Karlsruher Institut für Technologie

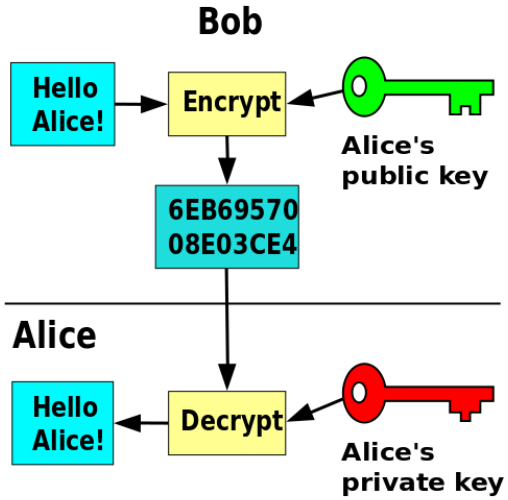
Quantum Algorithms via Linear Algebra

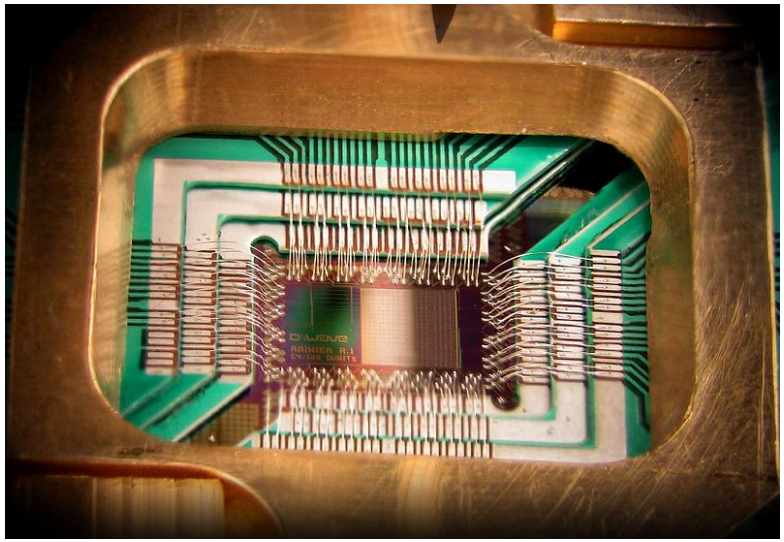
Schedule and Presentation of Topics, April 28, 2017

Meyerhenke, Glantz, Looz, Tzovas

Institute for Theoretical Computer Science

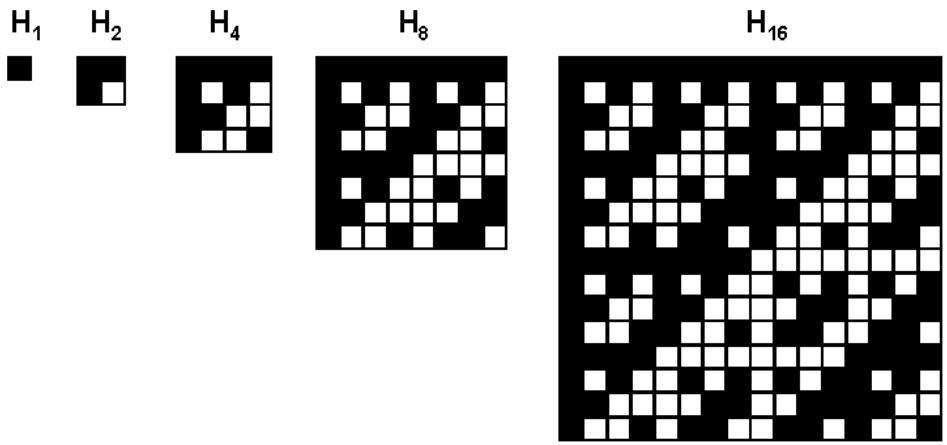
How hot is quantum computing?

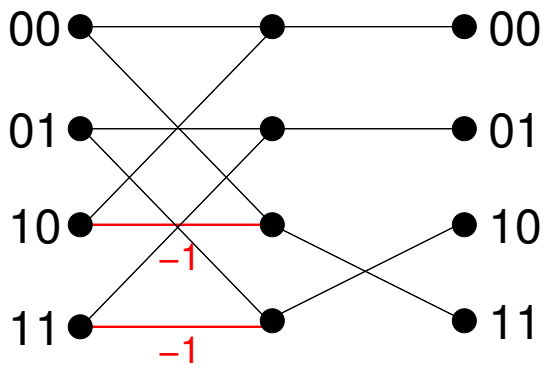




- Factorization and thus cryptograpy (RSA and other public key cryptosystems)
- "Quantum annealers" from D-WAVE for solving certain optimization problems

Matrices and Mazes

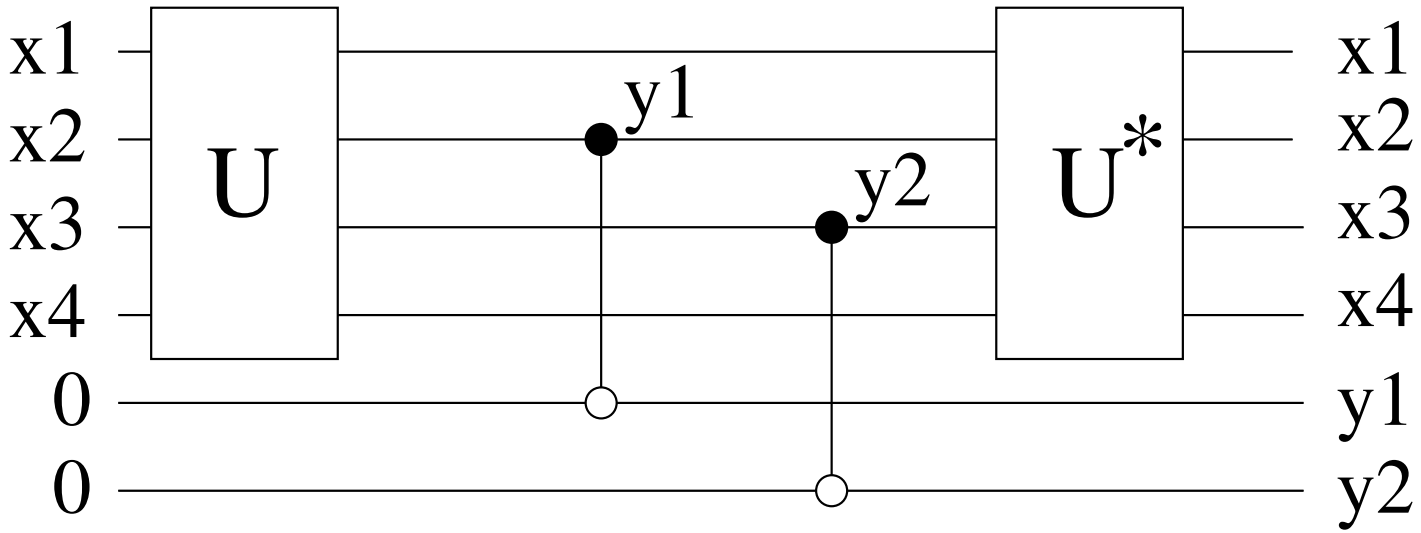




- Hadamard matrices [Sec. 5.1]
- Fourier matrices [Sec. 5.2]
- More matrices [Sec. 5.3 – 5.5]
- Phil's algorithm [Sec. 7]

Basics of quantum algorithm design

- Get another start vector [Sec. 6.1]
- Copying states [Sec. 6.2]
- Copy-uncompute [Sec. 6.3]
- More basics [Sec. 6.3 – 6.7]



The Deutsch(-Jozsa) Algorithm

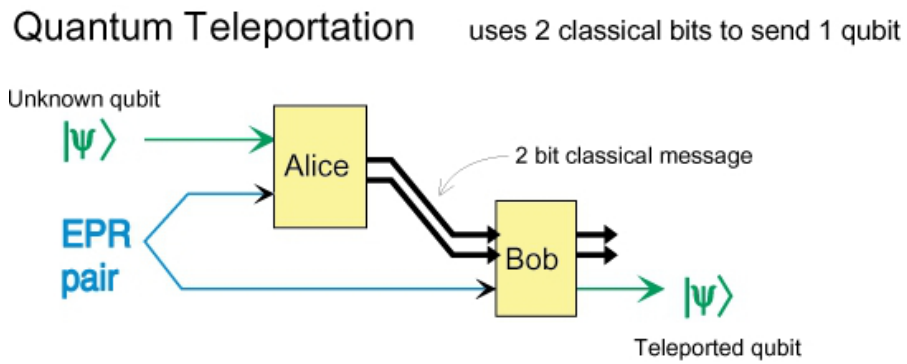
$$f : \{0,1\} \mapsto \{0,1\}$$

- Is $f(\cdot)$ constant, i. e., $f(0) = f(1)$?
- Find out by evaluating $f(\cdot)$ only once [Sec. 8.1 – 8.2].

$$g : \{0,1\}^n \mapsto \{0,1\}$$

- Is $g(\cdot)$ constant, i. e., $g(x) = g(y)$ for all $x, y \in \{0,1\}^n$, or
- balanced, i. e., $|g^{-1}(0)| = |g^{-1}(1)|$?
- Find out by evaluating $g(\cdot)$ only once [Sec. 9.1 – 9.2].

Teleportation and Simon's algorithm



- Quantum teleportation [Sec. 8.3].
- Simon's algorithm [Sec. 10].
  - $f : \{0,1\}^n \mapsto \{0,1\}^n$, $\exists\ s \in \{0,1\}^n$ such that

$$f(y) = f(z) \iff y = z \oplus s\ \forall y, z \in \{0,1\}^n. \tag{1}$$

  - Find period s.

Shor's algorithm and factorization

This is where quantum algorithms might get crucial in cryptography!

- $f : \mathbb{N} \mapsto \{0, 1, \ldots, M-1\}$, $\exists\, r \in \mathbb{N}$ such that

$$f(x + r) = f(x)\ \forall x \in \mathbb{N}.$$

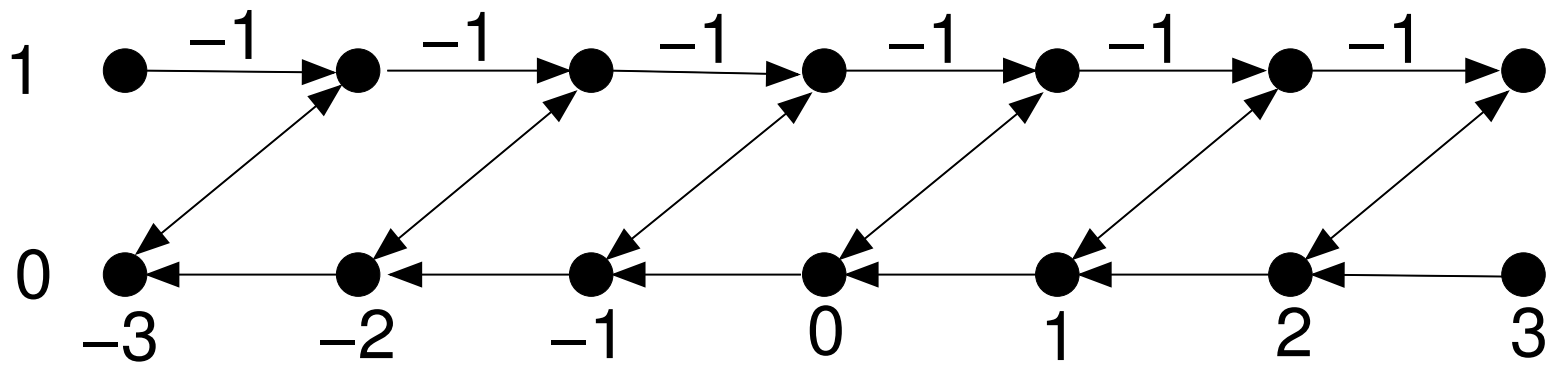
- Find period r [Sec 11].
- Find a factor of M with high probability in quantum polynomial time [Sec 12].

Grover's algorithm

- Given a set S of N potential solutions to a problem, N large.
- Only potential solutions in small $S' \subset S$ are really solutions.
- Find a solution [Sec 13].

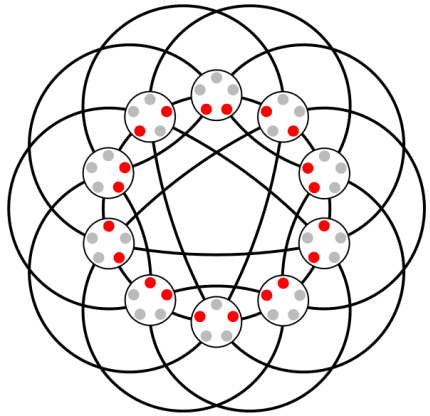
- Ideal state h such that $h(s) = 1$ for $s \in S'$, 0 otherwise.
- Start with h such that $h(s_1) = h(s_2)$ for all $s_1, s_2 \in S$.
- Make h more pronounced,

Quantum Walks



- Classical random walks [Sec. 14.1]
- Random walks and matrices [Sec. 14.2]
- Quantum walks [Sec. 14.3 – 14.6]

Quantum walk search algorithms



What is quantum walk search good for?

- Is $f : \{1, \ldots, n\} \mapsto \{1, \ldots, n\}$ bijective?
- $V_r := \{S_r \subset \{1, \ldots, n\} \mid |S_r| = r\}$ [Sec. 15.1].
- Perform quantum walks on Johnson graph $J_{n,r}$ [Sec. 15.2 – 15.10]

Bounded Error Quantum Polynomial Time (BQP)

From BPP(Bounded error Probabilistic Polynomial) to BQP:

Definition (BQP)

A function $f : \{0,1\}^* \mapsto \{0,1\}^*$ belongs to BQP if there are a polynomial p, a function g computable in classical $p(n)$ time, and a quantum Algorithm $\mathbf{A}$ such that for all n and inputs $x \in \{0,1\}^n$, and for some $r < p(n)$, $\mathbf{A}$ applied to the initial state $\mathbf{e}_{x0^r}$ yields within $p(n)$ basic quantum operations a quantum state $\mathbf{b}$ such that

$$\Pr[\text{measuring } \mathbf{b} \text{ yields } z \text{ such that } g(z) = f(x)] \geq 3/4. \qquad (2)$$

Which f belong to BQP? [Sec. 16]

Reference

R. J. Lipton and K. W. Regan.
Quantum Algorithms via Linear Algebra. A Primer.
The MIT Press, 2014.

Schedule

- Until May 5: Binding registration

Schedule

- Until May 5: Binding registration
- May 5, 16:00 – 18:00:
  Introduction to presentation techniques (H. Meyerhenke) and
  Introduction to quantum algorithms: part 1 (R. Glantz)

Schedule

- Until May 5: Binding registration
- May 5, 16:00 – 18:00:
  Introduction to presentation techniques (H. Meyerhenke) and
  Introduction to quantum algorithms: part 1 (R. Glantz)
- May 12, 15:45 – 17:30:
  Introduction to quantum algorithms: part 2 (M. Looz, H. Tzovas)

Schedule

- Until May 5: Binding registration
- May 5, 16:00 – 18:00:
  Introduction to presentation techniques (H. Meyerhenke) and
  Introduction to quantum algorithms: part 1 (R. Glantz)
- May 12, 15:45 – 17:30:
  Introduction to quantum algorithms: part 2 (M. Looz, H. Tzovas)
- June 9, 15:45 – 18:15: Short presentations

Schedule

- Until May 5: Binding registration
- May 5, 16:00 – 18:00:
  Introduction to presentation techniques (H. Meyerhenke) and
  Introduction to quantum algorithms: part 1 (R. Glantz)
- May 12, 15:45 – 17:30:
  Introduction to quantum algorithms: part 2 (M. Looz, H. Tzovas)
- June 9, 15:45 – 18:15: Short presentations
- June 30, 15:45 – 18:15: Presentations 1 – 3
- July 7, 15:45 – 18:15: Presentations 4 – 6
- July 14, 15:45 – 18:15: Presentations 7 – 9

Schedule

- Until May 5: Binding registration
- May 5, 16:00 – 18:00:
  Introduction to presentation techniques (H. Meyerhenke) and
  Introduction to quantum algorithms: part 1 (R. Glantz)
- May 12, 15:45 – 17:30:
  Introduction to quantum algorithms: part 2 (M. Looz, H. Tzovas)
- June 9, 15:45 – 18:15: Short presentations
- June 30, 15:45 – 18:15: Presentations 1 – 3
- July 7, 15:45 – 18:15: Presentations 4 – 6
- July 14, 15:45 – 18:15: Presentations 7 – 9
- August 18: Deadline for written summary