Квантовый компьютер: современное состояние

Ю.И.Ожигов[1,2]

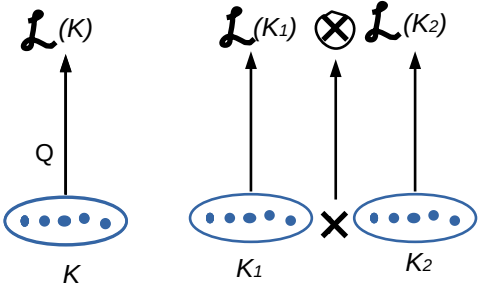
1 Московский Государственный Университет им. М.В.Ломоносова
Факультет ВМК, Кафедра суперкомпьютеров и квантовой информатики
2 Физико-Технологическсий институт РАН, лаборатория физики квантовых компьтеров

ozhigov@cs.msu.su

Содержание

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?



Дискретизация

Для перехода к квантовой механике необходимо дискретизировать пространство-время, выбрав зерно разрешения dx, dt. От этого зависят пробные заряды и массы частиц. Если устремить $dx \to 0, dt \to 0$, пробные заряды и массы будут меняться, но предстазания наблюдений будут только уточняться (теорема Боголюбова о перенормировках квантовой механики).

Это доказывает математическую корректность квантовой теории одной частицы, взаимодействующей с полем. Эксперимент (например, вычисленное значение электронного спина) показывает точность предсказаний квантовой теории до 10^7 - в случае одной частицы.

Для многих частиц ситуация неясна. Для 3 частиц найден эффективный алгоритм вычисления квантовой динамики (Л.Фаддеев и его группа, 2007). Для большего числа частиц есть только проект квантового компьютера.

Размерность тензорного произведения пространств есть произведение их размерностей.

Размерность пространства квантовых состояний растет как экспонента от числа реальных частиц.

Квантовый процесс невозможно имитировать в точности классическими средствами даже на одном шаге.

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 $ih|\dot{\Psi}\rangle = H|\Psi\rangle$

$$|\Psi(t)\rangle = U_t|\Psi(0)\rangle,\ U_t = e^{-\frac{i}{h}Ht}$$

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

В чем трудность моделирования на квантовом уровне

Операция $z, x, y \to z, x, y \oplus x$. В классическом случае она затронет только x и y.

В квантовом случае нам придется записывать ее результат для всевозможных z, которые непосредственно в этой операции не участвуют! Потому что квантовая операция $z, x, y \to z, x, y \oplus x$ действует не на одном наборе x, y, z, а на всех таких наборах, при любых z.

Что такое алгоритм и что такое вычисление

Алгоритм - это рецепт, что надо делать, точный рецепт, по шагам, но в сжатой форме, то есть с указанием возможных развилок и зацикливаний. Алгоритм, как правило, короткий, его можно написать на бумаге ручкой.

Вычисление - это практическая реализация рецепта. Она даже не всегда ведет к какому-то результату, и может длиться вечно. Вычисление, как правило, нельзя воспроизвести вручную, за исключением математических формул, которые обладают сакральным смыслом. В прочих случаях для вычисления нужен специальный прибор - компьютер.

Описать квантовый алгоритм очень просто: это просто классический алгоритм, указывающий, какие именно операции и над какими кубитами надо проделать.

Но осуществить вычисление по квантовому алгоритму (квантовое вычисление) - классическим путем - НЕВОЗМОЖНО из за непреодолимого сложностного барьера.

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

$$K(2,1) = \int\limits_{\gamma:\ 1\to 2} exp(\frac{i}{h} S[\gamma]) \mathcal{D}\gamma$$

где действие S вдоль траектории γ есть

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

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

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

$$K(2,1) = \int\limits_{\gamma:\ 1 \to 2} exp(\frac{i}{\hbar} S[\gamma]) \mathcal{D}\gamma$$

окрестности классической траектории складываются конструктивно, а окрестности прочих - деструктивно, если среднее действие на элементарном шаге превосходит постоянную Планка $h \approx 10^{-27} erg\ sec$. 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-Оппергеймера).

Р.Ф.Фейнман (1918-1988)

Квантовый компьютер как вызов квантовой теории

1. Квантовый алгоритм есть рецепт специально огранизованного 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.

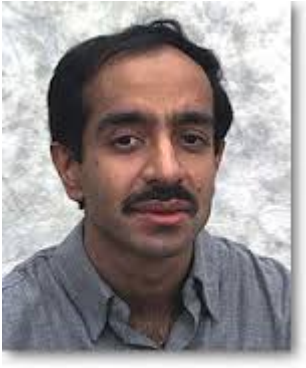
2. Всем математическим методам квантовой теории можно придать форму эффективных классических алгоритмов.

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 наблюдаемыой динамики от унитарного закона.

П.С.Шор

Л.К.Гровер



Квантовые гейты и подпрограммы

Гейты - элементарные унитарные операторы, затрагивающие явно 1-3 кубита. Из них комбинируются унитарные квантовые подпрограммы, реализующие полезные операции.
Примеры гейтов: NOT: $x \to x \oplus 1$. CNOT: $x, y \to x, y \oplus x$. CNOT- пример условного гейта. Любой гейт можно сделать условным, добавив управляющий кубит.
Примеры подпрограмм:
1). $I_{\bar{a}}: \ |\bar{b}\rangle \to (-1)^{\epsilon}|\bar{b}\rangle$, где $\epsilon = 0$, если $\langle a|b\rangle = 0$ и $\epsilon = 1$ в противном случае.
2). Оператор Гровера $G = -I_{\tilde{0}} I_{x_{tar}}$, где $|\tilde{0}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$, x_{tar}- решение уравнения $f(x) = 1$.
Реализация $I_{x_{tar}}$: добавляем анциллу в состоянии $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, и делаем преобразование $x, anc \to x, anc \oplus f(x)$. Затем анциллу выбрасываем.
Оператор Гровера есть поворот на угол $\alpha = 2\ arcsin(N^{-1/2})$ по направлению к $|x_{tar}\rangle$.

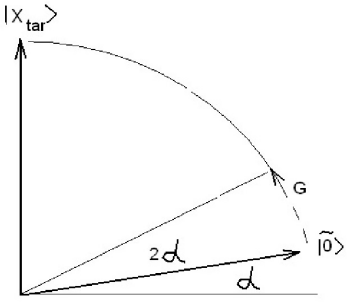
Алгоритм Гровера: квадратичное квантовое ускорение

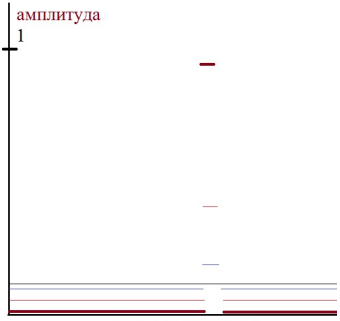
Задача на перебор: найти решение x_{tar} уравнения $f(x) = 1$, где f- булевская функция от n переменных, заданная в виде схем из функциональных элементов.

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 $|x, y\rangle \to |x, y \oplus f(x)\rangle$ - реализуется, исходя из классической схемы для функции f.

Алгоритм Гровера:
повторение оператора G
$\left[\frac{\pi\sqrt{N}}{4}\right]$ раз

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





Алгоритм Залки-Визнера

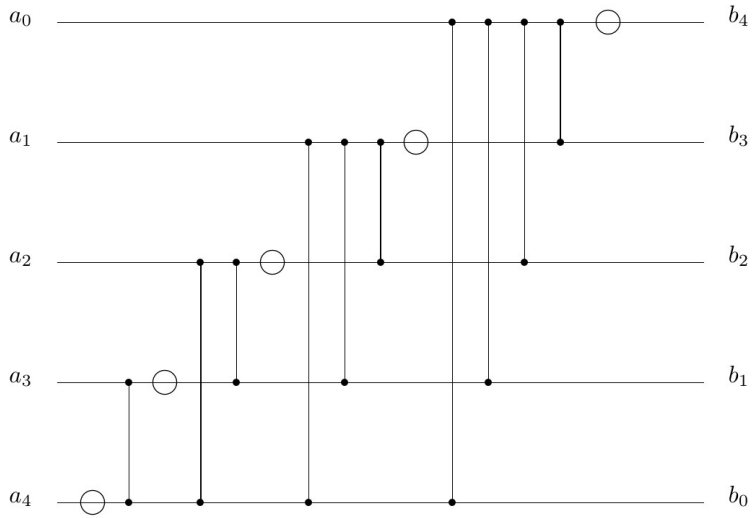
На квантовом компьютере можно моделировать решение уравнение Шредингера в случае простого потенциала за время $O(t^2)$, где t- время реального процесса, с памятью $O(n)$, где n- число частиц в реальной системе.

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

(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

Реализация обратного квантового преобразования Фурье $|a\rangle \to \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} exp(\frac{2\pi iab}{N})|b\rangle$



Окружности здесь обозначают преобразование Адамара
$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, матрица которого имеет вид:

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}, \tag{1}$$

двухкубитовые операции имеют вид:

$$U_{k,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{pmatrix}, \ k > j. \tag{2}$$

Набросок доказательства

В данной схеме вентилей амплитуда перехода от $a = \sum_j a_j 2^j$ к $b = \sum_j b_j 2^j$ имеет вид

$$\begin{aligned}
&\pi \sum_{l>k>j\geq 0} \frac{a_j b'_k}{2^{k-j}} + \pi \sum_{l>j\geq 0} a_j b'_j = \\
&2\pi \sum_{l>j+k\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} = \\
&2\pi \sum_{l>j,k\geq 0} \frac{a_j b_k 2^{j+k}}{2^l} = \\
&\frac{2\pi}{2^l} \sum_{l>j\geq 0} a_j 2^j \sum_{l>k\geq 0} b_k 2^j = \frac{2\pi}{2^l}.
\end{aligned} \tag{3}$$

что в точности соотвествует обратному преобразованию Фурье.

Главное назначение квантового компьютера - моделирование реальности на квантовом уровне

Квантовый компьютер способен находить решение уравнения Шредингера для n частиц за время $O(t^2)$ с использованием памяти $O(n)$, в дискретном приближении с зерном разрешения dx, dt, от которого зависят константы времени и памяти.

Создание QC означало бы новый этап в точном естествознании, так как появилась бы возможность моделировать сложные системы на квантовом уровне.

Существование QC не противоречит никаким законам физики.

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: $|x, y\rangle \to |x, x \oplus y\rangle$. 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 двух-кубитную операцию, например, CNOT.

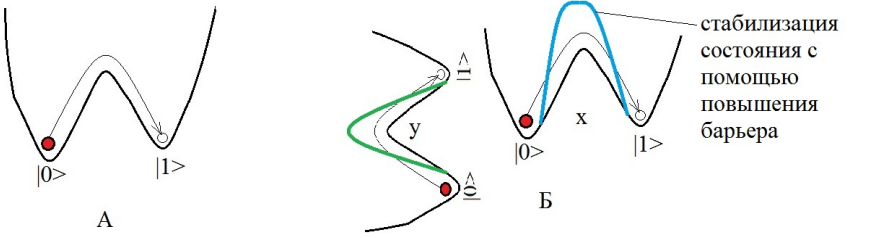


Figure: А. NOT на квантовой точке с двух-ямным потенциалом. Собственные состояния $|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ и $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Б. CNOT. Состояние точки x определяет высоту барьера в точке y (зеленый цвет), и скорость туннелирования в y.

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

Нелинейный фазовый сдвиг в оптической полости

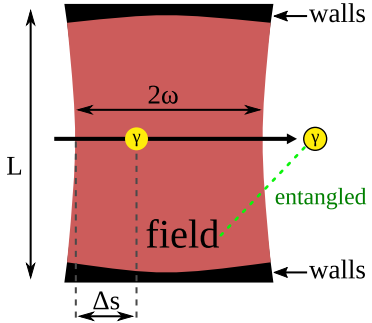


Figure: NPS: optical cavity, which the two-level atom flies through. The energy of the field in the cavity does not exceed $2\omega_c$. We choose the appropriate time $\tau_0 = \Delta s/v$ for finding the atom in the cavity for the realization of NFS: $|0\rangle \to |0\rangle$, $|1\rangle \to |1\rangle$,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

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

CSign $|x,y\rangle \to (-1)^{xy}|x,y\rangle$ на фотонных состояниях.

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

$$|n\rangle_{a_1}|m\rangle_{a_2} = \frac{1}{\sqrt{n!m!}}(a_1^+)^n(a_2^+)^m|0\rangle_{a_1}|0\rangle_{a_2} \longrightarrow$$
$$\longrightarrow \frac{1}{\sqrt{n!m!}}[\frac{1}{\sqrt{2}}(a_1^+ + a_2^+)]^n[\frac{1}{\sqrt{2}}(a_1^+ - a_2^+)]^m|0\rangle_{a_1}|0\rangle_{a_2} \quad (4)$$

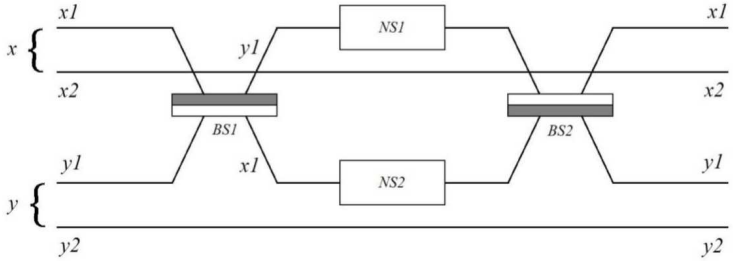


Figure: C-Sign gate array

Tavis-Cummings-Hubbard model

Hamiltonian of TCH model has the form:

$$H_{TCH} = \sum_i h\omega_c a_i^+ a_i + \sum_{i,j} h\omega_a^{ij} \sigma_{ij}^+ \sigma_{ij}^- + k \sum_i (a_{i+1}^+ a_i + a^+ a_{i+1}) + \sum_{i,j} \mu_{ij}(a_i + a_i^+)(\sigma_{ij}^+ + \sigma_{ij}^-) \quad (5)$$

where i designes 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 $\mu_{ij} \ll h\omega_a$ 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:

$$\begin{aligned} H &= H_{TCH} + H_B + H_I, \ H_B = \sum_{m,k} E_{mk} b_{mk}^+ b_{mk}, \\ H_I &= \tfrac{1}{2} \sum_{i,k,j} \sqrt{S_{ikj}} \omega_k (b_{ik}^+ + b_{ik}) \sigma_{ij}^+ \sigma_{ij}^- + h.c. \end{aligned} \quad (6)$$

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

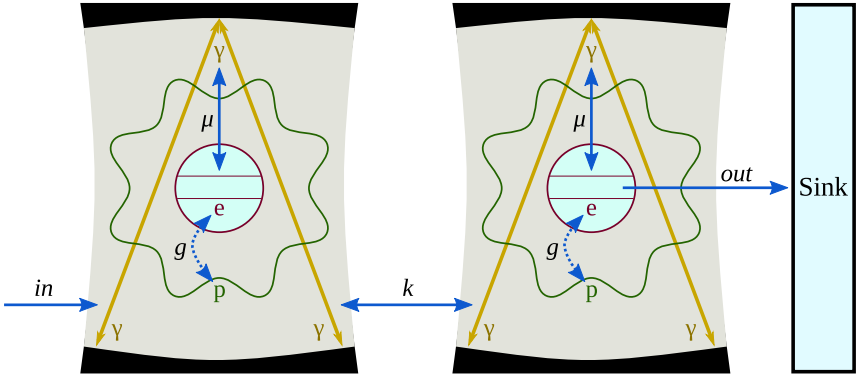


Figure: JC model with noise.

Декогерентность - главное препятствие на пути к QC

Отклонение от унитарного закона в отсутствии наблюдателя называется *декогерентностью*.

Математически декогетентность означает подавление недиагональных элементов матрицы плотности системы, переводящей ее из чистого (когерентного) состояния в классическую смесь различных состояний.
Принято считать, что декогерентность вызвана контактом рассматриваемой системы с ее окружением, которого полностью избежать невозможно.

Частичное описание декогерентности

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:

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

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.

Выводы

Квантовый компьютер - долговременный проект, в котором теоретические разработки и эксперименты одинаково важны.

Квантовая теория в области многих тел еще не разработана в должной мере.

Компьютерное и суперкомпьютерное моделирование - ключевой момент в развитии теории QC.