Quantum Information

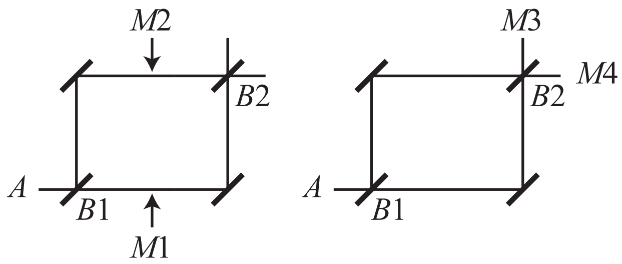
- Classical Information Unit: The *Bits;* $b \in \{0, 1\}$
- Quantum Information Unit: The *Qubit;* $|q\rangle \in \mathbb{C}^2$ with $||q|| = 1$.

- Classical Information: *Bit Strings;* $B \in \{0, 1\} \times \cdots \times \{0, 1\}$.
- Quantum Information: *Qubit Tensors;* $|Q\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.
  $|Q\rangle = |q\rangle_1 \otimes \cdots \otimes |q\rangle_n$ with $||q_i|| = 1$

- **Notation:**
  - $|x\rangle$: *Ket*-Notation of vectors
  - $\{|0\rangle, |1\rangle\}$ ONB of $\mathbb{C}^2$
  - $|1\rangle \otimes |0\rangle \otimes |1\rangle =: |1\rangle|0\rangle|1\rangle =: |101\rangle =: |5\rangle$
  - $\langle x| := |x\rangle^T$

Physical Background

- Why?
- Quantum states can be superpositions of states.
- Example 1: Interferometer



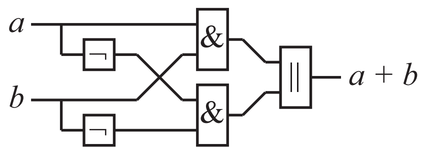
- Example 2: Schrödinger's cat is both dead and alive:

$$|\mathrm{cat}\rangle = \frac{1}{\sqrt{2}}\Big(|\mathrm{dead}\rangle + |\mathrm{alive}\rangle\Big)$$

- Measurement: Open the box and find out. Then $|\mathrm{cat}\rangle = |\mathrm{dead}\rangle$ or $|\mathrm{cat}\rangle = |\mathrm{alive}\rangle$.

Classical Computation

- Classical Computation: The *Circuit Model*
- Functions $f\colon \{0,1\}^n \to \{0,1\}^m$ are implemented in circuits.
- Example: Addition modulo 2



- AND, OR, and NOT build a uniform set of gates.
- Functions $f\colon \mathbb{N} \to \mathbb{N}$ are encoded by a *family* of circuits.

Quantum Computation

- Computational Model: *Quantum Circuit*
- Quantum gates are *unitary operators*
- Examples:

Hadamard Transform	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	epsfigfile=hadamard.eps
Controlled NOT	$\begin{pmatrix}1 & & & \\ & 1 & & \\ & & & 1\\ & & 1 & \end{pmatrix}$	epsfigfile=controlledNot.eps

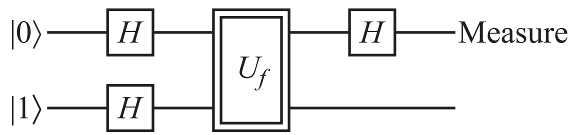
- Uniform set of gates: all unitary operators $\mathbb{C}^2 \to \mathbb{C}^2$ plus the Controlled NOT.

Example: Deutsch-Josza Algorithm

- Suppose $f\colon \{0,1\} \to \{0,1\}$ can be computed by a black box.
- Decide whether $f(0) = f(1)$ with computing f only once!
- Let $U_f\colon \mathbb{C}^2 \otimes \mathbb{C}^2$ be defined by

$$U_f|xy\rangle := |x, y \oplus f(x)\rangle \qquad (x, y \in \{0,1\})$$

  where $\oplus$ denotes the boolean XOR.
- Consider the quantum circuit



- The circuit computes

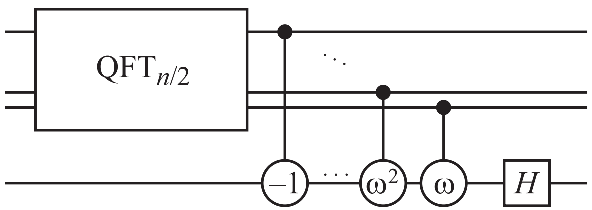
$$(H \otimes I) \cdot U_f \cdot (H \otimes H) \cdot |01\rangle.$$

Example: Deutsch-Josza Algorithm II

- What is $(H \otimes I) \cdot U_f \cdot (H \otimes H) \cdot |01\rangle$?
- $$\begin{aligned} &(H \otimes H)|01\rangle \\ &= (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &= |0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle) \end{aligned}$$
- $$\begin{aligned} &U_f\Big(|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)\Big) \\ &= |0\rangle\Big((|0\rangle - |1\rangle) \oplus |f(0)\rangle\Big) + |1\rangle\Big((|0\rangle - |1\rangle) \oplus |f(0)\rangle\Big) \\ &= \Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)(|0\rangle - |1\rangle) \end{aligned}$$
- $$\begin{aligned} &H\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \\ &= (-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle) \\ &= ((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle \end{aligned}$$
- Note that $(-1)^{f(0)} + (-1)^{f(1)} = 0$ iff $f(0) = f(1)$
- Hence, a measurement yields $|0\rangle$ iff $f(0) \neq f(1)$.

Quantum Fourier Transform

- **Definition:** Let $q = 2^l$, $\omega := \exp(2\pi \mathrm{i}/q)$. Then
$$\mathrm{QFT}\,|a\rangle = \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} \omega^{ab} |b\rangle.$$
defines the *quantum fourier transform* on $(C^2)^l$.
- Cooley-Tucky:
$$\mathrm{QFT}_{nm} = (\mathrm{QFT}_m \otimes I_n) \cdot T \cdot (I_m \otimes \mathrm{QFT}_n) \cdot P$$
for a permutation P and a diagonal matrix T.
- Quantum Circuit for the QFT:



- Needs only $\mathrm{O}(l^2)$ quantum gates!

Shor's Factoring Algorithm

- Let N be an L-digit number, a coprime to N.
- Let r be the *order* of $a \bmod N$.
- Suppose r is even. Then:

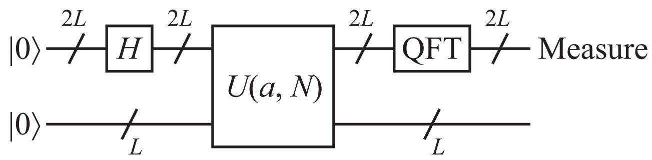
$$\begin{aligned} a^r &= 1 \bmod N \\ a^r - 1^2 &= 0 \bmod N \\ (a^{r/2} - 1)(a^{r/2} + 1) &= 0 \bmod N \end{aligned}$$

- Suppose $a^{r/2} \neq \pm 1$. Then $\gcd(N, a^{r/2} - 1)$ is a nontrivial factor of N.

- **Problem:** How to find the order of a.

Shor's Factoring Algorithm

- Main step of Shor's algorithm: Find the order of a.
- Let $U(a, N)$ be the unitary map $(x, y) \mapsto (x, y \oplus a^x\ (N))$.
- Consider the following circuit



- The measurement will favor values of y with
$$\frac{y_0}{2^{2L}} \approx \frac{k}{r}$$
for some integer k.
- y_0 and 2^{2L} are known. Also, $r < N$, so k/r can be guessed to be the closest fraction to $y_0/2^{2L}$ with denominator $< N$.
- This gives r (with reasonable probability) and we are done.