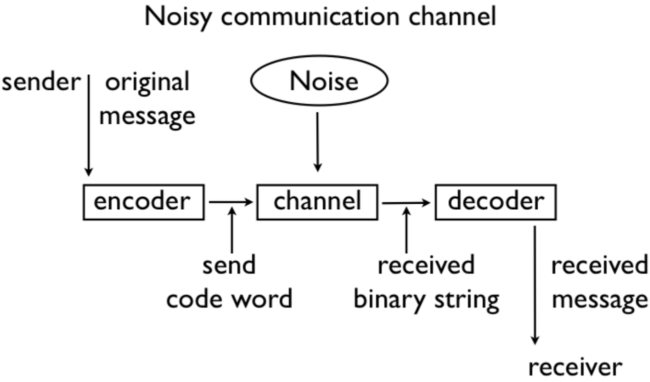
Quantum Communication

Bei Zeng

University of Guelph

Basic ideas for Quantum Communication



Shared entanglement

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Quantum Cryptography

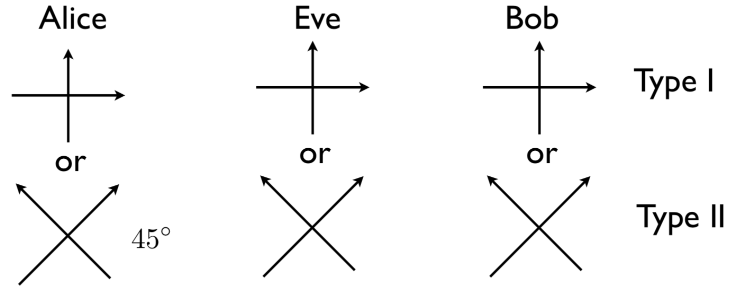
The idea of key distribution: random encoding

Quantum key distribution: BB84 Charles Bennett and Grilles Brassard

Alice prepares $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$.

Quantum Cryptography

The BB84 protocol:



Result analysis:

		1	2	3	4	5	6	7	8	9	⋯
Alice	Type	I	II	II	II	I	I	II	I	II	
	Status	0	1	0	1	1	0	1	0	0	
Bob	M Type	II	II	II	I	I	II	I	I	I	
	Outcome	1	1	0	0	1	0	0	0	0	

Quantum Cryptography

Another protocol with entanglement

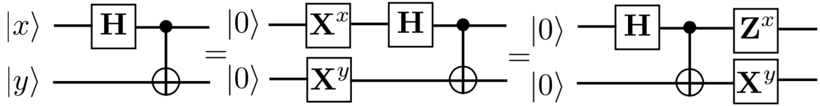
$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Notice that

$$\begin{aligned}
(\mathbf{H} \otimes \mathbf{H})|\Psi\rangle &= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \\
&= \frac{1}{2}\left((|0\rangle + |1\rangle)(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\right) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Psi\rangle.
\end{aligned}$$

Bell States

$$
\begin{aligned}
|\psi_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\psi_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\psi_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}
$$



Quantum Dense Coding

Alice   Bob

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \rightarrow \quad \text{one bit}$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\mathbf{I}_a|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad \mathbf{H}_a\mathbf{CNOT}_{ab}\mathbf{I}_a|\psi_{00}\rangle = |00\rangle$$

$$\mathbf{X}_a|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad \mathbf{H}_a\mathbf{CNOT}_{ab}\mathbf{X}_a|\psi_{00}\rangle = |01\rangle$$

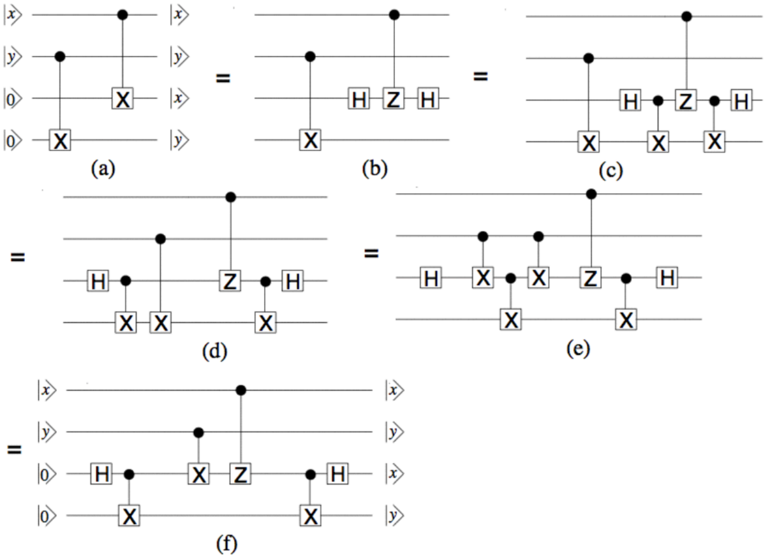
$$\mathbf{Z}_a|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad \mathbf{H}_a\mathbf{CNOT}_{ab}\mathbf{Z}_a|\psi_{00}\rangle = |10\rangle$$

$$\mathbf{Z}_a\mathbf{X}_a|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad \mathbf{H}_a\mathbf{CNOT}_{ab}\mathbf{Z}_a\mathbf{X}_a|\psi_{00}\rangle = |11\rangle$$

two bits

Quantum Dense Coding

A circuit-theoretical derivation of quantum dense coding protocol



Quantum Teleportation

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle & \rightarrow & |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \end{array}$$

Shared entanglement

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$(\alpha|0\rangle)_a + \beta|1\rangle_a)\frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) \xrightarrow{\mathbf{CNOT}_{12}}$$

$$\alpha|0\rangle_a\frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) + \beta|1\rangle_a\frac{1}{\sqrt{2}}(|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b)$$

$$\xrightarrow{\mathbf{H}\otimes\mathbf{H}} \alpha\frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a)\frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)$$

$$+\beta\frac{1}{\sqrt{2}}(|0\rangle_a - |1\rangle_a)\frac{1}{\sqrt{2}}(|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b)$$

Quantum Teleportation

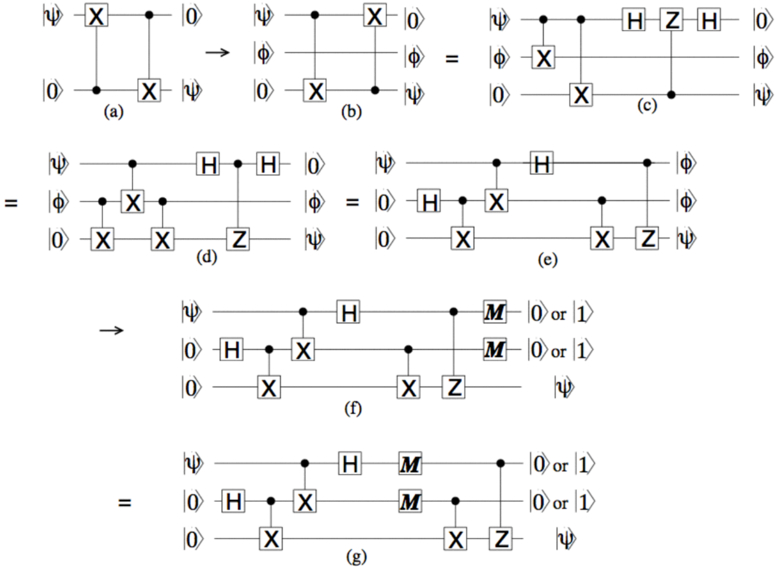
$$\begin{aligned} &= \frac{1}{2}|0\rangle_a|0\rangle_a(\alpha|0\rangle_b + \beta|1\rangle_b) + \frac{1}{2}|0\rangle_a|1\rangle_a(\alpha|1\rangle_b + \beta|0\rangle_b) \\ &+ \frac{1}{2}|1\rangle_a|0\rangle_a(\alpha|0\rangle_b - \beta|1\rangle_b) + \frac{1}{2}|1\rangle_a|1\rangle_a(\alpha|1\rangle_b - \beta|0\rangle_b) \end{aligned}$$

To summarize

Alice	Bob	
00	$\alpha\|0\rangle_b + \beta\|1\rangle_b$	**I**
01	$\alpha\|1\rangle_b + \beta\|0\rangle_b$	**X**
10	$\alpha\|0\rangle_b - \beta\|1\rangle_b$	**Z**
11	$\alpha\|1\rangle_b - \beta\|0\rangle_b$	**ZX**

Quantum Teleportation

A circuit-theoretical derivation of quantum teleportation protocol



Group: A Mathematical Structure

A group is a set G with an operation $\cdot$ satisfying for any

$$a \in G,\ b \in G, c \in G$$

- Closure: $a \cdot b \in G$
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Identity element: $1 \cdot a = a \cdot 1 = a$
- Inverse: $a \cdot b = b \cdot a = 1,\ b = a^{-1}$

Examples:

- Real number without 0 under the usual multiplication
- All invertible matrices under the usual matrix multiplication
- All unitary matrices under the usual matrix multiplication

The Pauli group $\mathcal{P}$

$$\sigma_0 = \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_3 = \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_4 = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$\mathcal{P} = \{\pm i\mathbf{I}, \pm i\mathbf{X}, \pm i\mathbf{Y}, \pm i\mathbf{Z}, \pm\mathbf{I}, \pm\mathbf{X}, \pm\mathbf{Y}, \pm\mathbf{Z}\}.$$

Group Generators

$$\{\mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$$

$$\{\mathbf{X}, \mathbf{Z}, i\mathbf{I}\}$$

n-qubit Pauli Group $\mathcal{P}_n$

$$\{\mathbf{X}_i, \mathbf{Z}_i, i\mathbf{I}\}$$

The Clifford Group

The automorphism group of the Pauli group:
take Pauli group element to Pauli group element

Hadamard

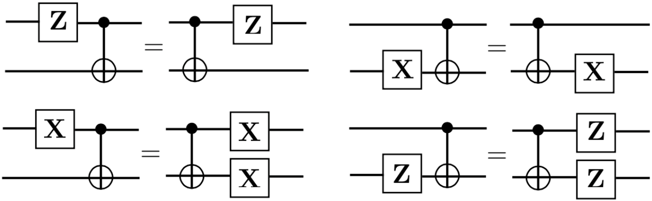
$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Phase

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

Single qubit Clifford group Cl

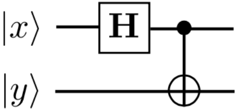
The Controlled-Not gate

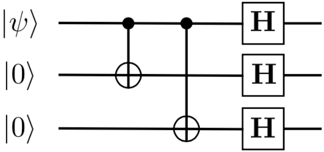


n-qubit Clifford group Cl_n

Generators $\{\mathbf{H}, \mathbf{P}, \mathbf{CNOT}\}$

Applications:





Fault-tolerance

The 7-qubit code

$$|0_L\rangle = (\mathbf{I}+\mathbf{M}_1)(\mathbf{I}+\mathbf{M}_2)(\mathbf{I}+\mathbf{M}_3)|0\rangle_7$$
$$|1_L\rangle = (\mathbf{I}+\mathbf{M}_1)(\mathbf{I}+\mathbf{M}_2)(\mathbf{I}+\mathbf{M}_3)\mathbf{X}_L|0\rangle_7$$

Syndrome Measurements

$$\begin{aligned}\mathbf{M}_1 &= \mathbf{X}_1\mathbf{X}_2\mathbf{X}_6\mathbf{X}_7 & \mathbf{N}_1 &= \mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_6\mathbf{Z}_7\\ \mathbf{M}_2 &= \mathbf{X}_2\mathbf{X}_3\mathbf{X}_5\mathbf{X}_6 & \mathbf{N}_2 &= \mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_5\mathbf{Z}_6\\ \mathbf{M}_3 &= \mathbf{X}_4\mathbf{X}_5\mathbf{X}_6\mathbf{X}_7 & \mathbf{N}_3 &= \mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6\mathbf{Z}_7\end{aligned}$$

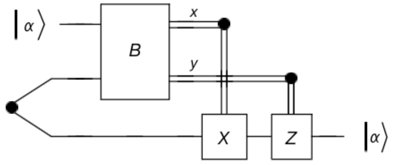
Logical operations

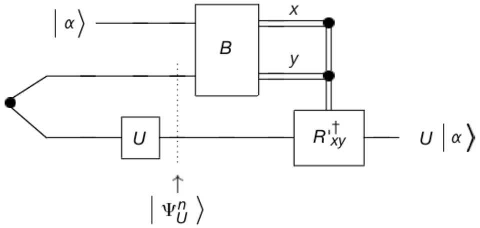
$$\begin{aligned}\mathbf{X}_L &= \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6\mathbf{X}_7\\ \mathbf{Z}_L &= \mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6\mathbf{Z}_7\\ \mathbf{H}_L &= \mathbf{H}_1\mathbf{H}_2\mathbf{H}_3\mathbf{H}_4\mathbf{H}_5\mathbf{H}_6\mathbf{H}_7\\ \mathbf{CNOT}_L &= \mathbf{C}_{1,8}\mathbf{C}_{2,9}\mathbf{C}_{3,10}\mathbf{C}_{4,11}\mathbf{C}_{5,12}\mathbf{C}_{6,13}\mathbf{C}_{7,14}\end{aligned}$$

Universality: Clifford + Any Non-Clifford

Gate teleportation

Reading: *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations.* Daniel Gottesman and Isaac L. Chuang, Nature 402, 390-393(1999).

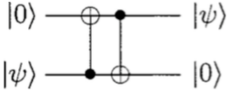


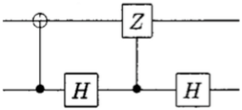


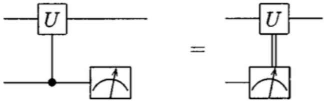
One-bit teleportation

Reading: *Methodology for quantum logic gate construction.* Xinlan Zhou, Debbie W. Leung and Isaac L. Chuang, PRA 62, 052316 (2000)

Some basic properties

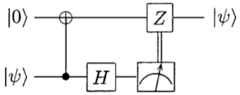




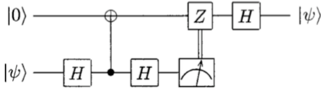


Z and X teleportation

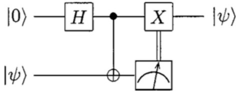
The **Z** teleportation



The Hadamard transform

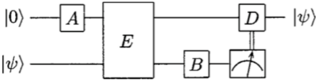


The **X** teleportation

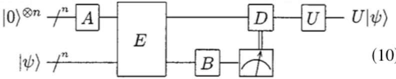


Fault-tolerant gates

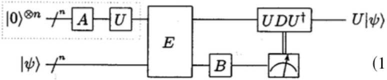
The one-bit teleportation in general



Fault-tolerant gates



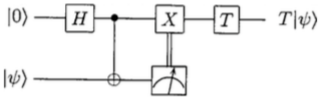
(10)

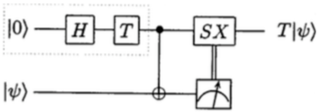


(11)

Example: the $\pi/8$ gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$





$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$