Quantum algorithms

Pranab Sen

and

Quantum information and error correction

Naresh Sharma

Joint lecture 2

Qubit

- Comes with its Hilbert space $\mathbb{C}^2$
- States are precisely the 1-D subspaces of $\mathbb{C}^2$, loosely represented by unit length vectors in $\mathbb{C}^2$
- Physical setup defines a distinguished orthonormal measurement basis of $\mathbb{C}^2$ called computational basis, denoted by $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Measuring state $\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ gives a classical bit with $\begin{pmatrix} |\alpha_0|^2 \\ |\alpha_1|^2 \end{pmatrix}$ as its prob. vector

From one to two

One qubit

Measured states: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

UP DOWN

Two qubits

Measured states:

$$|00\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

UP, UP

$$|01\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

UP, DOWN

$$|10\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

DOWN, UP

$$|11\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

DOWN, DOWN

From one to two (contd)

One qubit:

Unmeasured states:

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

$$\alpha_0, \alpha_1 \in \mathbb{C}, |\alpha_0|^2 + |\alpha_1|^2 = 1$$

$$\Pr[\text{“0”}] = |\alpha_0|^2, \Pr[\text{“1”}] = |\alpha_1|^2$$

Two qubits:

Unmeasured states:

$$\alpha_{00}|00\rangle + \alpha_{10}|10\rangle + \alpha_{01}|01\rangle + \alpha_{11}|11\rangle$$

$$\alpha_{00}, \alpha_{10}, \alpha_{01}, \alpha_{11} \in \mathbb{C}$$

$$|\alpha_{00}|^2 + |\alpha_{10}|^2 + |\alpha_{01}|^2 + |\alpha_{11}|^2 = 1$$

$$\Pr[\text{“00”}] = |\alpha_{00}|^2, \Pr[\text{“10”}] = |\alpha_{10}|^2,$$

$$\Pr[\text{“01”}] = |\alpha_{01}|^2, \Pr[\text{“11”}] = |\alpha_{11}|^2$$

Tensor product

- Hilbert spaces V, W of dimension m, n
- Orthonormal bases $\{|i\rangle\}_{i=1}^m, \{|j\rangle\}_{j=1}^n$, note $|i\rangle := \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} 1\text{st} \\ \vdots \\ i\text{th} \\ \vdots \\ m\text{th} \end{matrix}$
- Define

$$|i\rangle \otimes |j\rangle := \begin{pmatrix} 0 \cdot |j\rangle \\ \vdots \\ 1 \cdot |j\rangle \\ \vdots \\ 0 \cdot |j\rangle \end{pmatrix} \begin{matrix} 1\text{st} \\ \vdots \\ i\text{th} \\ \vdots \\ m\text{th} \end{matrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} 1\text{st} \\ \vdots \\ (n(i-1)+j)\text{th} \\ \vdots \\ (mn)\text{th} \end{matrix}$$

- $\left(\sum_{i=1}^m \alpha_i |i\rangle\right) \otimes \left(\sum_{j=1}^n \beta_j |j\rangle\right)$ is defined by distributivity
- $V \otimes W$ is defined as Hilbert space spanned by

$$|i\rangle \otimes |j\rangle, i = 1, \ldots, m, j = 1, \ldots, n$$

n qubits

Measured states: $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$

$$x \in \{0,1\}^n$$

Unmeasured states: $$\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$$

$$\alpha_x \in \mathbb{C}, \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1, \ \Pr[x] = |\alpha_x|^2$$

State vector of n qubits is a unit length vector in

$$\mathbb{C}^{2^n} \cong \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$$

Quantum algorithm

- Input: Intialised to a bit string $|x\rangle \otimes |\bar{0}\rangle, x \in \{0,1\}^n$
- Algorithm: Unitary transformation on input state
- Output: Bit string obtained by measuring state of computer at the end
- Require: With high probability, output is the correct answer

Tensor product again

- V_1, W_1, V_2, W_2 Hilbert spaces
- $T_1 : V_1 \to W_1, T_2 : V_2 \to W_2$ linear transformations
- $T_1 \otimes T_2 : V_1 \otimes V_2 \to W_1 \otimes W_2$ linear transformation, defined as $T_1 \otimes T_2(|i\rangle \otimes |j\rangle) := (T_1|i\rangle) \otimes (T_2|j\rangle), |i\rangle, |j\rangle$ bases of V_1, V_2, extended by linearity to all of $V_1 \otimes V_2$
- Matrix of $T_1 \otimes T_2$ given by

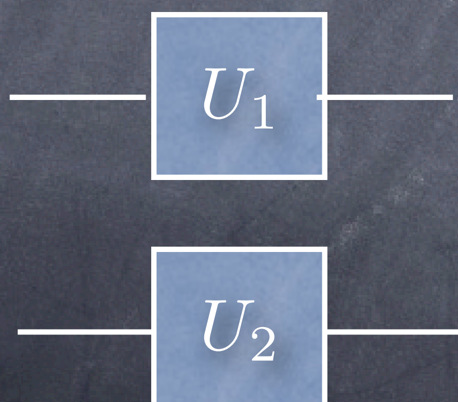
$$
\begin{array}{cc}
 & \begin{array}{ccc} \cdots & |i\rangle \otimes |*\rangle & \cdots \end{array} \\
\begin{array}{c} \vdots \\ |k\rangle \otimes |*\rangle \\ \vdots \end{array} & \left(\begin{array}{ccc} & \vdots & \\ & (t_1)_{ki} T_2 & \\ & \vdots & \end{array} \right)
\end{array}
$$

Single qubit gates

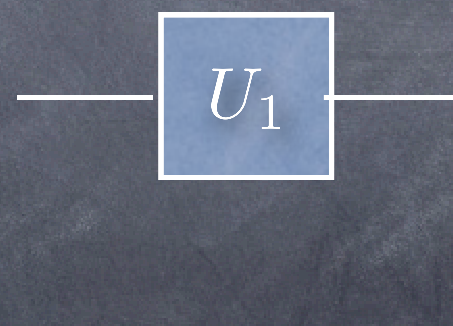
Unitary operators on $\mathbb{C}^2$

NOT: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ **Hadamard:** $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Phase: $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\pi/8\text{-gate:}\ \sqrt{P} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}$



$U_1 \otimes U_2$



$U_1 \otimes \mathbb{1}$

A two-qubit gate

- Controlled-NOT: $$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
- CNOT: $|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x \oplus y\rangle$
- CNOT is not a tensor product of single qubit gates
- CNOT, NOT, Hadamard, $\pi/8$-gate form a universal fault tolerant family for quantum computation (Boykin, Mor, Pulver, Roychowdhury, Vatan 1999)

Collapse on measurement

- Two qubit state: $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- Measuring both qubits: $\Pr[(i,j)] = |\alpha_{ij}|^2$

  State collapses to $|i\rangle \otimes |j\rangle$

- Measuring first qubit only: $\Pr[i] = |\alpha_{i0}|^2 + |\alpha_{i1}|^2$

  State collapses to $|i\rangle \otimes \left(\frac{\alpha_{i0}|0\rangle + \alpha_{i1}|1\rangle}{\sqrt{\Pr[i]}} \right)$

Deutsch's algorithm

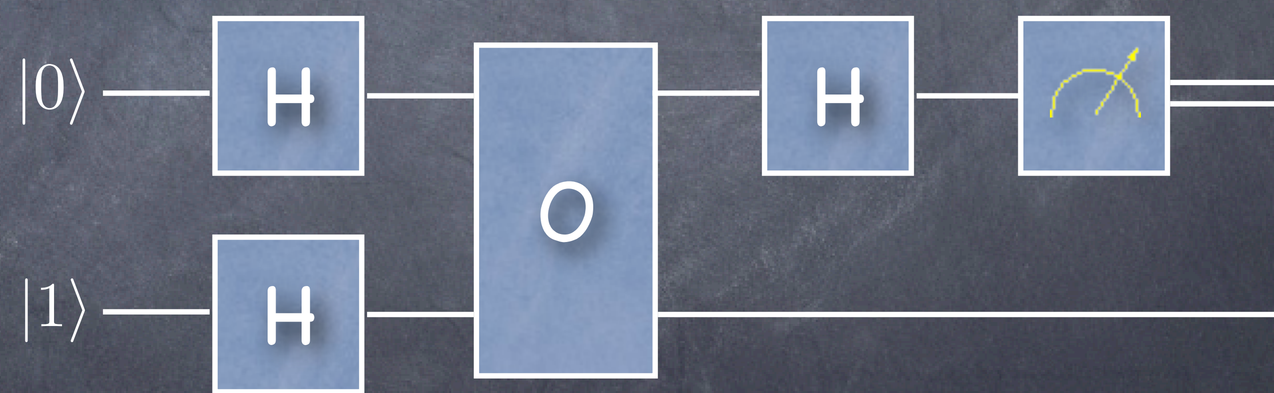
Problem: Compute parity of two bits x_0, x_1 given by an oracle

Classically: requires two queries to oracle

Quantumly: possible with **one** query only!

Classical oracle

Quantum oracle



Measurement outcome = 0 iff parity = 0

Database searching

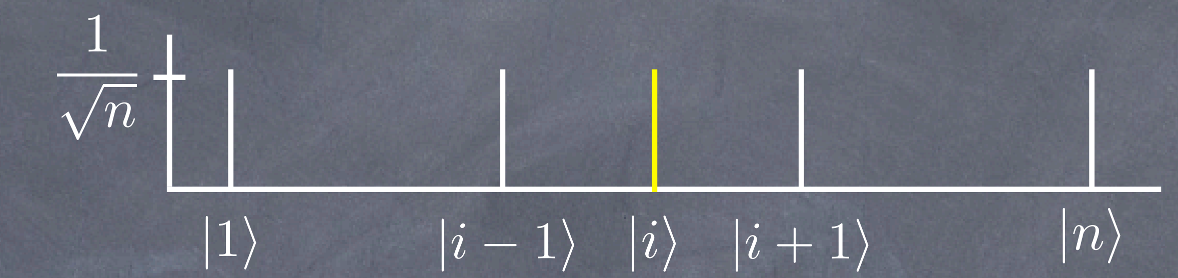
- **Problem:** Searching an unordered database with n items
- **Classically:** Requires time of order of n
- **Quantumly:** Can be done in time order of $\sqrt{n}$

Grover (1996)

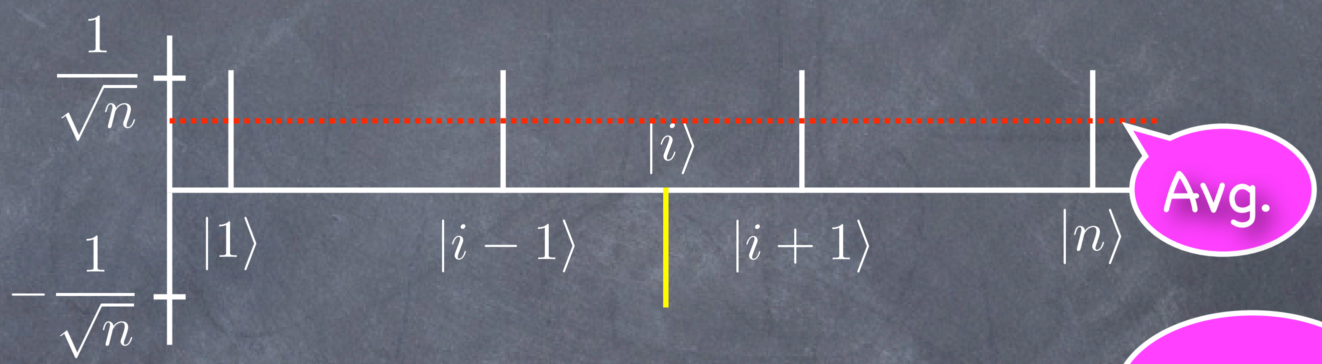
Speeds up many searching problems non-trivially

Grover's algorithm

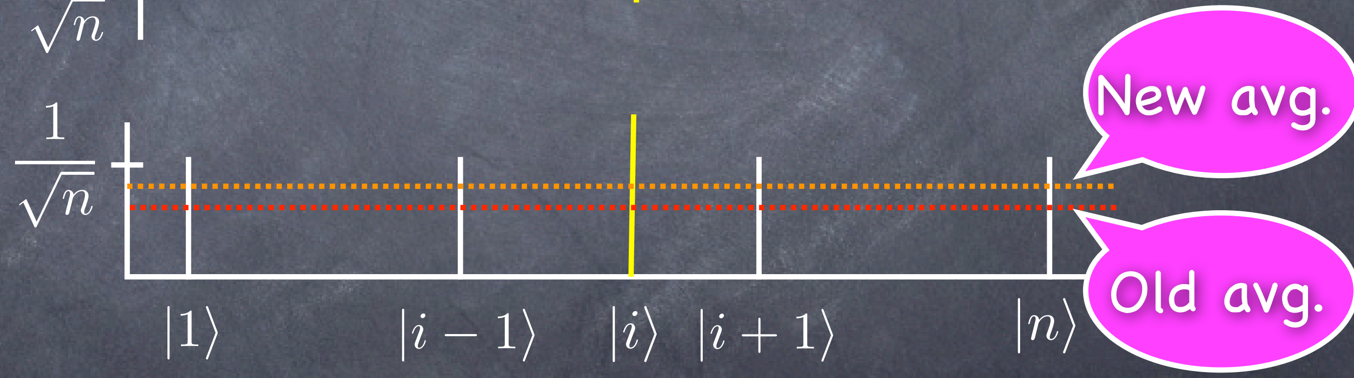
- Initialisation:
  (Easy to do)



- Inv. marked item:
  (Done by oracle)



- Inv. abt. average:
  (Easy to do)



Amplitude of marked item increases by around $\frac{2}{\sqrt{n}}$ in each iteration

Repeat around $\frac{\sqrt{n}}{2}$ times to get good prob. of detecting marked item

What more in algorithms?

- Faster algorithms for some other search problems by on quantum walks on Markov chains (later on)
- Efficient algorithm to factor integers: Peter Shor (1994), believed hard classically, at the heart of the popular RSA cryptosystem (later on)

- Efficient algorithms for several other number and group theoretic problems, believed hard classically (maybe later on)
- Efficient algorithms for some knot theoretic problems, believed hard classically (later on)

Information theory

- Mathematical theory of ``information transfer” or communication
- Entropy as a measure of uncertainty or lack of information in classical random variable (Shannon 1948)

- Coding theorems for noiseless and noisy channels
- Quantum analogues of above in terms of von Neumann entropy (later on)

- General notion of quantum operation and quantum noise (later on)

2 to 1 coding

Aim: Encode 2 bits into one qubit so that any single bit can be extracted with probability > 1/2

Classically: Impossible




Quantumly: Possible (Ambainis, Nayak, Ta-Shma, Vazirani ‘99)

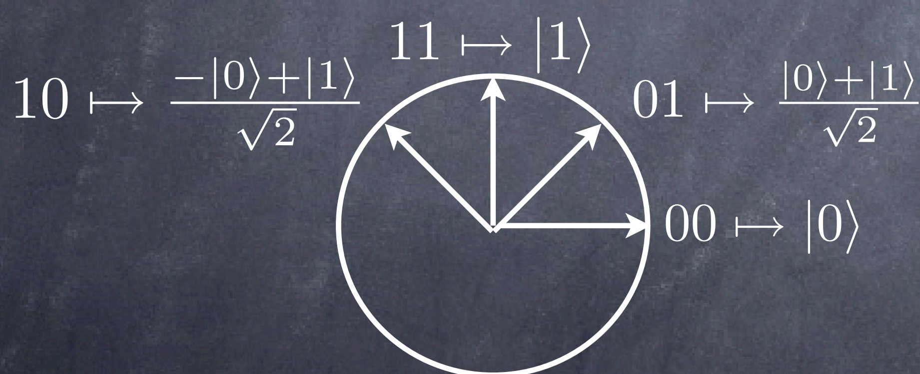
2 to 1 coding

Aim: Encode 2 bits into one qubit so that any single bit can be extracted with probability > 1/2

Classically: Impossible




Quantumly: Possible (Ambainis, Nayak, Ta-Shma, Vazirani '99)



Encoding

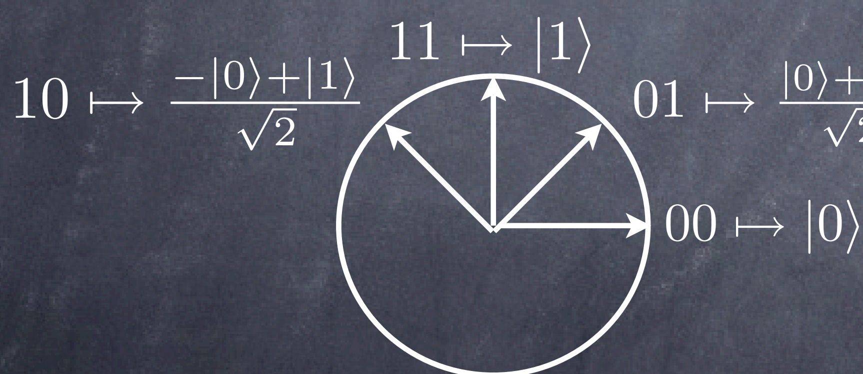
2 to 1 coding

Aim: Encode 2 bits into one qubit so that any single bit can be extracted with probability > 1/2

Classically: Impossible

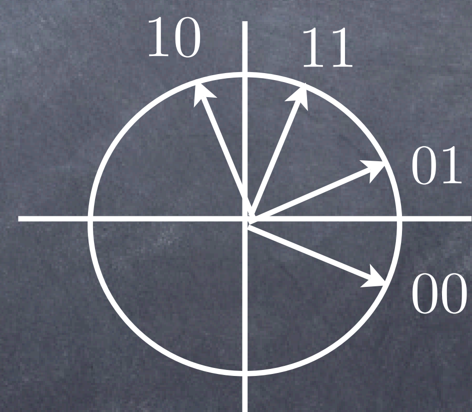



Quantumly: Possible (Ambainis, Nayak, Ta-Shma, Vazirani ‘99)



Encoding

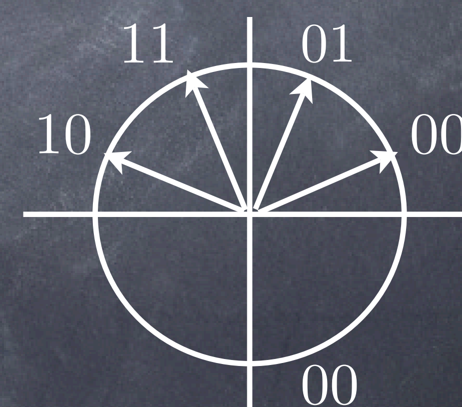
Success prob. $= \cos^2 \pi/8$
≈ 0.85



Extracting 1st bit

Rotate by $-\pi/8$

Measure



Extracting 2nd bit

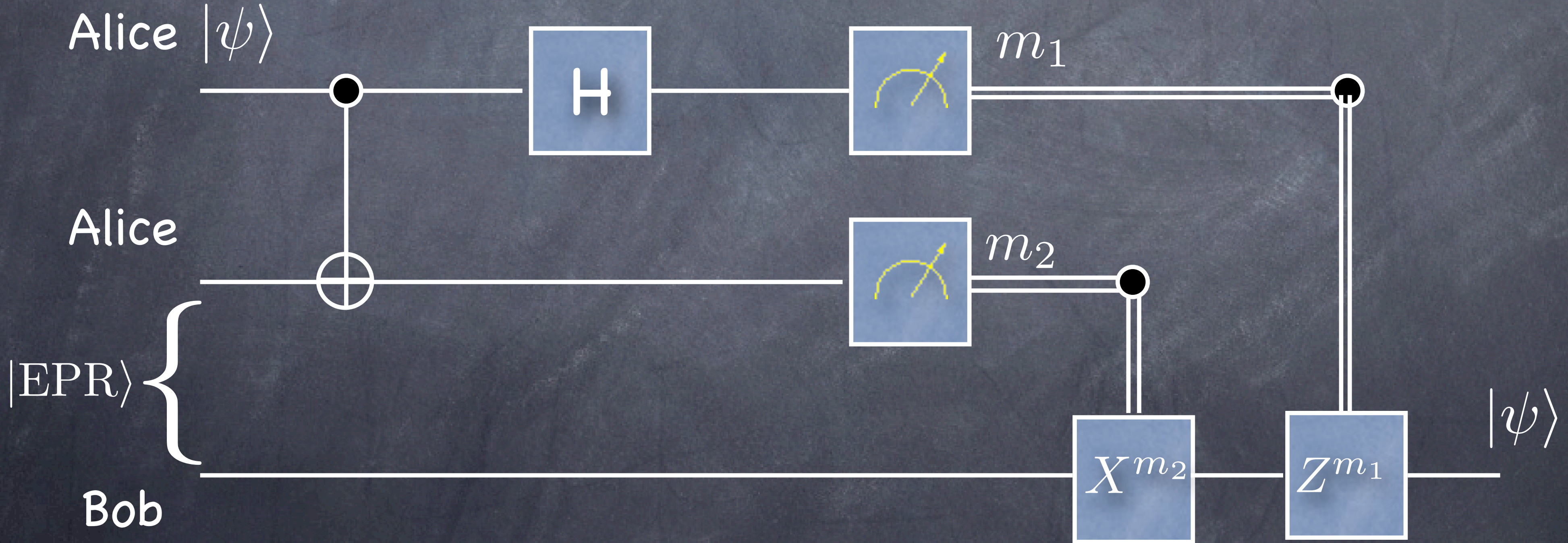
Rotate by $\pi/8$

Measure

Teleportation

Einstein-Podolsky-Rosen (EPR) pair: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

Unknown single qubit state: $|\psi\rangle$



$Z := P^2$

Error correction

- Classical error correcting codes required to protect classical information against errors
- Quantum error correcting codes required to protect quantum information against quantum errors; stabiliser codes of Gottesman (later on)

- Fault tolerant quantum computation and fault tolerance threshold of Aharonov-Ben Or (maybe later on)

Quantum cryptography

- Quantum computation breaks RSA, Diffie-Hellman etc. cryptosystems because of Shor's algorithms for factoring and discrete logarithm
- Quantum communication can be used to distribute a private key (Bennett-Brassard '84) without prior shared resources; impossible classically (maybe later on)

- Eavesdropper's actions amount to measuring transmitted qubits, which disturbs their state, leading to detection

Experiments

- Quantum key distribution close to practical reality
- Quantum computation immensely challenging experimentally
- Nuclear magnetic resonance (NMR), ion traps, superconducting junctions, quantum dots, ... proposed
- Every proposal has major implementation and/or scalability issues
- Current experimental implementations have error rates way above fault tolerance threshold