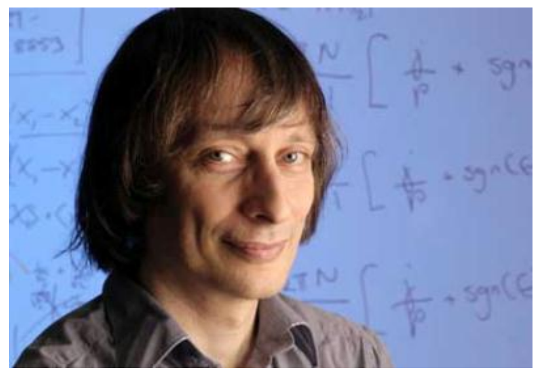
Evolving the system: quantum circuits and quantum gates

- One way of thinking about algorithm design and computation is via quantum Turing machines
- First described by David Deutsch in 1985, but both a quantum Turing machine's tape and its read-write head exist in superpositions of an exponential number states!



- Instead of using the Turing machine as a computational model, operations on a quantum computer most often described using quantum circuits (also introduced by Deutsch a few years later)
- Although circuits are computationally equivalent to Turing machines, they are usually much simpler to depict, manipulate and understand

Quantum gates represent unitary transformations

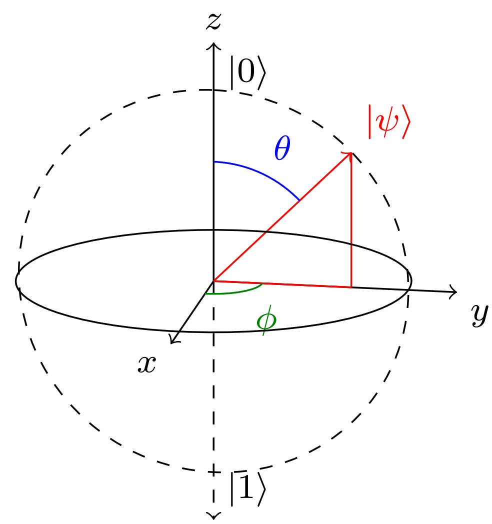
- Quantum gates are represented as transformation matrices, linear operators applied to a quantum register by tensoring the operator with the register
- All quantum linear operators must be *unitary*:
  - If a complex matrix U is unitary, then $U^{-1} = U^\dagger$, where $U^\dagger$ is the conjugate transpose: $U^\dagger = \overline{U}^{\mathrm{T}}$
  - It follows that $UU^\dagger = U^\dagger U = I$
  - Unitary operators preserve inner product:

$$\langle \mathbf{u} | U^\dagger U | \mathbf{v} \rangle = \langle \mathbf{u} | I | \mathbf{v} \rangle = \langle \mathbf{u} | \mathbf{v} \rangle$$

  - The composition of two unitary operators is also unitary:

$$(UV)^\dagger = V^\dagger U^\dagger = V^{-1} U^{-1} = (UV)^{-1}$$

The Bloch sphere



- Unitary transformations performed on a qubit may be visualized as rotations and reflections about the x, y, and z axes of the *Bloch sphere*
- All linear combinations $a_0 |0\rangle + a_1 |1\rangle$ in $\mathbb{C}^2$ correspond to all the points (θ, ψ) on the surface of the unit sphere, where $a_0 = \cos(\theta/2)$ and $a_1 = e^{i\phi} \sin(\theta/2) = (\cos\phi + i \sin\phi) \sin\frac{\theta}{2}$

The Hadamard operator

$$\text{---}\boxed{H}\text{---} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|$$

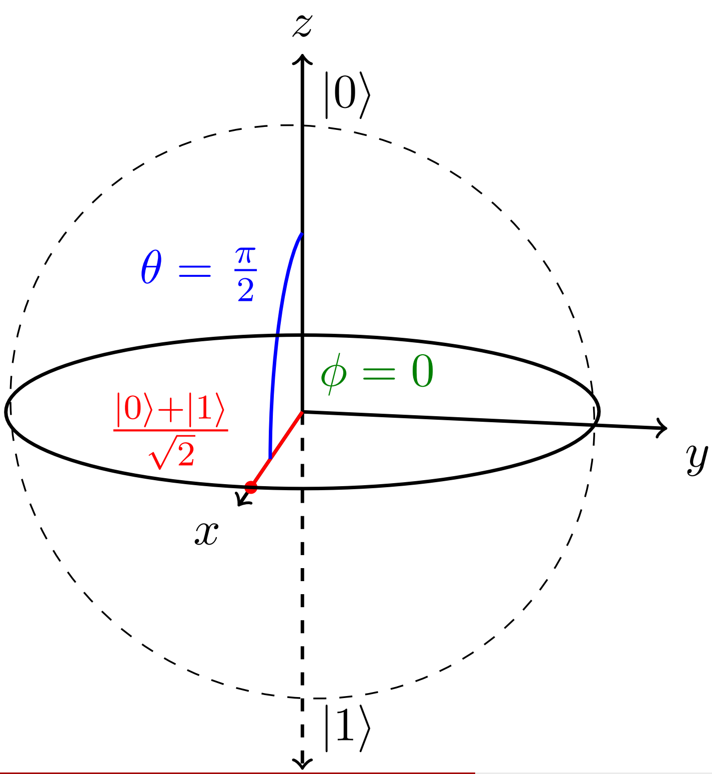
- Often referred to as a "fair coin flip," the Hadamard operator applied to a qubit with the value $|0\rangle$ or $|1\rangle$ will induce an equal superposition of the states $|0\rangle$ and $|1\rangle$:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0|1\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Many quantum algorithms begin by applying the Hadamard operator to each qubit in a register initialized to $|0\rangle^n$, which puts the entire register into an equal superposition of states

Bloch sphere representation of the Hadamard operator

- Geometrically, the Hadamard operator performs a rotation of $\pi/2$ about the y axis followed by a rotation about the x axis by π radians on the Bloch sphere:



The Pauli gates

- The three Pauli gates, named after yet another Nobel laureate Wolfgang Pauli, are also important single-qubit gates for quantum computation
- The Pauli-X gate swaps the amplitudes of $|0\rangle$ and $|1\rangle$:

$$-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$$

- The Pauli-Y gate swaps the amplitudes of $|0\rangle$ and $|1\rangle$, multiplies each amplitude by i, and negates the amplitude of $|1\rangle$:

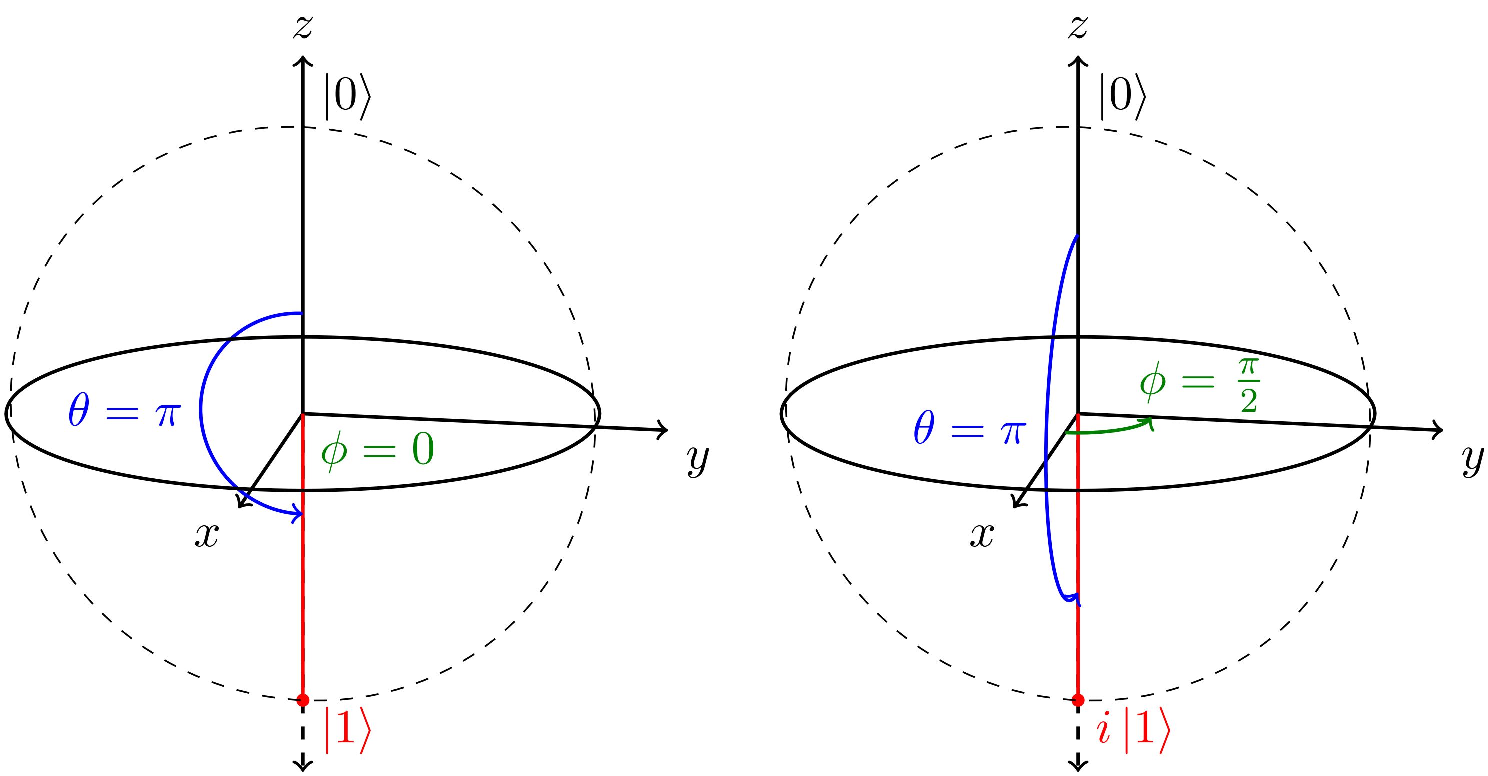
$$-\boxed{Y}- = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1|$$

- And the Pauli-Z gate negates the amplitude of $|1\rangle$, leaving the amplitude of $|0\rangle$ the same:

$$-\boxed{Z}- = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |1\rangle\langle 0| - |0\rangle\langle 1|$$

Bloch sphere representation of Pauli-X and -Y gates

- The Pauli-X, -Y, and -Z gates correspond to rotations by π radians about the x, y, and z axes respectively on the Bloch sphere

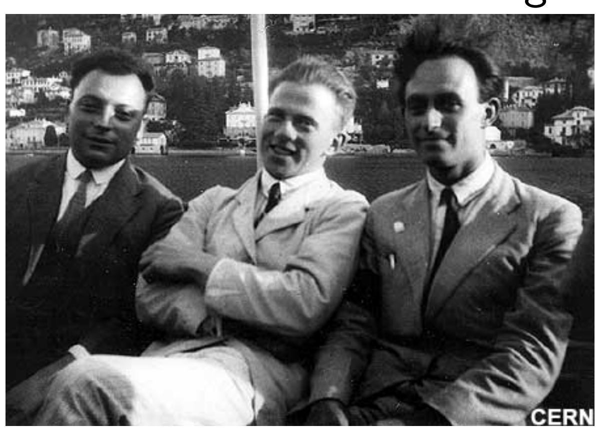


Generalized phase shift

- The Pauli-Z gate, altering only the phase of the system, is a special case of the more general phase-shift gate, which does not modify the amplitude of $|0\rangle$ but changes the phase of $|1\rangle$ by a factor of $e^{i\theta}$ for any value of θ:

$$—\boxed{R_\theta}— = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = |1\rangle\langle 0| + e^{i\theta}|0\rangle\langle 1|$$

- The Pauli-Z gate is equivalent to the phase-shift gate with $\theta = \pi$.
- Wolfgang Pauli with friends Werner Heisenberg and Enrico Fermi:



More phase shift gates

- Another special case of the phase-shift gate where $\theta = \pi/2$ is known as simply the phase gate, denoted S, which changes the phase of $|1\rangle$ by a factor of i:

$$\text{—}\boxed{S}\text{—} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = |1\rangle\langle 0| + i\,|0\rangle\langle 1|$$

- And the phase-shift gate where $\theta = \pi/4$ is referred to as the $\pi/8$ gate, or T:

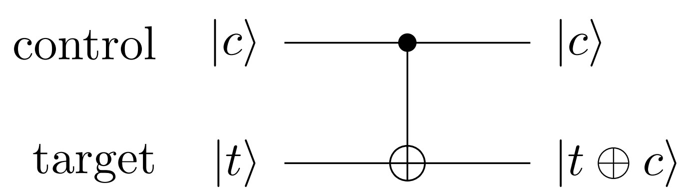
$$\text{—}\boxed{T}\text{—} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = |1\rangle\langle 0| + e^{i\pi/4}\,|0\rangle\langle 1|$$

With the name $\pi/8$ coming from the fact that this transformation can also be written as a matrix with $\pi/8$ along the diagonal:

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$$

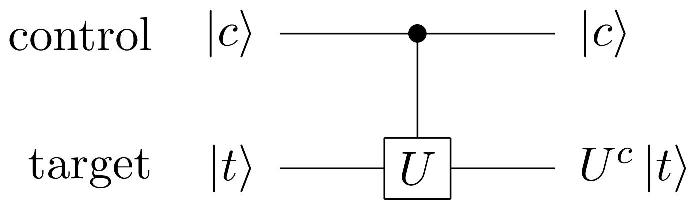
Controlled operations: CNOT

- Quantum computing also makes use of *controlled operations*, multi-qubit operations that change the state of a qubit based on the values of other qubits
- The quantum controlled-NOT or CNOT gate swaps the amplitudes of the $|0\rangle$ and $|1\rangle$ basis states of a qubit, equivalent to application of the Pauli-X gate, only if the controlling qubit has the value $|1\rangle$:



Generalized controlled operations

- Controlled operations are not restricted to conditional application of the Pauli-X gate; Any unitary operation may be performed:



- Matrix representation:

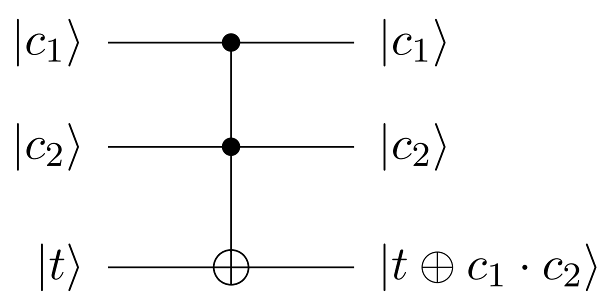
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{10} \\ 0 & 0 & x_{01} & x_{11} \end{bmatrix}$$

- Dirac equivalent:

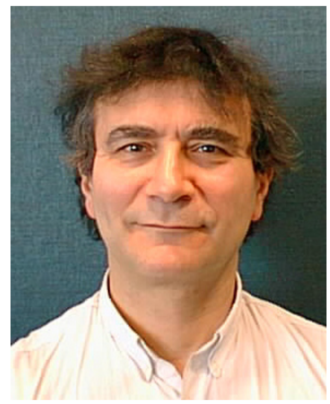
$$\begin{aligned} |00\rangle\langle 00| + |01\rangle\langle 01| + x_{00}\,|10\rangle\langle 10| + x_{01}\,|10\rangle\langle 11| \\ + x_{10}\,|11\rangle\langle 10| + x_{11}\,|11\rangle\langle 11| \end{aligned}$$

Controlled operations: Toffoli

- In fact, controlled operations are possible with any number n control qubits and any unitary operator on k qubits
- The Toffoli gate is probably the best known of these gates
- Also known as the controlled-controlled-NOT gate, the Toffoli gate acts on three qubits: two control qubits and one target
- If both control qubits are set, then the amplitudes of the target qubit are flipped:



Toffoli continued



- The Toffoli gate was originally devised as a universal, reversible *classical* logic gate by Tommaso Toffoli
- It is especially interesting because depending on the input, the gate can perform logical AND, XOR, NOT and FANOUT operations...
- This makes it universal for classical computing!
- Quantum computing is reversible:
  - All evolution in a quantum system can be described by unitary matrices, all unitary transformations are invertible, and thus all quantum computation is reversible
- The Toffoli gate implies that quantum computation is at least as powerful as classical computation