IQI 04, Seminar 1

Produced with pdflatex and xfig

- Seminar overview.
- Classical information units and processing.
- Information science: The big picture.
- Qubit state space.
- Simple qubit gates.
- Black box problems.

QUANTUM INFORMATION PROCESSING, SCIENCE OF - The theoretical, experimental and technological areas covering the use of quantum mechanics for communication and computation. Kluwer Enc. Math. III

E. "Manny" Knill: knill@boulder.nist.gov

Seminar overview

Goal: To learn the basic concepts and tools of quantum information, appreciate its power and limitations, and understand the issues involved in realizing it.
Prerequsites: Linear algebra, polynomials, binary logic, probability.
Structure: 15 seminars, each consisting of a 50min lecture, followed by discussions and/or problem solving.
Grading: Based on participation–see hand-out. Required meeting with me in the second half of the semester.
Assignments: Problems to be handed out. Errors in solutions handed in have no effect on grade.
Reading: References provided in handout, limited number of hard copies of LAScience issue.
Office hours: CU: Wednesdays after class, 1pm-3pm, S315 or by appointment. NIST: Thursdays after class, 2:15pm-3:15pm, Bldg 1, Rm 4049, or drop in any time I am there.
Sign-up: Please provide your email, if possible. Let me know if it is difficult for you to use PDF and PS attachments.

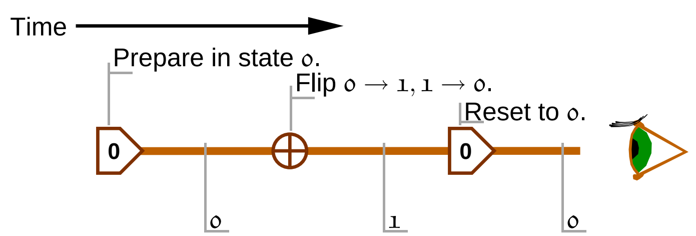
Classical Information Units

- The classical information unit is the *bit*.
  The bit is a *system* with state space $\{0, 1\}$.

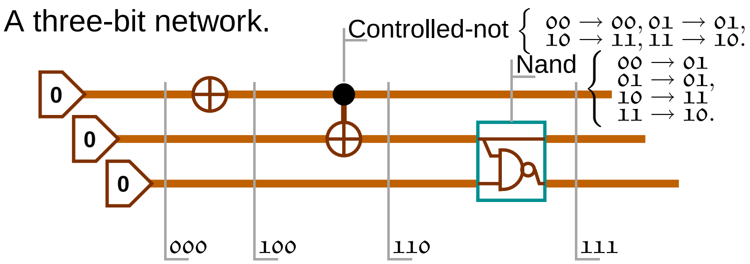
  - Physical examples:
    - Mag. domain on a hard disk, state of mag. moment.
      0 is "right", 1 is "left" magnetization.
    - Location on a piece of paper, ink pattern.
      0 if it looks like 0, 1 if it looks like 1.
- Multiple units' state space: By concatenation of states.
  - Two bits' state space: $\{00, 01, 10, 11\}$.
  - How many states do n bits have? Answer: 2^n.

Classical Gate Networks

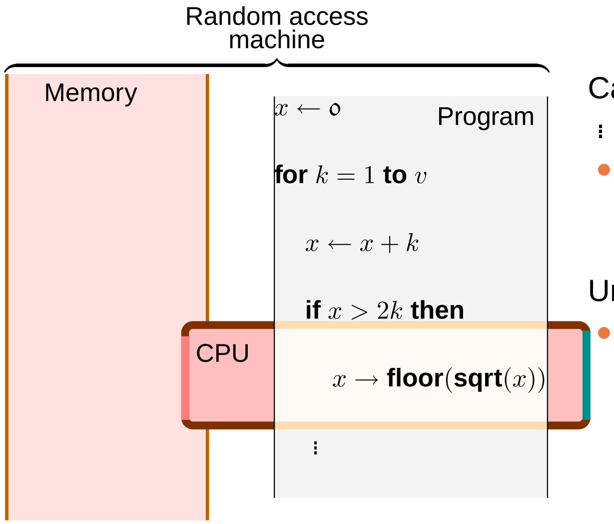
- A one-bit network.



- A three-bit network.



Classical Programming



Capabilities added:

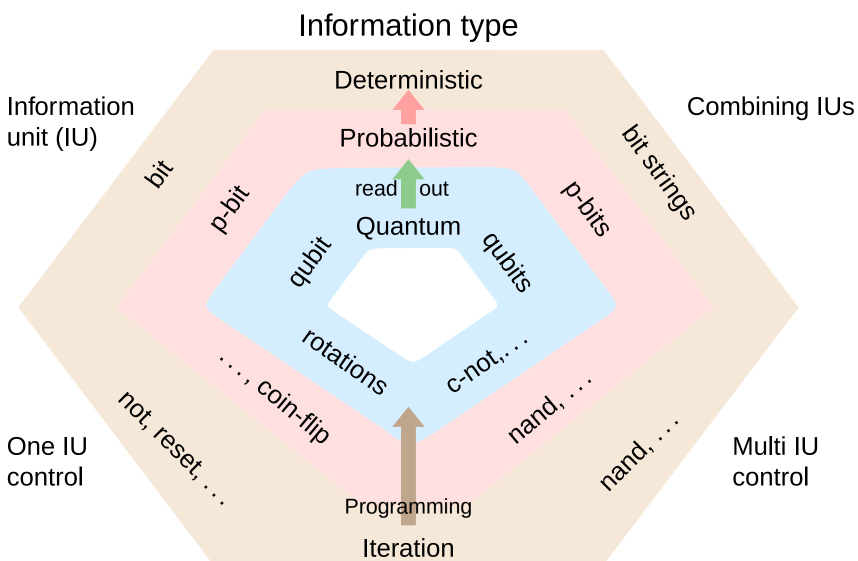
⋮

- Loops, iteration, recursion.

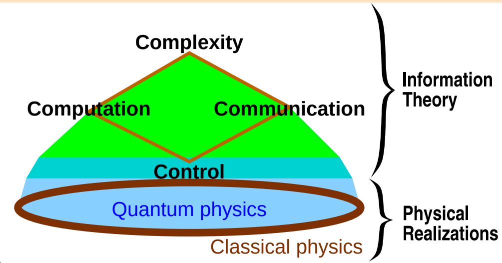
Universality:

- Anything "effective" can be computed by a RAM.

Guide to Information Processing



Quantum Information Science



- Motivation.
  - Quantum cryptography.
  - Quantum factoring.
  - . . . Quantum control,
  - Quantum physics simulation.
  - Unstructured search.
  - complexity theory, . . .
- Practical relevance.

> - QIP is physically realizable in principle:
>
> **Accuracy Threshold Theorem:** *If the error rate is sufficiently low, then it is possible to efficiently process quantum information arbitrarily accurately.*

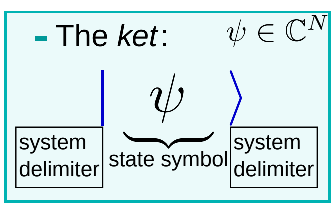
The Quantum Bit

- The *qubit*: A system with (pure) state space all superpositions of two *logical* states $|0\rangle$ and $|1\rangle$:

$$\{\ \alpha|0\rangle + \beta|1\rangle \text{ with } |\alpha|^2 + |\beta|^2 = 1\ \}$$

- Examples: $|0\rangle$, $|1\rangle$,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle,$$
$$\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle.$$



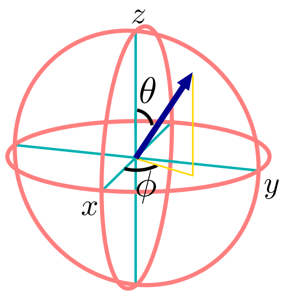
For example: $|\psi\rangle = \frac{3}{5}|0\rangle + \frac{4i}{5}|1\rangle$

State Space Representations

- Vectors.

$$\alpha|0\rangle + \beta|1\rangle \leftrightarrow \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

- Bloch sphere.



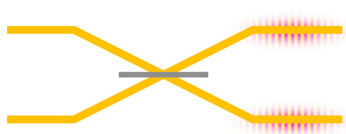
$$\alpha|0\rangle + \beta|1\rangle \cong e^{-i\phi/2}\cos(\theta/2)|0\rangle + e^{i\phi/2}\sin(\theta/2)|1\rangle$$

- Global phase:
  $\alpha|0\rangle + \beta|1\rangle$ and $e^{i\varphi}\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$ are the same state.

Photonic Qubit

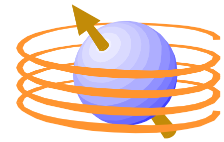
- Photonic qubit: One photon in a superposition of two modes.

  - Photonic qubits are usually "flying" qubits.
  - Making a superposition state:



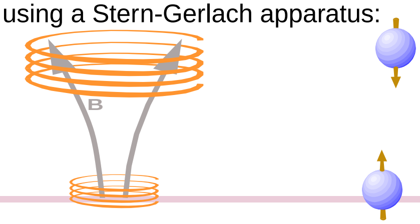
Spin $1/2$ Qubit

- Spin $1/2$ in oriented space: One particle in a superposition of the states "up" ($|\uparrow\rangle$) and "down" ($|\downarrow\rangle$).



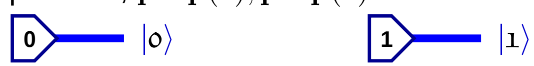
  - Orientation of magnetic moment (average) corresponds to the state in the Bloch sphere.
  - Examples include nuclear spins of ^{13}C and ^{1}H.
    These are observable by nuclear magnetic resonance.

- Distinguish $|\uparrow\rangle$ from $|\downarrow\rangle$ by using a Stern-Gerlach apparatus:



One-Qubit Gates I

- State preparation, $\mathbf{prep}(0), \mathbf{prep}(1)$.

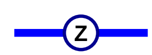


- Bit flip, $\mathbf{not}$.

$$\left.\begin{matrix}\alpha|0\rangle + \beta|1\rangle \\ \begin{pmatrix}\alpha \\ \beta\end{pmatrix}\end{matrix}\right\} \quad \oplus \quad \left\{\begin{matrix}\alpha|1\rangle + \beta|0\rangle \\ \begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \begin{pmatrix}\beta \\ \alpha\end{pmatrix}\end{matrix}\right.$$

- Sign flip, $\mathbf{sgn}$.

$$\left.\begin{matrix}\alpha|0\rangle + \beta|1\rangle \\ \begin{pmatrix}\alpha \\ \beta\end{pmatrix}\end{matrix}\right\} \quad Z \quad \left\{\begin{matrix}\alpha|0\rangle - \beta|1\rangle \\ \begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} = \begin{pmatrix}\alpha \\ -\beta\end{pmatrix}\end{matrix}\right.$$

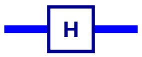


  - So far: Cannot generate proper superpositions.

One-Qubit Gates II

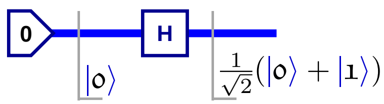
- Hadamard.

$$\left.\begin{matrix}\alpha|0\rangle + \beta|1\rangle \\ \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\end{matrix}\right\}$$



$$\left\{\begin{matrix}\frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle \\ \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\alpha+\beta\\ \alpha-\beta\end{pmatrix}\end{matrix}\right.$$

- Example: Prepare the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.



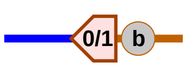
$\mathbf{prep}(0)\ .\ \mathbf{had}$

- With the gates so far, can we prepare $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$?

Read-out

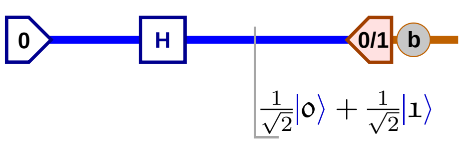
- Read-out reduces a state destructively to classical information.

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



$$\begin{cases} b = 0 & \text{with probability } |\alpha|^2, \\ b = 1 & \text{with probability } |\beta|^2. \end{cases}$$

- Example:



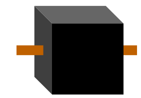
$$\begin{cases} 0 & \text{with probability } \left(\frac{1}{\sqrt{2}}\right)^2 = .5, \\ 1 & \text{with probability } \left(\frac{1}{\sqrt{2}}\right)^2 = .5. \end{cases}$$

$\mathbf{prep}(0)\ .\ \mathbf{had}\ .\ \mathbf{meas}(Z{\mapsto}b)$

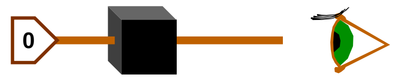
"Black Box" Problems

Classical:

- Given: Unknown one-bit device, a "black box".
  Promise: It either flips the bit or does nothing.
  Problem: Determine which using the device once.



- Solution:

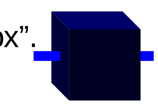


$$\begin{cases} 0: & \text{doesn't flip,} \\ 1: & \text{flips.} \end{cases}$$

"Black Box" Problems

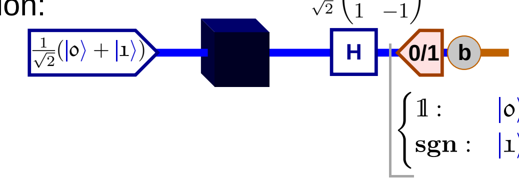
Quantum:

- Given: Unknown one-qubit device, a "black box".
  Promise: It either applies $\mathbf{sgn}$ or does nothing.
  Problem: Determine which using the device once.



- Solution:

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



- Given: Unknown one-qubit device, a "black box".
  Promise: It either applies $\mathbf{not}$, $\mathbf{sgn}$, $\mathbf{sgn.not}$ or does nothing.
  Problem: Determine which using the device once.
  - Is this possible?

Contents

References

[1] S. Wiesner. Conjugate coding. *Sigact News, (original manuscript ∼1969)*, 15:78–88, 1983.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key deistribution and coin tossing. In *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, Los Alamitos, Calif, 1984. IEEE Comp. Soc. Press.

[3] P. Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *J. Stat. Phys.*, 22:563–591, 1980.

[4] Y. I. Manin. *The Computable and the Not Computable*. Sovetskoye Radio, Moscow, 1980. In Russian.

[5] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[6] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35'th Annual Symposium on Foundations of Computer Science*, pages 124–134, Los Alamitos, California, 1994. IEEE Press.

[7] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.

[8] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, New York, 1996. ACM press.

[9] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52:1191–1249, 1997.

[10] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 176–188, New York, New York, 1996. ACM Press.

[11] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279:342–345, 1998.