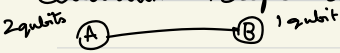
Quantum Teleportation



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ — other of Bell pair

One of Bell pair
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|\psi_{init}\rangle = \frac{1}{2}(\alpha(|000\rangle + |011\rangle) + \beta(|010\rangle + |111\rangle))$

If instead, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$(\alpha|0\rangle + \beta|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$

$= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle)$

No Cloning Theorem:

No unitary U exists s.t.
$U(|\psi 0\rangle) = |\psi\psi\rangle$

Pf: $U(|a0\rangle) = |aa\rangle$
$U(|b0\rangle) = |bb\rangle$
$c = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$

$U(|c0\rangle) = |cc\rangle = \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle)$ by defn

$= U\left(\left(\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)\right) \otimes 0\right)$

$= U\left(\frac{1}{\sqrt{2}}(|a0\rangle + |b0\rangle)\right)$

$= \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$

Teleportation:

① Apply CNOT gate @ A

$|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$

After ①,

$|\psi\rangle = \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle)$

② Apply Hadamard gate to first qubit

$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

After ②,

$|\psi\rangle = \frac{\alpha}{2}(|000\rangle + |100\rangle + |011\rangle + |111\rangle)$

$+ \frac{\beta}{2}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)$

③ A measures her 2 qubits to obtain 2 bits output $(r_0 r_1)$

After ③,

$r_0 r_1$	B's qubit
00	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle$

B's code:

$r_0 r_1$	Gate to apply
00	$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

x_0 x_1	Gate & Apply
01	$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
10	$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
11	$Y = ZX$

On measurement, we get

$\sum |i, \beta\rangle$

↳ in AP, with common diff $= r$

Shors Algorithm for PolyTime Integer Factoring

① Reduce IF to non trivial square roots of $1 \pmod N$

$x^2 \equiv 1 \pmod N$

ex: $4^2 \equiv 1 \pmod{15}$

If $N \mid x^2 - 1$

$N \mid (x-1)(x+1)$

$x - 1 < N$, $x + 1 < N$

$\Rightarrow gcd(x+1, N) = p$

② Reduce sqrt $(1) \bmod N$ to finding order of random $x \pmod N$

Order $(x) = r \Rightarrow x^r \equiv 1 \pmod N$

If r is even, then $x^{r/2}$ is a sqrt $(1) \bmod N$

③ Setup a $|\psi\rangle$ periodic non zero amplitude where period $= r =$ order (x)

$f(a) = x^a \bmod N$ periodic fn

period $= r =$ order (x)

$U_b \left(\sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |i, 0\rangle \right) \rightarrow \sum_{i=0}^{N-1} \frac{1}{\sqrt{N}} |i, f(i)\rangle$

④ QFT : $O(\log^3 N)$

FFT (n) < FFT $(n/2)$ odd, FFT $(n/2)$ even

QFT : uses H gate on LSB for superposition of odd & even

QFT (n) - QFT $(n/2)$ + ...

QFT (M) where $M > N$ & M is an exact power of 2. If M/r is not an integer, use continued fraction