_{\Xi,\eta}S!}{1-\rho_{\Xi,\eta}} \leqslant \left(\Sigma_\xi\right)_{k,\ell} \leqslant a_{k,\ell}^{(\xi)} + \frac{2C_{\Xi,\eta}\rho_{\Xi,\eta}S!}{1-\rho_{\Xi,\eta}} \tag{2.3.17}$$

*для некоторых констант* $\rho_{\Xi,\eta} \geqslant 0$, $\rho_{\Xi,\eta} < 1$ *и* $C_{\Xi,\eta} > 0$, *зависящих только от переходных вероятностей* $\{p_{ij}\}$.

*Доказательство.* Докажем сначала наличие сходимости (2.3.15). Для этого воспользуемся Теоремой 2.3.1. Заметим, что в рассматриваемых предположениях по Лемме 2.2.1 последовательность $\{\Xi_i, \eta_{i+1}\}_{i\geqslant 0}$ образует ОМЦ с единственным стационарным распределением. Вычисления всех математических ожиданий происходят, как это требуется в Теореме 2.3.1, в предположении, что ОМЦ $\left\{(\Xi_n, \eta_{n+1})^{\mathrm{T}}\right\}_{n\geqslant 0}$ является стационарной. Рассмотрим такое $g_1 : \mathfrak{S}_S \times \mathbb{S} \to \mathfrak{S}_S$, что $g_1(\alpha, k)$ есть решение уравнения $\alpha[g_1(\alpha, k)] = k$ для всех $\alpha \in \mathfrak{S}_S$ и $k \in \mathbb{S}$. Рассмотрим также такое $g_2 : \mathbb{S} \to \mathbb{R}^S$, что $g_2(k) = e_k$ для любого $k \in \mathbb{S}$, где $e_k$ — $k$-тый единичный орт. Положим такое $h : \mathfrak{S}_S \times \mathbb{S} \to \mathbb{R}^s$, что $h = (h_1, \ldots h_S)^{\mathrm{T}} = g_2 \circ g_1$. Тогда сходимость (2.3.15) следует из ЦПТ 2.3.1 с выбором $h$. Действительно, $\sum_{i=1}^n h(\Xi_{i-1}, \eta_i) = \tau_n^{(\xi)}$, а $\mathbb{E}h(\Xi_0, \eta_1) = \mathbb{E}g_2(\xi_1) = \mathbf{s}$.

Осталось вычислить компоненты ковариационной матрицы $\Sigma_\xi$ по формулам (2.3.4). Заметим, что $h_k(\Xi_{i-1}, \eta_i) = \mathbb{I}_k(\xi_i)$ и, следовательно, $\mathbb{E}h_k(\Xi_{i-1}, \eta_i) = s_k$ для каждого $k \in \mathbb{S}$ и любого $i \geqslant 1$. Начнем с первого слагаемого. Ясно, что для любых $k, \ell \in \mathbb{S}$

$$\mathbb{E}\Big[\big(\mathbb{I}_k(\xi_1) - s_k\big)\big(\mathbb{I}_\ell(\xi_1) - s_\ell\big)\Big] = a_{k,\ell}^{(\xi)}, \tag{2.3.18}$$

где $a_{k,\ell}^{(\xi)}$ введено в (2.3.12).

Для вычисления второго и третьего слагаемого в правой части (2.3.16) требуется

дополнительная подготовка. Для любых $k, \ell \in \mathbb{S}$ и всех $r \geqslant 1$

$$\mathbb{E}\mathbb{I}_k(\xi_1)\mathbb{I}_\ell(\xi_{r+1}) = \mathbb{E}\left(\sum_{t=1}^{S}\mathbb{I}_t(\eta_1)\sum_{\substack{\alpha\in\mathfrak{S}_S\\ \alpha_k=t}}\mathbb{I}_\alpha(\Xi_0)\right)\left(\sum_{q=1}^{S}\mathbb{I}_q(\eta_{r+1})\sum_{\substack{\beta\in\mathfrak{S}_S\\ \beta_\ell=q}}\mathbb{I}_\alpha(\Xi_r)\right) =$$

$$= \sum_{q,t,\alpha,\beta}\mathbb{E}\mathbb{I}_t(\eta_1)\mathbb{I}_\alpha(\Xi_0)\mathbb{I}_q(\eta_{r+1})\mathbb{I}_\beta(\Xi_r) =$$

$$= \sum_{q,t,\alpha,\beta}\mathbb{P}(\eta_{r+1}=q, \Xi_r=\beta, \eta_1=t, \Xi_0=\alpha) =$$

$$= \sum_{q,t,\alpha,\beta}\mathbb{P}(\eta_{r+1}=q, \Xi_r=\beta \,|\, \eta_1=t, \Xi_0=\alpha)\mathbb{P}(\eta_1=t, \Xi_0=\alpha) =$$

$$= \sum_{q,t,\alpha,\beta}\left[\pi_\beta p_{\mathrm{C}^S_\beta q} + p^{(\Xi,\eta)}_{(\alpha t\beta q)}(r) - \pi_\beta p_{\mathrm{C}^S_\beta q}\right]\pi_\alpha p_{\mathrm{C}^S_\alpha t} =$$

$$= s_k s_\ell + \sum_{q,t,\alpha,\beta}\left[p^{(\Xi,\eta)}_{(\alpha t\beta q)}(r) - \pi_\beta p_{\mathrm{C}^S_\beta q}\right]\pi_\alpha p_{\mathrm{C}^S_\alpha t}.$$

Следовательно, для любых $k, \ell \in \mathbb{S}$

$$\sum_{r=1}^{\infty}\mathbb{E}\Big[\big(\mathbb{I}_k(\xi_1) - s_k\big)\big(\mathbb{I}_\ell(\xi_{r+1}) - s_\ell\big)\Big] = b^{(\xi)}_{k,\ell}. \tag{2.3.19}$$

Заметим, что из (2.3.18) и (2.3.19) следует (2.3.16). Оценка (2.3.17) следует из Леммы 2.3.2. □

Таким образом, установлены ЦПТ для частот «входной» и «выходной» последовательностей. Эти ЦПТ можно использовать для доказательства ЦПТ для статистик критериев, вычисляемых по частотам. Сделаем это для статистики критерия $\chi^2$ для проверки гипотезы $\mathbb{H}_0$ (см. Введениие).

Обозначим

$$\rho_2^2(\eta) = \sum_{k=1}^{S}\Big(p_k^{(\infty)} - 1/S\Big)^2, \quad \rho_2^2(\xi) = \sum_{k=1}^{S}(s_k - 1/S)^2, \tag{2.3.20}$$

где $s_k$ для всех $k \in \mathbb{S}$ введены в (2.2.4). Введем статистики критерия $\chi^2$ для «входной» и «выходной» последовательности:

$$\chi_n^2(\eta) = \sum_{k=1}^{S}\frac{\Big(\tau^{(\eta)}_{k,n} - n/S\Big)^2}{n/S}, \quad \chi_n^2(\xi) = \sum_{k=1}^{S}\frac{\Big(\tau^{(\xi)}_{k,n} - n/S\Big)^2}{n/S}. \tag{2.3.21}$$

Ясно, что при $n \to \infty$

$$\frac{\chi_n^2(\eta)}{Sn} \xrightarrow{\mathbb{P}} \rho_2^2(\eta).$$

Из Теоремы 2.2.1 следует, что при $n \to \infty$

$$\frac{\chi_n^2(\xi)}{Sn} \xrightarrow{\mathbb{P}} \rho_2^2(\xi).$$

Обозначим

$$\sigma_\eta^2 = 4\sum_{k=1}^{S} p_k^{(\infty)}\left(p_k^{(\infty)} - 1/S\right)^2 - \left(\sum_{k=1}^{S} p_k^{(\infty)}\left(p_k^{(\infty)} - 1/S\right)\right)^2 + \\ + \sum_{k,\ell\in\mathbb{S}}\left(b_{k\ell}^{(\eta)} + b_{\ell k}^{(\eta)}\right)\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right) \tag{2.3.22}$$

и

$$\sigma_\xi^2 = 4\sum_{k=1}^{S} s_k(s_k - 1/S)^2 - \left(\sum_{k=1}^{S} s_k(s_k - 1/S)\right)^2 + \\ + \sum_{k,\ell\in\mathbb{S}}\left(b_{k\ell}^{(\xi)} + b_{\ell k}^{(\xi)}\right)(s_k - 1/S)(s_\ell - 1/S), \tag{2.3.23}$$

где для всех $k \in \mathbb{S}$ величины $s_k$ введены в (2.2.4), $a_k^{(\eta)}$ — в (2.3.5), $b_k^{(\eta)}$ — в (2.3.6), $a_k^{(\xi)}$ — в (2.3.12), $b_k^{(\xi)}$ — в (2.3.13).

**Теорема 2.3.4.** *Имеют место следующие сходимости при* $n \to \infty$

$$\mathcal{L}\left(\sqrt{n}\left(\frac{\chi_n^2(\eta)}{Sn} - \rho_2^2(\eta)\right)\right) \Rightarrow \mathcal{N}\left(0, \sigma_\eta^2\right), \quad \mathcal{L}\left(\sqrt{n}\left(\frac{\chi_n^2(\xi)}{Sn} - \rho_2^2(\xi)\right)\right) \Rightarrow \mathcal{N}\left(0, \sigma_\xi^2\right),$$

*где* $\chi_n^2(\eta)$ *и* $\chi_n^2(\xi)$ *определены в* (2.3.21), $\rho_2^2(\eta)$ *и* $\rho_2^2(\xi)$ *— в* (2.3.20), $\sigma_\eta^2$ *— в* (2.3.22) *и* $\sigma_\xi^2$ *— в* (2.3.23).

*Доказательство.* Докажем ЦПТ для $\chi_n^2(\eta)$ и вычислим предельную дисперсию $\sigma_\eta^2$. Доказательство для $\chi_n^2(\xi)$ и вычисление $\sigma_\xi^2$ аналогичны. Рассмотрим отображение $g : \mathbb{R}^S \to \mathbb{R}$ такое, что

$$g(x_1, \ldots, x_S) = \sum_{k=1}^{S}(x_k - 1/S)^2. \tag{2.3.24}$$

Очевидно, отображение $g$ является дифференцируемым в любой точке, причем

$$g(\mathbf{p}) = \rho_2^2(\eta), \quad g\left(\frac{\tau_n^{(\eta)}}{n}\right) = \frac{\chi_n^2(\eta)}{Sn}.$$

По теореме о сохранении асимптотической нормальности при гладком отображении из сходимости в Теореме 2.3.2 следует следующая сходимость

$$\mathcal{L}\left(\sqrt{n}\left(\frac{\chi_n^2(\eta)}{Sn} - \rho_2^2(\eta)\right)\right) \Rightarrow \mathcal{N}\left(0, \nabla_g^{\mathrm{T}}\left(\mathbf{p}^{(\infty)}\right)\Sigma_\eta \nabla_g\left(\mathbf{p}^{(\infty)}\right)\right).$$

Осталось вычислить асимптотическую дисперсию. Ясно, что $g'_{x_k} = 2(x_k - 1/S)$ для любого $k \in \mathbb{S}$.

$$\nabla_g^{\mathrm{T}}(\mathbf{s})\Sigma_\eta \nabla_g(\mathbf{s}) = 4\sum_{k,\ell}(\Sigma_\eta)_{k,\ell}\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right).$$

По (2.3.9) для всех $k, \ell \in \mathbb{S}$

$$(\Sigma_\eta)_{k,\ell} = a_{k,\ell}^{(\eta)} + b_{k,\ell}^{(\eta)} + b_{\ell,k}^{(\eta)}.$$

Отдельно рассмотрим две суммы:

$$\sum_{k,\ell} a_{k,\ell}^{(\eta)}\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right), \quad \sum_{k,\ell}\left(b_{k,\ell}^{(\eta)} + b_{\ell,k}^{(\eta)}\right)\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right).$$

Вторая из этих сумм не поддается упрощению, поэтому сосредоточим внимание на первой сумме.

$$\begin{aligned}
&\sum_{k,\ell} a_{k,\ell}^{(\eta)}\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right) = \\
&= \sum_{k=1}^{S} p_k^{(\infty)}\left(1 - p_k^{(\infty)}\right)\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right) - \\
&\quad - \sum_{k\neq\ell} p_k^{(\infty)} p_\ell^{(\infty)}\left(p_k^{(\infty)} - 1/S\right)\left(p_\ell^{(\infty)} - 1/S\right) = \\
&= \sum_{k=1}^{S} p_k^{(\infty)}\left(p_k^{(\infty)} - 1/S\right)^2 - \left(\sum_{k=1}^{S} p_k^{(\infty)}\left(p_k^{(\infty)} - 1/S\right)\right)^2.
\end{aligned}$$

Утверждение доказано. □

Аналогично можно получить ЦПТ и для статистик других критериев.

## 2.4. Сравнение предельных распределений входной и выходной последовательностей

Цель данного раздела заключается в сравнении при различных предположениях предельных распределений «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$ и «выходной» — $\{\xi_i\}_{i\geqslant 1}$, введенной в (1.1.2). Предельные распределения «входной» и «выходной» последовательностей будем обозначать $\mathcal{P}$ и $\mathcal{R}$ соответственно. Мы предполагаем, что вектор $\Xi_0$ и «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ независимы.

Сравнение распределений для произвольных «Book Stack»-подобных преобразований представляется достаточно затруднительным, поэтому мы сосредоточимся на стандартном «Book Stack»-преобразовании, введенном в разделе 1.2.

Во Введении обсуждалась корректность «Book Stack»-теста, а также сравнение предельных распределений «входной» и «выходной» последовательностей, в случае если последовательность $\{\eta_i\}_{i\geqslant 1}$ является набором независимых и одинаково, но не равномерно распределенных на $\mathbb{S}$ случайных величин.

Возникает естественный вопрос о сравнении предельных распределений в случае, если «входная» последовательность образует ЭОМЦ. Мы будем рассматривать частный случай, когда «входная» последовательность образует ЭОМЦ со стационарным равномерным распределением. Матрица переходных вероятностей ЭОМЦ $\{\eta_i\}_{i\geqslant 1}$ обозначается $\mathbf{P}^{(\eta)}$.

**Теорема 2.4.1.** *Пусть «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ — ЭОМЦ с $\mathcal{P} = \mathrm{U}_S$. Тогда предельная вероятность $s_1$, введенная в (2.2.4), имеет вид*

$$s_1 = \mathrm{tr}\left(\mathbf{P}^{(\eta)}\right)/S.$$

*Доказательство.* Так как $f$ — стандартное «Book Stack»-преобразование, то $\alpha_1$ — единственный элемент множества $\mathrm{C}_\alpha^S$, введенного в (1.1.5), для всех перестановок $\alpha \in \mathfrak{S}_S$. Поэтому

$$s_1 = \sum_{r=1}^{S}\sum_{\alpha_1=r}\pi_\alpha p_{\alpha_1 r} = \sum_{r=1}^{S}\sum_{\alpha_1=r}\pi_\alpha p_{rr} = \\ = \sum_{r=1}^{S} p_{rr}\sum_{\alpha_1=r}\pi_\alpha.$$

Заметим, что для любого $i \geqslant 1$ в стационарной ситуации, т.е. если $\mathcal{L}(\eta_i) = \mathcal{P} = \mathrm{U}_S$ и $\mathcal{L}(\Xi_0)$ совпадает со стационарным распределением ОМЦ $\{\Xi_i\}_{i\geqslant 1}$,

$$1/S = \mathbb{P}(\eta_i = r) = \sum_{\substack{\alpha\in\mathfrak{S}_S\\ \alpha_1=r}}\mathbb{P}(\Xi_i = \alpha) = \sum_{\alpha_1=r}\pi_\alpha.$$

Следовательно, $s_1 = \mathrm{tr}\left(\mathbf{P}^{(\eta)}\right)/S$. □

**Следствие 2.4.1.** Если $\mathrm{tr}\left(\mathbf{P}^{(\eta)}\right) \neq 1$, то $\mathcal{R} \neq \mathrm{U}_S$.

Обсудим полученный результат. Нам понадобится одно элементарное утверждение.

**Лемма 2.4.1.** *Стационарное распределение $\mu$ некоторой ОМЦ с конечным фазовым пространством является равномерным тогда и только тогда, когда ее матрица переходных вероятностей $\mathbf{P}$ является бистохастической.*

*Доказательство.* Утверждение очевидно, так как стационарное распределение ЭОМЦ является решением линейной системы $\mu\mathbf{P} = \mu$. □

**Пример 2.4.1.** Зафиксируем число $\delta \in (0,1)$ и положим $p_{ii} = \delta \in (0,1)$ для всех $i \in 1 : S$, а остальные $p_{ij} = (1-\delta)/(S-1)$. Согласно Теореме 2.4.1 $\mathcal{R} \neq \mathrm{U}_S$ при $\delta \neq 1/S$. Однако, в этом Примере результат можно уточнить. Так как матрица $\mathbf{P}^{(\eta)}$ является бистохастической, стационарное распределение ОМЦ является равномерным на множестве $\mathbb{S}$ при любом (фиксированном) $\delta$. Заметим, что в таком случае матрица $\mathbf{P}^{(\Xi)}$, определенная в (2.1.2), тоже является бистохастической. Действительно, в каждом ее столбце ровно $S$ ненулевых элементов, среди которых один равен $\delta$, а остальные по $(1-\delta)/(S-1)$. Следовательно, по Лемме 2.4.1 стационарное распределение ОМЦ $\{\Xi_i\}_{i\geqslant 1}$ является равномерным на множестве $\mathfrak{S}_S$. Далее легко проверить, что формула (2.2.4) принимает вид

$$s_j = \mathbb{P}(\xi_i = j) = \begin{cases} \delta & \text{при } j = 1, \\ (1-\delta)/(S-1) & \text{иначе.} \end{cases} \tag{2.4.1}$$

**Пример 2.4.2.** Приведем пример, демонстрирующий, что условие $s_1 = 1/S$ не влечет равенство $\mathcal{R} = \mathrm{U}_S$. Пусть $S = 3$ и

$$\mathbf{P}^{(\eta)} = \frac{1}{15}\begin{pmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{pmatrix}.$$

Так как матрица бистохастическая, то по Лемме 2.4.1 $\mathcal{P} = \mathrm{U}_S$. По Теореме 2.4.1 $s_1 = 1/S$. Однако, непосредственным вычислением можно показать, что $s_2 \neq 1/S$.

**Пример 2.4.3.** Покажем, что существует такая бистохастическая матрица $\mathbf{P}^{(\eta)}$, не все компоненты которой равны $1/S$, что ОМЦ $\{\eta_i\}_{i\geqslant 1}$ — эргодическая и $\mathcal{P} = \mathcal{R} = \mathrm{U}_S$. Возьмем $S = 3$ и

$$\mathbf{P}^{(\eta)} = \frac{1}{6}\begin{pmatrix} 4 & 0 & 2 \\ 2 & 1 & 3 \\ 0 & 5 & 1 \end{pmatrix}.$$

Так же, как и в предыдущем примере, $\mathcal{P} = \mathrm{U}_S$, а также $s_1 = 1/S$. На самом деле непосредственным вычислением можно показать, что и $s_2 = 1/S$.

Таким образом, для «входных» ЭОМЦ с матрицей переходных вероятностей, след которой не равен 1, и стационарным равномерным распределением предельное распределение «выходной» последовательности не является равномерным. Однако, если след соответствующей матрицы равен 1, неравномерность предельного распределения «выходной» последовательности не является обязательной. Эти соображения позволяют в следующем разделе исследовать статистические свойства теста «Book Stack».

## 2.5. Статистические приложения

Во Введении было дано формальное описание «Book Stack»-теста. Напомним, что проверяется гипотеза $\mathbb{H}_0$, заключающаяся в том, что «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является последовательностью независимых случайных величин с равномерным на $\mathbb{S}$ распределением. Проверка осуществляется с помощью стандартного критерия $\chi^2$. Суть теста состоит в том, что критерий $\chi^2$ применяется не к исходным случайным величинам $\{\eta_i\}_{i\geqslant 1}$, а к преобразованным $\{\xi_i\}_{i\geqslant 1}$ с той же степенью свободы.

В [20] и [21] исследовалась альтернативная гипотеза, заключающаяся в том, что «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является набором независимых и одинаково, но неравномерно распределенных случайных величин. Для критерия $\chi^2$ (а в [21] и для некоторых других критериев) было показано, что мощность при применении к «входному» потоку, как правило, оказывается асимптотически больше, чем при применении к «выходному» потоку. Более того, в [21] было показано, что для критерия отношения правдоподобия, мощность при применении к «входному» потоку всегда асимптотически строго больше, чем при применении к «выходному» потоку. В связи с этим применение «Book Stack»-теста против такой альтернативы вряд ли является перспективным.

Как уже упоминалось во Введении, в [20, Пример 2.7.5] в результате анализа вычислительного эксперимента было выдвинуто предположение о возможной перспективности изучения альтернатив, связанных с зависимыми $\{\eta_i\}_{i\geqslant 1}$. Теоретические результаты, полученные в данной работе, позволили подвердить это предположение.

Итак, рассмотрим альтернативную гипотезу $\mathbb{H}_1$, заключающуюся в том, что «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является эргодической однородной марковской цепью

с фазовым пространством $\mathbb{S}$, стационарным равномерным распределением и матрицей переходных вероятностей $\mathbf{P}^{(\eta)}$, след которой отличен от 1. Оказывается, что против такой альтернативы критерий $\chi^2$, примененный ко «входному» потоку, является несостоятельным, в то время как такой же критерий, примененный к «выходному» потоку, — состоятельный.

Начнем с результата, касающегося предельного распределения статистики $\chi^2_n(\eta)$, введенной в (2.3.21). Доказательство можно найти в [27].

**Теорема 2.5.1.** *Пусть «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является стационарной ЭОМЦ со стационарным равномерным распределением. Обозначим $\Sigma_\eta$ — предельную ковариационную матрицу для $\{\eta_i\}_{i\geqslant 1}$ (см. (2.3.9), в качестве стационарного распределения цепи выбрано равномерное). Обозначим $\{\mu_i\}_{i=1}^k$ — ненулевые собственные числа матрицы $S\Sigma_\eta$, где $k \leqslant S-1$. Тогда при $n\to\infty$*

$$\mathcal{L}\left(\chi^2_n(\eta)\right) \Rightarrow \mathcal{L}\left(\sum_{i=1}^k \mu_i \zeta_i^2\right),$$

*где $\{\zeta_i\}_{i=1}^k$ — набор независимых стандартных нормальных случайных величин.*

**Замечание 2.5.1.** 1. Доказательство теоремы основывается на ЦПТ 2.3.1, которая в рассматриваемых условиях не предполагает стационарности цепи, поэтому это условие в Теореме 2.5.1 можно опустить.

2. Если «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является набором независимых и одинаково распределенных случайных величин, то $k = S-1$ и $\mu_i = 1$ для всех $i \in 1:(S-1)$, поэтому результат становится стандартным:

$$\mathcal{L}\left(\chi^2_n(\eta)\right) \Rightarrow \chi^2(S-1).$$

Наконец, мы готовы сформулировать общее утверждение о свойствах теста «Book Stack» против рассматриваемой альтернативы.

**Теорема 2.5.2.** *Критерии $\chi^2$ для проверки $\mathbb{H}_0$ против альтернативы $\mathbb{H}_1$, состоящей в том, что «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ образует ЭОМЦ со стационарным равномерным распределением и матрицей переходных вероятностей, имеющей след отличный от 1, обладают следующими свойствами:*

1. *При применении к «входному» потоку $\{\eta_i\}_{i\geqslant 1}$ критерий несостоятельный.*
2. *При применении к «выходному» потоку $\{\xi_i\}_{i\geqslant 1}$ критерий состоятельный.*

*Доказательство.* 1. Следует из Теоремы 2.5.1. Действительно, из этой Теоремы следует, что $\chi^2_n(\eta) \overset{\mathbb{P}}{\not\to} \infty$, где $\chi^2_n(\eta)$ введено в (2.3.21). А, значит, мощность критерия не стремится по вероятности к 1.

2. Как уже отмечалось, из Теоремы 2.2.1 следует, что при $n \to \infty$

$$\frac{\chi^2_n(\xi)}{Sn} \overset{\mathbb{P}}{\to} \rho^2_2(\xi),$$

где $\chi^2_n(\xi)$ введено в (2.3.21), а $\rho^2_2(\xi)$ — в (2.3.20). По Следствию 2.4.1 $\rho^2_2(\xi) \neq 0$. Следовательно, $\chi^2_n(\xi) \overset{\mathbb{P}}{\to} \infty$. □

**Замечание 2.5.2.** Обсудим результат доказанной Теоремы. Пункт 1 верен и без предположения, что $\mathrm{tr}\left(\mathbf{P}^{(\eta)}\right) \neq 1$. Второй же пункт без такого предположения выполняться не обязан. Если окажется, как в Примере 2.4.3, что предельные распределение «выходного» потока является равномерным, причем у матрицы $\mathbf{P}^{(\eta)}$ не все элементы равны $1/S$, то критерий $\chi^2$, примененный к $\{\xi_i\}_{i\geqslant 1}$ не обязан быть состоятельным. Действительно, в таком случае $\rho^2_2(\xi) = 0$ и, вообще говоря, нельзя сделать вывод, что $\chi^2_n(\xi) \overset{\mathbb{P}}{\to} \infty$ при $n \to \infty$.

Продемонстрируем результат Теоремы 2.5.2 с помощью моделирования.

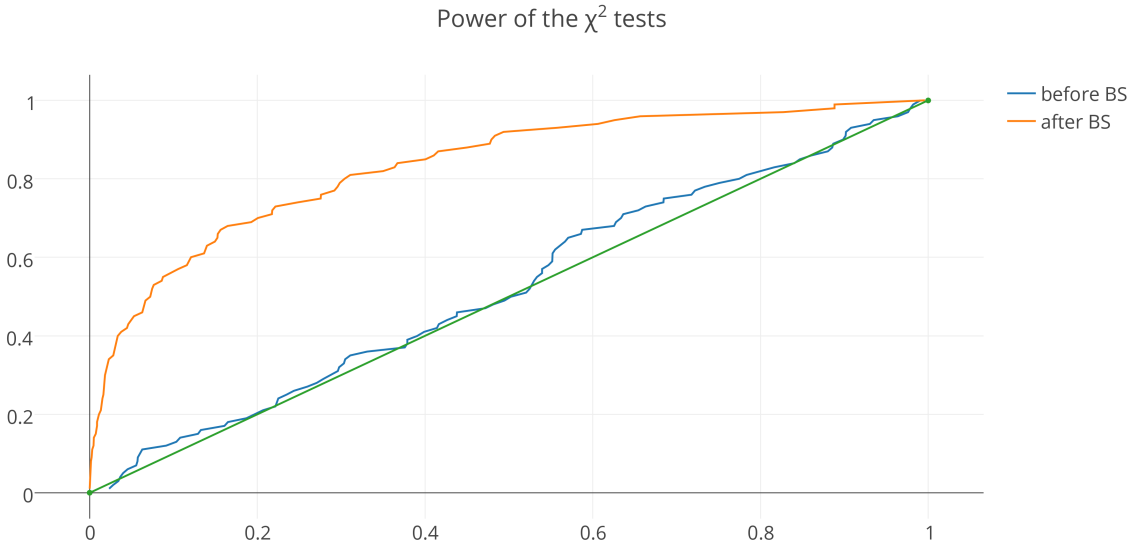


Рис. 2.1. Эмпирические оценки мощности одномерных критериев $\chi^2$ с $S-1$ степенью свободы до/после «Book Stack». Иллюстрация к Примерам 2.4.1 и 2.5.1. Для критерия $\chi^2$ «до» преобразования $P$-значение критерия Колмогорова при сравнении с равномерным распределением равно 0.48, «после» — меньше, чем $2.2 \cdot 10^{-16}$.

**Пример 2.5.1.** Рассмотрим модель из Примера 2.4.1. Пусть начальное распределение цепи $\{\eta_i\}_{i\geqslant 1}$ является равномерным. Будем сравнивать критерий $\chi^2$ с $S-1$ степенью свободы для проверки нулевой гипотезы, примененный к «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$ и такой же критерий, примененный к «выходной» последовательности $\{\xi_i\}_{i\geqslant 1}$. Промоделируем $m$ повторных независимых выборок объема $n$ из ОМЦ с матрицей переходных вероятностей $\mathbf{P}^{(\eta)}$. В результате получаем $m$ $P$-значений, график эмпирической функции распределений которых есть график (приближенной) зависимости мощности критерия от его уровня. Результаты моделирования с $S = 3$, $n = 10^4$, $m = 100$ и $\delta = 1/S + 0.01$ представлены на рисунке 2.1. На этом рисунке видно, что более мощным оказался критерий $\chi^2$, примененный к «выходному» потоку $\{\xi_i\}_{i\geqslant 1}$.

**Пример 2.5.2.** Рассмотрим модель из Примера 2.4.2 и пусть начальное распределение цепи $\{\eta_i\}_{i\geqslant 1}$ является равномерным. Моделирование проводится точно так же, как в Примере 2.5.1. Результаты моделирования с $S = 3$, $n = 10^3$, $m = 100$ представлены на рисунке 2.2. Выводы те же, что и в Примере 2.5.1.

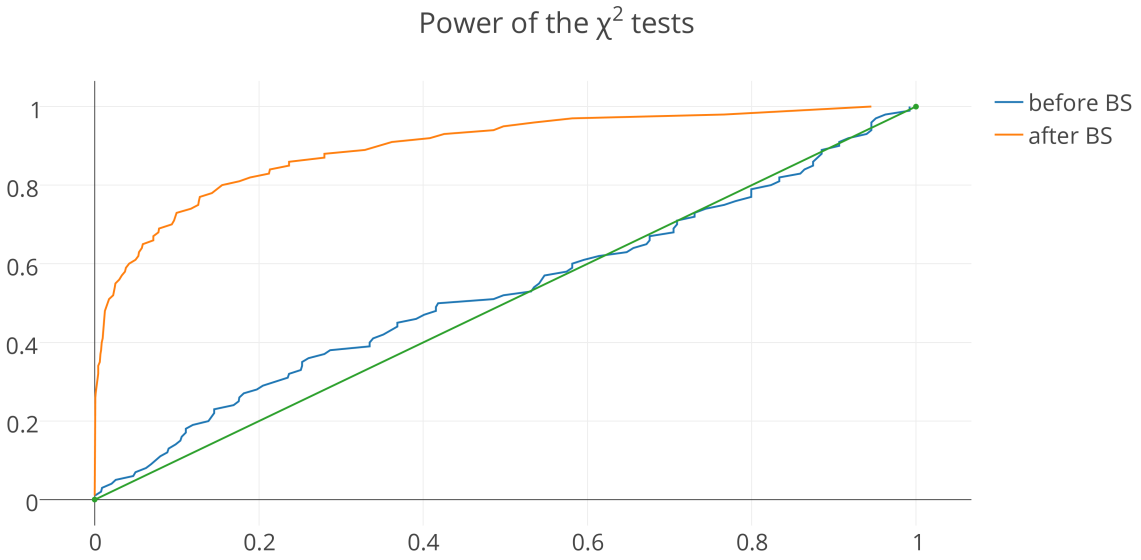


Рис. 2.2. Эмпирические оценки мощности одномерных критериев $\chi^2$ с $S-1$ степенью свободы до/после «Book Stack». Иллюстрация к Примерам 2.4.2 и 2.5.2. Для критерия $\chi^2$ «до» преобразования $P$-значение критерия Колмогорова при сравнении с равномерным распределением равно 0.256, «после» — меньше, чем $2.2 \cdot 10^{-16}$.

**Пример 2.5.3.** Рассмотрим модель из Примера 2.4.3 и пусть начальное распределение цепи $\{\eta_i\}_{i\geqslant 1}$ является равномерным. Моделирование проводится точно так же, как в

Примере 2.5.1. Результаты моделирования с $S = 3$, $n = 10^3$, $m = 100$ представлены на рисунке 2.3. Выводы те же, что и в Примерах 2.5.1 и 2.5.2. Заметим, что согласно Замечанию 2.5.2 критерий, примененный к «выходному» потоку, не обязан быть состоятельным.

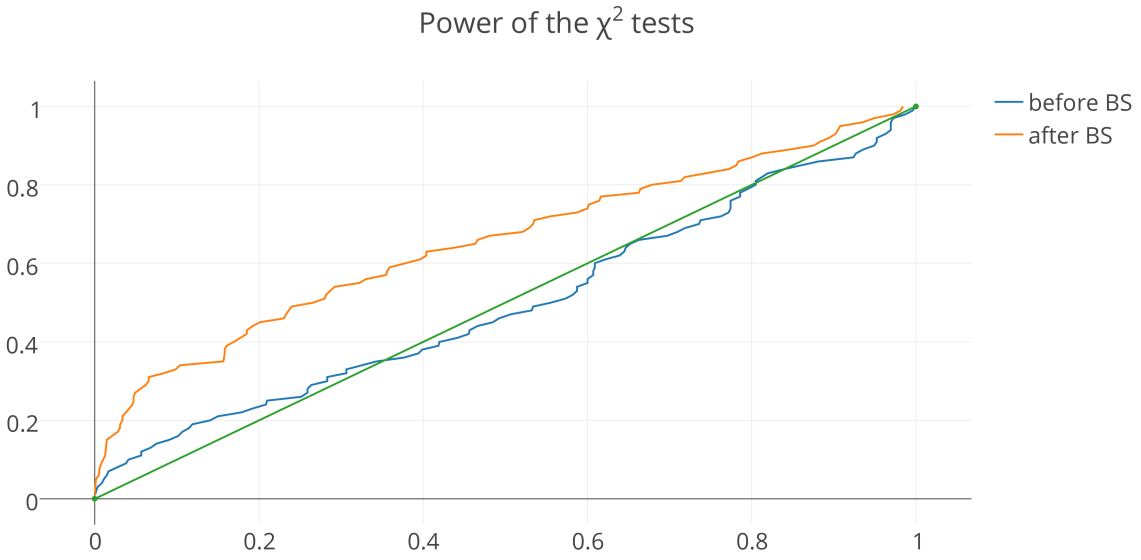


Рис. 2.3. Эмпирические оценки мощности одномерных критериев $\chi^2$ с $S-1$ степенью свободы до/после «Book Stack». Иллюстрация к Примерам 2.4.3 и 2.5.3. Для критерия $\chi^2$ «до» преобразования $P$-значение критерия Колмогорова при сравнении с равномерным распределением равно 0.64, «после» — $5.1 \cdot 10^{-6}$.

Теорема 2.5.2 позволяет сделать вывод о перспективности дальнейшего исследования свойств «Book Stack»-теста против альтернативы $\mathbb{H}_1$, а также других альтернатив, связанных с зависимыми $\{\eta_i\}_{i\geqslant 1}$.

# Глава 3

# «Order»-преобразование и «Order»-тест

## 3.1. Описание преобразования

Приведем сначала неформальное описание «Order»-преобразования, лежащего в основе одноименного теста. Рассмотрим целое $S > 1$ и множество $\mathbb{S} \stackrel{\text{def}}{=} \{1, 2, \ldots, S\}$. Из этого множества некоторым образом последовательно выбираются $n$ чисел $\eta_1, \eta_2 \ldots, \eta_n$ (возможно, с повторениями). На $i$-м шаге (для всех $i \in 1 : n$) вычисляется набор частот (без нормировки) $\Xi_1, \ldots \Xi_S$ для первых выбранных $i - 1$ чисел. Само преобразование заключается в том, что для очередного выбранного числа $\eta_i$ вычисляется номер $\xi_i$ его частоты в упорядоченном по невозрастанию списке всех частот (при совпадающих частотах выбирается минимальный из их номеров). Таким образом, если обозначить упорядоченный по невозрастанию набор частот $\Theta_1, \ldots \Theta_S$, то $\xi_i$ — минимальный такой номер, что $\Theta_{\xi_i} = \Xi_{\eta_i}$. Далее происходит обновление массива частот с учетом $\eta_i$ и процедура повторяется с заменой $\eta_i$ на $\eta_{i+1}$. Результат $n$-кратного «Order»-преобразования — это «выходная» последовательность $\xi_1, \ldots \xi_n$, которая определяется «входной» последовательностью $\eta_1, \ldots, \eta_n$.

Сформулируем общее алгоритмическое описание «Order»-процедуры.

**Общее алгоритмическое описание «Order» процедуры**

**Входные данные**: $n$, $S$, $(\eta_1, \eta_2 \ldots, \eta_n)$. **Результат**: $(\xi_1, \xi_2 \ldots, \xi_n)$.

**1.** (*Инициализация массива частот*) $(\Xi_1, \ldots, \Xi_S) \leftarrow (0, 0, \ldots, 0)$.

**2.** (*Цикл по шагам Order преобразования*) For $i = 1$ to $n$ do

- (*Инициализация*) $j \leftarrow 1$;
- (*Сортировка массива частот*) $(\Theta_1, \ldots, \Theta_S) \leftarrow \mathrm{Sort}(\Xi_1, \ldots, \Xi_S)$;
- (*Вычисление $\xi_i$* ) While $(\Theta_j \neq \Xi_{\eta_i})$ do $(j \leftarrow j + 1)$; $\xi_i \leftarrow j$;
- (*Обновление массива частот*) $\Xi_{\eta_i} \leftarrow \Xi_{\eta_i} + 1$.

**2.** (*Завершение работы*) STOP.

Дадим формальное описание Order-преобразования в удобных для дальнейшего терминах. Пусть $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Введем последовательность векторов $\{\Xi^{(i)} \in \mathbb{N}_0^S\}_{i \geqslant 0}$ так, что для $i \geqslant 1$ и всех $j \in \mathbb{S}$

$$\Xi^{(i)} = \left(\Xi_1^{(i)}, \Xi_2^{(i)}, \ldots, \Xi_S^{(i)}\right)^{\mathrm{T}}, \quad \Xi_j^{(i)} = \sum_{k=1}^{i} \mathbb{1}(\eta_k = j), \tag{3.1.1}$$

а $\Xi^{(0)}$ — нулевой вектор. Ясно, что для каждого $i \geqslant 1$ компоненты вектора $\Xi^{(i)}$ – это частоты значений последовательности случайных величин $\eta_1, \ldots, \eta_i$.

Введем последовательность векторов

$$\{\Theta^{(i)} \in \mathbb{N}_0^S\}_{i \geqslant 0} \tag{3.1.2}$$

так, что для $i \geqslant 0$ компоненты вектора $\Theta^{(i)}$ являются упорядоченными по невозрастанию компонентами вектора $\Xi^{(i)}$.

Наконец, определим последовательность $\{\xi_i\}_{i \geqslant 1}$, где $\xi_i \in \mathbb{S}$ задается следующим образом

$$\xi_i = \min\left\{k \in \mathbb{S} \,|\, \Theta^{(i-1)}[k] = \Xi^{(i-1)}\left[\eta_i\right]\right\}. \tag{3.1.3}$$

Заметим, что $\xi_i$ существует (и единственно) для любого $i \geqslant 1$.

Связь между $\{\Theta^{(i)}\}$ и $\{\xi_i\}$ раскрывает следующее утверждение.

**Лемма 3.1.1.** *Для всех $i \geqslant 1$ и любого $j \in \mathbb{S}$*

$$\Theta_j^{(i)} = \sum_{k=1}^{i} \mathbb{1}(\xi_k = j).$$

*Доказательство.* Доказательство ведем индукцией по $i$. База индукции при $i = 1$ очевидна, поскольку $\Theta^{(1)} = (1, 0, 0, \ldots, 0)^{\mathrm{T}}$. При этом, конечно, $\xi_1 = 1$. Пусть теперь утверждение верно для $i$. По определению последовательности $\Xi^{(i)}$ для всех $i \geqslant 0$ и каждого $k \in \mathbb{S}$

$$\Xi_k^{(i+1)} = \Xi_k^{(i)} + \mathbb{1}\left(k = \eta_{i+1}\right).$$

Из этого и определения $\xi_i$ легко заметить, что для всех $i \geqslant 0$ и каждого $k \in \mathbb{S}$

$$\Theta_k^{(i+1)} = \Theta_k^{(i)} + \mathbb{1}\left(k = \xi_{i+1}\right),$$

откуда следует доказываемое утверждение. □

Таким образом, $\Theta^{(i)}$ образует вектор частот последовательности $\xi_1, \ldots, \xi_i$.

## 3.2. Свойства «Order»-теста

Во введении было дано формальное описание «Order» теста. Напомним, что проверяется гипотеза $\mathbb{H}_0$, заключающаяся в том, что «входная» последовательность $\{\eta_i\}_{i\geqslant 1}$ является последовательностью независимых случайных величин, причем $\mathbb{P}(\eta_i = k) = 1/S$ при $1 \leqslant k \leqslant S$. Проверка осуществляется с помощью стандартного критерия $\chi^2$. Суть теста состоит в том, что критерий $\chi^2$ применяется не к исходным случайным величинам $\{\eta_i\}_{i\geqslant 1}$, а к преобразованным $\{\xi_i\}_{i\geqslant 1}$ с той же степенью свободы.

Лемма 3.1.1 позволяет сформулировать следующий результат про «Order»-тест.

**Предложение 3.2.1.** *Рассмотрим некоторую функцию $t_n : \mathbb{S}^n \to \mathbb{R}$. Предположим, что значение $t_n$ в точке $(x_1, x_2, \ldots, x_n)^{\mathrm{T}}$ определяется лишь частотами $\sum_{i=1}^n \mathbb{I}_k(x_i)$ для всех $k \in \mathbb{S}$ и инвариантно относительно перестановки этих частот. Тогда*

$$t_n(\eta_1, \ldots, \eta_n) = t_n(\xi_1, \ldots, \xi_n),$$

*где $\xi_i$ введено в (3.1.3).*

*Доказательство.* Следует из Леммы 3.1.1 и определения векторов $\Xi^{(i)}$, введенных в (3.1.1), и $\Theta^{(i)}$, введенных в (3.1.2). □

**Следствие 3.2.1.** Утверждение Предложения 3.2.1 верно, в частности, для статистики критерия $\chi^2$.

## 3.3. Связь между предельными свойствами входной и выходной последовательностей

Лемма 3.1.1 позволяет сформулировать следующий результат про связь предельных распределений частот последовательностей $\eta_n$ и $\xi_n$. Отметим, что никаких предварительных предположений о совместном распределении $\{\eta_i\}_{i\geqslant 1}$ не делается.

**Теорема 3.3.1.** *Рассмотрим некоторое распределение $\mathcal{P} = \{p_k\}_{k=1}^S$ на множестве $\mathbb{S}$. Обозначим $\{p_{[i]}\}$ — набор $\{p_i\}$ после упорядочивания по неубыванию: $p_{[1]} \geqslant p_{[2]} \ldots \geqslant p_{[S]}$. Предположим, что*

$$\frac{\Xi_n[k]}{n} \xrightarrow{\mathbb{P}} p_k$$

*для всех $k \in \mathbb{S}$, где $\Xi_i$ введено в (3.1.1).*

*Тогда*

$$\frac{\Theta_n[k]}{n} \xrightarrow{\mathbb{P}} p_{[k]}$$

*для всех* $k \in \mathbb{S}$*, где* $\Theta_i$ *введено в* (3.1.2).

*Доказательство.* Утверждение следует из непрерывности отображения $(x_1, \ldots, x_S)^{\mathrm{T}} \mapsto \left(x_{[1]}, \ldots, x_{[S]}\right)^{\mathrm{T}}$. □

**Следствие 3.3.1.** Для выполнения утверждения Теоремы 3.3.1 достаточно, чтобы случайные величины $\{\eta_n\}_{n\geqslant 1}$ образовывали однородную марковскую цепь с одним эргодическим классом и, может быть, несколькими несущественными состояниями.

*Доказательство.* Следует из Теоремы 2.1.1. □

**Замечание 3.3.1.** Конечно, для выполнения утверждения Теоремы 3.3.1, в частности, достаточно, чтобы случайные величины $\{\eta_n\}_{n\geqslant 1}$ являлись независимыми и одинаково распределенными с распределением $\mathcal{P} = \{p_k\}_{k=1}^{S}$.

Смысл Предложения 3.2.1 и Теоремы 3.3.1 заключается в том, что совершенно безразлично, применять статистический критерий для проверки гипотезы $\mathbb{H}_0$ к «входной» последовательности случайных величин $\eta_1, \ldots, \eta_n$ или же к «выходной» — $\xi_1, \ldots, \xi_n$. В связи с этим применение «Order»-теста вряд ли является целесообразным.

# Заключение

В работе рассмотрены статистические тесты «Book Stack» и «Order» для проверки нулевой гипотезы о независимости и равномерной распределенности некоторого набора дискретных случайных величин, имеющих одинаковый носитель. В основе этих тестов лежат соответственно «Book Stack»- и «Order»-преобразования. На вход преобразованиям подается набор дискретных случайных величин $\{\eta_i\}_{i\geqslant 1}$, принимающих значения на множестве $\{1, 2, \ldots, S\}$. Результатом применения преобразований является набор дискретных случайных величин $\{\xi_i\}_{i\geqslant 1}$. Нулевая гипотеза заключается в проверке независимости и равномерной распределенности набора дискретных случайных величин $\{\eta_i\}_{i\geqslant 1}$. Согласно описанию тестов, основанных на преобразованиях, критерий $\chi^2$ применяется не к исходному набору $\{\eta_i\}_{i\geqslant 1}$, а к $\{\xi_i\}_{i\geqslant 1}$.

В работе теоретически показано, что при выборе альтернативной гипотезы, заключающейся в том, что входная последовательность $\{\eta_i\}_{i\geqslant 1}$ образует эргодическую однородную марковскую цепь, выходная последовательность, полученная с помощью «Book Stack»-преобразования, $\{\xi_i\}_{i\geqslant 1}$ тоже имеет некоторое стационарное распределение, сходимость к которому обеспечена Законом Больших Чисел. Более того, показано, что в таких предположениях выполняется и Центральная Предельная Теорема для частот.

В работе получено обобщение «Book Stack» преобразования. Для такого обобщения те же теоретико-вероятностные результаты получены в предположении положительности всех вероятностей перехода «входной» однородной марковской цепи $\{\eta_i\}_{i\geqslant 1}$.

Для стандартного «Book Stack» преобразования в рамках той же альтернативы произведено сравнение предельных распределений «входной» и «выходной» последовательности. Показано, что в случае, если стационарное распределение «входной» ЭОМЦ является равномерным, то для очень широкого класса входных ЭОМЦ стационарное распределение «выходной» последовательности будет отличным от равномерного.

Именно поэтому при выборе в качестве альтернативной гипотезы, состоящей в том, что «входные» случайные величины $\{\eta_i\}_{i\geqslant 1}$ образуют эргодическую однородную марковскую цепь со стационарным равномерным распределением и матрицей переходных вероятностей, след которой отличен от 1, применение «Book Stack»-теста оказывается оправданным. Более того, применение этого теста может быть целесообразно и в рамках других альтернатив, связанных с зависимостью $\{\eta_i\}_{i\geqslant 1}$.

В работе также теоретически показано, что для «Order»-преобразования статистики любого статистического критерия для проверки гипотезы $\mathbb{H}_0$, которые определяются только частотами выборки и инвариантны относительно их перестановок, посчитанные по «входной» последовательности $\{\eta_i\}_{i=1}^n$ и «выходной» $\{\xi_i\}_{i=1}^n$ совпадают. Именно поэтому применение «Order»-теста вряд ли является целесообразным.

Таким образом, наиболее продуктивным представляется дальнейшее изучение поведения «Book Stack»-теста (и различных его обобщений) против различных альтернатив, связанных с зависимостью «входной» последовательности $\{\eta_i\}_{i\geqslant 1}$.

# Список литературы


1. Rukhin A., Solo J., Nechvatal J. et al. — A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. — National Institute of Standards and Technology, 2010.
2. Marsaglia G. Diehard battery of tests of randomness. — 1995.
3. L'Ecuyer P., Simard R. TestU01: A C Library for Empirical Testing of Random Number Generators // ACM Trans. Math. Softw. — 2007. — aug. — Vol. 33, no. 4.
4. Ryabko B., Pestunov A. "Book stack" as a new statistical test for random numbers. // Probl. Inf. Transm. — 2004. — Vol. 40, no. 1. — P. 66–71.
5. Рябко Б. Я. Сжатие информации с помощью стопки книг // Проблемы передачи информации. — 1980. — Т. 16. — С. 16–21.
6. A Locally Adaptive Data Compression Scheme / Jon Louis Bentley, Daniel D. Sleator, Robert E. Tarjan, Victor K. Wei // Commun. ACM. — 1986. — apr. — Vol. 29, no. 4.
7. Seward J. — bzip2 and libbzip2, version 1.0.5: A program and library for datacompression, 2007. — Accessed: 17.05.2017. URL: http://www.bzip.org/1.0.5/bzip2-manual-1.0.5.pdf.
8. Doroshenko S., Fionov A., Lubkin A. On ZK-crypt, Book Stack, and Statistical Tests // IACR Cryptology ePrint Archive. — 2006.
9. Doroshenko S., Ryabko B. The experimental distinguishing attack on RC4. — 2006.
10. Ryabko B. Y., Monarev V. A. Using information theory approach to randomness testing // Statistical Planning and Inference. — 2005. — Vol. 133. — P. 95–110.
11. Монарев В. А., Рябко Б. Я. Экспериментальный анализ генераторов псевдослучайных чисел при помощи нового статистического теста // ЖВМ и МФ. — 2004. — Т. 44, № 5. — С. 812–816.
12. Ryabko B., Monarev V., Shokin Y. A new test for randomness and its application to some cryptographic problems // Statistical Planning and Inference. — 2004. — Vol. 123, no. 2. — P. 365–376.
13. Рябко Б. Я., Монарев В. А., Шохин Ю. И. Новый класс статистических тестов для случайных чисел и его применение в задачах криптографии. — 2005. — С. 211–220.
14. Рябко Б. Я., Пестунов А. И. «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. — 2004. — Т. 40, № 1. — С. 73–78.

15. Монарев В. А., Рябко Б. Я. Экспериментальный анализ генераторов псевдослучайных чисел при помощи нового статистического теста // Журнал вычислительной математики и математической физики. — 2004. — Vol. 44, no. 5. — P. 812–816.
16. L'Ecuyer P. Tables of linear congruential generators of different sizes and good lattice structure // Mathematics of Computation. — 1999. — Vol. 68. — P. 249–260.
17. Кнут Д. Э. Искусство программирования. — Издат. дом «Вилиамс», 2001. — Т. 2. Получисленные алгоритмы. — 832 с.
18. Using Universal Coding Approach to Randomness Testing / Ed. by B. Ryabko, V. Monarev, Yu. Shokin. — International Symposium on Information Theory, 2004.
19. Matsumoto M., Nishimura T. Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator // ACM Trans. Model. Comput. Simul. — 1998. — jan. — Vol. 8, no. 1. — P. 3–30.
20. Бзикадзе А. В. Некоторые Свойства Статистического Теста Book Stack : Бакалаврская Выпускная Квалификационная Работа / А. В. Бзикадзе ; Санкт-Петербургский Государственный Университет. — 2015.
21. Bzikadze A. V., Nekrutkin V. V. On some statistical properties of the "book stack" transformation // Vestnik St. Petersburg University: Mathematics. — 2016. — Vol. 49, no. 4. — P. 305–312. — URL: http://dx.doi.org/10.3103/S106345411604004X.
22. Ширяев А. Вероятность-1. — Изд-во МЦНМО, 2011. — ISBN: 9785940577522.
23. Сираждинов С., Форманов Ш. Предельные теоремы для сумм случайных векторов, связанных в цепь Маркова. — Изд-во «Фан» Узбекской ССР, 1979.
24. Ширяев А. Вероятность-2. — Изд-во МЦНМО, 2011.
25. Боровков А. Теория вероятностей. — Изд-во «Наука», 1986.
26. Кельберт М. Я., Сухов Ю. М. Вероятность и статистика в задачах. — МЦНМО, 2009. — Т. 2, Марковские цепи как отправная точка теории случайных процессов и их приложения.
27. Tavare S., Altham P. Serial dependence of observations leading to contingency tables, and correctionts to chi-squared statistics // Biometrika. — 1983. — Vol. 70, no. 1. — P. 139–44.