Зуев С.В., канд. физ.-мат. наук
Белгородский государственный технологический университет им. В.Г. Шухова

МОДЕЛИРОВАНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ НА КЛАССИЧЕСКОМ КОМПЬЮТЕРЕ

sergey.zuev@bk.ru

Квантовые вычисления считаются будущим вычислительной техники. Давая экспоненциальный выигрыш в скорости решения самых востребованных NP задач, а также открывая возможности в построении систем искусственного интеллекта, криптографии и распознавания образов, квантовые алгоритмы сейчас не используются только по причине отсутствия собственно квантового компьютера. Это препятствие уже в ближайшее время может быть преодолено, поскольку ведущие компании мира вкладывают огромные ресурсы в разработки в этом направлении и первые результаты есть уже во многих странах, в том числе и в России.

Среди известных квантовых алгоритмов особое место занимают алгоритмы нахождения порядка и факторизации. Ввиду их важности в вопросах информационной безопасности, возникает вопрос о тестировании и модификации этих алгоритмов для прикладных задач на классическом компьютере. Успешное испытание квантового алгоритма на классическом компьютере делает его готовым к применению на квантовом устройстве незамедлительно после его появления.

В настоящей работе построены представления состояний кубита и операций над ними, позволяющие моделировать простейшие квантовые алгоритмы на классическом компьютере с заданной точностью.

***Ключевые слова**: квантовые вычисления, квантовый алгоритм, кубит, квантовое преобразование Фурье, алгоритм факторизации.*

Введение, постановка задачи

Согласно широко распространенному в научном сообществе мнению, выраженному в книгах, научных и научно-популярных статьях (например, [5], [3], [6], соответственно), эволюция компьютерной техники будет идти в области развития систем квантовых вычислений (квантовых компьютеров). Их принцип действия основан на фундаментальных физических закономерностях микромира – квантовой механике. Создание таких устройств сопряжено с успехами исследований на переднем крае современной физики: достаточно посмотреть на авторитетный электронный источник http://xxx.lanl.gov, раздел quant-ph, где большая часть статей посвящена вопросам, связанным с тематикой квантовых вычислений.

Базовой единицей информации в квантовых вычислениях является *кубит* – нормированный вектор в двумерном комплексном линейном векторном пространстве. Сам квантовый алгоритм иллюстрируется графически *квантовой схемой*, в которой кубиты занимают регистры, изображаемые горизонтальными прямыми, а элементы, осуществляющие преобразования кубитов, обозначаются прямоугольными блоками. Один из пионеров квантовых вычислений Дэвид Дойч в своей работе [1] показал, что преобразования кубита можно без потери общности осуществлять с помощью нескольких *квантовых элементов* (иначе называются *квантовые вентили* или, в английском варианте *quantum gates*).

Полезность квантовых вычислений заключается в возможности параллельной обработки информации с помощью преобразований системы кубитов. Трудности заключаются в свойстве *декогерентности* квантовых систем – при измерении кубит принимает определенное значение и остается в нем.

Известные на сегодняшний день квантовые алгоритмы обеспечивают значительный выигрыш в скорости вычислений по сравнению с классическими. Однако, их реализация наталкивается на трудности чисто физического характера – устройство для квантовых вычислений создать трудно и не менее трудно доказать, что созданное устройство выполняет квантовые вычисления. Кроме того, сами квантовые вычисления, ввиду вероятностной природы результатов квантовых измерений, выдают требуемые результаты лишь с определенной вероятностью. Ввиду этого возникает вопрос об оценке ошибок квантовых вычислений.

Последние исследования (см. [2] и ссылки в работе) показывают, что наиболее вероятным кандидатом на коррекцию ошибок квантовых вычислений является ренорм-группа высокого разрешения и другие топологические методы. Это позволяет надеяться на возможность классического моделирования квантовых вычислений с помощью дискретных преобразований в алгебрах Ли, в частности, в алгебре кватернионов, равных по модулю 1. Именно такая попытка предпринята в настоящей статье для широко

используемого в приложениях квантового преобразования Фурье.

Методика классического моделирования квантового алгоритма

Чтобы построить классическую модель квантового вычисления, следует построить с требуемой точностью конечные представления состояния кубита и модели действий квантовых вентилей на составных системах таких состояний. Хорошая модель должна позволять задавать уровень точности до начала вычислений.

Для представления состояний кубита воспользуемся его кватернионным представлением. Состояния кубита могут быть заданы парой комплексных чисел: $z = \sin\alpha\,(\cos\varphi + k\sin\varphi)$ и $w = \cos\alpha\,(\cos\psi + k\sin\psi)$, где $\alpha, \varphi, \psi \in [0,2\pi)$, $k^2 = -1$. В этом случае, состояние в базисе $|0\rangle, |1\rangle$ (*вычислительный базис*) представляется в виде $z|0\rangle + w|1\rangle$, а условие нормировки $|z|^2 + |w|^2 = 1$ выполняется тождественно. Записав кватернион q в виде

$$q = z + wj = \sin\alpha\cos\varphi - i\cos\alpha\sin\psi + \\ +j\cos\alpha\cos\psi + k\sin\alpha\sin\varphi = \\ = q(\alpha,\varphi,\psi),\ j^2 = -1, jk = -kj \equiv i, \quad (1)$$

получаем взаимно однозначное соответствие между кватернионом q и парой комплексных чисел z, w, связанных условием $|z|^2 + |w|^2 = 1$, которая собственно и является кубитом. Легко проверить, что $|q| = 1$.

Пусть имеется эффективный квантовый алгоритм, дающий решение какой-то задачи с существенным использованием квантового параллелизма и обеспечивающий выигрыш в количестве операций. Тогда этот алгоритм может быть реализован на классическом компьютере с помощью кватернионного представления состояния кубита: достаточно все операции, осуществляемые квантовыми элементами, представить как кватернионные преобразования, которые, в свою очередь, осуществляются классическим компьютером обычными операциями. Экономия в количестве операций при этом может быть достигнута только в кватернионном представлении. При переходе от кватернионного представления кубита к двоичному представлению данных, экономия теряется. Таким образом, на классическом компьютере добиться существенной экономии в числе операций не удастся, но имеется возможность тестирования и отладки квантовых алгоритмов.

Квантовое преобразование Фурье

Для иллюстрации предложенного метода классического моделирования квантовых вычислений, рассмотрим хорошо известное дискретное преобразование Фурье и его квантовый аналог.

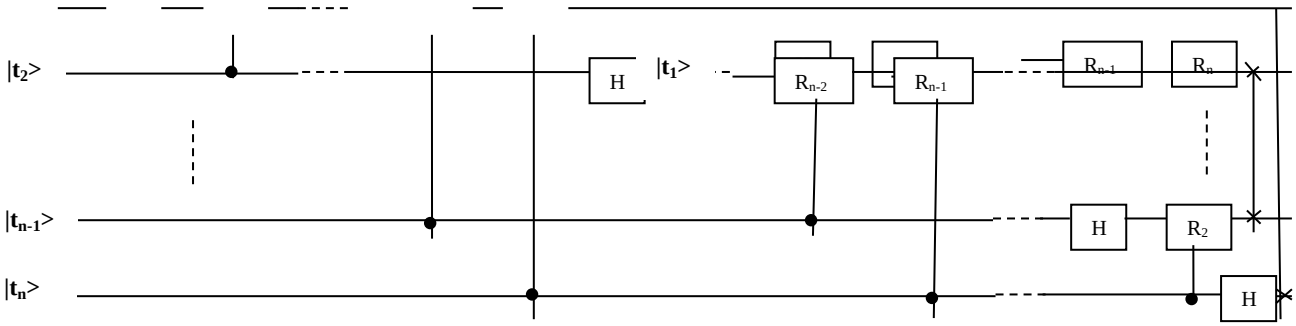

Рис. 1. Квантовая схема, осуществляющая дискретное преобразование Фурье

Дискретное преобразование Фурье – это унитарное преобразование комплексного вектора с координатами $x_0, \ldots, x_{N-1}$ в комплексный вектор с координатами $y_0, \ldots, y_{N-1}$ по формуле:

$$y_k = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1} x_l e^{2\pi i l k/N}. \quad (2)$$

Это преобразование используется во множестве приложений: от алгоритмов архивации до распознавания изображений, а в квантовых вычислениях – и как часть алгоритма нахождения порядка, который, в свою очередь, является частью алгоритма факторизации.

На рис. 1 изображена квантовая схема преобразования Фурье, представленная в книге [4]. Ее работа основана на том, что для $N = 2^n$ каждый комплексный N-мерный вектор можно представить как линейную комбинацию векторов вычислительного базиса $|0\rangle, \ldots, |N-1\rangle$ с комплексными коэффициентами, а сами векторы вычислительного базиса можно символически записать так

$$|0 \ldots n \text{ штук} \ldots 0\rangle, |0 \ldots 01\rangle, |1 \ldots 11\rangle, \quad (3)$$

так что, например, $|6\rangle \equiv |110\rangle$, где 110 – двоичная запись числа 6. В квантовой схеме предполагается, что исходный комплексный вектор представляется в виде

$$|x\rangle = x_0|0 \ldots 0\rangle + \cdots + x_{N-1}|1 \ldots 1\rangle \quad (4)$$

и подается на вход схемы, которая производит над ним унитарное преобразование U так, что на выходе получается вектор

$$|y\rangle = U|x \geq x_0 U|0 \ldots 0\rangle \\ > + \cdots + x_{N-1}U|1 \ldots 1 \geq y_0|0 \ldots 0\rangle + \cdots + \quad (5)$$

$$+y_{N-1}|1 \dots 1>.$$

Тем самым, для нахождения по заданным значениям $x_0, \dots, x_{N-1}$ величин $y_0, \dots, y_{N-1}$, достаточно знать, что схема осуществляет преобразование U, которое является квантовым преобразованием Фурье, и вычислить действие этого преобразования на векторы вычислительного базиса. Тогда координаты $y_0, \dots, y_{N-1}$ преобразованного вектора в том же базисе будут результатом применения дискретного преобразования Фурье к набору комплексных чисел $x_0, \dots, x_{N-1}$.

Представленная на рис. 1 квантовая схема реализует действие оператора квантового преобразования Фурье на базисный элемент $|t>$ для любого $t = 0, \dots N-1$. Для этого элемент $|t>$ записывается в двоичном представлении $|t_n \dots t_1>$, где каждый знак принимает значение 0 или 1, и на s-й регистр (горизонтальную линию схемы) подается кубит в чистом состоянии $|t_s>$. На выходе этого регистра появится состояние, являющееся суперпозицией базисных векторов $|0>$и $|1>$: $|\hat{t}_s>=\tau_{0s}|0>+\tau_{1s}|1>$, причем значения $\tau_{0s}(t)$ и $\tau_{1s}(t)$ для всех s будут зависеть от поданного на вход значения t. Преобразованное состояние $|\hat{t}>$ базисного элемента будет выглядеть как тензорное произведение состояний регистров:

$$|\hat{t}>=(\tau_{01}|0>+\tau_{11}|1>)\dots(\tau_{0n}|0>+\tau_{1n}|1>)=\tau_{01}\dots\tau_{0n}|0\dots0>+\tau_{01}\dots\tau_{1n}|0\dots1>+\dots+$$
$$+\tau_{11}\dots\tau_{1n}|1\dots1>. \quad (6)$$

В последней сумме находится $2^n = N$ слагаемых, которые являются компонентами вектора состояния составной системы из n кубитов после преобразования. Поскольку $|t>$ есть базисный элемент, то любой комплексный вектор с координатами $x_0, \dots, x_{N-1}$ представляется в виде:

$$|x>=x_0|0\dots0>+\dots+x_{N-1}|1\dots1>, \quad (7)$$

а следовательно, вектор $|y>$ будет иметь вид:

$$|y>=y_0|0\dots0>+\dots+y_{N-1}|1\dots1>=x_0[\tau_{01}(0)\dots\tau_{0n}(0)|0\dots0>+\dots+\tau_{11}(0)\dots\tau_{1n}(0)|1\dots1>]+$$
$$+x_{N-1}[\tau_{01}(N-1)\dots\tau_{0n}(N-1)|0\dots0>+\dots+\tau_{11}(N-1)\dots\tau_{1n}(N-1)|1\dots1>]. \quad (8)$$

В итоге дискретное преобразование Фурье будет представлено соотношениями:

$$y_0 = x_0\tau_{01}(0)\dots\tau_{0n}(0)+\dots+x_{N-1}\tau_{01}(N-1)\dots\tau_{0n}(N-1), \dots,$$
$$y_{N-1} = x_0\tau_{11}(0)\dots\tau_{1n}(0)+\dots+x_{N-1}\tau_{11}(N-1)\dots\tau_{1n}(N-1) \quad (9)$$

и для его полного определения достаточно определить значения $2n$ функций $\tau_{0i}(t), \tau_{1i}(t), i = 1, \dots, n,$ для целых аргументов от 0 до $N-1$.

Рассмотрим работу квантовой схемы преобразования Фурье в кватернионном представлении кубитов. Для этого запишем в кватернионном виде квантовые элементы:

$$H \equiv \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \text{ и } R_l \equiv \begin{pmatrix}1 & 0\\ 0 & e^{2\pi k/2^l}\end{pmatrix}. \quad (10)$$

Пусть под действием элемента H кубит из состояния q переходит в состояние $\hat{q}$. Тогда, по определению элемента H, имеем $\hat{q} = \frac{1}{\sqrt{2}}\big((z+w)+(z-w)j\big)$ или

$$\hat{q} = \frac{1}{\sqrt{2}}\big((\sin\alpha\cos\varphi+\cos\alpha\cos\psi)-i(\sin\alpha\sin\varphi-\cos\alpha\sin\psi)+j(\sin\alpha\cos\varphi-\cos\alpha\cos\psi)+$$
$$+k(\sin\alpha\sin\varphi+\cos\alpha\sin\psi)\big), \quad (11)$$

в то же время, $\hat{q} = \hat{q}\big(\hat{\alpha}, \hat{\varphi}, \hat{\psi}\big) = \sin\hat{\alpha}\cos\hat{\varphi} - i\cos\hat{\alpha}\sin\hat{\psi} + j\cos\hat{\alpha}\cos\hat{\psi} + k\sin\hat{\alpha}\sin\hat{\varphi}$, что приводит к соотношениям:

$$\sin\hat{\alpha}\cos\hat{\varphi} = \frac{1}{\sqrt{2}}(\sin\alpha\cos\varphi+\cos\alpha\cos\psi)$$
$$\cos\hat{\alpha}\sin\hat{\psi} = \frac{1}{\sqrt{2}}(\sin\alpha\sin\varphi-\cos\alpha\sin\psi)$$
$$\cos\hat{\alpha}\cos\hat{\psi} = \frac{1}{\sqrt{2}}(\sin\alpha\cos\varphi-\cos\alpha\cos\psi)$$
$$\sin\hat{\alpha}\sin\hat{\varphi} = \frac{1}{\sqrt{2}}(\sin\alpha\sin\varphi+\cos\alpha\sin\psi) \quad (12)$$

из которых получаем

$$cos\,\hat{\alpha} = \frac{\sqrt{1-sin\,2\alpha\,cos(\varphi-\psi)}}{\sqrt{2}},$$
$$\cos\hat{\varphi} = \frac{\sin\alpha\cos\varphi+\cos\alpha\cos\psi}{\sqrt{1+\sin 2\alpha\cos(\varphi-\psi)}},$$
$$cos\,\hat{\psi} = \frac{sin\,\alpha\,cos\,\varphi-cos\,\alpha\,cos\,\psi}{\sqrt{1-sin\,2\alpha\,cos(\varphi-\psi)}}. \quad (13)$$

Эти соотношения задают преобразование кватерниона под действием квантового элемента H.

Вычислим таким же путем преобразование для квантового элемента R_l: пусть q_l является результатом действия элемента R_l на q. Тогда, с одной стороны,

$$q_l = z + e^{2\pi k/2^l}wj = \sin\alpha\cos\varphi + k\sin\alpha\sin\varphi + \left(\cos\frac{\pi}{2^{l-1}} + k\sin\frac{\pi}{2^{l-1}}\right)\cos\alpha\,(\cos\psi + k\sin\psi)j =$$
$$= \sin\alpha\cos\varphi - i\cos\alpha\sin\left(\frac{\pi}{2^{l-1}}+\psi\right) + j\cos\alpha\cos\left(\frac{\pi}{2^{l-1}}+\psi\right) + k\sin\alpha\sin\varphi, \quad (14)$$

а с другой стороны, обозначая преобразованные параметры через $\alpha_l, \varphi_l, \psi_l$, имеем

$$q_l = \sin\alpha_l \cos\varphi_l - i\cos\alpha_l \sin\psi_l + \\ +j\cos\alpha_l \cos\psi_l + k\sin\alpha_l \sin\varphi_l \quad (15)$$

и преобразование будет сводиться к преобразованию параметра ψ:

$$\alpha_l = \alpha,\ \varphi_l = \varphi,\ \psi_l = \psi + \frac{\pi}{2^{l-1}}. \quad (16)$$

В итоге, композиция преобразований $R_l H$ $(l = 2, \dots n)$ есть преобразование исходного кубита вида $q(\alpha, \varphi, \psi) \to \hat{q}_l(\hat{\alpha}_l, \hat{\varphi}_l, \hat{\psi}_l)$, где новые параметры определяются соотношениями

$$\hat{\alpha}_l = \arccos\left(\frac{\sqrt{1-\sin 2\alpha\cos(\varphi-\psi)}}{\sqrt{2}}\right),$$
$$\hat{\varphi}_l = \arccos\left(\frac{\sin\alpha\cos\varphi+\cos\alpha\cos\psi}{\sqrt{1+\sin 2\alpha\cos(\varphi-\psi)}}\right),$$
$$\hat{\psi}_l = \arccos\left(\frac{\sin\alpha\cos\varphi-\cos\alpha\cos\psi}{\sqrt{1-\sin 2\alpha\cos(\varphi-\psi)}}\right) + \frac{\pi}{2^{l-1}}. \quad (17)$$

Заметим, что на вход схемы подаются только состояния вычислительного базиса: |0> или |1>, а кватернионы этих состояний находятся из соображений $z = 1, w = 0$ для состояния |0> и $z = 0, w = 1$ для состояния |1>. Легко найти, что они имеют вид:

$$q_{|0>}\left(\frac{\pi}{2}, 0, 0\right) = 1,\ q_{|1>}(0,0,0) = j \quad (18)$$

В схеме на рис. 1 операторы R_l работают только тогда, когда в управляющем ими регистре находится состояние |1>. Значит, в формулах (1) следует установить символ Кронекера и, с учетом начальных значений $\varphi = \psi = 0$, находим для *s*-го кубита:

$$\hat{\alpha}_s = \frac{\pi}{4}, \hat{\varphi}_s = 0,$$
$$\hat{\psi}_s = \pi\delta_{0\alpha} + \sum_{m=2}^{n-s+1}\frac{\pi}{2^{m-1}}\delta_{1,t_{m+s-1}}. \quad (19)$$

или, в кватернионном виде:

$$\hat{q}_s = \frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\sin\hat{\psi}_s + j\frac{1}{\sqrt{2}}\cos\hat{\psi}_s = \frac{1}{\sqrt{2}}\left(1 + e^{k\hat{\psi}_s}j\right), \quad (20)$$

а в векторном виде

$$|\hat{q}_s> = \frac{1}{\sqrt{2}}\left(|0> + e^{k\hat{\psi}_s}|1>\right). \quad (21)$$

Заметим теперь, что $|\hat{q}_s>$ есть те же самые векторы, что рассмотренные выше $|\hat{t}_s>$, с точностью до обращения порядка нумерации кубита: $|\hat{q}_1> = |\hat{t}_n>, \dots, |\hat{q}_n> = |\hat{t}_1>$, следовательно

$$\tau_{0s}(t) = \frac{1}{\sqrt{2}}, \tau_{11}(t) = \frac{1}{\sqrt{2}}e^{k\hat{\psi}_n(t)}, \dots, \tau_{1n}(t) = \\ = \frac{1}{\sqrt{2}}e^{k\hat{\psi}_1(t)} \quad (22)$$

где

$$\hat{\psi}_s(t) = \pi\delta_{1,t_s} + \sum_{m=2}^{n-s+1}\frac{\pi}{2^{m-1}}\delta_{1,t_{m+s-1}}. \quad (23)$$

В итоге имеем дискретное преобразование Фурье в виде:

$$y_0 = \frac{1}{2^{n/2}}(x_0 + \dots + x_{N-1}),$$
$$y_1 = \frac{1}{2^{n/2}}\left(x_0 e^{k\hat{\psi}_1(0)} + \dots + x_{N-1}e^{k\hat{\psi}_1(N-1)}\right),$$
$$y_{N-1} = \frac{1}{2^{n/2}}\left(x_0 e^{k\sum_{r=1}^{n}\hat{\psi}_r(0)} + \dots + x_{N-1}e^{k\sum_{r=1}^{n}\hat{\psi}_r(N-1)}\right). \quad (24)$$

Вычислительная реализация этого преобразования на классическом компьютере может быть произведена по формулам (19), где существенная часть, дающая взаимосвязь между начальным (t) и конечным (ψ) состояниями задана формулой (23).

Выводы

Для построения, тестирования и отладки квантовых алгоритмов можно использовать классические компьютеры. В частности, в работе показан способ моделирования квантовых вычислений на классическом компьютере с помощью кватернионного представления состояния кубита и его преобразований. Полученная математическая модель квантового преобразования Фурье может быть использована для полноценного тестирования квантового алгоритма нахождения порядка и, следовательно, для создания полного алгоритма факторизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Deutsch D. Quantum computational networks // Proc. R. Soc. Lond. 1989. A425. P.73-90.

2. Hutter A., Loss D., Wootton J.R. Improved HDRG decoders for qudit and non-Abelian quantum error correction [arXiv:1410.4478v1 [quant-ph] 16 Oct 2014]. Систем. требования: AdobeAcrobatReader. URL: http://xxx.lanl.gov/pdf/1410.4478.pdf (дата обращения: 21.10.2014).

3. Валиев К.А. Квантовые компьютеры и квантовые вычисления // УФН. 2005. Т. 175. С. 3-39.

4. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Пер. с англ. М.: Мир, 2006. 824 с.

5. Ожигов Ю.И. Конструктивная физика. Ижевск: Изд. РХД, 2010. 424 с.

6. Холево А. Квантовая информатика: прошлое, настоящее, будущее // В мире науки. 2008. №7. С. 68-7