Quantum algorithms – Introduction

Katalin Friedl
friedl@cs.bme.hu

Dept. of Computer Science and Information Theory

BME

June, 2025

Plan

- Basic notions, notations
  – mathematical model
  – ket vectors, unitary matrices, tensor product
- Teleportation is easy (in theory)
- Few simple algorithms
- Grover search
- Period finding and prime factorization

History

1965 Moore – transistor size is about an atom by around 2020

$\sim$1980 Benioff – good for what?

$\sim$ 1980 Feynman to simulate quantum physics

History

1965 Moore – transistor size is about an atom by around 2020

$\sim$1980 Benioff – good for what?

$\sim$ 1980 Feynman to simulate quantum physics

$\sim$1990 abstract (mathematical) model

$\sim$ 1994 P.Shor – prime factorization in expected polynomial time

$\sim$ 1996 L.Grover – search in $\Theta(\sqrt{n})$

History

1965 Moore – transistor size is about an atom by around 2020

$\sim$1980 Benioff – good for what?

$\sim$ 1980 Feynman to simulate quantum physics

$\sim$1990 abstract (mathematical) model

$\sim$ 1994 P.Shor – prime factorization in expected polynomial time

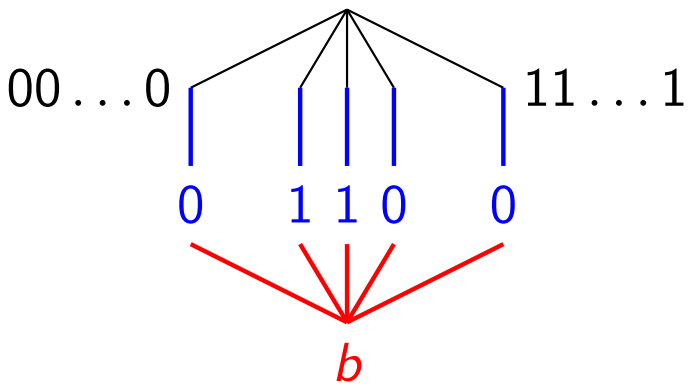
$\sim$ 1996 L.Grover – search in $\Theta(\sqrt{n})$

Today quantum computers with $\approx$100-200 quantum bits
not enough for interesting problems
simulators (free up to $\approx$15 quantum bits)

Main features

– parallel (exponential)
– randomized
– read out (measurement) changes the state

Simple scheme for a decision problem: find x s.t. $f(x) = 1$



generate all cases

parallel computation of f

$f(x)$

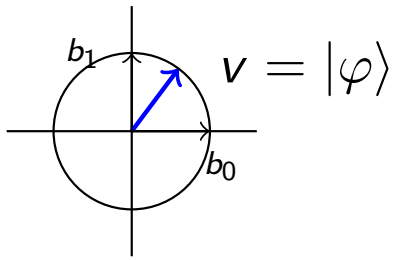
computation, measurement $\rightsquigarrow$
sample from $\{x : f(x) = b\}$

Goal: achieve $b = 1$ with high probability
(then we have a solution)

Qubit

Qubit = quantum bit = complex vector in 2D with unit length

Math: $v = \alpha b_0 + \beta b_1 \in \mathbb{C}^2, \quad ||v|| = 1$



Quantum:

$b_0 \rightsquigarrow |0\rangle$, $b_1 \rightsquigarrow |1\rangle$ ("ket" 0, "ket" 1),
$v \rightsquigarrow |\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$

linear combination of b_0 and $b_1 \rightsquigarrow$ **superposition** of $|0\rangle$ and $|1\rangle$
coefficient $\rightsquigarrow$ **amplitude**

ket vector = column vector $v = |\varphi\rangle$
bra vector = row vector $w^* = \langle\psi|$
inner product (bracket) $w^* v = \langle\psi|\varphi\rangle \in \mathbb{C}$
outer product $vw^* = |\varphi \times \psi| \in \mathbb{C}^{2\times 2}$

Operations

computational step:

linear transformation, qubit $\mapsto$ qubit

does not change distances $\Leftrightarrow$ **unitary** transformation

in matrix form: $A^{-1} = A^* \ \ (= \overline{A}^T)$

consequence: does not change angles

measurement (observation):

projections

simple version: $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \mapsto \begin{cases} |0\rangle & Pr = |\alpha|^2 \\ |1\rangle & Pr = |\beta|^2 \end{cases}$

(Note: $|\alpha|^2 + |\beta|^2 = 1$)

more general: in any orthonormal basis

2×2 unitary examples

Identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\qquad I = \overline{I} = I^T = I^{-1}$

2×2 unitary examples

Identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\qquad I = \overline{I} = I^T = I^{-1}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix}$ $\qquad$ unitary iff $z\overline{z} = |z|^2 = 1$

2×2 unitary examples

Identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad I = \overline{I} = I^T = I^{-1}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix}$ $\quad$ unitary iff $z\overline{z} = |z|^2 = 1$

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad X^2 = I$

2×2 unitary examples

Identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\qquad I = \overline{I} = I^T = I^{-1}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix}$ $\qquad$ unitary iff $z\overline{z} = |z|^2 = 1$

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\qquad X^2 = I$

$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $\qquad Y^* = Y,\ Y^2 = I$ $\qquad$ (here $i^2 = -1$)

X, Y, and Z with $z = -1$: Pauli matrices

Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H \cdot H = I \Rightarrow H^{-1} = H = H^*$$

$$H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad H \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

Apply H to $|0\rangle$ two times:

Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H \cdot H = I \Rightarrow H^{-1} = H = H^*$$

$$H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad H \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

Apply H to $|0\rangle$ two times:

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

Apply H to $|0\rangle$ two times **with measurement** in between:

Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H \cdot H = I \Rightarrow H^{-1} = H = H^*$$

$$H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad H \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

Apply H to $|0\rangle$ two times:

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

Apply H to $|0\rangle$ two times **with measurement** in between:

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{M} \text{ random bit } \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \xrightarrow{M} \text{ random bit}$$

So, **measurement changes** the result!

Tensor product

for $v \in \mathbb{C}^k$ and $w \in \mathbb{C}^m$ $\qquad v \otimes w = \begin{pmatrix} v_1 w \\ \vdots \\ v_k w \end{pmatrix} \in \mathbb{C}^{km}$

for matrices $A \in \mathbb{C}^{k_1 \times k_2}$ and $B \in \mathbb{C}^{m_1 \times m_2}$

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1k_2}B \\ \cdots & \cdots & \cdots \\ a_{k_1 1}B & \cdots & a_{k_1 k_2}B \end{pmatrix} \in \mathbb{C}^{k_1 m_1 \times k_2 m_2}$$

Properties

- $v, z \in \mathbb{C}^k$ and $w \in \mathbb{C}^m \quad \Rightarrow \quad (v + z) \otimes w = (v \otimes w) + (z \otimes w)$
- $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$ for $\alpha \in \mathbb{C}$
- $A, C \in \mathbb{C}^{k \times k}$ and $B, D \in \mathbb{C}^{m \times m} \Rightarrow (A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$
- $A \in \mathbb{C}^{k_1 \times k_2}, B \in \mathbb{C}^{m_1 \times m_2}$, and $v \in \mathbb{C}^{k_2}, w \in \mathbb{C}^{m_2} \quad \Rightarrow$
  $(A \otimes B) \cdot (v \otimes w) = (Av) \otimes (Bw)$
- $A \in \mathbb{C}^{k \times k}$, $B \in \mathbb{C}^{m \times m}$ unitary $\Leftrightarrow A \otimes B$ is unitary

Example

$|0\rangle, |1\rangle \in \mathbb{C}^2$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle,$$

Example

$|0\rangle, |1\rangle \in \mathbb{C}^2$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle, \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle,$$

Example

$|0\rangle, |1\rangle \in \mathbb{C}^2$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle, \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle,$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle,$$

Example

$|0\rangle, |1\rangle \in \mathbb{C}^2$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle, \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle,$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle, \qquad |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle$$

Simplified notation:
$|00\rangle = |0\rangle\,|0\rangle = |0\rangle$, $|01\rangle = |0\rangle\,|1\rangle = |1\rangle$, $|10\rangle = |1\rangle\,|0\rangle = |2\rangle$, $|11\rangle = |1\rangle\,|1\rangle = |3\rangle$

In general $|0\cdots00\rangle = |0\rangle\cdots|0\rangle\,|0\rangle = |0\rangle$, $|0\cdots10\rangle = |0\rangle\cdots|1\rangle\,|0\rangle = |2\rangle$,
$|1\cdots11\rangle = |1\rangle\cdots|1\rangle\,|1\rangle = |2^n - 1\rangle$

Hadamard

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

$$H \otimes H \left|b_0 b_1\right\rangle = H \left|b_0\right\rangle \otimes H \left|b_1\right\rangle = \frac{1}{2}(\left|0\right\rangle + (-1)^{b_0}\left|1\right\rangle) \otimes (\left|0\right\rangle + (-1)^{b_1}\left|1\right\rangle) =$$

Hadamard

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

$$H \otimes H \left|b_0 b_1\right\rangle = H \left|b_0\right\rangle \otimes H \left|b_1\right\rangle = \frac{1}{2}(\left|0\right\rangle + (-1)^{b_0}\left|1\right\rangle) \otimes (\left|0\right\rangle + (-1)^{b_1}\left|1\right\rangle) =$$
$$\frac{1}{2}(\left|00\right\rangle + (-1)^{b_1}\left|01\right\rangle + (-1)^{b_0}\left|10\right\rangle + (-1)^{b_0+b_1}\left|11\right\rangle)$$

In general $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$

$H^{\otimes n}\left|b_0 \cdots b_{n-1}\right\rangle =$

Hadamard

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

$$H \otimes H\,|b_0 b_1\rangle = H\,|b_0\rangle \otimes H\,|b_1\rangle = \frac{1}{2}(|0\rangle + (-1)^{b_0}\,|1\rangle) \otimes (|0\rangle + (-1)^{b_1}\,|1\rangle) =$$
$$\frac{1}{2}(|00\rangle + (-1)^{b_1}\,|01\rangle + (-1)^{b_0}\,|10\rangle + (-1)^{b_0+b_1}\,|11\rangle)$$

In general $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$

$$H^{\otimes n}\,|b_0 \cdots b_{n-1}\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle + (-1)^{b_0}\,|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{b_{n-1}}\,|1\rangle) =$$

Hadamard

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

$$H \otimes H \left|b_0 b_1\right\rangle = H\left|b_0\right\rangle \otimes H\left|b_1\right\rangle = \frac{1}{2}(\left|0\right\rangle + (-1)^{b_0}\left|1\right\rangle) \otimes (\left|0\right\rangle + (-1)^{b_1}\left|1\right\rangle) =$$
$$\frac{1}{2}(\left|00\right\rangle + (-1)^{b_1}\left|01\right\rangle + (-1)^{b_0}\left|10\right\rangle + (-1)^{b_0+b_1}\left|11\right\rangle)$$

In general $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$

$$H^{\otimes n}\left|b_0 \cdots b_{n-1}\right\rangle = \frac{1}{\sqrt{2^n}}(\left|0\right\rangle + (-1)^{b_0}\left|1\right\rangle) \otimes \cdots \otimes (\left|0\right\rangle + (-1)^{b_{n-1}}\left|1\right\rangle) =$$
$$\sum_{c_0 \cdots c_{n-1}} (-1)^{\sum b_j c_j}\left|c_0 \cdots c_{n-1}\right\rangle$$

Special case: $H^{\otimes n}\left|0 \cdots 00\right\rangle = \sum_{c_0 \cdots c_{n-1}}\left|c_0 \cdots c_{n-1}\right\rangle$

– typical first step to generate all possibilities

More qubits

n qubit register: $v \in \mathbb{C}^{2^n} \qquad ||v|| = 1$

basis – bit sequences of length n: $|0\cdots00\rangle\,,\ |0\cdots01\rangle\,,\ \ldots,\ |1\cdots11\rangle$

vectors – linear combinations of basis vectors with coeff's $\alpha_{b_0\cdots b_{n-1}} \in \mathbb{C}$:

$$|\varphi\rangle = \sum_{b_0,\cdots,b_{n-1}} \alpha_{b_0\cdots b_{n-1}}\,|b_0\cdots b_{n-1}\rangle\,, \qquad \sum_{b_0,\cdots,b_{n-1}} |\alpha_{b_0\cdots b_{n-1}}|^2 = 1$$

Operations:
– unitary ($A^{-1} = A^*$), acting on a few bits only ($A = I \otimes T \otimes I$, T is small)
– measurement $|\varphi\rangle \mapsto |b_0\cdots b_{n-1}\rangle \quad$ with $Pr = |\alpha_{b_0\cdots b_{n-1}}|^2$

More general: outcome = projection to a subspace,
Pr= squared length
e.g. measuring 0th bit: $|1\rangle$ with $Pr = \sum_{b_1,\cdots,b_{n-1}} |\alpha_{1b_1\cdots b_{n-1}}|^2$

CNOT

Controlled NOT: changes b_1 if $b_0 = 1$

$$\text{CNOT} : |b_0 b_1\rangle \mapsto \begin{cases} |b_0 b_1\rangle & \text{if } b_0 = 0 \\ |b_0 \overline{b_1}\rangle & \text{if } b_0 = 1 \end{cases} \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$CNOT$ is unitary, $CNOT^2 = I$

Example:

$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The result is an **entangled** state: measuring the 0th bit fixes the 1st bit

classical	quantum
bit	qubit
AND, OR, NOT	1-qubit unitaries, CNOT (or other complete set)
typical form not invertable ($x = x \wedge y$)	invertable

w/o measurement – quantum algo **reversible**
and measurements can be pushed to the end

classical algorithm $\leftrightarrow$ quantum algorithm
(since classical can be made reversible; quantum can be simulated)

differences in efficiency/complexity

No-cloning

Theorem

No lin.transformation $A : |\varphi\rangle |0\rangle \mapsto |\varphi\rangle |\varphi\rangle$ *for every* φ

Proof:

Assume there is such $A \Rightarrow$

$$A : |0\rangle |0\rangle \mapsto |0\rangle |0\rangle \text{ and } A : |1\rangle |0\rangle \mapsto |1\rangle |1\rangle$$

by linearity

$$A : |\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle |0\rangle + |1\rangle |0\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle |0\rangle + |1\rangle |1\rangle) = |\psi\rangle$$

No-cloning

Theorem

No lin.transformation $A : |\varphi\rangle\,|0\rangle \mapsto |\varphi\rangle\,|\varphi\rangle$ *for every* φ

Proof:

Assume there is such $A \Rightarrow$

$$A : |0\rangle\,|0\rangle \mapsto |0\rangle\,|0\rangle \text{ and } A : |1\rangle\,|0\rangle \mapsto |1\rangle\,|1\rangle$$

by linearity

$$A : |\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|0\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = |\psi\rangle$$

but

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle) \quad \text{by def.} \quad \rightarrow$$

No-cloning

Theorem

No lin.transformation $A : |\varphi\rangle\,|0\rangle \mapsto |\varphi\rangle\,|\varphi\rangle$ *for every* φ

Proof:

Assume there is such $A \Rightarrow$

$$A : |0\rangle\,|0\rangle \mapsto |0\rangle\,|0\rangle \text{ and } A : |1\rangle\,|0\rangle \mapsto |1\rangle\,|1\rangle$$

by linearity

$$A : |\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|0\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = |\psi\rangle$$

but

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle) \quad \text{by def.} \quad \rightarrow \quad \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) =$$

No-cloning

Theorem

No lin.transformation $A : |\varphi\rangle\,|0\rangle \mapsto |\varphi\rangle\,|\varphi\rangle$ *for every* φ

Proof:

Assume there is such $A \Rightarrow$

$$A : |0\rangle\,|0\rangle \mapsto |0\rangle\,|0\rangle \text{ and } A : |1\rangle\,|0\rangle \mapsto |1\rangle\,|1\rangle$$

by linearity

$$A : |\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|0\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = |\psi\rangle$$

but

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle) \quad \text{by def.} \rightarrow \quad \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) =$$

$$\frac{1}{2}(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |1\rangle\,|1\rangle) \neq |\psi\rangle$$

□

Teleportation

by Bennett, Brassard, Crépau, 1992
2 players, **A** has $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ – **B** wants it
can use: classical channel, entangled bits

Algorithm

$$|\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0\,0\rangle + |1\,1\rangle) = \frac{1}{\sqrt{2}}(\alpha\,|00\,0\rangle + \alpha\,|01\,1\rangle + \beta\,|10\,0\rangle + \beta\,|11\,1\rangle) \xrightarrow{A:CNOT}$$

Teleportation

by Bennett, Brassard, Crépau, 1992
2 players, **A** has $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ – **B** wants it
can use: classical channel, entangled bits

Algorithm

$$|\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0\,0\rangle + |1\,1\rangle) = \frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|10\,0\rangle + \beta|11\,1\rangle) \xrightarrow{A:CNOT}$$

$$\frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|11\,0\rangle + \beta|10\,1\rangle) \xrightarrow{A:H\otimes I}$$

Teleportation

by Bennett, Brassard, Crépau, 1992
2 players, **A** has $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ – **B** wants it
can use: classical channel, entangled bits

Algorithm

$$|\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0\,0\rangle + |1\,1\rangle) = \frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|10\,0\rangle + \beta|11\,1\rangle) \xrightarrow{A:CNOT}$$

$$\frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|11\,0\rangle + \beta|10\,1\rangle) \xrightarrow{A:H\otimes I}$$

$$\frac{1}{2}(\overbrace{\alpha(|00\,0\rangle + |10\,0\rangle)} + \overbrace{\alpha(|01\,1\rangle + |11\,1\rangle)} + \overbrace{\beta(|01\,0\rangle - |11\,0\rangle)} + \overbrace{\beta(|00\,1\rangle - |10\,1\rangle)}) =$$

)

Teleportation

by Bennett, Brassard, Crépau, 1992

2 players, **A** has $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ – **B** wants it

can use: classical channel, entangled bits

Algorithm

$$|\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0\,0\rangle + |1\,1\rangle) = \frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|10\,0\rangle + \beta|11\,1\rangle) \xrightarrow{A:CNOT}$$

$$\frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|11\,0\rangle + \beta|10\,1\rangle) \xrightarrow{A:H\otimes I}$$

$$\frac{1}{2}(\overbrace{\alpha(|00\,0\rangle + |10\,0\rangle)} + \overbrace{\alpha(|01\,1\rangle + |11\,1\rangle)} + \overbrace{\beta(|01\,0\rangle - |11\,0\rangle)} + \overbrace{\beta(|00\,1\rangle - |10\,1\rangle)}) =$$

$$\frac{1}{2}(|00\rangle\ (\alpha|0\rangle + \beta|1\rangle) + |01\rangle\ (\alpha|1\rangle + \beta|0\rangle) + |10\rangle\ (\alpha|0\rangle - \beta|1\rangle) +$$

$$|11\rangle\ (\alpha|1\rangle - \beta|0\rangle))$$

Teleportation

by Bennett, Brassard, Crépau, 1992

2 players, **A** has $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ – **B** wants it

can use: classical channel, entangled bits

Algorithm

$$|\varphi\rangle \otimes \frac{1}{\sqrt{2}}(|0\,0\rangle + |1\,1\rangle) = \frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|10\,0\rangle + \beta|11\,1\rangle) \xrightarrow{A:CNOT}$$

$$\frac{1}{\sqrt{2}}(\alpha|00\,0\rangle + \alpha|01\,1\rangle + \beta|11\,0\rangle + \beta|10\,1\rangle) \xrightarrow{A:H\otimes I}$$

$$\frac{1}{2}(\overbrace{\alpha(|00\,0\rangle + |10\,0\rangle)} + \overbrace{\alpha(|01\,1\rangle + |11\,1\rangle)} + \overbrace{\beta(|01\,0\rangle - |11\,0\rangle)} + \overbrace{\beta(|00\,1\rangle - |10\,1\rangle)}) =$$

$$\frac{1}{2}(|00\rangle\ (\alpha|0\rangle + \beta|1\rangle) + |01\rangle\ (\alpha|1\rangle + \beta|0\rangle) + |10\rangle\ (\alpha|0\rangle - \beta|1\rangle) +$$

$$|11\rangle\ (\alpha|1\rangle - \beta|0\rangle))$$

A makes measurement (on her own bits)

$\frac{1}{2}(|00\rangle\ (\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\ (\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\ (\alpha\,|0\rangle - \beta\,|1\rangle) +$
$11\ (\alpha\,|1\rangle - \beta\,|0\rangle)$ **A** measures and tell the result

result at **A**	qubit at **B**	$\|\psi\rangle \to \|\varphi\rangle = \alpha\,\|0\rangle + \beta\,\|1\rangle$
$\|00\rangle$	$\|\psi\rangle = \alpha\,\|0\rangle + \beta\,\|1\rangle$	$\|\varphi\rangle = \|\psi\rangle$

$\frac{1}{2}(|00\rangle\ (\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\ (\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\ (\alpha\,|0\rangle - \beta\,|1\rangle) +$
$11\ (\alpha\,|1\rangle - \beta\,|0\rangle)$ **A** measures and tell the result

result at **A**	qubit at **B**	$\lvert\psi\rangle \to \lvert\varphi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
$\lvert00\rangle$	$\lvert\psi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\lvert\varphi\rangle = \lvert\psi\rangle$
$\lvert01\rangle$	$\lvert\psi\rangle = \alpha\,\lvert1\rangle + \beta\,\lvert0\rangle$	$\lvert\varphi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \lvert\psi\rangle = X\,\lvert\psi\rangle$

$\frac{1}{2}(|00\rangle\ (\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\ (\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\ (\alpha\,|0\rangle - \beta\,|1\rangle) +$
$11\ (\alpha\,|1\rangle - \beta\,|0\rangle)$ **A** measures and tell the result

result at **A**	qubit at **B**	$\lvert\psi\rangle \to \lvert\varphi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
$\lvert00\rangle$	$\lvert\psi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\lvert\varphi\rangle = \lvert\psi\rangle$
$\lvert01\rangle$	$\lvert\psi\rangle = \alpha\,\lvert1\rangle + \beta\,\lvert0\rangle$	$\lvert\varphi\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\lvert\psi\rangle = X\,\lvert\psi\rangle$
$\lvert10\rangle$	$\lvert\psi\rangle = \alpha\,\lvert0\rangle - \beta\,\lvert1\rangle$	$\lvert\varphi\rangle = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\lvert\psi\rangle = Z\,\lvert\psi\rangle$

$\frac{1}{2}(|00\rangle\ (\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\ (\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\ (\alpha\,|0\rangle - \beta\,|1\rangle) +$
$11\ (\alpha\,|1\rangle - \beta\,|0\rangle)$ **A** measures and tell the result

result at **A**	qubit at **B**	$\lvert\psi\rangle \to \lvert\varphi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
$\lvert00\rangle$	$\lvert\psi\rangle = \alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\lvert\varphi\rangle = \lvert\psi\rangle$
$\lvert01\rangle$	$\lvert\psi\rangle = \alpha\,\lvert1\rangle + \beta\,\lvert0\rangle$	$\lvert\varphi\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\lvert\psi\rangle = X\,\lvert\psi\rangle$
$\lvert10\rangle$	$\lvert\psi\rangle = \alpha\,\lvert0\rangle - \beta\,\lvert1\rangle$	$\lvert\varphi\rangle = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\lvert\psi\rangle = Z\,\lvert\psi\rangle$
$\lvert11\rangle$	$\lvert\psi\rangle = \alpha\,\lvert1\rangle - \beta\,\lvert0\rangle$	$\lvert\varphi\rangle = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\lvert\psi\rangle = XZ\,\lvert\psi\rangle$

B does the transformation and obtains $|\varphi\rangle$ (w/o knowing what it is)

Used: 1 entangled pair; 3 quantum steps by **A**; communication of 2 bits; 1 quantum step by **B**

How to specify **input**, like $f : \{0,1\}^n \to \{0,1\}$

classical **black box**: $x \in \{0,1\}^n$

$$x \longrightarrow \boxed{f} \longrightarrow f(x)$$

For quantum algorithms – **quantum box** (simple version, encoding in phase)

$$|x\rangle \longrightarrow \boxed{f} \longrightarrow (-1)^{f(x)} |x\rangle$$

Can be used for linear combination $\sum_x \alpha_x |x\rangle \longrightarrow \sum_x (-1)^{f(x)} \alpha_x |x\rangle$

Property: This quantum box describes a unitary transformation
(since it is a diagonal ± 1 matrix)

Remark: useful for Boolean functions

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions =

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions $= 2^{n-1} + 1$

Quantum: 1 query to the quantum box

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle$$

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions $= 2^{n-1} + 1$

Quantum: 1 query to the quantum box

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle$$

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions $= 2^{n-1} + 1$

Quantum: 1 query to the quantum box

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle$$

$$\overset{H^{\otimes n}}{\to} \frac{1}{2^n} \sum_{b_0 \cdots b_{n-1}} \sum_{c_0 \cdots c_{n-1}} (-1)^{\sum_i b_i c_i} (-1)^{f(b_0 \cdots b_{n-1})} |c_0 \cdots c_{n-1}\rangle \overset{M}{\to} ??$$

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions $= 2^{n-1} + 1$

Quantum: 1 query to the quantum box

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle$$

$$\overset{H^{\otimes n}}{\to} \frac{1}{2^n} \sum_{b_0 \cdots b_{n-1}} \sum_{c_0 \cdots c_{n-1}} (-1)^{\sum_i b_i c_i} (-1)^{f(b_0 \cdots b_{n-1})} |c_0 \cdots c_{n-1}\rangle \overset{M}{\to} ??$$

Coefficient of $|0^n\rangle$?

Deutsch-Jozsa algorithm

Given $f : \{0,1\}^n \to \{0,1\}$
Promise: either constant or balanced: $|\{x : f(x) = 0\}| = 2^{n-1}$
Decide which one
Classical: f given by a black box. Number of questions $= 2^{n-1} + 1$

Quantum: 1 query to the quantum box

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle$$

$$\overset{H^{\otimes n}}{\to} \frac{1}{2^n} \sum_{b_0 \cdots b_{n-1}} \sum_{c_0 \cdots c_{n-1}} (-1)^{\sum_i b_i c_i} (-1)^{f(b_0 \cdots b_{n-1})} |c_0 \cdots c_{n-1}\rangle \overset{M}{\to} ??$$

Coefficient of $|0^n\rangle$?

$$\frac{1}{2^n} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} = \begin{cases} \pm 1 & \text{if } f \text{ constant} \\ 0 & \text{if } f \text{ balanced} \end{cases}$$

Finish by measurment – if the result is $|0^n\rangle$ then f constant, o/w balanced

Bernstein–Vazirani algorithm

Given $f : \{0,1\}^n \to \{0,1\}$, s.t. $f(b_0, \ldots, b_{n-1}) = \sum_i a_i b_i \pmod 2$
for some $a_i \in \{0,1\}$

Determine $a_0, \ldots, a_{n-1}$

Classical: 1 question $\longrightarrow$ 1 equation $\pmod 2$

need n (independent) equations for unique solution

Quantum: with 1 query

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle =$$

Bernstein–Vazirani algorithm

Given $f : \{0,1\}^n \to \{0,1\}$, s.t. $f(b_0, \ldots, b_{n-1}) = \sum_i a_i b_i \pmod 2$
for some $a_i \in \{0,1\}$

Determine $a_0, \ldots, a_{n-1}$

Classical: 1 question $\longrightarrow$ 1 equation $\pmod 2$

need n (independent) equations for unique solution

Quantum: with 1 query

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{\sum_i a_i b_i} |b_0 \cdots b_{n-1}\rangle \overset{H^{\otimes n}}{\to}$$

Bernstein–Vazirani algorithm

Given $f : \{0,1\}^n \to \{0,1\}$, s.t. $f(b_0, \ldots, b_{n-1}) = \sum_i a_i b_i \pmod 2$
for some $a_i \in \{0,1\}$

Determine $a_0, \ldots, a_{n-1}$

Classical: 1 question $\longrightarrow$ 1 equation $\pmod 2$

need n (independent) equations for unique solution

Quantum: with 1 query

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{\sum_i a_i b_i} |b_0 \cdots b_{n-1}\rangle \overset{H^{\otimes n}}{\to} |a_0 \cdots a_{n-1}\rangle$$

Bernstein–Vazirani algorithm

Given $f : \{0,1\}^n \to \{0,1\}$, s.t. $f(b_0, \ldots, b_{n-1}) = \sum_i a_i b_i \pmod 2$
for some $a_i \in \{0,1\}$

Determine $a_0, \ldots, a_{n-1}$

Classical: 1 question $\longrightarrow$ 1 equation $\pmod 2$

need n (independent) equations for unique solution

Quantum: with 1 query

$$|0^n\rangle \overset{H^{\otimes n}}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} |b_0 \cdots b_{n-1}\rangle \overset{f}{\to} \frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{f(b_0 \cdots b_{n-1})} |b_0 \cdots b_{n-1}\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{b_0 \cdots b_{n-1}} (-1)^{\sum_i a_i b_i} |b_0 \cdots b_{n-1}\rangle \overset{H^{\otimes n}}{\to} |a_0 \cdots a_{n-1}\rangle$$

a measurement reveals $a_0, \ldots, a_{n-1}$

Simon algorithm

Given $f : \{0,1\}^n \to \{0,1\}^n$, s.t. for some $s \in \{0,1\}^n, s \neq 0 \cdots 0$
$f(x) = f(z) \Leftrightarrow z = x$ or $z = x + s$ (here $+$ is bitwise addition mod 2)

Classical:

– if we find x, z, s.t $f(x) = f(z) \Rightarrow s = x + z$, s is found
– if $f(x) \neq f(z) \Rightarrow s \neq x + z$

Simon algorithm

Given $f : \{0,1\}^n \to \{0,1\}^n$, s.t. for some $s \in \{0,1\}^n, s \neq 0 \cdots 0$
$f(x) = f(z) \Leftrightarrow z = x$ or $z = x + s$ (here $+$ is bitwise addition mod 2)

Classical:

– if we find x, z, s.t $f(x) = f(z) \Rightarrow s = x + z$, s is found
– if $f(x) \neq f(z) \Rightarrow s \neq x + z$
after k queries, if the answers are different $\Rightarrow \binom{k}{2}$ excluded $s \Rightarrow \#$ queries $\Omega(\sqrt{2^n})$

Remark: after $k = \sqrt{2^{n-\varepsilon}}$ queries Prob(good s) = small

Simon algorithm

Given $f : \{0,1\}^n \to \{0,1\}^n$, s.t. for some $s \in \{0,1\}^n, s \neq 0 \cdots 0$
$f(x) = f(z) \Leftrightarrow z = x$ or $z = x + s$ (here $+$ is bitwise addition mod 2)

Classical:
– if we find x, z, s.t $f(x) = f(z) \Rightarrow s = x + z$, s is found
– if $f(x) \neq f(z) \Rightarrow s \neq x + z$
after k queries, if the answers are different $\Rightarrow \binom{k}{2}$ excluded $s \Rightarrow \#$ queries $\Omega(\sqrt{2^n})$

Remark: after $k = \sqrt{2^{n-\varepsilon}}$ queries Prob(good s) = small

Quantum: needs a more general **quantum box** for non-Boolean f

$$|x\rangle\,|y\rangle \quad \longrightarrow \boxed{f} \longrightarrow |x\rangle\,|f(x) + y\rangle$$

can be extended to linear combinations

$$\sum_{x,y} \alpha_{x,y}\,|x\rangle\,|y\rangle \mapsto \sum_{x,y} \alpha_{x,y}\,|x\rangle\,|f(x) + y\rangle$$

Property: This quantum box describes unitary transformation
(since it is a permutation matrix)

Quantum algorithm:

– start with 2 n-qubit registers $|0^n\rangle\,|0^n\rangle$

– steps: $H^{\otimes n} \otimes I, \quad f, \quad H^{\otimes n} \otimes I, \quad M$

Details:

$$|0^n\rangle\,|0^n\rangle \to \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|0^n\rangle \to \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|f(x)\rangle \to$$

$$\frac{1}{2^n} \sum_x \sum_z (-1)^{\sum_i x_i z_i} |z\rangle\,|f(x)\rangle$$

Quantum algorithm:

– start with 2 n-qubit registers $|0^n\rangle\,|0^n\rangle$

– steps: $H^{\otimes n} \otimes I, \quad f, \quad H^{\otimes n} \otimes I, \quad M$

Details:

$$|0^n\rangle\,|0^n\rangle \to \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|0^n\rangle \to \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|f(x)\rangle \to$$

$$\frac{1}{2^n} \sum_x \sum_z (-1)^{\sum_i x_i z_i} |z\rangle\,|f(x)\rangle$$

coefficient of $|z\rangle\,|y\rangle$:

$$\frac{1}{2^n} \sum_{x:f(x)=y} (-1)^{\sum_i x_i z_i} = \frac{1}{2^n}((-1)^{\sum_i x_i z_i} + (-1)^{\sum_i (x_i+s_i) z_i}) =$$

$$\frac{1}{2^n}(-1)^{\sum_i x_i z_i}(1 + (-1)^{\sum_i s_i z_i}) = \begin{cases} 0 & \text{if } \sum_i s_i z_i = 1 \pmod 2 \\ \pm 2^{-n+1} & \text{if } \sum_i s_i z_i = 0 \pmod 2 \end{cases}$$

Measurement $\to z$ s.t. $\sum_i s_i z_i = 0 \pmod 2$

any of these with same probability – **uniform sample** from subspace

$$s^\perp = \{z : \sum_i s_i z_i = 0\}$$

dimension of subspace $dim(s^\perp) = n - 1$
$n - 1$ linearly independent z determines s

Theorem

For $4n$ independent random sample $Pr(n - 1$ are lin. independent$) > 2/3$

Corollary

$4n$ queries: prob. of error $\leq 1/3$
$20n$ queries: prob. of error $< 1/200$
$O(n^2)$ queries: prob. of error is exponentially small
(error = no unique solution for s)

Search problems

Basic version Given elements $a_0, a_2, \ldots, a_{N-1}$ and b, find k s.t. $a_k = b$

General version Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$, find k s.t. $f(k) = 1$

Deterministic algorithm

Number of queries

worst case: N
average case: $\approx N/2$

Search problems

Basic version Given elements $a_0, a_2, \ldots, a_{N-1}$ and b, find k s.t. $a_k = b$

General version Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$, find k s.t. $f(k) = 1$

Deterministic algorithm

Number of queries	worst case: N average case: $\approx N/2$

Probabilistic algorithm

Number of queries	$\approx N/10$ for success prob. 0.1

Search problems

Basic version Given elements $a_0, a_2, \ldots, a_{N-1}$ and b, find k s.t. $a_k = b$

General version Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$, find k s.t. $f(k) = 1$

Deterministic algorithm

Number of queries — worst case: N
average case: $\approx N/2$

Probabilistic algorithm

Number of queries — $\approx N/10$ for success prob. 0.1

Quantum algorithm (L. Grover 1996)

Number of queries — $O(\sqrt{N})$, with high probability

uses the simple quantum box

$$\sum_x \alpha_x \, |x\rangle \longrightarrow \boxed{f} \longrightarrow \sum_x (-1)^{f(x)} \alpha_x \, |x\rangle$$

Applications

In any algorithm which uses search

- search in a huge database

Applications

In any algorithm which uses search

- search in a huge database
- break passwords

Applications

In any algorithm which uses search

- search in a huge database
- break passwords
- graph algorithms
  – graph traversals
    idea: looking for an unvisited neighbor is a search problem —
    use Grover's algorithm

    BFS, DFS : classical $O(N^2) \longrightarrow$ quantum $O(N^{3/2})$

  – shortest path : classical $O(N^2) \longrightarrow$ quantum $\tilde{O}(N^{3/2})$

Views

One algorithm – different views

- geometric – intuition
- algebraic – general tool
- quantum algorithm

Views

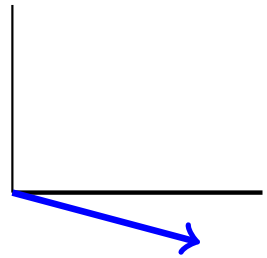
One algorithm – different views

- geometric – intuition
- algebraic – general tool
- quantum algorithm

Now assume: **exactly one** solution ($t = 1$)

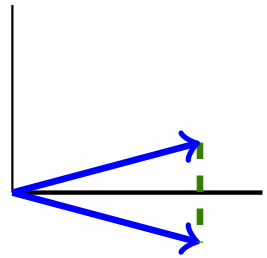
Geometry

Flipping the sign of one component — reflection



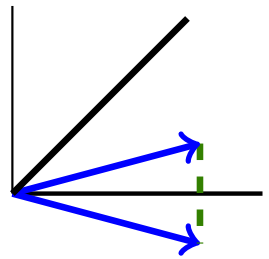
Geometry

Flipping the sign of one component — reflection



Geometry

Flipping the sign of one component — reflection

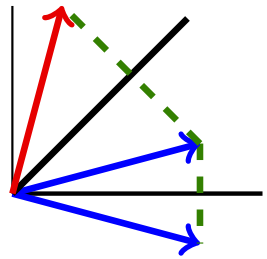


two reflections=one rotation by 2α
($\alpha =$ the angle of the two vectors)

Geometry

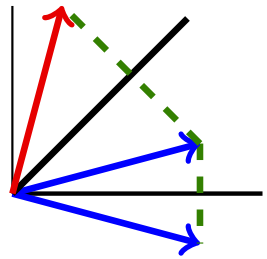
Flipping the sign of one component — reflection

two reflections=one rotation by 2α
($\alpha =$ the angle of the two vectors)



Geometry

Flipping the sign of one component — reflection

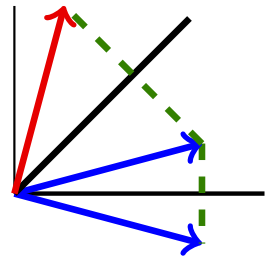


two reflections=one rotation by 2α
($\alpha =$ the angle of the two vectors)

For larger dimensions Reflection R to $v^{\perp}$, the hyperplane orthogonal to v: $Rv = -v, \quad Rw = w$ if $w \perp v$

Geometry

Flipping the sign of one component — reflection



two reflections=one rotation by 2α
($\alpha =$ the angle of the two vectors)

For larger dimensions Reflection R to $v^\perp$, the hyperplane orthogonal to v: $Rv = -v, \quad Rw = w$ if $w \perp v$

U unitary $\Longrightarrow$ URU^{-1} is a reflection to $(Uv)^\perp$

$URU^{-1}(Uv) = -Uv, \quad URU^{-1}(Uw) = Uw$ if $w \perp v$, i.e., $Uw \perp Uv$

Grover's idea

Setup N elements $\longrightarrow$ N dimensional space
elements $\longrightarrow$ orthogonal basis
$a_x \mapsto |x\rangle$

Given: quantum box for f — reflection R to $|k\rangle^{\perp}$
(k is the only solution of $f(x) = 1$)

Goal: determine k — find the corresponding basis vector $|k\rangle$

Need: $N = 2^n$

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

easy (conditional phase shift)

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$

(H is the Hadamard operator on n qubits, $H = H^{-1}$)

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$

(H is the Hadamard operator on n qubits, $H = H^{-1}$)

Use R_uR several times — rotations by angle 2α

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$

(H is the Hadamard operator on n qubits, $H = H^{-1}$)

Use R_uR several times — rotations by angle 2α

Stop when target $|k\rangle$ is close

measurement gives $|k\rangle$ by high probability

Angle

How do we know that we are close to $|k\rangle$?
Angle of rotations $= 2\alpha$

$\alpha =$ angle of the vectors $|k\rangle$ and $H|0\rangle$ – **same for each** $|k\rangle$

$H|0\rangle = N^{-1/2} \sum_x |x\rangle$

α can be computed by **inner product**

$\Rightarrow N^{-1/2} = \cos\alpha$ (unit vectors)

So, for large N $\alpha \approx \pi/2$, $2\alpha \approx \pi$ **too large**

Reducing the angle

2D Replacing R_u by $-R_u$ gives reflection to the orthogonal direction

the **new angle** is $\alpha' = \pi/2 - \alpha$

then $\cos\alpha = \sin\alpha' = N^{-1/2}$

so, $\alpha' \approx N^{-1/2}$ for large N

angle of rotation: $2\alpha' \approx \dfrac{2}{\sqrt{N}}$

Reducing the angle

2D Replacing R_u by $-R_u$ gives reflection to the orthogonal direction

the **new angle** is $\alpha' = \pi/2 - \alpha$

then $\cos\alpha = \sin\alpha' = N^{-1/2}$

so, $\alpha' \approx N^{-1/2}$ for large N

angle of rotation: $2\alpha' \approx \dfrac{2}{\sqrt{N}}$

Grover operator $G = -R_u R = H(-R_0)HR$

Algorithm

- Start with basis vector $|0\rangle$
- Apply H
- $\left\lceil \frac{\pi/2}{2\alpha'} \right\rceil$ times apply
- Measure

Here

$N = 2^n$

$H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H = H_2^{\otimes n}$

$(-R_0) =$ conditional phase shift: $|x\rangle \mapsto \begin{cases} |x\rangle & \text{if } x = 0 \\ -|x\rangle & \text{if } x \neq 0 \end{cases}$

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant (non-zero) probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant (non-zero) probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

The result can be checked

and if it is not a solution, repeat the process

Repeating several times increases success probability.

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant (non-zero) probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

The result can be checked

and if it is not a solution, repeat the process

Repeating several times increases success probability.

Warning: only a few further step does not necessarily improve the approximation!

Remarks

Looking the geometry in 2D is not cheating:

- Interesting things happen only in the span of $|k\rangle$ and $H|0\rangle$
- Vectors in the orthogonal subspace are fixed (or their signs are changed)

When there are $t > 1$ solutions

- if t is known

$$\frac{1}{\sqrt{t}} \sum_{f(k)=1} |k\rangle \quad \text{replaces} \quad |k\rangle$$

  angle of rotation $\approx 2\sqrt{t/N}$
  number of queries $O(\sqrt{N/t})$

- if t is unknown
  similarly to binary search or
  random number of iterations works (with large probability)

Algebraic view

$R_0 = I - 2P_0$, where P_0 is a **projection** to $|0\rangle$

$HR_0H = I - 2P$, where P is a **projection** to $H|0\rangle = \sum_x |x\rangle$

In matrix form

$$HR_0H = \begin{pmatrix} 1-\frac{2}{N} & -\frac{2}{N} & \cdots & -\frac{2}{N} \\ -\frac{2}{N} & 1-\frac{2}{N} & \cdots & -\frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{2}{N} & -\frac{2}{N} & \cdots & 1-\frac{2}{N} \end{pmatrix}$$

Algebraic view

The action of $H(-R_0)H$ on a vector is

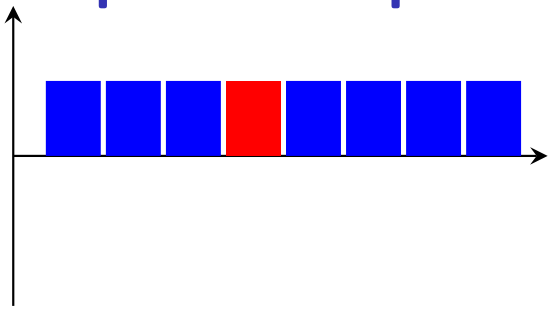
$$\sum_x \alpha_x |x\rangle \mapsto \sum_x (2A - \alpha_x) |x\rangle$$

where A is the average $A = \frac{\sum_x \alpha_x}{N}$

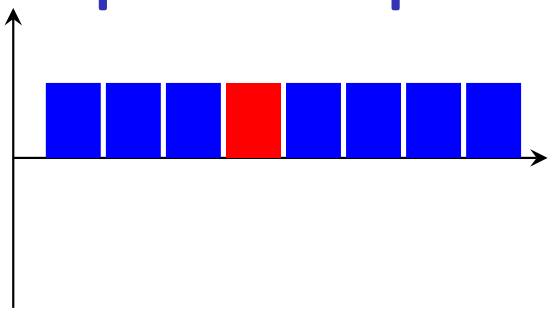
Transformation of coordinates: $\alpha_x \mapsto 2A - \alpha_x = A + (A - \alpha_x)$ is

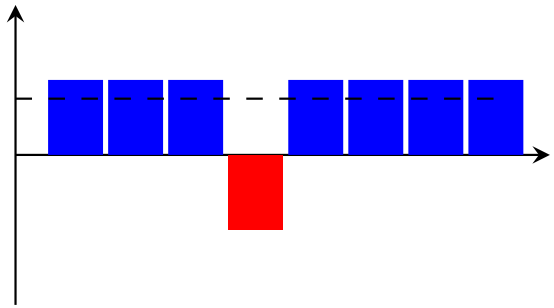
reflection to average

Amplitude amplification

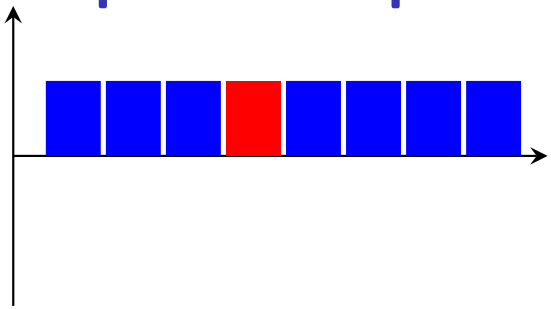


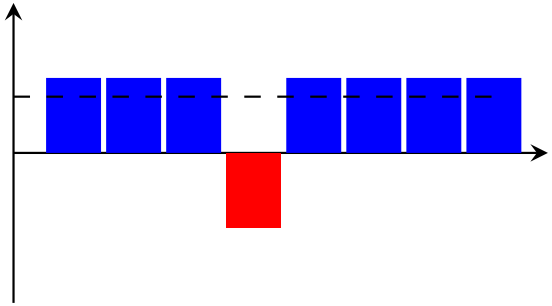
Amplitude amplification

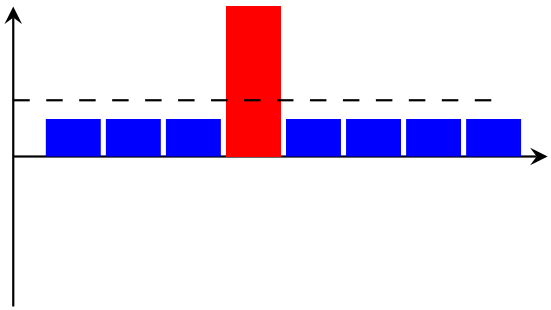




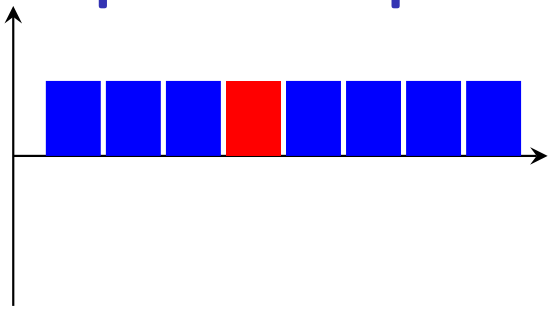
Amplitude amplification

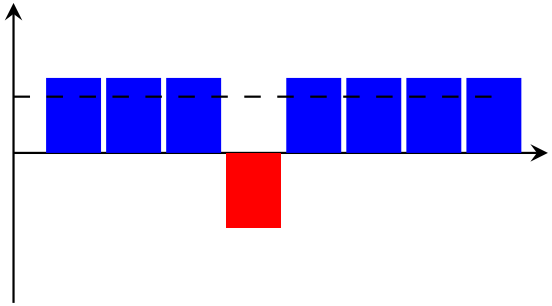


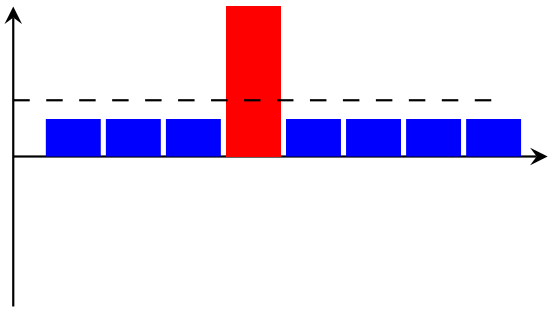


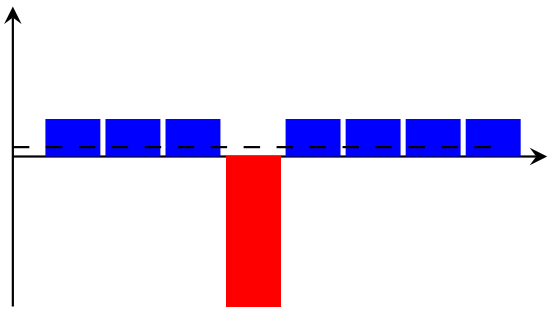


Amplitude amplification

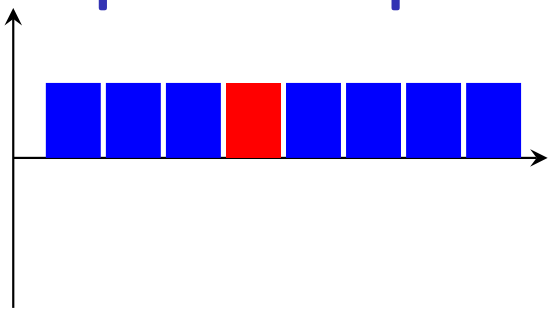


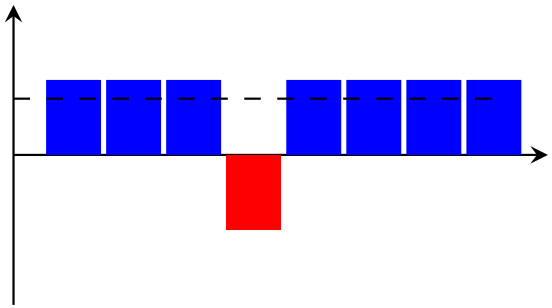


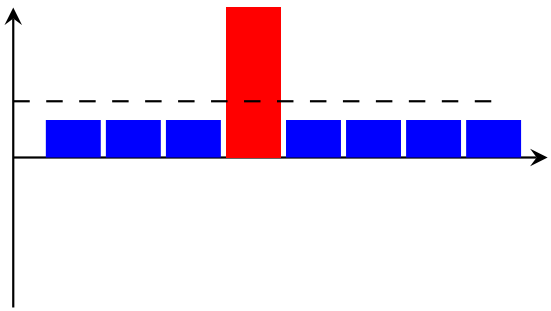


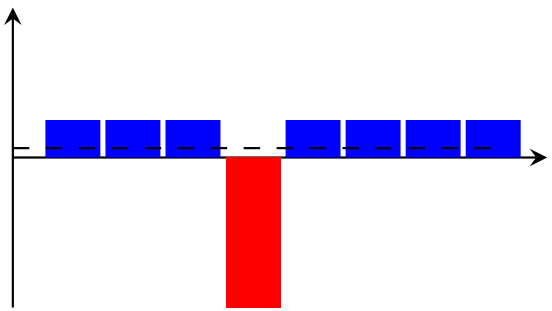


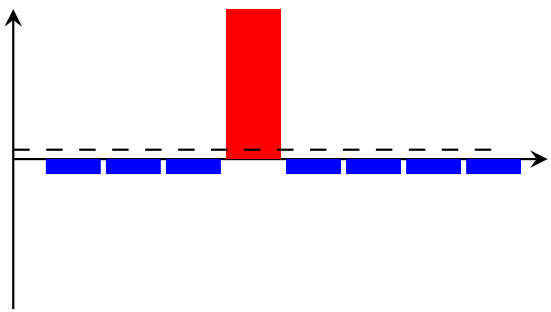
Amplitude amplification



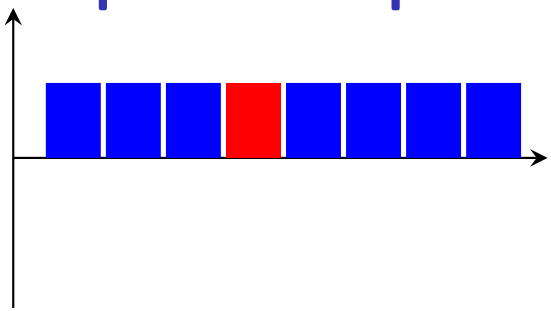


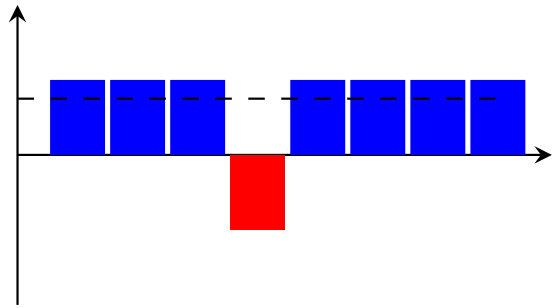


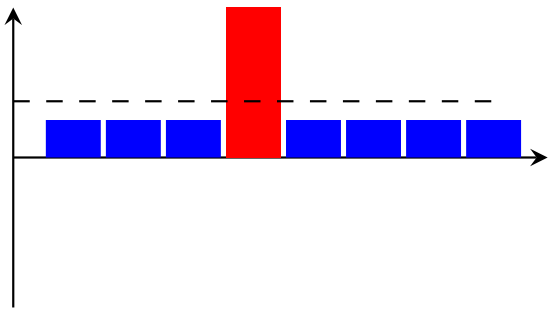


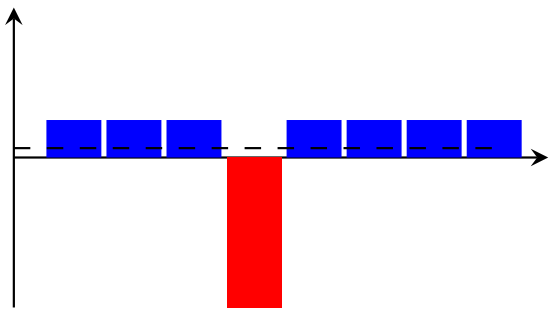


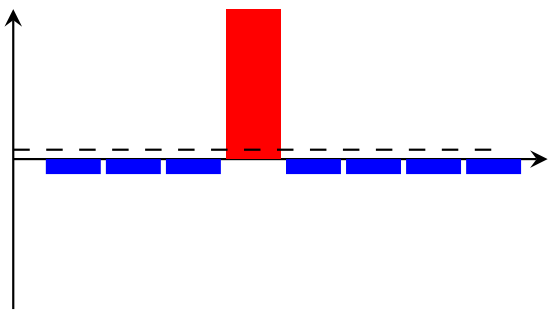
Amplitude amplification

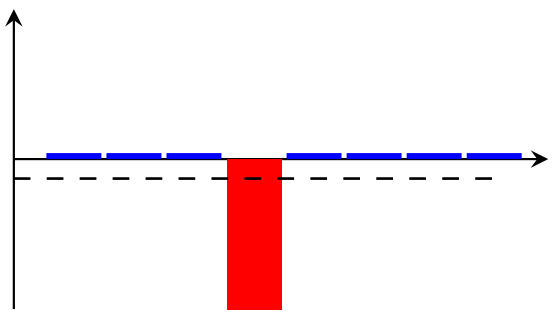




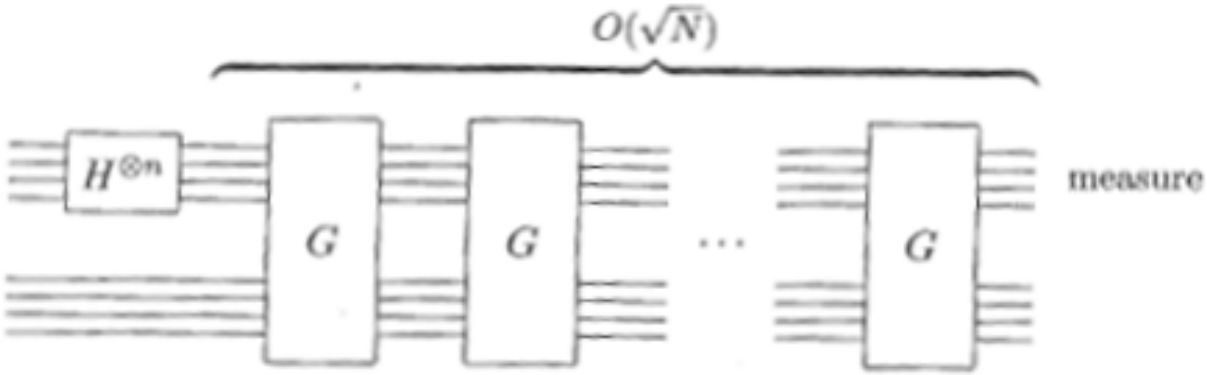




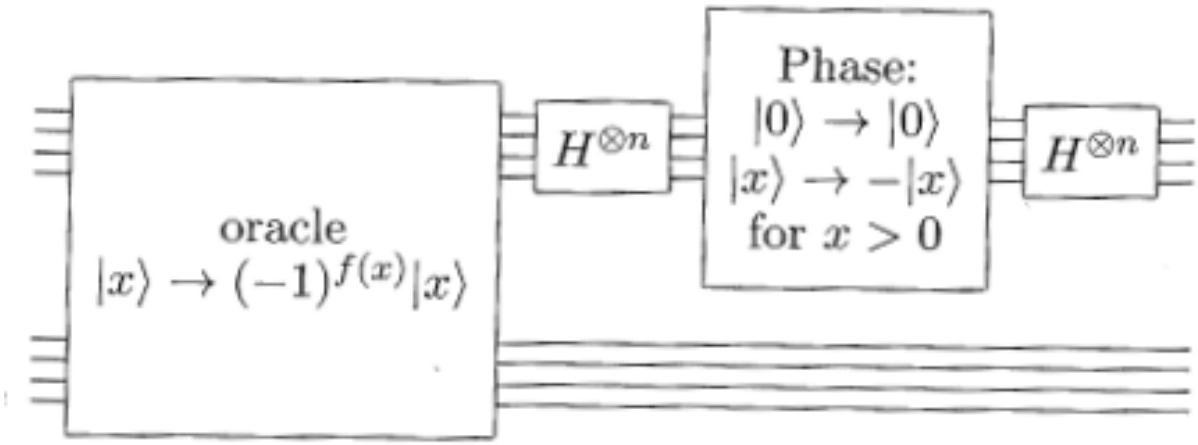




Circuit form



Grover operation



Related problems

Smallest, largest elements

Grover's algorithm can be used $O(\sqrt{N})$ queries

Approximate counting

Grover's algorithm + phase estimation

Ordered search

very different — Grover does not help

classical: $\log n$ queries

Related problems

Smallest, largest elements

Grover's algorithm can be used $O(\sqrt{N})$ queries

Approximate counting

Grover's algorithm + phase estimation

Ordered search

very different — Grover does not help

classical: $\log n$ queries

quantum **algorithm** $\approx 0.4 \log n$ (Child, Landahl, Parillo 2006)

quantum **lower bound** $\approx 0.22 \log n$ (Høyer, Neerbek, Shi 2001)

Quantum algorithms and cryptography

Cryptosystem based on the difficulty of prime factorization (RSA) is not safe – against (large enough) quantum computer

Two directions:

- find better systems
  different suggestions, much more complicated than RSA
  Post-quantum cryptography – hard math – not in this talk
- use quantum to generate secret keys for classical systems
  simple, working

based on the idea of Wiesner from 1970s
scheme from Bennett, Brassard – BB84

Quantum key distribution

2 players **A** and **B** **goal**: generate a common random bit sequence

Algorithm

A generates random bits – a subsequence will be the common sequence

2 ways of encoding: $+$: $0 \mapsto |0\rangle$ $1 \mapsto |1\rangle$, X: $0 \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $1 \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

A n random bits: 0 1 1 0 1 0 1

Quantum key distribution

2 players **A** and **B** **goal**: generate a common random bit sequence

Algorithm

A generates random bits – a subsequence will be the common sequence

2 ways of encoding: $+$: $0 \mapsto |0\rangle$ $1 \mapsto |1\rangle$, X: $0 \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $1 \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

A	n random bits:	0	1	1	0	1	0	1
	n random encodings:	$+$	X	X	$+$	$+$	X	$+$

Quantum key distribution

2 players **A** and **B** **goal**: generate a common random bit sequence

Algorithm

A generates random bits – a subsequence will be the common sequence

2 ways of encoding: $+$: $0 \mapsto |0\rangle$ $1 \mapsto |1\rangle$, X: $0 \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $1 \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

A	n random bits:	0	1	1	0	1	0	1
	n random encodings:	$+$	X	X	$+$	$+$	X	$+$
	qubit sent to **B**:	$\rightarrow$	$\searrow$	$\searrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\uparrow$

Quantum key distribution

2 players **A** and **B** **goal**: generate a common random bit sequence

Algorithm

A generates random bits – a subsequence will be the common sequence

2 ways of encoding: $+$: $0 \mapsto |0\rangle$ $1 \mapsto |1\rangle$, X: $0 \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $1 \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

A	n random bits:	0	1	1	0	1	0	1
	n random encodings:	$+$	X	X	$+$	$+$	X	$+$
	qubit sent to **B**:	$\rightarrow$	$\searrow$	$\searrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\uparrow$
B	random basis	X	$+$	**X**	X	**+**	**X**	X

Quantum key distribution

2 players **A** and **B** **goal**: generate a common random bit sequence

Algorithm

A generates random bits – a subsequence will be the common sequence

2 ways of encoding: $+$: $0 \mapsto |0\rangle$ $1 \mapsto |1\rangle$, X: $0 \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $1 \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

A	n random bits:	0	1	1	0	1	0	1
	n random encodings:	$+$	X	X	$+$	$+$	X	$+$
	qubit sent to **B**:	$\rightarrow$	$\searrow$	$\searrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\uparrow$
B	random basis	X	$+$	**X**	X	**+**	**X**	X
	measure	0/1	0/1	**1**	0/1	**1**	**0**	0/1

B tells his choices of basis (when measurement is finished)
A tells where he guessed right – here are the common bits ($\approx n/2$)

eavesdropper: changes qubits – caught if A and B checks a few
improvement: use error correcting code for the bits (because of noise)

Given positive integer n find its **prime factors**
No deterministic polynomial algorithm is known

can be assumed that n is odd and $n \neq m^k$
(easy to find $k > 1$ and m if they exist)

method to find one **non-trivial factor** is enough
(can be repeated to get prime factors)

Goal: find $1 < a < n$ s.t. $\gcd(a, n) > 1$
(such gcd is a non-trivial factor of n)

Given positive integer n find its **prime factors**
No deterministic polynomial algorithm is known

can be assumed that n is odd and $n \neq m^k$
(easy to find $k > 1$ and m if they exist)

method to find one **non-trivial factor** is enough
(can be repeated to get prime factors)

Goal: find $1 < a < n$ s.t. $\gcd(a, n) > 1$
(such gcd is a non-trivial factor of n)

If $\gcd(a, n) = 1$ then there is $n > r > 0$: $a^r \equiv 1 \pmod{n}$
order of a: $o(a) = \min\{r > 0 : a^r \equiv 1 \pmod{n}\}$

Property $\gcd(a, n) = 1$ and $o(a) = 2k$ even $\Rightarrow \gcd(a^k + 1, n) > 1$
(since $n | a^{2k} - 1 = (a^k - 1)(a^k + 1)$ and $k < o(a)$)

Factorization by using orders

Probabilistic algorithm

– pick random $1 < a < n$
– compute $(gcd(a, n)$ if this is > 1, stop
– compute $o(a)$
– if $o(a) = 2k$ and $\gcd(a^k + 1, n) < n$, stop
– otherwise repeat

Factorization by using orders

Probabilistic algorithm

– pick random $1 < a < n$
– compute $(gcd(a, n)$ if this is > 1, stop
– compute $o(a)$
– if $o(a) = 2k$ and $\gcd(a^k + 1, n) < n$, stop
– otherwise repeat

Lemma

n has $t \geq 2$ *different prime divisors* $\Rightarrow Pr(o(a) =$ *odd* $) \leq 2^{-t}$ *and if* $o(a) = 2k \Rightarrow Pr(\gcd(a^k + 1, n) = n) \leq 2^{-(t-1)}$

Factorization by using orders

Probabilistic algorithm

– pick random $1 < a < n$
– compute $(gcd(a, n)$ if this is > 1, stop
– compute $o(a)$
– if $o(a) = 2k$ and $\gcd(a^k + 1, n) < n$, stop
– otherwise repeat

Lemma

n has $t \geq 2$ different prime divisors $\Rightarrow Pr(o(a) = \text{ odd }) \leq 2^{-t}$ *and*
if $o(a) = 2k \Rightarrow Pr(\gcd(a^k + 1, n) = n) \leq 2^{-(t-1)}$

Corollary

A random $1 < a < n$ *is good with probability* $\geq (1 - 2^{-t})(1 - 2^{-(t-1)}) \geq \frac{3}{8}$

Probability that none of 5 random a is good $< 1/100$

Factorization by using orders

Probabilistic algorithm

– pick random $1 < a < n$
– compute $(gcd(a, n)$ if this is > 1, stop
– compute $o(a)$
– if $o(a) = 2k$ and $\gcd(a^k + 1, n) < n$, stop
– otherwise repeat

Lemma

n has $t \geq 2$ different prime divisors $\Rightarrow Pr(o(a) = \text{ odd }) \leq 2^{-t}$ *and*
if $o(a) = 2k \Rightarrow Pr(\gcd(a^k + 1, n) = n) \leq 2^{-(t-1)}$

Corollary

A random $1 < a < n$ *is good with probability* $\geq (1 - 2^{-t})(1 - 2^{-(t-1)}) \geq \frac{3}{8}$

Probability that none of 5 random a is good $< 1/100$

But

no known efficient algorithms (deterministic or probabilistic) to compute orders

this is where **quantum helps**

Quantum Fourier transform

QFT mod $N > 0$

$\omega \in \mathbb{C}$: primitive root of unity, $\omega^N = 1$, $\omega^k \neq 1$ if $k < N$

can take the first: $\omega = \cos(2\pi/N) + i\sin(2\pi/N) = e^{-2\pi i/N}$

QFT : $|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x\cdot y} |y\rangle \quad (0 \leq x \leq N-1)$

In matrix form

$$QFT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

$\Rightarrow QFT^T = QFT$, $\overline{QFT}$ is similar with ω^{-1} instead of ω, QFT is unitary:

$(QFT \cdot QFT^*)_{k,\ell} = \frac{1}{N} \sum_j \omega^{kj} \omega^{-j\ell} =$

Quantum Fourier transform

QFT mod $N > 0$

$\omega \in \mathbb{C}$: primitive root of unity, $\omega^N = 1$, $\omega^k \neq 1$ if $k < N$

can take the first: $\omega = \cos(2\pi/N) + i\sin(2\pi/N) = e^{-2\pi i/N}$

QFT : $|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x\cdot y} |y\rangle \quad (0 \leq x \leq N-1)$

In matrix form

$$QFT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

$\Rightarrow QFT^T = QFT$, $\overline{QFT}$ is similar with ω^{-1} instead of ω, QFT is unitary:

$(QFT \cdot QFT^*)_{k,\ell} = \frac{1}{N} \sum_j \omega^{kj} \omega^{-j\ell} = \frac{1}{N} \sum_j \omega^{(k-\ell)j} =$

Quantum Fourier transform

QFT mod $N > 0$

$\omega \in \mathbb{C}$: primitive root of unity, $\omega^N = 1$, $\omega^k \neq 1$ if $k < N$

can take the first: $\omega = \cos(2\pi/N) + i\sin(2\pi/N) = e^{-2\pi i/N}$

QFT : $|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x\cdot y} |y\rangle \quad (0 \leq x \leq N-1)$

In matrix form

$$QFT = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

$\Rightarrow QFT^T = QFT$, $\overline{QFT}$ is similar with ω^{-1} instead of ω, QFT is unitary:

$$(QFT \cdot QFT^*)_{k,\ell} = \frac{1}{N} \sum_j \omega^{kj} \omega^{-j\ell} = \frac{1}{N} \sum_j \omega^{(k-\ell)j} = \begin{cases} 1 & \text{if } k = \ell \\ 0 & \text{if } k \neq \ell \end{cases}$$

QFT and periodic functions

$f : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ p-**periodic**: $f(x+p) = f(x)$

Assumption: $p|N$ and $f(x) = f(z)$ iff $x - z = j \cdot p$ for some $0 \leq j \leq N/p - 1$

Goal: find p

Quantum algorithm:

start with 2 n-qubit registers $|0\rangle |0\rangle$

– steps: $QFT \otimes I$, f, $QFT^{-1} \otimes I$, M

Details:

$$|0\rangle |0\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle \to$$

$$\frac{1}{N} \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \omega^{xz} |z\rangle |f(x)\rangle = \frac{1}{N} \sum_z \sum_y \sum_{x:f(x)=y} \omega^{xz} |z\rangle |y\rangle$$

QFT and periodic functions

$f : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ p-**periodic**: $f(x+p) = f(x)$

Assumption: $p|N$ and $f(x) = f(z)$ iff $x - z = j \cdot p$ for some $0 \le j \le N/p - 1$

Goal: find p

Quantum algorithm:

start with 2 n-qubit registers $|0\rangle|0\rangle$

– steps: $QFT \otimes I$, f, $QFT^{-1} \otimes I$, M

Details:

$$|0\rangle|0\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \to$$

$$\frac{1}{N} \sum_{x=0}^{N-1} \sum_{z=0}^{N-1} \omega^{xz} |z\rangle|f(x)\rangle = \frac{1}{N} \sum_z \sum_y \sum_{x:f(x)=y} \omega^{xz} |z\rangle|y\rangle$$

coefficient of $|z\rangle|y\rangle$:

$$\frac{1}{N} \sum_j \omega^{(x+jp)z} = \frac{1}{N} \omega^{xz} \sum_j \omega^{pzj} = \begin{cases} \omega^{xz}/p & \text{if } \omega^{pz} = 1 \\ 0 & \text{o/w} \end{cases}$$

Measurement $\rightarrow z$ s.t. $\omega^{pz} = 1 \Leftrightarrow pz \equiv 0 \pmod{N}$

any of these with same probability – **uniform sample**

$$z \in \{0, N/p, 2N/p, \ldots, (N/p-1)N/p\}$$

$\Rightarrow z/N = k/p$ here left side is known

Measurement $\rightarrow z$ s.t. $\omega^{pz} = 1 \Leftrightarrow pz \equiv 0 \pmod{N}$

any of these with same probability – **uniform sample**

$$z \in \{0, N/p, 2N/p, \ldots, (N/p-1)N/p\}$$

$\Rightarrow z/N = k/p$ here left side is known

find a reduced form of $z/N \Rightarrow$ denominator is p if $\gcd(k, p) = 1$

Measurement $\to z$ s.t. $\omega^{pz} = 1 \Leftrightarrow pz \equiv 0 \pmod{N}$

any of these with same probability – **uniform sample**

$$z \in \{0, N/p, 2N/p, \ldots, (N/p-1)N/p\}$$

$\Rightarrow z/N = k/p$ here left side is known

find a reduced form of $z/N \Rightarrow$ denominator is p if $\gcd(k, p) = 1$

can achieve this with high probability
(collect samples $z_1, \ldots, z_t$ and take $z = \gcd(z_1, \ldots, z_t)$)

Application to factorization

for a random $1 < a < n$ with $\gcd(a, n) = 1$

$f(x) = f_a(x) = a^x \pmod{n}$ is periodic, $p = o(a)$

Application to factorization

for a random $1 < a < n$ with $\gcd(a, n) = 1$

$f(x) = f_a(x) = a^x \pmod{n}$ is periodic, $p = o(a)$

difficulties:

– need a multiple of period for N

– get QFT – easy when $N = 2^s$

solution for both: $N = 2^s \quad (N \approx n^2)$ then QFT is ok

period only approximate: $N = pt + r$ but error r is small compare to N

$|z/N - k/p|$ is small

so the task: for given z/N find a k/p close to it where p is small –

rational approximation – there is classical algo (continued fractions)

Theorem

A non-trivial factor of n can be found in time poly$(\log n)$ *with constant (non-zero) probability.*

Remarks

1-qubit Hadamard is QFT for $N = 2$

Remarks

1-qubit Hadamard is QFT for $N = 2$

n-qubit Hadamard is QFT for group $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$
$\Rightarrow$ Simon is also finding the period of functions

Remarks

1-qubit Hadamard is QFT for $N = 2$

n-qubit Hadamard is QFT for group $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$
$\Rightarrow$ Simon is also finding the period of functions

More general setting: **Hidden subgroup problem**
same scheme+classical post-processing
(needs efficient QFT on the group and group theory for the end)

Remarks

1-qubit Hadamard is QFT for $N = 2$

n-qubit Hadamard is QFT for group $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$
$\Rightarrow$ Simon is also finding the period of functions

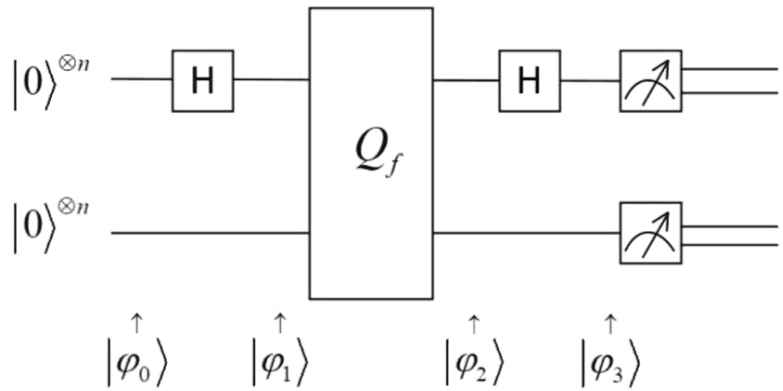
More general setting: **Hidden subgroup problem**
same scheme+classical post-processing
(needs efficient QFT on the group and group theory for the end)

– an interesting application would be: graph isomorphism
for graphs on n vertices – hidden subgroup problem in S_{2n}
problem to handle QFT and obtain enough information from the quantum part

Quantum algorithms in general

more complicated

described by quantum circuit (not with arrows), for example Simon's algo:



pure state $|\varphi\rangle \rightsquigarrow$ **mixed states**= distributions: $|\varphi_i\rangle$ with prob. p_i

– described by density matrix $\rho = \sum_i p_i |x_i\rangle \langle x_i|$

If $|x_i\rangle$ are orthogonal then $\rho |x_i\rangle = p_i |x_i\rangle$, $\langle x_i| \rho |x_i\rangle = p_i$.
$\Rightarrow |x_i\rangle$ are eigenvectors with eigenvalues p_i

Summary

quantum and classical differ in efficiency, can be combined

There are problems

– where quantum is more efficient (unordered search)

– where it is not big help (ordered search)

– where better than currently known classical (prime factorization)

Requires quantum box (quantum oracle), special input preparation
not always easy to make

Other approaches (quantum walks, adiabatic computing, etc)

Current quantum computers: not enough quantum bits, large prob. of error

Future ??