*Моим родителям*

Scott Aaronson

# Quantum Computing since Democritus

Скотт Аронсон

# Квантовые вычисления со времен Демокрита

Перевод с английского

АЛЬПИНА НОН-ФИКШН

Москва
2018

УДК 51-72:530.145
ББК 22.314
А12

*Издательство благодарит Российский квантовый центр и Сергея Белоусова за помощь в подготовке издания*

Переводчик Н. Лисова
Научный редактор А. Львовский
Редактор И. Лисов

**Ааронсон С.**

А12 Квантовые вычисления со времен Демокрита / Скотт Ааронсон ; Пер. с англ. — М. : Альпина нон-фикшн, 2018. — 494 с.

ISBN 978-5-91671-751-8

Написанная известным теоретиком в области квантовых вычислений Скоттом Ааронсоном, эта книга проведет вас через поразительное разнообразие тем, исследуя самые глубокие идеи математики, информатики и физики от теории множеств, вычислительной сложности, квантовых вычислений до интерпретации квантовой механики. Кроме того, вы познакомитесь с дискуссиями относительно путешествий во времени, парадокса Ньюкома, антропного принципа и взглядов британского физика и математика Роджера Пенроуза.

Неформальный стиль Ааронсона делает эту поразительную книгу доступной для читателей с научной подготовкой, а также для студентов и исследователей, работающих в области физики, информатики, математики и философии.

УДК 51-72:530.145
ББК 22.314

*Все права защищены. Никакая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, включая размещение в сети интернет и в корпоративных сетях, а также запись в память ЭВМ для частного или публичного использования, без письменного разрешения владельца авторских прав. По вопросу организации доступа к электронной библиотеке издательства обращайтесь по адресу mylib@alpina.ru*

© Scott Aaronson, 2013
© Издание на русском языке, перевод, оформление. ООО «Альпина нон-фикшн», 2018

ISBN 978-5-91671-751-8 (рус.)
ISBN 978-0-521-19956-8 (англ.)

# Оглавление

# Предисловие

*Критический обзор книги Скотта Ааронсона «Квантовые вычисления со времен Демокрита»,*
написанный им самим

«Квантовые вычисления со времен Демокрита» — достойный кандидат на звание самой странной книги, когда-либо опубликованной издательством Кембриджского университета. Ее необычность начинается с названия, которое загадочным образом не объясняет, о чем, собственно, говорится в этой книге. Быть может, это очередной учебник по квантовым вычислениям — модной области науки на стыке физики, математики и информатики, которая уже лет двадцать обещает миру новый тип компьютера, но пока не создала реального устройства, способного на что-нибудь более впечатляющее, чем разложение 21 на множители $3 \times 7$ (правда, с высокой вероятностью)? Если так, то что добавит именно эта книга к десяткам других, в которых уже изложены основы теории квантовых вычислений? Или, может быть, эта книга — наивная попытка связать квантовые вычисления с историей древнего мира? Но какое отношение может иметь Демокрит — древнегреческий философ-атомист — к книге, содержание которой по крайней мере наполовину было бы откровением для ученых даже в 1970-е годы, не говоря уже о IV веке до н. э.?

Теперь, когда я прочел эту книгу, я должен признать, что поистине блестящий и невыразимо оригинальный взгляд

автора на всё — от квантовых вычислений (заявленных в заголовке) до теорем Гёделя и Тьюринга, от вопроса о соотношении между **P** и **NP** до интерпретации квантовой механики, от искусственного интеллекта до парадокса Ньюкома и проблемы исчезновения информации в черной дыре — вынес мне мозг и заставил полностью пересмотреть свою картину мира. Так что если кто-то просматривает эту книгу в магазине, то я *несомненно* посоветовал бы этому человеку немедленно ее приобрести. Я также хотел бы добавить к этому, что автор необычайно хорош собой.

Трудно, однако, избежать подозрения в том, что «Квантовые вычисления со времен Демокрита» — это, по существу, «дамп памяти»: не особенно систематизированная коллекция мыслей о теории вычислительных систем, физике, математике и философии, которые присутствовали в сознании автора осенью 2006 г., когда он прочел серию лекций в Университете Ватерлоо; из этих лекций и выросла данная книга. Ее материал объединяет скучноватый юмор автора, его «сократический» подход к каждому вопросу и его одержимость теорией вычислений и тем, как она соотносится с физическим миром. Но если в книге и присутствует некий главный «тезис», который должен вынести из нее читатель, то я, хоть убейте, не могу его сформулировать.

Можно также задаться вопросом, на какого читателя рассчитана данная книга. С одной стороны, она *намного* глубже, чем полагается быть популярной книге. Как и «Путь к реальности» Роджера Пенроуза, — чье предисловие обещает легкую прогулку даже тем читателям, которым в начальной школе плохо давались дроби, но первые же несколько глав заводят неосторожного в дебри голоморфных функций и расслоённых пространств, — «Квантовые вычисления со времен Демокрита» не годятся для людей с фобией к математике. *Разумеется*, любопытный дилетант сможет извлечь из этой книги немало информации, но при этом он (или она) должен быть готов пропускать некоторые особо темные места, — возможно,

для того, чтобы вернуться к ним позже. Так что если вы из тех, кто может переварить «научный текст» только после того, как из него тщательно вычистили всю науку, вам лучше поискать что-нибудь другое.

С другой стороны, книга получилась *также* слишком многотемной, легкомысленной и своеобразной, чтобы ее можно было использовать как учебник или справочник. Конечно, в ней есть теоремы, доказательства и упражнения и она охватывает основы поразительного числа научных областей, таких как логика, теория множеств, вычислимость, сложность, криптография, квантовая информация и теория вычислительного обучения. Представляется, что студенты высших учебных заведений в любой из этих областей, от предпоследнего курса и выше, могли бы обогатиться при помощи этой книги ценной информацией — или использовать ее в качестве занимательного самоучителя или курса переподготовки. Помимо основ, в книге содержится также значительный материал по квантовой теории сложности, к примеру о силе квантовых доказательств и совета, что (насколько известно автору настоящего обзора) нигде больше не в виде книги не издавалось. Но все же книга перескакивает с предмета на предмет слишком поспешно, чтобы ее можно было считать каноническим текстом на какую-либо тему.

Итак, для кого же предназначена эта книга? Неужели для неспециалистов, которые *в реальности* не пройдут дальше первой главы, но которые захотят впечатлить гостей, положив такую интеллектуальную книгу на журнальный столик? Я вижу лишь одну иную возможность: существует определенная аудитория (как правило, ей уделяют мало внимания) у научных книг, которые нельзя отнести ни к «популярной», ни к «профессиональной» категории. Речь идет о книгах, которые описывают участок интеллектуального ландшафта с позиции некоего исследователя (весьма предвзятой) и пользуются при этом примерно тем же языком, каким этот исследователь мог бы обсуждать свою тему в коридоре университета

с коллегой из другой научной области. Возможно, помимо упомянутых коллег, эта гипотетическая «неохваченная аудитория» могла бы включать одаренных студентов или, скажем, программистов и инженеров, которым в университете нравились теоретические курсы и которые хотят выяснить, что в соответствующей области появилось нового. Возможно, это та же аудитория, что регулярно посещает «научные блоги», о которых мне приходилось слышать: онлайновые площадки, где кто угодно может, судя по всему, наблюдать, как настоящие ученые, люди с переднего края человеческого познания, занимаются мелкими дрязгами, обзывают друг друга и демонстрируют другие формы подросткового поведения. Там можно даже спровоцировать ученых и вынудить их показать себя с еще более неприглядной стороны. (Следует отметить, что автор книги ведет особенно эпатажный и скандальный блог такого рода.) *Если* такая аудитория действительно существует, то, быть может, автор знает, что делает, когда обращается к ней. Однако мне кажется, что автор получил при подготовке этой книги слишком много удовольствия, чтобы поверить, что он руководствовался сколько-нибудь проработанным планом.

## А теперь — настоящее предисловие

Хотя я ценю добрые слова автора рецензии о моей книге (и даже о моей внешности!), которые вы могли видеть на предыдущих страницах, я при всем том категорически возражаю против высказанного им невежественного утверждения о том, что в книге «Квантовые вычисления со времен Демокрита» нет обобщающего тезиса. Он в книге *есть* — хотя, как ни странно, не я первым сумел понять, в чем он состоит. За формулировку центральной мысли этой книги я должен поблагодарить Love Communications — рекламное агентство из Сиднея (Австралия), вложившее эту мысль в уста гламурных моделей с целью повышения продаж принтеров.

Позвольте мне рассказать эту историю — она того стоит.

В 2006 г. я читал курс «Квантовые вычисления со времен Демокрита» в Университете Ватерлоо. В течение следующего года я выкладывать краткие заметки по этому курсу в своем блоге *Shtetl-Optimized** — именно из этих заметок позже сложилась данная книга. Меня тогда воодушевил энтузиазм, с которым заметки были встречены читателями блога; должен сказать, что именно реакция читателей убедила меня опубликовать их в виде книги. Но был один отклик, который ни я, ни кто-либо другой не мог предвидеть заранее.

1 октября 2007 г. я получил электронное письмо от некоего австралийца по имени Уоррен Смит, который писал, что видел по телевизору интересную рекламу принтеров Ricoh. В ней, продолжал он, две девушки-модели в гримерной вели следующий диалог:

> *Первая модель:* Но если квантовая механика — это не физика в обычном смысле слова, если она не занимается ни веществом, ни энергией, ни волнами, то чем же она занимается?
>
> *Вторая модель:* Ну, с моей точки зрения, она занимается информацией, вероятностями, наблюдаемыми величинами и тем, как все они соотносятся между собой.
>
> *Первая модель:* Как интересно!

После этого в ролике вспыхивал слоган: «Наша модель умнее», после которого появляется изображение принтера Ricoh.

Смит сообщил, что заинтересовался происхождением столь необычного рекламного текста и стал гуглить его. Поиск привел его к девятой главе моих конспектов на тему «Квантовые

---

* www.scottaaronson.com/blog. Использованное в названии блога слово *штетл* обозначало еврейское местечко в черте оседлости Российской империи. — *Прим. пер.*

вычисления со времен Демокрита», где на стр. 175 он обнаружил следующий пассаж:

> Но если квантовая механика — это не физика в обычном смысле слова, если она не занимается ни веществом, ни энергией, ни волнами, ни частицами, то *чем же* она занимается? С моей точки зрения, она занимается информацией, вероятностями, наблюдаемыми величинами, и еще тем, как все они соотносятся между собой.

Оказалось, что в рекламном диалоге присутствовала ровно одна фраза, которую написал *не я* («Как интересно!»). Смит нашел ссылку*, по которой я смог сам увидеть этот рекламный ролик на YouTube, и вся история подтвердилась.

Меня это больше позабавило, нежели рассердило. Я сделал в блоге запись под заголовком «Австралийские актрисы сплагиатили мою лекцию по квантовой механике, чтобы продавать принтеры»**. После изложения происшедшего и ссылки на видео пост заканчивался так:

> Едва ли не впервые в жизни я не нахожу слов. Я не знаю, как на это реагировать. Не знаю, какую из 500 000 возможных шуток выбрать. Помогите мне, читатели. Должен ли я чувствовать себя польщенным? Или, может быть, пора звонить юристу?

Этому посту суждено было стать самым популярным из всех, когда-либо мной написанных. На следующее утро эта история попала на страницы в *Sydney Morning Gerald* («Профессор: “Рекламное агентство сплагиатило запись моей лекции”»***),

---

* www.youtube.com/watch?v=saWCyZupO4U. Здесь и далее примечания автора даются без дополнительных указаний.

** www.scottaaronson.com/blog/?p=277

*** www.smh.com.au/news/technology/professor-claims-ad-agency-cribs-lecturenotes/2007/10/03/1191091161163.html

на сайт Slashdot («Скотт Ааронсон рекламирует принтеры»*) и еще на нескольких новостных сайтах. Я в тот момент находился в Латвии в гостях у своего коллеги Андриса Амбайниса, но журналистам удалось каким-то образом меня разыскать в рижской гостинице; меня разбудили в пять утра, чтобы взять интервью.

Тем временем реакция читателей в моем блоге и на других онлайн-форумах оказалась смешанной. Некоторые говорили, что я поступлю глупо, если не подам в суд на рекламное агентство и не получу с него максимально возможную компенсацию. Что, если бы они вставили в свой рекламный ролик несколько тактов из какой-нибудь песни *Rolling Stones,* не получив предварительно на то разрешения? Выплаты по подобным процессам, заверили меня, иногда составляют миллионы долларов. Другие читатели утверждали, что сама *постановка вопроса* делает меня стереотипным американцем-сутяжником, воплощением всех недостатков этого мира. Я должен чувствовать себя польщенным, продолжали они, что авторы рекламного текста сочли нужным дать *моим* взглядам на квантовую механику такую бесплатную рекламу. В десятках комментариев мне в разных выражениях предлагалась одна и та же пошлая шутка: потребовать в качестве компенсации свидание с «моделями». (На это я ответил, что, если уж говорить о компенсации, предпочел бы получить бесплатный принтер.) Кто-то из комментаторов написал просто: «Да уж, не исключено, что эта история — самое смешное, что когда-либо происходило».

Love Communications, со своей стороны, признали, что использовали в рекламе текст моей лекции, но заявили, что консультировались с юристом и были уверены, такая практика не выходит за рамки добросовестного использования. Я тем временем все-таки *связался* с австралийским юристом,

* idle.slashdot.org/story/07/10/02/1310222/scott-aaronson-printer-shill

специализирующимся на интеллектуальных правах, и он сказал, что мое дело вполне может оказаться выигрышным, но участие в процессе потребует усилий и времени. Я колебался: с одной стороны, плагиат — один из немногих непростительных грехов научного мира, да и бесцеремонный ответ рекламного агентства, пойманного на горячем, вызвал у меня раздражение. С другой стороны, если бы они меня *спросили,* я, вероятно, с радостью разрешил бы им использовать свои слова — либо за символическую сумму, либо вообще бесплатно.

В конце концов мы нашли решение, которое понравилось всем. Love Communications извинились (не признавая при этом, что поступили неправильно) и пожертвовали 5000 долларов двум австралийским научно-просветительским организациям, которые я назвал*. В ответ я отказался от всяких дальнейших действий и почти что забыл об этой истории и вспоминаю теперь о ней только тогда, когда коллеги начинают надо мной подшучивать, вспоминая австралийских моделей (им это никак не надоест).

Но замечательна эта история — и потому я ее здесь пересказываю (ну, помимо того, что это подлинная забавная история, связанная с этой книгой) — что если бы мне нужно было выбрать из всей книги один абзац для телепередачи, я, кажется, выбрал бы именно тот, что выбрали копирайтеры агентства, хотя они, вероятно, просто просматривали книгу по диагонали в поисках какой-нибудь наукообразной ерунды, а я никак эту мысль не выделил, поскольку даже не задумался о ее важности.

Идея о том, что квантовая механика занимается информацией, вероятностями и наблюдаемыми величинами, а вовсе не волнами и частицами, безусловно, нельзя назвать оригинальной. Физик Джон Арчибальд Уилер говорил нечто подобное еще в 1970-е гг.; сегодня вокруг этой идеи построена вся

* www.scottaaronson.com/blog/?p=297

научная область, связанная с квантовыми вычислениями и информацией. В самом деле, во время дискуссии в моем блоге, развернувшейся после эпизода с австралийскими моделями, один из наиболее частых аргументов (и наиболее забавных, по-моему) состоял в том, что мне, по существу, не на что жаловаться, поскольку заимствованный отрывок *не отличался ничем особенным;* в нем высказана очевидная мысль, которую можно найти в любой книге по физике!

Как бы мне хотелось, чтобы это было действительно так! Даже сегодня, в 2013 г., взгляд на квантовую механику как на теорию информации и вероятностей остается в общем и в целом точкой зрения меньшинства. Возьмите почти любую книгу по физике — хоть популярную, хоть теоретическую, и вы узнаете, что (а) в современной физике полно парадоксальных на первый взгляд утверждений, к примеру что волны — это частицы, а частицы — это волны, (б) никто по-настоящему глубоко этих вещей не понимает, (в) даже на перевод их на язык математики требуются годы интенсивной работы, но (г) благодаря им атомные спектры удается рассчитать правильно, а именно это, в конце концов, и важно.

Так, красноречивое изложение этого «традиционного взгляда» можно найти в книге Карла Сагана «Мир, полный демонов»:

«Предположим, вы решили всерьез разобраться в квантовой механике. Сначала нужно овладеть математическим аппаратом, целым рядом математических дисциплин, каждая из которых подводит к следующей, более высокой ступени. Арифметика, геометрия Евклида, алгебра по программе старших классов, дифференциальное и интегральное исчисление, дифференциальные уравнения, обычные и в частных производных, векторное исчисление, некоторые специальные функции математической физики, матричная алгебра и теория групп… Нелегка задача популяризатора науки, который захочет дать широкой публике, не прошедшей весь этот обряд посвящения, хоть какое-то представление о квантовой

механике. На мой взгляд, удачных популяризаций квантовой механики просто не существует, и отчасти по этой самой причине. На все эти математические сложности накладывается тот факт, что квантовая теория демонстративно контринтуитивна. Подходить к ней, вооружившись здравым смыслом, почти бесполезно. Как говорил в свое время Ричард Фейнман, бессмысленно спрашивать, *почему* так. Этого никто не знает. Так устроено, и все тут».

Можно понять, почему так говорят физики: физика — наука экспериментальная. В физике *можно* сказать: «Правила здесь вот такие, не потому, что они разумны, но потому, что мы провели эксперимент и получили вот такой результат». Можно даже сказать это гордо и восхищенно, *бросая вызов* скептикам: а попробуйте-ка противопоставить свои косные представления вердикту Природы!

Лично я просто *верю* экспериментаторам, когда они говорят, что мир устроен и работает совершенно иначе, чем я себе представлял. Дело не в том, чтобы убедить меня. Кроме того, я не пытаюсь предсказывать, что экспериментаторы откроют в следующий раз. Единственное, что я хочу знать: *Что случилось с моей интуицией? Как мне ее поправить, чтобы интуиция не слишком расходилась с результатами экспериментов? Как мог бы я рассуждать, чтобы реальное поведение мира не удивляло бы меня так сильно?*

Если говорить о нескольких предыдущих научных революциях — о ньютоновой физике, дарвиновой эволюции, о специальной теории относительности, то я, как мне кажется, примерно представляю себе ответы на приведенные вопросы. И если моя интуиция пока еще не до конца приспособилась даже к этим теориям, то я, по крайней мере, знаю, как ее *нужно* настроить. А потому, если бы я, к примеру, создавал новую вселенную, я мог бы сделать ее инвариантной или не инвариантной относительно преобразований Лоренца, но я определенно *рассмотрел бы* такую возможность и я бы понял, почему Лоренц-инвариантность является неизбежным

следствием пары других свойств, которые мне могли бы понадобиться для новой вселенной.

Но с квантовой механикой все иначе. Здесь, уверяют нас физики, *никто не знает,* как нужно настроить интуицию, чтобы поведение элементарных частиц перестало казаться столь безумным. Более того, не исключено, что такого способа просто *не существует*; может быть, субатомное поведение навсегда останется для нас всего лишь произвольным грубым фактом, и нам нечего будет сказать о нем, помимо того, что «такие-то и такие-то формулы дают верный ответ». Моя реакция на это достаточно радикальна: если это правда, то *мне нет дела* до того, как ведут себя элементарные частицы. Несомненно, кому-то другому *необходимо* это знать, к примеру тем, кто разрабатывает лазеры или транзисторы, — так пусть они и изучают. Что до меня, я просто займусь изучением какого-нибудь другого предмета, более мне понятного, скажем теории вычислительных систем. Сказать мне, что моя физическая интуиция не работает, и не дать никакого способа *скорректировать* эту интуицию, — все равно что завалить меня на экзамене и даже не намекнуть, в чем дело и как можно было бы добиться лучшего результата. Как только появится возможность, я просто переключусь на другие курсы, где у меня есть возможность заработать высший балл, где моя интуиция *работает*.

К счастью, мне представляется, что в результате нескольких десятилетий работы в области квантовых вычислений и квантовых принципов мы получили возможность добиться куда большего, чем просто назвать квантовую механику набором загадочных бессмысленных фактов. Короче говоря, вот что ожидает вас в этой книге:

> *Квантовая механика — это красивое обобщение законов вероятности, обобщение, основанное скорее на второй норме, нежели на первой, и скорее на комплексных, нежели на неотрицательных действительных числах.*

*Ее можно изучать совершенно отдельно от ее приложения к физике (более того, такое изучение обеспечивает хороший старт для последующего изучения приложений к физике). Эта обобщенная теория вероятностей естественным образом приводит нас к новой вычислительной модели — к модели квантовых вычислений, которая бросает вызов всем нашим идеям, связанным с вычислениями и считавшимся прежде само собой разумеющимися. Эту модель специалисты по теории вычислительных систем могли бы предложить и сами для собственного удобства, даже если бы она не была связана с физикой. Короче говоря, хотя квантовая механика была придумана сто лет назад для решения технических проблем физики, сегодня ее можно плодотворно объяснить с совершенно иной точки зрения: как часть истории идей в математике, логике, вычислительных системах и философии, идей о пределах познаваемого.*

В этой книге я попытаюсь выполнить сделанные обещания, двигаясь к цели неторопливым кружным путем. Наш путь начнется в главе 1 настолько близко к «началу», насколько это возможно, — с древнегреческого философа Демокрита. Дошедшие до нас фрагменты трудов Демокрита, который рассуждает, в частности, о том, что все природные явления проистекают из сложных взаимодействий между несколькими разновидностями крохотных «атомов», стремительно летающих в пустом по большей части пространстве, ближе к современному научному мировоззрению, чем что бы то ни было в античности (и много ближе, чем любые идеи Платона и Аристотеля). Но стоит Демокриту сформулировать атомную гипотезу, как он замечает с тревогой, что она стремится «целиком поглотить» тот самый чувственный опыт, который он как будто пытался объяснить с самого начала. Каким образом *его* можно свести к движению атомов? Демокрит изложил эту дилемму в форме диалога между Разумом и Чувствами:

*Разум:* Только по договоренности между людьми существует сладость, по договоренности — горечь, по договоренности — цвет, на самом деле существуют только атомы и пустота.

*Чувства:* Глупый разум! Неужели ты стремишься ниспровергнуть нас, хотя именно от нас получаешь все данные?

Этот обмен репликами служит, по существу, краеугольным камнем всей книги. Одной из тем для моих рассуждений будет то, что квантовая механика снабжает, судя по всему, *и Разум, и Чувства* новыми аргументами в их 2400-летнем споре, хотя по-прежнему (я так считаю) не обеспечивает чистой победы ни для одной стороны.

В главах 2 и 3 я перехожу к обсуждению самой глубокой из всех имеющихся у нас областей знания, совершенно намеренно *не зависящей* от «грубых фактов» об окружающем мире, а именно математики. Даже здесь что-то внутри меня (и, как я подозреваю, внутри многих других компьютерщиков!) с подозрением относится к тем *разделам* математики, которые несут на себе явный отпечаток физики, — это, к примеру, дифференциальные уравнения в частных производных, дифференциальная геометрия, группы Ли и что угодно еще, выглядящее «слишком непрерывным». Поэтому я начинаю с самых «нефизических» разделов математики, известных на данный момент, — с теории множеств, логики и вопросов вычислимости. Я рассказываю о великих открытиях Кантора, Фреге, Гёделя, Тьюринга и Коэна, которые помогли нанести на карту контуры математических рассуждений как таковых и которые — в процессе демонстрации причин, по которым всю математику невозможно свести к фиксированному «механическому процессу», — продемонстрировали также, сколь значительную часть ее все же *можно* свести к такому процессу; заодно удалось прояснить, что, собственно, представляет собой сей «механический процесс». Поскольку я никак не могу

от этого удержаться, в главе 4 я углубляюсь в давний спор о том, не сводится ли работа человеческого разума к «устоявшимся механическим процессам». Я стараюсь излагать позиции сторон в этом споре как можно беспристрастнее (хотя мои собственные пристрастия, несомненно, тоже заметны).

В главе 5 представлена молодая сестра теории вычислимости — *теория вычислительной сложности,* которая в дальнейшем играет в книге центральную роль. Я пытаюсь проиллюстрировать, в частности, как вычислительная сложность позволяет нам методично брать «глубокие философские загадки» о пределах человеческого знания и превращать их во «всего лишь» безумно сложные нерешенные математические задачи, в которых, по мнению некоторых, отражается большая часть того, что нам хотелось бы знать! Невозможно придумать лучший пример такого превращения, чем так называемая проблема перебора, или вопрос о равенстве классов сложности **P** и **NP**, о котором я расскажу в главе 6. Затем, в качестве разогрева перед квантовыми вычислениями, в главе 7 будут рассмотрены многочисленные применения *классического* понятия случайности — как в теории сложности вычислений, так и в других областях жизни; а глава 8 объяснит, как при помощи идей из области вычислительной сложности начиная с 1970-х гг. удалось по-настоящему революционизировать теорию и практику *криптографии*.

Все это — всего лишь подготовка сцены для самой тяжелой части книги — главы 9, в которой представлен мой взгляд на квантовую механику как «обобщенную теорию вероятностей». В главе 10 объясняются основы моей собственной научной области — *квантовой теории вычислений,* которую можно кратко определить как соединение квантовой механики и теории вычислительной сложности.

В качестве «награды» за упорство глава 11 предлагает критический разбор идей сэра Роджера Пенроуза, убежденного, как известно, в том, что мозг — это не просто квантовый компьютер, но квантовый *гравитационный* компьютер,

способный решать невычислимые по Тьюрингу задачи, и что это или что-то подобное можно показать при помощи теоремы Гёделя о неполноте. Указать на проблемы и недостатки этих идей проще простого, и я это делаю, но еще интереснее, как мне кажется, задаться вопросом о том, не скрываются ли все же в рассуждениях Пенроуза крупицы истины.

В главе 12 рассматривается то, что я считаю главной концептуальной проблемой квантовой механики: не то, что будущее неопределенно (а кому до этого есть дело?), но то, что прошлое *также* неопределенно! Я разбираю две очень разные реакции на эта проблему: во-первых, популярное среди физиков обращение к *декогеренции* и «эффективной стреле времени» на базе Второго начала термодинамики; и во-вторых, «теории со скрытыми параметрами», такие как теория волны-пилота (она же теория де Бройля — Бома). Я считаю, что теории со скрытыми параметрами, даже если они будут отвергнуты, ставят перед нами необычайно интересные математические вопросы.

В оставшейся части книги рассматривается приложение всего изложенного выше к тем или иным серьезным, захватывающим или противоречивым вопросам математики, информатики, философии и физики. В этих главах значительно больше, чем в начальных, уделено внимание *недавним исследованиям,* в основном в области квантовой информации и вычислительной сложности, но также в области квантовой гравитации и космологии; мне представляется, что появляется некоторая надежда пролить свет на эти «коренные вопросы». Поэтому мне кажется, что именно последние главы устареют первыми! Несмотря на кое-какие не слишком существенные логические завязки, в первом приближении можно сказать, что эти последние главы можно читать в любом порядке.

- В главе 13 говорится о новых концепциях математического доказательства (включая вероятностное доказательство и доказательство с нулевым разглашением), а затем рассказывается

о приложении этих новых понятий к пониманию вычислительной сложности теорий со скрытыми параметрами.

- В главе 14 поднимается вопрос о «размере» квантовых состояний: действительно ли в них зашифровано экспоненциальное количество классической информации? Кроме того, этот вопрос соотносится, с одной стороны, с дебатами о квантовой интерпретации, а с другой — с недавними исследованиями квантовых доказательств и совета на базе теории сложности.
- В главе 15 разбираются аргументы *скептиков* квантовых вычислений — тех, кто считает, что создать реальный квантовый компьютер не просто сложно (с чем согласны решительно все!), но *невозможно* по некоторым фундаментальным причинам.
- В главе 16 разбирается юмова проблема индукции; она используется как трамплин для обсуждения *теории вычислительного обучения,* а также недавних работ по изучаемости квантовых состояний.
- В главе 17 рассказывается о некоторых прорывных открытиях, меняющих наши представления о классических и квантовых интерактивных системах доказательства (к примеру, о теоремах **IP** = **PSPACE** и **QIP** = **PSPACE**); в основном эти открытия интересуют нас постольку, поскольку ведут к *нерелятивизирующим нижним оценкам сложности схемы* и, следовательно, могли бы осветить некоторые аспекты вопроса о равенстве **P** и **NP**.
- В главе 18 разбираются знаменитый антропный принцип и «аргумент Судного дня»; дискуссия начинается как сугубо философическая (разумеется), но постепенно сводится к обсуждению *квантовых вычислений с постселекцией* и теоремы **PostBQP** = **PP**.
- В главе 19 обсуждаются парадокс Ньюкома и свобода воли, что выливается в рассказ о «теореме о свободе воли» Конуэя — Кохена и использовании неравенства Белла для генерации «случайных чисел по Эйнштейну».
- глава 20 посвящена путешествиям во времени: разговор уже традиционно начинается с широкой философской дискуссии,

а заканчивается доказательством того, что классические *и* квантовые компьютеры с замкнутыми времениподобными траекториями выдают вычислительную мощность, в точности равную **PSPACE** (при допущениях, которые открыты для интересных возражений, о чем я расскажу подробно).

- В главе 21 речь пойдет о космологии, темной энергии, пределе Бекенштейна и голографическом принципе, но, что не удивительно, с акцентом на то, что все эти вещи значат для *пределов вычислений*. К примеру: сколько бит можно сохранить или просмотреть и сколько операций над этими битами можно проделать, не использовав при этом столько энергии, что вместо вычислений возникнет черная дыра?
- глава 22 остается «на десерт»; в ее основе лежит завершающая лекция курса «Квантовые вычисления со времен Демокрита», на которой студенты могли задавать мне абсолютно любые вопросы и смотреть, как я с ними справлюсь. Среди затронутых тем: возможность падения квантовой механики; черные дыры и так называемые пушистые клубки; что дают оракулы в вопросе о вычислительной сложности; **NP**-полные задачи и творческое начало; «сверхквантовые» корреляции; дерандомизация рандомизированных алгоритмов; наука, религия и природа разума; а также почему информатика не является разделом физики.

И последнее замечание. Чего вы точно *не найдете* в этой книге, так это рассуждений о практической стороне квантовых вычислений: ни о физической реализации, ни о коррекции ошибок, ни о деталях базовых квантовых алгоритмов, таких как алгоритмы Шора, Гровера и др. Одна из причин такого подхода кроется в случайном обстоятельстве: книга основана на лекциях, которые я читал в Канаде в Институте квантовых вычислений Университета Ватерлоо, и студенты, слушавшие его, уже разбирались со всеми этими аспектами на других курсах. Вторая причина заключается в том, что эти аспекты рассматриваются

в десятках других книг* и выложенных в сеть лекций (включая и мои собственные), и я не видел смысла изобретать велосипед. Но есть и третья причина: техническая перспектива создания компьютера нового типа, конечно, интересна, но не ради этого я занялся квантовыми вычислениями. (Только *тс-с-с*, не передавайте моих слов директорам агентств, занимающихся финансированием науки.)

Поясняю. На мой взгляд, вполне вероятно, что я еще увижу при своей жизни действующие квантовые компьютеры (разумеется, возможно также, что и *не увижу*). И если у нас *действительно* появятся масштабируемые универсальные квантовые компьютеры, то они почти наверняка найдут себе реальное применение (даже если не говорить о взломе шифров): мне кажется, что по большей части это будут специализированные задачи, такие как квантовое моделирование, и в меньшей степени — решение задач комбинаторной оптимизации. Если это произойдет, я, естественно, обрадуюсь не меньше прочих и буду гордиться, если какие-то результаты моей работы найдут применение в этом новом мире. С другой стороны, если бы кто-то завтра дал мне реальный квантовый компьютер, то ума не приложу, к чему лично я мог бы его применить: в голову лезут только варианты его использования *другими* людьми!

Отчасти именно поэтому, если бы вдруг кому-то удалось доказать, что масштабируемые квантовые вычисления *невозможны*, это заинтересовало бы меня в тысячу раз сильнее, чем доказательство их возможности. Ведь такая неудача подразумевала бы, что с нашими представлениями о квантовой механике что-то не так; это была бы настоящая революция в физике! Будучи прирожденным пессимистом, я *полагаю*, однако, что Природа не будет настолько добра к нам и что

* Стандартным учебным пособием в этой области остаются «Квантовые вычисления и квантовая информация» Майкла Нильсена (Michael Nielsen) и Айзека Чуанга (Isaac Chuang).

в конце концов возможность масштабируемых квантовых вычислений будет окончательно выявлена.

В общем, можно сказать, что я работаю в этой области не столько потому, что квантовые компьютеры могут принести нам какую-то пользу, сколько потому, что сама *возможность* создания квантовых компьютеров *уже* меняет наши представления об окружающем мире. Либо реальный квантовый компьютер можно построить, и тогда пределы познаваемого оказываются совсем не такими, как мы считали прежде; либо его построить нельзя, и тогда сами принципы квантовой механики нуждаются в пересмотре; *или же* существует, может быть, какой-то способ эффективно моделировать квантовую механику при помощи традиционных компьютеров, о котором никто пока не подозревает. Все три эти варианта сегодня звучат как пустой бездоказательный треп, но ведь по крайней мере один из них верен! Так что к какому бы результату мы ни пришли в конце концов, что тут можно сказать, кроме как сплагиатить в ответ фразу из того самого рекламного ролика: «Это интересно»?

## Что нового

Просматривая рукопись перед публикацией в виде книги, я больше всего удивился тому, как много всего *произошло* в этих областях между моментом, когда я читал этот курс впервые (2006 г.), и «настоящим» моментом (2013 г.). Эта книга замышлялась как посвященная глубоким вопросам, древним, как физика и философия, или по крайней мере возникшим одновременно с квантовой механикой и информатикой почти столетие назад. На повседневном уровне никак не ощущается, чтобы в дискуссии по этим вопросам что-то менялось. Поэтому необходимость существенно перерабатывать и расширять лекции по прошествии всего лишь шести лет стала для меня невыразимо приятной обязанностью.

Чтобы проиллюстрировать развитие вещей, позвольте мне привести неполный список достижений, о которых пойдет

речь в книге, но о которых *не могла идти речь* на лекциях 2006 г. по той простой причине, что события эти на тот момент еще не произошли. Компьютер Watson фирмы IBM выиграл у чемпиона мира по «Своей игре» Кена Дженнингса, вынудив меня дополнить разговор об ИИ новым примером (см. с. 81), совершенно иным по характеру, чем предыдущие, такие как ELIZA и Deep Blue. Вирджиния Василевская-Уильямс, опираясь на работы Эндрю Стозерса, нашла способ перемножить две матрицы $n \times n$ с использованием всего $O(n^{2,373})$ шагов, *слегка* превзойдя при этом результат Копперсмита и Винограда $O(n^{2,376})$, который держался так долго, что число 2,376 начало уже восприниматься как природная константа (см. с. 97).

Достаточно серьезные события произошли в области *криптографии на решетках,* которая представляется самой перспективной базой для создания систем шифрования с открытым ключом, устойчивых даже против квантовых компьютеров (см. с. 68–71). Следует особо отметить, что Крейг Джентри смог решить задачу, которая никому не давалась 30 лет: он использовал решетки, чтобы предложить первые *полностью гомоморфные криптосистемы*. Эти системы позволяют клиенту доверить любые вычисления незащищенному серверу, при этом на сервер передаются зашифрованные входные данные, а обратно получаются зашифрованные результаты, и только сам клиент может расшифровать результат и удостовериться в его подлинности; сервер же не получает никакой информации о том, что именно ему поручили считать.

Если говорить об основах квантовой механики, Чирибелла с соавторами (см. с. 201) привели новый аргумент в пользу того, «почему» в квантовой механике должны действовать именно такие правила. А именно: они доказали, что только эти правила совместимы с некоторыми общими аксиомами теории вероятностей и *одновременно* с немного загадочной аксиомой о том, что «любые смешанные состояния могут быть очищены», то есть всякий раз в том случае, когда мы знаем о физической системе А не все, что можно знать, наше

незнание должно полностью объясняться предположением о корреляциях между A и некоторой далекой системой B, такой, что мы должны иметь полные данные об объединенной системе AB.

В теории квантовых вычислений задача Бернштейна — Вазирани о «рекурсивной выборке Фурье», которой в лекциях 2006 г. я посвятил довольно много времени, была вытеснена моей задачей о «проверке коэффициентов Фурье» (см. с. 218). Задача Бернштейна — Вазирани осталась в истории как первая когда-либо предложенная задача с черным ящиком, которую квантовый компьютер доказуемо может решить сверхполиномиально быстрее, чем классический вероятностный компьютер, и, следовательно, как важный предшественник прорывных открытий Саймона и Шора. Но сегодня, если нам потребуется кандидат на роль задачи класса **BQP/PH**, иными словами, задачи, которую квантовый компьютер может решить с легкостью, но которая вообще не входит в классическую «полиномиальную иерархию», то представляется, что «проверка коэффициентов Фурье» во всех отношениях превосходит «рекурсивную выборку Фурье».

Несколько задач, которые излагались в моих лекциях 2006 г. как нерешенные, успели с тех пор изменить свой статус. Так, мы с Эндрю Друкером показали, что класс **BQP/qpoly** входит в класс **QMA/poly** (к тому же доказательство получилось релятивизирующее), опровергнув тем самым мою гипотезу о том, что эти классы должны различаться по оракулам (см. с. 305). Кроме того, произошел справедливо отмеченный прорыв в теории квантовых вычислений: Джайн с соавторами доказал, что **QIP = PSPACE** (см. с. 365); это означает, что квантовые интерактивные системы доказательства не мощнее классических. В этом случае я по крайней мере угадал правильный ответ!

(На самом деле был *еще один* прорыв в исследовании квантовых интерактивных систем доказательства, о котором *я не буду* рассказывать в этой книге. Недавно мой постдок

Томас Видик вместе с Цуёси Ито* показал, что **NEXP** $\subseteq$ **MIP***; это означает, что любую интерактивную систему доказательства с *многими* доказателями можно «привить» против того, чтобы эти доказатели втайне скоординировали свои отклики посредством квантовой запутанности.)

В главе 20 этой книги обсуждается предложенная Дэвидом Дойчем модель квантовой механики в присутствии замкнутых времениподобных траекторий, а также мой и Джона Ватруса новый (на тот момент) вывод о том, что модель Дойча обеспечивает в точности вычислительную мощность **PSPACE.** (Отсюда, в частности, следует, что путешествующие во времени квантовые компьютеры оказались бы не более мощными, чем *классические* компьютеры того же назначения, если вас почему-то интересовал этот вопрос.) Однако после 2006 г. вышли новые важные статьи, в которых подвергаются сомнению предположения, положенные в основу модели Дойча, и предложены альтернативные модели, что, как правило, ведет к вычислительной мощности *меньшей,* чем **PSPACE.** К примеру, одна из моделей, предложенная Ллойдом с соавторами, «всего лишь» позволит путешественнику во времени решить все задачи класса **PP**! Об этих достижениях речь пойдет на с. 436–440.

А что с нижними оценками сложности схемы (для специалистов по теоретической информатике это, по существу, кодовое слово, обозначающее «попытку доказать **P** $\neq$ **NP**», точно так же как для физиков «замкнутые времени подобные траектории» — кодовое слово для обозначения путешествий во времени)? Рад сообщить, что и здесь после 2006 г. имеются интересные подвижки — безусловно, более серьезные, чем можно было тогда ожидать. В качестве примера скажу, что Рахул Сантханам при помощи интерактивных методик доказательства

* T. Ito and T. Vidick, A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers. In *Proceedings of IEEE Symposium on Foundations of Computer Science* (2012), pp. 243–252.

получил нерелятивизирующий результат, согласно которому класс **PromiseMA** не имеет схем какого бы то ни было фиксированного полиномиального размера (см. с. 358). Результат Сантханама, в частности, побудил меня и Ави Вигдерсона в 2007 г. сформулировать теорему о *барьере алгебраизации* (см. там же) — обобщение теоремы о барьере релятивизации Бейкера, Гилла и Соловея, сформулированной еще в 1970-е гг. (см. с. 343–344). Алгебраизация объясняет, почему методики интерактивного доказательства в попытке доказать $\mathbf{P} \neq \mathbf{NP}$ позволяют нам лишь дойти до определенного предела и не более того — к примеру, почему эти методики привели к сверхлинейной нижней оценке сложности схемы для класса **PromiseMA,** но не для класса **NP**, который всего лишь «чуть ниже его». Мы поставили задачу разработки новых методик поиска нижней оценки сложности схемы, которые позволяли бы убедительно *обойти* барьер алгебраизации. Эту задачу решил в 2010 г. Райан Уильямс своим прорывным доказательством того, что $\mathbf{NEXP} \not\subset \mathbf{ACC}^0$ (речь об этом идет на с. 362).

Конечно, даже интереснейший результат Уильямса чертовски далек еще от доказательства $\mathbf{P} \neq \mathbf{NP}$. Но в последние шесть лет наблюдается еще и растущий интерес — и, соответственно, прогресс — к программе создания геометрической теории сложности Кетана Мулмулея (см. с. 363–364); теория эта играет для доказательства $\mathbf{P} \neq \mathbf{NP}$ почти в точности ту же роль, что теория струн в физике для цели создания Теории Всего. То есть, если говорить о конкретных результатах, программа геометрической теории сложности пока даже отдаленно не приблизилась к конечному результату, и даже самые рьяные ее сторонники предсказывают несколько десятилетий кропотливой работы, тогда как остальных просто отпугивает ее математическая сложность. В активе этой программы две вещи: во-первых, то, что она создает математические связи, «слишком глубокие и поразительные, чтобы их можно было считать простым совпадением», и во-вторых, то, что (хотя так считают далеко не все!) на безрыбье и рак рыба и что это

единственный реальный претендент на успех, имеющий хоть какие-то шансы.

Позвольте мне упомянуть еще три открытия, сделанных после 2006 г. и важных для содержания этой книги.

В 2011 г. мы с Алексом Архиповым предложили «бозонную выборку» (см. с. 396–397) — рудиментарную, почти наверняка *не* универсальную модель квантовых вычислений с участием невзаимодействующих фотонов, которая совсем недавно была продемонстрирована в небольшом масштабе. Уверенность в том, что бозонную выборку трудно смоделировать на классическом компьютере, кажется, даже выше, чем в том, что трудно смоделировать (к примеру) алгоритм Шора разложения на множители.

В 2012 г. Умеш Вазирани и Томас Видик, опираясь на более ранние работы Пиронио с соавторами, показали, как можно использовать нарушения неравенства Белла для достижения *экспоненциального расширения случайности* (см. с. 418), то есть превращения $n$ случайных бит в $2n$ бит, которые гарантированно будут почти совершенно случайными, *если только* Природа не воспользуется сверхсветовой связью, чтобы их изменить.

Тем временем дебаты об «информационном парадоксе черной дыры» — то есть об очевидном конфликте между принципами квантовой механики и локальностью пространства-времени, когда биты и кубиты падают в черную дыру, — развивались с 2006 г. в новых направлениях. Самыми, возможно, важными достижениями здесь стали возросшая популярность и подробность модели черной дыры как «пушистого клубка», выдвинутой Самиром Матхуром, и спорное утверждение Алмхейри с соавторами о том, что наблюдатель, падающий в черную дыру, никогда даже не приблизится к сингулярности, а встретит на своем пути «огненную стену» и сгорит на горизонте событий. Я в меру своих сил расскажу об этих достижениях на с. 471–475.

Несколько дополнений и изменений в книге объясняются не какими-то новыми открытиями или аргументами, а просто