An introduction to quantum computing

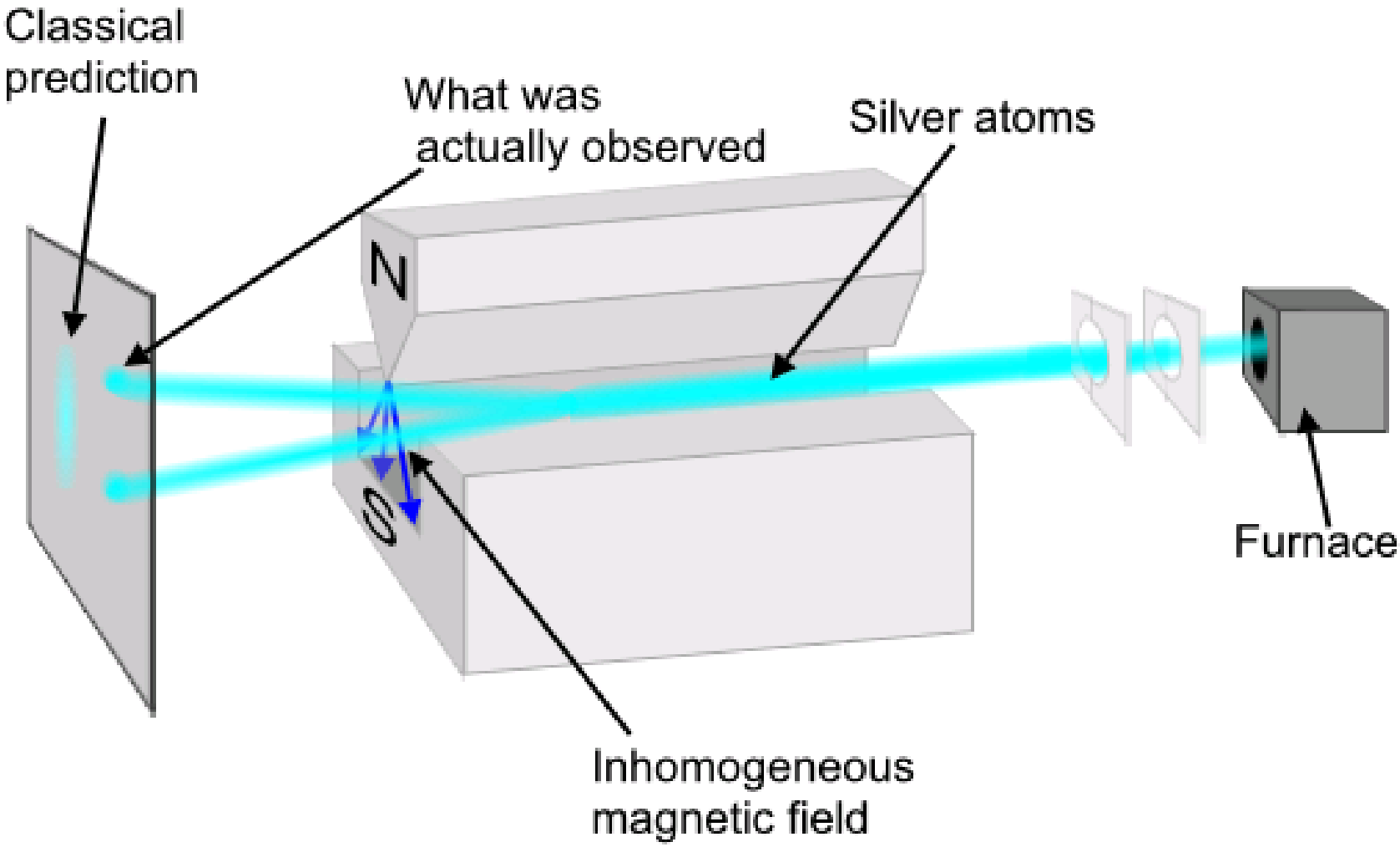
Martin Leslie

Department of Mathematics
University of Arizona

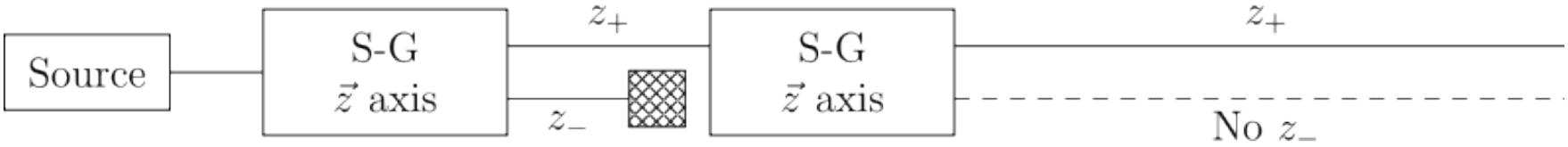
October 17, 2012

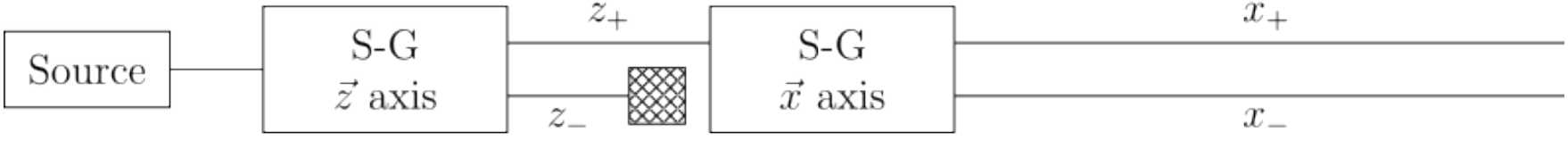
A fake history of quantum mechanics

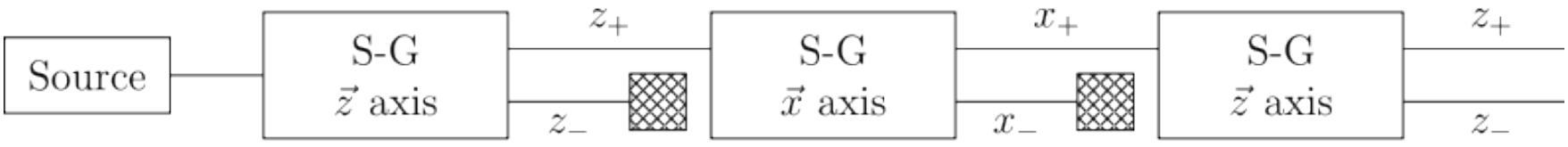
- The Stern-Gerlach experiment with hydrogen atoms was done in 1927.



Results of Stern-Gerlach







Explaining Stern-Gerlach: qubits

- The hydrogen atom is modeled as a *qubit*, a vector in $\mathcal{H}_1 = \{|\psi\rangle = a|0\rangle + b|1\rangle : a, b \in \mathbb{C} \text{ with } |a|^2 + |b|^2 = 1\}$.
- When we send a qubit through the "S-G z axis" we are doing a *measurement* in the $|0\rangle, |1\rangle$ basis:

Measurement	Beam movement	Prob.	New state
0	z_+	$\|a\|^2$	$\|0\rangle$
1	z_-	$\|b\|^2$	$\|1\rangle$

- When we send a qubit through the "S-G x axis" we are doing a measurement with respect to a different basis

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- Since we have

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \text{ and } |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

this explains the results.

Qubits in general

- Let $|0\rangle = [1,0]^T$ and $|1\rangle = [0,1]^T$ be the *computational basis* for $\mathbb{C}^2$.
- A *qubit* is described by a vector in $\mathcal{H}_1 = \{|\psi\rangle = a|0\rangle + b|1\rangle : a, b \in \mathbb{C} \text{ with } |a|^2 + |b|^2 = 1\}$.
- For n qubits, the state is described by an element of $\mathcal{H}_n = \mathcal{H}_1^{\otimes n}$.
- So for $|\psi\rangle \in \mathcal{H}_n$ we can write

$$|\psi\rangle = \sum_{i \in \mathbb{F}_2^n} a_i |i\rangle$$

  where $|i\rangle = |i_1\rangle \otimes \ldots \otimes |i_n\rangle$ and $\sum_i |a_i|^2 = 1$.
- Actually, we're really in projective Hilbert space

$$\mathbb{P}((\mathbb{C}^2)^{\otimes n}) = (\mathbb{C}^2)^{\otimes n} / \sim$$

  where $|\psi\rangle \sim \lambda|\psi\rangle$ (we don't distinguish between states differing only by a *global phase factor*).

Linear algebra in quantum mechanics notation

- Define $A^\dagger = (A^*)^T$ to be the conjugate transpose of A. Matrix A is *Hermitian* if $A^\dagger = A$ and *unitary* if $A^\dagger A = I$.
- If we take (column) vectors $|\psi\rangle, |\varphi\rangle \in \mathcal{H}_n$ then $|\psi\rangle^\dagger$ is a row vector and $|\psi\rangle^\dagger|\varphi\rangle$ is the complex dot product of $|\psi\rangle$ and $|\varphi\rangle$.
- For this reason define $\langle\psi| = |\psi\rangle^\dagger$.
- Then the inner product is $\langle\psi|\varphi\rangle = \langle\psi||\varphi\rangle$.

Quantum mechanics on qubits

- The evolution of the state $|\psi\rangle$ of a closed quantum system from one time to another is given by a unitary matrix U (i.e. $U^\dagger = U^{-1}$) via

$$|\psi\rangle \mapsto U|\psi\rangle.$$

- We will think of such a U that our quantum computer can implement as a *quantum gate*.
- Notice that since U is invertible we must have our quantum gates be reversible.

Quantum measurement

- We can describe a measurement in the computational basis of some or all qubits by three facts:
  - The result of a measurement is always 0's and 1's.
  - The probability of a certain measurement is the sum of the squares of the magnitudes of the coefficients of consistent states.
  - The post-measurement state is the sum of the consistent states normalized by dividing by the square root of the probability of that state.
- For example: assume $|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and we measure the first qubit. With probability $1/4$ we measure 0 and the system is now in state $|00\rangle$. Alternatively, with probability $|-i/2|^2 + |1/\sqrt{2}|^2 = 3/4$ we measure 1 and the system is now in state $-\frac{i}{\sqrt{3}}|10\rangle + \frac{\sqrt{2}}{\sqrt{3}}|11\rangle$.

No-cloning theorem

No arbitrary-qubit-copying machine can be built.

Proof.
Assume unitary U is our copying machine and that we can copy qubits $|\psi\rangle$ and $|\varphi\rangle$. Thus

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \text{ and } U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle.$$

Take the inner product of the two equalities to get

$$\langle\psi|\langle 0|U^\dagger U|\varphi\rangle|0\rangle = \langle\psi|\langle\psi||\varphi\rangle|\varphi\rangle.$$

This simplifies to $\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$. Thus the two qubits must be equal or orthogonal. □

Some quantum gates

- The following Hermitian, unitary operators act on one qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

- We think of X as a bit flip

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle$$

Z as a phase flip

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$$

and $Y = iXZ$ as both. The Hadamard gate H takes $|0\rangle$ and $|1\rangle$ to the *dual basis*

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

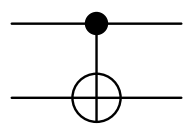
A 2-qubit gate

- The CNOT gate (controlled not) acts by

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

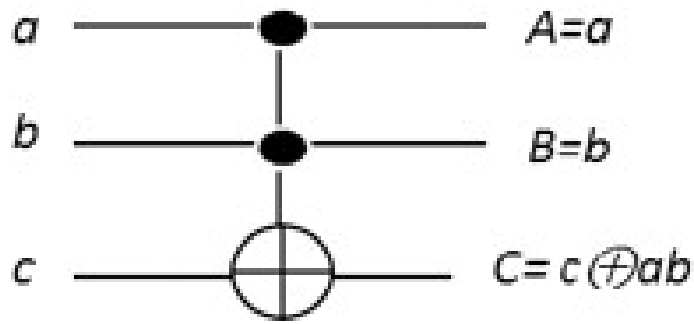
  extended linearly.

- We represent it by the following circuit where the top wire is the control and the bottom wire is the target



Quantum gates can simulate classical computing

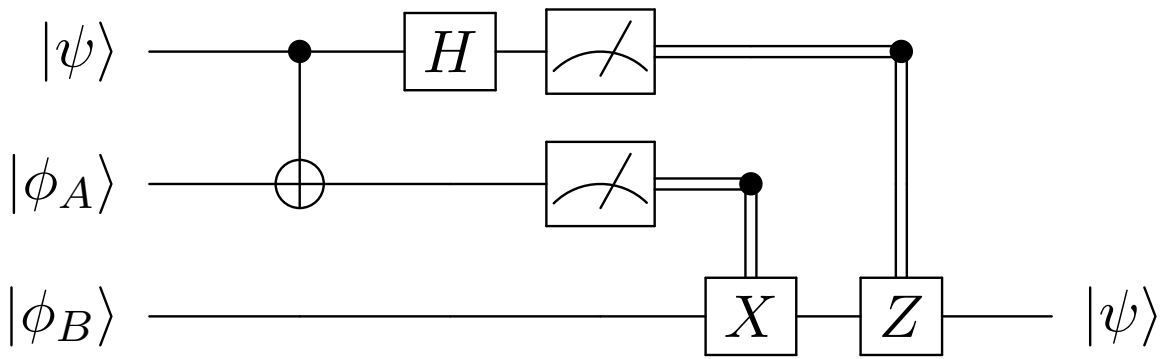
- Classical computers can be described by Turing machines or classical logic circuits.
- Classical circuits can be made reversible and implemented by (for example) the Toffoli gate (also called CCNOT).



- The Toffoli gate can be implemented in a quantum computer.

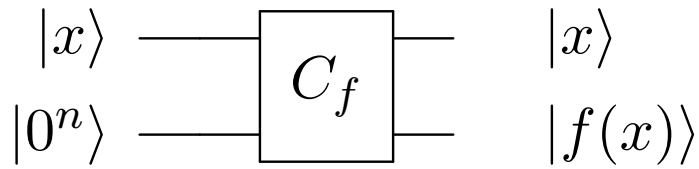
Something new: quantum teleportation

- Alice and Bob share a pair of "entangled" qubits whose state is $(|00\rangle + |11\rangle)/\sqrt{2}$.
- Now Alice and Bob each take their qubit and separate in space. How can Alice now send Bob an arbitrary qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ by transmitting only classical information?



A weird problem

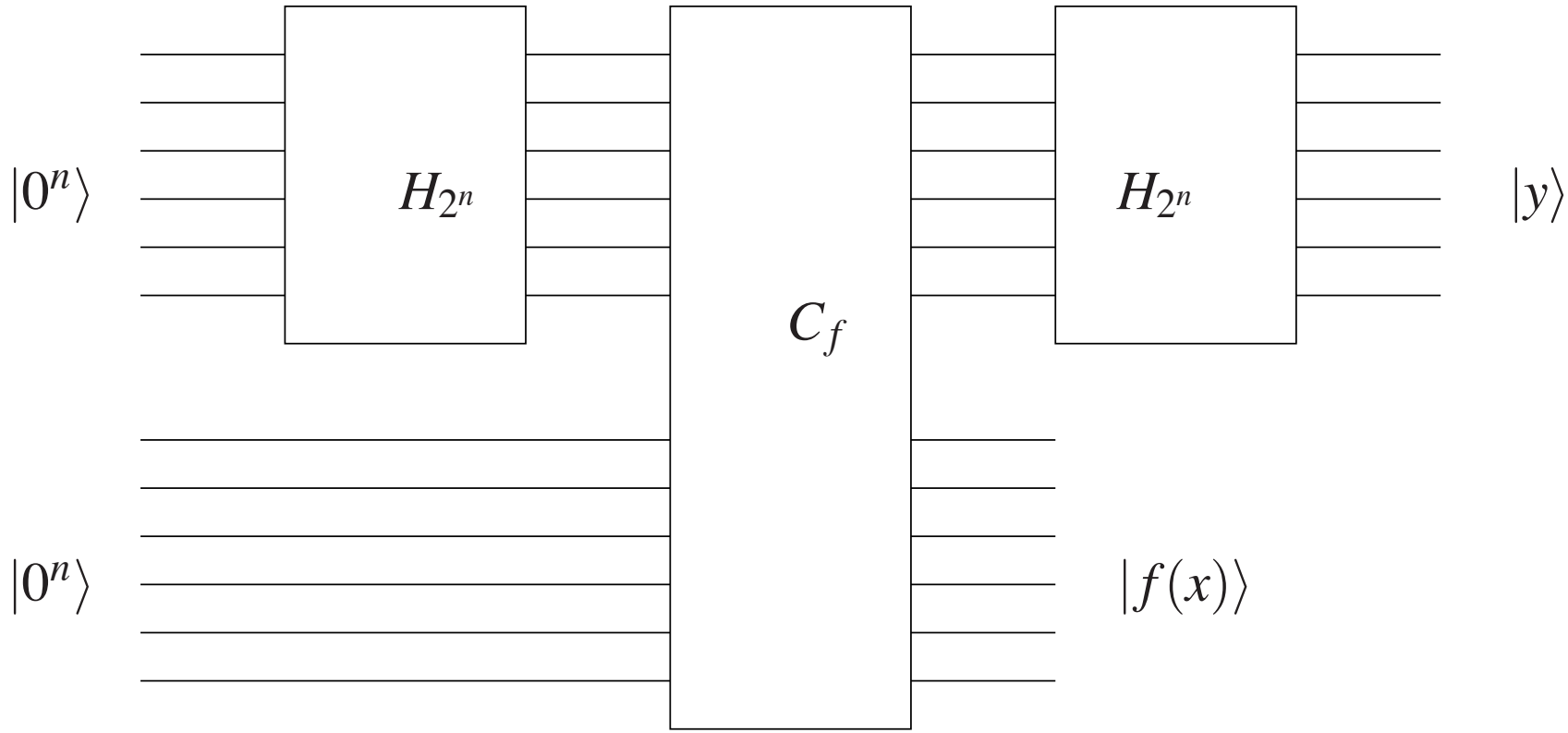
- We want to find out something about a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ given a quantum black box evaluator C_f.



- The function f has a property: there is an $a \in \mathbb{F}_2^n \setminus \{0^n\}$ such that $f(x) = f(y)$ iff $x + y = a$ or $x = y$.
- The problem: find a with high probability with a small number of uses of the black box.

Simon's algorithm

- Probabilistic classical algorithms require on the order of $2^{n/2}$ queries to succeed with probability greater than $2/3$.
- The best quantum algorithm, due to Daniel Simon, uses on the order of n queries to succeed with probability greater than $2/3$.



A real problem: integer factorization

- The best known classical algorithm for factoring an integer N, the general number field sieve, runs in $O\left(e^{(\frac{64}{9}\log N)^{1/3}(\log\log N)^{2/3}}\right)$ time.
- Shor's algorithm factors an integer in $O((\log N)^3)$ time.

Building a quantum computer

- Requirements:
  - Represent qubits
  - Perform universal family of unitary transformations
  - Prepare initial states
  - Measure output results
- You also need to guard against noise. The *quantum fault tolerance theorem* says that if you can get your components to work with some threshold accuracy then you can use quantum error correction to get any desired accuracy.

Experimental progress

- D-Wave Systems will sell you a 128 qubit adiabatic quantum computer but it is somewhat controversial whether it does anything quantum.
- More encouraging results with ion traps, superconducting circuits, quantum optics etc:
  - In 2001 IBM researchers factored 15 with an NMR quantum computer. This has since been repeated with optical (2007) and superconducting (2012) quantum computers. I have also seen references to 21 and 143 being factored.
  - In 2011 Thomas Monz created 14 "controllably entangled" qubits in an ion trap.