Introduction to Quantum Computation

Nils Anders Danielsson

nad@cs.chalmers.se

April 28, 2003

Qubits

- *Qubit*:

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

  $|\alpha|^2 + |\beta|^2 = 1$, $\alpha, \beta \in \mathbb{C}$, $|0\rangle\,, |1\rangle \in \mathbb{C}^2$.

- Difference from classical bit: *Superposition* of states possible.

- Example of *computational basis*:

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

Realisation

- Qubits can in principle be realised by any two-level quantum system such as:
  - The polarisation of a photon.
  - The state (alive/dead) of Schrödinger's cat.
- System interacts with the environment $\Rightarrow$ superposition will eventually break down (decoherence).
- System needs to be isolated.
- Error correcting techniques necessary.
- Using the cat isn't a good idea.

Registers

- A quantum *register* consisting of n qubits:

$$|a_1 \dots a_n\rangle = |a_1\rangle \otimes \cdots \otimes |a_n\rangle \in \mathbb{C}^{2^n}.$$

- $\otimes : \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^{mn}$ is the *tensor product*:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_1 b_n \\ \vdots \\ a_m b_1 \\ \vdots \\ a_m b_n \end{pmatrix}.$$

- Example: $|1\rangle \otimes |0\rangle = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle = |2\rangle$.

- $\otimes$ is often omitted: $|0\rangle \otimes |1\rangle = |0\rangle\,|1\rangle = |01\rangle$.

More registers

- Superpositions are possible:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle ,$$

  $\sum_i |\alpha_i|^2 = 1.$

- Not all n-qubit states can be written as a tensor product of single qubit states (they are *entangled*):

$$\alpha_0 |00\rangle + \alpha_3 |11\rangle , \ \alpha_1, \alpha_3 \neq 0.$$

Measurement

- If we measure the qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ *with respect to* the computational basis $\{\,|0\rangle\,,\;|1\rangle\,\}$ the result is:
  - $|0\rangle$ with probability $|\alpha|^2$.
  - $|1\rangle$ with probability $|\beta|^2$.
- Upon measurement the qubit *changes its state* to the measured value.
- More general measurements possible.

Measuring registers

If we measure *the first* qubit in a register setup as

$$\alpha_0 \left|00\right\rangle + \alpha_1 \left|01\right\rangle + \alpha_2 \left|10\right\rangle + \alpha_3 \left|11\right\rangle$$

we get:

- $\frac{1}{\sqrt{|\alpha_0|^2+|\alpha_1|^2}} \left(\alpha_0 \left|00\right\rangle + \alpha_1 \left|01\right\rangle\right)$ with probability $|\alpha_0|^2 + |\alpha_1|^2$.
- $\frac{1}{\sqrt{|\alpha_2|^2+|\alpha_3|^2}} \left(\alpha_2 \left|10\right\rangle + \alpha_3 \left|11\right\rangle\right)$ with probability $|\alpha_2|^2 + |\alpha_3|^2$.

Unitary matrices

- A matrix $M \in \mathbb{C}^{n \times n}$ is *unitary* if
$$M^\dagger = M^{-1}.$$
This holds iff the columns form an ON-basis.

- $M^\dagger$ is the *adjoint*, or conjugate transpose, of M:
$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ e^{i\varphi} & e^{i\varphi} \end{pmatrix}^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi} \\ -1 & e^{-i\varphi} \end{pmatrix}.$$

- An operator is unitary if one, and hence all, of its representations are unitary.

Change

- A linear function maps a qubit to a qubit iff it is unitary.
- The state evolution of a *closed* (no external interaction, so no measurements) quantum system is determined by unitary operators:

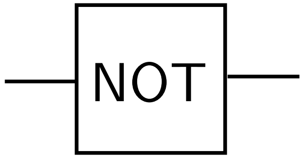
$$|\psi_{i+1}\rangle = U\,|\psi_i\rangle\,, \quad U \text{ unitary.}$$

- This is a discrete version of the Schrödinger equation.
- Note that all unitary operations are reversible.

Quantum gates

Usually a circuit model is used. Some example gates:

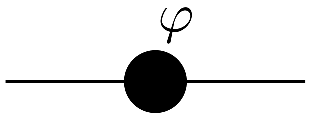
NOT:



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

$$|0\rangle \mapsto |1\rangle$$
$$|1\rangle \mapsto |0\rangle$$

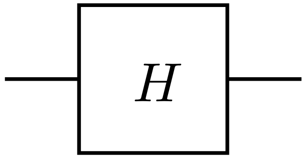
PHASE$_\varphi$:



$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

$$|x\rangle \mapsto e^{ix\varphi}\,|x\rangle$$

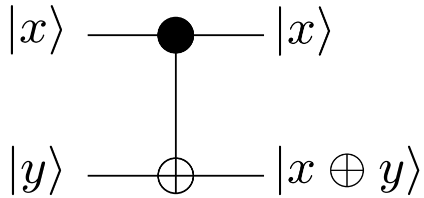
Hadamard:



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

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

CNOT:



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

$$|x\rangle\,|y\rangle \mapsto |x\rangle\,|x \oplus y\rangle$$

($\oplus$ is exclusive or.)

Universal sets of gates

All unitary operations on n qubits can be implemented

- exactly using $\mathcal{O}(n^2 4^n)$ CNOT and single qubit gates.
- to an accuracy ϵ using $\mathcal{O}\left(n^2 4^n \log^c\left(\frac{n^2 4^n}{\epsilon}\right)\right)$ gates ($c \approx 2$) from the set

$$\{\,\mathsf{CNOT},\ H,\ \mathsf{PHASE}_{\frac{\pi}{4}}\,\}.$$

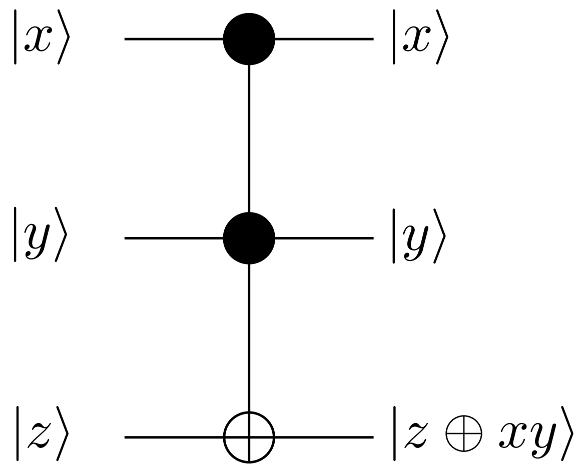
Lower bound: $\Omega\left(2^n \frac{\log \frac{1}{\epsilon}}{\log n}\right)$.

Computability

- Quantum computers can simulate classical computers (and vice versa).
- Obstacle for simulation: All functions reversible.
- Solution: Save input. (Have to take care of garbage as well.)

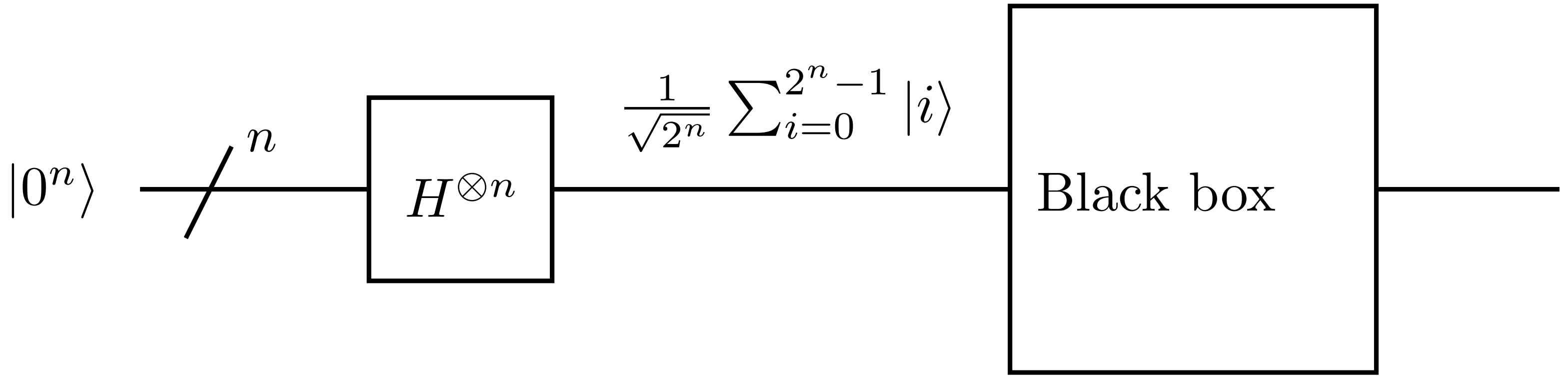
$$|x\rangle\,|y\rangle \mapsto |x\rangle\,|y \oplus f(x)\rangle$$

- Can use *Toffoli gate*:



No cloning

- Take advantage of superpositions.
- Example: 2^n computations in one step.



- But: Can only measure output once. Can't even copy it.
- *No-cloning theorem*: There is no unitary operator U such that

$$U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle \quad \text{for all qubits } |\psi\rangle\,.$$

- No general FANOUT.

Extended example: Grover's search algorithm

- $N = 2^n$ elements: $\mathbb{N}_N$.
- M solutions, $M \geq 1$.
- Oracle $f : \mathbb{N}_N \to \mathbb{N}_1$, $f(x) = 1$ iff x solution.
- Problem: Find one solution.

Use an n-qubit register initialised to a superposition of all elements in the search space

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{N}_N} |x\rangle ,$$

and one oracle qubit initialised to

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

- Assume that we have an oracle circuit O:

$$O(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle\,.$$

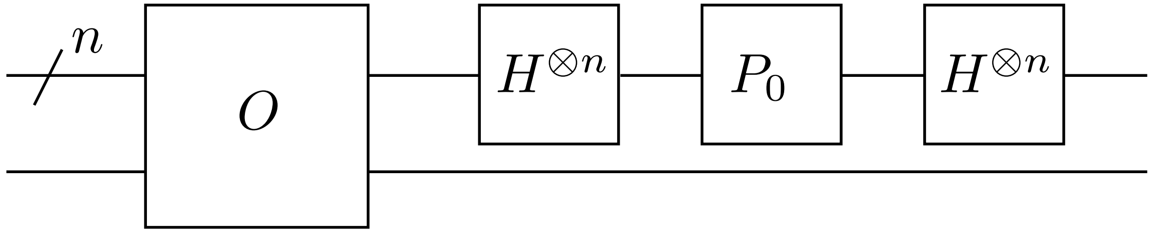
- Notice that O maps

$$|x\rangle\,\frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle) \;\mapsto\; (-1)^{f(x)}\,|x\rangle\,\frac{1}{\sqrt{2}}\,(|0\rangle - |1\rangle)\,.$$

- So let us ignore the oracle qubit:

$$O\left(\sum_{x\in\mathbb{N}_N} \alpha_x\,|x\rangle\right) = \sum_{x\in\mathbb{N}_N} (-1)^{f(x)}\alpha_x\,|x\rangle\,.$$

- Grover operator $G = H^{\otimes n} P_0 H^{\otimes n} O$.



- Conditional phase shift:

$$P_0 |x\rangle = \begin{cases} |x\rangle, & x = 0, \\ -|x\rangle, & x \neq 0. \end{cases}$$

- $\langle x| \, |y\rangle = \langle x|y\rangle = |x\rangle^\dagger |y\rangle$.
- $P_0 = 2 |0\rangle \langle 0| - I$ and $H^\dagger = H \Rightarrow$

$$H^{\otimes n} P_0 H^{\otimes n} = H^{\otimes n}(2 |0\rangle \langle 0| - I) H^{\otimes n} = 2 |\psi\rangle \langle\psi| - I.$$

- Define $S_0 = \{\, x \in \mathbb{N}_N \mid f(x) = 0 \,\}$, $S_1 = \mathbb{N}_N \setminus S_0$,

$$|\sigma\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in S_0} |x\rangle\,, \quad |\tau\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S_1} |x\rangle\,.$$

- We get

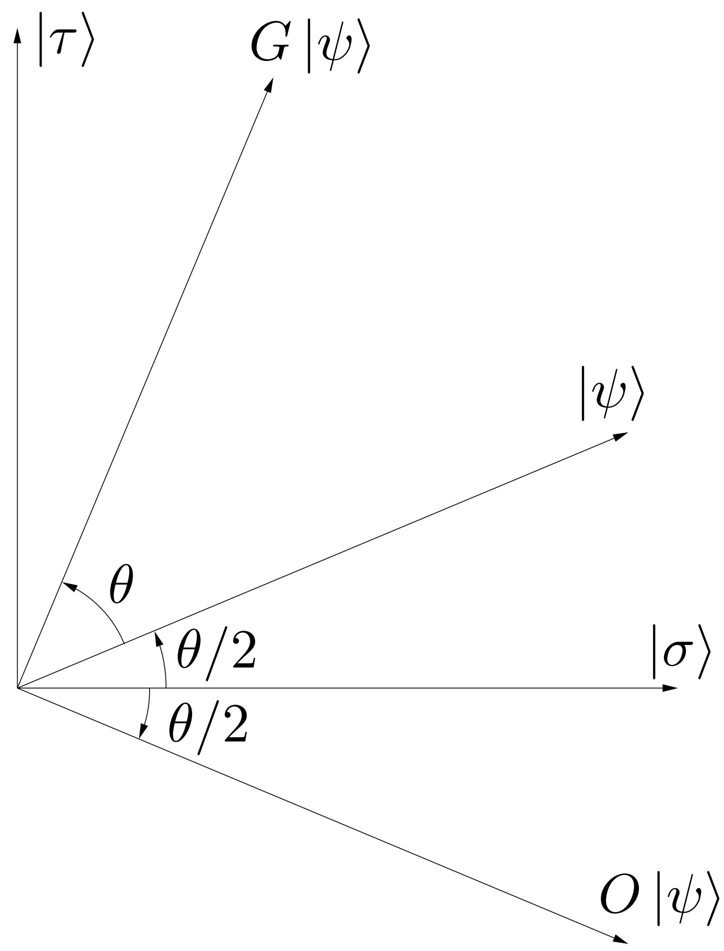
$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\sigma\rangle + \sqrt{\frac{M}{N}}\,|\tau\rangle\,,$$

i.e. $|\psi\rangle$ is contained in the plane spanned by $|\sigma\rangle$ and $|\tau\rangle$.

- O is a reflection about $|\sigma\rangle$:

  $$O(\alpha|\sigma\rangle + \beta|\tau\rangle) = \alpha|\sigma\rangle - \beta|\tau\rangle.$$

- $2|\psi\rangle\langle\psi| - I$ is reflection about $|\psi\rangle$.
- The composition of two reflections is a rotation.



- Initially:

$$|\psi\rangle = \cos\frac{\theta}{2}\,|\sigma\rangle + \sin\frac{\theta}{2}\,|\tau\rangle\,,$$

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}, \quad \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

- After m iterations:

$$G^m\,|\psi\rangle = \cos\left(\frac{2m+1}{2}\theta\right)|\sigma\rangle + \sin\left(\frac{2m+1}{2}\theta\right)|\tau\rangle\,.$$

- We want

$$\frac{2m+1}{2}\theta = \frac{\pi}{2}.$$

- Best approximation:

$$m = \left\lfloor \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil.$$

$\lfloor x \rceil$: the integer closest to x, rounding down in case of ambiguity.

- After m iterations $G^m |\psi\rangle$ is within $\frac{\theta}{2}$ of $|\tau\rangle$.
- $M \leq \frac{N}{2} \Rightarrow \frac{\theta}{2} \leq \frac{\pi}{4} \Rightarrow$ probability of success $\geq \frac{1}{2}$.
- What if $M > \frac{N}{2}$?
  - Choose element on random or
  - extend the search space to contain $2N$ keys.
- What if M is unknown? See below.

- $m \leq \lfloor \frac{\pi}{2\theta} \rfloor$ and $\frac{\theta}{2} \geq \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}$ implies that

$$m \leq \left\lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \right\rfloor \in \mathcal{O}\left(\sqrt{\frac{N}{M}} \right).$$

- This is actually optimal.
- For a classical computer $\mathcal{O}\left(\frac{N}{M}\right)$ oracle calls are needed.

Fourier transform

Several algorithms are based on the quantum Fourier transform ($\mathcal{O}(n^2)$):

- Phase estimation (estimates phase of eigenvalue of unitary operator, $\mathcal{O}\left(n^2 + \log^2\left(\frac{1}{\epsilon}\right)\right)$ gates and black boxes).
- Counting (counts solutions to search problem, $\mathcal{O}\left(\sqrt{N}\right)$ oracle calls, accuracy $\mathcal{O}\left(\sqrt{M}\right)$, probability of success $\mathcal{O}(1)$).
- Order finding (finds least positive integer r such that $x^r \equiv 1 \pmod{N}$, $\mathcal{O}\left(\log^3 N\right)$).
- Factoring ($\mathcal{O}\left(\log^3 N\right)$).

Complexity

- **BQP** is the quantum analogue to **BPP**.
- **BPP** $\subseteq$ **BQP** $\subseteq$ **PSPACE**.
- Grover's algorithm can be used to speed up naive search, but no exponential speedup, so no hope of solving **NP**-complete problems efficiently without more sophisticated approaches.
- Variations of the basic computational model used might make a difference. This model is e.g. limited to finite dimensional state spaces, with qubits initially in computational basis states.

Acknowledgements

- This presentation is heavily based on course notes written by Abbas Edalat (`http://www.doc.ic.ac.uk/~ae/`).
- Those notes are in turn heavily based on Nielsen and Chuang's book [NC00].

References

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.