Al Aho
aho@cs.columbia.edu

Компиляторы для квантовых компьютеров

COMPUTER SCIENCE AT
COLUMBIA UNIVERSITY

KAUST
27 февраля 2011 г.

Квантовые компьютеры: взгляд разработчика компиляторов

1. Откуда воодушевление насчет квантовых компьютеров?
2. Вычислительная модель для квантового программирования
3. Потенциальные технологии целевой машины
4. Языки квантового программирования
5. Нерешенные проблемы в построении квантовых компьютеров

Что говорят физики

«Квантовая информация – это радикальный скачок в области информационных технологий, отличающаяся от современных технологий более глубоко, чем цифровой компьютер – от абака.»

William D. Phillips, лауреат Нобелевской премии в области физики 1997 г.

Алгоритм Шора факторизации целого числа

Задача: Дано составное *n*-битное число, найти нетривиальный множитель.

Наилучший известный детерминистический алгоритм на классическом компьютере имеет вычислительную сложность $\exp(O(n^{1/3} \log^{2/3} n))$.

Квантовый компьютер способен решить эту задачу за $O(n^3)$ операций.

Peter Shor

Algorithms for Quantum Computation: Discrete Logarithms and Factoring
***Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134**

Факторизация целого числа: оценка времени

Классический алгоритм: просеивание по числовым полям

- Вычислительная сложность: $\exp(O(n^{1/3} \log^{2/3} n))$
- Время для 512-битового числа: 8400 MIPS лет
- Время для 1024-битового числа: в 1.6 миллиардов раз дольше

Квантовый алгоритм: алгоритм Шора

- Вычислительная сложность: $O(n^3)$
- Время для 512-битового числа: 3,5 часа
- Время для 1024-битового числа: 31 час
  (для квантового прибора 1 GHz)

M. Oskin, F. Chong, I. Chuang
A Practical Architecture for Reliable Quantum Computers
***IEEE Computer*, 2002, pp. 79-87**

На пути к вычислительной модели языков квантового программирования

Физические основания квантовых вычислений

Четыре постулата квантовой механики

М. Нильсен, И. Чанг
Квантовые вычисления и квантовая информация
М.: «Мир», 2006

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

Пространство состояний

Постулат 1

Состояние изолированной квантовой системы описывается единичным вектором комплексного гильбертова пространства.

Кубит: квантовый бит

- **Состояние квантового бита в 2-мерном комплексном гильбертовом пространстве описывается единичным вектором (в обозначениях Дирака)**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

где α и β — комплексные коэффициенты, называемые амплитудами базисных состояний |0i и |1i и

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

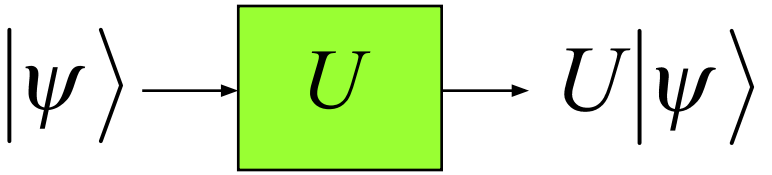
- **В привычных алгебраических обозначениях**

$$\begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Эволюция

Постулат 2

Эволюция замкнутой квантовой системы описывается унитарным оператором U.
(Оператор U унитарный, если $U^{\dagger} = U^{-1}$.)



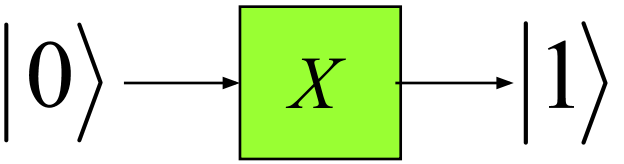
состояние системы в момент времени t_1

состояние системы в момент времени t_2

Полезные квантовые операторы: операторы Паули

Операторы Паули

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



В привычной линейной алгебре эквивалентно $X|0\rangle = |1\rangle$

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

Полезные квантовые операторы: оператор Адамара

Матричное представление оператора Адамара:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Действие H на состояния вычислительного базиса:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Заметим, что $HH = I$.

Составные системы

Постулат 3

Пространство состояний составной системы представляет собой тензорное произведение пространств состояний входящих в нее систем.

Если одна система находится в состоянии $|\psi_1\rangle$ а другая система – в состоянии $|\psi_2\rangle$, то составная система находится в состоянии $|\psi_1\rangle \otimes |\psi_2\rangle$.

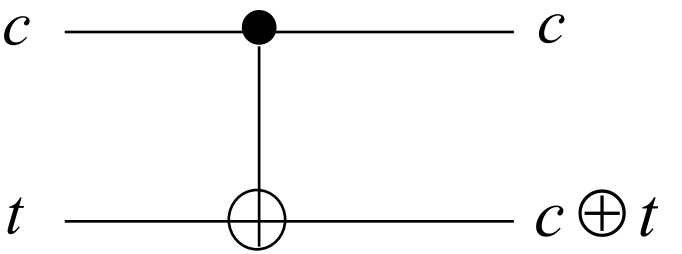
Вместо $|\psi_1\rangle \otimes |\psi_2\rangle$ часто пишут $|\psi_1\rangle|\psi_2\rangle$ или $|\psi_1\psi_2\rangle$.

Полезные квантовые операторы: оператор CNOT

Двухкубитовый оператор CNOT (управляемое NOT):

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

CNOT переворачивает управляемый бит t тттк управляющий бит c принимает значение 1:



Действие элемента CNOT

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle$$

Квантовые измерения

Постулат 4

Квантовые измерения описываются набором операторов $\{M_m\}$, действующих на пространстве состояний системы. Если состояние системы до измерения – $|\psi\rangle$, то вероятность получения результата m составляет

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

а состояние системы после измерения –

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

Квантовые измерения

Операторы измерения удовлетворяют уравнению полноты:

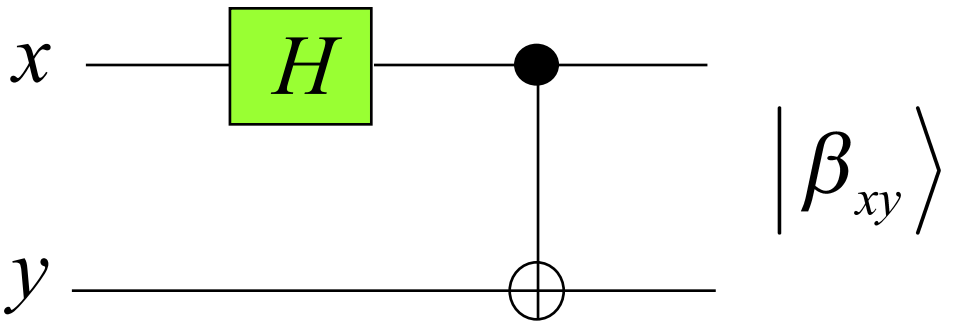
$$\sum_m M_m^\dagger M_m = I$$

Уравнение полноты говорит о том, что сумма вероятностей равна единице:

$$\sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M | \psi \rangle = 1$$

Квантовые схемы: модель квантовых вычислений

Квантовая схема для создания состояний Белла (Эйнштейна-Подольского-Розена):



Действие схемы:

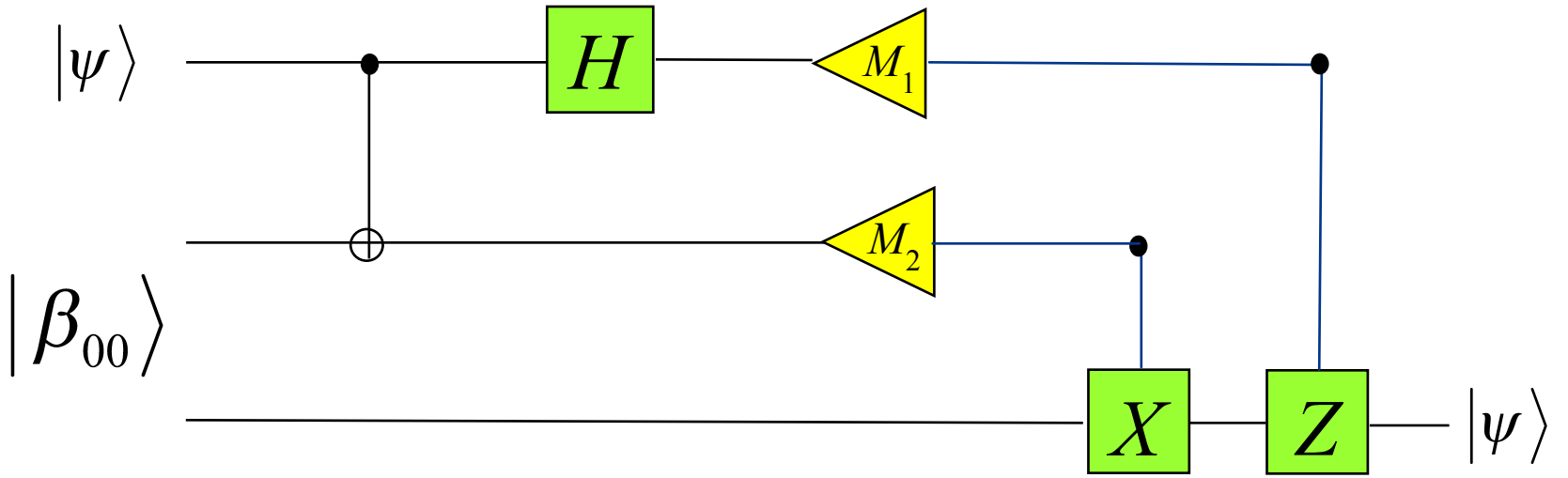
$$|00\rangle \to \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}, |01\rangle \to \frac{(|01\rangle+|10\rangle)}{\sqrt{2}}, |10\rangle \to \frac{(|00\rangle-|11\rangle)}{\sqrt{2}}, |11\rangle \to \frac{(|01\rangle-|10\rangle)}{\sqrt{2}}$$

Каждый результат – запутанное состояние, которое не может быть представлено в виде произведения.
(Эйнштейн: «Пугающее действие на расстоянии.»)

Задача доставки состояния кубита Алисы и Боба

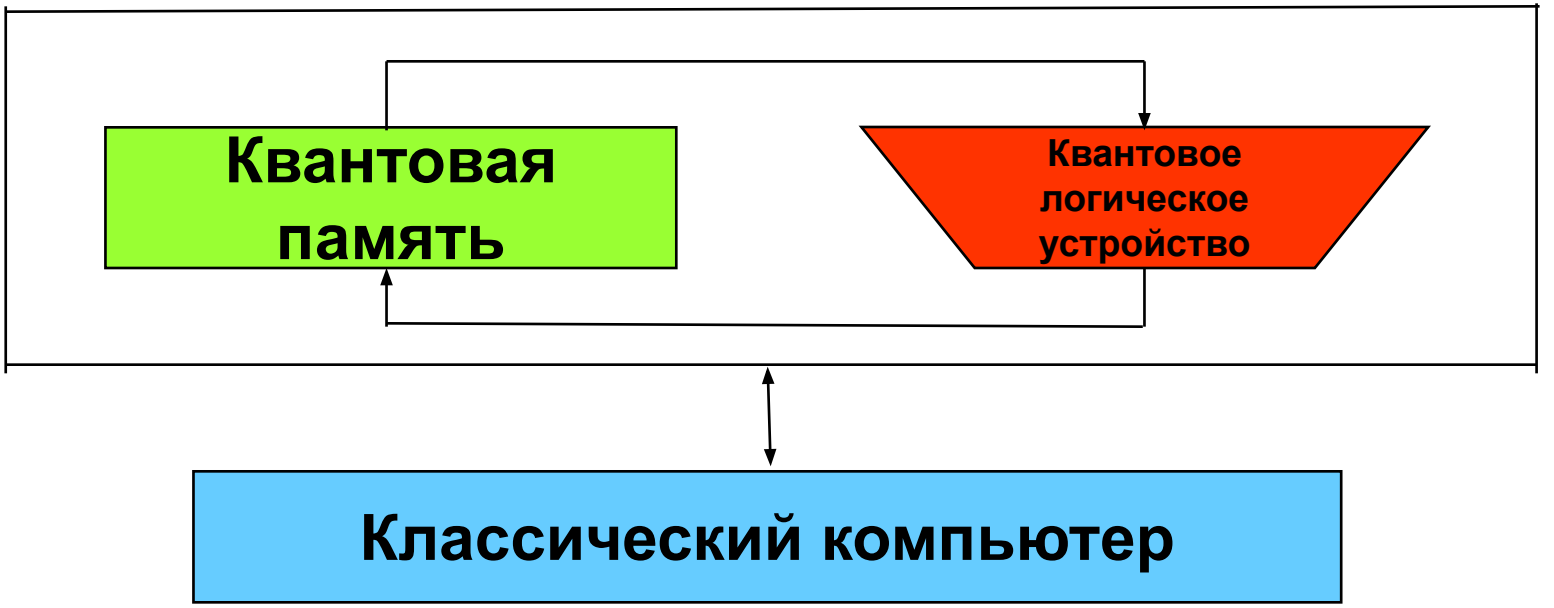
- **Алиса знает, что в будущем ей потребуется послать Бобу состояние важного секретного кубита.**
- **Ее друг Боб уезжает далеко, и у него будет очень узкополосное интернет-соединение.**
- **Таким образом, Алисе потребуется послать состояние ее кубита Бобу как можно дешевле.**
- **Как могут решить такую задачу Алиса и Боб?**

Решение для Алисы и Боба: квантовая телепортация!



- **Алиса и Боб генерируют ЭПР-пару.**
- **Алиса берет одну половину пары; Боб берет другую половину. Боб уезжает.**
- **Алиса приводит свой секретный кубит $|\psi\rangle$ во взаимодействие со своей ЭПР-половиной и проводит измерение двух кубитов.**
- **Алиса посылает два получившихся классических измерения Бобу.**
- **Боб декодирует свою половину ЭПР-пары, с 2 битами, получая $|\psi\rangle$.**

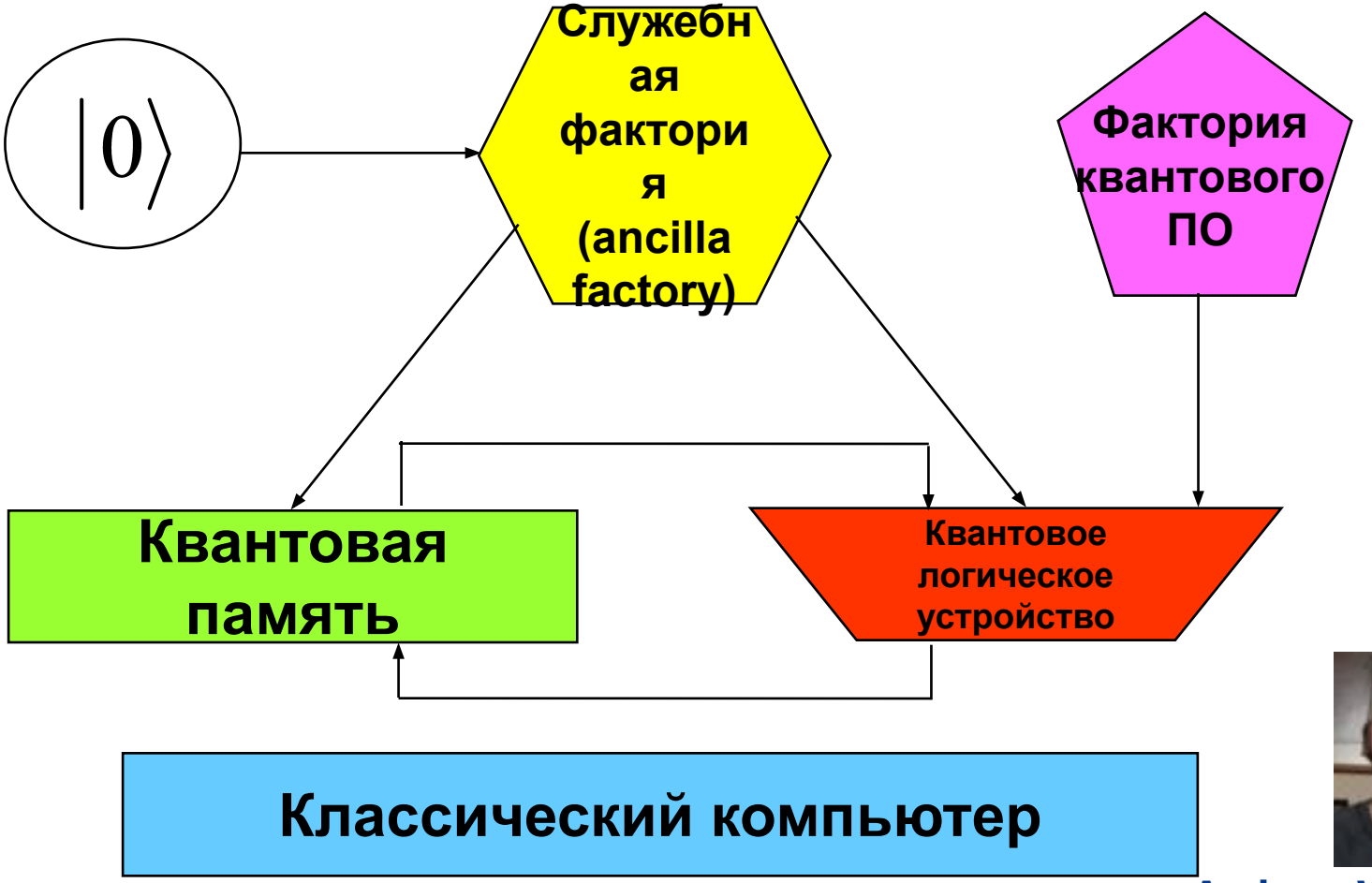
Архитектура квантового компьютера



Knill [1996]: Квантовая память, классический компьютер с квантовым прибором с операциями для инициализации регистров кубитов и применения квантовых операций и измерений

E. Knill
Conventions for Quantum Pseudocode
Los Alamos National Laboratory, LAUR-96-2724, 1996

Архитектура отказоустойчивого квантового компьютера Кросса



Andrew W. Cross

Fault-Tolerant Quantum Computer Architectures Using Hierarchies of Quantum Error-Correcting Codes

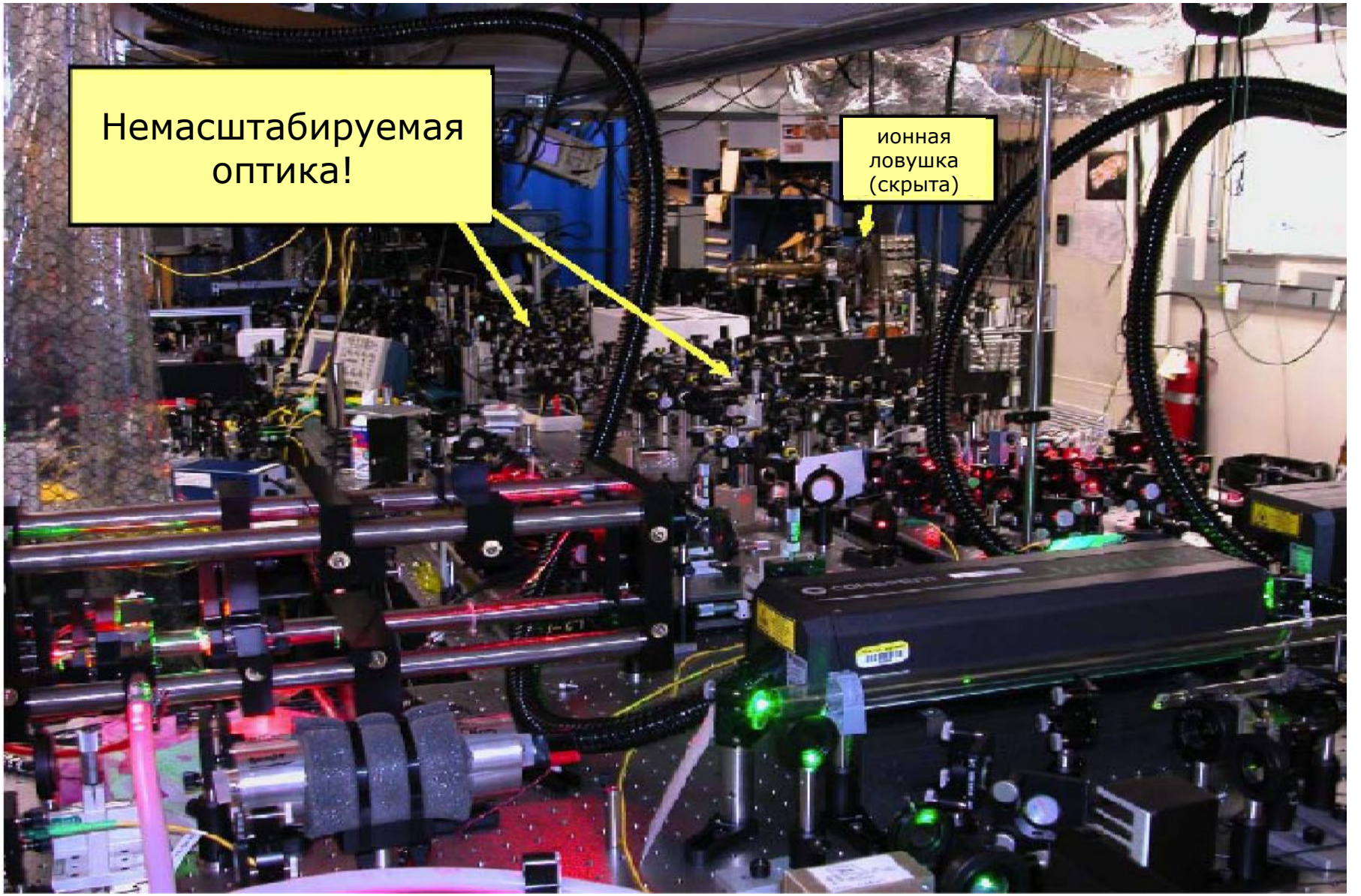
PhD Thesis, MIT, June 2008

Потенциальные технологии целевой машины

- Ионные ловушки
- Переходы Джозефсона
- Ядерный магнитный резонанс
- Оптические фотоны
- Квантовая электродинамика оптического резонатора
- Квантовые точки
- Неабелевы анионы дробного квантового эффекта Холла

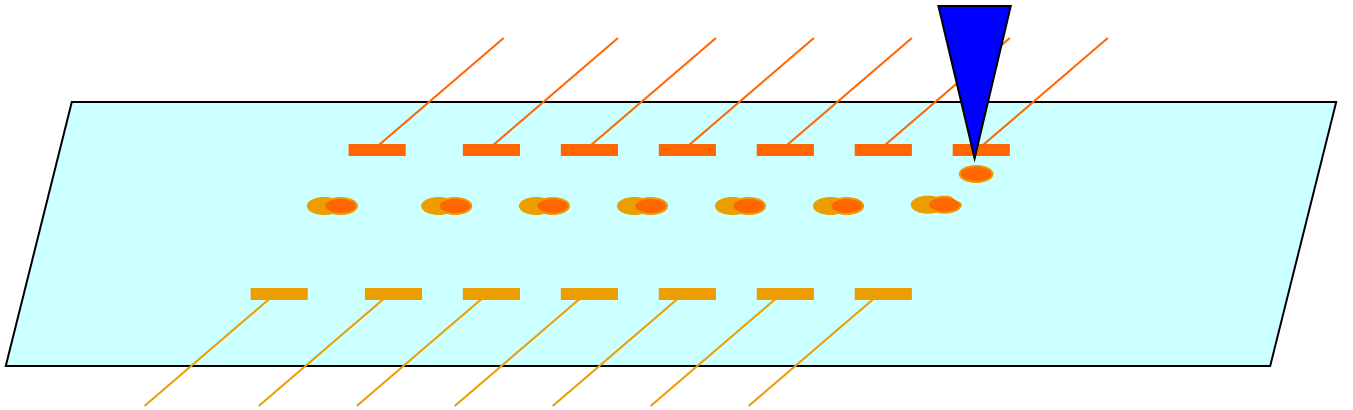
Симулятор ионной ловушки MIT

Квантовый компьютер, основанный на ионной ловушке: реальность



Топологический квантовый компьютер

Теорема: **В любом топологическом квантовом компьютере все вычисления могут быть произведены посредством передвижения единственной квазичастицы!**



S. Simon, N. Bonesteel, M. Freedman, N. Petrovic, and L. Hormozi
Topological Quantum Computing with Only One Mobile Quasiparticle
Phys. Rev. Lett, 2006

Критерии ДиВинченцо для квантового компьютера

1. **Масштабируемая система с хорошо определенными кубитами**
2. **Возможность инициализации в простое фидуциальное состояние**
3. **Большое время декогеренции**
4. **Наличие универсального набора квантовых логических элементов**
5. **Возможность эффективных покубитовых измерений**

David DiVincenzo
Solid State Quantum Computing
http://www.research.ibm.com/ss_computing

Универсальные наборы квантовых элементов

Набор логических элементов *универсален для квантовых вычислений*, если любой унитарный оператор может быть аппроксимирован до произвольной точности квантовой схемой, использующей элементы из этого набора.

Фазовый элемент *S* = $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$; **элемент *π*/8 *T* =** $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Примеры универсальных наборов квантовых элементов:

- **{ *H*, *S*, CNOT, *T* }**
- **{ *H*, *I*, *X*, *Y*, *Z*, *S*, *T*, CNOT }**

Однокубитовый и CNOT-элементы точно универсальны для квантовых вычислений.

Квантовый алгоритм факторизации Шора

Ввод: Составное число *N*
Вывод: Нетривиальный делитель *N*

```
если N четное, то возврат 2;
если N = a^b для целых a >= 1, b >= 2, то
 возврат a;
x := rand(1,N-1);
если нод(x,N) > 1, то возврат нод(x,N);
r := порядок(x mod N); // квантовый шаг
если r четное и x^(r/2) != (-1) mod N, то
 {f1 := нод(x^(r/2)-1,N);  f2 := нод(x^(r/2)+1,N)};
если f1 – нетривиальный делитель, то возврат f1;
иначе если f2 – нетривиальный делитель, то возврат
 f2;
иначе возврат неудача;
```

Nielsen and Chuang, 2000

Задача нахождения порядка

Для натуральных чисел x и N, $x < N$, таких что нод(x, N) = 1, порядок x (mod N) – это наименьшее натуральное r такое, что $x^r \equiv 1 \pmod{N}$.

Например, порядок 5 (mod 21) равен 6.

Задача нахождения порядка состоит в нахождении порядка x (mod N) при данных x и N.

Все известные классические алгоритмы нахождения порядка суперполиномиальны по числу бит в N.

Квантовое нахождение порядка

Задача нахождения порядка может быть решена с помощью квантовой схемы, содержащей

$$O((\log N)^2 \log\log(N) \log\log\log(N))$$

элементарных квантовых логических элементов.

Лучшие из известных классических алгоритмов требуют

$$\exp(O((\log N)^{1/2} (\log\log N)^{1/2})$$

времени.

Предлагаемые квантовые языки программирования

- **Квантовый псевдокод [Knill, 1996]**
- **Императивные: напр., QCL [Ömer, 1998-2003]**
  - **синтаксис на основе C**
  - **классическое управление потоком передачи данных**
  - **классические и квантовые данные**
  - **перемежающиеся измерения и квантовые операторы**
- **Функциональные: напр., QFC, QPL, QML**
  - **линейная логика Жирара**
  - **квантовое лямбда-исчисление**

Абстракции и ограничения языка

- **Состояния — это суперпозиции**
- **Операторы — это унитарные преобразования**
- **Состояния кубитов могут стать запутанными**
- **Измерения приводят к разрушению**
- **Теорема о невозможности копирования: нельзя копировать неизвестное квантовое состояние!**

Методы разработки квантовых алгоритмов

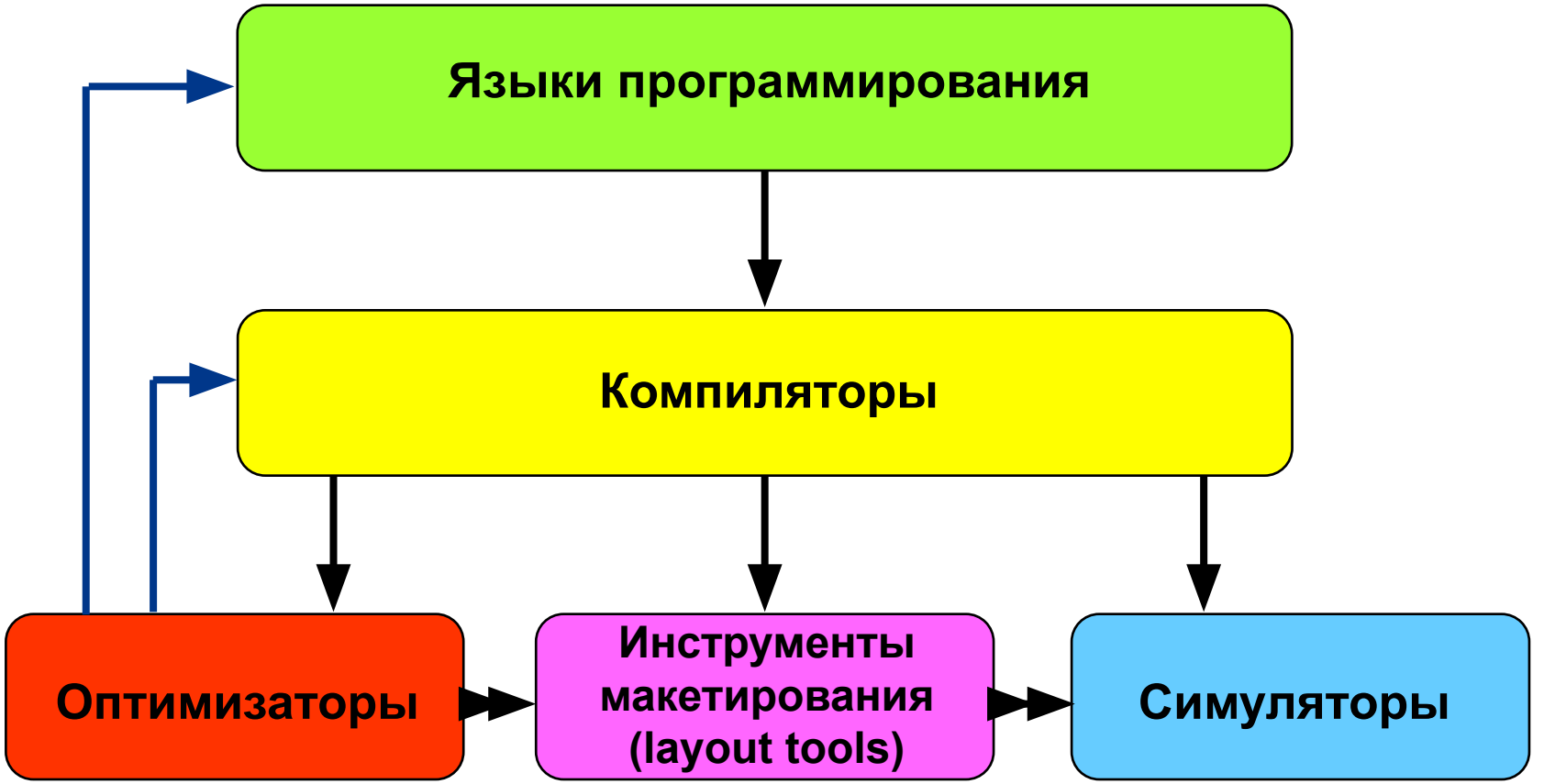
- Оценка фазы
- Квантовое преобразование Фурье
- Нахождение периода
- Оценка собственных значений
- Алгоритм поиска Гровера
- Усиление амплитуды

Инуструменты разработки для квантового компьютера: желаемое

- Среда разработки (design flow), которая переводит высокоуровневые квантовые программы в эффективные устойчивые к ошибкам реализации на различных квантовых вычислительных машинах с различной технологией
- Языки, компиляторы, эмуляторы и инструменты разработки для поддержки среды разработки
- Хорошо определенные интерфейсы между компонентами
- Эффективные методы инкорпорирования устойчивости к ошибкам и квантового исправления ошибок
- Эффективные алгоритмы для оптимизации и верификации квантовых программ

Иерархия инструментов квантовой разработки

- **Представление: послойная иерархия с хорошо определенными интерфейсами**

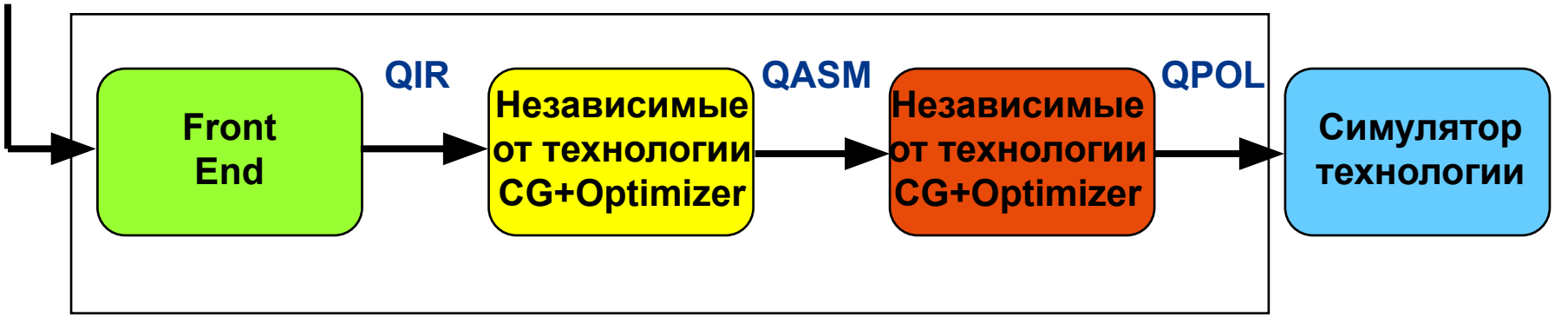


K. Svore, A. Aho, A. Cross, I. Chuang, I. Markov
A Layered Software Architecture for Quantum Computing Design Tools
***IEEE Computer*, 2006, vol. 39, no. 1, pp.74-83**

Языки и абстракции в Design Flow

исходная квантовая программа

QIR: quantum intermediate representation – квантовое промежуточное представление
QASM: quantum assembly language – квантовый ассемблер
QPOL: quantum physical operations language – квантовый язык физических операций



Квантовый компилятор

АБСТРАКЦИИ

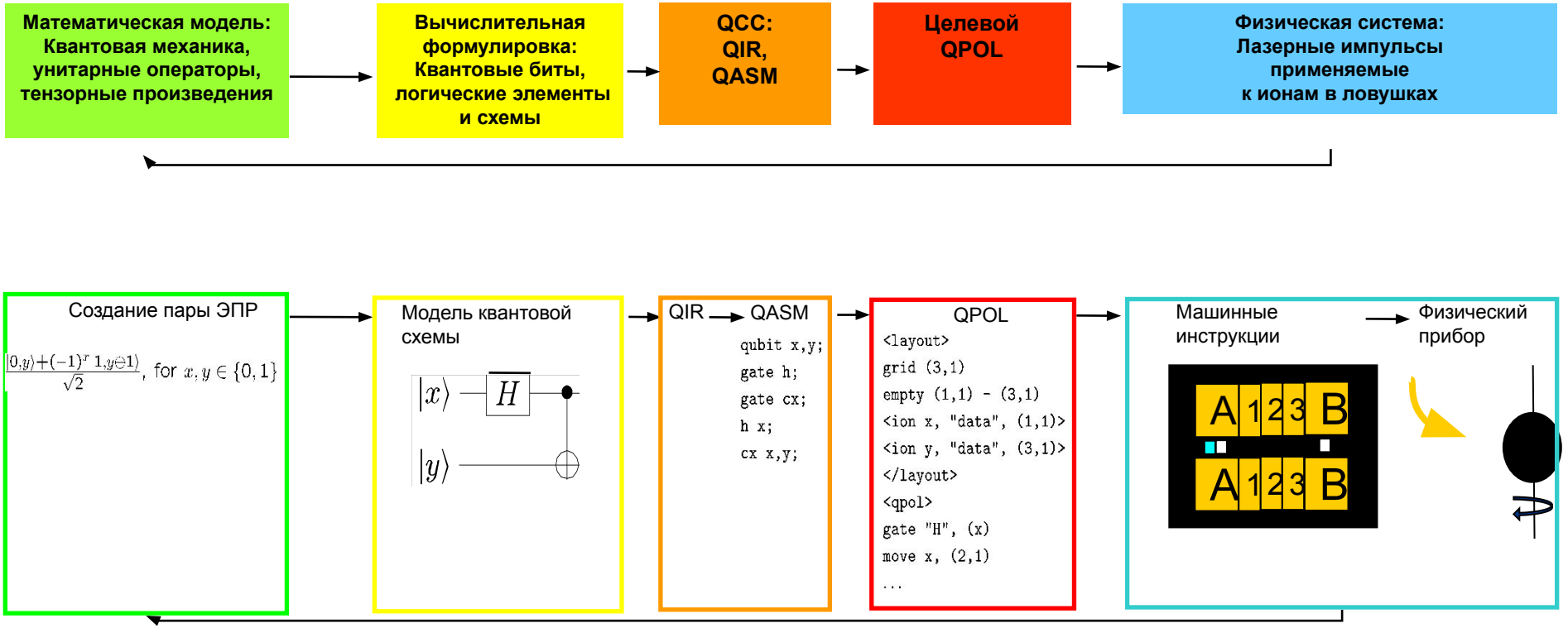
квантовая механика

квантовая схема

квантовая схема

квантовый прибор

Design Flow for Ion Trap



Устойчивость к ошибкам

- **В квантовом компьютере, устойчивом к ошибкам, более 99% ресурсов вероятно будут расходоваться на квантовое исправление ошибок [Chuang, 2006].**

- **Схема, содержащая N (свободных от ошибок) элементов может быть симулирована с вероятностью ошибки, не превосходящей ε, с использованием $N \log(N/\varepsilon)$ неустойчивых к ошибкам логических элементов, дающих ошибку с вероятностью p, покуда $p < p_{th}$ [von Neumann, 1956].**

Устойчивость к ошибкам

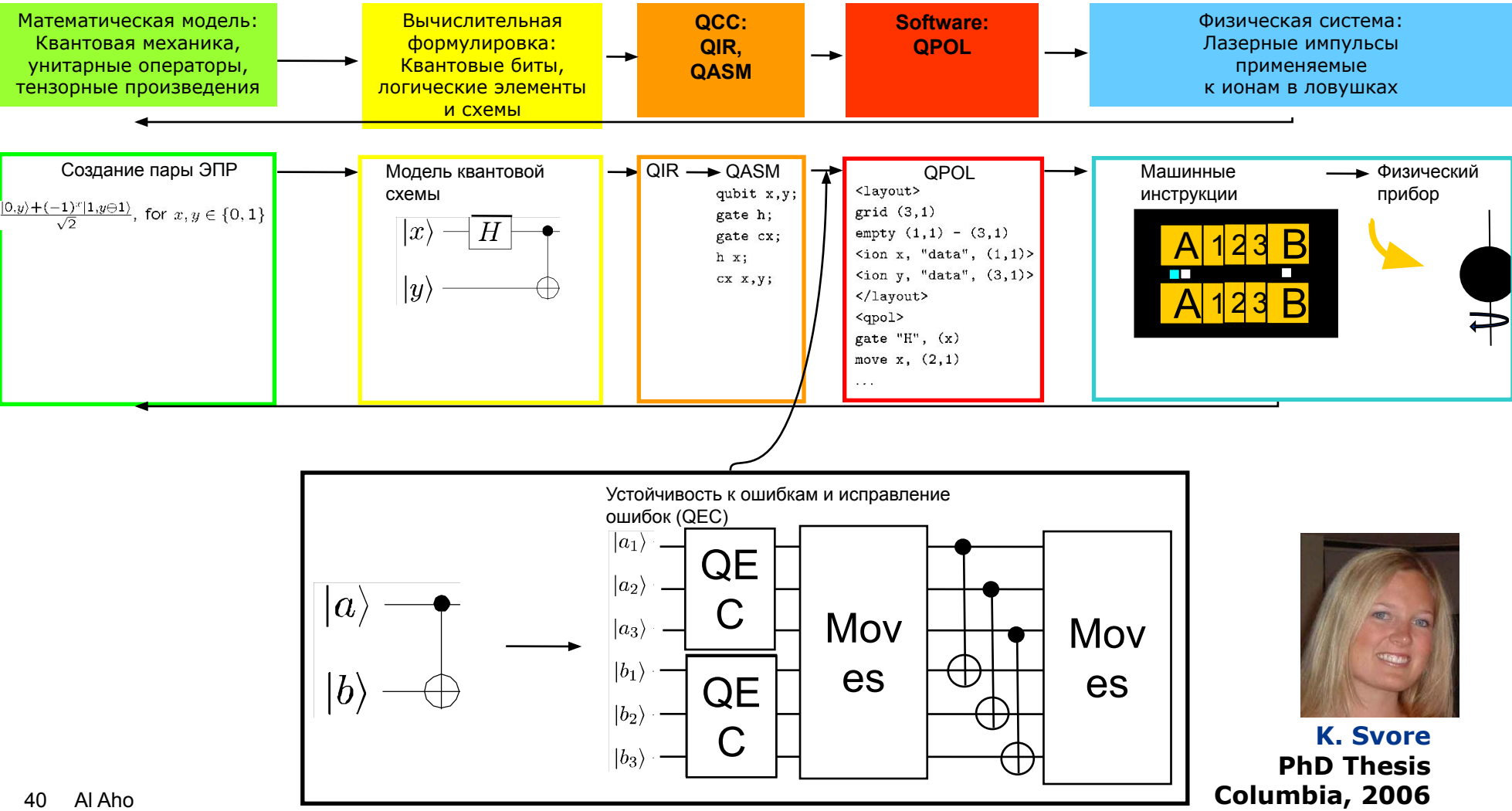
- **Препятствия к применению классического исправления ошибок к квантовым цепям:**
  - **запрет клонирования**
  - **непрерывность ошибок**
  - **измерения уничтожают информацию**

- **Shor [1995] и Steane [1996] показали, что эти препятствия могут быть преодолены с помощью с помощью каскадированных квантовых кодов, исправляющих ошибки.**

P. W. Shor
Scheme for Reducing Decoherence in Quantum Computer Memory
Phys. Rev. B 61, 1995

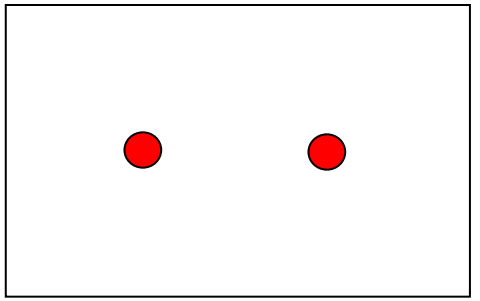
A. Steane
Error Correcting Codes in Quantum Theory
Phys. Rev. Lett. 77, 1966

Среда разработки с устойчивостью к ошибкам и исправлением ошибок

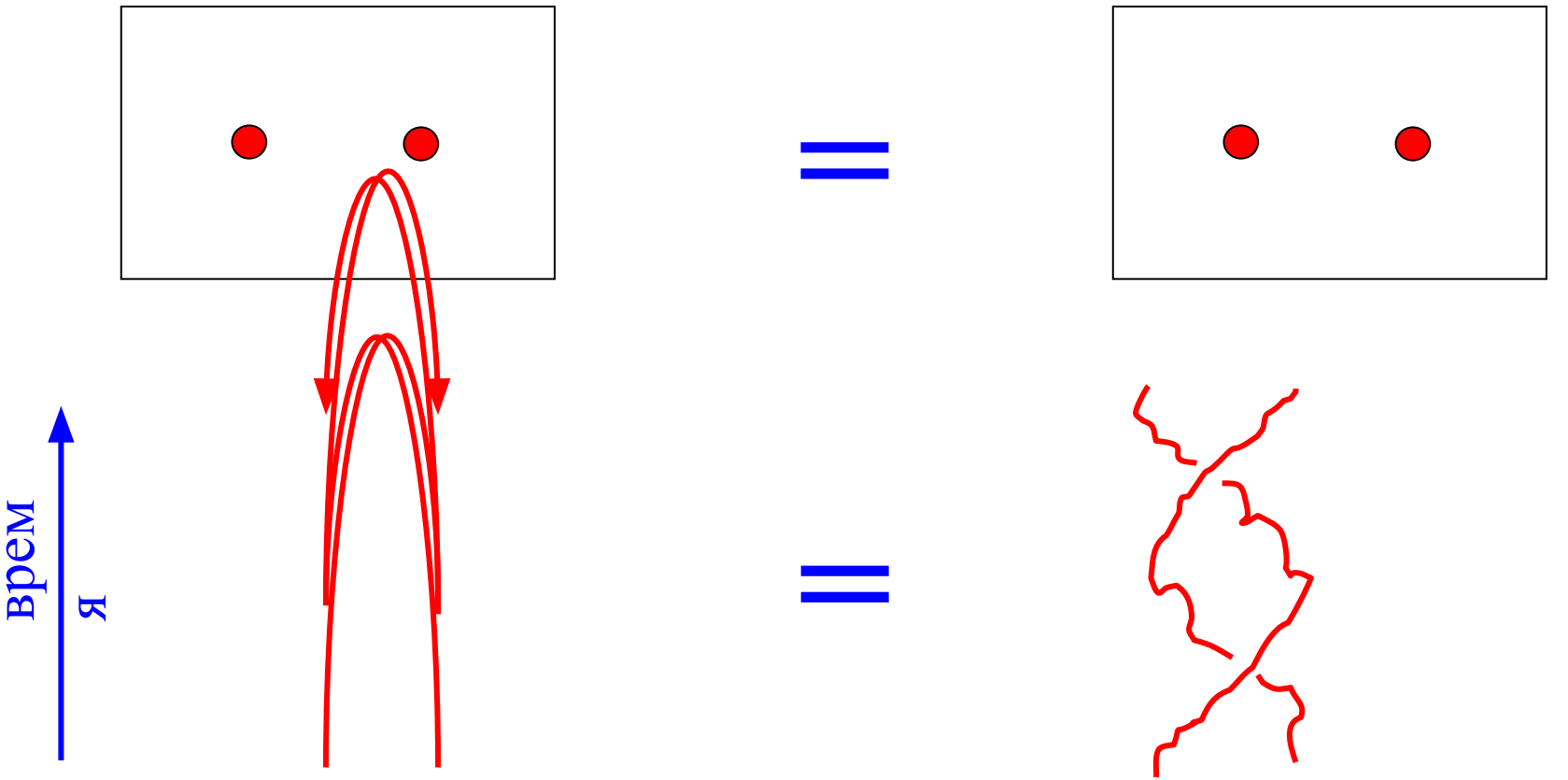


K. Svore
PhD Thesis
Columbia, 2006

Топологическая робастность

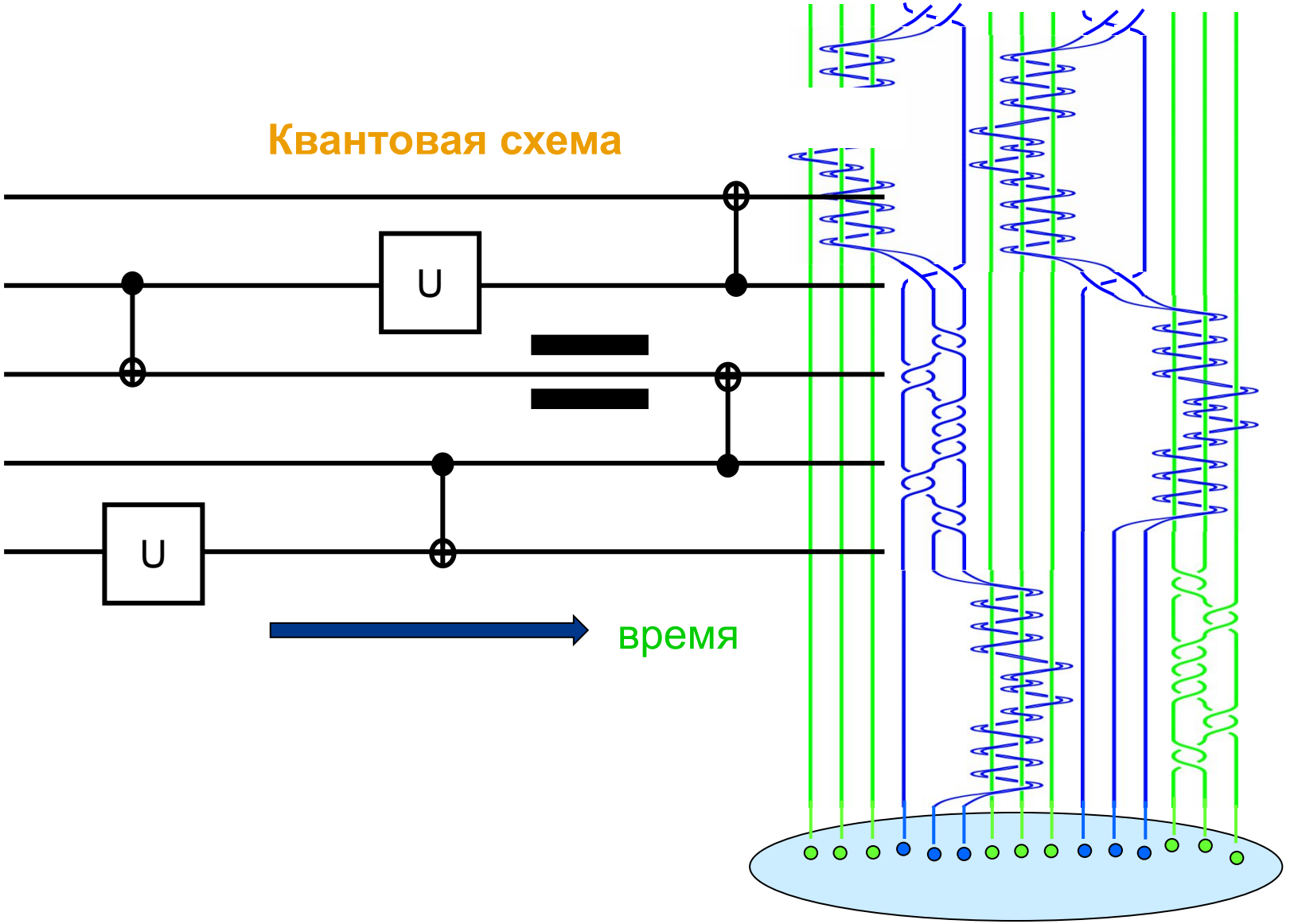


Топологическая робастность



Bonesteel, Hormozi, Simon, … ; PRL 2005, 2006; PRB 2007

Брейд («косичка»)



1. **Вырожденные основные состояния (in punctured system) действуют как кубиты.**

2. **Унитарные операторы (логические элементы) выполняются на основном состоянии путем сплетения punctures (квазичастиц) вокрг друг друга.**
   Конкретные брейды соответствуют конкретным вычислениям.

3. **Состояние может быть инициализовано путем “вытягивания” пары из вакуума. Состояние может быть измерено попыткой возврата пары в вакуум.**

4. **Возможны варианты схем 2,3.**

Kitaev Freedman

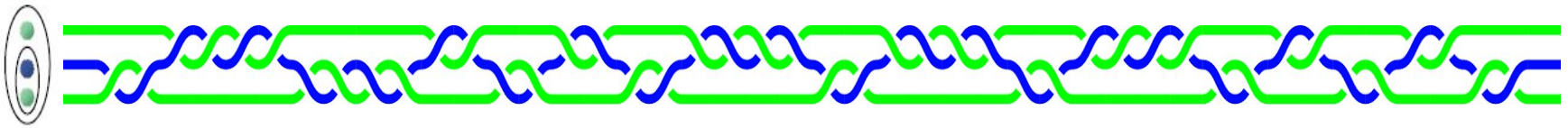
Преимущества:

- **Топологическая квантовая «память» хорошо защищена от шума**
- **Операции (логические элементы) также топологически робастны**

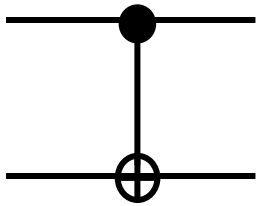
C. Nayak, S. Simon, A. Stern, M. Freedman, S. DasSarma
Non-Abelian Anyons and Topological Quantum Computation
Rev. Mod. Phys., June 2008

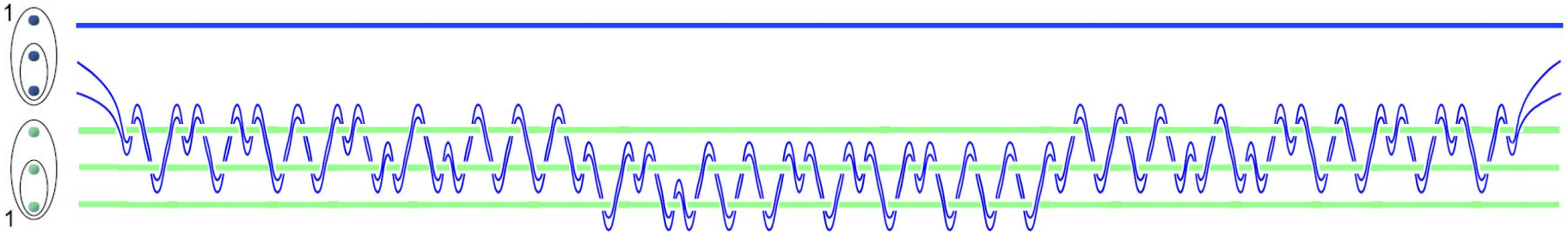
Универсальные набор топологически робастных логических элементов

Вращение одного кубита: $|\psi\rangle$ — U_ϕ — $U_\phi|\psi\rangle$



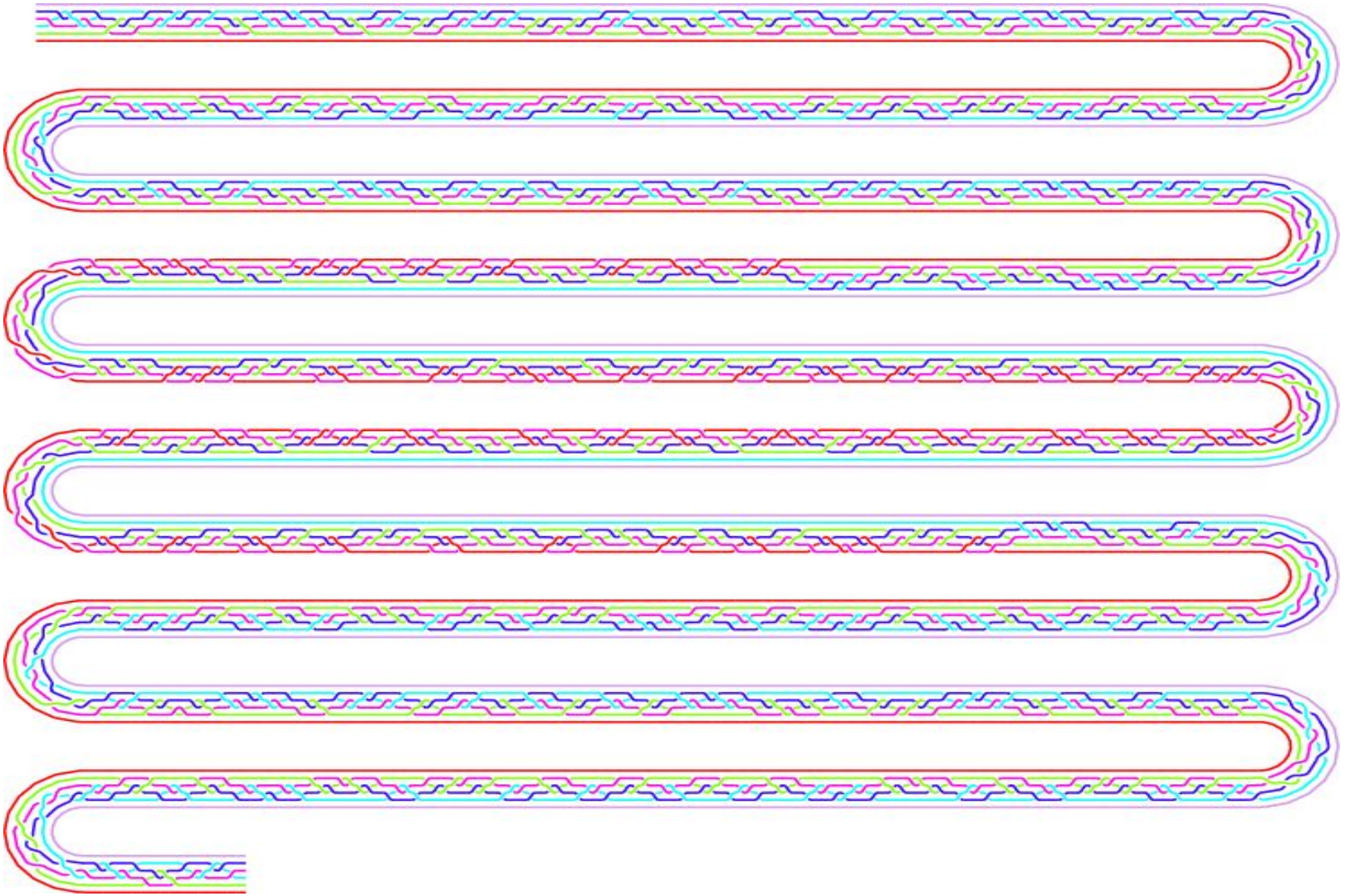
Управляемое NOT:





Bonesteel, Hormozi, Simon, 2005, 2006

Брейд целевого кода для элемента CNOT
с оптимизацией Соловея-Китаева



Задачи для исследования

Больше кубитов

Масштабируемые, устойчивые к ошибкам архитектуры

Естественные языки программирования

Больше алгоритмов!

Соавторы

Isaac Chuang
MIT

Andrew Cross
MIT
now SAIC

Igor Markov
U. Michigan

Krysta Svore
Columbia
now Microsoft Research

Топологические квантовые компьютеры:
Steve Simon
Bell Labs
now Oxford

Al Aho

aho@cs.columbia.edu

Компил[illegible]овых

Спасибо за внимание!

COMPUTER SCIENCE AT
COLUMBIA UNIVERSITY

Перевел П. Новиков
с разрешения автора

KAUST

27 февраля 2011 г.