Содержание

Введение

Сегодня всё больше и больше теоретических работ и даже практических разработок появляется в области так называемых квантовых вычислений, то есть новой вычислительной модели, которая вместо давно известного понятия бита (который, в свою очередь, пришёл к нам из работ Алана Тьюринга и Джона фон Неймана) основана на понятии «кубита», то есть квантового бита.

Квантовый бит – это некая квантовая система, которая до измерения находится в произвольной линейной суперпозиции двух базисных квантовых состояний (то есть, по сути, может принимать бесконечно большое разнообразие возможных значений), а в результате измерения с той или иной вероятностью принимает одно из двух возможных значений. Поэтому он и называется битом, поскольку возможных значений два, но, с другой стороны, он квантовый, поскольку эти два значений находятся в суперпозиции друг с другом.

Эта вычислительная модель в последнее время привлекает к себе всё больше и больше внимания как учёных, так и инженеров, поскольку её реализация, что называется, в «железе» откроет широчайшие возможности для решения задач, для которых в традиционной вычислительной модели не было вполне эффективных алгоритмов решения. Например, к таким задачам относится задача факторизации заданного числа, то есть поиска списка простых делителей этого числа (на гипотезе о невозможности быстро и эффективно найти разложение числа на простые множители основаны практически все современные методы криптографии). Есть ещё ряд задач такого же плана, решение которых в модели квантовых вычислений является полиномиальным, а не экспоненциальным, как в традиционной модели.

Это делает модель квантовых вычислений крайне интересной областью исследования. Однако, как это обычно бывает, основная масса исследований проводится за рубежом в университетах и исследовательских центрах западных стран. В России если и находятся энтузиасты, то все их работы «плетутся» в хвосте передовых исследований в данном перспективнейшем направлении. Связано это отчасти с тем, что методическая база для обучения специалистов у нас настолько устарела, что говорить о подготовке высококлассных специалистов в этой области просто не приходится.

Энтузиасты пользуются англоязычной литературой, которая часто настолько сложна для понимания просто в силу того, что западная

мысль уже далеко ушла вперёд, что нашему исследователю сложно найти и ухватить нить повествования. Небольшое количество переводной литературы не спасает дело. А вот наличие некоторого количества монографий и учебников по квантовым вычислениям на русском языке скорее удручает, чем восхищает. Дело всё в том, что для того, чтобы читать и понимать всю эту литературу на русском языке, необходимо полноценно владеть теорией модели квантовых вычислений. Получается замкнутый круг – научиться негде и не у кого, а для учёбы надо уже всё знать.

В какой-то мере разорвать этот порочный круг призвана данная небольшая книга, в которой даётся самое-самое введение в модель квантовых вычислений. Для её чтения необходимо лишь владеть острым умом, желанием научиться и идти дальше в самостоятельном поиске, иметь базовые знания в математике и понимание принципов функционального программирования. Желательно наличие знания языка Haskell, его синтаксиса и операционной семантики. Это поможет понимать примеры, которыми изобилует эта книга.

Я постарался как можно больше избегать формул, строгой математики и «жёсткого матана», насколько это вообще возможно при рассмотрении подобной темы. Все понятия объясняются на пальцах, как можно более наивно. Поэтому я сразу же прошу прощения у читателя, который знаком с моделью квантовых вычислений, – многие объяснения могут показаться настолько упрощёнными и наивными, что будут балансировать на грани «ликбеза». Но именно такова цель этой книги – дать объяснение новой вычислительной модели как можно более широкому кругу читателей.

Да, для чтения книги желательно, чтобы читатель был знаком с языком функционального программирования Haskell. Это связано с несколькими причинами. Во-первых, функциональное программирование в целом и язык Haskell в частности являются моей областью интереса и исследований. Пропаганда и распространение информации о языке Haskell – это то, чем я занимаюсь уже на протяжении многих лет. К тому же это единственный язык программирования, на котором я могу реализовывать программы, поэтому все примеры в этой книге волей-неволей пришлось писать именно на нём.

Во-вторых, функциональное программирование как парадигма разработки программного обеспечения самым гармоничным образом легла на модель квантовых вычислений, поскольку понятие «функция» включает в себя понятие «унитарное преобразование», используемое в модели квантовых вычислений. Так что в рамках

функционального программирования квантовые алгоритмы выражаются самым естественным образом. Поэтому нет никакого удивления в том, что современное предложение по реализации нового языка программирования Quipper, который используется для выражения квантовых вычислительных схем, полностью основано на языке Haskell.

Ну а в-третьих, есть одна важная особенность у модели квантовых вычислений. Разработать квантовый алгоритм – это значит настолько переформатировать себе мозги и «сдвинуть парадигму», что дальше уже просто нельзя. Квантовая механика по своей сути абсолютно **контр**интуитивна, и у нас нет никаких эмпирических навыков работы с бесконечномерными гильбертовыми пространствами и траекториями в них. И я считаю, что именно функциональное программирование наиболее близко из других способов программирования к парадигме квантовых вычислений. Расстояние от функционального до квантового программирования несколько короче, чем от любого иного.

Данная книга разбита на пять глав. В первой главе заинтересованному читателю предлагается описание модели квантовых вычислений, выраженное самыми простыми словами, которые только нашлись у меня. Из этой главы можно будет узнать, что такое кубит, как кубиты можно связывать друг с другом для получения многокубитовых состояний, что такое квантовая вычислительная схема и т. д. Прочитав эту главу, читатель сможет уже обратиться к более сложным источникам информации по квантовым вычислениям.

Вторая глава посвящена разработке фреймворка для выполнения квантовых вычислений на языке Haskell. Этот фреймворк позволяет решать многочисленные задачи по квантовым вычислениям и квантовой механике в целом. Реализация такого фреймворка позволяет более глубоко проникнуть в понимание модели квантовых вычислений, вынести «на пальцах» основные объекты и операции модели квантовых вычислений. После чтения этой главы, а особенно после самостоятельной работы с реализованным фреймворком, читатель сможет легко оперировать понятиями квантовых вычислений на практическом уровне. Но сам фреймворк будет дополняться по мере продвижения по тексту книги, особенно в четвёртой главе.

В третьей главе описывается новый язык программирования Quipper, который был разработан на базе языка Haskell для реализации квантовых алгоритмов. Приводятся описание языка, его синтаксис и несколько примеров реализации квантовых схем. После ознакомления с этой главой читатель будет знать об одной из самых

современных задач в рамках дальнейшей разработки модели квантовых вычислений в практическом русле. Несмотря на то что этот новый язык ещё не реализован в виде квантового компилятора и до реализации в «железе» ещё довольно далеко, он может быть одной из перспективнейших идей, которая будет реализована в ближайшем будущем.

Далее четвёртая и пятая главы посвящены описанию разработанных к настоящему времени квантовых алгоритмов. Не секрет, что в имеющейся литературе по квантовым вычислениям зачастую приводят описания двух или максимум трёх алгоритмов, которые разработаны к этому времени (алгоритм Дойча для распознавания сбалансированной функции, алгоритм Шора для факторизации и алгоритм Гровера для поиска – это тот самый максимум, что можно найти в современной литературе). Однако на сегодняшний момент разработано уже несколько десятков квантовых алгоритмов, и число это с каждым месяцем и годом растёт. Наверняка к моменту выхода этой книги в свет число разработанных квантовых алгоритмов увеличится, и описание уже станет неполным. Однако, ознакомившись с приведёнными в книге описаниями, читателю станет намного проще ориентироваться в имеющемся разнообразии алгоритмов. Соответственно, в четвёртой главе кратко описываются алгоритмы Гровера, Дойча (и Дойча-Йожи), Саймона и два алгоритма Шора (включая алгоритм квантового преобразования Фурье) как наиболее простые алгоритмы квантовой модели вычислений. А в пятой главе приводятся краткие описания других алгоритмов.

Поскольку литература по рассматриваемому вопросу очень немногочисленна, то я считаю своим долгом произвести более или менее полноценный обзор всего, что имеется на текущий момент на русском языке. В разделе «Обзор литературы о квантовых вычислениях» приводятся ссылки на литературу и краткая аннотация к каждой книге или иному материалу. Этот раздел будет полезен тем из читателей, кто хочет углубить свои знания в этой важной теме.

Ну и немаловажным и небезынтересным будет смежный раздел «Обзор видеокурсов по квантовым вычислениям и смежным темам», поскольку сегодня со всё большим и большим внедрением в повседневную жизнь новых методов обучения (так называемые MOOC – *Massive Open Online Courses*, то есть «массовые открытые онлайн-курсы») любому человеку становятся доступны знания в виде видеолекций и интерактивных обучающих программ по практически любому направлению знаний, в том числе и по квантовым вычисле-

ниям. Для того чтобы ориентироваться и иметь представление о правильном выборе, читатель может обратиться к этому разделу.

К книге прикладываются многочисленные файлы с исходными кодами на языке Haskell, которые описываются по тексту книги. Читателю будет интересно разобраться самостоятельно с теми примерами, которые приводятся, и приложенные файлы помогут ему в этом. В случае если вы получили эту книгу без приложенных к ней файлов с примерами, вы всегда можете обратиться ко мне по электронной почте (roman.dushkin@gmail.com), чтобы получить их.

Структура и стиль этой книги устроены так, что описание многих понятий вводится постепенно, как бы исподволь. Понимание концепций модели квантовых вычислений будет накатываться на читателя «волнами». И если в начале чтения книги может показаться, что что-то из написанного весьма непонятно, то дальше при изложении тех же понятий (возможно, иными словами и выражениями) понимание будет углубляться, расширяться и разъясняться. Я заранее прошу прощения у тех из читателей, кто сложно воспринимает подобный стиль, однако, по моему сугубому мнению, в данном издании именно он будет наиболее применим.

Я искренне надеюсь, что этот мой скромный труд даст начало новому направлению работы в нашем научном сообществе. Я буду рад всем конструктивным отзывам, комментариям, замечаниям и особенно благодарностям моих читателей.

В добрый путь!

Душкин Р. В.
Москва, 2014

Глава 1

Наивное понимание модели квантовых вычислений

Если вы думаете, что понимаете квантовую механику, значит, вы её не понимаете.

Ричард Фейнман

Книгу, текст которой вы читаете или просматриваете в настоящий момент (вы же вряд ли держите в руках бумажный экземпляр, но наверняка читаете с экрана или компьютера, или электронной книгочиталки), уважаемый читатель, вряд ли можно назвать книгой по квантовой механике. Здесь нет практически ничего из того, что обычно изучают в университетах на строгих курсах по «квантам», – всех этих уравнений Шрёдингера, Гейзенберга, Паули и т. д., фотоэффектов, парадоксов типа ЭПР, элементарных частиц и так называемой стандартной модели, квантования энергии и т. д., и т. п. Эта книга рассказывает о модели квантовых вычислений – новом способе осуществления вычислительных процессов таким образом, чтобы переложить на «квантовую природу» нашего мира возможность эффективной параллелизации вычислений. Квантовые вычисления – это пока лишь модель, которая ещё не нашла своего воплощения в «железе». Примерно так же воспринимали наши деды и прадеды вычислительную модель Тьюринга и фон Неймана, когда она только была разработана, – до полноценной реализации в «железе» тогда было ещё очень далеко (впрочем, некоторые пытались её реализовать в «дереве»).

В рамках кибернетики давно известен принцип, гласящий, что лучшей моделью системы является сама система. Видимо, используя именно этот принцип, Ричард Фейнман как-то выразил мнение,

что раз природа вокруг нас имеет квантово-механическую природу, то лучше всего её помогут смоделировать квантово-механические системы. Развивая эту мысль, можно сказать, что любое моделирование какого-либо физического процесса, выполненное при помощи современных средств вычислительной техники, будет неточным и неполным, но только лишь приближённым до какой-то степени точности, и у нас есть очень ограниченные средства повышения оной точности. В итоге любая такая модель так и останется неточной.

Однако если для моделирования использовать именно квантово-механические системы с внутренне присущей им неопределённостью и недетерминированностью, то такое моделирование позволит точно отразить те физические процессы, которые в своей основе являются абсолютно такими же – неопределёнными и недетерминированными. Это понимание и стало основой развития модели квантовых вычислений.

Другой момент, который необходимо отразить в преддверии описания модели квантовых вычислений, относится к пониманию математики как научного языка. В самом общем понимании математика оперирует символами, при этом интерпретация символов всецело зависит от решаемой задачи, но не от самих символов. Математика просто описывает алфавит, из которого можно создавать символы, задаёт систему аксиом и правил преобразования, при помощи которых можно оперировать символами чисто синтаксическим порядком. Именно так работает классический компьютер – «он» нисколько не понимает смысла производимых с битами (0 и 1) операций, «он» просто манипулирует символами. И даже наименования для битов «0» и «1» – это чистая условность, которая введена людьми для собственного удобства, поскольку компьютер манипулирует двумя различимыми состояниями.

Таким образом, математика – это система синтаксического манипулирования символами. Конечно, это несколько однобокое понимание, и в рамках математики есть системы, которые отрицают или расширяют такой подход. Но в целом именно этим и занимаются учёные-математики, и чем выше уровень абстракции символов, которыми они оперируют, тем меньше в них реального смысла и больше чистого синтаксиса.

Принимая во внимание оба описанных соображения, можно сказать, что квантовые вычисления – это некоторая математическая модель, формализм, помогающий в теории осуществить решение задач, которые сложно решить в традиционной модели вычислений за при-

емлемое время. Это достигается «автоматической» параллелизацией вычислительного процесса, что обусловлено квантово-механической природой модели.

Здесь необходимо отметить такой нюанс. Сама квантовая механика является всего лишь хорошо работающей теорией, которая позволяет прогнозировать (очень точно) результаты экспериментов и решать прикладные задачи. Узнать, действительно ли эта теория описывает наблюдаемую нами объективную реальность, невозможно. Но теория очень хорошо согласуется с практикой, и сегодня нет никаких причин отказываться от этой прекрасной теории, поскольку ничего более точного не разработано.

Таким образом, модель квантовых вычислений является неким подмножеством квантовой механики, а сама квантовая механика является неплохо подтверждаемой практикой теорией, описывающей объективную реальность. Это наводит на мысль о том, что, несмотря ни на что, в конце концов модель квантовых вычислений можно будет реализовать в «железе», и все разработанные алгоритмы можно будет реализовать на квантово-механическом компьютере.

На сегодняшний день, к сожалению, реализации в «железе» ещё не существует. Есть несколько перспективнейших направлений исследований, однако большинство из них упирается пока ещё в непреодолимые технологические ограничения. Но, в конце концов, все ограничения будут сняты, ибо нет фундаментальных ограничений, и тогда модель квантовых вычислений будет реализована в виде работающего квантового компьютера. В этой книге мы не будем рассматривать исследования по реализации модели в «железе», но читатель должен помнить, что рано или поздно квантовый компьютер будет создан, и тогда все знания, полученные при помощи чтения этой и многих подобных книг, будут востребованы на вес золота.

Кроме того, большинство имеющихся на сегодняшний момент книг по квантовым вычислениям содержат описания физических экспериментов, всевозможные наукоёмкие перспективные технологии (ядерно-магнитные резонансные компьютеры, компьютеры на ионных ловушках, компьютеры на одиночных молекулах и др.), а вот простому описанию модели внимания уделяется мало, незаслуженно мало. И получается некоторый перекос – для физиков-теоретиков и физиков-экспериментаторов научной литературы по квантовым вычислениям довольно много, а для программистов нет вообще. А среднестатистический разработчик программного обеспечения даже в рамках классической вычислительной модели вряд ли знаком с физикой про-

цессов, происходящих внутри процессора. Так и здесь, в этой новой области исследований требуется литература, которая будет готовить специалистов, которые смогут не физически реализовывать какие-либо устройства, а программировать их на логическом уровне.

Ну и теперь получается, что, ознакомившись с информацией в этой книге, вдумчивый читатель будет готов к переходу к более серьёзной литературе по теме. В соответствующем справочном разделе в конце книги всякий читатель найдёт для себя продолжение, если после прочтения возникнет непреодолимое желание погрузиться в тему дальше. Поэтому я как автор надеюсь, что мой скромный труд станет тем трамплином, который поможет вырастить мириады новых программистов.

Квантовые состояния и кубиты

Прежде всего для понимания модели квантовых вычислений необходимо овладеть понятийным аппаратом, который используется для описания и работы. Вся терминология пришла прямиком из квантовой механики, поэтому для тех, кто вполне владеет квантово-механическим аппаратом, понимание модели квантовых вычислений будет простым (хотя и здесь придётся приложить усилия к изучению нескольких терминов, пришедших из теории информации и теории вычислений). Здесь будут даны самые простейшие определения терминов. Тем же читателям, кто захочет полностью и глубоко понять математический аппарат, лежащий за описываемой моделью, имеет смысл обратиться к серьёзной литературе по квантовой механике.

Перед рассмотрением основного понятия в модели квантовых вычислений – кубита – необходимо изучить понятие квантового состояния. Квантовым состоянием будем называть совокупность из некоторого символа (наименования квантового состояния) и приписанного к нему коэффициента, причём этот коэффициент является комплексным числом. Квантовое состояние будет записываться как

$\alpha|s\rangle$,

где α – комплексночисленный коэффициент, а s – наименование квантового состояния. Последнее обычно состоит из одного символа, например: «0», «1», «+», «–». Так что квантовыми состояниями, например, являются такие объекты, как $|0\rangle$ и $|1\rangle$. А можно придумать и более сложные квантовые состояния, например $\frac{1-i}{2}|\uparrow\rangle$.

Кубитом в этом случае называется просто список квантовых состояний. Это слишком общее определение, и в других книгах по квантовым вычислениям обычно даётся иное определение. Однако здесь мы заострим внимание на этом аспекте – кубит состоит из списка квантовых состояний, при этом есть одно ограничение – сумма квадратов модулей всех комплексночисленных коэффициентов обязательно должна равняться 1.

Обычно и всегда это введённое таким образом понятие ограничивают. Поскольку традиционный бит представляет собой возможность выбора из двух альтернатив (0 или 1), то и кубит ограничивают двумя квантовыми состояниями в списке. Далее станет понятно, почему именно так, а теперь имеет смысл перейти к рассмотрению понятия «базис».

Базисом называется набор кубитов, которые взаимно ортогональны друг другу. Если ограничивать рассмотрение кубитов двумя квантовыми состояниями, то, само собой разумеется, базис состоит из двух кубитов. Однако же что такое «ортогональность» в применении к кубитам? Если кубит – это всего лишь список комплексных чисел, к которым приписаны некоторые наименования квантовых состояний, что как могут быть ортогональны такие «именованные комплексные числа»?

Всё просто. Дело в том, что базис выбирается тоже произвольным образом. Для простоты понимания и соответствия традиционному пониманию бита базисом назван набор кубитов $|0\rangle$ и $|1\rangle$, после чего было введено векторное представление кубита. Для этих двух базисных кубитов векторное представление следующее:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix};$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

И, собственно, ортогональность в таком случае определяется как равенство нулю скалярного произведения двух векторных представлений кубитов. Но что из себя представляют эти числа 0 и 1 в векторах? Это не что иное, как комплексно-численные коэффициенты α при базисных кубитах, то есть так и получается, что $|0\rangle = 1|0\rangle + 0|1\rangle$, а $|1\rangle = 0|0\rangle + 1|1\rangle$. Таким образом, произвольный кубит можно разложить в базисе, и такое разложение записывается как $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, и оно называется *линейной суперпозицией базисных состояний*, и, соответственно, в виде вектора такой кубит представляется как

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix},$$

где α и β – некоторые комплексные числа, такие, что сумма квадратов их модулей равна строго 1.

Всё дело в том, что комплексный коэффициент при базисном кубите, или, что то же, при базисном квантовом состоянии, – это так называемая *амплитуда вероятности*. Это понятие из квантовой механики, и оно обозначает тот простой факт, что при измерении вероятность обнаружения кубита в этом квантовом состоянии равна квадрату модуля его амплитуды. Именно поэтому сумма квадратов модулей должна равняться строго единице, поскольку при измерении кубит будет обнаружен либо в том, либо в другом базисном квантовом состоянии.

Но что такое измерение? Это понятие пришло непосредственно из квантовой механики, где оно определяется достаточно сложно. Здесь же для упрощения рассмотрим такое определение. Измерение кубита – это попытка ответить на вопрос типа «Находится ли данный кубит в квантовом состоянии $|0\rangle$?» или «Каковы амплитуды вероятности нахождения данного кубита в квантовых состояниях, определяемых некоторым базисом?». Ответом на первый вопрос становится амплитуда вероятности нахождения кубита в запрашиваемом квантовом состоянии, а ответом на второй вопрос – набор амплитуд вероятностей, соответствующих базисным квантовым состояниям, сумма которых, конечно же, равна единице.

Необходимо отметить, что, как следует из положений квантовой механики, после измерения кубит переходит в какое-либо состояние из числа входящих в базис, в рамках которого производится измерение, при этом вероятность перехода кубита в это состояние равна как раз квадрату модуля амплитуды при этом состоянии в базисе. Понять это проще всего на нескольких незамысловатых примерах, однако перед их рассмотрением стоит более подробно изучить используемую нотацию.

Читатель уже заметил эти странные скобки – $|s\rangle$. Это так называемая «нотация Дирака». Придумана она давным-давно, однако именно такой её внешний вид позволяет с лёгкостью понимать смысл вычислений и применять модель квантовых вычислений. Прежде всего надо отметить, что $|s\rangle$ называется «кет-вектором», а $\langle s|$, соответственно, «бра-вектором». Словечки «бра» и «кет» – это две части английского слова «bracket», которое переводится как «скобка».

Собственно, кет-вектор – это вектор-столбец, его мы уже видели при обсуждении векторного представления кубитов. А бра-вектор – это комплексно-сопряжённый с соответствующим кет-вектором вектор-строка. То есть, например, если у нас есть некоторый кубит

$$|\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

то соответствующим бра-вектором будет

$$\langle\varphi| = (\alpha^* \beta^*),$$

где α^* и β^* – комплексные сопряжённые чисел α и β соответственно (для комплексного числа $a + bi$ комплексным сопряжённым будет комплексное число $a - bi$).

Из этого следует простое мнемоническое правило: если соединить бра- и кет-вектор, чтобы получился «брaкет», то это будет *скалярным произведением* двух векторов:

$$\langle\varphi|\varphi\rangle = (\alpha^* \beta^*)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^*\alpha + \beta^*\beta = |\alpha|^2 + |\beta|^2$$

(если комплексное число умножить на его комплексное сопряжённое, то, без всяких сомнений, получится квадрат модуля этого числа, что каждый читатель может легко проверить при помощи формулы перемножения многочленов).

А что будет, если соединить бра- и кет-векторы в обратном порядке, то есть в виде «кетбра»? Это, само собой разумеется, записывается как $|\varphi\rangle\langle\varphi|$, а поскольку это векторы, то результатом такого их перемножения явится матрица. Если векторы имеют размерность 2, то такая матрица будет иметь размерность 2×2:

$$|\varphi\rangle\langle\varphi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}(\alpha^* \beta^*) = \begin{pmatrix} \alpha\alpha^* & \alpha\beta^* \\ \beta\alpha^* & \beta\beta^* \end{pmatrix}.$$

Это так называемая *матрица плотности* $\rho = |\varphi\rangle\langle\varphi|$. Данный термин ещё пригодится при детальном изучении модели квантовых вычислений.

Таким образом, есть два простых мнемонических правила:

- $\langle\varphi|\varphi\rangle$ – скалярное произведение, которое называется «брaкет» (от англ. *bracket*);
- $|\varphi\rangle\langle\varphi|$ – матрица плотности, что проще всего запомнить в виде эдакого неформального преобразования $|\varphi\rangle\langle\varphi| \rightarrow |\varphi\times\varphi|$, то есть обращённые одна к другой угловые скобки как бы превратились в знак умножения.

Теперь можно более чётко понять, что такое измерение. Например, чтобы ответить на вопрос «Находится ли данный кубит $|\varphi\rangle$ в квантовом состоянии $|0\rangle$?», необходимо просто выполнить операцию $\langle 0|\varphi\rangle$, и ответом на вопрос станет квадрат модуля полученного в результате вычисления числа. Само собой разумеется, что для квантового состояния $|0\rangle$ это тривиально, но то же самое правило действует и для других квантовых состояний – необходимо просто посчитать скалярное произведение, взять модуль результата и возвести его в квадрат.

Всё это понять ещё легче, если обратиться к графическому представлению. Несмотря на то что до этого момента для иллюстрации понятий квантовое состояние и кубит использовались некоторые символы и манипуляции ими, этим символам можно дать определённые интерпретации, в частности графическую. Но для этого для начала необходимо несколько упростить задачу – пусть коэффициенты перед квантовыми состояниями будут не комплексными, а действительными. В этом случае всё очень просто: каждый кубит представляет собой единичный вектор, а его разложение в базисе – это всего лишь проекции данного вектора на произвольно выбранные ортогональные «оси» (рис. 1).

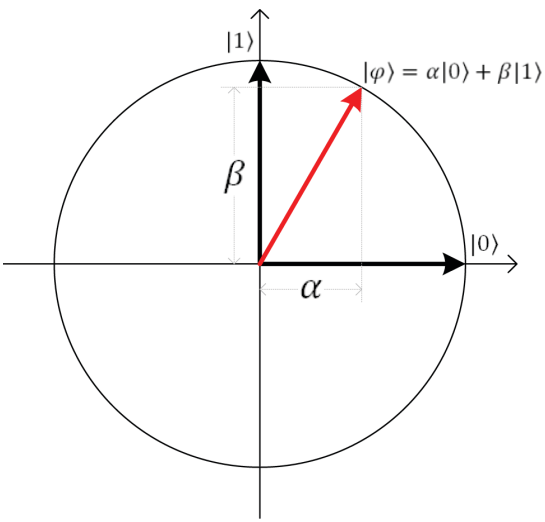

Рис. 1 ❖ Графическое представление разложения кубита в базисе в случае действительных коэффициентов

В этом случае становится понятным, почему $\alpha^2 + \beta^2 = 1$ – это всего лишь теорема Пифагора (конечно же, окружность в данном случае всегда имеет радиус 1).

Тут так же необходимо отметить, что «оси», то есть базисные квантовые состояния, выбраны абсолютно произвольно, – единственное условие, которому они должны удовлетворять, – это ортогональность. Просто так уж сложилось по традиции, что выбирают горизонтальный вектор $|0\rangle$ и вертикальный вектор $|1\rangle$. Но, само собой разумеется, это не единственный базис. Базисов может существовать бесконечное количество – любая пара ортогональных единичных векторов может служить базисом.

Например, другим часто используемым базисом является базис $\{|+\rangle, |-\rangle\}$ (рис. 2).

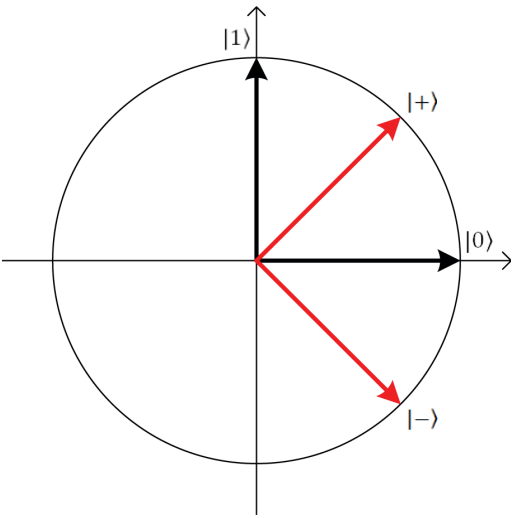

Рис. 2 ❖ Базис $\{|+\rangle, |-\rangle\}$ и его расположение относительно стандартного базиса

Естественно, что оба квантовых состояния этого базиса можно выразить через основной базис $\{|0\rangle, |1\rangle\}$, и сделать это довольно просто. Даже не вдаваясь в серьёзные расчёты (хотя и это можно было бы сделать), но используя только упомянутую ранее теорему Пифагора, можно вычислить значения коэффициентов α и β, которые в данном случае равны. Это делается так (помним, что α в данном случае – дей-

ствительное число, поэтому квадрат его модуля равен просто квадрату этого числа):

$$2\alpha^2 = 1 \;\Rightarrow\; \alpha^2 = \frac{1}{2} \;\Rightarrow\; \alpha = \frac{1}{\sqrt{2}},$$

то есть

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle;$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Этот базис также часто используется в модели квантовых вычислений, поэтому его хорошо бы постоянно держать в уме. По крайней мере, формулы пересчёта из одного базиса в другой полезно помнить наизусть.

Эти формулы помогут, к примеру, отвечать на такие вопросы, как «Если выполнить измерение заданного кубита в базисе $\{|+\rangle, |-\rangle\}$, то с какой вероятностью кубит примет значение $|+\rangle$?», и подобные. Ведь если есть кубит, для которого имеется выражение в стандартном базисе $|\varphi\rangle$, то для ответа на этот вопрос достаточно произвести операцию $\langle +|\varphi\rangle$, и в результате будет получена амплитуда искомой вероятности.

Например, если кубит $|\varphi\rangle$ разлагается в стандартном базисе как $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, то для перевода его в базис $\{|+\rangle, |-\rangle\}$ можно воспользоваться следующей формулой:

$$|\varphi\rangle_{+|-} = \langle +|\varphi\rangle|+\rangle + \langle -|\varphi\rangle|-\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle.$$

Эта формула поясняется при помощи диаграммы на рис. 3.

Собственно, матричные операции дают возможность не только ответить на первый вопрос об измерении, но и на второй, то есть сразу узнать, каковы амплитуды вероятности нахождения данного кубита в квантовых состояниях, определяемых некоторым базисом. Для этого надо перемножать не векторы, а сразу умножить сопряжённую матрицу, представляющую собой базис, на векторное представление кубита. В результате получится вектор, представляющий собой именно амплитуды вероятностей.

Например, матрица стандартного базиса выглядит как

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

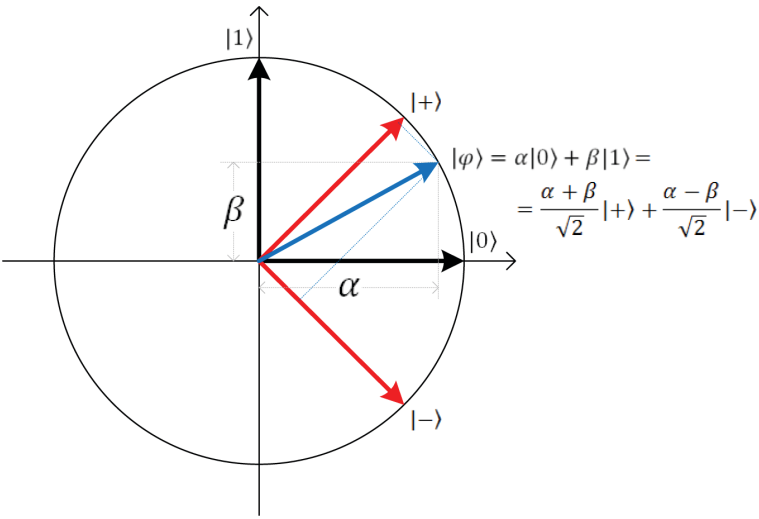

Рис. 3 ❖ Перевод кубита в базис $\{|+\rangle, |-\rangle\}$

и её комплексно-сопряжённая матрица выглядит точно так же. Если эту матрицу умножить на представление кубита в стандартном базисе, то в результате, как ни странно, получатся коэффициенты α и β, то есть амплитуды вероятности нахождения кубита в базисных состояниях $|0\rangle$ и $|1\rangle$. А вот матрица базиса $\{|+\rangle, |-\rangle\}$ выглядит так:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

и её комплексно-сопряжённая матрица абсолютно такая же. Соответственно, можно произвести умножение комплексно-сопряжённой матрицы на кубит $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \frac{\alpha+\beta}{\sqrt{2}} \\ \frac{\alpha-\beta}{\sqrt{2}} \end{pmatrix},$$

что полностью соответствует полученному ранее результату.

Все эти примеры, которые рассматривались выше, имеют один нюанс – коэффициенты в квантовых состояниях кубитов в них действи-

тельные. Честно говоря, это нисколько не уменьшает силу квантовой вычислительной модели, однако в объективном мире уж так устроено, что квантовая механика оперирует с комплексными коэффициентами. Такова модель описания реальности, принятая в квантовой механике, а потому она перенесена и в вычислительную модель, поскольку в конце концов кубиты будут реализованы в «железе», и такая реализация кубитов будет иметь дело именно с комплексными коэффициентами. Поэтому здесь надо рассмотреть дополнительную визуализацию модели при помощи диаграммы, но уже с квантовыми коэффициентами.

Если действительные коэффициенты при двух базисных квантовых состояниях приводили к появлению одномерного пространства состояний (окружность), то резонно предположить, что использование комплексных коэффициентов приведёт к появлению двумерного пространства – сферы. Так оно и есть, и такая визуализация называется *сферой Блоха*.

Тут есть один тонкий момент (те, кто не любит формул, могут сразу же перейти к следующей странице и посмотреть на приятную взору диаграмму). Поскольку каждый кубит нормирован, его длина всегда равна единице (то есть, напомним, $|\alpha|^2 + |\beta|^2 = 1$), то разложение в стандартном базисе можно записать как

$$|\varphi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\omega}\sin\frac{\theta}{2}|1\rangle\right).$$

Это выражение для кубита $|\varphi\rangle$ осуществляется на основании широко известной формулы Эйлера ($e^{ix} = \cos x + i\sin x$). Поскольку коэффициенты α и β являются комплексными числами, то ничто не мешает записать их как систему уравнений:

$$\alpha = e^{i\gamma}\cos\frac{\theta}{2} = \cos\gamma\cos\frac{\theta}{2} + i\sin\gamma\cos\frac{\theta}{2};$$

$$\beta = e^{i\gamma}e^{i\omega}\sin\frac{\theta}{2} = e^{i(\gamma+\omega)}\sin\frac{\theta}{2} =$$

$$= \cos(\gamma+\omega)\sin\frac{\theta}{2} + i\sin(\gamma+\omega)\sin\frac{\theta}{2}.$$

Так уж получилось, что в квантовом мире множитель e^{iy} можно опустить, поскольку он не приводит к каким-либо наблюдаемым эффектам – это просто некоторый фазовый коэффициент, который при проведении измерения никак не влияет на результаты. Это значит, что в данном случае приведённые выше уравнения можно переписать в виде:

$$\alpha = \cos\frac{\theta}{2} + i\sin\frac{\theta}{2};$$

$$\beta = \cos\omega\sin\frac{\theta}{2} + i\sin\omega\sin\frac{\theta}{2}.$$

Так что кубит описывается двумя угловыми параметрами – θ и ω, а они приводят к чёткой геометрической интерпретации кубита с комплексными коэффициентами в виде точки на сфере:

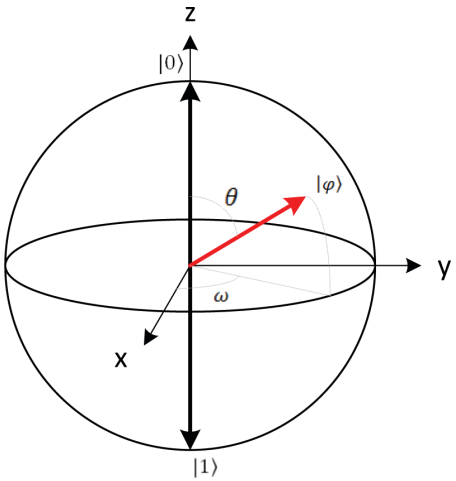

Рис. 4 ❖ Кубит как точка на сфере Блоха

Как видно, в данном представлении базис представляется парой квантовых состояний, не ортогональных друг другу, но разнонаправленных и лежащих на одной прямой. На диаграмме показан стандартный базис, но вдумчивый читатель может решить вышеприведённые уравнения для базиса $\{|+\rangle, |-\rangle\}$ и отобразить его на сфере Блоха.

И теперь осталось упомянуть об одной важной особенности операции измерения в модели квантовых вычислений, которая, если можно так выразиться, контринтуитивна. Измерение – это дорога в один конец. Другими словами, если мы произвели измерение кубита и получили какой-то конкретный результат (с определённой вероятностью), то сам кубит принял значение, полученное в результате измерения, и вся суперпозиция базисных состояний была потеряна. Восстановить её невозможно.

Таким образом, после измерения вся квантовая информация, которая хранилась посредством суперпозиции базисных состояний с комплексными коэффициентами, теряется, а остаётся только одна из двух альтернатив. Именно поэтому кубит и называется «битом» – несмотря на то что потенциально в нём в «скрытом виде» хранится бесконечное количество информации (произвольная суперпозиция двух ортонормированных базисных состояний), при измерении из него можно выудить только один бит информации – либо одно, либо другое состояние в базисе измерения.

Несколько кубитов

Итак, из рассмотренного до сего времени сложно сделать выводы о том, что модель квантовых вычислений даёт какое-то преимущество по сравнению с традиционной вычислительной моделью. Ну да, один кубит содержит в скрытом виде бесконечное количество информации, но мы никак не можем этим воспользоваться. Это именно скрытая информация, которая используется внутри кубита неизвестным для нас способом. В чём же дело?

Интересная особенность квантовых вычислений проявляется тогда, когда на сцену выходят многокубитовые системы. Дело в том, что правила комбинации кубитов разительно отличаются от правил комбинации битов. Проще всего рассмотреть вариант комбинации двух кубитов.

В квантовой механике и при обычном рассмотрении модели квантовых вычислений считается, что любые два кубита всегда находятся в разных пространствах состояний, поэтому даже если обозначения их базисов одинаковые, то всё равно считается, что базисы разные (и для этого иногда используют индексы, которые тут же начинают опускать). Однако это – усложнение рассмотрения, поэтому далее будет считаться, что все кубиты находятся в одном и том же пространстве состояний и раскладываются на суперпозицию в одинаковых базисах.

Так что пусть есть два кубита $|\varphi\rangle$ и $|\psi\rangle$. Они представляют собой две суперпозиции базисных состояний, скажем, в стандартном базисе: $|\varphi\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ и $|\psi\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ – это просто два обычных кубита. Но что будет, если их соединить в двухкубитовую систему? Всё просто:

$$|\varphi\rangle|\psi\rangle = \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\beta_2|1\rangle|1\rangle.$$