Quantum Computing

Benjamin Maier

"Models of Computation" – Department of Philosophy

12 June 2012

Universiteit Utrecht

Table of Contents

Table of Contents

Universiteit Utrecht

Origins

- problems for classical computers: electronical elements get smaller

$\Rightarrow$ QM effects

- computation possible despite QM effects?
- even *use* these effects?

- R. Feynman (1982): classically acting computer, solely based on QM (picture: wikipedia.org)

- D. Deutsch (1985): QC is hypothetically superior to classical computation (picture: wired.com)

Universiteit Utrecht

Dry Stuff that We Can Hopefully Skip: Quantum Theory

- in QM, we express states of systems as linear combination of complex base vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \qquad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \end{pmatrix}, \qquad \ldots$$

- states "kets": $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \ldots,$
- α_i: probabilities
- dual space "bras"

$$\langle 0| = (1, 0, \ldots)^*, \qquad \langle 1| = (0, 1, \ldots)^*,$$

  obtained by hermitian conjugation: $\langle\psi| = |\psi\rangle^\dagger$ (speak: dagger)
- scalar products: "bra-kets" (brackets) $\langle\psi|\phi\rangle$, probability amplitude of measuring ϕ to be ψ
- states represent probability $\Rightarrow$ normed to 1, $\langle\psi|\psi\rangle = 1$, states form an orthonormal base, $\langle m|n\rangle = \delta_{mn}$
- operators (matrices): $|\psi\rangle\langle\phi|$

Table of Contents

Universiteit Utrecht

Storage of a QC

- classical computers: bits, 0 and 1
- use two-state systems:

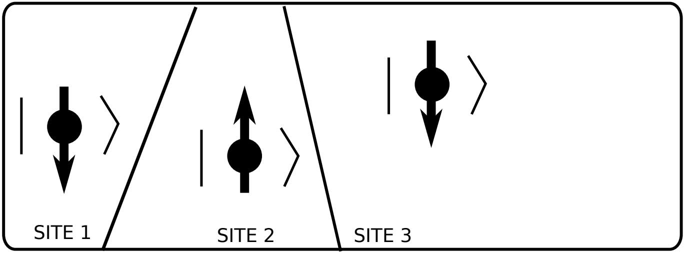
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- a "qubit" $|q\rangle$ can be $|0\rangle$,$|1\rangle$ or a superposition of both, e.g.
  $|q\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
- storage of n bits: n-body system of two-state systems in interaction, living in sites

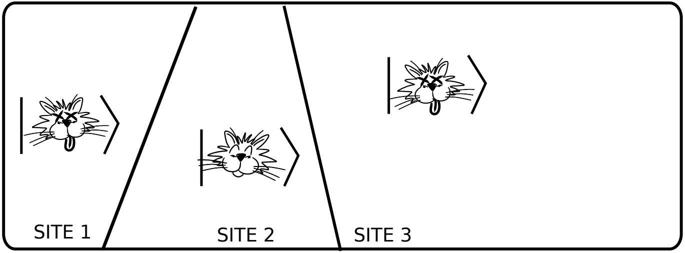
$$|\psi\rangle = |q_1\rangle \otimes |q_2\rangle \otimes \ldots \otimes |q_n\rangle = |q_1\rangle|q_2\rangle\ldots|q_n\rangle = |q_1 q_2 q_3 \ldots q_n\rangle$$

Storage of a QC

spin quantum storage



Schrödinger's quantum storage



Universiteit Utrecht

actual computation?

Operations on a Storage

- operators necessary $\Rightarrow$ represented by matrices
- obtained by creation and annihilation operators

$$\begin{aligned}
\text{creation: } a^\dagger &= |1\rangle\langle 0| \qquad a^\dagger|0\rangle = |1\rangle\,\langle 0|0\rangle = |1\rangle, \qquad a^\dagger|1\rangle = 0,\\
\text{annihilation: } a &= |0\rangle\langle 1| \qquad a\,|1\rangle = |0\rangle\,\langle 1|1\rangle = |0\rangle, \qquad a\,|0\rangle = 0,
\end{aligned}$$

$\Rightarrow$ everything we need, e.g.

$$\begin{aligned}
NOT &= a + a^\dagger = |1\rangle\langle 0| + |0\rangle\langle 1|,\\
NOT(a|0\rangle + b|1\rangle) &= \Big(|1\rangle\langle 0| + |0\rangle\langle 1|\Big)\ \Big(a|0\rangle + b|1\rangle\Big)\\
&= a|1\rangle \underbrace{\langle 0|0\rangle}_{=1} + a|0\rangle \underbrace{\langle 1|0\rangle}_{=0} + b|1\rangle \underbrace{\langle 0|1\rangle}_{=0} + b|0\rangle \underbrace{\langle 1|1\rangle}_{=1}\\
&= a|1\rangle + b|0\rangle\\
PROJECTION_0 &= aa^\dagger = IF_0\\
\mathbf{1} &= IF_0 + IF_1
\end{aligned}$$

Universiteit Utrecht

Reversibility

- solves a lot of problems
  - minimizes needed energy (hypothetically to zero $\Leftarrow$ entropy change is zero)
  - easier formulation of operators in terms of common physics
  - handy for computations (phase shift)
- *more in "Reversible Computing"*
- operator A is reversible, if there exists A^{-1}
- easiest operators to achieve this: unitary $U^{-1} = U^{\dagger}$
- *NOT* is unitary and reversible (*NOT* twice yields initial state)
- *IF* is not unitary and not reversible

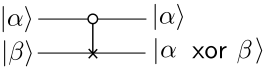
You still have not shown an actual computation!!

Bit Addition à la Feynman

suppose input states $|\alpha\beta\rangle$ and $|\alpha\beta\gamma\rangle$

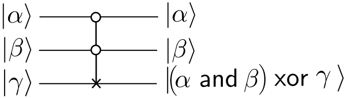
necessary reversible gates:

Controlled Not



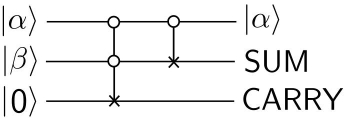
$$CNOT_{\alpha,\beta} = \mathbf{1} + (NOT^{(\beta)} - \mathbf{1})IF_1^{(\alpha)}$$

Controlled Controlled Not



$$CCNOT_{\alpha\beta,\gamma} = \mathbf{1} + (NOT^{(\gamma)} - \mathbf{1})IF_1^{(\alpha)}IF_1^{(\beta)}$$

Adder



$$CNOT_{\alpha,\beta}\ CCNOT_{\alpha\beta,\gamma} = \Big(\mathbf{1} + (b + b^\dagger - \mathbf{1})a^\dagger a\Big)$$
$$\times \Big(\mathbf{1} + (c + c^\dagger - \mathbf{1})a^\dagger a b^\dagger b\Big)$$

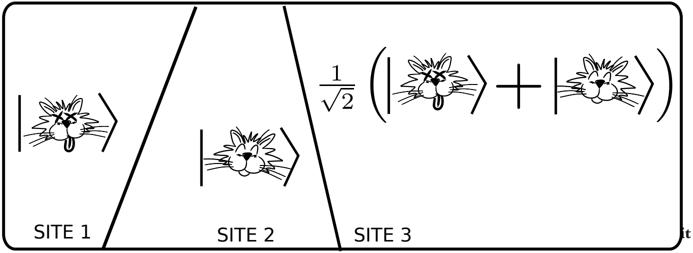
Advantages of QC

- until now: take state $|\alpha\beta 0\rangle$, perform the bit addition - done - nothing new!
- but wait why don't we just perform everything at once?
- Hadamard transformation

$$|0\rangle \to \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

- get superposition in initial state - what does that mean?

Schrödinger's quantum storage after Hadamard application



Quantum parallelism

- initial state: $|000\rangle$
- Hadamard transformation on first two qubits

$$|\psi\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle$$

- performing bit addition of first two qubits, yielding

$$CNOT_{\alpha,\beta} CCNOT_{\alpha\beta,\gamma}|\psi\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|101\rangle$$

- all possible results at once!
- but wait again! How do we read the results?
- measurements only with projections $\rightarrow$ destroying the state
- copying states first and then perform measurements? No-Cloning Theorem
- what can we do?

Universiteit Utrecht

Deutsch's Problem - I

- take function $f : \{0,1\} \to \{0,1\}$ - question: is f balanced $(f(0) \neq f(1))$ or constant $(f(0) = f(1))$?
- classical: calculation of input bit 0, then on 1, takes 24h per Bit $\to$ 48h
- QC: prepare a two-bit state and use a unitary transformation

$$U_f|x\rangle|y\rangle = |x\rangle|y \text{ xor } f(x)\rangle$$

- set $|y\rangle = |1\rangle$ and perform Hadamard transformation – initial state

$$\begin{aligned}\frac{1}{\sqrt{2}} U_f \; |x\rangle \left(|0\rangle - |1\rangle\right) &= \frac{1}{\sqrt{2}}|x\rangle \left(|f(x)\rangle - |1 \text{ xor } f(x)\rangle\right) \\ &= \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle \left(|0\rangle - |1\rangle\right)\end{aligned}$$

$\Rightarrow$ isolation in sign factor

Universiteit Utrecht

Deutsch's Problem - II

- is $f : \{0,1\} \to \{0,1\}$ balanced $(f(0) \neq f(1))$ or constant $(f(0) = f(1))$?
- prepare first state as well

$$|\phi\rangle = \frac{1}{2} U_f \Big(|0\rangle + |1\rangle\Big) \Big(|0\rangle - |1\rangle\Big) = \frac{1}{2}\Bigg[(-1)^{f(0)}|0\rangle \Big(|0\rangle - |1\rangle\Big) + (-1)^{f(1)}|1\rangle \Big(|0\rangle - |1\rangle\Big)\Bigg]$$

$$|\phi\rangle = \begin{cases} \frac{\pm 1}{2}\Big[|0\rangle + |1\rangle\Big] \Big(|0\rangle - |1\rangle\Big) \\ \frac{\pm 1}{2}\Big[|0\rangle - |1\rangle\Big] \Big(|0\rangle - |1\rangle\Big) \end{cases}$$

- measurement or projection of first bit in basis $|\pm\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle \pm |1\rangle\Big]$
- Success! Same result as classical computer in half of time!

Other Quantum Algorithms

- Shor's algorithm
  - prime number factorization in polynomial time
  - probabilistic nature: gives right answer with certain probability
  - has been successfully performed on a 7-qubit system (2001)

- Gover-Iteration: search in unsorted list
  - classical: $\mathcal{O}(n)$
  - Gover: $\mathcal{O}(\sqrt{n})$
  - "rotates" solution in list in hyperplane, s.t. probability amplitude increases
  - probabilistic nature: gives right answer with certain probability

Table of Contents

Turing Machines

- shown to be equivalent by D. Deutsch (1985)
- finite "processor" state

  $$|n\rangle = |n_0 n_1 n_2 \ldots n_{\max}\rangle$$

- infinite "memory" state

  $$|m\rangle = |\ldots m_{-1} m_0 m_1 m_2 \ldots.\rangle$$

- m's and n's are two-state systems
- head label $|x\rangle$ with $x \in \mathbf{Z}$, marking current position
- full state $|\psi\rangle = |x; n; m\rangle$
- unitary transition matrix U, determining whether x- - or x++, depending on current n_x and m_x
- QC cannot halt, condition: a special state has been marked

Semi-Thue Systems - I

- recap: Given alphabet Σ, words $w, v \in \Sigma^*$ and substitution rules $S : \Sigma^* \times \Sigma^*$, is there a way that v is derivable from w in S?
- First direction: quantum computing $\Rightarrow$ semi-Thue
- recode every alphabet $\Sigma = \{a, b, c, d, ...\}$ to $\Sigma_2 = \{0, 1\}$

$$a \rightarrow 01$$

$$b \rightarrow 0011, \qquad \text{and so forth}$$

- prepare initial state from initial word
- How to implement substitution?
- easy, in principle
  - take input qubits $|i_1 ... i_n\rangle$ and output qubits $|o_1 ... o_m\rangle$
  - choose rule
  - input fits to rule?
  - if yes, flip certain bits in output

$$CNOT_{i_1 \ldots i_n, o_1 \ldots o_m} = \mathbf{1} + \left(\bigotimes_{q \in \text{bits to be flipped}} NOT^{(o_q)} - \mathbf{1} \right) IF_{S_1^1}^{(i_1)} ... IF_{S_1^n}^{(i_n)}$$

  - use permutation to exchange input and output

Semi-Thue Systems - II

- substitution is reversible
- possible to perform? Infinitely many substitution rules!
- possible to use QC more advanced? Maybe applying all rules at once!
- However: How to determine whether it has stopped?

Semi-Thue Systems - III

- quantum computing $\Leftarrow$ semi-Thue
- I thought I would have something, but yesterday I discovered that I don't – suggestions?

Summary

- QC is theoretically possible (experimentally on small scales)
- is in some cases superior to classical computing ("natural" parallelism)
- possible to connect to classical models and to compare them

Backup 1 – Complexity Classes