Основы квантовых вычислений

Использовались: статьи, лекции, рисунки и материалы, доступные через интернет, а также книга

M.Nielsen and I.Chuang
Quantum Computation and
Quantum Information
Cambridge University Press, 2000

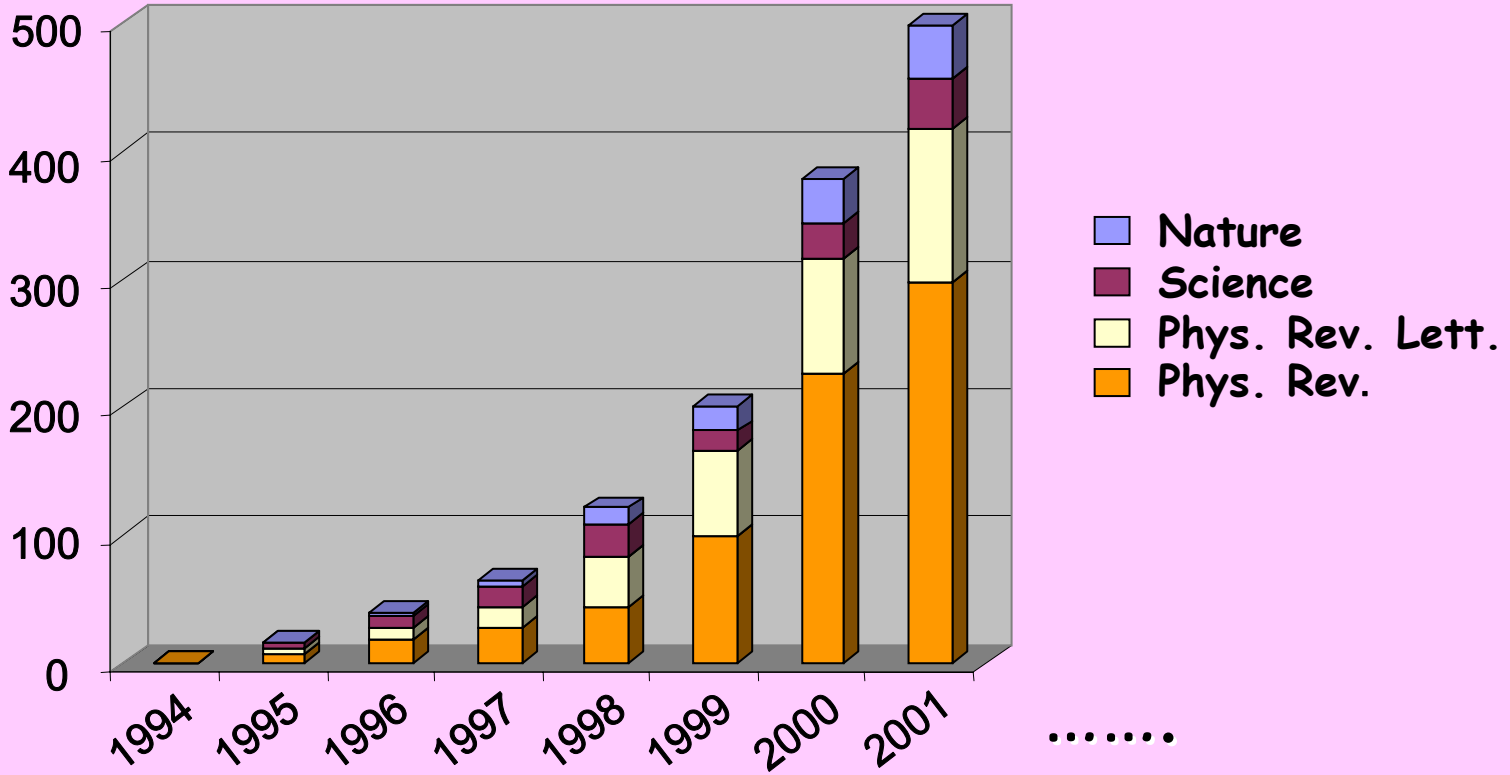
Deutsch (1985)

Shor (1994) Быстрая факторизация целых

Grover (1996) Быстрый поиск в базе данных

Число публикаций по "Кв. информации" или "Кв. компьютингу"

(P.Halian)



.....

Зачем нужны квантовые вычисления?

1. Современные компьютеры все еще неспособны решать ряд важных задач:

   - Криптография
   - Моделирование квантово-механических систем

2. Хотя классические компьютеры становятся все мощнее и мощнее, имеются физические ограничения на рост их производительности.

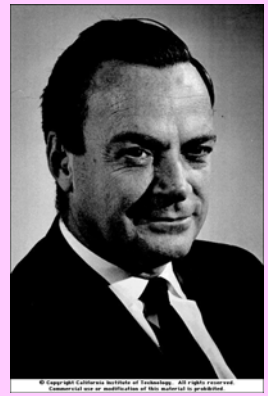
Моделирование физических систем

Может ли универсальный классический компьютер *точно* промоделировать квантовомеханические системы?

Может ли классический компьютер *эффективно* моделировать квантовомеханические процессы?

"I'm not happy with all the analyses that go with just classical theory, because Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem!"

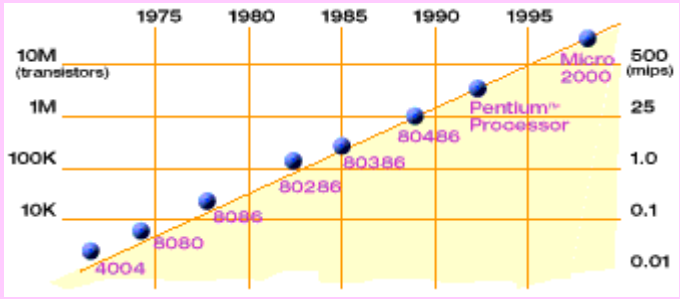
Richard Feynman 1981

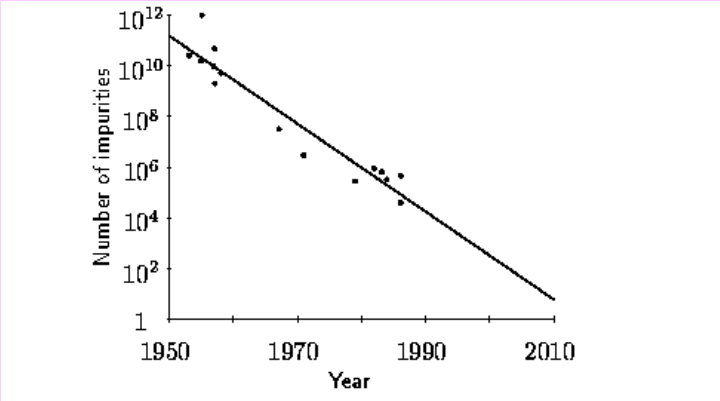


Ограничения классических компьютерных технологий (H.Wiedman)

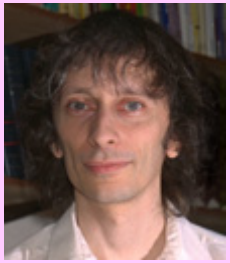
- Закон Мура:
  - Gordon E. Moore
  - Сформулирован в 1965.
  - Предсказывает, что число транзисторов в чипе будет удваиваться каждые
  - 18-24 месяца.

- Проблема:
  - Транзистор станет 10^{-8} см
  - Большинство фирм ожидают что это произойдет в ближайшие 20 лет





Что значит «вычисление»?



Тезис Черча-Тюринга: алгоритмический процесс или вычисление это то, что можно сделать на машине Тюринга

Дойч (1985):

Вытекает ли этот тезис из законов физики?

Квантовомеханические системы очень трудно моделировать на классических компьютерах

Может быть компьютеры, основанные на квантовой механике невозможно эффективно моделировать на машине Тюринга? → Нарушение тезиса!

Возможно ли, что такие компьютеры могут решать некоторые задачи быстрее, чем выроятностная машина Тюринга?

Кандидат на универсальный компьютер: квантовый компьютер

Тезис Черча-Тюринга-Дойча

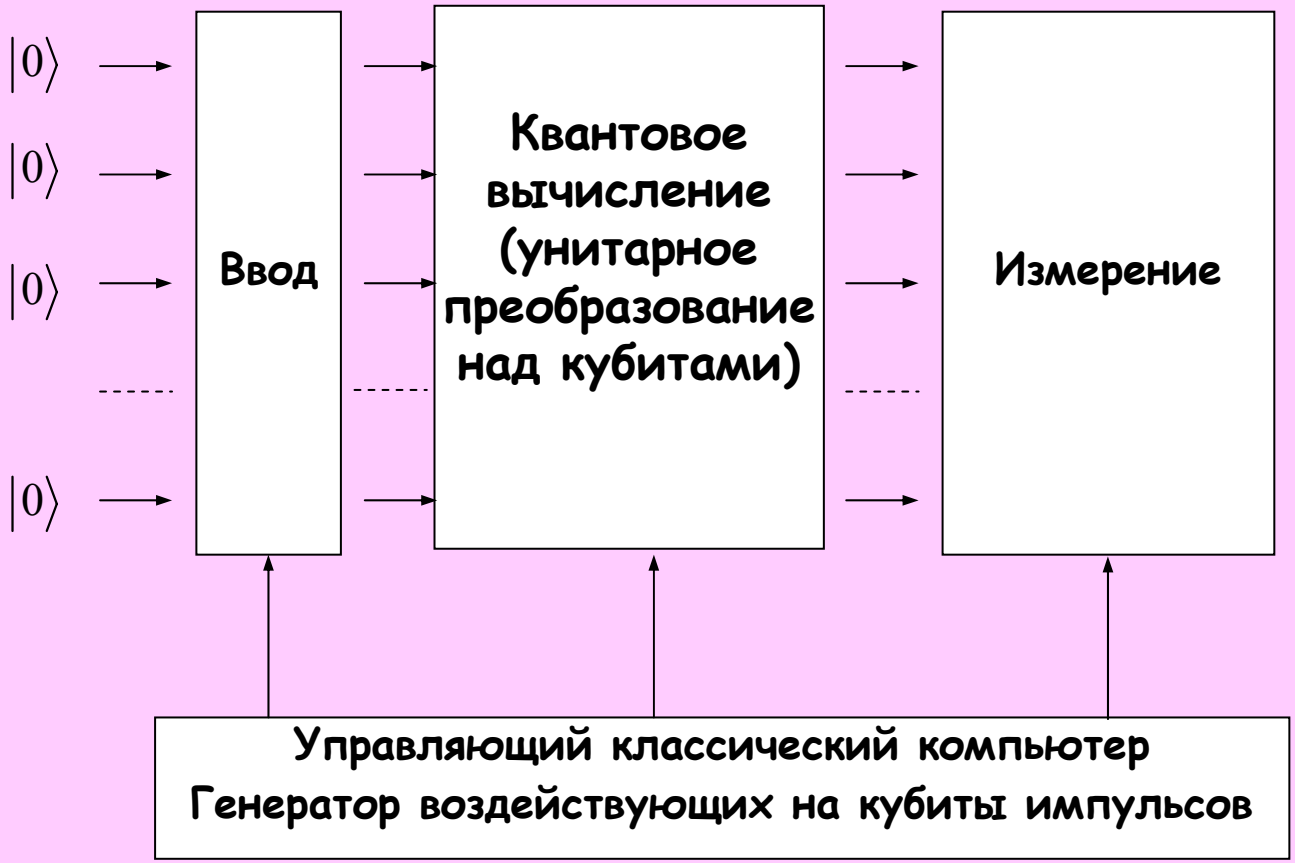
Любой физический процесс может быть эффективно
Промоделирован на квантовом компьютере.

Что такое квантовый компьютер?

Квантовый компьютер – это вычислительный прибор, который основан на использовании для вычислений таких квантовомеханических явления как суперпозицию и перепутывание состояний для преобразования входных данных в выходные. В классическом компьютинге количество данных измеряется битами, а в квантовом компьютинге – кубитами. Основополагающий принцип квантовых вычислений состоит в использовании квантовомеханических объектов для представления данных и их обработки.

Схема квантового компьютера

К.А.Валиев, А.А.Кокин



Основы квантовой механики

4 постулата

1. Описание состояний замкнутой системы.

   "вектора состояний " и "пространство состояний"

2. Описание динамики квантовой системы.

   "унитарные преобразования"

3. Описание измерений.

   "проективные измерения"

4. Описание состояний составных систем.

   "тензорные произведения"

Схемная модель вычислений

Классическая

Единица: бит

1. Подготовка *n*-битного ввода
2. 1- и 2-битные вентили
3. Считывание значений битов на выводе

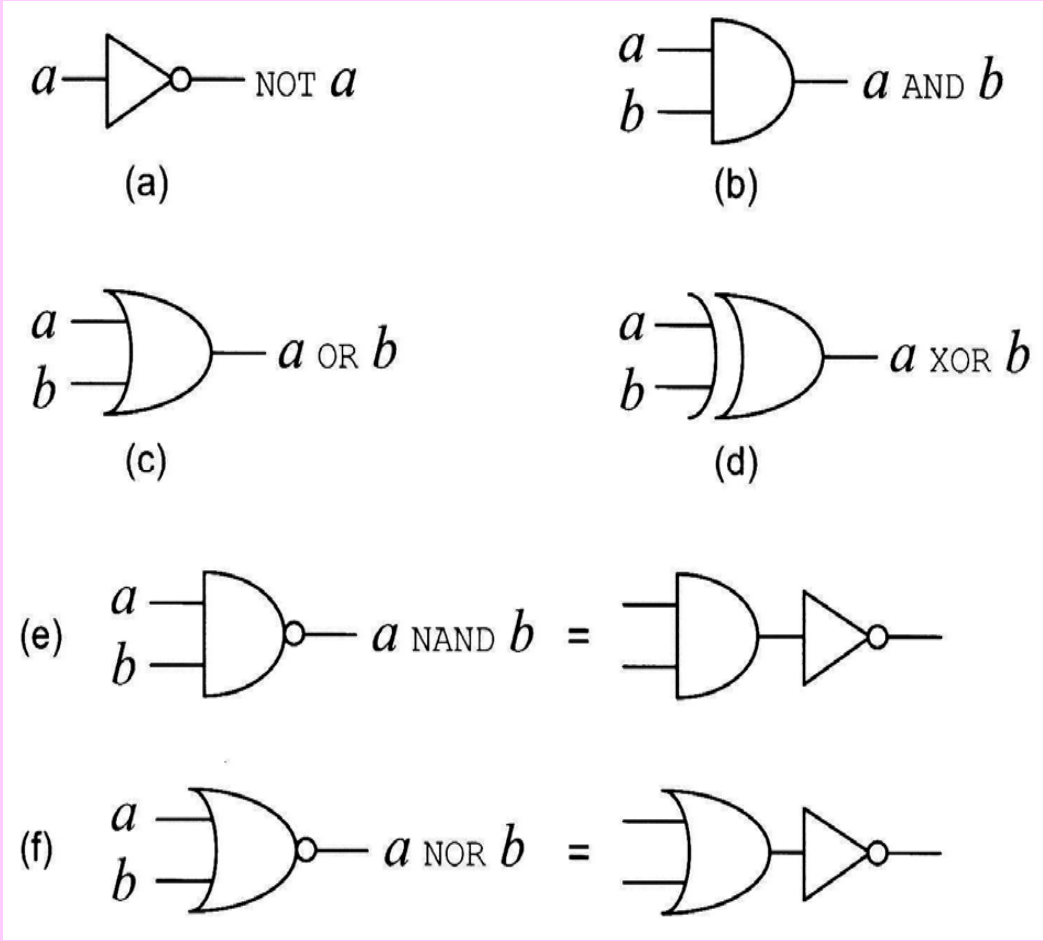
Квантовая

Единица: кубит $|x_1, x_2, \ldots, x_n\rangle$

1. Подготовка *n*-кубитного ввода в заданном базисе.
2. Унитарные 1- и 2-кубитные вентили
3. Считывание частичной информации о состоянии кубитов путем измерения

Внешнее управление классическим компьютером

Классические логические вентили



A	B	AND	OR	XOR	NOT B
0	0	0	0	0	1
0	1	0	1	1	0
1	0	0	1	1	1
1	1	1	1	0	0

Динамика: квантовые логические вентили (гейты)

Квантовый "not" вентиль:

$$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle.$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow ?$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$

Матричное представление: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Динамика замкнутой квантовой системы может быть представлена унитарной матрицей.

Однокубитные квантовые вентили

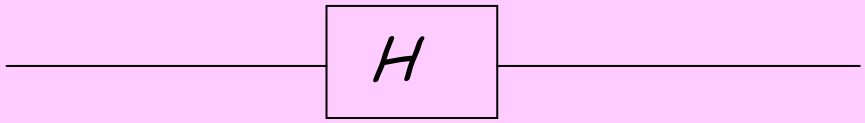
Паули

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$\pi/8$

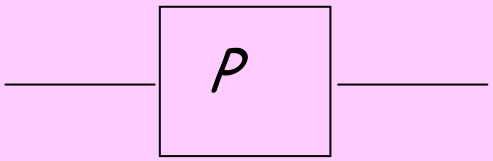
$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Адамара

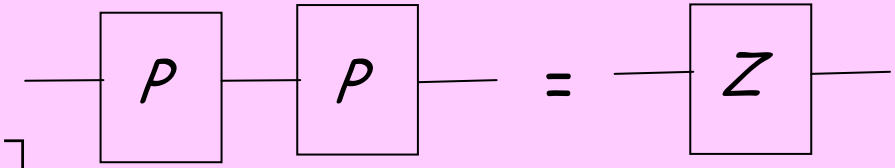


$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Phase



$$P|0\rangle = |0\rangle; \quad P|1\rangle = i|1\rangle \quad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

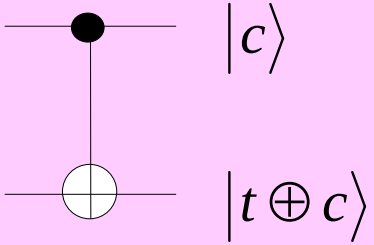


$$P^2 = Z$$

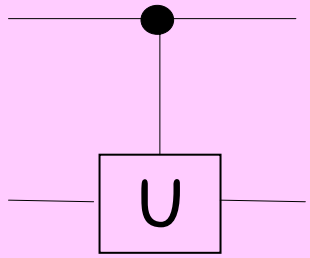
Контролируемый "not" вентиль

Контроли-
рующий $|c\rangle$

Контроли-
руемый $|t\rangle$

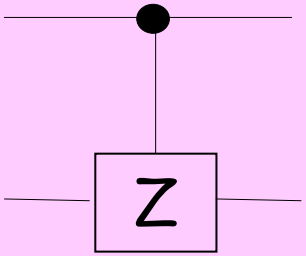


$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

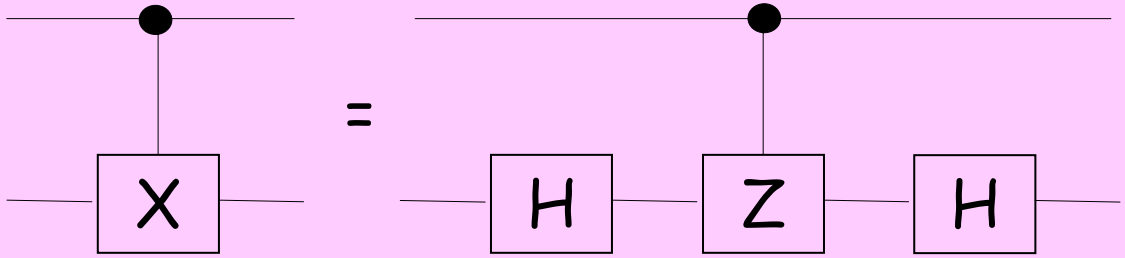


CNOT
когда U=X

Контролируемый "Z" вентиль



$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

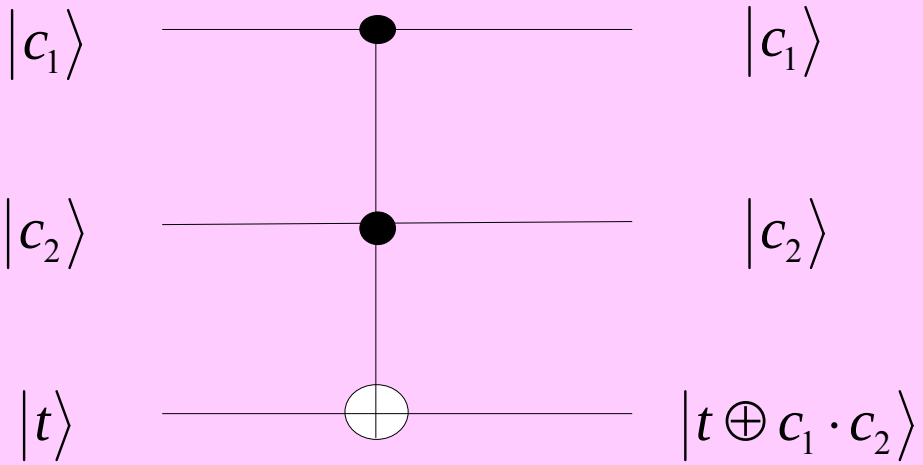


Тоффоли вентиль

Контролирующий кубит 1

Контролирующий кубит 2

Контролируемый кубит



Постулаты квантовой механики

Постулат 1: Состояние замкнутой квантовой системы задается единичным вектором в комплексном гильбертовом пространстве, образующим пространство состояний.

Постулат 2: Эволюция замкнутой квантовой системы описывается унитарным преобразованием.

$$|\psi(t)\rangle = U|\psi(0)\rangle = \exp(-iHt)|\psi(0)\rangle$$

Постулат 3: Измерение $|\psi\rangle$ в ортонормальном базисе $|e_1\rangle,\ldots,|e_d\rangle$ дает результат j с вероятностью

$$P(j) = \left|\langle e_j|\psi\rangle\right|^2.$$

Измерение переводит систему в состояние $|e_j\rangle$, соотвествующее результату j

Постулат 4: Пространство состояний составной системы является тензорным произведением пространств состояний ее компонент

Постулат 1

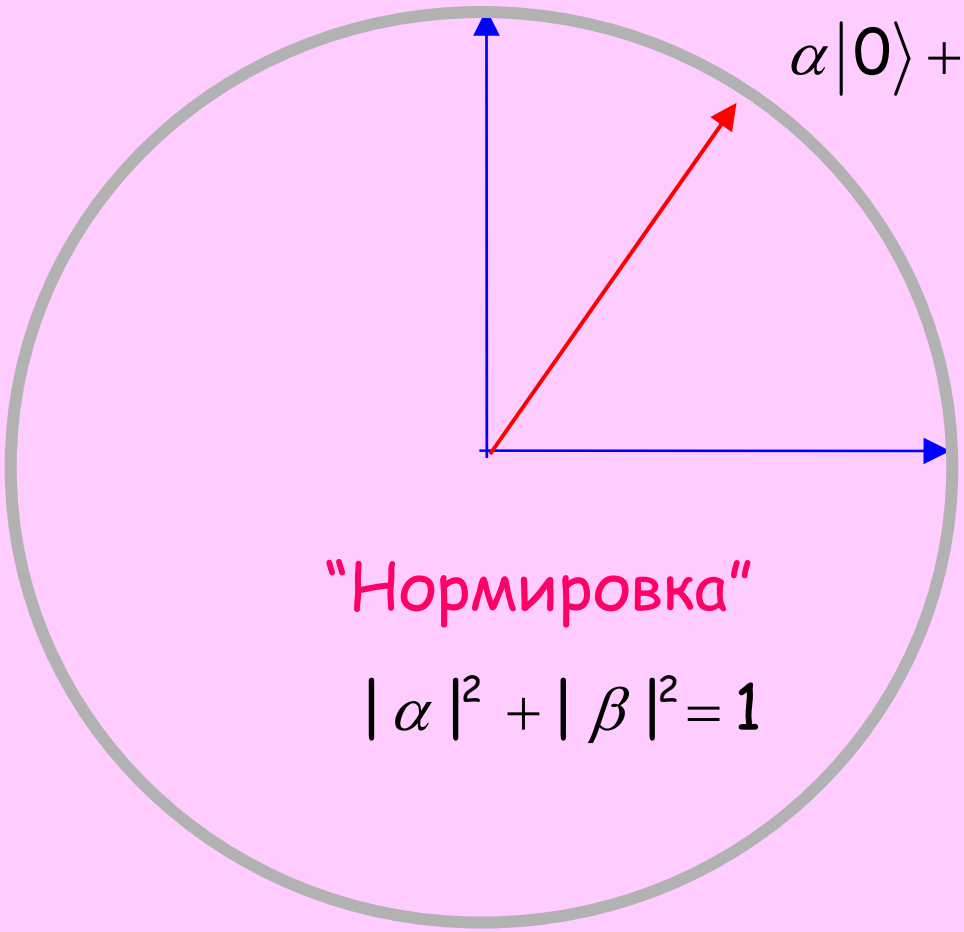
С каждой квантовой системой ассоциируется комплексное векторное пространство – пространство состояний.

Состояние замкнутой квантовой системы описывается единичным вектором в пространстве состояний.

Пример: мы будем иметь дело, главным образом, с кубитами, которым соответствует пространство состояний C^2.

$$\alpha|0\rangle + \beta|1\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Пример: кубит
(двухуровневая квантовая система)



Фотон,
Частица
спина $\frac{1}{2}$,
и т.д.

"Нормировка"

$$|\alpha|^2 + |\beta|^2 = 1$$

$|0\rangle$ и $|1\rangle$

"вычислительный" базис

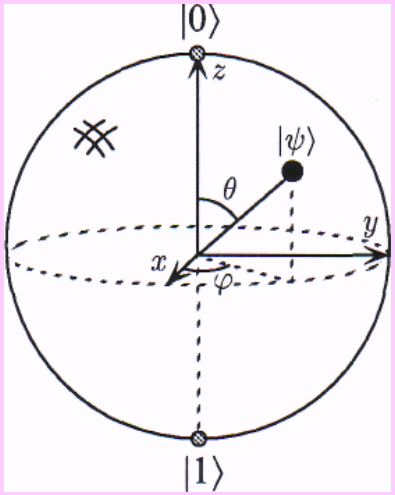
"All we do is draw little arrows on a piece of paper - that's all."
- Richard Feynman

Сфера Блоха

В силу нормировки $|\alpha|^2+|\beta|^2=1$

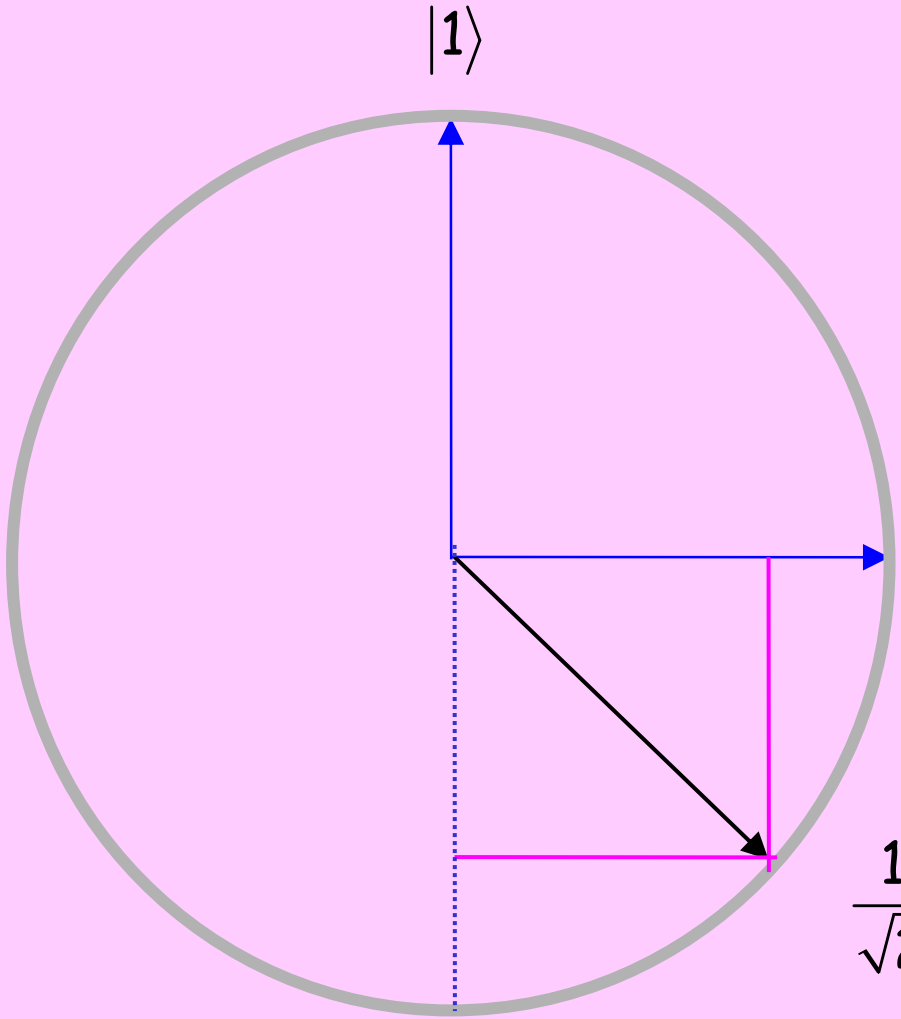
Имеет место параметризация

$$|\psi\rangle = e^{i\gamma}\left(Cos\frac{\theta}{2}|0\rangle + e^{i\varphi}Sin\frac{\theta}{2}|1\rangle\right) \Rightarrow |\psi\rangle = \left(Cos\frac{\theta}{2}|0\rangle + e^{i\varphi}Sin\frac{\theta}{2}|1\rangle\right)$$



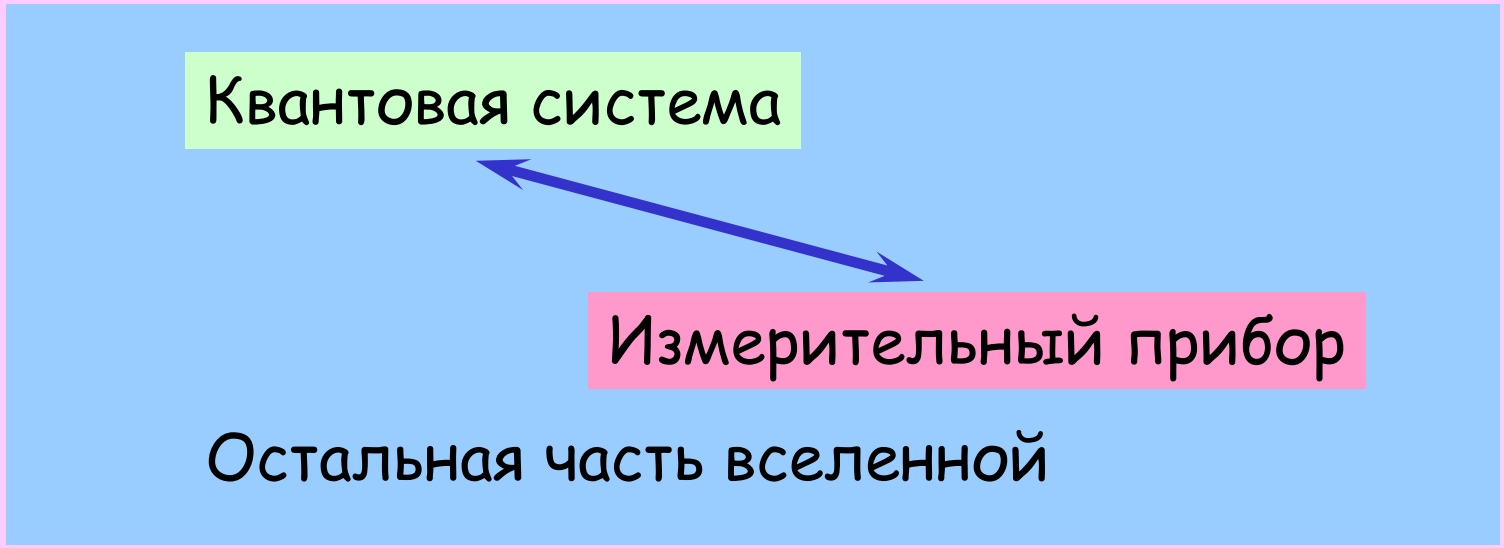
Глобальная фаза ненаблюдаема

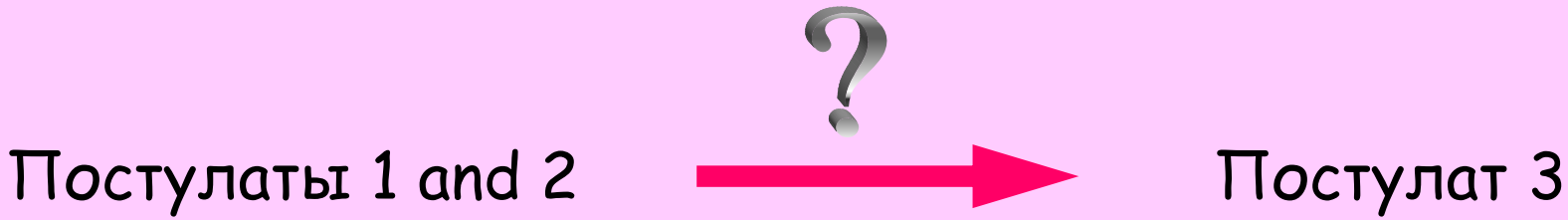
Измерение кубита



$$P(0) = P(1) = \frac{1}{2}$$

Проблема измерения





Исследовательская задача: решить проблему измерения.

Многокубитные системы

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Измерение в вычислительном базисе: $P(x,y) = |\alpha_{xy}|^2$

Общее состояние из n кубит: $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$

Для классического представления этого состояния требуется $O(2^n)$ бит.

"Hilbert space is a big place" - Carlton Caves

"Возможно [...] нам недостает математической теории квантовых автоматов. [...] квантовое пространство состояний обладает гораздо большей емкостью, чем классическое: [...] там, где в классике имеется N дискретных состояний, в квантовой теории, допускающей их суперпозицию, имеется C^N [...] ячеек. [...] Эти [...] подсчеты показывают большую потенциальную сложность квантового поведения по сравнению с его классической имитацией." – Ю.И. Манин (1980)

Постулат 4

Пространство состояний составной физической системы является тензорным произведением пространств состояний ее составляющих.

Пример: Двухкубитное пространство состояний $C^2 \otimes C^2 = C^4$

Вычислительные базисные состояния:

$|0\rangle \otimes |0\rangle;\ |0\rangle \otimes |1\rangle;\ |1\rangle \otimes |0\rangle;\ |1\rangle \otimes |1\rangle$

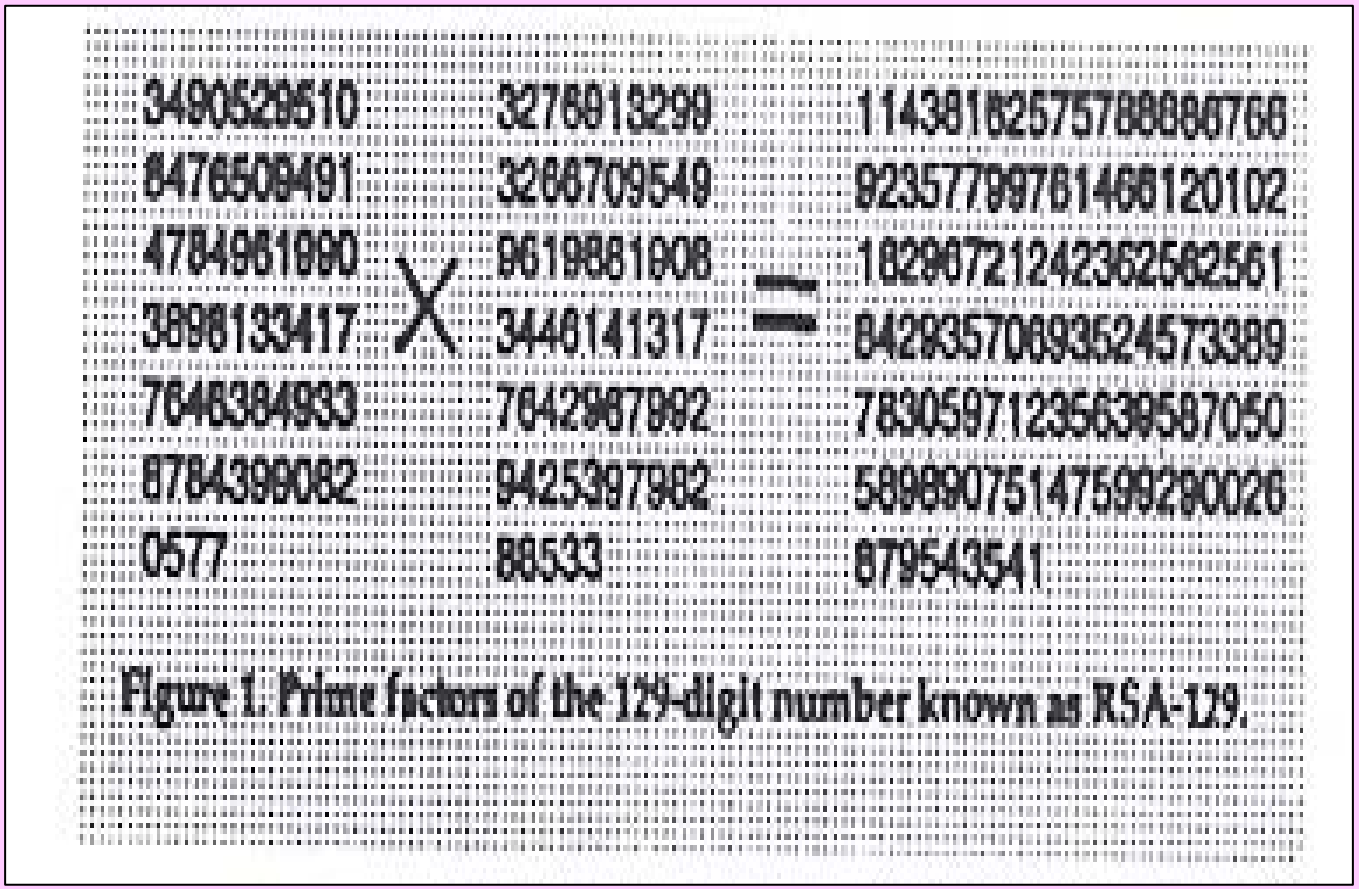
Альтернативные обозначения: $|0\rangle|0\rangle;\ |0,0\rangle;\ |00\rangle.$

Преимущество квантовых компьютеров: криптография

- Современные криптосистемы (RSA) основаны на разложении целого числа на множители.
  - Пример: 15=5*3.
  - Разложение очень легко сделать для маленьких чисел.
- В наиболее криптостойких системах используются целые с ~ 400 цифрами.
  - На современных компьютерах потребуется ~10^9 лет для разложения такого числа на множители.
  - Квантовый компьютер, равный по скорости счета современным компьютерам, справится с этой задачей за секунды (алгоритм Шора)

Пример длинного числа: RSA-129

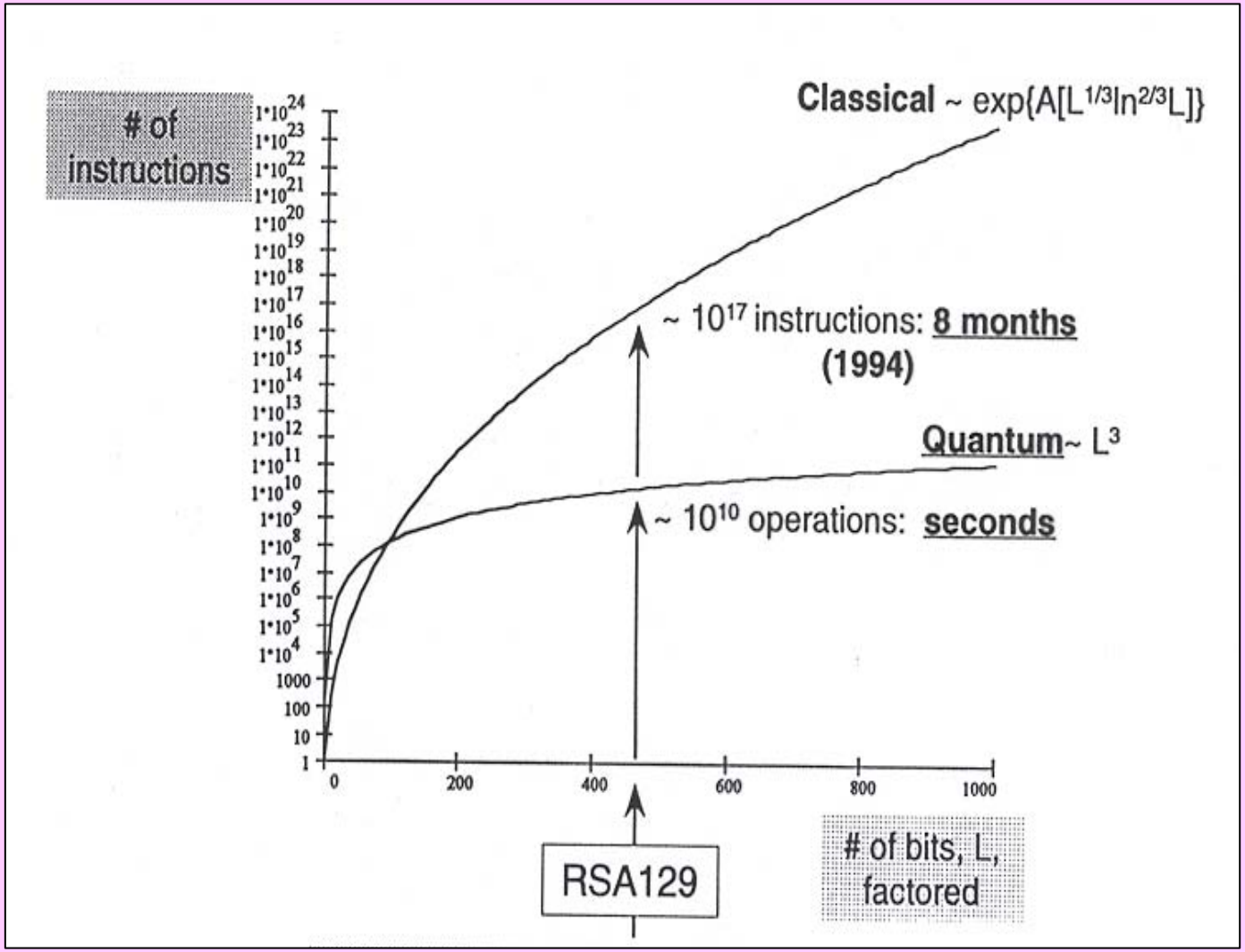
T.Hey and D. Ross



3490529510		3276913299		1143816257578888676
8476508491		3266709549		9235779976146612010 2
4784961980	×	8619881908	=	1829072124236256256 1
3896133417		3446141317		8429357069352457338 9
7646384933		7642987992		7830597123563958705 0
8784396082		9425397982		5989907514759929002 6
0577		88533		879543541

Figure 1. Prime factors of the 129-digit number known as RSA-129.

Сравнение классического и квантового компьютеров для RSA-129



Задача Дойча

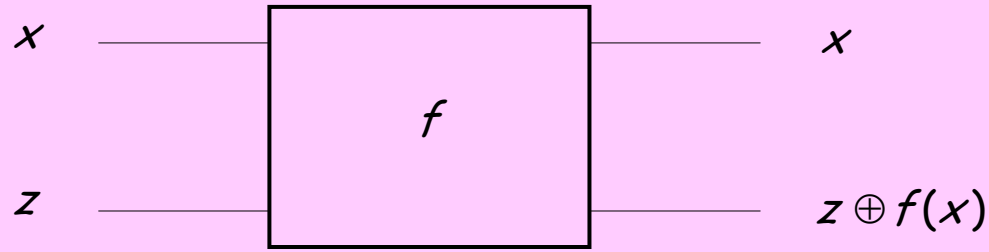
Пусть задан черный ящик вычисляющий функцию

$f : \{0,1\} \to \{0,1\}$

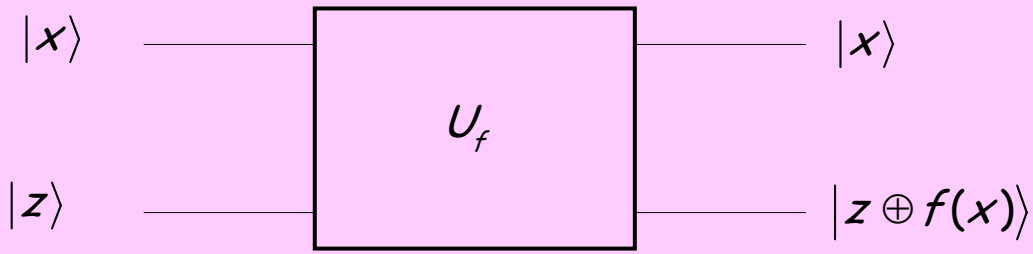
Задача: определить f - константа или нет?

Классически нужно вычислять оба значения $f(0)$ и $f(1)$.
В квантовом случае достаточно вычислить черный ящик для $f(\bullet)$ один раз!

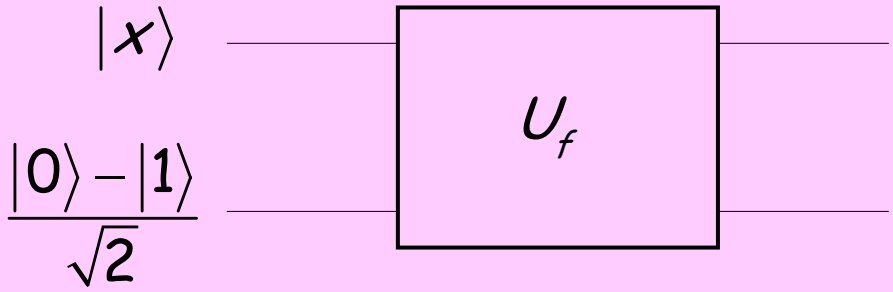
Классический черный ящик



Квантовый черный ящик



Перенос информации в фазу



$f(x) = 0$:

$$|x\rangle(|0\rangle - |1\rangle) \to |x\rangle(|0\rangle - |1\rangle)$$

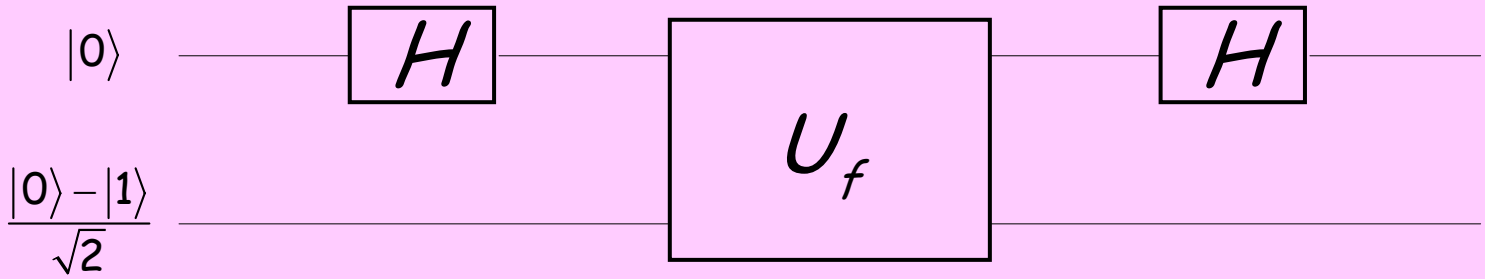
$f(x) = 1$:

$$|x\rangle(|0\rangle - |1\rangle) \to |x\rangle(|1\rangle - |0\rangle) = -|x\rangle(|0\rangle - |1\rangle)$$

$$|x\rangle(|0\rangle - |1\rangle) \to (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

$$\boxed{|x\rangle \to (-1)^{f(x)}|x\rangle}$$

Квантовый алгоритм для задачи Дойча



Квантовый параллелизм

$$|0\rangle \to |0\rangle + |1\rangle$$

$$\to (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$

$$\to (-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)$$

$$= \left[(-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle + \left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1\rangle$$

f - константа $\Rightarrow$ результат - $|0\rangle$.

f - переменная $\Rightarrow$ результат - $|1\rangle$.

Универсальность квантовой схемной модели

Классически, любая функция $f(x)$ может быть вычислена через nand и fanout – универсальный набор гейтов для классических вычислений.

Пусть U – произвольное унитарное преобразование n кубитов.

Тогда U может быть составлено из «controlled-not» вентиля и однокубитных вентилей H, P и T.

Так же как в классическом случае, можно показать, что существуют U, которые требуют бесконечно много базисных вентилей.

Работа квантовой схемной модели

Вход: n-битная строка x, задающая задачу.

Пример: x - число, которое надо разложить на множители.

Инициализация: $|0\rangle^{\otimes m}$, где m - вычислимая функция n.

Схема: состоит из однокубитных и C-not вентилей и применяется к кубитам. Применение вентилей управляется внешним классическим компьютером.

Выход: Измерение заданного подмножества кубитов в конце вычислений в выбранном вычислительном базисе. Результат измерения содержит решение задачи.

Пример: Для логической задачи измеряется только первый кубит и с результатом "да" или "нет".

Преимущество квантовых компьютеров: быстрый поиск

- Квантовый компьютер сможет найти запись в случайной базе данных гораздо быстрее чем классический компьютер.
  - В случайной (неотсортированной) базе данных с N записями обычный компьютер будет в среднем делать ~ N/2 поисковых попыток прежде чем он обнаружит искомую запись
  - Для поиска на квантовом компьютере в той же базе данных размера N потребуется всего ~ $N^{1/2}$ попыток (алгоритм Гровера)

Современное состояние квантовых вычислений

- Уже проведен ряд экпериментов по физической реализации реализации квантовомеханических вычислительных операций на малом числе кубитов. Теоретические и экпериментальные исследования проводятся очень высокими темпами. За рубежом многие правительственные и военные организации поддерживают исследования в области квантовых вычислений и квантовой информации в надежде создания реалистических квантовых компьютеров для гражданских целей и целей защиты информации (криптоанализа).

- Квантовые космьютеры могут быть полезны не только для прямого моделирования квантовомеханических систем и целочисленной факторизации. Они могут найти эффективное применение в других задачах физики, математики, материаловедении, нанотехнологии, биологии и медицине. Применение классического компьютинга в указанных областях ограничено из-за его низкой эффективности для кванновомеханического моделирования.

Когда квантовые вычисления эффективны

Рассмотрим задачу со следующими свойствами:

- Единственный практический путь решения состоит в угадывании результата и затем проверки догадки,
- Имеется N возможных ответов.
- Проверка каждого возможного ответа требует одинаковых вычислительных затрат.
- Нет предпочтения одного возможного ответа перед другим: случайный выбор возможных ответов так же хорош как и любая другая стратегия выбора.

Пример такой задачи - подбор ключа для зашифрованного файла. Для указанного класса задач в среднем потребуется $(N + 1)/2$ попыток, чтобы найти ответ на классическом компьютере. Время счета на квантовом компьютере пропорционально квадратному корню из N. Это может быть очень большое ускорение.

Требования к физической реализации квантовых компьютеров

Валиев К.А, Кокин А.А.

1. Выделение и фиксирование в пространстве достаточно большого числа ($L \sim 10^2 \div 10^3$) 2-х уровневых частиц-кубитов, на которые можно было бы избирательно воздействовать для организации их квантовой эволюции в соответствии с выполняемым алгоритмом.

2. Возможность приготовления L кубитов входного регистра в исходном базисном состоянии $|0_1, 0_2, 0_3, \ldots., 0_L\rangle$ (*инициализация*).

3. *Помехоустойчивость* вычислительных процессов и *подавление эффектов декогерентности* квантовых состояний, обусловленных взаимодействием кубитов с окружающей средой. Время декогерентости должно в $\geq 10^4$ раз превосходить время выполнения основных квантовых операций (время такта). Ошибка при выполнении отдельной операции должна быть $\leq 10^{-4}$.

Требования к физической реализации квантовых компьютеров

4. Так как любая унитарная квантовая операция может сводится к совокупности однокубитных и двухкубитных операций, то при выборе физической системы необходимо *наличие* определенных *нелинейных взаимодействий* между управляемыми кубитами, обеспечивающих выполнение двухкубитных операций. Управляемые операциями импульсы должны контролироваться с точностью не хуже, чем 10^{-4} .

5. *Выполнение измерения* состояния квантовой системы на выходе *с высокой точностью* .

Требования к реальному квантовому компьютеру

(D. DiVincenzo)

- Масштабируемость (возможность увеличения) числа кубитов
- Кубиты могут быть инициализированы в любое начальное состояние.
- Квантовые вентили должны срабатывать бестрее времени декогеренции.
- Реализация полного набора вентилей Тюринга
- Считывание информации с кубитов

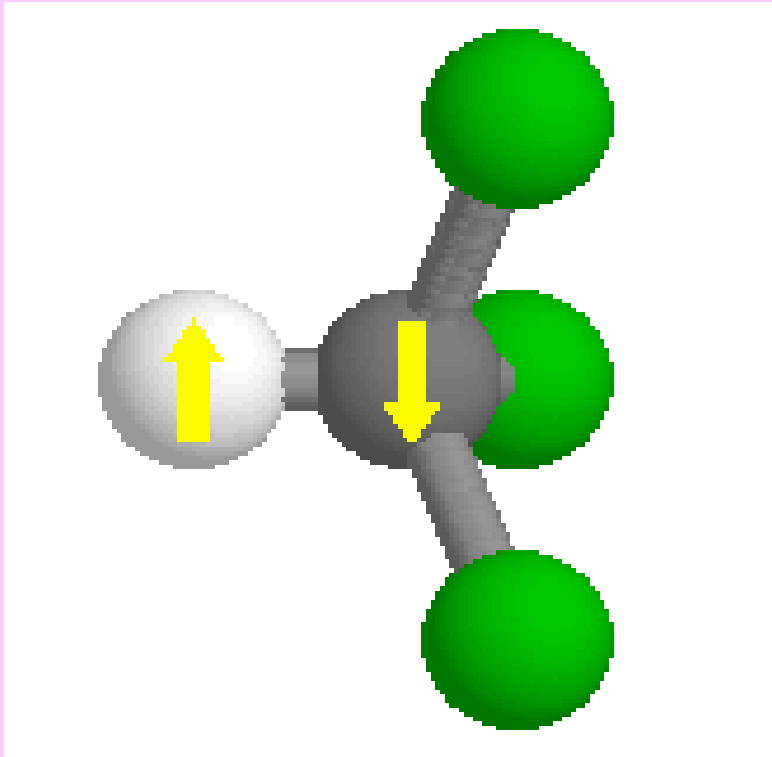
В настоящее время имеется много проблем на пути построения квантовых компьютеров и пока что модельные малокубитные компьютеры могут решать только тривиальные проблемы. Главная прблема - декогеренция.

Кандидаты
(H.Wiedman)

- Ядерный магнитный резонанс (NMR)
- Ионные ловушки
- Квантовые точки
- ……

Ядерные магнитно-резонансные компьютеры

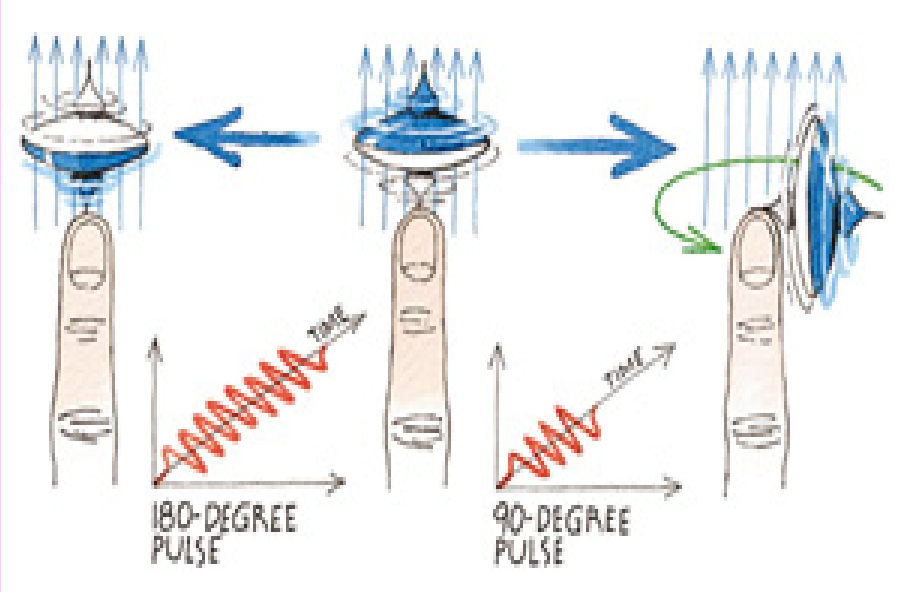
- Предложен в 1997 и создается, например, в ИБМ.
- Протоны и нейтроны обладают спином.
  - Суммарный спин основных атомов хим. элементов равен нулю (спины сокращаются).
  - В изотопах имеются дополнительные нейтроны.
  - Эти дополнительные нейтроны приводят к положительному или отрицательному спину атома.



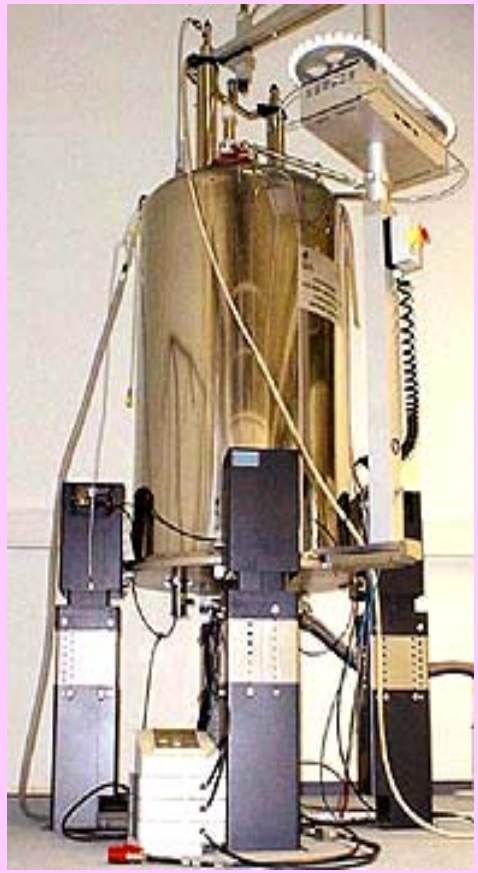
ЯМР-компьютеры: реализация операций

- Выравнивание спинов
  - Молекулы (например, хлороформ $^{13}CHCl_3$) помещаются в растворитель (например, дейтерированный ацетон $(CD_3)_2CO$).
  - Затем раствор помещается в магнитное поле спектрометра.
  - Магнитное поле выравнивает все спины.
- Воздействие радиочастотным импульсом
  - Один из атомарных спинов либо опрокидывается, либо нет, в зависимости от состояния спинов других атомов.
- Воздействие последовательностью импульсов
  - Реализация квантового алгоритма.

ЯМР-компьютеры: пример



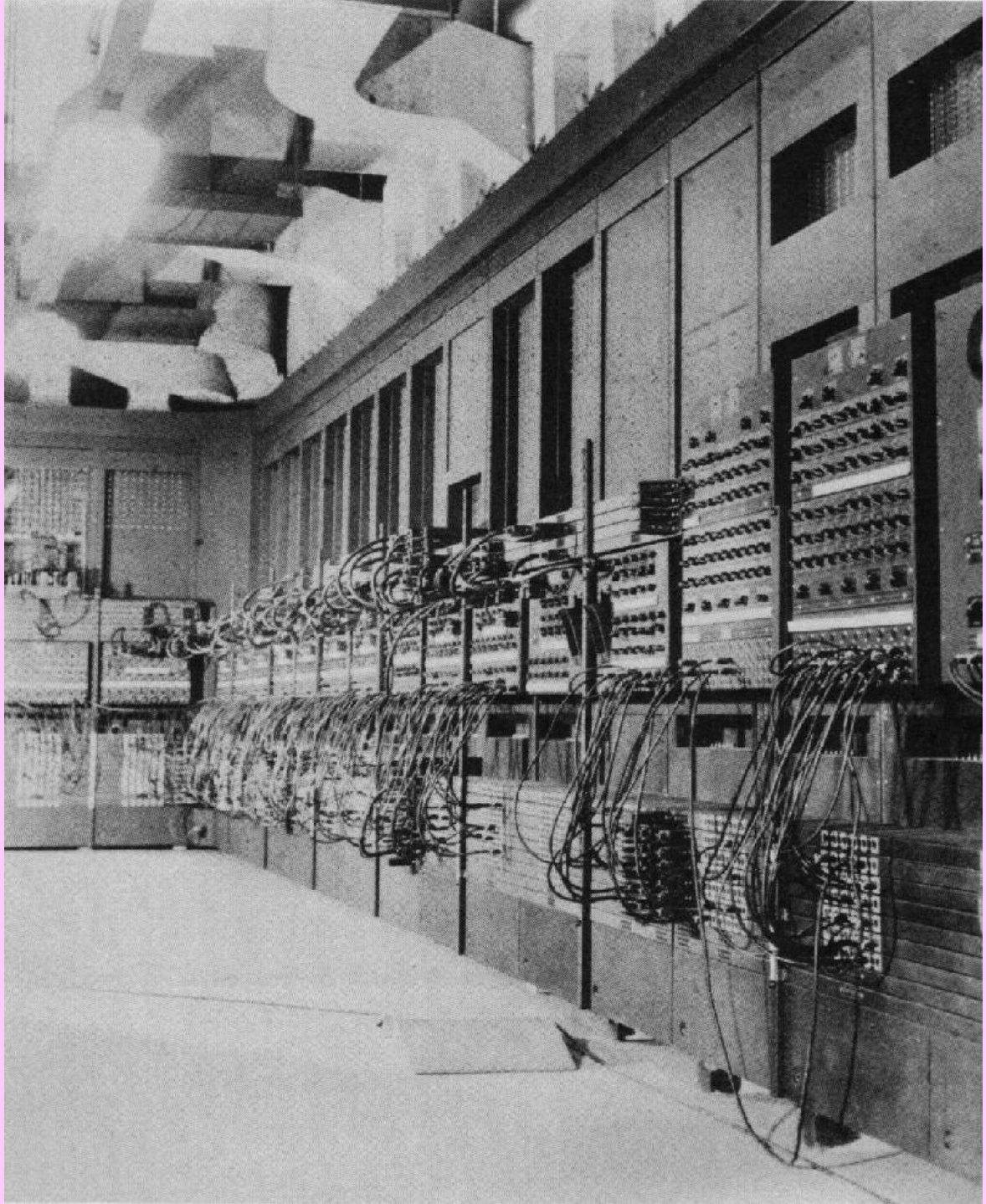
Пример взаимодействия радиочастотного импульса с ядерным спином



Современный ЯМР-компьютер

ЯМР-компьютеры: за и против

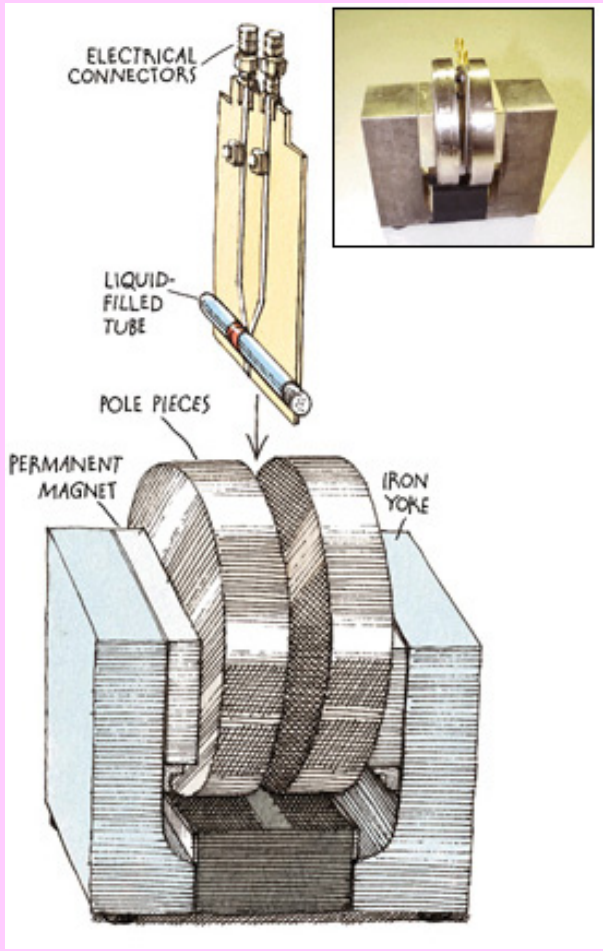
- За
  - Ядра хорошо защищены от внешнего воздействия.
    - Если спины выровнены, то они будут долгое время оставаться в таком состоянии.
  - Ядерные кубиты уже существуют в природе.
  - Технология воздействия на ядерные кубиты уже отработана.
    - ЯМР-томография интенсивно используется в медицине.
- Против
  - Очень большой размер таких компьютеров.
    - Большинство из них имеют три и более метров в высоту.



ENIAC
(1946)

ЯМР-компьютеры: современная ситуация

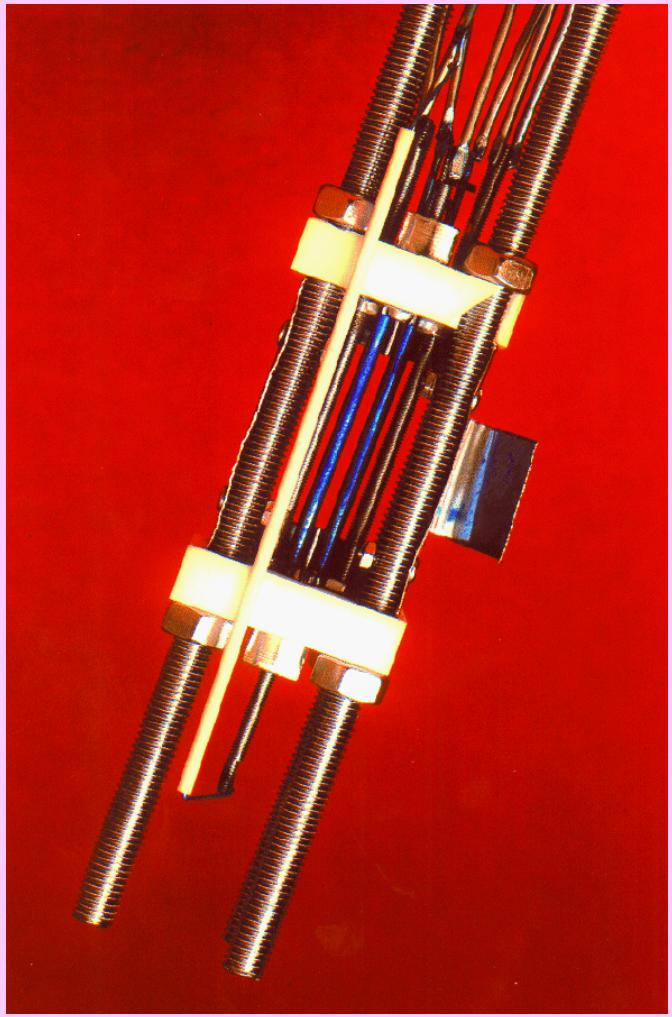
- Сейчас уже имеются ЯМР-компьютеры с 3 и 7 кубитами.
- ИБМ сейчас создает 10-кубитовую машину.
- В разработке находятся также ЯРМ-компьютеры меньшего размера и работающие при комнатных температурах.



Компьютеры на ионных ловушках

- Ионы (например Ca^+, Ba^+, Sr^+, Hg^+) в ловушке образуют одномерный кристалл. и взаимодействуют друг с другом, обмениваясь колебательными возбуждениями

  (вспомогательный кубит).
- Состояние каждого иона находится под управлением поляризованного и сфокусированного лазерного пучка.

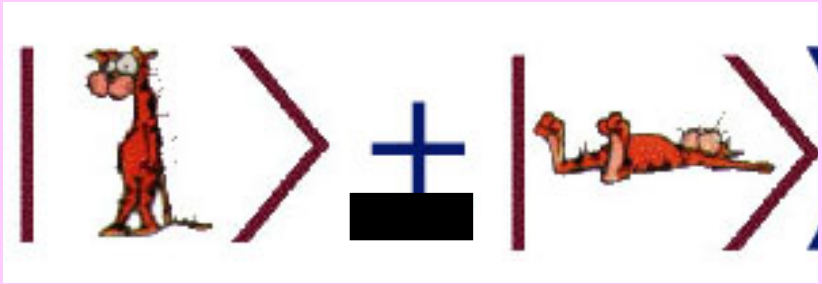


Вид реальной ловушки

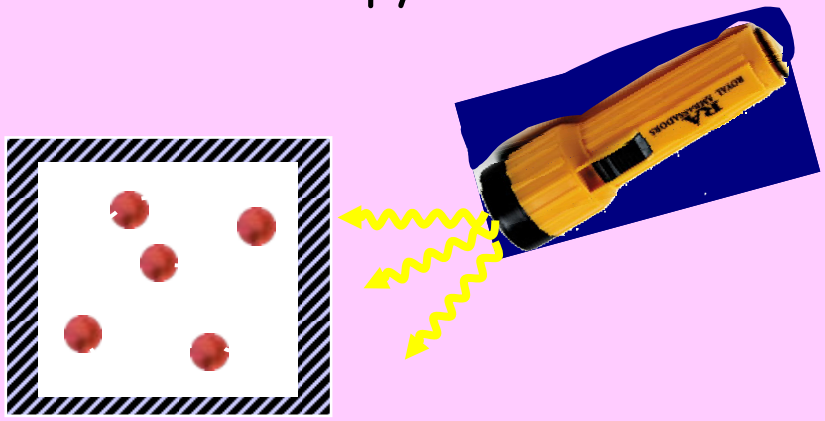
Требования к оборудованию квантового компьютера (P.Halian)

1. Допуск состояний типа

$$|000\ldots0\rangle + |111\ldots1\rangle$$

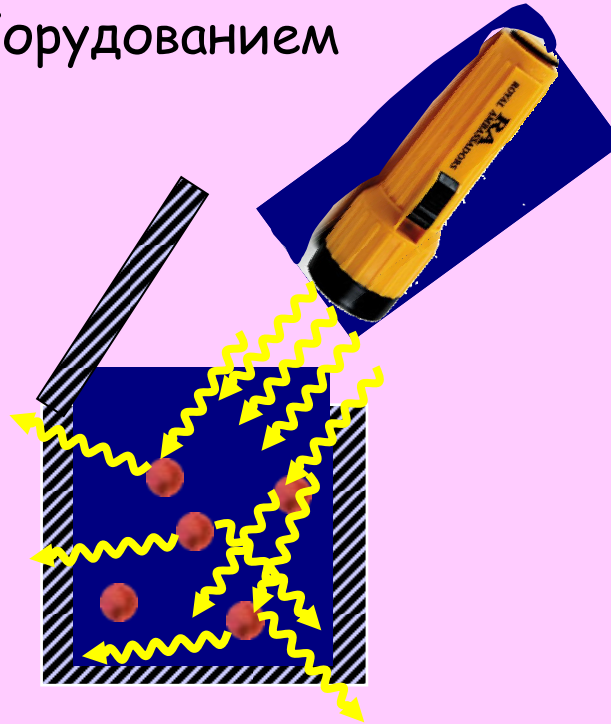


- сильное взаимодействие кубитов
- слабая связь с оборудованием



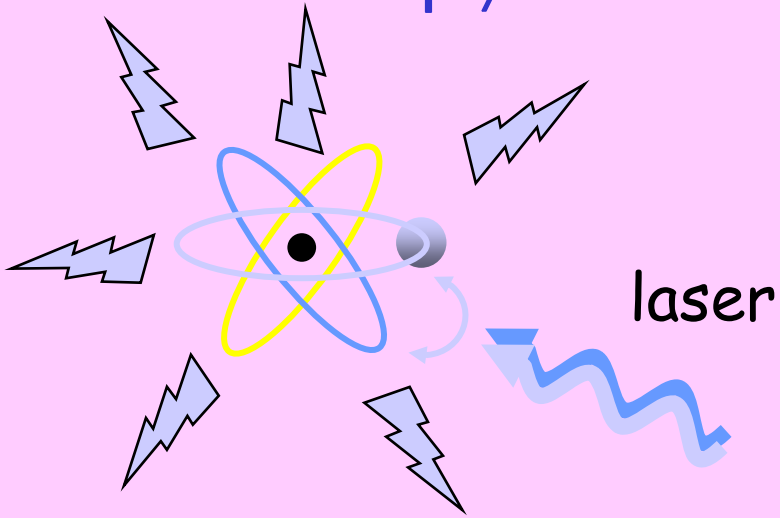
2. Высокоточное измерение состояний

- Сильная связь с оборудованием



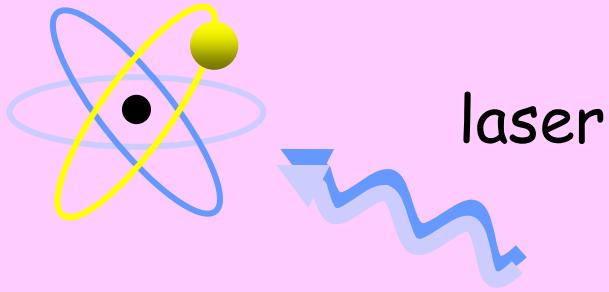
Квантовое измерение отдельного атома

state $|0\rangle$

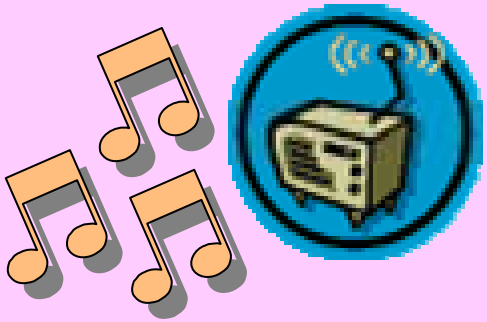


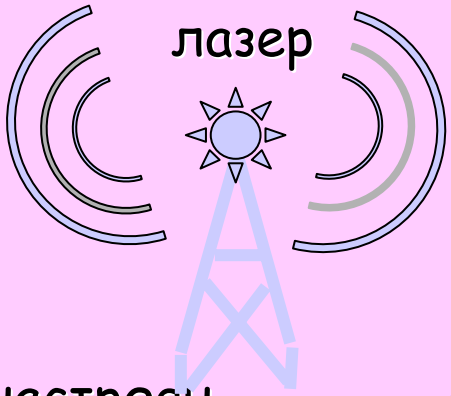
атом излучает 10^8 фотонов/сек

state $|1\rangle$



атом остается темным





Атомный приемник настроен
на лазерную волну

молчание

Атомный приемник не
Настроен на лазерную волну

Компьютеры на квантовых точках

- *Квантовые точки* представляют собой искусственные атомоподобные наноструктурные элементы с конечным числом дискретных энергетических уровней.
- На электрон, захваченный группой атомов, воздействует лазерный пучок определенной частоты. Это переводит электрон в возбужденное состояние. Возбужденное состояние может рассматриваться как |1 >, а основное состояние как |0 >
- Тем самым облучение лазерным светом можно рассматривать как контролируемый "not"-вентиль.