

Основы квантовых вычислений и связь с физикой

Кейсукэ Фуджи, Центр фотонной науки, Высшая инженерная школа, Токийский университет

8 июня 2017 г. __

1 Введение

Этот текст начинается с обзора квантовой механики и подробно объясняет основы квантовой информации и квантовых вычислений. С другой стороны, когда я читаю лекции, я не обязательно обсуждаю подробные расчеты и доказательства. Мы бы хотели, чтобы каждый из вас попробовал посчитать самостоятельно на основе текста и привыкнуть к описанию с использованием квантовой информации (Конечно, мы будем рады, если вы придете и зададите нам вопросы вне лекций). С другой стороны, из-за нехватки места мы не смогли включить такие темы, как топологический порядок и топологические квантовые вычисления с использованием майорановских частиц. Я подробно объясню это во время лекции.

Квантовая информация предназначена для универсального описания явлений в сложных квантовых системах, максимально не зависящих от конкретных физических систем. Поступая таким образом, мы можем широко использовать методы информатики, такие как теория вычислений и теория информации, для проведения подробных обсуждений. Кроме того, из обсуждения универсальности, объясненного в этом тексте, квантовый компьютер может эффективно имитировать динамику любой квантовой системы. Поэтому понимание поведения и ограничений квантовых компьютеров приведет к более глубокому пониманию физики. Например, недавно теория квантовой коррекции ошибок, которая была создана для защиты квантовых компьютеров от шума, использовалась для понимания топологического порядка и черных дыр. Ожидается, что в будущем число таких случаев будет увеличиваться. Кроме того, реальная реализация квантовых компьютеров, даже в небольшом масштабе, позволит по-новому взглянуть на физику на пределе сложности, который невозможно понять с помощью численных расчетов с использованием только решаемых моделей и классических компьютеров. получение знаний. Само собой разумеется, что квантовые компьютеры полезны при решении проблем, которые потенциально могут быть определены на языке «квантов», таких как квантовый дизайн материалов и квантово-химические расчеты. Квантовые компьютеры могут внести значительный вклад даже в несвязанные области, учитывая сложность их работы. реализация.

С другой стороны, обычные студенты-физики не касались понятий информации и вычислений. Поэтому, пока вы не привыкнете, вам может быть трудно почувствовать связь с физикой, потому что развитие дискуссии брутальное (что тоже хорошо). Недавно в сети был опубликован небольшой, но универсальный настоящий квантовый компьютер (квантовый опыт IBM), и любой может использовать его (пока) бесплатно. Возможно, стоит проверить, что написано в этом тексте, самостоятельно с помощью квантового компьютера на сервере.

На этот раз у меня нет времени вдаваться в физику квантовых устройств, но теория квантовых компьютеров — это поддерживающее ее квантовое устройство. Физика и экспериментальная технология обычного компьютера поддерживаются накоплением физики твердого тела и технологии полупроводников. (как сообщается). Лучшее понимание физики квантовых информационных устройств, таких как сверхпроводящие кубиты, и технологии управления ими также является важным ключом к реализации квантовых компьютеров. Амбициозные студенты, интересующиеся экспериментами, также должны попробовать физику квантовых информационных устройств.

2 От обзора квантовой механики к квантовой информации

В этом разделе в качестве обзора квантовой механики мы вводим методы записи, часто используемые в квантовой информации, эволюции во времени (квантовые операции), измерениях, операциях плотности и т. д.

В этом разделе объясняется, как обращаться с арифметическими и другими функциями. Если вы уже знаете, пожалуйста, пропустите этот раздел и читайте следующий раздел.

2.1 Квантовое состояние: гильбертово пространство

Квантовое состояние описывается элементом $|\psi\rangle$ N комплексного гильбертова пространства N , которое является полным² комплексным линейным пространством с определенным скалярным произведением¹. В случае конечномерного комплексного гильбертова пространства $|\psi\rangle$ является комплексным вектор-столбцом $|\psi\rangle = (c_1, \dots, c_d)$. Можно смело предположить, что это T . Обозначим через $\langle\psi|$ элемент двойственного пространства³ N^* и через $\langle\psi|\psi\rangle$ скалярное произведение. В конечномерном комплексном векторном пространстве элементом двойственного пространства является комплексный вектор-строка $\langle\psi| = (c_1^*, \dots, c_d^*)$ в T . Обозначение скобок Дирака описывает гильбертово пространство и элементы в его двойственном пространстве с помощью $|\dots\rangle$ (ket) и $\langle\dots|$ (bra). Пусть A — линейный оператор из гильбертова пространства N в N . $|\psi\rangle$ N отображается посредством A $|\psi\rangle$ N в N . Обозначение $A^\dagger$ Оператор $A^\dagger$, удовлетворяющий условию $\langle\psi|A^\dagger|\phi\rangle = \langle A|\psi||\phi\rangle$, становится сопряженным оператором оператора A . Элементы двойственного пространства, $\langle\psi|$ и $|\phi\rangle$ N , но $\langle\psi|A^\dagger|\phi\rangle = \langle A|\psi||\phi\rangle$ удовлетворяющий условию $\langle\psi|A^\dagger|\phi\rangle = \langle A|\psi||\phi\rangle$, становится сопряженным оператором оператора A . Соответствующие записываются с использованием знака $\langle\psi|A^\dagger|\phi\rangle$. Другими словами, мы можем сказать, что $A^\dagger$ — это то, что записано в исходном пространстве и соответствует действию A на двойственном пространстве⁴. Мы также пишем $\langle\psi| = (\langle\psi|)^\dagger$ для элементов двойственного пространства, соответствующего $|\psi\rangle$. В конечномерном комплексном векторном пространстве сопряженное † эквивалентно транспонированию и комплексному сопряжению, то есть эрмитовому сопряжению.

2.2 . Связь между уравнением Шредингера и волновой функцией

Давайте посмотрим на связь с волновой функцией, которую мы изучали на уроках квантовой механики. Уравнение Шредингера, описывающее эволюцию состояния квантовой системы во времени, имеет вид

$$i\hbar \frac{\partial}{\partial t} \psi(x, t) = H\psi(x, t) \quad (1)$$

где $\psi(x, t)$ — волновая функция (которая может быть нормирована соответствующими граничными условиями), а гамильтониан H — оператор, соответствующий энергии $\langle H \rangle$. Плотность вероятности нахождения частицы в положении x в момент времени t разделяет $|\psi(x, t)|^2$ на пространство и время, а собственная функция энергии

$$H\psi_k(x) = E_k\psi_k(x) \quad (2)$$

$$H\psi_k(x) = E_k\psi_k(x) \quad (2)$$

можно решить, найдя E_k — собственное значение k -й собственной функции энергии. Мы рассматриваем только случай, когда граничные условия заданы корректно и $\psi_k(x)$ можно

нормализовать, т. е. $\int dx |\psi_k(x)|^2$ сходится. Далее предполагается, что $\psi_k(x)$ нормирована. Эволюция во времени этой собственной функции энергии равна

$$\psi_k(x, t) = \psi_k(x) e^{-iE_k t / \hbar} \quad (3)$$

^{*1} Скалярный продукт — это соответствие между любыми двумя элементами $|\psi\rangle$ и $|\phi\rangle$ в линейном пространстве и комплексным числом $\langle\psi|\phi\rangle$.

^{*2} $\langle\phi|\phi\rangle = 0$. Полнота означает, что последовательность Коши $\langle\phi|\phi\rangle = 0$ сходится к элементу пространства $|\psi\rangle$ $\langle\phi|\psi\rangle = 0$. Для конечномерного комплексного линейного пространства полнота линейного пространства гарантируется полнотой комплексных чисел. ^{*3} Рассмотрим функционал $f: V \rightarrow \mathbb{C}$, который действует на элемент v гильбертова пространства V и возвращает комплексное число. Для функционалов f и g также можно определить $f + g$ и скалярное умножение af , поэтому множество функционалов также является линейным пространством, которое называется двойственным пространством V^* к линейному пространству V . Согласно теореме Рисса, некоторый функционал f всегда использует элемент v гильбертова пространства V и скалярное произведение $\langle v|v'\rangle = \langle v, v'\rangle$, такой функционал запишем в виде $f v$. Скобочное обозначение Дирака состоит в том, чтобы обозначать элемент v из V как $\text{ket } |v\rangle$ и элемент $f v$ двойственного пространства V^* как $\text{bra } \langle v|$. $\langle v|v'\rangle = \langle v|A^\dagger v'\rangle$

$f A v = \langle v|A^\dagger v'\rangle$

, поэтому $\psi_k(x, t) = e^{-iE_k t/\hbar} \psi_k(x)$. В волновом уравнении $\hbar \frac{\partial \psi}{\partial t} = \hat{H} \psi$ (скалярное уравнение), которое допускает суперпозицию решений, является общим решением, суперпозиция собственных функций энергии $\Psi(x, t) = \sum_k c_k \psi_k(x, t)$ определяет сумму (суперпозицию) собственных функций. Волновая функция представляет собой линейное пространство

Вы видите, что он настроен. Кроме того, два решения $\Psi(x, t)$ и $\Phi(x, t)$ пространственно интегрированы $\int dx \Psi^* \Phi$. Поскольку вы можете получить комплексные числа с помощью $\int dx \Psi^* \Phi$, вы также можете определить внутренние продукты. Кроме того, тот факт, что его можно нормализовать с помощью подходящего граничного условия, означает, что норма $\int dx |\Psi|^2$ равна единице. Это означает, что $\Psi(x, t)$ является элементом гильбертова пространства. Другими словами, множество решений уравнения Шредингера образует комплексное гильбертово пространство. Рассмотрим ситуацию, когда нас интересует только собственное состояние с конечной энергией d из-за ограничений, таких как интересующая шкала энергии. При этом любое квантовое состояние есть состояние $(k = 1, 2, \dots, d)$.

$$\Psi(x, t) = \sum_{k=1}^d c_k \psi_k(x, t) \quad (\text{Четыре})$$

Я звоню. Пусть $\psi_k(x, t)$ — элемент гильбертова пространства и пишут $|\psi_k\rangle$ ($k = 1, \dots, d$). Используя собственные энергетические состояния, гамильтониан имеет вид $\hat{H} = \sum_{k=1}^d E_k |\psi_k\rangle \langle \psi_k|$ и умножения $\hat{H}^\dagger = \hat{H}$, т. е. является самосопряженным (эрмитовым для конечномерного случая) оператором. Следовательно, для двух собственных энергетических состояний $|\psi_k\rangle$ и $|\psi_j\rangle$ $\langle \psi_k | \hat{H} | \psi_j \rangle = E_k \langle \psi_k | \psi_j \rangle = E_j \langle \psi_k | \psi_j \rangle$, два собственных состояния ортогональны $\langle \psi_k | \psi_j \rangle = 0$, когда $E_j \neq E_k$. Более того, даже в вырожденном случае $E_j = E_k$ из двух неортогональных собственных состояний $|\psi_k\rangle$ и $|\psi_j\rangle$, $|\psi_j\rangle = \frac{1}{\sqrt{\langle \psi_k | \psi_j \rangle}} |\psi_k\rangle$, новый $|\psi\rangle$ Мы можем получить ортогональные состояния, определив (ортогонализация Грама-Шмидта). Выражая волновую функцию $|\Psi(x, t)\rangle$ как вектор-столбец с использованием этих ортонормированных базисов $\{|\psi_k\rangle\}$, волновая функция и комплексный вектор-столбец соответствуют.

2.3 Эволюция времени: унитарные операторы

Перепишем уравнение Шредингера в скобочных обозначениях:

$$i\hbar \frac{d}{dt} |\Psi(x, t)\rangle = \hat{H} |\Psi(x, t)\rangle \quad (\text{Пять})$$

Учитывая состояние $|\Psi(x, 0)\rangle$ (волновая функция) в момент времени $t = 0$, формальное решение уравнения Шредингера дает

$$|\Psi(x, t)\rangle = e^{-i\hat{H}t/\hbar} |\Psi(x, 0)\rangle, \quad (6)$$

получается. Поскольку $\hat{H}$ был эрмитовым оператором, $e^{-i\hat{H}t/\hbar}$ становится унитарным оператором (который удовлетворяет условию $U^\dagger U = Id$).

Таким образом, эволюция квантовой системы во времени описывается унитарным оператором U , действующим в комплексном гильбертовом пространстве.

2.4. Квантовые измерения: проекционный оператор

Состояние в физике определяется путем выбора значений физических величин, экспериментально полученных из целевой физической системы, и прогнозов, связанных с их статистическими

Нужно было дать слова. Измерение в квантовой системе является проективным измерением с использованием d свойствами, и основанных на этих значениях. оператора проектирования $\{P_i\}$. Операторами проекции являются $P_i P_j = \delta_{ij} P_i$ и $\sum_{i=1}^d P_i = Id$. Например, ортонормированный базис $\{|i\rangle\}_{i=1}^d$ и положим $P_i = |i\rangle \langle i|$, получим оператор проектирования. состояние $|\Psi\rangle$, вероятность p_i получения результата измерения i при выполнении проекционного измерения с помощью проекционного оператора $\{P_i\}$ равна

$$p_i = \langle \Psi | P_i | \Psi \rangle = \langle \Psi | i \rangle \langle i | \Psi \rangle \quad (7)$$

^[1] Пусть Id — тождественный оператор в d - мерном пространстве.

дан кем-то $\sum_i p_i = 1$ в силу свойства оператора проектирования. Поскольку временная эволюция является унитарным оператором (сохраняющим скалярный продукт), вероятности всегда сохраняются, если начальное состояние нормализовано. В отличие от классического состояния, даже если квантовое состояние является фиксированным состоянием $|\psi\rangle$, результат дается стохастически в зависимости от метода измерения. Состояние после получения результата измерения i равно $|\psi_i\rangle / p_i$. До сих пор было дано описание состояния, эволюции во времени и измерений в квантовой системе. Рассмотрим ситуацию, в которой нам задано много одинаковых квантовых состояний $|\psi\rangle$, и мы неоднократно их измеряем. Если получен результат измерения i , энергия Пусть a_i — физическая величина (случайная величина), когда Например, энергетическая проективная мера $\{|\psi_k\rangle\langle\psi_k|\}$ d Ge $\sum_{k=1}^d$ результат измерения i , энергия собственное значение E_k . В это время среднее значение физической величины дается эрмитовым оператором $A = \sum_{k=1}^d E_k |\psi_k\rangle\langle\psi_k|$ используя айпи

$$A = \sum_{i=1}^d a_i p_i = \sum_{i=1}^d |\psi_i\rangle\langle\psi_i|, \quad (8)$$

можно рассчитать как Наоборот, если используется эрмитов оператор, спектральное разложение $A = \sum_{i=1}^d a_i |\psi_i\rangle\langle\psi_i|$ айпи _

A называется наблюдаемой величиной, потому что можно вычислить проективное измерение физической величины A и среднее значение физической величины A .

2.5 Составные системы: тензорные произведения

Рассмотрим составную систему, состоящую из двух квантовых систем 1,2. Поскольку составная система является также квантовой системой в целом, квантовое состояние составной системы может быть записано как элемент некоторого гильбертова пространства $H_{1,2}$. Примеры таких состояний включают состояние прямого произведения $(|\psi_1\rangle, |\phi_2\rangle)$ состояния $|\psi_1\rangle$ H_1 квантовой системы 1 и состояния $|\phi_2\rangle$ H_2 квантовой системы 2. Оно должно иметь был Из-за линейности составной системы два декартовых состояния произведения $(|\psi_1\rangle, |\phi_2\rangle)$ и $(|\psi_1'\rangle, |\phi_2'\rangle)$ (линейная сумма 2) также входит в составную систему $H_{1,2}$. Таким образом, линейное пространство, натянутое на состояния прямого произведения состояний H_1 и H_2 , называется пространством тензорного произведения. Назовем его $H_{1,2} = H_1 \otimes H_2$. Состояние произведения равно $|\psi\rangle$ вместо $(|\psi_1\rangle, |\phi_2\rangle)$. $|\psi\rangle = \sum_{i,j} c_{ij} |\psi_i\rangle |\phi_j\rangle$ или $|\psi\rangle = \sum_{i,j} c_{ij} |\psi_i\rangle |\phi_j\rangle$, если это не сбивает с толку $|\psi\rangle$ и написать В качестве базы пространства тензорного произведения базой H_1 и H_2 является $\{|\psi_i\rangle\}_{i=1}^d$ и $\{|\phi_j\rangle\}_{j=1}^{d'}$. Как состояние произведения $|\psi\rangle = \sum_{i,j} c_{ij} |\psi_i\rangle |\phi_j\rangle$ можно принять. Таким образом, размерность $H_{1,2}$ равна dd' . вычислить тензорное произведение подчиняется следующему правилу (билинейности):

$$(|\psi\rangle + |\psi'\rangle) |\phi\rangle = |\psi\rangle |\phi\rangle + |\psi'\rangle |\phi\rangle, \quad (9)$$

$$|\psi\rangle (|\phi\rangle + |\phi'\rangle) = |\psi\rangle |\phi\rangle + |\psi\rangle |\phi'\rangle, \quad (10)$$

$$|\psi\rangle (\alpha |\phi\rangle) = (\alpha |\psi\rangle) |\phi\rangle = (\alpha |\psi\rangle) |\phi\rangle. \quad (11)$$

$\{|\psi_i\rangle\}_{i=1}^d$ и $\{|\phi_j\rangle\}_{j=1}^{d'}$ состояние, выраженное как вектор-столбец $|\psi\rangle = (a_1, \dots, a_d)$ и $|\phi\rangle = (b_1, \dots, b_{d'})$. Т. Десять из состояние произведения $|\psi\rangle |\phi\rangle$ 2 как базис $\{|\psi_i\rangle |\phi_j\rangle\}$ При выражении в виде вектора для

$$|\psi\rangle |\phi\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_{d'} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_{d'} \\ \vdots \\ a_d b_1 \\ \vdots \\ a_d b_{d'} \end{pmatrix} \quad (12)$$

становится. Построение dd' -мерного вектора из d -мерного вектора и d' - мерного вектора таким образом называется произведением Кронекера.

Вызов. Состояния на $H_{1,2}$ не обязательно записываются как $|\psi\rangle |\phi\rangle$. В частности, случай, когда можно записать $|\psi\rangle |\phi\rangle$, называется состоянием декартова произведения, а состояние, которое не перемножается, называется запутанным состоянием.

Действие оператора тензорного произведения $A \otimes B$ в операторов A и B на H_1 и H_2 на $H_{1,2}$ таково:

$$(A \otimes B) |\psi\rangle |\phi\rangle = (A |\psi\rangle) (B |\phi\rangle) \quad (13)$$

определяется. Оператор тензорного произведения также билинейный

$$(A + A') (B + B') = A'B + A'B' + A'B + A'B' \quad (14)$$

держит. Следовательно, если $A = \sum_i |i\rangle\langle i|$, то $A \otimes B = \sum_{i,j} |i\rangle\langle i| \otimes |j\rangle\langle j|$

оператор тензорного произведения равен

$$(A \otimes B)_{ij, i'j'} = \sum_{k,l} A_{ik} B_{jl} \delta_{ki} \delta_{lj} = A_{ii'} B_{jj'} \quad (15)$$

поэтому произведение Кронекера двух матриц равно

$$A \otimes B = \begin{pmatrix} a_{11} & \dots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \dots & a_{dd} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & \dots & b_{1d'} \\ \vdots & \ddots & \vdots \\ b_{d'1} & \dots & b_{d'd'} \end{pmatrix} \quad (16)$$

$$= \begin{pmatrix} a_{11}b_{11} & \dots & a_{11}b_{1d'} & \dots & a_{1d}b_{11} & \dots & a_{1d}b_{1d'} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{11}b_{d'1} & \dots & a_{11}b_{d'd'} & \dots & a_{1d}b_{d'1} & \dots & a_{1d}b_{d'd'} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{d1}b_{11} & \dots & a_{d1}b_{1d'} & \dots & a_{dd}b_{11} & \dots & a_{dd}b_{1d'} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{d1}b_{d'1} & \dots & a_{d1}b_{d'd'} & \dots & a_{dd}b_{d'1} & \dots & a_{dd}b_{d'd'} \end{pmatrix} \quad (17)$$

2.6. Операторы плотности, общие квантовые операции, обобщенные измерения

До сих пор мы рассматривали ситуацию, в которой одно фиксированное квантовое состояние $|\psi\rangle$ задано с вероятностью 1. Расширяя это, давайте рассмотрим ситуацию, в которой различные квантовые состояния заданы стохастически. Для этого удобно описывать состояние с помощью оператора плотности $\rho = |\psi\rangle\langle\psi|$ (может быть любым). Проективное измерение с оператором проектирования $\{P_k\}$

$$p_k = \langle\psi|P_k|\psi\rangle = \sum_{j=1}^d \langle j|P_k|j\rangle \langle\psi|j\rangle\langle j|\psi\rangle = \sum_{j=1}^d \langle j|P_k|\psi\rangle\langle\psi|j\rangle \quad (18)$$

$$= \text{Tr}[P_k |\psi\rangle\langle\psi|] \quad (19)$$

можно вычислить, используя трассировку $\text{Tr}[\rho] = \sum_{i=1}^d \langle i|\rho|i\rangle$ следующим образом. Однако ортонормированный базис $\{|i\rangle\}$ d-свойственен полон выполняется, используется идентификатор. След Tr определяется независимо от выбора ортонормированного базиса, и $\text{Tr}[ABC] = \text{Tr}[CAB]$

Теперь рассмотрим ситуацию, когда нам даны различные квантовые состояния $\{|\psi_j\rangle\}$ с вероятностями $\{q_j\}$, и мы проводим проективное измерение $\{P_i\}$, ассоциативный закон вероятности, вероятность получения результата измерения i равна

$$p_i = \sum_{j=1}^d q_j \text{Tr}[P_i |\psi_j\rangle\langle\psi_j|] = \text{Tr}[P_i \sum_{j=1}^d q_j |\psi_j\rangle\langle\psi_j|] \quad (20)$$

становится. Следовательно, если мы примем $\rho = \sum_{j=1}^d q_j |\psi_j\rangle\langle\psi_j|$ в качестве оператора плотности, то распределение вероятностей

проективного измерения для такого классического стохастического смешанного состояния задается выражением $p_i = \text{Tr}[P_i \rho]$. Подтвердим

свойства оператора плотности ρ . Требуется $\text{Tr}[\rho] = 1$, можно разложить ρ по операторам $|j\rangle\langle j|$ и определить $\rho =$

когда $\rho = |\psi\rangle\langle\psi|$, оно называется чистым состоянием. Если ρ — это смесь чистых состояний, то ρ называется смешанным состоянием. В частности, для оператора плотности

$$|\psi\rangle\langle\psi|$$
 называется чистотой, а $\text{Tr}[\rho^2] = 1$ чисто

*6 Оператор A такой, что $\langle v|Av\rangle \geq 0$ для любого $|v\rangle$, называется положительно-полуопределенным оператором. Также это может быть оператор со всеми собственными значениями ≥ 0 .

Почему мы вообще должны вводить оператор плотности? Если мы когерентно опишем квантовое состояние составной системы как чистое состояние $\rho = |\psi\rangle\langle\psi|$, включая устройство, которое стохастически подготавливает квантовое состояние, мы можем исключить классическое состояние всей вселенной) в том числе составные системы. В ситуации, когда доступ к устройству, отправляющему квантовое состояние, недоступен, расчет плотности может быть выполнен только с подсистемой в качестве смешанного состояния.

Часто можно кратко описать состояние, написав его как ребенка.

Например, предположим, что у нас есть состояние $\rho_{1,2} = |\Psi\rangle\langle\Psi|$ составной системы квантовых систем 1,2. В это время вероятность выполнения проекционного измерения $\{P_k\}$ только с квантовой системой 1 без получения какой-либо информации от квантовой системы 2 равна

$$p_k = \text{Tr}[(P_k \otimes I) \rho_{1,2}]$$

становится. След в составной системе $\rho_{1,2}$ $\rho_1 = \text{Tr}_2[\rho_{1,2}]$ принимается за состояние

$$\rho_1 = \text{Tr}_2[\rho_{1,2}] = \sum_{j=1}^d (\text{Id} \otimes |j\rangle\langle j|) \rho_{1,2} (\text{Id} \otimes |j\rangle\langle j|)$$

К

$$p_k = \text{Tr}_1 [P_k \rho_1]$$

Получение следа о подсистеме таким образом называется частичным следом, а оператор плотности ρ_1 , принимающий частичный след, называется приведенным оператором плотности. В случае предыдущего примера $\rho = |\psi\rangle\langle\psi|$, если доступности устройства, мы получили смешанное состояние $\rho = |\psi\rangle\langle\psi|$ как приведенное получен оператор плотности ρ_1 . Таким образом, даже если состояние Вселенной в целом является чистым состоянием, когда мы делаем закрытый аргумент только для интересующей нас подсистемы, система может рассматриваться как классическое смешанное состояние с использованием оператора плотности. . Обратно, любой оператор плотности может быть записан как $\rho = \sum_{j,q} c_{jq} |\psi_j\rangle\langle\psi_q|$ в терминах ортогональных состояний $\{|\psi_j\rangle\}$ с помощью спектрального разложения, поэтому мы можем добавить к ним некоторую вспомогательную систему чистое состояние называется очищением. Точно так же эволюция унитарного времени и проективные измерения на составной системе с добавлением составной системы могут быть описаны только подсистемами.

Квантовые операции и квантовые измерения могут быть обобщены в форме, замкнутой только подсистемами.

Рассмотрим наиболее общие физически допустимые квантовые операции для операторов плотности. Физически допустимые операции плотности Потомок ρ был положительно полуопределенным оператором со следом 1. Если квантовые операции также сохраняют вероятности, кажется, что квантовые операции физически допускают отображения, которые сохраняют следы и поддерживают положительную полуопределенность. Однако этого еще недостаточно. Как и в предыдущем обсуждении, при работе с операторами плотности мы хотим включить ситуации, когда добавляются вспомогательные системы. По этой причине существует сильное требование не только к положительной определенности самого оператора плотности, но и к состоянию составной системы с добавлением какой-либо вспомогательной системы для сохранения положительной определенности. Карта CPTP (полностью положительная карта с сохранением трассировки) удовлетворяет этому требованию. Пусть $L(H)$ — пространство операторов, действующих на H , тогда CPTP-отображение $E: L(H) \rightarrow L(H)$ есть

$$E(\rho + \sigma) = E(\rho) + E(\sigma), \text{ (линейность)} \quad (24)$$

$$\text{Tr}[E(\rho)] = 1 \text{ (где } \text{Tr}[\rho] = 1), \text{ (сохранение следа)} \quad (25)$$

$$E(I \otimes \tilde{\rho}) \geq 0 \text{ (полная положительность)} \quad (26)$$

Это удовлетворяет I — операция тождества над дополнительной вспомогательной системой, $\tilde{\rho}$ — оператор плотности составной системы, включающей вспомогательную систему, 0 означает положительную полуопределенность. Давайте рассмотрим конкретный пример, который требует, чтобы точная положительность была физической операцией. Оператор транспонирования плотности

$T(\rho) = \rho^T$. Рассмотрим операцию, которая принимает Пусть $\rho = \sum_{ij} \rho_{ij} |i\rangle\langle j|$, тогда $T(\rho) = \sum_{ij} \rho_{ji} |i\rangle\langle j|$. с другой стороны,

$$\sum_{ij} \rho_{ij} |i\rangle\langle j| = \sum_{ij} \rho_{ji} |j\rangle\langle i| \quad (27)$$

$$= \left(\sum_{ij} \rho_{ij} |i\rangle\langle j| \right)^* \quad (28)$$

Поскольку $\rho \geq 0$, можно также сказать, что $T(\rho) \geq 0$. Следовательно, операция транспонирования удовлетворяет свойству положительности. Запутанные состояния в сложных системах

$$2 \frac{|01\rangle\langle 02| + |11\rangle\langle 12|}{\sqrt{2}} \quad (29)$$

Рассмотрим операцию $T \otimes I$, которая выполняет транспонирование только в одной системе. Оператор плотности

$$|\Phi^+\rangle\langle\Phi^+| = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad (30)$$

Таким образом, транспонирование следствия 1 равно

$$T \otimes I(|\Psi^+\rangle\langle\Phi^+|) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad (31)$$

, который не является положительно полуопределенным оператором, поскольку имеет отрицательное собственное значение. Мы не хотим допускать никаких квантовых манипуляций,

которые приводят к нефизическому состоянию путем выполнения квантовой манипуляции с одним из запутанных состояний. Поэтому может сохраняться не только положительная

определенность рассматриваемой системы, но и положительная определенность составной системы с дополнительными вспомогательными системами. Карта CPTP E всегда

κ Используя оператор Крауса E_k , удовлетворяющий $E^\dagger_k E_k = I$,

$$E_\rho = \sum_k E_k \rho E_k^\dagger \quad (32)$$

(представление Крауса). Кроме того, такая карта CPTP получается путем отслеживания вспомогательной системы до унитарной временной эволюции $U_{s,a}$ на составной системе

вспомогательной системы (a) и интересующей системы (s):

$$E_\rho = \text{Tr}_a[U_{s,a} \rho_{s,a} U_{s,a}^\dagger] = \sum_k E_k \rho E_k^\dagger, \quad (33)$$

Тогда с $\{|k\rangle_a\}$ в качестве ортонормированного базиса вспомогательной системы оператор Крауса записывается как $E_k = (I_s \otimes |k\rangle_a\langle a|) U_{s,a} (I_s \otimes |e\rangle_a\langle e|)$. Когда мы говорим о картах CPTP и квантовых операциях, нам может казаться, что мы делаем сложные вещи, которые в корне отличаются от эволюции унитарного времени. Однако невозможно манипулировать или наблюдать за всей вселенной, и описать всю вселенную затруднительно. в первую очередь.

Поэтому написано только в закрытой и удобной форме только для интересующей системы.

Аналогично, в составной системе, состоящей из интересующей системы (s) и вспомогательной системы (a), унитарная временная эволюция составной системы определяется как $U_{s,a}$,

Пусть a будет a и проективное измерение $\{|k\rangle_k\}$ во вспомогательной системе. Вероятность получения результата измерения k равна

$$p_k = \text{Tr}_{s,a}[I_s \otimes |k\rangle_k\langle k| U_{s,a} (\rho_s \otimes |e\rangle_a\langle e|) U_{s,a}^\dagger] \quad (34)$$

$$= \text{Tr}_s[E_k E_k^\dagger \rho_s] \quad (35)$$

становится. Другими словами, подставляя вместо оператора проектирования оператор $M_k = E_k^\dagger E_k$, определяемый как $E_k = \sum_i |a_i\rangle \langle a_i|$, мы получаем замкнутую форму интересующей нас системы,

$$p_k = \text{Tr}[M_k \rho]$$
 (36)

можно записать как Из определения очевидно, что $M_k \geq 0$ и $\sum_k M_k = I$, а p_k действительно является вероятностью (составная система проективное измерение). Состояние после измерения, когда получен результат измерения k , равно

$$E_k \rho E_k^\dagger / \text{Tr}[E_k \rho E_k^\dagger]$$
 (37)

Этот Таким образом, мы обычно называем $M_k \geq 0$ (положительная $\sum_k M_k = I$). Пусть множество $\{M_k\}$ таких операторов, что $M_k = I$, является оператором POVM (операторнозначная мера), обобщенная мера (мера POVM),

$$p_k = \text{Tr}[M_k \rho]$$
 (38)

определено. Измеряемым состоянием является оператор измерения $E_k = \sum_i |a_i\rangle \langle a_i|$, определенный через некоторый унитарный оператор U_k . Поэтому

$$E_k \rho E_k^\dagger / \text{Tr}[E_k \rho E_k^\dagger]$$
 (39)

дан кем-то Как описано выше, оператор плотности, оператор CPTP и измерение POVM были получены путем выполнения измерений чистого состояния, унитарной эволюции во времени и проективных измерений на составной системе и путем описания только интересующей системы.

3 кубита

3.1. Сфера Блоха

Поскольку я объяснил общий подход к квантово-механическим системам (конечные размерности), я перейду к основной теме квантовых компьютеров. Сказку порекомендую. Наименьшая единица информации в мире классической информации — это переменная с двумя значениями, 0 и 1, называемая битом. Точно так же наименьшая единица информации в квантовом мире описывается состоянием, кубитом, в двумерном комплексном гильбертовом пространстве. Квантовый бит имеет два ортогональных состояния

как линейная сумма

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ и } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle,$$
 (40)

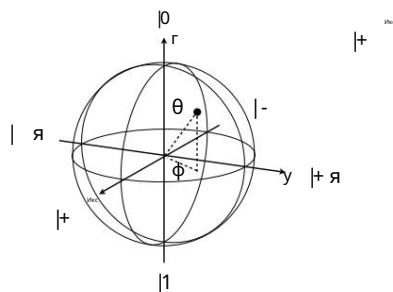
можно записать в общем виде где α и β — $|\alpha|^2 + |\beta|^2 = 1$ — комплексное число. Два ортогональных состояния $|0\rangle$ и $|1\rangle$ являются двумя ортогональными состояниями, такими как два энергетических состояния атомов, ортогональные состояния поляризации фотонов и спины электронов/ядер.

Любое квантовое состояние прекрасно. Эти комплексные числа задаются с помощью $\theta \in [0, 2\pi)$ и $\phi \in [0, \pi/2)$ как

$$\alpha = \cos \frac{\theta}{2} e^{i\phi}, \beta = \sin \frac{\theta}{2},$$
 (41)

можно записать как Обратите внимание, что фаза $e^{i\phi}$, действующая на все квантовое состояние, игнорируется, поскольку она не дает вклада в вероятность измерения. Используя эти θ и ϕ , состояние кубита можно представить на сфере радиуса 1 (сфера Блоха).

*7 Функция $f(A)$ эрмитова (самосопряженного) оператора A определяется как спектральный сегмент $f(a_i)\rho_i$ с использованием собственного значения $\{a_i\}$ оператора A и оператора проекции $\{\rho_i\}$ на собственное пространство. В частности, он определяется как $f(A) = \sum_i f(a_i)\rho_i$.



3.2 Оператор Паули

Давайте определим операторы для кубитов, необходимых для квантовых вычислений. Наиболее важным оператором является оператор Паули

быть:

$$\text{Я знак равенства } |0\rangle\langle 0|, \text{ Икс знак равенства } |1\rangle\langle 1|, \text{ Y знак равенства } \frac{1}{2}(|0\rangle\langle 1| + |1\rangle\langle 0|), \text{ Z знак равенства } \frac{1}{2}(|0\rangle\langle 0| - |1\rangle\langle 1|) \quad (42)$$

X, Y и Z иногда записывают как σ_1 , σ_2 и σ_3 , но часто удобно записывать их как X, Y и Z в квантовой информации, поэтому мы записываем их так.

Я решу. $X^2 = Y^2 = Z^2 = I$, $XZ = -ZX$ (любые два антикоммутируют друг друга), $Y = iXZ$ и т. д. часто используются,

так что давайте запомним их. Базис, определяющий кубит, - это $|0\rangle$ и $|1\rangle$ собственное состояние Z $|0\rangle = |0\rangle$ Z-оператора Паули, $Z|1\rangle = -|1\rangle$. Действие оператора X Паули на вычислительном базисе $\{|0\rangle, |1\rangle\}$ таково:

$$|1\rangle = X|0\rangle, |0\rangle = X|1\rangle. \quad (43)$$

Это имеет эффект инвертирования кубита как Как собственное состояние оператора X Паули, состояние суперпозиции $|0\rangle$ и $|1\rangle$,

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |1\rangle \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad (44)$$

Давайте определим Аналогично, как собственное состояние оператора Y Паули

$$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, \quad (45)$$

Давайте определим Пусть эти Паули X, Y.

, Пусть базой собственных состояний оператора Z являются X и Y, назвать это Z- базисом

Собственные состояния этих операторов Паули лежат на осях x, y, z на сфере Блоха. Координаты на сфере Блоха задаются с помощью оператора Паули

$$(rx, ry, rz) = (\text{Tr}[X\rho], \text{Tr}[Y\rho], \text{Tr}[Z\rho]), \quad (46)$$

можно также дать как В этом случае могут быть описаны не только чистые состояния, но и произвольные смешанные состояния одного кубита.

Чистота $\text{Tr}[\rho^2] = \text{Tr}[\rho]^2 + \text{Tr}[\rho^2]$ Следовательно, чистое состояние находится на сфере радиуса 1, а смешанное состояние — на ее поверхности.

соответствует внутри. Смешанное состояние с вероятностью 1/2 с вероятностями $|0\rangle$, $|1\rangle$ $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ соответствует началу сферы Блоха

Классические биты и их стохастические смеси соответствуют состояниям на оси z в сфере Блоха, в то время как общие квантовые состояния

Поскольку сферу и ее внутреннюю часть можно рассматривать как состояния, то можно видеть, что общая информация может быть выражена больше, чем классическая информация.

3.3 Адамар-топологический оператор

Следующими по важности однокубитными операторами являются оператор Адамара H и топологический оператор S:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S \text{ знак равенства } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Эти операторы переводят один базис Паули в другой базис Паули. Например, $H: \{|0\rangle, |1\rangle\} \rightarrow \{|\uparrow\rangle, |\downarrow\rangle\}$,

$S: \{|\uparrow\rangle, |\downarrow\rangle\} \rightarrow \{|\uparrow i\rangle, |\downarrow i\rangle\}$. Это соответствует тому, что сопряжение^{*8} этих операторов с операторами Паули дает другие операторы Паули :

$$X = HZH, Y = SXS^\dagger. \quad (47)$$

Действие оператора Адамара H на сфере Блоха соответствует перестановке осей x и z. Действие топологического оператора S заключается в вращении на $\pi/2$ вокруг оси z. Оператор, переводящий оператор Паули в оператор Паули при сопряжении таким образом, называется оператором Клиффорда^{*9}.

3.4 Произвольное вращение одного кубита

Можно построить произвольный 1-кубитный унитарный оператор, используя многократно действующие операторы Адамара и топологические операторы.

Я не могу сделать такую вещь. Однокубитный унитарный оператор U, вообще говоря,

$$U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \quad (48)$$

описывается четырьмя комплексными числами, а из $U^\dagger U = I$,

$$|u_{11}|^2 + |u_{21}|^2 = 1, \quad u_{11}^* u_{12} + u_{21}^* u_{22} = 0, \quad |u_{22}|^2 + |u_{12}|^2 = 1 \quad (49)$$

удовлетворит Любое комплексное число, которое удовлетворяет этому, должно быть

$$u_{11} = e^{i\alpha} e^{-i(\beta+\delta)/2} \cos(\gamma/2), \quad u_{21} = e^{i\alpha} e^{-i(\beta-\delta)/2} \sin(\gamma/2), \quad u_{12} = e^{i\alpha} e^{i(\beta-\delta)/2} \sin(\gamma/2), \quad u_{22} = e^{i\alpha} e^{i(\beta+\delta)/2} \cos(\gamma/2), \quad (50)$$

$$\sin(\gamma/2), \quad u_{22} = e^{i\alpha} e^{i(\beta-\delta)/2} \cos(\gamma/2), \quad (51)$$

можно записать как Из этого,

$$U = e^{i\alpha} e^{-i(\beta/2)Z} e^{i(\gamma/2)Y} e^{i(\delta/2)Z} e^{i\alpha} \quad (52)$$

можно разложить как где $e^{-i(\theta/2)A} = \cos(\theta/2)I - i\sin(\theta/2)A$ ($A = X, Y, Z$) — оси x, y, z на сфере Блоха, что соответствует к операции по

вращению θ вокруг. Следовательно, любой 1-кубитный унитарный оператор имеет общую фазу $e^{i\alpha}$

Кроме, его можно разложить на вращения вокруг двух ортогональных осей (разложение Эйлера).

В общем случае направление (r_x, r_y, r_z) на сфере Блоха ($|r_x|^2 + |r_y|^2 + |r_z|^2 = 1$), вращение θ равно

$$e^{i(\theta/2)(r_x X + r_y Y + r_z Z)} e \quad (53)$$

становится. Это можно показать из следующих фактов. Во-первых, если U — унитарный оператор, переводящий точку (1, 0, 0) на сфере

Блоха в (r_x, r_y, r_z) , то точка (1, 0, 0) соответствует $|\uparrow\rangle$. Используя

$$(r_x, r_y, r_z) = (\text{Tr}[U|\uparrow\rangle\langle\uparrow| + |U|\uparrow X|], \text{Tr}[U|\uparrow\rangle\langle\uparrow| + |U|\uparrow Y|], \text{Tr}[U|\uparrow\rangle\langle\uparrow| + |U|\uparrow Z|]) \quad (54)$$

удовлетворен. Поскольку $\text{Tr}[\sigma_i \sigma_j] = 2\delta_{ij}$, где σ_i ($i = 0, 1, 2, 3$) — оператор Паули (I, X, Y, Z),

$$U|\uparrow\rangle\langle\uparrow| + |U|\uparrow\rangle\langle\uparrow| = \frac{Y + X^\dagger}{2} U^\dagger = \frac{I + r_x X + r_y Y + r_z Z}{2} \quad (55)$$

$$UXU^\dagger = r_x X + r_y Y + r_z Z, \quad (56)$$

^{*8} Сопряжения оператора A с оператором B определяется $ABA^\dagger$. ^{*9} Если группа, порожденная

оператором Паули, является группой Паули, то оператор Клиффорда делает группу Паули инвариантной относительно сопряжения, т. е. группа Паули является

Это оператор, имеющий нормальную подгруппу. Такие операторы образуют группы и называются группами Клиффорда.

"=

*10 Операторная 1-норма есть $\text{Tr} \, A A^\dagger$ или разложение по сингулярным числам A и суммы всех сингулярных значений из A . 1-знак равно $A^\dagger A$ (собственных значений $A A^\dagger$). Кроме того, субаддитивность $A + B \leq A + B$ и субмультипликативное свойство $AB \leq A B$.

Следовательно, приближенное распределение вероятностей находится в пределах погрешности $2N\epsilon$ в смысле l_1 -нормы. Другими словами, если ошибку ϵ одной унитарной операции можно сделать достаточно меньшей, чем общее число N унитарных операторов, можно получить достаточно высокоточный результат.

3.6 Алгоритм Соловея-Китаева

Операторы Адамара и топологические операторы соответствовали перестановке осей и вращению $\pi/2$ на сфере Блоха, поэтому произведение этих операторов не может составлять произвольный унитарный оператор. Для аппроксимации 1-кубитного унитарного оператора с произвольной точностью ϵ мы также используем оператор $\pi/8$

$$T = e^{-i(\pi/8)Z} \quad (69)$$

Требуется. Поскольку вращение $\pi/8$ является рациональным числом, кратным π , кажется, что произведение этого оператора (и H и S) не может быть использовано для построения произвольного 1-кубитного унитарного оператора, но на самом деле направление, в котором $T H N$ Из следующего обсуждения видно, что вращение иррационально кратно π по отношению к π . первый,

$$V^{-1} T H N = e^{-i(\pi/8)Z} e^{-i(\pi/8)X} = \frac{1}{2} \begin{bmatrix} (2+1)I - iX - iZ - i(2-1)Y \\ (2-1)I + iX + iZ + i(2+1)Y \end{bmatrix}, \quad (70)$$

$$B^\dagger = \frac{1}{2} \begin{bmatrix} (2+1)I + iX + iZ + i(2-1)Y \\ (2-1)I - iX - iZ - i(2+1)Y \end{bmatrix}, \quad (71)$$

Затем,

$$V X V^\dagger = \frac{1}{2} (X + Y + Z) \quad (72)$$

$$B B^\dagger = \frac{1}{2} (X + Y - Z) \quad (73)$$

$$B Z B^\dagger = \frac{1}{2} (X - Y + Z) \quad (74)$$

, так что $X + \frac{1}{2}(Y+Z)$ инвариантен относительно сопряжения V . перпендикулярно направлению $(1, \frac{1}{2}, 1)$

Если мы выберем направление точки $(1/\sqrt{2}, 0, 1/\sqrt{2})$ на сфере Блоха в качестве направления вращения и $(\frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{4}, \frac{1}{2})$ есть повернем его на V , мы получим точку $(0, 1, 0)$.

$$\theta \text{ знак равно } \arccos \left(\frac{1}{\sqrt{2}} \right) \quad (75)$$

это угол, который удовлетворяет Этот угол поворота иррационально кратен π .

Он плотен для направленных вращений (может приближаться к любому углу поворота). Кроме того, из аналогичного рассуждения $H V N$ равно $\frac{1}{2}(X - Y + Z)$. Вращение иррационально кратно π вокруг направления $(1, 1, -2)$. Поскольку мы можем аппроксимировать любой угол поворота вокруг двух разных осей, мы можем аппроксимировать любой однокубитный унитарный оператор, повторяя их. Поэтому мы обнаружили, что произвольные 1-кубитные унитарные операции могут быть приближенно построены из двух 1-кубитных операций $\{H, T\}$. Из теоремы Соловея-Китаева известно, что многочлена от $\log(1/\epsilon)$ достаточно для количества $\{H, T\}$, необходимого для аппроксимации ошибки ϵ в смысле операторной нормы (например, [1] или [2]). Исходя из приведенного выше обсуждения, поскольку $1/\epsilon$ возрастает только полиномиально по отношению к числу операций с 1 кубитом, мы можем очень эффективно аппроксимировать идеальные операции с 1 кубитом.

4. Универсальные квантовые вычисления

Универсальное квантовое вычисление — это квантовое вычисление, которое может приблизительно выполнить любую унитарную операцию с n кубитами. Учитывая, что наш мир описывается квантовой механикой, универсальный квантовый компьютер может

Можно сказать, что это машина, которая может двигаться и совместима с любой физической системой, включающей в себя динамику любой квантовой системы. хотеть

Следовательно, когда становится очевидным какое-то ограничение на эволюцию во времени (квантовые вычисления) в универсальном квантовом компьютере, любая физическая система должна подчиняться этому ограничению (до тех пор, пока она следует квантовой механике). Далее мы увидим, как произвольная унитарная операция n кубитов может быть построена из конечного числа квантовых операций.

4.1 Работа CNOT

Чтобы построить произвольную n -кубитную унитарную операцию, нам нужны двухкубитные операции, требующие взаимодействия.

Становится. Типичной операцией с двумя кубитами является операция CNOT (управляемое не),

$$\Lambda_{c,t}(X) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c X_t,$$

*11. Когда c -система (система управления) равна 1, оператор X Паули применяется к t -системе (целевой системе). Для входных данных $|i\rangle_c |j\rangle_t$ базы расчета операция

CNOT выводит исключающее ИЛИ (XOR) в целевую систему, $\Lambda_{c,t}(X)|i\rangle_c |j\rangle_t = |i\rangle_c |i \oplus j\rangle_t$. Когда входное состояние системы c является состоянием суперпозиции $|+\rangle_c |0\rangle_t$,

выходное состояние максимально запутано

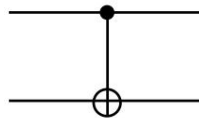
-состояние

н

C.

$$\Lambda_{c,t}(X)|+\rangle_c |0\rangle_t = (|00\rangle + |11\rangle)/\sqrt{2}, \quad (77)$$

становится. Работа CNOT описана на следующей принципиальной схеме с черными кружками на стороне управления и белыми кружками на целевой стороне:



Следуя классическим логическим схемам, горизонтальные линии представляют собой провода, по которым проходят кубиты, с квантовыми состояниями,

прогрессирующими слева направо. Λ_X работает при проходе по диаграмме операции CNOT.

"_"

Операция Адамара H и топологическая операция S были операциями Клиффорда, которые отображают операторы Паули в операторы Паули. операция CNOT

Паули $\{\pm I, \pm i\} \times \{I, X, Y, Z\}$ состоит из двухкубитных операторов Паули, инвариантных относительно сопряжения $U^\dagger$ и U . Пусть группа U Клиффорда

Назовем его оператором. Для операции CNOT, в частности

$$\Lambda_{c,t}(X)_c^\dagger I_t \Lambda_{c,t}(X) = X_c X_t, \quad (78)$$

$$\Lambda_{c,t}(X)_c^\dagger I_t \Lambda_{c,t}(X) = I_c X_t, \quad (79)$$

$$\Lambda_{c,t}(X)_c^\dagger Z_t \Lambda_{c,t}(X) = Z_c I_t, \quad (80)$$

$${}_c^\dagger \Lambda_{c,t}(X)_c^\dagger I_t \Lambda_{c,t}(X) = Z_c Z_t, \quad (81)$$

, что подтверждает, что это оператор Клиффорда. Любая n -кубитная операция Клиффорда может быть построена из операций Клиффорда $\{H, S, \text{CNOT}\}$, которые мы видели до сих пор.

*11 Пусть оператор A , действующий на k -й кубит, равен

$$A_k = \overbrace{A}^{k-1} \cdots \overbrace{A}^{n-k-1} \quad (76)$$

будет написано как

4.2 Арифметика Клиффорда и теорема Готтсмана-Книлла

В случае 1-кубита мы не могли построить унитарную операцию 1-кубита из H и S. Точно так же невозможно построить произвольные n-кубитные унитарные операторы из операций Клиффорда {H, S, CNOT}. Напротив, квантовые вычисления^{*12}, состоящие из подготовки начального состояния в Z-базисе, операций Клиффорда и проекционных измерений в Z-базисе, могут быть эффективно смоделированы на классическом компьютере (запутанное состояние. Вы можете генерировать столько, сколько хотите). Чтобы понять это, давайте охарактеризуем квантовые вычисления в терминах операторов. Сначала подготавливается n как начальное состояние. Это состояние представлено оператором {Zⁱ} n-членных n кубитов |0>. Состояние, полученное после применения n-кубитной операции Клиффорда U, равно U|0>.

Собственное состояние является собственным значением +1.

$$U|0\rangle^H = UZ_i|0\rangle^H = UZ_iU^\dagger(U|0\rangle^H) = Si(U|0\rangle^H), \quad (82)$$

Следовательно, {Sⁱ} n i=1 (Sⁱ = UZ_iU[†]). Поскольку теперь U ограничивается операциями Клиффорда, оказывается, что {Sⁱ} является тензорным произведением n-кубитных операторов Паули, которые коммутируют друг с другом. Распределение вероятностей проективного измерения собственного состояния {Sⁱ} с помощью Z-базиса может быть эффективно вычислено из коммутационного соотношения между {Sⁱ} и Z-оператором (теорема Готтсмана-Книлла, например [1] или [2]). Таким образом, форма, которая описывает квантовое состояние с помощью оператора стабилизатора, который имеет состояние в качестве собственного состояния, называется формой стабилизатора. Готтсман-Нилл

Теорема означает, что квантовая схема, состоящая только из операций Клиффорда, может быть классически смоделирована, но в то же время это также означает, что в некоторых случаях можно эффективно описать даже сильно запутанные и сложные квантовые состояния. На самом деле, многие запутанные состояния многих тел, важные для квантовой информации, такие как квантовые коды с исправлением ошибок и состояния ресурсов в квантовых вычислениях, основанных на измерениях, могут быть эффективно описаны в форме стабилизатора (см., например, [3]).

4.3 Управление унитарным режимом

Вернемся к универсальным квантовым вычислениям. На самом деле, {H, T}, которая может аппроксимировать любую уже введенную однокубитную унитарную операцию, Любая унитарная операция может быть построена из трех типов унитарных операций CNOT. Метод построения довольно сложен, поэтому давайте построим его поэтапно. Во-первых, требуется операция управления U.

$$\Lambda_{c,t}(U) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c U_t, \quad (83)$$

является. Если управляющая система |0>, ничего не делается, а если |1>, то к целевой системе применяется унитарная операция U. Думайте об этом как об обобщении операции CNOT. Давайте посмотрим, как построить эту операцию управления U из CNOT и унитарных операций с 1 кубитом. Во-первых, поскольку унитарная операция U есть U = e^{iφ} e^{iβZ} e^{iγX} e^{iδZ} из разложения Эйлера, для U = e^{iαI} *13 и U = e^{i(θ/2)A} (A = X, Y, Z) Хорошо, если Λ(U) реализуется Во-первых, поскольку Λ(e^{iαI}) есть не что иное, как «относительная фаза» кубитов в системе управления, мы можем применить e^{i(α/2)Z} к системе управления. Далее рассмотрим Λ(e^{i(θ/2)Z}), где A = Z. e^{i(θ/2)Z} = e^{i(θ/4)Z} e^{i(θ/4)ZX}

Используя I = e^{i(θ/4)Z} I e^{i(θ/4)Z} I,

$$\Lambda_{c,t}(e^{-i(θ/2)Z}) = \Lambda_{c,t}(X) e^{-i(θ/4)Z} \Lambda_{c,t}(X) e^{-i(θ/4)Z} \quad (84)$$

^{*12} Поскольку базис можно преобразовать с помощью арифметики Клиффорда, то же самое можно сделать, даже если начальное состояние и измерение выполняются в базисе Паули.

^{*13e} Вы можете подумать, что iδ не имеет значения, потому что это общая фаза, но в случае расчета управления она становится относительной фазой, поэтому с ней нужно обращаться правильно. не иметь.

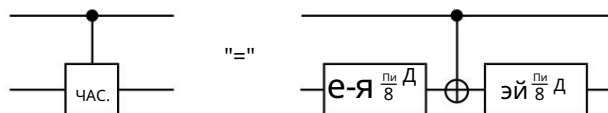
1 0 0

Сопряженно воздействуя H и S на целевую систему, можно аналогичным образом вращать ее вокруг оси Y. Вот что

управляющая операция Адамара Λ (H) есть $H = e$

"="

Используя тот факт, что CBA $\pi/8Y X e \pi/8$, это реализуется следующим образом: например,



(Обратите внимание, что схема идет слева направо, но формула умножается слева.)

4.4 Арифметика Тоффоли и обратимые вычисления

Далее введем еще одну унитарную операцию, операцию Тоффоли, важную для доказательства универсальности. Тоффоли

Операция представляет собой унитарную операцию, действующую на три кубита,

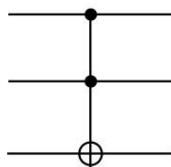
"="

$$\Lambda^2_{c1,c2,t}(X) = (I_{c1} I_{c2} |1\rangle\langle 1|_{c1} |1\rangle\langle 1|_{c2}) I_t + |1\rangle\langle 1|_{c1} |1\rangle\langle 1|_{c2} X_t, \quad (85)$$

определяется как Существуют две системы управления, обе из которых являются обобщениями операции CNOT, которые применяют оператор X Паули к целевой системе только тогда, когда существует состояние $|1\rangle$. Для входного состояния $|i1c1 i2c2 jt\rangle$ базиса вычислений

$$\Lambda^2_{c1,c2,t}(X) |i1c1 i2c2 jt\rangle = |it1 i2c2 j\rangle (i1 i2) X_t. \quad (86)$$

Выводит логическое произведение (И) в целевую систему.

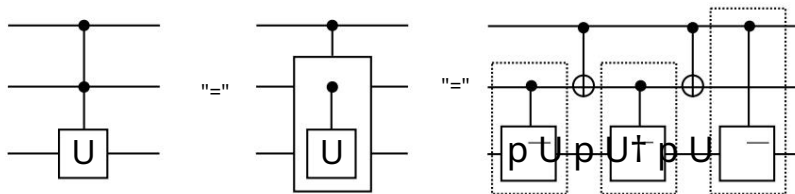


Покажем, что операции Тоффоли также могут быть построены из $\{H, T, CNOT\}$. Операция Тоффоли управляется операцией CNOT. Поскольку все, что нам нужно сделать, это добавить систему, мы должны реализовать $\Lambda(\Lambda(X))$. Λ в целом $\Lambda^2(U) = \Lambda(\Lambda(U))$ есть

$$\Lambda_{c,t}(U) = U_t X_c \Lambda_{c,t}(U^\dagger) X_c \Lambda_{c,t}(\bar{U}) \quad (87)$$

Поэтому, чтобы дополнительно контролировать это,

$$\Lambda^2_{c1,c2,t}(U) = \Lambda_{c1,t}(\bar{U}) \Lambda_{c1,c2}(X) \Lambda_{c2,t}(\bar{U}^\dagger) \Lambda_{c1,c2}(X) \Lambda_{c,t}(\bar{U}) \quad (88)$$



(89)

Хорошо, если Если $U = X$, то можно построить арифметику Тоффоли. $\Lambda(X)$ выражается как

"="

T†

XT

T† T

T†

ЧАС.

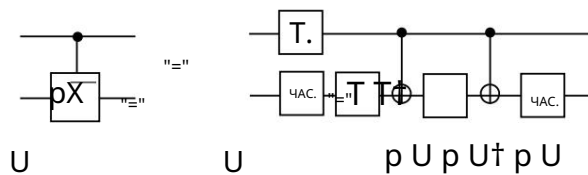
$$T = e(-i\pi/8)Z$$

XT T†

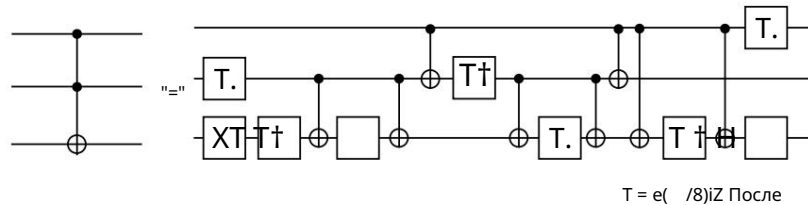
T.

T† H

$$T = e(-i\pi/8)Z$$

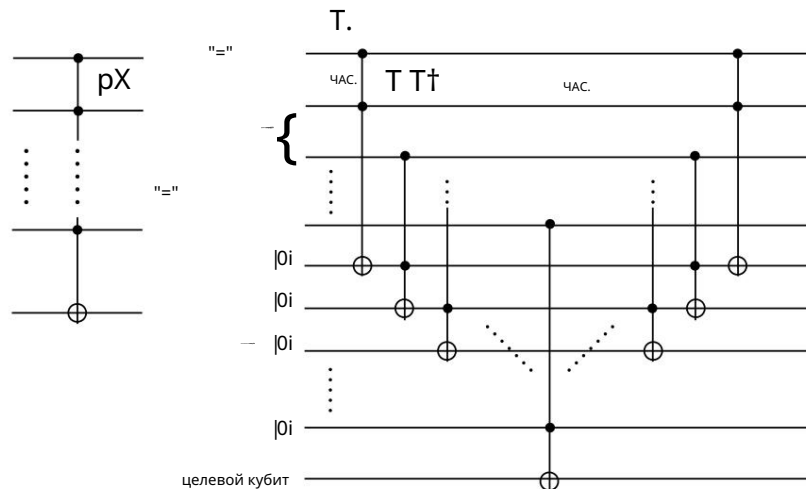


, а операцию Тоффоли можно разложить с помощью операции T следующим образом.



$$T = e(-i\pi/8)Z$$

того, как операция Тоффоли построена, мы можем произвольно умножать систему управления, используя вспомогательные системы следующим образом:



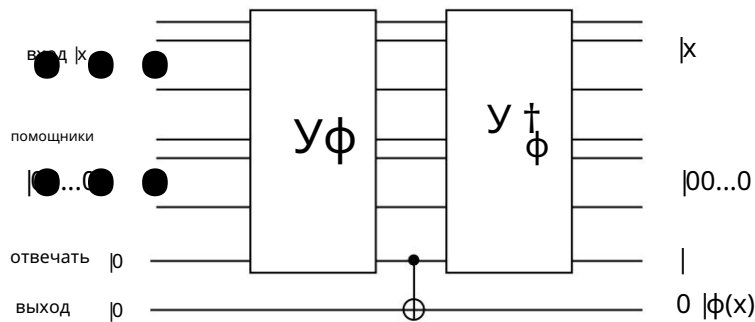
В операции Тоффоли, если входное состояние целевой системы равно $|1\rangle$, выход целевой системы равен $|0\rangle$. Это соответствует операции NAND. Другими словами, операция Тоффоли реализует операцию И-НЕ с обратимой унитарной операцией. Схемы произвольной логики (булевы функции) могут быть построены из операций И-НЕ, и известно, что классические логические схемы обладают универсальностью. Кроме того, поскольку квантовые вычисления выполняются с использованием унитарных операций, вычисления могут быть обратимыми. Построим обратимое вычисление выхода булевой функции $f: \{0, 1\}^n \rightarrow \{0, 1\}$ для входа $x \in \{0, 1\}^n$. Поскольку мы знаем, что операция Тоффоли строится из операций И-НЕ, мы можем использовать обратимую унитарную операцию U_f соответствующую

$$U_f |x\rangle |0\rangle \dots |0\rangle |0\rangle_{\text{ответ}} = |x\rangle |g(x)\rangle |f(x)\rangle_{\text{ответ}}, \quad (90)$$

и получается выход $f(x)$. Однако, чтобы сделать вычисления обратимыми, вспомогательные кубиты оставляют некоторый вычислительный мусор $|g(x)\rangle$ ancilla, и можно подумать, что эта инициализация потребует необратимой операции. Однако этот мусор копирует результат вычисления $f(x)$ в новый кубит и сохраняет его (поскольку он ортогонален, его можно скопировать), а обратное вычисление

(без вычисления) $U^\dagger$ Вы можете восстановить исходное состояние, выполнив:
 ϕ

$$\begin{aligned} & f \wedge \text{answer, out}(X) U^\dagger |x_{\text{вход}}|0\dots 0 \text{анцилла}|0 \text{ответ}|0 \text{выход} \\ &= U^\dagger |x_{\text{вход}}|g(x) \text{анцилла}|f(x) \text{ответ}|f(x) \text{out} \\ &= |x_{\text{вход}}|0\dots 0 \text{анцилла}|0 \text{ответ}|f(x) \text{выход}. \end{aligned} \quad (91)$$



Как описано выше, мы обнаружили, что $f(x)$ можно вычислить, не оставляя мусора, только из обратимых операций. Этот результат был получен Тоффли и другими в процессе исследования физических пределов вычислений (проблемы потребления энергии и тепловыделения) в 1980-х годах, до формализации квантовых вычислений. Получено Fredkin et al. С тех пор исследования перешли к универсальным квантовым вычислениям, которые активно используют квантовую механику для вычислений. стал.

4.5 Универсальные квантовые вычисления

Теперь, когда мы наконец готовы, давайте покажем, что мы можем приблизительно построить любой n -кубитный унитарный оператор из $\{H, T, CNOT\}$. Во-первых, мы показываем, что любой n -кубитный унитарный оператор U , действующий на 2^n -мерном комплексном гильбертовом пространстве H_n , может быть разложен на унитарные операторы (двухуровневые унитарные операторы) в 2-мерном подпространстве n . Переобозначая базис с целыми числами от 1 до m , мы имеем двухуровневый унитарный оператор для двух базисов $|i\rangle$ и $|j\rangle$ ($i, j \in \{1, 2, \dots, m\}$) вида Пусть это будет T_{ij} . *14 В это время, соответствующим образом выбрав элементы $T_{m-1, m-2} \dots T_{m-1, 1}$,

$$U T_{m-1, m-2} \dots T_{m-1, 1} = \begin{pmatrix} U_{11} & \dots & U_{1, m-1} \\ \vdots & \ddots & \vdots \\ U_{m-1, 1} & \dots & U_{m-1, m-1} \end{pmatrix}, \quad (92)$$

может быть преобразован в U где $(U)_{kl} = u_{kl}$ — матричный элемент U . Повторяя эту операцию,

$$U T_{m-1, m-2} \dots T_{m-1, 1} = \begin{pmatrix} u_{11} & \dots & u_{1, m-1} \\ \vdots & \ddots & \vdots \\ u_{m-1, 1} & \dots & u_{m-1, m-1} \end{pmatrix} = \begin{pmatrix} u_{11} & \dots & u_{1, m-1} \\ \vdots & \ddots & \vdots \\ u_{m-1, 1} & \dots & u_{m-1, m-1} \end{pmatrix} \quad (93)$$

Вы можете установить в m -й строке все нули, кроме диагональных членов, как в U . Кроме того, поскольку это унитарный

оператор, мы автоматически знаем, что $u_{mm} = 0$ и $|u_{mm}| = 1$. Мы называем его диагональным унитарным оператором D . Мы можем преобразовать эту операцию R_k в $k = 1, \dots, m$:

$$U = D(R_m R_1)^\dagger. \quad (94)$$

*14 Когда матричный элемент T_{ij} равен $(T_{ij})_{kl}$, когда $k, l = i, j$, $(T_{ij})_{kl} = \delta_{kl}$, а четыре элемента, соответствующие $k, l = i, j$, равны 2×2 . Постройте унитарный оператор. Обратите внимание, что он действует как тождественный оператор вне подпространства $\{|i\rangle, |j\rangle\}$.

Поскольку D больше не имеет только диагональных членов, его тривиально разложить на произведение двухуровневых унитарных операторов (диагональных). Следовательно, мы можем разложить U в произведение двухуровневых унитарных операторов.

Наконец, мы показываем, что двухуровневый унитарный оператор T_{ij} может быть реализован с помощью операций Тоффоли и операций управления U (и $\{H, T, CNOT\}$). Поскольку и операция Тоффоли, и операция управления U могут быть построены из $\{H, T, CNOT\}$, мы можем построить любую n -кубитную унитарную операцию из $\{H, T, CNOT\}$.

Хотя i и j являются целыми числами от 1 до m , они переписываются с использованием двоичных чисел (n -битных строк) как $s = s_1s_2\dots s_n$ и $t = t_1t_2\dots t_n$ соответственно. Затем последовательность $\{g_k\}$ битовых последовательностей, начинающихся с s и инвертирующих только один бит на каждом шаге k .

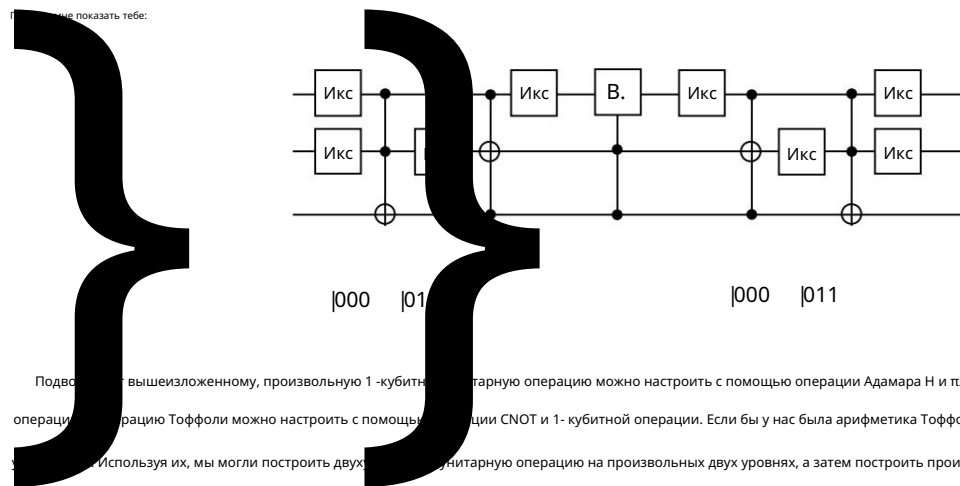
$$s = g_0 \quad g_1 \quad g_d = t \quad (95)$$

можно легко найти. Здесь d — общее количество различных битов (расстояние Хэмминга) двух битовых строк s и t .

Поскольку битовые строки s и g_1 отличаются только одним битом, используя операцию Паули X или операцию Тоффоли, в качестве управляющей системы используется одна и та же часть битовой строки, а целевая система — разные биты. Можно построить унитарный оператор, который преобразует $|s\rangle$ в $|g_d\rangle$. Повторяя это, мы можем преобразовать $|s\rangle$ в $|g_d\rangle$. Наконец, поскольку $|t\rangle$ и $|g_d\rangle$ отличаются только одним битом, в этом базисе двухуровневый унитарный оператор становится однокубитным (подпространственным) унитарным оператором с той же битовой строкой, что и управляющая система. Сделав это с помощью управляющих унитарных операций и вернувшись к исходному базису, мы смогли построить двухуровневые унитарные операции $|s\rangle$ и $|t\rangle$.

В качестве конкретного примера приведем пример реализации унитарного оператора, действующего на подпространстве $\{|000\rangle, |011\rangle\}$ из 3 кубитов (8-мерное пространство).

Итак, давайте покажем тебе:



Подводя итог вышесказанному, произвольную 1-кубитную унитарную операцию можно настроить с помощью операции Адамара H и $\pi/8$ -операции T , а управляющую унитарную операцию Тоффоли можно настроить с помощью операции $CNOT$ и 1-кубитной операции. Если бы у нас была арифметика Тоффоли, мы могли бы добавить систему U и T . Используя их, мы могли бы построить двухуровневую унитарную операцию на произвольных двух уровнях, а затем построить произвольный n -кубитный унитарный оператор.

Следовательно, если есть три типа операций $\{H, T, CNOT\}$, можно выполнить универсальное квантовое вычисление. Такой набор операций называется универсальным набором операций.

5 квантовых алгоритмов

Здесь мы объясним, чем квантовые компьютеры превосходят классические компьютеры, используя квантовый алгоритм, называемый тестом Адамара. В качестве расширения теста Адамара можно понять алгоритм оценки фазы и алгоритм простой факторизации, которые являются очень важными квантовыми алгоритмами.

5.1 Косвенное измерение

Как и в детекторах фотонов, часто бывает так, что квантовое состояние после измерения разрушается. В таких случаях после измерения

Чтобы оставить проектное состояние включенным, необходимо провести косвенное измерение с помощью вспомогательной системы. Пусть A эрмитова с собственными значениями ± 1

Diagram 1: A quantum circuit with two qubits. The first qubit starts in state $|0\rangle$ and passes through a Hadamard gate (H). The second qubit starts in state $|1\rangle$ and passes through a Hadamard gate (H). Both qubits then enter a CNOT gate, with the first qubit as the control and the second qubit as the target. Finally, the first qubit is measured, and the result is shown on a meter.

$$\frac{I + (1)SA}{\psi} / \frac{\text{Tr}[I + (1)SA/2|\psi\rangle\langle\psi|, |0\rangle\langle 0|_2]}{\psi} \quad (96)$$

Вот что происходит.	$ \Phi\rangle$	3.	m1
Алиса			
	$ +\rangle$	Икс	m2

$$= \frac{1}{2} [\langle \psi | \psi \rangle + \langle U \psi | U \psi \rangle] \quad (97)$$
$$p_0 = \frac{1}{4} \begin{pmatrix} 1 & (I+U) \\ -U & 1 \end{pmatrix} |\psi\rangle, \quad p_1 = (I - \dots) \quad (98)$$
$$1 - \frac{1}{2} \frac{\text{Re}(\psi^\dagger U \psi)}{\|\psi\|^2}, p_1 = \frac{1}{2} \frac{\text{Re}(\psi^\dagger U \psi)}{\|\psi\|^2}, p_0 = \frac{1}{2} \frac{\text{Re}(\psi^\dagger U \psi)}{\|\psi\|^2} \quad (99)$$

$$\psi|U|\psi \quad (100)$$

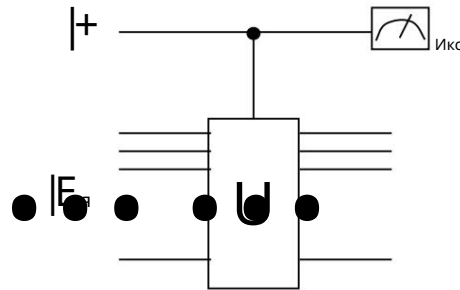
$$\overline{M} \cdot P_0 > \epsilon \Rightarrow 2e^{2M}, \quad (101)$$

кроме как работать с матрицами соответствующего размера. Здесь наглядно показано превосходство квантового компьютера над классическим.

Подобные квантовые алгоритмы могут быть построены. Гамильтонова динамика e^{-iHt} и U

5.3 Оценка фазы

Я МОГ

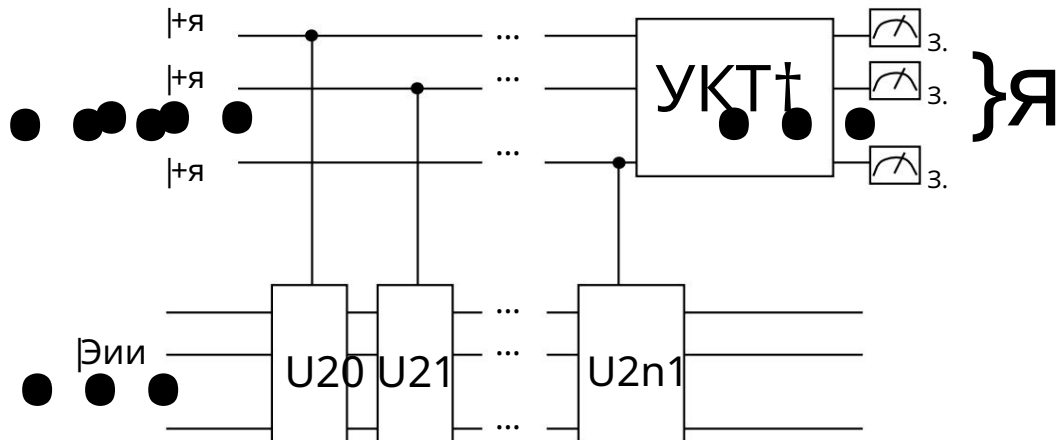


К сожалению, тест Адамара не может найти фазу ϕ в показателе степени собственного значения $e^{i\phi}$ с экспоненциальной точностью (до полиномиальных цифр).

Однако, используя алгоритм оценки фазы Китаева, который имеет хорошо построенную вспомогательную систему, мы можем оценить ϕ с экспоненциальной точностью. Число может быть определено фазой ϕ с двоичными десятичными знаками как $e^{2\pi i 0.j_1 j_2 \dots j_n}$ ($j_k \in \{0, 1\}$). Я напишу. Определение двоичного десятичного

$$e^{2\pi i 0.j_1 j_2 \dots j_n} = \prod_{k=1}^n e^{2\pi i j_k / 2^k} \quad (102)$$

является. В отличие от теста Адамара алгоритм оценки фазы использует вспомогательную систему из n кубитов для нахождения битовых последовательностей $j_1, \dots, j_n$ по следующей схеме:



Здесь UQFT представляет собой квантовое преобразование Фурье, которое будет объяснено позже. n вспомогательных кубитов установлены в $|1\rangle$, и каждый из них используется в качестве управляющего кубита для получения соответствующего значения $j_k \in \{0, 1\}$ ($k = 1, 2, \dots, n$), квантовое состояние вспомогательных кубитов перед каждым измерением равно $|1\rangle$.

Собственное состояние $e^{2\pi i 0.j_1 j_2 \dots j_n}$ — откат по фазе. Эй

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i 0.j_1 j_2 \dots j_n} |j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i 0.j_1 j_2 \dots j_n} |j\rangle \quad (103)$$

становится. Конечная цель состоит в том, чтобы преобразовать это состояние в $|j_1\rangle |j_2\rangle \dots |j_n\rangle$ и получить информацию о $j_1, \dots, j_n$ из измерений вычислительного базиса. Действие квантового преобразования Фурье

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i 0.j_1 j_2 \dots j_n} |j\rangle \xrightarrow{\text{UQFT}} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i 0.j_1 j_2 \dots j_n} |j\rangle \quad (104)$$

, заставив обратное квантовое преобразование Фурье точно решить целевую задачу. Квантовая схема для обратного квантового преобразования Фурье

$$U_{x|us} = e^{-2\pi i(s/r)} |_{us}, \quad (108)$$

Видно что есть. Поскольку входным состоянием для оценки фазы является $|1\rangle = \frac{1}{\sqrt{2}}(|s\rangle + |t\rangle)$, ввод $|1\rangle$ дает стохастическое собственное состояние $|s\rangle$ путем оценки фазы. Используя алгоритм оценки фазы, можно эффективно оценить s/r , а r можно получить, переписав его в рациональных числах, используя разложение в непрерывные дроби. Если $|s\rangle$ выбирается случайным образом из $|1\rangle$, s и r взаимно просты с высокой вероятностью, поэтому порядок r может быть получен. Также с Он также гарантированно будет четным. Поэтому x^p большой вероятностью полученный порядок преобразует $= 1 \pmod{N}$ в $(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{N}$ (так как $x^p \equiv 1 \pmod{N}$ и $x^{r/2} \equiv \pm 1 \pmod{N}$). Если $x^{r/2} \not\equiv \pm 1 \pmod{N}$, то $(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{N}$ делится на N , и $x^{r/2} \pm 1$ делится на N . Если $x^{r/2} \equiv \pm 1 \pmod{N}$, то $x^{r/2} - 1$ делится на N , и $x^{r/2} + 1$ делится на N .

Исс

Исс

можно прикрепить.

5.5 Задача BQP и тест Адамара

До сих пор я создавал квантовые алгоритмы, основанные на тесте Адамара. Поскольку тест Адамара является примером квантовой схемы, может показаться, что задача нахождения матричных элементов $\langle \psi | U | \psi \rangle$ с помощью теста Адамара уже, чем класс задач, которые может решить квантовый компьютер. Но также можно показать, что они одинаково трудны. Во-первых, давайте определим задачу, которую может решить квантовый компьютер. Так как многие задачи можно свести к задачам, возвращающим два значения да (0) и нет (1), рассмотрим простейшую задачу суждения да или нет. Например, при простой факторизации для целых чисел N и M , где $1 \leq M \leq N$, делится ли N на x , где $x \leq M$? Мы можем рассмотреть проблему решения. Выполняя бинарный поиск по ответам «да» и «нет», мы практически можем найти множитель x . Другим типом проблемы принятия решения является задача проверки простоты, которая определяет, является ли целое число N простым. Известно, что она разрешима за полиномиальное время на классическом компьютере.

Теперь вернемся к определению проблемы решения, которую может решить квантовый компьютер. Для квантовых систем выходные данные обычно задаются стохастически.

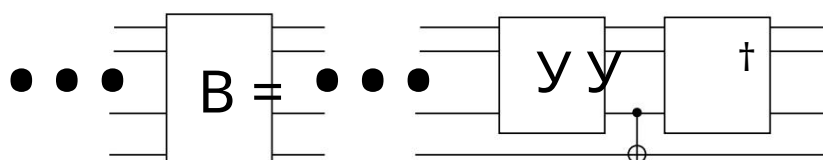
Поэтому ставим условие, что правильный ответ должен быть получен с очень большой вероятностью. Другими словами, существует квантовая схема U полиномиального размера для размера задачи n .

$$\text{Вероятность (да | да)} > 1/2 + \delta, \text{ Вероятность (да | нет)} < 1/2 - \delta \quad (109)$$

Если да, то все в порядке. δ — параметр, не зависящий от размера задачи n . Кроме того, если $0 < \delta < 1/2$, класс задач можно определить вне зависимости от его значения. Это связано с тем, что если в U включить квантовую схему, которая выполняет голосование большинством, вероятность успеха может быть максимально увеличена. Поэтому, включив при необходимости в квантовую схему U схему усилителя, можно получить правильный ответ с вероятностью, экспоненциально близкой к 1. Класс задач, которые могут быть решены в этом смысле, называется BQP (вычисление квантового полиномиального времени с ограниченной ошибкой). Выходом квантовой схемы, которая решает вышеупомянутую проблему принятия решения, является измерение в 1 кубит, но используется обратный расчет, используемый для обратимого расчета.

, новый унитарный оператор V есть

$$V = U \dagger A(X) U, \quad (110)$$



(111)

Определяя

$$p_0 = \text{Tr}[p_0 U(|0\rangle\langle 0| \otimes \dots \otimes |0\rangle\langle 0| U^\dagger)] = \langle 0| \otimes \dots \otimes \langle 0| V |0\rangle\langle 0| \otimes \dots \otimes |0\rangle\langle 0| \quad (112)$$

можно записать как Следовательно, всегда существует унитарный оператор $V^* = V^{-1} = V^\dagger$, соответствующий квантовой схеме U , решающей задачу решения ϕ , и его матричный элемент $\langle 0 | \langle 2n(V^{-1} V^\dagger) | 0 \rangle$ классическая задача решения принадлежит к классу BQP (или BQP), если она столь же сложна, как и задача решения BQP -трудной, если она столь же сложна, как и задача решения BQP -полной, если она столь же сложна, как и задача решения BQP -полной. Следовательно, для данного унитарного оператора W проблема определения того, является ли $\langle 0 | \langle nW | 0 \rangle$ больше $1/2 + \delta$ или меньше $1/2 - \delta$, является BQP -полной, называемой проблемой. Задача BQP может показаться искусственной, далекой от физики, но может ли она с хорошей точностью аппроксимировать матричные элементы унитарного оператора? Поскольку это совместимо с проблемой

Можно сказать, что он становится

Например, рассмотрим следующий гамильтониан в гибридной системе n -кубитов и $(M + 1)$ -мерных квантовых систем:

$$H = \sum_{j=0}^M (U_{j+1} |j+1\rangle \langle j| + U_j^\dagger |j\rangle \langle j+1|). \quad (113)$$

Это гамильтониан, придуманный Фейнманом в 1980-х годах, где n -кубитная система — это рабочее пространство для выполнения квантовых вычислений, а M -мерная квантовая система — это пространство часов, соответствующее вычислительным временным шагам. Пусть начальное состояние равно $|0\rangle^n$. Пусть $|j\rangle$ будет состоянием суперпозиции (называемым историческим состоянием) состояния, в котором квантовое вычисление продвинулось к шагу k при эволюции во времени стационарным гамильтонианом.

$$e^{-iHt} |0\rangle^n |0\rangle^M = \sum_{k=0}^M C_k(t) \left(\sum_{j=1}^n U_j |j\rangle \right) |k\rangle. \quad (114)$$

получается. Следовательно, матричный элемент унитарного оператора по стационарному гамильтониану равен

$$\langle 0 | \langle n | e^{-iHt} | 0 \rangle^n | 0 \rangle^M = \langle 0 | \langle n | C_M(t) \left(\sum_{j=1}^n U_j \right) | 0 \rangle^n. \quad (115)$$

Поскольку полная задача BQP может быть встроена, *15 амплитуда вероятности перехода динамики в реальном времени при естественном стационарном гамильтониане также встроена со сложным вычислением, эквивалентным универсальному квантовому вычислению. H , построенная Фейнманом, может показаться искусственной моделью, но в настоящее время взаимодействие двух ближайших соседей (частиц со спином $1/2$) для кубитов (частиц со спином $1/2$), расположенных на двумерной квадратной решетке со случайностью, представляет собой известно, что такую динамику можно вложить в гамильтониан действия. Следовательно, можно сказать, что динамика квантовых систем многих тел в реальном времени, включая случайность, которую изучает некий физик конденсированного состояния, непреднамеренно имеет дело с такими сложными проблемами, как универсальные квантовые компьютеры.

Неудивительно, что может быть

6 Квантовая декогеренция

В общем, квантовое состояние уязвимо для декогеренции из-за связи с окружающей средой, и квантовая природа быстро теряется. Например, при использовании в качестве кубита основного состояния и возбужденного состояния возникают явления продольной релаксации, при которых возбужденное состояние выделяет энергию и становится основным состоянием, и явления фазовой релаксации, при которых энергетический интервал флуктуирует из-за влияния внешнего поля. Попробуем понять декогеренцию, вызванную сцеплением (запутыванием) с внешним миром, используя простую модель. Сначала рассмотрим составную систему, состоящую из системы кубитов (систем) и системы окружения (е). Состояние кубита: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Для простоты система окружения также состоит из одного кубита, а начальное состояние — $|0\rangle_e$. Это состояние является гамильтонианом

$$H_{\text{ЭМ}} = \gamma (\sigma_c^+ \sigma_e + \sigma_c^- \sigma_e^+) \quad (116)$$

*15 Либо точно вычислить $C_M(t)$, либо получить $p_{0,1}$, соответствующий выходу задачи решения из соотношения $\langle 1 | \langle 0 | \langle n | e^{-iHt} | 0 \rangle^n | 0 \rangle^M$.

Пусть время развивается под где $\sigma = \pm 1$

$|1 \ 0\rangle, \sigma = -1$ — низкоэнергетическое состояние, $|1 \ 1\rangle$ — высокоэнергетическое состояние.

оператор, повышающий и понижающий энергию. *16 Квантовое состояние в момент времени t равно

$$e^{-iH_{\text{amp}}t} = e^{-igt(\sigma_c^+ \sigma_e^- + \sigma_c^- \sigma_e^+)} |\psi\rangle \quad (117)$$

$$|0\rangle = \alpha |00\rangle + \beta [\cos(gt)|10\rangle + i \sin(gt)|01\rangle] \quad (118)$$

Видно, что кубит запутан с окружающей средой. Предполагая, что система окружающей среды недоступна, получение приведенной матрицы плотности системы s дает

$$\rho_s = \frac{1}{2} \sin^2(gt) |0\rangle\langle 0| + \frac{1}{2} \cos^2(gt) |1\rangle\langle 1| \quad (119)$$

$$\rho_s = \frac{1}{2} \begin{pmatrix} \alpha^2 + \beta^2 \cos^2(gt) & \alpha\beta \cos(gt) \\ \alpha\beta \cos(gt) & \beta^2 \sin^2(gt) \end{pmatrix} \quad (120)$$

, а амплитуда состояния $|\psi\rangle$ уменьшается. $|\psi\rangle \rightarrow \rho_s$ — оператор Крауса

$$E_1 = (1 \ 0 \cos(gt)), \quad E_2 = (0 \ \sin(gt) \ 0), \quad (121)$$

Как

$$E_{\text{amp}}[t](\rho) = E_1 \rho E_1^\dagger + E_2 \rho E_2^\dagger \quad (122)$$

дан кем-то

Давайте посмотрим на другой пример. Начальное состояние системы окружения есть $|1\rangle$, а гамильтониан взаимодействия есть

$$H_{\text{int}} = (r/2) Z_s Z_e \quad (\text{одни два три})$$

Рассмотрим ситуацию, заданную В отличие от предыдущего примера здесь нет обмена энергией с окружающей системой. Состояние составной системы в момент времени t состояние

$$e^{-iH_{\text{int}}t} = \frac{1}{2} e^{i\alpha/2} (|00\rangle + |11\rangle) + \frac{1}{2} e^{-i\alpha/2} (|01\rangle + |10\rangle) \quad (124)$$

, который снова запутывается с окружающей средой. Отслеживая систему e и вычисляя сокращенный оператор плотности для системы s ,

$$\rho_s = \frac{1}{2} \begin{pmatrix} \alpha^2 + \cos^2(gt) & \alpha\beta \cos(gt) \\ \alpha\beta \cos(gt) & \beta^2 \sin^2(gt) \end{pmatrix} \quad (125)$$

а недиагональные члены уменьшаются. Отображение $E_{\text{ph}}[t]$ отображения $|\psi\rangle \rightarrow \rho_s$ есть

$$E_{\text{ph}}[t](\rho) = \frac{1 + \cos(gt)}{2} \rho + \frac{\cos(gt)}{2} \sigma_z \rho \sigma_z \quad (126)$$

Можно написать, что оператор Паули Z действует с вероятностью $1 - \cos(gt)$. Обсуждение до этого

момента рассматривало систему окружения, состоящую из одного кубита, поэтому связность системы становится очевидной через некоторое время.

Я вернусь. Однако в действительности система окружающей среды, окружающая исследуемую систему, часто является системой с большими степенями свободы.

Поэтому предположим, что каждая связь g мала (всегда выполняется $gt \ll 1$), и рассмотрим ситуацию, в которой система окружения независимо связывается с M кубитами.

Карта, соответствующая времени t в первом примере,

$$(E_{\text{amp}}[t])_{M \times M} = \quad (127)$$

$$= E_1 \rho E_1^\dagger + \sum_{k=2}^M (E_k \rho E_k^\dagger) + \sum_{k=0}^{M-1} (E_k \rho E_k^\dagger) \quad (128)$$

*16 Гамильтониан $H_s = \omega_s Z_s$ и $H_e = \omega_e Z_e$ каждого кубита явно не рассматривается, но картина взаимодействия принимается как $\omega_e = \omega_s$
Вы можете думать об этом как о размышлениях о

можно записать как где использовалось $E_2 = 0$. более того,

$$E_1^M = \begin{pmatrix} 1 & 0 \\ 0 & \cos M(gt) \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 \\ 0 & \cos M(gt) \end{pmatrix} = (0 \sin(gt) \cos M_1 \sin(gt)) \quad (129)$$

становится. Отсюда оператор Крауса отображения в момент времени t при $\gamma = gM$ (фиксированном gM в пределе $g \rightarrow 0$) равен

$$E_1^M = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\gamma t} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & M_1 \cos M_1 k = 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & e^{-\gamma t} \end{pmatrix}, \quad (130)$$

дан кем-то Это шум с демпфированием амплитуды, амплитуда которого $|1|$ затухает экспоненциально относительно времени t . Аналогично, при расчете для второго примера

$$(\Phi[\tau])_M = \frac{1 + \cos M(gt)}{e^{\rho + \frac{1}{2} \gamma t}} \frac{\cos M(gt)}{e^{\frac{1}{2} \gamma t}} = e^{-\frac{1}{2} \gamma t} \quad (131)$$

$$= \frac{1}{2} \quad \frac{1}{2} \quad ZpZ \quad (132)$$

, а недиагональные члены ослабляются с константой затухания $\gamma = gM$. Это называется шумом затухания фазы. В таких пределах когерентность больше не возвращается к системе. Если произойдет декогеренция, квантовая информация будет потеряна, и квантовый компьютер не будет работать должным образом. Методом решения этой проблемы является квантовая коррекция ошибок, которая будет объяснена далее.

7 Квантовая коррекция ошибок

При квантовой коррекции ошибок квантовая информация встраивается в подпространство многомерного гильбертова пространства (пространства, состоящего из множества кубитов) для защиты квантового состояния от шума. По этой причине необходимо эффективно описать подпространство, мы объясним форму стабилизатора, которая является одним из методов для этой цели, и введем определяемый им код стабилизатора. Рассмотрим $2n$ - мерное гильбертово пространство, состоящее из n кубитов. n -кубитная группа Паули, состоящая из тензорного произведения n -кубитных операторов, образующих

$$\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^n \quad (133)$$

Определим стабилизирующую группу S , которая является коммутативной подгруппой группы и элементы которой не содержат I на n . (мы будем писать все тождественные операторы как I независимо от размерности). Пусть оператор, действующий на i -й кубит, равен

$$A_i = I \otimes \dots \otimes A \otimes I \otimes \dots \otimes I \quad (134)$$

Например, $S_2 = \{I, X_1 X_2, Z_1 Z_2, Y_1 Y_2\}$ — коммутативная группа, не содержащая I , поэтому она является группой-стабилизатором. Чтобы определить такую группу стабилизаторов, мы определяем образующую, которая является наибольшим набором независимых членов группы стабилизаторов. Здесь независимость означает, что элемент, содержащийся в наборе, не может быть представлен произведением других элементов, содержащихся в наборе. Например, в приведенном выше примере $\{X_1 X_2, Z_1 Z_2\}$ можно выбрать в качестве образующей, а группу стабилизаторов S_2 можно получить, замыкая произведение этого элемента. Тогда мы пишем $S_2 = \langle X_1 X_2, Z_1 Z_2 \rangle$. В форме стабилизатора вместо явного определения состояния состояние определяется как состояние, которое является устойчивым при действии группы стабилизатора (элементов) на состояние, то есть собственное состояние с собственным значением $+1$. Например, состояние стабилизатора для группы стабилизаторов S_2 выше — это состояние максимальной запутанности $(|00\rangle + |11\rangle) / \sqrt{2}$. Это,

$$Z_1 Z_2 \frac{|01\rangle|02\rangle + |11\rangle|12\rangle}{2 \sqrt{|01\rangle|02\rangle + |11\rangle|12\rangle}} = \frac{|01\rangle|02\rangle + |11\rangle|12\rangle}{2 + |11\rangle|12\rangle} \quad (135)$$

$$X_1 X_2 \frac{12}{2} = \quad (136)$$

Таблица 1 Ошибки переворота битов и синдромы для кодов стабилизатора Z_1Z_2, Z_2Z_3 .

$Z_1Z_2 \setminus Z_2Z_3$	+1	1
+1	Я, $X_1X_2X_3$ X3, X_1X_2	
1	X_1, X_2X_3 X2, X_1X_3	

Это подтверждается тем, что

Поскольку группа стабилизаторов не содержит I , элементом генератора $\{S_i\}$ является $S_i^2 = Я$. Следовательно, собственное значение составляет ± 1 из 2. Я знаю, что это будет правильно. Поскольку каждый генератор разделен на два собственных пространства с собственными значениями +1 и -1 , количество генераторов равно m . Все состояния в n - m размерном подпространстве

Это становится стабилизирующим состоянием. Назовем такое подпространство стабилизатором. стабилизатор

Код — это квантовый код, исправляющий ошибки, который встраивает информацию в такое стабилизирующее подпространство.

Прежде чем дать общее определение, рассмотрим подпространство стабилизатора, оператор стабилизатора которого задается как Z_1Z_2, Z_2Z_3 , и построим код стабилизатора. Поскольку количество генераторов равно 2 для количества кубитов 3, 2

Определено подпространство (вырожденное) измерений. Основой этого подпространства является состояние кода, и генерируются логические кубиты.

построить логический кубит. Для решения этого вырождения выберем оператор Z_1 , не зависящий от оператора стабилизатора и коммутативный со стабилизатором $Z_1 \Gamma^1 = \Gamma^1$ является логическим базисом

$$\Gamma^0, \lvert 00 \rangle, \Gamma^1, \lvert 11 \rangle \tag{137}$$

определять. Точно так же вы можете выбрать $X_1X_2X_3$, чтобы указать основу. В действии такого оператора, коммутативного с группой стабилизаторов и не зависящего от группы стабилизаторов, подпространство стабилизатора инвариантно. С другой стороны, в отличие от оператора стабилизатора, он нетривиально работает внутри подпространства, например $X_1X_2X_3 \Gamma^0 = \Gamma^1$. Такой оператор называется логическим оператором в том смысле, что он действует на закодированные логические кубиты. Z_1 и

Оказывается, $X_1X_2X_3$ антикоммутирует друг другу и ведут себя как оператор Паули для знаковых состояний $\alpha \Gamma^0 + \beta \Gamma^1$. Обратите внимание, что этот выбор логических операторов не уникален. Это связано с тем, что оператор стабилизатора тривиально действует на знаковое состояние $\lvert \psi^- \rangle$

$$S_i \lvert \psi^- \rangle = \lvert \psi^- \rangle \text{ для всех } S_i \in S \tag{138}$$

Следовательно, если L — логический оператор, то $LS_i (S_i \in S)$ — также логический оператор с тем же эффектом. То есть действие логического оператора является классом эквивалентности на группе стабилизаторов операторам, коммутирующим с группой стабилизаторов. ручка.

Предположим, что в первом кубите произошла ошибка инвертирования бита X_1 . Кодовое состояние $\alpha \Gamma^0 + \beta \Gamma^1$ имеет базис $\{X_1 \Gamma^0 = \lvert 100 \rangle, X_1 \Gamma^1 = \lvert 011 \rangle\}$ в ортогональное пространство, ограниченное. Поскольку оператор стабилизатора Z_1Z_2 и оператор битового реверса X_1 антикоммутируют, собственные значения меняются местами с +1 на -1 . Другими словами, обращение собственного значения оператора стабилизатора дает информацию о возникновении ошибки (находится ли она в правильном подпространстве). По этой причине собственное значение оператора стабилизатора после ошибки называется значением синдрома, а множество значений синдрома называется синдромом. Соответствие между типом ошибки и синдромом кода стабилизатора, состоящего из 3 кубитов, о котором мы сейчас думаем, равно 1. Если ошибка переворота битов возникает только в одном кубите, мы можем определить ошибку по таблице соответствий и исправить ошибку. Однако, когда ошибки двух кубитов возникают одновременно, например, X_2X_3 , их нельзя отличить от X_1 , что приводит к логической ошибке с другим состоянием кода. Этот код называется 3-кубитным кодом с инвертированием битов, потому что возможна коррекция ошибок для инвертирования битов.

В общем, для кода стабилизатора, состоящего из $m = n - k$ образующих стабилизаторов $S_1, \dots, S_m$, k независимых логических операторов, которые независимы и коммутативны операторам стабилизатора, можно выбрать Z^k и определить k логических кубитов как собственные состояния. Синдром задается набором $\{s_i\}$ собственных значений генератора-стабилизатора $\{S_i\}$. Кроме того, операторы X_i^- ($i = 1, \dots, k$) антикоммутируют с каждым оператором, т. е. для всех $i, j = 1, \dots, k$ для

$$X_i^- Z_j^- = (-1)^{\delta_{ij}} Z_j^- X_i^- \quad X_i^- X_j^- = X_j^- X_i^- \quad (139)$$

Всегда существует оператор X_i^- , который удовлетворяет. Пусть $\{X_i^-, Z_i^-\}$ — оператор Паули, действующий на i -й логический кубит в закодированных степенях свободы.

Кодовое расстояние является показателем для измерения устойчивости к ошибкам кода стабилизатора, определенного таким образом. Кодовое расстояние определяется как минимальное значение d , когда количество операторов Паули, входящих в логический оператор, минимизируется для всех логических операторов. Другими словами, если число операторов Паули (отличных от I), входящих в оператор A , равно $wt(A)$, а L — группа логических операторов, то $d = \min_L wt(L)$. Например, кодовое расстояние $d = 1$ для 3-кубитного кода, описанного выше. Это означает, что даже если одна ошибка Паули Z сработает, она останется в пространстве стабилизатора, и ошибка не может быть обнаружена и исправлена. Чтобы построить аккуратный квантовый код исправления ошибок требует несколько более сложной конструкции.

Хотя это несколько парадоксально, но при выборе генератора группы стабилизаторов следующим образом, 5-квант с $d = 3$ Можно построить код битового стабилизатора:

$$S_1 = X_1 Z_2 Z_3 X_4 I_5 \quad (140)$$

$$S_2 = I_1 X_2 Z_3 Z_4 X_5 \quad (141)$$

$$S_3 = X_1 I_2 X_3 Z_4 Z_5 \quad (142)$$

$$S_4 = Z_1 X_2 I_3 X_4 Z_5 \quad (143)$$

Например, X_1 и Z_5 — логические операторы.

Поскольку это дочерний элемент, можно убедиться, что $d = 3$, проверив все логические операторы.

Кодовое расстояние d вычисляется путем последовательного применения оператора Паули, начиная с одного состояния кода в кодовом пространстве. Он выражает расстояние между двумя разными состояниями в кодовом пространстве в том смысле, что состояния кода различны только тогда, когда они объединены. нижний Следовательно, если оператор Паули $(d - 1)/2$ или меньше возникает как ошибка (ошибка Паули) для данного состояния кода, состояние кода, ближайшее к этому состоянию, однозначно вернется к исходному состоянию кода. Поэтому, если происходит ошибка и состояние кода перемещается в ортогональное пространство, определяемое некоторым синдромом $\{s_i\}$, для восстановления используется минимальный оператор Паули, который может быть восстановлен из этого пространства обратно в исходное кодовое пространство. $d - 1)/2$ Ошибки Паули можно исправить. Такой метод декодирования называется декодированием с минимальным расстоянием. Поскольку упомянутый выше код стабилизатора с 5 кубитами имеет $d = 3$, он может исправить ошибку Паули на один кубит. Следовательно, в дополнение к ошибкам реверсирования битов (X) могут быть исправлены все ошибки реверсирования фазы (Z) и ошибки инверсии бит/фазы (Y).

Пространство из 5 кубитов является 32 -мерным и делится на подпространства, соответствующие 16 синдромам, 4 генераторами. С другой стороны, общее количество паттернов ошибок Паули для одного кубита равно 3 типам для каждого кубита, поэтому имеется $3 \times 5 = 15$ паттернов. Обратите внимание, что существует однозначное соответствие между 16 ортогональными подпространствами и 16 образами ошибок (включая отсутствие ошибок). так

Минимальный код, который удовлетворяет этим свойствам, — это приведенный выше 5-кубитный код стабилизатора.

Как уже упоминалось, если оператор стабилизатора выбран соответствующим образом, состояние, в котором ошибка X , вызывающая инверсию битов, ошибка Z , вызывающая инверсию фазы, или ошибка Y , вызывающая обе эти ошибки, будет частью ортогонального пространства стабилизатора. Если количество ошибок $t = (d - 1)/2$ или меньше, его можно исправить. Что происходит, когда квантовый шум задается общей картой СРТР? Фактически, вывод Крауса 1-кубитной карты СРТР

Оператор E_k можно расширить на основе оператора Паули следующим образом.

$$E_k = \prod_{j \in K} \sigma_j^x + \prod_{j \in K} \sigma_j^y + \prod_{j \in K} \sigma_j^z + \prod_{j \in K} \sigma_j^0. \quad (144)$$

Основываясь на этом факте и способности исправлять все типы ошибок X , Y и Z , ниже показано, что можно исправить даже общий квантовый шум. Пусть R — гипероператор, восстанавливающийся после ошибки Паули, а его оператор Крауса — R_j . Тогда для состояния кода стабилизатора $|\Psi\rangle$ ошибка Паули $A = X, Y, Z$ успешно исправлена и исходное состояние восстановлено. При выполнении следующего выражение:

$$R_j A |\Psi\rangle = |\Psi\rangle. \quad (145)$$

Применение этого условия к каждому из разложений уравнения (144) дает $R_j E_k |\Psi\rangle = |\Psi\rangle$, поэтому

$$R(E_k |\Psi\rangle) = |\Psi\rangle, \quad (146)$$

(где R и E использовали сохранение трассировки). Следовательно, код стабилизатора с кодовым расстоянием d может исправлять произвольный квантовый шум, для которого число кубитов, на которые нетривиально действует оператор Крауса, не превосходит d . Это будет возможно.

В отличие от классических битов, квантовые состояния имеют непрерывные степени свободы (волновые функции). Поэтому квантовый шум для квантового состояния считается аналоговым шумом, который тонко изменяет непрерывную степень свободы, а наоборот, считается сложным. Аналоговые компьютеры могут быть определены в классическом мире, но если не принимать во внимание аналоговый шум и бесконечную точность аналоговых вычислений.

Предположим, что у нас есть компьютер (хотя я сомневаюсь, что законы физики позволят нам построить такую машину), у нас есть NP-задача PSPACE.

Даже очень сложные проблемы, включая проблемы, могут быть решены эффективно. В PSPACE объем памяти полиномиален в обычной классической машине Тьюринга (которую можно рассматривать как цифровой классический компьютер), но время вычислений может быть экспоненциальным.

Это очень сложный класс задач. Однако причина, по которой такой мощный аналоговый компьютер не был реализован, заключается в том, что аналоговый шум невозможно преодолеть (это не означает, что аналоговые компьютеры бесполезны, но с помощью классического цифрового компьютера можно моделировать, например, эксперименты в аэродинамической трубе). В последние годы были попытки ускорить задачи оптимизации и машинного обучения за счет использования параллелизма аналоговых устройств). Если бы квантовые компьютеры использовали аналоговую природу квантовой механики для ускорения вычислений в смысле аналоговых машин, их интерес был бы более ограниченным (конечно, квантовые вычисления также полезны в качестве аналоговых квантовых вычислений, таких как симулятор). Однако интересно, что ошибка может быть дискретизирована как ошибка Паули и исправлена с использованием обратного принципа суперпозиции. Другими словами, аналоговая ошибка для квантового состояния с некоторой аналоговой информацией может быть дискретизирована и исправлена путем введения запутанной структуры в квантовой системе многих тел, называемой кодом исправления квантовых ошибок. В этом смысле универсальные квантовые вычисления, защищенные квантовой коррекцией ошибок, можно назвать цифровыми квантовыми вычислениями. Тот факт, что квантовый компьютер с устойчивостью к ошибкам может быть построен с помощью квантовой коррекции ошибок, является теорией, согласно которой вычислительная модель квантового компьютера является подходящей моделью для достижения теоретических ограничений вычислений, допускаемых законами физики. гарантия.

Рекомендации

[1] Нильсен, М.А., Чуанг, И.Л. Квантовые вычисления и квантовая информация. (Cambridge University Press 2010).

[2] К. Фуджи, Квантовые вычисления с топологическими кодами — от кубита к топологической отказоустойчивости — SpringerBriefs по математической физике (Springer-Verlag 2015).