Машины, логика и квантовая физика

Д. Дойч А. Экерт Р. Лупачини

Хотя истины логики и чистой математики объективны и не зависят от известных нам фактов или законов природы, наше *знание* этих истин существенно зависит от знания физических законов. Подтверждением тому служит недавний прогресс в квантовой теории вычислений, вынуждающий отказаться от классической точки зрения на вычисление (а, следовательно, и на математическое доказательство) как на чисто логическое понятие, не зависящее от физической природы вычисления. Отныне доказательство должно рассматриваться не как абстрактный объект или процесс, а как физический процесс (разновидность вычисления), результаты и достоверность которого зависят от нашего знания физики используемого вычислительного устройства.

1. Математика и физический мир

Подлинно научное[1)] знание не имеет априорного обоснования. Оно должно формулироваться как гипотеза, проверяемая впоследствии экспериментом. Поэтому знания нужно выражать на языке, пригодном для высказывания точных, эмпирически проверяемых утверждений. Таким языком является математика.

Само признание возможности получения научных (в указанном выше смысле) знаний уже приводит к определённым представлениям о физическом мире. Как говорил Галилей: «Вселенная написана на языке математики» [5]. Введение Галилеем в физику математически формулируемых, эмпирически проверяемых теорий означало переход от аристотелевского понимания физики, основанного на априорных принципах, к современному статусу естественной науки. Вместо поисков непогрешимого универсального математического плана мироздания галилеева наука использует математику для выражения количественных предсказаний, относящихся к объективной физической реальности.

Итак, математика — язык описания наших знаний о физическом мире. Язык этот не только необычайно выразителен и точен, но и эффективен в практических приложениях. Юджин Вигнер обращал внимание на «непостижимую эффективность математики в физических науках» [12]. Но так ли уж непостижима или сверхъестественна эта эффективность?

Посмотрим, как мы изучаем математику. Имеем ли мы, точнее, наш мозг, прямой доступ к миру абстрактных понятий и отношений между ними? (В это верил Платон, а сейчас такую точку зрения защищает Роджер Пенроуз [8].) Или

http://xxx.lanl.gov/math.HO/9911150 Перевод с незначительными сокращениями. Переводчик М. Н. Вялый.

[1)] По-русски обычно говорят — естественно-научное. *Прим. пер.*

мы изучаем математику опытным путём, взаимодействуя с физическими объектами? Мы склоняемся ко второму варианту. Это не означает, что математические сущности являются в каком-либо смысле частью физического мира или производны от него. Мы не отрицаем особую, не зависящую от предписаний законов природы, реальность чисел, множеств, групп и алгебр. Их свойства вполне объективны, как и полагал Платон. Но даны нам эти структуры только через физический мир. Лишь физические объекты, будь то компьютер или человеческий мозг, дают нам возможность заглянуть в абстрактный мир математики. Но как?

С незапамятных времен известно, что простые физические системы (пальцы, счётные палочки или счёты) можно использовать для представления некоторых математических сущностей и действий. Исторически именно арифметические действия удалось первыми поручить машинам. Как только стало ясно, что сложение и умножение можно разбить на последовательность базисных процедур, реализуемых физическими операциями, механические устройства, изобретённые Блезом Паскалем, Готфридом Вильгельмом Лейбницем и другими, начали освобождать людей от утомительных работ вроде перемножения двух больших чисел [6]. В XX веке следом за арифметикой удалось механизировать и логическое понятие вычислимости. Чтобы формализовать понятие «эффективности», подразумеваемое в интуитивном представлении о вычислимости, были изобретены машины Тьюринга. Алан Тьюринг предположил, что те абстрактные машины, с помощью которых он определил вычисление, способны выполнить любую *конечную эффективную* процедуру (алгоритм). Стоит отметить, что машины Тьюринга задумывались так, чтобы воспроизвести любое точно определённое действие, на которое способен *человек-вычислитель*, следующий предписанным инструкциям. Метод Тьюринга состоял в том, чтобы думать в терминах физических действий и представлять каждое действие, выполняемое вычислителем как «некоторое изменение физической системы, состоящей из вычислителя и его ленты» [11]. Поскольку результат работы не зависит от способа построения «машины для выполнения работы этого вычислителя», эффективность человека-вычислителя может быть имитирована логической машиной.

Машина Тьюринга была абстрактным понятием, но благодаря последующему прогрессу алгоритмы сейчас исполняются реальными вычислительными устройствами. Возникает естественный вопрос: какие логические процедуры может исполнить физическое устройство? Теория машин Тьюринга принципиально не может ответить на этот вопрос, равно как и любой подход, основанный на формализации традиционных представлений об эффективных процедурах. Вместо этого нужно обобщить идею Тьюринга о *механизации* процедур, в частности, процедур, связанных с понятием выводимости. Это позволило бы определить математическое доказательство как нечто механически воспроизводимое и за счёт этого эффективно проверяемое. Универсальность и достоверность логических процедур гарантируются при таком подходе наличием механических процедур, эффективно выполняющих логические действия. И не более того. Но что значит включить реальные физические машины в определение логического понятия? И что можно из этого заключить, в противоположность Вигнеру, об «эффективности физики в математических науках»?

Абстрактные модели машин, используемые в классической теории вычислений, являются чисто математическими понятиями, которым можно приписать любые не противоречащие друг другу свойства. Изучение реальных вычислительных устройств как физических объектов должно учитывать их физические свойства и потому опираться на законы природы. Машины Тьюринга (с произвольно длинными лентами) можно построить, но никто этого не делал, разве что шутки ради. Они были бы очень медленными и громоздкими. Имеющиеся сейчас компьютеры куда лучше. Но почему мы уверены, что компьютер порождает тот же выход, что и соответствующая абстрактная машина Тьюринга? Или даже, почему, покрутив ручку арифмометра, мы увидим в итоге правильный ответ? Ведь никто не проверяет машину, следуя за всеми возможными логическими шагами, или делая все вычисления, которые она может выполнить. Прежде всего, если бы у кого-то была возможность и желание делать такие проверки, не было бы нужды в изготовлении компьютеров. Причина, по которой мы доверяем машине, не может основываться целиком на логике, она также включает в себя наше знание природы этой машины. Мы опираемся на законы физики, управляющие вычислением, т. е. физическим процессом, который переводит машину из начального состояния (вход) в конечное состояние (выход). Более того, наш анализ опирается на физические теории, которые подтверждаются или опровергаются экспериментально. С этой точки зрения Тьюринг на самом деле предположил, что возможно сконструировать универсальный компьютер: машину, которую можно запрограммировать на любое вычисление, доступное какому-либо физическому объекту. Другими словами, возможно построение одного физического объекта, способного, при надлежащем обслуживании, источнике энергии и расширении памяти при необходимости, точно имитировать поведение и реакции любого другого физически возможного объекта или процесса. Гипотеза Тьюринга в этой форме (в аналогичном контексте Дойч назвал её принципом Чёрча – Тьюринга [3]) может рассматриваться как утверждение о физическом мире.

Есть очевидные и логические, и физические ограничения на возможные вычисления. Например, логика говорит нам, что никакая машина не найдёт более одного чётного простого числа, в то время как физика утверждает, что никакая машина не может нарушить законы термодинамики. Логические и физические ограничения по сути связаны между собой, как показывает «проблема остановки». Из логического анализа следует несуществование алгоритма, который определяет, остановится ли данная машина, начинающая работу из данного состояния. С физической точки зрения это означает, что некоторые машины нельзя создать. Сформулированная таким образом, проблема остановки становится утверждением о физической реальности.

Так откуда же берётся эффективность математики? Это не просто чудо, «восхитительный дар, который мы не понимаем, и которого мы не заслуживаем» [12]. По крайней мере, это не большее чудо, чем способность к постижению *эмпирического* знания. Наше знание математики и логики неразрывно сплетено со знанием о физической реальности: приемлемость математического доказательства зависит от того, как мы представляем правила, которым подчиняются некоторые физические объекты, такие как компьютеры или человеческий мозг. Следовательно, прогресс в понимании физической реальности может дать

средства для улучшения понимания логики, математики и формальных понятий. Так что мы вынуждены признать зависимость математического *знания* от физики (но, подчеркнём ещё раз, не математических истин самих по себе). А раз так, пора отказываться от классической точки зрения на вычисление как на чисто логическое понятие, не зависящее от физической природы вычислителя. Ниже мы покажем как, в частности, квантовая механика меняет понимание природы вычисления.

2. Квантовая интерференция

Чтобы объяснить разницу между квантовыми компьютерами и их классическими аналогами, начнём с явления квантовой интерференции. Рассмотрим вычислительное устройство (машину), чьим входом может быть одно из двух состояний, помеченных 0 и 1.

Эта машина преобразует вход a (0 или 1) в выход b (0 или 1) с вероятностью p_{ab}. Кажется очевидным, что рис. 1 (вероятности p_{ab} должны удовлетворять стандартному условию $\sum_b p_{ab} = 1$) описывает все устройства, отображающие $\{0,1\}$ в себя. (Действие машины не зависит от иной информации, подаваемой на вход или хранящейся в памяти.) Есть два предельных случая, когда

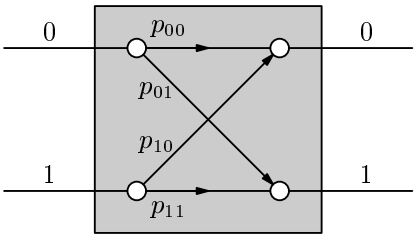

Рис. 1. *Схема наиболее общего устройства, отображающего* $\{0,1\}$ *в себя*

поведение устройства детерминировано: при $p_{01} = p_{10} = 0$, $p_{00} = p_{11} = 1$ (тождественное преобразование) и при $p_{01} = p_{10} = 1$, $p_{00} = p_{11} = 0$ (отрицание **not**). В остальных случаях имеем устройство со случайным поведением. Пусть, к примеру, $p_{01} = p_{10} = p_{00} = p_{11} = 0{,}5$. Вновь кажется очевидным, что единственный вид такой машины, это случайный переключатель, равновероятно преобразующий каждый вход в один из двух возможных выходов. Однако это не так. Мы имеем в виду машину, удовлетворяющую тому же свойству, но такую, что при последовательном соединении двух одинаковых экземпляров её на выходе всегда получается отрицание входа (рис. 2).

Это утверждение радикально противоречит интуиции. Каждая машина по отдельности выдаёт 0 или 1 равновероятно и независимо от входа, но две последовательно соединённые машины реализуют логическую операцию **not**. По этой причине назовём такую машину $\sqrt{\textbf{not}}$. В логике такой операции нет, так что разумно предположить, что машина $\sqrt{\textbf{not}}$ не существует. Но на самом деле такая машина в природе есть! Для физика, изучающего одночастичную интерференцию, построение такой машины — обычное дело. Простейший вариант —

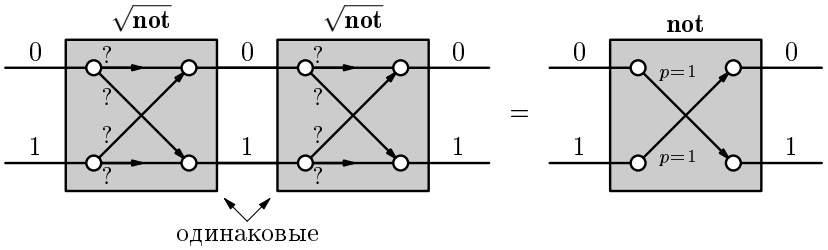

Рис. 2. *Последовательное подключение двух одинаковых машин, отображающих* $\{0,1\}$ *в себя, каждая из которых работает как случайный переключатель. При последовательном подключении случайность исчезает: суммарный эффект есть логическая операция* **not**. *Это очевидным образом противоречит аксиоме аддитивности теории вероятностей!*

полупрозрачное зеркало, т. е. зеркало, с вероятностью 50% отражающее падающий на него фотон, и с вероятностью 50% пропускающее его. Последовательное соединение двух этих машин реализуется двумя полупрозрачными зеркалами, при этом фотон означает 0, если он находится на одном из двух возможных путей, и 1 в противном случае.

Читатель может поинтересоваться, что делать с аксиомой аддитивности теории вероятностей, утверждающей про пару несовместных событий E_1 и E_2, что вероятность события E_1 **or** E_2 есть сумма вероятностей событий E_1, E_2. Ведь переход $0 \to 0$ в составной машине может происходить двумя взаимоисключающими способами: либо $0 \to 0 \to 0$, либо $0 \to 1 \to 0$. Их вероятности $p_{00}p_{00}$ и $p_{01}p_{10}$ соответственно, значит, сумма $p_{00}p_{00}+p_{01}p_{10}$ равна вероятности перехода $0 \to 0$ в новой машине. Она отлична от нуля, если p_{00} или $p_{01}p_{10}$ отлично от нуля.

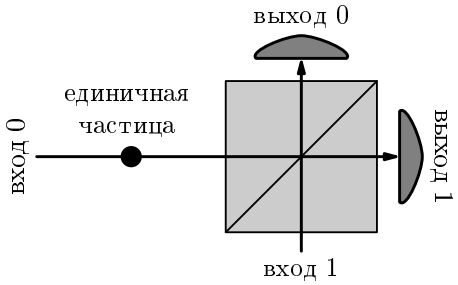

Рис. 3. *Экспериментальная реализация элемента* $\sqrt{\textbf{not}}$. *Полупрозрачное зеркало отражает половину падающего на него света. Но единичный фотон не расщепляется: когда мы посылаем фотон сквозь такое зеркало, регистрируются выход 0 или выход 1 с равными вероятностями. Не нужно думать, однако, что фотон проходит зеркало по одному из двух случайно выбранных путей, он идёт по обоим путям! В этом можно убедиться, соединяя последовательно два полупрозрачных зеркала, как показано на следующем рисунке*

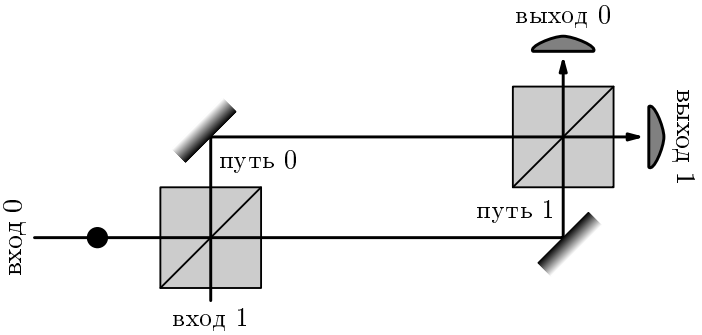

Рис. 4. *Одночастичная интерференция — экспериментальная реализация двух соединённых последовательно элементов* $\sqrt{\mathbf{not}}$. *Фотон, который входит в интерферометр через вход 0, всегда попадает в детектор у выхода 1 и никогда в детектор у выхода 0*

И тем не менее мы построили машину, в которой p_{00} и $p_{01}p_{10}$ не равны нулю, а вероятность перехода $0 \to 0$ в составной машине равна нулю. Что же неверно в приведённом рассуждении?

Неверно то, что процессы $0 \to 0 \to 0$ и $0 \to 1 \to 0$ взаимно исключают друг друга. Любое объяснение, которое предполагает, что фотон избирает один из двух путей по интерферометру, приводит к выводу, что каждый из детекторов должен срабатывать в среднем в половине случаев. Но эксперимент показывает обратное! Так что на самом деле происходят оба перехода одновременно. Это нельзя получить ни из теории вероятностей, ни из любой другой математической конструкции. Такое знание можно получить из наилучшей имеющейся в настоящий момент физической теории, а именно, квантовой механики. Квантовая теория объясняет поведение $\sqrt{\mathbf{not}}$ и правильно предсказывает вероятности для всех возможных выходов при любых способах соединения таких машин. Это знание возникло как результат гипотез, экспериментов и опровержений. Следовательно, на основании физических экспериментов, подтверждающих эту теорию, логики вправе ввести новую логическую операцию $\sqrt{\mathbf{not}}$, поскольку физическая модель для неё существует в природе!

Рассмотрим теперь математический аппарат квантовой механики, с помощью которого описываются квантовые вычислительные устройства: от простейших, таких как $\sqrt{\mathbf{not}}$, до самых сложных — квантового обобщения универсальной машины Тьюринга.

Квантовая механика вводит понятие *амплитуд вероятности* — комплексных чисел c, квадраты модуля которых $|c^2|$ при некоторых обстоятельствах можно понимать как вероятности. Когда некоторый переход, наподобие рассмотренного выше, может происходить несколькими способами, его амплитуда вероятности есть сумма амплитуд вероятности по всем возможным способам, рассматриваемым порознь.

Вероятности переходов в машине $\sqrt{\mathbf{not}}$ изображены на рис. 5. Эта машина сохраняет значение бита с амплитудой вероятности $c_{00} = c_{11} = i/\sqrt{2}$, меняет

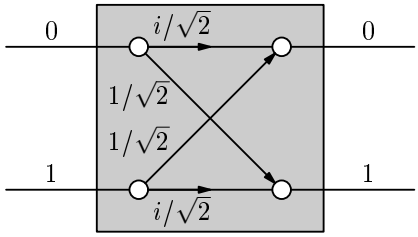

Рис. 5. *Переходы в квантовых машинах описываются не вероятностями, а амплитудами вероятности*

на противоположное — с амплитудой $c_{01} = c_{10} = 1/\sqrt{2}$. Соответствующие вероятности получаются возведением в квадрат модулей амплитуд вероятности, в каждом из случаев получаем $1/2$. Этим объясняется поведение $\sqrt{\mathbf{not}}$ на рис. 1. При последовательном соединении машин, как на рис. 2, для подсчёта вероятности выхода 0 при входе 0 нужно сложить амплитуды вероятности по всем путям, ведущим от входа 0 к выходу 0. Таких две: $c_{00}c_{00} = -1/2$ и $c_{01}c_{10} = 1/2$. Их сумма равна 0, так что и вероятность выхода 0 равна 0. В отличие от вероятностей, амплитуды могут взаимно сокращаться!

3. Квантовые алгоритмы

Сложение амплитуд вероятности вместо вероятностей является одним из основных правил квантовой механики и применимо ко всем физическим объектам, в том числе, и к квантовым вычислительным устройствам. Если вычисляющая машина начинает работать в заданной начальной конфигурации (вход), то вероятность того, что она, проходя через ряд промежуточных конфигураций, закончит работу в заданной конечной конфигурации (выход), равна квадрату модуля суммы амплитуд вероятности по всем вычислительным путям, соединяющим вход с выходом. Амплитуды — это комплексные числа. При сложении они могут взаимно сокращаться (*деструктивная интерференция*) или увеличиваться по абсолютной величине (*конструктивная интерференция*). Основная идея квантового вычисления состоит в том, чтобы усилить правильные ответы и подавить неправильные. Мы покажем это на примере одного из вариантов первого квантового алгоритма, предложенного Д. Дойчем в 1985 г.

Рассмотрим булевы функции f, отображающие $\{0,1\}$ в себя. Есть ровно четыре таких функции: две постоянных ($f(0) = f(1) = 0$ и $f(0) = f(1) = 1$) и две биекции ($f(0) = 0$, $f(1) = 1$ и $f(0) = 1$, $f(1) = 0$). Предположим, что можно вычислить значение функции *только один раз* (потому, например, что алгоритм вычисления функции очень длинный, или потому, что к таблице её значений позволено обратиться только один раз). Нужно определить, является ли f биекцией. Заметим, что конкретные значения f нас не интересуют, мы проверяем некоторое глобальное свойство функции f. Наша классическая интуиция подсказывает, а классическая теория вычислений подтверждает, что для проверки этого свойства нужно вычислить оба значения $f(0)$ и $f(1)$, т. е. вычислять f дважды. Однако это неверно в реальном физическом мире, в котором можно

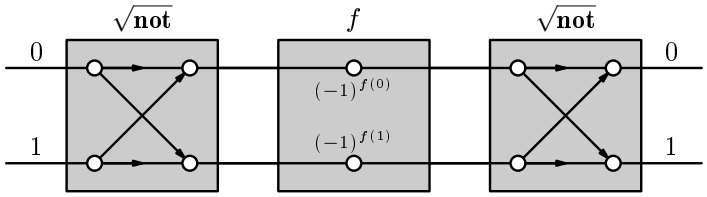

Рис. 6. *Схема квантовой машины, решающей задачу Дойча за одно вычисление функции*

осуществить квантовое вычисление, решающее задачу Дойча и вычисляющее значение f только раз. Машина, решающая эту задачу, использует квантовую интерференцию и состоит из двух $\sqrt{\mathbf{not}}$, между которыми вставлено вычисление значения функции (рис. 6).

Нам нет нужды вдаваться в подробности реализации $f(x)$. Для нашего примера достаточно указать, что есть два пути, индексированные 0 и 1, а действие машины, реализующей $f(x)$, заключается в том, что амплитуда вероятности на пути x умножается на фазовый множитель $\exp(\pi i f(x))$, т. е. на $(-1)^{f(0)}$ (на пути 0) и на $(-1)^{f(1)}$ (на пути 1). Теперь подсчитаем амплитуду вероятности выхода 0 при входе 0. Амплитуды вероятности на двух различных вычислительных путях равны $i/\sqrt{2} \times (-1)^{f(0)} \times i/\sqrt{2} = -1/2 \times (-1)^{f(0)}$ и $1/\sqrt{2} \times (-1)^{f(1)} \times 1/\sqrt{2} = 1/2 \times (-1)^{f(1)}$. Их сумма

$$\frac{1}{2}\left((-1)^{f(1)} - (-1)^{f(0)}\right), \tag{1}$$

равна 0, если f — постоянная, и ± 1, если f — биекция. Итак, вероятность (квадрат модуля амплитуды) выхода 0 на входе 0 равна 0 для постоянных функций и 1 для биекций.

С этого результата Дойча началась новая область исследований: квантовые вычисления. Последовательная работа по улучшению квантовых алгоритмов привела в 1994 г. к открытию Питером Шором квантового алгоритма, способного эффективно факторизовать числа [10]. А поскольку трудность факторизации лежит в основе надёжности многих известных криптографических систем, включая наиболее популярную криптосистему с открытым ключом RSA [9][2)], алгоритм Шора быстро стал популярен как первое “killer application” для квантового вычисления — нечто весьма полезное, что может делать только квантовый компьютер.

Мало кто из специалистов сомневается в том, что факторизация не принадлежит классу **BPP** (**BPP** означает «вероятностное вычисление за полиномиальное время с ограниченной вероятностью ошибки»). Интересно, однако, что это не доказано. В теории вычислительной сложности обычно трактуют принадлежность задачи классу **BPP** как указание на её «несложность» или «практическую

[2)] В декабре 1997 г. британское правительство официально признало, что эта криптосистема с открытым ключом была изначально изобретена в Центре Правительственных Коммуникаций (GCHQ) в Челтенхэме. В 1975 году Джеймс Эллис, Клиффорд Кокс и Малькольм Вильямсон из GCHQ открыли то, что позднее было переоткрыто в академической науке и стало известно как RSA и обмен ключами Диффи – Хэллмана. — *Прим. авт.*

разрешимость», а задачи, не принадлежащие **BPP**, напротив, понимаются как «трудные» или «нерешаемые на реальных компьютерах» (см., например, [7][3)]). Алгоритм из класса **BPP** — это такой эффективный (= быстрый) алгоритм, который на любом входе даёт правильный ответ с вероятностью, превышающей некоторый порог $\delta > 1/2$. Мы, вообще-то, не можем проверить правильность ответа. Но можно повторить все вычисление k раз и взять тот ответ, который встретился чаще всего. Увеличивая k, можно добиться вероятности правильного ответа, сколь угодно близкой к 1.

Результат Шора показывает, что в реальности, описываемой квантовой физикой, факторизация не является трудной задачей.

Еще Ричард Фейнман, выступая на первом конгрессе по физике вычислений в MIT (1981 год), заметил, что эволюцию общей квантовой системы скорее всего нельзя эффективно моделировать на классическом вероятностном компьютере [4]. Количество классической информации, требуемой для описания квантового состояния эволюционирующей системы, растет экспоненциально по времени, так что лобовое классическое моделирование эволюции происходит с экспоненциальным замедлением. Фейнман же предложил рассматривать этот факт не как препятствие, а как возможность. В самом деле, раз результат эксперимента по многочастичной интерференции описывается сложными и длинными вычислениями, то сам эксперимент и измерение выхода в нем равносильно выполнению некоторого сложного вычисления. Далее Фейнман предположил, что возможно эффективное моделирование квантовой эволюции, если само моделирующее устройство подчиняется законам квантовой механики. Более того, Фейнман предположил, что существует универсальное квантовое устройство, пригодное для моделирования квантовой эволюции произвольной системы. В 1985 году Дойч показал, что такое устройство (универсальный квантовый компьютер) действительно существует [3]. Тогда же было показано, что время и другие требуемые ресурсы не растут экспоненциально в зависимости от размера или степени точности описания моделируемой физической системы, так что такое моделирование является «эффективным» по стандартам теории сложности вычислений [1].

Это и есть иллюстрация нашей основной мысли: чем больше мы знаем о физике, тем больше можем узнать о вычислениях и математике. Только используя квантовую механику, удалось придумать, как эффективно решать задачу факторизации чисел; другого способа пока не найдено, а, возможно, его и вовсе нет.

4. Детерминированные, вероятностные и квантовые компьютеры

Любой квантовый компьютер, включая и универсальный, можно описать так же, как мы описывали выше простые примеры машин, меняя вероятности на амплитуды вероятности. Начнем с классической машины Тьюринга. Она задается конечным набором пятерок вида

$$(q, s, q', s', d), \tag{2}$$

[3)] Или предыдущий номер «Математического просвещения». *Прим. пер.*

в которых первые два символа описывают условие на применимость данного шага вычислений, а последние три — результат применения данной команды (q — текущее состояние, s — прочитанный в данный момент символ, q' — состояние, в которое переходит машина, s' — символ, которым заменяется s, d указывает сдвиг головки относительно ленты (на один символ влево или вправо, или остаться на месте)). На этом языке вычисление описывается так. Машине на вход подается конечное слово в алфавите Σ, записанное в ячейках ленты, затем машина начинает работу из начального состояния q_0 (читающая головка стоит над самым левым символом входа, выполняет последовательно элементарные действия, описанные выше, и останавливается при достижении финального состояния q_h. (При некоторых входах вычисление может продолжаться бесконечно.) Результат вычисления определяется как содержимое некоторой указанной части ленты после достижения финального состояния (если этого не случится, результат вычисления не определен)).

При вычислении возникает последовательность конфигураций машины (слово, записанное на ленте, состояние головки и ее положение на ленте). Например, начальная конфигурация описывается входным словом, состоянием q_0 и положением головки над самым левым символом входа. Конфигураций бесконечно много, однако в успешном вычислении машина проходит лишь через конечное количество конфигураций. Переходы между конфигурациями полностью описываются пятерками (2).

Рис. 7. *Трехшаговое детерминированное вычисление*

Вычисления, вообще говоря, не обязаны быть детерминированными. Мы можем расширить возможности машины Тюринга, добавляя «подбрасывание монеты», что позволяет выбирать ей следующий шаг случайно. Такое вероятностное вычисление можно представлять ациклическим ориентированным графом с корнем, каждая вершина которого соответствует некоторой конфигурации машины, а ребро — одному шагу вычисления. Вычисление начинается с корня, представляющего начальную конфигурацию, каждая его ветвь ведет в вершины, отвечающие конфигурациям, достижимым из начальной с ненулевой вероятностью. Работа машины полностью задается конечным списком вида

$$\delta\colon Q \times \Sigma \times Q \times \Sigma \times \{\text{влево, вправо, на месте}\} \mapsto [0,1], \tag{3}$$

где $\delta(q, s, q', s', d)$ задает вероятность того, что будет выполнено действие, описываемое пятеркой (q, s, q', s', d). Это описание должно согласовываться с законами теории вероятностей. Каждому ребру дерева вычислений можно сопоставить вероятность перехода по этому ребру, и нужно потребовать, чтобы сумма вероятностей на ребрах, выходящих из данной вершины, равнялась 1. Вероятность пути из корня в данную вершину есть произведение вероятностей ребер, входящих в этот путь, а вероятность перехода в заданную конфигурацию после n шагов равна сумме вероятностей путей длины n, соединяющих начальную и заданную конфигурации.

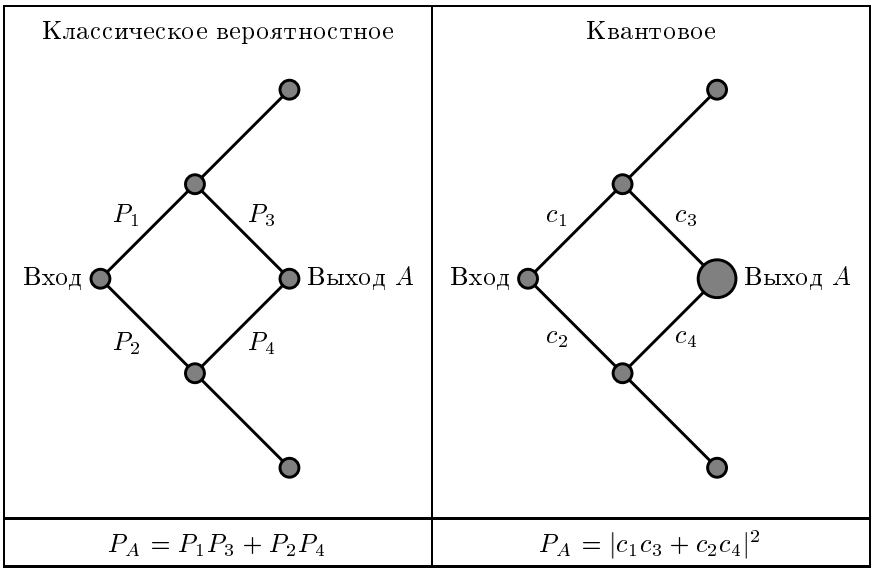

Рис. 8. *В вероятностной машине (слева) вероятность выхода A есть сумма вероятностей вычислений, ведущих в A. В квантовой машине (справа) вероятность выхода A получается сложением амплитуд вероятности и взятием квадрата модуля полученной суммы. Так что в квантовом случае возможны как конструктивная (вероятности усиливаются), так и деструктивная (вероятности гасятся) интерференция*

Есть вероятностные алгоритмы, которые решают некоторые задачи (со сколь угодно близкой к 1 вероятностью успеха) гораздо быстрее, чем все известные детерминированные алгоритмы.

Описанная выше классическая модель подсказывает естественное квантовое обобщение. Квантовое вычисление можно представлять ориентированным ациклическим графом, как и классическое. Каждому ребру этого графа мы сопоставим амплитуду вероятности того, что вычисление пойдет по этому ребру. Как и выше, амплитуда вероятности пути есть произведение амплитуд вероятности по ребрам этого пути, а амплитуда вероятности заданной конфигурации — сумма амплитуд вероятности по всем путям, ведущим из начальной конфигурации в заданную. Если, в частности, финальная конфигурация достижима ровно по двум путям с амплитудами c и $-c$, вероятность попадания в эту конфигурацию $|c - c|^2 = 0$, несмотря на то, что вероятность того, что вычисление пойдет по любому из этих двух путей, равна $|c^2|$. Один-единственный квантовый компьютер может следовать по многим вычислительным путям одновременно и его выход определяется интерференцией всех этих путей. Напротив, классическая вероятностная машина Тьюринга следует по *единственному* (хоть и случайно выбранному) пути вычисления. Работа квантовой машины полностью задается конечным списком вида

$$\delta\colon Q \times \Sigma \times Q \times \Sigma \times \{\text{влево}\,, \text{вправо}\,, \text{на месте}\} \mapsto \mathbb{C}, \tag{4}$$

где $\delta(q, s, q', s', d)$ задает амплитуду вероятности выполнения действия, описываемого пятеркой (q, s, q', s', d).

5. Дальнейшие следствия

Когда в начале 60-х годов начинали изучать физику вычислений, одним из основных стимулов было опасение, что квантовомеханические эффекты могут давать фундаментальные (=неустранимые) границы на точность, с которой физические объекты могут воспроизводить свойства абстрактных сущностей, таких как логические переменные и операции в теории вычислений. То есть боялись, что мощь и элегантность теории вычислений, такие ее понятия, как вычислительная универсальность, такие ее фундаментальные принципы, как тезис Чёрча – Тьюринга, равно как и более мощные результаты в современной теории сложности, окажутся не более чем плодами математического воображения, не имеющими отношения ни к чему в природе.

Эти опасения оказались беспочвенными. Квантовая механика не только не накладывает ограничений на возможности машин Тьюринга, но и дает новые возможности вычислений, обсуждавшиеся выше. Сохранилась элегантность теории, более того, оказалось, что квантовая теория вычислений весьма естественно сочетается с фундаментальными теориями в других областях, чего было трудно даже ожидать от классического приближения. Само слово «квант» означает то же самое, что и «бит» — элементарный кусочек — это замечательным образом согласуется с тем фактом, что классические физические системы, будучи подвержены неустойчивости общего вида, именуемой «хаос», не могут в принципе поддерживать цифровое вычисление (так что даже машины Тьюринга, теоретический образец всех классических компьютеров, всегда имели квантовомеханический характер, о чем умалчивалось). Тезис Чёрча – Тьюринга в классической теории (об эквивалентности всех «естественных» моделей вычисления) никогда не был доказан. Его аналог в квантовой теории вычислений (принцип Чёрча – Тьюринга, утверждающий, что универсальный квантовый компьютер способен моделировать поведение любой конечной физической системы) был доказан прямо из определения в работе Дойча 1985 года [3]. Более сильный результат (также предполагавшийся, но никогда не доказанный в классической теории), а именно, что такое моделирование возможно за время, зависящее полиномиальным образом от времени эволюции моделируемой системы, также был доказан в квантовом случае [1].

Наряду с прочими приложениями, квантовые вычисления существенно повлияли (по крайней мере, в принципе) на понятие математического доказательства. Выполнение вычисления, которое дает некоторый определенный результат, равносильно доказательству того, что наблюдаемый результат возможен при данном вычислении. Мы можем описать вычислительные операции математически, поэтому всегда можем перевести такое вычисление в доказательство некоторой теоремы. Так же обстоит дело и в классическом случае, но при отсутствии интерференции возможно сделать запись всех шагов вычисления, порождая таким образом доказательство, удовлетворяющее классическому определению — «цепочка утверждений, каждое из которых является аксиомой или следует из предыдущих утверждений в цепочке по правилам вывода» (правильность тако-

го доказательства также можно проверить пошагово). Теперь мы вынуждены отказаться от такого определения. Отныне доказательство должно рассматривать как процесс — вычисления самого по себе. Мы должны признать, что в будущем квантовые компьютеры будут доказывать теоремы методами, которые нельзя будет проверять пошагово, так как распечатка «цепочки утверждений», соответствующих этому доказательству, не поместится в наблюдаемой части Вселенной.

6. Заключительные замечания

В этом коротком обсуждении мы прошлись по самым верхам быстро развивающейся теории квантовых вычислений. Основное внимание было уделено принципиальным вопросам, оставляя в стороне физические подробности и нюансы технологической реализации. Стоит, однако, сказать, что квантовое вычисление — серьезная перспектива для будущих поколений вычислительных устройств. Это одна из причин, по которой квантовые вычисления привлекают все большее внимание как академических исследователей, так и промышленных кругов по всему миру. В настоящее время неясно когда, каким образом, да и будут ли вообще, реализованы полномасштабные квантовые компьютеры; но несмотря на это, уже сейчас квантовая теория вычислений играет гораздо более важную роль в общем понимании мира, чем ее классическая предшественница. Мы считаем, что всякий, кто добивается фундаментального понимания физики, вычислений или логики, должен учитывать достижения этой теории.

Список литературы

[1] *Bernstein E., Vazirani U.* Quantum complexity theory // Proc. of the 25th Ann. Symp. on the Theory of Comput. New York: ACM, 1993. P. 11–20.

[2] *Cleve R., Ekert A., Macchiavello C., Mosca M.* Quantum Algorithms Revisited // Proc. of the Royal Soci., A, 1998. Vol. 454. P. 339–354.

[3] *Deutsch D.* Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. of the Royal Soc., A, 1985. Vol. 400. P. 97–117.

[4] *Feynman R. P.* Simulating physics with computers // Int. J. of Theor. Physics, 1982. Vol. 21. P. 467-488.

[5] *Galilei G.* Saggiatore, 1623. / Opere. (Favaro A. (ed.)) Vol. 6. Firenze: Edizione Nazionale, 1896.

[6] *Goldstine H.H.* The Computer from Pascal to von Neumann. Princeton: Princeton University Press, 1972.

[7] *Papadimitriou C. H.* Computational Complexity. Reading: Addison-Wesley, 1994.

[8] *Penrose R.* Shadows of the mind. Oxford: Oxford University Press, 1994.

[9] *Rivest R., Shamir A., Adleman L.* On Digital Signatures and Public-Key Cryptosystems. Tech. Rep. MIT/LCS/TR-212. MIT Laboratory for Computer Science, January 1979.

[10] *Shor P.* Algorithms for quantum computation: discrete log and factoring // Proc. of the 35th Ann. Symp. on the Foundations of Computer Science, S. Goldwasser (editor). Los Alamitos: IEEE Computer Society Press, 1994. P. 124–134.

[11] *Turing A.* On computable numbers with an application to the Entscheidungsproblem // Proc. of the London Math. Soc., 2, 1936–37. Vol.42. P. 230–265.

[12] *Wigner E. P.* The unreasonable effectiveness of mathematics in the natural sciences // Comm. on Pure and Appl. Math., 1960. Vol. 13. P. 1–14.