ФГАОУ ВПО УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА
Б.Н.ЕЛЬЦИНА

На правах рукописи

Закс Юлия Иосифовна

Синхронизируемость конечных автоматов в экстремальном и среднем случаях

(05.13.17 — Теоретические основы информатики)

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук,
профессор
Михаил Владимирович Волков

Екатеринбург
— 2012 —

Оглавление

Введение **3**

0.1 Синхронизируемые автоматы 3

0.2 Синхронизируемость автоматов в экстремальном случае, гипотеза Черни 11

0.3 Синхронизируемость автоматов в среднем случае 15

0.4 Апробация результатов 20

1 Синхронизируемые автоматы с буквой дефекта 2 **22**

1.1 Формулировка и обсуждение результатов 22

1.2 $\mathscr{B}_n$: серия автоматов с буквой-бактрианом 24

1.3 $\mathscr{D}_n$: серия автоматов с буквой-дромадером 34

2 Синхронизируемые автоматы с буквой большого дефекта **41**

2.1 Постановка задачи и основные определения 41

2.2 Медленно синхронизируемые автоматы с буквой большого дефекта 42

2.3 Экспериментальная проверка экстремальности серий при небольших n 54

3 Синхронизируемость случайных автоматов **57**

3.1 Предварительные сведения 57

3.2 Случайные автоматы, синхронизируемые с высокой вероятностью 61

3.3 Случайные автоматы, для которых выполняется гипотеза Черни 66

3.4 Случайные автоматы, синхронизируемые с конечной вероятностью 77

Литература **83**

Введение

0.1 Синхронизируемые автоматы

Детерминированным конечным автоматом, или просто *автоматом* называется тройка объектов $\mathscr{A} = (Q, \Sigma, \delta)$, где Q – конечное множество *состояний*, Σ – конечный входной *алфавит*, и $\delta : Q \times \Sigma \to Q$ – всюду определенная *функция переходов* автомата. Заметим, что в теории формальных языков к набору данных, определяющему конечный детерминированный автомат, обычно добавляют выделенное *начальное* состояние и множество *заключительных* состояний, но мы таким вариантом определения пользоваться не будем. Состояния из множества Q мы будем обозначать буквами преимущественно из середины латинского алфавита, выделенными жирным шрифтом, например, $\mathbf{p}$, $\mathbf{q}$. Буквы алфавита Σ будем обозначать буквами из начала латинского алфавита, например, a, b, c.

Как обычно, через Σ^* обозначим свободный моноид над Σ. Элементы свободного моноида мы будем называть *словами* и обозначать буквами из конца латинского алфавита, например, w, v. Функция δ естественным образом продолжается на множество $Q \times \Sigma^*$, это продолжение мы также будем обозначать через δ. Таким образом, каждый элемент свободного моноида $w \in \Sigma^*$, в частности, каждая буква алфавита Σ, порождает отображение $\delta(\_, w) : Q \to Q$ множества Q в себя. Мы будем отождествлять слово w с этим отображением и пользоваться выражениями “слово w действует на автомате $\mathscr{A}$” или “под действием слова w состояние $\mathbf{q}_1$ переходит в состояние $\mathbf{q}_2$”. Образ состояния $\mathbf{q}$ под действием слова w для краткости мы будем часто обозначать через $\mathbf{q}w$.

В данной работе мы будем систематически использовать наглядное представление конечного автомата в виде ориентированного графа. При этом представлении автомат изображается в виде диаграммы, на которой состояния автомата изображаются в виде точек или кругов, а переходы – в виде стрелок, помеченных буквами входного алфавита. Если в автомате $\mathscr{A}$ выполняется $\mathbf{q}a = \mathbf{p}$, это означает, что в диаграмме, его визуализирующей, из точки, соответствующей $\mathbf{q}$, в точку, соответствующую $\mathbf{p}$, ведет стрелка, помеченная буквой a. В дальнейшем мы часто будем отож-

дествлять автомат с его графическим представлением, а переходы будем называть *стрелками*. Заметим, что стиранием букв со стрелок автомата $\mathscr{A}$ и "склеиванием" одинаковых стрелок мы получим ориентированный граф: назовем его *графом автомата*. Более строго, граф автомата $\mathscr{A}$ – это орграф, множество вершин которого совпадает с множеством состояний автомата $\mathscr{A}$, а дуги соответствуют переходам автомата, т. е. из вершины q есть дуга в вершину p тогда и только тогда, когда $qa = p$ для некоторой буквы $a \in \Sigma$.

Основное понятие, изучаемое в данной диссертации, – это понятие синхронизируемого автомата. Автомат $\mathscr{A} = (Q, \Sigma, \delta)$ называется *синхронизируемым*, если существует слово $w \in \Sigma^*$, переводящее его в одно состояние, независимо от текущего состояния автомата. В символах это свойство выражается равенством $pw = qw$ для всех $p, q \in Q$. Любое слово с таким свойством называется *синхронизирующим* для автомата $\mathscr{A}$. Пример синхронизируемого автомата с четырьмя состояниями приведен на рис. 0.1. Нетрудно проверить, что слово $w = ab^3ab^3a$ синхронизирует

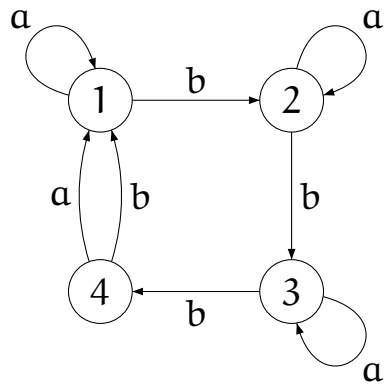


Рис. 0.1: Автомат Черни $\mathscr{C}_4$

этот автомат, а именно, применение этого слова к любому состоянию автомата приводит его в состояние 1. Более того, w является кратчайшим словом с таким свойством, хотя проверка этого факта уже менее тривиальна.

Синхронизируемые автоматы нашли широкое практическое применение в различных областях: роботике, а точнее в производстве механизмов для сортировки, обработки и установки деталей определенной конструкции [**45**], тестировании реагирующих систем и протоколов [**56**]. Тео-

ретическая мотивация к изучению синхронизируемых автоматов происходит из таких областей математики, как теория полугрупп [**14**], многозначная логика и символическая динамика [**43**], теория подстановочных систем [**28**]. Подробнее о различных применениях синхронизируемых автоматов см. недавние обзоры [**56**, **65**].

Особо хочется остановиться на мотивации, одновременно интересной теоретически и непосредственно практически применимой, а именно, на мотивации из теории кодирования. Для описания данной мотивации нам понадобится несколько определений, связанных со словами. Слово $u \in \Sigma^*$ называется *префиксом* слова $w \in \Sigma^*$, если существует слово $v \in \Sigma^*$ такое, что $w = uv$. Если слово v непустое, то префикс называется *собственным*. Слово $x \in \Sigma^*$ является *фактором* слова $w \in \Sigma^*$, если существуют слова $u, v \in \Sigma^*$ такие, что $w = uxv$. *Префиксным кодом* над конечным алфавитом Σ называется множество X слов из Σ^* таких, что никакое слово из X не является префиксом никакого другого слова из X. Префиксный код называется *максимальным*, если он не содержит другого префиксного кода над тем же алфавитом. Максимальный префиксный код X над алфавитом Σ называется *синхронизируемым*, если существует слово $x \in X^*$ такое, что для любого слова $w \in \Sigma^*$ выполняется $wx \in X^*$. Такое слово x называется *синхронизирующим словом* кода X. Преимущество синхронизирующих кодов состоит в том, что в случае возникновения помех при передаче информации от передатчика к приемнику, передачу можно восстановить. Достаточно передать синхронизирующее слово, и все последующие символы будут декодироваться верно. Более того, поскольку вероятность того, что некоторое слово $v \in \Sigma^*$ содержит фиксированный фактор x, с ростом длины слова стремится к 1, при передаче большого количества информации в некоторые моменты времени синхронизирующие коды синхронизируются сами. Как показано в [**23**], это свойство синхронизирующих кодов является характеристическим.

Рассмотрим пример, иллюстрирующий введенные понятия. Пусть $\Sigma = \{0, 1\}$, $X = \{000, 0010, 0011, 010, 0110, 0111, 10, 110, 111\}$. Слова кода – это листья бинарного дерева на рис. 0.3 слева. Легко проверить, что X является максимальным префиксным кодом и каждое из слов 010, 011110, 01111110, $\ldots$ его синхронизирует. Допустим, передатчик передает кодовое

слово 000, а приемник в силу помех в канале принимает слово 100. Тогда приемник интерпретирует слово 10 как кодовое, и синхронизация между приемником и передатчиком будет потеряна. Однако, с высокой вероятностью[1] синхронизация быстро восстановится, а именно в тот момент, когда в потоке передаваемых данных встретится одна из этих последовательностей 010, 011110, 01111110, ... Некоторые примеры синхронизации потоков приведены на рис. 0.2, вертикальными линиями отмечено разделение потоков на кодовые слова, жирным шрифтом выделены слова, содержащие позицию, с которой восстанавливается синхронизация.

Передано	000 | 0010 | **0111** | ...
Получено	10 | 000 | 10 | **0111** | ...
Передано	000 | 0111 | 110 | 0011 | 000 | 10 | **110** | ...
Получено	10 | 0011 | 111 | 000 | 110 | 0010 | **110** | ...
Передано	000 | 000 | 111 | **10** | ...
Получено	10 | 000 | 0111 | **10** | ...

Рис. 0.2: Пример синхронизации префиксного кода

Пусть X – максимальный конечный префиксный код над алфавитом Σ, тогда он может быть декодирован с помощью автомата, определенного следующим образом. В качестве Q возьмем множество всех собственных префиксов слов из X, включая пустое слово λ, в качестве алфавита – Σ, функцию переходов для $q \in Q$ и $a \in \Sigma$ определим следующим образом:

$$\delta(q, a) = \begin{cases} qa, & \text{если } qa \text{ – собственный префикс некоторого слова из } X, \\ \lambda, & \text{если } qa \in X. \end{cases}$$

Получившийся автомат $\mathscr{A}_X$ полон в силу того, что X максимален. Нетрудно видеть, что $\mathscr{A}_X$ – синхронизируемый автомат тогда и только тогда, когда X – синхронизируемый код. Более того, слово x синхронизирует код X тогда и только тогда, когда оно переводит автомат $\mathscr{A}_X$ в состояние λ. Рис 0.3 иллюстрирует описанные построения для кода $X =$

[1]Под *высокой вероятностью* мы понимаем вероятность, которая стремится к 1 при длине символьной последовательности, стремящейся к бесконечности.

$\{000, 0010, 0011, 010, 0110, 0111, 10, 110, 111\}$ из примера выше. Сплошные и пунктирные линии соответствуют символам 0 и 1.

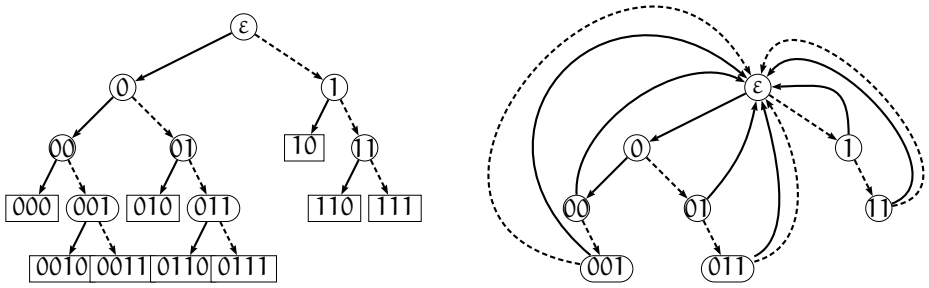


Рис. 0.3: Синхронизируемый код (слева) и его автомат (справа)

Отметим, что в случае, когда нам известно о помехах и мы посылаем синхронизирующие слова намеренно, трудоемкость синхронизации прямо зависит от длины синхронизирующего слова, и задача поиска кратчайшего слова с таким свойством приобретает большую актуальность.

Интересно, что, несмотря на большое практическое значение, само понятие синхронизируемого автомата произошло не из практики, а из некоторых достаточно абстрактных рассмотрений – так называемых "умозрительных экспериментов" (в оригинале Gedanken Experiments) Мура [**44**]. Предположим, что мы управляем некоторым дискретно работающим устройством, являющимся опечатанным "черным ящиком", получать информацию о его состояниях мы можем только воздействуя на него некоторыми входными сигналами и наблюдая за выходными. Пусть в устройстве произошел сбой и мы утратили контроль над нам, наша задача на основании только этих наблюдений восстановить контроль над устройством, т. е. установить его текущее состояние. Процедура определения заключительного состояния устройства после введения в него некоторой конечной входной последовательности сигналов и наблюдения за выходной последовательностью называется *экспериментом*. В 1956 году Мур [**44**] показал существование такого эксперимента при некоторых условиях. Эксперимент Мура был *адаптивным*: на каждом шаге следующий сигнал выбирался на основании предыдущих наблюдений. Позднее Гинзбург [**33**] рассмотрел *однородный* эксперимент, т. е. эксперимент, в котором входная последовательность выбиралась заранее и не менялась в ходе эксперимен-

та.

А что, если мы не можем наблюдать за ответами нашего “черного ящика” и должны восстановить контроль над ним вслепую? В этом случае мы должны применить к устройству такую входную последовательность символов, которая приведет его в какое-то заранее определенное состояние. Эта идея легла в основу определения синхронизируемого автомата, которое дал в 1964 году словацкий математик Ян Черни [**24**]. Мотивацией его исследований стала задача восстановления контроля над космическим спутником в моменты, когда он находится вне пределов видимости станций слежения.

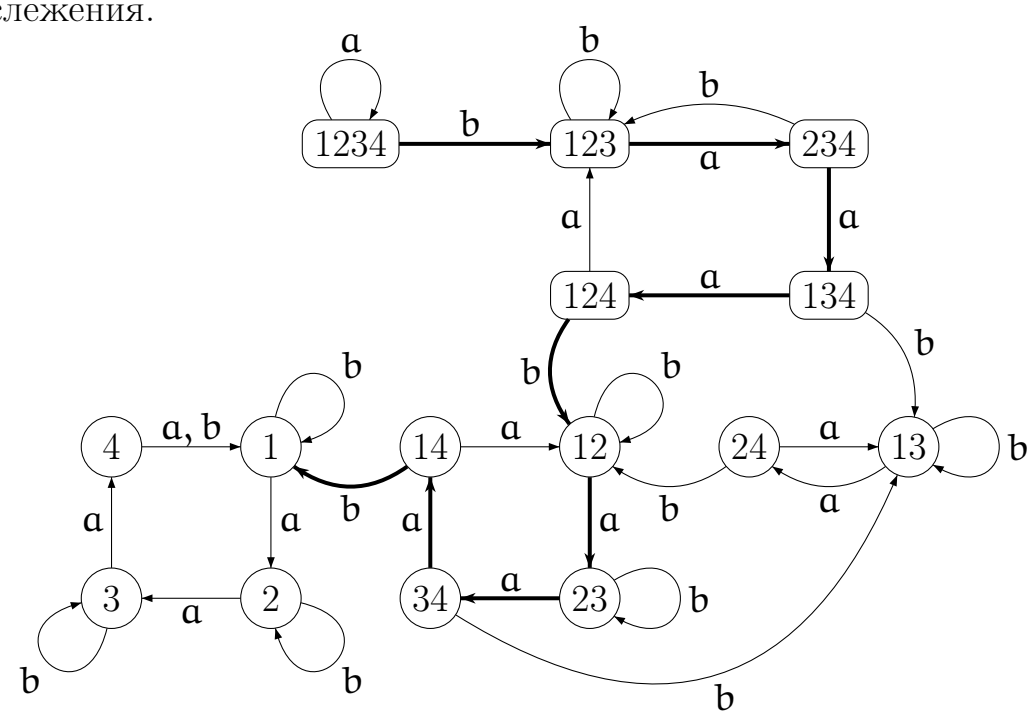


Рис. 0.4: Автомат подмножеств $\mathcal{P}(\mathscr{C}_4)$

В связи с введенным понятием синхронизируемости возникает ряд естественных вопросов:

— Как по данному автомату проверить, является ли он синхронизируемым?

— Как по данному синхронизируемому автомату найти некоторое слово, его синхронизирующее?

— Как по данному синхронизируемому автомату найти кратчайшее

синхронизирующее слово этого автомата?

Алгоритм, отвечающий на все три вопроса сразу, использует такую классическую конструкцию, как *автомат подмножеств* $\mathcal{P}(\mathscr{A})$. Данная конструкция была введена в 1959 году Рабиным и Скоттом [**50**] и использовалась в алгоритме детерминизации конечного недетерминированного автомата. Множество состояний автомата подмножеств определяется как множество $\mathcal{P}'(Q)$ всех непустых подмножеств множества Q, а функция переходов – как естественное продолжение функции δ на множество $\mathcal{P}'(Q) \times \Sigma$ (это продолжение также обозначается через δ). Рассмотрим некоторое множество состояний автомата $Q' = \{q_1, \ldots, q_k\}$, тогда $\delta(Q', a) = \{\delta(q_1, a), \ldots, \delta(q_k, a)\}$.

На рис. 0.4 приведен автомат подмножеств для автомата $\mathscr{C}_4$, представленного на рис. 0.1. Нетрудно видеть, что некоторое слово $w \in \Sigma^*$ синхронизирует автомат $\mathscr{A}$ тогда и только тогда, когда оно читается вдоль пути в автомате $\mathcal{P}(\mathscr{A})$ из состояния Q в некоторое одноэлементное подмножество. Таким образом, задача проверки синхронизируемости автомата сводится к задаче достижимости в графе, которая легко решается поиском в ширину (см. [**4**]). Слово, прочитанное вдоль пути, найденного поиском в ширину, очевидно, будет кратчайшим синхронизирующим словом данного автомата. Такой способ поиска кратчайшего слова будет использоваться нами в главе 2. На рис. 0.4 жирным шрифтом выделены стрелки пути, вдоль которого читается кратчайшее синхронизирующее слово.

Отметим, что приведенный алгоритм не является вычислительно эффективным, поскольку использует автомат подмножеств, число состояний которого экспоненциально зависит от числа состояний исходного автомата. Существует полиномиальный алгоритм определения синхронизируемости данного автомата. Этот алгоритм разработан Эпштейном [**27**] на основании следующего критерия синхронизируемости, предложенного Черни [**24**]:

Лемма 0.1 Автомат $\mathscr{A} = (Q, \Sigma, \delta)$ является синхронизируемым тогда и только тогда, когда для любой пары состояний $p, q \in Q$ существует слово $w \in \Sigma^*$ такое, что $pw = qw$.

Иными словами, автомат является синхронизируемым тогда и толь-

ко тогда, когда любую пару $(\mathbf{p}, \mathbf{q})$ состояний можно "склеить", или "слить", т. е. подходящим словом перевести $\mathbf{p}$ и $\mathbf{q}$ в некоторое состояние $\mathbf{r}$. Этот критерий будет использоваться нами при доказательстве синхронизируемости в главе 3.

Алгоритм Эпштейна работает за время $O(|Q|^2)$, однако он отвечает только на первый вопрос, на выходе он не строит никакого синхронизирующего слова[2]. Алгоритм, строящий некоторое синхронизирующее слово автомата, также предложен Эпштейном [**27**], за время $O(|Q|^3)$ он строит синхронизирующее слово длины $O(|Q|^3)$. Что касается последнего вопроса – поиска кратчайшего синхронизирующего слова – существенно улучшить алгоритм с автоматом подмножеств не удастся. Задача, в которой для заданного автомата $\mathscr{A}$ и заданного натурального числа ℓ требуется определить, имеет ли автомат $\mathscr{A}$ синхронизирующее слово длины не больше ℓ, является NP-полной[3] [**27**].

Самотий [**55**] указал, что задача проверки того, что кратчайшее слово, синхронизирующее автомат $\mathscr{A}$, имеет длину ровно ℓ, является NP-трудной и co-NP-трудной. Таким образом, если co-NP$\neq$NP, эта задача не может принадлежать NP. Хотя построения Самотия оказались ошибочными, заявленный результат верен и может быть доказан другими способами. Точная сложность данной задачи установлена сравнительно недавно Гавричовским [**31**] и, независимо, Ольшевским и Уммельсом [**46**]. Они показали, что задача DP-полна. Класс сложности DP (Difference Polynomial-Time) был введен Пападимитриоу и Яннакакисом [**47**]. Этот класс состоит из языков вида $L_1 \cap L_2$, L_1 из NP, а L_2 из coNP.

Более того, не существует полиномиального алгоритма, вычисляю-

[2]Обозначения O, o и Θ в работе полагаются известными. Формальное определение o вводится в §3.1, более подробно с понятиями можно ознакомиться в книге [**4**].

[3]Вопросы сложности алгоритмов не затрагиваются в диссертации и обсуждаются в данном параграфе сугубо для введения читателя в проблематику и обоснования актуальности проблемы. Поскольку владение понятийным аппаратом теории сложности не требуется для понимания результатов диссертации, определения в работе не приводятся. С терминологией можно ознакомиться в [**4**].

щего длину кратчайшего синхронизирующего слова с "хорошим" приближением. Берлинков [20] показал, что не существует полиномиального алгоритма, вычисляющего длину кратчайшего синхронизируемого слова с любой конечной относительной погрешностью (в предположении $\mathrm{P} \neq \mathrm{NP}$).

0.2 Синхронизируемость автоматов в экстремальном случае, гипотеза Черни

В связи с тем, что задача нахождения кратчайшего синхронизирующего слова для конкретного автомата трудна, особую актуальность приобретает вопрос оценки длины кратчайшего синхронизирующего слова сверху. Пусть $\mathscr{A}$ – автомат с n состояниями (далее для краткости будем называть такие автоматы n-автоматами, символом n всегда будем обозначать число состояний), пусть $\mathscr{A}$ синхронизируем. Длину кратчайшего синхронизирующего слова автомата $\mathscr{A}$ будем обозначать через $\mathfrak{C}(\mathscr{A})$. Отображение, ставящее в соответствие автомату $\mathscr{A}$ число $\mathfrak{C}(\mathscr{A})$, будем называть *функцией Черни*. Аналогичным образом введем функцию Черни для классов синхронизируемых автоматов. Для натурального числа n и класса синхронизируемых автоматов $\mathscr{K}$ через $\mathfrak{C}_{\mathscr{K}}(n)$ обозначим наибольшую длину кратчайших синхронизирующих слов среди всех синхронизируемых n-автоматов из класса $\mathscr{K}$, т. е.

$$\mathfrak{C}_{\mathscr{K}}(n) = \max_{\mathscr{A} \in \mathscr{K},\ |Q_{\mathscr{A}}|=n} \mathfrak{C}(\mathscr{A}).$$

Эту функцию называют функцией Черни, ограниченной на класс $\mathscr{K}$. Символом $\mathfrak{C}(n)$ будем обозначать функцию Черни для класса всех n-автоматов.

В 1964 году Черни [24] построил бесконечную серию n-автоматов $\mathscr{C}_n$ над двухбуквенным алфавитом, кратчайшее синхронизирующее слово которых имеет длину $(n-1)^2$, т. е. для которых $\mathfrak{C}(\mathscr{C}_n) = (n-1)^2$. Автомат $\mathscr{C}_4$ приведен на рис 0.1. Позднее Черни предположил, что данная серия реализует наихудший в смысле скорости синхронизации случай, т. е. что ***любой синхронизируемый n-автомат обладает синхронизирующим словом длины не более*** $(n-1)^2$. Во введенных обозначениях это можно записать равенством $\mathfrak{C}(n) = (n-1)^2$. Это предположение, впоследствие получившее название *гипотезы Черни*, все еще остается открытым.

Это одна из самых "старых" открытых проблем в теории автоматов, при том, что гипотеза привлекает внимание многочисленных исследователей, работы, связанные с различными продвижениями в этой области, публикуются ежегодно (например, [15, 26, 40, 54, 59, 62, 64]).

Долгое время наилучшей верхней оценкой $\mathfrak{C}(n)$ была кубическая оценка, полученная в 1983 году Пэном [49] с использованием комбинаторного результата Франкля [29]. Пэн показал, что $\mathfrak{C}(n) \leq \frac{n^3-n}{6}$. Сравнительно недавно, в 2011 году, результат Пэна был незначительно улучшен Трахтманом [63], который показал, что $\mathfrak{C}(n) \leq \frac{n(7n^2+6n-16)}{48}$. Таким образом, с учетом того, что серия Черни доставляет нижнюю оценку для функции Черни, текущее состояние проблемы можно выразить следующим двойным неравенством:

$$(n-1)^2 \leq \mathfrak{C}(n) \leq \frac{n(7n^2+6n-16)}{48}.$$

Оставаясь открытой в общем случае, гипотеза Черни доказана для большого количества частных классов автоматов. Приведем некоторые результаты из этой области.

1. Первый класс, который мы рассмотрим, это класс *циклических* автоматов, обозначим его через *cycle*. Автомат называется циклическим, если одна из его букв действует на множестве состояний как циклическая перестановка. Этот класс автоматов интересен тем, что в него попадает серия автоматов Черни, соответственно, $\mathfrak{C}_{\mathtt{cycle}}(n) \geq (n-1)^2$. В 1998 году Дюбук [26] нашел для этих автоматов и оценку сверху, показав, что $\mathfrak{C}_{\mathtt{cycle}}(n) \leq (n-1)^2$. Таким образом,

$$\mathfrak{C}_{cycle}(n) = (n-1)^2.$$

В работе [19] Беал, Берлинков и Перрен рассматривают класс *однокластерных* автоматов – обобщение класса циклических автоматов. Автомат называется однокластерным, если он имеет "связную" букву, т. е. такую букву $a \in \Sigma$, что для любой пары состояний $p, q \in Q$ найдутся натуральные числа k, ℓ такие, что $pa^k = qa^\ell$. Граф действия этой буквы представляет собой один цикл, из которого "растут" деревья. Авторы показали, что для этого класса автоматов справедливо неравенство:

$$\mathfrak{C}_{cluster}(n) \leq 2n^2 - 7n + 7.$$

Стейнберг [60] усиливает результат Беал, Берлинкова и Перрена, показывая, что

$$\mathfrak{C}_{cluster}(n) \leq 2n^2 - 9n + 14.$$

Кроме того, Стейнберг доказывает, что для подкласса однокластерных автоматов – однокластерных автоматов с циклом простой длины – выполняется гипотеза Черни.

2. В 2003 году Кари [40] получил верхнюю оценку функции Черни для класса синхронизируемых автоматов, чей граф является *эйлеровым*, т. е. входящая степень каждой вершины равна исходящей. Гусев [34] в 2011 году получил нижнюю оценку функции Черни для таких автоматов. Таким образом, была доказана справедливость следующего двойного неравенства.

$$\frac{n^2 - 3n + 4}{2} \leq \mathfrak{C}_{euler}(n) \leq n^2 - 3n + 3.$$

Для нижней оценки построен пример, на котором она достигается; вопрос точности верхней оценки остается открытым.

3. *Моноидом переходов* $M(\mathscr{A})$ автомата $\mathscr{A} = (Q, \Sigma, \delta)$ называется моноид преобразований множества состояний Q, порожденный действием букв алфавита Σ на этом множестве. Моноид называется *апериодическим*, если все его подгруппы тривиальны; автомат называется *апериодическим*, если его моноид переходов является апериодическим. Апериодические автоматы играют важную роль в теории формальных языков. В теории синхронизируемых автоматов этот класс интересен тем, что верхняя оценка функции Черни для него существенно отличается от нижней. Первая получена в 2007 году Трахтманом [62], вторая – в 2005 году Ананичевым [1, 12]. Было показано, что верно следующее двойное неравенство:

$$n + \left\lfloor \frac{n-1}{2} \right\rfloor \leq \mathfrak{C}_{aper}(n) \leq \frac{n(n-1)}{2}.$$

4. Рассмотрим класс *автоматов с нулем*, т. е. автоматов, обладающим выделенным состоянием 0, таким что $0a = 0$ для любой буквы a. Обозначим этот класс через *zero*. Ясно, что если автомат с 0 синхронизируем, то 0 достижим из любого другого состояния автомата и, поэтому, длина синхронизирующего слова не больше суммы длин кратчайших

путей из вершин автомата в 0. Следовательно, легко получается оценка сверху $\mathfrak{C}_{zero}(n) \leq \frac{n(n-1)}{2}$ (см. например, [54]). Более того, для каждого n несложно построить синхронизируемый n-автомат с нулем, имеющий $n-1$ букв, для которого кратчайшее синхронизирующие слово имеет длину $\frac{n(n-1)}{2}$. Следовательно,

$$\mathfrak{C}_{zero}(n) = \frac{n(n-1)}{2}.$$

Гораздо более интересной задачей является построение серий синхронизируемых автоматов с нулем с постоянным количеством букв и квадратичной длиной синхронизирующего слова, т. е. рассмотрение класса автоматов с нулем с k символами (обозначим через $zero_k$). Для этого класса, с учетом оценки сверху, в [9,42] доказано неравенство для функции Черни

$$\frac{n^2}{4} + \frac{n}{2} - 1 \leq \mathfrak{C}_{zero_2}(n) \leq \frac{n(n-1)}{2}.$$

Результат для автомата с нулем интересен тем, что ввиду того, что автоматы с нулем удовлетворяют гипотезе Черни, получение оценки сверху для любого автомата можно свести к случаю, когда граф автомата сильно-связен (см. например, [64, предложение 3]).

В главе 1 мы вводим новый класс автоматов – автоматы с буквой дефекта 2 (обозначим этот класс *def2*). *Дефект* буквы определяется стандартно как дефект отображения, порождаемого этой буквой, $\mathrm{df}(a) = |Q| - |\delta(Q, a)|$. Мотивацией изучения этого класса служит тот факт, что квадратичность верхней оценки функции Черни для этого класса влечет ее квадратичность для всех автоматов, или, точнее, из неравенства $\mathfrak{C}_{def2}(n) \leq f(n)$, где $f(n)$ – квадратичная функция, следует неравенство $\mathfrak{C}(n) \leq 16f(n)$. В главе 1 нами получены следующие нижние оценки функции Черни для описанного класса автоматов:

$$\mathfrak{C}_{def2}(n) \geq (n-2)^2 + 1,$$

$$\mathfrak{C}_{def2}(n) \geq (n-1)(n-2), \text{если } n \text{ нечетно}.$$

Отметим, что полученные нами в главе 1 бесконечные серии автоматов представляют самостоятельный интерес в силу того, что на текущий момент известно очень мало серий *медленно синхронизируемых автоматов*, т. е. автоматов с кратчайшим синхронизирующим словом длины $\Theta(n^2)$. Длительное время единственной известной бесконечной серией

была серия Черни, кроме нее было известно только несколько отдельных медленно синхронизируемых автоматов с небольшим числом состояний [39,52,61]. В нашей работе [68] в 2007 году были описаны две первые серии автоматов, существенно отличных от серии Черни. Сравнительно недавно, в 2010 году, в работе Ананичева, Волкова и Гусева было получено еще некоторое количество бесконечных серий, а также предложен новый метод доказательства оценки длины кратчайшего синхронизирующего слова, проходящий в том числе для серии Черни и для одной из наших серий [13].

В главе 2 мы также обращаемся к автоматам, имеющим фиксированный дефект выделенной буквы. В данном случае мы рассматриваем дефект буквы, близкий к числу состояний автомата, т. е. дефект в некотором смысле экстремальный. В качестве мотивации рассмотрения этого класса отметим, что доля автоматов с большим дефектом выделенной буквы довольно существенна. В монографии [37] Хиггинс показал, что математическое ожидание дефекта отображения n-элементного множества в себя, выбранного равномерно случайно из множества всех таких отображений, стремится к $\frac{n}{e}$ при $n \to \infty$. Применив схожие рассуждения, можно получить, что дисперсия этого дефекта стремится к $\frac{n(e-1)}{e^2}$. Используя неравенство Чебышева, получим, что с высокой вероятностью дефект случайного отображения (а значит и дефект буквы в случайном автомате) имеет порядок $\Theta(n)$. В главе 2 нами доказано несколько нижних оценок функции Черни для автоматов с различными значениями дефекта выделенной буквы.

0.3 Синхронизируемость автоматов в среднем случае

С точки зрения практического применения синхронизируемых автоматов представляется более важным изучить поведение длины кратчайшего синхронизирующего слова в среднем случае, нежели исследовать экстремальные – квадратичные – значения этой длины, которые, как уже отмечалось ранее, крайне редки.

Результаты вычислительных экспериментов показывают, что поведение этой величины в среднем существенно отличается от ее поведения экстремальных случаях. Скворцов и Типикин [57] с помощью вычис-

лительного эксперимента над автоматами со 100 состояниями получили оценку средней длины кратчайшего синхронизирующего слова случайного n-автомата с двумя буквами входного алфавита, которая оказалась сублинейной, а именно равной $1,95n^{0,55}$. Кисилевич, Ковальски и Сзыкула [41] провели эксперименты над автоматами с 300 состояниями и получили оценку, приблизительно равную $2,5(n-5)^{0,5}$.

Синхронизируемость случайных автоматов ранее не привлекала внимание исследователей, при этом, для ряда других характеристик конечных автоматов получены оценки как для всего множества автоматов, так и для почти всех автоматов[4], т. е. в среднем случае. Перед тем, как привести обзор подобных результатов, дадим строгое определение случайного автомата.

Рассмотрим множество состояний Q и алфавит Σ. Выберем функцию переходов δ равномерно случайно из множества функций $\{\delta : Q \times \Sigma \to \to Q\}$. Получившаяся тройка (Q, Σ, δ) определяет *случайный (конечный детерминированный) автомат*. Следует отметить, что случайный автомат может быть построен следующим образом: для каждого состояния $q \in Q$ и для каждой буквы $a \in \Sigma$ выбираем $q' = \delta(q, a)$ равномерно случайно из Q.

Обозначим через $\mathcal{A}(n, k)$ множество всех конечных автоматов $\mathscr{A} = = (Q, \Sigma, \delta)$ таких, что $|Q| = n \geq 2$, $|\Sigma| = k \geq 1$.

Пусть $q_1, q_2 \in Q$ – состояния некоторого автомата $\mathscr{A} = (Q, \Sigma, \delta)$. *Отклонением* состояния q_2 от q_1 называется величина $d_{\mathscr{A}}(q_1, q_2)$, равная длине кратчайшего слова $w_{q_1 \to q_2} \in \Sigma^*$ такого, что $q_1.w_{q_1 \to q_2} = q_2$, если оно существует, и бесконечности в противном случае. Величина $d_{\mathscr{A}} = = \max d_A(q_i, q_j)$ называется *диаметром* автомата $\mathscr{A}$, максимум берется по всем парам состояний q_i, q_j таким, что q_j достижимо из q_i.

Нетрудно видеть, что диаметр любого автомата оценивается сверху числом $n-1$, причем эта оценка точна. Результат впервые был сформулирован и доказан Муром в [44]. Барздинь и Коршунов показали, что верно следующее утверждение.

[4]Под *почти всеми автоматами* мы понимаем долю автоматов, стремящуюся к 1 при $n \to \infty$.

Теорема 0.1 (Барздинь, Коршунов, 1967)
Пусть $k \geq 2$, $n + k \to \infty$. Тогда не менее, чем $|\mathcal{A}(n,k)|(1-1/k)$ автоматов $\mathscr{A} \in \mathcal{A}(n,k)$ имеют диаметр $d_{\mathscr{A}}$, удовлетворяющий неравенствам:

$$\log_n(k) \leq d_{\mathscr{A}} < c_1 \log_n(k),$$

где $c_1 \to 1$ при $n \to \infty$.

В [2] приводится доказательство данной теоремы при условии, что $k = const \geq 2$. В более поздней работе [7] Коршунов отмечает, что результат верен при любом $k \geq 2$.

Следующий параметр определяется для т. н. автоматов с выходом, или *автоматов Мили*. Напомним, что автоматом Мили называется пятерка $\mathscr{B} = (Q, \Sigma, \Lambda, \delta, \lambda)$, где Q – множество состояний, Σ, Λ – соответственно входной и выходной алфавиты, $\delta : Q \times \Sigma \to Q$ – функция переходов, $\lambda : Q \times \Sigma \to \Lambda$ – функция выходов. Иными словами, автомат Мили представляет собой конечный детерминированный автомат, в котором стрелки дополнительно подписаны буквами выходного алфавита. Аналогично множеству $\mathcal{A}(n,k)$ мы будем определять множество $\mathcal{B}(n,m,k)$ всех автоматов Мили с n состояниями, k буквами входного алфавита и m выходного.

Степенью различимости состояний q_1 и q_2 автомата Мили $\mathscr{B}$ называется величина $h_{\mathscr{B}}(q_1, q_2)$, равная длине кратчайшего слова $w_{q_1,q_2} \in \Sigma^*$ такого, что $\lambda(q_1, w_{q_1,q_2}) \neq \lambda(q_1, w_{q_1,q_2})$, если оно существует, и бесконечности в противном случае. Величина $h_{\mathscr{B}} = \max h_{\mathscr{B}}(q_i, q_j)$ называется *степенью различимости* автомата B, максимум берется по всем парам неэквивалентных состояний q_i, q_j.

Аналогично оценке для диаметра автомата (отметим, что результат для диаметра распространяется на автоматы Мили без изменений), оценка сверху степени различимости также точна, составляет $n - 1$ и описана Муром в [44].

Теорема 0.2 (Коршунов, 1967, [5])
При любых $n \geq 2$, $m \geq 2$, $k \geq 2$ и $n + k \to \infty$ среди всех попарно неизоморфных (по состояниям) автоматов из $\mathcal{B}(n,m,k)$ почти все автоматы имеют степень различимости $h_{\mathscr{B}}$, удовлетворяющую неравенствам:

$$\log_n \log_m(k) \leq h_{\mathscr{B}} < [\log_n \log_m(k)] + 4.$$

Последний параметр, который мы рассмотрим, это длина кратчайшего однородного эксперимента по распознаванию заключительного состояния автомата Мили, т. е. длины заранее определенного слова, применение которого к автомату позволяет, исследуя выходную последовательность, определить его заключительное состояние. В современных источниках (например, [10]) эксперименты по распознаванию заключительного состояния часто называются *установочными последовательностями*. Обозначим эту длину через $u_{\mathscr{B}}$. Однородные эксперименты рассматриваются на множестве $\mathcal{B}_1(n, m, k) \subset \mathcal{B}(n, m, k)$ *приведенных* автоматов, т. е. автоматов, все состояния которых попарно различимы.

Оценка длины эксперимента в экстремальном и среднем случаях получены соответственно Хиббардом [35] и Коршуновым [6].

Теорема 0.3 (Хиббард, 1961)
Для любого автомата $\mathscr{B} \in \mathcal{B}_1(n, m, k)$

$$u_{\mathscr{B}} \leq n(n-1)/2.$$

Теорема 0.4 (Коршунов, 1969)
При любых $m = \mathrm{const} \geq 2$ и $n = \mathrm{const} \geq 2$ для почти всех автоматов $\mathscr{B} \in \mathcal{B}_1(n, m, k)$ выполняется неравенство

$$u_{\mathscr{B}} < 5 \log_n k.$$

Отметим, что оценка Хиббарда является неулучшаемой для автоматов Мили[5].

[5]Результат Хиббарда может быть улучшен для *автоматов Мура*, отличающихся от автоматов Мили тем, что выходной буквой у них помечены не переходы, а состояния. Или, что эквивалентно, все стрелки, выходящие из одного состояния, помечены одной и той же буквой. Соответствующий результат был получен Карацубой в 1960 году [3].

Теорема 0.5 (Карацуба, 1960)
Для любого приведенного автомата Мура $\mathscr{D}$

$$u_{\mathscr{D}} \leq (n-1)(n-1)/2 + 1.$$

Результат Коршунова справедлив как для автоматов Мили, так и для автоматов Мура.

Как мы видим, поведение параметров автоматов, связанных, как и длина кратчайшего синхронизирующего слова, с длинами путей в автоматах, в среднем случае существенно отличается от оценки сверху, которая, заметим, в данном случае точна. Особенно интересен последний пример. Однородные эксперименты и синхронизирующие слова довольно близки по сути: применяя их к некоторому неизвестному состоянию конечного автомата, мы получаем другое состояние, о котором у нас уже есть информация – мы либо знаем его заранее (случай синхронизируемости), либо можем определить на основании выхода (случай однородного эксперимента). Кроме того, они появились из схожих соображений, оба используются в тестировании реагирующих систем и совместно исследуются [**56**].

Все приведенные обстоятельства делают изучение синхронизируемости случайных автоматов, вычисление *наиболее вероятной* длины кратчайшего синхронизирующего слова не только важным с практической точки зрения, но и интересным с позиции теоретических исследований.

Начиная исследования в новой области, мы поставили следующие вопросы:

1. Какой размер входного алфавита достаточен, чтобы почти все автоматы над алфавитом этого размера были синхронизируемы, и какой будет наиболее вероятная длина кратчайшего синхронизирующего слова для таких автоматов?

2. Какой размер входного алфавита достаточен, чтобы почти все автоматы над алфавитом этого размера были синхронизируемы и удовлетворяли гипотезе Черни?

3. Какой размер входного алфавита достаточен, чтобы автомат над алфавитом этого размера был синхронизируем с конечной вероятностью[6]?

На первые два вопроса дает частичный ответ результат, полученный Хиггинсом в 1988 году [**36**]. Результат Хиггинса касается случайных отображений, но может быть интерпретирован в терминах конечных автоматов. Хиггинс показал, что композиция $2n$ случайных отображений

[6] *Конечной* мы называем вероятность, ограниченную снизу некоторой положительной константой при $n \to \infty$.

множества размера n в себя с высокой вероятностью имеет образ размерности 1. В терминах теории автоматов это означает, что случайный автомат с алфавитом размера больше $2n$ с высокой вероятностью синхронизируем словом длины $2n$ (т. е. меньшим, чем устанавливается гипотезой Черни). В самом деле, если мы выберем автомат равномерно случайно из множества всех автоматов на n состояниях с алфавитом из $2n$ букв, то действие слова, составленного из всех букв алфавита, на этот автомат будет эквивалентно отображению, представляющему собой композицию $2n$ случайных отображений.

Мы показали, что верхняя оценка размера алфавита $2n$ может быть улучшена в контексте обоих вопросов. В главе 3 показано, что если размер алфавита больше $72 \ln n$, то автомат синхронизируем с высокой вероятностью (§3.2), а если алфавит состоит более чем из $n^{1/2+\epsilon}$ букв для некоторого положительного числа ϵ, то с высокой вероятностью автомат удовлетворяет гипотезе Черни (§3.3). Кроме того, в главе 3 дан ответ и на третий вопрос: показано, что автомат над четырехбуквенным алфавитом синхронизируем с конечной вероятностью (§3.4).

В 2011 году Кэмерон, так же, как и Хиггинс, изучая случайные отображения, выдвинул гипотезу, что случайный автомат уже над двухбуквенным алфавитом синхронизируем с вероятностью $1-o(1)$ при $n \to \infty$ [22]. Предположение Кэмерона полностью согласуется с результатами вычислительных экспериментов, однако остается недоказанным теоретически.

0.4 Апробация результатов

Основные результаты диссертации опубликованы в [67–72]. Совместные работы [69–71] с Е. С. Скворцовым выполнены в нераздельном соавторстве. Совместные работы [67, 68] с Д. С. Ананичевым и М. В. Волковым содержат два независимых результата, один из которых получен автором самостоятельно, второй – в нераздельном соавторстве. Работы [67, 68, 70] опубликованы в изданиях, входящих в перечень утвержденных ВАК.

Ссылки на результаты диссертации присутствуют в работах других авторов: [13, 21, 25, 53, 57–60, 65].

Основные результаты диссертации докладывались на следующих кон-

ференциях и семинарах:

— Спутниковый семинар по словам и автоматам к международному симпозиуму “Компьютерные науки в России” WoWA’06 (Санкт-Петербург, 2006).

— Международная конференция по теории формальных языков DLT’06 (Санта-Барбара, США, 2006).

— Международная конференция “Автоматы: от математики к приложениям” AutoMathA’09 (Льеж, Бельгия, 2009).

— Русско-финский симпозиум по дискретной математике RuFiDiM (Санкт-Петербург, 2011).

— Заседания семинара “Теоретические компьютерные науки” (УрФУ).

— Заседание семинара математического факультета университета Турку (Турку, Финляндия, 2007).

Автор выражает глубокую благодарность своему научному руководителю профессору М. В. Волкову за постановки задач, помощь в подготовке текстов и постоянное внимание к работе.

Глава 1

Синхронизируемые автоматы с буквой дефекта 2

1.1 Формулировка и обсуждение результатов

Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – автомат с $|Q| \geq 3$. Если буква $a \in \Sigma$ такова, что преобразование множества состояний Q, порождаемое действием a, имеет дефект 2, то возможны в точности две следующие ситуации.

1. Существует четыре различных состояния $q_1, q_2, q_3, q_4 \in Q$ такие, что

$$\delta(q_1, a) = \delta(q_2, a) \neq \delta(q_3, a) = \delta(q_4, a).$$

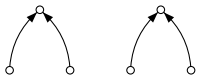
В этом случае будем говорить, что a – *буква-бактриан.*

2. Существует три различных состояния $q_1, q_2, q_3 \in Q$ такие, что

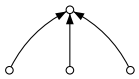
$$\delta(q_1, a) = \delta(q_2, a) = \delta(q_3, a).$$

В этом случае назовем a *буквой-дромадером.*

Рис. 1.1 иллюстрирует введенные понятия и поясняет выбранную терминологию.



Действие буквы-бактриана



Действие буквы-дромадера

Рис. 1.1: Два типа букв дефекта 2

Простым способом получения медленно синхронизируемых автоматов с буквой дефекта 2 обоих типов является модификация автомата Черни. Рассмотрим автомат Черни $\mathscr{C}_{n-1}$, состояния которого пронумерованы числами от 0 до $n-2$, а буквы входного алфавита a и b действуют следующим образом:

$$\delta(m, a) = \begin{cases} 1 & \text{для } m = 0, \\ m & \text{для } 1 < m < n-1; \end{cases} \qquad \delta(m, b) = m + 1 \pmod{n-1}.$$

Добавим к $\mathscr{C}_{n-1}$ дополнительное состояние, помеченное $n-1$, и определим на нем функцию переходов следующим образом: $\delta(n-1,a)=2$, $\delta(n-1,b)=n-1$. В результате получим n-автомат $\mathscr{C}'_n$ с буквой a, являющейся буквой-бактрианом. Определив на новом состоянии действие δ иначе, а именно $\delta(n-1,a)=1$, $\delta(n-1,b)=n-1$, получим другой n-автомат $\mathscr{C}''_n$, в котором буква a является буквой-дромадером. Обе модификации показаны на рис. 1.2.

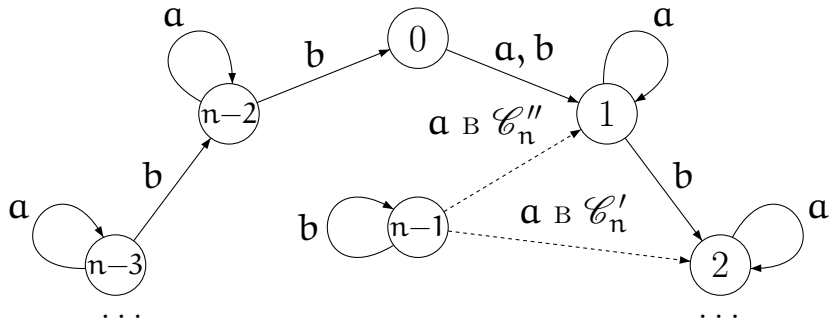


Рис. 1.2: Автоматы $\mathscr{C}'_n$ и $\mathscr{C}''_n$

Нетрудно видеть, что слово $(ab^{n-2})^{n-3}a$, синхронизирующее автомат $\mathscr{C}_{n-1}$, синхронизирует также и автоматы $\mathscr{C}'_n$ и $\mathscr{C}''_n$, причем это кратчайшее синхронизирующее слово для обоих автоматов. Следовательно, длина данного слова $(n-2)^2$ доставляет нижнюю оценку минимальной длины синхронизирующего слова n-автоматов с буквой дефекта 2 обоих типов. По аналогии с гипотезой Черни можно предположить, что эта оценка точна, однако наши результаты показывают, что это не так.

Наш первый результат существенно улучшает нижнюю границу для автоматов с буквой-бактрианом:

Теорема 1.1 Для любого нечетного $n>3$ существует синхронизируемый автомат $\mathscr{B}_n$ с n состояниями и двумя буквами входного алфавита, одна из которых – буква-бактриан, такой, что кратчайшее синхронизирующее слово $\mathscr{B}_n$ имеет длину $(n-1)(n-2)$.

Доказательство теоремы 1.1 приведено в §1.2. На наш взгляд, это доказательство представляет самостоятельный интерес, поскольку в нем, по-видимому, впервые был использован теоретико-игровой подход к задачам синхронизируемости. Позднее этот подход применялся другими авторами (например, [8]). Кроме того, он, в силу своей наглядности, нашел

применение в учебном процессе.

Заметим, что ограничение на число состояний в теореме 1.1 существенно. Если n четно, автомат, подобный $\mathscr{B}_n$, по-прежнему можно построить, однако он не будет синхронизируемым. Для $n = 6$ мы нашли четыре неизоморфных синхронизируемых автомата с двумя буквами входного алфавита, одна из которых – буква-бактриан, и кратчайшим синхронизирующим словом длины $(6-1)(6-2) = 20$, но уже для $n = 8$ наш лучший пример с буквой-бактрианом имеет длину кратчайшего синхронизирующего слова $40 < (8-1)(8-2) = 42$. Эти примеры также представлены в §1.2.

Сейчас обратимся к автоматам с буквой-дромадером. В этом случае нам удалось незначительно улучшить нижнюю границу, установленную автоматами "типа Черни" $\mathscr{C}''_n$, при этом в отличие от случая буквы-бактриана нам понадобился трехбуквенный входной алфавит.

Теорема 1.2 Для любого $n > 4$ существует синхронизируемый автомат $\mathscr{D}_n$ с n состояниями и 3 буквами входного алфавита, одна из которых – буква-дромадер, такой, что кратчайшее синхронизирующее слово $\mathscr{D}_n$ имеет длину $(n-2)^2 + 1$.

Идея доказательства теоремы 1.2 схожа с идеей доказательства теоремы 1.1, однако само доказательство более громоздко, оно приведено в §1.3.

Для $n = 5$ и $n = 6$ нами найдены примеры автоматов с тремя буквами входного алфавита, одна из которых – буква-дромадер, кратчайшее синхронизирующее слово которых на одну букву короче, чем для $\mathscr{D}_5$ и $\mathscr{D}_6$ соответственно. Полученные примеры показывают, что может существовать серия синхронизируемых n-автоматов над трехбуквенным алфавитом, имеющих букву-дромадера, длина кратчайшего синхронизирующего слова которых равна $(n-2)^2 + 2$. На текущий момент такая серия не построена.

1.2 $\mathscr{B}_n$: серия автоматов с буквой-бактрианом

Пусть $n = 2s + 1$, $s > 1$. Состояния автомата $\mathscr{B}_n$ помечены полной системой вычетов по модулю n, буквы его входного алфавита a и b действуют

на множестве состояний следующим образом:

$$\delta(m,a)=\begin{cases} m-2 \pmod n & \text{для } m=0,1,\\ m & \text{для } 1<m<n; \end{cases} \qquad \delta(m,b)=m-1 \pmod n.$$

Заметим, что a – буква-бактриан. Автомат серии с наименьшим числом состояний представлен на рис. 1.3.

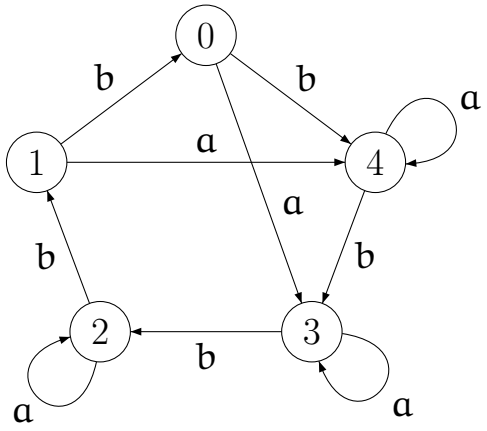


Рис. 1.3: Автомат $\mathscr{B}_5$

Для получения нижней оценки длины кратчайшего синхронизирующего слова автомата $\mathscr{B}_n$ мы воспользуемся игровым подходом: граф автомата будет служить полем некоторой игры.

Предположим, что некоторые состояния автомата покрыты *монетами*, как показано на рис. 1.4. *Ходом* в игре является применение буквы $c \in \{a,b\}$, при совершении хода монеты перемещаются по стрелкам, подписанным буквой c так, что состояние m будет покрыто монетой по завершении хода, если и только если существует состояние ℓ, покрытое монетой на начало хода такое, что $\delta(\ell,c)=m$. Если в какой-то момент в одно состояние m приходит две монеты, то, в соответствии со структурой $\mathscr{B}_n$, это означает, что $c=a$, $m=n-1$ или $m=n-2$, и состояния m и $m+2 \pmod n$ были покрыты монетами на начало хода; тогда мы оставляем на поле монету, которая покрывала m, и удаляем монету с $m+2 \pmod n$. Рис. 1.5 показывает, как меняется игровая позиция с рис. 1.4 под действием каждой из букв.

Пусть в начале игры все состояния $\mathscr{B}_n$ покрыты монетами, и пусть слово $w \in \{a,b\}^*$ действует на эту начальную позицию (действие слова

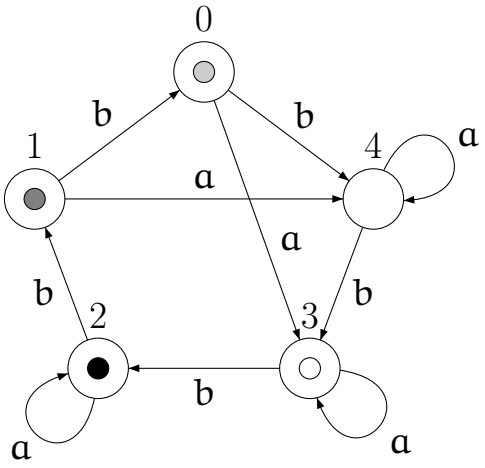


Рис. 1.4: Игровая позиция на $\mathscr{B}_5$

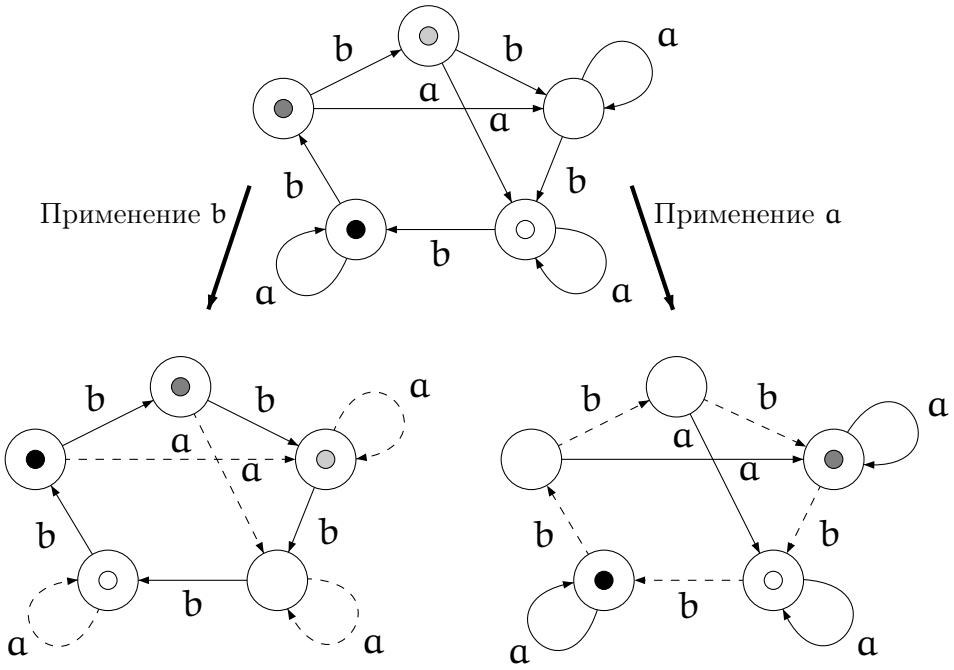


Рис. 1.5: Перемещение монет под действием букв $\mathtt{b}$ (слева) и $\mathtt{a}$ (справа)

есть последовательное действие всех букв этого слова). Нетрудно видеть, что после завершения этого действия монетами будут покрыты в точности состояния, лежащие в образе преобразования $\delta(\_, w)$. В частности, если w синхронизирует $\mathscr{B}_n$, то в результате действия w останется только одна монета.

Приведем некоторую оценку длины кратчайшего слова автомата $\mathscr{B}_n$.

Лемма 1.1 Пусть $n = 2s + 1$, $s > 1$. Тогда слово

$$(ab^{2s-1})^{s-1}ab^{2s-2}(ab^{2s-1})^{s-1}a \tag{1.1}$$

синхронизирует автомат $\mathscr{B}_n$. Соответственно, длина кратчайшего слова, синхронизирующего $\mathscr{B}_n$, не превышает длину слова (1.1), равную $2s(s-1) + 2s - 1 + 2s(s-1) + 1 = 2s(2s-1) = (n-1)(n-2)$.

Доказательство. Справедливость данной леммы проверяется непосредственно. Рассмотрим автомат $\mathscr{B}_n$, все состояния которого покрыты монетами, применим к нему слово (1.1) и убедимся, что осталась одна монета.

Применим к автомату первую букву нашего слова a. В результате, монеты, покрывавшие состояния 0 и 1, встретятся с монетами, покрывавшими состояния $n-1$ и $n-2$, и будут удалены (мы будем называть такие состояния, не покрытые монетами, *дырками*), остальные монеты останутся на месте. Применим b^{2s-1}. Все монеты сдвинутся по часовой стрелке на $2s-1$ шаг и будут покрывать все состояния, кроме 2 и 3. Теперь применим a. Поскольку состояния 0, 1, $n-2$ и $n-1$ по-прежнему покрыты монетами, результат будет тот же, что и при первом применении буквы a, в состояниях 0 и 1 образуются новые дырки, появится последовательность из четырех дырок в состояниях 0, 1, 2, 3. Последовательность дырок мы будем называть *лакуной*. Применение b^{2s-1} сдвинет лакуну в состояния 2, 3, 4, 5. Нетрудно видеть, что каждое последующее применение ab^{2s-1} увеличивает лакуну на два состояния против часовой стрелки. Таким образом, после применения префикса нашего слова $(ab^{2s-1})^{s-1}$ лакуна будет состоять из $2s-2$ дырок, монетами будут покрыты только состояния 0, 1, $n-1$. Следующее применение a увеличит числа дырок еще на единицу, монеты останутся только на состояниях $n-1$ и $n-2$. Интересно, что нам потребовалось меньше половины слова, чтобы сократить число монет с n до двух, бóльшая часть слова нужна, чтобы удалить всего одну монету. Сейчас монеты занимают соседние состояния, для того, чтобы удалить одну из монет, нужно, чтобы они располагались через одно состояние.

Приступим к удалению последней монеты. Применение b^{2s-2} приведет монеты в состояния 1 и 2. Применим a, монета в 2 останется на месте, монета из 1 переместится в $n-1$. После применения b^{2s-1} монеты переместятся в состояния 1 и 4. Еще одно применение ab^{2s-1} сначала переведет

монеты в $n-1$, 4, а затем в 1, 6. Очевидно, что после каждого следующего применения этого подслова одна монета оказывается в состоянии 1, а вторая каждый раз сдвигается на два состояния против часовой стрелки. Таким образом, применив подслово ab^{2s-1} $s-1$ раз, мы приведем одну монету в 1, а другую в $2+2(s-1) = n-1$. Последнее применение a удаляет последнюю "лишнюю" монету и завершает доказательство. □

Отметим, что у $\mathscr{B}_n$ есть по крайней мере еще одно синхронизирующее слово той же длины, это слово $ab^{2s-2}(ab^{2s-1})^{s-3}ab^{2s}ab^{2s-2}(ab^{2s-1})^{s-1}a$.

Для завершения доказательства теоремы 1.1 осталось показать, что длина всех синхронизирующих слов для $\mathscr{B}_n$ не меньше $(n-1)(n-2)$, т. е. что приведенная оценка точна.

Для доказательства этого факта воспользуемся следующей идеей. Пусть заданы синхронизирующее слово w и начальное положение монет P_0, при котором монеты покрывают все n состояний $\mathscr{B}_n$. Обозначим через P_i, $0 \le i \le |w|$, игровую позицию, которая возникает после применения к начальной позиции P_0 префикса w длины i. Каждой позиции P_i сопоставим целочисленный параметр $\mathrm{wg}(P_i)$ (так называемый *вес* позиции), для которого выполняются следующие три условия:

(i) $\mathrm{wg}(P_0) \ge (n-1)^2$;

(ii) $\mathrm{wg}(P_{|w|}) \le n-1$;

(iii) для любого $i = 1, \ldots, |w|$, действие i-й буквы слова w уменьшает вес позиции P_{i-1} не более, чем на единицу, т. е. $1 \ge \mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)$.

Очевидно, что если такая весовая функция существует, то суммируя все неравенства (iii) и подставляя в результат (i) и (ii), мы получим требуемое неравенство:

$$|w| = \sum_{i=1}^{|w|} 1 \ge \sum_{i=1}^{|w|} \bigl(\mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i)\bigr) = \mathrm{wg}(P_0) - \mathrm{wg}(P_{|w|}) \ge$$
$$\ge (n-1)^2 - (n-1) = (n-1)(n-2).$$

Осталось построить весовую функцию, удовлетворяющую условиям (i)–(iii). Это непростая задача, поскольку в результате некоторых ходов могут быть удалены две монеты сразу. Чтобы преодолеть эту трудность, сделаем монеты отличимыми друг от друга, это позволит ввести зависимость значений весовой функции от применяемого синхронирующего сло-

ва, в то время как универсальная функция, работающая одинаково для всех слов, может и не существовать.

Итак, зафиксируем синхронизирующее слово w и начальную позицию P_0 из n монет, покрывающих состояния автомата $\mathscr{B}_n$. Как уже говорилось ранее, действие w на P_0 удаляет $n-1$ монету. Единственную оставшуюся монету будем называть *золотой* и обозначать G. Теперь зафиксируем позицию P_i, $0 \leq i \leq |w|$. Для каждой монеты C, которая присутствует в этой позиции, обозначим через $m_i(C)$ состояние, которое покрывает C. Обозначим через $d_i(C)$ наименьшее неотрицательное целое число такое, что $\delta\left(m_i(C), b^{2d_i(C)}\right) = m_i(G)$. Проще говоря, $d_i(C)$ – это число двойных шагов, отмеренных по часовой стрелке по "основному циклу" $\mathscr{B}_n$ от состояния, покрытого C, до состояния, покрытого золотой монетой. Определим *вес* монеты C в позиции P_i как

$$\mathrm{wg}(C, P_i) = (n-1) \cdot d_i(C) + m_i(C).$$

(Отметим, что здесь мы умножаем и складываем целые числа, а не вычеты по модулю n.) Для иллюстрации этого определения предположим, что черная монета в игровой позиции, изображенной на рис. 1.4, золотая. Тогда вес белой монеты в этой позиции равен $4 \cdot 3 + 3 = 15$, поскольку белая монета покрывает состояние 3, и для того, чтобы достичь из него состояние 2, покрытое золотой монетой, нужно совершить 3 двойных шага по часовой стрелке. Аналогично, вес темно-серой монеты на рис. 1.4 равен $4 \cdot 2 + 1 = 9$, а вес светло-серой – $4 \cdot 4 + 0 = 16$. Вес черной(=золотой) монеты равен $4 \cdot 0 + 2 = 2$, поскольку, по определению, вес золотой монеты в любой позиции равен номеру покрываемого ей состояния.

Теперь определим *вес* $\mathrm{wg}(P_i)$ позиции P_i как максимум из весов монет этой позиции. Например, вес позиции, изображенной на рис. 1.4, равен 16 (если, как и в примере выше, золотой считать черную монету). Осталось убедиться, что определенная нами весовая функция удовлетворяет условиям (i)–(iii).

Условие (i): $\mathrm{wg}(P_0) \geq (n-1)^2$**.** В начальной позиции все состояния покрыты монетами. Рассмотрим монету C, покрывающую состояние $m_0(G) - 2 \pmod{n}$, то есть состояние, находящееся в одном двойном шаге по часовой стрелке от состояния, покрытого золотой монетой. Нетрудно видеть, что $d_0(C) = n-1$, откуда $\mathrm{wg}(C, P_0) = (n-1) \cdot (n-1) + m_0(C) \geq$

$\geq (n-1)^2$. Поскольку вес позиции не меньше веса любой монеты в этой позиции, получаем $\mathrm{wg}(P_0) \geq (n-1)^2$.

Условие (ii): $\mathrm{wg}(P_{|w|}) \leq n-1$. В финальной позиции остается только одна золотая монета G, значит, вес позиции $P_{|w|}$ равен весу G. Как было отмечено ранее, $\mathrm{wg}(G, P_i) = m_i(G)$ для любой позиции P_i, откуда $m_i(G) \leq n-1$.

Условие (iii): $\mathrm{wg}(P_{i-1}) - \mathrm{wg}(P_i) \leq 1$ для любого $i = 1, \ldots, |w|$. Зафиксируем C – монету максимального веса в позиции P_{i-1}. Сначала рассмотрим случай, когда переход позиции P_{i-1} в позицию P_i произошел по букве b. Вспомним, что $\delta(m, b) = m - 1 \pmod n$, откуда $d_i(C) = d_{i-1}(C)$ (взаимное положение монет не изменилось) и

$$m_i(C) = \begin{cases} m_{i-1}(C) - 1, & \text{если } m_{i-1}(C) > 0, \\ n-1, & \text{если } m_{i-1}(C) = 0. \end{cases}$$

Таким образом,

$$\begin{aligned} &\mathrm{wg}(P_i) \geq \mathrm{wg}(C, P_i) = (n-1) \cdot d_i(C) + m_i(C) \geq \\ &\geq (n-1) \cdot d_{i-1}(C) + m_{i-1}(C) - 1 = \mathrm{wg}(C, P_{i-1}) - 1 = \mathrm{wg}(P_{i-1}) - 1. \end{aligned}$$

Теперь положим, что переход из позиции P_{i-1} в позицию P_i произошел по букве a. Вспомним, что a переводит состояния 0 и 1 в состояния $n-2$ и $n-1$ соответственно (то есть перемещает на один двойной шаг по часовой стрелке) и оставляет на месте все другие состояния. Если монета C покрывает состояние, отличное от 0 и 1, то $m_i(C) = m_{i-1}(C)$. Отсюда

$$d_i(C) = \begin{cases} d_{i-1}(C), & \text{если золотая монета } G \text{ покрывает состояние,} \\ & \text{отличное от } 0 \text{ и } 1, \\ d_{i-1}(C) + 1, & \text{если } G \text{ покрывает } 0 \text{ или } 1. \end{cases}$$

В результате

$$\begin{aligned} &\mathrm{wg}(P_i) \geq \mathrm{wg}(C, P_i) = (n-1) \cdot d_i(C) + m_i(C) \geq \\ &\qquad \geq (n-1) \cdot d_{i-1}(C) + m_{i-1}(C) = \mathrm{wg}(C, P_{i-1}) = \mathrm{wg}(P_{i-1}). \end{aligned}$$

То есть переход из позиции P_{i-1} в позицию P_i не уменьшает вес.

Осталось рассмотреть подслучай, когда монета C покрывает состояние 0 или 1. Поскольку оба варианта анализируются совершенно одинаково, будем считать, что монета C покрывает состояние 0. Тогда в позиции P_i состояние $n-2$ будет покрыто монетой C' (которая может совпасть с C, а может не совпасть). Если в позиции P_{i-1} золотая монета G покрывает 0 или 1, то $d_i(C') = d_{i-1}(C)$, откуда

$$\begin{aligned}\mathrm{wg}(P_i) \geq \mathrm{wg}(C', P_i) = (n-1)\cdot d_i(C') + n - 2 > \\ > (n-1)\cdot d_{i-1}(C) = \mathrm{wg}(C, P_{i-1}) = \mathrm{wg}(P_{i-1}).\end{aligned}$$

Как мы видим, в данном случае вес даже возрастает. Наконец, если монета G покрывает состояние, отличное от 0 и 1, она не переместится, откуда $d_i(C') = d_{i-1}(C) - 1$. Следовательно,

$$\begin{aligned}&\mathrm{wg}(P_i) \geq \mathrm{wg}(C', P_i) = (n-1)\cdot d_i(C') + n - 2 = \\ &= (n-1)\cdot(d_{i-1}(C) - 1) + n - 2 = (n-1)\cdot d_{i-1}(C) - 1 = \\ &= \mathrm{wg}(C, P_{i-1}) - 1 = \mathrm{wg}(P_{i-1}) - 1,\end{aligned}$$

что и требовалось доказать.

Итак, мы убедились, что наша весовая функция удовлетворяет условиям (i)–(iii) и завершили доказательство теоремы 1.1.

Отметим, что теорема 1.1 была повторно доказана Ананичевым, Гусевым и Волковым [13] с использованием совершенно иной техники.

Можно предположить, что выражение $(n-1)(n-2)$ задает точную оценку длины кратчайшего синхронизирующего слова n-автомата с буквой-бактрианом в случае нечетного $n \geq 5$. Однако подтвердить это предположение мы можем только для случая $n = 5$ (тем самым отвечая на вопрос, поставленный Пэном в обзоре [48]), а также случаев $n = 7$ и $n = 9$.

Как упоминалось в §1.1, существуют синхронизируемые автоматы с двумя буквами входного алфавита, одна из которых – буква-бактриан, кратчайшее синхронизирующее слово которых имеет длину 20, что совпадает с нижней границей $(n-1)(n-2)$, установленной в теореме 1.1 для нечетных n. Эти автоматы изображены на рис. 1.6, 1.7, 1.8 и 1.9; их кратчайшие синхронизирующие слова приведены ниже:
$\mathscr{B}_6^{(1)}$: $ab^3abab \cdot ab^3aab \cdot ab^3a$,

$\mathscr{B}_6^{(2)}$: $ab^3ab^2 \cdot ab^3aab^2 \cdot ab^3a$,
$\mathscr{B}_6^{(3)}$: $(ab^3ab^2)^2aab^3a$,
$\mathscr{B}_6^{(4)}$: $(ab^3ab^2)^2ab^4a$.

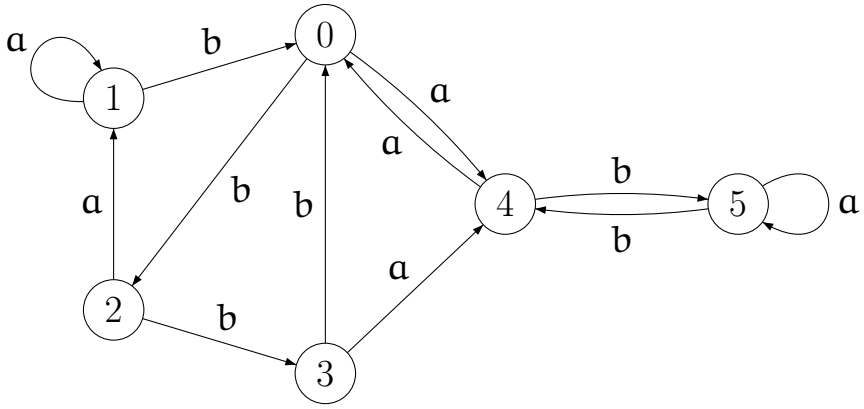


Рис. 1.6: Автомат $\mathscr{B}_6^{(1)}$

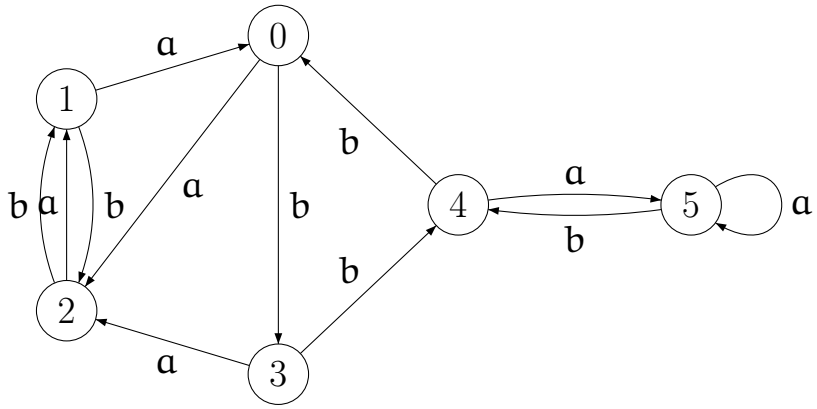


Рис. 1.7: Автомат $\mathscr{B}_6^{(2)}$

Полный перебор всех автоматов на восьми состояниях с двумя буквами входного алфавита, одна из которых – буква-бактриан, не нашел ни одного автомата с кратчайшим синхронизирующим словом длины $(8-1)(8-2)=42$; более того, максимальная длина кратчайшего слова для таких автоматов оказалась равна 40. Причем, данное значение длины достигается на единственном автомате $\mathscr{B}_8^{(1)}$, показанном на рис. 1.10. Его кратчайшее синхронизирующее слово имеет вид

$$ab^3abab(a^2b^3a^2bab)^2ab^3a^2bab^3a.$$

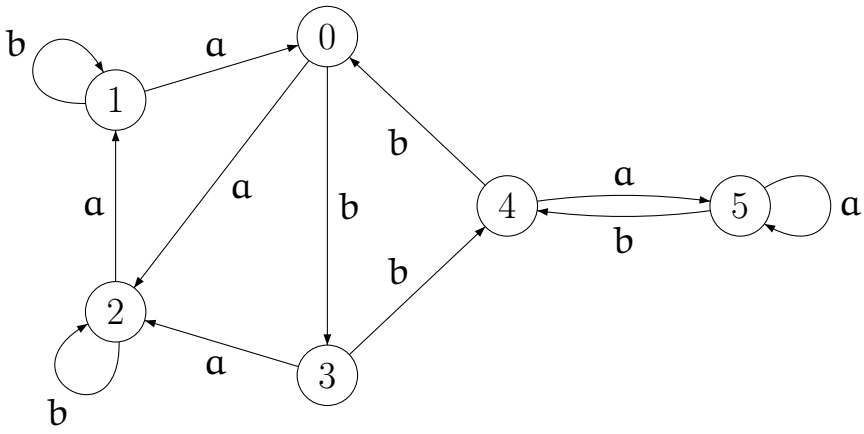


Рис. 1.8: Автомат $\mathscr{B}_6^{(3)}$

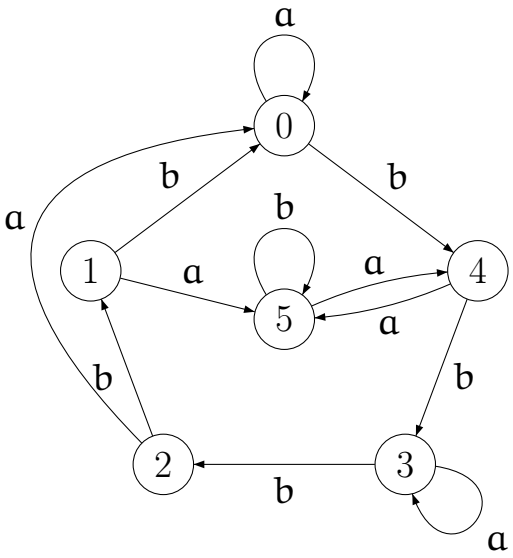


Рис. 1.9: Автомат $\mathscr{B}_6^{(4)}$

Интересно, что во всех рассмотренных автоматах, кроме $\mathscr{B}_6^{(4)}$, буква b также имеет ненулевой дефект, при том, что в автоматах $\mathscr{B}_n$ она действует как перестановка. Примеры $\mathscr{B}_6^{(1)}$ и $\mathscr{B}_8^{(1)}$ имеют схожую структуру автомата и его синхронизирующего слова и могут быть развернуты в бесконечную серию автоматов, однако длина синхронизирующего слова n-автомата, принадлежащего данной серии, будет равна $10(n-4)$, т. е. будет линейной относительно числа состояний автомата. Поэтому получившаяся серия интереса не представляет.

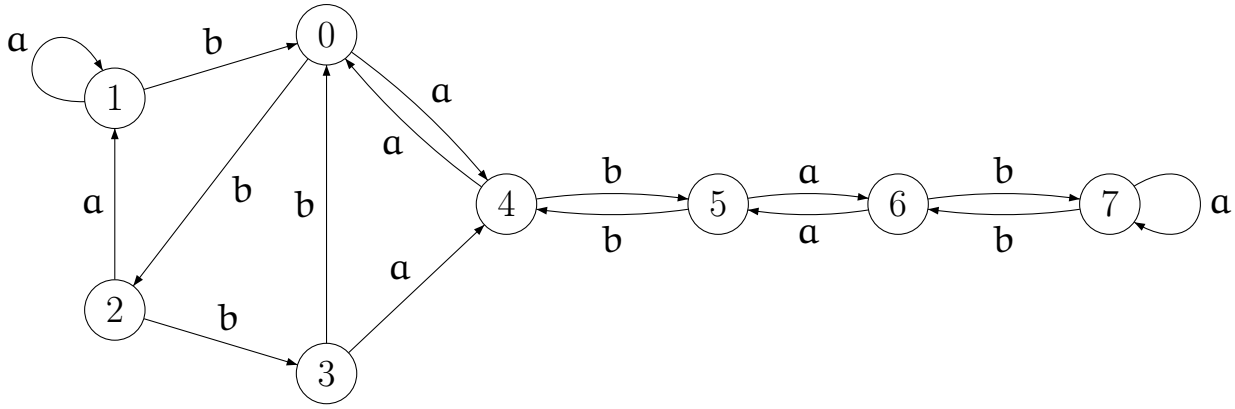


Рис. 1.10: Автомат $\mathscr{B}_8^{(1)}$

1.3 $\mathscr{D}_n$: серия автоматов с буквой-дромадером

Пусть $n > 4$ и $\mathscr{D}_n$ – серия автоматов с множеством состояний $\{1, 2, \ldots, n\}$, входным алфавитом $\{a, b, c\}$ и функцией переходов δ, определенной следующим образом:

m	1	2	3	4	5	...	n
$\delta(m, a)$	1	1	1	4	5	...	n
$\delta(m, b)$	1	1	2	4	5	...	n
$\delta(m, b)$	4	1	4	5	6	...	3

То есть буквы a и b оставляют состояния множества $\{4, 5, \ldots, n\}$ на месте, а буква c действует на множестве состояний $\{3, 4, \ldots, n\}$ как циклическая перестановка. Автомат $\mathscr{D}_n$ изображен на рис. 1.11.

Справедливость следующей леммы проверяется непосредственно. Ее доказательство полностью аналогично доказательству леммы 1.1, поэтому

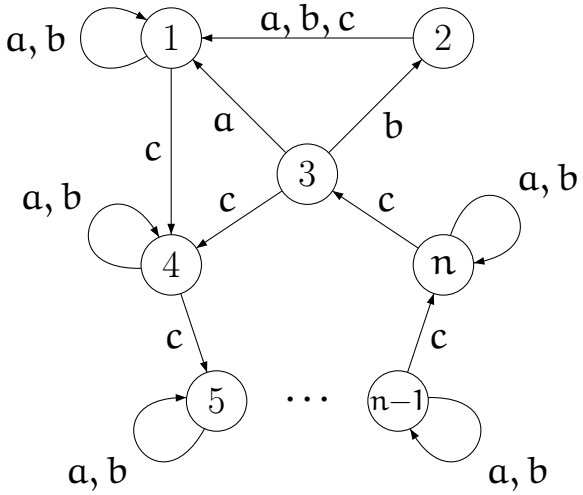


Рис. 1.11: Автомат $\mathscr{D}_n$

мы позволим себе его опустить.

Лемма 1.2 Пусть $n > 4$. Тогда слово

$$c^2(bc^{n-1})^{n-4}bc^2 \tag{1.2}$$

синхронизирует автомат $\mathscr{D}_n$.

Длина слова (1.2) равна $n(n-4)+5 = (n-2)^2+1$. Докажем, что это в точности длина кратчайшего синхронизирующего слова для $\mathscr{D}_n$. Заметим, что слово (1.2) не содержит букву a и, следовательно, также синхронизирует автомат, получаемый из $\mathscr{D}_n$ удалением буквы a. Таким образом, что несколько неожиданно, добавление буквы дефекта 2 к синхронизируемому автомату, в котором все буквы имеют дефект 1, не обязательно уменьшает длину его кратчайшего синхронизирующего слова.

Как и при доказательстве теоремы 1.1, мы будем использовать игровой подход. Однако в отличие от §1.2 мы будем считать все монеты, используемые в игре, неразличимыми. Как и выше, *ход* – это действие буквы; состояние m покрыто монетой после завершения хода с использованием буквы $d \in \{a, b, c\}$, если и только если существует состояние ℓ такое, что $\delta(\ell, d) = m$ и ℓ было покрыто монетой перед ходом. Таким образом, правило гласит: при совершении хода монеты скользят по стрелкам, помеченным d, и, если несколько монет встречаются в одном состоянии, все, кроме одной, удаляются.

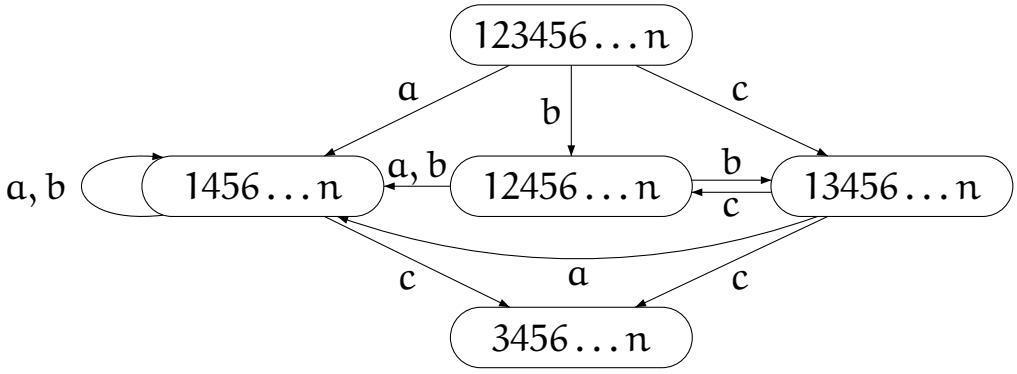


Рис. 1.12: Фрагмент автомата подмножеств $\mathscr{D}_n$

Пусть в начале игры все состояния автомата $\mathscr{D}_n$ покрыты монетами. Как и в доказательстве теоремы 1.1, легко проверить, что слово $w \in \{a, b, c\}^*$ синхронизирует $\mathscr{D}_n$, если и только если его действие на начальную позицию удаляет $n - 1$ монету. Рассмотрим "верхнюю" часть автомата подмножеств $\mathscr{D}_n$ (см. рис 1.12). Заметим, что синхронизирующее слово минимальной длины должно начинаться на ac или на c^2. Действие любого из этих слов освобождает от монет состояния 1 и 2, соответственно, после этого действия монеты покрывают в точности состояния множества $\mathscr{C} = \{3, 4, \ldots, n\}$; будем называть это множество *основным циклом* $\mathscr{D}_n$.

Очевидно, что для того, чтобы удалить монету, расположенную в одном из состояний основного цикла, сперва нужно вывести ее из $\mathscr{C}$ через состояние 3. Будем говорить, что две монеты, покрывающие некоторые состояния $m, \ell \in \mathscr{C}$, могут быть *слиты*, если существует слово $z \in \Sigma^*$, называемое *сливающим*, такое, что:

— $mz = \ell z$;

— $mz' \neq \ell z'$ для любого z' – собственного префикса z;

— в процессе применения z каждая из монет покидает основной цикл не более одного раза.

Более строго последнее условие означает, что у слова z существует не более одного префикса $z_1 = a_1 \ldots a_{|z_1|}$, удовлетворяющего условиям $mz_1 \notin \mathscr{C}$, $m(a_1 \ldots a_{|z_1|-1}) \in \mathscr{C}$, и не более одного префикса $z_2 = a_1 \ldots a_{|z_2|}$, удовлетворяющего условиям $\ell z_2 \notin \mathscr{C}$, $\ell(a1 \ldots a_{|z_2|-1}) \in \mathscr{C}$.

Лемма 1.3 Пусть две монеты, покрывающие состояния основного цикла, могут быть слиты. Назовем монету, которая первой покидает $\mathscr{C}$, C_1,

вторую монету – C_2. Тогда монета C_2 покрывает состояние, следующее по часовой стрелке на $\mathscr{C}$ за состоянием, покрытым C_1.

Доказательство. Пусть $\mathtt{z}$ – соответствующее сливающее слово. Как было отмечено ранее, единственный путь из основного цикла проходит через состояние 3. Обозначим через $\mathtt{y}$ префикс $\mathtt{z}$, перемещающий монету C_1 из ее начального состояния в состояние 3 к началу хода, в процессе которого монета покинет основной цикл. Рассуждая от противного, предположим, что $\mathtt{y}$ переводит монету C_2 в состояние $\mathtt{m} \in \mathscr{C}$, отличное от $\mathtt{n}$. Тогда под действием следующей буквы $\mathtt{d} \in \{\mathtt{a}, \mathtt{b}\}$ слова $\mathtt{z}$ монета C_1 выйдет из основного цикла, а C_2 останется на состоянии $\mathtt{m}$.

Если в процессе применения $\mathtt{z}$ монета C_2 также покидает основной цикл, она должна из состояния $\mathtt{m}$ достигнуть состояния 3. Это можно сделать только по слову $\mathtt{z}'$, в котором буква $\mathtt{c}$ встречается больше одного раза. Подслово $\mathtt{z}'$ должно встретиться в слове $\mathtt{z}$ после префикса $\mathtt{yd}$. Однако, действие $\mathtt{z}'$ вернет монету C_1 в некоторое состояние $\ell \in \mathscr{C}$, не совпадающее с состоянием 3, и слияние станет невозможно.

Если C_2 остается в основном цикле в процессе применения $\mathtt{v}$, то единственным состоянием, в котором возможно слияние, является состояние 4. Привести монету C_2 из состояния $\mathtt{m}$ в состояние 4 можно при помощи слова $\mathtt{z}''$, в котором буква $\mathtt{c}$ встречается по крайней мере два раза. Поскольку $\mathtt{z}'''$ следует в $\mathtt{z}$ после префикса $\mathtt{yd}$, его действие вернет монету C_1 в круг в некоторое состояние $\ell \in \mathscr{C}$, отличное от 4. Снова приходим к противоречию. □

Принимая во внимание лемму 1.3, можно предположить, что монеты, которые могут быть слиты, покрывают состояния 3 и $\mathtt{n}$. Общий случай сводится к описанному с помощью циклического сдвига, вызванного действием подходящей степени буквы $\mathtt{c}$. Монеты могут быть слиты в состоянии 1 или 4. Обратимся к еще одному фрагменту автомата подмножеств для $\mathscr{D}_\mathtt{n}$, изображенному на рис. 1.13.

Анализ рис 1.13 показывает, что сливающее слово может начинаться только с буквы $\mathtt{b}$. Действие $\mathtt{c}$ оставляет монеты в основном цикле без слияния, а действие $\mathtt{a}$ переводит их в пару состояний $\{\mathtt{1}, \mathtt{n}\}$, из которой они могут лишь вернуться в основной цикл без слияния. Более того, можно заключить, что любое сливающее слово для данной пары состояний

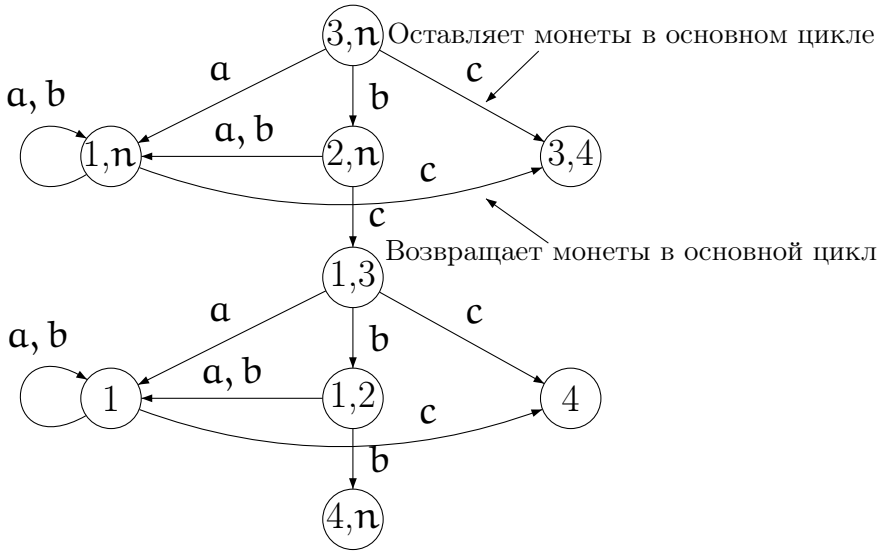


Рис. 1.13: Другой фрагмент автомата подмножеств $\mathscr{D}_{\mathfrak{n}}$

совпадает с одним из нижеперечисленных слов:

$$\mathfrak{bcc}, \mathfrak{bcax}, \mathfrak{bcbax}, \mathfrak{bcbbx}, \mathfrak{bcaxc}, \mathfrak{bcbaxc}, \mathfrak{bcbbxc}, \tag{1.3}$$

где $\mathfrak{x}$ – произвольное слово в языке $\{\mathfrak{a}, \mathfrak{b}\}^*$. Непосредственно проверяется, что при применении каждого из этих слов монеты, за исключением сливаемых, не покидают основной цикл. Монета, которая появляется в результате слияния, покрывает состояние 1 или 4. Если она покрывает состояние 1, то при следующем применении $\mathfrak{c}$ она возвращается в основной цикл. Также отметим, что кратчайшее слово в списке (1.3) имеет длину 3.

Нетрудно видеть, что лакуна (последовательность дырок в основном цикле) может расти только по часовой стрелке, т. е. новые дырки могут появляться в ней только на месте состояний, следующих за лакуной в отрицательном направлении обхода цикла. Действительно, рассмотрим некоторую лакуну: пусть C – монета, следующая за ней по часовой стрелке. Мы перемещаем C в состояние 3 и применяем слово из списка (1.3). Это переводит C в состояние 4 и удлинняет лакуну на одно состояние. Заметим, что если состояние, следующее за C по часовой стрелке, покрыто монетой, указанное действие приведет к слиянию этой монеты с C и образованию новой дырки. Если за C следует дырка, описанное выше действие переставит их местами, и рассматриваемая лакуна станет длиннее за счет

сокращения следующей лакуны.

Если нужно последовательно наращивать лакуну, на каждом шаге нужно возвращать монету C из состояния 4 в состояние 3, это можно сделать при помощи слова y, в котором буква c встречается не меньше $n-3$ раз, т. е. $|y| \geq n-3$.

Пусть w – произвольное синхронизирующее слово автомата $\mathscr{D}_n$. Напомним, что оно должно начинаться с ac или c^2, и после действия этого префикса монеты покрывают в точности состояния основного цикла. В этот момент нет ни одной лакуны, а по завершении действия w в цикле есть лакуна из $n-3$ дырок. Следовательно, требуется повторение действия, описанного выше, $n-3$ раз. Первая дырка появляется после применения некоторого слова из списка (1.3) (его длина, напомним, не меньше 3), после чего нужно чередовать применение слова длиной не менее $n-3$ со словом из списка (1.3) не менее $n-4$ раз. Таким образом,

$$|w| \geq 2+3+(n-4)((n-3)+3) = n^2-4n+5 = (n-2)^2+1,$$

что и требовалось доказать.

На рис. 1.14 изображен автомат с пятью состояниями и тремя буквами входного алфавита, кратчайшее синхронизирующее слово которого имеет длину $(5-2)^2+2 = 11$, превышающую оценку из теоремы 1.2. Нами найдено несколько подобных автоматов на пяти состояниях. Для автома-

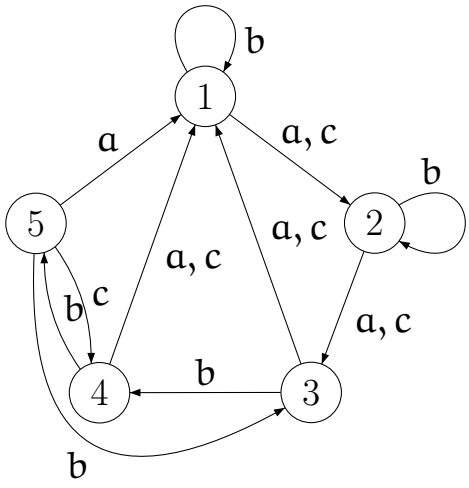


Рис. 1.14: Автомат на 5 состояниях с кратчайшим синхронизирующим словом $ab^2c^2b^2cbc^2$

тов на 6 состояниях оценка из теоремы 1.2 также не точна. Пример с 18-буквенным синхронизирующим словом приведен на рис. 1.15. Несмотря на то, что автоматы на рис. 1.14 и 1.15 имеют сходное строение, нам пока не удалось построить аналогичный пример хотя бы для семи состояний.

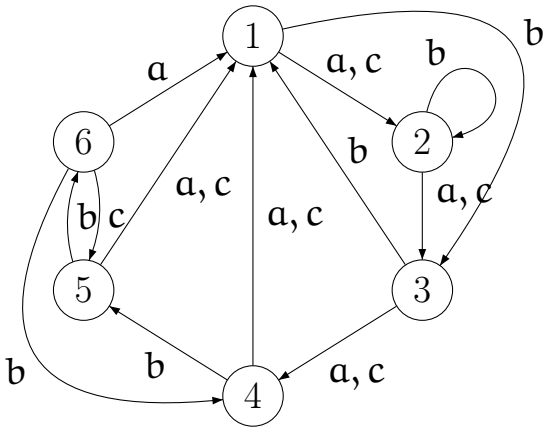


Рис. 1.15: Автомат на 6 состояниях с кратчайшим синхронизирующим словом $ab^2cbacb^2c^2b^5c^2$

Глава 2

Синхронизируемые автоматы с буквой большого дефекта

2.1 Постановка задачи и основные определения

Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – автомат с $|Q| \geq 3$. Пусть в автомате есть буква $a \in \Sigma$ такая, что для этой буквы существуют $q_1, q_2, \ldots, q_k \in Q$ для некоторого k такие, что $\delta(q_1, a) = \delta(q_2, a) = \ldots = \delta(q_k, a)$. Будем называть букву a k-*веерной*, или без указания k просто *веерной*. Коэффициент k будем называть *веерностью* буквы a. Отметим, что дефект k-веерной буквы превосходит k.

Наиболее простым способом получения автоматов с длинным кратчайшим синхронизирующим словом и веерной буквой является модификация серии автоматов Черни на множестве состояний $Q = \{1, 2, \ldots, n\}$, в которой буквы a и b действуют следующим образом:

$$\delta(m, a) = \begin{cases} 2 & \text{for } m = 1, \\ m & \text{for } 1 < m < n - k + 3, \\ 2 & \text{for } n - k + 3 \leq m \leq n; \end{cases}$$

$$\delta(m, b) = \begin{cases} m + 1 \pmod{n - k + 2} & \text{for } 1 \leq m < n - k + 3, \\ m & \text{for } n - k + 3 \leq m \leq n. \end{cases}$$

Данная модификация для случая $k = 4$ изображена на рис. 2.1.

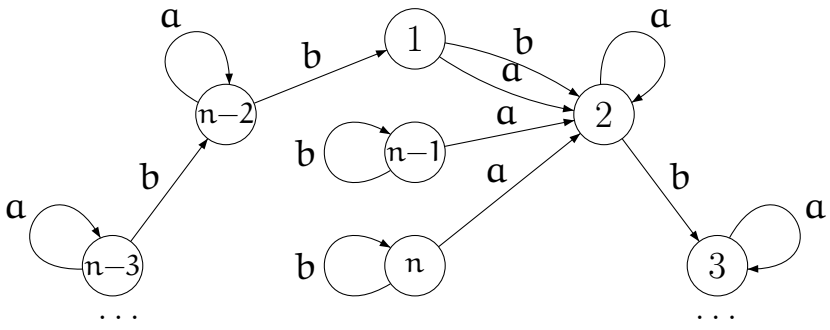


Рис. 2.1: Модификации автомата Черни

В статье Романа [51] представлены результаты численных экспериментов, показывающие, что в классе автоматов, имеющих букву дефекта больше двух, уже над двухбуквенным алфавитом существуют автоматы, синхронизирующиеся более длинным словом, чем автомат – модификация автомата Черни с тем же дефектом буквы и числом состояний.

Данная глава посвящена построению бесконечных серий автоматов, имеющих k-веерную букву, обладающую свойством $n - k = \mathrm{const}$. В §2.2 рассматриваются бесконечные серии автоматов, приводится доказательство точности оценок для части полученных серий. В §2.3 обсуждается вопрос экстремальности полученных серий для автоматов с небольшим числом состояний и описываются проведенные численные эксперименты.

2.2 Медленно синхронизируемые автоматы с буквой большого дефекта

Рассмотрим конечные автоматы с множеством состояний $Q = \{1, 2, \ldots, n\}$ и алфавитом $\Sigma = \{a, b\}$. Все рассматриваемые нами серии автоматов будут входить в это множество, так что, определяя автомат, мы будем задавать только его функцию перехода.

Рассмотрим автомат с функцией перехода δ, заданной следующей таблицей.

m	1	2	3	4	5	…	n
$\delta(m, a)$	1	3	2	2	2	…	2
$\delta(m, b)$	3	2	4	5	6	…	1

Обозначим его через $\mathscr{VA}_n$. Изображение этого автомата приведено на рис. 2.2. Отметим, что для данного автомата выполняется равенство $n - k = 2$.

Теорема 2.1 Длина кратчайшего синхронизирующего слова автомата $\mathscr{VA}_n$, $n > 4$ равна $n + 4$.

Доказательство. Построим автомат подмножеств, достижимых из множества всех состояний автомата $\mathscr{VA}_n$. Мы будем использовать следующие обозначения подмножеств – состояний автомата подмножеств: будем перечислять состояния $\mathscr{VA}_n$, составляющие подмножество, в круглых скобках без разделителей. Например, подмножество $\{1, 2, 3\}$ в наших обозначени-

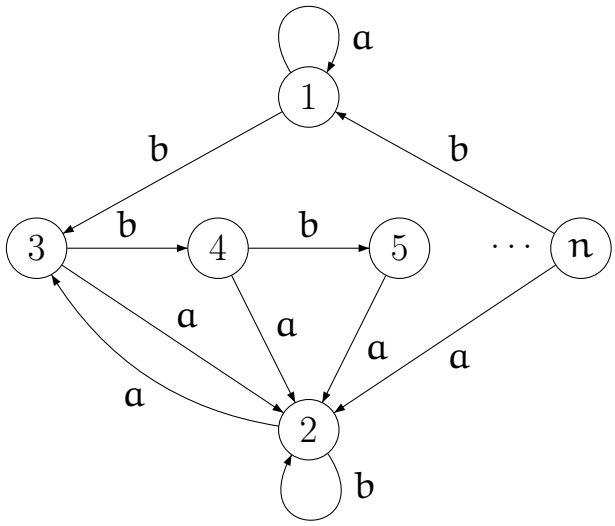


Рис. 2.2: Автомат $\mathscr{VA}_n$

ях будет выглядеть как (1 2 3); на рисунке скобки будем опускать. Такая запись отличается от общепринятой, однако позволяет сделать текст доказательства менее громоздким, а также упростить сопоставление рассуждений, приведенных в доказательстве, и их иллюстраций.

Будем строить автомат подмножеств поиском в ширину из множества всех состояний $\mathscr{VA}_n$, пока не достигнем одноэлементного множества или пока не построим автомат полностью. Достижение одноэлементного множества будет означать наличие у $\mathscr{VA}_n$ синхронизирующего слова, по построению данное слово будет кратчайшим словом с таким свойством. Покажем, что построенный нами автомат будет представлять собой в точности автомат, изображенный на рис. 2.3. Будем строить автомат по частям, на рисунке эти части обведены пунктирными линиями и подписаны римскими цифрами.

1. Начнем построение автомата из состояния (1 .. n). Применение b оставит это состояние на месте, поскольку буква b действует на всем множестве состояний $\mathscr{VA}_n$ как перестановка; применив же a, мы перейдем в состояние (1 2 3). Отсюда у нас есть путь только по b – в состояние (2 3 4), a оставляет состояние на месте. Из (2 3 4) возможны оба перехода: по a в (2 3) и по b в (2 4 5). Отметим, что все описанные переходы произойдут для автомата с любым числом состояний. Построенная часть автомата обозначена на рисунке через I.

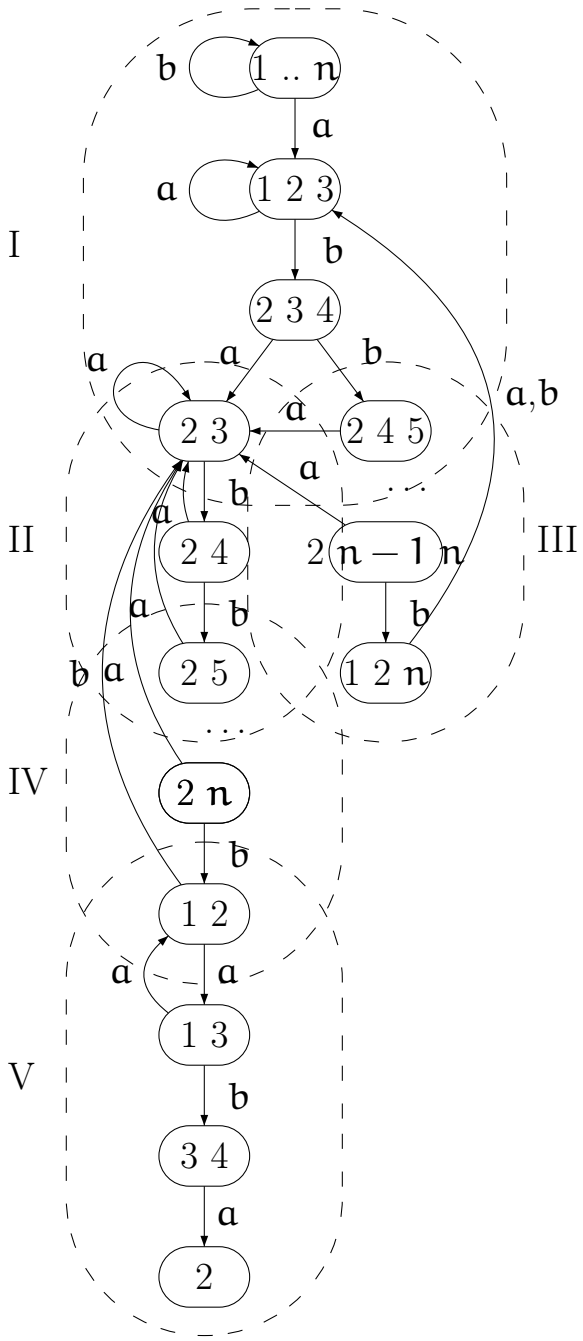


Рис. 2.3: Автомат подмножеств, достижимых из $(1 \,..\, n)$, для $\mathscr{V}\mathscr{A}_n$

2. Продолжим строить автомат из состояния $(2\ \ 3)$. Действие a оставляет данное состояние на месте, а действие b переводит его в $(2\ \ 4)$, откуда по a мы вернемся в $(2\ \ 3)$, а по b перейдем в $(2\ \ 5)$. Эти переходы также не зависят от числа состояний автомата $\mathscr{VA}_n$. Построенная часть автомата подмножеств обозначена на рисунке через II.

3. Рассмотрим действие букв на состояния вида $(2\ \ m-1\ \ m)$, где $4 < m < n$. Все возможные варианты этого действия изображены на рис. 2.4. Из рисунка следует, что из состояния $(2\ \ 4\ \ 5)$ может быть построена часть автомата подмножеств следующего вида:

$$(2\ \ 4\ \ 5) \xrightarrow{b} (2\ \ 5\ \ 6) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ n-1\ \ n) \xrightarrow{b} (1\ \ 2\ \ n).$$

По a все состояния переходят в $(2\ \ 3)$, $(1\ \ 2\ \ n)$ по обеим буквам переходит в $(1\ \ 2\ \ 3)$, которое уже встречалось в I. Построенную часть автомата обозначим через III.

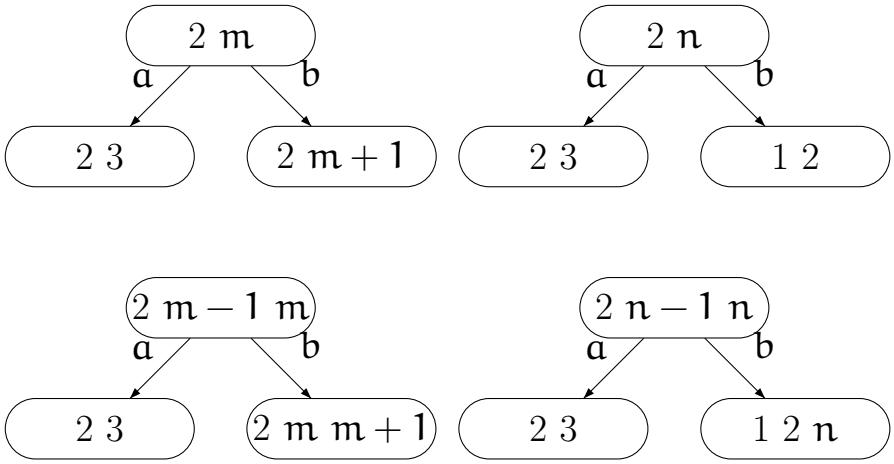


Рис. 2.4: Фрагменты автомата подмножеств для $\mathscr{VA}_n$

4. Вернемся к состоянию $(2\ \ 5)$ и построим из него часть IV. Из рассуждений, аналогичных проведенным в п. 3, следует, что эта часть автомата имеет вид

$$(2\ \ 5) \xrightarrow{b} (2\ \ 6) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ n) \xrightarrow{b} (1\ \ 2).$$

По a все состояния переходят в $(2\ \ 3)$. Длина "цепи" от $(2\ \ 5)$ до $(2\ \ n)$, соответственно, равна $n-5$.

5. Состоянием $(1\ \ 2)$ начинается часть автомата V, она имеет вид

$$(1\ \ 2) \xrightarrow{a} (1\ \ 3) \xrightarrow{b} (3\ \ 4) \xrightarrow{a} (2).$$

По b из $(1\ \ 2)$ мы возвращаемся в состояние $(2\ \ 3)$, уже встречавшееся нам в частях I и II. Из $(1\ \ 3)$ по a переходим в $(1\ \ 2)$.

Таким образом, мы показали, что построенный нами автомат подмножеств, достижимых из $(1\,..\,n)$, в точности изображен на рис. 2.3. Отсюда следует, что кратчайшее синхронизирующее слово для $\mathscr{VA}_n$ имеет вид $(aba)(bb)b^{n-5}(b)(aba) = abab^{n-2}aba$, его длина равна $n+4$. □

Для случая $n-k=3$ будем рассматривать серию, определенную только на автоматах с четным числом состояний. Автоматы серии имеют следующий вид:

m	1	2	3	4	5	...	n
$\delta(m,a)$	1	3	4	2	2	...	2
$\delta(m,b)$	4	3	2	5	6	...	1

Обозначим их через $\mathscr{VB}_n$. Изображение $\mathscr{VB}_n$ приведено на рис. 2.5.

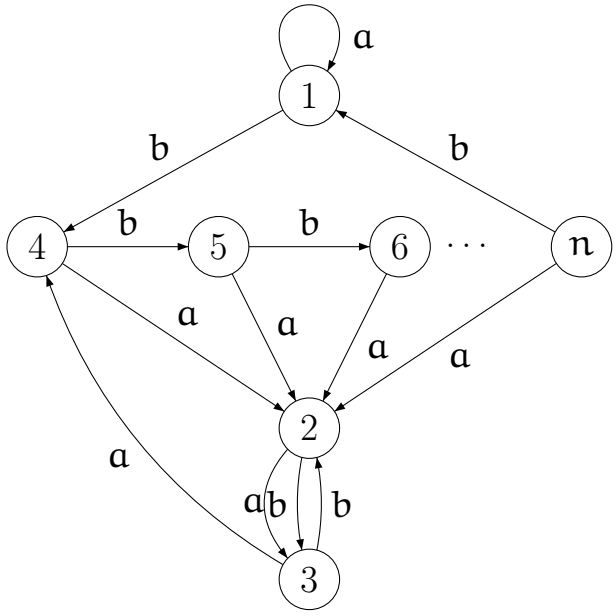


Рис. 2.5: Автомат $\mathscr{VB}_n$

Теорема 2.2 Длина кратчайшего синхронизирующего слова автомата $\mathscr{VB}_n$, $n>6$, n-нечетное, равна $2n+4$.

Доказательство. Доказательство теоремы будем проводить методом, уже применявшимся нами для доказательства теоремы 2.1. Построим автомат подмножеств, достижимых из множества всех состояний автомата $\mathscr{VB}_n$ до достижения одноэлементного множества и покажем, что в результате получится автомат, изображенный на рис. 2.6. Некоторые состояния автомата подмножеств на рисунке изображены дважды для удобства использования рисунка. К примеру, дуга из состояния $(2\ \ 5\ \ 6)$ в состояние $(2\ \ 3)$ имела бы большое количество пересечений с другими дугами, что существенно осложнило бы чтение рисунка. Поэтому состояние $(2\ \ 3)$ было скопировано и переход из $(2\ \ 5\ \ 6)$ нарисован не в само состояние, а в его копию. Все копии состояний на рисунке обведены пунктирной линией.

1. Начнем строить автомат с состояния $(1\ ..\ n)$. Первые шаги нашего построения не зависят от размера автомата $\mathscr{VB}_n$. Результатом этих шагов будет часть автомата, помеченная на рисунке цифрами I и II. Это пути поиска в ширину с началом в состоянии $(1\ ..\ n)$ и окончаниями в состояниях $(2\ \ 3\ \ 5\ \ 6)$ и $(2\ \ 3\ \ 6)$, в которых мы продолжим построение в следующих пунктах.

2. Продолжим построение из состояния $(2\ \ 3\ \ 5\ \ 6)$. На рис. 2.7а) показано действие букв на состояние вида $(2\ \ 3\ \ m-1\ \ m)$, где $5 < m < n$. Из рисунка следует, что состоянием $(2\ \ 3\ \ 5\ \ 6)$ начинается часть автомата подмножеств следующего вида:

$$(2\ \ 3\ \ 5\ \ 6) \xrightarrow{b} (2\ \ 3\ \ 6\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ 3\ \ n-1\ \ n) \xrightarrow{b} (1\ \ 2\ \ 3\ \ n).$$

По a все состояния переходят в $(2\ \ 3\ \ 4)$, $(1\ \ 2\ \ 3\ \ n)$ по обеим буквам переходит в $(1\ \ 2\ \ 3\ \ 4)$, которое уже встречалось в I. Полученная часть автомата на рис. 2.6 обозначена через III.

3. Теперь обратимся к состоянию $(2\ \ 3\ \ 6)$ и продолжим построение из него. Из рассуждений, аналогичных проведенным в п.2 следует, что мы получим часть автомата следующего вида:

$$(2\ \ 3\ \ 6) \xrightarrow{b} (2\ \ 3\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ 3\ \ n) \xrightarrow{b} (1\ \ 2\ \ 3).$$

По a все состояния переходят в $(2\ \ 3\ \ 4)$. Длина "цепи" от $(2\ \ 3\ \ 6)$ до $(2\ \ 3\ \ n)$, соответственно, равна $n-6$, цепь выделена на рисунке в часть IV.

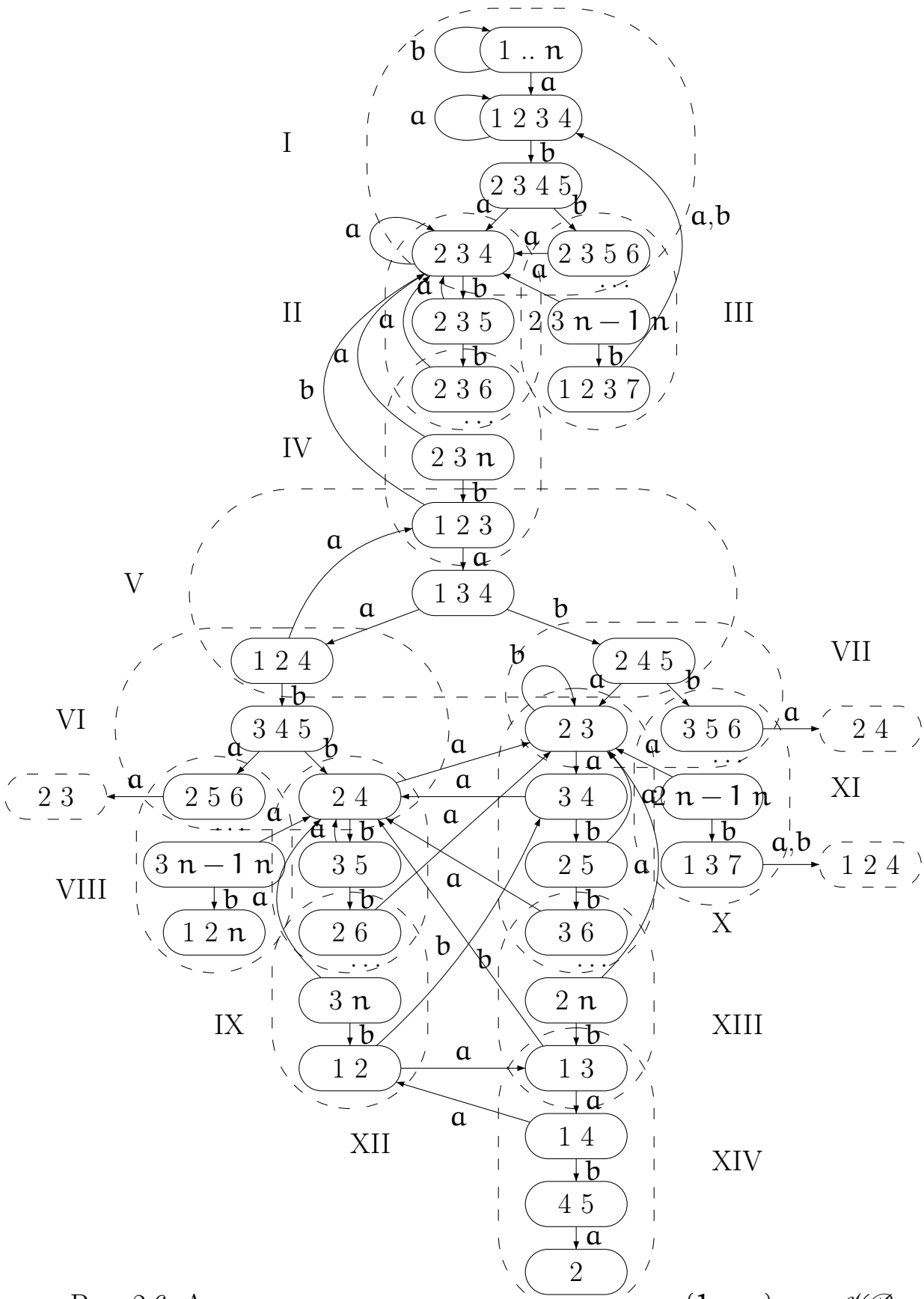


Рис. 2.6: Автомат подмножеств, достижимых из $(1\ ..\ n)$, для $\mathscr{VB}_n$

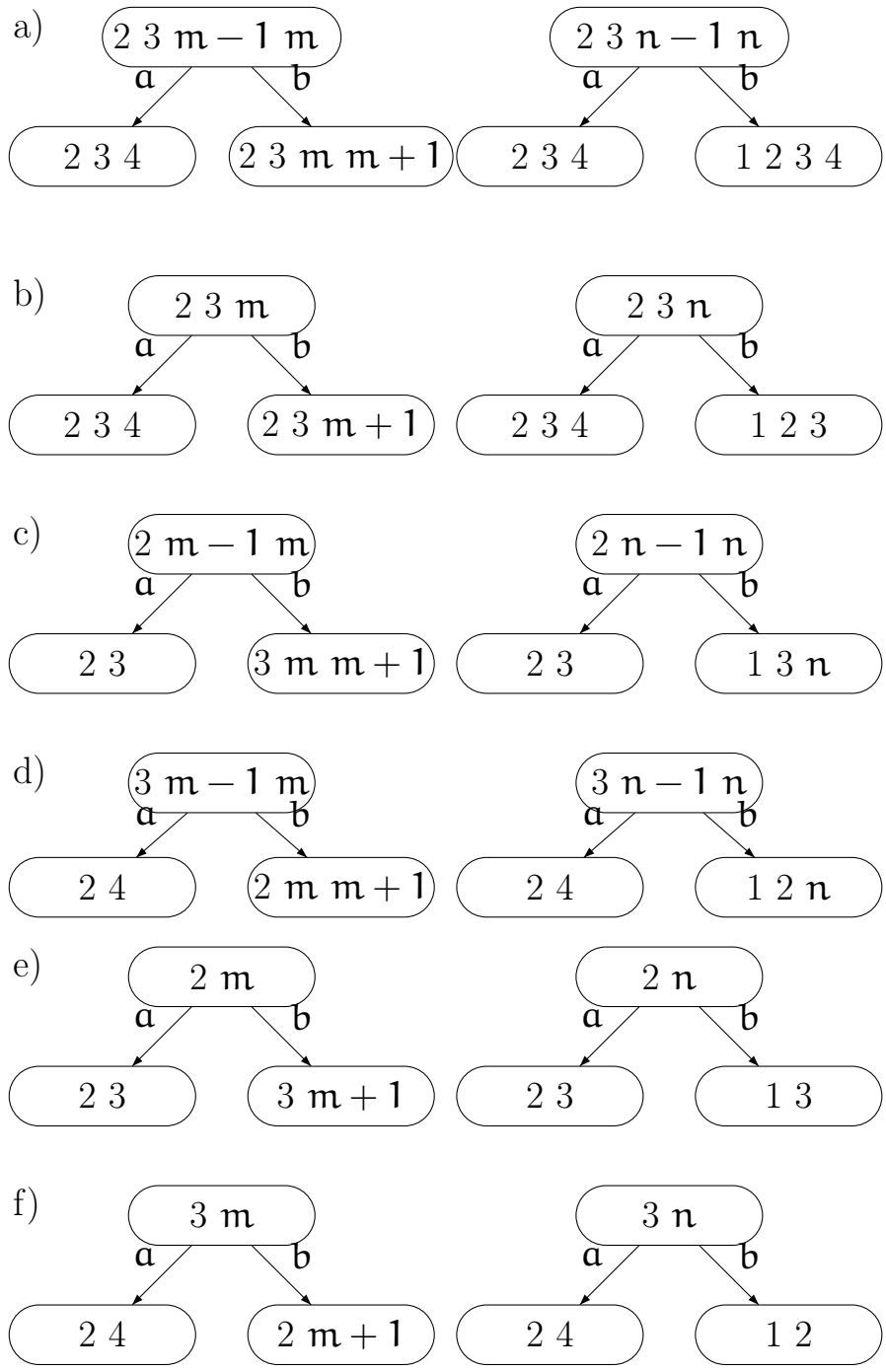


Рис. 2.7: Фрагменты автомата подмножеств для $\mathscr{VB}_n$

4. Продолжив поиск из состояния $(1\ \ 2\ \ 3)$, придем в состояния $(2\ \ 5\ \ 6)$, $(3\ \ 5\ \ 6)$, $(2\ \ 6)$ и $(3\ \ 6)$. Текстовое доказательство этого факта мы опустим, все переходы ясны из рисунка (части V, VI, VII, IX и X). Отметим, что все изображенные в этих частях переходы не зависят от размера автомата $\mathscr{VB}_n$.

5. Продолжая построения, аналогичные сделанным в п.2 из состояний $(2\ \ 5\ \ 6)$ и $(3\ \ 5\ \ 6)$, получим следующее:

$$\text{VIII}: \quad (2\ \ 5\ \ 6) \xrightarrow{b} (3\ \ 6\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (3\ \ n-1\ \ n) \xrightarrow{b} (1\ \ 2\ \ n),$$

$$\text{XI}: \quad (3\ \ 5\ \ 6) \xrightarrow{b} (2\ \ 6\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ n-1\ \ n) \xrightarrow{b} (1\ \ 3\ \ n).$$

Заметим, что число состояний автомата $\mathscr{VB}_n$ нечетно, соответственно, число переходов по b от 6 до n в автомате $\mathscr{VB}_n$, равное $n-6$, также нечетно. Очевидно, что "цепь" строится следующим образом:

$$\ldots(2\ \ m-1\ \ m) \xrightarrow{b} (3\ \ m\ \ m+1) \xrightarrow{b} (2\ \ m+1\ \ m+2)\ldots.$$

Состояния 2 и 3 в ней "чередуются". Поскольку длина "цепи" от $(2\ \ 5\ \ 6)$ до $(3\ \ n-1\ \ n)$ (как и "цепи" от $(3\ \ 5\ \ 6)$ до $(2\ \ n-1\ \ n)$) нечетна, то если в первом элементе цепи присутствует 2, в последнем встретится 3 и наоборот.

Состояния вида $(2\ \ m-1\ \ m)$ по a переходят в $(2\ \ 3)$, а вида $(3\ \ m-1\ \ m)$ – в $(2\ \ 4)$. $(1\ \ 2\ \ n)$ переходит по a в $(1\ \ 2\ \ 3)$, а по b в $(1\ \ 3\ \ 4)$, оба состояния уже встречались в V. $(1\ \ 3\ \ n)$ переходит и по a, и по b в $(1\ \ 2\ \ 4)$, которое также встречалось в V.

$$\text{XII}: \quad (2\ \ 6) \xrightarrow{b} (3\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (3\ \ n) \xrightarrow{b} (1\ \ 2)$$

$$\text{XIII}: \quad (3\ \ 6) \xrightarrow{b} (2\ \ 7) \xrightarrow{b} \cdots \xrightarrow{b} (2\ \ n) \xrightarrow{b} (1\ \ 3)$$

Состояния вида $(2\ \ m)$ по a переходят в $(2\ \ 3)$, а вида $(3\ \ m)$ – в $(2\ \ 4)$. $(1\ \ 2)$ переходит по a в $(1\ \ 3)$, которое встречалось в XIII, а по b в $(3\ \ 4)$, которое уже встретилось в X.

Длина "цепи" от $(3\ \ 6)$ до $(2\ \ n)$ также равна $n-6$.

6. Завершает конструирование построение последней части XIV, начинающейся с состояния $(1\ \ 3)$ и завершающейся одноэлементным множеством (2).

Таким образом, мы показали, что построенный нами автомат подмножеств в точности изображен на рис. 2.6. Отсюда следует, что кратчайшее синхронизирующее слово для $\mathscr{VB}_n$ имеет вид $(aba)(bb)b^{n-6}(b)(abaa)(bb)b^{n-6}(b)(aba) = abab^{n-3}abaab^{n-3}aba$, его длина равна $2n+4$. □

Доказательства соответствующих теорем для двух следующих серий, реализующих случай $n-k=4$, полностью аналогичны проведенному для $\mathscr{VA}_n$ и $\mathscr{VB}_n$, а автоматы подмножеств слишком громоздки. Поэтому мы ограничимся изображением автоматов серий, формулировкой теорем и указанием вида кратчайшего синхронизирующего слова.

Итак, автоматы первой серии, определенной только для таких n, что $n \equiv 1 \pmod 3$, имеют вид:

m	1	2	3	4	5	5	...	n
$\delta(m,a)$	1	5	4	3	2	2	...	2
$\delta(m,b)$	5	3	4	2	6	7	...	1

Обозначим их через $\mathscr{VC}_n$. Изображение $\mathscr{VC}_n$ приведено на рисунке 2.8.

Для автоматов этой серии справедлива следующая теорема.

Теорема 2.3 Длина кратчайшего синхронизирующего слова автомата $\mathscr{VC}_n$, $n > 7$, $n \equiv 1 \pmod 3$, равна $3n+4$.

Кратчайшее синхронизирующее слово автомата $\mathscr{VC}_n$ имеет вид $abab^{n-4}ababaab^{n-4}abaab^{n-4}aba$.

Перейдем ко второй серии, определенной только для нечетных n. Автоматы этой серии мы будем обозначать через $\mathscr{VD}_n$. Действие букв на состояниях этих автоматов задается таблицей:

m	1	2	3	4	5	5	...	n
$\delta(m,a)$	1	3	4	5	2	2	...	2
$\delta(m,b)$	5	3	2	4	6	7	...	1

Автомат $\mathscr{VD}_n$ изображен на рисунке 2.9.

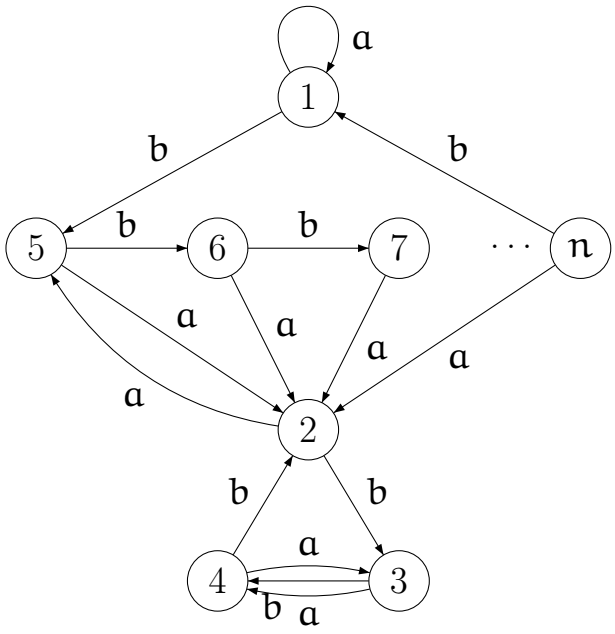


Рис. 2.8: Автомат $\mathscr{VC}_n$

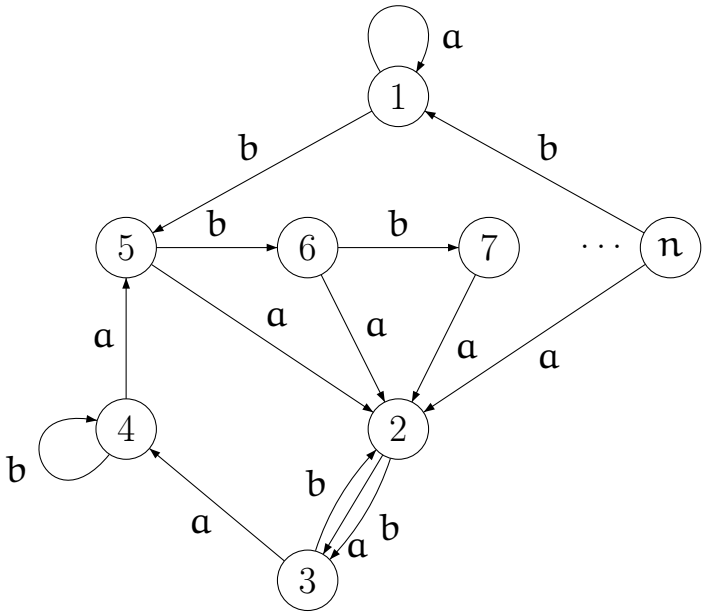


Рис. 2.9: Автомат $\mathscr{VD}_n$

Для данного автомата справедлива следующая теорема.

Теорема 2.4 Длина кратчайшего синхронизирующего слова автомата $\mathscr{VD}_n$, $n > 7$, n-нечетное, равна $3n + 3$.

Кратчайшее синхронизирующее слово автомата $\mathscr{VD}_n$ имеет вид $abab^{n-4}aabab^{n-4}abaaab^{n-4}aba$.

Заметим, что при некоторых n определен как $\mathscr{VC}_n$, так и $\mathscr{VD}_n$. В этом случае $\mathscr{VC}_n$ синхронизируется более длинным словом.

Рассмотрим серию автоматов $\mathscr{VG}_{n,k}$, k – нечетное, в которой параметрами являются и число состояний автомата, и веерность выделенной буквы, действие букв на автоматах серии определены так:

$m = 1$	$\delta(m, a) = 1$	$\delta(m, b) = 2$
$m = 2$	$\delta(m, a) = n - k + 1$	$\delta(m, b) = 3$
$2 < m < n - k, m = 2t + 1$	$\delta(m, a) = m + 1$	$\delta(m, b) = m - 1$
$2 < m < n - k, m = 2t$	$\delta(m, a) = m - 1$	$\delta(m, b) = m + 1$
$m = n - k, m = 2t + 1$	$\delta(m, a) = m$	$\delta(m, b) = m - 1$
$m = n - k, m = 2t$	$\delta(m, a) = m - 1$	$\delta(m, b) = m$
$n - k < m < n$	$\delta(m, a) = 2$	$\delta(m, b) = m + 1$
$m = n$	$\delta(m, a) = 2$	$\delta(m, b) = 1$

Автомат $\mathscr{VG}_{7,3}$ изображен на рисунке 2.10.

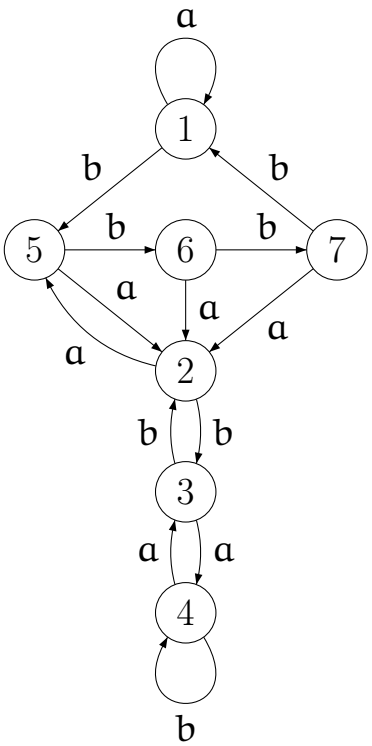


Рис. 2.10: $\mathscr{VG}_{7,3}$

Сформулируем гипотезу оценки длины кратчайшего синхронизирующего слова нашей серии.

Гипотеза 2.1 Длина кратчайшего синхронизирующего слова автомата $\mathscr{VG}_{n,k}$, k – нечетное, равна $(k+5)(n-k-2)+k+6$, где k – веерность буквы a. Кратчайшее слово имеет вид $aba((b^k ab)(baa))^{n-k-2}(b^k ab)a$.

Серия естественным образом разбивается на однопараметрические серии с условием $n-k=\mathrm{const}$. Для каждой из этих серий могут быть проведены рассуждения, аналогичные описанным в доказательстве теорем данной главы. Эти рассуждения были проведены для серий, начинающихся с автоматов $\mathscr{VG}_{n,3}$, $n<10$, полученные результаты соответствуют выдвинутой гипотезе. Кроме того, гипотеза непосредственно проверена для автоматов $\mathscr{VG}_{n,3}$, $n<25$. Доказательство гипотезы в общем случае пока остается открытой проблемой.

2.3 Экспериментальная проверка экстремальности серий при небольших n

В данном параграфе мы обращаемся к проблеме экстремальности полученных серий в своем классе автоматов. Иными словами, для каждой из описанных серий нужно установить, существует ли на ее области определения автомат, имеющий букву такой же веерности, но синхронизируемый более длинным словом. Мы отвечаем на данный вопрос для небольших n, используя численный эксперимент, в рамках которого вычисляется длина кратчайшего синхронизирующего слова для всех автоматов определенного класса с фиксированным числом состояний.

В статье [51] приведена таблица длин кратчайших синхронизирующих слов для автоматов с n состояниями над двухбуквенным алфавитом, имеющих выделенную букву веерности k специального вида для $n<10$.

Мы провели серию экспериментов для $n\geq 10$, ограничив класс автоматов, поскольку для общего случая перебор слишком велик. Заметим, что в автоматах всех рассмотренных серий действие букв на $k+1$ состояниях определены одинаково (см. рис. 2.11). Мы ограничили перебор автоматами, действия букв на $k+1$ состояниях которых определены так же. Далее под экстремальностью мы будем понимать экстремальность на области, на которой проводился численный эксперимент.

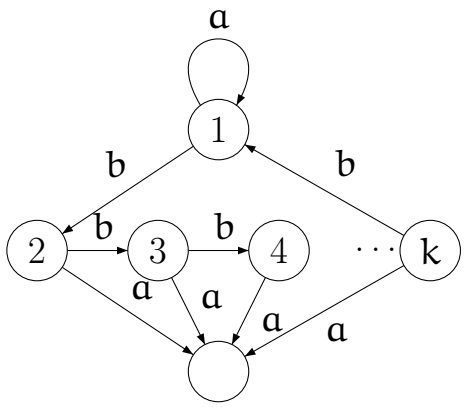


Рис. 2.11: Действие букв на состояниях автомата

В таблице 2.12 приведены результаты экспериментов Романа из [**51**] (автоматы с числом состояний менее 10) и результаты наших экспериментов.

n/k	2	3	4	5	6	7	8	9	10
2	1								
3	4	1							
4	9	4	1						
5	16	9	4	1					
6	25	17	10	4	1				
7	36	25	18	11	4	1			
8	49	36	28	21	12	4	1		
9		49	37	31	22	13	4	1	
10				42	33	25	14	4	1
11				51	44	37	26	15	4
12					56	49	39	29	16
13					66	61	53	43	30
14							65	58	46
15							79	71	61
16									76
17									91

Рис. 2.12: Сводная таблица результатов численных экспериментов

В результате эксперимента получено следующее:

$\mathscr{VA}_n$: серия экстремальна, $n \leq 12$.

$\mathscr{VB}_n$: серия экстремальна, $n \leq 13$.

$\mathscr{VC}_n$: серия экстремальна, $n \leq 14$.

$\mathscr{VD}_n$: серия экстремальна для всех пар (n, k), на которых определена серия $\mathscr{VD}_n$, но не определена $\mathscr{VC}_n$, в противном случае экстремальна последняя, $n \leq 14$.

$\mathscr{VG}_{n,k}$: серия экстремальна в тех случаях, когда длина кратчайшего синхронизирующего слова n-автомата серии не превосходит $(n-k+1)^2$, кроме случая (14,8), когда она не экстремальна, но доставляет наилучшую из всех серий оценку, $n \leq 15$.

Полученные результаты позволяют высказать гипотезу, что серии $\mathscr{VA}_n$, $\mathscr{VB}_n$, $\mathscr{VC}_n$ и $\mathscr{VD}_n$ на всей области определения и серия $\mathscr{VG}_{n,k}$ при $n - k = 3$ и $n - k = 4$ для любого n экстремальны.

Глава 3
Синхронизируемость случайных автоматов

3.1 Предварительные сведения

В доказательствах теорем текущей главы используются известные утверждения из разных областей математики. В данном параграфе мы сформулируем эти утверждения, зафиксируем используемую терминологию, а также докажем несколько несложных "технических" лемм.

Сведения из теории вероятностей

Все приведенные в параграфе формулировки известных утверждений взяты из [**18**]. Понятия *вероятностного пространства*, *события*, *случайной величины* и ее основных параметров будем считать известными.

Для доказательства того, что с высокой вероятностью[1] ни в одном событии из множества не наступит отрицательный исход, мы часто будем использовать неравенство Буля:

Лемма 3.1 (Неравенство Буля)
Пусть $E_1, \ldots, E_n$ – произвольные события из некоторого вероятностного пространства. Тогда

$$\mathbf{P}\left(\bigcup_{i=1}^{n} E_i\right) \leq \sum_{i=1}^{n} \mathbf{P}\left(E_i\right).$$

Пусть X – случайная величина (вероятностное пространство мы в последующих рассуждениях указывать не будем). *Математическое ожидание* этой случайной величины мы будем обозначать через $\mathbf{M}(X)$, а ее *дисперсию* – через $\mathsf{Var}X$. Отметим, что $\mathsf{Var}X = \mathbf{M}\left(X^2\right) - \mathbf{M}\left(X\right)^2$. Сформулируем ряд известных утверждений, связывающих эти понятия.

Лемма 3.2 (Неравенство Чебышева)
Для любой случайной величины X и любого действительного числа k выполняется следующее неравенство

$$\mathbf{P}\left(|X - \mathbf{M}\left(X\right)| > k\sqrt{\mathsf{Var}X}\right) \leq 1/k^2.$$

[1] Напомним, что высокой мы называем вероятность, которая стремится к 1 при n, идущем к бесконечности.

Лемма 3.3 (Граница Чернова)
Пусть $X_1, \ldots, X_n$ – независимые случайные величины, принимающие значения из отрезка $[0, 1]$. Пусть $X = \sum_{i=1}^{n} X_i$.

(a) Пусть $\delta \in [0; 1]$. Тогда $\mathbf{P}(X \leq (1-\delta)\mathbf{M}(X))) \leq (\frac{e^{-\delta}}{(1-\delta)^{1-\delta}})^{\mathbf{M}(X)}$.

(b) Пусть $\delta \geq 0$. Тогда $\mathbf{P}(X \geq (1+\delta)\mathbf{M}(X))) \leq (\frac{e^{\delta}}{(1+\delta)^{1+\delta}})^{\mathbf{M}(X)}$.

Граница Чернова существует в нескольких формулировках для разных значений параметра δ, приведем формулировку, которую мы будем использовать в доказательствах.

Следствие 3.1 Пусть $X_1, \ldots, X_n$ – независимые случайные величины, принимающие значения из отрезка $[0, 1]$. Пусть $X = \sum_{i=1}^{n} X_i$. Тогда для любого $d \geq 6\mathbf{M}(X)$ выполняется неравенство $\mathbf{P}(X \geq d) \leq 2^{-d}$.

Докажем небольшой технический результат.

Лемма 3.4 Пусть X – случайная величина, принимающая значения из отрезка $[0, 1]$. Тогда имеет место неравенство

$$\mathbf{P}(X \geq \mathbf{M}(X)/2) \geq \frac{\mathbf{M}(X)}{2 - \mathbf{M}(X)}.$$

Доказательство. Пусть c – константа такая, что $0 < c < 1$. В определении математического ожидания случайной величины X оценим сверху константой c значения X, не превышающие c, и константой 1 – значения, превышающие c. Получим следующее неравенство

$$\mathbf{M}(X) \leq c\mathbf{P}(X \leq c) + (1 - \mathbf{P}(X \leq c)),$$

или

$$\mathbf{P}(X \leq c) \leq \frac{1 - \mathbf{M}(X)}{1 - c},$$

откуда

$$\mathbf{P}(X \geq c) \geq \frac{\mathbf{M}(X) - c}{1 - c}.$$

Положив c равным $\mathbf{M}(X)/2$, завершаем доказательство. □

Процесс Гальтона-Ватсона

Рассмотрим процесс развития популяции, в которой каждая особь размножается независимо от остальных. Для моделирования этого процесса используется *процесс Гальтона-Ватсона* [16]. Простой процесс Гальтона-Ватсона – последовательность случайных величин $\{X_n\}$, удовлетворяющих условию

$$X_n = \sum_{i=1}^{X_{n-1}} \xi, \tag{3.1}$$

где ξ – некоторая предопределенная случайная величина. В терминах развития популяции X_1 представляет собой изначальный размер популяции, а X_n – количество особей в n-м поколении. Распределение случайной величины ξ показывает распределение числа потомков одной особи. Одним из важнейших параметров популяции является вероятность ее вымирания, т. е. того, что в некотором поколении особей не будет, или $\mathbf{P}(X_n = 0$ для некоторого $n)$. Известно следующее утверждение, описывающее этот параметр.

Лемма 3.5 (Утверждение 1.2, [16])
Пусть

$$X_n = \sum_{i=1}^{X_{n-1}} \xi, X_1 > 0, \mathbf{M}(\xi) > 1. \tag{3.2}$$

Тогда существует константа r такая, что $\mathbf{P}(X_n = 0) > r$ для всех n.

Обозначим $q = \lim\limits_{n\to\infty} \mathbf{P}(X_n = 0)$.

Теорема 3.1 (Теорема 3, С. 30, [17])
Пусть $\{X_n : n = 1, 2, \dots\}$ – процесс Гальтона-Ватсона, $\mathbf{M}(\xi) > 1$, $X_1 = 1$. Тогда существует последовательность констант $\{C_n\}$, $C_n \to \infty$, $C_n^{-1} C_{n+1} \to m$ при $n \to \infty$, такая, что последовательность случайных величин $W_n = C_n^{-1} Z_n$ с высокой вероятностью сходится к случайной величине W такой, что $\mathbf{P}(W > 0) = 1 - q$.

Теорема Вормальда

Один из инструментов нашего анализа – применение теоремы, доказанной Вормальдом [66], которая позволяет заменить вероятностный анализ

комбинаторного алгоритма решением детерминированной системы дифференциальных уравнений.

Мы будем говорить, что функция g является $o(f)$, если $\lim\limits_{n\to\infty}(g/f) = 0$. Причем предел в данном случае равномерный по всем остальным переменным.

Пусть дана последовательность Ω_n, $n = 1, 2, \ldots$ вероятностных пространств. Пусть X_n – набор случайных величин, причем X_n определена на пространстве Ω_n. Для случайной величины X мы будем говорить, что $X = o(f(n))$ выполняется *всегда*, если $\max\{x \mid \mathbf{P}(X = x) \neq 0\} = o(f(n))$. Мы будем говорить, что событие в Ω_n происходит *почти наверное*, если его вероятность равна $1 - o(1)$.

Дискретным случайным процессом мы называем последовательность векторных случайных величин $\overrightarrow{X_t}$. *Историей случайного процесса* к моменту t_0 называется матрица H_{t_0}, строчками которой являются значения вектора $\overrightarrow{X_t}$ для $t < t_0$.

Все рассматриваемые случайные процессы являются дискретными. Такой процесс представляет собой вероятностное пространство Ω, обозначаемое через $(Q_0, Q_1, \ldots)$, где каждое Q_i принимает значения из некоторого множества S.

Функция $f(u_1, \ldots, u_j)$ удовлетворяет *условию Липшица* на множестве $D \subseteq \mathbb{R}^j$, если существует константа $L > 0$ со свойством:

$$|f(u_1, \ldots, u_j) - f(v_1, \ldots, v_j)| \leq L \sum_{i=1}^{j} |u_j - v_i|,$$

выполняющимся для всех $(u_1, \ldots, u_j)$ и $(v_1, \ldots, v_j)$ из D.

Теорема 3.2 (Вормальд, [66])

Пусть $\overrightarrow{Y_t^n}$ – семейство случайных процессов размерности k, для краткости индекс n мы будем опускать. Через $Y_t^{(\ell)}$ мы будем обозначать ℓ-ю координату $\overrightarrow{Y_t}$. Для ℓ, $1 \leq \ell \leq k$, пусть функция $f_\ell\colon \mathbb{R}^{k+1} \to \mathbb{R}$ такова, что для некоторой константы C и для всех ℓ и t выполняется $|Y_t^{(\ell)}| < Cn$. Предположим также, что для некоторой функции $m = m(n)$:

(i) для всех ℓ и равномерно по всем $t < m$, $\mathbf{P}\left(|Y_{t+1}^{(\ell)} - Y_t^{(\ell)}| > n^{1/5} \mid H_t\right) = o(n^{-3})$ всегда;

(ii) для всех ℓ и равномерно по всем $t < m$, $\mathbf{M}\left(Y_{t+1}^{(\ell)} - Y_t^{(\ell)} \mid H_t\right) = f_\ell(t/n, Y_t^{(1)}/n, \ldots, Y_t^{(k)}/n) + o(1)$ всегда;

(iii) для каждого ℓ функция f_ℓ непрерывна и удовлетворяет условию Липшица на D, где D – некоторое ограниченное связное открытое множество, содержащее пересечение множества $\{(t, z^{(1)}, \ldots, z^{(k)}) \mid t \geq 0\}$ с некоторой окрестностью множества $\{(0, z^{(1)}, \ldots, z^{(k)}) \mid \mathbf{P}\left(Y_0^{(\ell)} = z^{(\ell)} n, 1 \leq \ell \leq k\right) \neq 0$ для некоторого $n\}$.

Тогда:

(a) Для любой точки $(0, \hat{z}^{(1)}, \ldots, \hat{z}^{(k)}) \in D$ система дифференциальных уравнений

$$\frac{dz_\ell}{ds} = f_\ell(s, z_1, \ldots, z_k),\ \ell = 1, \ldots, k, \tag{3.3}$$

имеет на множестве D единственное решение $(s, z_1, \ldots, z_k)$, $z_\ell \colon \mathbb{R} \to \mathbb{R}$ со свойством $z_\ell(0) = \hat{z}^{(\ell)}$, $1 \leq \ell \leq k$. Это решение может быть распространено на точки сколь угодно близкие к границе D.

(b) Если $\hat{z}^{(\ell)} = Y_0^{(\ell)}/n$, $0 \leq t \leq \min\{\sigma n, m\}$ и $\sigma = \sigma(n)$ является супремумом таких s, на которые решение системы (3.3) может быть продолжено, то равенство;

$$Y_t^{(\ell)} = n z_\ell(t/n) + o(n)$$

справедливо почти наверное, равномерно для $0 \leq t \leq \min\{\sigma n, m\}$.

3.2 Случайные автоматы, синхронизируемые с высокой вероятностью

В этом параграфе мы обратимся к следующему вопросу, поставленному во введении:

— Какой размер входного алфавита достаточен, чтобы почти все автоматы над алфавитом этого размера были синхронизируемы, и какой будет наиболее вероятная длина кратчайшего синхронизирующего слова для таких автоматов?

Для ответа на этот вопрос определим процесс на автомате, направленный на синхронизицию некоторой пары состояний, и изучим его поведение.

Пусть $\mathbf{p}, \mathbf{q}$ – пара состояний случайного автомата $\mathscr{A} = (Q, \Sigma, \delta)$. Определим для этой пары состояний процесс VACUUM, цель которого – найти слово $w = a_1 \ldots a_k$ такое, что $\mathbf{p}w = \mathbf{q}w$.

На первом шаге процесса мы случайным образом выбираем[2] букву $a_1 \in \Sigma$ и совершаем переходы из $p_0 = p$ в $p_1 = p_0 a_1$ и из $q_0 = q$ в $q_1 = q_0 a_1$. Если $p_1 = q_1$, то процесс успешно завершается, вернув слово $w = a_1$, иначе он продолжается.

На m-м шаге процесса мы оказываемся в состояниях p_{m-1} и q_{m-1}. Выбираем букву a_m, которая ранее не применялась для переходов из состояний p_{m-1} и q_{m-1}. Если такой буквы нет, процесс завершается неуспехом. Если мы смогли выбрать a_m, переходим с ее помощью из p_{m-1}, q_{m-1} в p_m, q_m соответственно, аналогично первому шагу. Если $p_m = q_m$, процесс завершается построением $w = a_1 a_2 \dots a_m$, иначе он продолжается. Очевидно, каждый шаг процесса имеет 3 возможных исхода: процесс завершается неуспехом, процесс завершается построением слова и процесс продолжается. Таким образом, если процесс не завершится неуспехом ранее, на некотором шаге k он завершится построением слова $w = a_1 \dots a_k$ такого, что $pw = qw$.

Формальное описание процесса представлено на рис. 3.1.

Изучим поведение процесса Vacuum.

Перед тем как сформулировать первую лемму, введем необходимые определения. Рассмотрим ориентированный граф $G = (V, E)$. Напомним, что орграф называется *полным*, если из любой его вершины в любую ведет дуга, т.е. для любых вершин $q_1, q_2 \in V$ найдется дуга $e \in E$ такая, что $e = (q_1 q_2)$. *Случайным блужданием* называется такой путь в полном ориентированном графе, в котором каждая следующая вершина выбирается случайно и не зависит от истории.

Лемма 3.6 Если процесс Vacuum применяется к случайному автомату $\mathscr{A} = (Q, \Sigma, \delta)$ и паре его состояний $p_0 \in Q, q_0 \in Q$ и проходит не менее t шагов, то каждый из путей $\{p_0, \dots, p_t\}$, $\{q_0, \dots, q_t\}$ не отличим от случайного блуждания в полном ориентированном графе.

Доказательство. Чтобы получить требуемое в лемме, необходимо доказать, что каждое состояние p_i в пути $\{p_0, \dots, p_t\}$ выбирается случайно (доказательство для q_i проводится полностью аналогично). Действитель-

[2]Здесь и далее под *случайным выбором* мы будем понимать равномерно случайный, т. е. выбор, при котором любое значение может быть выбрано с равной вероятностью.

Вход: Случайный автомат $\mathscr{A} = (Q, \Sigma, \delta)$ и пара состояний $p \in Q, q \in Q$
Выход: ***неуспех*** или слово $w = a_1 \dots a_k$ такое, что $pw = qw$
Описание процесса:

пусть $\Delta_r \subseteq \Sigma$, $w \in \Sigma^*$
Установить $\Delta_r = \varnothing$ для всех $r \in Q$, $w = \varepsilon$
пока $pw \neq qw$
  если $\Delta_{pw} \cup \Delta_{qw} \neq \Sigma$ **то**
    Выбрать $a \in \Sigma \setminus (\Delta_{pw} \cup \Delta_{qw})$
  иначе
    Вернуть ***неуспех***
  Установить $\Delta_{pw} = \Delta_{pw} \cup \{a\}$, $\Delta_{qw} = \Delta_{qw} \cup \{a\}$
  Установить $w = wa$
Вернуть w

Рис. 3.1: Процесс Vacuum

но, в рамках процесса Vacuum на каждом шаге i мы выбираем букву a_i, которая до этого не использовалась в состоянии p_{i-1}, и совершаем переход $p_i = p_{i-1}a_i$. Случайный выбор новой буквы для перехода из состояния в случайном автомате эквивалентен случайному выбору результата перехода – состояния p_i. Таким образом, p_i выбирается случайно из Q и не зависит от истории.

Это же утверждение может быть доказано конструктивно. Пусть $B = (Q, E)$ – полный орграф; $\{p_0, \dots, p_t\}$ и $\{q_0, \dots, q_t\}$ – случайные блуждания в B длины t. Построим из B случайный автомат A с двумя путями, представляющими собой первые t шагов процесса Vacuum. Пометим дуги из E буквами алфавита Σ по следующему правилу: двигаясь вдоль дуг, составляющих случайное блуждание, мы помечаем дугу, исходящую из p_i (аналогично из q_i), произвольной буквой алфавита, которая ранее не использовалась для исходящей дуги этой вершины; остальные дуги помечаем равномерно случайно так, чтобы из каждой вершины исходило $|\Sigma|$ дуг, помеченных разными буквами. После помечивания удаляем все непомеченные дуги. В результате, получится случайный автомат по определению, а наши блуждания в нем станут в точности первыми t шагами

процесса VACUUM, поскольку при помечивании дуг мы руководствовались теми же принципами.

Построение B из A состоит в добавлении недостающих дуг и стирании меток с имеющихся. Объяснение того факта, что $\{p_0, \ldots, p_t\}$ и $\{q_0, \ldots, q_t\}$ являются случайными блужданиями в B, полностью повторяет рассуждения, проведенные в первом доказательстве леммы. □

Теперь ограничим вероятность того, что процесс VACUUM может пройти большое количество шагов.

Лемма 3.7 Пусть процесс VACUUM применен к паре состояний p, q случайного n-автомата $\mathscr{A} = (Q, \Sigma, \delta)$. Тогда для произвольной константы $K > 1$ вероятность того, что процесс совершит не менее $Kn \ln n$ шагов, меньше n^{-K}.

Доказательство. Допустим, процесс совершил не менее $Kn \ln n$ шагов. Значит, на каждом проделанном им шаге $t < Kn \ln n$ он не закончил свою работу, вернув слово w. Следовательно, как мы заметили ранее, он либо закончился неуспехом, либо продолжился. Состояния p_t и q_t выбираются случайно и независимо из Q. Вероятность того, что p_t и q_t совпадут, равна $\frac{1}{n}$, а вероятность других исходов – $\left(1 - \frac{1}{n}\right)$. Таким образом, вероятность того, что процесс не остановится в течение первых $Kn \ln n$ шагов, меньше $\left(1 - \frac{1}{n}\right)^{Kn \ln n} \leq n^{-K}$. □

Мы доказали, что вероятность существования длинных путей вида $u_1 u_2 \ldots u_t$ довольно низкая. Возникает следующий вопрос: как часто состояния в таком пути повторяются? Для ответа на этот вопрос нам потребуется сформулированный ниже факт, касающийся случайного блуждания в полном орграфе.

Лемма 3.8 Пусть $q_1, \ldots, q_{Kn \ln n}$ для некоторой константы $K > 1$ – случайное блуждание в полном орграфе с n вершинами. Тогда для любой константы L, $L \geq 6K$, вероятность существования вершины x, которая встречается в этом блуждании не менее чем $L \ln n$ раз, меньше $n^{1 - \frac{L}{2}}$.

Доказательство. Зафиксируем вершину $x \in Q$. Эта вершина встречается в пути $q_1, \ldots, q_{Kn \ln n}$ $|\{i \mid q_i = x\}|$ раз с вероятностью $\frac{1}{n}$ на каждом шаге. Случайная величина $|\{i \mid q_i = x\}|$ имеет математическое ожидание $\frac{1}{n} \times Kn \ln n = K \ln n$.

Применим для этой случайной величины границу Чернова из следствия 3.1 с $d = L \ln n = \frac{L}{K} K \ln n \geq 6M\left(|\{i \mid q_i = x\}|\right)$ и получим следующее неравенство:

$$\mathbf{P}\left(|\{i \mid q_i = x\}| \geq L \ln n\right) \leq 2^{-L \ln n} = n^{-L \ln 2} \leq n^{-\frac{L}{2}}.$$

Вероятность существования вершины с указанными свойствами оценивается суммой вероятностей для всех вершин $x \in Q$, т. е. значением $n^{1-\frac{L}{2}}$. Лемма доказана. □

Теперь мы готовы к доказательству ключевой леммы параграфа.

Лемма 3.9 Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – случайный автомат, $|Q| = n, |\Sigma| \geq \geq 72 \ln n$. Тогда для двух любых состояний $p \in Q, q \in Q$ процесс Vacuum не закончится неуспехом с высокой вероятностью.

Доказательство. Подставляя $K = 3$ в лемму 3.7, получаем, что процесс Vacuum не завершится за $3n \ln n$ шагов с вероятностью не более n^{-3}. Это значит, что наш процесс завершится построением слова w или неуспехом с вероятностью не менее $1 - n^{-3}$.

Подставляя $L = 18$ в лемму 3.8 и используя лемму 3.6, получаем, что вероятность того, что p_t или q_t посетит некоторое состояние не менее чем $18 \ln n$ раз, меньше $2n^{-8}$.

Процесс может завершиться неуспехом на j-м шаге, если мы не сможем выбрать букву, по которой мы не переходили как из p_{j-1}, так и из q_{j-1}. Заметим, что до шага j мы могли посетить каждое состояние в рамках обеих прогулок. Пусть $|\Sigma| \geq 72 \ln n$. Если процесс завершился неуспехом, это значит, что по крайней мере одно из состояний p_{j-1} и q_{j-1} встретилось в соответствующей прогулке не менее, чем в $18 \ln n$-й раз. То есть вероятность того, что процесс завершится неуспехом, меньше $2n^{-8}$.

Существует только две ситуации, при которых слово w не будет найдено до $3n \ln n$-го шага — завершение процесса неуспехом или продолжение процесса после этого шага, отсюда, вероятность не найти слово w до шага $3n \ln n$ не более $n^{-3} + 2n^{-8} \leq 3n^{-3}$. Это означает, что процесс Vacuum успешно завершится с вероятностью $1 - 3n^{-3}$. Лемма доказана. □

Из леммы 3.9 легко вытекает доказательство следующей теоремы, основного результата этого параграфа:

Теорема 3.3 Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – случайный автомат такой, что $|Q| = n$, $|\Sigma| \geq 72 \ln n$. Тогда A синхронизируем с высокой вероятностью. Более того, длина кратчайшего синхронизирующего слова этого автомата с высокой вероятностью меньше $3n^2 \ln n$.

Доказательство. В соответствии с леммой 3.9, процесс VACUUM для некоторой пары состояний $p, q \in Q$ не завершится успехом с вероятностью $3n^{-3}$. Применение неравенства Буля по всем n^2 парам состояний завершает доказательство синхронизируемости. Оценка длины синхронизирующего слова выводится из того факта, что любые два состояния автомата могут быть синхронизированы за $3n \ln n$ шагов. Для того чтобы синхронизировать автомат, мы последовательно синхронизируем $n - 1$ пару. □

Полученная оценка на размер алфавита, на наш взгляд, неточна. Экспериментальные данные показывают, что уже над двухбуквенным алфавитом почти все автоматы синхронизируемы. В то же время это наилучший известный теоретический результат.

Длина кратчайшего синхронизирующего слова $3n^2 \ln n$ меньше доказанной Пэном, но все еще больше границы Черни. Ограничения на алфавит, необходимые для того, чтобы автомат удовлетворял гипотезе Черни, рассмотрены в следующем параграфе.

3.3 Случайные автоматы, для которых выполняется гипотеза Черни

В предыдущем параграфе мы получили условие на входной алфавит, гарантирующий синхронизацию почти всех автоматов над этим алфавитом. В этом параграфе ужесточим требования и получим ответ на следующий вопрос:

— Какой размер входного алфавита достаточен, чтобы почти все автоматы над алфавитом этого размера были синхронизируемы и удовлетворяли гипотезе Черни?

Для получения оценки аналогично предыдущему параграфу определим некоторый процесс на конечном автомате.

Рассмотрим автомат над 2-буквенным алфавитом. Определим на нем процесс EPIDEMIA. Получая на вход автомат $\mathscr{A} = (Q, \{a, b\}, \delta)$ и состояние $x \in Q$, этот процесс возвращает Q_2 – множество всех состояний,

из которых достижимо состояние x.

Положим, что состояние $q \in Q$ больно некоторой болезнью, и эта болезнь может распространяться по автомату вдоль стрелок в обратном направлении, т. е. если состояние q больно, то через некоторые время все состояния $\{p \mid (pa = q) \vee (pb = q)\}$ также заболеют. В этих терминах цель процесса – найти все состояния, которые могут быть заражены, если изначально больно только состояние x.

Алгоритм работает следующим образом. На каждом шаге работы алгоритма мы рассматриваем 3 множества: Q_2 – множество состояний, которые на текущий момент больны и уже заразили всех своих соседей, Q_1 – множество состояний, которые уже больны, но еще не заразили своих соседей, Q_0 – множество здоровых состояний.

На первом шаге $Q_0 = Q \setminus \{x\}, Q_1 = \{x\}, Q_2 = \varnothing$. На каждом шаге процесса мы случайным образом выбираем состояние $q \in Q_1$ и рассматриваем множество $N = \{p \in Q_0 \mid (pa = q) \vee (pb = q)\}$ всех здоровых состояний, которые могут быть непосредственно заражены состоянием q. На этом шаге мы исключаем множество N из Q_0 и включаем в Q_1 – с этого момента состояния из множества N больны и могут заразить своих соседей на следующих шагах алгоритма. Состояние q переходит в множество Q_2, оно более не опасно для здоровых состояний. На некотором шаге множество Q_1 становится пустым: все состояния, которые могли бы быть заражены, уже заражены и, соответственно, множество Q_2 построено.

Формальное описание процесса приведено на рис. 3.2. Шаг процесса проиллюстрирован на рис. 3.3.

Нам потребуется следующий технический результат.

Лемма 3.10 Пусть $\mathscr{A} = (Q, \{a, b\}, \delta)$ – случайный n-автомат. Тогда для любой буквы $a \in \Sigma$ вероятность того, что существует состояние q такое, что найдется не менее $n^{1/5}$ состояний q', для которых $q'a = q$, не более $n^{-cn^{1/5}}$ для некоторой константы c.

Доказательство. Известно, что для любых n, m выполняется

$$\binom{n}{m} \leq \left(\frac{ne}{m}\right)^m. \tag{3.4}$$

Зафиксируем состояние q и множество M из $n^{1/5}$ других состояний. Вероятность того, что для всех состояний из множества M стрелки, поме-

Вход: Случайный автомат $\mathscr{A} = (Q, \{a, b\}, \delta)$ и состояние $x \in Q$
Выход: множество Q_2 всех состояний, из которых достижимо состояние x
Описание процесса:

пусть Q_0, Q_1, Q_2 – подмножества Q
Установить $Q_0 = Q \setminus \{x\}, Q_1 = \{x\}, Q_2 = \varnothing$
пока $Q_1 \neq \varnothing$
  Выбрать $q \in Q_1$ случайно
  Установить $N = \{p \in Q_0 \mid (pa = q) \vee (pb = q)\}$
  Установить $Q_0 = Q_0 \setminus N$, $Q_1 = (Q_1 \setminus \{q\}) \cup N$, $Q_2 = Q_2 \cup \{q\}$
Вернуть Q_2

Рис. 3.2: Процесс Epidemia

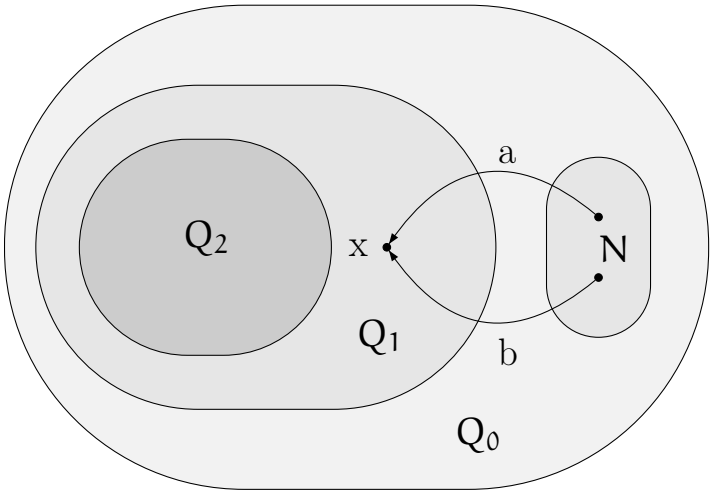


Рис. 3.3: Один шаг процесса Epidemia

ченные буквой a, ведут в q, меньше

$$n^{-n^{1/5}} = e^{-n^{1/5} \ln n}.$$

Количество способов выбора q и M оценивается следующим образом:

$$n\binom{n}{n^{1/5}} \leq n(n^{1-1/5}e)^{n^{1/5}} \leq e^{(\frac{4}{5}+o(1))n^{1/5} \ln n}.$$

По неравенству Буля вероятность существования множества M и состояния q оценивается сверху величиной $e^{-(\frac{1}{5}+o(1))n^{1/5}\ln n}$. $\square$

Приступим к доказательству ключевой леммы параграфа.

Лемма 3.11 Пусть $\mathscr{A} = (Q, \{a, b\}, \delta)$ – случайный автомат над двухбуквенным алфавитом, $x \in Q$. Тогда существует константа r, $0 < r < 1$, такая, что для достаточно больших n вероятность того, что для каждого состояния $q \in Q$ существует слово $w_{q\to x} \in \{a, b\}^*$, удовлетворяющее условию $qw_{q\to x} = x$, больше r.

Доказательство. Рассмотрим состояние $x \in Q$ и вычислим вероятность того, что оно может быть достигнуто из любого состояния из Q, т. е. процесс Epidemia с состоянием x на входе вернет $Q_2 = Q$. Вычисление можно разбить на 3 этапа:

— вычисление вероятности того, что процесс не остановится в начале, проделав не более $0.1n$ шагов;

— вычисление вероятности того, что процесс не остановится в середине, с числом шагов между $0.1n$ и $0.9n$;

— вычисление вероятности того, что процесс не остановится в конце, до того как $|Q_2| = n$, т. е. вероятности того, что сделав $0.9n$ шагов, процесс сделает n.

Начнем с вычисления первой вероятности. Заметим, что если на некотором шаге $t < 0.1n$ мы получим $|Q_1| > 0.2n$, то процесс не завершится к шагу $0.1n$, на данном шаге мы получим $|Q_1| \geq 0.1n$. В противном случае, на шаге t мы получим $|Q_2| + |Q_1| \leq 0.3n$ и, следовательно, $|Q_0| > 0.7n$. Каждое состояние $q' \in Q_0$ с вероятностью больше $\frac{2}{n} - \frac{1}{n^2}$ удовлетворяет $q' \in N$. Отсюда матожидание числа элементов множества N на шаге $t < 0.1n$ не меньше $\frac{2}{n} \cdot 0.7n + o(1) \geq 1.3$. Рассмотрим процесс Гальтона-Ватсона на автомате $\mathscr{A}$. В качестве X_1 возьмем состояние x, а в качестве ξ – размер множества N для соответствующего состояния q. Видоизменим процесс Epidemia так, что состояние q из Q_1 будем выбирать не случайно, а будем брать состояния в том порядке, в котором они были добавлены к Q_1. Заметим, что матожидание числа элементов в N у нового процесса то же, что и у Epidemia, и если этот процесс пройдет $0.1n$ шагов, то и Epidemia их пройдет.

Данный видоизмененный процесс EPIDEMIA можно рассматривать в следующем виде. На каждом шаге у нас есть популяция особей Q_1. Одна из них (назовем ее q) на этом шаге умирает, но может оставить потомство, ее потомки составляют множество N. Иными словами, наш видоизмененный процесс представляет собой процесс Гальтона-Ватсона, только более растянутый по времени; в множестве Q_1 могут одновременно находятся особи двух поколений. В соответствии с теоремой 3.1, если матожидание числа потомков больше 1, то по крайней мере с конечной вероятностью[3] процесс Гальтона-Ватсона на числе шагов, соответствующем $0.1n$ шагам процесса EPIDEMIA, не прекратится, число живых особей в популяции составит не менее ℓn для некоторой неотрицательной константы ℓ.

Рассмотрим t-й шаг процесса EPIDEMIA, где $t \in (0.1n, 0.9n)$. Через $Q_i(t)$ обозначим множества Q_i на шаге t процесса. Проверим, что к дискретному случайному процессу $Y(t) = (|Q_0(t)|, |Q_1(t)|, |Q_2(t)|)$ применима теорема Вормальда, т. е. выполняются ее условия (i)-(iii).

(i) Поскольку, в соответствии с леммой 3.10, полустепень захода каждой вершины превышает $n^{1/5}$ с экспоненциально малой вероятностью, получим $\mathbf{P}\left(|Q_0(t+1) - Q_0(t)| > n^{1/5}\right) < n^{-3}$. Аналогично неравенство выполняется для $|Q_1(t)|$. Изменение $|Q_2(t)|$ константное, для него условие выполняется с очевидностью.

(ii) Вычислим матожидание изменения $|Q_0|, |Q_1|$ и $|Q_2|$:

$$\begin{aligned}
\mathbf{M}\left(|Q_0(t+1)| - |Q_0(t)|\right) &= -2 \times \frac{|Q_0(t)|}{n - |Q_2(t)|}, \\
\mathbf{M}\left(|Q_1(t+1)| - |Q_1(t)|\right) &= -1 + 2 \times \frac{|Q_0(t)|}{n - |Q_2(t)|}, \\
\mathbf{M}\left(|Q_2(t+1)| - |Q_2(t)|\right) &= 1.
\end{aligned}$$

Изменение $|Q_i|$ на каждом шаге имеет постоянное матожидание, которое может быть выражено через функции $Q_0(t), Q_1(t)$ и $Q_2(t)$.

(iii) Функции в правой части уравнений непрерывны и дифференцируемы на отрезке $[0.1, 0.9]$. Так что условие Липшица выполняется.

[3]Напомним, что конечной мы называем вероятность, которая ограничена снизу некоторой положительной константой при n, идущем к бесконечности.

Таким образом, выполняются все условия теоремы Вормальда. Применив теорему и обозначив t/n через y, получим следующую систему дифференциальных уравнений относительно переменных q_0, q_1 и q_2, соответствующих $|Q_0|, |Q_1|$ и $|Q_2|$.

$$\begin{aligned}
\frac{dq_0}{dy} &= -2 \times \frac{q_0(y)}{1 - q_2(y)}, \\
\frac{dq_1}{dy} &= -1 + 2 \times \frac{q_0(y)}{1 - q_2(y)}, \\
\frac{dq_2}{dy} &= 1
\end{aligned}$$

или, короче,

$$\begin{cases}
\dot{q_0} = -\frac{2q_0}{1-q_2} \\
\dot{q_1} = -1 + \frac{2q_0}{1-q_2} \\
\dot{q_2} = 1.
\end{cases}$$

Нетрудно видеть, что на шаге t процесса Epidemia получим $|Q_2(t)| = t$. Таким образом, нас интересует решение системы, в котором $q_2(y) = y$. Подставив выражение для q_2 в первое уравнение, получим линейное дифференциальное уравнение. Решим его относительно q_0. Итак, q_0 и q_2 известны, выразим q_1 интегрированием правой части второго уравнения. Получим параметризованное множество решений

$$q_0 = (y-1)^2 c, \; q_1 = (2c-1)y - y^2 c + d, \; q_2 = y$$

с параметрами c и d. По определению q_i $q_0 + q_1 + q_2 = 1$, следовательно, $c + d = 1$. Очевидно, $q_0 \geq 0$, отсюда $c \geq 0$. Наконец, $0 \leq c \leq 1$ и анализ квадратичной функции q_1 показывает, что $q_1(0.9n) > 0$. Процесс с высокой вероятностью продолжится по меньшей мере до шага $0.9n$, на котором $|Q_2| = 0.9n$. Таким образом, мы показали, что с конечной вероятностью вершина x достижима из $0.9n$ вершин.

Завершим доказательство, показав, что с высокой вероятностью не существует множества состояний, по размеру существенно меньше n/e, без исходящих стрелок. В терминах процесса Epidemia это означает, что если на некотором шаге $|Q_0| < n/e$, то следующий шаг всегда возможен, и в итоге мы получим $Q_2 = Q$.

Действительно, для фиксированного множества состояний размера m ($m = n/c$ для некоторой константы $c > e$) вероятность того, что из него не выходит ни одной стрелки, равна $(m/n)^{2m}$. Всего таких множеств размера m будет $\binom{n}{m}$, что не превосходит $\left(\frac{ne}{m}\right)^m$ в соответствии с (3.4). Из неравенства Буля получаем, что вероятность того, что существует множество размера m без исходящих стрелок, меньше

$$\left(\frac{m}{n}\right)^{2m}\left(\frac{ne}{m}\right)^m = \left(\frac{me}{n}\right)^m \underset{n\to\infty}{\longrightarrow} 0.$$

□

Для доказательства теоремы 3.4 нам нужна еще одна лемма.

Лемма 3.12 Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – случайный автомат такой, что $|Q| = n$, $|\Sigma| = n^\beta$, $\beta > 0.5$. Пусть Σ_1, Σ_2 – случайная пара множеств таких, что $\Sigma \supseteq \Sigma_1 \cup \Sigma_2$, $\Sigma_1 \cap \Sigma_2 = \varnothing$, $|\Sigma_1| = |\Sigma_2| = n^\alpha$ для действительного числа α такого, что $0.5 < \alpha < \beta$. Тогда с высокой вероятностью множество троек (a, b, q), $a \in \Sigma_1, b \in \Sigma_2$, для которых выполняется

$$qa = qb = q, \tag{3.5}$$

содержит более $n^{2\alpha-1}/2$ элементов.

Доказательство. Обозначим множество $\Sigma_1 \times \Sigma_2 \times Q$ через T, а случайную величину

$$|\{(a, b, q) \in T \mid qa = qb = q\}|$$

через X. Применим неравенство Чебышева (лемма 3.2) для доказательства того, что $X > n^{2\alpha-1}/2$ с высокой вероятностью.

Вычислим матожидание случайной величины X. Вероятность того, что тройка $(a, b, q) \in \Sigma_1 \times \Sigma_2 \times Q$ удовлетворяет (3.5), равна n^{-2}. Всего троек $n^{2\alpha+1}$, отсюда

$$\mathbf{M}(X) = n^{2\alpha+1} \times n^{-2} = n^{2\alpha-1}.$$

Теперь получим оценку сверху для дисперсии X. Поскольку

$$\mathsf{Var}X = \mathbf{M}\left(X^2\right) - \mathbf{M}(X)^2,$$

нужно получить оценку сверху для $\mathbf{M}\left(X^2\right)$. Определим случайную величину $\Delta_{(a,b,q)}$ следующим образом

$$\Delta_{(a,b,q)} = \begin{cases} 1, & qa = qb = q, \\ 0, & \end{cases}$$

и оценим $\mathbf{M}\left(X^2\right)$.

$$\begin{aligned}
\mathbf{M}\left(X^2\right) &= \mathbf{M}\left(\left(\sum_{(a,b,q)\in T}\Delta_{(a,b,q)}\right)^2\right) = \\
&= \sum_{\{(a_i,b_i,q_i)\}_{i=1,2}} \mathbf{M}\left(\Delta_{(a_1,b_1,q_1)}\cdot\Delta_{(a_2,b_2,q_2)}\right) = \\
&= \sum_{\{(a_i,b_i,q_i)\}_{i=1,2}\in T^2, q_1\neq q_2} \mathbf{M}\left(\Delta_{(a_1,b_1,q_1)}\cdot\Delta_{(a_2,b_2,q_2)}\right) + \\
&\quad + \sum_{a_1\neq a_2, b_1\neq b_2, q} \mathbf{M}\left(\Delta_{(a_1,b_1,q)}\cdot\Delta_{(a_2,b_2,q)}\right) + \\
&\quad + \sum_{a, b_1\neq b_2, q} \mathbf{M}\left(\Delta_{(a,b_1,q)}\cdot\Delta_{(a,b_2,q)}\right) + \\
&\quad + \sum_{a_1\neq a_2, b, q} \mathbf{M}\left(\Delta_{(a_1,b,q)}\cdot\Delta_{(a_2,b,q)}\right) + \\
&\quad + \sum_{a,b,q} \mathbf{M}\left(\Delta_{(a,b,q)}\cdot\Delta_{(a,b,q)}\right).
\end{aligned}$$

Заметив, что $|\Sigma_1| = |\Sigma_2| = n^\alpha, |Q| = n$, получим

$$\mathbf{M}\left(X^2\right) = n^{4\alpha}n(n-1)n^{-4} + n^{2\alpha}(n^\alpha-1)^2 n n^{-4} + 2n^{2\alpha}(n^\alpha-1)n n^{-3} + n^{2\alpha}n n^{-2}$$

и, отсюда,

$$\mathbf{M}\left(X^2\right) \leq n^{4\alpha-2} + n^{4\alpha-3} + 2n^{3\alpha-2} + n^{2\alpha-1} \leq \mathbf{M}\left(X\right)^2 + o(n) + \mathbf{M}\left(X\right).$$

Таким образом,

$$\mathsf{Var}X = \mathbf{M}\left(X^2\right) - \mathbf{M}\left(X\right)^2 \leq \mathbf{M}\left(X\right) + o(n) \leq 2\mathbf{M}\left(X\right).$$

Неравенство Чебышева в применении к X с учетом того, что $\mathsf{Var}X \leq \leq 2\mathbf{M}\left(X\right)$, имеет вид

$$\mathbf{P}\left(|X - \mathbf{M}\left(X\right)| > k\sqrt{2\mathbf{M}\left(X\right)}\right) \leq 1/k^2.$$

В качестве k возьмем $\frac{\sqrt{\mathbf{M}(X)}}{2\sqrt{2}}$ и, пользуясь тем, что $\mathsf{Var}X < 2\mathbf{M}(X), \mathbf{M}(X) = n^{2\alpha-1}$, получим

$$\mathbf{P}(|X - \mathbf{M}(X)| > 0.5\mathbf{M}(X)) \leq 8/\mathbf{M}(X) = o(1),$$

откуда $\mathbf{P}\left(X > n^{2\alpha-1}/2\right) = o(1)$. □

Используя доказанные леммы, докажем теорему, отвечающую на поставленный в начале параграфа вопрос.

Теорема 3.4 Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – случайный автомат такой, что $|Q| = n$, $|\Sigma| > n^{1/2+\epsilon}$ для некоторой константы $\epsilon > 0$. Тогда $\mathscr{A}$ синхронизируем с высокой вероятностью. Более того, длина кратчайшего синхронизирующего слова этого автомата с высокой вероятностью не превышает $n(n-1)/2$.

Доказательство. Пусть α – действительное число, удовлетворяющее условию $0.5 < \alpha < \min(2/3, 0.5 + \varepsilon)$. Обозначим через $\Sigma_1 \subseteq \Sigma$, $\Sigma_2 \subseteq \Sigma$ такие множества букв, для которых $|\Sigma_1| = |\Sigma_2| = n^\alpha$, $\Sigma_1 \cap \Sigma_2 = \varnothing$. Пусть $T \subseteq \mathbf{T}$ – множество всех троек вида $(a, b, x), a \in \Sigma_1, b \in \Sigma_2, x \in Q$ таких, что $xa = xb = x$. По лемме 3.12, в множестве L с высокой вероятностью более $n^{2\alpha-1}/2$ элементов. Для каждой тройки $(a, b, x) \in T$ по лемме 3.11 вероятность события $\mathscr{S}(a, b, x)$ =“для каждого состояния $q \in Q$ существует слово $w_{q\to x} \in \{a, b\}^*$, удовлетворяющее $w_{q\to x}q = x$” больше некоторой константы r. Следовательно, матождание случайной величины

$$Z = |\{(a, b, x) \mid \mathscr{S}(a, b, x), (a, b, x) \in T\}|$$

больше или равно $r'n^{2\alpha-1}$, где $r' = 0,5r$. Для того чтобы применить неравенство Чебышева и показать, что с высокой вероятностью $Z > 0$, нужно доказать, что события $\mathscr{S}(a, b, x)$ попарно независимы для троек $(a, b, x) \in T$. Чтобы доказать это, мы покажем, что с высокой вероятностью для любой пары троек $(a_1, b_1, x_1) \in T$, $(a_2, b_2, x_2) \in T$ выполняется

$$a_1 \neq a_2,\ b_1 \neq b_2.$$

Заметим, что $a_i \neq b_j$, поскольку $\Sigma_1 \cap \Sigma_2 = \varnothing$.

Вычислим вероятность того, что существуют различные тройки (a_1, b_1, x_1), (a_2, b_2, x_2) такие, что утверждение $a_1 \neq a_2$, $b_1 \neq b_2$ не выполняется, при этом выполняется $(a_1, b_1, x_1) \in T$, $(a_2, b_2, x_2) \in T$, т. е.

$$x_1a_1 = x_1,\ x_1b_1 = x_1,\ x_2a_2 = x_2,\ x_2b_2 = x_2. \tag{3.6}$$

Если различные тройки (a_1, b_1, x_1), (a_2, b_2, x_2) не удовлетворяют условию $a_1 \neq a_2$, $b_1 \neq b_2$, они должны удовлетворять одному из следующих условий:

1. $x_1 = x_2$, $a_1 = a_2$, $b_1 \neq b_2$,
2. $x_1 = x_2$, $a_1 \neq a_2$, $b_1 = b_2$,
3. $x_1 \neq x_2$, $a_1 = a_2$, $b_1 \neq b_2$,
4. $x_1 \neq x_2$, $a_1 \neq a_2$, $b_1 = b_2$,
5. $x_1 \neq x_2$, $a_1 = a_2$, $b_1 = b_2$.

Для каждого условия C из этого списка вычислим вероятность события "существуют тройки $(a_1, b_1, x_1), (a_2, b_2, x_2)$, которые удовлетворяют условию C и уравнению (3.6)".

Для выбора тройки, удовлетворяющей условию 1, нужно установить значения x_1, a_1, b_1 и b_2, это можно сделать $n \cdot n^{\alpha} \cdot (n^{2\alpha} - 1)/2 \leq n \cdot n^{3\alpha}$ способами, соответственно, столько пар троек удовлетворяет условию 1. Для этих пар троек уравнение (3.6) принимает вид

$$x_1 a_1 = x_1 \wedge x_1 b_1 = x_1 \wedge x_1 b_2 = x_1,$$

вероятность его выполнения равна n^{-3}. Таким образом, вероятность того, что существует пара троек, удовлетворяющая условию 1 и уравнению (3.6), может быть ограничена сверху следующим значением

$$n n^{3\alpha} \times n^{-3} = n^{3\alpha-2} \underset{n\to\infty}{\longrightarrow} 0.$$

Аналогичным образом для условий $2, \ldots, 5$ получаются оценки $n n^{3\alpha} \times$ $\times n^{-3}$, $n^2 n^{3\alpha} \times n^{-4}$, $n^2 n^{3\alpha} \times n^{-4}$, $n^2 n^{2\alpha} \times n^{-4}$, соответственно. Нетрудно видеть, что все они стремятся к нулю при n, идущем к бесконечности. Таким образом, с высокой вероятностью для любой пары различных троек $(a_1, b_1, x_1) \in T$, $(a_2, b_2, x_2) \in T$ получим $a_1 \neq a_2$, $b_1 \neq b_2$.

Мы доказали, что с высокой вероятностью $|T| > n^{2\alpha-1}/2$ и для любых $(a_1, b_1, x_1) \in T, (a_2, b_2, x_2) \in T$ выполняются неравенства $a_1 \neq a_2$, $b_1 \neq$ $\neq b_2$. Матожидание для Z не меньше $r' n^{2\alpha-1}$, и Z представляет собой сумму попарно независимых случайных величин

$$I_{\mathscr{S}(a,b,x)} = \begin{cases} 1, \mathscr{S}(a, b, x) \text{выполняется}, \\ 0, \text{в противном случае.} \end{cases} \tag{3.7}$$

Аналогично лемме 3.12 применяем неравенство Чебышева и получаем, что с высокой вероятностью $Z > r'n^{2\alpha-1}/2$. Значит, с высокой вероятностью $Z > 0$ и существует тройка $(a, b, x) \in T$ такая, что для любого состояния q найдется слово $w_{q\to x} \in \{a, b\}^*$, удовлетворяющее $w_{q\to x}q = x$. Поскольку $(a, b, x) \in T$ и $w_{q\to x} \in \{a, b\}$, значит, $xw = x$.

Заметим, что получившийся автомат представляет собой автомат с нулем, соответственно, длина синхронизирующего его слова не превышает $n(n-1)/2 < (n-1)^2$ (см. например, [54]). □

Доказанная теорема отвечает на поставленный вопрос, но оставляет открытым вопрос верхней оценки длины кратчайшего синхронизирующего слова для случайного автомата. Мы полагаем, что такая оценка должна быть сублинейной.

Доказательство теоремы (а точнее, леммы 3.11) представляет самостоятельный интерес. Обсудим его отдельно.

Во-первых, при доказательстве используется теорема Вормальда. Это, по-видимому, первое использование данной теоремы в теории конечных автоматов. Изначально этот метод был разработан для анализа алгоритмов на случайных графах [66] и позднее был использован для доказательства эффективности алгоритмов решения задачи случайной выполнимости [11]. Как правило, система дифференциальных уравнений, получаемая при использовании теоремы, решается только численными методами. В нашем случае система решена аналитически.

Во-вторых, заметим, что ни от одного этапа доказательства леммы 3.11 нельзя отказаться, расширив границы других этапов. Теорема Вормальда не может использоваться на всем отрезке $[0, n]$, поскольку на его границах не выполняются условия теоремы Вормальда. На правой границе отрезка не определены правые части дифференциальных уравнений, знаменатель обращается в ноль. Отступая от левого края, мы исключаем решение $q_1 = 0$, т. е. гарантируем, что процесс не завершится неуспехом в самом начале (оставшееся решение гарантирует, что процесс не завершится неуспехом на всем отрезке). Заметим, что ранее при применении теоремы Вормальда такой проблемы не было, поскольку она применялась к процессам, которые не могли “умереть”, не доработав до конца. При доказательстве с использованием процесса Гальтона-Ватсона существен-

но, что рассматриваются только первые шаги процесса, это обеспечивает высокое матожидание количества потомков и саму возможность применения теоремы 3.1. Утверждение третьего этапа верно только тогда, когда относительно немного состояний, не более $n/e \approx 0,37n$, остались непросмотренными.

Кроме того, в процессе получения оценки нами также доказан побочный результат, касающийся задачи заражения инфекцией, которая распространяется по дугам ориентированного графа, соответствующего двум случайным отображениям, в обратном направлении. Задача распространения эпидемии по дугам орграфа, соответствующего одному случайному отображению, сформулирована и первично изучена Гертбахом [**32**], а в дальнейшем исследована Яворским [**38**]. Мы показали, что в орграфе с дугами, соответствующими двум случайным отображениям, если одна особь заражена, то вся популяция будет заражена с конечной вероятностью.

3.4 Случайные автоматы, синхронизируемые с конечной вероятностью

В результатах предыдущих параграфов размер входного алфавита рос вместе с числом его состояний. Для анализа синхронизируемости автоматом над входным алфавитом из константного числа букв несколько ослабим входные условия и поставим следующий вопрос:

— Какой размер входного алфавита достаточен, чтобы автомат над алфавитом этого размера был синхронизируем с конечной вероятностью?

Пусть p, q – пара состояний случайного автомата $\mathscr{A} = (Q, \Sigma, \delta)$. Определим для этой пары состояний процесс Roomba, цель которого – найти слово $w = a_1 \cdots a_k$ такое, что $pw = qw$.

На первом шаге процесса мы случайным образом выбираем букву $a_1 \in \Sigma$ и совершаем переход из $p_0 = p$ в $p_1 = p_0 a_1$ и из $q_0 = q$ в $q_1 = q_0 a_1$. Если $p_1 = q_1$, то процесс успешно завершается построением слова $w = a_1$, иначе он продолжается.

На m-м шаге процесса мы оказываемся в состояниях p_{m-1} и q_{m-1}. (Не исключено, что какое-то из них или их оба мы уже посещали на предыдущих шагах процесса.) Выбираем букву a_m, которая ранее не при-

менялась для переходов из состояния p_{m-1} или из состояния q_{m-1}. Если мы смогли выбрать такую букву, то переходим с ее помощью из состояний p_{m-1}, q_{m-1} в состояния $p_m = p_{m-1}a_m$, $q_m = q_{m-1}a$ соответственно, аналогично первому шагу. Назовем этот переход *ключевым переходом* процесса. Если $p_m = q_m$, то процесс завершается построением слова $w = a_1 a_2 \dots a_m$, иначе он продолжается.

Если мы не можем выбрать букву (это означает, что к каждому из состояний p_{m-1}, q_{m-1} мы уже применили все имеющиеся буквы алфавита), то действуем следующим образом. Запускаем поиск в ширину состояния, из которого не применена хотя бы одна буква алфавита, одновременно из состояний p_{m-1} и q_{m-1}. Если поиск не находит такого состояния, то процесс заканчивается неуспехом. В противном случае мы находим состояние, достижимое, допустим, из состояния p_{m-1} по слову $z \in \Sigma^*$. Перейдем из p_{m-1} и q_{m-1} в $p_m = p_{m-1}z$ и $q_m = q_{m-1}z$ и продолжим процесс. Назовем эту часть процесса *поиском слова* z.

Отметим, что процесс Roomba схож с процессом Vacuum, описанным в 3.2, в них различается только принцип определения буквы или слова для следующего хода. Формальное описание процесса Roomba приведено на рис. 3.4.

Отметим ряд полезных свойств описанного процесса, совершаемого с автоматом над двухбуквенным алфавитом.

Предложение 3.1 Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ – случайный автомат такой, что $|Q| = n$ и $|\Sigma| = 2$. Тогда процесс Roomba, начав с любой пары состояний $p, q \in Q$, завершается построением слова w после ключевого перехода с вероятностью $1/n$.

Доказательство. По определению ключевого перехода мы совершаем его по букве a_i, которая ранее не использовалась из состояния p_{i-1} или из состояния q_{i-1}, допустим, из p_{i-1}. Значит, мы выбираем состояние p_i случайно из Q и оно совпадет с некоторым состоянием q_i с вероятностью $1/n$. □

Предложение 3.2 Существует константа $c_1 > 0$ такая, что для произвольного случайного автомата $\mathscr{A} = (Q, \Sigma, \delta)$ с $|Q| = n$ и $|\Sigma| = 2$ процесс Roomba, начав с любой пары состояний $p, q \in Q$, пройдет через ключевой переход по крайней мере $c_1 n$ раз с высокой вероятностью, если не

Вход: Случайный автомат $\mathscr{A} = (Q, \Sigma, \delta)$ и пара состояний $p \in Q, q \in Q$
Выход: ***неуспех*** или слово $w = a_1 \dots a_k$ такое, что $pw = qw$
Описание процесса:

пусть $\Delta_r \subseteq \Sigma$, $w \in \Sigma^*$
Установить $\Delta_r = \varnothing$ для всех $r \in Q$, $w = \varepsilon$
пока $pw \neq qw$
  если $\Delta_{pw} \cap \Delta_{qw} \neq \Sigma$, **то** *ключевой переход*
    Выбрать $a \in \Sigma \setminus (\Delta_{pw} \cap \Delta_{qw})$
    Установить $\Delta_{pw} = \Delta_{pw} \cup \{a\}$, $\Delta_{qw} = \Delta_{qw} \cup \{a\}$
    Установить $w = wa$
  иначе
    поиск слова z
    Установить $w = wz$
Вернуть w

Рис. 3.4: Процесс Roomba

завершится построением слова w ранее.

Доказательство. Сначала покажем, что произвольное множество состояний из Q, размером существенно меньшее чем n/e, с высокой вероятностью имеет исходящую стрелку. Для фиксированного множества состояний размера m, где $m < n/e$, вероятность того, что из него не выходит ни одной стрелки, равна $(m/n)^{2m}$. Всего таких множеств размера m имеется $\binom{n}{m} \leq \left(\frac{ne}{m}\right)^m$. Из неравенства Буля получаем, что вероятность того, что существует множество размера m без исходящих стрелок, меньше

$$\left(\frac{m}{n}\right)^{2m} \left(\frac{ne}{m}\right)^m = \left(\frac{me}{n}\right)^m \underset{n\to\infty}{\longrightarrow} 0.$$

Суммируя по всем таким m, получим, что с высокой вероятностью все множества размера менее $c_1 n$ для некоторой константы c_1 с $0 < c_1 < 1/e$ имеют исходящую стрелку. Откуда легко выводится утверждение, что с высокой вероятностью из любого состояния $r \in Q$ достижимо не менее $c_1 n$ состояний. При этом константа c_1 не зависит ни от вида автомата, ни от числа его состояний.

Таким образом, поиск в ширину слова z на некотором шаге процесса

ROOMBA сделает по крайней мере $c_1 n$ шагов, если успешно не завершится ранее. В силу конечности всех объектов, для процесса в целом есть две возможности: сделать в какой-то момент указанное число шагов поиска и построить слово w ранее.

Заметим, что по определению поиска на путях из p_{m-1} и q_{m-1}, помеченных словом z, встречаются только те стрелки, которые были использованы нами ранее. Тот факт, что мы встречаем незнакомую стрелку, означает, что мы могли завершить поиск с более коротким словом z. Таким образом, мы используем стрелку в первый раз только при ключевом переходе.

Тот факт, что поиск из некоторого p_j сделал $c_1 n$ шагов, означает, что в автомате есть $2c_1 n$ уже просмотренных стрелок. Все эти стрелки были когда-то использованы в первый раз, т. е. ключевой переход был произведен по меньшей мере $c_1 n$ раз. □

Установленные свойства позволяют доказать следующую лемму.

Лемма 3.13 Существуют константы $p_0 > 0$ и $c_0 > 0$ такие, что для любого натурального числа n и любого случайного автомата $\mathscr{A} = (Q, \Sigma, \delta)$ такого, что $|Q| = n$ и $\Sigma = \{a, b\}$, вероятность события

$$\frac{|\{(p, q) \in Q^2 \mid \exists w\ pw = qw\}|}{n^2} > c_0$$

превышает p_0. Иными словами, конечная доля пар состояний в случайном автомате синхронизируема с конечной вероятностью.

Доказательство. Возьмем пару состояний $(p, q) \in Q \times Q$ и попробуем синхронизировать ее с помощью процесса ROOMBA. Согласно предложению 3.2, ключевой переход будет произведен не менее $c_1 n$ раз для некоторой константы c_1, если процесс не завершится успехом ранее. В соответствии с предложением 3.1, при каждом ключевом переходе синхронизация произойдет с вероятностью $1/n$. Ключевые переходы независимы, так что используя неравенство Буля по всем ключевым переходам, мы получим, что пара состояний синхронизируема с вероятностью, ограниченной снизу некоторой константой c_2.

Следовательно, математическое ожидание случайной величины

$$|\{(p, q) \in Q \times Q \mid \exists w\ pw = qw\}|$$

больше $c_2 n^2$. Применение леммы 3.4 к случайной величине

$$\chi = \frac{|\{(p, q) \in Q \times Q \mid \exists w \; pw = qw\}|}{n^2}$$

завершает доказательство. □

Таким образом, мы доказали все необходимые вспомогательные утверждения и готовы к формулировке и доказательству основного результата параграфа.

Теорема 3.5 Существует константа $p_0 > 0$ такая, что для любого n случайный автомат $\mathscr{A} = (Q, \Sigma, \delta)$ с $|Q| = n, |\Sigma| = 4$ синхронизируем с вероятностью больше p_0.

Доказательство. Пусть $\Sigma = \{a, b, d, f\}$. По лемме 3.13, с конечной вероятностью p_0 существует подмножество $T \subset Q \times Q$ такое, что $|T| > c_0 n^2$ и любая пара состояний из T синхронизируема некоторым словом w_1 над алфавитом $\{a, b\}$. Покажем, что для любой пары состояний, не принадлежащей T, существует путь из нее в пару состояний из T.

Рассмотрим произвольную пару состояний $p, q \in Q \setminus T$. Воспользовавшись фактом, полученным при доказательстве предложения 3.2, получим, что из состояния p достижимо с помощью слов над алфавитом $\{d, f\}$ не менее $c_3 n$ состояний для некоторой константы c_3. Обойдем эти состояния поиском в ширину, параллельно выполняя те же переходы из состояния q. В результате, получим $c_3 n$ пар состояний, среди которых не менее $\frac{c_3 n}{2}$ различных. Вероятность того, что множество из $\frac{c_3 n}{2}$ случайных пар не пересекается с T, ограничено сверху выражением $(1-c_0)^{c_3 n/2}$, которое стремится к 0 при $n \to \infty$. Обозначим через w_2 слово над алфавитом $\{d, f\}$, помечающее путь из p, q в пару из T.

Применив неравенство Буля по всем парам состояний, получаем, что с конечной вероятностью каждая пара состояний автомата будет синхронизирована по слову w_1, либо по слову $w_2 w_1$. В соответствии с леммой 0.1, если любая пара состояний автомата может быть синхронизирована, то и автомат в целом синхронизируем. □

Вычислительные эксперименты показывают, что верно и более сильное утверждение – автомат над четырехбуквенным (и даже двухбуквенным) алфавитом синхронизируем с высокой вероятностью. Однако доказанный нами результат можно считать этапом доказательства высокой

вероятности. Например, в [**30**] доказательство строится по следующему принципу: доказывается конечная вероятность, а потом высокая выводится из конечной.

Литература

[1] Ананичев Д. С. *Порог аннуляции для частично монотонных автоматов* // Известия вузов. Математика. – 2010. – №1. – С. 3–13.

[2] Барздинь Я. М., Коршунов А. Д. *О диаметре приведенных автоматов* // Дискретный анализ. Сб. трудов Института математики СО АН СССР. – 1967. – Вып. 9. – С. 3–45.

[3] Карацуба А. А. *Решение одной задачи из теории конечных автоматов* // Успехи математических наук. – 1960. – Вып. 15:3(93). – С. 157–159.

[4] Кормен Т., Лейзерсон С., Ривест Р., Штайн К. *Алгоритмы: построение и анализ*, 2-е издание. – М:Вильямс. – 2011.

[5] Коршунов А. Д. *О степени различимости автоматов* // Дискретный анализ. Сб. трудов Института математики СО АН СССР. – 1967. – Вып. 10. – С. 39–59.

[6] Коршунов А. Д. *О верхней оценке длин кратчайших однородных экспериментов по распознаванию заключительного состояния для почти всех автоматов* // Доклады АН СССР. – 1969. – Т. 184.– №1. – С. 28–29.

[7] Коршунов А. Д. *О перечислении конечных автоматов* // Проблемы кибернетики. – 1978. – Т. 34. – С. 5–82.

[8] Мартюгин П. В. *Задачи,связанные с синхронизацией конечных автоматов*: диссертация на соискание ученой степени кандидата физ.-мат. наук. – Екатеринбург, 2008. – 173 с.

[9] Прибавкина Е.В. *Медленно синхронизируемые автоматы с нулем и непокрывающие множества* // Матем. заметки. – 2011. – Т. 90 – №3. – С. 422–430.

[10] Сперанский Д.В. *Установочные и диагностические последовательности для линейных автоматов* // Автомат. и телемех. – 1997. – №5. – С. 133–141.

[11] Achlioptas D. *Lower bounds for random 3-SAT via differential equations* // Theoret. Comput. Sci. – 2001. – V. 265. – P. 159–185.

[12] Ananichev D. S. *The mortality threshold for partially monotonic automata* // Developments in Language Theory, Lect. Notes Comput.

Sci. – 2005. – V. 3572. – P. 112–121.

[13] Ananichev D. S., Gusev V. V., Volkov M. V. *Slowly synchronizing automata and digraphs* // Mathematical Foundations of Computer Science, Lect. Notes Comput. Sci. – 2010. – V. 6281. – P. 55–64.

[14] Ananichev D. S., Volkov M. V *Some results on Černý type problems for transformation semigroups* // Semigroups and Languages, World Scientific, Singapore. – 2004. – P. 23–42.

[15] Ananichev D. S., Volkov M. V. *Synchronizing generalized monotonic automata* // Theoret. Comput. Sci. – 2005. – V. 330. – P. 3–13.

[16] Asmussen S., Hering H. *Branching processes* – Birkhäuser, Boston. – 1983.

[17] Athreya K. B., Ney P. E. *Branching processes* – Springer-Verlag, Berlin; Heidelberg; New York. – 1972.

[18] Auger A., Doerr B. (eds.) *Theory of randomized search heuristics* – World Scientific, Singapore. – 2011.

[19] Béal M., Berlinkov M., Perrin D. *A quadratic upper bound on the size of a synchronizing word in one-cluster automata* // Int. J. of Found. of Comput. Sci. – 2011. – V. 22. – P. 277–288.

[20] Berlinkov M. *Approximating the minimum length of synchronizing words is hard* // 5th Int. Computer Science Symposium in Russia, CSR 2010, Kazan, Russia. Lect. Notes Comput. Sci. – 2010. – V. 6072. – P. 37–47.

[21] Biskup M.T., Plandowski W. *Shortest synchronizing strings for Huffman codes* // Theoret. Comput. Sci. – 2009. – V. 410. – №38–40. – P. 3925–3941.

[22] Cameron P. *Dixon's theorem and probability of synchronization* [Электронный ресурс] / http://caul.cii.fc.ul.pt/GSConf2011/Slides/cameron.pdf

[23] Capocelli R. M., Gargano L., Vaccaro U. *On the characterization of statistically synchronizable variable-length codes* // IEEE Transactions on Information Theory. – 1988. – V. 34(4). – P. 817—825.

[24] Černý J. *Poznámka k homogénnym eksperimentom s konečnými automatami* // Mat.-Fyz. Čas. Slovensk. Akad. Vied. – 1964. – V. 14. – P. 208–216.

[25] Chmiel K., Roman A. *COMPAS: a computing package for synchronization* // Impementation and aplication of automata, Lect.

Notes in Comput. Sci. – 2011. – V. 6482. – P. 79–86.

[26] Dubuc L. *Sur les automates circulaires eta la conjecture de Černý* // RAIRO Theoret. Inform. and Appl. – 1998. – V. 32. – P. 21–34.

[27] Eppstein D. *Reset sequences for monotonic automata* // SIAM J. Comput. – 1990. – V. 19. – P. 500–510.

[28] Fogg N. P. *Substitutions in dynamics, arithmetics and combinatorics* – V. 1794: Lect. Notes in Math. – 2002.

[29] Frankl P. *An extremal problem for two families of sets* // Eur. J. Comb. – 1982. – V. 3. – P. 125–127.

[30] Friedgut E. (appendix by Bourgain J.) *Sharp thresholds of graph properties, and the* k*-SAT problem* // J. Amer. Math. Soc. – 1999. – V. 12. – P. 1017–1054.

[31] Gawrychowski P. *Complexity of shortest synchronizing word* – Unpublished note, – 2008.

[32] Gertbakh B. *Epidemic process on a random graph: some preliminary results* // J. Appl. Prob. – 1977. – V. 14. – P. 427–438.

[33] Ginsburg S. *On the length of the smallest uniform experiment which distinguishes the terminal states of a machine* // J. Assoc. Comput. Mach. – 1958. – V. 5. – P. 266–280.

[34] Gusev V. V. *Lower Bounds for the Length of Reset Words in Eulerian Automata* // Reachibility problems, Lecture Notes in Comput. Sci. – 2011. V. 6945. – P. 180–190.

[35] Hibbard T.N. *Least upper bounds on minimal terminal state experiments for two classes of sequential machines* // J. Assoc. Comput. Math. – 1961. – V. 8. – №4 – P. 601–612.

[36] Higgins P. *The range order of a product of* i *transformations from a finite full transformation semigroup* // Semigroup Forum. – 1988. – V. 37. – P. 31–36.

[37] Higgins P. *Techniques of semigroup theory* – Oxford University Press; Oxford; New York; Tokyo, 1992.

[38] Jaworski J. *Epidemic processes on digraphs of random mappings* // J. Appl. Probab. – 1999. – V. 36. – P. 780–798.

[39] Kari J. *A counter example to a conjecture concerning synchronizing words in finite automata* // Bull. European Assoc. Theoret. Comput. Sci. – 2001.

– V. 73:146. – P. 18.

[40] Kari J. *Synchronizing finite automata on eulerian digraphs* // Theoret. Comput. Sci. – 2003. – V. 295. – P. 223–232.

[41] Kisielewicz A., Kowalski J., Szykula M. *Fast algorithm finding the shortest reset words* [Электронная публикация] // http://arxiv.org/pdf/1203.2822.pdf

[42] Martjugin P. V. *A series of slowly synchronizing automata with a zero state over a small alphabet* // Inform. and Comput. – 2008. – V. 206. – P. 1197–1203.

[43] Mateescu A., Salomaa A. *Many-valued truth functions, Černý's conjecture and road coloring* // EATCS Bull. – 1999. – V. 68. – P. 134–150.

[44] Moore E. *Gedanken-experiments with sequential machines* // Automata Studies, Ann. Math. Studies, Princeton Univ. Press, Princeton, N.J. – 1956. – V. 34. – P. 129–153. (имеется русский перевод: Мур Э. *Умозрительные эксперименты с последовательными машинами* // Сб. "Автоматы". – М.:ИЛ. – 1956. – С. 179–210.)

[45] Natarajan B. K. *Some paradigms for the automated design of parts feeders* // Int. J. of Robotics Research. – 1989. – V. 8. – №6. – P. 89–109.

[46] Olschewski J., Ummels M. *The complexity of finding reset words in finite automata* // Mathematical Foundations of Computer Science, Lecture Notes in Comput. Sci. – 2010. – V. 6281. – P. 568–579.

[47] Papadimitriou C. H., Yannakakis M. *The complexity of facets (and some facets of complexity)* // J. Comput. System Sci. – 1984. – V. 28(2). – P. 244–259.

[48] Pin J.-E. *Le probléme de la synchronisation et la conjecture de Černý* // Non-commutative Structures in Algebra and Geometric Combinatorics [Quaderni de la Ricerca Scientifica 109], CNR, Roma. – 1981. – P. 37–48.

[49] Pin J.-E. *On two combinatorial problems arising from automata theory* // Ann. Discrete Math. – 1983. – V. 17. – P. 535–548.

[50] Rabin M. O., Scott D. *Finite automata and their decision problems* // IBM J. Res. Develop. – 1959. – V. 918. – №3(2). – P.114–125.

[51] Roman A. *Synchronization of finite automaton. Computations for different alphabet sizes* [Электронная публикация] // Proc. WoWA'06, Saint-Petersburg. – 2006.

[52] Roman A. *A note on Černý Conjecture for automata over 3-letter alphabet* // J. Automata, Languages and Combinatorics. – 2008. – V. 13. – №2. – P. 141–143.

[53] Roman A. *Genetic algorithm for synchronization* // Languages and Automata: Theory and Applications. LATA 2009, Lect. Notes Comp. Sci. – 2009. – V. 5457. – P. 684–695.

[54] Rystsov I. K. *Reset words for commutative and solvable automata* // Theoret. Comput. Sci. – 1997. – V. 172. – P. 273–279.

[55] Samotij W. *A note on the complexity of the problem of finding shortest synchronizing words* [Электронная публикация] // Proc. Int. Conf. AutoMathA'07, Palermo. – 2007.

[56] Sandberg S. *Homing and synchronizing sequences* // Model-Based Testing of Reactive Systems, Lect. Notes Comput. Sci. – 2005. – V. 3472. – P. 5–33.

[57] Skvortsov E., Tipikin E. *Experimental study of the shortest reset word of random automata* // Implementation and Application of Automata, Lect. Notes Comput. Sci. – 2011. – V. 6807. – P. 290–298.

[58] Steinberg B. *Cerny's conjecture and group representation theory* // J. Algebraic Combinatorics: An International Journal. – 2010. – V. 31. – №1. – P. 83–109.

[59] Steinberg B. *The averaging trick and the Černý conjecture* // Int. J. of Foundations of Comp. Sci. – 2011. – V. 22. – №7. – P. 1697–1706.

[60] Steinberg B. *The Černý conjecture for one-cluster automata with prime length cycle* // Theoret. Comput. Sci. – 2011. – V. 412(39). – P. 5487–5491.

[61] Trahtman A. *An efficient algorithm finds noticeable trends and examples concerning the Černý conjecture* // 31st Int. Symp. Math. Foundations of Comput. Sci., Lect. Notes in Comput. Sci. – 2006. – V. 4162. – P. 789–800.

[62] Trahtman A. *The Černý conjecture for aperiodic automata* // Discrete Math. Theoret. Comput. Sci. – 2007. – V.9. – №2. – P. 3–10.

[63] Trahtman A. *Modifying the upper bound on the length of minimal synchronizing word* // Fundamentals of Computation Theory, Lect. Notes Comput. Sci. – 2011. – V. 6914. – P. 173–180.

[64] Volkov M. V. *Synchronizing automata preserving a chain of partial orders*

// Implementation and Application of Automata. Proc. 12th Int. Conf. CIAA 2007, Lect. Notes Comput. Sci. – 2007. – V.4783. – P.27–37.

[65] Volkov M. V. *Synchronizing automata and the Černý conjecture* // Languages and Automata: Theory and Applications. LATA 2008, Lect. Notes Comput. Sci. – 2008. – V. 5196. – P. 11–27.

[66] Wormald N. C. *Differential equations for random processes and random graphs* // Ann. Appl. Probab. – 1995. – V. 5(4). – P. 1217–1235.

Работы автора по теме диссертации

[67] Ananichev D. S., Volkov M. V., Zaks Yu.I. *Synchronizing automata with a letter of deficiency 2* // Developments in Language Theory, Lect. Notes Comput. Sci. – 2006. – V. 4036. – P. 433–442.

[68] Ananichev D. S., Volkov M. V., Zaks Yu.I. *Synchronizing automata with a letter of deficiency 2* // Theoret. Comput. Sci. – 2007. – V. 376. – P. 30–41.

[69] Skvortsov E., Zaks Yu. *Synchronizing random automata* // AutoMathA'09, Proceedings; Liege. – 2009. – P. [39–46].

[70] Skvortsov E., Zaks Yu. *Synchronizing random automata* // Discr. Math. Theoret. Comput. Sci. – 2010. – V. 12:4. – P. 95–108.

[71] Skvortsov E., Zaks Yu. *Synchronizing random automata on 4-letter alphabet* // First Russian-Finnish Symposium on Discrete Mathematics, Abstracts. – 2011. – P. 62–63.

[72] Закс Ю. И. *Синхронизация конечных автоматов с буквой большого дефекта* – Гуманитарный ун-т. – Екатеринбург, 2012. – Деп. в ВИНИТИ 17.04.2012, №154-В2012.