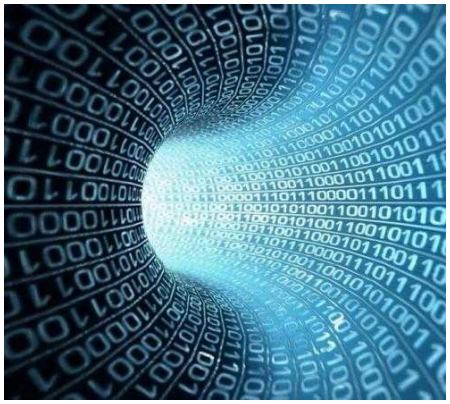
Введение в квантовую информатику и ее вычислительные аспекты



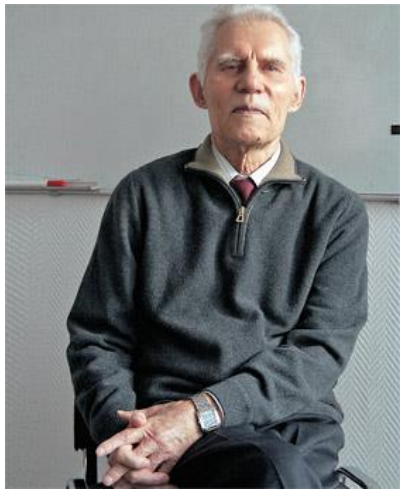
Чернявский А.Ю.

Физико-технологический институт РАН

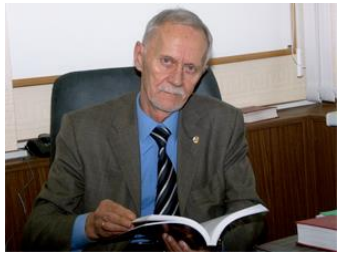
Кафедра суперкомпьютеров и квантовой информатики ВМК МГУ

super computers & quantum informatics

К.А. Валиев (1931-2010)



Лаборатория физики квантовых компьютеров ФТИАН



акакд. А. А. Орликовский (директор)

Ю.И. Богданов (зав. лаб.)

Кафедра (суперкомпьютеров и) квантовой информатики ВМК МГУ

чл.-корр. Вл. В. Воеводин (зав. каф.)

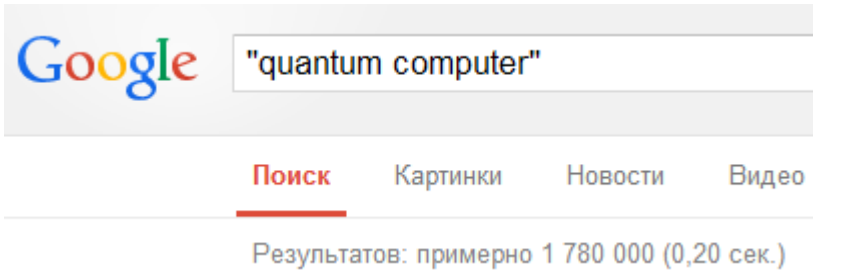
проф. С.Н. Молотков

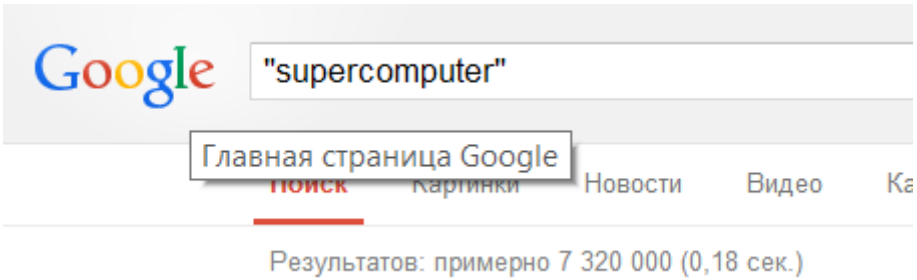
проф. Ю.И. Ожигов

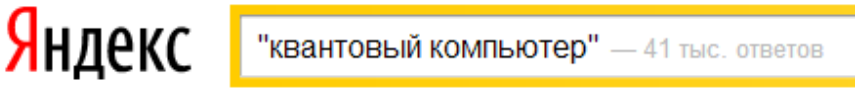
Проблема

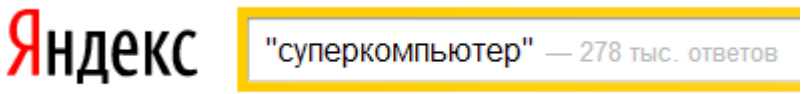
Далеко не все, особенно в России, принимают квантовые информационные технологии

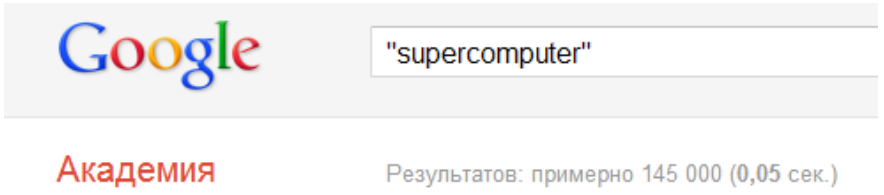
Интернет-популярность квантовой информатики











В России

- Ситуация имеет сходство с квантовой механикой, генетикой, кибернетикой в СССР.
- Специальность 05.13.20 Квантовые методы обработки информации введена в 2009 г.
- Единицы учебных курсов (МГУ, КГУ, ННГУ)
- Небольшое число лабораторий
- Ситуация меняется (например, RQC)

Другие страны

- Один пример: конференция *Quantum Information 2013*, Benasque, Spain
- Примерно 150 участников, примерно 80% европейской молодежи

Timeline of quantum computing

From Wikipedia, the free encyclopedia

This is a **timeline of quantum computing**.

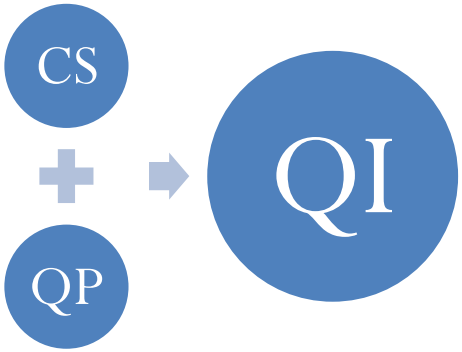
1970s [edit]

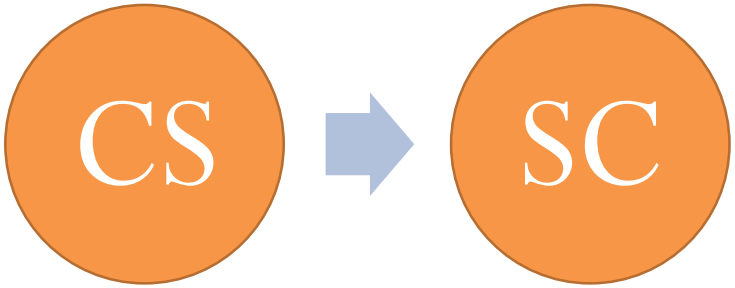
- 1970
  - Stephen Wiesner invents conjugate coding.
- 1973
  - Alexander Holevo publishes a paper showing that *n* qubits cannot carry more than *n* classical bits of information (a result known as "Holevo's theorem" or "Holevo's bound"). Charles H. Bennett shows that computation can be done reversibly.
- 1975
  - R. P. Poplavskii publishes "Thermodynamical models of information processing" (in Russian)[1] which showed the computational infeasibility of simulating quantum systems on classical computers, due to the superposition principle.
- 1976
  - Polish mathematical physicist Roman Stanisław Ingarden publishes a seminal paper entitled "Quantum Information Theory" in Reports on Mathematical Physics, vol. 10, 43–72, 1976. (The paper was submitted in 1975.) It is one of the first attempts at creating a quantum information theory, showing that Shannon information theory cannot directly be generalized to the quantum case, but rather that it is possible to construct a quantum information theory, which is a generalization of Shannon's theory, within the formalism of a generalized quantum mechanics of open systems and a generalized concept of observables (the so-called semi-observables).

1980s [edit]

- 1980
  - Yuri Manin proposed an idea of quantum computing[2]
- 1981
  - Richard Feynman in his talk (and yet also in his famous lecture,/speech "There's Plenty of Room at the Bottom", too) at the *First Conference on the Physics of Computation*, held at MIT in May, observed that it appeared to be impossible in general to simulate an evolution of a quantum system on a classical computer in an efficient way. He proposed a basic model for a quantum computer that would be capable of such simulations[3]

Изучение квантовой информатики





Квантовая информатика	Суперкомпьютеры
Квантовая физика	**Программирование**
Линейная алгеба	Алгоритмы
Алгоритмы	Математика
Математика	Вычислительные системы
Программирорвание	
Физика	
…	

Новости и слухи

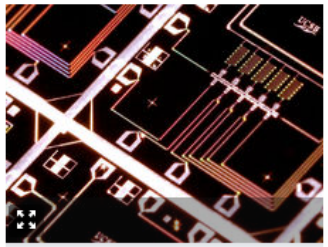


Фото:


Найден способ ускорить запуск квантовых компьютеров в 72 раза

24.06.2014 | 14:10

Автор: Ася Горина

Tweet 3 Сохранить

Я рекомендую 3 пользователя рекомендуют это. Станьте первым из своих друзей.

Главная, Новости, № 03 2014 430 прочтений

Технологии

Квантовые компьютеры готовят реванш

В этом году компания D-Wave планирует выпустить быстрый квантовый компьютер с процессором, объединяющим 1024 кубита

Агам Шах

Служба новостей IDG, Нью-Йорк

Главная » Новости » Международные деловые новости »

18.06.2014 г., 18:48 Нравится 0

Ученые рассказали, какими будут компьютеры следующего поколения

Ученые предсказывают, что вскоре на обычные компьютеры сменят квантовые.

По прогнозам экспертов уже совсем скоро, лет через 10, микросхемы в

Читайте также:

Слух, который хотелось бы опровергнуть

- Квантовые компьютеры - конкуренты суперкомпьютеров

VS.

super
computers
&
quantum
informatics

Что изучает квантовая информатика?

Очертить рамки очень сложно

- Квантовые вычисления
- Квантовая криптография
- Математическая физика квантовых систем:
  - Квантовая запутанность
  - Квантовые корреляции в целом
  - Теория многочастичной квантовой механики
  - …
- Моделирование квантовых систем
- Приложения:
  - Квантовые игры
  - Квантовая телепортация
  - …
- Квантовая теория информации (основоположник А. С. Холево)
- Экспериментальная квантовая информатика

План доклада

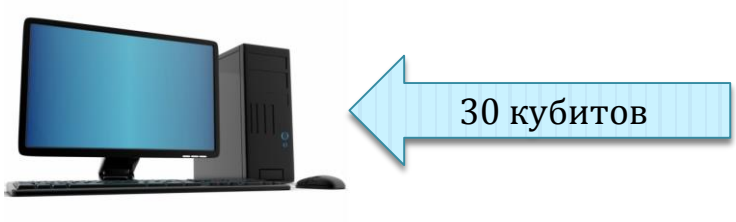
- Квантовые вычисления
  - Формализм
  - Успехи и проблемы
  - Вычислительные задачи
- Другие направления и вычислительные задачи КИ
- Квантовая запутанность

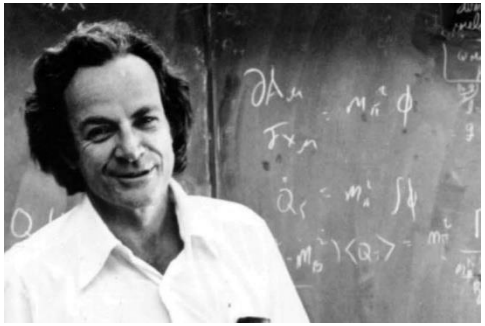
Квантовые вычисления

Основная идея

Экспоненциальный рост размерности.

Для всего лишь 50 кубитов (простейших двухуровневых квантовых систем) необходимы 18,014,398,509,481,984 байт





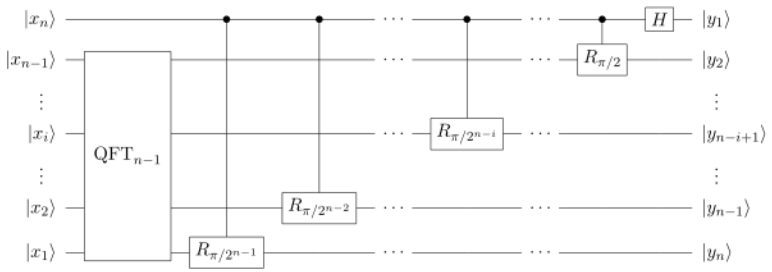
Р. Фейнман, Ю. Манин

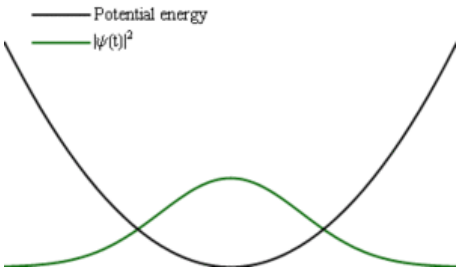
Нельзя ли использовать квантовые системы для нового типа вычислений?

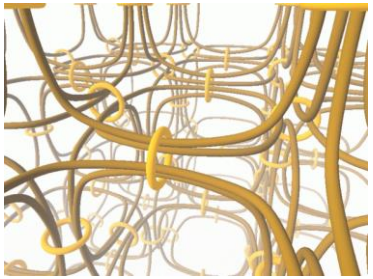
- *Feynman R.* Simulating Physics with Computers // Int. J. Theor. Phys. 1982. V.21. №6/7. P.467-488.
- *Feynman R.* Quantum Mechanical Computers // Found. of Phys. 1986. V.16. №6. P.507-531.
- *Манин Ю.И.* Вычислимое и невычислимое. М. Советское Радио. 1980. 128с.

Формализм гейтовой модели КК

Разработаны несколько моделей квантовых вычислений (гейтовая модель, адиабатические вычисления, топологические вычисления)







Формализм идеального квантового компьютера

- Аналог классического бита - кубит (qubit, q-bit, квантовый бит)

$$c_0 |0\rangle + c_1 |1\rangle \in C^2$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix};$$

- Нет доступа к амплитудам. Лишь вероятности и унитарные преобразования (повороты)

$$|c_i|^2$$

- Что будет с двумя кубитами?

Тензорное произведение

- Два кубита

$$c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \in C^2 \otimes C^2$$

- Многокубитные состояния

$$\left(C^2\right)^{\otimes n}$$

- Базисные состояния – все возможные n-битные строки

- **Размерность растет экспоненциально!**

Преобразование одного кубита

Квантовое n-кубитное состояние – комплексный вектор длины 2^n.

$$v = (a_0, a_1, \ldots, a_{2^n})^T$$

$$\Updownarrow$$

$$(a_{00\ldots0}, a_{00\ldots1}, \ldots, a_{11\ldots1})^T$$

Действуем на k-й кубит унитарной операцией $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$

$$v \to I_{k-1} \otimes U \otimes I_{n-k} \cdot v$$

$$\begin{bmatrix} a & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & b & 0 & 0 & 0 & 0 \\ c & 0 & d & 0 & 0 & 0 & 0 & 0 \\ 0 & c & 0 & d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & b \\ 0 & 0 & 0 & 0 & c & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & c & 0 & d \end{bmatrix}$$

Альтернативные представления

Матричная форма

$$A = \begin{pmatrix} a_{00\ldots0_k\ldots0} & a_{00\ldots0_k\ldots1} & \cdots & a_{11\ldots0_k\ldots1} \\ a_{00\ldots1_k\ldots0} & a_{00\ldots1_k\ldots1} & \cdots & a_{11\ldots1_k\ldots1} \end{pmatrix}^T$$

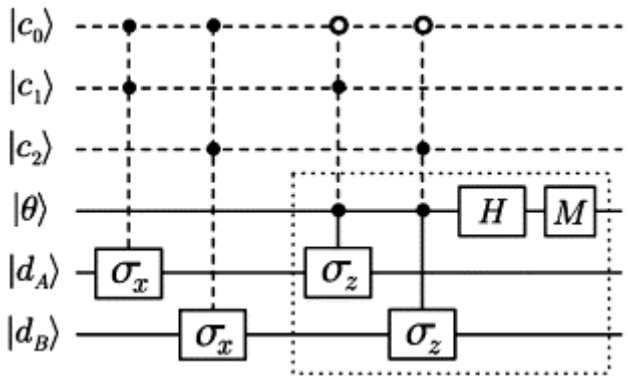
$$A \to UA$$

Прямая формула

$$b_{i_1\ldots i_k\ldots i_n} = u_{i_k 0} \cdot a_{i_1\ldots 0\ldots i_n} + u_{i_k 1} \cdot a_{i_1\ldots 1\ldots i_n}$$

Гейтовая модель

- Квантовый алгоритм задается схемой (возможно, зависящей от входных данных)



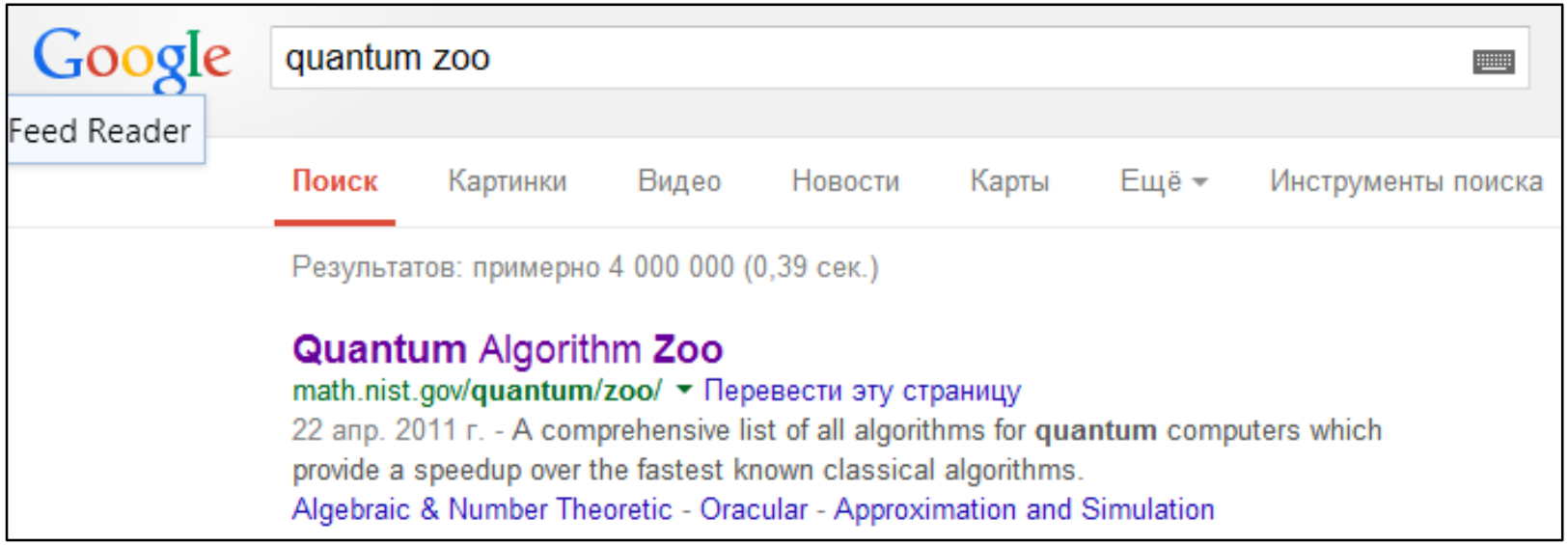
- Таким образом вычисление – список малокубитных операций
- Необходимо максимизировать вероятность правильного ответа.
- Любая классическая схема может быть превращена в обратимую и представлена квантовой
- Достаточно одно- и двухкубитных операций

Где «спрятана» вычислительная мощь?

- Даже при однокубитной операции меняются ВСЕ амплитуды.
- Экспоненциальный параллелизм.
- Набор операций сильно ограничен.
- Каждый новый алгоритм – «произведение искусства».



Для чего хорош квантовый компьютер?



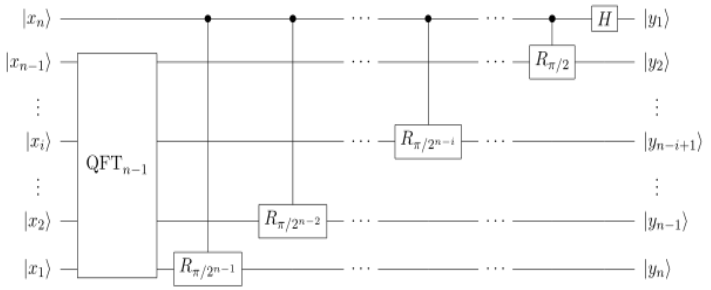
Алгоритм Шора (1994)

- Алгоритм разложения числе на простые множители

$$L_{clas} \approx \exp\left((64/9)^{1/3} n^{1/3} (\ln(n))^{2/3}\right)$$

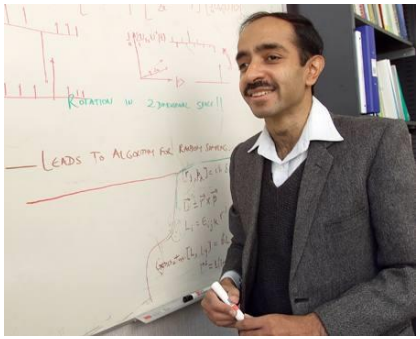
$$L_{quant} \approx n^2 \ln(n) \ln(\ln(n))$$

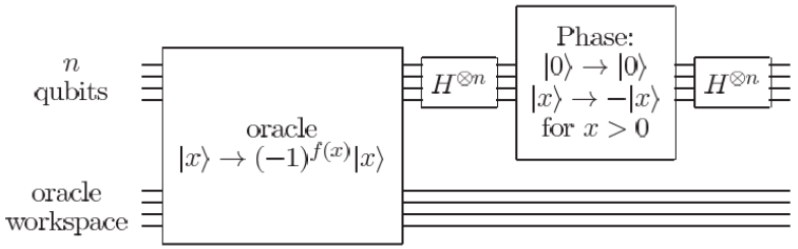
Классический компьютер петафлопсного диапазона (10^{15} оп/сек) против квантового компьютера Мегагерцового диапазона (1 млн. оп/сек)			
Число десятичных знаков k	k=250	k=500	k=1000
Трудоемкость классического алгоритма (лет)	22 года	5 миллиардов лет	$4 \cdot 10^{20}$ лет
Трудоёмкость квантового алгоритма (сек)	4 сек	18 сек	84 сек



Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE, 1994.

Алгоритм Гровера (1996)





- Решает переборные задачи с квадратичным ускорением.
- Для классического компьютера (нельзя ускорить) $O(N)$
- Алгоритм Гровера $O(\sqrt{N})$

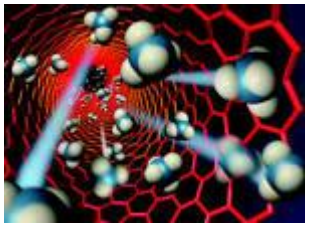
Grover, Lov K. "A fast quantum mechanical algorithm for database search."*Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM, 1996.

Моделирование квантовых систем

- На квантовом компьютере возможно полноценное моделирование произвольных квантовых систем

- При успешном его создании некоторые области науки и технологий выйдут на совершенно новый уровень:
  - Химия
  - Нанотехнологии
  - Фармакология и медицина в целом
  - …



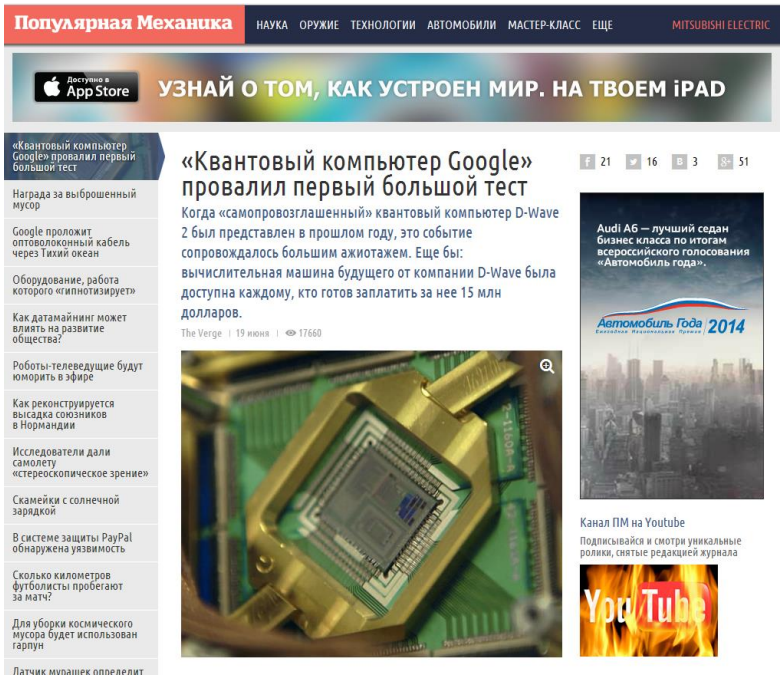



Как обстоят дела с реализацией квантового компьютера?

Полноценный квантовый компьютер не создан

Но что же уже есть?

Компания D-Wave



- Компьютер компании D-Wave не является универсальным квантовым компьютером, а осуществляет квантовый отжиг
- Доказано наличие квантовых эффектов
- Не доказано ускорение

Перспективные технологии

- Квантовые точки
- Ионы в ловушке
- Фотоны
- Сверхпроводниковые кубиты
- NV-центры в алмазах
- и др.

Препятствия на пути реализации

Технологии изготовления не отвечают необходимым требованиям

Трудности в измерении и контроле

Трудности в подавлении декогерентизации

Не удается достичь необходимой точности выполнения операций

Экспериментальные успехи

Timeline [edit]

In 2001, researchers were able to demonstrate Shor's algorithm to factor the number 15 using a 7-qubit NMR computer.[38]

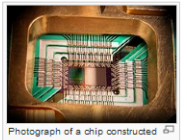
In 2005, researchers at the University of Michigan built a semiconductor chip that functioned as an ion trap. Such devices, produced by standard lithography techniques, may point the way to scalable quantum computing tools.[39] An improved version was made in 2006.[*citation needed*]

In 2009, researchers at Yale University created the first rudimentary solid-state quantum processor. The two-qubit superconducting chip was able to run elementary algorithms. Each of the two artificial atoms (or qubits) were made up of a billion aluminum atoms but they acted like a single one that could occupy two different energy states.[40][41]

Another team, working at the University of Bristol, also created a silicon-based quantum computing chip, based on quantum optics. The team was able to run Shor's algorithm on the chip.[42] Further developments were made in 2010.[43] Springer publishes a journal ("Quantum Information Processing") devoted to the subject.[44]

In April 2011, a team of scientists from Australia and Japan made a breakthrough in quantum teleportation. They successfully transferred a complex set of quantum data with full transmission integrity achieved. Also the qubits being destroyed in one place but instantaneously resurrected in another, without affecting their superpositions.[45][46]

In 2011, D-Wave Systems announced the first commercial quantum annealer on the market by the name D-Wave One. The company claims this system uses a 128 qubit processor chipset.[47] On May 25, 2011 D-Wave announced that Lockheed Martin Corporation entered into an agreement to purchase a D-Wave One system.[48] Lockheed Martin and the University of Southern California (USC) reached an agreement to house the D-Wave One Adiabatic Quantum Computer at the newly formed USC Lockheed Martin Quantum Computing Center, part of USC's Information Sciences Institute campus in Marina del Rey.[49] D-Wave's engineers use an empirical approach when designing their quantum chips, focusing on whether the chips are able to solve particular problems rather than designing based on a thorough understanding of the quantum principles involved. This approach was liked by investors more than by some academic critics, who said that D-Wave had not yet sufficiently demonstrated that they really had a quantum computer. Such criticism softened once D-Wave published a paper in Nature giving details, which critics said proved that the company's chips did have some of the quantum mechanical properties needed for quantum computing.[50][51]



Photograph of a chip constructed by D-Wave Systems Inc., mounted and wire-bonded in a sample holder. The D-Wave processor is designed to use 128 superconducting logic elements that exhibit controllable and tunable coupling to perform operations.

During the same year, researchers working at the University of Bristol created an all-bulk optics system able to run an iterative version of Shor's algorithm. They successfully factored 21.[52]

In September 2011 researchers also proved that a quantum computer can be made with a Von Neumann architecture (separation of RAM).[53]

In November 2011 researchers factorized 143 using 4 qubits.[54]

In February 2012 IBM scientists said that they had made several breakthroughs in quantum computing with superconducting integrated circuits that put them "on the cusp of building systems that will take computing to a whole new level."[55]

In April 2012 a multinational team of researchers from the University of Southern California, Delft University of Technology, the Iowa State University of Science and Technology, and the University of California, Santa Barbara, constructed a two-qubit quantum computer on a crystal of diamond doped with some manner of impurity, that can easily be scaled up in size and functionality at room temperature. Two logical qubit directions of electron spin and nitrogen kernels spin were used. A system which formed an impulse of microwave radiation of certain duration and the form was developed for maintenance of protection against decoherence. By means of this computer Grover's algorithm for four variants of search has generated the right answer from the first try in 95% of cases.[56]

In September 2012, Australian researchers at the University of New South Wales said the world's first quantum computer was just 5 to 10 years away, after announcing a global breakthrough enabling manufacture of its memory building blocks. A research team led by Australian engineers created the first working "quantum bit" based on a single atom in silicon, invoking the same technological platform that forms the building blocks of modern day computers, laptops and phones.[57] [58]

In October 2012, Nobel Prizes were presented to David J. Wineland and Serge Haroche for their basic work on understanding the quantum world—work which may eventually help make quantum computing possible.[59][60]

In November 2012, the first quantum teleportation from one macroscopic object to another was reported.[61][62]

In December 2012, the first dedicated quantum computing software company, 1QBit was founded in Vancouver, BC.[63] 1QBit is the first company to focus exclusively on commercializing software applications for commercially available quantum computers, including the D-Wave Two processor. 1QBit's research demonstrated the ability of superconducting quantum annealing processors to solve real-world problems.[64]

In February 2013, a new technique, boson sampling, was reported by two groups using photons in an optical lattice that is not a universal quantum computer but which may be good enough for practical problems. *Science* Feb 15, 2013

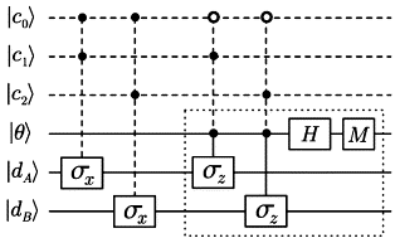
In May 2013, Google Inc announced that it was launching the Quantum Artificial Intelligence Lab, to be hosted by NASA's Ames Research Center. The lab will house a 512-qubit quantum computer from D-Wave Systems, and the USRA (Universities Space Research Association) will invite researchers from around the world to share time on it. The goal is to study how quantum computing might advance machine learning.[65]

In early 2014 it was reported, based on documents provided by former NSA contractor Edward Snowden, that the U.S. National Security Agency (NSA) is running a $79.7 million research program (titled "Penetrating Hard Targets") with the aim of developing a quantum computer capable of breaking encryption vulnerable to quantum computers.[66] The same year, a group of researchers from ETH Zürich, USC, Google, Microsoft published a report how to define quantum speedup, and reported that they were not able to measure quantum speedup with the D-Wave Two device. But, they did explicitly not rule out that quantum speedups might be possible and might depend on the question posed.[67][68]

- 2001 г. Продемонстрированы 7 кубитов на технологии ЯМР
- 2011 г. Продемонстрированы 4 кубита (разложили число 143)
- Интересны результаты с оптическими квантовыми компьютерами (разложены числа 15, 21)

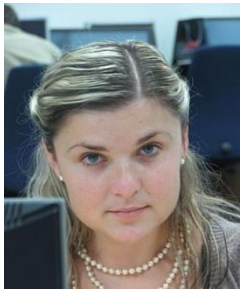
Некоторые ресурсоемкие вычислительные задачи на пути построения КК

Моделирование идеальных квантовых алгоритмов



super computers & quantum informatics

Коробков С.В.



Корж О.В.

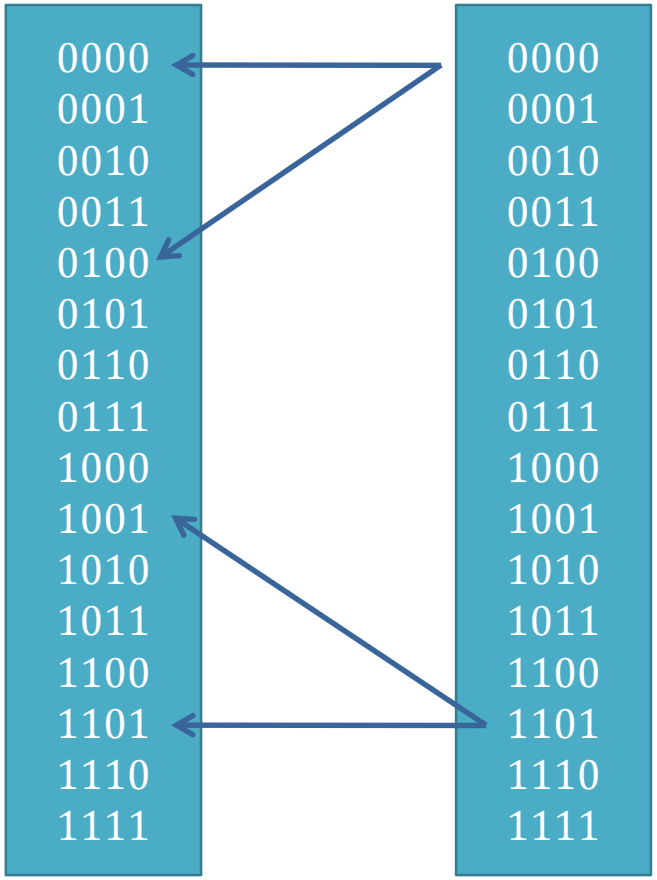
Андреев Д.Ю.

Персональные компьютеры: ~ 30 кубитов

Рекорд: 42 кубит (Julich), суперкомпьютер Jugene

Вычислительные трудности

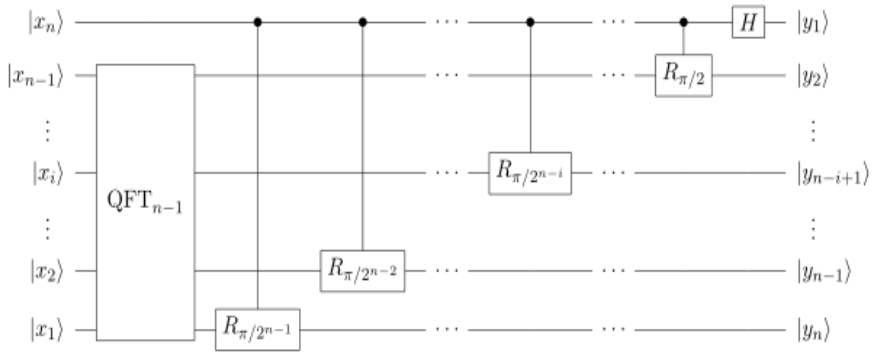
- Основная проблема распараллеливания – зависимость по памяти.



Суперкомпьютер «Ломоносов»

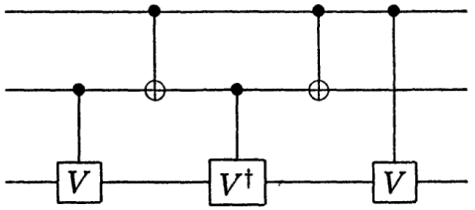
- Мощность 1,37 Пфлоп/с
- 252 квадратных метра
- 2,8 МВт
- Использовались 512 узлов: Intel® Xeon 5670 Westmere, 24ГБ
- В силу технических трудностей использовались не все мощности.

Квантовое преобразование Фурье



Алгоритм Гровера

В качестве поворота относительно $|\tilde{0}\rangle$ использовалась простейшая схема с элементами Тоффоли и анциллами



Реализация

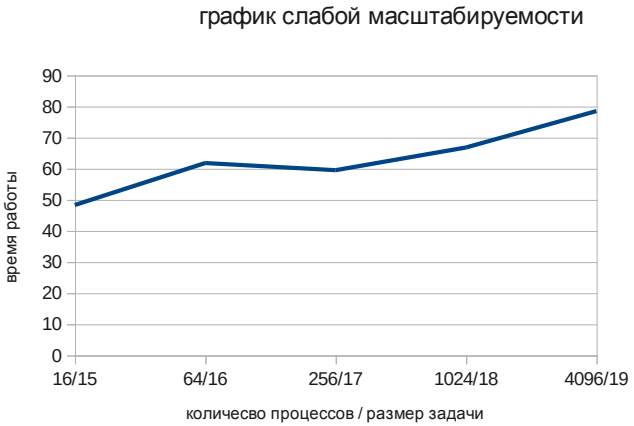
- Стандартный подход – MPI (Message Passing Interface).
  - Не подходит в силу зависимости данных

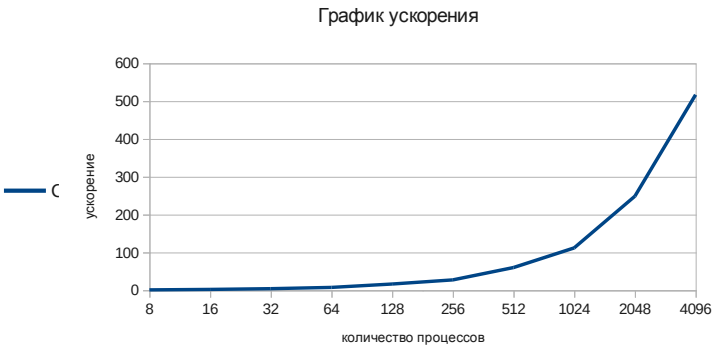
- Использовался DISLIB (library to scale Data-Intensive applications on petascale systems).

Трудности использования суперкомпьютеров

- На данный момент суперкомпьютеры схожи с компьютерами времен перфокарт.
  - Необходимость регистрации и т.п.
  - Регулярные технические проблемы
    - Профилактические закрытия и выходы из строя суперкомпьютеров
    - не удалось использовать все узлы
    - решение ошибки настроек профиля МВС-100К заняло 2 дня.
  - Отсутствие современных сред разработки, отладки и т.п.
  - Постоянно меняющиеся подходы, парадигмы. Отсутствие стандартов.
  - Даже стандартные пакеты крайне сложны к освоению и нестабильны.
  - За рубежом уже стали учитывать затраты на разработку при оценке высокопроизводительных систем.
- Вывод: пока разумнее сотрудничать с суперкомпьютерными специалистами, особенно для решения нестандартных задач.
- Перечисленные проблемы временные.

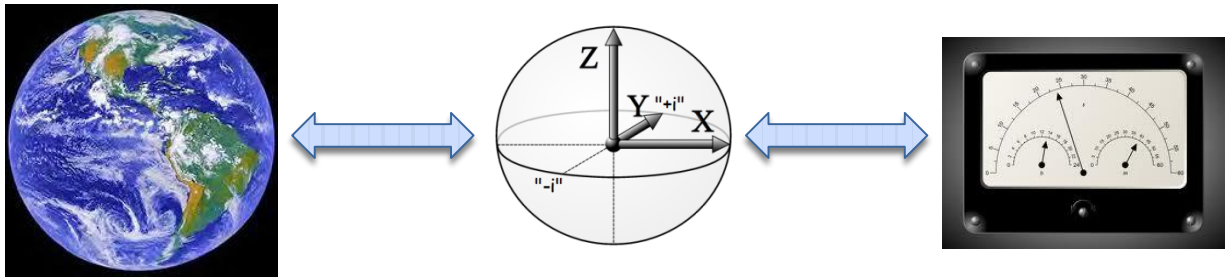
Результаты



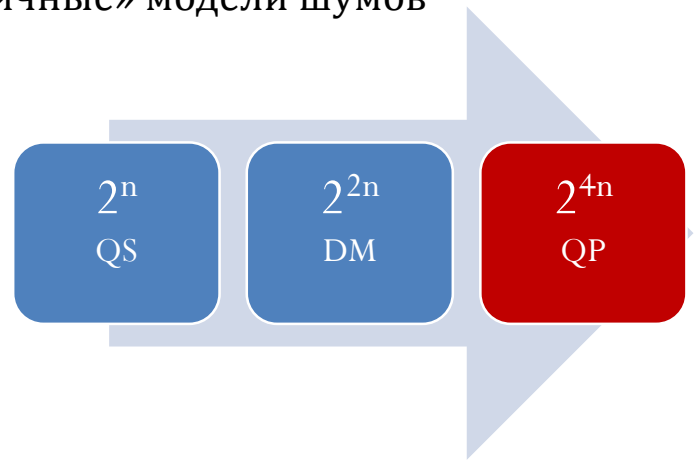


- Удалось избежать проблем с памятью
- Реализована работа с 39 кубитами
- Время одной однокубитной операции для 38 кубитов ~2 сек.

Моделирование зашумленных квантовых алгоритмов



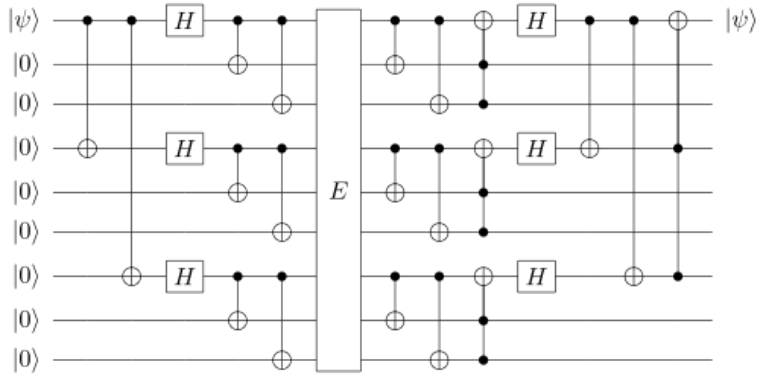
- Квантовые шумы – главное препятствие на пути создания КК
- Оставаясь в рамках описанного формализма, можно учитывать только простые «нефизичные» модели шумов



- Имеется реализация для МВС-100К, МВС-10П, “Ломоносов”
- Используется Dislib, и собственная библиотека SHMEM и активных сообщений

Без чего были бы невозможны успешные цифровые технологии?

Коды коррекции квантовых ошибок

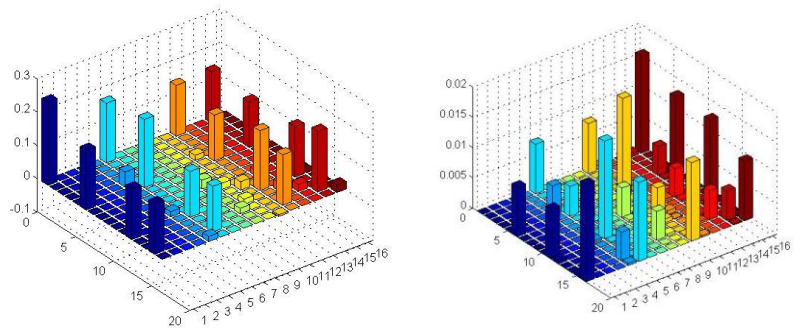


- Без ECC вычисления невозможны
- QECC дают надежды на создание КК
- “Квантовая магия”:
  - Континуум ошибок
  - Состояния неизвестно
  - Коды всё равно работают!
  - Мы «портим» состояние, чтобы его исправить

Квантовая томография

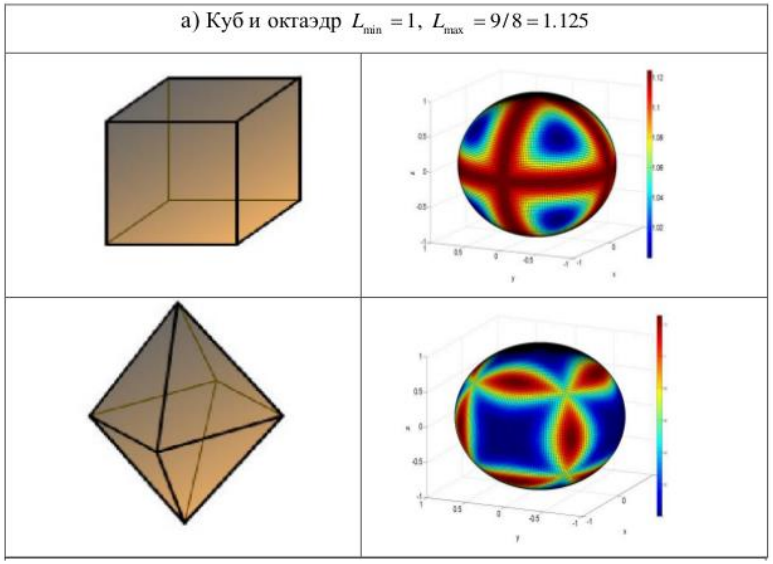
Мы не можем получить доступ к амплитудам квантового состояния, как же тогда узнавать результаты эксперимента?

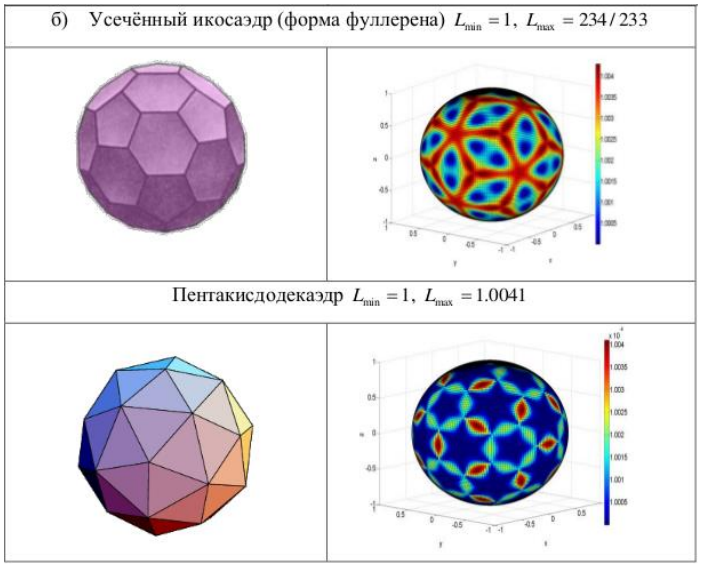
Квантовая томография



- Задача восстановления значения амплитуд состояния по измерению множества его копий
- Критически необходима для экспериментов
- Измерения производятся в различных базисах, поэтому возможно полное восстановление
- Даже для малого числа кубитов (например, 5) задача ресурсоемкая

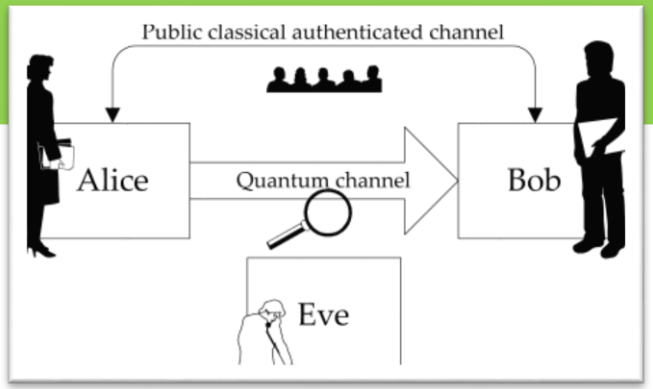
Пример (использован МВС-100К)





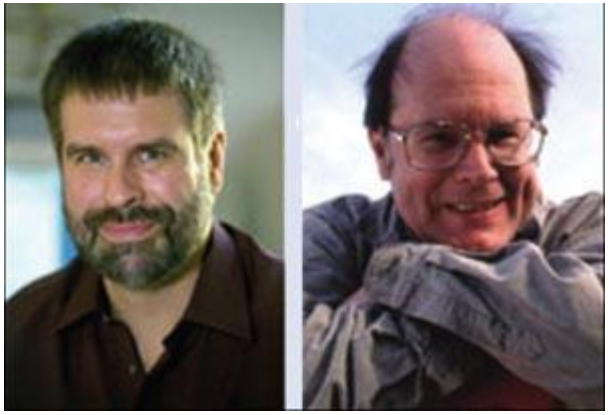
	1 кубит	2 кубита	3 кубита	4 кубита
Тетраэдр ($m = 4$)	$3/2 = 1.5$	4.442971458	≈ 10.4	≈ 18.1
Куб ($m = 6$)	$9/8 = 1.125$	≈ 3.5839	≈ 8.2	≈ 16.5
Октаэдр ($m = 8$)	$9/8 = 1.125$	≈ 3.4867	≈ 7.9	≈ 16.3
Додекаэдр ($m = 12$)	$36/35$	≈ 3.42	≈ 7.8	≈ 16.2
Икосаэдр ($m = 20$)	$45/44$	≈ 3.39	≈ 7.8	≈ 16.2
Фуллерен ($m = 32$) (усечённый икосаэдр)	$\approx 234/233$	≈ 3.38	≈ 7.7	≈ 16.1

Квантовая криптография



- Квантовые состояния невозможно скопировать
- Снова ограничения привели к полезному использованию

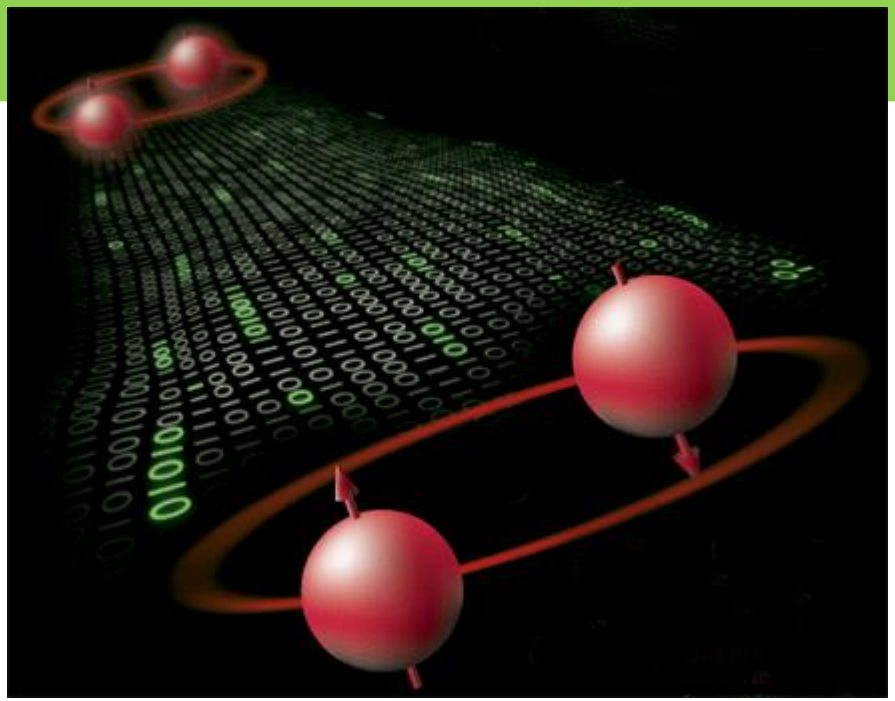
BB84



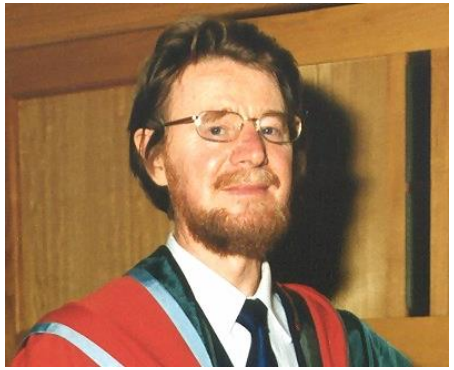
- В отличии от классической криптографии протокол основан на законах природы
- Созданы множество протоколов
- Существуют коммерческие реализации

Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Vol. 175. No. 0. 1984.

Квантовая запутанность

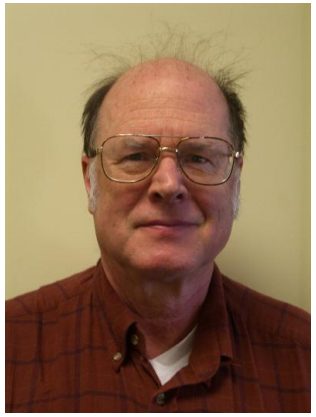


Что такое запутанность?

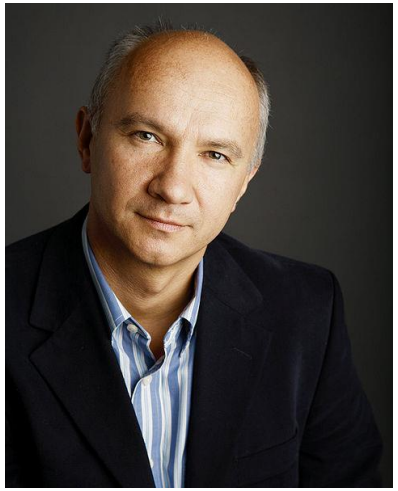


Дж. Белл: «Квантовая запутанность - это корреляция, которая сильнее любой классической корреляции.»

А. Перес: «Квантовая запутанность - это трюк, используемый квантовыми волшебниками для создания феноменов, которые не могут повторить классические волшебники.»



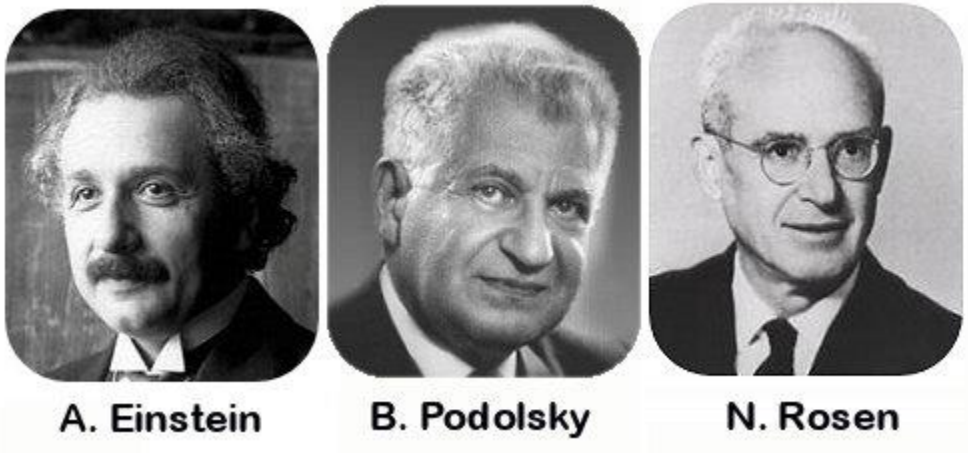
Ч. Беннет: «Квантовая запутанность - это ресурс, делающий возможным квантовую телепортацию.»



А. Экерт: «Квантовая запутанность - это инструмент для защищенной связи.»

П. Шор: «Квантовая запутанность - это глобальная структура волновой функции, разрешающая быстрые алгоритмы.»

Семья Городецки: «Квантовая запутанность - это необходимость впервые применить положительные отображения в физике.»



Э. Шредингер: Для запутанного состояния «наилучшее возможное знание всего не включает наилучшее возможное знание частей».

Die gegenwärtige Situation in der Quantenmechanik / E. Schrödinger // *Naturwissenschaften.— 1935.— Vol. 23, no. 49.—* Pp. 823–828.

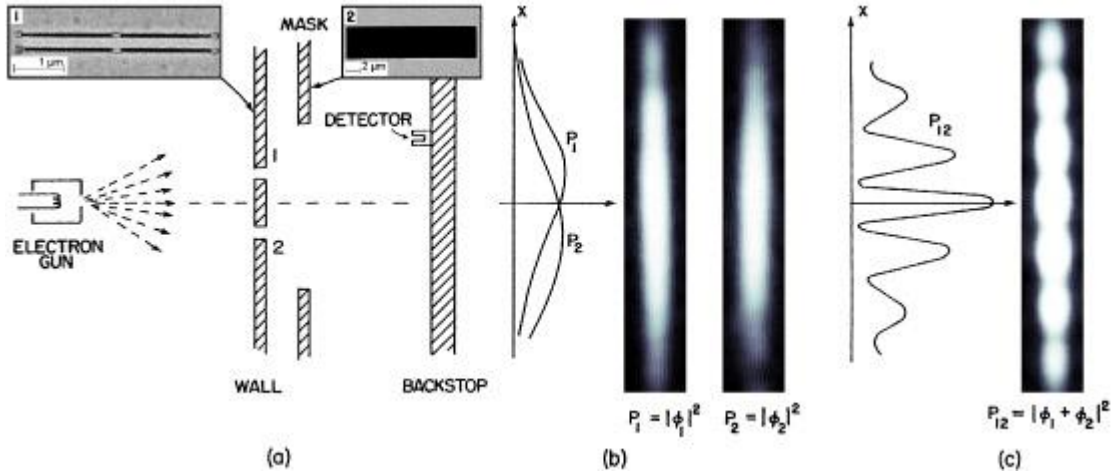
Эйнштейн/Подольский/Розен: «Запутанная волновая функция не описывает физическую реальность в полной мере.»

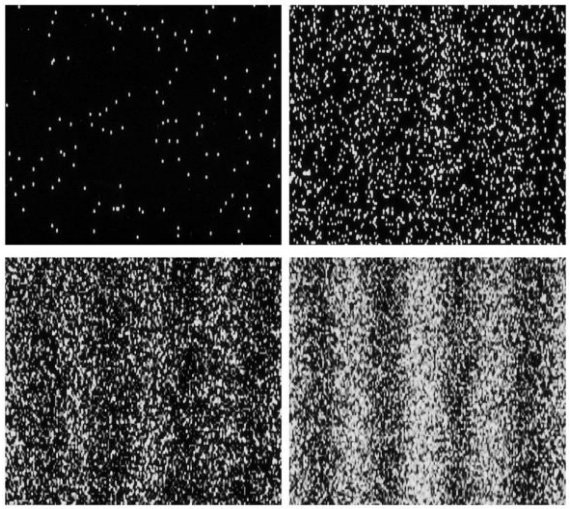
Can quantum-mechanical description of physical reality be considered complete? / A. Einstein, B. Podolsky, N. Rosen et al. // *Physical review.—* 1935.— Vol. 47, no. 10.— Pp. 777–780.

Verschränkung
1935

Основы квантовой запутанности

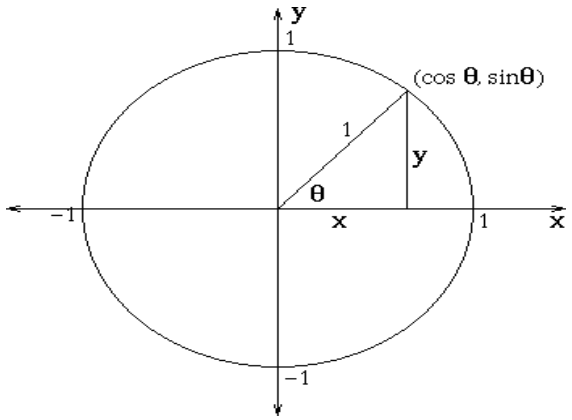
Двухщелевой эксперимент





Амплитуды вероятности!

Квантовая суперпозиция

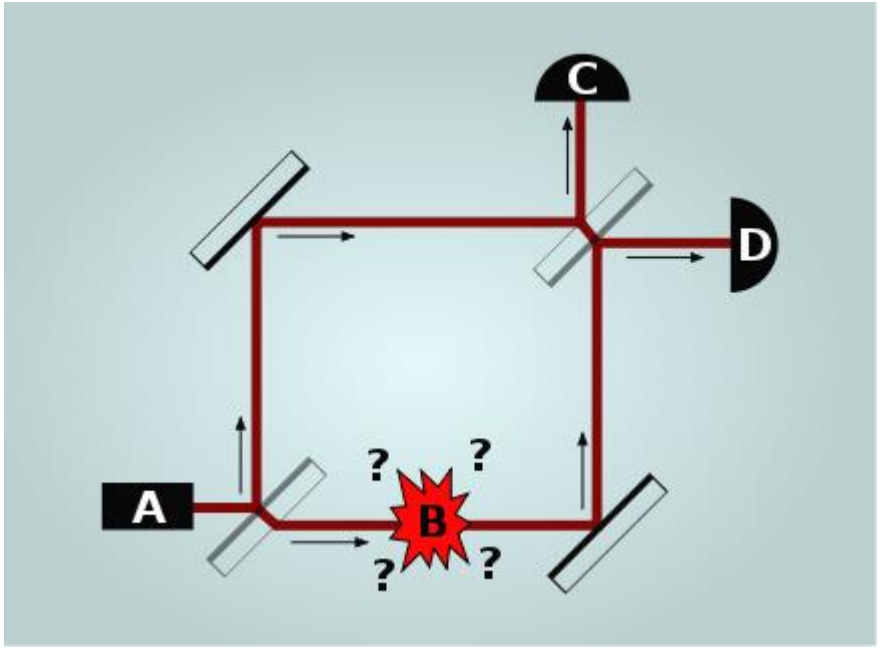


$$c_0 |0\rangle + c_1 |1\rangle$$

$$|c_i|^2$$

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

Задача Элицура-Вайдмана (1993)

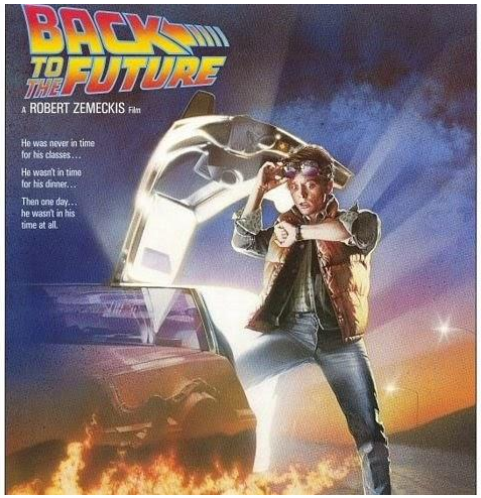


Эксперимент: P. G. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich (1994-95)

Можно ли узнать информацию быстрее скорости света?

- Информация не может быть передана быстрее скорости света

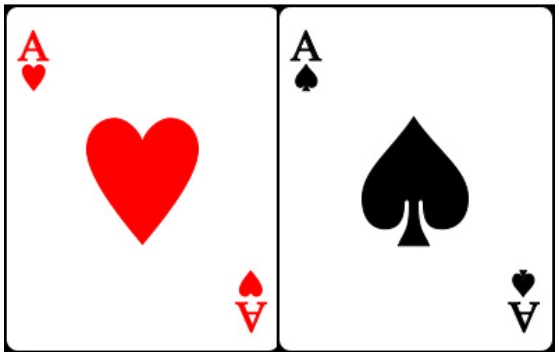
- Если нарушить этот запрет, станет возможно отправлять послания в прошлое!



Можно ли узнать информацию быстрее скорости света?

Мгновенно узнать информацию можно!

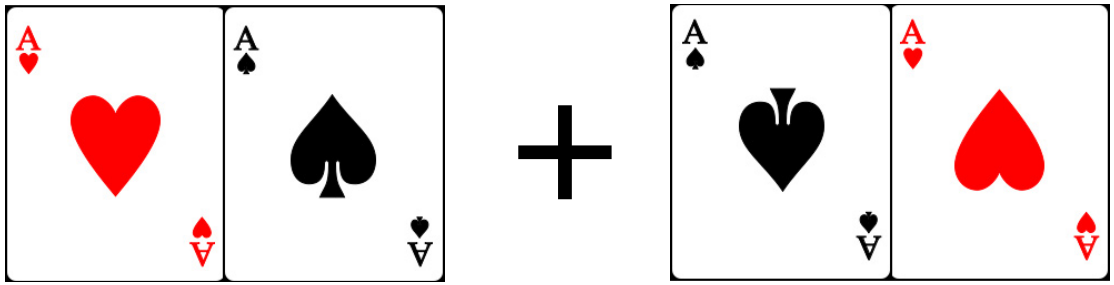
- Представим эксперимент с двумя игральными картами (одна красная, одна черная):
  - Карты перемешиваются, чтобы никто не знал из расположение
  - Алиса берет вслепую одну карту, Боб другую.
  - Находясь на произвольном расстоянии, Алиса может узнать карту Боба, открыв свою.



Переход к запутанности

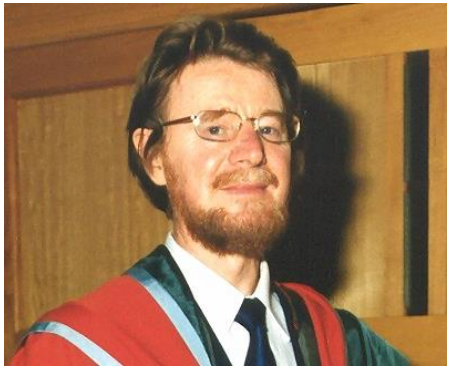
- Мы предположили, что не знаем расположение карт (естественно, никакой квантовой запутанности в нашем эксперименте нет).

- Квантовая механика (принцип суперпозиции) позволяет выполнить это предположение на физическом уровне!



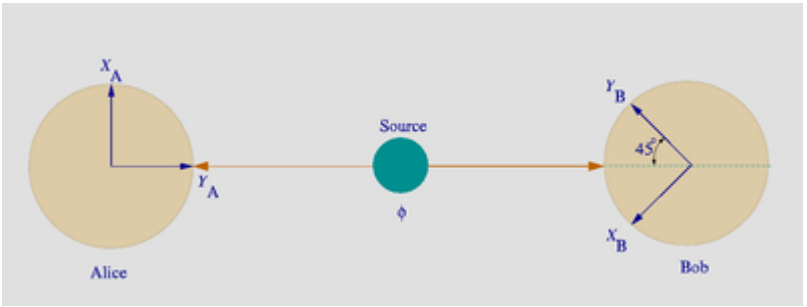
Экспериментальное наблюдение запутанности

Неравенства Белла (1964)



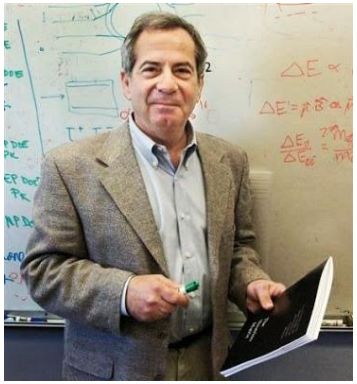
Дж. Белл: «Квантовая запутанность - это корреляция, которая сильнее любой классической корреляции.»

CHSH John Clauser, Michael Horne, Abner Shimony and Richard Holt



$$\langle A(a)B(b)\rangle + \langle A(a')B(b')\rangle + \langle A(a')B(b)\rangle - \langle A(a)B(b')\rangle = \frac{4}{\sqrt{2}} = 2\sqrt{2} > 2$$

Эксперименты по нарушению неравенств Белла



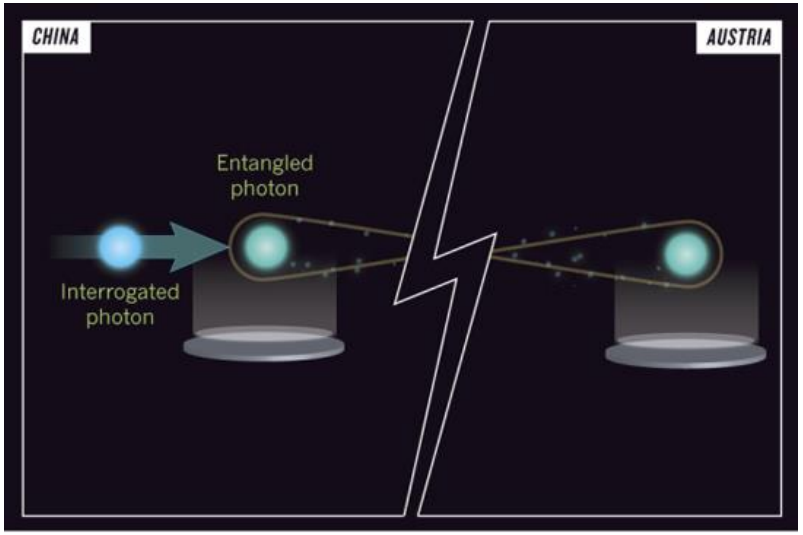
Freedman and Clauser, 1972

Alain Aspect, 1981-82

2003, violating on mesons

Использование квантовой запутанности

Квантовая телепортация



- Передается неизвестное квантовое состояние.
- Использует запутанное состояние
- Необходима передача классической информации.

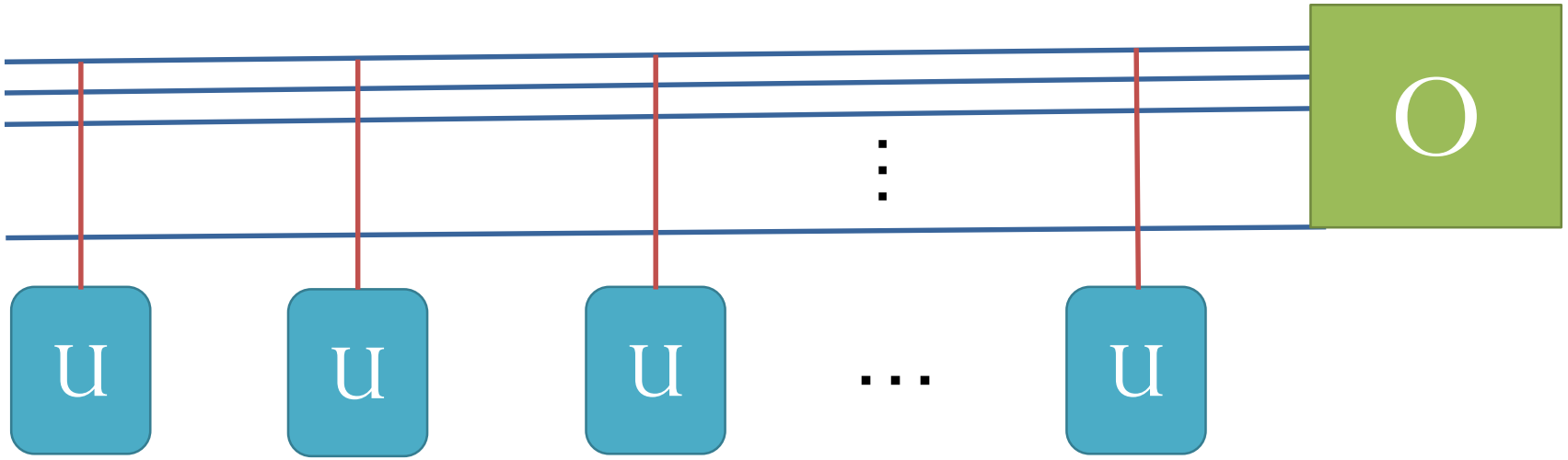
Игры

+1	-1	+1
-1	-1	+1
+1	-1	-1

- Алиса и Боб против судьи. Никаких средств связи.
- Алиса заполняет строки, Боб столбцы
- Судья выбирает произвольно строку и столбец
- А. и Б. выигрывают, если числа совпадут
- Можно ли выиграть?

- Использование запутанных состояний позволяет выиграть!!!

Улучшение вычислительных коммуникаций



Необходимо посчитать сумму битов: 10101 -> 11

Научные задачи

- Генерация и детектирование запутанности
- Структура запутанности
  - Определение, геометрия, …
  - Меры запутанности
    - Детектирование
    - Монотонность
    - Аддитивность

- Применение запутанности
- Роль запутанности в физических и биологических явлениях

Вычисления

- Отличить запутанное состояние от незапутанного – NP-сложная задача
- Вычисление мер запутанности почти всегда требует глобальной оптимизации многопараметрических функций
  - Используются современные методы оптимизации (эволюционные алгоритмы, выпуклая оптимизация)
  - Очень сложные задачи с вычислительной точки зрения
  - Используются суперкомпьютеры, GPU
- Вычисление мер квантовых корреляций важно для анализа:
  - квантовых алгоритмов
  - кодов коррекции ошибок,
  - экспериментальных данных

Выводы

- Квантовая компьютер – не является конкурентом суперкомпьютера, однако, его создание позволит решать многие важные задачи, недоступные классическим вычислительным устройствам

- Квантовая информатика критически нуждается в современных суперкомпьютерных вычислениях

- Вычислительные задачи КИ сложны и интересны с точки зрения высокопроизводительных вычислений
  - Для «простых» пользователей суперкомпьютеров пока имеются определенные трудности