

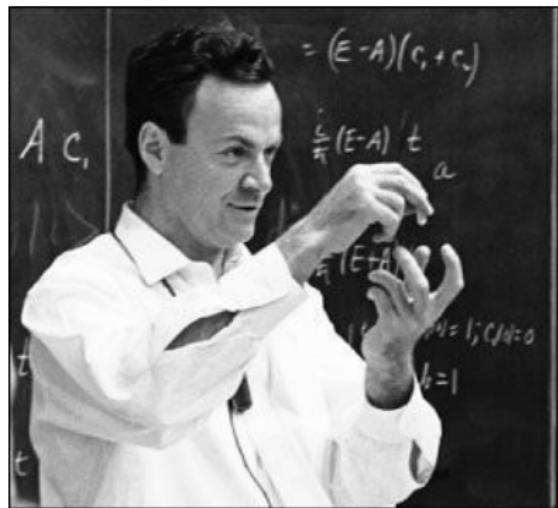
Квантовая информатика – что, зачем и почему?

Ширай Андрей

27 сентября 2013 г.

- Исторический экскурс.
- Как это работает.
- Примеры физических реализаций.
- Квантовые алгоритмы Шора(факторизация) и Гровера(поиск по неупорядоченной БД).
- Как это повлияет на надежность крипtosистем?
- Как квантовая информатика повлияла на другие направления теоретической информатики/математики/физики.
- Моделирование квантовых вычислений

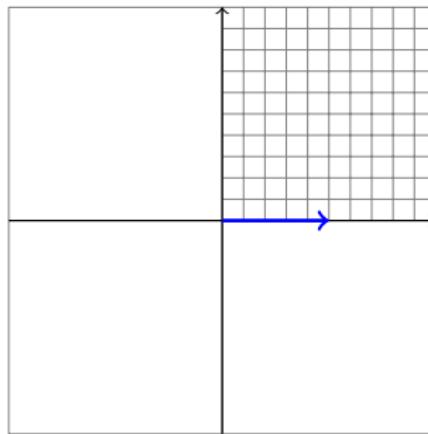
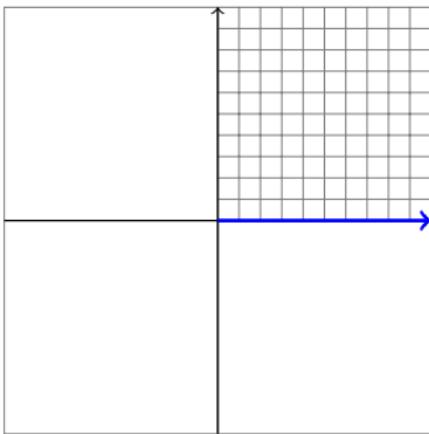
Вы, конечно же шутите, мистер Фейнман!



Feynman, R. P. (1982). *"Simulating physics with computers"*. International Journal of Theoretical Physics 21 (6): 467–488.

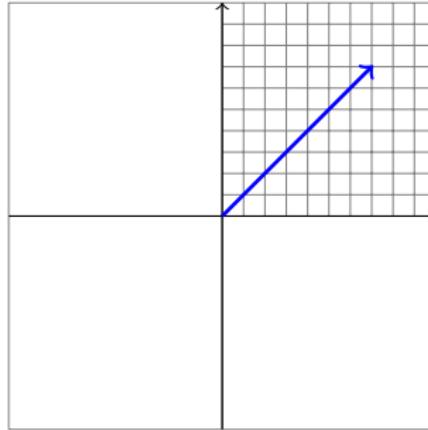
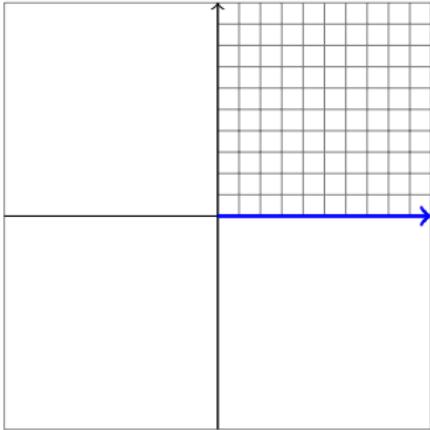
Освой линейную алгебру за 240 секунд!

$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}$$



Освой линейную алгебру за 240 секунд!

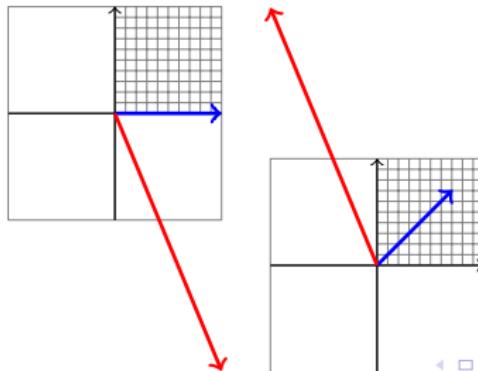
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$



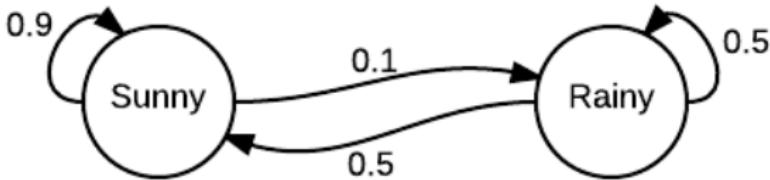
Определение

Собственный вектор – любой ненулевой вектор \vec{x} , который отображается оператором в коллинеарный $\lambda\vec{x}$, а соответствующий скаляр λ называется **собственным значением оператора**.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ -\sqrt{2} - 1 \end{pmatrix} = \begin{pmatrix} -1 \\ \sqrt{2} + 1 \end{pmatrix}$$



Стохастические вычисления



$P = \begin{pmatrix} 0.9 & 0.5 \\ 0.1 & 0.5 \end{pmatrix}$ – матрица перехода для некоторой цепи

Маркова. Входные данные: $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ – у нас хорошая погода.

$$\begin{pmatrix} 0.9 & 0.5 \\ 0.1 & 0.5 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.9 \\ 0.1 \end{pmatrix}$$

– с вероятностью 10% завтра пойдет дождь.

Неподвижная точка $\approx \begin{pmatrix} 0.833 \\ 0.167 \end{pmatrix}$

$$\begin{array}{c} \text{Стохастика} \\ \left(\begin{array}{ccc} s_{11} & \dots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \dots & s_{nn} \end{array} \right) \left(\begin{array}{c} p_1 \\ \vdots \\ p_n \end{array} \right) = \left(\begin{array}{c} q_1 \\ \vdots \\ q_n \end{array} \right) \\ p_i \geq 0, \sum_{i=1}^n p_i = 1 \end{array} \quad \left| \quad \begin{array}{c} \text{“Кванты”} \\ \left(\begin{array}{ccc} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{array} \right) \left(\begin{array}{c} \alpha_1 \\ \vdots \\ \alpha_n \end{array} \right) = \left(\begin{array}{c} \beta_1 \\ \vdots \\ \beta_n \end{array} \right) \\ \alpha \in \mathbb{C}, \sum_{i=1}^n \|\alpha_i\|^2 = 1 \end{array} \right.$$

Сформулировано страшно коряво, в каком-то смысле даже неверно, но зато правильно и понятно. ©

Постулат

Физическое состояние замкнутой квантовой системы описывается нормированным вектором состояния $|\psi\rangle$ в линейном комплексном пространстве с внутренним произведением(Гильбертовом пространстве)

Постулат

Динамическая эволюция замкнутой квантовой системы описывается унитарным преобразованием:

$$|\psi(t)\rangle = \hat{U}(t) |\psi(0)\rangle$$

Суперпозиция

... Одна из причин этого в том, что 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 планковских ячеек. При объединении классических систем их числа состояний N_1 и N_2 перемножаются, а в квантовом варианте получается $c^{N_1 N_2}$.

Ю. Манин “Вычислимое и невычислимое”

... Одна из причин этого в том, что 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 планковских ячеек. При объединении классических систем их числа состояний N_1 и N_2 перемножаются, а в квантовом варианте получается $c^{N_1 N_2}$.

Постулат

При измерении наблюдаемой A ее состояние редуцируется в один из векторов оператора \hat{A}

Постулат

При измерении наблюдаемой A ее состояние редуцируется в один из векторов оператора \hat{A}

$$\frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$$



КОТ ШРЁДИНГЕРА

ШРЁДИНГЕР

Операторы

Запутанность

Квантовые потоки

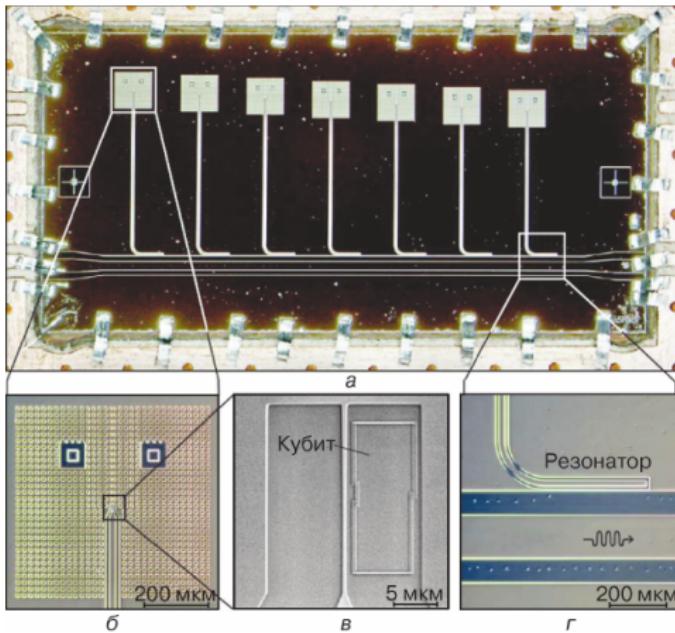
Квантовые потоки

Квантовые потоки

Квантовые потоки

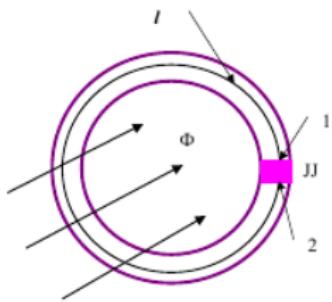
Квантовое лямбда-исчисление

Джозефсоновские кубиты



M. Jerger, S. Poletto, P. Macha, U. Hübner, A. Lukashenko, E. Il'ichev, A. V. Ustinov *Readout of a qubit array via a single transmission line*, *Europhys. Lett.* 96, (2011) 40012

Джозефсоновские кубиты





Sergio Boixo, Troels F. Rønnow, Sergei V. Isakov, Zhihui Wang, David Wecker, Daniel A. Lidar, John M. Martinis, Matthias Troyer *Quantum annealing with more than one hundred qubits*, arXiv:1304.4595

Универсальная задача перебора

Оптимальность алгоритма Гровера...

Оптимальность алгоритма Гровера... или почему $\mathcal{P} \neq \mathcal{NP}$

- ① Линейность¹ квантовой механики → Предел Гровера \sqrt{N}
- ② А если у нас будут нелинейные квантовые операторы, сохраняющие нормировку? (“Приличная” нелинейная КМ)

¹В смысле линейность интегрального оператора, а не подинтегрального выражения!

Оптимальность алгоритма Гровера... или почему $\mathcal{P} \neq \mathcal{NP}$

- ① Линейность квантовой механики → Предел Гровера \sqrt{N}
- ② Нелинейная КМ передает сигналы быстрее с и решает $\#\mathcal{P}$ -полные проблемы за полиномиальное время!² Ура!

²Ограничиваюсь нелинейными преобразованиями **сохраняющими норму**

Оптимальность алгоритма Гровера... или почему $\mathcal{P} \neq \mathcal{NP}$

- ① Линейность квантовой механики → Предел Гровера \sqrt{N}
- ② Нелинейная КМ передает сигналы быстрее с и решает $\#\mathcal{P}$ -полные проблемы за полиномиальное время! Ура!
- ③ ... попутно экспоненциально размножая ошибку. $\#\$%\hat\&^*$!

Оптимальность алгоритма Гровера... или почему $\mathcal{P} \neq \mathcal{NP}$

- ➊ Линейность квантовой механики → Предел Гровера \sqrt{N}
- ➋ Нелинейная КМ передает сигналы быстрее с и решает $\#\mathcal{P}$ -полные проблемы за полиномиальное время! Ура!
- ➌ ... попутно экспоненциально размножая ошибку. $\#\$%&^*$!
- ➍ Скрытые параметры? Предел Гровера улучшается с $N^{\frac{1}{2}}$ до $N^{\frac{1}{3}}$ – поиск по “историям” траекторий частичек

Оптимальность алгоритма Гровера... или почему $\mathcal{P} \neq \mathcal{NP}$

- ① Линейность квантовой механики → Предел Гровера \sqrt{N}
- ② Нелинейная КМ передает сигналы быстрее с и решает $\#P$ -полные проблемы за полиномиальное время! Ура!
- ③ ... попутно экспоненциально размножая ошибку. $\#\$\%&^*$!
- ④ Скрытые параметры? Предел Гровера улучшается с $N^{\frac{1}{2}}$ до $N^{\frac{1}{3}}$ – поиск по “историям” траекторий частичек
- ⑤ Зеноновские вычисления и всякие прочие супертьюринговые вычисления накрываются по достижении планковской длины.

Алгоритм Шора

Алгоритм Шора

Симметричные и ассиметричные криптосистемы

Задача о скрытой подгруппе

Неабелевый случай

Влияние – квантовая связь



Влияние – квантовая связь



Широко известные не в столь узких кругах обсуждения
“информационных” аспектов физики:

- Konrad Zuse *Rechnender Raum*³ (1967)
- Lloyd, S., *Programming the Universe: A Quantum Computer Scientist Takes On the Cosmos* (2006)
- Хокинг, Прескилл, Сасскинд и срачик о термодинамике
черных дыр, которые “теряют” информацию.

³Вычислительное пространство

Интерпретации квантовой механики:

- ① Копенгагенская
- ② Многомировая
- ③ Теории скрытого параметра(Schrödinger, Bohmian Mechanics)

В чем же разница?

Интерпретации квантовой механики:

- ① Копенгагенская
- ② Многомировая
- ③ Теории скрытого параметра(Schrödinger, Bohmian Mechanics)

В чем же разница?

РАЗНЫЕ ВСЕЛЕННЫЕ!
с разными вычислительными ресурсами!

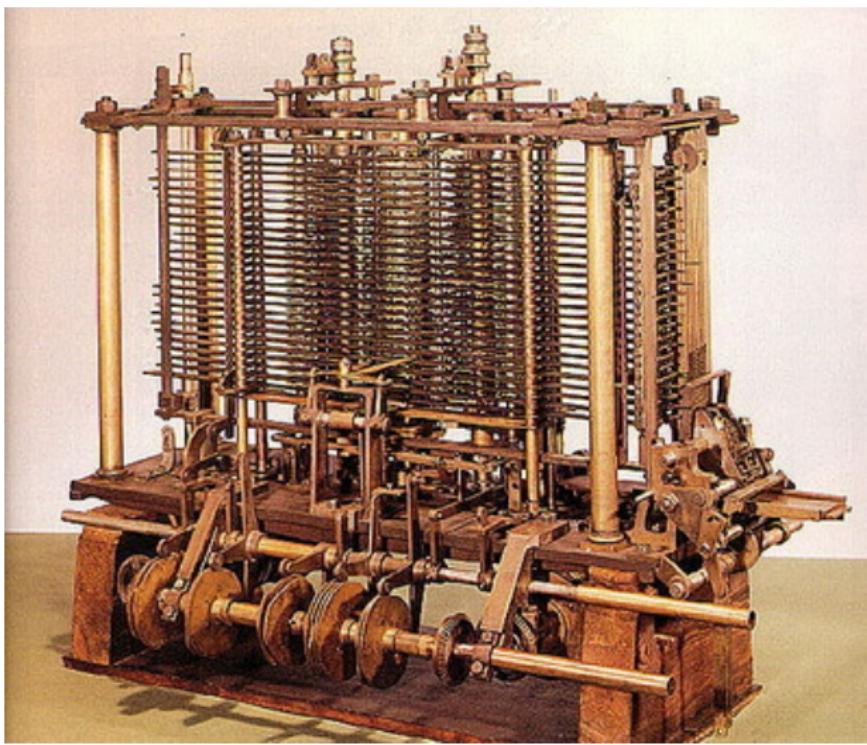
We should expect a mathematical question to have a definite answer, if and only if we can phrase the question in terms of a physical process we can imagine.

David Deutsch

У нас есть разные модели для

Влияние – теория сознания

Аналитическая машина



Квантовое Функциональное Программирование

Квантовое Функциональное Программирование

Квантовое Функциональное Программирование

Что? Scheme

Где? <http://www.het.brown.edu/people/andre/qlambda/>

Кто виноват? André van Tonder.

Что? Haskell

Где? <http://hackage.haskell.org/package/QIO>

Кто виноват? Alexander S. Green

Что? Maxima

Где? <http://www.johnlapeyre.com/qinf/>

Кто виноват? G. John Lapeyre, Jr.

List of QC simulators

- http://www.quantiki.org/wiki/List_of_QC_simulators
- curl, grep, sort -u, wc -l, немногого магии...
- 95
- ??????
- PROFIT

Книги/лекции:

- CS191x Quantum Mechanics and Quantum Computation
- Лекции – Preskill(Caltech), Vazirani(Berkeley), Watrous(Waterloo), ...
- Reference textbook – Nielsen and Chuang, *Quantum Computation and Quantum Information*⁴
- А. Китаев, А. Шень, М. Вялый. *Классические и квантовые вычисления*.
- MIT OCW 6.845 *Quantum Complexity Theory* – Scott Aaronson
- Scott Aaronson *Quantum Computing Since Democritus*
- Feynman lectures on computation

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

Статьи:

- Feynman, R. P. (1982). "*Simulating physics with computers*".
(Перепечетано в Feynman lectures on computation)
- *Quantum annealing with more than one hundred qubits*,
arXiv:1304.4595
- *Physics, Topology, Logic and Computation: A Rosetta Stone*,
arXiv:0903.0340
- *Quantum Proofs for Classical Theorems*,
10.4086/toc.gs.2011.002
- *NP-complete Problems and Physical Reality*,
quant-ph/0502072

Feci, quod potui, faciant meliora potentes

Dixi