САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

Первышев Константин Вячеславович

ИЕРАРХИИ ПО ВРЕМЕНИ ДЛЯ НЕКОТОРЫХ КЛАССОВ ЭВРИСТИК, АЛГОРИТМОВ С ПОДСКАЗКОЙ, КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ

05.13.17 — Теоретические основы информатики

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата физико-математических наук

Санкт-Петербург — 2008

Работа выполнена на кафедре информатики математико-механического факультета Санкт-Петербургского государственного университета

Научный руководитель: доцент, кандидат физ.-мат. наук
Гирш Эдуард Алексеевич

Официальные оппоненты: академик, доктор физ.-мат. наук
Матиясевич Юрий Владимирович
(ПОМИ РАН)

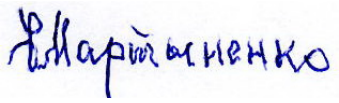
профессор, доктор физ.-мат. наук
Верещагин Николай Константинович
(механико-математический факультет МГУ)

Ведущая организация: Математический институт им. В.А. Стеклова
Российской академии наук

Защита состоится “26” февраля 2009 года в 15 часов 30 минут на заседании совета Д 212.232.51 по защите докторских и кандидатских диссертаций при Санкт-Петербургском государственном университете по адресу: 198504, Санкт-Петербург, Старый Петергоф, Университетский пр. 28, ауд. 405.

С диссертацией можно ознакомиться в Научной библиотеке им. М. Горького Санкт-Петербургского государственного университета по адресу: 199034, Санкт-Петербург, Университетская наб. 7/9.

Автореферат разослан “ ” января 2009 года.

Ученый секретарь
диссертационного совета,
доктор физ.-мат. наук  Мартыненко Б. К.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Вопрос о том, дает ли большее количество вычислительных ресурсов возможность решать более трудные задачи, способствовал развитию теоретической информатики в начале 60-х годов. В одной из самых первых работ по вычислительной теории сложности Ю. Хартманис и Р. Стирнс [1] доказали существование иерархии по времени для детерминированных алгоритмов: имеется некоторый язык, который может быть распознан неким детерминированным алгоритмом за время $O(n^{k+\epsilon})$, но не может быть распознан никаким детерминированным алгоритмом за меньшее время $O(n^k)$. Иными словами, чуть большее количество времени позволяет решить некоторую более сложную задачу.

За детерминированными алгоритмами настал черед других вычислительных моделей. Так, в начале 70-х годов С. Кук [2] первым показал, что иерархия по времени существует и для недетерминированных алгоритмов. В последующей статье Дж. Сейферас, М. Фишер и А. Мейер [3] предложили альтернативное доказательство этой иерархии. Однако, классической стала работа [4], в которой С. Жак изобрел технику *отложенной диагонализации*.

Техника отложенной диагонализации позволяет доказать иерархию по времени для практически любой *синтаксической модели* вычислений. Такие модели, в отличие от семантических моделей вычислений, не предъявляют никаких специальных требований к машинам (к примеру, ограниченности вероятности ошибки). Примером синтаксических моделей вычислений как раз и являются детерминированные и недетерминированные алгоритмы.

Вопрос о существовании иерархии по времени в *семантических моделях* остается открытым до сих пор. Так, различные типы вероятностных алгоритмов составляют именно семантические модели. Самыми распространенными типами вероятностных алгоритмов являются вероятностные алгоритмы с ограниченной двусторонней ошибкой, с ограниченной односторонней ошибкой, без ошибки. Ни для одного из этих типов вероятностных алгоритмов существование иерархии по времени не доказано.

В последних исследованиях предметом рассмотрения стали алгоритмы с подсказкой, которые являются промежуточным вариантом между машинами Тьюринга и вычислительными схемами. В серии работ [5, 6, 7], авторами которых являются Б. Барак, Л. Фортноу, Р. Сантанам и Л. Тревисан, был получен следующий интересный результат. Иерархии по времени существуют для вероятностных алгоритмов с ограниченной двусто-

ронней ошибкой и *одним битом подсказки*. Напомним, что существование иерархии для подобных алгоритмов без подсказки является открытым вопросом. Также, было показано существование иерархии для вероятностных алгоритмов с односторонней ошибкой и одним битом подсказки. Последняя из этих статей ([7]) в качестве открытого вопроса указывает существование иерархии для алгоритмов с одним битом подсказки в других семантических моделях.

Фокус самых последних исследований, касающихся иерархий по времени, сместился с "классических" алгоритмов, которые обязаны правильно решать задачу на каждом из возможных входов, к алгоритмам эвристическим. Так, Л. Фортноу и Р. Сантанам [6] показали наличие иерархии по времени для вероятностных *эвристических* алгоритмов с двусторонней ошибкой (эвристики - эта такие алгоритмы, которые могут неверно обрабатывать некоторые входы). Подобный результат верен и для квантового аналога указанного класса эвристик. Недавний обзор тех же авторов [8] в качестве открытого оставляет вопрос о существовании иерархий для эвристик из других вычислительных моделей.

Цели работы.

1. Получить ответ на вопрос о существовании иерархий по времени для эвристических алгоритмов (без подсказки) в различных семантических, а также синтаксических моделях вычислений, для которых подобные иерархии еще не доказаны.

   В частности, интересным было бы доказать иерархию по времени для эвристик из модели недетерминированных алгоритмов, являющейся синтаксической, а также для эвристик из некоторых семантических моделей.

2. Получить ответ на вопрос о существовании иерархий по времени для алгоритмов с одним битом подсказки в различных семантических классах, для которых подобные иерархии еще не доказаны.

   В частности, интересным было бы доказать иерархию для вероятностных алгоритмов с одним битом подсказки, которые не допускают ошибок. Особенно интересным было бы доказать, что иерархия существует для любых моделей вычислений с одним битом подсказки.

3. Исследовать наличие иерархий по времени для вычислительных задач, возникающих в криптографии. В частности, было бы интересно

исследовать существование иерархии легко вычислимых функций по времени их обращения.

Общая методика работы. В работе используются методы, традиционные для теоретической информатики. Доказан ряд теорем о существовании иерархий по времени. Часть доказательств основана на методе диагонализации, применяемом к вычислительным задачам. Вариант этого метода был усовершенствован в ходе работы над диссертацией. Методы теории вычислительной сложности применены к исследованию надежности основных криптографических примитивов. В качестве основной модели вычислений используется многоленточная машина Тьюринга.

Основные результаты.

1. Доказано существование иерархии по времени для *эвристических алгоритмов* из вычислительных классов NP, MA и AM. Дано новое доказательство иерархии по времени для эвристических алгоритмов из класса BPP.

2. Доказано существование иерархии по времени для *алгоритмов с одним битом подсказки* из вычислительного класса ZPP.

3. В стандартных криптографических предположениях доказано наличие иерархии легко вычислимых с одним битом подсказки функций по времени их обращения.

Научная новизна. Все основные результаты диссертации являются новыми.

Практическая и теоретическая ценность. Работа носит теоретический характер. Доказанные теоремы вносят вклад в изучение фундаментальных свойств эффективных алгоритмов, вычислительных процессов и криптографических конструкций. Кроме того, предложенная в работе техника упрощает доказательства некоторых ранее известных теорем.

Апробация работы. Результаты диссертации докладывались на следующих семинарах, симпозиумах и конференциях:

1. Заседание Санкт-Петербургского математического общества;
2. Семинар по дискретной математике ПОМИ РАН;
3. Международная научная школа по информатике для аспирантов (Эстония, 2006);
4. Международный симпозиум по алгоритмам и теории вычислительной сложности (Москва, 2007);
5. Международный симпозиум по сложности булевых функций (Даггштуль, Германия, 2006);
6. Международная конференция по теории вычислительной сложности (IEEE Computational Complexity Conference, Прага, Чехия, 2006 и Сан Диего, США, 2007).

Публикации. Основные результаты диссертации опубликованы в семи работах [9, 10, 11, 12, 13, 14, 15], перечисленных в конце автореферата. Работы [13] и [15] опубликованы в изданиях, входящих в перечень ВАК. Работа [11] опубликована в издании, входившем в перечень ВАК на момент публикации.

В работах [12, 13] Первышеву К. В. принадлежит результат о существовании иерархий по времени для алгоритмов с одним битом подсказки, принадлежащих произвольным вычислительным моделям, основанным на машинах Тьюринга (в частности, вероятностных). Совместно с Д. ван Мелкебеком дано упрощенное доказательство указанной теоремы, развивающее классический метод диагонализации. В работах [10, 11] Первышеву К. В. принадлежит доказательство иерархии легко вычислимых с одним битом подсказки функций по времени их обращения, а Григорьеву Д. Ю. и Гиршу Э. А. принадлежит аналогичный результат для языков.

Структура и объем работы. Диссертация состоит из введения и четырех глав. Нумерация разделов, формул, алгоритмов, процедур, примеров, лемм и теорем ведется отдельно для каждой главы. Текст диссертации изложен на 88 страницах (исключая список литературы). Список литературы содержит 28 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Определения и обозначения. Прежде всего приведем некоторые определения, необходимые для изложения содержания работы.

Начнем с определения тех *классов вычислительной сложности*, которые встречаются в формулировках доказываемых теорем. Напомним, что класс P состоит из тех и только тех языков, которые распознаются детерминированными машинами Тьюринга за полиномиальное время. Здесь и далее мы рассматриваем многоленточные машины Тьюринга.

Определим сложностной класс NP, который соответствует недетерминированным алгоритмам. Язык L принадлежит классу NP, если существует некоторая многоленточная машина Тьюринга $M(x,w)$ и некий полином $p(n)$, такие что $M(x,w)$ совершает не более $p(|x|)$ шагов, а также

$$\exists\, w \in \{0,1\}^{p(|x|)} : M(x,w) = 1 \quad (\text{при } x \in L)$$
$$\forall\, w \in \{0,1\}^{p(|x|)} : M(x,w) = 0 \quad (\text{при } x \notin L).$$

Определим сложностные классы BPP, RP и ZPP, которые соответствуют трем наиболее распространенным типам вероятностных алгоритмов — вероятностным алгоритмам с ограниченной двусторонней ошибкой (BPP), с ограниченной односторонней ошибкой (RP) и без ошибки (ZPP).

Язык L принадлежит классам BPP, RP или ZPP, если существует некоторая многоленточная машина Тьюринга $M(x,r)$ и некий полином $p(n)$, такие что $M(x,r)$ совершает не более $p(|x|)$ шагов, а также

$$\begin{array}{lll}
(\text{для BPP}) & \mathbf{Pr}\,[\,M(x,r)=1\,] > 2/3 & (\text{при } x \in L) \\
& \mathbf{Pr}\,[\,M(x,r)=0\,] > 2/3 & (\text{при } x \notin L) \\
\\
(\text{для RP}) & \mathbf{Pr}\,[\,M(x,r)=1\,] > 1/2 & (\text{при } x \in L) \\
& \mathbf{Pr}\,[\,M(x,r)=0\,] = 1 & (\text{при } x \notin L) \\
\\
(\text{для ZPP}) & \mathbf{Pr}\,[\,M(x,r)=1\,] > 1/2 & \\
& \quad \text{и } \mathbf{Pr}\,[\,M(x,r)=0\,] = 0 & (\text{при } x \in L) \\
& \mathbf{Pr}\,[\,M(x,r)=0\,] > 1/2 & \\
& \quad \text{и } \mathbf{Pr}\,[\,M(x,r)=1\,] = 0 & (\text{при } x \notin L),
\end{array}$$

где вероятность берется по случайной строке r, равномерно распределенной на множестве $\{0,1\}^{p(|x|)}$. Машине M позволено выдавать ответы, отличные от 0 и 1. Это оказывется существенным при определении класса ZPP.

Определим сложностные классы AM и MA, которые соответсвтуют двум наиболее распространенным типам одноraундовых интерактивных протоколов — играм типа Артур-Мерлин (AM) и играм типа Мерлин-Артур (MA).

Язык L принадлежит классам AM или MA, если существует некоторая многоленточная машина Тьюринга $M(x,r,w)$ и некий полином $p(n)$, такие что $M(x,r,w)$ совершает не более $p(|x|)$ шагов, а также

$$\begin{array}{ll} \text{(для AM)} & \mathbf{Pr}\left[\exists w \in \{0,1\}^{p(|x|)} : M(x,r,w)=1\right] > 2/3 \quad (\text{при } x \in L) \\ & \mathbf{Pr}\left[\forall w \in \{0,1\}^{p(|x|)} : M(x,r,w)=0\right] > 2/3 \quad (\text{при } x \notin L) \end{array}$$

$$\begin{array}{ll} \text{(для MA)} & \exists w \in \{0,1\}^{p(|x|)} : \mathbf{Pr}\left[M(x,r,w)=1\right] > 2/3 \quad (\text{при } x \in L) \\ & \forall w \in \{0,1\}^{p(|x|)} : \mathbf{Pr}\left[M(x,r,w)=0\right] > 2/3 \quad (\text{при } x \notin L), \end{array}$$

где вероятность берется по случайной строке r, равномерно распределенной на множестве $\{0,1\}^{p(|x|)}$.

В данных выше определениях мы требовали, чтобы функция $p(n)$ являлась некоторым полиномом. Если вместо этого потребовать, чтобы функция $p(n)$ была $O(t(n))$ для некоторой фиксированной функции $t(n)$, то мы получим вычислительные классы DTime$[t(n)]$,NTime$[t(n)]$, BPTime$[t(n)]$ и т. д. Эти классы содержат языки, которые распознаются за время $O(t(n))$ в соответствующих вычислительных моделях.

Эвристический алгоритм для некоторой задачи есть такой алгоритм, который правильно решает эту задачу на многих входах, но не обязательно на всех.

Определим формально класс языков, распознаваемых за полиномиалное время вероятностными эвристическими алгоритмами, обладающими ограниченной двусторонней ошибкой:

$$\mathsf{heur}_{1-\delta(n)}\mathsf{BPP} = \left\{ L : \exists L' \in \mathsf{BPP} : \forall n \underset{x\in\{0,1\}^n}{\mathbf{Pr}}[L(x)=L'(x)] \geq 1-\delta(n) \right\},$$

где вероятность берется по случайному входу x, равномерно распределенному на множестве $\{0,1\}^n$.

Аналогичным образом можно определить классы языков, распознаваемых эвристическими алгоритмами из других вычислительных моделей, а также классы языков, распознаваемых эвристическим алгоритмами за время $O(t(n))$.

Алгоритм с подсказкой есть такой алгоритм, который с каждым входом получает некоторую строку, называемую подсказкой. Подобная подсказка может помочь машине Тьюринга получить правильный ответ на данном входе. Однако, подсказки для всех входов одной длины должны быть одинаковыми. Соответственно, чем короче подсказка, тем меньше она помогает при вычислении ответа.

Формально, определим класс языков, распознаваемых за полиномиалное время вероятностными алгоритмами с ограниченной двусторонней ошибкой, получающими один бит подсказки. Язык L принадлежит классу $\mathsf{BPP}/1$, если существует некоторая многоленточная машина Тьюринга $M(x, r, a)$, последовательность однобитовых строк $\{a_n\}_{n=1}^{\infty}$ и некий полином $p(n)$, такие что $M(x, r, a_{|x|})$ совершает не более $p(|x|)$ шагов, а также

$$\begin{aligned}
&\mathbf{Pr}\left[\, M(x, r, a_{|x|}) = 1 \,\right] > 2/3 \quad (\text{при } x \in L) \\
&\mathbf{Pr}\left[\, M(x, r, a_{|x|}) = 0 \,\right] > 2/3 \quad (\text{при } x \notin L)
\end{aligned}$$

где вероятность берутся по случайной строке r, равномерно распределенным на множестве $\{0,1\}^{p(|x|)}$.

Если разрешить строкам a_n иметь длину $l(n)$, где $l(n)$ есть некоторая фиксированная функция, то мы получим класс $\mathsf{BPP}/l(n)$ — класс языков, распознаваемых вероятностными алгоритмами с ограниченной двусторонней ошибкой, получающими подсказку длины $l(n)$.

Кроме того, можно определить классы языков, распознаваемых алгоритмами с подсказкой, принадлежащими другим вычислительным моделям, а также классы языков, распознаваемых алгоритмами с подсказкой, работающими время $O(t(n))$.

Функция $T : \mathbb{N} \to \mathbb{N}$ называется *правильной*, если ее значение, представленное в единичной системе счисления строкой $1^{T(n)}$, вычислимо за время $O(n + T(n))$.

Вероятностная машина Тьюринга A называется $r(n)$-успешным взломщиком функции G, если для бесконечно многих n выполнено

$$\mathbf{Pr}\, A(G(x)) \in G^{-1}(G(x)) \geq \frac{1}{r(n)},$$

где вероятность берется по строке x, равномерно распределенной на множестве $\{0,1\}^n$, и по случайным числам машины A.

Класс $\mathsf{FPTime}[n^k]/1$ состоит из функций $G : \{0,1\}^* \to \{0,1\}^*$, вычислимых некоторой детерминированной машиной Тьюринга с одним битом подсказки за время $O(n^k)$.

Описание глав. Во **введении** обсуждается состояние исследований, связанных с темой диссертации, формулируются основные результаты диссертации, поясняется их положение в контексте текущих исследований, описывается структура диссертации.

В **первой главе** определяются основные понятия и вводятся обозначения, используемые на протяжении всей диссертации. В частности, определяются эвристические алгоритмы и алгоритмы с подсказкой; формально описываются основные вычислительные модели; объясняется различие между моделями синтаксическими и моделями семантическими.

На примере доказательства иерархии для недетерминированных алгоритмов дается общая схема доказательства иерархий по времени. Поясняются некоторые стандартные приемы, используемые в доказательствах иерархий.

Вторая глава посвящена иерархиям по времени для эвристических алгоритмов. Строится семейство графов-миксеров, используемых при доказательстве иерархии по времени для эвристических алгоритмов из модели недетерминированных вычислений; доказываются важные свойства этого семейства. Дается само доказательство иерархии для недетерминированных эвристических алгоритмов:

Теорема 3.2. *Для любых положительных a и c,*

$$\mathsf{NP} \not\subseteq \mathsf{heur}_{1/2+1/n^a}\mathsf{NTime}[n^c].$$

Дается альтернативное доказательство усиления ранее известной теоремы о существовании иерарахии для вероятностных эвристических алгоритмов с ограниченной двусторонней ошибкой:

Теорема 3.3. *Для любых положительных a и c,*

$$\mathsf{heur}_{1-1/n^a}\mathsf{BPP} \not\subseteq \mathsf{heur}_{1/2+1/n^a}\mathsf{BPTime}[n^c].$$

Доказывается теорема о существовании иерархии для эвристических алгоритмов из модели однораундовых игр типа Мерлин-Артур:

Теорема 3.5. *Для любых положительных a и c,*

$$\mathsf{heur}_{1-1/n^a}\mathsf{MA} \not\subseteq \mathsf{heur}_{1/2+1/n^a}\mathsf{MATime}[n^c].$$

Доказательство данной теоремы может быть модифицировано, с тем чтобы получить иерархию по времени для эвристических алгоритмов из модели однораундовых игр типа Артур-Мерлин:

Теорема 3.7. *Для любых положительных a и c,*

$$\mathsf{heur}_{1-1/n^a}\mathsf{AM} \not\subseteq \mathsf{heur}_{1/2+1/n^a}\mathsf{AMTime}[n^c].$$

Необходимые модификации приводятся в конце главы. Также обсуждается обобщение иерархии эвристических алгоритмов по времени с модели недетерминированных вычислений на другие синтаксические модели, замкнутые относительно операции "взятия большинства".

Третья глава посвящена иерархиям по времени для алгоритмов с подсказкой. Доказывается иерархия по времени для не допускающих ошибок вероятностных алгоритмов с одним битом подсказки:

Теорема 4.1. *Для любого положительного c,*

$$\mathsf{ZPP}/1 \not\subseteq \mathsf{ZPTime}[n^c]/1.$$

В качестве следствия выводится существование более плотной иерархии по времени:

Следствие 4.1. *Для любых положительных c и d, где $c < d$,*

$$\mathsf{ZPTime}[n^d]/1 \not\subseteq \mathsf{ZPTime}[n^c]/1.$$

В конце главы обсуждается обобщение иерархии на любые иные семантические модели вычислений с одним битом подсказки, основанные на многоленточных машинах Тьюринга.

В **четвертой главе** рассматривается задача обращения лекго вычислимых функций. Функции, легко вычислимые, но трудно обратимые, являются самым основным криптографическим примитивом и называются *односторонними функциями*.

Ставится вопрос о существовании иерархий по времени для задачи обращения легко вычислимых функций. Доказывается вспомогательная лемма об односторонних функциях. Доказывается существование иерархии по времени обращения для функций, вычислимых за линейное время с одним битом подсказки:

Теорема 5.1. *Предположим, что односторонние функции существуют. Рассмотрим произвольную функцию $r(n) = n^\rho$, где $\rho > 0$. Рассмотрим произвольную правильную функцию $\zeta(n)$, неубывающую и неограниченную.*

Тогда для любого $k \geq 1$ существует функция $G \in \mathsf{FPTime}[n]/1$, не имеющая $r(n)$-успешного взломщика, работающего время $O(n^k)$, однако имеющая $r(n)$-успешного взлщомщика, работающего время

$$O(\, n^k \log n \cdot r(n) \cdot \zeta^3(2n)\,).$$

В конце главы обсуждаются обобщения этой теоремы на перестановочные функции и функции с секретом.

ЛИТЕРАТУРА

[1] *Hartmanis J., Stearns R.* On the computational complexity of algorithms // *Transactions of the American Mathematical Society*. — 1965. — Vol. 117. — Pp. 285–306.

[2] *Cook S.* A hierarchy for nondeterministic time complexity // *Journal of Computer and System Sciences*. — 1973. — Pp. 343–353.

[3] *Seiferas J., Fischer M., Meyer A.* Separating nondeterministic time complexity classes // *Journal of the ACM*. — 1978. — Vol. 25. — Pp. 146–167.

[4] *Žák S.* A Turing machine time hierarchy // *Theoretical Computer Science*. — 1983. — Pp. 327–333.

[5] *Barak B.* A probabilistic-time hierarchy theorem for "slightly nonuniform" algorithms // International Workshop on Randomization and Approximation Techniques in Computer Science. — LNCS, 2002. — Pp. 194–208.

[6] *Fortnow L., Santhanam R.* Hierarchy theorems for probabilistic polynomial time // IEEE Symposium on Foundations of Computer Science. — 2004. — Pp. 316–324.

[7] *Fortnow L., Santhanam R., Trevisan L.* Hierarchies for semantic classes // ACM Symposium on Theory of Computing. — 2005. — Pp. 348–355.

[8] *Fortnow L., Santhanam R.* Recent work on hierarchies for semantic classes // *SIGACT News*. — 2006. — Vol. 37, no. 3.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

[9] *Pervyshev K.* Time hierarchies for computations with a bit of advice // Electronic Colloquium on Computational Complexity. — No. 54. — 2005. — 13 pp.

[10] *Grigoriev D., Hirsch E. A., Pervyshev K.* Time hierarchies for cryptographic function inversion with advice // Electronic Colloquium on Computational Complexity. — No. 76. — 2005. — 14 pp.

[11] *Grigoriev D., Hirsch E. A., Pervyshev K.* Time hierarchies for cryptographic function inversion with advice // PDMI Preprints. — No. 20. — 2006. — 14 pp.

[12] *van Melkebeek D., Pervyshev K.* A generic time hierarchy for semantic models with one bit of advice // IEEE Conference on Computational Complexity. — IEEE Computer Society, 2006. — Pp. 129–142.

[13] *van Melkebeek D., Pervyshev K.* A generic time hierarchy with one bit of advice // *Computational Complexity*. — 2007. — June. — Vol. 16, no. 2. — Pp. 139–179.

[14] *Pervyshev K.* On heuristic time hierarchies // IEEE Conference on Computational Complexity. — IEEE Computer Society, 2007. — June. — Pp. 347–358.

[15] *Первышев К.* Иерархии по времени для алгоритмов с одним битом подсказки // *Вестник Санкт-Петербургского университета*. — 2008. — Сер. 10, no. 3. — Pp. 136–143.