QIC Cheat Sheet

Quantum postulates - States

1. Representation of States

(a) Pure unentangled: $|\psi\rangle \in \mathcal{H}, \langle\psi|\psi\rangle = 1, |\psi\rangle = \bigotimes_i |\phi_i\rangle$

(b) Pure entangled: $|\psi\rangle \in \mathcal{H}, \langle\psi|\psi\rangle = 1, |\psi\rangle \neq \bigotimes_i |\phi_i\rangle$

(c) Mixed: $\rho \in \mathcal{B}_{sa}(\mathcal{H}), \mathrm{Tr}[\rho] = 1, \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

2. Bloch-Sphere Representation

(a) Pauli matrices:

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

$\vec{\sigma} = (X, Y, Z)$

(b) Bloch vector:

$$\begin{aligned} \vec{r} &:= (\mathrm{Tr}[X\rho], \mathrm{Tr}[Y\rho], \mathrm{Tr}[Z\rho]) \\ &= (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) (\text{for pure states}) \end{aligned}$$

Matrix form: $\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) = \frac{1}{2}(I + r_x X + r_y Y + r_z Z)$

Boundary: $||\vec{r}|| = 1$(only for qubits)

Inner product: $|\langle\psi_1|\psi_2\rangle|^2 = \frac{1}{2}(1 + \vec{r_1}\cdot\vec{r_2})$

Orthogonality: $|\psi_1\rangle \perp |\psi_2\rangle$ iff $\vec{r_1} = -\vec{r_2}$(only for qubits)

Quantum postulates - Composition

1. Product state: $\Rightarrow \mathcal{H}_A \otimes \mathcal{H}_B, |\psi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B$

2. Schmidt decomposition:

$\forall|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B, \exists$ONB $\{|\alpha_i\rangle\}_{i=1}^d, \{|\beta_i\rangle\}_{i=1}^d$ s.t.:

$$|\psi\rangle = \sum_{i=1}^d \lambda_i |\alpha_i\rangle|\beta_i\rangle$$

$d = \min(\dim\mathcal{H}_A, \dim\mathcal{H}_B)$, λ_i: Schmidt coefficient

Quantum postulates - Evolution

1. Closed quantum system: Unitary matrices U:

$UU^\dagger = U^\dagger U = I \Rightarrow$ reversible

2. Open quantum system: CPTP matrices Λ:

$\Lambda > 0 \ \wedge \ \mathrm{Tr}[\Lambda M] = \mathrm{Tr}[M] \ \forall M$

3. Rotations: $(A^2 = I \Rightarrow e^{i\theta A} = \cos\theta + i\sin\theta A)$

$$R_x(\phi) := e^{-i\frac{\phi}{2}X} = \begin{bmatrix} \cos(\frac{\phi}{2}) & -i\sin(\frac{\phi}{2}) \\ -i\sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix}$$

$$R_y(\phi) := e^{-i\frac{\phi}{2}Y} = \begin{bmatrix} \cos(\frac{\phi}{2}) & \sin(\frac{\phi}{2}) \\ \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix}$$

$$R_z(\phi) := e^{-i\frac{\phi}{2}Z} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

$$R_{\hat{n}}(\phi) := e^{-i\frac{\phi}{2}\hat{n}\cdot\vec{\sigma}}$$

Quantum postulates - Measurement

1. Projective measurement(PVM) $\{P_m\}$

(a) Completeness relation: $\sum_m P_m = \sum_m |\psi_m\rangle\langle\psi_m| = I$

(b) The Born rule: $\Pr_\psi(\text{outcome } m) = \langle\psi|P_m|\psi\rangle$

(c) Post-measurement: $|\psi'\rangle = \frac{P_m|\psi\rangle}{||P_m|\psi\rangle||} = \frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}}$

2. General measurement(POVM) $\{\Pi_m\}$: $\Pi_m \geq 0$

(a) Completeness relation: $\sum_m \Pi_m = I$

(b) The Born rule: $\Pr_\rho(\text{outcome } m) = \mathrm{Tr}[\rho\Pi_m]$

(c) Post-measurement: $|\psi'\rangle = \frac{\sqrt{\Pi_m}\rho\sqrt{\Pi_m}}{\mathrm{Tr}[\rho\Pi_m]}$

No-go Theorems

1. No-signaling: $\sum_a \Pr(a, b|x, y) = \Pr(b|x, y) = \Pr(b|y)$

2. No-cloning: $\forall|\psi_0\rangle \not\perp |\psi_1\rangle, \nexists U$ s.t. $|\psi_i\rangle|0\rangle \xrightarrow{U} |\psi_i\rangle|\psi_i\rangle$

3. No-deleting: $\forall|\psi_0\rangle \not\perp |\psi_1\rangle, \nexists U$ s.t. $|\psi_i\rangle|\psi_i\rangle \xrightarrow{U} |\psi_i\rangle|0\rangle$

4. No-perfect-discrimination:

$$\forall|\psi_0\rangle, |\psi_1\rangle, P_s^* = \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}$$

Resource Inequality

1 qubit $\geq$ 1 cbit	N cbit $\ngeq$ 1 ebit ($\forall N \geq 1$)
1 qubit $\ngeq$ N cbit ($\forall N > 1$)	N cbit $\ngeq$ 1 qubit ($\forall N \geq 1$)
N ebit $\ngeq$ 1 cbit ($\forall N \geq 1$)	N ebit $\ngeq$ 1 qubit ($\forall N \geq 1$)
1 cbit $\ngeq$ N cbit ($\forall N > 1$)	1 ebit $\ngeq$ N ebit ($\forall N > 1$)

M cbits + 1 qubit $\ngeq$ N qubits ($\forall N > 1, M \geq 1$)

M ebits + 1 qubit $\ngeq$ N qubits ($\forall N > 1, M \geq 1$)

Basic Protocols

1. Entangle distribution (1 qubit $\geq$ 1 ebit)

$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CX} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$

$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_{A'} + |1\rangle_A|1\rangle_{A'}) \xrightarrow{[qq]} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$.

2. Quantum dense coding (1 qubit + 1 ebit $\geq$ 2 cbits)

$\sigma_0 = I, \sigma_1 = X, \sigma_2 = Z, \sigma_3 = XZ = -iY$

$|\Phi^+\rangle_{AB} \xrightarrow{\sigma_m\otimes I} \xrightarrow{[qq]} \{{}_0|\Phi^+\rangle, {}_1|\Psi^+\rangle, {}_2|\Phi^-\rangle, {}_3|\Psi^-\rangle\}_{B'B}$

Bell measurement:

$\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\} \xrightarrow{(H\otimes I)CX} \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

3. Quantum teleportation (2 cbits + 1 ebit $\geq$ 1 qubit)

$|\psi\rangle_A|\Phi^+\rangle_{A'B} \xrightarrow{((H\otimes I)CX)\otimes I} \frac{1}{2}\sum_{i,j}|ij\rangle_{AA'}(X^jZ^i|\psi\rangle_B)$

A gets "ij"$\Rightarrow |ij\rangle_{AA'}(X^jZ^i|\psi\rangle_B) \xrightarrow{I\otimes Z^iX^j} |ij\rangle_{AA'} \otimes |\psi\rangle_B$

BB84 QKD

Mutually unbiased bases(MUB):

$\mathcal{B}_0 : \{|\psi_{00}\rangle = |0\rangle, |\psi_{10}\rangle = |1\rangle\}$

$\mathcal{B}_1 : \{|\psi_{01}\rangle = |+\rangle, |\psi_{11}\rangle = |-\rangle\}$

1a. A: Random bit string $x = x_1 \ldots x_m, y = y_1 \ldots y_m$

1b. A sends $\bigotimes_{i=1}^m |\psi_{x_iy_i}\rangle$(x: message, y: basis) to B

2a. B: Random bit string $y' = y_1 \ldots y_m$

2b. B measures to $\mathcal{B}_{y_i}$ and get x'

3. A and B publicly compare their basis choice y, y',then B discard x'_i measured with the wrong basis $y_i \neq y'_i$.

4. A and B compare ramdom sample of x, x', say $\tilde{x}, \tilde{x}'$, if BER is too large, abort communication.

5. A and B can use BER to estimate maximum information obtained by Eve.

Oracle Model

Oracle: $f : \{0,1\}^n \to \{0,1\}^m$

Quantum oracle:

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle, \forall x \in \{0,1\}^n, \forall y \in \{0,1\}^m$

Quantum parallelism:

$$|0\rangle^{\otimes n}|0\rangle \xrightarrow{H^{\otimes n}\otimes I} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}^n}|x\rangle|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}^n}|x\rangle|f(x)\rangle$$

Deutsch-Jozsa Algorithm

Problem: Determine whether f is constant or balanced.

(i) Constant function: $f(x) = 0, \forall x$ or $f(x) = 1, \forall x$

(ii) Balanced function: $f(x) = 0$ or 1 with 50%-50%

$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H^{\otimes(n+1)}} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}^n}|x\rangle|-\rangle$

$\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}|x\rangle|-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}(-1)^{f(x)}|x\rangle|-\rangle := |f\rangle$

If f is constant: $|f\rangle = \pm|0\rangle^{\otimes n}$, measure Z gets all-zero

If f is balanced: $\langle f|H^{\otimes n}|0\rangle^{\otimes n} = 0 \Rightarrow H^{\otimes n}|f\rangle \perp |0\rangle^{\otimes n}$

$\Rightarrow$ measure Z gets non-zero string

Bernstein-Vazirani algorithm

Problem: $f_a(x) = x \cdot a = \bigoplus_{i=1}^n x_ia_i$, find bit string a.

Note that $H_n|a\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_2^n}(-1)^{a\cdot y}|y\rangle$ and $H_n^2 = I$

$|0\rangle^{\otimes n}|1\rangle \xrightarrow{H^{\otimes(n+1)}} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}^n}|x\rangle|-\rangle$

$\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}^n}|x\rangle|-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}(-1)^{a\cdot x}|x\rangle|-\rangle$

$\frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}(-1)^{a\cdot x}|x\rangle|-\rangle \xrightarrow{H_n\otimes I} |a\rangle|-\rangle$, measure gets a.

Grover's Search Algorithm

Problem: Find the unique x such that $f(x)=1$.
Reflection operator: $I_{|\phi\rangle} := I - 2|\phi\rangle\langle\phi|$
(Note that $UI_{|\phi\rangle}U^\dagger = I_{U|\phi\rangle}$)
Grover diffusion operator: Rotate $2\angle(|\psi_0\rangle, |x_0^\perp\rangle)$
$\mathcal{G} := -H_n I_{|0\rangle} H_n I_{|x_0\rangle} = I_{|\psi_0^\perp\rangle} I_{|x_0\rangle}$
$\Rightarrow$ Reflect about $|x_0^\perp\rangle$ then the mean $|\psi_0\rangle = H_n|0\rangle$
$I_{|x_0\rangle}|x\rangle = (-1)^{f(x)}|x\rangle \Rightarrow$ using phase kickback of U_f

Quantum Fourier Transform(QFT)

$Q_N : |x\rangle \to \frac{1}{\sqrt{N}}\sum_{y\in\mathbb{Z}_N}\omega^{xy}|y\rangle, \omega = e^{\frac{2\pi i}{N}}$ (freq.-time)
$Q_N^{-1} : |y\rangle \to \frac{1}{\sqrt{N}}\sum_{x\in\mathbb{Z}_N}\omega^{-xy}|x\rangle, \omega = e^{\frac{2\pi i}{N}}$ (time-freq.)
$[Q_N]_{jk} = \frac{1}{\sqrt{N}}\omega^{jk}, [Q_N^{-1}]_{jk} = \frac{1}{\sqrt{N}}\omega^{-jk}, Q_N$ is unitary.

Phase Estimation Algorithm (With Promise)

Problem: Given eigenvector $|\psi\rangle, U|\psi\rangle = e^{2\pi i\phi}$, find ϕ.
Promise: $\exists x = N\phi \in \mathbb{Z}_N, N = 2^n$
Controlled-U gate c-U: $|y\rangle|\psi\rangle \to |y\rangle U^y|\psi\rangle$
$|0\rangle^{\otimes n}|\psi\rangle \overset{Q_N\otimes I}{\longrightarrow} \frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N}|y\rangle|\psi\rangle$
$\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N}|y\rangle|\psi\rangle \overset{\text{c-}U}{\longrightarrow} \frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N} e^{2\pi i\frac{x}{N}y}|y\rangle|\psi\rangle$
$\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N} e^{2\pi i\frac{x}{N}y}|y\rangle|\psi\rangle \overset{Q_N^{-1}\otimes I}{\longrightarrow} |x\rangle|\psi\rangle$, measure gets x
Implementation of c-U for $y \in \mathbb{Z}_{2^n}$: $y = (y_1y_2\dots y_n)_2$
c-$U = \prod_{k=1}^n (U^{2^{n-k}})^{y_k} \Rightarrow$ splited to several c-gates.

Period Finding Algorithm

Problem: $f:\mathbb{Z}_N \to Y, f(x+r) = f(x)$, find r. $(r|N)$
Oracle: $\frac{1}{\sqrt{N}}\sum_{x\in\mathbb{Z}_N}|x\rangle \Rightarrow |f\rangle := \frac{1}{\sqrt{N}}\sum_{x\in\mathbb{Z}_N}|x\rangle|f(x)\rangle$
Measuring output register gets outcome y_0, and the input register collapses to $|\text{per}\rangle$:
$|\text{per}\rangle = \frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|x_0 + jr\rangle, m = \frac{N}{r}$ (imp. train $T_0 = r$)
$Q_N|\text{per}\rangle = \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}\omega^{x_0 lm}|lm\rangle$ (imp. train $T_0 = m$)
Measure $Q_N|\text{per}\rangle$ gets $c = l_0 m, 0 \le l_0 \le r-1$
$\frac{c}{N} = \frac{l_0}{r} \Rightarrow$ use continued fraction to read off r if $l_0 \not| r$. If $l_0|r \Rightarrow$ check $f(x) = f(x+r)$, if not, repeat algorithm.

Phase Estimation Algorithm (Arbitrary Phase)

Problem: Estimate ϕ with $\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N} e^{2\pi i\phi y}|y\rangle|\psi\rangle$
$\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_N} e^{2\pi i\phi y}|y\rangle|\psi\rangle \overset{Q_N^{-1}\otimes I}{\longrightarrow} |x\rangle|\psi\rangle \Rightarrow \hat{x}$
$\Pr(|\phi - \frac{\hat{x}}{N}| \le \frac{1}{2N}) \ge \frac{4}{\pi^2}$. $\Rightarrow$ constant rate to get best $\hat{x}$.

Period Finding Algorithm (With t Qubits)

Problem: Estimate r where:
$|\text{per}\rangle = \frac{1}{\sqrt{m_{x_0}}}\sum_{j:0\le x_0+jr<2^t-1}|x_0 + jr\rangle$
$m_{x_0} = \lfloor\frac{2^t-b}{r}\rfloor$ or $\lfloor\frac{2^t-b}{r}\rfloor + 1$ (unknown)
Measure $Q_{2^t}|\text{per}\rangle$ will get y, $\Pr\left(\left|\frac{y}{2^t} - \frac{l}{r}\right| < \frac{1}{2^{t+1}}\right) \ge \frac{4}{\pi^2 r}$
To find unique $\frac{l}{r}$, choose $\min t$ s.t. $2^t \ge N^2$ $(r<N)$
And $\frac{l}{r}$ is a convergent of the continued fraction of $\frac{y}{2^t}$

Shor's Factoring Algorithm

Euler's thm: If a and N are coprime:
$\exists \min r = \text{ord}_N(a) \in (1, N)$ s.t. $a^r = 1 \mod N$
Where r is the period of sequence $\langle a^k \mod N\rangle_{k\in\mathbb{N}}$
Find factors using order:
Suppose $2|r$, $a^r - 1 = (a^{r/2}-1)(a^{r/2}+1) = 0 \mod N$
If N doesn't divide $(a^{r/2}+1)$, then N partly divide into $(a^{r/2}+1)$ and $(a^{r/2}-1)$, $\Pr(2|r \wedge a^{r/2} \ne -1 \mod N) \ge \frac{1}{2}$
$\Rightarrow N = \gcd(a^{r/2}+1, N)\gcd(a^{r/2}-1, N)$
Reduction of problem:
Integer fac. $\overset{O(\log N)}{\rightarrow}$ Splitting odd non-prime int.
$\rightarrow$ Finding $r = \text{ord}_N(a) \rightarrow$ Sampling estimate $\frac{k}{r}$
Steps:
1. If $2|N$, output 2 and stop.
2. Use AKS primality test, check if N is prime-powered
3. Randomly choose $1 \le a \le N$, check $\gcd(a, N)$
4. If $\gcd(a,N) = 1$, find $r = \text{ord}_N(a)$ (period finding*)
5a. If r is odd, go back to 3.
5b. If r is even, compute $p = \gcd(a^{r/2}+1, N)$
5c. If $p = 1$ or N, go back to 3., otherwise output p

***Steps of period finding:**
1. Create states $\sum_{x\in\mathbb{Z}_{2^t}}\frac{1}{\sqrt{2^t}}|x\rangle|a^x \mod N\rangle$
2. Measure output register:
$|\text{per}\rangle = \frac{1}{\sqrt{m_{x_0}}}\sum_{j:0\le x_0+jr<2^t-1}|x_0 + jr\rangle$
3. Measuring $Q_{2^t}|\text{per}\rangle$ gets $y \in \mathbb{Z}_{2^t}$
4. Use continued fraction alg. to find $r < N$
5. Check if $a^r = 1 \mod N$. If not, go back to 1.
(Gives desired r with prob. $O(1)$ in $O(\log\log N)$ times)

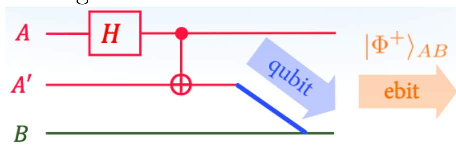
Complexity: $n = \log_2 N$
Quantum part:
(*1): H gates $\Rightarrow O(n)$, $f(x) \Rightarrow O(n^2\log n\log\log n)$
(*2): 1-qubit measurement $\Rightarrow O(n)$, QFT $\Rightarrow O(n^2)$
(4): Running $O(\log n)$ times gives r with constant prob.
$O(\log n)\cdot(O(n) + O(n^2\log n\log\log n) + O(n^2) + O(n))$
$= O(n^2\log^2 n\log\log n)$
Classic part: (*4): Continued fraction $\Rightarrow O(n^3)$
Total: $O(n^2\log^2 n\log\log n) + O(n^3) = O(n^3) = O(\log^3 N)$

Nonlocal Games

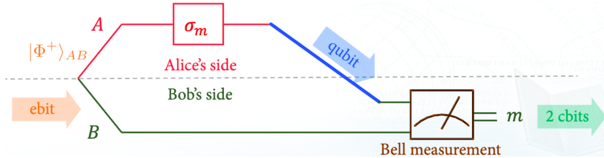
The CHSH game:
Questions: $x \in \{0,1\}$ to Alice, $y \in \{0,1\}$ to Bob.
Answers: Alice $\Rightarrow x \in \{0,1\}$, Bob $\Rightarrow y \in \{0,1\}$.
Winning rule: $x \wedge y = a \oplus b$
Winning prob.: $\Pr(\text{Win}) = \mathbb{E}_{XYAB}[1_{X\wedge Y = A\oplus B}]$
$= \frac{1}{4}\sum_{x,y,a,b}1_{x\wedge y = a\oplus b}p_{AB|XY}(a,b|x,y)$
Classical strategies: $\max\Pr(\text{Win}) = 75\%$
Quantum strategies:
$\{|\alpha_0(\theta)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \alpha_1(\theta) = -\sin\theta|0\rangle + \cos\theta|1\rangle\}$
1. Before game, Alice and Bob share an EPR pair $|\Phi^+\rangle$
2. Alice measure with $\theta = 0$ if $x = 0$, $\theta = \frac{\pi}{4}$ if $x = 1$
3. Bob measure with $\theta = \frac{\pi}{8}$ if $y = 0$, $\theta = -\frac{\pi}{8}$ if $y = 1$
For $(x,y) = (0,0),(0,1),(1,0)$, $\Pr(a\oplus b = 0) = \cos^2(\frac{\pi}{8})$
For $(x,y) = (1,1)$, $\Pr(a\oplus b = 1) = \cos^2(\frac{\pi}{8})$
$\Rightarrow$ Winning prob. is $\cos^2(\frac{\pi}{8}) \approx 85\%$
The CHSH inequality:
$\langle A_xB_y\rangle := \mathbb{E}_{P_{AB|X=x,Y=y}}[(-1)^A(-1)^B] =: \langle\phi|A_x\otimes B_y|y\rangle$
Score function $S := \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle$
$S_{\text{classical}} \le 2$, is violated by $S^*_{\text{quantum}} = 2\sqrt{2}$

Quantum Circuits

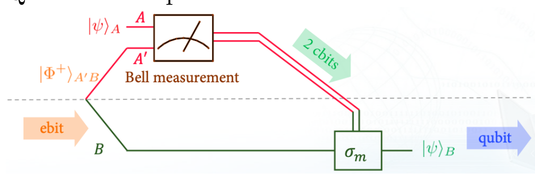
Entangle distribution:



Quantum dense coding:



Quantum teleportation:



QFT: