Квантовые вычисления для программистов

Васильев А.В.

1 Введение

Начало работ в области квантовых вычислений связывается со статьей [6], опубликованной Ричардом Фейнманом в 1982 году и посвященной компьютерному моделированию квантово-механических процессов на вычислительных машинах. Он заметил, что с ростом размерности физической задачи пространство состояний возрастает экспоненциально, поэтому эффективное моделирование многочастичной квантовой механики на классическом компьютере невозможно. Исходя из этого, Фейнман выдвинул идею "квантового компьютера" – компьютера, использующего в своей основе квантовые эффекты, такие, как суперпозиция и, главное, запутанность. С этой работы начались современные исследования проблемы использования квантово механических эффектов при решении задач, требующих больших вычислительных ресурсов.

Впервые формальная модель универсального квантового компьютера (квантовая машина Тьюринга) была предложена П. Бениоффом году и развита Д. Дойчем [4]. Более наглядная модель квантовых вычислений (эквивалентная квантовой машине Тьюринга) – квантовые схемы, была предложена Д. Дойчем [5].

Отметим, что квантовые модели вычислений не нарушают тезис Тьюринга-Черча, т.к. могут быть промоделированы на детерминированных аналогах. Различие между классическими и квантовыми моделями проявляются лишь в эффективности вычислений.

В чем же преимущества квантовых вычислений и какие у них слабости?

Наибольшие надежды возлагаются на *квантовый параллелизм* – возможность квантового регистра находиться одновременно во всех своих состояниях. Так, если классический n-битный регистр находится ровно в одном из своих состояний, то n-битный квантовый регистр сразу во всех 2^n базисных состояниях. С одной стороны, это позволяет производить вычисления сразу на множестве наборов, в том числе на всех наборах сразу. Однако непосредственное применение этого приема ничего не дает, поскольку достоверно извлечь нужный ответ не удастся. Потребуется преобразование состояния таким образом, чтобы нужный ответ получил бы большую амплитуду, а значит проявился при измерении с большой вероятностью. В решении указанной проблемы может помочь другая особенность квантовых вычислителей – наличие интерференции между состояниями, возникающей из-за того, что новые амплитуды базисных состояний оказываются линейными комбинациями старых амплитуд. Это позволяет строить алгоритмы таким образом, чтобы неверные решения исчезали за счет деструктивной интерференции (уменьшающей амплитуду), в то время как желаемые состояния усиливались при конструктивной интерференции (увеличивающей амплитуду).

Важной особенностью также является возможность создавать *запутанные состояния (entangled states)* совокупности кубит, когда невозможно приписать определенное состояние каждому из них. Запутанные состояния можно задать экспоненциальным числом комплекснозначных амплитуд, а для не запутанного состояния достаточно их линейного числа. При

этом квантовая запутанность является необходимым условием для экспоненциального ускорения в квантовых вычислениях. Джозса и Линден показали [7], что если максимальный ранг Шмидта (дискретная мера двухчастичной запутанности) при квантовых вычислениях является константой (не зависит от числа кубит), то такое вычисление можно за полиномиальное время смоделировать на квантовом компьютере. Более сильный результат был получен Видалом [11]. Результат состоит в том, что эффективное (за полиномиальное время) классическое моделирование возможно, даже если максимальное число Шмидта полиномиально зависит от числа кубит.

Слабости квантовых вычислений являются продолжением их сильных сторон. Так, квантовые вычисления происходят в "черном ящике", а ответ можно получить лишь в результате измерения, которое является вероятностным процессом и приводит к безвозвратной потере информации об амплитудах полученных базисных состояний (об их величине можно судить лишь по статистике многократных экспериментов). Кроме того, в классических алгоритмах можно прервать вычисления, если ответ уже получен. Квантовые же алгоритмы всегда выполняются до конца (в модели с единственным финальным измерением), что также требует специальной их организации. Поэтому разработка квантовых алгоритмов требует особой интуиции – классические подходы срабатывают далеко не всегда.

Еще одна особенность квантовых вычислений – обратимость используемых преобразований – не представляет проблемы, если нет ограничений на размер квантового регистра. Однако при довольно умеренных ограничениях (порядка $O(\log n)$ кубит, где n – длина входного набора) вычисление многих функций оказывается затруднено, а соответствующие задачи в таких моделях с ограничениями могут иметь экспоненциальную сложность [9].

Отметим также, что многочастичная запутанность, будучи необходимым условием квантового ускорения, является и главным останавливающим фактором на пути к созданию квантового компьютера. Для эффективных вычислений необходимо не только управлять, но и сохранять квантовую запутанность, чему мешает процесс декогерентности. В современной трактовке декогерентность — разрушение квантового состояния (и, главное, его запутанности) под действием внешней среды.

2 Математический аппарат квантовых вычислений – Линейная алгебра

Квантовые вычисления основываются на том, что носителями информации являются квантово-механические системы из микромира, а, следовательно, их состояния и преобразования описываются постулатами квантовой механики. Приведем необходимые обозначения и сведения из книги [8].

Пусть $\mathcal{H}^d$ – d-мерное гильбертово пространство (комплексное линейное векторное пространство с определенным в нем скалярным произведением). Для обозначения элементов пространства $\mathcal{H}^d$ принято использовать "bra-ket" нотацию Дирака: $|\psi\rangle$ и $\langle\psi|$ для вектора-столбца и вектора-строки, соответственно. Также будем использовать $\langle\psi_1|\psi_2\rangle$ для скалярного произведения.

Тензорное произведение. Введем обозначение $A \otimes B$ – *тензорное (правое кронекерово) произведение* матриц A, B.

$$\text{Для } A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \text{ и } B = \begin{pmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & \ddots & \vdots \\ b_{l1} & \cdots & b_{lk} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

Для векторов $|a_1\rangle, \ldots, |a_q\rangle \in \mathcal{H}^2$ будем также использовать обозначения

$$|a_1\rangle \otimes \cdots \otimes |a_q\rangle = |a_1 \ldots a_q\rangle \in \mathcal{H}^{2^q}.$$

Стандартный вычислительный базис в $\mathcal{H}^{2^q}$ В качестве стандартного базиса в $\mathcal{H}^2$ рассматривается следующий:

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

Для пространств $\mathcal{H}^d$ большей размерности вводятся дополнительные обозначения:

$$\begin{array}{rcccl} |1\rangle & = & |00\ldots0\rangle & = & (100\ldots0\ldots0)^T \\ |2\rangle & = & |00\ldots1\rangle & = & (010\ldots0\ldots0)^T \\ & \vdots & & & \\ |i\rangle & = & |bin(i-1)\rangle & = & (000\ldots1\ldots0)^T \\ & \vdots & & & \\ |d\rangle & = & |11\ldots1\rangle & = & (000\ldots0\ldots1)^T. \end{array}$$

Здесь у вектора $|i\rangle$ на i-й позиции 1, а все остальные компоненты нулевые.

Указанные равенства легко проверить. Например, рассмотрим вектор-столбец, соответствующий $|010\rangle = |3\rangle$:

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|010\rangle = |0\rangle \otimes |10\rangle = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |3\rangle.$$

Очевидно, что система векторов $|1\rangle$, $|2\rangle$, …, $|i\rangle$, …, $|d\rangle$ образует ортонормированный базис в пространстве $\mathcal{H}^d$. Будем также обозначать указанные векторы через $|00\ldots0\rangle$, $|00\ldots1\rangle$, …, $|bin(i-1)\rangle$, …, $|11\ldots1\rangle$, где $bin(i)$ – это двоичное представление числа i. Такая система векторов называется стандартным вычислительным базисом. В дальнейшем будем рассматривать вычисления только в этом базисе.

Пространство состояний. Согласно первому постулату, с любой изолированной физической системой можно связать гильбертово пространство, называемое пространством состояний системы. Состояние системы полностью описывается единичным вектором из пространства состояний, называемым вектором состояния (или, сокращенно, состоянием).

Квантовый бит (*кубит*) является ключевым понятием теории квантовых вычислений. Он рассматривается как квантово-механическая система, состояние которой описывается комплекснозначным вектором двумерного гильбертова пространства $\mathcal{H}^2$, т.е.

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

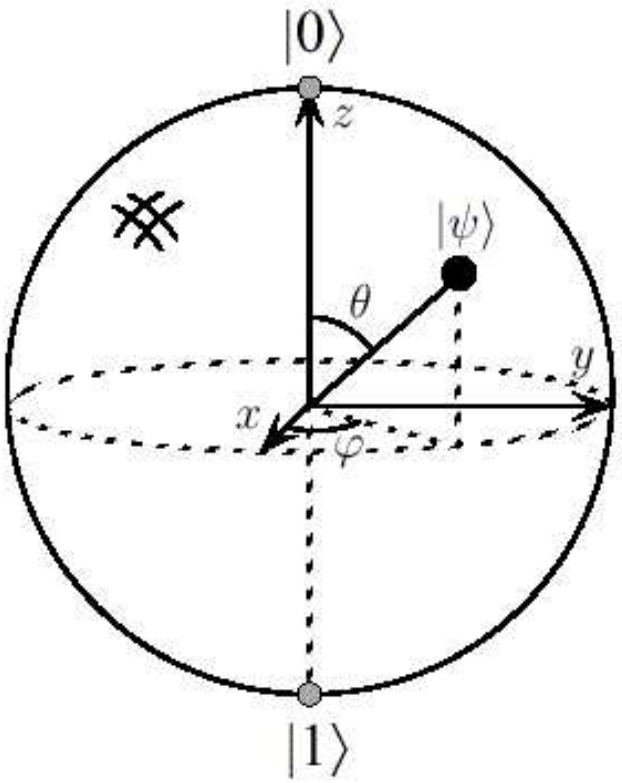
где векторы $|0\rangle$ и $|1\rangle$ образуют ортонормированный базис в $\mathcal{H}^2$, а комплексные числа α и β удовлетворяют условию $|\alpha|^2 + |\beta|^2 = 1$. Таким образом, в отличие от классического бита кубит может одновременно находиться в *суперпозиции* своих базисных состояний $|0\rangle$ и $|1\rangle$ с амплитудами α и β соответственно.

Каждое состояние кубита $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ можно представить в виде

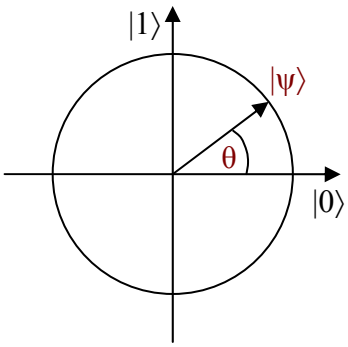
$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,,$$

где $0 \le \phi < 2\pi$, $0 \le \theta \le \pi$.

Пусть $e^{i\phi}\frac{\theta}{2} = x + iy$ и обозначим $z = \cos\frac{\theta}{2}$. Тогда $x^2 + y^2 + z^2 = 1$, т.е. каждое состояние кубита соответствует точке на единичной сфере, задаваемой полярными координатами θ и ϕ и называемой *сферой Блоха*.



Описанное представление иллюстрирует состояние кубита в общем случае. Однако в случае вещественных амплитуд условие нормировки $\alpha^2 + \beta^2 = 1$ есть уравнение единичной окружности, и, следовательно, кубит может быть представлен точкой на ней:



Таким образом, состояние кубита в вещественном случае вырождается в

$$|\psi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$

для некоторого $\theta \in [0, 2\pi)$.

Составные системы. При рассмотрении квантового регистра (т.е. совокупности отдельных кубит), квантовая механика постулирует, что пространство состояний такой составной системы будет описываться тензорным произведением пространств состояний подсистем. Например, если n кубит находятся в состояниях $|\psi_1\rangle$, $|\psi_2\rangle$, $\ldots$, $|\psi_n\rangle$, то состояние $|\psi\rangle$ квантового регистра, состоящего из этих кубит, будет выражаться через тензорное произведение их состояний:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle\,.$$

Такие состояния называются разложимыми.

В то же время существуют так называемые *неразложимые или запутанные состояния* квантовых регистров, которые не могут быть представлены тензорным произведением состояний отдельных кубит. Такими состояниями являются, например, ЭПР-пары или состояния Белла, играющие ключевую роль в квантовой телепортации и сверхплотном кодировании.

Таким образом, постулируется, что регистр из n кубит в общем случае может быть описан единичным вектором из пространства $\mathcal{H}^{2^n}$:

$$\sum_{i=1}^{2^n} \alpha_i\,|i\rangle\,,\ \text{где}\ \sum_{i=1}^{2^n} |\alpha_i|^2 = 1.$$

Такие линейные комбинации принято называть суперпозициями базисных состояний $|i\rangle$ с амплитудами α_i.

Измерение. На классическом компьютере считывание значений переменных не представляет сложности. В квантовых моделях вычислений ситуация сложнее. Квантовая система должна функционировать изолированно – любое вмешательство в ее работу (в том числе считывание результатов вычисления) приводит к изменению состояния.

И, хотя кубиты и могут одновременно находиться в различных состояниях, информация об этом доступна лишь опосредованно – путем измерения состояния. Причем это вероятностный процесс, т.е., измеряя суперпозицию (состояние системы) $|\psi\rangle = \sum_i \alpha_i\,|i\rangle$, мы получим любое из состояний $|i\rangle$ с вероятностью $|\alpha_i|^2$.

При этом состояния, отличающиеся лишь фазовым множителем $e^{i\phi}$ считаются неотличимыми, поскольку при измерении $|\psi\rangle$ и $e^{i\phi}|\psi\rangle$ имеют одинаковое распределение вероятностей получения базисных состояний.

Таким образом, из бесконечного объема информации, который можно сохранить в амплитудах квантового бита, доступен лишь единственный бит, соответствующий базисному состоянию.

Другой вариант извлечения большого объема информации из одного кубита состоит в многократном копировании результатов вычислений и статистическом анализе результатов вычислений. Однако и этот вариант невозможен ввиду того, что в общем случае нельзя клонировать неизвестное квантовое состояние.

Впрочем, это не означает бесполезность квантовых суперпозиций, а лишь указывает на невозможность их классического использования.

Мы будем использовать вариант квантового измерения, называемый проективным измерением. Для задания такого измерения достаточно перечислить полный набор ортогональных проекторов P_m, удовлетворяющих соотношениям $\sum_m P_m = I$ и

$$P_m P_{m'} = \begin{cases} P_m, \text{ если } m = m' \\ I, \text{ иначе} \end{cases}.$$

Вероятность исхода m в таком случае можно выразить как

$$Pr(m) = ||P_m|\psi\rangle||_2^2 = \langle\psi| P_m^\dagger P_m |\psi\rangle,$$

а состоянием $|\psi'\rangle$ системы после измерения будет

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{Pr(m)}}.$$

Динамика изменения. Следующий постулат гласит, что динамика изменения состояния замкнутой квантовой системы описывается унитарными преобразованиями. Другими словами, состояние $|\psi_1\rangle$ системы в момент времени t_1 связано с состоянием $|\psi_2\rangle$ в момент времени t_2 следующим образом:

$$|\psi_1\rangle = U|\psi_2\rangle,$$

где U – это унитарный оператор.

Унитарные операторы. Множество унитарных операторов континуально, но их можно сколь угодно точно представить в виде произведения унитарных операций из некоторого конечного универсального набора [8].

Таковым набором является, например, совокупность следующих операторов:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};\ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix};\ T = \pi/8 = e^{i\pi/8}\begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix};$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Известно [8], что любое однокубитное унитарное преобразование можно с произвольной точностью ϵ представить в виде произведения $O(\log^c 1/\epsilon)$ операторов H и $\pi/8$ (константа c приблизительно равна 2), а произвольное унитарное преобразование, действующее на q кубитах может быть представлено в виде произведения $O(q^2 4^q)$ однокубитных и CNOT операторов. Фазовый оператор S включается в стандартный набор для реализации контролируемых операторов и для организации помехоустойчивых вычислений.

Следующие унитарные операторы называются *операторами вращения*, потому что соответствуют вращениям на угол θ вокруг осей $\hat{x}$, $\hat{y}$ и $\hat{z}$ сферы Блоха:

$$R_{\hat{x}}(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix};$$

$$R_{\hat{y}}(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix};$$

$$R_{\hat{z}}(\theta) = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}.$$

Вообще, т.к. любой унитарный оператор сохраняет норму вектора, он может интерпретироваться на сфере Блоха как вращение вокруг некоторой оси [8]. Заметим, что $R_{\hat{n}}(\alpha) \cdot R_{\hat{n}}(\beta) = R_{\hat{n}}(\alpha + \beta)$ для любой фиксированной оси $\hat{n}$.

Кроме того, известно, что любой унитарный оператор U представим в виде:

$$U = e^{i\alpha} R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma) R_{\hat{z}}(\delta)$$

для некоторых вещественных чисел α, β, γ и δ. Это соответствует тому факту, что любое вращение точки на трехмерной сфере можно сконструировать из ортогональных вращений.

Заметим, что вращения на угол 2π не приводят к тождественному преобразованию – для этого требуется поворот на угол 4π:

$$R_{\hat{z}}(2\pi) = -I,$$
$$R_{\hat{z}}(4\pi) = I.$$

Получаемые в результате применения таких операторов состояния отличаются лишь на множитель -1, не проявляющийся при измерении, и поэтому соответствуют одной и той же точке на сфере Блоха.

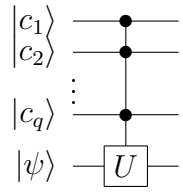
Таким образом, каждому вращению на сфере Блоха соответствуют два различных унитарных преобразования, что формализуется в теории групп как *двойное покрытие* группы $SO(3)$ группой $SU(2)$.

Контролируемые операторы, реализующие некоторое преобразование при выполнении определенного условия, являются основой для квантового параллелизма. Пусть кубиты $|c_1\rangle$, $|c_2\rangle$, ..., $|c_q\rangle$ находятся в некотором базисном состоянии. Оператор $C^q(U)$, управляемый кубитами $|c_1\rangle$, $|c_2\rangle$, ..., $|c_q\rangle$, можно задать уравнением вида

$$C^q(U) |c_1\rangle |c_2\rangle \ldots |c_q\rangle |\psi\rangle = |c_1\rangle |c_2\rangle \ldots |c_q\rangle U^{c_1 \cdot c_2 \cdots c_q} |\psi\rangle,$$

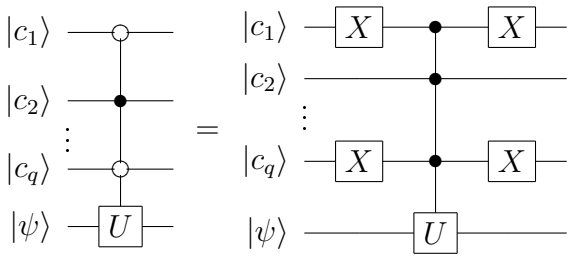
т.е. унитарное преобразование U применяется к *целевому* кубиту $|\psi\rangle$, если все *управляющие* кубиты $|c_1\rangle, |c_2\rangle, \ldots, |c_q\rangle$ находятся в базисном состоянии $|1\rangle$, в противном случае применяется тождественное преобразование I. В квантовых схемах из функциональных элементов

такие операторы принято обозначать следующим образом:



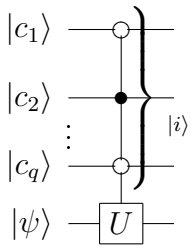
Известно, что произвольный контролируемый оператор $C^q(U)$, где U – однокубитное унитарное преобразование, можно реализовать при помощи $O(q^2)$ однокубитных и CNOT операторов.

Контролируемые операторы можно обобщить на случай, когда для срабатывания управляющие кубиты должны находиться в состоянии $|0\rangle$, а не $|1\rangle$. Для этого до и после применения контролируемого оператора соответствующий кубит инвертируется при помощи оператора отрицания X. Кроме того, вводится специальное обозначение:



Пусть $d = 2^q$, а $|1\rangle$, $|2\rangle$, ..., $|i\rangle$, ..., $|d\rangle$ – это ортонормированный базис в d-мерном гильбертовом пространстве.

Обозначим через $C_i^q(U)$ (или $C_i(U)$) контролируемый оператор с q управляющими кубитами, если преобразование U применяется к целевому регистру, только когда управляющий регистр находился в состоянии $|i\rangle$. На схемах будем обозначать такой оператор следующим образом:



3 Квантовые модели вычислений

Неформально, квантовые алгоритмы состоят в применении последовательности унитарных операторов к начальному состоянию кубитов, т.е. последовательность умножений унитарных матриц на комплексный вектор. При этом, последовательность матриц можно заменить одной (их произведением), из чего следует, что квантовый алгоритм при отсутствии внешнего воздействия, по сути, задается унитарной матрицей. В общем случае, это справедливо лишь для участков квантового алгоритма между взаимодействиями с внешней средой.

3.1 Квантовая машина Тьюринга

Квантовая машина Тюринга (QTM), основанная на использовании квантовой суперпозиции – квантовый аналог вероятностной машины Тьюринга – впервые была определена Дойчем [4].

Дойч предположил, что эта модель может быть эффективнее, чем классическая, для некоторых задач. Он также показал существование универсальной квантовой машины Тьюринга (а также модели квантовых сетей – квантовый аналог классических схем). Однако его модель универсальной квантовой машины Тьюринга имела один недостаток – моделирование других квантовых машин Тьюринга могло иметь экспоненциальную сложность. Эта проблема была решена Бернштейном и Вазирани (1993) [3]. Они показали существование универсальной QTM, способной моделировать другие QTM в полиномиальное время.

Квантовая машина Тьюринга. Как и в случае недерминированных машин Тьюринга в квантовых машинах может быть несколько команд с заданной левой частью:

$$\begin{aligned} qa &\xrightarrow{\delta_1} q^{(1)}a^{(1)}\{L,S,R\} \\ &\xrightarrow{\delta_2} q^{(2)}a^{(2)}\{L,S,R\} \\ &\cdots \\ &\xrightarrow{\delta_r} q^{(r)}a^{(r)}\{L,S,R\}, \end{aligned}$$

причем каждая из них помечена некоторым комплексным числом. Семантика выполнения таких команд заключается в параллельном их выполнении с амплитудой, заданной числом δ_i.

Соответственно, можно задать функцию переходов

$$\delta : Q \times \Sigma \times Q \times \Sigma \times \{L,S,R\} \to \mathbb{C},$$

где $\mathbb{C}$ – это множество комплексных чисел, а $\delta(q,a,q',a',d)$ – амплитуда, с которой машина, находясь в состоянии q и считывая a на ленте, перейдет в состояние q', запишет a' на ленту и сдвинется в направлении d на входной ленте.

Определение 3.1. *Квантовая Машина Тьюринга (Quantum Turing Machine) – это пятерка* $M = \langle \Sigma, Q, \delta, q_1, q_0 \rangle$, *состоящая из конечного множества состояний* Q, *начального состояния* $q_1 \in Q$, *заключительного состояния* $q_0 \in Q$, *конечного входного алфавита* Σ, *и функции переходов* δ, *удовлетворяющей условию*

$$\sum_{(q',a',d) \in Q \times \Sigma \times \{L,S,R\}} |\delta(q,a,q',a',d)|^2 = 1$$

для любых $(q,a) \in Q \times \Sigma$.

Аналогично детерминированной модели определяются понятие конфигурации, начальной и заключительной конфигураций. В общем случае конфигурация может рассматриваться как комбинация

$$\alpha_1 c_1 + \ldots + \alpha_m c_m + \ldots$$

базисных конфигураций. Ассоциируя базисные конфигурации с элементами ортонормированного базиса в гильбертовом пространстве, замечаем, что конфигурации квантовой машины Тьюринга являются единичными векторами в соответствующем векторном пространстве, а функция переходов задает в нем линейное отображение U_δ.

Согласно постулатам квантовой механики отображение U_δ должно быть унитарным. Говорят, что квантовая машина Тьюринга является *хорошо сформированной* (well-formed), если линейный оператор U_δ является унитарным.

Когда машина M, находящаяся в суперпозиции своих конфигураций $\psi = \sum \alpha_i c_i$ измеряется, то с вероятностью $|\alpha_i|^2$ результатом измерения является конфигурация c_i. Входное слово принимается, если результатом измерения является принимающая конфигурация, и отвергается, если результатом измерения является отвергающая конфигурация. Таким образом, результат вычисления является вероятностным. Аналогично вероятностной модели определяются критерии распознавания с ограниченной и неограниченной ошибкой языка L квантовой машиной Тьюринга.

Заметим, что представление квантовых алгоритмов машинами Тьюринга не являются удобочитаемым, поэтому в области квантовых вычислений преобладает *схемное* представление алгоритмов (в виде квантовых схем из функциональных элементов или квантовых ветвящихся программ) ввиду его наглядности. Более того, подавляющее большинство известных квантовых алгоритмов описаны в схемном представлении.

Квантовые классы сложности

- **BQP** – класс языков распознаваемых с ограниченной ошибкой квантовой машиной Тьюринга за полиномиальное время.
- **PrQP** – класс языков распознаваемых с неограниченной ошибкой квантовой машиной Тьюринга за полиномиальное время.

Прежде всего, следует отметить, что квантовые вычислители не могут решать проблемы, не разрешимые на классической машине Тьюринга. Это следует из того, что все вычислимое в квантовой модели может быть смоделировано на классической машине просто вычислением амплитуд суперпозиции и записи их на рабочую ленту. Различие между классическими и квантовыми вычислениями лежит только в вопросе их сложности. Тривиальное моделирование квантовых вычислений классическим экспоненциально по времени и памяти. Bernstein и Vazirani [3] показали, что моделирование может быть полиномиально по памяти, хотя все еще экспоненциально по времени.

Известны следующие соотношения:

- **BQP** $\subseteq$ **PSPACE** [3]
- Соотношение между классами **BQP** и **NP** неизвестно.

3.2 Квантовые схемы

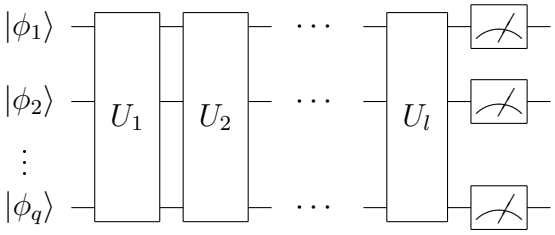
Однородные вычислительные модели, такие как машина Тьюринга, конечные автоматы, ориентированы на решение вычислительной проблемы с произвольной длиной входа. Далее будут рассмотрены неоднородные модели вычислений, обрабатывающие входные слова фиксированной длины.

Наиболее распространенной квантовой моделью вычислений являются квантовые схемы (*quantum circuits*). В основе определения квантовых схем лежит понятие квантового вентиля (*quantum gate*).

Определение 3.2. *Квантовым вентилем на q кубитах называется унитарное отображение в гильбертовом пространстве $\mathcal{H}^{2^q} = \mathcal{H}^2 \otimes \ldots \otimes \mathcal{H}^2$, воздействующее нетривиальным образом на фиксированное (не зависящее от q) число кубит.*

Определение 3.3. *Квантовая схема на q кубитах – это унитарное отображение в гильбертовом пространстве $\mathcal{H}^{2^q} = \mathcal{H}^2 \otimes \ldots \otimes \mathcal{H}^2$, которое может быть представлено в виде соединения конечного числа квантовых вентилей.*

Квантовые схемы принято изображать следующим образом:



Сложностью квантовых схем называют число квантовых вентилей в ней. Известно [12], что полиномиальные по сложности квантовые схемы равномощны полиномиальным по времени квантовым машинам Тьюринга.

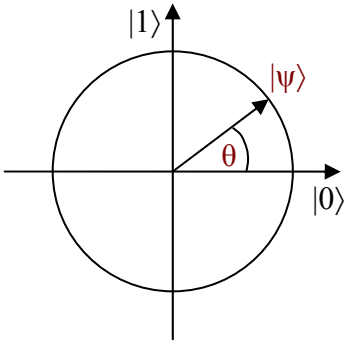
3.3 Примеры квантовых алгоритмов

Квантовые алгоритмы на основе fingerprinting. Пусть $\sigma = \sigma_1 \ldots \sigma_n$ – входной набор, а $g(\sigma)$ – значение характеристической функции, проверяющей наличие некоторого свойства у σ. σ обладает свойством $g \iff g(\sigma) = 0 \bmod m$.

Повернем начальное состояние $|0\rangle$ на угол

$$\theta = \frac{\pi g(\sigma)}{m}$$

$$|0\rangle \to \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \to |0\rangle \iff g(\sigma) = 0 \bmod m$$

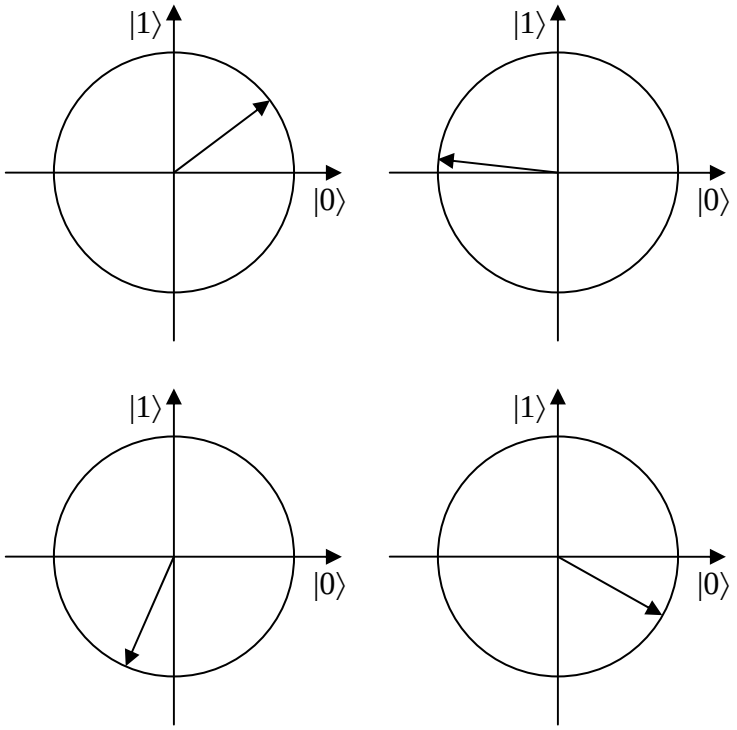


Пусть $k_1, \ldots, k_t \in \{1, \ldots, m-1\}$. Повернем t кубит на углы

$$\theta_i = \frac{\pi k_i g(\sigma)}{m}$$

$$|0\rangle \to \cos\theta_i\,|0\rangle + \sin\theta_i\,|1\rangle \to |0\rangle \text{ , если } g(\sigma) = 0 \bmod m$$

При $t = O(\log m)$ существует множество $K = \{k_1, \ldots, k_t\}$, для которого $Pr_{error} < 1/m$.



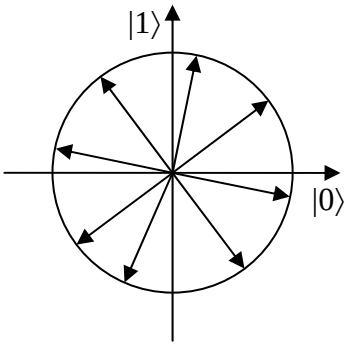
Используя квантовый параллелизм и интерференцию, можно добиться значительного сокращения числа кубит.

$$\underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{\log t} \otimes |0\rangle$$

$$\downarrow$$

$$\frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \left(\cos\theta_i |0\rangle + \sin\theta_i |1\rangle \right)$$

$$\theta_i = \frac{2\pi k_i g(\sigma)}{m}$$



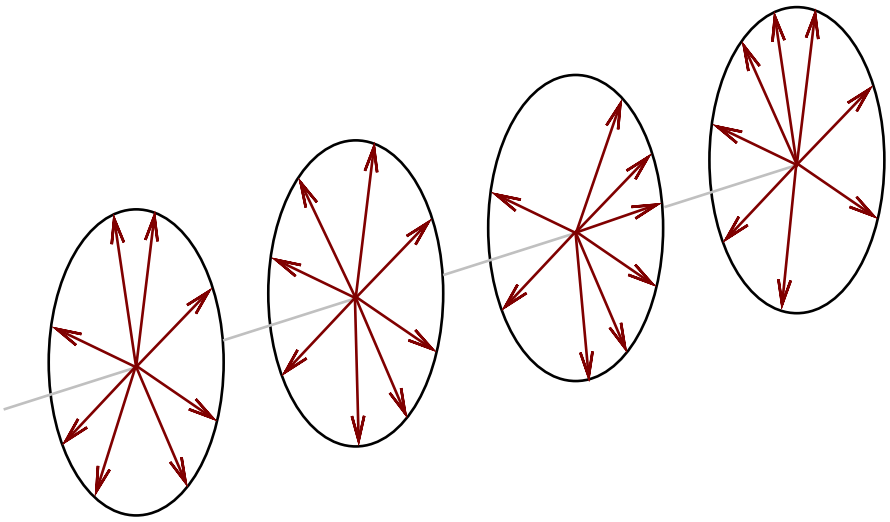
Описанная схема проверки свойства g у входного набора σ реализуется следующим алгоритмом:

$$
\begin{array}{l}
|0\rangle^{\otimes \log t} |0\rangle \\
\quad \downarrow \\
\frac{1}{\sqrt{t}} \sum\limits_{j=1}^{t} |j\rangle |0\rangle \\
\quad \downarrow \\
\frac{1}{\sqrt{t}} \sum\limits_{j=1}^{t} |j\rangle \left(\cos \frac{2\pi k_j g(\sigma)}{m} |0\rangle + \sin \frac{2\pi k_j g(\sigma)}{m} |1\rangle \right) \\
\quad \downarrow \\
\left(\frac{1}{t} \sum\limits_{l=1}^{t} \cos \frac{2\pi k_l g(\sigma)}{m} \right) |0\rangle^{\otimes \log t} |0\rangle + \ldots \\
\quad \downarrow \\
g = 0 \iff \text{результат измерений} - |0\rangle^{\otimes \log t} |0\rangle
\end{array}
$$

Возможно также обобщение данного подхода для проверки одновременного выполнения ряда свойств, закодированных функциями g_1, g_2, …, g_l. Для этого по входному набору σ создается квантовая суперпозиция вида

$$\left|h^i_\sigma(j)\right\rangle = \cos \frac{\pi k_i g_j(\sigma)}{m} |0\rangle + \sin \frac{\pi k_i g_j(\sigma)}{m} |1\rangle \; |h_\sigma\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \left|h^i_\sigma(1)\right\rangle \left|h^i_\sigma(2)\right\rangle \ldots \left|h^i_\sigma(l)\right\rangle \quad .$$

Неформально, это можно проиллюстрировать следующим образом:



Другими словами, здесь реализуется комбинация классического и квантового параллелизма: l кубит используются параллельно (в классическом смысле), и каждый из них параллельно (в квантовом смысле) вращается на t различных углов.

4 Квантовые вычисления для программистов

Разработка квантовых компьютеров ставит множество задач как для математиков, так и для инженеров. Причем обе категории исследователей движутся навстречу друг другу: одни разрабатывают быстрые и эффективные по памяти квантовые алгоритмы, а вторые продвигаются в создании полномасштабных квантовых вычислителей, способных устойчиво работать достаточно продолжительное время.

Однако на данный момент вычислители сильно ограничены как по времени жизни системы, так и по числу одновременно доступных кубит. Поэтому реалистичным представляется вариант гибридного квантового компьютера, состоящего из небольшого (по памяти) квантового устройства, работающего под управлением классического компьютера, который задает последовательность применения унитарных операций, получает результаты измерения, а также может производить вспомогательные расчеты.

4.1 Задачи для программистов

Хотя создание квантовых компьютеров все еще находится в экспериментальной стадии, уже сейчас можно сформулировать задачи в классическом программировании, решение которых будет способствовать развитию области квантовых вычислений.

- Эмуляция квантовых вычислений, в том числе эффективное моделирование квантовой запутанности. Последнее позволит решать задачи и проверять гипотезы в теории квантовой информации.

  Одним из вариантов эмуляции квантового сопроцессора могла быть стать разработка виртуального драйвера для популярных операционных систем, который позволит тестировать разнообразные квантовые алгоритмы, а также другие программные разработки, связанные с функционированием квантовых вычислителей.

- Разработка системы программирования квантового сопроцессора.

  Данная задача тесно связана с предыдущей и может основываться на предположении, что квантовый сопроцессор предоставляет некоторый интерфейс (через драйвер, установленный в операционной системе), для взаимодействия с которым создается библиотека классов, скажем на C#.

  Такой набор классов основывается на возможности создания (инициализации) регистра квантовых битов в нулевом состоянии, применения базисных операций к произвольным кубитам регистра, а также измерение квантового регистра (получение результата вычислений).

  Для удобства в библиотеке должны быть также реализованы “общеупотребительные” квантовые операторы, поскольку их всегда можно выразить через базис. На основе данной библиотеки можно будет реализовывать известные эффективные квантовые алгоритмы в виде обычной функции на языке вроде C#.

- Разработка визуальной среды для конструирования и анализа квантовых алгоритмов.

  Данная задача подразумевает создание инструментальных средств, позволяющих наглядно представлять квантовые алгоритмы в модели квантовых схем из функциональных элементов. Разрабатываемая среда должна предоставлять средства для разложения отдельных квантовых преобразований по вычислительному базису, а также объединения отдельных частей алгоритма в составные операторы. Кроме того, предполагается реализации оптимизационных процедур для сокращения числа элементарных операторов, а также для сокращения числа шагов за счет параллельного выполнения некоторых операторов.

Основные обозначения

$\lceil a \rceil$ – наименьшее целое число, не меньшее a.

$\lfloor a \rfloor$ – наибольшее целое число, не превосходящее a.

$\log a = \log_2 a$.

$|K|$ – мощность конечного множества K.

B_n – множество булевых функций от n переменных.

Нормы вектора $a = (a_1, \ldots, a_d)$:
$||a||_1 = \sum_{i=1}^{d} a_i$,
$||a||_2 = \sqrt{\sum_{i=1}^{d} |a_i|^2}$.

$\mathcal{H}^d$ – d-мерное комплексно-значное векторное (Гильбертово) пространство с нормой $||.|| = ||.||_2$.

U^* – матрица, комплексно-сопряженная к U.

U^T – транспонированная матрица U.

$U^\dagger = (U^T)^*$ – эрмитово сопряжение к U.

$|a\rangle$ – вектор-столбец (кет-вектор) a.

$\langle b| = (|b\rangle^T)^*$ – вектор-строка (бра-вектор) b^*.

$\langle a\,|\,b\rangle$ – скалярное произведение $|a\rangle$ и $|b\rangle$.

$|a\rangle \otimes |b\rangle$ – *тензорное (правое кронекерово) произведение* векторов a, b.
Для $|a\rangle = (a_1, \ldots, a_d)^T$ и $|b\rangle = (b_1, \ldots, b_l)^T$
$|a\rangle \otimes |b\rangle = (a_1 b_1, a_1 b_2, \ldots, a_1 b_l, a_2 b_1, \ldots, a_d b_l)^T$.

$|a\rangle\,|b\rangle = |ab\rangle = |a\rangle \otimes |b\rangle$

$|a\rangle\,\langle b| = |a\rangle \otimes \langle b|$

$A \otimes B$ – *тензорное (правое кронекерово) произведение* матриц A, B

Для $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ и $B = \begin{pmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & \ddots & \vdots \\ b_{l1} & \cdots & b_{lk} \end{pmatrix}$

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$$

$A^{\otimes d} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{d}$.

$(A \otimes B)(|\phi\rangle \otimes |\psi\rangle) = A\,|\phi\rangle \otimes B\,|\psi\rangle$.

$\Big(|\phi_1\rangle \otimes |\psi_1\rangle \, , |\phi_2\rangle \otimes |\psi_2\rangle \Big) = \langle \phi_1 | \phi_2 \rangle \langle \psi_1 | \psi_2 \rangle$.

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – тождественное преобразование в $\mathcal{H}^2$.

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ – преобразование Адамара (Уолша-Адамара).

$R_{\hat{y}}(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$ – вращение на угол θ вокруг оси $\hat{y}$ сферы Блоха.

$C(R_{\hat{y}}(\theta)) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ 0 & 0 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$ – контролируемое вращение.

$f(n) = O(g(n))$ – существуют положительные константы c и n_0, такие, что $0 \leq f(n) \leq cg(n)$ для всех $n \geq n_0$.

$f(n) = \Omega(g(n))$ – существуют положительные константы c и n_0, такие, что $0 \leq cg(n) \leq f(n))$ для всех $n \geq n_0$.

$f(n) = \Theta(g(n))$, если $f(n) = O(g(n))$ и $f(n) = \Omega(g(n))$.

Список литературы

[1] Bennett, C.H. Logical reversibility of computations / C.H. Bennett // IBM Jounal of Res. Develop. – 1973. – V. 17. – P. 525-532.

[2] Benioff, P.A. Quantum mechanical hamiltonian models of turing machines / P.A. Benioff // Journal of Statistical Physics. – 1982. – V. 29, N 3. – P. 515-546.

[3] Bernstein, E. Quantum complexity theory / E. Bernstein, U. Vazirani // SIAM J. Comput. – 1997. – V. 26, N 5. – P. 1411-1473.

[4] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proceedings of the Royal Society of London. – Series A, Mathematical and Physical Sciences. – 1985. – PP. 97–117.

[5] Deutsch D. Quantum computational networks // Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences. – 1989. – PP. 73–90.

[6] Feynman R. Simulation physics with computers // Int. J. of Theor. Phys. – 1982. – V. 21. – No 467.

[7] Jozsa R., Linden N. On the role of entanglement in quantumcomputational speed-up // Proceedings: Mathematical, Physical and Engineering Sciences. – 2003. – Vol. 459, no. 2036. – PP. 2011–2032.

[8] Нильсен, М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг; Пер. с англ. под ред. М.Н. Вялого и П.М. Островского с предисловием К.А. Валиева. – М.: Мир, 2006. – 824 с.

[9] Sauerhoff, M. Quantum branching programs and space-bounded nonuniform quantum complexity / M. Sauerhoff, D. Sieling // http://xxx.lanl.gov/archive/quant-ph. – ph/0403164. – 2004.

[10] Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P. Shor // SIAM J. on Computing. – 1997. – V. 26, N 5. – P. 1484-1509.

[11] Vidal G. Efficient classical simulation of slightly entangled quantum computations // Physical Review Letters. – 2003. – Vol. 91, no. 14. – P. 147902. 120.

[12] Yao A. Quantum circuit complexity / A. Yao // Proc. 34th IEEE Symposium on Foundation of Computer Science. – 1993. – P. 352-361.