Сентябрь 2024 г. *Том 194, № 9*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

МЕТОДИЧЕСКИЕ ЗАМЕТКИ

Квантовые генераторы случайных чисел, экстракция доказуемо случайных битовых последовательностей из траекторий цепи Маркова

И.М. Арбеков, С.Н. Молотков

Исследуется одна из главных проблем в построении квантовых генераторов случайных чисел — получение доказуемо случайной выходной последовательности из результатов физических измерений — исходной последовательности, вырабатываемой физическим генератором случайных чисел. Обсуждаются вопросы о принципиальной возможности и условиях, при которых можно "дотянуться" до случайности, а также то, что понимать под доказуемой случайностью. Рассмотрены методы экстракции доказуемо случайных битовых последовательностей из стационарных цепей Маркова конечного порядка, т.е. в предположении о конечной глубине зависимости результатов физических измерений от предыстории, которое является адекватным приближением к реальной ситуации. Продемонстрировано извлечение выходной доказуемо случайной битовой последовательности из исходной последовательности результатов физических измерений с использованием эффективного метода арифметического кодирования В.Ф. Бабкина. Показано, что даже из первичных последовательностей результатов физических измерений, которые являются зависимыми (коррелированными) на любую конечную глубину (предысторию), можно доказуемо получать случайные битовые последовательности. Цель, которую ставили перед собой авторы — показать связь различных приближений, которые используются при разработке и описании методов получения случайных битовых последовательностей с фундаментальными физическими ограничениями Природы. Математические доказательства доведены до практических алгоритмов, которые используются в реальных генераторах случайных чисел. Необходимые математические доказательства приводятся на интуитивно понятном для физической аудитории уровне, не требуют предварительных специальных знаний и доступны студентам старших курсов университетов.

Ключевые слова: квантовые генераторы случайных чисел, цепи Маркова, случайные битовые последовательности

PACS numbers: **02.50.–r**, **03.67.–a**, 42.50.Ex DOI: https://doi.org/10.3367/UFNr.2024.02.039658

Содержание

И.М. Арбеков [1, a], **С.Н. Молотков** [1, 2, 3, 4, b]
[1] Академия криптографии Российской Федерации, а/я 100, 119331 Москва, Российская Федерация
[2] Институт физики твердого тела им. Ю.А. Осипьяна РАН, ул. Академика Осипьяна 2, 142432 Черноголовка, Московская. обл., Российская Федерация
[3] Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики, Ленинские горы 1, стр. 52, 119991 Москва, Российская Федерация
[4] Московский государственный университет им. М.В. Ломоносова, Центр квантовых технологий, Ленинские горы 1, стр. 35, 119991 Москва, Российская Федерация
E-mail: [a] arbekov53@mail.ru, [b] molotkov@issp.ac.ru

Статья поступила 25 декабря 2023 г., после доработки 20 февраля 2024 г.

Истина слишком сложна, нам дано лишь немного приблизиться к ней
Джон фон Нейман

1. Введение

Случайные числа широко применяются в различных областях науки и техники — это компьютерные пароли

доступа, PIN коды смарт карт и других электронных устройств. Наиболее важное применение случайные последовательности находят в системах квантовой криптографии — квантового распределения ключей, где требуется большое число случайных битов. В системах квантовой криптографии при распределении секретных ключей требуется до 10^8 случайных битов на формирование одного общего ключа. Для выработки случайных последовательностей большого объёма требуются высокоскоростные генераторы случайных чисел.

Все генераторы случайных чисел можно разделить на два типа: *математические* и *физические*.

Математические генераторы, часто называемые также программными генераторами случайных чисел (ПГСЧ), основаны на математическом преобразовании, обычно рекурсивном, некоторого затравочного числа (в англоязычных работах seed). Алгоритм математического преобразования публично известен, неизвестно только затравочное число. Если затравочное число известно, то вся последующая битовая последовательность также известна. По этой причине математические генераторы выдают только псевдослучайную битовую последовательность, "случайность" которой зиждется лишь на неизвестном затравочном числе.

Физические генераторы случайных чисел (ФГСЧ) основаны на обработке результатов измерений над некоторой физической системой.

ФГСЧ можно также разделить на два типа — *классические* и *квантовые*.

Классические генераторы основываются на извлечении случайности из некоторого физического процесса, эволюция которого во времени описывается законами классической физики. Эволюцию любой, даже сколь угодно сложной классической системы, можно описать дифференциальными уравнениями. Последовательности, которые получаются на выходе такого генератора, вряд ли можно назвать истинно случайными, поскольку они полностью определяются начальными условиями. В классической области случайность при наблюдении над физической системой возникает лишь как результат неопределённости начальных условий. При известных начальных условиях и одной и той же эволюции классической системы результат наблюдений является полностью детерминированным.

Квантовые генераторы основываются на измерении некоторой квантовой системы. В отличие от классической физики, измерения над квантовой системой, каждый раз приготовленной в определённом и одном и том же состоянии, дают случайный результат, что является фундаментальным законом Природы в микромире. При реализации ФГСЧ желательно найти подходящую физическую систему, результаты измерений над которой имели бы чисто квантовую природу.

Представляется, что истинная случайность существует только в квантовой области, в том смысле, что результат измерения над квантовой системой, каждый раз приготовленной в одних и тех же начальных условиях, является принципиально непредсказуемым.

В квантовой области вероятность встроена в математическое описание измерения над квантовой системой.

Тем не менее возникают следующие принципиальные вопросы.

• Что понимать под истинной случайностью?

• Позволяют ли фундаментальные законы Природы "дотянуться" до истинной случайности в реальных физических экспериментах и устройствах? Или нам дано Природой лишь приближаться к истинной случайности, в духе высказывания фон Неймана, приведённого в виде эпиграфа?

• Как проверять, что полученные выходные битовые последовательности являются истинно случайными?

Реализация любого — классического или квантового ФГСЧ — включает следующие стадии:

— выбор физической системы (источника "шума"), измерения над которой дают исходную случайную последовательность;

— оценку количества случайности — числа случайных 0 и 1, которые можно извлечь из исходной случайной последовательности;

— экстракцию случайных 0 и 1 из исходной случайной последовательности — постобработку исходной последовательности — преобразование исходной случайной последовательности в выходную битовую последовательность;

— доказательство того факта, что выходная битовая последовательность, в рамках принятых приближений при описании выбранной физической системы, является истинно случайной битовой последовательностью, в которой вероятности 0 и 1 равны $1/2$, и все позиции в последовательности независимы друг от друга.

Оказывается, что существуют принципиальные ограничения на генерацию исходной последовательности независимых результатов физических измерений.

Существуют фундаментальные ограничения на скорость генерации случайных чисел в квантовых генераторах, которые связаны с тем, что спектр любой устойчивой физической системы должен лежать на положительной полуоси энергий (частот)[1]. Данный факт формализуется известной теоремой Винера – Пэли.

• Любой физический случайный процесс — квантовый или классический — характеризуется корреляционной функцией и спектральной плотностью мощности, связанных между собой парой преобразований Фурье. Спектральная плотность мощности, по физическим ограничениям, должна обращаться в нуль при значениях частоты ниже некоторого порогового значения. В этом случае скорость спадания корреляционной функции не может быть быстрее (или равной) экспоненциальной, что диктуется фундаментальной теоремой Винера – Пэли. Это означает, что извлекаемые из случайного процесса в разные моменты времени результаты измерений оказываются коррелированными (зависимыми). Формально некоррелированными измерения становятся только при разнесении моментов измерения во времени на бесконечный интервал.

Рассмотрим спектральную плотность

$$g(\omega) = \begin{cases} 0\,, & \omega < \omega_{\min}\,, \\ g'(\omega)\,, & \omega \geqslant \omega_{\min} > -\infty \end{cases}$$

и корреляционную функцию

$$R(t) = \int_{-\infty}^{\infty} g(\omega) \exp\left(-\mathrm{i}\omega t\right) \mathrm{d}\omega\,.$$

[1] Естественно, что выбор начала отсчёта энергий на полуоси не важен.

Согласно теореме Винера – Пэли [1, 2], для любой квадратично интегрируемой функции следующий интеграл должен сходиться:

$$\int_{-\infty}^{\infty} \frac{\left|\ln |R(t)|\right|}{1+t^2}\, \mathrm{d}t < \infty\,.$$

Из этого условия следует, что скорость спадания функции $|R(t)|$ должна быть медленнее экспоненциальной:

$$\left|R(t)\right| \underset{t\to\infty}{\sim} \exp\left(-ct^q\right), \quad c>0\,, \quad q<1\,.$$

Отсюда формально следует, что измерения могут быть независимыми только при бесконечном интервале времени между ними.

Отметим, что фундаментальные ограничения на скорость спадания корреляций во времени приводят к тому, что α-распад[2] не может быть строго экспоненциальным на больших и малых временах (см. подробности [2]). Тот факт, что спектр устойчивой физической системы лежит на положительной оси энергий (частот), диктует фундаментальные ограничения на предельную скорость генерации случайных битовых последовательностей. Этот вопрос исследовался в работах [3, 4].

Почему так важна независимость исходной последовательности результатов физических измерений? Если бы можно было за конечное время достичь независимости между последовательными измерениями, то проблема высокоскоростных ФГСЧ была бы решена принципиально, поскольку существуют доказуемые эффективные методы экстракции истинно случайных битовых последовательностей из исходной последовательности независимых измерений (см. ниже, а также [5]). Однако фундаментальные ограничения Природы не позволяют получить исходную последовательность как последовательность независимых измерений.

Единственное, что можно сделать — это ограничиться конечной глубиной зависимости от предыстории и считать, что условная вероятность какого-либо результата измерения зависит только от r предыдущих исходов, т.е. имеет место конечная глубина корреляций.

В этом случае мы будем говорить о цепях Маркова порядка r. Данное предположение о том, что исходная последовательность является стационарной цепью Маркова конечного порядка r, является наиболее широким предположением, при котором вообще возможно конструктивное построение доказуемо случайной выходной последовательности (см. ниже).

Обсудим вопрос об экстракции битовых последовательностей из исходной последовательности результатов измерений физической системы.

Методы экстракции случайных битовых последовательностей из результатов измерений можно разделить на два класса.

1. Вероятностные экстракторы.

2. Детерминистические экстракторы.

Ранее было показано [5], что детерминистические экстракторы эффективно работают для исходных последовательностей независимых измерений.

Выходная последовательность ФГСЧ считается приемлемой для применения в криптографии, если она получена в соответствии со схемой равновероятных испытаний Бернулли, т.е. представляет собой реализацию последовательности независимых, равновероятных случайных величин. Известный подход для проверки этого предположения связан с применением совокупности статистических критериев согласия значений выходной последовательности с гипотезой о независимости и равновероятности вырабатываемых данных и наиболее полно отражён в [6]. Теоретические вопросы, связанные с нахождением предельных распределений соответствующих статистик, подробно представлены в книге [7].

Долгое время указанный подход был единственным для проверки качества выходных последовательностей, но его ограниченность вполне очевидна — критерии согласия успешно проходят выходные последовательности программных генераторов случайных чисел (ПГСЧ), где случайной является так называемая затравка — битовый отрезок конечной длины, значительно меньшей, чем длина вырабатываемой ПГСЧ последовательности. Выходную последовательность ПГСЧ вряд ли можно считать полученной в соответствии со схемой равновероятных испытаний Бернулли, хотя бы из мощностных соображений — мощность множества последовательностей ПГСЧ ограничена мощностью множества "затравочных" двоичных векторов.

Неформально говоря, сказанное означает, что количество истинно случайных битов в выходной псевдослучайной последовательности не может быть больше, чем число затравочных чисел в битовом представлении.

Представляется, что упомянутые выше мощностные соображения, числовым "эквивалентом" которых служит понятие предельной энтропии Шеннона, были положены в идеологическую основу методики [8].

Методика [8] содержит ряд тестов (оценок) минимальной энтропии $H_{\min}$ на символ. Минимальная энтропия является нижней оценкой энтропии Шеннона и, в пересчёте на бит, удовлетворяет неравенству $0 \leqslant H_{\min} \leqslant 1$. Максимальное значение $H_{\min} = 1$ достигается для схемы равновероятных испытаний Бернулли. Минимальная энтропия является весьма консервативной оценкой мощности, так как существенно занижает предельную энтропию Шеннона.

При получении числовой оценки $H_{\min} < 1$ предлагается производить соответствующее сжатие — хэширование исходной последовательности.

Результат применения хэш-функции является выходной последовательностью ФГСЧ. Вопрос о выборе хэш-функции, эффективной в том или ином смысле, к настоящему времени остаётся открытым.

Для случайно выбираемой хэш-функции (вероятностном экстракторе) оценка качества выходной последовательности может быть произведена с использованием известной Леммы об остатках — Leftover Hash Lemma [9].

Пусть имеется распределение вероятностей $P(X)$ на исходной последовательности $X = (x_1, x_2, \ldots, x_N) \in \in \{0,1\}^N$. Из некоторых модельных предположений относительно $P(X)$ строится оценка min-энтропии

$$H_{\min} = -\frac{1}{N}\log_2 \max_{X\in\{0,1\}^N} P(X)\,,$$

$$0 < H_{\min} < 1\,.$$

[2] Следует отметить, что ранее предпринимались попытки использовать α-распад для генерации случайных чисел, однако данный способ не нашел дальнейшего применения из-за технических сложностей и малой скорости.

Для получения выходной последовательности $Y = (y_1, y_2, \ldots, y_\ell) \in \{0,1\}^\ell$, $\ell < N$ (экстракции случайных битов), используется сжатие — хэширование:

$$g : \{0,1\}^N \to \{0,1\}^\ell .$$

Применение хэш-функции g индуцирует распределение на битовой строке $Y = (y_1, y_2, \ldots, y_\ell)$:

$$P_g(Y) = \sum_{X \in \{0,1\}^N : g(X) = Y} P(X) .$$

Для случайно выбираемой функции g из класса универсальных хэш-функций G [10] с использованием Left-over Hash Lemma можно установить справедливость неравенства, характеризующего близость распределения вероятностей $P_g(Y)$ к равновероятному распределению:

$$\sum_{g \in G} P(g) \sum_{Y \in \{0,1\}^\ell} \left| P_g(Y) - \frac{1}{2^\ell} \right| \leqslant \sqrt{2^{-NH_{\min} + \ell}} .$$

При достаточно большой длине N правая часть неравенства становится меньше сколь угодно малого значения ε.

Главная проблема здесь состоит в том, что оценка $H_{\min}$ требует трудно контролируемых модельных предположений о свойствах исходной последовательности как результата физических измерений и дополнительной случайности для выбора хэш-функции. Многократное использование одной и той же случайности при выборе хэш-функции приводит (при фиксированных N, ℓ) к росту оценочной границы ε.

Вопрос, который мы поднимаем в этой статье, — это вопрос о том, можно ли на основе каких-либо приближений относительно природы исходной последовательности, возникшей в результате измерений, построить доказуемо случайную выходную последовательность, а именно, имеющую вероятность $2^{-\ell}$, ℓ — длина последовательности. В этом случае отдельные биты, как случайные величины, являются независимыми и равновероятными.

Известен метод построения (экстракции) доказуемо случайной выходной последовательности, имеющей вероятность $2^{-\ell}$, из последовательности независимых неравновероятных испытаний (см., например, [5]). Этот метод использует метод арифметического кодирования В.Ф. Бабкина [11] и реализован в экспериментально разработанных квантовых ФГСЧ [12–15], основанных на последовательной регистрации фотоотсчётов ослабленного лазерного излучения.

Остановимся кратко на некоторых вопросах реализации квантового ФГСЧ такого типа.

Первопричина статистического характера фотоотсчётов при детектировании лазерного излучения носит принципиально квантовый характер и обусловлена поглощением фотонов атомами. Лавинные фотодетекторы не различают число фотонов, поэтому случайными событиями являются два события: наличие $(*)$ фотоотсчёта во временном окне или его отсутствие $(\sqcup)$.

Лавинные фотодетекторы обладают конечным временем восстановления после регистрации. При сильном ослаблении лазерного излучения средняя частота фотоотсчётов становится малой и детектор успевает восстановиться до следующего акта регистрации. В этом случае предполагается, что обеспечивается статистическая независимость последовательных фотоотсчётов, которая является исходной последовательностью ФГСЧ.

В предположении независимости последовательных фотоотсчётов, как случайных величин, на выходе квантового ФГСЧ можно получить доказуемо случайную выходную последовательность, имеющую вероятность $2^{-\ell}$, при этом знание самих вероятностей $p = P(\sqcup)$ и $1 - p = P(*)$ не требуется.

Из-за малой средней частоты фотоотсчётов такие квантовые ФГСЧ являются достаточно медленными. Стремление увеличить скорость работы приводит к увеличению средней частоты фотоотсчётов и к соответствующему негативному эффекту — появлению зависимостей в исходной последовательности, где текущий исход измерений зависит от предыдущих исходов.

В работах [16, 17] исследуются методы экстракции случайной последовательности из траекторий цепи Маркова. В [17] был предложен оригинальный метод экстракции доказуемо случайной последовательности из траекторий простой ($r = 1$) цепи Маркова с конечным числом состояний, многие доказательства работы достаточно сложны и являются многоходовыми.

Ниже, следуя основному принципу доказательства случайности в работе [17], состоящему в разбиении вероятностного пространства на подмножества эквивалентных (одинаково вероятных) траекторий, мы проведём обобщение результатов работы [17] на марковские цепочки произвольного порядка.

Используя конструктивные особенности экстракции случайных битов в методе арифметического кодирования В.Ф. Бабкина [11], мы сначала дадим подробное доказательство случайности выходных последовательностей для независимого источника, которое затем распространим на марковские последовательности.

Следуя общей концепции работы [17] будет показано, что для исходных последовательностей ФГСЧ в виде траекторий цепи Маркова с двумя состояниями, произвольного порядка r, выходные последовательности имеют одинаковую вероятность $2^{-\ell}$.

Необходимо ещё раз уточнить, что понимается под словами "доказуемая случайность".

Будет показано, что если глубина корреляций конечна, то наш метод выдает на выходе действительно истинно случайную последовательность 0 и 1.

Под истинной случайностью обычно понимается, что любая позиция в выходной последовательности 0 и 1 реализуется строго с вероятностью $1/2$ и каждая позиция независима от остальных.

Оказывается, что доказать данное утверждение "в лоб" невозможно даже в рамках используемого предположения о конечной глубине корреляций.

Будет доказано эквивалентное утверждение.

А именно, будет показано, что выходные последовательности 0 и 1 при любой длине ℓ содержат всевозможные комбинации 0 и 1

$$\overbrace{(000\ldots000)}^{\ell}, \overbrace{(000\ldots001)}^{\ell}, \ldots, \overbrace{(111\ldots111)}^{\ell}$$

и все такие последовательности имеют одинаковую вероятность $2^{-\ell}$, независимо от глубины корреляций. В этом случае отдельные биты, как случайные величины,

являются независимыми и равновероятными, т.е. являются истинно случайными.

Такова фактическая ситуация. Идеальная случайность слишком "сильный и сложный" информационный ресурс. Как будет показано ниже, даже в рамках используемых приближений к реальной ситуации доказательство истинной случайности является далеко не тривиальной задачей.

Рассмотрение будет проведено в два этапа.

На первом этапе будет предъявлен эффективный и доказуемый метод получения случайных последовательностей 0 и 1 из последовательности независимых испытаний.

На втором этапе будет показано, как свести задачу по экстракции доказуемо случайных битов из траектории цепи Маркова к задаче экстракции из последовательностей независимых испытаний.

2. Источник независимых состояний

Люди не верят в простоту математики лишь потому, что не понимают, насколько сложна реальность
Джон фон Нейман

Прежде чем показать, как получается доказуемое извлечение случайности из последовательности независимых испытаний, приведём неформальное объяснение. Общую идею можно понять на примере подбрасывания несимметричной монеты, у которой вероятности выпадения Орла (O) p и Решки (P) $1-p$, вероятность p неизвестна, каждое подбрасывание независимо от других.

Разобьём всю последовательность, получающуюся при подбрасывании, на блоки (последовательности) одинаковой длины, но имеющие разные числа O и P. Блоки с одинаковым числом O и P имеют одинаковую вероятность, равную $p^{n_O}(1-p)^{n_P}$ (n_O, n_P — числа O и P в блоке), и отличаются только перестановкой символов O и P, $n_O + n_P$ — длина блока.

Отнесём блоки с одинаковым числом O и P в один класс. Пусть в некотором классе число блоков N_{n_O,n_P}. Перенумеруем блоки (последовательности) в каждом классе, начиная нумерацию с 0. Предположим (в качестве упрощения), что число одинаково вероятных блоков в классе является степенью 2, т.е. $N_{n_O,n_P} = 2^L$, где L — число двоичных разрядов, необходимых для того, чтобы представить номера от 0 до $N_{n_O,n_P} - 1 = 2^L - 1$.

Иначе говоря, каждому i-му блоку ($0 \leqslant i \leqslant 2^L - 1$) в классе одинаково вероятных блоков сопоставлен номер, двоичное представление которого даёт двоичную последовательность длиной L.

Двоичные последовательности пробегают по одному разу всевозможные комбинации 0 и 1 длиной L_i, поэтому являются равновероятными в своём классе.

Таким образом, обрабатывая последовательно, по мере появления, блоки результатов измерений (отсчёт детектора — O, отсутствие отсчёта — P) — блоки независимых испытаний, и соединяя — конкатенируя последовательно двоичные последовательности, получаем, при условии независимости отсчётов, истинно случайные последовательности 0 и 1.

На интуитивном уровне, ситуацию можно понимать так, что каждый блок реализуется с некоторой вероятностью $p_O^{n_O} p_P^{n_P}$, источник выдаёт равновероятно одну из истинно случайных последовательностей 0 и 1 длины L_i. Это эквивалентно тому, что имеется N источников по числу классов последовательностей (N — длина блока из O и P). Каждый источник "включается" с вероятностью $p_O^{n_O} p_P^{n_P}$ и выдаёт на выход одну из равновероятных двоичных последовательностей длины L_i, которые затем конкатенируются в общую выходную последовательность 0 и 1.

Возникает вопрос, если все интуитивно достаточно прозрачно, то в чем проблема?

Проблема состоит в нумерации блоков в каждом классе "на ходу". Дело в том, что число возможных блоков в классе экспоненциально велико. Например, при длине обрабатываемого блока $L = 64$ (что связано с архитектурой 64-разрядного процессора), это число составляет величину $2^{64} \approx 10^{22}$. Нумерация через таблицу требует компьютерной памяти в 10^{22} битов. Чтобы наглядно представить масштаб такой памяти, приведём следующий пример. Пусть объём пямяти "средней" флэшки составляет 1 Гб (10^9 бит). В рюкзак умещается 1000 флэшек, итого $1000 \times 10^9 = 10^{12}$ битов. Таким образом, нужно 10^{10} — десять миллиардов рюкзаков — на каждого жителя Земли больше, чем по рюкзаку флэшек, тогда набирается память в $10^{10} \times 10^3 \times 10^9 = 10^{22}$ битов.

Очевидно, что такой способ нумерации невозможен.

Однако существует метод нумерации "на ходу", который представлен ниже, и который требует всего 64×64 битов памяти и шагов обработки 64, т.е. требуемые ресурсы 64^3 битов.

Перейдём к подробному выводу метода нумерации "на ходу" и экстракции битовых последовательностей 0 и 1 из независимых бернуллиевских последовательностей.

Пусть имеется источник, порождающий бернуллиевские (независимые) последовательности из двух символов.

Экстракция случайных последовательностей 0 и 1 из бернуллиевских последовательностей происходит в два шага.

Первый шаг: нумерация "на ходу" бернуллиевских последовательностей — метод Бабкина.

Второй шаг: формирование блока случайных 0 и 1 по полученному номеру бернуллиевской последовательности, последовательные блоки конкатенируются в выходную случайную последовательность.

2.1. Первый этап: нумерация бернуллиевских последовательностей — метод Бабкина, бинарный алфавит

Пусть имеется источник, который порождает символы из бинарного алфавита $A = \{s_1, s_2\}$.

Рассмотрим последовательность — блок длиной n, где имеется k символов s_1. Всего таких блоков C_n^k. Пусть k символов s_1 встретились на местах $(i_1, i_2, \ldots, i_k)$, $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$. Присвоим блоку номер

$$\mathrm{Num}\,(i_1, i_2, \ldots, i_k) = C_{i_1-1}^1 + C_{i_2-1}^2 + \ldots + C_{i_{k-1}-1}^{k-1} + C_{i_k-1}^k\,,$$

где полагается $C_j^i = 0$, если $j < i$. Данное равенство даёт способ нумерации блоков методом В.Ф. Бабкина [11].

Утверждение 1.
Имеют место соотношения

$$\min_{i_1,i_2,\ldots,i_k} \mathrm{Num}\,(i_1, i_2, \ldots, i_k) = 0\,,$$

$$\max_{i_1,i_2,\ldots,i_k} \mathrm{Num}\,(i_1, i_2, \ldots, i_k) = C_n^k - 1\,.$$

Утверждение 2.

Соотношение между блоками с k событиями s_1 на местах $(i_1, i_2, \ldots, i_k)$ и номерами $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$ *взаимно однозначное.*

Таким образом, любой последовательности, содержащей ровно k символов s_1 на местах $(i_1, i_2, \ldots, i_k)$ однозначно приписывается номер $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$.

2.1.1. Поточная нумерация по таблице. Нумерация блоков выполняется последовательно, по мере поступления события s_1.

Задаётся размер блока n, вычисляется один раз таблица биномиальных коэффициентов (табл. 1) размером $(n-1)\times n$. Значение k заранее не фиксируется.

Таблица 1

	1	2	3	4	5	…	$n-1$	n
i_1	0	1	C_2^1	C_3^1	C_4^1	…	C_{n-2}^1	C_{n-1}^1
i_2	0	0	1	C_3^2	C_4^2	…	C_{n-2}^2	C_{n-1}^2
i_3	0	0	0	1	C_4^3	…	C_{n-2}^3	C_{n-1}^3
…	…	…	…	…	…	…	…	…
i_{n-1}	0	0	0	0	0	…	0	1

Нумерация последовательностей сводится к движению по некоторой траектории на таблице с последовательным суммированием биномиальных коэффициентов.

Если в первый раз событие s_1 встретилось на m_1 месте, то берётся значение биномиального коэффициента на пересечении строки с номером i_1 (первое событие s_1) со столбцом с номером m_1.

Если второй раз событие s_1 встретилось на месте m_2 ($m_2 > m_1$), то берётся значение биномиального коэффициента на пересечении строки с номером i_2 со столбцом с номером m_2 и прибавляется к предыдущему значению биномиального коэффициента.

Если в k-й раз событие s_1 встретилось на месте m_k ($m_k > m_{k-1}$), то берётся значение биномиального коэффициента на пересечении строки с номером i_k со столбцом с номером m_k и прибавляется к предыдущей сумме биномиальных коэффициентов.

Процесс останавливается, когда просмотрен весь блок размера n. В соответствии с предыдущим разделом, получается номер $\mathrm{Num}\,(m_1, m_2, \ldots, m_k)$ блока с событиями s_1 и s_2 в виде двоичного представления — это ещё не случайные биты.

После того, как номер конкретной последовательности из s_1 и s_2 получен, из его двоичного представления извлекается блок случайных 0 и 1.

2.2. Второй этап: экстракция случайных двоичных последовательностей из номера последовательности

Мощность множества блоков $\mathcal{R}_n(k)$ с k событиями s_1 и $n-k$ событиями s_2 есть $|\mathcal{R}_n(k)| = C_n^k$. Нумерация блоков происходит, начиная с 0 до $C_n^k - 1$.

Пусть n чётное. Рассмотрим представление $|\mathcal{R}_n(k)|$ в виде суммы

$$\left|\mathcal{R}_n(k)\right| = 2^{r_m} + \ldots + 2^{r_1} + 2^{r_0}\,, \quad r_m > r_{m-1} > \ldots > r_1 > r_0\,.$$

Пусть реализовался блок, имеющий состав $(i_1, i_2, \ldots, i_k)$ событий s_1. Номер блока имеет двоичное разложение вида

$$\mathrm{Num}\,(i_1, i_2, \ldots, i_k) = \varepsilon_{r_m+1}2^{r_m+1} + \varepsilon_{r_m}2^{r_m} + \\ + \varepsilon_{r_m-1}2^{r_m-1} + \ldots + \varepsilon_1 2^1 + \varepsilon_0 2^0\,, \quad \varepsilon_r \in \{0,1\}\,,$$

и соответствующее двоичное представление

$$(\varepsilon_{r_m+1}, \varepsilon_{r_m}, \varepsilon_{r_m-1}, \ldots, \varepsilon_1, \varepsilon_0)\,.$$

Извлечение блока $\{\varepsilon\}$ случайных 0 и 1 производится из двоичного представления $(\varepsilon_{r_m+1}, \varepsilon_{r_m}, \varepsilon_{r_m-1}, \ldots, \varepsilon_1, \varepsilon_0)$ номера $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$. Производится по-разному, в зависимости от того, в каком диапазоне чисел между 0 и $C_n^k - 1$ лежит номер $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$ текущего блока.

А именно:

Номер	Блок $\{\varepsilon\}$ случайных 0 и 1
$0 \leqslant \mathrm{Num}\,(i_1, i_2, \ldots, i_k) \leqslant 2^{r_0} - 1\,,$	$\varepsilon_{r_0-1}, \ldots, \varepsilon_0\,,$
$2^{r_0} \leqslant \mathrm{Num}\,(i_1, i_2, \ldots, i_k) \leqslant 2^{r_0} + 2^{r_1} - 1\,,$	$\varepsilon_{r_1-1}, \ldots, \varepsilon_0\,,$
$2^{r_0} + 2^{r_1} \leqslant \mathrm{Num}\,(i_1, i_2, \ldots, i_k) \leqslant 2^{r_0} + 2^{r_1} + 2^{r_2} - 1\,,$	$\varepsilon_{r_2-1}, \ldots, \varepsilon_0\,,$
…	…
$2^{r_0} + \ldots + 2^{r_m} \leqslant \mathrm{Num}\,(i_1, i_2, \ldots, i_k) \leqslant 2^{r_0} + \ldots + 2^{r_m} - 1\,,$	$\varepsilon_{r_m-1}, \ldots, \varepsilon_0\,.$

Пронумеруем строки (неравенства) как $0, \ldots, j, \ldots, m$. В j-й строке — подклассе — содержится 2^{r_j} различных номеров $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$, которым однозначно соответствуют двоичные векторы из пространства $\{0,1\}^{r_j}$. Тогда, по каждому текущему номеру $\mathrm{Num}\,(i_1, i_2, \ldots, i_k)$ на выход выдаётся соответствующий ему блок $\{\varepsilon\} = \varepsilon_{r_j-1}, \ldots, \varepsilon_0$, состоящий из 0 и 1.

Рассмотрим примеры, иллюстрирующие общий метод, для $n = 8$, $k = 1, 2$.

Пример 1. $n = 8$, $k = 1$.

$$\left|\mathcal{R}_n(k)\right| = \frac{8!}{1!\,7!} = 8 = 2^3\,, \quad m = 0, \quad r_0 = 3\,.$$

Длина двоичного выхода (табл. 2, четвёртая колонка) равна 3.

Таблица 2. Алгоритм Бабкина, двоичный выход, $n = 8$, $k = 1$

Позиции s_1 и s_2 (i_1)	Номер $N(i_1)$	Двоичное представление	Случайный блок $\{\varepsilon\} = \varepsilon_{r_0-1}, \ldots, \varepsilon_0$
$\boldsymbol{s_1}s_2s_2s_2s_2s_2s_2s_2$	0	000	000
…	1	001	001
	2	010	010
$j = 0$	3	011	011
	4	100	100
	5	101	101
…	6	110	110
$s_2s_2s_2s_2s_2s_2s_2\boldsymbol{s_1}$	$7 = 2^{r_0} - 1$	111	111

Пример 2. $n = 8$, $k = 2$.

$$\left|\mathcal{R}_n(k)\right| = \frac{8!}{2!\,6!} = 28 = 2^4 + 2^3 + 2^2,$$

$$m = 2, \quad r_2 = 4, \quad r_1 = 3, \quad r_0 = 2\,.$$

Длина двоичного выхода (табл. 3, четвёртая колонка) равна 2, 3 и 4.

Обращаем внимание на то, что двоичный выход после нумерации по методу Бабкина и экстракции блока 0 и 1 (четвёртые колонки в табл. 2 и 3) содержит все двоичные векторы фиксированной длины ровно по одному разу.

Таблица 3. Алгоритм Бабкина, двоичный выход, $n = 8$, $k = 2$

Позиции s_1 и i_2, i_1, i_2	Номер $N(i_1, i_2)$	Двоичное представление	Случайный блок $\{\varepsilon\} = \varepsilon_{r_{j-1}}, \ldots, \varepsilon_0$
$\boldsymbol{s_1 s_1} s_2 s_2 s_2 s_2 s_2 s_2$	0	00000	00
...	1	00001	01
$j = 0$	2	00010	10
	$3 = 2^{r_0} - 1$	00011	11
	4	00100	100
	5	00101	101
	6	00110	110
$j = 1$	7	00111	111
	8	01000	000
	9	01001	001
	10	01010	010
	$11 = 2^{r_1} + 2^{r_0} - 1$	01011	011
	12	01100	1100
	13	01101	1101
	14	01110	1110
	15	01111	1111
	16	10000	0000
	17	10001	0001
$j = 2$	18	10010	0010
	19	10011	0011
	20	10100	0100
	21	10101	0101
	22	10110	0110
	23	10111	0111
	24	11000	1000
	25	11001	1001
	26	11010	1010
$s_2 s_2 s_2 s_2 s_2 s_2 \boldsymbol{s_1 s_1}$	$27 = 2^{r_2} + 2^{r_1} + 2^{r_0} - 1$	11011	1011

2.3. Алгоритм Бабкина, *m*-арный алфавит

Рассмотрим источник, который порождает символы из m-арного алфавита $A = \{s_1, \ldots, s_m\}$.

Пусть $\mathcal{R}_n(k_1, \ldots, k_m)$ — множество блоков длиной n, где имеется $k_1, \ldots, k_m$ символов $s_1, \ldots, s_m$, $k_1 + \ldots + k_m = n$. Всего таких блоков

$$\left|\mathcal{R}_n(k, \ldots, k_m)\right| = \frac{n!}{k_1! k_2! \ldots k_m!}\,.$$

В работе [11] для m-арного алфавита В.Ф. Бабкиным предложен алгоритм присваивания "на ходу" номера $0 \leqslant \mathrm{Num}\,(\ldots) \leqslant |\mathcal{R}_n(k_1, \ldots, k_m)| - 1$ конкретному блоку из множества $\mathcal{R}_n(k_1, \ldots, k_m)$.

Далее извлечение случайных битов из двоичного представления $\mathrm{Num}\,(\ldots)$ происходит аналогично случаю бинарного алфавита $A = \{s_1, s_2\}$. Соответствующая таблица становится богаче — может содержать двоичные выходы большей длины.

Отметим опять же, что при фиксированной длине двоичный выход алгоритма Бабкина в соответствующей таблице для m-арного алфавита будет также содержать в четвёртой колонке все двоичные векторы фиксированной длины ровно по одному разу. Этот факт является одним из главных моментов для доказательства в дальнейшем равновероятности двоичных последовательностей на выходе алгоритма Бабкина.

Алгоритм Бабкина для m-арного алфавита используется в дальнейшем для доказательства случайности битов, извлекаемых из траектории простой цепи Маркова порядка $r = 1$ с m состояниями $\{s_1, \ldots, s_m\}$. В работе [18] m-й алгоритм Бабкина использовался для генерации случайных последовательностей в квантовых генераторах случайных чисел, основанных на гомодинном детектировании — "флуктуациях вакуума".

При извлечении доказуемо случайных битов из интересного для нас практического случая цепи Маркова порядка $r \geqslant 2$ с двумя состояниями $\{s_1, s_2\}$, алгоритм для m-арного алфавита не понадобится — будет работать алгоритм Бабкина для бинарного алфавита.

2.4. Основной принцип доказательства равновероятности — разбиение исходного вероятностного пространства на классы эквивалентных (одинаково вероятных) последовательностей

Случайность описывает порядок посреди беспорядка, хаос — беспорядок посреди порядка
К.Р. Рао

Эпиграф носит эмоциональный оттенок и является скорее противоречивой игрой слов, чем математическим определением. Случайность имеет чёткое математическое определение. Случайность — в нашем случае истинная случайность последовательностей из 0 и 1, понимаемая как равновероятность и независимость появления в каждой позиции 0 и 1, представляет собой наивысшую степень беспорядка — непредсказуемости, а отнюдь не порядок среди беспорядка. Энтропия Шеннона для независимых испытаний является мерой беспорядка, для истинно случайной последовательности 0 и 1 энтропия имеет максимальное значение, равное единице в пересчёте на каждую позицию.

Прежде чем перейти к формальным доказательствам, приведём неформальные качественные соображения относительно извлечения случайности из исходных последовательностей.

Рассмотрим простой пример. Мы подбрасываем игральную кость с равновероятными исходами $\Omega = \{1, 2, \ldots, 6\}$, которые мы называем элементарными событиями, и извлекаем случайные биты $\varepsilon \in \{0, 1\}$ при появлении чётного или нечётного исходов соответственно. При этом, как нетрудно видеть, при одинаковой вероятности событий в чётном $\{2, 4, 6\}$ и нечётном $\{1, 3, 5\}$ подмножествах, получаем равновероятность случайных битов:

$$\Pr(\varepsilon = 0) = \Pr(\varepsilon = 1) = \frac{1}{2}\,.$$

Легко представить себе и более сложную конструкцию извлечения равновероятных случайных битов из наблюдений над элементарными событиями исходного вероятностного пространства.

Предположим, что всё вероятностное пространство $\Omega = \{\omega\}$ разбито на подмножества (классы) одинаково вероятных элементарных событий:

$$\Omega = \bigcup_i S_i, P(\omega) = P(\omega')\,, \text{ как только } \omega, \omega' \in S_i\,.$$

Если в каждом подмножестве (классе) S_i число элементарных событий, порождающих значение $\varepsilon = 0$, равно числу элементарных событий, порождающих значение $\varepsilon = 1$, то, очевидно, $\Pr(\varepsilon = 0) = \Pr(\varepsilon = 1)$. Подсчёт вероятностей $\Pr(\varepsilon = 0)$ и $\Pr(\varepsilon = 1)$ — это суммирование вероятностей элементарных событий по соответствующим подмножествам. Мы также можем говорить об

условной равновероятности в том смысле, что

$$\Pr\left(\varepsilon = 0 \,|\, \omega \in \Omega_\varepsilon\right) = \Pr\left(\varepsilon = 1 \,|\, \omega \in \Omega_\varepsilon\right) = \frac{1}{2}\,,$$

где Ω_ε — множество элементарных событий, порождающих случайные биты ε.

Принцип разбиения на классы одинаково вероятных элементарных событий используется для доказательства равновероятности выходных последовательностей.

Практически работающий алгоритм Бабкина обрабатывает входную последовательность блоками.

Предположим для примера, что на входе алгоритма имеется бернуллиевская последовательность из трёх блоков одинакового размера $n = 8$:

$$X = (X_1, X_2, X_3)\,.$$

Это одно из возможных элементарных событий исходного вероятностного пространства $\Omega = \{X\} = \{s_1, s_2\}^{24}$.

Обозначим через:

— $Y_i = \Psi(X_i)$ — двоичный выход алгоритма Бабкина от блока X_i, $|Y_i|$ — длина двоичного выхода, $i = \overline{1,3}$,

— $Y = Y_1 \,\|\, Y_2 \,\|\, Y_3 = \Psi(X_1) \,\|\, \Psi(X_2) \,\|\, \Psi(X_3)$ — полный выход алгоритма Бабкина от последовательности X в виде конкатенации отдельных выходов.

Для облегчения обозначений мы будем также записывать $Y = \Psi(X)$, $|Y|$ — длина полного выхода.

Рассмотрим полный двоичный выход $Y = (01011100)$, $|Y| = 8$.

Для подсчёта вероятности этого выхода мы должны просуммировать вероятности тех элементарных событий X, из которых получается $Y = (01011100)$.

Рассмотрим подмножество $S \subseteq \Omega = \{X = (X_1, X_2, X_3)\}$, где блоки (X_1, X_2, X_3) содержат ровно $k = 1, 2, 2$ событий s_1 соответственно.

Тем самым образуется класс S элементарных событий, где $X = (X_1, X_2, X_3)$ отличается от $X' = (X'_1, X'_2, X'_3)$ перестановкой внутри блоков, при этом, как нетрудно видеть, вероятности последовательностей X и X' одинаковы:

$$P_S(X) = P_S(X') = \left[P(s_1)\right]^5 \left[P(s_2)\right]^{24-5}.$$

Класс S одинаково вероятных последовательностей мы называем классом эквивалентности.

Может ли получиться выход $Y = (01011100)$, $|Y| = 8$ из последовательностей $X \in S$?

Исходя из рассмотрения четвёртых колонок табл. 2 и 3, мы видим, что:

— первый блок X_1 даёт на выходе $Y_1 = \Psi(X_1)$ с битовой длиной $|Y_1| = 3$,

— второй блок X_2 даёт на выходе $Y_2 = \Psi(X_2)$ с битовой длиной $|Y_2| = 2, 3, 4$,

— третий блок X_3 даёт на выходе $Y_3 = \Psi(X_3)$ с битовой длиной $|Y_3| = 2, 3, 4$,

при этом возможная длина $|Y| = |Y_1| + |Y_2| + |Y_3|$ меняется в пределах от 7 до 11.

Частичный двоичный выход $Y_i = \Psi(X_i)$ — это двоичный выход от номера X_i в алгоритме Бабкина, т.е. $Y_i = \Psi(\mathrm{Num}\,(X_i))$.

Ниже на рис. 1 представлено разбиение номеров последовательностей X_i по блокам. Размер каждого блока является степенью двойки. Длина двоичного выхода из каждого блока (штриховая и пунктирная линии) одинакова и не зависит от битового состава, причём выходные битовые строки длиной $|Y_i| = |Y'_i|$ пробегают все битовые комбинации 0 и 1 (см. табл. 2, 3).

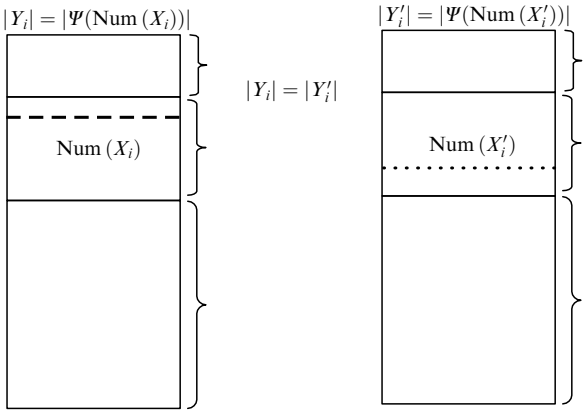

Рис. 1. Разбиение номеров последовательностей из одного класса эквивалентности по блокам.

Длина полного двоичного выхода $|Y| = 8$ может получиться как $|Y| = 3 + 2 + 3$ или как $|Y| = 3 + 3 + 2$, при этом конкретный двоичный выход $Y = (01011100)$ получается в классе S как конкатенация частичных двоичных выходов (см. табл. 2, 3)

$$Y_1 = 010 \,\|\, Y_2 = 11 \,\|\, Y_3 = 100$$

или

$$\widetilde{Y}_1 = 010 \,\|\, \widetilde{Y}_2 = 111 \,\|\, \widetilde{Y}_3 = 00,$$

т.е.

$$Y = (01011100) = 010 \,\|\, 11 \,\|\, 100 = 010 \,\|\, 111 \,\|\, 00\,.$$

Поскольку при фиксированной длине двоичный выход в правой колонке в табл. 2 и 3 содержит все двоичные векторы ровно по одному разу, то можно утверждать, что для $Y = (01011100)$ в классе S существуют ровно два прообраза — две последовательности X и $\widetilde{X}$, такие, что $\Psi(X) = \Psi(\widetilde{X}) = Y$.

Мы будем также говорить, что для $Y = (01011100)$ в классе S существуют ровно два допустимых разбиения конкретного выхода Y, а именно (Y_1, Y_2, Y_3) и $(\widetilde{Y}_1, \widetilde{Y}_2, \widetilde{Y}_3)$, для которых находятся соответствующие прообразы X и $\widetilde{X}$.

Множество допустимых разбиений Y для класса S обозначим через $\mathbb{Y}_S(Y)$, его мощность — через $|\mathbb{Y}_S(Y)|$, в данном случае $|\mathbb{Y}_S(Y)| = 2$.

Крайне важно заметить, что для любого другого двоичного выхода той же самой длины, например, $Y' = (11010011)$, также по построению алгоритма Бабкина мы получаем ровно две конкатенации частичных выходов:

$$Y'_1 = 110 \,\|\, Y'_2 = 10 \,\|\, Y'_3 = 011\,,$$

$$\widetilde{Y}'_1 = 110 \,\|\, \widetilde{Y}'_2 = 100 \,\|\, \widetilde{Y}'_3 = 11\,.$$

Этим конкатенациям соответствуют свои два прообраза из множества S.

Отсюда заключаем, что мощности множеств допустимых разбиений выходов $Y = (01011100)$ и $Y' = (11010011)$ одинаковы:

$$\left|\mathbb{Y}_S(Y)\right| = \left|\mathbb{Y}_S(Y')\right| = 2\,.$$

Соответствующий обобщающий вывод можно сделать и для остальных возможных длин $|Y| = 7 \div 11$ двоичного выхода алгоритма Бабкина.

А именно: для любых Y, Y' с совпадающей длиной $|Y| = |Y'|$ мощности множеств допустимых разбиений для класса S одинаковы:

$$\left|\mathbb{Y}_S(Y)\right| = \left|\mathbb{Y}_S(Y')\right|\,.$$

Нетрудно видеть, что подобные классы эквивалентности S, состоящие из одинаково вероятных последовательностей, можно построить при любом составе $k = k_1, k_2, k_3$, $0 \leqslant k_i \leqslant 8$, событий s_1 в блоках X_1, X_2, X_3. Тем самым мы получаем разбиение вероятностного пространства $\Omega = \{X = (X_1, X_2, X_3)\}$ на классы эквивалентности S, состоящие из одинаково вероятных последовательностей.

Отметим, что конкретный двоичный выход $Y = (01011100)$ может получиться для некоторой входной последовательности $X \in S'$, $S' \neq S$, т.е. в другом классе эквивалентности. Опять же можно утверждать, что для любых Y, Y' с совпадающей длиной $|Y| = |Y'|$ мощности множеств допустимых разбиений для класса S' одинаковы:

$$\left|\mathbb{Y}_{S'}(Y)\right| = \left|\mathbb{Y}_{S'}(Y')\right|\,.$$

Таким образом, для полных выходных последовательностей Y, Y' с совпадающей длиной $|Y| = |Y'|$ в каждом классе одинаково вероятных последовательностей существует одинаковое число прообразов — последовательностей X. Отсюда неформально можно заключить, что для Y, Y' вероятности должны быть равны: $P(Y) = P(Y')$.

Изложенные выше рассуждения служат иллюстрацией к доказательству равновероятности выходной двоичной последовательности для общего случая m-арного алфавита $A = \{s_1, \ldots, s_m\}$.

2.5. Доказательство равновероятности двоичной последовательности на выходе алгоритма Бабкина

Рассмотрим общий случай, когда источник порождает символы из m-арного алфавита $A = \{s_1, \ldots, s_m\}$.

Пусть на входе алгоритма Бабкина имеется последовательность X независимых испытаний из конечной вероятностной схемы с исходами $\{s_1, \ldots, s_m\}$ — это исходное вероятностное пространство. Вероятности $\{P(a_1), \ldots, P(a_m)\}$ неизвестны.

Ниже мы приведём доказательство равновероятности двоичной последовательности на выходе алгоритма Бабкина. В основу положим рассмотренную выше идею разбиения множества входных последовательностей на классы эквивалентности. Этот приём будет использоваться и далее, при рассмотрении на входе траекторий цепи Маркова.

Итак, практически работающий алгоритм Бабкина обрабатывает входную последовательность блоками. Не теряя общности, предположим, что на входе алгоритма имеется последовательность

$$X = (X_1, X_2, \ldots, X_M),\ X_1 \in \{s_1, \ldots, s_m\}^{n_1}, \ldots, X_M \in \{s_1, \ldots, s_m\}^{n_M}, \tag{1}$$

где M — количество обрабатываемых блоков, $n_1, \ldots, n_M$ — размеры обрабатываемых блоков.

Разобьём все возможные последовательности $X \in \{s_1, \ldots, s_m\}^{(n_1+\ldots+n_M)}$ на классы эквивалентности и используем G для обозначения множества классов.

Определение.

Две последовательности

$$X = (X_1, X_2, \ldots, X_M),\quad X' = (X'_1, X'_2, \ldots, X'_M)$$

принадлежат к одному классу эквивалентности S тогда и только тогда, когда блок X'_j является перестановкой блока X_i для любого $i = \overline{1, M}$.

Перестановку будем обозначать как

$$X'_i \equiv X_i\,.$$

Обратим внимание на то, что классу эквивалентности S отвечает некоторый определенный состав символов $\{s_1, \ldots, s_m\}$ в блоках $X_1, X_2, \ldots, X_M$.

А именно, для каждого блока X_i фиксируются числа $k_1^{(i)}, \ldots, k_m^{(i)}$, $k_1^{(i)} + \ldots + k_m^{(i)} = n_i$, где $k_j^{(i)}$ — число вхождений символа s_j в блок X_i.

Утверждение 3.

Любые две последовательности $X = (X_1, X_2, \ldots, X_M)$ и $X' = (X'_1, X'_2, \ldots, X'_M)$, принадлежащие одному классу эквивалентности S, имеют одинаковую вероятность:

$$P_S(X) = P_S(X')\,.$$

Доказательство легко следует из исходного предположения о том, что входная последовательность X является последовательностью независимых испытаний над конечной вероятностной схемой.

Таким образом, разбиение на классы эквивалентности является разбиением всего множества входных последовательностей на классы одинаково вероятных последовательностей.

Пусть входная последовательность $X \in S$ — некоторому классу эквивалентности.

Пусть $Y = \Psi(X) \in \{0,1\}^*$ — полный двоичный выход алгоритма Бабкина в виде конкатенации частичных выходов $Y_i = \Psi(X_i)$.

Здесь мы ввели обозначение $\{0,1\}^*$, подчёркивая неопределённость длины $|Y|$ выходной двоичной последовательности, зависящей от конкретного состава исходов $\{s_1, \ldots, s_m\}$ в блоках.

Для $Y \in \{0,1\}^*$ обозначим через B_Y множество последовательностей $X \in \{s_1, \ldots, s_m\}^{(n_1+\ldots+n_M)}$ таких, что $\Psi(X) = Y$. Множество B_Y является объединением всех прообразов по всем классам. Ясно, что могут существовать классы S с пустым множеством прообразов.

Утверждение 4.

Для любого класса $S \in G$ мощность множества $|S \cap B_{Y'}| = |S \cap B_Y|$ всякий раз, когда совпадают длины: $|Y'| = |Y|$.

Доказательство.

Пусть задан конкретный выход $Y \in \{0,1\}^*$ с длиной $|Y|$. Рассмотрим класс S. Он состоит из исходной последовательности блоков $X = (X_1, X_2, \ldots, X_M)$ и всех перестановок внутри блоков.

Сопоставим полному двоичному выходу $Y \in \{0,1\}^*$ разбиение на частичные двоичные выходы

$$Y_1, \ldots, Y_M, \quad |Y| = |Y_1| + |Y_2| + \ldots + |Y_M|,$$

такое, что конкатенация

$$Y_1 \| \ldots \| Y_M = Y.$$

Определим S_i как множество, состоящее из всех перестановок блока X_i, $i = \overline{1, M}$, и введём обозначение

$$S_i(Y_i) = \{X_i \in S_i : \Psi(X_i) = Y_i\}.$$

По построению алгоритма Бабкина (четвёртые колонки табл. 2, 3), при фиксированной длине $|Y_i|$ мощность $|S_i(Y_i)| = 1$ или $|S_i(Y_i)| = 0$, если длина $|Y_i|$ — не подходящая для множества S_i.

Рассмотрим $Y' \in \{0,1\}^*$, не совпадающий с Y, но имеющий ту же самую длину $|Y'| = |Y|$ и соответствующее разбиение:

$$Y'_1, \ldots, Y'_M, \ |Y'| = |Y'_1| + |Y'_2| + \ldots + |Y'_M|,$$
$$|Y'_i| = |Y_i|.$$

Опять же, по построению алгоритма Бабкина, мощность $|S_i(Y'_i)| = 1$ или $|S_i(Y_i)| = 0$.

Следовательно, ровно по одной последовательности $X_i, X'_i \in S_i$ (т.е. по одной из всех перестановок S_i) в алгоритме Бабкина дают частичные выходы Y_i и Y'_i или, вообще говоря, не дают, если длина $|Y_i|$ — не подходящая для множества S_i.

Следовательно, не для всякого разбиения $Y_1, Y_2, \ldots, Y_n$, такого, что конкатенация $Y_1 \| \ldots \| Y_M = Y$, возможно найти последовательность

$$X = (X_1, X_2, \ldots, X_M) \in S$$

такую, что $\Psi(X) = Y$.

Например, первый блок X_1 может оказаться скудным — содержащим, например, только пару исходов $\{s_1, s_2\}$, $k_1^{(1)} + k_2^{(1)} = n_1$. Тогда длина $|Y_1|$ двоичного выхода первого блока не может быть большой, что, вообще говоря, допустимо при другом разбиении.

Мы говорим что разбиение $Y_1, Y_2, \ldots, Y_M$ такое, что конкатенация $Y_1 \| \ldots \| Y_M = Y$, является допустимым для данного класса S, если $|S_i(Y_i)| = 1$ для всех $i = \overline{1, M}$ и обозначаем $\mathbb{Y}_S(Y)$ — множество допустимых разбиений.

Таким образом, нас интересуют разбиения $(Y_1, Y_2, \ldots, Y_M) \in \mathbb{Y}_S(Y)$ — множеству допустимых разбиений.

Проведённые выше рассуждения о конструктивном построении алгоритма Бабкина, позволяют заключить, что мощность $|\mathbb{Y}_S(Y)|$ зависит от класса S и от длины $|Y|$, но никак ни от битового состава Y, т.е.

$$|\mathbb{Y}_S(Y')| = |\mathbb{Y}_S(Y)|,$$

как только $|Y'| = |Y|$.

Отсюда следует, что

$$|S \cap B_Y| = \sum_{\substack{Y_1, Y_2, \ldots, Y_M: \\ |Y_1| + |Y_2| + \ldots + |Y_M| = |Y|}} \prod_{i=1}^{n} |S_i(Y_i)| =$$
$$= \sum_{(Y_1, Y_2, \ldots, Y_M) \in \mathbb{Y}_S(Y)} 1 = |\mathbb{Y}_S(Y)|$$

— мощности множества допустимых разбиений.

Как было установлено выше, мощность $|\mathbb{Y}_S(Y)|$ зависит только от класса S и от длины $|Y|$.

Тогда для Y', $|Y'| = |Y|$, имеем

$$|S \cap B_{Y'}| = \sum_{\substack{Y'_1, Y'_2, \ldots, Y'_M: \\ |Y'_1| + |Y'_2| + \ldots + |Y'_M| = |Y'|}} \prod_{i=1}^{n} |S_i(Y'_i)| =$$
$$= \sum_{(Y'_1, Y'_2, \ldots, Y'_M) \in |\mathbb{Y}_S(Y')|} 1 = |\mathbb{Y}_S(Y')| = |\mathbb{Y}_S(Y)|.$$

Следовательно, $|S \cap B_{Y'}| = |S \cap B_Y|$ всякий раз, когда $|Y'| = |Y|$.

Утверждение 4 доказано.

В том случае, когда для данного класса S прообразы отсутствуют при любом разбиении $Y_1, Y_2, \ldots, Y_M$, т.е. $S_i(Y_i) = \{X_i \in S_i : \Psi(X_i) = Y_i\} = \emptyset$ для всех $i = \overline{1, M}$, тогда $|\mathbb{Y}_S(Y)| = 0$ и, следовательно, $|S \cap B_Y| = |S \cap B_{Y'}| = 0$.

Сформулируем теперь теорему о равновероятности двоичного выхода алгоритма Бабкина.

Теорема 1.

Пусть последовательность $X = (X_1, X_2, \ldots, X_M)$ независимых испытаний из конечной вероятностной схемы с исходами $\{s_1, \ldots, s_m\}$ используется в качестве входных данных для алгоритма Бабкина.

Тогда двоичный выход $Y \in \{0,1\}^\ell$, получающийся при любом возможном ℓ, имеет вероятность

$$P(Y) = 2^{-\ell}.$$

Доказательство.

Рассмотрим класс S, отвечающий некоторому составу символов $\{s_1, \ldots, s_m\}$ в блоках $X_1, X_2, \ldots, X_M$.

Выше, в Утверждении 3 было установлено, что для любых $X, X' \in S$ вероятность $P_S(X) = P_S(X')$.

Тогда для $Y \in \{0,1\}^\ell$ имеем

$$P(Y) = P(X \in B_Y) =$$
$$= \sum_{S \in G} P(X \in S)\, P(X \in B_Y \mid X \in S) =$$
$$= \sum_{S \in G} P(X \in S)\, \frac{P(X \in S \cap B_Y)}{P(X \in S)} =$$
$$= \sum_{S \in G} P(X \in S)\, \frac{P_S(X)\, |S \cap B_Y|}{P_S(X)\, |S|} =$$
$$= \sum_{S \in G} P(X \in S)\, \frac{|S \cap B_Y|}{|S|}.$$

Рассмотрим теперь любой другой выход $Y' \in \{0,1\}^\ell$. При совпадающих длинах $|Y'| = |Y|$ из Утверждения 4 следует, что совпадают и мощности прообразов:

$$|S \cap B_{Y'}| = |S \cap B_Y|.$$

Отсюда немедленно заключаем, что

$$P(Y) = P(Y').$$

Поскольку это равенство выполняется для любых $Y, Y' \in \{0,1\}^\ell$, то отсюда следует, что $P(Y) = 2^{-\ell}$.

Теорема 1 доказана.

Сделаем комментарий.

1. Как мы отмечали выше, может оказаться так, что в некоторых классах S не найдётся последовательности $X = (X_1, X_2, \ldots, X_M)$, которая порождает Y заданной

длины $|Y| = \ell$, что, вообще говоря, как бы сужает исходное вероятностное пространство. Таким образом, мы приходим к тому, что выше, по сути дела, обосновывается равновероятный выбор Y при условии наблюдения (фиксации) длины $|Y| = \ell$.

2. Доказательство равновероятности двоичного выхода основывается на построении классов эквивалентности — классов одинаково вероятных последовательностей. При этом предполагается, что при реализации алгоритма Бабкина для другой последовательности $X' = (X'_1, X'_2, \ldots, X'_M)$ в классе эквивалентности не меняется порядок обработки блоков:

$$(Y'_1, Y'_2, \ldots, Y'_M) = \big(\Psi(X'_1), \Psi(X'_2), \ldots, \Psi(X'_M)\big)\,.$$

Для независимой последовательности это предположение является естественным, поскольку блоки обрабатываются в едином потоке поступления символов.

Для цепей Маркова, рассмотренных ниже, сохранение порядка обработки блоков в классе эквивалентности является ключевым для доказательства равновероятности двоичного выхода алгоритма Бабкина. Сохранение порядка обработки блоков в классе эквивалентности порождает особенность реализации алгоритма считывания блоков на обработку, при которой они встают в очередь.

3. Цепь Маркова

Прежде чем дать подробное объяснение, как извлекается доказуемо истинная случайность из коррелированных последовательностей — траекторий цепи Маркова с конечной глубиной зависимости в предыстории измерений, приведём качественные пояснения, как можно свести задачу к предыдущему случаю независимых измерений — бернуллиевских последовательностей.

Общая идея также состоит в разбиении различных траекторий цепи Маркова на классы эквивалентности траекторий, которые, как целое, одинаково вероятны. Если это удаётся сделать, то далее также можно провести нумерацию траекторий в каждом классе одинаково вероятных траекторий, по аналогии с тем, как это было сделано выше с нумераций бернуллиевских последовательностей в одном классе одинаково вероятных последовательностей. Далее каждому номеру сопоставляется блок истинно случайных 0 и 1, затем блоки конкатенируются.

Главная проблема состоит в том, как разбить на классы эквивалентности различные траектории цепи Маркова, отвечающие коррелированным последовательностям результатов измерений.

Оказывается, что каждой траектории можно сопоставить замкнутый граф — граф Эйлера. Вершинам отвечают состояния, неформально говоря, результат измерения вместе с предисторией. Рёбрам отвечают переходы между состояниями цепи Маркова.

Как будет показано ниже, к траекториям в одном классе одинаково вероятных траекторий относятся такие траектории цепи Маркова, которым отвечают графы Эйлера, отличающиеся друг от друга порядком обхода рёбер в графе.

Центральным местом является то, что допускается только такой порядок обхода рёбер замкнутого графа, который не затрагивает ребро, соединяющее конец и начало траектории цепи Маркова.

После разбиения на классы одинаково вероятных траекторий цепи Маркова, задача экстракции истинно случайных последовательностей сводится к задаче экстракции случайных последовательностей из независимых испытаний, решение которой было приведено выше.

Перейдём к подробному выводу. Далее рассматриваются траектории цепи Маркова — элементарные события

$$X = x_1 x_2 \ldots x_N\,,$$

где $x_i \in A = \{s_1, \ldots, s_m\}$ — множеству состояний цепи. Задаётся начальное распределение

$$P(s_1), \ldots, P(s_m), \quad \sum_{i=1}^{m} P(s_i) = 1$$

и матрица переходных вероятностей размера $m \times m$:

$$\big\|P(s_j \,|\, s_i)\big\|, \quad i, j = \overline{1, m}, \quad \sum_{j=1}^{m} P(s_j \,|\, s_i) = 1\,.$$

Вероятность элементарного события (траектории) X определяется как

$$P(X) = P(x_1 x_2 \ldots x_N) = P(x_1) \prod_{i=1}^{N-1} P(x_{i+1} \,|\, x_i)\,.$$

Матрица переходных (условных) вероятностей содержит в условии зависимость только от одного предыдущего состояния. В этом случае мы говорим о стационарной цепи Маркова порядка $r = 1$. Строго говоря, для стационарности цепи должно ещё выполняться определённое условие для начального распределения, но оно для нас несущественно.

Далее для цепи Маркова с m состояниями, порядка $r = 1$, мы опишем алгоритм получения доказуемо случайной двоичной последовательности и распространим его на интересующий нас практический случай цепи Маркова с двумя состояниями $\{s_1, s_2\}$, порядка $r \geqslant 2$.

3.1. Построение классов эквивалентности, связь с эйлеровыми графами

Для доказательства равновероятности выходных последовательностей требуется разбиение траекторий цепей Маркова на классы с одинаковой вероятностью. Интуитивно понятный способ разбиения основан на некоторых фактах из теории графов.

Удивительным образом задача о разбиении на классы эквивалентности марковских цепочек (результатов измерений) связана с эйлеровыми графами, которые возникли в широко известной задаче об однократном обходе кенигсбергских мостов — в задаче, которая была решена Леонардом Эйлером (см., например, [19])[3].

Итак, ближайшая цель — построение классов эквивалентности (одинаково вероятных) траекторий цепи Маркова.

Для траектории цепи Маркова $X = x_1 x_2 \ldots x_N$ генерируется совокупность π-последовательностей

$$\pi(X) = \big[\pi_1(X), \pi_2(X), \ldots, \pi_m(X)\big]\,,$$

[3] Напомним, что однократный обход кенигсбергских мостов оказался невозможным, что связано с конкретной конфигурацией соединений мостов между собой.

где $\pi_i(X)$ — подпоследовательность состояний из $X = x_1x_2\ldots x_N$, следующих за состоянием s_i:

$$\pi_i(X) = \{x_{j+1} : x_j = s_i,\ 1 \leqslant j \leqslant N\}\,.$$

Например, для $X = s_1\boldsymbol{s_4}s_2s_1\boldsymbol{s_3}s_2s_3s_1\boldsymbol{s_1s_2}s_3s_4s_1$ получаем π-последовательности

$$\pi(X) = \big[\pi_1(X) = (\boldsymbol{s_4s_3s_1s_2}), \pi_2(X) = (s_1s_3s_3),$$
$$\pi_3(X) = (s_2s_1s_4), \pi_4(X) = (s_2s_1)\big]\,.$$

Утверждение 5.

Последовательность X однозначно определяется через x_1 и $\pi(X)$.

Смысл Утверждения 5 состоит в том, что если X — уже траектория цепи Маркова, а мы её не знаем, то через начальное состояние x_1 и $\pi(X) = [\pi_1(X), \pi_2(X), \ldots, \pi_m(X)]$ траектория X восстанавливается однозначно [17].

Мы обозначаем $Y \equiv X$, если Y есть любая перестановка X, и обозначаем $Y \overset{\bullet}{\equiv} X$, если Y есть перестановка X с фиксированным хвостом (с фиксированным последним элементом).

Например:

$$s_1s_2s_2s_3 \equiv s_3s_2s_2s_1\,,$$
$$s_2s_3s_2\boldsymbol{s_1} \overset{\bullet}{\equiv} s_3s_2s_2\boldsymbol{s_1}\,.$$

Утверждение 6.

Две траектории цепи Маркова $X = x_1x_2\ldots x_N$ и $X' = x'_1x'_2\ldots x'_N$ при совпадающем начале $x_1 = x'_1$ имеют одинаковую вероятность, если $\pi_i(X') \equiv \pi_i(X)$ для всех $1 \leqslant i \leqslant m$.

Доказательство.

Заметим, что вероятность

$$P(X) = P(x_1)P(x_2\,|\,x_1)\ldots P(x_N\,|\,x_{N-1}) =$$
$$= P(x_1)\prod_{i=1}^{m}\prod_{s_j\in\pi_i(X)} P(s_j\,|\,s_i)\,,$$

вероятность

$$P(X') = P(x'_1)\prod_{i=1}^{m}\prod_{s_j\in\pi_i(X')} P(s_j\,|\,s_i)\,.$$

Если $P(x_1) = P(x'_1)$ и $\pi_i(X') \equiv \pi_i(X)$ для всех $1 \leqslant i \leqslant m$, то, переставляя члены в $\pi_i(X)$, нетрудно получить, что $P(X') = P(X)$.

Утверждение 6 доказано.

Таким образом, при $x_1 = x'_1$ перестановка символов внутри π-последовательностей: $\pi_i(X) \equiv \pi_i(X')$ для всех $1 \leqslant i \leqslant m$ не меняет вероятности траектории цепи Маркова, однако после перестановки символов π-последовательности должны соответствовать траектории цепи Маркова. В некоторых случаях после перестановки символов внутри π-последовательностей невозможно построить траекторию цепи Маркова.

Вопрос о том, какие перестановки являются допустимыми при построении класса одинаково вероятных траекторий, является одним из ключевых в работе [17]. Он решается с помощью следующего Утверждения.

Утверждение 7 (Допустимые перестановки).

Пусть даны:

1) *траектория цепи Маркова $X = x_1x_2\ldots x_N$ с последним состоянием $x_N = s_\chi$,*

2) π-последовательности $\pi(X) = [\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)]$,

3) совокупность последовательностей $[\Lambda_1, \ldots, \Lambda_\chi, \ldots, \Lambda_m]$ такая, что

$\Lambda_\chi \equiv \pi_\chi(X)$ — любая перестановка, s_χ — последнее состояние в X,

$\Lambda_i \overset{\bullet}{\equiv} \pi_i(X)$, $i \neq \chi$, — перестановка с фиксированным хвостом.

Тогда существует траектория цепи Маркова $X' = x'_1x'_2\ldots x'_N$ с начальным состоянием $x'_1 = x_1$, конечным состоянием $x'_N = x_N$ и π-последовательностями $\pi(X') = [\Lambda_1, \Lambda_2, \ldots, \Lambda_m]$.

Доказательство этого Утверждения в [17] весьма объёмно, использует ряд промежуточных результатов.

Приведём интуитивно понятное доказательство этого Утверждения с некоторыми комментариями.

Сопоставим траектории цепи Маркова ориентированный граф. Вершинами графа являются состояния цепи, помеченными рёбрами — переходы от состояния к состоянию в соответствии с траекторией цепи Маркова.

Пусть дана траектория цепи Маркова с числом состояний $m = 4$, длиной $N = 9$:

$$X = s_1s_3s_1s_2s_4s_1s_2s_1s_3s_2\,,$$

где последнее состояние $s_\chi = s_2$, а π-последовательности равны

$$\pi(X) = \big[\pi_1 = (s_3s_\chi s_\chi s_3), \pi_\chi = (s_4s_1), \pi_3 = (s_1s_\chi), \pi_4 = (s_1)\big]\,.$$

Введём фиктивное состояние s_0, предшествующее первому элементу $x_1 = s_1$. Замкнём граф ребром, исходящим из последнего элемента s_χ и входящим в s_0. Замыкание представим в виде ребра, обозначенного пунктирной линией.

Представим новую траекторию в виде

$$X^* = s_0 \xrightarrow{1} s_1 \xrightarrow{2} s_3 \xrightarrow{3} s_1 \xrightarrow{4} s_\chi \xrightarrow{5} s_4 \xrightarrow{6} s_1 \xrightarrow{7} s_\chi \xrightarrow{8} s_1 \xrightarrow{9} s_3 \xrightarrow{10} s_\chi \xrightarrow{11} s_0\,.$$

Очевидно, что имеет место взаимно однозначное соответствие исходной траектории цепи Маркова X и траектории X^*.

Соответствующий граф изобразим на рис. 2.

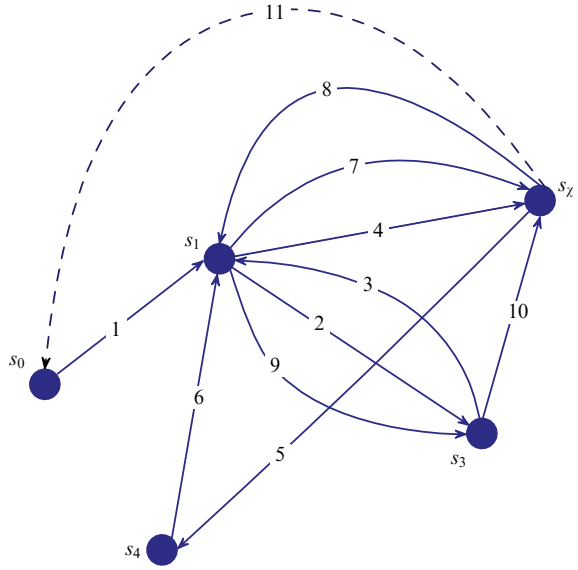

Рис. 2. Ориентированный граф, отвечающий траектории X^*.

Каждая вершина графа имеет чётную степень — число входящих и выходящих рёбер в каждую вершину одинаково. Тогда имеем эйлеров граф. Стартуя с s_0, можно осуществить полный обход графа и вернуться в состояние s_0, проходя каждое ребро только один раз.

Траекториям X^*, равно как и траекториям цепи Маркова X, отвечает полный обход соответствующего графа.

Траектория X^* имеет "расширенные" π-последовательности по сравнению с траекторией цепи Маркова X:

$$\pi(X) = \left[\pi_1 = (s_3 s_\chi s_\chi s_3), \pi_\chi = (s_4 s_1), \pi_3 = (s_1 s_\chi), \pi_4 = (s_1)\right],$$

$$\pi(X^*) = \left[\pi_0^* = (s_1), \pi_1^* = (s_3 s_\chi s_\chi s_3), \pi_\chi^* = (s_4 s_1 s_0), \pi_3^* = (s_1 s_\chi), \pi_4^* = (s_1)\right].$$

Не принимая во внимание несущественный блок $\pi_0^* = (s_1)$, видно, что основное отличие состоит в блоке $\pi_\chi^* = (s_4 s_1 s_0)$, отвечающем последнему элементу цепи χ. В этом блоке добавляется замыкающее состояние s_0.

Отсюда нетрудно видеть, что для выполнения Утверждения 7 достаточно показать существование новой траектории — полного обхода графа — при какой-либо транспозиции в новых блоках π_i^*, не затрагивающей последние состояния в блоках π_i^*. В исходном блоке $\pi_\chi = (s_4 s_1)$ эта транспозиция уже может затрагивать последнее состояние блока s_1. Двигаясь последовательно по транспозициям, можно перейти к любым перестановкам в π-последовательностях, удовлетворяющим условиям Утверждения 7.

Ясно, что если после допустимой транспозиции (в каком-либо блоке π_i^*) возможен полный обход графа, то тем самым показывается существование соответствующей траектории цепи Маркова.

При построении рёбер графа осуществляется движение между блоками π_i^*. Направление на следующий блок указывает соответствующее текущее состояние в блоке. Как только оно пройдено — оно вычёркивается из состояний блока.

Если при транспозиции не трогать последние состояния в блоках π_i^*, то при построении новой траектории (движении между блоками) последний элемент в блоке будет вычеркнут только тогда, когда в этот блок уже не будет нового захода, а дальнейшее движение будет происходить по оставшимся блокам, и так до самого конца до исчерпания всех состояний. Тем самым становится возможным построение полного обхода соответствующего графа.

Это относится и к блоку $\pi_\chi^* = (s_4 s_1 s_0)$, где последним элементом (в блоке) будет s_0. Следовательно, транспозиция, затрагивающая предпоследний элемент в блоке $\pi_\chi^* = (s_4 s_1 s_0)$, возможна. А это означает что возможна любая транспозиция или любая перестановка в блоке $\pi_\chi(X)$ исходной траектории X.

Проиллюстрируем построение траекторий на примере

$$X^* = s_0 \overset{1}{\to} s_1 \overset{2}{\to} s_3 \overset{3}{\to} s_1 \overset{4}{\to} s_\chi \overset{5}{\to} s_4 \overset{6}{\to} s_1 \overset{7}{\to} s_\chi \overset{8}{\to} s_1 \overset{9}{\to} s_3 \overset{10}{\to} s_\chi \overset{11}{\to} s_0 .$$

Возьмём *допустимую* транспозицию в блоке $\pi_1^* = (s_3 s_\chi s_\chi s_3) \to \pi_1^{**} = (s_\chi s_3 s_\chi s_3)$. Тогда

$$\pi(X^{**}) = \left[\pi_0^{**} = (s_1), \pi_1^{**} = (s_\chi s_3 s_\chi s_3), \pi_\chi^{**} = (s_4 s_1 s_0), \pi_3^{**} = (s_1 s_\chi), \pi_4^{**} = (s_1)\right],$$

$$X^{**} = s_0 \overset{1}{\to} s_1 \overset{2}{\to} s_\chi \overset{3}{\to} s_4 \overset{4}{\to} s_1 \overset{5}{\to} s_3 \overset{6}{\to} s_1 \overset{7}{\to} s_\chi \overset{8}{\to} s_1 \overset{9}{\to} s_3 \overset{10}{\to} s_\chi \overset{11}{\to} s_0.$$

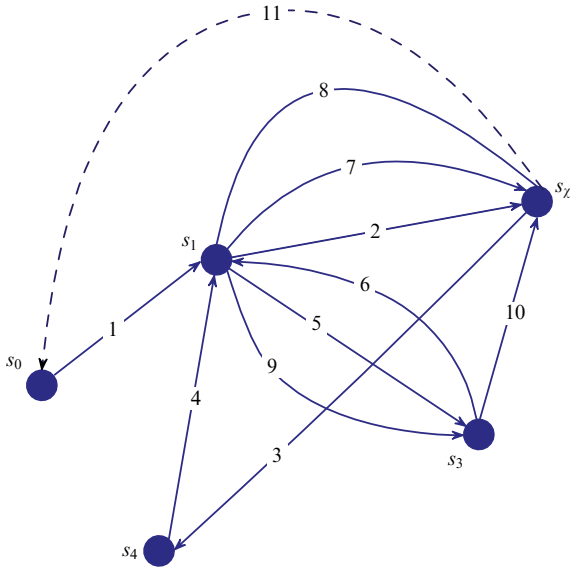

Рис. 3. Ориентированный граф, отвечающий траектории X^{**}.

Заметим, что траектория X^{**} — это новый полный обход эйлерова графа.

Возьмём *недопустимую* транспозицию в блоке $\pi_3^* = (s_1 s_\chi) \to \pi_3^{***} = (s_\chi s_1)$. Тогда

$$\pi(X^{***}) = \left[\pi_0^{***} = (s_1), \pi_1^{***} = (s_3 s_\chi s_\chi s_3), \pi_\chi^{***} = (s_1 s_4 s_0), \pi_3^{***} = (s_\chi s_1), \pi_4^{***} = (s_1)\right],$$

$$X^{***} = s_0 \overset{1}{\to} s_1 \overset{2}{\to} s_3 \overset{3}{\to} s_\chi \overset{4}{\to} s_1 \overset{5}{\to} s_\chi \overset{6}{\to} s_4 \overset{7}{\to} s_1 \overset{8}{\to} s_\chi \overset{9}{\to} s_0 \overset{10}{\to} ? .$$

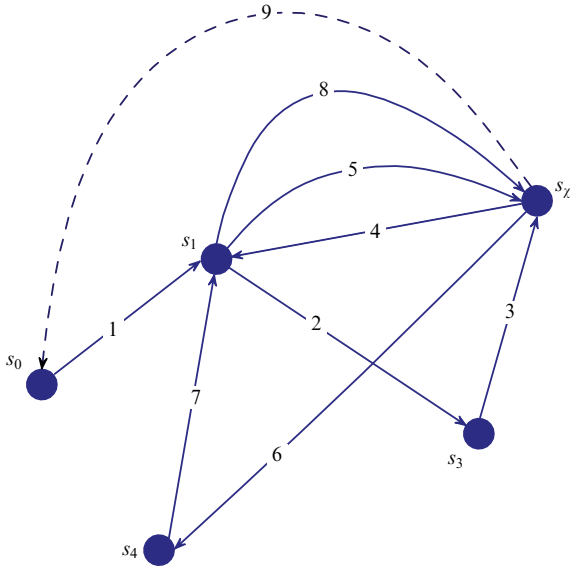

Рис. 4. Ориентированный граф, отвечающий траектории X^{***}.

Происходит обрыв траектории на 9-м шаге. На 9-м шаге до исчерпания состояния s_3 в блоке $\pi_1^{***} = (* * * s_3)$ и s_1 в блоке $\pi_3^{***} = (* s_1)$ получаем возврат в блок $\pi_0^{***} = (s_1)$, где уже имеется запрет на движение к состоянию s_1.

Полученное Утверждение 7 позволяет разбить все возможные траектории цепи Маркова $X \in \{s_1, s_2, \ldots, s_m\}^N$ на классы эквивалентности (одинаково вероятных траекторий).

А именно, рассмотрим некоторую траекторию цепи Маркова $X = x_1x_2\ldots x_N$ как задающую класс S и включим $X' = x'_1x'_2\ldots x'_N$ в класс S, если:

1) $x'_1 = x_1$ и $x'_N = x_N = s_\chi$ для некоторого χ — начало и конец траекторий X и X' одинаковы,

2) $\pi_\chi(X') \equiv \pi_\chi(X)$ — любая перестановка,

3) $\pi_i(X') \overset{\bullet}{\equiv} \pi_i(X)$, $i \neq \chi$, — перестановка с фиксированным хвостом.

В соответствии с Утверждением 7 для таких π-последовательностей существуют траектории цепи Маркова. Из Утверждения 6 следует, что они одинаково вероятны:

$$P_S(X') = P_S(X)\,.$$

3.2. Алгоритм А: экстракция случайных битов, требующая большой памяти

Ниже будет рассмотрен Алгоритм А извлечения случайных битов, требующий хранения в памяти всех π-последовательностей траектории цепи Маркова.

3.2.1. Описание Алгоритма А

Вход: траектория цепи Маркова $X = x_1x_2\ldots x_N$, $x_i \in \{s_1, s_2, \ldots, s_m\}$.

Выход: битовая последовательность $Y = \Psi(X) \in \{0,1\}^*$.

Алгоритм А:

• формирует π-последовательности $\pi(X) = \{\pi_1(X), \pi_2(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)\}$, $s_\chi = x_N$ — последний элемент цепи,

• для всех $i \neq \chi$ берётся блок $\pi_i(X)$ без последнего элемента блока: $\pi_i(X)^{|\pi_i(X)|-1}$,

• для всех $i \neq \chi$ к блокам $\pi_i(X)^{|\pi_i(X)|-1}$ применяется m-арный алгоритм Бабкина: $Y_i = \Psi(\pi_i(X)^{|\pi_i(X)|-1})$,

• блок $\pi_\chi(X)$ используется целиком: $Y_\chi = \Psi(\pi_\chi(X))$,

• частичные двоичные выходы конкатенируются:

$$Y = \Psi(X) = \Psi\big(\pi_1(X)^{|\pi_1(X)|-1}\big) \,\|\, \Psi\big(\pi_2(X)^{|\pi_2(X)|-1}\big) \,\|\, \ldots$$
$$\ldots \,\|\, \Psi\big(\pi_\chi(X)\big) \,\|\, \ldots \,\|\, \Psi\big(\pi_m(X)^{|\pi_m(X)|-1}\big)\,.$$

3.2.2. Равновероятность двоичного выхода

Теорема 2 (Алгоритм А).

Пусть траектория цепи Маркова $X = x_1x_2\ldots x_N$, $x_i \in \{s_1, s_2, \ldots, s_m\}$, используется в качестве входных данных для Алгоритма А, $\Psi(\ldots)$ — двоичный выход m-арного алгоритма Бабкина,

$$Y = \Psi(X) = \Psi\big(\pi_1(X)^{|\pi_1(X)|-1}\big) \,\|\, \Psi\big(\pi_2(X)^{|\pi_2(X)|-1}\big) \,\|\, \ldots$$
$$\ldots \,\|\, \Psi\big(\pi_\chi(X)\big) \,\|\, \ldots \,\|\, \Psi\big(\pi_m(X)^{|\pi_m(X)|-1}\big)\,.$$

Тогда двоичный выход $Y \in \{0,1\}^\ell$, получающийся при некотором ℓ, имеет вероятность

$$P(Y) = 2^{-\ell}\,.$$

Доказательство.

Ниже мы дадим доказательство Теоремы 2, полученное в [17], добавляя некоторые полезные уточнения и изменения.

Для любой траектории цепи Маркова имеем однозначное соответствие:

$$X = x_1x_2\ldots s_\chi \Longleftrightarrow \pi(X) = \big\{\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)\big\}\,. \tag{2}$$

Все траектории цепи Маркова разбиваются на классы эквивалентности (одинаково вероятных траекторий) $S \in G$. Траектории X' и X принадлежат одному классу S, если

1) $x'_1 = x_1$, $x'_N = s_\chi$,

2) $\pi(X') = \big\{\pi_1(X') \overset{\bullet}{\equiv} \pi_1(X), \ldots, \pi_\chi(X') \equiv$
$\equiv \pi_\chi(X), \ldots, \pi_m(X') \overset{\bullet}{\equiv} \pi_m(X)\big\}$.

Из (2) и равенства вероятностей траекторий

$$P_S(X') = P_S(X)$$

следует равенство вероятностей π-последовательностей:

$$P_S\big(\pi_1(X'), \ldots, \pi_\chi(X'), \ldots, \pi_m(X')\big) =$$
$$= P_S\big(\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)\big)\,. \tag{3}$$

Двоичный выход алгоритма Бабкина для Алгоритма А есть

$$Y = \Psi(X) = \Psi\big(\pi_1(X)^{|\pi_1(X)|-1}\big) \,\|\, \ldots \,\|\, \Psi\big(\pi_\chi(X)\big) \,\|\, \ldots$$
$$\ldots \,\|\, \Psi\big(\pi_m(X)^{|\pi_m(X)|-1}\big) = Y_1 \,\|\, \ldots \,\|\, Y_m\,.$$

Блоки

$$\pi_1(X)^{|\pi_1(X)|-1}, \ldots, \pi_\chi(X), \ldots, \pi_m(X)^{|\pi_m(X)|-1}$$

имеют длины $n_1, \ldots, n_\chi, \ldots, n_m$ и некоторый определённый состав символов $\{s_1, \ldots, s_m\}$ в блоках.

В таком представлении реализация алгоритма Бабкина аналогична реализации алгоритма Бабкина для независимого источника (1) при числе блоков $M = m$ и последовательной обработке теперь уже блоков

$$\pi_1(X)^{|\pi_1(X)|-1}, \ldots, \pi_\chi(X), \ldots, \pi_m(X)^{|\pi_m(X)|-1}\,.$$

Отличие состоит в том, что сначала надо дождаться полной реализации цепи Маркова $X = x_1x_2\ldots x_N$, сформировать $\pi_1(X), \ldots, \pi_\chi(X), \ldots, \pi_m(X)$ и затем, перед применением алгоритма Бабкина, исключить крайний элемент во всех блоках $\pi_i(X)$, кроме $\pi_\chi(X)$, где χ отвечает последнему элементу траектории: $x_N = s_\chi$.

Обозначим, как и в случае независимого источника, через B_Y множество траекторий цепи Маркова $X = x_1x_2\ldots x_N$ таких, что $\Psi(X) = Y$.

Пусть для данного класса эквивалентности S у нас есть допустимое разбиение $Y_1, Y_2, \ldots, Y_m$ такое, что

$$Y = Y_1 \,\|\, \ldots \,\|\, Y_m = \Psi\big(\pi_1(X)^{|\pi_1(X)|-1}\big) \,\|\, \ldots$$
$$\ldots \,\|\, \Psi\big(\pi_\chi(X)\big) \,\|\, \ldots \,\|\, \Psi\big(\pi_m(X)^{|\pi_m(X)|-1}\big)\,.$$

Нетрудно видеть, что то, что мы включаем в класс эквивалентности перестановки не полного множества, не отменяет конструктивного свойства алгоритма Бабкина: ровно по одной последовательности $\pi_i(X)^{|\pi_i(X)|-1}$ или $\pi_i(X')^{|\pi_i(X')|-1}$ из класса эквивалентности дают Y_i или Y'_i всякий раз, когда $|Y_i| = |Y'_i|$. Отсюда легко следует основное соотношение о равенстве мощностей прообразов $|S \cap B_Y| = |S \cap B_{Y'}|$.

Далее, с использованием одинаковой вероятности π-последовательностей, принадлежащих одному классу эквивалентности S (3), доказательство Теоремы 2 легко завершается по аналогии с доказательством Теоремы 1 для независимого источника.

Теорема 2 доказана.

3.3. Алгоритм B: экстракция случайных битов "на ходу"

С использованием Алгоритма A из входной траектории цепи Маркова $X = x_1x_2\ldots x_N$ можно генерировать равновероятные двоичные последовательности.

Тем не менее Алгоритм A имеет определённые недостатки:

— вся входная последовательность должна храниться,

— вход не может быть потоком или бесконечно длинным, потому что никакие выходные случайные биты 0 и 1 не могут быть сгенерированы до тех пор, пока вся входная траектория цеми Маркова не будет получена,

— Алгоритм A не вычислим в ожидаемое линейное время.

При практическом использовании оказывается эффективным Алгоритм B — алгоритм генерации случайных битов 0 и 1 "на ходу". Данный алгоритм не требует большой памяти и не требует хранения всей траектории, а выдает случайные 0 и 1 по мере поступления состояний цепи Маркова.

3.3.1. Описание Алгоритма B

Вход: траектория цепи Маркова $X = x_1x_2\ldots x_N$, $x_i \in \{s_1, s_2, \ldots, s_m\}$.

Параметр Алгоритма B: *размер окна* ϖ. *Окно нужно, чтобы вырезать последовательные блоки из* $\pi_i(X)$.

Выход: битовая последовательность $Y = \Psi(X) \in \{0,1\}^*$.

Алгоритм B:

• распараллеливает текущие состояния траектории цепи Маркова на текущие π-последовательности $\pi_1(X), \ldots, \pi_m(X)$, добавляя следующее состояние s_j в последовательность $\pi_i(X)$, только если перед s_j было состояние s_i,

• если в последовательности $\pi_i(X)$ набрался текущий блок F_{ik}, $k = 1, 2, \ldots$, размера ϖ, тогда он:

— сразу отправляется для преобразования $\Psi(F_{ik})$, если последний элемент в F_{ik} равен s_i,

— если последний элемент в F_{ik} не равен s_i, то блок F_{ik} ждёт отправки на обработку до тех пор, пока в цепи Маркова не появится s_i,

— блок F_{ik} вообще не отправляется на обработку, если ему не удалось дождаться появления s_i,

• частичные двоичные выходы по блокам конкатенируются:

$$Y = \Psi(F_{i_1j_1}) \parallel \Psi(F_{i_2j_2}) \parallel \ldots \parallel \Psi(F_{i_Lj_L})\,.$$

Здесь $i_1j_1, i_2j_2, \ldots, i_Lj_L$ — номера блоков из $\pi_{i_1}(X)$, $\pi_{i_2}(X), \ldots, \pi_{i_L}(X)$, последовательно поступающих на обработку.

Мы можем говорить, что наполненные блоки в параллельных π-последовательностях $\pi_1(X), \ldots, \pi_m(X)$ становятся в очередь на обработку. Их считывание Алгоритмом B не совпадает с естественно-временны́м появлением блоков. Как мы увидим ниже, порядок считывания блоков Алгоритмом B для данной траектории цепи Маркова сохраняется также и при считывании блоков любой траектории цепи Маркова в классе эквивалентности S (будет определено ниже), что открывает прямой путь к доказательству равновероятности двоичной последовательности на выходе алгоритма Бабкина по аналогии с независимым источником.

Пусть траектория цепи Маркова $X = x_1x_2\ldots x_N$ с последним элементом $x_N = s_\chi$ была прочитана с использованием Алгоритма B.

Для всех $1 \leqslant i \leqslant m$ мы можем написать

$$\pi_i(X) = F_{i1}F_{i2}\ldots F_{i\alpha_i}E_i\,,$$

где F_{ij}, $1 \leqslant j \leqslant \alpha_i$, — это блоки, используемые для генерации выходных двоичных данных.

Отметим, что E_i — это оставшийся "кусок" выходной последовательности $\pi_i(X)$, из которого двоичные данные не производятся.

Для всех производящих биты отрезков имеем

$$|F_{ij}| = \varpi\,,$$

и

$$0 \leqslant |E_\chi| < \varpi\,, \quad 0 < |E_i| \leqslant \varpi\,, \quad i \neq \chi\,. \tag{4}$$

Пояснение.

Условие (4) появляется из-за способа построения Алгоритма B.

1. Пусть последний элемент в последнем блоке $F_{i\alpha_i}$ равен i. Тогда он может быть и совсем последним, т.е. $i = \chi$. В этом случае как раз $|E_\chi| = 0$.

2. Пусть $i \neq \chi$ — последнему элементу всей траектории. Тогда для отправки на обработку последнего блока $F_{i\alpha_i}$ надо дождаться s_i, но он не последний во всей траектории. Следовательно, если удалось дождаться s_i, то после него что-то идёт и оно включается в E_i, т.е появляется непустой добавок с длиной $|E_i| > 0$. Если такого s_i не удаётся дождаться, тогда длина последнего блока $|E_i| = \varpi$, и, согласно Алгоритму B, он не отправляется на обработку.

Пример 3. $N = 29$, $m = 2$, $\varpi = 3$.

$$X = s_1s_2s_2s_1s_1s_2s_2s_1s_1s_2s_2s_1s_1\mathbf{s_2}s_2s_1s_1\mathbf{s_2}s_2s_1s_1s_2s_2s_1s_1s_2s_2s_1s_1\,,$$

$$\pi_1(X) = \overbrace{s_2--s_1s_2}^{F_{11}} - - \overbrace{s_1s_2--s_1}^{F_{12}}\overbrace{s_2--s_1s_2}^{F_{13}} -- \overbrace{s_1s_2--s_1}^{F_{14}}\overbrace{s_2--s_1}^{E_1}\,,$$

$$\pi_2(X) = -\overbrace{s_2s_1--s_2}^{F_{21}}\overbrace{s_1--s_2s_1}^{F_{22}} -- \overbrace{s_2s_1--s_2}^{F_{23}}\overbrace{s_1--s_2s_1}^{F_{24}} - - \overbrace{s_2s_1}^{E_2} - .$$

Порядок считывания блоков Алгоритмом B:

$$F_{21}\ldots F_{11}\ldots F_{12}\ldots F_{22}\ldots F_{23}\ldots F_{13}\ldots F_{14}\ldots F_{24}\,.$$

Естественно-временной порядок считывания блоков:

$$F_{11}\ldots F_{21}\ldots F_{22}\ldots F_{12}\ldots F_{13}\ldots F_{23}\ldots F_{24}\ldots F_{14}\,.$$

Как мы видим, эти порядки считывания блоков не совпадают.

Теорема 3 (Алгоритм B).

Пусть траектория цепи Маркова $X = x_1x_2\ldots x_N$, $x_i \in \{s_1, s_2, \ldots, s_m\}$, *используется в качестве входных данных для Алгоритма B,* $\Psi(\ldots)$ *— двоичный выход m-арного алгоритма Бабкина,*

$$Y = \Psi(X) = \Psi(F_{i_1j_1}) \parallel \Psi(F_{i_2j_2}) \parallel \ldots \parallel \Psi(F_{i_Lj_L})\,.$$

Тогда двоичный выход $Y \in \{0,1\}^\ell$, *получающийся при некотором* ℓ, *имеет вероятность*

$$P(Y) = 2^{-\ell}\,.$$

Доказательство.

Ниже мы дадим доказательство Теоремы 3, полученное в [17], добавляя некоторые полезные уточнения и изменения.

Разобьём все возможные траектории цепи Маркова $X \in \{s_1, s_2, \dots, s_n\}^N$ на классы эквивалентности (одинаковой вероятности).

Рассмотрим траекторию X как задающую класс S и включим X' в класс S, если:

1) $x_1 = x'_1$ и $x_N = x'_N$ — начало и конец совпадают;

2) для всех $1 \leqslant i \leqslant m$

$$\begin{aligned} \pi_i(X) &= F_{i1}F_{i2}\dots F_{i\alpha_i}E_i\,, \\ \pi_i(X') &= F'_{i1}F'_{i2}\dots F'_{i\alpha_i}E_i\,, \end{aligned} \tag{5}$$

где F_{ij} и F'_{ij} — блоки, используемые для генерации выходных данных;

3) для всех i, j имеем $F_{ij} \equiv F'_{ij}$ — полная перестановка.

Обратим внимание на то, что не обрабатываемые части E_i для траекторий X и X' совпадают.

Согласно Утверждению 7 (Допустимые перестановки), такая траектория X' существует. Здесь достаточно заметить, что, согласно сделанному выше Пояснению, полная перестановка всей последовательности $\pi_i(X)$ возможна только тогда, когда $i = \chi$ — последнему элементу всей траектории X и может случиться так, что длина $|E_\chi| = 0$. Если же $i \neq \chi$, то обязательно появляется непустой добавок $|E_i| > 0$. Поскольку при переходе к построению X' мы не трогаем E_i, то эти условия как раз вписываются в условия Утверждения 7. Кроме того, согласно Утверждению 6, траектории в классе S одинаково вероятны.

В последовательностях $\pi_i(X) = F_{i1}F_{i2}\dots F_{i\alpha_i}E_i$, $1 \leqslant i \leqslant m$, последовательность блоков $F_{i1}, F_{i2}, \dots, F_{i\alpha_i}$ определяет порядок, в котором эти блоки считывались на обработку именно для состояний, следующих за s_i-м состоянием.

В то же время, порядок считывания блоков

$$F_{11}, \dots, F_{1\alpha_1}, F_{21}, \dots, F_{2\alpha_2}, \dots, F_{m1}, \dots, F_{m\alpha_m}\,. \tag{6}$$

Алгоритмом B в реальном времени появления состояний цепи Маркова может быть весьма произвольным, но строго задаваемым исходной цепью Маркова $X = x_1x_2\dots x_N$ (см. Пример 3 выше). Для облегчения рассуждений предположим, что он именно такой (6).

Предположим теперь, что порядок считывания блоков Алгоритмом B для всех траекторий $X' = x'_1x'_2\dots x'_N$ из класса S сохраняется и равен

$$F'_{11}, \dots, F'_{1\alpha_1}, F'_{21}, \dots, F'_{2\alpha_2}, \dots, F'_{m1}, \dots, F'_{m\alpha_m}\,.$$

Пусть, как и в случае независимого источника, B_Y обозначает множество траекторий цепи Маркова $X = x_1x_2\dots x_N$ таких, что $\Psi(X) = Y$ и для данного класса эквивалентности S у нас есть допустимое разбиение

$$Y_{11}, \dots, Y_{1\alpha_1}, Y_{21}, \dots, Y_{2\alpha_2}, \dots, Y_{m1}, \dots, Y_{m\alpha_m}\,,$$

такое, что

$$\begin{aligned} Y = \Psi(X) = \Psi(Y_{11}) \parallel \dots \parallel \Psi(Y_{1\alpha_1}) \parallel \Psi(Y_{21}) \parallel \dots \\ \dots \parallel \Psi(Y_{2\alpha_2}) \parallel \dots \parallel \Psi(Y_{m1}) \parallel \dots \parallel \Psi(Y_{m\alpha_m})\,. \end{aligned}$$

Тогда, при сохранении порядка считывания блоков Алгоритмом B, имеет место конструктивное свойство алгоритма Бабкина: ровно по одной последовательности F_{ij}, F'_{ij} дают Y_{ij}, Y'_{ij} всякий раз, когда $|Y_i| = |Y'_i|$. Отсюда легко следует основное соотношение о равенстве мощностей прообразов $|S \cap B_Y| = |S \cap B_{Y'}|$ всякий раз, когда $|Y| = |Y'|$. Далее, с использованием того, что траектории цепи Маркова внутри классов эквивалентности S одинаково вероятны, доказательство Теоремы 3 легко завершается по аналогии с доказательством Теоремы 1 для независимого источника.

Осталось доказать, что порядок считывания блоков Алгоритмом B сохраняется для всех траекторий цепи Маркова $X = x_1x_2\dots x_N$ из класса эквивалентности S.

1. Ясно, что достаточно доказать равенство порядка считывания блоков только для одной траектории $X' = x'_1x'_2\dots x'_N$ в классе S, отличающейся от $X = x_1x_2\dots x_N$ одной транспозицией для произвольного i в произвольном блоке F_{ik}:

$$X' = x'_1x'_2\dots x'_N \Longleftrightarrow \left\{ \begin{array}{l} \pi_i(X') = F_{i1}F_{i2}\dots F'_{ik}\dots F_{i\alpha_i}E_i\,, \\ \pi_j(X') = F_{j1}F_{j2}\dots F_{j\alpha_j}E_j\,,\ j \neq i \end{array} \right\}.$$

Тогда, двигаясь последовательно по транспозициям, можно перейти к любой перестановке с сохранением порядка считывания блоков.

2. Рассмотрим часть исходной траектории цепи Маркова X^a, которая заканчивается на состоянии x_a, после которого следует считывание блока F_{ik} для конвертации в биты. При этом, согласно считыванию блоков Алгоритмом B, $x_a = s_i$ и, кроме того,

$$\begin{aligned} &\pi_i(X^a) = F_{i1}F_{i2}\dots F_{ik}\,, \\ &\pi_j(X^a) = F_{j1}F_{j2}\dots F_{jk_j}, \widehat{E}_j,\quad j \neq i\,, \\ &0 < |\widehat{E}_j| \leqslant \varpi\,. \end{aligned}$$

Мы используем обозначение $\widehat{E}_j$, поскольку X^a — это часть траектории X.

Ясно, что $|\widehat{E}_i| = 0$, поскольку F_{ik} — последний считываемый блок и в этом случае либо последний элемент в F_{ik} равен s_i, либо s_i входит в какое-то $\widehat{E}_j$, после чего F_{ik} считывается.

Можем ли мы построить часть траектории цепи Маркова, произведя транспозицию в блоке F_{ik}?

Поскольку последний элемент $x_a = s_i$, то мы можем произвести любую транспозицию в блоке F_{ik} — это как если бы мы устроили любую перестановку на всей $\pi_i(X^a) = F_{i1}F_{i2}\dots F_{ik}$, цепляя и последний элемент.

Получаем

$$\begin{aligned} &\pi_i(X'^a) = F_{i1}F_{i2}\dots F'_{ik}\,, \\ &\pi_j(X'^a) = F_{j1}F_{j2}\dots F_{jk_j}\widehat{E}_j,\quad j \neq i\,, \\ &|\widehat{E}_j| > 0\,, \end{aligned} \tag{7}$$

что допустимо для построения начального отрезка X'^a траектории цепи Маркова согласно Утверждению 7.

Кроме того, согласно Утверждению 7, длина $|X'^a| = |X^a|$ и последние элементы совпадают: $x'_a = x_a = s_i$. А это значит, что в нашей конфигурации для начального куска траектории цепи Маркова блок F'_{ik} обязательно отправится на обработку. Будет ли он последним?

Если $x'_a = s_i$ и входит последним в F'_{ik}, то F'_{ik} отправляется на обработку (обнуляется) последним.

Если это не так, то должен быть еще один s_i, который обнуляет F'_{ik} перед каким-нибудь F_{js}, а потом уже должен появиться и наш, окончательно последний $x'_a = s_i$.

Тогда мы должны получить

$$\pi_i(X'^a) = F_{i1}F_{i2}\ldots F'_{ik}s_i\,.$$

Противоречие. Следовательно, блок F'_{ik} считывается последним.

3. Нетрудно видеть, что после элемента x_a траектории X и X' совпадают и порядок считывания блоков не меняется.

4. Рассмотрим начальную часть траектории цепи Маркова X'^b, которая заканчивается на состоянии x_b $(b = i)$, после которого следует первый элемент блока F'_{ik}. Нетрудно видеть, что до элемента x_b траектории X и X' совпадают и порядок считывания блоков не меняется.

Отсюда можно сделать вывод, что порядок считывания блоков Алгоритмом B для траекторий X и X' одинаков.

Теорема 3 доказана.

Рассмотрим пример, иллюстрирующий сохранение порядка считывания блоков Алгоритмом B.

Пример 4. $N = 29$, $m = 3$, $\varpi = 3$.

1. *Исходная траектория*

$$X = \overbrace{s_1s_2s_2s_3s_2s_3s_1s_1s_2s_2s_3s_3s_1}^{X^b}\,s_1s_2s_1s_3s_2s_1\,\overbrace{s_3s_2s_1s_2s_3s_1s_1s_2s_3s_2}^{X_a}\,.$$

Движение по блокам

$$\pi_1(X) = \overbrace{s_2------s_1s_2}^{F_{11}}----\overbrace{s_1s_2-s_3}^{F_{12}}--\overbrace{s_3--s_2--s_1}^{F_{13}}\overbrace{s_2}^{E_1}--\,,$$

$$\pi_2(X) = -\overbrace{s_2s_3-s_3}^{F_{21}}---\overbrace{s_2s_3-----s_1}^{F_{22}}--\overbrace{s_1--s_1-s_3}^{F_{23}}---\overbrace{s_3}^{E_2}-\,,$$

$$\pi_3(X) = ---\overbrace{s_2-s_1-----s_3}^{F_{31}}\overbrace{s_1-----s_2--s_2}^{F_{32}}---\overbrace{s_1---s_2}^{E_3}\,.$$

Порядок считывания блоков Алгоритмом B

$$F_{21}\ldots F_{31}\ldots F_{11}\ldots F_{22}\ldots F_{12}\ldots F_{32}\ldots F_{13}\ldots F_{23}\,.$$

2. *Траектория после транспозиции в блоке*

Произведём транспозицию в $F_{12} = s_1s_2s_3 \to F'_{12} = s_1s_3s_2$. После транспозиции

$$\pi_1(X') = \{F_{11} = s_2s_1s_2,\, F'_{12} = s_1s_3s_2,\, F_{13} = s_3s_2s_1,\, E_1 = s_2\}\,,$$

$$\pi_2(X') = \{F_{21} = s_2s_3s_3,\, F_{22} = s_2s_3s_1,\, F_{23} = s_1s_1s_3,\, E_2 = s_3\}\,,$$

$$\pi_3(X') = \{F_{31} = s_2s_1s_3,\, F_{32} = s_1s_2s_2,\, E_3 = s_1s_2\}\,.$$

Траектория

$$X' = \overbrace{s_1s_2s_2s_3s_2s_3s_1s_1s_2s_2s_3s_3s_1}^{X'^b=X^b}\,s_1s_3s_2s_1s_2s_1\,\overbrace{s_3s_2s_1s_2s_3s_1s_1s_2s_3s_2}^{X'_a=X_a}\,.$$

Движение по блокам

$$\pi_1(X') = \overbrace{s_2------s_1s_2}^{F_{11}}----\overbrace{s_1s_3--s_2}^{F'_{12}}-\overbrace{s_3--s_2--s_1}^{F_{13}}\overbrace{s_2}^{E_1}--\,,$$

$$\pi_2(X') = -\overbrace{s_2s_3-s_3}^{F_{21}}---\overbrace{s_2s_3-----s_1}^{F_{22}}-\overbrace{s_1--s_1-s_3}^{F_{23}}---\overbrace{s_3}^{E_2}-\,,$$

$$\pi_3(X') = ---\overbrace{s_2-s_1----s_3}^{F_{31}}\overbrace{s_1--s_2----s_2}^{F_{32}}---\overbrace{s_1---s_2}^{E_3}\,.$$

Порядок считывания блоков Алгоритмом B

$$F_{21}\ldots F_{31}\ldots F_{11}\ldots F_{22}\ldots F'_{12}\ldots F_{32}\ldots F_{13}\ldots F_{23}\,.$$

Порядок считывания блоков Алгоритмом B для траекторий X и X' одинаков.

3.4. Пример неоднозначности двоичного выхода алгоритма Бабкина при естественно-временно́м считывании блоков на обработку

Один из основных моментов в доказательстве Теоремы 3 основывается на том, что в классе эквивалентности S количество прообразов полного двоичного выхода $Y \in \{0,1\}^*$ при фиксированной длине $|Y| = \ell$ одинаково при любом двоичном составе Y.

Это будет так, если порядок считывания блоков в классе эквивалентности траекторий цепи Маркова (π-последовательностей) отвечает Алгоритму B.

Возникает вопрос, не сохраняется ли это свойство при естественно-временно́м считывании блоков, которое является более простым при практической реализации.

Ниже мы приведём пример, для которого при естественно-временно́м считывании блоков это свойство нарушается — количество прообразов различно при некоторых Y и Y' одинаковой длины.

Рассмотрим исходную траекторию цепи Маркова X как задающую класс S, $N = 10$, $m = 2$, $\varpi = 4$:

$$X = s_1s_1s_1s_2s_2s_2s_1s_2s_2\boldsymbol{s_1}\,,$$

$$\pi_1(X) = \overbrace{s_1s_1s_2---s_2}^{F_{11}}--\,,$$

$$\pi_2(X) = ---\overbrace{s_2s_2s_1-s_2}^{F_{21}}\overbrace{s_1}^{E_2}\,.$$

Согласно Алгоритму B, сначала отправится на обработку блок $F_{21} = (s_2s_2s_1s_2)$, поскольку s_2 — последний элемент в блоке, а затем — $F_{11} = (s_1s_1s_2s_2)$.

Порядок считывания Алгоритмом B сохраняется для всех траекторий X из класса эквивалентности, определяемого перестановками в блоках $F_{11} = (s_1s_1s_2s_2)$ и $F_{21} = (s_2s_2s_1s_2)$. Естественно-временной порядок считывании блоков: $F_{11} = (s_1s_1s_2s_2)$, $F_{21} = (s_2s_2s_1s_2)$.

Используя исходную траекторию цепи Маркова, создаём класс эквивалентности S.

Имеется шесть перестановок внутри блока $F_{11} = (\boldsymbol{s_1s_1}s_2s_2)$ и четыре перестановки внутри блока $F_{21} = (s_2s_2\boldsymbol{s_1}s_2)$.

Совокупно в класс эквивалентности S войдут 24 перестановки, определяющие 24 одинаково вероятные траектории цепи Маркова.

Таблица 4

№ п/п	F_{11}, перестановки	Num (i_1, i_2)	Двоичный выход
1	$(\boldsymbol{s_1 s_1} s_2 s_2)$	Num $(1,2) = 0$	0
2	$(\boldsymbol{s_1} s_2 \boldsymbol{s_1} s_2)$	Num $(1,3) = 1$	1
3	$(s_2 \boldsymbol{s_1 s_1} s_2)$	Num $(2,3) = 2$	00
4	$(\boldsymbol{s_1} s_2 s_2 \boldsymbol{s_1})$	Num $(1,4) = 3$	01
5	$(s_2 \boldsymbol{s_1} s_2 \boldsymbol{s_1})$	Num $(2,4) = 4$	10
6	$(s_2 s_2 \boldsymbol{s_1 s_1})$	Num $(3,4) = 5$	11

Таблица 5

№ п/п	F_{11}, перестановки	Num (i_1)	Двоичный выход
1	$(\boldsymbol{s_1} s_2 s_2 s_2)$	Num $(1) = 0$	00
2	$(s_2 \boldsymbol{s_1} s_2 s_2)$	Num $(2) = 1$	01
3	$(s_2 s_2 \boldsymbol{s_1} s_2)$	Num $(3) = 2$	10
4	$(s_2 s_2 s_2 \boldsymbol{s_1})$	Num $(4) = 3$	11

В таблицах 4, 5 (отвечающих табл. 3, 2 раздела 2.2) для первого блока F_{11} обозначаем (i_1, i_2) — позиции появления состояния s_1, для второго блока F_{21} обозначаем (i_1) — позицию появления состояния s_1. Нумерация метода Бабкина:

$$\text{Num}\,(i_1, i_2) = C^1_{i_1 - 1} + C^2_{i_2 - 1}\,, \quad \text{Num}\,(i_1) = C^1_{i_1 - 1}\,,$$

где $C^i_j = 0$, если $j < i$. Четвёртая колонка задаёт двоичный выход алгоритма Бабкина.

Для каждой пары блоков (F_{11}, F_{21}) и дополнительному блоку $E_2 = s_1$ строятся траектории цепи Маркова X, определяются порядки считывания блоков по Алгоритму В и по естественно-временно́му (ЕВ) порядку. Для каждого порядка считывания строится двоичный выход алгоритма Бабкина $Y = \Psi(X)$.

Например, для блоков $F_{11} = (\boldsymbol{s_1 s_1} s_2 s_2)$, $F_{21} = (s_2 \boldsymbol{s_1} s_2 s_2)$, что соответствует выбору номеров $(1,2)$ в первых колонках табл. 4, 5, имеем

$$X = s_1 \boldsymbol{s_1 s_1} s_2 s_2 \boldsymbol{s_1} s_2 s_2 s_2 s_1\,,$$
$$\pi_1(X) = \overbrace{\boldsymbol{s_1 s_1} s_2 - - s_2}^{F_{11}} - - -\,,$$
$$\pi_2(X) = - - - \overbrace{s_2 \boldsymbol{s_1} - s_2 s_2}^{F_{21}} \overbrace{s_1}^{E_2}\,.$$

Получаем следующий порядок считывания.

1. **Алгоритм В**: F_{21}, F_{11}, двоичный выход $Y = \Psi(X) = 01 \,\|\, 0 = 010$.

2. **ЕВ**: F_{11}, F_{21} двоичный выход $Y = \Psi(X) = 0 \,\|\, 01 = 001$.

В таблице 6 двоичные выходы упорядочены в соответствии с выбором пар номеров (перестановок) в первых колонках табл. 4, 5:

$$\text{№}\,1 — (1,1),\ \text{№}\,2 — (1,2), \ldots, \text{№}\,24 — (6,4)\,.$$

Полученные результаты показывают, что при естественно-временно́м ЕВ считывании блоков:

— при длине выхода $|Y| = 3$ число прообразов комбинации $Y = \mathbf{110}$ равно 2, у комбинации $Y = \mathbf{001}$ прообразов нет, остальные комбинации $Y \in \{0,1\}^3$ имеют по одному прообразу,

Таблица 6

№ п/п	Алгоритм В считывание	Двоичный выход Y	ЕВ считывание	Двоичный выход Y
№ 1 (1,1)	F_{21}, F_{11}	000	F_{21}, F_{11}	000
№ 2 (1,2)	F_{21}, F_{11}	010	F_{11}, F_{21}	001
№ 3 (1,3)	F_{21}, F_{11}	100	F_{11}, F_{21}	010
№ 4 (1,4)	F_{21}, F_{11}	110	F_{21}, F_{11}	**110**
№ 5 (2,1)	F_{21}, F_{11}	001	F_{11}, F_{21}	100
№ 6 (2,2)	F_{21}, F_{11}	011	F_{11}, F_{21}	101
№ 7 (2,3)	F_{21}, F_{11}	101	F_{11}, F_{21}	**110**
№ 8 (2,4)	F_{21}, F_{11}	111	F_{21}, F_{11}	111
№ 9 (3,1)	F_{21}, F_{11}	0000	F_{11}, F_{21}	0000
№ 10 (3,2)	F_{21}, F_{11}	0100	F_{11}, F_{21}	**0001**
№ 11 (3,3)	F_{21}, F_{11}	1000	F_{11}, F_{21}	0010
№ 12 (3,4)	F_{21}, F_{11}	1100	F_{21}, F_{11}	1100
№ 13 (4,1)	F_{21}, F_{11}	0001	F_{21}, F_{11}	**0001**
№ 14 (4,2)	F_{21}, F_{11}	0101	F_{21}, F_{11}	0101
№ 15 (4,3)	F_{21}, F_{11}	1001	F_{21}, F_{11}	1001
№ 16 (4,4)	F_{21}, F_{11}	1011	F_{21}, F_{11}	1101
№ 17 (5,1)	F_{21}, F_{11}	0010	F_{21}, F_{11}	0010
№ 18 (5,2)	F_{21}, F_{11}	0110	F_{21}, F_{11}	0110
№ 19 (5,3)	F_{21}, F_{11}	1010	F_{21}, F_{11}	1010
№ 20 (5,4)	F_{21}, F_{11}	1110	F_{21}, F_{11}	1110
№ 21 (6,1)	F_{21}, F_{11}	0011	F_{21}, F_{11}	0011
№ 22 (6,2)	F_{21}, F_{11}	0111	F_{21}, F_{11}	0111
№ 23 (6,3)	F_{21}, F_{11}	1011	F_{21}, F_{11}	1011
№ 24 (6,4)	F_{21}, F_{11}	1111	F_{21}, F_{11}	1111

— при длине выхода $|Y| = 4$ число прообразов комбинации $Y = \mathbf{0001}$ равно 2, у комбинации $Y = \mathbf{0100}$ прообразов нет, остальные комбинации $Y \in \{0,1\}^4$ имеют по одному прообразу.

3.5. Цепь Маркова из двух состояний конечного порядка r

Рассмотренные выше алгоритмы извлечения случайных битов построены для простых ($r = 1$) стационарных цепей Маркова, имеющих начальное распределение $P(s_i)$ и матрицу переходных вероятностей $P(s_j \,|\, s_i)$, $s_i, s_j \in \{s_1, \ldots, s_m\}$.

Вероятность произвольной траектории цепи Маркова $X_N = x_1 x_2 \ldots x_N$ определяется как

$$P(X_N) = P(x_1) \prod_{i=1}^{N-1} P(x_{i+1} \,|\, x_i)\,.$$

На практике при построении квантового ФГСЧ, связанного с регистрацией фотоотсчётов, мы имеем символы из бинарного алфавита $A = \{*, \sqcup\}$ и некоторый произвольный порядок $r \geqslant 2$.

В практических применениях удобно представить алфавит в двоичном виде: $A = \{0,1\}$.

Цепь Маркова с двумя состояниями $A = \{0,1\}$, порядка $r \geqslant 2$, задаётся начальным распределением

$$P(\varepsilon_1, \ldots, \varepsilon_r), \sum_{(\varepsilon_1, \ldots, \varepsilon_r) \in \{0,1\}^r} P(\varepsilon_1, \ldots, \varepsilon_r) = 1\,,$$

и матрицей переходных вероятностей размера $2^r \times 2$

$$\| P(\varepsilon_{r+1} | \varepsilon_1, \ldots, \varepsilon_r) \|,\ \varepsilon_{r+1} \in \{0,1\},\ (\varepsilon_1, \ldots, \varepsilon_r) \in \{0,1\}^r\,.$$

Вероятность траектории

$$E = \varepsilon_1\varepsilon_2\ldots\varepsilon_L, \quad \varepsilon_i \in \{0,1\},$$

определяется как

$$P(E) = P(\varepsilon_1,\ldots,\varepsilon_r)\prod_{i=1}^{L-r} P(\varepsilon_{i+r}\,|\,\varepsilon_i,\ldots,\varepsilon_{i+r-1}).$$

Перейти к простой цепи Маркова порядка $r=1$ можно путём укрупнения алфавита, где число состояний $m = 2^r$.

Введём новый алфавит

$$A' = \{s_1,\ldots,s_m\} = \{s_1 = (0\ldots0),\ldots,s_m = (1\ldots1)\},$$

объединяя соседние r битов в траектории $E_L = \varepsilon_1\varepsilon_2\ldots\varepsilon_L$ с зацеплением на 1 бит в один символ, получим траекторию длины $N = L - r$:

$$X = (\varepsilon_1\varepsilon_2\ldots\varepsilon_r)(\varepsilon_2\varepsilon_3\ldots\varepsilon_{r+1})(\varepsilon_3\varepsilon_4\ldots\varepsilon_{r+2})\ldots$$
$$\ldots(\varepsilon_{L-r+1}\varepsilon_{L-r+2}\ldots\varepsilon_L) = x_1x_2\ldots x_N, \quad x_i \in \{0,1\}^r.$$

Рассмотрим переходные вероятности

$$P(x_{i+1}\,|\,x_i) = P(\boldsymbol{\varepsilon_{i+1}},\ldots,\boldsymbol{\varepsilon_{i+r-1}},\varepsilon_{i+r}\,|\,\varepsilon_i,\boldsymbol{\varepsilon_{i+1}},\ldots,\boldsymbol{\varepsilon_{i+r-1}}).$$

Часть условия $\varepsilon_{i+1},\ldots,\varepsilon_{i+r-1}$ (выделено жирным шрифтом) фиксирована, поэтому переходная вероятность зависит только от значения ε_{i+r} и, как нетрудно видеть, равна

$$P(x_{i+1}\,|\,x_i) = P(\boldsymbol{\varepsilon_{i+1}},\ldots,\boldsymbol{\varepsilon_{i+r-1}},\varepsilon_{i+r}\,|\,\varepsilon_i,\boldsymbol{\varepsilon_{i+1}},\ldots,\boldsymbol{\varepsilon_{i+r-1}}) =$$
$$= P(\varepsilon_{i+r}\,|\,\varepsilon_i,\ldots,\varepsilon_{i+r-1}).$$

Тогда вероятность траектории

$$P(X) = P(E) = P(\varepsilon_1,\ldots,\varepsilon_r)\prod_{i=1}^{L-r} P(\varepsilon_{i+r}\,|\,\varepsilon_i,\ldots,\varepsilon_{i+r-1}) =$$
$$= P(\varepsilon_1,\ldots,\varepsilon_r)\prod_{i=1}^{L-r} P(\varepsilon_{i+1},\ldots,\varepsilon_{i+r-1},\varepsilon_{i+r}\,|\,\varepsilon_i,\ldots,\varepsilon_{i+r-1}) =$$
$$= P(x_1)\prod_{i=1}^{N} P(x_{i+1}\,|\,x_i).$$

Таким образом мы приходим к стационарной цепи Маркова порядка 1.

Здесь мы будем иметь существенно разреженную матрицу переходных вероятностей — в каждой строке будут только две ненулевые переходные вероятности.

Это связано с тем, что для любого состояния $s_i = (\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_r)$ возможен переход только в два состояния: $(\varepsilon_2,\ldots,\varepsilon_r,0)$ и $(\varepsilon_2,\ldots,\varepsilon_r,1)$.

На примере $r=2$ матрица переходных вероятностей (табл. 7) выглядит следующим образом.

Формируемые π-последовательности

$$\{\pi_i(X) = F_{i1}F_{i2}\ldots F_{i\alpha_i}E_i, 1 \leqslant i \leqslant m\}$$

Таблица 7

	00 (s_1)	01 (s_2)	10 (s_3)	11 (s_4)
00 (s_1)	$P(s_1\|s_1)$	$P(s_2\|s_1)$	0	0
01 (s_2)	0	0	$P(s_3\|s_2)$	$P(s_4\|s_2)$
10 (s_3)	$P(s_1\|s_3)$	$P(s_2\|s_1)$	0	0
11 (s_4)	0	0	$P(s_3\|s_4)$	$P(s_4\|s_4)$

будут бинарными, применять m-арный алгоритм Бабкина не потребуется.

Пример работы Алгоритма B при $r=2, N=36, m=4$, $\varpi = 3$.

Вверху в траектории E индексированы состояния траектории цепи Маркова X с укрупнённым алфавитом, внизу — № такта

$$E = 01_1^2 0_2^3 0_3^1 1_4^2 0_5^3 1_6^2 1_7^4 0_8^3 1_9^2 0_{10}^3 0_{11}^1 1_{12}^2 1_{13}^4 1_{14}^4 1_{15}^4 0_{16}^3 0_{17}^1 1_{18}^2 0_{19}^3 1_{20}^2$$
$$0_{21}^3 0_{22}^1 0_{23}^1 1_{24}^2 1_{25}^4 1_{26}^4 0_{27}^3 0_{28}^1 0_{29}^1 0_{30}^1 1_{31}^2 1_{32}^4 0_{33}^3 0_{34}^1 1_{35}^2 0_{36}^3,$$

π-последовательности:

$$\pi_1(X) = {}_{1\cdot2\cdot3}\overbrace{2_{4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11}2_{12\cdot13\cdot14\cdot15\cdot16\cdot17}2_{18}}^{F_{11}}{}_{\cdot19\cdot20\cdot21\cdot22}$$
$$\overbrace{1_{23}2_{24\cdot25\cdot26\cdot27\cdot28}\mathbf{1}_{29}}^{F_{12}}\overbrace{1_{30}2_{31\cdot32\cdot33\cdot34}2_{35}}^{E_1}{}_{\cdot36},$$

$$\pi_2(X) = {}_1\overbrace{3_{2\cdot3\cdot4}3_{5\cdot6}4_7}^{F_{21}}{}_{\cdot8\cdot9}\overbrace{\mathbf{3}_{10\cdot11\cdot12}4_{13\cdot14\cdot15\cdot16\cdot17\cdot18}3_{19}}^{F_{22}}{}_{\cdot20}$$
$$\overbrace{3_{21\cdot22\cdot23\cdot24}4_{25\cdot26\cdot27\cdot28\cdot29\cdot30\cdot31}4_{32}}^{F_{23}}{}_{\cdot33\cdot34\cdot35}\overbrace{3_{36}}^{E_2},$$

$$\pi_{3(\chi)}(X) = {}_{1\cdot2}\overbrace{1_{3\cdot4\cdot5}2_{6\cdot7\cdot8}\mathbf{2}_9}^{F_{31}}{}_{\cdot10}\overbrace{1_{11\cdot12\cdot13\cdot14\cdot15\cdot16}1_{17\cdot18\cdot19}2_{20}}^{F_{32}}{}_{\cdot21}$$
$$\overbrace{1_{22\cdot23\cdot24\cdot25\cdot26\cdot27}1_{28\cdot29\cdot30\cdot31\cdot32\cdot33}1_{34}}^{F_{33}}{}_{\cdot35\cdot36},$$

$$\pi_4(X) = {}_{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7}\overbrace{3_{8\cdot9\cdot10\cdot11\cdot12\cdot13}4_{14}\mathbf{4}_{15}}^{F_{41}}$$
$$\overbrace{3_{16\cdot17\cdot18\cdot19\cdot20\cdot21\cdot22\cdot23\cdot24\cdot25}4_{26}3_{27}}^{F_{42}}{}_{\cdot28\cdot29\cdot30\cdot31\cdot32}$$
$$\overbrace{3_{33}}^{E_4}{}_{\cdot34\cdot35\cdot36}.$$

Порядок считывания блоков Алгоритмом B:

$$F_{21}\ldots F_{31}\ldots F_{41}\ldots F_{22}\ldots F_{32}\ldots F_{11}\ldots$$
$$\ldots F_{12}\ldots F_{42}\ldots F_{23}\ldots F_{33}.$$

4. Заключение

Эпиграф, приведённый в начале работы, как нельзя лучше отражает ситуацию с получением истинно случайных последовательностей 0 и 1.

Как видно из рассмотрения выше, существуют фундаментальные физические ограничения Природы на скорость убывания корреляций во времени, которые, в свою очередь, вытекают из того факта, что спектр устойчивой физической системы должен лежать на положительной полуоси энергий (частот). По этой причине "дотянуться" до истинной случайности можно лишь за неограниченное время — для независимости последовательных результатов измерений необходимо разносить измерения на неограниченное время. Корреляции (зависимость) между измерениями проникают на неограниченную глубину по времени.

Если бы последовательные измерения были независимыми, то можно было бы предъявить эффективные методы экстракции истинно случайных последовательностей 0 и 1 из исходной последовательности.

Реальные эксперименты всегда проводятся на конечном временно́м отрезке, поэтому результаты последовательных измерений невозможно сделать независимыми.

Фактически, всё что нам позволяется Природой, так это считать и учитывать корреляции между измерениями

на конечную глубину по времени. Причём явный (функциональный) вид корреляций в ситуации реального эксперимента неизвестен. В такой ситуации приходится прибегать к приближениям. Адекватным приближением является учёт корреляций на конечную глубину, которое достигается в рамках стационарных цепей Маркова конечного порядка. В этом приближении корреляции описываются переходными (условными) вероятностями между результатами измерений. Причём явный вид самих переходных вероятностей неизвестен и не требуется при построении алгоритмов экстракции случайных битов.

Как было продемонстрировано выше, при конечной глубине корреляций удаётся получить доказуемо случайные выходные битовые последовательности даже при условии зависимых событий в исходной последовательности. В этом подходе, в отличие от других подходов, например, с вероятностными экстракторами, используется фактически единственное предположение — о конечной глубине корреляций. Таким образом, любые подходы к получению истинной случайности, по причине фундаментальных ограничений Природы, являются лишь приближением. Вопрос состоит лишь в том, насколько конкретное приближение адекватно описывает реальную ситуацию и сколько предположений содержится внутри данного приближения.

Доказательство случайности выходной битовой последовательности является нетривиальной задачей даже в рамках выбранного приближения — стационарных цепей Маркова. Далеко не все подходы позволяют получить доказуемую случайность в том смысле, как это обсуждалось выше.

Благодарности. Выражаем благодарность за активное сотрудничество, полезные обсуждения и поддержку: коллегам по Академии криптографии Российской Федерации, В.О. Миронкину, коллегам по Центру квантовых технологий МГУ имени М.В. Ломоносова К.А. Балыгину, А.Н. Климову, С.П. Кулику, сотруднику СФБ Лаборатории, г. Москва, В.А. Кирюхину.

Список литературы

1. Paley R, Wiener N *Fourier Transforms in the Complex Domain* (American Mathematical Society. Colloquium Publ., Vol. 19) (New York: American Mathematical Society, 1934); Пер. на русск. яз.: Винер Н, Пэли Р *Преобразование Фурье в комплексной области* (М.: Наука, 1964)
2. Fonda L, Ghirardi G C, Rimini A *Rep. Prog. Phys.* **41** 587 (1978)
3. Молотков С Н *ЖЭТФ* **157** 442 (2020); Molotkov S N *J. Exp. Theor. Phys.* **130** 370 (2020)
4. Molotkov S N *Laser Phys. Lett.* **20** 035202 (2023)
5. Арбеков И М, Молотков С Н *УФН* **191** 651 (2021); Arbekov I M, Molotkov S N *Phys. Usp.* **64** 617 (2021)
6. Rukhin A et al. "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication 800-22, Revision 1a (Gaithersburg, MD: National Institute of Standards and Technology, 2010) https://doi.org/10.6028/NIST.SP.800-22r1a
7. Ивченко Г И, Медведев Ю И *Введение в математическую статистику* (М.: Изд-во ЛКИ, 2010)
8. Turan M S et al. "Recommendation for the entropy sources used for random bit generation", NIST Special Publication 800-90B (Gaithersburg, MD: National Institute of Standards and Technology, 2018) https://doi.org/10.6028/NIST.SP.800-90B
9. Impagliazzo R, Levin L A, Luby M "Pseudo-random generation from one-way functions", in *STOC89: 21st Annual ACM Symp. on the Theory of Computing, Seattle, Washington, USA May 14–17, 1989* (New York: Association for Computing Machinery, 1989) p. 12, https://doi.org/10.1145/73007.73009
10. Bennett C H et al. *IEEE Trans. Inform. Theory* **41** 1915 (1995)
11. Бабкин В Ф *Проблемы передачи информации* **7** (4) 13 (1971)
12. Молотков С Н *Письма в ЖЭТФ* **105** 374 (2017); Molotkov S N *JETP Lett.* **105** 395 (2017)
13. Балыгин К А и др. *ЖЭТФ* **153** 879 (2018); Balygin K A et al. *J. Exp. Theor. Phys.* **126** 728 (2018)
14. Balygin K A et al. *Laser Phys. Lett.* **14** 125207 (2017)
15. Балыгин К А и др. *Письма в ЖЭТФ* **106** 451 (2017); Balygin K A et al. *JETP Lett.* **106** 470 (2017)
16. Blum M *Combinatorica* **6** 97 (1986) https://doi.org/10.1007/BF02579167
17. Zhou H "Randomness and noise in information systems", Ph.D. Thesis (Pasadena, CA: California Institute of Technology, 2013) Defended June 1, 2012, https://doi.org/10.7907/82KV-2H11
18. Molotkov S N *Laser Phys.* **32** 055202 (2022)
19. Ore Ø *Theory of Graphs* (American Mathematical Society. Colloquium Publ., Vol. 38) (Providence, RI: American Mathematical Society, 1962); Пер. на русск. яз.: Оре О *Теория графов* (М.: Наука, 1980)

Quantum random number generators, extraction of provably random bit sequences from Markov chain trajectories

I.M. Arbekov [1, a], **S.N. Molotkov** [1, 2, 3, 4, b]
[1] *Academy of Cryptography of the Russian Federation, PO Box 100, 119331 Moscow, Russian Federation*
[2] *Osipyan Institute of Solid State Physics, Russian Academy of Sciences, ul. Akademika Osip'yana 2, 142432 Chernogolovka, Moscow region, Russian Federation*
[3] *Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, Leninskie gory 1, str. 52, 119991 Moscow, Russian Federation*
[4] *Lomonosov Moscow State University, Quantum Technology Center, Leninskie gory 1, str. 35, 119991 Moscow, Russian Federation*
E-mail: [a] *arbekov53@mail.ru,* [b] *molotkov@issp.ac.ru*

One of the main problems in the construction of quantum random number generators — obtainment of a provably random output sequence from physical measurements, i.e., from an initial sequence generated by a physical random number generator — is investigated. The conceptual feasibility and the conditions under which randomness can be 'reached,' as well as the meaning of the 'provable randomness' term, are discussed. We consider the methods of extracting provably random bit sequences from stationary Markov chains of finite order, i.e., under the assumption of the finite depth of the dependence of the results of physical measurements on the prehistory, which is an adequate approximation of the real situation. The extraction of the output provably random bit sequence from the initial sequence of the results of physical measurements using V.F. Babkin's effective arithmetic coding method is demonstrated. It is shown that random bit sequences can be provably obtained even from primary sequences of the results of physical measurements, which are dependent on (correlated to) any finite depth (prehistory). We aim to reveal the connection of various approximations employed in the development and description of methods for obtaining random bit sequences with the basic physical limitations of Nature. The mathematical proofs are detailed to the level of practical algorithms applied in real random number generators. The necessary mathematical propositions are presented at an intuitive level for physicists, do not require prior knowledge in this area, and are comprehensible to undergraduate university students.

Keywords: quantum random number generators, Markov chains, random bit sequences

PACS numbers: **02.50.–r**, **03.67.–a**, 42.50.Ex

Bibliography — 19 references
Uspekhi Fizicheskikh Nauk **194** (9) 974–993 (2024)
DOI: https://doi.org/10.3367/UFNr.2024.02.039658

Received 25 December 2023, revised 20 February 2024
Physics–Uspekhi **67** (9) (2024)
DOI: https://doi.org/10.3367/UFNe.2024.02.039658