Quantum algorithms

Andrew Childs
University of Waterloo

Pawel Wocjan
University of Central Florida

10th Canadian Summer School on Quantum Information
17–19 July 2010

Outline

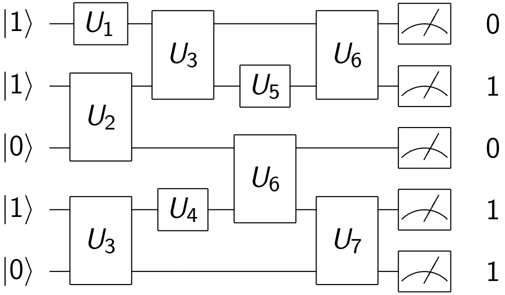
Part I

Quantum circuits

Quantum circuit model

Quantum circuits are generalizations of Boolean circuits

input transformation output (probabilistic)



Classical bit

Classical bit (bit): $\mathbb{B} := \{0, 1\}$

- Basis state: either 0 or 1
- General state: a probability distribution $p = (p_0, p_1)$ on $\mathbb{B}$

Classical register

Classical register: $\mathbb{B}^n := \underbrace{\mathbb{B} \times \mathbb{B} \times \ldots \times \mathbb{B}}_{n}$

- Basis state: a binary string $x \in \mathbb{B}^n$
- General state: a probability distribution $p = (p_x : x \in \mathbb{B}^n)$ on $\mathbb{B}^n$ (written as a column vector)

Remark: Note that p is a vector with positive entries that is normalized with respect to the ℓ_1-norm (the sum of the absolute values of the entries)

Classical transformation

Transformations on the classical register $\mathbb{B}$ are described by stochastic matrices

Stochastic matrices preserve the ℓ_1-norm, i.e., probability distributions are mapped on probability distributions

Let p be the state of the register. The state after the transformation P is given by the matrix-vector-product

$$Pp$$

Qubit

Quantum bit (qubit): two-dimensional complex Hilbert space $\mathbb{C}^2$

- Computational basis states (classical states):

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{and} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- General states: superpositions

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle\,, \quad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

the coefficients $\alpha_0, \alpha_1 \in \mathbb{C}$ are called probability amplitudes

Quantum register

Quantum register: 2^n-dimensional complex Hilbert space $(\mathbb{C}^2)^{\otimes n}$ with tensor product structure

$$(\mathbb{C}^2)^{\otimes n} := \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n}$$

- Computational basis states (classical states):

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle , \quad x \in \mathbb{B}^n$$

- General state:

$$|\psi\rangle = \sum_{x \in \mathbb{B}^n} \alpha_x |x\rangle , \quad \sum_x |\alpha_x|^2 = 1$$

Remark: Note that $|\psi\rangle$ is a column vector (ket) that is normalized with respect to the ℓ_2-norm (Euclidean norm)

Quantum transformations

Transformations on the quantum register $\mathcal{H} := (\mathbb{C}^2)^{\otimes n}$ are described by unitary matrices $U \in \mathcal{U}(\mathcal{H})$

Unitary matrices preserve the ℓ_2-norm

Let $|\psi\rangle \in \mathcal{H}$ be the state of the quantum register; the state after the transformation U is given by the matrix-vector product

$$U|\psi\rangle$$

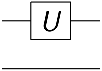
Quantum circuit

Each transformations U has to be implemented by a quantum circuit, i.e., a sequence of elementary gates

Quantum circuit model $=$ Quantum mechanics $+$ Notion of complexity

Single qubit gate on two qubits

single-qubit gate U on first qubit



action on basis states of $\mathbb{C}^2 \otimes \mathbb{C}^2$

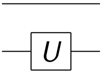
$$\begin{aligned}
|0\rangle \otimes |0\rangle &\mapsto (U|0\rangle) \otimes |0\rangle \\
|0\rangle \otimes |1\rangle &\mapsto (U|0\rangle) \otimes |1\rangle \\
|1\rangle \otimes |0\rangle &\mapsto (U|1\rangle) \otimes |0\rangle \\
|1\rangle \otimes |1\rangle &\mapsto (U|1\rangle) \otimes |1\rangle
\end{aligned}$$

corresponding matrix

$$U \otimes I = \left(\begin{array}{c|c} u_{00} \cdot I & u_{01} \cdot I \\ \hline u_{10} \cdot I & u_{11} \cdot I \end{array}\right) = \begin{pmatrix} u_{00} & 0 & u_{01} & 0 \\ 0 & u_{00} & 0 & u_{01} \\ u_{10} & 0 & u_{11} & 0 \\ 0 & u_{10} & 0 & u_{11} \end{pmatrix}$$

Single qubit gate on two qubits

single-qubit gate U on second qubit



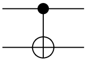
action on basis states of $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$\begin{aligned} |0\rangle \otimes |0\rangle &\mapsto |0\rangle \otimes U|0\rangle \\ |0\rangle \otimes |1\rangle &\mapsto |0\rangle \otimes U|1\rangle \\ |1\rangle \otimes |0\rangle &\mapsto |1\rangle \otimes U|0\rangle \\ |1\rangle \otimes |1\rangle &\mapsto |1\rangle \otimes U|1\rangle \end{aligned}$$

corresponding matrix

$$I \otimes U = \left(\begin{array}{c|c} 1 \cdot U & 0 \cdot U \\ \hline 0 \cdot U & 1 \cdot U \end{array}\right) = \begin{pmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$

Controlled-NOT gate

control: first qubit; target: second qubit 

action on basis states of $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$|c\rangle \otimes |t\rangle \mapsto |c\rangle \otimes |c \oplus t\rangle$$

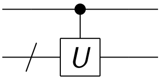
corresponding matrix

$$\left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right) = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes X$$

where $I_2 = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$

Controlled U gate

control: qubit; target: m-qubit register



let U be a unitary acting on the m-qubit register

action on basis states of $\mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes m}$

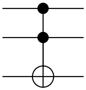
$$|c\rangle \otimes |t\rangle \mapsto |c\rangle \otimes U^c |t\rangle \quad \text{where } b \in \mathbb{B}, t \in \mathbb{B}^m$$

corresponding matrix

$$\left(\begin{array}{c|c} I & 0 \\ \hline 0 & {\color{blue}U} \end{array}\right) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes {\color{blue}U}$$

Toffoli gate

control: first and second qubits; target: third qubit



action on basis states of $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$

$$|c_1\rangle \otimes |c_2\rangle \otimes |t\rangle \mapsto |c_1\rangle \otimes |c_2\rangle \otimes |(c_1 \wedge c_2) \oplus t\rangle$$

corresponding matrix

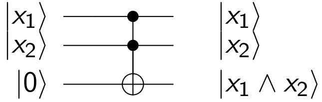
$$\left(\begin{array}{cc|cc|cc|cc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right) = (I_4 - |11\rangle\langle 11|) \otimes I_2 + |11\rangle\langle 11| \otimes X$$

Simulating irreversible gates with Toffoli gate

The classical AND gate is irreversible because if the output is 0 then we cannot determine which of the three possible pairs was the actual input

x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

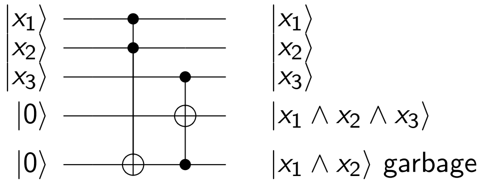
But it is easy to simulate the AND gate with one Toffoli gate



Problem of garbage

To simulate irreversible circuits with Toffoli gates, we keep the input and intermediary results to make everything reversible

Consider the function $y = x_1 \wedge x_2 \wedge x_3$

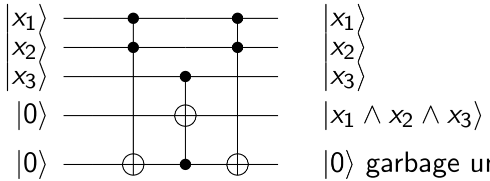


It is important to not leave any garbage; otherwise, we could not make use of quantum parallelism and constructive interference effects

Reversible garbage removal

It is always possible to reversibly remove (uncompute) the garbage

In the case $y = x_1 \wedge x_2 \wedge x_3$, this can be done with the circuit



Simulating irreversible circuits with Toffoli gates

Let $f : \{0,1\}^n \to \{0,1\}$ be any boolean function

Assume this function can be computed classically using only t classical elementary gates such as AND, OR, NAND

We can implement a unitary U_f on $(\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes w}$ such that

$$U_f\left(|x\rangle_{\text{in}} \otimes |y\rangle_{\text{out}} \otimes |0\rangle_{\text{work}}^{\otimes w}\right) = |x\rangle \otimes |y \oplus f(x)\rangle \otimes |0\rangle^{\otimes w}$$

U_f is built from polynomially many in t Toffoli gates and the size w of the workspace register is polynomial in t

During the computation the qubits of the workspace register are changed, but at the end they reversibly reset to $|0\rangle^{\otimes w}$

Universal gate set – exact implementation

Each unitary $U \in \mathcal{U}(\mathcal{H})$ can be implemented exactly by quantum circuits using only:

- CNOT gates (acting on adjacent qubits)
- arbitrary single qubit gates

Gate complexity of unitaries – exact implementation

The gate complexity $\kappa(U)$ of a unitary $U \in \mathcal{U}(\mathcal{H})$ is minimal number of elementary gates needed to implement U

For example, quantum Fourier Transform has complexity $O(n^2)$

$\implies$ Shor's factorization algorithm

Universal gate set – approximate implementation

For each $\epsilon \in (0,1)$ and each unitary $U \in \mathcal{U}(\mathcal{H})$, there is a unitary V such that

$$\|U - V\| \leq \epsilon \quad \text{where} \quad \|U - V\| = \sup_{|\psi\rangle} \|(U - V)|\psi\rangle\|$$

and V is implemented by quantum circuits using only:

- CNOT gates (acting on adjacent qubits)
- the single qubit gates

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad R(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \quad \text{with } \theta = \frac{\pi}{4}$$

There are other universal gate sets

Gate complexity of unitaries – approximate implementation

The gate complexity $\kappa_\epsilon(U)$ of a unitary U is the minimal number of gates (from a universal gate set) need to implement a unitary V with $\|U - V\| \leq \epsilon$

The Solovay-Kitaev theorem implies that

$$\kappa_\epsilon(U) = O\Big(\kappa(U) \cdot \log^c \big(\kappa(U)/\epsilon\big)\Big)$$

for some small constant c

Counting arguments show that most n-qubit unitaries have gate complexity exponential in n.

Quantum measurement

A general measurement is described by a collection $P_0, \ldots, P_{m-1}$ of orthogonal projectors such that

$$\sum_{i=0}^{m-1} P_i = I_{\mathcal{H}} \quad \text{where } \mathcal{H} \text{ denotes the identity on } \mathcal{H}$$

Let $|\psi\rangle$ be the state of the quantum register. The probability of obtaining the outcome i is given by

$$\Pr(i) = \| P_i |\psi\rangle \|^2$$

The post-measurement state (collapse of the wavefunction) is

$$\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$$

Elementary quantum measurements

A measurement has to be realized by first applying a suitable quantum circuit followed by an elementary measurement

An elementary measurement on the n-qubit quantum register $\mathcal{H}$ consists of measuring the first (w.l.o.g.) m qubits ($m \leq n$) with respect to the computational basis

The 2^m orthogonal projectors P_b are labeled by m-bit strings $b \in \mathbb{B}^m$ and are defined by

$$P_b = |b_1\rangle\langle b_1| \otimes |b_2\rangle\langle b_2| \otimes \cdots \otimes |b_m\rangle\langle b_m| \otimes I_{2^{n-m}}$$

The probability of obtaining outcome b is given by

$$\Pr(b) = \|P_b|\psi\rangle\|^2 = \sum_{x_{m+1},\ldots,x_n \in \mathbb{B}} |\alpha_{b_1,\ldots,b_m,x_{m+1},\ldots,x_n}|^2$$

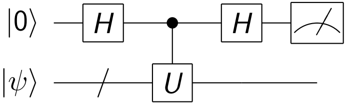
Structure of quantum algorithms

A quantum algorithm consists of

- preparing the initial state $|x\rangle$ with $x \in \mathbb{B}^n$,
- applying a quantum circuit of polynomially many in n gates from some universal gate set, and
- performing an elementary measurement

These steps are repeated polynomially many times to collect enough samples and followed by classical post-processing $\Longrightarrow$ solution of the problem

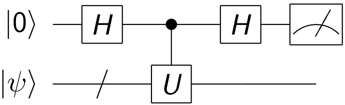
Hadamard test



The probabilities of obtaining the outcomes 0 and 1 are:

$$\Pr(0) = \frac{1}{2}\left(1 + \mathrm{Re}\langle\psi|U|\psi\rangle\right) \qquad \Pr(1) = \frac{1}{2}\left(1 - \mathrm{Re}\langle\psi|U|\psi\rangle\right)$$

Hadamard test



$$
\begin{aligned}
& |0\rangle \otimes |\psi\rangle \\
\mapsto \quad & \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |\psi\rangle \\
= \quad & \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |\psi\rangle \\
\mapsto \quad & \frac{1}{\sqrt{2}}|0\rangle \otimes |\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes U|\psi\rangle \\
\mapsto \quad & \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\psi\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes U|\psi\rangle \\
= \quad & \frac{1}{2}|0\rangle \otimes \left(|\psi\rangle + U|\psi\rangle\right) + \frac{1}{2}|1\rangle \otimes \left(|\psi\rangle - U|\psi\rangle\right) \\
=: \quad & |\Phi\rangle
\end{aligned}
$$

Hadamard test

$$
\begin{aligned}
& \Pr(0) \\
= \;& \| P|\Phi\rangle \|^2 \quad \text{with} \quad P = |0\rangle\langle 0| \otimes I \\
= \;& \| \left(|0\rangle\langle 0| \otimes I \right) \left(\frac{1}{2}|0\rangle \otimes (|\psi\rangle + U|\psi\rangle) + \frac{1}{2}|1\rangle \otimes (|\psi\rangle - U|\psi\rangle) \right) \|^2 \\
= \;& \| \frac{1}{2}|0\rangle \otimes (|\psi\rangle + U|\psi\rangle) \|^2 \\
= \;& \frac{1}{4} \| |0\rangle \|^2 \cdot \| |\psi\rangle + U|\psi\rangle \|^2 \\
= \;& \frac{1}{4} \left(\langle\psi| + \langle\psi|U^\dagger \right) \left(|\psi\rangle + U|\psi\rangle \right) \\
= \;& \frac{1}{4} \left(\langle\psi|\psi\rangle + \langle\psi|U|\psi\rangle + \langle\psi|U^\dagger|\psi\rangle + \langle\psi|U^\dagger U|\psi\rangle \right) \\
= \;& \frac{1}{4} \left(2 + \langle\psi|U|\psi\rangle + \overline{\langle\psi|U|\psi\rangle} \right) \\
= \;& \frac{1}{2} \left(1 + \mathrm{Re}\langle\psi|U|\psi\rangle \right)
\end{aligned}
$$

Hadamard test – Figure it out yourself

How can you estimate the imaginary part of $\langle\psi|U|\psi\rangle$?

Hint: Add a simple gate on the control register before the measurement.

SWAP test – Figure it out yourself

Let S denote the swap gate acting on two qubits

$$S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

Determine the matrix representation of S with respect to the computational basis

Consider the Hadamard test where the controlled operation is

$$|0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes S$$

and the state of the target register $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

Determine the probability of obtaining 0 and 1 for the cases:

- arbitrary $|\psi_1\rangle$ and $|\psi_2\rangle$,
- $\langle\psi_1|\psi_2\rangle = 0$ (orthogonal), and
- $\langle\psi_1|\psi_2\rangle = 1$ (the same).

Part II

Elementary quantum algorithms

Black box problems

Standard computational problem: determine a property of some input data

- Example: Find the prime factors of N

Alternate model: Input is provided by a *black box* (or *oracle*)

- Query: On input x, black box returns $f(x)$
- Determine a property of f using as few queries as possible
- The minimum number of queries is the *query complexity*
- Example: Given a black box for $f : \{1, 2, \ldots, N\} \to \{0, 1\}$, is there some x such that $f(x) = 1$?
- Why black boxes?
  - Facilitates proving lower bounds
  - Can lead to algorithms for standard problems

Black boxes for reversible/quantum computing

Black box $x \;—\boxed{f}—\; f(x)$ is not reversible

Reversible version:

$$\begin{array}{lcl} x & \multirow{2}{*}{$\boxed{f}$} & x \\ z & & z \oplus f(x) \end{array}$$

Given a circuit that computes f non-reversibly, we can implement the reversible version with little overhead

Quantum version:

$$\begin{array}{lcl} |x\rangle & \multirow{2}{*}{$\boxed{f}$} & |x\rangle \\ |z\rangle & & |z \oplus f(x)\rangle \end{array}$$

A reversible circuit is a quantum circuit

Deutsch's problem

Problem

- Given: a black-box function $f : \{0,1\} \to \{0,1\}$
- Task: determine whether f is *constant* or *balanced*

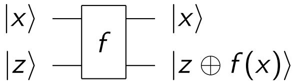
$$\underbrace{\begin{array}{c|c} x & f_1(x) \\ \hline 0 & 0 \\ 1 & 0 \end{array} \qquad \begin{array}{c|c} x & f_2(x) \\ \hline 0 & 1 \\ 1 & 1 \end{array}}_{\text{constant: } f(0) = f(1)} \qquad \underbrace{\begin{array}{c|c} x & f_3(x) \\ \hline 0 & 0 \\ 1 & 1 \end{array} \qquad \begin{array}{c|c} x & f_4(x) \\ \hline 0 & 1 \\ 1 & 0 \end{array}}_{\text{balanced: } f(0) \neq f(1)}$$

How many queries are needed?

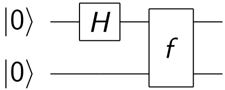
- Classically: 2 queries are necessary and sufficient
- Quantumly: ?

Toward a quantum algorithm for Deutsch's problem

Quantum black box for f:



Compute f in superposition:

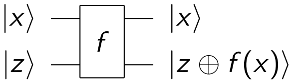


$$
\begin{aligned}
|0\rangle \otimes |0\rangle &\mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \\
&\mapsto \frac{1}{\sqrt{2}}(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle)
\end{aligned}
$$

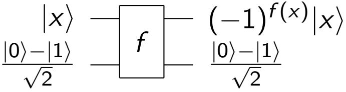
Can't extract more than one bit of information about f

Phase kickback

Quantum black box for f:

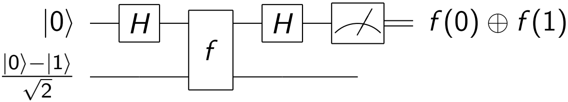


Phase kickback:



$$\begin{aligned}
|x\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= \tfrac{1}{\sqrt{2}}(|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle) \\
&\mapsto \tfrac{1}{\sqrt{2}}(|x\rangle \otimes |f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle) \\
&= |x\rangle \otimes \tfrac{1}{\sqrt{2}}(|f(x)\rangle - |\overline{f(x)}\rangle) \\
&= \underbrace{(-1)^{f(x)}}_{\text{not necessarily global}} |x\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}$$

Quantum algorithm for Deutsch's problem



$$
\begin{aligned}
|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} &\mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\mapsto \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= (-1)^{f(0)} \frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\mapsto (-1)^{f(0)} |f(0) \oplus f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}
$$

1 quantum query vs. 2 classical queries!

The Deutsch-Jozsa problem

Problem

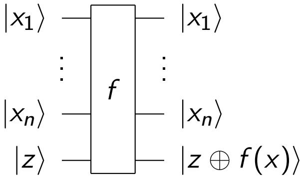
- Given: a black-box function $f : \{0, 1\}^n \to \{0, 1\}$
- Promise: f is either
  constant ($f(x)$ is independent of x)
  or *balanced* ($f(x) = 0$ for exactly half the values of x)
- Task: determine whether f is constant or balanced

How many queries are needed?

- Classically: $2^n/2 + 1$ queries to answer with certainty
- Quantumly: ?

Phase kickback for a Boolean function of n bits

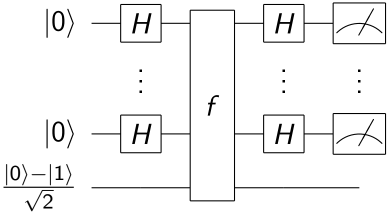
Black box function:



Phase kickback:

$$|x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mapsto (-1)^{f(x)} |x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Quantum algorithm for the Deutsch-Jozsa problem



$$\begin{aligned}
|0\rangle^{\otimes n} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} &\mapsto \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\mapsto \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}$$

Hadamard transform

What do the final Hadamard gates do?

$$
\begin{aligned}
H|x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \\
&= \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}} (-1)^{xy}|y\rangle
\end{aligned}
$$

$$
\begin{aligned}
H^{\otimes n}(|x_1\rangle \otimes \cdots \otimes |x_n\rangle) &= \bigotimes_{i=1}^{n} \left(\frac{1}{\sqrt{2}} \sum_{y_i\in\{0,1\}} (-1)^{x_i y_i}|y_i\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle
\end{aligned}
$$

Quantum D-J algorithm: Finishing up

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \overset{H^{\otimes n}}{\mapsto} \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle$$

- If f is constant, the amplitude of $|y\rangle$ is

$$\pm \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} = \pm \begin{cases} 1 & \text{if } y = 0 \dots 0 \\ 0 & \text{otherwise} \end{cases}$$

  so we definitely measure $0 \dots 0$
- If f is balanced, the amplitude of $|0 \dots 0\rangle$ is

$$\sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0$$

  so we measure some nonzero string

The Deutsch-Jozsa problem: Quantum vs. classical

Above quantum algorithm uses only one query.

Need $2^n/2 + 1$ classical queries to answer with certainty.

What about randomized algorithms? Success probability arbitrarily close to 1 with a constant number of queries.

Can we get a separation between randomized and quantum computation?

Simon's problem

Problem

- Given: a black-box function $f : \{0,1\}^n \to \{0,1\}^m$
- Promise: there is some $s \in \{0,1\}^n$ such that $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus s$
- Task: determine s

One classical strategy:

- query a random x
- repeat until we find $x_i \neq x_j$ such that $f(x_i) = f(x_j)$
- output $x_i \oplus x_j$

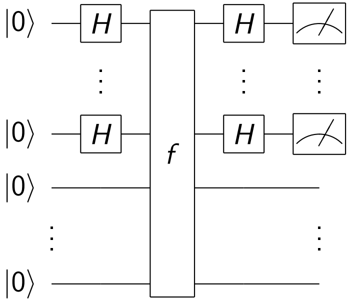
By the birthday problem, this uses about $\sqrt{2^n}$ queries.

It can be shown that this strategy is essentially optimal.

Quantum algorithm for Simon's problem

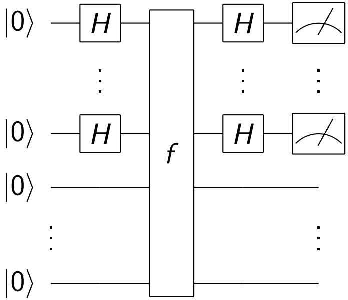
Quantum black box: $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$

$(x \in \{0,1\}^n,\ y \in \{0,1\}^m)$



Repeat many times and post-process the measurement outcomes

Quantum algorithm for Simon's problem: Analysis I



$$|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m}$$

$$\mapsto \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle^{\otimes m}$$

$$\mapsto \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle$$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in R} \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} \otimes |f(x)\rangle$$

for some $R \subset \{0, 1\}^n$

Quantum algorithm for Simon's problem: Analysis II

Recall $H^{\otimes n}|x\rangle = \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$

$$H^{\otimes n}\left(\frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} [(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}]|y\rangle$$
$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y}[1 + (-1)^{s \cdot y}]|y\rangle$$

Two cases:

- if $s \cdot y = 0 \bmod 2$, $1 + (-1)^{s \cdot y} = 2$
- if $s \cdot y = 1 \bmod 2$, $1 + (-1)^{s \cdot y} = 0$

Measuring gives a random y orthogonal to s (i.e., $s \cdot y = 0$)

Quantum algorithm for Simon's problem: Post-processing

Measuring gives a random y orthogonal to s ($s \cdot y = 0$)

Repeat k times, giving vectors $y_1, \ldots, y_k \in \{0,1\}^n$; solve a system of k linear equations for $s \in \{0,1\}^n$:

$$y_1 \cdot s = 0, \quad y_2 \cdot s = 0, \quad \ldots, \quad y_k \cdot s = 0$$

How big should k be to give a unique (nonzero) solution?

- Clearly $k \geq n-1$ is necessary
- It can be shown that $k = O(n)$ suffices

$O(n)$ quantum queries, $O(n^3)$ quantum gates

Compare to $\Omega(2^{n/2})$ classical queries (even for bounded error)

Recap

We have seen several examples of quantum algorithms that outperform classical computation:

- Deutsch's problem: 1 quantum query vs. 2 classical queries
- Deutsch-Jozsa problem: 1 quantum query vs. $2^{\Omega(n)}$ classical queries (deterministic)
- Simon's problem: $O(n)$ quantum queries vs. $2^{\Omega(n)}$ classical queries (randomized)

Quantum algorithms for more interesting problems build on the tools used in these examples.

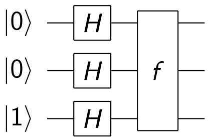
Exercise: One-out-of-four search

Let $f : \{0,1\}^2 \to \{0,1\}$ be a black-box function taking the value 1 on exactly one input. The goal is to find the unique $(x_1, x_2) \in \{0,1\}^2$ such that $f(x_1, x_2) = 1$.

- Write the truth tables of the four possible functions f.
- How many classical queries are needed to solve the problem?
- Suppose f is given as a quantum black box U_f acting as

  $$|x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$

  Determine the output of the following quantum circuit for each of the possible black-box functions f:

- Show that the four possible outputs obtained in the previous part are pairwise orthogonal. What can you conclude about the quantum query complexity of one-out-of-four search?

Part III

The QFT and phase estimation

Quantum phase estimation

Problem

We are given a unitary U and an eigenvector $|\psi\rangle$ of U with unknown eigenvalue

We seek to determine its eigenphase $\varphi \in [0, 1)$ such that

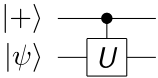
$$U|\psi\rangle = e^{2\pi i \varphi}|\psi\rangle$$

More precisely, we want to obtain an estimate $\hat{\varphi}$ such that

$$\Pr\left(|\hat{\varphi} - \varphi| \leq \frac{1}{2^n}\right) \geq \frac{3}{4}$$

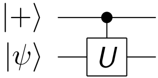
The deviation $|\hat{\varphi} - \varphi|$ is computed modulo 1

Phase kick back



$$
\begin{aligned}
\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle &= \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \\
&\mapsto \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes U|\psi\rangle \\
&= \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle + \frac{|1\rangle}{\sqrt{2}} \otimes e^{2\pi i\varphi}|\psi\rangle \\
&= \frac{|0\rangle}{\sqrt{2}} \otimes |\psi\rangle + \frac{e^{2\pi i\varphi}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \\
&= \frac{|0\rangle + e^{2\pi i\varphi}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle
\end{aligned}
$$

Phase kick back



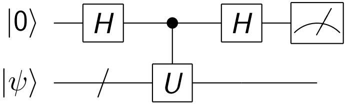
$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle \mapsto \frac{|0\rangle + e^{2\pi i\varphi}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle$$

The eigenstate $|\psi\rangle$ in the target register emerges unchanged

$\Rightarrow$ It suffices to focus on the control register

The state $|0\rangle + |1\rangle$ of the control qubit is changed to $|0\rangle + e^{2\pi i\varphi}|1\rangle$ by phase kick back

Hadamard test + phase kick back



$$
\begin{aligned}
& \frac{|0\rangle + e^{2\pi i \varphi}|1\rangle}{\sqrt{2}} \\
\mapsto \quad & \frac{1}{2}\left((|0\rangle + |1\rangle) + e^{2\pi i \varphi}(|0\rangle - |1\rangle)\right) \\
\mapsto \quad & \frac{1}{2}\left((1 + e^{2\pi i \varphi})|0\rangle + (1 - e^{2\pi i \varphi})|1\rangle)\right) := |\varphi\rangle
\end{aligned}
$$

Hadamard test + phase kick back

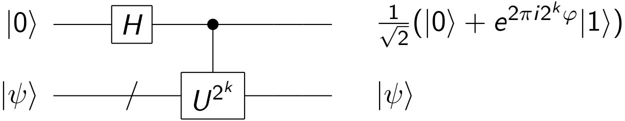
$$|\varphi\rangle = \frac{1}{2}\left((1+e^{2\pi i\varphi})|0\rangle + (1-e^{2\pi i\varphi})|1\rangle)\right)$$

The probability of obtaining 0 is

$$\begin{aligned}
\Pr(0) &= \| |0\rangle\langle 0|\,|\varphi\rangle \|^2 \\
&= |\frac{1}{2}\,(1+e^{2\pi i\varphi})|^2 \\
&= \frac{1}{4}\,|e^{\pi i\varphi} + e^{-\pi i\varphi})|^2 \\
&= \frac{1}{4}\,|2\cos(\pi\varphi)|^2 \\
&= \cos^2(\pi\varphi) = \frac{1}{2}\left(1+\cos(2\pi\varphi)\right)
\end{aligned}$$

Phase kick back due to higher powers of U

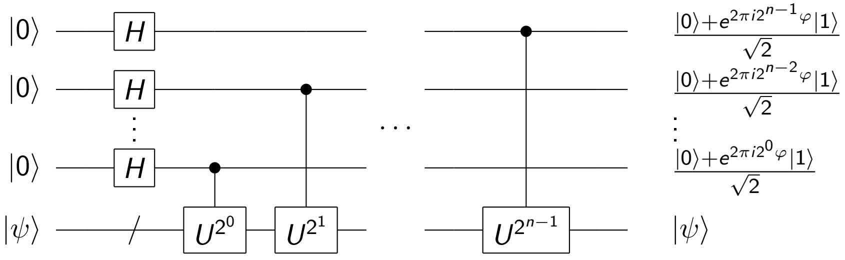
For arbitrary k, we obtain



since

$$U^{2^k}|\psi\rangle = e^{2\pi i 2^k \varphi}|\psi\rangle$$

Phase kick back part of phase estimation



We set

$$|\varphi\rangle := \frac{|0\rangle + e^{2\pi i 2^{n-1}\varphi}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i 2^{n-2}\varphi}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle}{\sqrt{2}}$$

Binary fractions

Assume that the eigenphase φ is an exact n-bit binary fraction, i.e.,

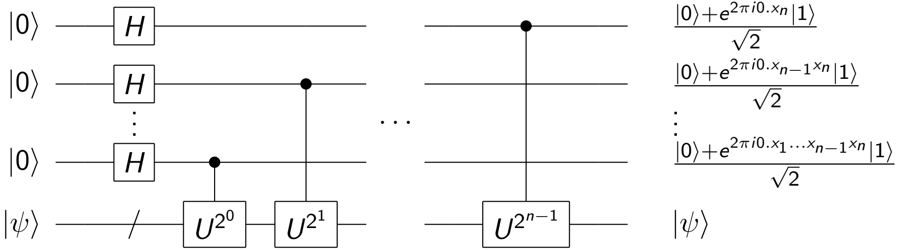
$$\varphi = 0.x_1 x_2 \dots x_n = \sum_{i=1}^{n} \frac{x_i}{2^i}$$

For arbitrary $k \in \{0, \dots, n-1\}$, we have

$$2^k \varphi = x_1 x_2 \dots x_k . x_{k+1} \dots x_n$$

$$\begin{aligned}
e^{2\pi i 2^k \varphi} &= e^{2\pi i (x_1 x_2 \dots x_k . x_{k+1} \dots x_n)} \\
&= e^{2\pi i (x_1 x_2 \dots x_k + 0.x_{k+1} \dots x_n)} \\
&= e^{2\pi i (x_1 x_2 \dots x_k)} \cdot e^{2\pi i (0.x_{k+1} \dots x_n)} \\
&= e^{2\pi i (0.x_{k+1} \dots x_n)}
\end{aligned}$$

Phase kick back part of phase estimation



Quantum Fourier transform

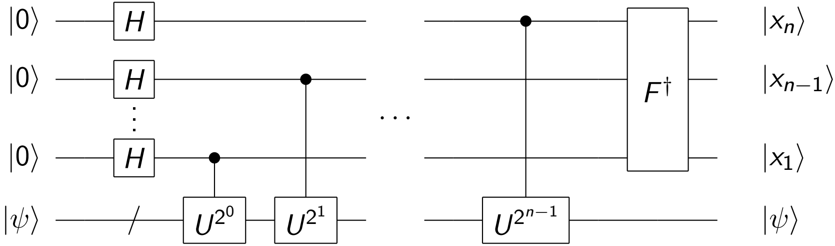
The quantum Fourier transform F is defined by

$$
\begin{aligned}
& F\big(|x_n\rangle \otimes |x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle\big) \\
= \quad & \frac{|0\rangle + e^{2\pi i 0.x_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i 0.x_{n-1}x_n}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{2\pi i 0.x_1x_2\ldots x_n}|1\rangle}{\sqrt{2}}
\end{aligned}
$$

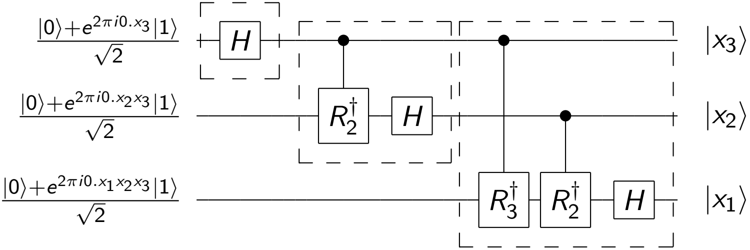
We use inverse quantum Fourier transform $F^\dagger$ to obtain the bits of the eigenphase

Note: QFT is defined by $F|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle = |0.x_1x_2\ldots x_n\rangle$ in the literature; we use the above definition for the sake of notational simplicity (otherwise, we would have to include the so-called bit-reversal)

Quantum circuit for phase estimation



Inverse quantum Fourier transform for 3 bits

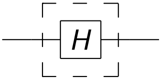


The phase shift R_k is defined by

$$R_k := \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

QPE: least significant bit – top qubit

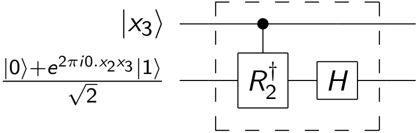
$\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}}$



$$\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + (-1)^{x_3}|1\rangle}{\sqrt{2}}$$

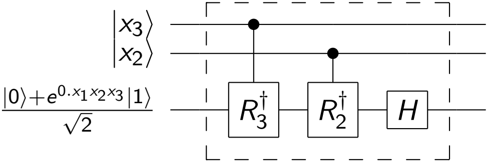
$$\xrightarrow{H} \quad |x_3\rangle$$

QPE: second bit – middle qubit



$$
\begin{aligned}
& |x_3\rangle \otimes \frac{|0\rangle + e^{2\pi i 0.x_2x_3}|1\rangle}{\sqrt{2}} \\
\xrightarrow{ctrl\ R_2^\dagger}\quad & |x_3\rangle \otimes \frac{|0\rangle + e^{2\pi i 0.x_2 0}|1\rangle}{\sqrt{2}} \\
\xrightarrow{I \otimes H}\quad & |x_3\rangle \otimes |x_2\rangle
\end{aligned}
$$

QPE: most significant bit – bottom qubit



$$
\begin{aligned}
& |x_3\rangle \otimes |x_2\rangle \otimes \frac{|0\rangle + e^{2\pi i 0.x_1x_2x_3}|1\rangle}{\sqrt{2}} \\
\xrightarrow{ctrl\ R_3^\dagger} \quad & |x_3\rangle \otimes |x_2\rangle \otimes \frac{|0\rangle + e^{2\pi i 0.x_1x_20}|1\rangle}{\sqrt{2}} \\
\xrightarrow{ctrl\ R_2^\dagger} \quad & |x_3\rangle \otimes |x_2\rangle \otimes \frac{|0\rangle + e^{2\pi i 0.x_100}|1\rangle}{\sqrt{2}} \\
\xrightarrow{I\otimes I\otimes H} \quad & |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle
\end{aligned}
$$

Summary of phase estimation circuit

We use phase kick back due to the controlled U^{2^k} gate to prepare the state

$$\frac{|0\rangle + e^{2\pi i 0.x_{k+1}x_{k+2}\dots x_n}|1\rangle}{\sqrt{2}}$$

Using the previously determined bits $x_{k+2}, \dots, x_n$, we change this state to

$$\frac{|0\rangle + e^{2\pi i 0.x_{k+1}0\dots 0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + (-1)^{x_k}|1\rangle}{\sqrt{2}}$$

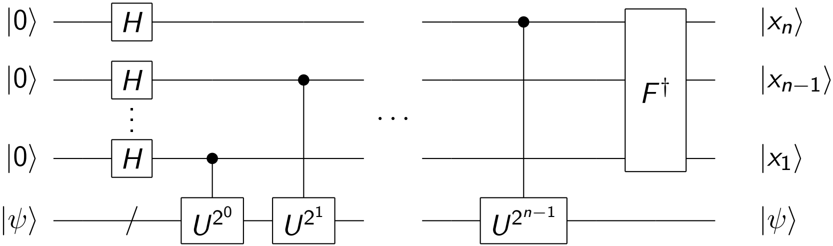
We apply the Hadamard gate to obtain

$$|x_{k+1}\rangle$$

The controlled phase shifts enable us to reduce the problem of determining each bit to distinguishing between $|+\rangle$ and $|-\rangle$ (deterministic Hadamard test)

Special case: exact n-bit binary fraction

Assume that φ is an exact n-bit binary fraction, i.e., $\varphi = 0.x_1 \dots x_{n-1} x_n$



$\Rightarrow$ The measurment of the qubits yields the bits $x_n, x_{n-1}, \dots, x_1$ deterministically

General case: arbitrary eigenphases

Let φ be arbitrary

Unless φ is an exact n-bit fraction, the application of the inverse quantum Fourier transform

$$F^{\dagger}|\varphi\rangle$$

produces a superposition of n-bit strings

Geometric summation

Lemma

We have

$$\begin{aligned}\sum_{y=0}^{N-1} e^{2\pi i\theta y} &= N \text{ for } \theta = 0\\ \sum_{y=0}^{N-1} e^{2\pi i\theta y} &= \frac{1-e^{2\pi i N\theta}}{1-e^{2\pi i\theta}} \text{ for } \theta \in (0,1)\end{aligned}$$

Assume that $\theta = \frac{x}{N}$ for some $x \in [0, N-1]$

$\Rightarrow$ We have

$$\sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y} = N\,\delta_{x,0}$$

Probability of obtaining a certain estimate

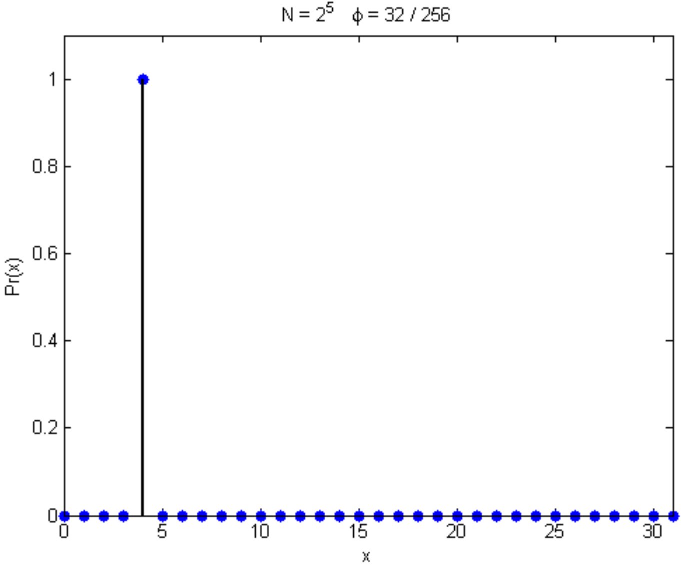
Lemma

Let $x = \sum_{k=1}^{n} x_i 2^{n-i}$ *and* $\varphi_x := 0.x_1 x_2 \ldots x_n = \frac{x}{2^n}$ *be the corresponding n-bit fraction*

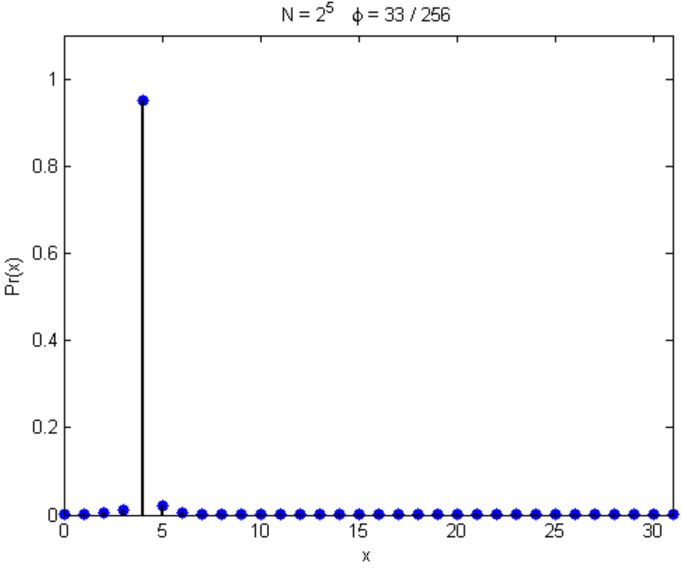
The probability of obtaining the estimate φ_x *is*

$$\Pr(x) = \frac{1}{2^{2n}} \frac{\sin^2\left(2^n \pi \left(\varphi - \varphi_x\right)\right)}{\sin^2\left(\pi \left(\varphi - \varphi_x\right)\right)}$$

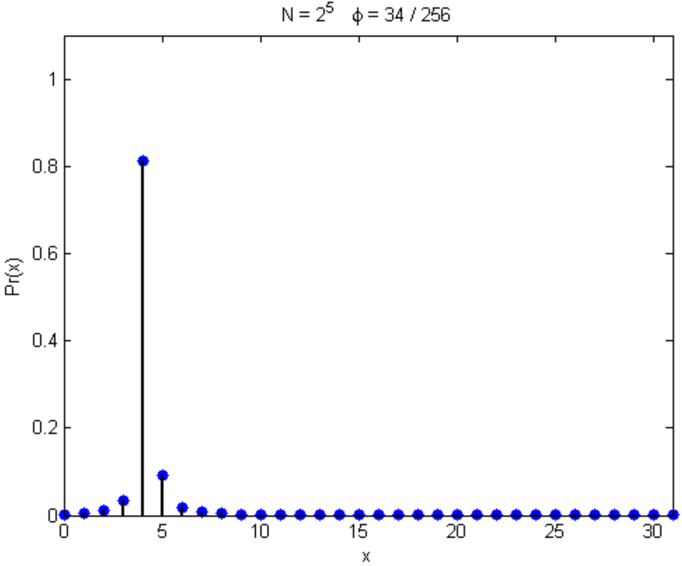
Examples of probability distributions for different φ



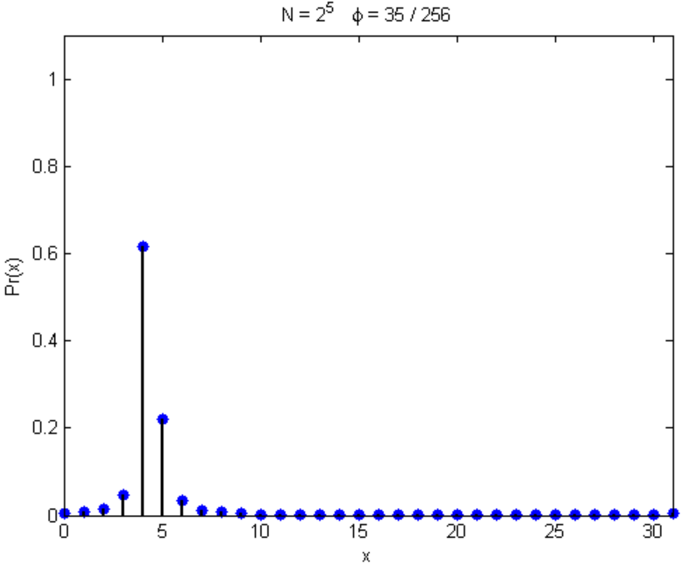
Examples of probability distributions for different φ



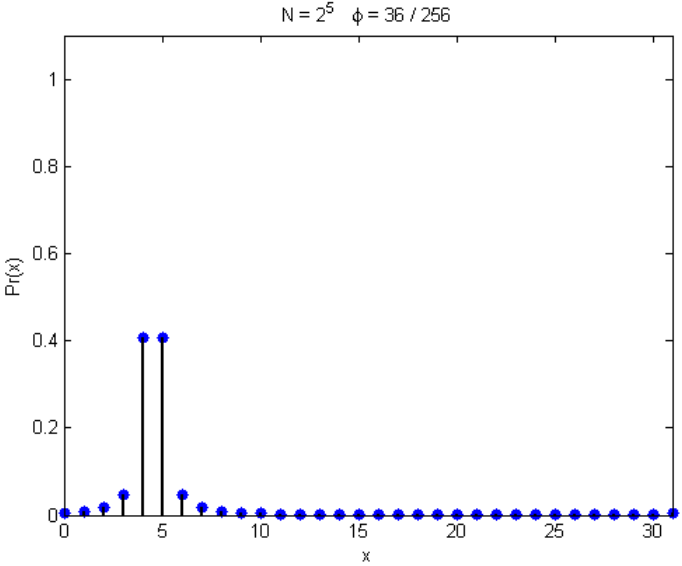
Examples of probability distributions for different φ



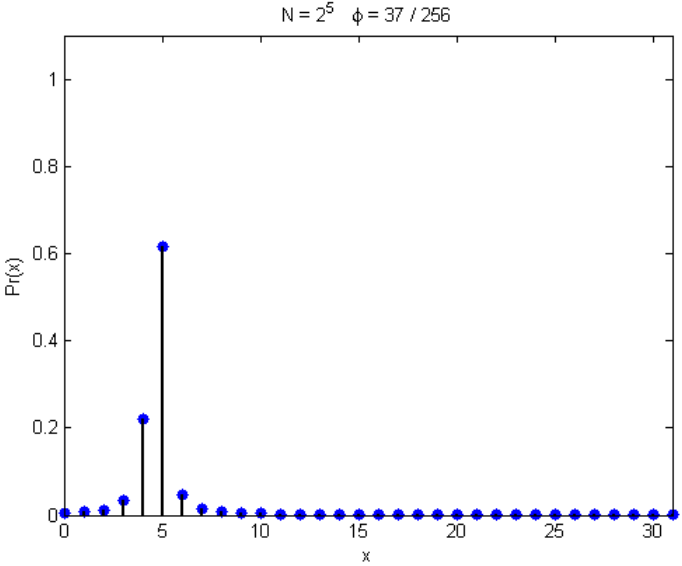
Examples of probability distributions for different φ



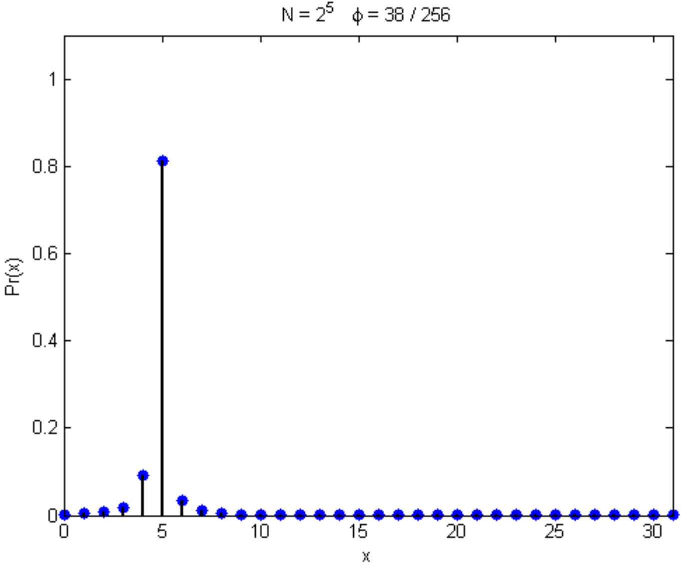
Examples of probability distributions for different φ



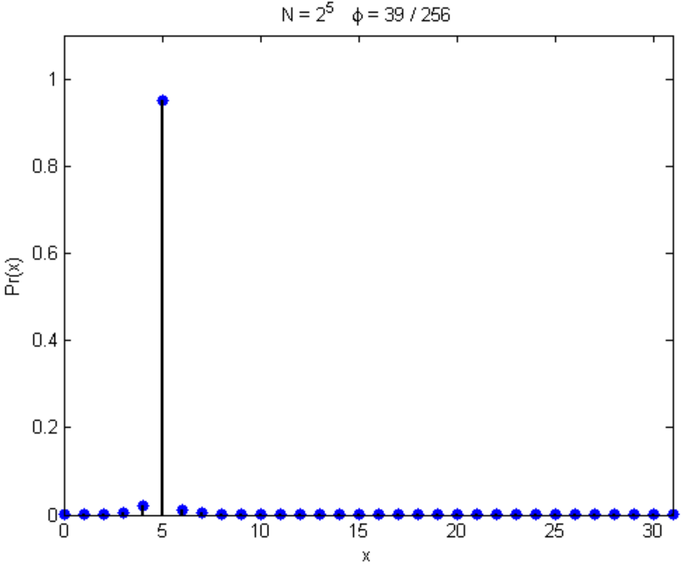
Examples of probability distributions for different φ



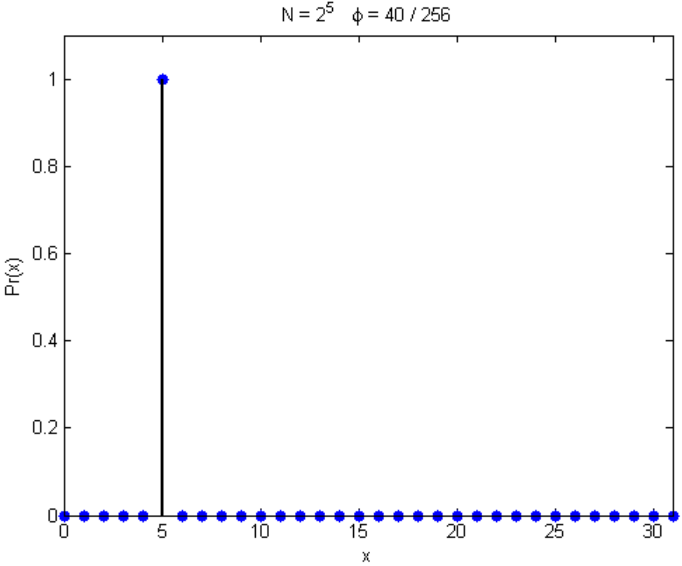
Examples of probability distributions for different φ



Examples of probability distributions for different φ



Examples of probability distributions for different φ



Probability of obtaining a certain estimate

Proof.

The probability of obtaining the estimate φ_x is

$$
\begin{aligned}
& \Pr(x) \\
= \quad & |\langle x|F^{\dagger}|\varphi\rangle|^2 \\
= \quad & |\langle \varphi_x|\varphi\rangle|^2 \\
= \quad & \frac{1}{2^{2n}}\Big|\sum_{y=0}^{2^n-1} e^{2\pi i\,(\varphi-\varphi_x)\,y}\Big|^2 \quad \text{geometric summation} \\
= \quad & \frac{1}{2^{2n}}\left|\frac{1-e^{2\pi i(2^n(\varphi-\varphi_x))}}{1-e^{2\pi i(\varphi-\varphi_x)}}\right|^2 \quad |1-e^{i2\theta}| = |e^{-i\theta}-e^{i\theta}| = 2|\sin\theta| \\
= \quad & \frac{1}{2^{2n}}\frac{\sin^2(2^n\,\pi(\varphi-\varphi_x))}{\sin^2(\pi(\varphi-\varphi_x))}
\end{aligned}
$$

□

Lower bound on success probability

Theorem

Let x be such that $\frac{x}{2^n} \leq \varphi < \frac{x+1}{2^n}$

The probability of returning one of the two closest n-bit fractions φ_x and φ_{x+1} is at least $\frac{8}{\pi^2}$

Proof of lower bound on success probability

$$\begin{aligned}\Pr(\text{success}) &:= \Pr(x) + \Pr(x+1)\\ &= \frac{1}{2^{2n}}\left(\Big|\sum_{y=0}^{2^n-1} e^{2\pi i(\varphi-\varphi_x)y}\Big|^2 + \Big|\sum_{y=0}^{2^n-1} e^{2\pi i(\varphi-\varphi_x)y}\Big|^2 \right)\end{aligned}$$

This function attains its minimum at $\varphi = \frac{1}{2}(\varphi_x + \varphi_{x+1}) \quad \Rightarrow$

$$\begin{aligned}\Pr(\text{success}) &\geq \frac{2}{2^{2n}}\left(\Big|\sum_{y=0}^{2^n-1} e^{2\pi i \frac{y}{2^{n+1}}}\Big|^2 \right)\\ &\geq \frac{2}{2^{2n}} \frac{4}{4\sin^2(\frac{\pi}{2^{n+1}})}\\ &\geq \frac{8}{\pi^2}\end{aligned}$$

The last inequality follows from $\frac{1}{|\sin\theta|^2} \geq \frac{1}{|\theta|^2}$

Summary of phase estimation

We are given a unitary U and an eigenvector $|\psi\rangle$ of U with unknown eigenphase φ

We obtain an estimate $\hat{\varphi}$ such that

$$\Pr\left(|\hat{\varphi} - \varphi| \leq \frac{1}{2^n}\right) \geq \frac{8}{\pi^2}$$

To do this, we need invoke each of the controlled U, $U^2, \ldots, U^{2^{n-1}}$ gates once

We can boost the success probability to $1 - \epsilon$ by repeating the above algorithm $O(\log(1/\epsilon))$ times and outputting the median of the outcomes

Phase estimation applied to superpositions of eigenstates

We are given a unitary U with eigenvectors $|\psi_i\rangle$ and corresponding eigenphases φ_i

Let

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$$

What happens if we apply phase estimation to $|0\rangle^{\otimes n} \otimes |\psi\rangle$?

After the n phase kick-backs due to U^{2^0}, U^{2^1}, $\ldots$ $U^{2^{n-1}}$, we obtain

$$\sum_i \alpha_i |\varphi_i\rangle \otimes |\psi_i\rangle$$

After applying the inverse quantum Fourier transform, we obtain

$$\sum_i \alpha_i |\tilde{x}_i\rangle \otimes |\psi_i\rangle$$

where $|\tilde{x}_i\rangle$ denotes a superpositions of n-bit estimates of φ_i

Part IV

Factoring

The fundamental theorem of arithmetic

Theorem

Every positive integer larger than 1 can be factored as a product of prime numbers, and this factorization is unique (up to the order of the factors).

$$N = 2^{n_2} \times 3^{n_3} \times 5^{n_5} \times 7^{n_7} \times \cdots$$

Examples

$$15 = 3 \times 5$$

$$239815173914273 = 15485863 \times 15486071$$

$$
\begin{array}{r}
3107418240490043721350750 \\
0358885679300373460228427 \\
2754572016194882320644051 \\
8081504556346829671723286 \\
7824379162728380334154710 \\
7310850191954852900733772 \\
4822783525742386454014691 \\
736602477652346609
\end{array}
=
\begin{array}{l}
16347336458092538484 \\
43133883865090859841 \\
78367003309231218111 \\
08523893331001045081 \\
51212118167511579 \\
\qquad\qquad\times \\
19008712816648221131 \\
26851573935413975471 \\
89678996851549366663 \\
85390880271038021044 \\
98957191261465571
\end{array}
$$

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

– Carl Friedrich Gauss, Disquisitiones Arithmeticæ (1801)

RSA

Alice

Eve

Bob

M
message

primes p, q

n $\quad$ n $\quad$ $n = pq$

e $\quad$ e $\quad$ $e \in \mathbb{Z}^{\times}_{(p-1)(q-1)}$
encryption key

$d := e^{-1} \mod (p-1)(q-1)$
decryption key

$C := M^e \mod n$
ciphertext

C

$C^d = M^{ed} \mod n = M$

Order finding

Definition

Given $a, N \in \mathbb{Z}$ with $\gcd(a, N) = 1$, the *order* of a modulo N is the smallest positive integer r such that $a^r \equiv 1 \pmod{N}$.

Problem

- Given: $a, N \in \mathbb{Z}$ with $\gcd(a, N) = 1$
- Task: find the order of a modulo N

Spectrum of a cyclic shift

Let P be a cyclic shift modulo r: $P|x\rangle = |x + 1 \bmod r\rangle$

Claim. For any $k \in \mathbb{Z}$, the state $|u_k\rangle := \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i k x / r} |x\rangle$ is an eigenstate of P.

Proof.
$$
\begin{aligned}
U|u_k\rangle &= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i k x / r} |x + 1 \bmod r\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{2\pi i k / r} e^{-2\pi i k (x+1) / r} |x + 1 \bmod r\rangle \\
&= e^{2\pi i k / r} \frac{1}{\sqrt{r}} \sum_{x=1}^{r} e^{-2\pi i k x / r} |x \bmod r\rangle \\
&= e^{2\pi i k / r} |u_k\rangle
\end{aligned}
$$
$\square$

The multiplication-by-a map

Define U by $U|x\rangle = |ax\rangle$ for $x \in \mathbb{Z}_N$.

Computing U:

$$\begin{aligned} |x, 0\rangle &\mapsto |x, ax\rangle && \text{(reversible multiplication by } a\text{)} \\ &\mapsto |ax, x\rangle && \text{(swap)} \\ &\mapsto |ax, 0\rangle && \text{(uncompute reversible division by } a\text{)} \end{aligned}$$

High powers of U can be implemented efficiently using repeated squaring

Spectrum of the multiplication-by-a map

Define U by $U|x\rangle = |ax\rangle$ for $x \in \mathbb{Z}_N$.

Claim. Let r be the order of a modulo N. For any $k \in \mathbb{Z}$, the state

$$|u_k\rangle := \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi \mathrm{i} kx/r} |a^x \bmod N\rangle$$

is an eigenstate of U with eigenvalue $e^{2\pi \mathrm{i} k/r}$.

Proof.
Same as for the cyclic shift, due to the isomorphism

$$x \bmod r \quad \leftrightarrow \quad a^x \bmod N \qquad \square$$

Order finding and phase estimation

$U|u_k\rangle = e^{2\pi i k/r}|u_k\rangle$

Phase estimation of U on $|u_k\rangle$ can be used to approximate k/r.

Problems:

- We don't know r, so we can't prepare $|u_k\rangle$.
- We only get an approximation of k/r.
- Even if we knew k/r exactly, k and r could have common factors.

Estimating k/r in superposition

A useful identity:

$$\sum_{k=0}^{r-1} e^{2\pi \mathrm{i} kx/r} = \begin{cases} r & \text{if } x = 0 \\ 0 & \text{otherwise} \end{cases}$$

Consider

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = \frac{1}{r} \sum_{k,x=0}^{r-1} e^{-2\pi \mathrm{i} kx/r} |a^x \bmod N\rangle$$

$$= |a^0 \bmod N\rangle = |1\rangle$$

Phase estimation:

$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |0\rangle \otimes |u_k\rangle \mapsto \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\widetilde{k/r}\rangle \otimes |u_k\rangle$$

Measurement gives an approximation of k/r for a random k

Continued fractions

Problem

Given samples x of the form $\lfloor k\frac{2^n}{r} \rfloor$, $\lceil k\frac{2^n}{r} \rceil$ ($k \in \{0, 1, \dots, r-1\}$), determine r.

Continued fraction expansion:

$$\frac{x}{2^n} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Gives an efficiently computable sequence of rational approximations

Theorem

If $2^n \geq N^2$, then k/r is the closest convergent of the CFE to $x/2^n$ among those with denominator smaller than N.

Since $r < N$, it suffices to take $n = 2\log_2 N$

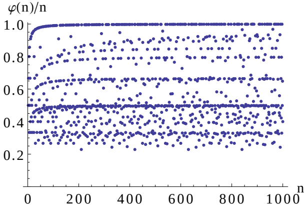
Common factors

If $\gcd(k, r) = 1$, then the denominator of k/r is r

Fact

The probability that $\gcd(k, r) = 1$ *for a random* $k \in \{0, 1, \ldots, r-1\}$ *is*

$$\frac{\phi(r)}{r} = \Omega\left(\frac{1}{\log\log r}\right)$$



Thus $\Omega(\log\log N)$ repetitions suffice to give r with constant probability

Alternatively, find two (or more) denominators and take their least common multiple; then $O(1)$ repetitions suffice

Factoring $\rightarrow$ finding a nontrivial factor

Suppose we want to factor the positive integer N.

Since primality can be tested efficiently, it suffices to give a procedure for finding a nontrivial factor of N with constant probability.

```
function factor(N)

if N is prime
     output N
else
     repeat
          x=find_nontrivial_factor(N)
     until success
     factor(x)
     factor(N/x)
end if
```

We can assume N is odd, since it is easy to find the factor 2.

We can also assume that N contains at least two distinct prime powers, since it is easy to check if it is a power of some integer.

Reduction of factoring to order finding

Factoring N reduces to order finding in $\mathbb{Z}_N^\times$ [Miller 1976].

Choose $a \in \{2, 3, \ldots, N-1\}$ uniformly at random.

If $\gcd(a, N) \neq 1$, then it is a nontrivial factor of N.

If $\gcd(a, N) = 1$, let r denote the order of a modulo N.

Suppose r is even. Then

$$\begin{gathered} a^r = 1 \bmod N \\ \Updownarrow \\ (a^{r/2})^2 - 1 = 0 \bmod N \\ \Updownarrow \\ (a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N \end{gathered}$$

so we might hope that $\gcd(a^{r/2} - 1, N)$ is a nontrivial factor of N.

Miller's reduction

Question

Given $(a^{r/2}-1)(a^{r/2}+1) = 0 \bmod N$, when does $\gcd(a^{r/2}-1, N)$ give a nontrivial factor of N?

Note that $a^{r/2} - 1 \neq 0 \bmod N$ (otherwise the order of a would be $r/2$, or smaller).

So it suffices to ensure that $a^{r/2} + 1 \neq 0 \bmod N$.

Lemma

Suppose $a \in \mathbb{Z}_N^\times$ is chosen uniformly at random, where N is an odd integer with at least two distinct prime factors. Then with probability at least $1/2$, the order r of a is even and $a^{r/2} \neq -1 \bmod N$.

Proof (part 1 of 2)

$$\begin{aligned} \text{Let } N &= p_1^{m_1} \times \cdots \times p_k^{m_k} \quad (p_i \text{ distinct odd primes, } k \geq 2) \\ a &= a_i \bmod p_i^{m_i} \\ r_i &= \text{order of } a_i \bmod p_i^{m_i} \\ 2^{c_i} &= \text{largest power of 2 that divides } r_i \end{aligned}$$

Claim 1. *If r is odd or $a^{r/2} + 1 = 0 \bmod N$, then $c_1 = \cdots = c_k$.*

Since $r = \mathrm{lcm}(r_1, \ldots, r_k)$, r is odd iff $c_1 = \ldots = c_k = 0$.

If r is even and $a^{r/2} = -1 \bmod N$, then $a^{r/2} = -1 \bmod p_i^{m_i}$ for each i, so r_i does not divide $r/2$; but notice that r_i does divide r.

Hence r/r_i is an odd integer for each i, and every r_i must contain the same number of powers of 2 as r.

Proof (part 2 of 2)

Claim 2. $\Pr(c_i = \textit{any particular value}) \leq 1/2$

(Then the lemma follows, since in particular $\Pr(c_1 = c_2) \leq 1/2$.)

$$\begin{array}{c} a \in \mathbb{Z}_N^\times \\ \text{uniformly at random} \end{array} \quad \Leftrightarrow \quad \begin{array}{c} a_i \in \mathbb{Z}_{p_i^{m_i}}^\times \\ \text{uniformly at random} \end{array}$$

Since $\mathbb{Z}_{p_i^{m_i}}^\times$ is cyclic and of even order, exactly half its elements have the maximal value of c_i, so in particular the probability of any particular c_i is at most $1/2$.

Shor's algorithm

Input: Integer N
Output: A nontrivial factor of N

1. Choose a random $a \in \{2, 3, \ldots, N-1\}$
2. Compute $\gcd(a, N)$; if it is not 1 then it is a nontrivial factor, and otherwise we continue
3. Perform phase estimation with the multiplication-by-a operator U on the state $|1\rangle$ using $n = 2\log_2 N$ bits of precision
4. Compute the continued fraction expansion of the estimated phase, and find the best approximation with denominator less than N; call the result r
5. Compute $\gcd(a^{r/2} - 1, N)$. If it is a nontrivial factor of N, we are done; if not, go back to step 1

Quantum vs. classical factoring algorithms

Best known classical algorithm for factoring N

- Proven running time: $2^{O((\log N)^{1/2}(\log\log N)^{1/2})}$
- With plausible heuristic assumptions: $2^{O((\log N)^{1/3}(\log\log N)^{1/3})}$

Shor's quantum algorithm

- QFT modulo 2^n with $n = O(\log N)$: takes $O(n^2)$ steps
- Modular exponentiation: compute a^x for $x < 2^n$. With repeated squaring, takes $O(n^3)$ steps
- Running time of Shor's algorithm: $O(\log^3 N)$

Beyond factoring

There are many fast quantum algorithms based on related ideas

- Computing discrete logarithms
- Decomposing abelian/solvable groups
- Estimating Gauss sums
- Counting points on algebraic curves
- Computations in number fields (Pell's equation, etc.)
- Abelian hidden subgroup problem
- Non-abelian hidden subgroup problem?

Part V

Quantum search

Unstructured search

Quantum computers can quadratically outperform classical computers at a very basic computational task, called unstructured search.

There is a set X containing N items, some of which are marked

We are given a Boolean black box $f : X \to \{0, 1\}$ that indicates whether a given item is marked

The problem is to decide if any item is marked, or alternatively, to find a marked item given that one exists

Applications of unstructured search

Unstructured search can be thought of as a model for solving problems in NP by brute force search

If a problem is in NP, then we can efficiently recognize a solution, so one way to find a solution is to solve unstructured search

Of course, this may not be the best way to find a solution in general, even if the problem is NP-hard

We don't know if NP-hard problems are really "unstructured"

Unstructured search

It is obvious that even a randomized classical algorithm needs $\Omega(N)$ queries to decide if any item is marked

On the other hand, a quantum algorithm can do much better!

Phase oracle

We assume that we a unitary operator U satisfying

$$U|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & x \text{ is not marked} \\ -|x\rangle & x \text{ is marked} \end{cases}$$

Target state

We consider the case where there is exactly one $x \in X$ element that is marked; call this element m

Our goal is to prepare the state $|m\rangle$

Initial state

We have no information about which item might be marked

$\Rightarrow$ We take

$$|\psi\rangle := \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

as the initial state

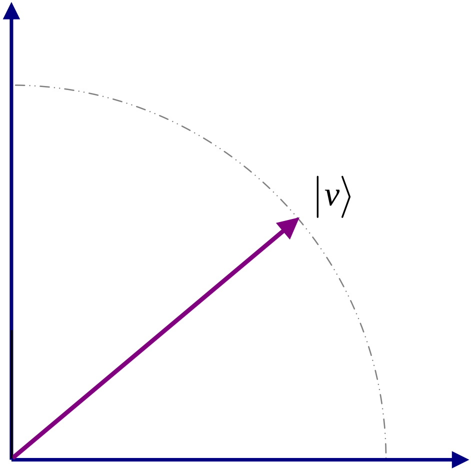
Rough idea behind Grover search

We start with the initial state $|\psi\rangle$

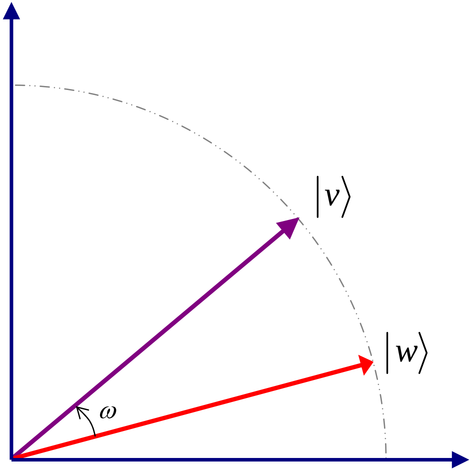
We prepare the target state $|m\rangle$ by implementing a rotation that moves $|\psi\rangle$ toward $|m\rangle$

We realize the rotation with the help of two reflections

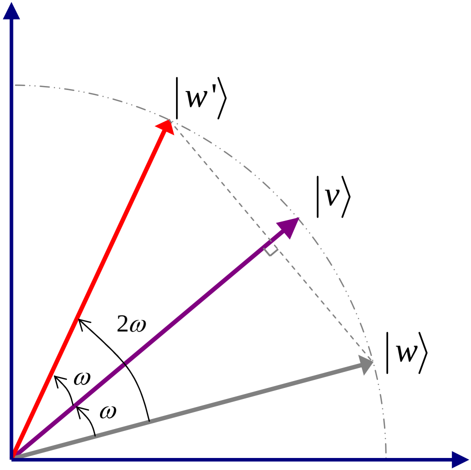
Visualization of a reflection in $\mathbb{R}^2$



Visualization of a reflection in $\mathbb{R}^2$



Visualization of a reflection in $\mathbb{R}^2$



Reflections

$U = I - 2|m\rangle\langle m|$ is a reflection about the target state $|m\rangle$

$V = I - 2|\psi\rangle\langle\psi|$ is the reflection around about the initial state $|\psi\rangle$:

$$\begin{aligned} V|\psi\rangle &= -|\psi\rangle \\ V|\psi^\perp\rangle &= \quad |\psi^\perp\rangle \end{aligned}$$

for any state $|\psi^\perp\rangle$ orthogonal to $|\psi\rangle$

Structure of Grover

The algorithm is as follows:

- start in $|\psi\rangle$,
- apply the Grover iteration $G := V\,U$ some number of times,
- make a measurement, and hope that the outcome is m

Invariant subspace

Observe that $\mathrm{span}\{|m\rangle, |\psi\rangle\}$ is a U- and V-invariant subspace, and both the inital and target states belong to this subspace

$\Rightarrow$ It suffices to understand the restriction of VU to this subspace

Consider an orthonormal basis $\{|m\rangle, |\phi\rangle\}$ for $\mathrm{span}\{|m\rangle, |\psi\rangle\}$

The Gram-Schmidt process yields

$$|\phi\rangle = \frac{|\psi\rangle - \alpha|m\rangle}{\sqrt{1-\alpha^2}}$$

where $\alpha := \langle m|\psi\rangle = 1/\sqrt{N}$

Invariant subspace

Now in the basis $\{|m\rangle, |\phi\rangle\}$, we have

$$
\begin{aligned}
|\psi\rangle &= \sin\theta|m\rangle + \cos\theta|\phi\rangle \text{ where } \sin\theta = \langle m|\psi\rangle = 1/\sqrt{N} \\
U &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\
V &= I - 2|\psi\rangle\langle\psi| \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - 2\begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix}\begin{pmatrix} \sin\theta & \cos\theta \end{pmatrix} \\
&= \begin{pmatrix} 1 - 2\sin^2\theta & -2\sin\theta\cos\theta \\ -2\sin\theta\cos\theta & 1 - 2\cos^2\theta \end{pmatrix} \\
&= -\begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}
\end{aligned}
$$

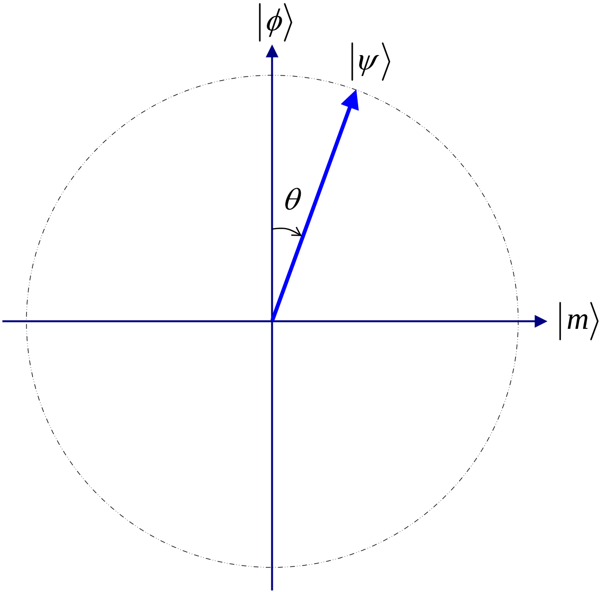
Grover iteration within the invariant subspace

$\Rightarrow$ We find

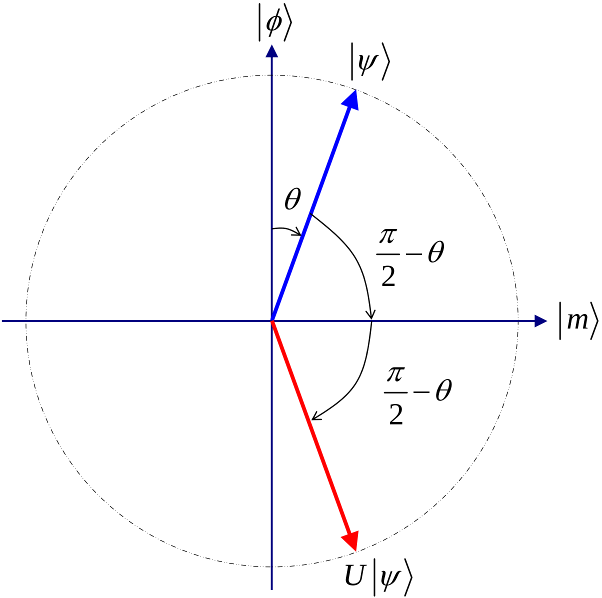
$$\begin{aligned} V\,U &= -\begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= -\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix} \end{aligned}$$

This is a rotation up to a minus sign

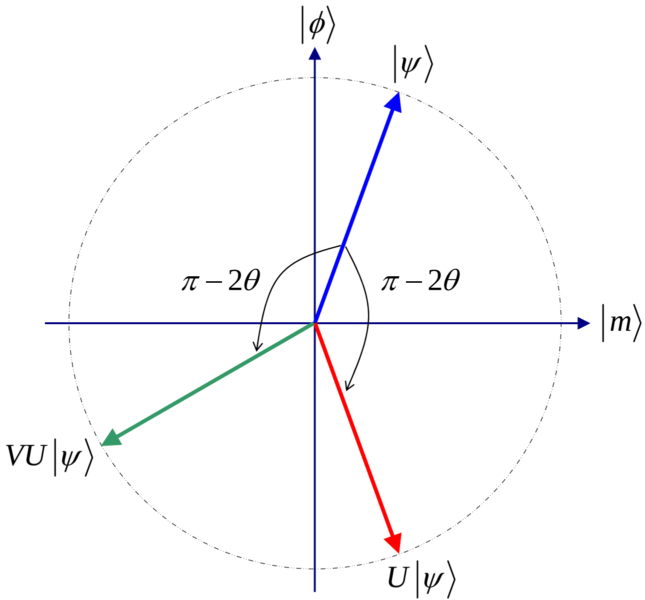
Visualization of first Grover iteration



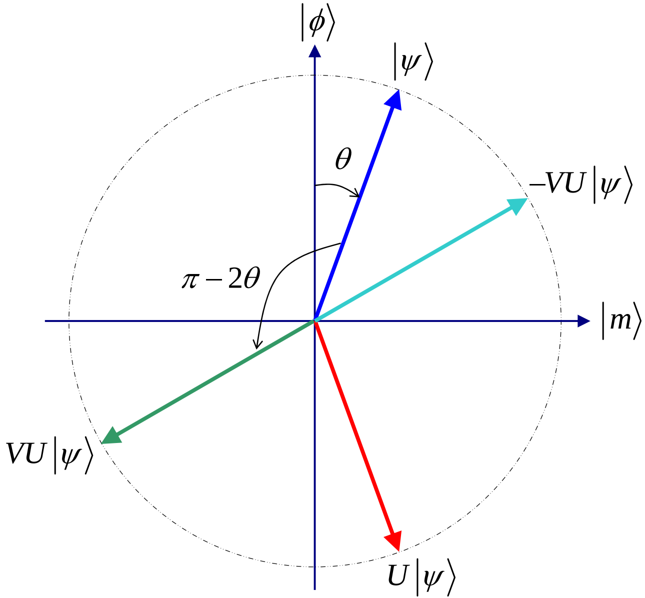
Visualization of first Grover iteration



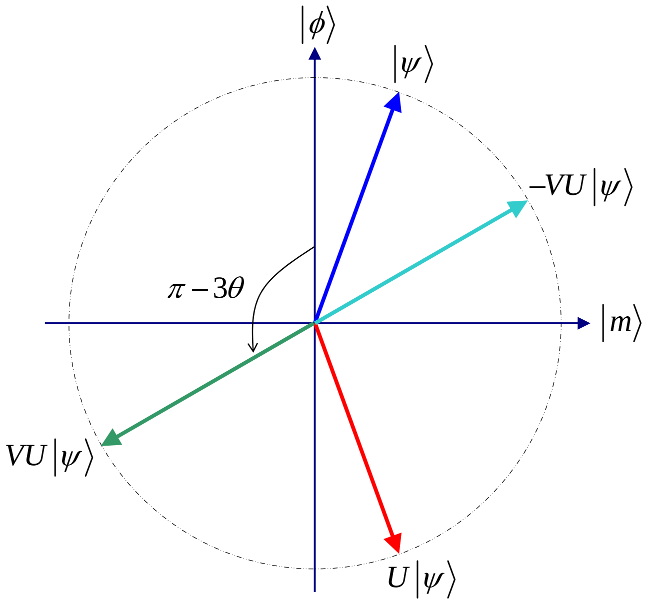
Visualization of first Grover iteration



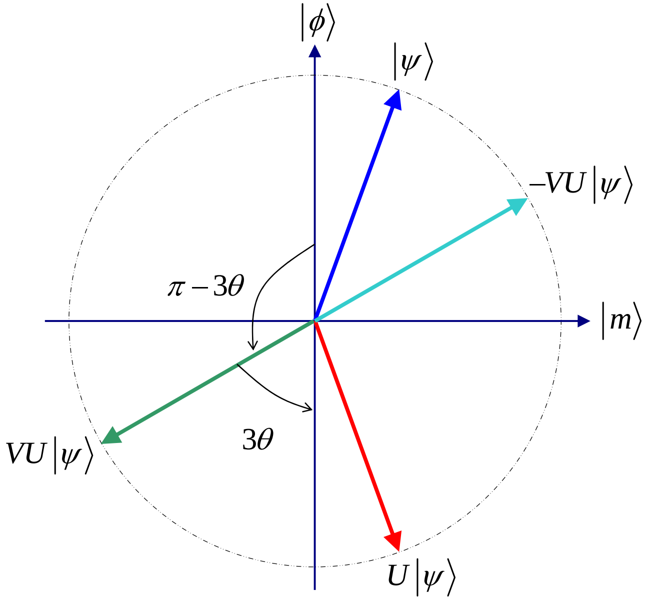
Visualization of first Grover iteration



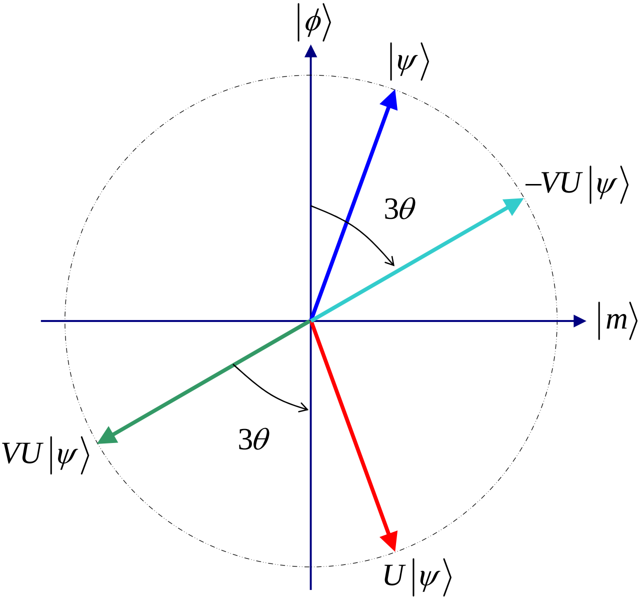
Visualization of first Grover iteration



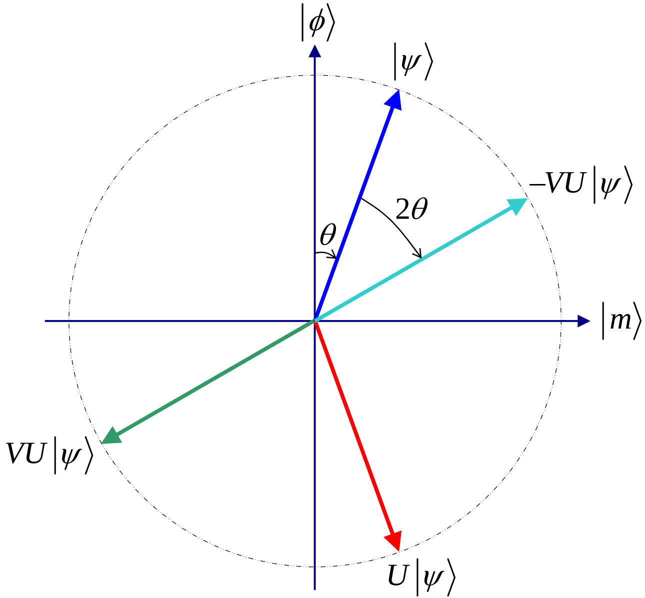
Visualization of first Grover iteration



Visualization of first Grover iteration



Visualization of first Grover iteration



Grover search

Geometrically, U is a reflection around the $|m\rangle$ axis and V is a reflection around the $|\psi\rangle$ axis, which is almost but not quite orthogonal to the $|m\rangle$ axis

The product of these two reflections is a clockwise rotation by an angle 2θ, up to an overall minus sign

From this geometric picture, or by explicit calculation using trig identities, it is easy to verify that

$$(VU)^k = (-1)^k \begin{pmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{pmatrix}$$

Grover search

Recall that our initial state is $|\psi\rangle = \sin\theta|m\rangle + \cos\theta|\phi\rangle$

How large should k be before $(VU)^k|\psi\rangle$ is close to $|m\rangle$?

We start an angle θ from the $|\phi\rangle$ axis and rotate toward $|m\rangle$ by an angle 2θ per iteration

$\Rightarrow$ To rotate by $\pi/2$, we need

$$\begin{aligned} \theta + 2k\theta &= \pi/2 \\ k &\approx \frac{\pi}{4}\theta^{-1} \approx \frac{\pi}{4}\sqrt{N} \end{aligned}$$

Grover search

It is easy to calculate that

$$|\langle m|(VU)^k|\psi\rangle|^2 = \sin^2((2k+1)\theta)$$

This is the probability that, after k steps of the algorithm, a measurement reveals the marked state

We are solving a completely unstructured search problem with N possible solutions, yet we can find a unique solution in only $O(\sqrt{N})$ queries!

While this is only a polynomial separation, it is very generic, and it is surprising that we can obtain a speedup for a search in which we have so little information to go on

Grover search

It can also be shown that this quantum algorithm is optimal

Any quantum algorithm needs at least $\Omega(\sqrt{N})$ queries to find a marked item (or even to decide if some item is marked)

Multiple solutions

Assume that there are t marked items

$\Rightarrow$ There is a two-dimensional invariant subspace spanned by span$\{|\mu\rangle, |\psi\rangle\}$ where

$$|\mu\rangle = \frac{1}{\sqrt{t}} \sum_{x \text{ marked}} |x\rangle$$

is the uniform superposition of all solutions

The Gram-Schmidt process yields the ONB $\{|\mu\rangle, |\phi\rangle\}$ where

$$|\phi\rangle = \frac{1}{\sqrt{N - t}} \sum_{x \text{ unmarked}} |x\rangle$$

is the uniform superposition of all non-solutions

Invariant subspace

Now in the basis $\{|\mu\rangle, |\phi\rangle\}$, we have

$$
\begin{aligned}
|\psi\rangle &= \sin\theta|\mu\rangle + \cos\theta|\phi\rangle \text{ where } \sin\theta = \langle\mu|\psi\rangle = \sqrt{\frac{t}{N}} \\
VU &= -\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}
\end{aligned}
$$

Overshooting

The success probability is given by

$$\sin((2k+1)\theta) \text{ where } \sin\theta = \sqrt{\frac{t}{N}}$$

$\Rightarrow$ We need to apply VU

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{t}}$$

times

Due to the oscillatory behaviour of the success probability it is important not to overshoot, i.e., to choose a number of iterations that it too large, so that the probability starts decreasing

Quantum counting

The eigenvalues of

$$-VU = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}$$

are $e^{i2\theta}$ and $e^{-i2\theta}$

The initial state $|\psi\rangle$ is a superposition of the two eigenvectors corresponding to the above two eigenvalues

$\Rightarrow$ Using phase estimation, we can obtain an estimate $\tilde{\theta}$ such that

$$|\theta - \tilde{\theta}| \leq \epsilon$$

by invoking the controlled version of $-VU$

$$O(1/\epsilon) \text{ times}$$

Quantum counting

Using the estimate $\tilde{\theta}$, we obtain an estimate $\tilde{t}$ satifying

$$|t - \tilde{t}| \leq (2\sqrt{tN} + \epsilon)\,\epsilon$$

Quantum counting

We use the following two inequalities:

$$
\begin{aligned}
|\sin\theta + \sin\tilde{\theta}| &\leq 2\sin\theta + |\theta - \tilde{\theta}| \leq 2\sqrt{\frac{t}{N}} + \epsilon \\
|\sin\theta - \sin\tilde{\theta}| &\leq |\theta - \tilde{\theta}| \leq \epsilon
\end{aligned}
$$

We have

$$
\begin{aligned}
\left|\frac{t}{N} - \frac{\tilde{t}}{N}\right| &= |\sin^2\theta - \sin^2\tilde{\theta}| \\
&= |\sin\theta + \sin\tilde{\theta}|\,|\sin\theta - \sin\tilde{\theta}| \\
&\leq \left(2\sqrt{\frac{t}{N}} + \epsilon\right)\epsilon
\end{aligned}
$$

Amplitude amplification

Assume that there is a classical (randomized) algorithm that produces a solution to some problem with probability p

Assume that we can recognized if the output produced by the algorithm is a valid solution or not

$\Rightarrow$ We repeat the algorithm until we obtain a solution

The expected number of times we have to repeat is $O(1/p)$ (geometric random variable)

Quantum amplitude amplification makes it possible to reduce the complexity to $O(1/\sqrt{p})$

Part VI

Quantum walk

Randomized algorithms

Randomness is an important tool in computer science

Black-box problems

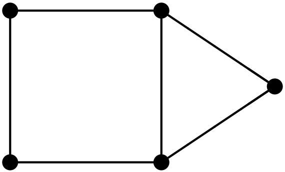
- Huge speedups are possible (Deutsch-Jozsa: $2^{\Omega(n)}$ vs. $O(1)$)
- Polynomial speedup for some total functions (game trees: $\Omega(n)$ vs. $O(n^{0.754})$)

Natural problems

- Majority view is that derandomization should be possible (P=BPP)
- Randomness may give polynomial speedups (Schöning algorithm for k-SAT)
- Can be useful for algorithm design

Random walk

Graph $G = (V, E)$



Two kinds of walks:

- Discrete time
- Continuous time

Random walk algorithms

Undirected s–t connectivity in log space

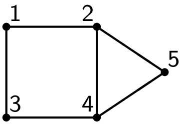
- Problem: given an undirected graph $G = (V, E)$ and $s, t \in V$, is there a path from s to t?
- A random walk from s eventually reaches t iff there is a path
- Taking a random walk only requires log space
- Can be derandomized (Reingold 2004), but this is nontrivial

Markov chain Monte Carlo

- Problem: sample from some probability distribution (uniform distribution over some set of combinatorial objects, thermal equilibrium state of a physical system, etc.)
- Create a Markov chain whose stationary distribution is the desired one
- Run the chain until it converges

Continuous-time quantum walk

Graph G



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

adjacency matrix

$$L = \begin{pmatrix} -2 & 1 & 1 & 0 & 0 \\ 1 & -3 & 0 & 1 & 1 \\ 1 & 0 & -2 & 1 & 0 \\ 0 & 1 & 1 & -3 & 1 \\ 0 & 1 & 0 & 1 & -2 \end{pmatrix}$$

Laplacian

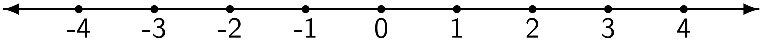
Random walk on G

- State: probability $p_v(t)$ of being at vertex v at time t
- Dynamics: $\frac{\mathrm{d}}{\mathrm{d}t}\vec{p}(t) = -L\vec{p}(t)$

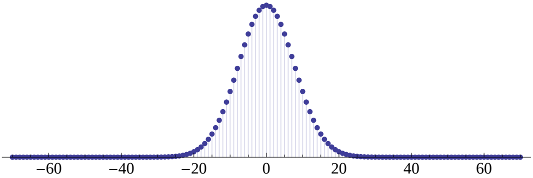
Quantum walk on G

- State: amplitude $q_v(t)$ to be at vertex v at time t (i.e., $|\psi(t)\rangle = \sum_{v \in V} q_v(t)|v\rangle$)
- Dynamics: $\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}t}\vec{q}(t) = -L\vec{q}(t)$

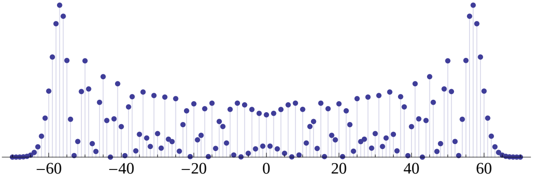
Random vs. quantum walk on the line



Classical:

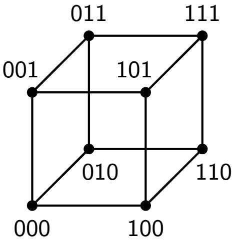


Quantum:



Random vs. quantum walk on the hypercube

$n = 3$:



$V = \{0,1\}^n$

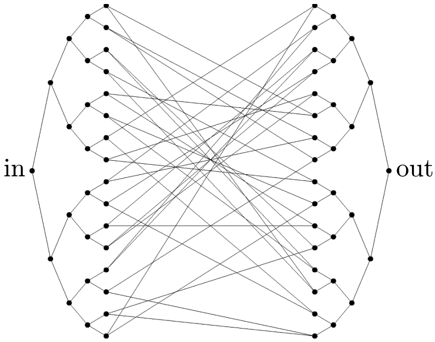
$E = \{(x,y) \in V \times V :$ x and y differ in exactly one bit$\}$

Classical random walk: reaching $11\ldots1$ from $00\ldots0$ is exponentially unlikely

Quantum walk: with $A = \sum_{j=1}^{n} X_j$,

$$e^{-\mathrm{i}At} = \prod_{j=1}^{n} e^{-\mathrm{i}X_j t} = \bigotimes_{j=1}^{n} \begin{pmatrix} \cos t & -\mathrm{i}\sin t \\ -\mathrm{i}\sin t & \cos t \end{pmatrix}$$

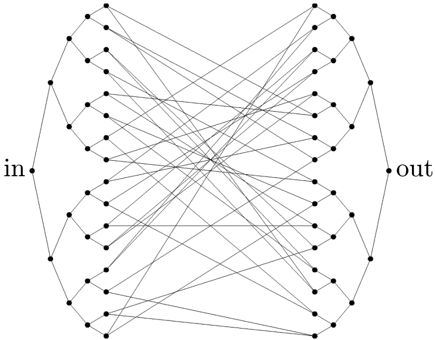
Glued trees problem



Black-box description of a graph

- Vertices have arbitrary labels
- Label of 'in' vertex is known
- Given a vertex label, black box returns labels of its neighbors
- Restricts algorithms to explore the graph locally

Glued trees problem: Classical query complexity

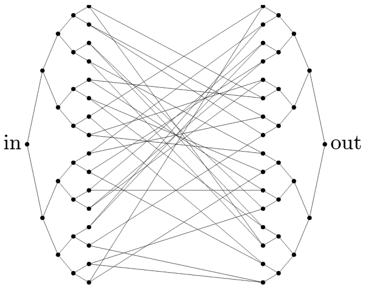


Let n denote the height of one of the binary trees

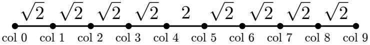
Classical random walk from 'in': probability of reaching 'out' is $2^{-\Omega(n)}$ at all times

In fact, the classical query complexity is $2^{\Omega(n)}$

Glued trees problem: Exponential speedup



$\downarrow$



Column subspace

$$|\mathrm{col}\ j\rangle := \frac{1}{\sqrt{N_j}} \sum_{v \in \mathrm{column}\ j} |v\rangle$$

$$N_j := \begin{cases} 2^j & \text{if } j \in [0, n] \\ 2^{2n+1-j} & \text{if } j \in [n+1, 2n+1] \end{cases}$$

Reduced adjacency matrix

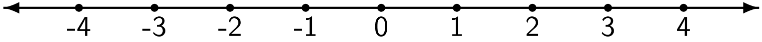
$$\langle \mathrm{col}\ j|A|\mathrm{col}\ j+1\rangle$$
$$= \begin{cases} \sqrt{2} & \text{if } j \in [0, n-1] \\ \sqrt{2} & \text{if } j \in [n+1, 2n] \\ 2 & \text{if } j = n \end{cases}$$

Discrete-time quantum walk: Need for a coin

Quantum analog of discrete-time random walk?

Unitary matrix $U \in \mathbb{C}^{|V|\times|V|}$ with $U_{vw} \neq 0$ iff $(v, w) \in E$

Consider the line:

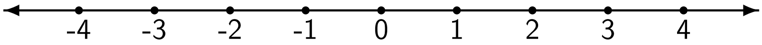


Define walk by $|x\rangle \mapsto \frac{1}{\sqrt{2}}(|x-1\rangle + |x+1\rangle)$?

But then $|x+2\rangle \mapsto \frac{1}{\sqrt{2}}(|x+1\rangle + |x+3\rangle)$, so this is not unitary!

In general, we must enlarge the state space.

Discrete-time quantum walk on a line

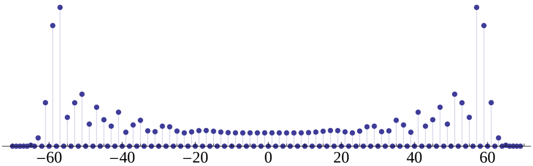


Add a "coin": state space $\mathrm{span}\{|x\rangle \otimes |{\leftarrow}\rangle, |x\rangle \otimes |{\rightarrow}\rangle : x \in \mathbb{Z}\}$

Coin flip: $C := I \otimes H$

Shift: $$\begin{aligned} S|x\rangle \otimes |{\leftarrow}\rangle &= |x-1\rangle \otimes |{\leftarrow}\rangle \\ S|x\rangle \otimes |{\rightarrow}\rangle &= |x+1\rangle \otimes |{\rightarrow}\rangle \end{aligned}$$

Walk step: SC



The Szegedy walk

State space: $\mathrm{span}\{|v\rangle \otimes |w\rangle, |w\rangle \otimes |v\rangle : (v, w) \in E\}$

Let W be a stochastic matrix (a discrete-time random walk)

$$\text{Define} \quad |\psi_v\rangle := |v\rangle \otimes \sum_{w \in V} \sqrt{W_{wv}}|w\rangle \quad (\text{note } \langle\psi_v|\psi_w\rangle = \delta_{v,w})$$

$$R := 2\sum_{v \in V} |\psi_v\rangle\langle\psi_v| - I$$

$$S(|v\rangle \otimes |w\rangle) := |w\rangle \otimes |v\rangle$$

Then a step of the walk is the unitary operator $U := SR$

Spectrum of the walk

Let $T := \sum_{v \in V} |\psi_v\rangle\langle v|$, so $R = 2TT^\dagger - I$.

Theorem (Szegedy)

Let W be a stochastic matrix. Suppose the matrix

$$\sum_{v,w} \sqrt{W_{vw} W_{wv}} |w\rangle\langle v|$$

has an eigenvector $|\lambda\rangle$ with eigenvalue λ. Then

$$\frac{I - e^{\pm \mathrm{i} \arccos \lambda} S}{\sqrt{2(1-\lambda^2)}} T|\lambda\rangle$$

are eigenvectors of $U = SR$ with eigenvalues

$$e^{\pm \mathrm{i} \arccos \lambda}.$$

Proof of Szegedy's spectral theorem

Proof sketch.

Straightforward calculations give

$$TT^\dagger = \sum_{v \in V} |\psi_v\rangle\langle\psi_v| \qquad T^\dagger T = I$$

$$T^\dagger S T = \sum_{v,w \in V} \sqrt{W_{vw} W_{wv}} |w\rangle\langle v| = \sum_\lambda |\lambda\rangle\langle\lambda|$$

which can be used to show

$$U(T|\lambda\rangle) = ST|\lambda\rangle \qquad U(ST|\lambda\rangle) = 2\lambda ST|\lambda\rangle - T|\lambda\rangle.$$

Diagonalizing within the subspace span$\{T|\lambda\rangle, ST|\lambda\rangle\}$ gives the desired result. □

Exercise. Fill in the details

Random walk search algorithm

Given $G = (V, E)$, let $M \subset V$ be a set of *marked vertices*

Start at a random unmarked vertex

Walk until we reach a marked vertex:

$$W'_{vw} := \begin{cases} 1 & w \in M \text{ and } v = w \\ 0 & w \in M \text{ and } v \neq w \\ W_{vw} & w \notin M. \end{cases}$$

$$= \begin{pmatrix} W_M & 0 \\ V & I \end{pmatrix} \quad (W_M\text{: delete marked rows and columns of } W)$$

Question. How long does it take to reach a marked vertex?

Classical hitting time

Take t steps of the walk:

$$
\begin{aligned}
(W')^t &= \begin{pmatrix} W_M^t & 0 \\ V(I + W_M + \cdots + W_M^{t-1}) & I \end{pmatrix} \\
&= \begin{pmatrix} W_M^t & 0 \\ V\frac{I-W_M^t}{I-W_M} & I \end{pmatrix}
\end{aligned}
$$

Convergence time depends on how close $\|W_M\|$ is to 1, which depends on the spectrum of W

Lemma

Let $W = W^T$ be a symmetric Markov chain. Let the second largest eigenvalue of W be $1-\delta$, and let $\epsilon = |M|/|V|$ (the fraction of marked items). Then the probability of reaching a marked vertex is $\Omega(1)$ after $t = O(1/\delta\epsilon)$ steps of the walk.

Quantum walk search algorithm

Start from the state $\frac{1}{\sqrt{N-|M|}} \sum_{v \notin M} |\psi_v\rangle$

Consider the walk U corresponding to W':

$$\sum_{v,w \in V} \sqrt{W'_{v,w} W'_{w,v}} |w\rangle\langle v| = \begin{pmatrix} W_M & 0 \\ 0 & I \end{pmatrix}$$

Eigenvalues of U are $e^{\pm \mathrm{i} \arccos \lambda}$ where the λ are eigenvalues of W_M

Perform phase estimation on U with precision $O(\sqrt{\delta\epsilon})$

- no marked items $\implies$ estimated phase is 0
- ϵ fraction of marked items $\implies$ nonzero phase with probability $\Omega(1)$

Further refinements give algorithms for *finding* a marked item

Grover's algorithm revisited

Problem

Given a black box $f : X \to \{0, 1\}$, is there an x with $f(x) = 1$?

Markov chain on $N = |X|$ vertices:

$$W := \frac{1}{N} \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} = |\psi\rangle\langle\psi|, \quad |\psi\rangle := \frac{1}{\sqrt{N}} \sum_{x \in X} |x\rangle$$

Eigenvalues of W are $0, 1 \implies \delta = 1$

Hard case: one marked vertex, $\epsilon = 1/N$

Hitting times

- Classical: $O(1/\delta\epsilon) = O(N)$
- Quantum: $O(1/\sqrt{\delta\epsilon}) = O(\sqrt{N})$

Element distinctness

Problem

Given a black box $f : X \to Y$, are there distinct x, x' with $f(x) = f(x')$?

Let $N = |X|$; classical query complexity is $\Omega(N)$

Consider a quantum walk on the Hamming graph $H(N, M)$

- Vertices: $\{(x_1, \ldots, x_M) : x_i \in X\}$
- Store the values $(f(x_1), \ldots, f(x_M))$ at vertex $(x_1, \ldots, x_M)$
- Edges between vertices that differ in exactly one coordinate

Element distinctness: Analysis

Spectral gap: $\delta = O(1/M)$

Fraction of marked vertices: $\epsilon \geq \binom{N-2}{M-2} / \binom{N}{M} = \Theta(M^2/N^2)$

Quantum hitting time: $O(1/\sqrt{\delta\epsilon}) = O(N/\sqrt{M})$

Quantum query complexity:

- M queries to prepare the initial state
- 2 queries for each step of the walk (compute f, uncompute f)
- Overall: $M + O(N/\sqrt{M})$

Choose $M = N^{2/3}$: query complexity is $O(N^{2/3})$ (optimal!)

Quantum walk algorithms

Quantum walk search algorithms

- Spatial search
- Finding a triangle in a graph
- Checking matrix multiplication
- Testing if a black-box group is abelian

Evaluating Boolean formulas

Exponential speedup for a natural problem?