

Квантовый компьютер

Ю.И.Ожигов^{1,2}

1 Московский Государственный Университет им. М.В.Ломоносова
Факультет ВМК, Кафедра суперкомпьютеров и квантовой информатики

2 Физико-Технологический институт РАН

ozhigov@cs.msu.su

Содержание

Введение

Краткое описание квантовой механики

Быстрые квантовые алгоритмы

Реализация квантовых гейтов

Декогерентность

Введение

Квантовая теория должна объяснять все.

1900 - 1960 гг.: анализ микромира с точки зрения точного описания отдельных частиц, погружение "вглубь" микрокосма.

1970 - н.в. : синтез сложных систем на микроуровне, конденсированные состояния , квантовый компьютер, суперкомпьютерное моделирование динамики на квантовом уровне.

Далее: квантовая биология (много-частичная КМ необходима для объяснения отдельных эффектов), квантовая экономика, квантовая политика, квантовое принятие решений (отдельные результаты).

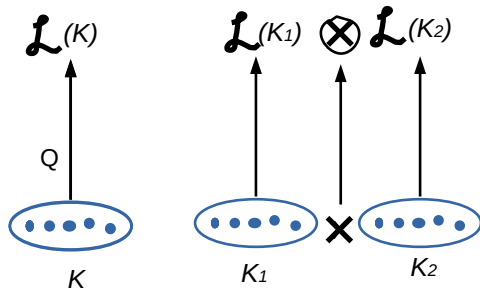




Figure: П.Дирак, Р.Фейнман, Л.Ландау, Н.Боголюбов

Квантовые состояния как линейные комбинации классических

Процедура квантования - переход к линейной оболочке. $\mathcal{L}(K)$ состоит из линейных комбинаций $|\Psi\rangle = \sum_j \lambda_j |j\rangle$, где все $|j\rangle \in K$ считаются взаимно ортогональными с единичной нормой. Объединение реальных систем приводит к тензорному произведению - что ведет к экспоненциальному росту размерности пространства квантовых состояний. Основная проблема: Сколько элементов может быть в множестве классических состояний K ?



Принцип интерференции

Амплитуда вдоль одного пути умножается на комплексное число, пропорциональное пройденному пути.

Амплитуды вдоль разных путей, приходящих в одну точку, складываются. При этом надо учесть всевозможные пути, ведущие в данную точку.

Вероятность есть квадрат модуля амплитуды.

Это правило точно формализуется в виде матричной эволюции

Фейнмановские диаграммы

Зерно разрешения - фундаментальное число, требуемое для математической корректности квантовой механики

Заряд электрона - амплитуды взаимодействия его с фотоном.

Заряд электрона точно не известен.

Фиксируется зерно разрешения по пространству и времени dx и dt .

Устанавливается пробное значение заряда электрона и его массы.

Определяется амплитуда основного процесса: взаимодействия электрона с фотоном, так что вероятность, рассчитанная по этой амплитуде, дает согласие с экспериментами.

При уменьшении зерна разрешимости dx , dt пробные заряды и массы изменятся, но вероятность будет только точнее совпадать с экспериментами. При этом значения заряда и массы, подобранные для одного эксперимента, дают столь же точное предсказание для всех других экспериментов.

Сходимость процесса назначения зарядов и масс называется теоремой и перенормировках квантовой электродинамики. Она была строго доказана Н.Боголюбовым в 1955 г.

Обычная квантовая механика. Эволюция квантового состояния во времени

1. Эволюция в присутствии наблюдателя, который измеряет систему. Измерение системы, находящейся в состоянии $|\Psi\rangle = \sum_j \lambda_j |j\rangle$ есть случайная величина, принимающая значения $|j\rangle$ с вероятностями $p_j = |\lambda_j|^2$.
2. Эволюция в отсутствии наблюдателя: решение уравнения Шредингера $i\hbar|\dot{\Psi}\rangle = H|\Psi\rangle$

$$|\Psi(t)\rangle = U_t |\Psi(0)\rangle, \quad U_t = e^{-\frac{i}{\hbar} H t}$$

$U_t : |\Psi(0)\rangle \rightarrow |\Psi(t)\rangle$ - оператор эволюции, $H = E_{kin} + E_{pot}$ - эрмитов оператор энергии; для одной частицы в потенциале V гамильтониан $H = \frac{p^2}{2m} + V(r)$, $p = -i\hbar\nabla$. Для конечномерного приближения H и U_t - матрицы, $|\Psi\rangle$ - столбец, зависящий от времени.

Интеграл Фейнмана по путям - непрерывный аналог матричной механики

Если есть k шагов продолжительности dt : $U_t = U_k U_{k-1} \dots U_0$, матричный элемент перехода будет

$$u_t(i, j) = \sum_{q_1, q_2, \dots, q_k} u_{dt}(q_1, j) u_{dt}(q_2, q_1) \dots u_{dt}(i, q_k)$$

что в непрерывном случае дает оператор эволюции в виде фейнмановского ядра

$$K(2, 1) = \int_{\gamma: 1 \rightarrow 2} \exp\left(\frac{i}{\hbar} S[\gamma]\right) \mathcal{D}\gamma$$

где действие S вдоль траектории γ есть

$S[\gamma] = \int_{t_0}^{t_1} L(\dot{x}, x, t) dt$, $L = E_{kin} - E_{pot}$, $\gamma: x = x(t)$, $t_0 \leq t \leq t_1$. Эволюция имеет вид

$$\Psi(2) = \int K(2, 1) \Psi(1) d1, \quad 1 = x_1, \quad 2 = x_2$$

Классическая механика как следствие интерференции амплитуд

Классическая траектория γ_{cl} отличается от прочих тем, что на ней $\frac{\delta S[\gamma_{cl}]}{\delta \gamma} = 0$. Поэтому в интеграле

$$K(2,1) = \int_{\gamma: 1 \rightarrow 2} \exp\left(\frac{i}{\hbar} S[\gamma]\right) \mathcal{D}\gamma$$

окрестности классической траектории складываются конструктивно, а окрестности прочих - деструктивно, если среднее действие на элементарном шаге превосходит постоянную Планка $\hbar \approx 10^{-27} \text{ erg sec}$. Если же среднее действие мало, неклассические траектории могут дать серьезный вклад.

Необходимость применять квантовую механику зависит от продолжительности dt элементарного шага моделирования процесса, то есть от сценария процесса.

Например, в задаче вычисления возможных состояний ассоциации молекул можно считать ядра классическими, а электроны нужно считать - квантовыми (модель Борна-Оппенгеймера).

Р.Ф.Фейнман (1918-1988)



Квантовый компьютер как вызов квантовой теории

1. Квантовый алгоритм есть рецепт специально организованного классического управления Гамильтонианом $H = H(t)$. Квантовое вычисление - соответствующая этому гамильтониану эволюция волновой функции квантового состояния определенной системы частиц.

Предположим, что нет никаких ограничений на размер множества K классических состояний, подлежащих квантованию. Тогда эволюция волновой функции $|\Psi\rangle$ при этом может привести к непредсказуемому результату, который невозможно получить никаким классическим алгоритмом в обозримое время. Такие способы управления называются быстрыми квантовыми алгоритмами.

2. Всем математическим методам квантовой теории можно придать форму эффективных классических алгоритмов.

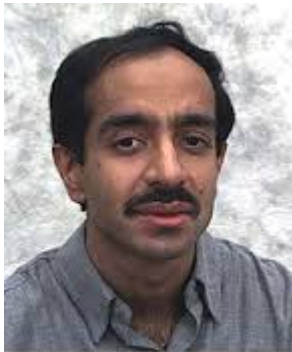
3. Физика квантовых компьютеров требует новых методов и более общего взгляда на область приложений квантовой механики.

4. Критерий качества математической модели: неизбежная редукция волновой функции от унитарной эволюции в ходе вычисления должна совпадать с наблюдаемой в экспериментах декогерентностью - спонтанным отклонением наблюдаемой динамики от унитарного закона

П.С.Шор



Л.К.Гровер



Алгоритм Гровера: квадратичное квантовое ускорение

Задача на перебор: найти решение x_{tar} уравнения $f(x) = 1$, где f - булевская функция от n переменных, заданная в виде схем из функциональных элементов.

Оператор Гровера G - поворот на угол $\arcsin(N^{-1/2})$. Реализуется с помощью двух зеркальных отражений: вдоль вектора $|\tilde{0}\rangle = \frac{1}{\sqrt{N}} \sum_j |j\rangle$ и вдоль неизвестного вектора $|x_{tar}\rangle$.

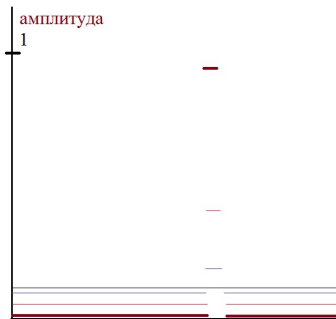
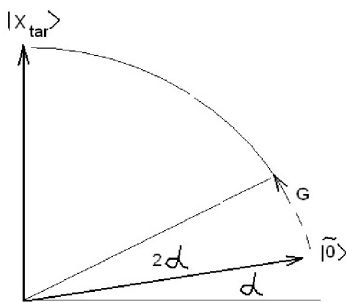
Последнее можно представить как $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ - реализуется, исходя из классической схемы для функции f .

Алгоритм Гровера:

повторение оператора G

$\left\lceil \frac{\pi\sqrt{N}}{4} \right\rceil$ раз

*Grover L.K., Proceedings,
28th Annual ACM Symposium
on the Theory of Computing,
1996*



Алгоритм Залки-Визнера

На квантовом компьютере можно моделировать решение уравнение Шредингера в случае простого потенциала за время $O(t^2)$, где t - время реального процесса, с памятью $O(n)$, где n - число частиц в реальной системе.

$$\exp(-\frac{i}{h}(H_{kin} + V(r))t) \approx (\exp(-\frac{i}{h}H_{kin}dt)\exp(-\frac{i}{h}V(r)dt))^{t/dt}$$

(Формула Троттера, ошибка $O(dt^2)$). Оператор $\exp(-\frac{i}{h}V(r)dt)$ диагонален, и его можно выполнить с помощью квантового алгоритма с памятью порядка размера реальной системы. Оператор $\exp(-\frac{i}{h}H_{kin}dt)$ приводится к диагональному переходом к импульсному базису. Квантовое преобразование Фурье требует ресурса $O(n)$ по времени и по памяти (Шор); достижение малой результирующей ошибки потребует $dt = O(1/t)$, что даст квадратичное замедление по времени по сравнению с реальным процессом.

C.Zalka, Proc.Roy.Soc.Lond. A454 (1998) 313-322, S.Wiesner, arXiv:quant-ph/9603028

Теоретические пределы возможностей квантового компьютера

Generic Machine Simulation Problem (GMSP): Нахождение результата t - кратного применения заданной функции F к данному аргументу x . GMSP- P-полная проблема, не допускающая распараллеливания (*Limits to Parallel Computation: P-Completeness Theory*, R.Greenlaw et al., University of New Hampshire, 1995).

На квантовом компьютере в модели F как "черного ящика" при $t = O(N^{1/7})$ (N - число всех состояний машины) с вероятностью 1 GSMP не допускает квантового ускорения даже на 1 шаг. Без ограничения на t квантовое время решения GSMP проблемы с вероятностью 1 не может быть больше $\Omega(\sqrt{t})$ (*Ozhigov Y.I., Chaos, Solitons and Fractals, 1999, 10 and Proc.R.Soc.Lond. A 1999, 455*).

Квантовый параллелизм оказывается тесно связан с классическим. Быстрые квантовые алгоритмы есть редкий феномен, имеющий место лишь для классических алгоритмов, допускающих распараллеливание (FNC класс сложности).

Гроверовское ускорение является типичным верхним пределом для большинства задач. Этот предел может превышаться только для отдельных частных случаев, например, факторизация целых чисел (алгоритм Шора P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, Proc. 35nd Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press , 1994).

CNOT гейт: $|x, y\rangle \rightarrow |x, x \oplus y\rangle$. на зарядовых состояниях

К.А.Валиев, Л.Е.Федичкин, Квантовые компьютеры и квантовые вычисления, т.9, 1, 2009

Для реализации произвольного унитарного оператора достаточно реализовать все однокубитные и какую-либо запутывающую левх-кубитную операцию например CNOT.

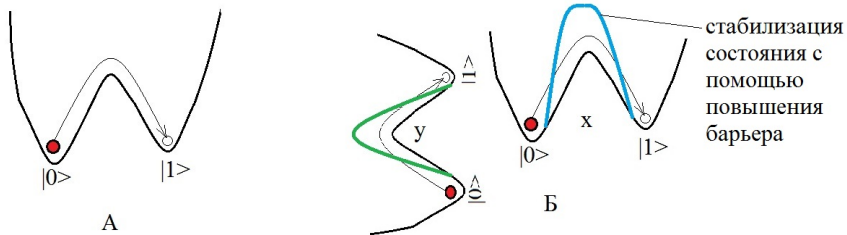


Figure: A. NOT на квантовой точке с двух-ямным потенциалом. Собственные состояния $|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ и $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Б. CNOT. Состояние точки x определяет высоту барьера в точке y (зеленый цвет), и скорость туннелирования в y .

Квантовые точки на NV- центрах в алмазе *F.Jelezko, S.Kilin, A.Nizovtsev, J.Wrachtrup, C.Tietz, A.Grubber, I.Popa, Single Molecules, 2001, vol.2, 4, 255*

Нелинейный фазовый сдвиг в оптической полости

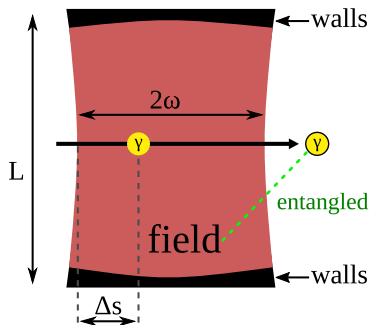


Figure: NPS: optical cavity, which the two-level atom flies through. The energy of the field in the cavity does not exceed $2\omega_c$. We choose the appropriate time $\tau_0 = \Delta s/v$ for finding the atom in the cavity for the realization of NFS: $|0\rangle \rightarrow |0\rangle$, $|1\rangle \rightarrow |1\rangle$, $|2\rangle \rightarrow -|2\rangle$

H.Azuma, Quantum computation with the Jaynes–Cummings model, Prog. Theor. Phys. 126 (2011), 369–385.

C-Sign $|x, y\rangle \rightarrow (-1)^{xy} |x, y\rangle$ на фотонных состояниях.

Добротность можно довести до 90%. Используется 2 полости для нелинейных фазовых сдвигов и 2 линейные светоделители, действующие так:

$$\begin{aligned} |n\rangle_{a_1} |m\rangle_{a_2} &= \frac{1}{\sqrt{n!m!}} (a_1^+)^n (a_2^+)^m |0\rangle_{a_1} |0\rangle_{a_2} \longrightarrow \\ &\longrightarrow \frac{1}{\sqrt{n!m!}} \left[\frac{1}{\sqrt{2}} (a_1^+ + a_2^+) \right]^n \left[\frac{1}{\sqrt{2}} (a_1^+ - a_2^+) \right]^m |0\rangle_{a_1} |0\rangle_{a_2} \end{aligned} \quad (1)$$

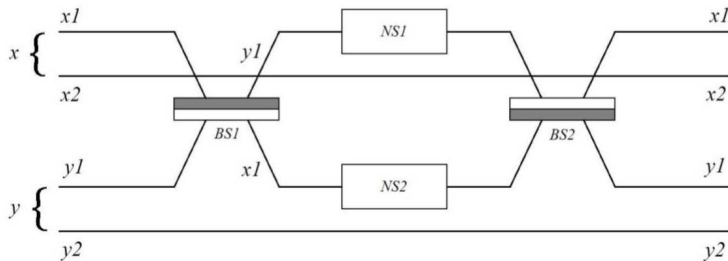


Figure: C-Sign gate array

Tavis-Cummings-Hubbard model

Hamiltonian of TCH model has the form:

$$H_{TCH} = \sum_i \hbar \omega_c a_i^\dagger a_i + \sum_{i,j} \hbar \omega_a^{ij} \sigma_{ij}^+ \sigma_{ij}^- + k \sum_i (a_{i+1}^\dagger a_i + a_i^\dagger a_{i+1}) + \sum_{i,j} \mu_{ij} (a_i + a_i^\dagger) (\sigma_{ij}^+ + \sigma_{ij}^-) \quad (2)$$

where i designates cavity, j - atom, $a_i^{(+)}$ are operators of creation-annihilation of photons in i -th cavity, $\sigma_{ij}^{(\pm)}$ are operators of creation-annihilation of excitation of j -th atom in i -th cavity, $\omega_c - \omega_a = d \ll \omega_a$. If $\mu_{ij} \ll \hbar \omega_a$ summands not conserving energy can be omitted (RWA approximation).

Influence of thermal phonons gives the deposit in the form of dephasing $b_{mk}^{(+)}$ are phonon operators, S_{ikj} - Juang-Rhys factors for interaction between j -th atom in i -th cavity with phonon mode k :

$$\begin{aligned} H &= H_{TCH} + H_B + H_I, \quad H_B = \sum_{m,k} E_{mk} b_{mk}^\dagger b_{mk}, \\ H_I &= \frac{1}{2} \sum_{i,k,j} \sqrt{S_{ikj}} \omega_k (b_{ik}^\dagger + b_{ik}) \sigma_{ij}^+ \sigma_{ij}^- + h.c. \end{aligned} \quad (3)$$

Jaynes-Tavis-Cummings-Hubbard-Dick model with dephasing noise

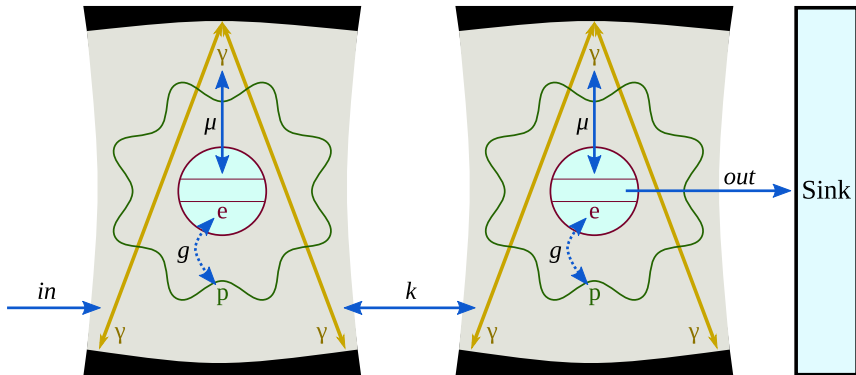


Figure: JC model with noise.

Декогерентность

Отклонение от унитарного закона в отсутствии наблюдателя называется *декогерентностью*. Если *декогерентность* вызвана контактом с окружением, она проявляется в виде подавления недиагональных элементов в матрице плотности $\rho(t)$, которая в случае определенного (чистого) квантового состояния имеет вид $\rho = |\Psi\rangle\langle\Psi|$, а в случае классической неопределенности (например, в результате частичного измерения состояния) - вид $\rho_{mix} = \sum_i p_i |\phi\rangle\langle\phi|$, где p_i - вероятность того, что система находится в состоянии $|\phi\rangle$.

Динамика матрицы плотности в случае отсутствия памяти у окружения подчиняется квантовой марковской динамике - удовлетворяет уравнению

Коссаковского-Линдблада-Глаубера-Сударшана:

$$i\hbar\dot{\rho} = [H, \rho] + i \sum_{j=1}^{N^2-1} g_j (L_j \rho L_j^\dagger - \frac{1}{2} \{L_j^\dagger L_j, \rho\})$$

где $g_j \geq 0$, L_j вместе с тождественным оператором образуют ортогональный базис в операторном пространстве Лиувилля. Для особо интересного случая немарковской динамики нет подобного общего подхода, есть только отдельные частные результаты.