3 Принципа квантового компьютинга

Ю.И.Ожигов[1,2]

1. МГУ им. М.В.Ломоносова, Факультет ВМК,
2. ФТИАН им. К.А.Валиева
...
http://sqi.cs.msu.ru
https://vql.cs.msu.ru
http://fkk.ftian.ru

Содержание

Суть

1. Итог более чем 20 летних экспериментов в области квантовых компьютеров:
- получение и надежное детектирование запутанных состояний десятков частиц и подтверждение квантовой нелокальности;
-создание надежно работающих квантовых криптографических линий связи,
- необходимость существенной модификации квантовой теории в области сложных систем.

2. Ограничение копенгагенской квантовой теории соотношением неопределенностей "сложность - точность" для любой квантовой системы:

$$C(|\Psi\rangle)A(|\Psi\rangle) \leq Q.$$

3. Принципы квантового компьютинга: опора на конечномерные модели, ограничение локальных вычислительных ресурсов, аналогия процессов разной природы.

Введение. Краткая история проекта КК

Квантовый компьютер как проект есть применение квантовой теории к сложным системам для предсказательного моделирования их динамики.

1982. Р.Фейнман: КК должен строиться из элементарных устройств - гейтов, соединением их в схему, наподобие электронных микросхем. Контр-интуитивные свойства запутанности - мгновенное действие на расстоянии - экспериментальный факт (А.Аспек, А.Цайлингер).
1985. Д.Дейч: квантовое вычисление есть унитарная эволюция состояния системы кубитов под управлением классического компьютера. Квантовая криптография физически реализована.
1994-2000. Математики: квантовое вычисление способно решать задачи перебора принципиально быстрее любого классического компьютера (П.Шор, Л.Гровер и др., в том числе нижние оценки квантовой сложности). Декогерентность преодолеем кодами коррекции и разными технологиями квантовых процессоров.

Введение. Проблема настоящего времени

2000 - н.в. Эксперимент: несколько кубитов работают удовлетворительно.
Декогерентность - общая проблема для всех технологий, и не решается кодами коррекции. Описание декогерентности в виде квантового основного уравнения неприменимо к сложным системам: их окружение не марковское.
Мы можем создавать простые квантовые устройства, но не знаем, как управлять их композицией.
Есть железо для КК но нет квантовой операционной системы.
Стандартный, фейнмановский путь упирается в предел на уровне 10-20 кубитов для любой технологии.

КК - не технический проект, а фундаментальный вопрос.

Как правильно ограничить квантовый формализм для продвижения в мир сложных процессов?

Квантовое описание любой системы частиц - только статистическое.

Квантовое состояние $|\Psi\rangle = \sum_{j \in J} \lambda_j |\psi_j\rangle$ **относится не к одной системе а к серии одинаково приготовленных систем.**

Можно говорить о волновой функции электрона в атоме водорода только потому, что таких атомов гигантское число.
Уникальная система не может иметь квантового состояния.

Сложность квантовых состояний. Наивный подход

Квантовое состояние n частиц имеет вид

$$|\Psi\rangle = \sum_{j \in J} \lambda_j |j\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$$

Наивная сложность $\nu(\Psi)$ есть число частиц в ядре - максимальном запутанном подмножестве частиц.

Например, для состояния n кубитов

$$\frac{1}{\sqrt{N}} \sum_{j=1}^{N-1} |j\rangle = \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}} (|0\rangle_j + |1\rangle_j)$$

в C^N, $N = 2^n$ наивная сложность равна 1:

В чем недостаток наивной сложности: для состояния n кубитов $\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$ она равна n, но это состояние очень простое: его можно распутать последовательным применением операторов CNOT.

Нужно более правильное определение сложности.

Каноническое преобразование и квазичастицы

Каноническое преобразование есть перестановка векторов базиса.
Это основной метод редукции сложности в физике многих частиц. Например, если представлять координаты $\bar{q}$ в виде последовательности битов в их бинарном разложении, так можно упростить динамику цепочки взаимодействующих осцилляторов.
Перейдем к другим координатам по формуле

$$\bar{Q} = \mathcal{F}(\bar{q}), \ \ Q_k = Q_k(q_1, q_2, ..., q_n), \ \ k = 1, 2, ..., n$$

где $\mathcal{F}$ - преобразование Фурье; мы будем иметь незапутанные состояния так называемых квазичастиц с новыми координатами Q_k - фононов. Это - перестановка базисных векторов, при которой кубиты уже играют совершенно иную роль.

Квантовая сложность $C(\Psi) = min_{\tau \in S_N} \nu(\tau|\Psi\rangle)$ **- минимальная наивная сложность состояния по всем перестановкам базисных векторов.**

Сложность квантовых состояний

Пример канонического преобразования - CNOT: $|x, y\rangle \to |x, x \oplus y\rangle$. Оно распутывает ЭПР пару $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

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

Сложность гамильтонианов

Разложение гамильтониана H:

$$H = H_{X_1} + H_{X_2} + \dots + H_{X_s}$$

Каноническое преобразование есть перестановка переменных, минимизирующая максимальное из чисел $|X_1|, |X_2|, \dots, |X_s|$; оно называется сложностью $C(H)$ гамильтгниана.

Пример: CNOT есть каноническое преобразование для гамильтониана H_1.

$CNOT\ H_1\ CNOT = H_q = \sigma_x^{(1)} \otimes I_2 + I_1 \sigma_x^{(2)}$.

$$H_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = CNOT \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} CNOT.$$

Если мы стартуем с незапутанного состояния, то в эволюции не может появиться состояния сложности большей чем сложность гамильтониана, так как

$$exp(-\frac{i}{\hbar}Ht) = exp(-\frac{i}{\hbar}H_{X_1}t) \otimes exp(-\frac{i}{\hbar}H_{X_2}t) \otimes \dots \otimes exp(-\frac{i}{\hbar}H_{X_s}t).$$

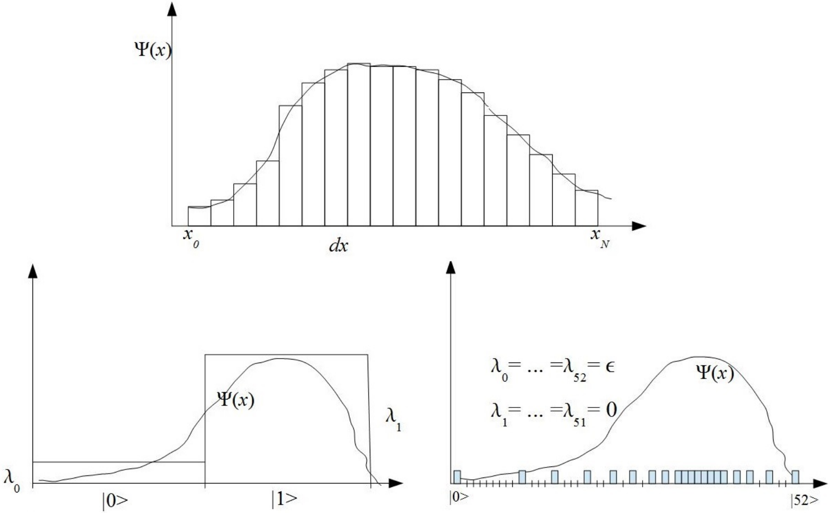
Точность квантового состояния

Точность есть число одинаково приготовленных экземпляров физической системы.

Figure: Сложность $\cdot$ точность $=$ общее число кубитов не может превышать размера оперативной памяти главного компьютера

$$C(|\Psi\rangle)A(|\Psi\rangle) \leq Q.$$

"Сложность vs точность"



Общее ограничение вычислительного ресурса имеет физичексий смысл

Сфера применимости квантовой теории органичена соотношением:

$$A(\Psi)C(\Psi) \leq Q \tag{1}$$

где константа Q должна быть найдена в эксперименте. В копенгагенской теории предполагалось что $Q = \infty$, современные эксперименты показывают, что эта величина конечна.

Наилучший путь нахождения данной константы - реализация алгоритма Гровера GSA.

Квантование амплитуды

Квантовое состояние $|\Psi\rangle = \sum_{j \in J} \lambda_j |\psi_j\rangle$ **относится не к одной системе а к серии одинаково приготовленных систем.** При этом $|\lambda_j|^2$ есть вероятность обнаружить состояние $|\psi_j\rangle$ при ее измерении в данном базисе.

Не существует вычислительных ресурсов для фиксации бесконечно маловероятных исходов при точной фиксации возможных базисных состоянийй, поэтому ненулевые амплитуды λ_j должны быть ограничены снизу некой константой ϵ.
Из линейности следует, что они имеют вид

$$\lambda_j = \epsilon n_j + i\epsilon m_j \tag{2}$$

где $n_j, m_j \in Z$ - целые, а в силу нормировки $\epsilon = 2^{-Q/2}$.

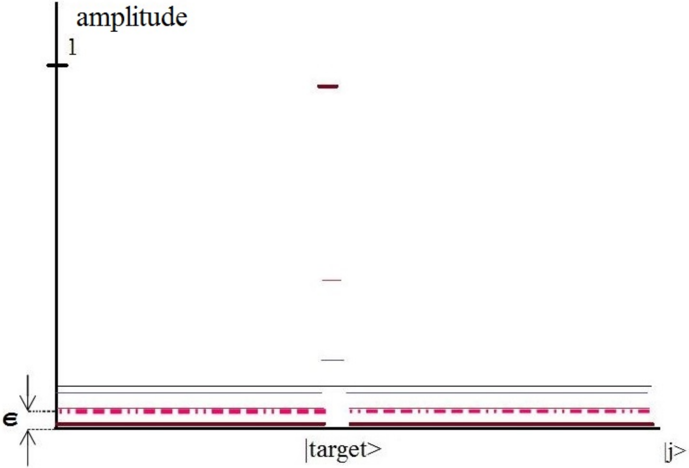
Нахождение порядка константы Q с помощью алгоритма Гровера GSA

GSA решает проблему поиска неизвестного состояния $|j_0\rangle$ через концентрацию на нем всей амлитуды.
GSA работает на состояниях вида

$$|\Psi_{GSA}(t)\rangle = \alpha \sum_{j \neq j_0, 0 \leq j < N} |j\rangle + \beta |j\rangle, \tag{3}$$

где $\alpha = cos(t)/\sqrt{N-1}$, $\beta = sin(t)$ для некоторого t, и $N = 2^n$. Сложность этого состояния равна n при $t \neq k\pi/2$ ни для какого целого k.
Порядок величины Q можно оценить как максимальное число кубитов, для которых алгоритм GSA дает верный ответ.

Нахождение порядка константы Q с помощью алгоритма Гровера GSA



GSA как мера сложности квантового описания реальных процессов

$C(|\Psi_{GSA}\rangle) = n$:
мы можем оценить возможность описания физического процесса в терминах общего числа кубитов, для которых GSA дает верный ответ.

Пусть t - общее время процесса, dt - шаг по времени, находимый из соотношения неопределенностей $dE\ dt = \hbar$; тогда число базисных состояний, требуемое для "точной прорисовки" процесса есть $N = t/dt$ (квантовое блуждание имеет линейную скорость, в противоположность классическому, имеющему скорость $\sqrt{t}$.)

КЭД vs ядерная физика

Пример 1 Осцилляции Раби для возбужденных состояний атома рубидия Ru^{85}: длина волны 1.4 cm $E_{QED} = \hbar\omega \approx 10^{-17}$, $dt \approx \hbar/E_{QED} = 10^{-10}$. Общее время рабиевских осцилляций $t \approx 10^{-6}$ sec дает $N = t/dt \approx 10^4$, $Q \geq 10^4 \approx 2^{13}$ и для того, чтобы их можно было описать в терминах стандартной квантовой механики, GSA должен работать на примерно 13 кубитах, что представляется вполне реальным.

Пример 2 Распад нестабильного ядра изотопа гелия $Helium - 6$:
$He^6 \rightarrow He^5 + n \rightarrow He^4 + 2n$ $E \approx 10$ $Mev \approx 10^{-5}$ erg, $dt \approx 10^{-22}$ sec.
$t \approx 1.6$ sec,$N = t/dt \approx 10^{22} \approx 2^{73}$, и если бы с помощью квантовой механики можно было бы корректно описать данный процесс, алгоритм GSA должен был бы работать для хотя бы 73 кубитов, что очень маловероятно.

(About quantum computer software, Quantum Information and Computation, Vol. 20, No. 7&8 (2020) 570-580)

Компьютерное моделирование на квантовом уровне

Квантовая операционная система на суперкомпьютере

Физическая часть квантового компьютера — прообраз реальной системы на квантовых точках, оптических полостях, волноводах

Реальная система

Заключение

Проект квантового компьютера не является техническим, он относится к фундаментальной области - физике сложных систем.

Математический формализм квантовой теории имеет ограничение в виде соотношения неопределенностей ''сложность - точность'', что ставит предел масштабированию квантового компьютера. Константа этого соотношения имеет физический смысл; от ее значения зависит конфигурация операционной системы квантового компьютера.

Главная цель экспериментов в области квантового компьютинга - определение значения константы в этом соотношении. Это можно сделать, реализуя алгоритм GSA.

Задача ближайшего времени - создание квантовой операционной системы для гибридного квантового компьютера, пользователь которого будет взаимодействовать только с его классической частью. Это - математическая задача, и ее роль дает возможность нам преодолеть известное отставание в приборной области за счет компьютерного моделирования.

Благодарности

Работы последнего года по теме доклада выполнены в Московском центре фундаментальной и прикладной математики.

Литература

- Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134. — ISBN 0-8186-6580-7 — doi:10.1109/SFCS.1994.365700
- L.Grover, A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219. Proceedings, Melville, NY, 2006, vol. 810.
- C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Demonstration of a Fundamental Quantum Logic Gate, Phys. Rev. Lett. 75, 4714 (1995).
- G. Rempe, H. Walther, and N. Klein. Observation of quantum collapse and revival in a one-atom maser, Phys. Rev. Lett., 1987, Vol. 58, no. 4, p. 353.
- A.Khrennikov, Vaxjo Interpretation of Wave Function: 2012, Reconsideration of Foundations-6, AIP, 1508, 244-252 (2012), DOI: 10.1063/1.4773136.

Литература

- Aspect, Alain; Dalibard, Jean; Roger, Gérard (December 1982). "Experimental Test of Bell's Inequalities Using Time- Varying Analyzers". Physical Review Letters. 49 (25): 1804–1807.
- Jian-Wei Pan; D. Bouwmeester; M. Daniell; H. Weinfurter; A. Zeilinger (2000). "Experimental test of quantum nonlocality in three-photon GHZ entanglement". Nature. 403 (6769): 515–519.
- J. Bell, "On the Einstein Podolsky Rosen Paradox"; Physics, (1964), 1 (3): 195–200.
- Y.Ozhigov, About quantum computer software, Quantum Information and Computation, Vol. 20, No. 7&8 (2020) 570-580.
- Y.I.Ozhigov, Distributed synthesis of chains with one-way biphotonic control, Quantum Information and Computation, vol. 18, 7-8, pp. 0592-0598.

- V. Ladunov, Y. Ozhigov, N. Skovoroda , Computer simulation of quantum effects in Tavis-Cummings model and its applications, SPIE Proceedings, vol. 10224, International Conference on Micro- and Nano-Electronics 2016; 102242X (2017) https://doi.org/10.1117/12.2267190
- Y.Ozhigov, Dark states of atomic ensembles: properties and preparation, Proc. SPIE 10224, International Conference on Micro- and Nano-Electronics 2016, 102242Y (December 30, 2016); doi:10.1117/12.2264516.
- V.M.Akulin, Dynamics of Complex Quantum Systems, Theoretical and Mathematical Physics, Spinger, 2006.