Quantum Computing
Information is Physical

information is always tied to a physical realization

**fundamental limits:**
- speed-limit: \( c \) (relativity)
- resetting a bit costs \( > kT \ln 2 \) (statistical mechanics)

- dynamical RAM represents bit by charge on capacitor:
  - \( b=1 \) – capacitor charged
  - \( b=0 \) – capacitor uncharged

**alternative:** represent bit by spin-\( \frac{1}{2} \)

- superposition of (classical) bits

\[
| b \rangle = \alpha | 0 \rangle + \beta | 1 \rangle
\]
Quantum Information

Qbits cannot be copied
(no-cloning theorem)

disadvantage:
information in Qbit not fully accessible
(uncertainty!)

advantage:
eavesdropping on a quantum channel detectable
⇒ quantum cryptography
**No-Cloning Theorem**


It is impossible to copy an unknown quantum state proof by *reductio ad absurdum*.

A single quantum cannot be cloned

W. K. Wootters

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130-55, California Institute of Technology, Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, then it is impossible for any deterministic measurement that atoms will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But it is possible that Wootters might use this option to demonstrate that atoms cannot simultaneously emit two photons of identical polarization. But then the photons would have to be in a state of equal polarization, which is not possible. The photons would then have to be in a state of equal polarization, which is not possible. The photons would then have to be in a state of equal polarization, which is not possible. The photons would then have to be in a state of equal polarization, which is not possible.

**LETTERS TO NATURE**

**Nov 299, 802 (1982)**

Milburn (unpublished work) has shown that the process of stimulated emission does not lead to quantum amplification, and that any attempt to amplify such a process would lead to the amplification of the original.

It is possible that a more sophisticated amplification process could be used to increase the size of the original.

We stress the question of replicating individual photons, which is related to the quantum limits on the size of amplifiers. Moreover, an experiment designed to establish the extent of which to which single photons can be counted has shown that the full set of stimulated emission is under way by (A. Gourari, personal communication; and see ref. 1). The quantum mechanical prediction is quite definite; for each perfect observation, there is a chance to be observed by a randomly polarized, spontaneously emitted, photon.

We thank Alonzo Angel, Alexei Andronov, Ted Jacobson, Dino Manes, Marian Scully, Pierre Meystre, Don Furrer, and Robert Loudon for discussions and encouragement. This work was supported in part by the NSF (P78-26492 and AST-79-23012-A1). W.H.Z. acknowledges a Richard Chase Tomlin Fellowship.
quantum parallelism

$$U_H|0\rangle U_H|0\rangle \ldots U_H|0\rangle = U_H^\otimes n|00\ldots 0\rangle = \sum_x |x\rangle$$

superposition of all $2^n$ basis states

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

$$U_f|x\rangle |y\rangle := |x\rangle |y \oplus f(x)\rangle$$

then

$$U_f U_H^\otimes n|0\rangle |0\rangle = U_f \sum_x |x\rangle |0\rangle = \sum_x |x\rangle |f(x)\rangle$$

simultaneous evaluation of $2n$ function values

problem: only one (random!) $f(x)$ can be measured
classical logics

Boolean operations

<table>
<thead>
<tr>
<th>NOT gate</th>
<th>AND gate</th>
<th>XOR gate</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>(\neg a)</td>
<td>a</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- NOT gate: not reversible!
- AND gate
- XOR gate: reversible: cNOT
reversible logics

e.g. controled NOT and Toffoli gates

example: full adder

c_{out} = (a_{cin}) \oplus (b (a \oplus c_{in}))

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

quantum gates without classical analogon:
e.g. Hadamard gate (creates superpositions)

\[ U_H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
\[ U_H |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \]
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

<table>
<thead>
<tr>
<th>problem</th>
<th>classical algorithm</th>
<th>quantum algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>factoring $N$</td>
<td>number field sieve $O(e^{(\log N)^{\frac{1}{2}} (\log \log N)^{\frac{1}{2}}})$</td>
<td>Shor algorithm: $O(\log^3 N)$</td>
</tr>
<tr>
<td>unstructured search in $N$ items</td>
<td>brute force: $O(N)$</td>
<td>Grover algorithm: $O(\sqrt{N})$</td>
</tr>
</tbody>
</table>
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)
how to build a computer from relais

Charles Petzold: **Code**  
The Hidden Language of Computer Hardware and Software  
Microsoft Press, 2000

Still the lightbulb doesn't light because the bottom switch is still open and that relay isn't triggered. We can try opening the top switch and closing the bottom switch:

The lightbulb is still not lit. The current can't reach the lightbulb because the first relay isn't triggered. The only way to get the bulb to light up is to close both switches:

Thursday, February 6, 2014
Quantum Cryptography

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