

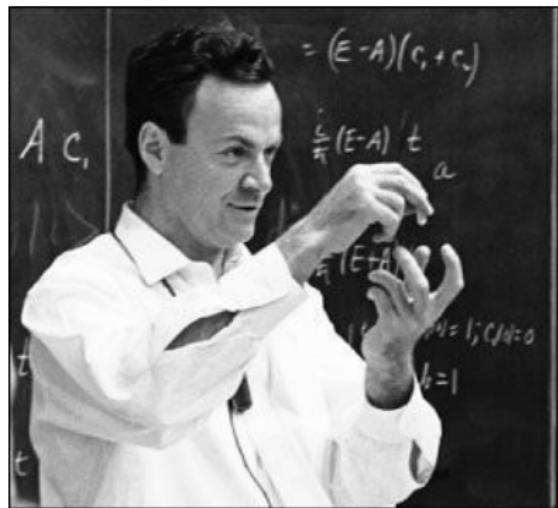
Квантовая информатика – что, зачем и почему?

Ширай Андрей

27 ноября 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

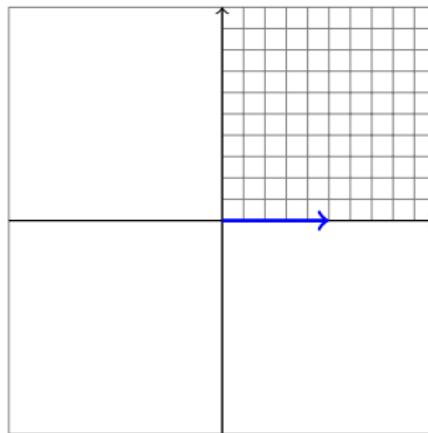
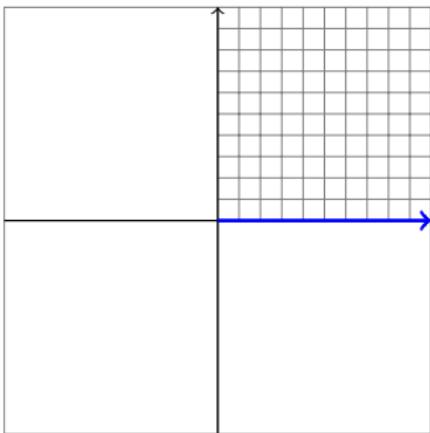
Вы, конечно же шутите, мистер Фейнман!



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

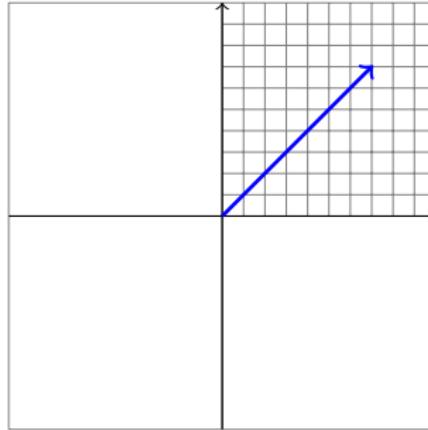
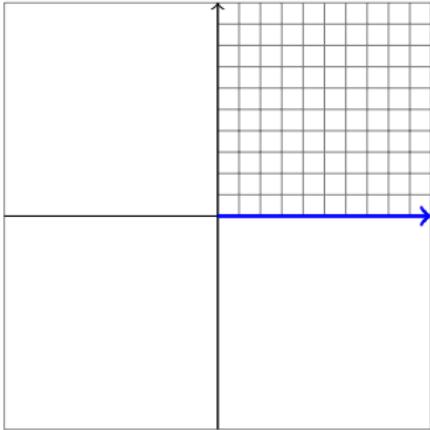
Освой линейную алгебру за 240 секунд!

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

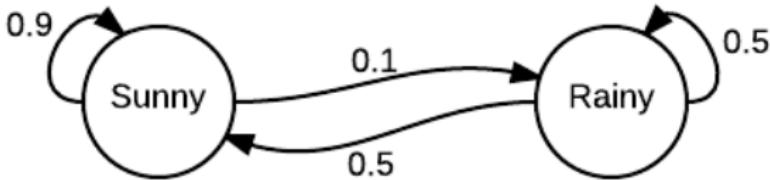


Освой линейную алгебру за 240 секунд!

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



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. ©

Гильбертово пространство

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}

Измерение и наблюдаемые

Постулат

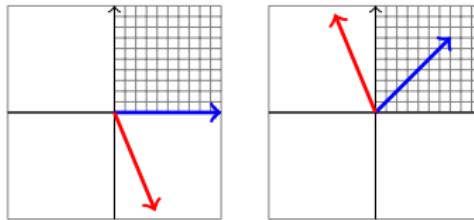
При измерении наблюдаемой A ее состояние редуцируется в один из собственных векторов оператора \hat{A}



Определение

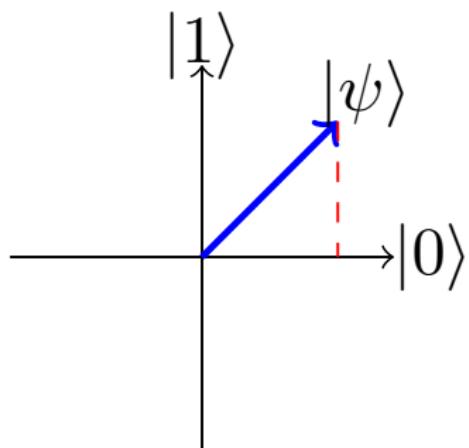
Собственный вектор – любой ненулевой вектор \vec{x} , который отображается оператором в коллинеарный $\lambda\vec{x}$, а соответствующий скаляр λ называется **собственным значением оператора**.

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

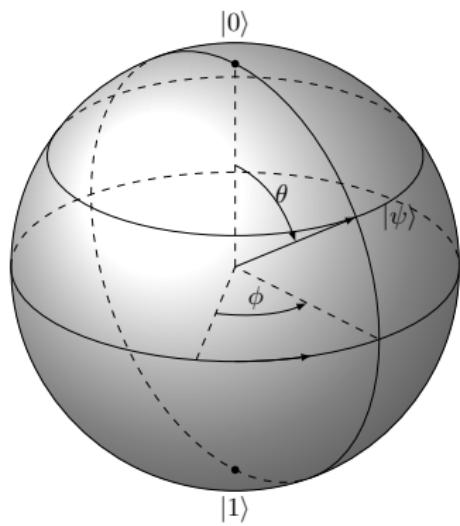


Определение

Оператор \hat{P} , для которого $\hat{P}^2 = \hat{P}$ называется **проектором**.



Сфера Блоха



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

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

$$|\psi\rangle = e^{-i\phi/2} \cos \frac{\theta}{2} |0\rangle + e^{i\phi/2} \sin \frac{\theta}{2} |1\rangle$$

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
'Even Though 'Correct.'

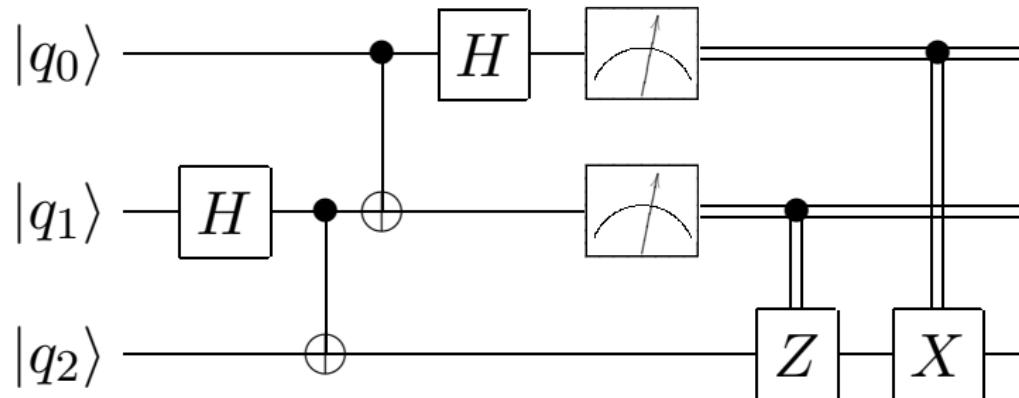
Сепарабельное состояние:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \quad (1)$$

Несепарабельное состояние:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (2)$$

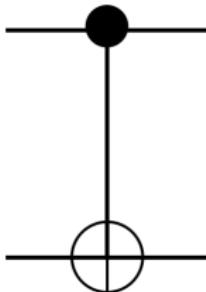
Квантовые схемы



Квантовые схемы

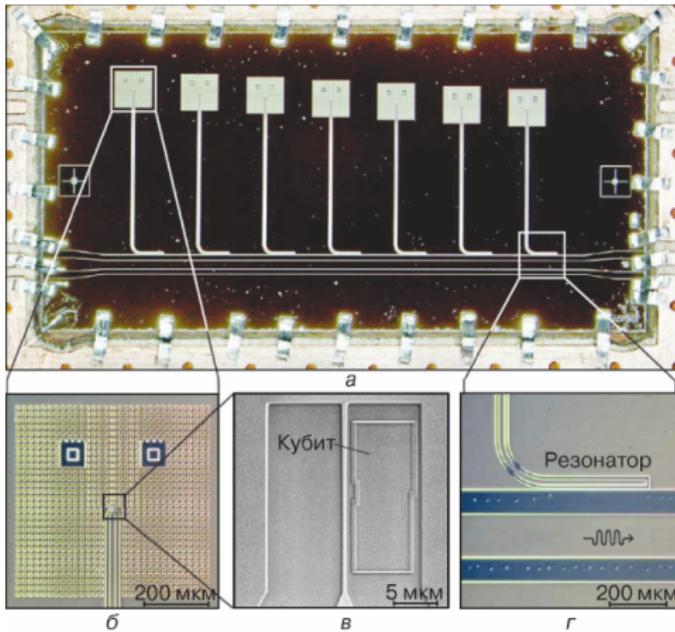
X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X 0\rangle = 1\rangle$ $X 1\rangle = 0\rangle$
Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$Z 0\rangle = 0\rangle$ $Z 1\rangle = - 1\rangle$
H	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	$H 0\rangle = +\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $H 1\rangle = -\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

Квантовые схемы



$|00\rangle \rightarrow |00\rangle$
 $|01\rangle \rightarrow |00\rangle$
 $|10\rangle \rightarrow |11\rangle$
 $|11\rangle \rightarrow |10\rangle$

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



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

Алгоритм Гровера

Сначала формируют равномерную суперпозицию всех состояний: $H^{\otimes n} |0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$. Чуть дальше будет обозначать для краткости равномерную суперпозицию как $|\psi\rangle$. Потом последовательно применяется оператор Гровера:

- ① К входу применяется оракул $O: |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$. Т.е. это единичная матрица, где на месте ответов стоят -1 .¹
- ② Опять преобразование Адамара $H^{\otimes n}$
- ③ Условный сдвиг фазы: $|x\rangle \rightarrow -(-1)^{\delta_{0x}}|x\rangle$, этой операции соответствует унитарный оператор $|0\rangle\langle 0| - I$.
- ④ Опять преобразование Адамара $H^{\otimes n}$

$$G = (|\psi\rangle\langle\psi| - I)O$$

¹ Очевидно, что $O^2 = I$, так что унитарность сохраняется.

Алгоритм Гровера

Оператор Гровера G :

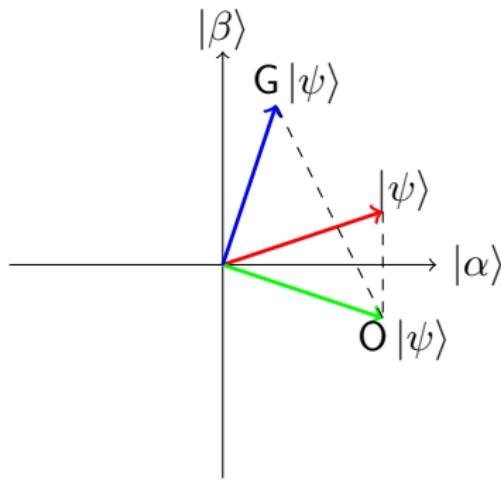


Геометрическая интерпритация алгоритма Гровера

Мы можем переписать $|\psi\rangle$, как:

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \cos \frac{\theta}{2}|\alpha\rangle + \sin \frac{\theta}{2}|\beta\rangle$$

, где $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \neq f(x)} |x\rangle$ и $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)} |x\rangle$



$$G^k |\psi\rangle = \cos \frac{(2k+1)\theta}{2} |\alpha\rangle + \sin \frac{(2k+1)\theta}{2} |\beta\rangle$$

И необходимое количество итераций:

$$R = \lfloor \arcsin \frac{\sqrt{M/N}}{\theta} \rfloor \stackrel{M \leq N/2}{=} \lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \rfloor$$

Теорема

Алгоритм Гровера – оптимальный

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

- ① Линейность² квантовой механики → Предел Гровера \sqrt{N}
- ② А если у нас будут нелинейные квантовые операторы, сохраняющие нормировку? (“Приличная” нелинейная КМ)

²В 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!³ Ура!

³Ограничиваюсь 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

$$N = pq$$

Факторизация сводится к так называемому поиску периода:

- ① Выбрать случайный остаток a по модулю N
- ② Проверить $\text{НОД}(a, N) = 1$
- ③ Найти порядок r остатка a по модулю N

Определение

Порядок a по модулю N – минимальное r такое, что $a^r \equiv 1 \pmod{N}$

- ④ Если r четен, вычислить $\text{НОД}(a^{r/2} - 1, N)$

Собственно алгоритм Шора – это поиск периода функции $f(x) = a^x \pmod{N}$, который и будет порядком.

Алгоритм Шора

- На самом деле Алгоритм Шора мы рассматривать не будем :Р
- Он просто строит состояние с периодом r , а потом “выуживает” период с помощью преобразований Фурье.
- Мы поговорим о том, почему же это работает?!

Постулат

Алгоритм Шора работает, потому что, разложение на множители единственно.



Задача о скрытой подгруппе

- У нас есть группа G , она имеет подгруппу H .

Определение

$f : G \rightarrow X$ – прячет подгруппу H , если

$$\forall g_1, g_2 \in G : f(g_1) = f(g_2) \Leftrightarrow g_1 H = g_2 H$$



Задача о скрытой подгруппе – задача о восстановлении образующих элементов подгруппы по отображению, которое принимает одинаковые значения на всех (левых) классах смежности относительно этой подгруппы.

Постулат

Алгоритм Шора может эффективно решить HSP для конечных абелевых групп.

Ну и ЧО?

Большинство специалистов сходятся во мнении, что достаточно стойкие симметричные шифры останутся стойкими и в квантовой модели вычислений

Коммутативные и локально-коммутативных шифры в опасности. Под этот случай подпадают схема Месси-Омуры, схема направленной подписи, система шифрования Эль-Гамаля, схемы групповой и слепой подписей и т.д.

Ничего толком не известно про неабелевый случай.

List of QC simulators

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

Квантовое лямбда-исчисление

$t ::=$

x

$(\lambda x. t)$

$(t \ t)$

c

$!t$

$(\lambda !x. t)$

$c ::=$

$0 \mid 1 \mid H \mid S \mid R_3 \mid cnot \mid X \mid Y \mid Z \mid \dots$

terms:

variable

abstraction

application

constant

nonlinear term

nonlinear abstraction

constants:

Что? Scheme

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

Кто виноват? André van Tonder.

Что? Maxima

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

Кто виноват? G. John Lapeyre, Jr.

Что? Haskell

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

Кто виноват? Alexander S. Green

Что? Haskell Quipper

Где? <http://www.mathstat.dal.ca/~selinger/quipper/>

Кто виноват? Peter Selinger

Влияние – квантовая связь



Влияние – квантовая связь



Влияние – квантовая связь



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

- Konrad Zuse *Rechnender Raum*⁴ (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.

⁴Вычислительное 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

Новые математические методы, придуманные, пока возились с КК, можно использовать и в мирной жизни:

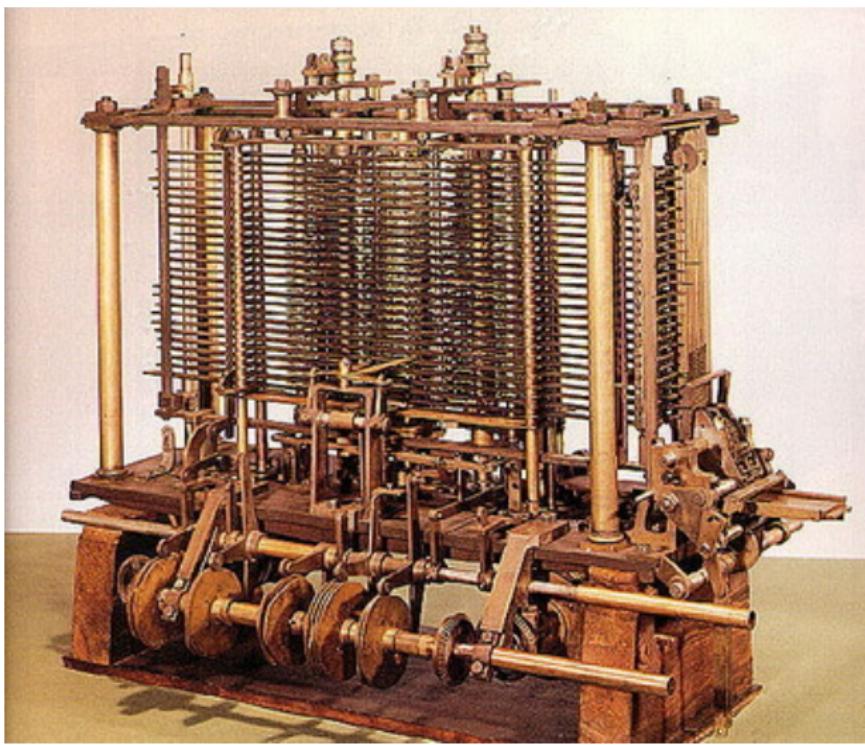
- ① ϵ -approximating polynomials for symmetric functions
- ② Robust polynomials
- ③ Lower bounds on locally decodable codes

*If we want a machine to be intelligent, it can't also be infallible.
There are theorems that say almost exactly that.*

Turing

- ① Consciousness is reducible to computation (Strong-AI)
- ② Consciousness can be simulated by a computer, but the simulation couldn't produce "real understanding" (John Searle)
- ③ Consciousness can't even be simulated by computer, but nevertheless has a scientific explanation (Penrose)
- ④ Consciousness doesn't have a scientific explanation at all (99% хомячков населения)

Аналитическая машина



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*⁵
- 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

⁵Нильсен 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