Квантовая информатика – что, зачем и почему?

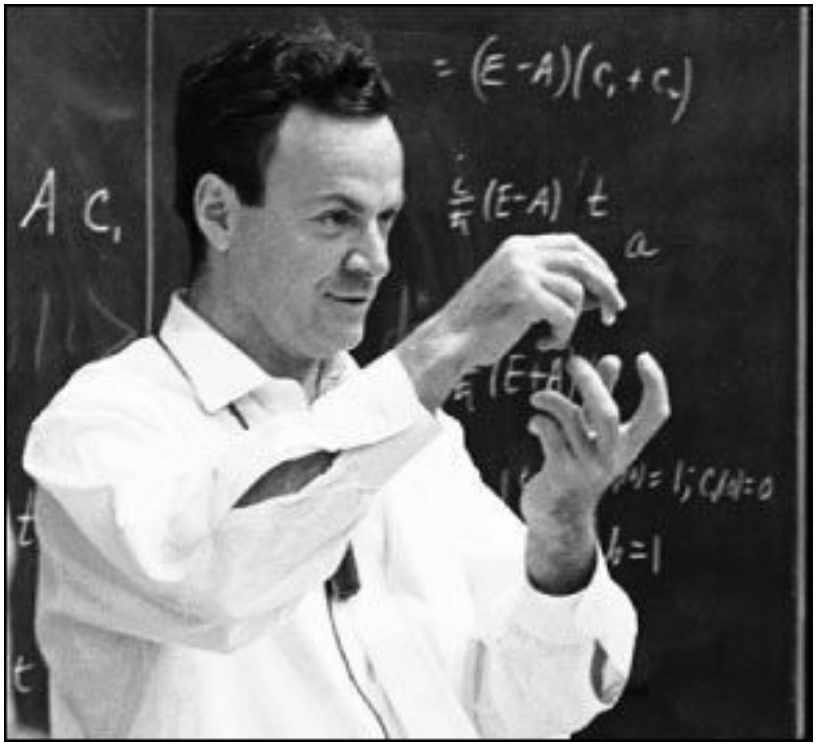
Ширай Андрей

22 сентября 2013 г.

We have a plan!

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

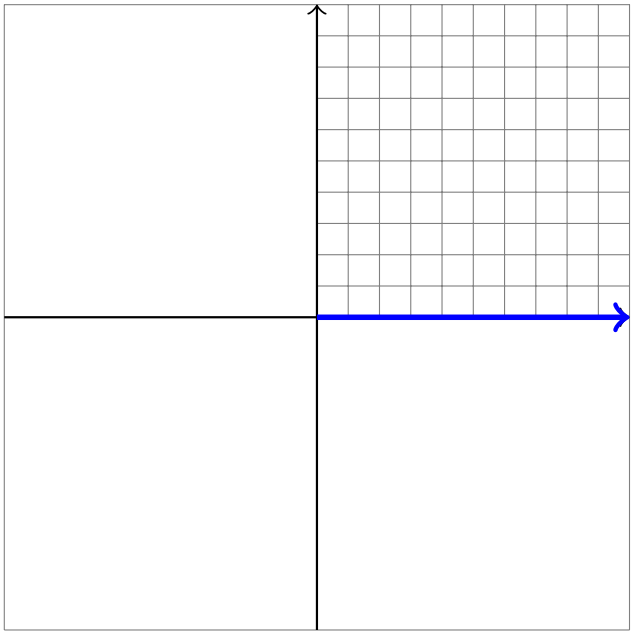
Вы, конечно же шутите, мистер Фейнман!

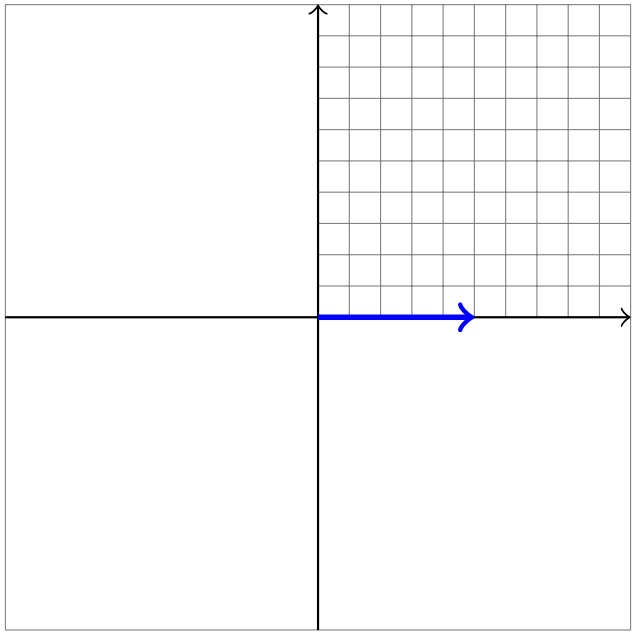


Feynman, R. P. (1982). *"Simulating physics with computers"*. International Journal of Theoretical Physics 21 (6): 467–488.

Освой линейную алгебру за 240 секунд!

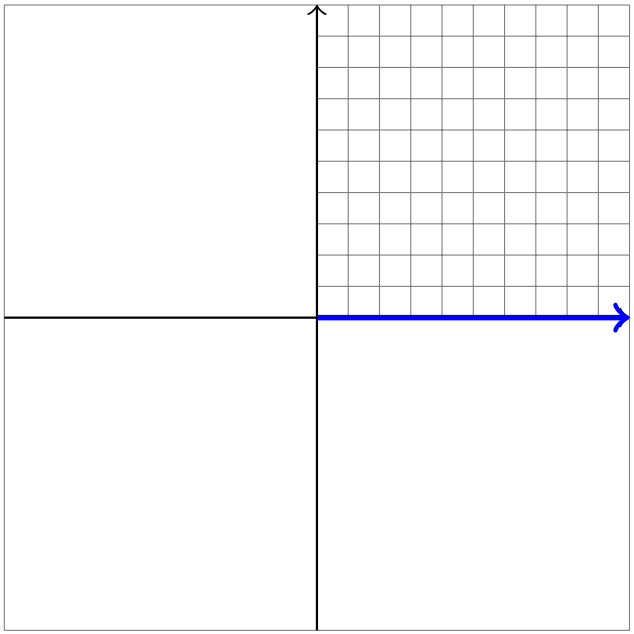
$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix}$$

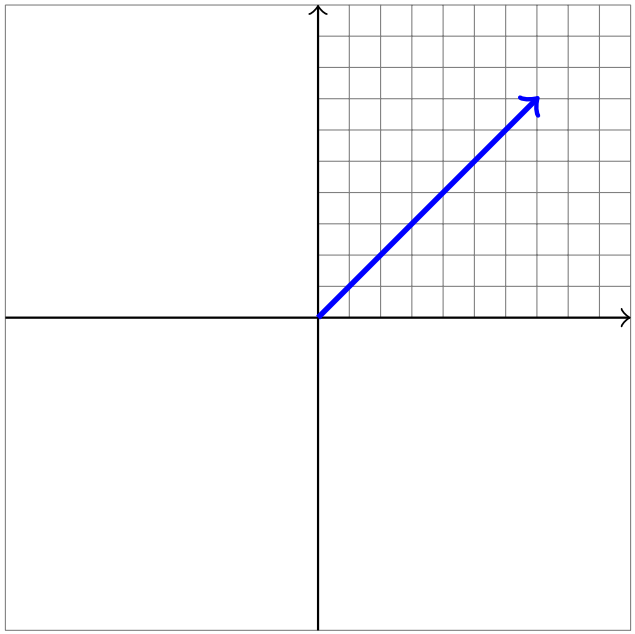




Освой линейную алгебру за 240 секунд!

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





Освой линейную алгебру за 240 секунд!

Стохастические вычисления

Квантовая механика одним слайдом

Стохастика

$$\begin{pmatrix} s_{11} & \dots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \dots & s_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$$

$$p_i \geq 0, \sum_{i=1}^{n} p_i = 1$$

“Кванты”

$$\begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \dots & u_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

$$\alpha \in \mathbb{C}, \sum_{i=1}^{n} \|\alpha_i\|^2 = 1$$

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 внутреним 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”*

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 $c^{N_1 N_2}$.

Постулат

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

Суперпозиция

Постулат

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

Операторы

Запутаность

Квантовые потоки

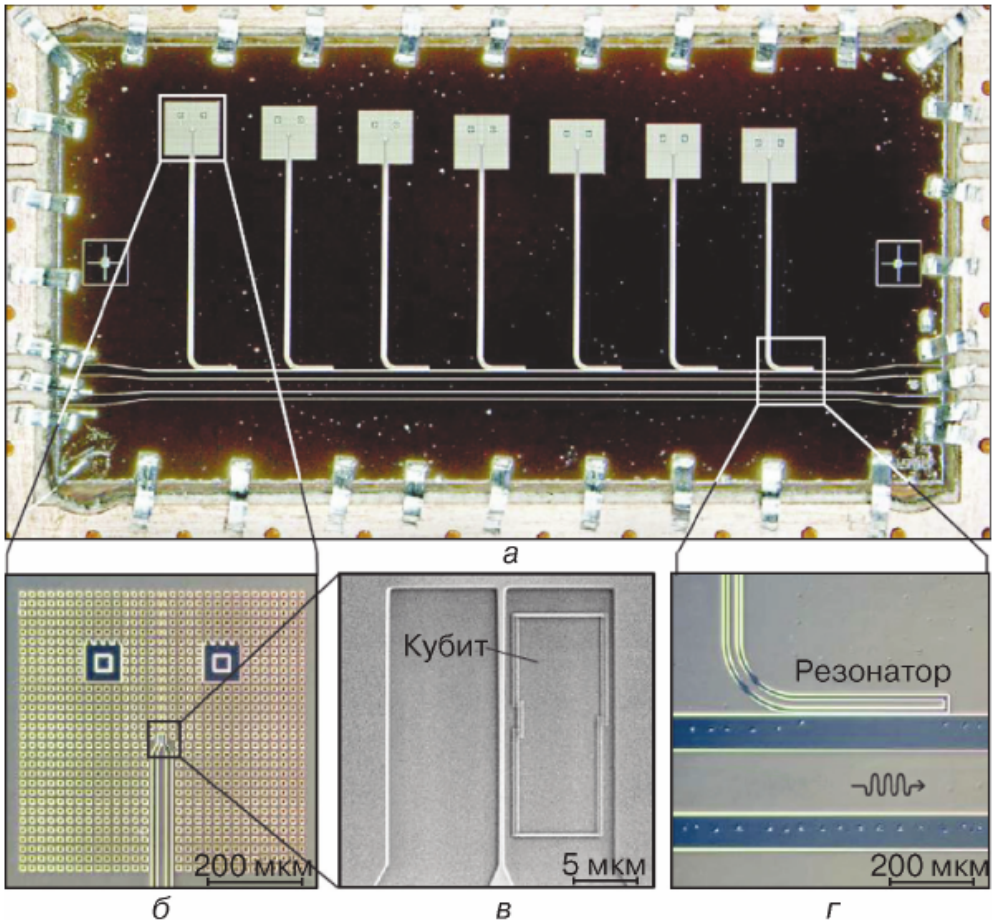
Квантовые потоки

Квантовые потоки

Квантовые потоки

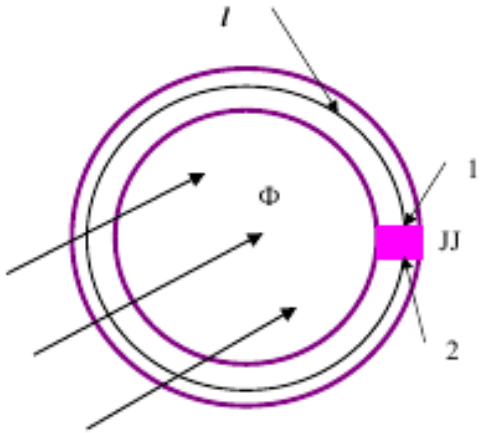
Квантовое лямбда-исчисление

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



D-Wave

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. Линейность[1] квантовой механики $\rightarrow$ Предел Гровера $\sqrt{N}$
2. А если у нас будут нелинейные квантовые операторы, сохраняющие нормировку? (“Приличная” нелинейная КМ)

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

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

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

[2] Ограничиваясь нелинейными преобразованиями **сохраняющими норму**

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

1. Линейность квантовой механики $\rightarrow$ 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. #\$%&*!

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

1. Линейность квантовой механики $\rightarrow$ 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. $\#\$\hat{\%}\&*!$
4. 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 $\rightarrow$ 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. #\$%&*!
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 – цифровая физика

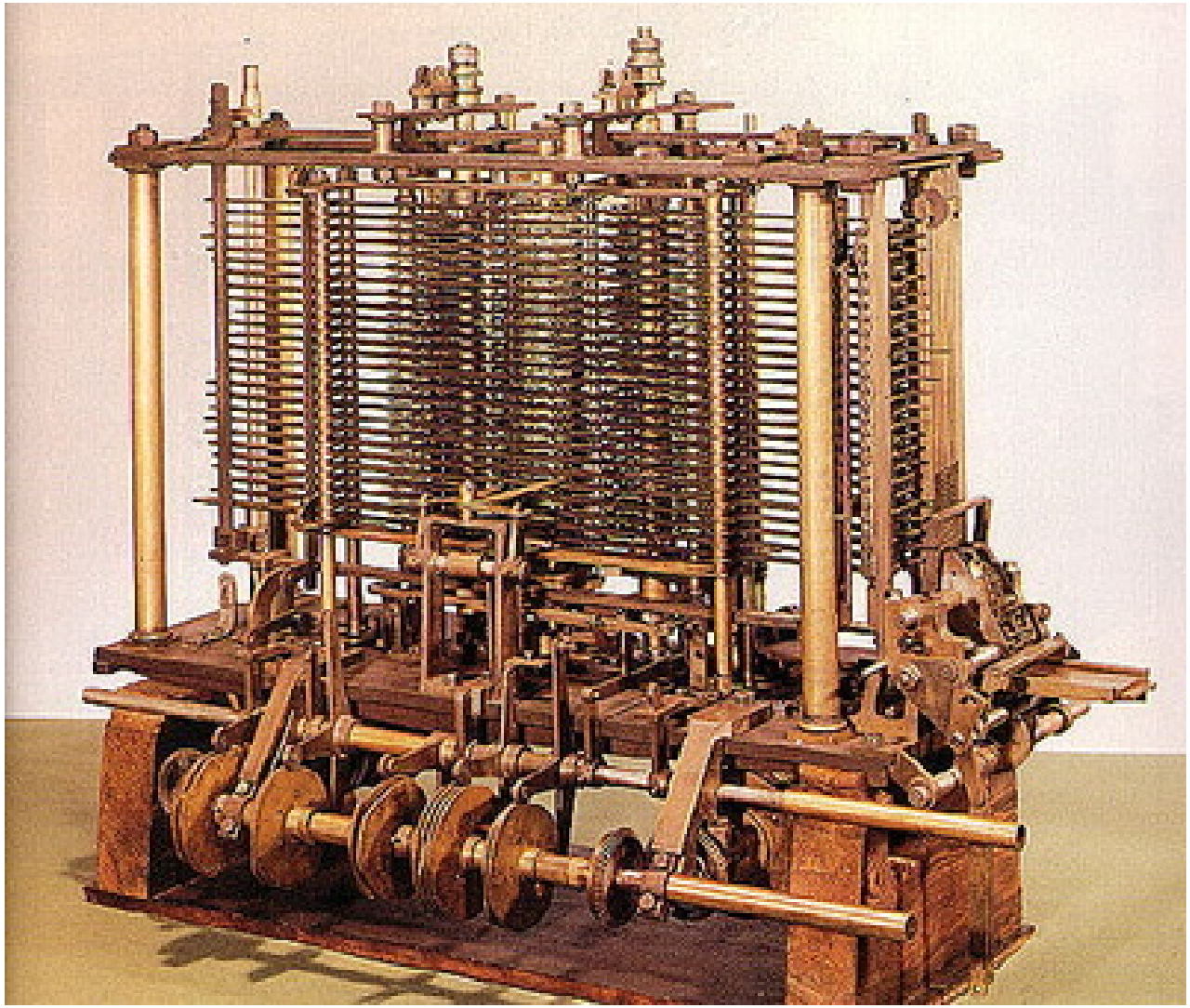
Влияние – квантовая связь

Влияние – матан

Влияние – теория эволюции

Влияние – теория сознания

Аналитическая машина



Квантовое Функциональное Программирование

Квантовое Функциональное Программирование

Квантовое Функциональное Программирование

Scheme simulator

Scheme simulator

Scheme simulator

QIO – Quantum IO Monad

QIO – Quantum IO Monad

QIO – Quantum IO Monad

Maxima – qinf

Что почитать?

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*[3]
- 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

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

Что почитать?

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
-
-
-

Dixi