Quantum Computing

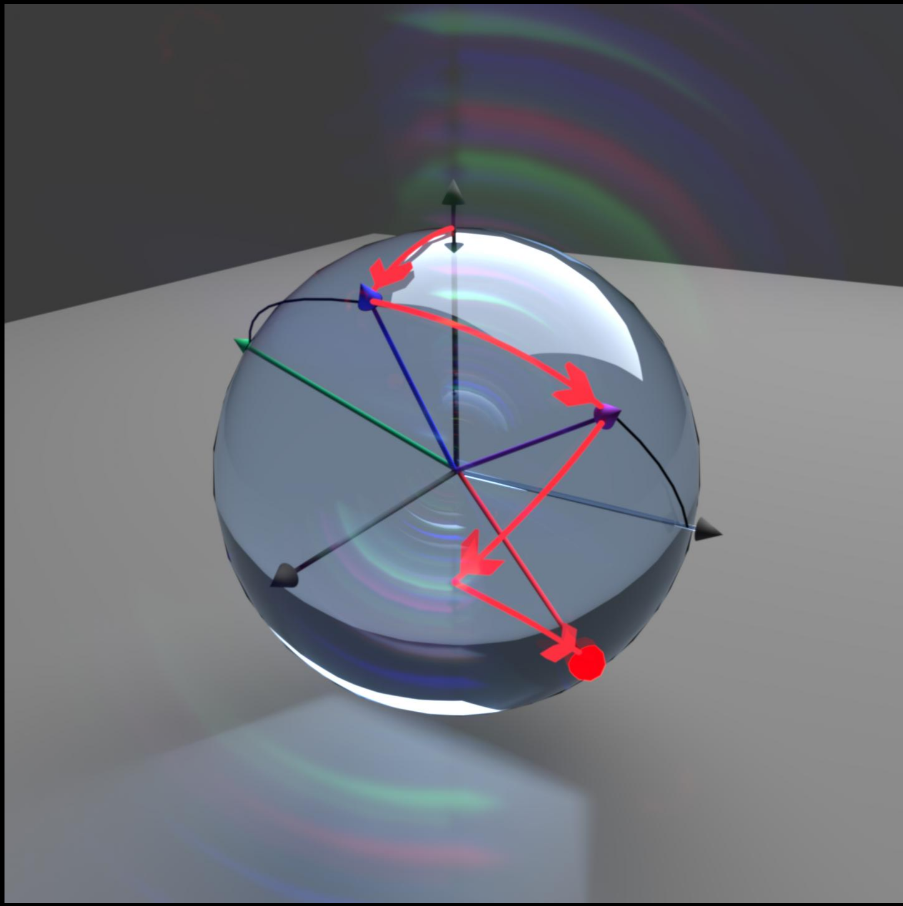
FC Langbein

Motivation

- *Church-Turing thesis*: An algorithm is what we can do on a Turing machine (1930-1952)
- Richard Feynman: *There is plenty of room at the bottom* (1959)
- David Deutsch: *Can we justify the C-T thesis using laws of physics?*
- Quantum mechanics appear hard to simulate on a traditional computer (memory and time limited)
  - So could a *machine exploiting quantum mechanics* efficiently simulate a Turing machine?
  - *Church-Turing-Deutsch principle*: Any physical process can be efficiently simulated on a quantum computer
- *Research problem*: Derive or refute the Church-Turing-Deutsch principle, starting from the laws of physics

Qubits

- Consider *two states*: $|0\rangle, |1\rangle$
  - A qubit is $|\Psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}$
  - Normalised: $a^2 + b^2 = 1$
- This is a point (θ, ψ) on the Bloch sphere (ignoring global phase γ)
  - $a = e^{i\gamma} \cos\frac{\theta}{2}$ and $b = e^{i(\gamma+\psi)} \sin\frac{\theta}{2}$



Dynamics

- The evolution of a *closed quantum system* is described by a *unitary transformation*

$$|\Psi(t)\rangle = U(t)|\Psi(0)\rangle$$

  - where $U(t)$ is the solution to the (time-dependent) *Schrödinger equation*

$$i\hbar\frac{d|\Psi(t)\rangle}{dt} = H|\Psi(t)\rangle; \qquad U(t) = e^{-i/\hbar Ht}$$

  - Calculated as the *matrix exponential* of the *Hamiltonian* H
  - Note, H is not necessarily constant over time!

- Any *quantum algorithm* is a *unitary transformation* of the initial state with *measurement(s)* at some time(s) t

Measurements

- *Quantum measurements* are described by a collection $\{M_m\}$ of measurement operators
  - Operators on the state space where the index m refers to the measurement outcomes
- The *probability* that result m occurs (at time t) is give by
$$p(m) = \langle \Psi(t) | M_m^\dagger M_m | \Psi \rangle$$
- The *state of the system after the measurement* is
$$\frac{M_m |\Psi\rangle}{\sqrt{p(m)}}$$
- The measurement operators satisfy the *completeness equation*
$$\sum_m \frac{M_m |\Psi\rangle}{\sqrt{p(m)}} = I$$
- Important measurement operators: $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$
  - Note, $p(0) = \langle \Psi | M_0^\dagger M_0 | \Psi \rangle = \langle \Psi | 0 \rangle \langle 0 | 0 \rangle \langle 0 | \Psi \rangle = \langle \Psi | 0 \rangle \langle 0 | \Psi \rangle = |a|^2$

Multi-Qubit Systems

- *Multiple qubits*
  - *Tensor product* of single qubit states!
  - States of two qubits:
    $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
  - States of three qubits:
    $|000\rangle, |001\rangle, |010\rangle, |100\rangle, |011\rangle, |101\rangle, |110\rangle, |111\rangle$
  - ...
- So $|\Psi_1\rangle = a|0\rangle + b|1\rangle$ and $|\Psi_2\rangle = c|0\rangle + d|1\rangle$ give

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = |\Psi_1\Psi_2\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

- This is the essence of *superposition*
  - A system can be in *multiple states at the same time*, with certain probabilities to get them as measurement results
- This *correlates* measured states of individual qubits

Entanglement

- Create an EPR pair: start with $|\Psi_1\rangle = |0\rangle$, $|\Psi_2\rangle = |0\rangle$
  - Apply $\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$: $\quad |\Psi_1'\rangle = \mathrm{H}|\Psi_1\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - Take the tensor product $|\Psi_1'\rangle \otimes |\Psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle$
  - Apply $\mathrm{C}_{\mathrm{NOT}} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$: $\quad \mathrm{C}_{\mathrm{Not}}|\Psi_1'\Psi_2\rangle = \dfrac{1}{\sqrt{2}}|00\rangle + \dfrac{1}{\sqrt{2}}|11\rangle$
- It is *not possible to decompose the state space* into component spaces!
  - There is no $|\Psi_1\rangle$ and $|\Psi_2\rangle$ such that $|\Psi_1\rangle \otimes |\Psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- *Entanglement* is a strong correlation of measurements, stronger than classically possible (carries more information)

Quantum Circuit Model

- *Classical*
  - Unit: bit
  - Prepare n-bit input
  - Apply 1 and 2 bit logic gates
  - Readout value of bits
- *Quantum*
  - Unit: qubit
  - Prepare n-qubit input in the computational basis
  - Apply unitary 1- and 2- qubit quantum logic gates
  - Measure partial information about qubits

Single-qubit Quantum Logic Gates

- Pauli gates

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Phase gate

$$P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

  - Note, $P^2 = Z$

Multi-qubit Gates

- Controlled-not gate

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

  - Can turn this into a controlled-U gate (if the first bit is 1, then U is applied to the second bit)
- Toffoli gate, CCNOT (universal for classical reversible logic)

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Classical and Quantum Logic

- Quantum logic is *reversible* (unitary operations)
- Classical logic is *irreversible* (cannot invert and/or)
- *Classical NAND* gate: `x NAND y = NOT (x AND y)`
- *Reversible classical NAND*: CCNOT (Toffoli)
  - When the third bit is 1, CCNOT maps NAND of the first two bits onto the third
  - `CCNOT(x,y,1) = (x,y, x NAND y)`
- Quantum NAND is the CCNOT/Toffoli gate

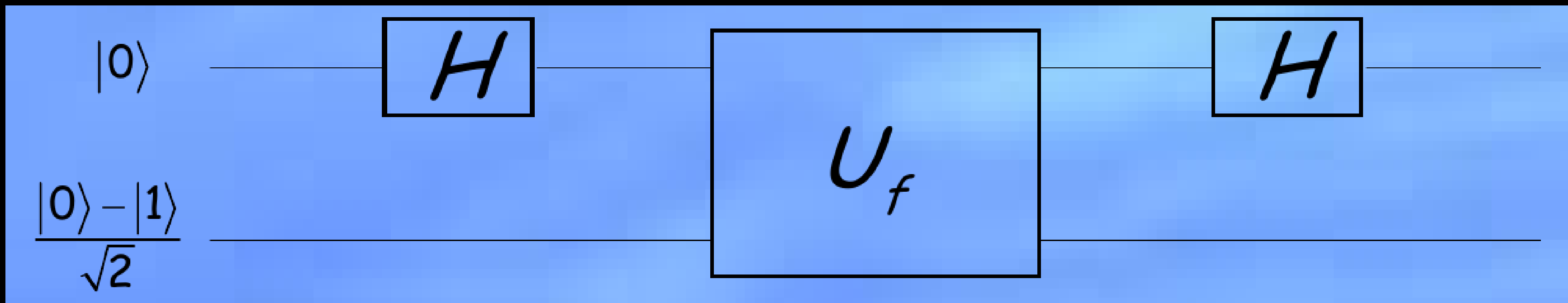
Deutsch's Problem

- Given a black box computing a function $f : \{0,1\} \to \{0,1\}$
  - Determine whether f *is constant or balanced*
- Classically we need to *evaluate both* $f(0)$ and $f(1)$
  - $f(x,z) = (x, x \oplus f(x))$
- Quantumly we only need the black box for f *once*
  - $U_f\,(|x\rangle, |z\rangle) = (|x\rangle, |x \oplus f(x)\rangle)$
  - Put the information in the phase:

$$U_f\left(|x\rangle, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

  - $f(x) = 0$: $|x\rangle(|0\rangle - |1\rangle) \to |x\rangle(|0\rangle - |1\rangle)$
  - $f(x) = 1$: $|x\rangle(|0\rangle - |1\rangle) \to |x\rangle(|1\rangle - |0\rangle) = -|x\rangle(|0\rangle + |1\rangle)$

$$|x\rangle \to (-1)^{f(x)}|x\rangle$$



$$
\begin{aligned}
|0\rangle &\to |0\rangle + |1\rangle \\
&\to (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \\
&\to (-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle) \\
&= ((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle
\end{aligned}
$$

- f *constant* $\Rightarrow$ all amplitude in $|0\rangle$
- f *balanced* $\Rightarrow$ all amplitude in $|1\rangle$

Universality in the Quantum Circuit Model

- *Classically*, any function f can be computed using just NAND and FANOUT
  - We say those operations are universal for classical computation
- Suppose U is an *arbitrary unitary transformation* on n qubits
  - Then U can be composed from *controlled-not* gates and *single-qubit* quantum gates
  - As in the classical case, a counting argument can be used to show that there are U that take exponentially many gates to implement
- Importantly, for this we have *ignored noise*
  - Fabrication variability, uncertainty in control pulses, unwanted interaction with the environment, measurement backaction, . . .
  - *Quantum error correction* can counteract this (with only polynomial effect on the gates), but makes many assumptions
  - (Quantum) *thermodynamics*: What are the physical limits for what we can do in the universe?

Models for Quantum Computation

- *Gate model*:
  - Prepare a computational basis state
  - Do a sequence of one- and two-qubit unitary gates
  - Measure in the computational basis
- *Topological quantum computer*:
  - Create pairs of “quasiparticles” in a lattice
  - Move those pairs around the lattice
  - Bring pairs together to annihilate
  - This gives a unitary operation on the state of the lattice
  - Only depends on the topology of the path traversed by the quasiparticles

Models for Quantum Computation

- *Quantum computation via entanglement and single-qubit measurements*:
  - Create a particular fixed entangled state of a large lattice of qubits
  - Perform computation via single-qubit measurements
- *Quantum computation as equation solving*:
  - Quantum computation is equivalent to counting the number of solutions to certain sets of quadratic equations (modulo 8)!
- *Quantum computation via measurement alone*:
  - Perform a quantum computation by a sequence of two-qubit measurements
  - Does not require unitary dynamics, except quantum memory

The No-Programming Theorem

- Can we build a *programmable quantum computer*?
- *Classically*: *stored program architecture*, e.g. von Neumann-Zuse
  - Input data and the computer programs are both stored in memory
  - Can dynamically create and run new programs in memory
- *Quantum computing*
  - We *cannot create a programmable quantum computer* using the stored program architecture!
  - Unitary operators $U_1, \dots, U_n$ which are distinct, even up to global phase factors, require orthogonal programs $|U_1\rangle, \dots, |U_n\rangle$
  - Each quantum program is a unitary transformation
  - Distinct programs come from distinct unitary operators (these are orthogonal)
  - Thus, we cannot create a unitary operator that can write another unitary operator

Quantum Control

- Find *optimal fields* $u_k(t)$ to steer the dynamics of a quantum system

$$i\hbar\frac{\partial|\Psi\rangle}{\partial t} = \underbrace{\left(H_0 + \sum_k u_k(t)H_k\right)}_{\text{Hamiltonian } H_u}|\Psi\rangle$$

  - by *maximising* a fidelity, e.g. to implement a unitary operator U

$$f(u_1,\ldots,u_n) = \frac{1}{N}\left|\mathrm{tr}\left(U^\dagger e^{-i\hbar H_u t_f}\right)\right|$$

  - Typically $u_k(t)$ are piecewise constant

- Also over *static biases* D:
$H = H_0 + D$

- The *target time* t_f

- Use the *environment as controller*

$$i\hbar\frac{\partial\rho}{\partial t} = [H_u,\rho] + \mathfrak{L}_u\rho$$

...