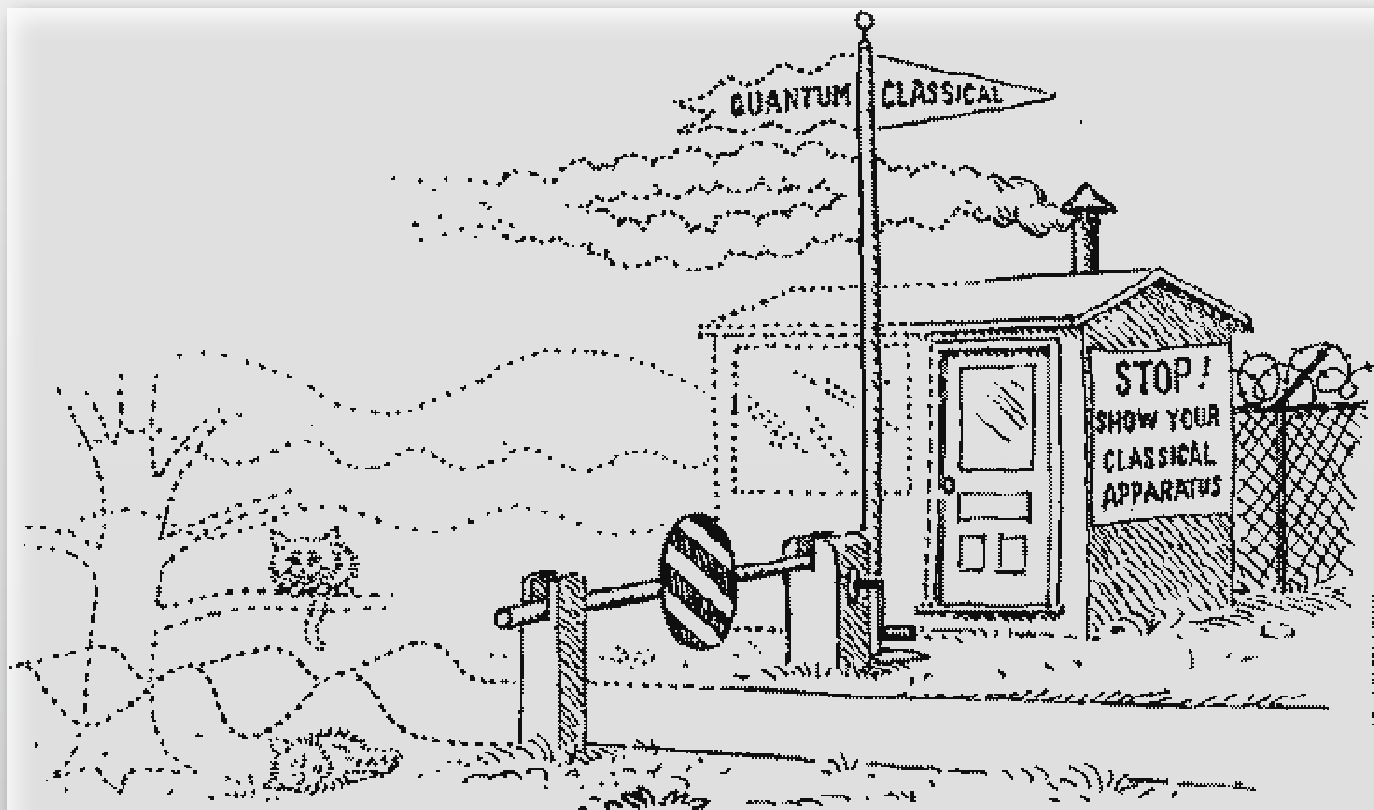
Programming a Quantum Computer

Erik Koch, IFF-FZ Jülich



Information is Physical

R. Landauer

Information is always tied to a physical realization:

relativity: transmission speed < c
statistical mechanics: resetting a Cbit costs > $kT \ln 2$

dynamical RAM: represent bit by charge of capacitor:

b = 1 – capacitor charged

b = 0 – capacitor uncharged

Information is Physical

R. Landauer

Information is always tied to a physical realization:

relativity: transmission speed < c
statistical mechanics: resetting a Cbit costs > kT ln2

dynamical RAM: represent bit by charge of capacitor:

b = 1 – capacitor charged

b = 0 – capacitor uncharged

alternative: represent bit by spin-½:

$$|b\rangle = \alpha|0\rangle + \beta|1\rangle$$

superposition of (classical) basis states

Quantum Information

Qbits cannot be copied
(no-cloning theorem)

disadvantage:
information in Qbit not fully accessible
(uncertainty)

advantage:
eavesdropping on a quantum channel detectable
$\Rightarrow$ quantum cryptography

No-Cloning Theorem

Wooters&Zurek *Nature* **299**, 802 (1982)

It is impossible to copy an *unknown* quantum state

proof by reductio ad absurdum

let U be unitary cloning operator: $U|\Psi\rangle|s\rangle = |\Psi\rangle|\Psi\rangle$ for *any* $|\Psi\rangle$

$$\text{then} \quad \langle s|\langle\Psi|U^\dagger \cdot U|\Phi\rangle|s\rangle \overset{\text{unitary}}{=} \underbrace{\langle s|s\rangle}_{=1}\langle\Psi|\Phi\rangle$$

$$\overset{\text{def}}{=} \quad \langle\Psi|\langle\Psi| \cdot |\Phi\rangle|\Phi\rangle = \langle\Psi|\Phi\rangle^2$$

thus $\langle\Psi|\Phi\rangle^2 \overset{!}{=} \langle\Psi|\Phi\rangle$; only possible if $\langle\Psi|\Phi\rangle = 0$ or 1

$\Rightarrow$ only orthogonal basis states can be cloned

(reversible copying of classical bits)

Classical Logics

AND gate

a	b	a b
0	0	0
0	1	0
1	0	0
1	1	1

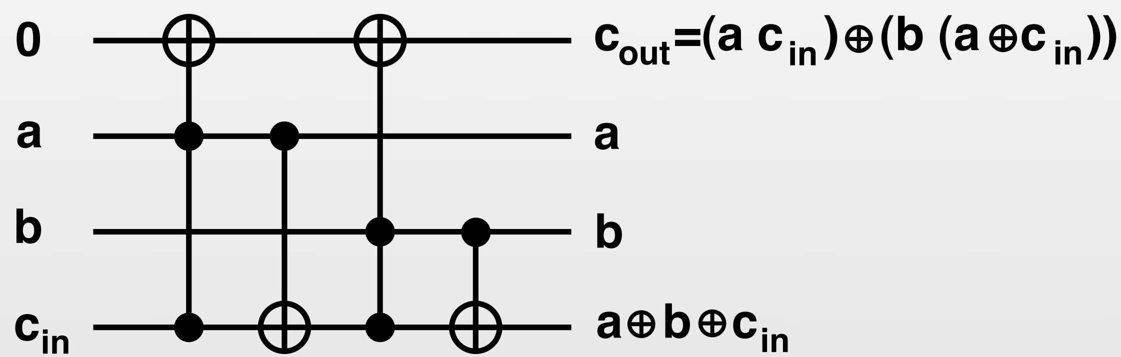
not reversible!

Reversible Logics

Ch. Bennett

e.g. controlled NOT and Toffoli gates

example:
full adder



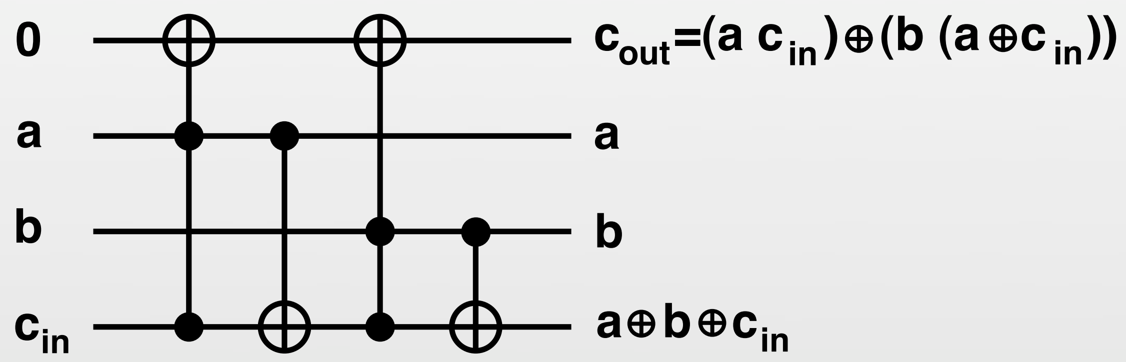
reversible gate defines operation on basis states
naturally extends to unitary operators

Reversible Logics

Ch. Bennett

e.g. controlled NOT and Toffoli gates

example:
full adder



reversible gate defines operation on basis states naturally extends to unitary operators

quantum gates without classical analog:

e.g. Hadamard gate (to create superpositions)

$$
\begin{aligned}
U_H|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\
U_H|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)
\end{aligned}
$$

Quantum Parallelism

$$U_H|0\rangle\, U_H|0\rangle\ \ldots\ U_H|0\rangle = U_H^{\otimes n}\,|00\ldots0\rangle = \sum_{\mathbf{x}} |\mathbf{x}\rangle$$

superposition of all 2^n basis states

implement classical function *f(x)* as unitary operator:

$$U_f\,|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|f(\mathbf{x}) \oplus \mathbf{y}\rangle$$

then $\quad U_f\, U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_{\mathbf{x}} |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_{\mathbf{x}} \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}_{\text{x and } f(\text{x}) \text{ entangled!}}$

simultaneous evaluation of 2^n function values

problem: only one (random!) *f(x)* can be measured

Quantum Parallelism

$$U_H|0\rangle\, U_H|0\rangle\, \ldots\, U_H|0\rangle = U_H^{\otimes n}\,|00\ldots0\rangle = \sum_{\mathrm{x}} |\mathbf{x}\rangle$$

superposition of all 2^n basis states

implement classical function *f(x)* as unitary operator:

$$U_f\,|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|f(\mathbf{x}) \oplus \mathbf{y}\rangle$$

then $\quad U_f\, U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_{\mathrm{x}} |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_{\mathrm{x}} \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}_{\text{x and } f(\text{x}) \text{ entangled!}}$

simultaneous evaluation of 2^n function values

problem: only one (random!) *f(x)* can be measured

The Art of Quantum Computing:

use interference to extract relevant information

Dimension of Hilbert space

n Qbit – Hilbert space: C^{2^n}

n	2^n		
10	1 024	1 kb	(kilo)
20	1 048 576	1 Mb	(Mega)
30	1073 741 824	1 Gb	(Giga)
40	1 099 511 627 776	1 Tb	(Tera)
50	1 125 899 906 842 624	1 Pb	(Peta)
60	1 152 921 504 606 846 976	1 Eb	(Exa)
70	1 180 591 620 717 411 303 424	1 Zb	(Zetta)
80	1 208 925 819 614 629 174 706 176	1 Yb	(Yotta)

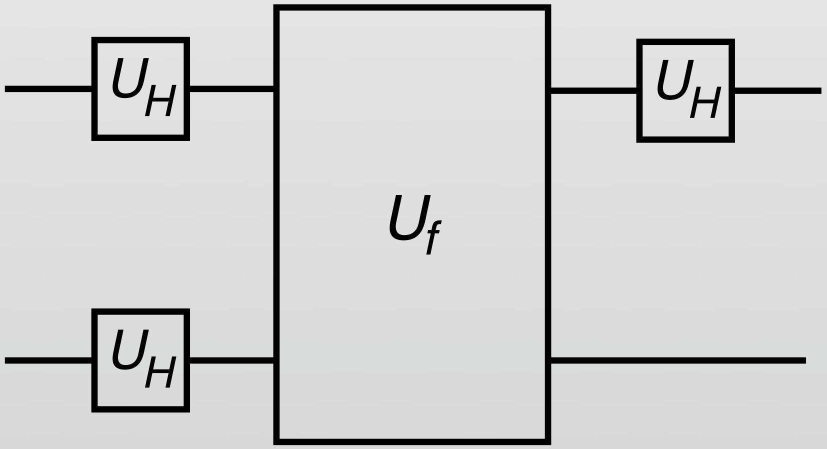
Deutsch algorithm

Proc. Roy. Soc. London, Ser. A ***400***, 97 (1985)

given $f : \{0,1\} \to \{0,1\}$ $\qquad$ $f(0)=f(1)$ or not?

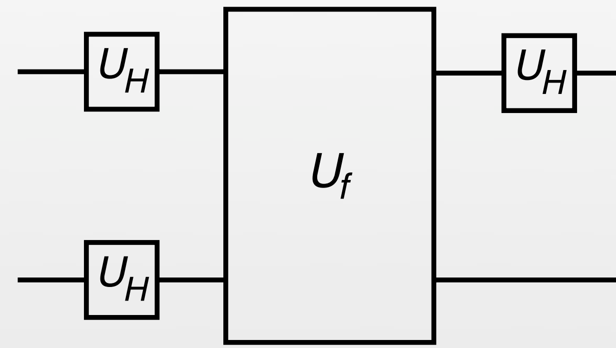
classical computing: two calls to f (gives full information on f)

quantum computing: single call to f sufficient!



Deutsch algorithm

Proc. Roy. Soc. London, Ser. A ***400***, 97 (1985)



prepare superposition

$$
\begin{aligned}
U_H|0\rangle\, U_H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \tfrac{1}{2}\Big(|0\rangle|0\rangle \quad - |0\rangle|1\rangle \quad + |1\rangle|0\rangle \quad - |1\rangle|1\rangle \Big)
\end{aligned}
$$

evaluate f (using $0 \oplus a = a$ and $1 \oplus a = \overline{a}$)

$$
\begin{aligned}
&\xrightarrow{U_f} \tfrac{1}{2}\Big(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle \Big) \\
&= \tfrac{1}{2}\Big(|0\rangle|f(0)\rangle \quad - |0\rangle|\overline{f(0)}\rangle \quad + |1\rangle|f(1)\rangle \quad - |1\rangle|\overline{f(1)}\rangle \Big) \\
&= \tfrac{1}{2}\Big(|0\rangle\, [|f(0)\rangle - |\overline{f(0)}\rangle] \quad + |1\rangle\, [|f(1)\rangle - |\overline{f(1)}\rangle] \Big)
\end{aligned}
$$

interference step

$$
= \begin{cases}
\tfrac{1}{2}(|0\rangle + |1\rangle)\, [|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \tfrac{1}{\sqrt{2}}|0\rangle\, [|f(0)\rangle - |\overline{f(0)}\rangle] & \text{if } = \\
\tfrac{1}{2}(|0\rangle - |1\rangle)\, [|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \tfrac{1}{\sqrt{2}}|1\rangle\, [|f(0)\rangle - |\overline{f(0)}\rangle] & \text{if } \neq
\end{cases}
$$

Quantum Computing

notion of computability unchanged
quantum systems can be simulated on a classical computer

computational complexity reduced:
quantum computers can be much faster than classical ones

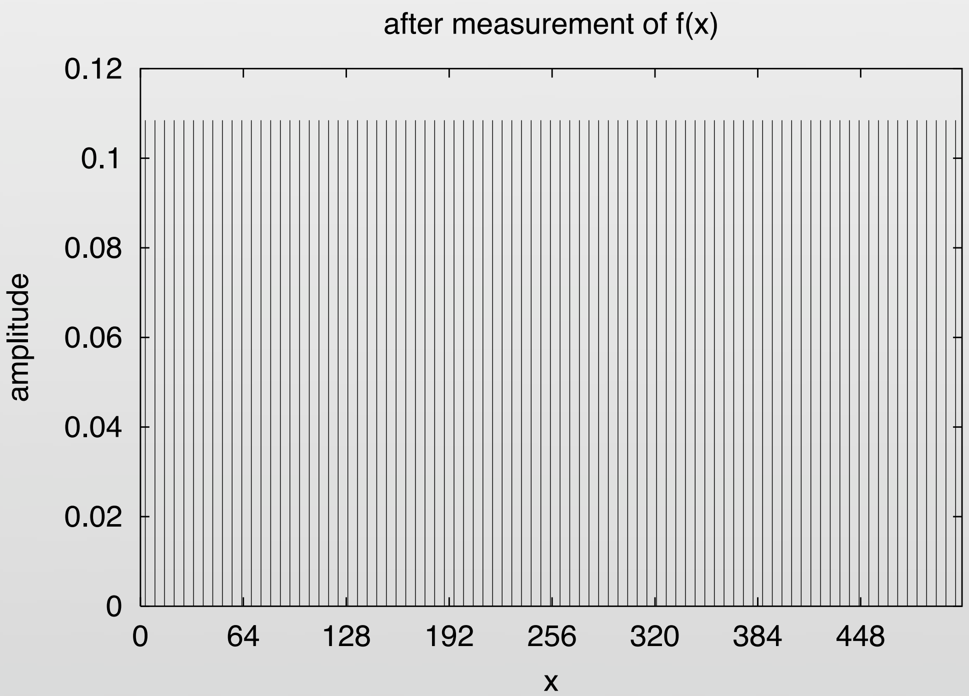
problem	classical algorithm	quantum algorithm
factoring N	number field sieve $O(e^{(\log N)^{1/3} (\log \log N)^{2/3}})$	Shor algorithm: $O(\log^3 N)$
unstructured search in N items	brute force: $O(N)$	Grover algorithm: $O(\sqrt{N})$

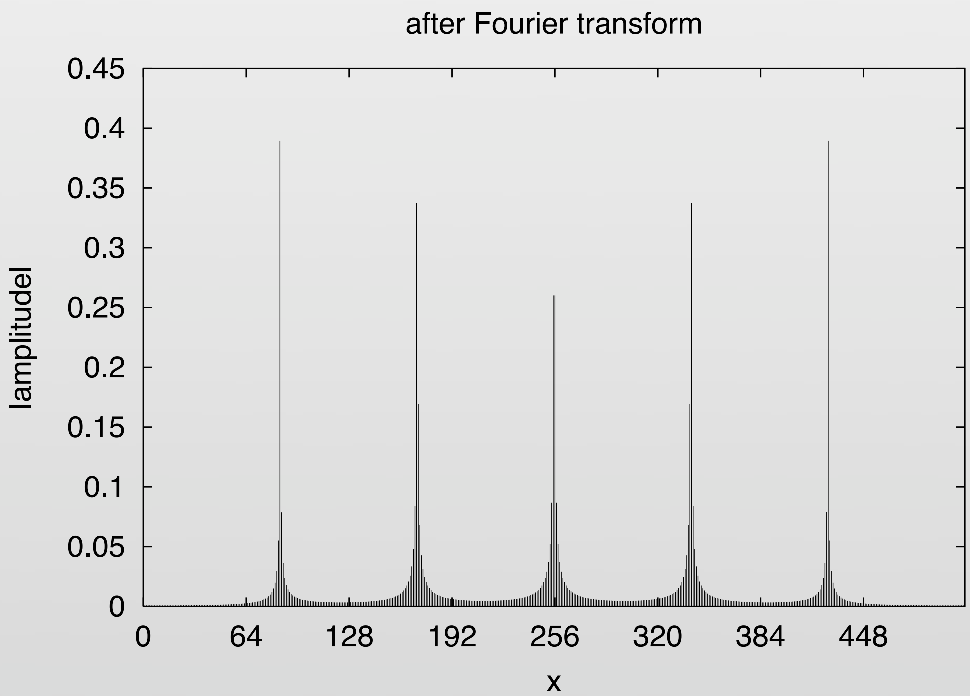
Shor algorithm

factor M; pick a=11 < M with gcd(M,a)=1

calculate $f(x)=a^x \bmod M$; find period $f(x+r)=f(x)$

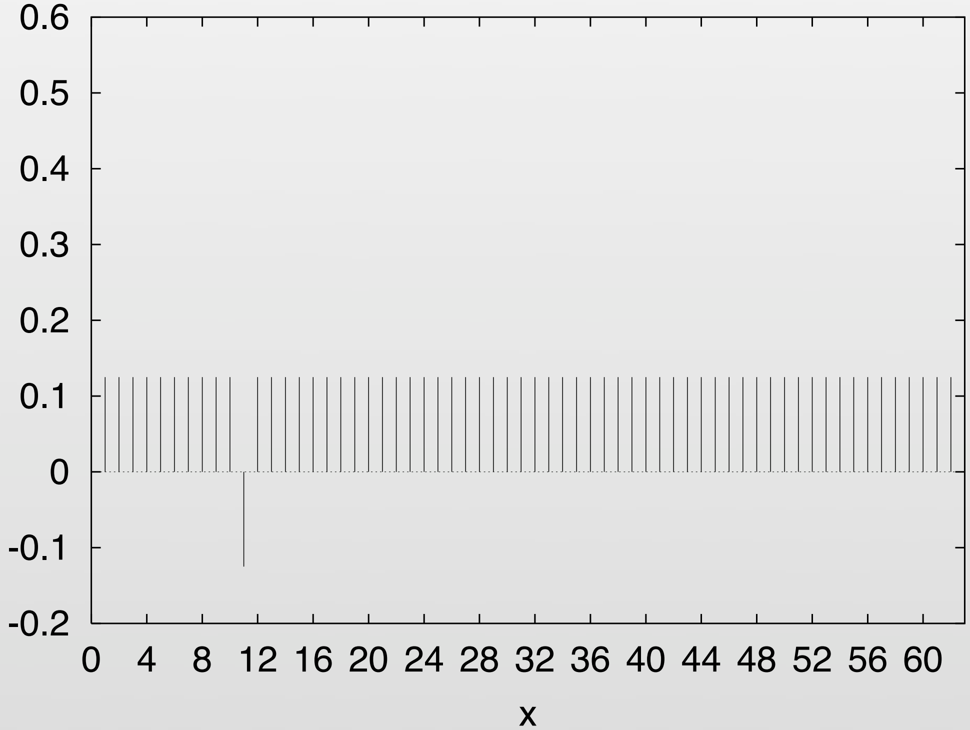
then $\gcd(a^{r/2}\pm 1, M)$ gives divisor of M

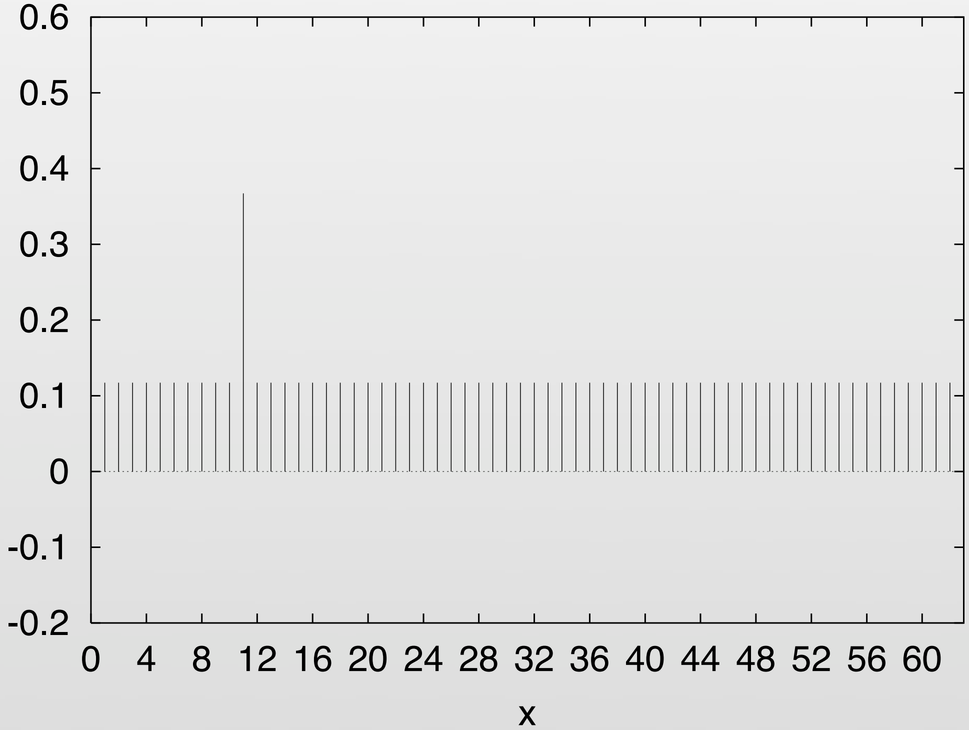




Grover algorithm

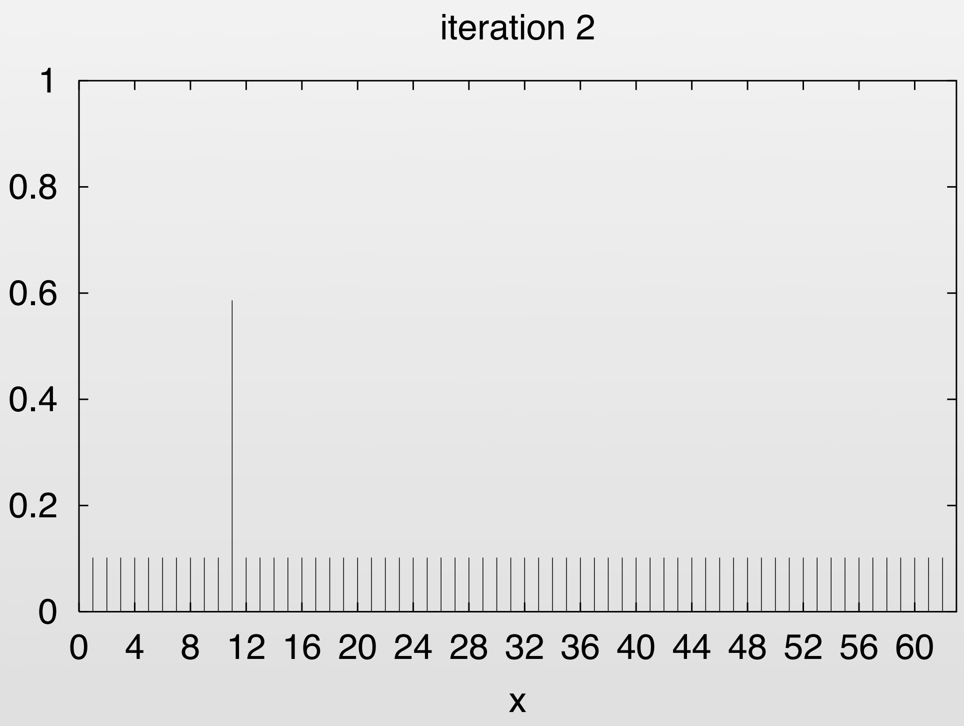
amplitude apmplification:
make amplitude of traget state negative
invert all amplitudes about average

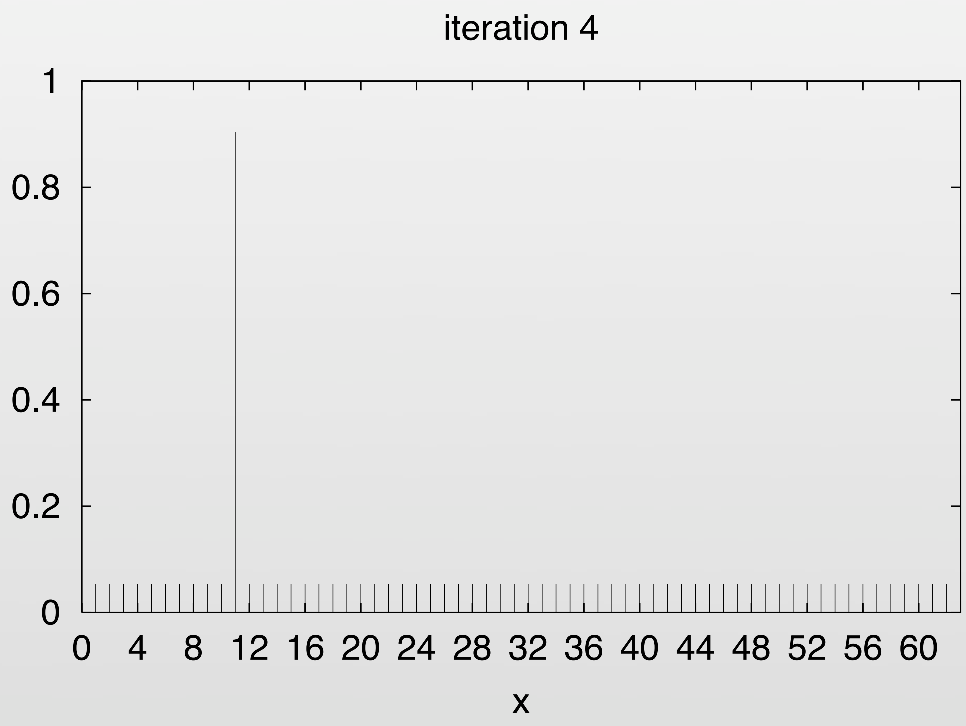




Grover algorithm

higher iterations





Qbits – analog or digital?

$$|b\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in \mathbb{C}$$ — Qbit analog!?

but: α, β not accessible — measurement returns only 0 or 1

Spaghetti Computer

A.K. Dewdney, Scientific American ***250***, 19-26 (June 1984)

Spaghetti Sort:

given: list of numbers

cut uncooked (!) spaghetti to length matching numbers

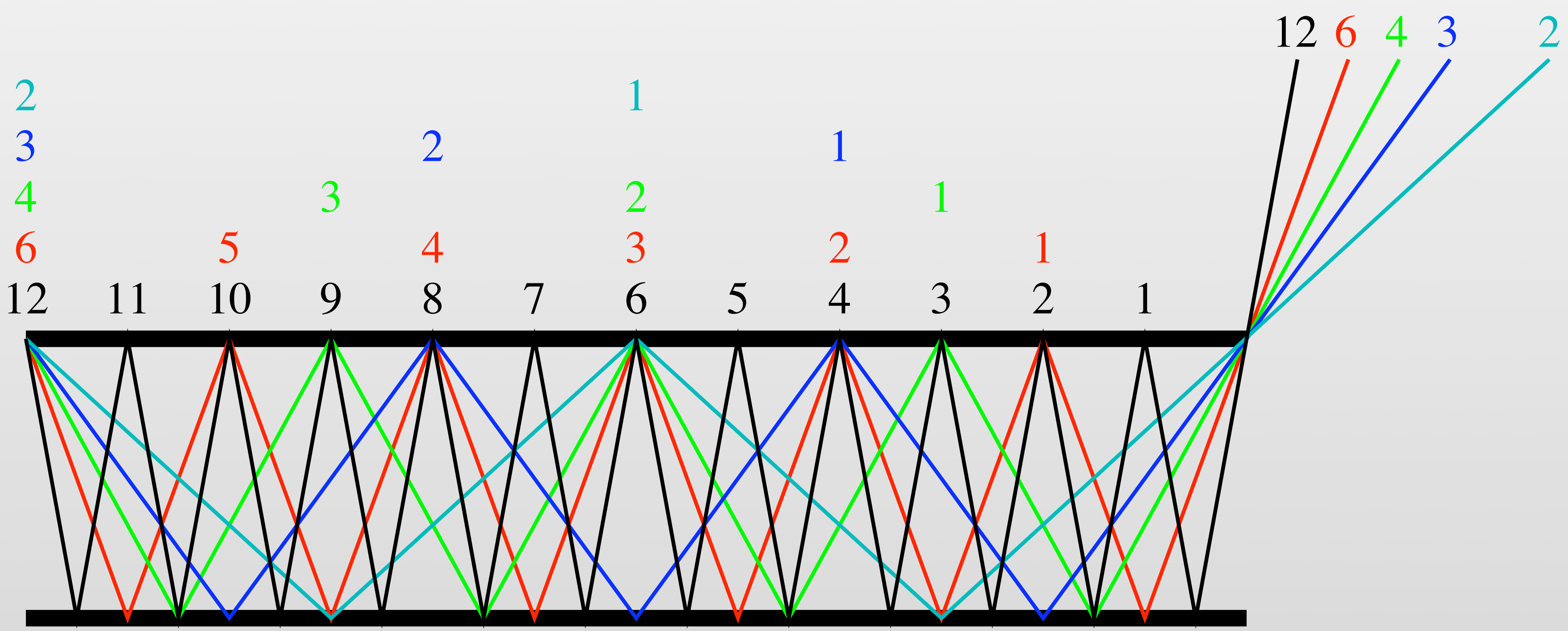
hold bundle of spaghetti loosely in hand and tap vertically on table

tallest spaghetti – the one sticking up furthest – represents the largest number;
once removed the next longest piece is obvious ...

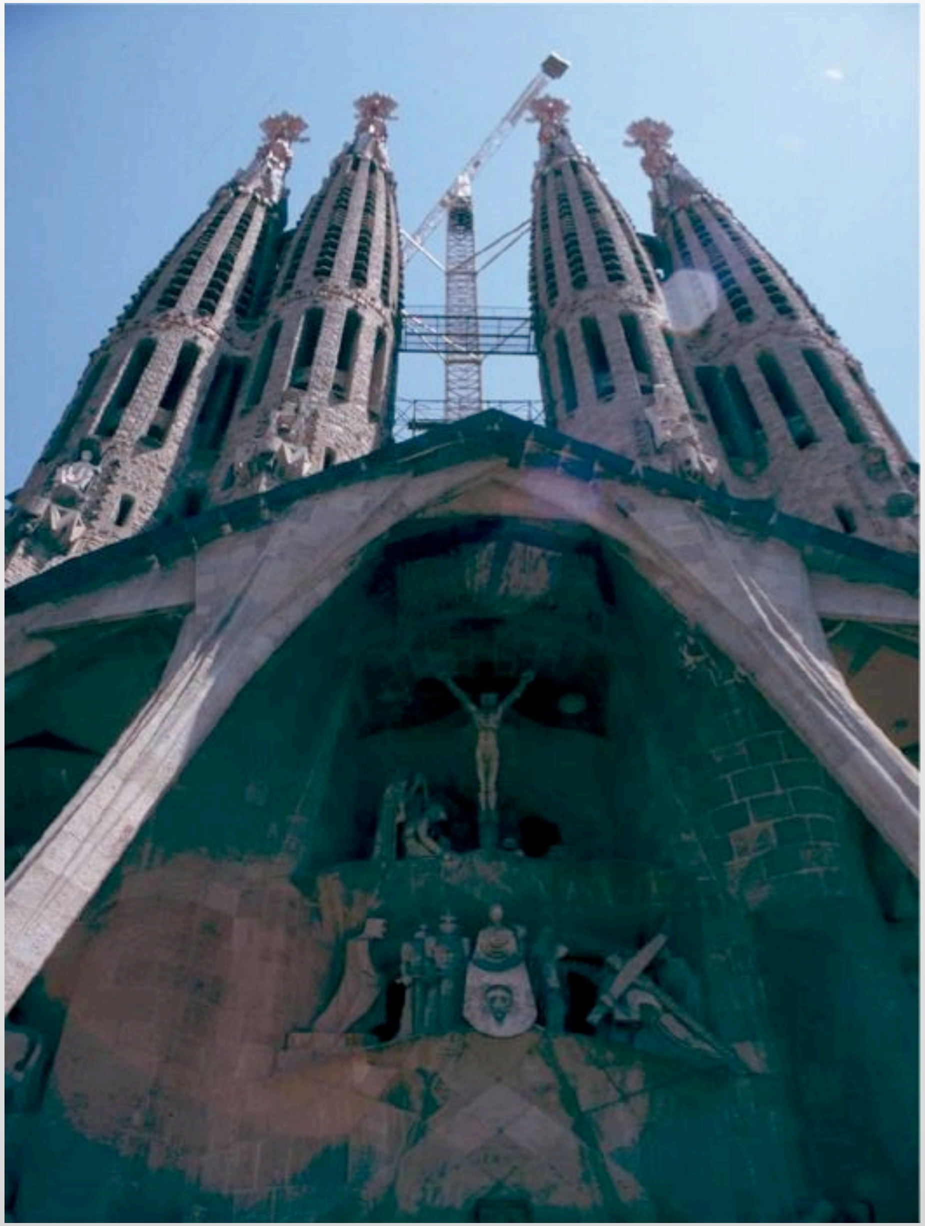
O(N) – faster than QuickSort O(N log N)

Factoring optics?

factoring N=12; n=2, 3, 4, 6



Gaudí: La Sagrada Familia



Qbits – analog or digital?

$|b\rangle = \alpha|0\rangle + \beta|1\rangle$ $\alpha, \beta \in \mathbb{C}$ — Qbit analog!?

but: α, β not accessible — measurement returns only 0 or 1

error correction possible — digital!

idea: bit errors can be described by Pauli matrices:
(discrete errors)

$\mathbf{I}$	—	no error	σ_x	—	bit-flip
σ_z	—	phase-flip	σ_y	—	bit-&phase-flip

project on one of the four error states and correct

DiVincenzo Criteria

Fortschr. Physik ***48***, 771-783 (2000)

- scalable physical system of well characterized Qbits
- ability to initialize Qbits
- decoherence times $\gg$ gate-operation time
- universal set of quantum gates
- ability to measure Qbits
- ability to transfer Qbits

QI Roadmap

http://qist.lanl.gov

QIST Quantum Computing Roadmap

Table 4.0-1
The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria: Quantum Computation #1	#2	#3	#4	#5	QC Networkability #6	#7
NMR	🔴	🟡	🟡	🟢	🟡	🔴	🔴
Trapped Ion	🟡	🟢	🟡	🟢	🟢	🟡	🟡
Neutral Atom	🟡	🟢	🟡	🟡	🟡	🟡	🟡
Cavity QED	🟡	🟢	🟡	🟡	🟢	🟡	🟡
Optical	🟡	🟡	🟢	🟡	🟡	🟡	🟢
Solid State	🟡	🟡	🟡	🟡	🟡	🔴	🔴
Superconducting	🟡	🟢	🟡	🟡	🟡	🔴	🔴
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.						

Legend: 🟢 = a potentially viable approach has achieved sufficient proof of principle

🟡 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

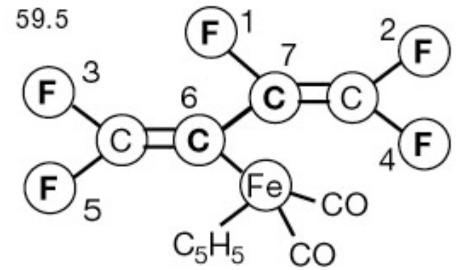
🔴 = no viable approach is known

Quantum Hardware: NMR

NMR in liquids

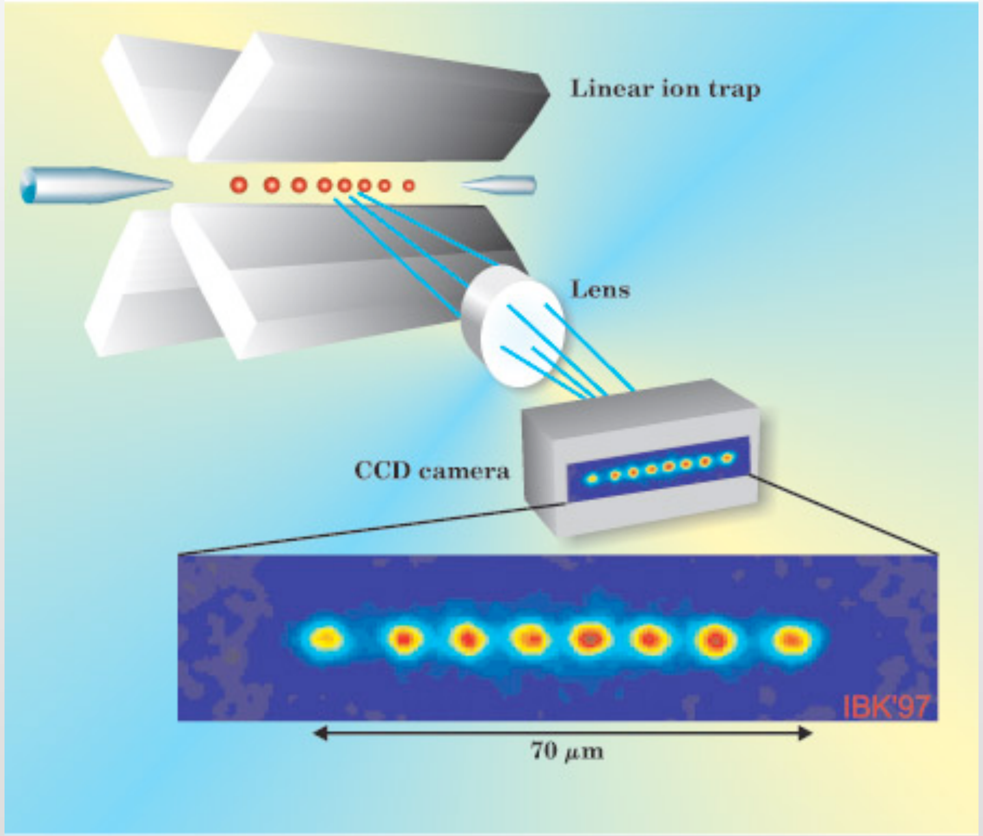
- nuclear spin in molecules
- 7 Qbits realized
- problem: does not scale
- Nature ***414***, 883 (2001): Shor-factorization 15=3x5

i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	−22052.0	5.0	1.3	−221.0	37.7	6.6	−114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	−3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	−13.5	41.6	12.9		
4	−4918.7	10.0	1.7	54.1	−5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	−4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						



Quantum Hardware: Ion Trap

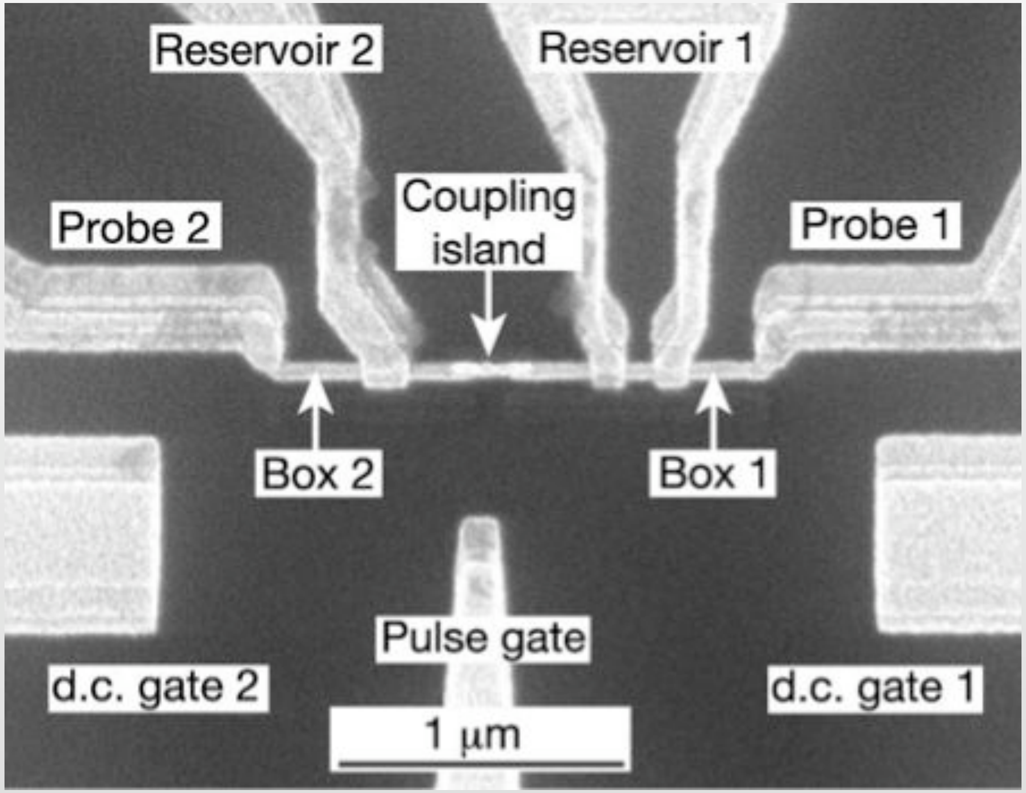
- 1 Qbit operation via laser
- 2 Qbit operations
  via phonons
- 2 Qbits realized
- Nature ***422***, 408 (2003)
  Physics Today March 2004



Quantum Hardware: Josephson

Josephson contacts (solid state)

- phase or occupation
- 2 Qbit operations within reach
- Nature ***421***, 823 (2003)



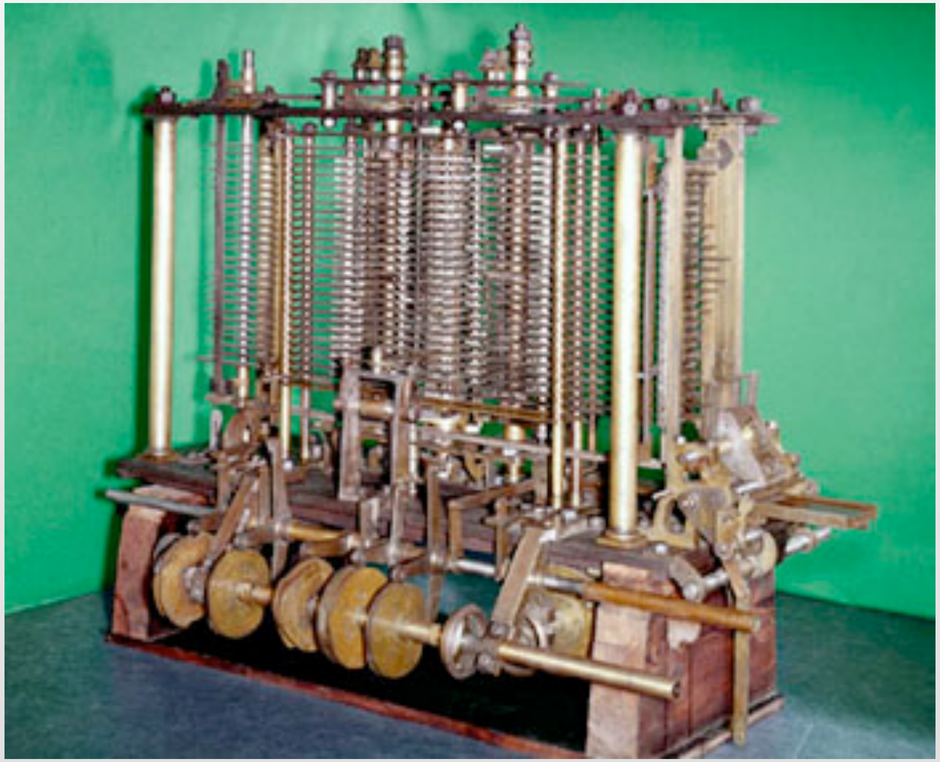
Landauer's disclaimer

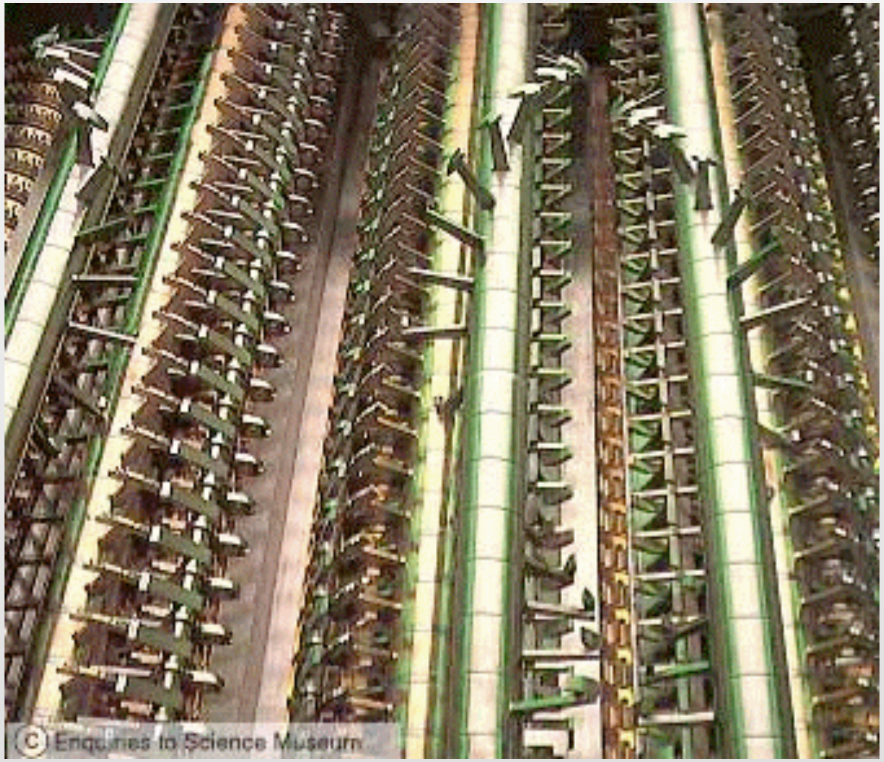
Nature ***400***, 720 (1999)

This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work.

Inappropriate Hardware:

mechanical computers





Charles Babbage: Analytical Engine (1834)

Quantum Cryptography

MagiQ: www.magiqtech.com
id quantique: www.idquantique.com

Figure 3: id Quantique's system exchanged keys over 67 km of standard optical fiber.

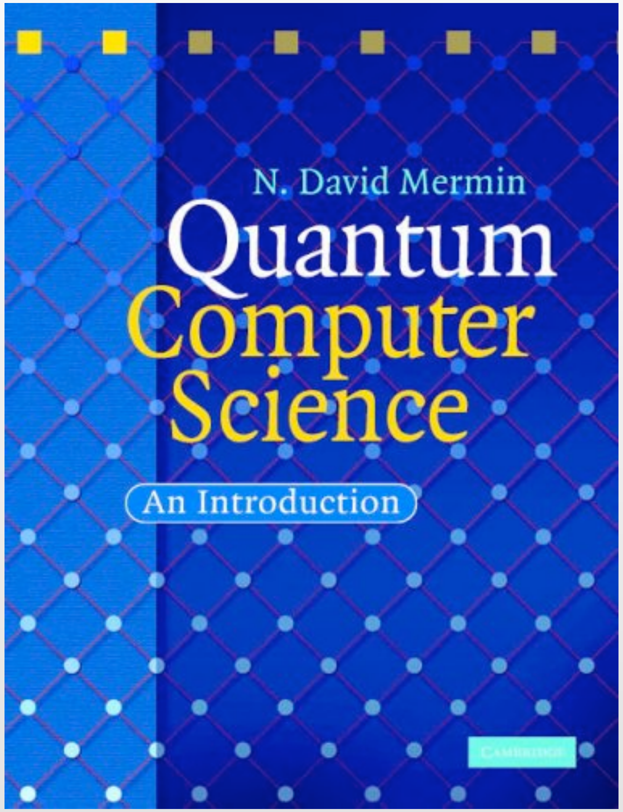
What makes Quantum Computers efficient?

- superposition
  (quantum parallelism; exp large Hilbert space)
- entanglement of input and result
- interference, to obtain measurable result
  the art of quantum computing

Confused?

Möglicherweise ist es, nebenbei gesagt, für die Kopenhagener Interpretation der Quantenmechanik wichtig, dass ihre Sprache in einem gewissen Grad unbestimmt ist, und ich bezweifle, dass sie durch den Versuch, diese Unbestimmtheit zu vermeiden, klarer werden kann. (W. Heisenberg)

Literatur

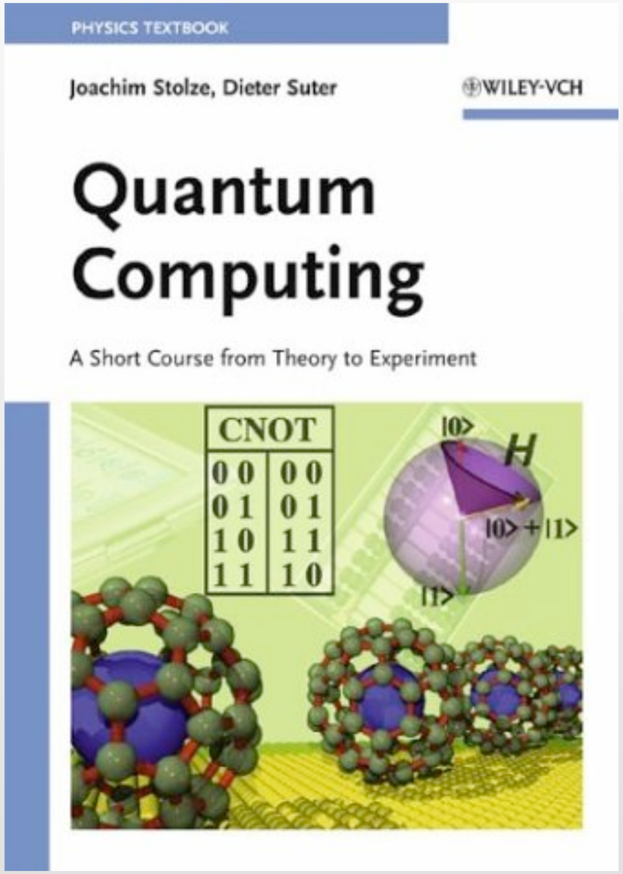


N.D. Mermin
Quantum Computer Science
Cambridge Univ. Press, 2007
220 pages

excellent textbook; focus on QM and algorithms

http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html

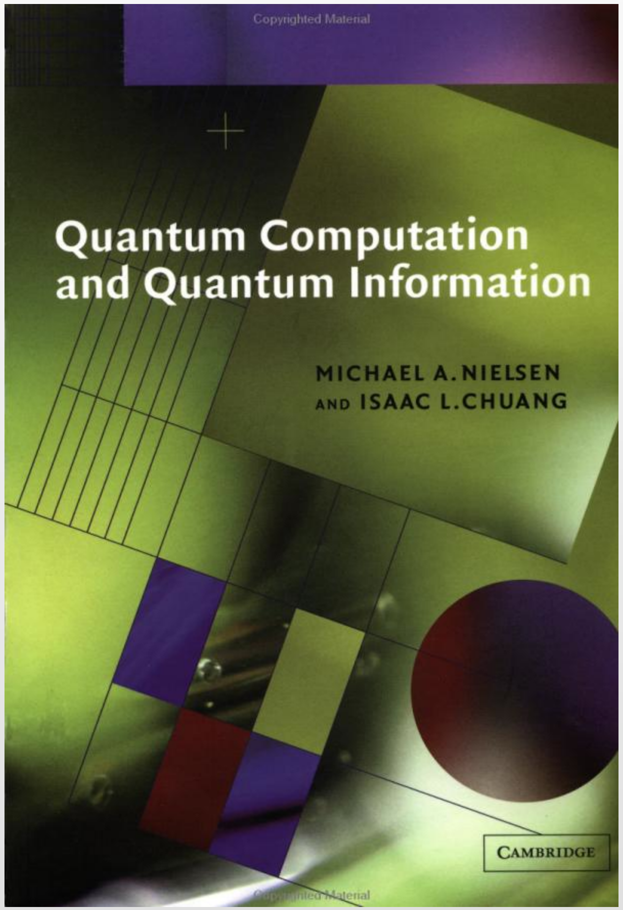
Literatur



J. Stolze, D. Suter
Quantum Computing
Wiley-VCH, 2008
265 pages

broader view, shorter on algorithms

Literatur



M.A. Nielsen, I.L. Chuang
Quantum Computation
and Quantum Information
Cambridge Univ. Press, 2000
676 pages

the reference book

slides at

http://iffwww.iff.kfa-juelich.de/~ekoch/QC09/QCintro.pdf