Ex. 3

$$|0\rangle|\psi_1\rangle|\psi_2\rangle \xrightarrow{H'} |+\rangle|\psi_1\rangle|\psi_2\rangle$$

$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} |\psi_1\rangle|\psi_2\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_1\rangle|\psi_2\rangle \right)$$

$$\xrightarrow{C\text{-}SWAP} \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_2\rangle|\psi_1\rangle \right)$$

$$\xrightarrow{H'} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} |\psi_1\rangle|\psi_2\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}} |\psi_2\rangle|\psi_1\rangle \right)$$

$$= \frac{1}{2}\left((|0\rangle+|1\rangle)|\psi_1\rangle|\psi_2\rangle + (|0\rangle-|1\rangle)|\psi_2\rangle|\psi_1\rangle \right)$$

$$= \frac{1}{2}\Big(|0\rangle\left(|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle\right) +$$
$$|1\rangle\left(|\psi_1\rangle|\psi_2\rangle - |\psi_2\rangle|\psi_1\rangle\right)\Big)$$

$tr(F_1 |\psi_{final}\rangle)$

$M\{F_0, F_1\}$, $F_0 = |0\rangle\langle 0| \otimes I \otimes I$, $F_1 = |1\rangle\langle 1| \otimes I \otimes I$

$$\langle \psi_{final} | F_0 | \psi_{final}\rangle = \langle \psi_{final} | 0\rangle\langle 0 | \psi_{final}\rangle$$

$$= \frac{1}{4} \langle \Omega | \Omega \rangle$$

where $|\Omega\rangle = |\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle$

$$\langle \Omega | \Omega \rangle = 2(1 + \langle \psi_1 | \psi_2 \rangle\langle \psi_2 | \psi_1 \rangle)$$
$$= 2(1 + |\langle \psi_1 | \psi_2 \rangle|^2)$$

$\Downarrow$

probability of outputting "0" is $\dfrac{1 + |\langle \psi_1 | \psi_2 \rangle|^2}{2}$

$|\phi\rangle = |\phi_1\rangle|\phi_2\rangle$
$|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$

$\Rightarrow \langle \phi | \psi \rangle = \langle \phi_1 | \psi_1 \rangle \langle \phi_2 | \psi_2 \rangle$

Ex. 4

Alice has a random string $x = (x_1, \dots, x_n)$, n even.
Bob has M. list of $\frac{n}{2}$ disjoint pairs.

Bob outputs (i, j, b), they win iff $(i,j) \in M$
$x_i \oplus x_j = b$

Alice: $|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_{\ell=1}^{n} (-1)^{x_\ell} |\ell\rangle$

Bob: $M = ((i_1, j_1), \dots, (i_{n/2}, j_{n/2}))$

$\Pi = \{\Pi_i\}_{i \in \{1, \dots, n/2\}}$ projective measurement with
$\Pi_k = |i_k\rangle\langle i_k| + |j_k\rangle\langle j_k|$

output: (i, j, b)

1. Size of $|\psi_x\rangle$ can be determine by the number of bits of $|l\rangle$ which is essentially the binary representation of n. $\Rightarrow l|_2$.

which is $\lceil \log_2(n) \rceil$

2. For Π to be a quantum measurement

Since Π is projective measurement, $\forall k$ $\Pi_k \geq 0$

$\sum_k \Pi_k = I$,

because $\sum_k \Pi_k = \sum_{k=1}^{n/2} |i_k\rangle\langle i_k| + |j_k\rangle\langle j_k|$

$= \sum_{i=1}^{n} |i\rangle\langle i|$ becau all terms appears exactly once, either i_k or j_k.

$= I$ because $\{|i\rangle\}_{i\in\{1,\dots,n\}}$ is athonormal basis

3. Probability of outputting $K = \langle \psi_x | \Pi_k | \psi_x \rangle$

$$\Pi_k = |i_k\rangle\langle i_k| + |j_k\rangle\langle j_k|$$

$$|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_{l=1}^{n} (-1)^{x_l} |l\rangle$$

$$= \frac{1}{\sqrt{n}} \Big(\underbrace{(-1)^{i_k}}_{l=i_k} |i_k\rangle + \underbrace{(-1)^{j_k}}_{l=j_k} |j_k\rangle + \sum_{\substack{i=1 \\ i \neq i_k \\ j \neq j_k}}^{n} (-1)^{x_i} |i\rangle \Big)$$

$$|i_k\rangle\langle i_k|\psi_x\rangle = \frac{1}{\sqrt{n}}(-1)^{i_k} |i_k\rangle$$

$$|j_k\rangle\langle j_k|\psi_x\rangle = \frac{1}{\sqrt{n}}(-1)^{j_k} |j_k\rangle$$

$$\Pi_k|\psi_x\rangle = \frac{1}{\sqrt{n}}\left((-1)^{i_k}|i_k\rangle + (-1)^{j_k}|j_k\rangle\right)$$

$$\langle \psi_x | \Pi_k | \psi_x \rangle = \frac{1}{n}\left((-1)^{2i_k} + (-1)^{2j_k}\right)$$

$$= \frac{2}{n}.$$

4. $|\psi_x\rangle = \frac{1}{\sqrt{n/2}} \sum_k |\psi_x^k\rangle$

where " we gather terms in i_k, j_k in $|\psi_x^k\rangle$:

$$|\psi_x^k\rangle = \frac{(-1)^{x_{i_k}}|i_k\rangle + (-1)^{x_{j_k}}|j_k\rangle}{\sqrt{2}}$$

when we get outcome k, the resulting state is $|\psi_x^k\rangle$.

$$\rightarrow = (-1)^{i}\frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^{j+i}|1\rangle\right]$$

$j+i=0 \rightarrow |+\rangle$

$j+i=1 \rightarrow |-\rangle$

so,

if $x_{i_k} \oplus x_{j_k} = 0$

$$|\psi_x^k\rangle = \frac{(-1)^{x_{i_k}}}{\sqrt{2}}\left[|i_k\rangle - |j_k\rangle\right]$$

if $x_{i_k} \oplus x_{j_k} = 1$

$$|\psi_x^k\rangle = \frac{(-1)^{x_{i_k}}}{\sqrt{2}}\left[|i_k\rangle - |j_k\rangle\right]$$

Define $|+_k\rangle = \frac{1}{\sqrt{2}}\left[|i_k\rangle + |j_k\rangle\right]$

$$|-_k\rangle = \frac{1}{\sqrt{2}}\left[|i_k\rangle - |j_k\rangle\right]$$

this is an othonormal basis

Bob can measure $|\psi_x^k\rangle$ in the $\{|+_k\rangle, |-_k\rangle\}$ basis

when $x_{i_k} \oplus x_{j_k} = 0$, he gets $|+_k\rangle$ with probability 1.

In that case he outputs $(i_k, j_k, 0)$

when $x_{i_k} \oplus x_{j_k} = 1$, he gets $|-_k\rangle$ w.p. 1 and

in that case he compute $(i_k, j_k, 1)$

QINTRO-TD5

Ex. 5

Goal: find a lower bound for $P_{success}$

↳ find lower bound for $P_{collision}$

$L = \{l_i\}_{i \in [\![1, 3p]\!]}$

k_{l_i} : point to which l_i belongs

$P[\forall l_j \in [\![p+1, 3p]\!], \forall l_i \in [\![1, p]\!]$
$k_{l_j} \neq k_{l_i}]$ is an lower bound on having no collision

Assume no pairing in $\{l_1, \dots, l_p\}$

let $l_i \in [1, p]$

$$P[k_{l_j} = k_{l_i}] = \frac{\#\left\{\substack{\text{indices } l_j \\ \text{for which} \\ \text{success}}\right\}}{\#\left\{\substack{\text{all options} \\ \text{for } l_j}\right\}} = \frac{1}{n-p}$$

we all got lost ......

modern art - h.C.I

the S - h.C.I