Quantum Computing – Two Applications

Which two?

1. In Communication Complexity: [2].

2. In Cryptography: [1].

Bibliography

References

[1] Mark Adcock and Richard Cleve, "A quantum Goldreich-Levin theorem with cryptographic applications," *STACS 2002*, 323–334.

[2] Harry Buhrman, Richard Cleve, John Watrous and Ronald de Wolf, "Quantum fingerprinting," *PRL*, **87(16)**, 2001.

Communication Complexity

Communication Complexity – Model Description

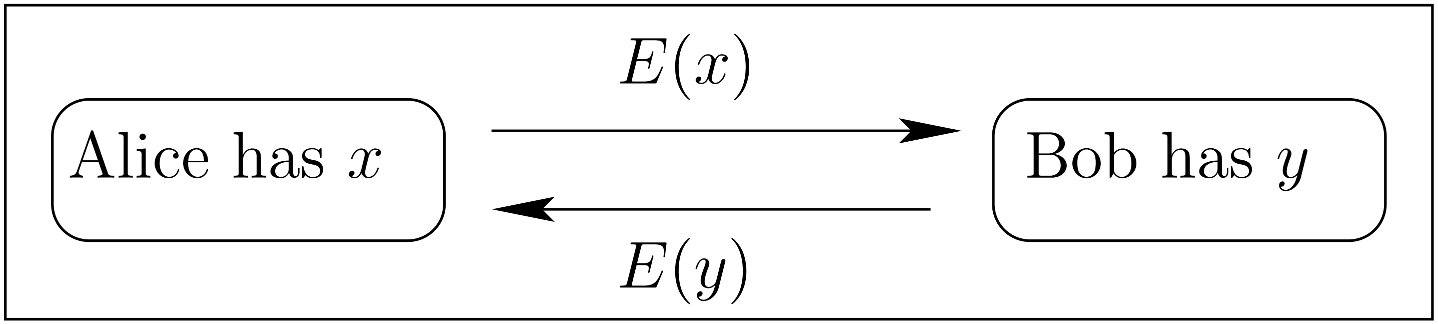


Figure 1: A protocol **P** for computing $\mathbf{f}(x, y)$

Model Description:

- $|x| = |y| = n,\ E(v)$: encoding of $v(= x$ or $y)$.
- $\mathbf{f}(x, y)$: a Boolean predicate of x and y.
  $(\mathbf{f} : \{0,1\}^n \times \{0,1\}^n \longmapsto \{0,1\})$

Communication Complexity – Goal

Goal:

- Design a protocol **P** such that
  - $\mathbf{Pr}[\mathbf{P}(x, y) = \mathbf{f}(x, y)] \geq 1 - \varepsilon$.
    (for $0 \in [0, \frac{1}{2}]$)
  - The length of $E(v)$ is as minimum as possible.

Communication Complexity – Definition

Definition:

- Communication Complexity of **P**:

$$C_{\mathbf{P}} \triangleq \max_{(x,y)}\{E(x), E(y)\} \text{ (of the protocal } \mathbf{P}\text{).}$$

- Communication Complexity of **f**:

$$C(\mathbf{f}) \triangleq \min_{\mathbf{P}} C_{\mathbf{P}}.$$

SMM (Simultaneous Message Model)

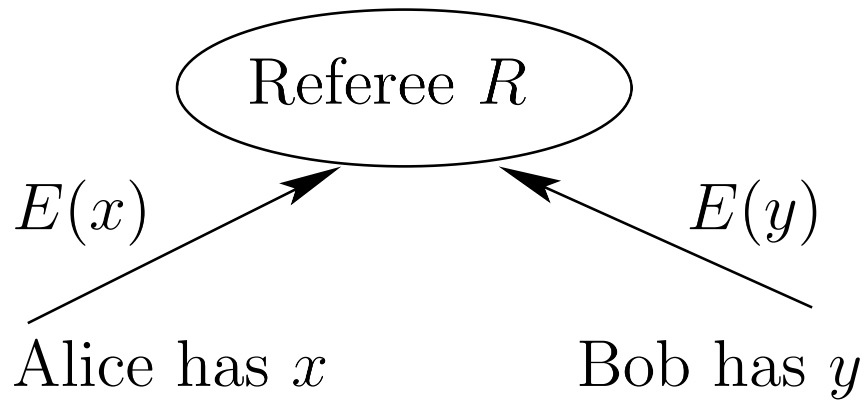


Figure 2: A protocol **P** for computing $\mathbf{f}(x, y)$ in the **SMM**.

- Alice and Bob cannot interact with each other.
- $E(x)$ and $E(y)$ can be sent to the Referee R only.
- Only **one** round to send $E(x)$ and $E(y)$.

EQ_ε(x,y) Problem

- (We only care the protocols in **SMM** hereafter.)
- (We only care $\mathbf{f}(x,y) = \mathsf{EQ}_\varepsilon(x,y)$ hereafter.)
- **Definition**

$$\mathsf{EQ}_\varepsilon(x,y) : \begin{cases} \mathbf{Pr}[\mathsf{EQ}_\varepsilon(x,y) = 1] = 1, & \text{when } x = y; \\ \mathbf{Pr}[\mathsf{EQ}_\varepsilon(x,y) = 0] \geq 1 - \varepsilon, & \text{when } x \neq y. \end{cases} \tag{1}$$

- Amazingly, $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = \Theta(\sqrt{n})$!

Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = O(\sqrt{n})$ – Warmup!

Good code $E(v)$ (**Justesen code**):

- $E : \{0,1\}^n \longmapsto \{0,1\}^{cn}$ for $c > 1$
- $d(\boldsymbol{x}, \boldsymbol{y})$: Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$.

  For $0 \leq \varepsilon \leq \frac{1}{2}$, we have:
  $$\begin{cases} d(E(x), E(y)) = 0, & x = y; \\ d(E(x), E(y)) \geq (1-\varepsilon)cn, & x \neq y. \end{cases} \tag{2}$$

  (Compare with (1)).

Justesen code – construction (1)

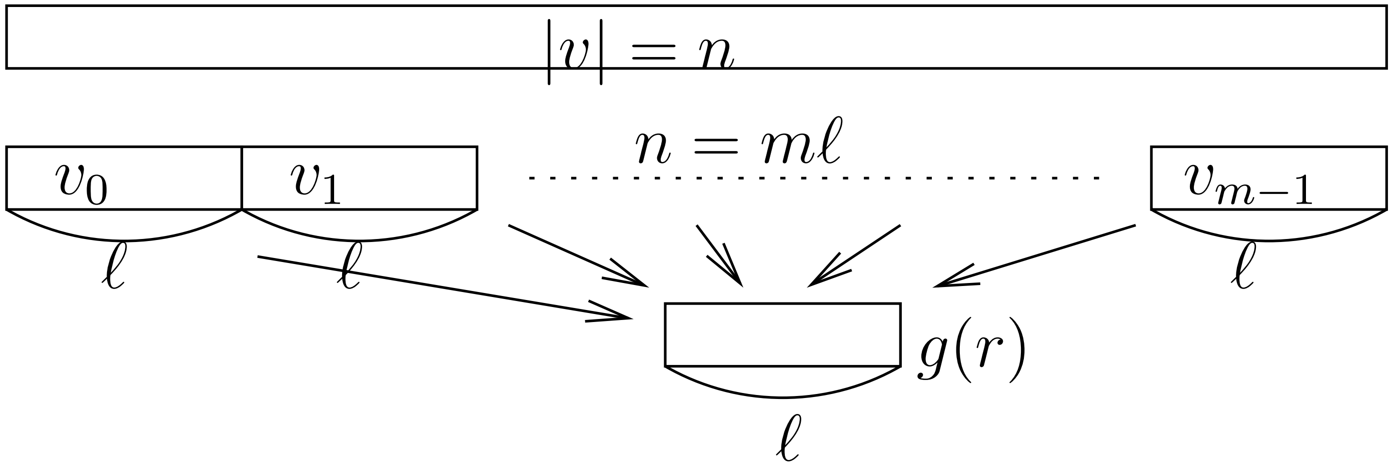
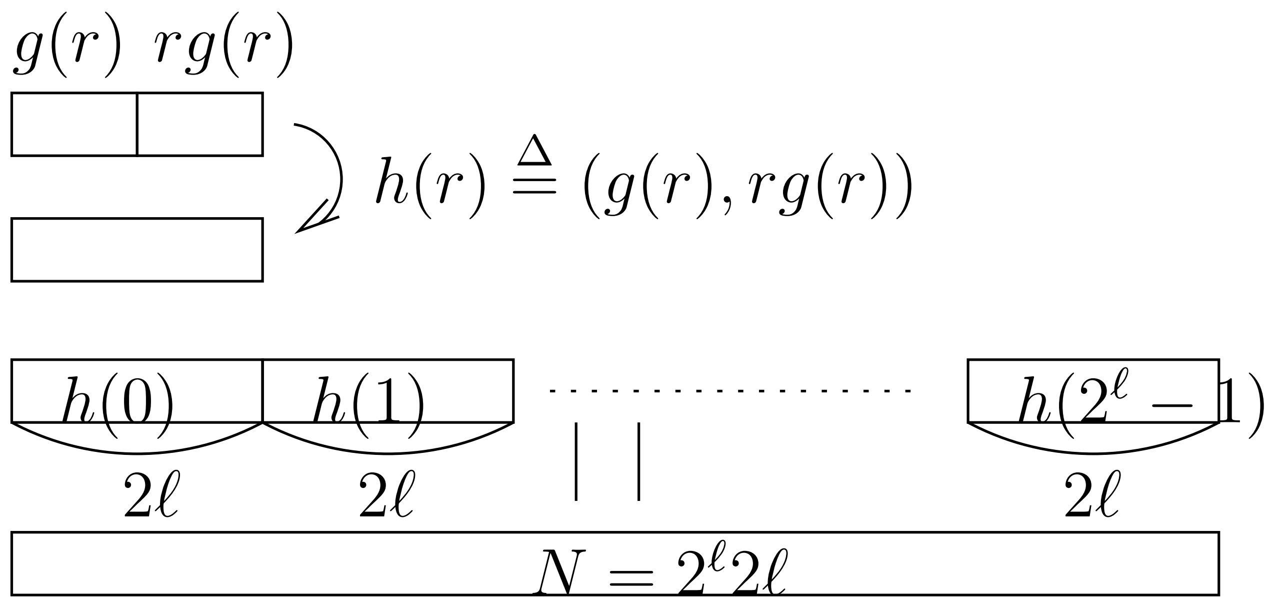


Figure 3: Divide v into m piece of equal length ℓ ($m \leq 2^{\ell-1}$, suggested)

$$g(r) \triangleq \sum_{i=0}^{m-1} v_i r^i \pmod{2^\ell}. \tag{3}$$

Justesen code – construction (2)



Justesen code – construction (3)

- Let $h(r) \triangleq (g(r), rg(r))$, then

$$E(v) \quad \leftarrow \quad \{h(r)\}_{r \in GF(2^\ell)} \leftarrow \{(3), r(3)\}_{r \in GF(2^\ell)} \quad (4)$$

  is a Justesen code of v for $|E(v)| = 2^\ell 2\ell$.

- Analysis of case $m \leq 2^{\ell-1}$:
  - $c = \frac{|E(v)|}{|v|} \geq \frac{2^\ell 2\ell}{m\ell} = 4$
  - Hamming distance: at least $\delta(2^\ell - m)2\ell$.
  - Compare with (2), we have $\varepsilon \geq 1 - \frac{\delta}{2}$ because $\delta(2^\ell - m)2\ell \geq 2\delta m\ell \geq (1-\varepsilon)cn \geq 4(1-\varepsilon)m\ell$.

Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = O(\sqrt{n})$ – Step 1

Step 1:

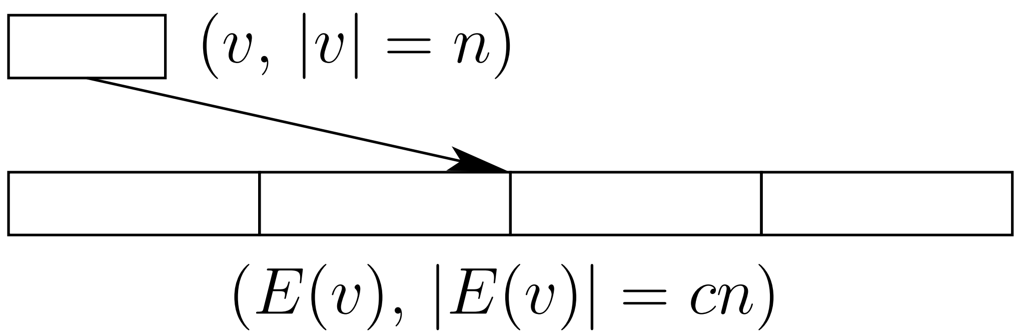
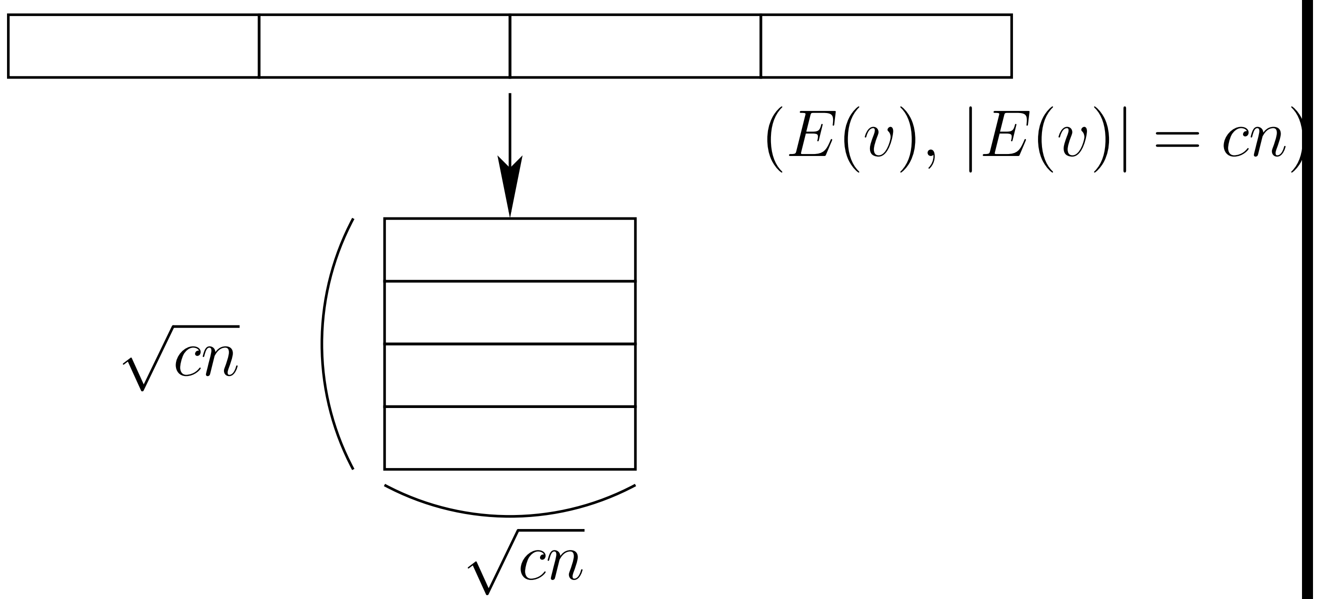


Figure 4: Encode v by Justesen code

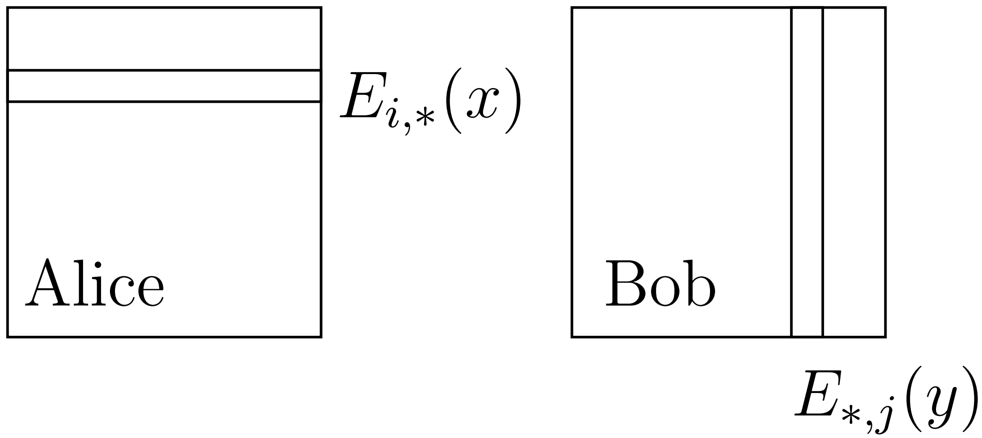
Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = O(\sqrt{n})$ – Step 2

Step 2. Rearrange $E(x)$ into a $\sqrt{cn} \times \sqrt{cn}$ square:



Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_{\varepsilon}) = O(\sqrt{n})$ – Step 3

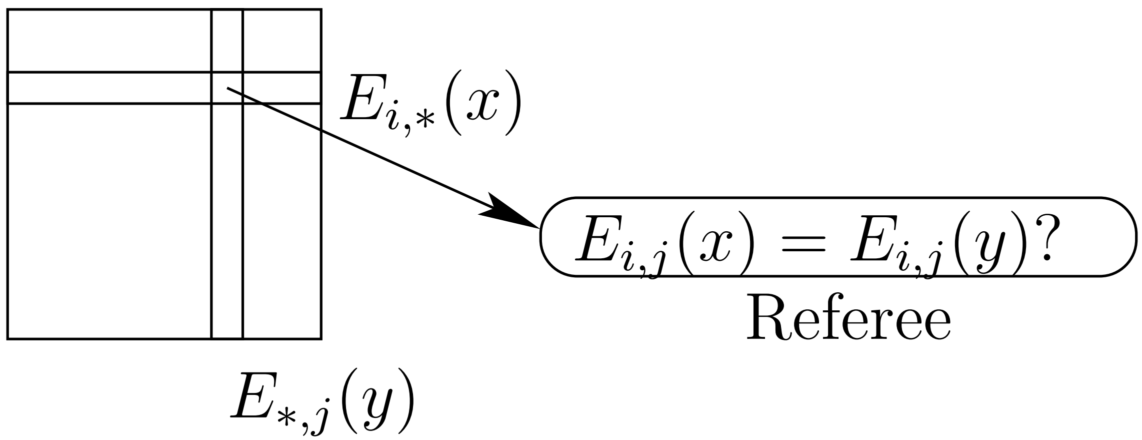
Step 3:



- Alice choose $i \in \{1, 2, \ldots, \sqrt{cn}\}$ and send $E_{i,*}(x)$ to Referee R.
- Bob choose $j \in \{1, 2, \ldots, \sqrt{cn}\}$ and send $E_{*,j}(x)$ to Referee R.

Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = O(\sqrt{n})$ – Step 4

Step 4 Referee R checks whether $E_{i,j}(x) = E_{i,j}(y)$:



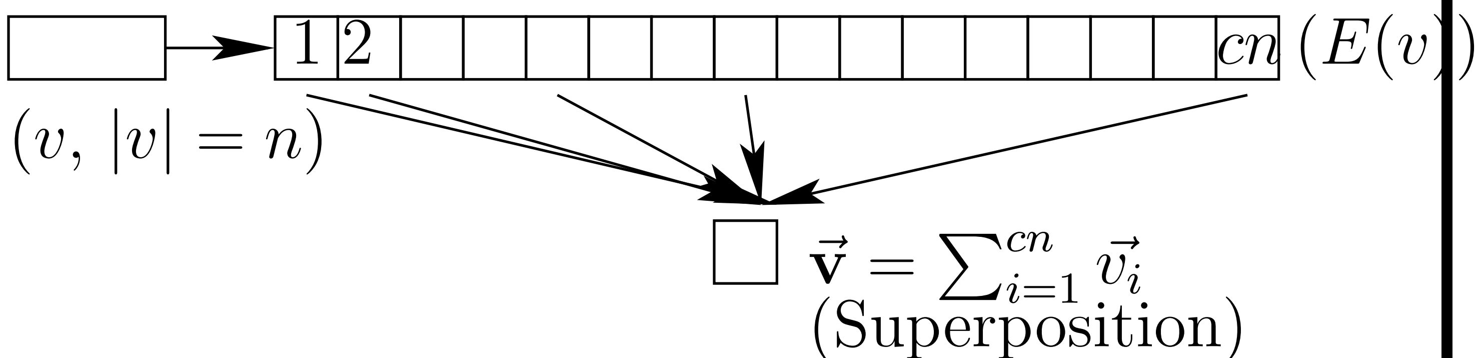
Protocol s.t. $C_{\mathbf{SMM}}(\mathsf{EQ}_\varepsilon) = O(\sqrt{n})$ – Analysis

Analysis:

- $x = y$: $E_{i,j}(x) = E_{i,j}(y)$.
- $x \neq y$: $\mathbf{Pr}[E_{i,j}(x) \neq E_{i,j}(y)] \geq 1 - \varepsilon$.
  (Because $[d(E(x), E(y))] \geq (1 - \varepsilon)cn$)

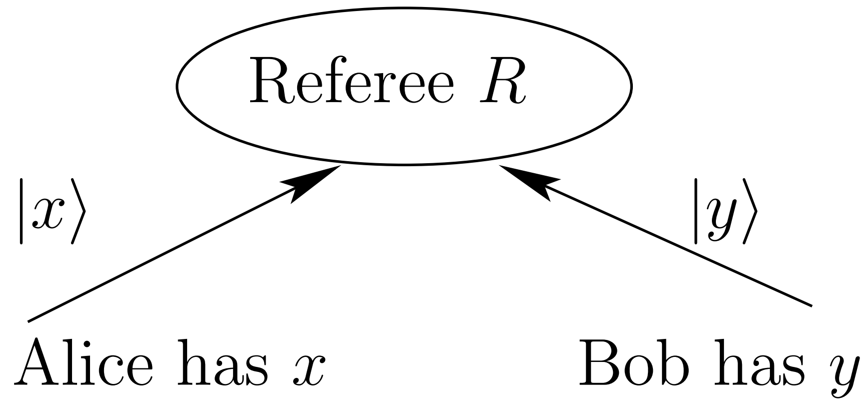
EQ_ε(x,y) Problem in Quantum World $\mathcal{M}$

Idea. Recall that encoding v by Justesen code:



Encode v in $\mathcal{M}$ (1)

Idea. Let x be encoded as $|x\rangle$, and y as $|y\rangle$ (in $\mathcal{M}$).



Find a way of encoding s.t.

$$|\langle x|y\rangle| \begin{cases} = 1, & x = y, \\ \leq \varepsilon, & x \neq y. \end{cases}$$

Encode v in $\mathcal{M}$ (2)

Let $m \triangleq cn = |E(v)|$. Encode x into

$$|x\rangle = \sum_{i=0}^{m-1} \frac{1}{\sqrt{m}} |i\rangle \otimes |E_i(x)\rangle ,$$

and y into

$$|y\rangle = \sum_{i=0}^{m-1} \frac{1}{\sqrt{m}} |i\rangle \otimes |E_i(y)\rangle .$$

Then

$$\langle x \,|\, y\rangle = \frac{1}{m} \sum_{i=1}^{m} E_i(x) E_i(y)$$

Encode v in $\mathcal{M}$ (3)

- Here, $dim(|i\rangle) = m$ and $dim(|E_i(v)\rangle) = 2$.
- It's easy to verify that when $x \neq y$

$$\langle x \,|\, y \rangle = \frac{1}{m} \sum_{i=1}^{m} E_i(x) E_i(y) \leq \frac{1}{m} \varepsilon m$$

because $d[(E(x), E(y))] \geq (1 - \varepsilon)m$.

- What should Referee R do then?

Referee's Circuit

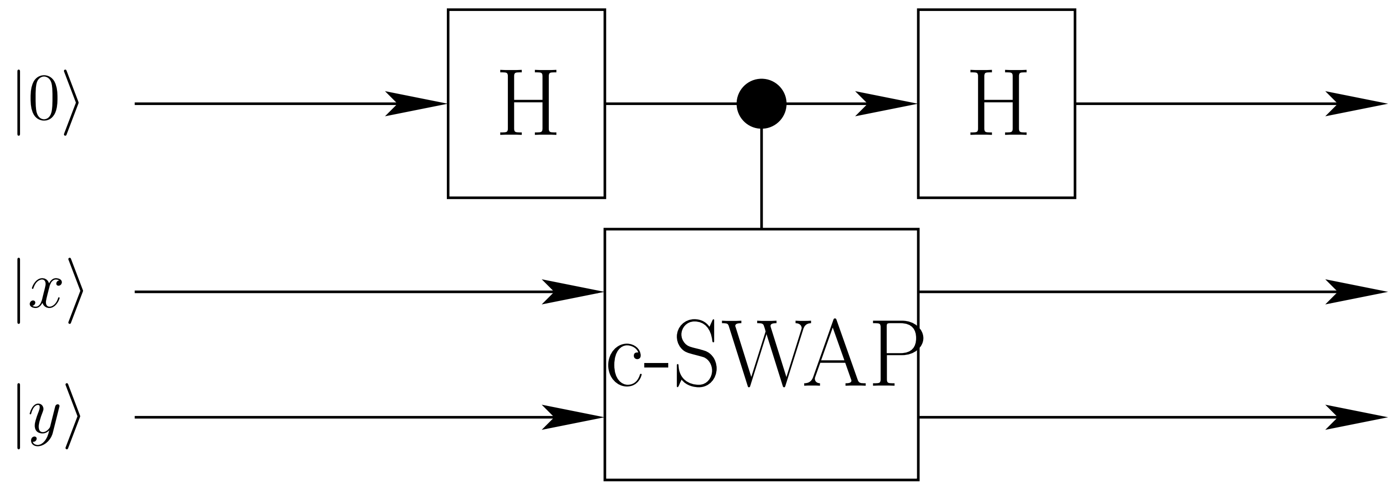
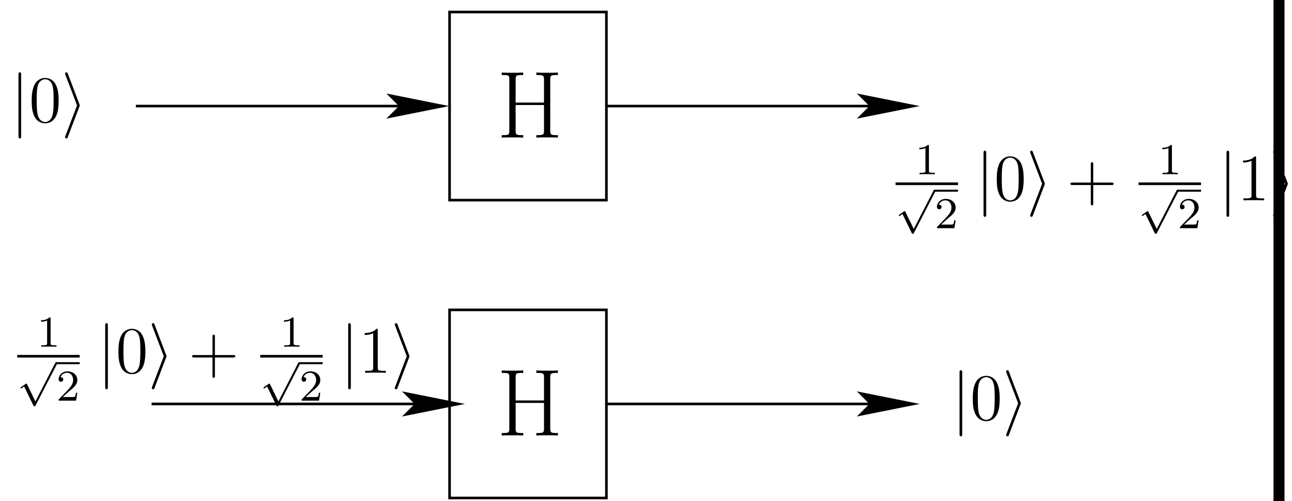
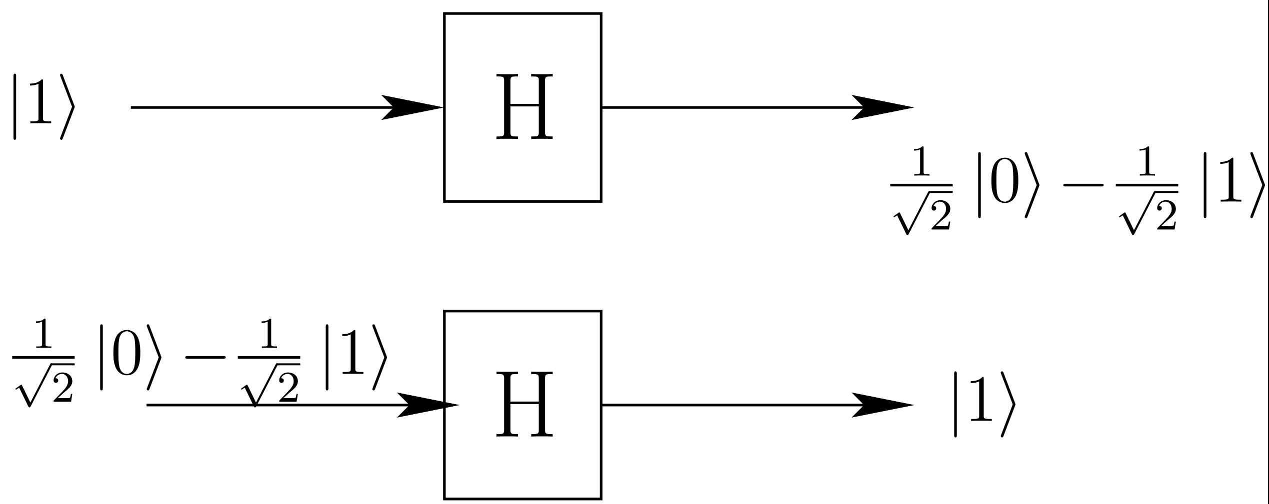


Figure 5: A circuit for testing if $|x\rangle = |y\rangle$ or $|\langle x|y\rangle| \leq \varepsilon$

What is H? (1)

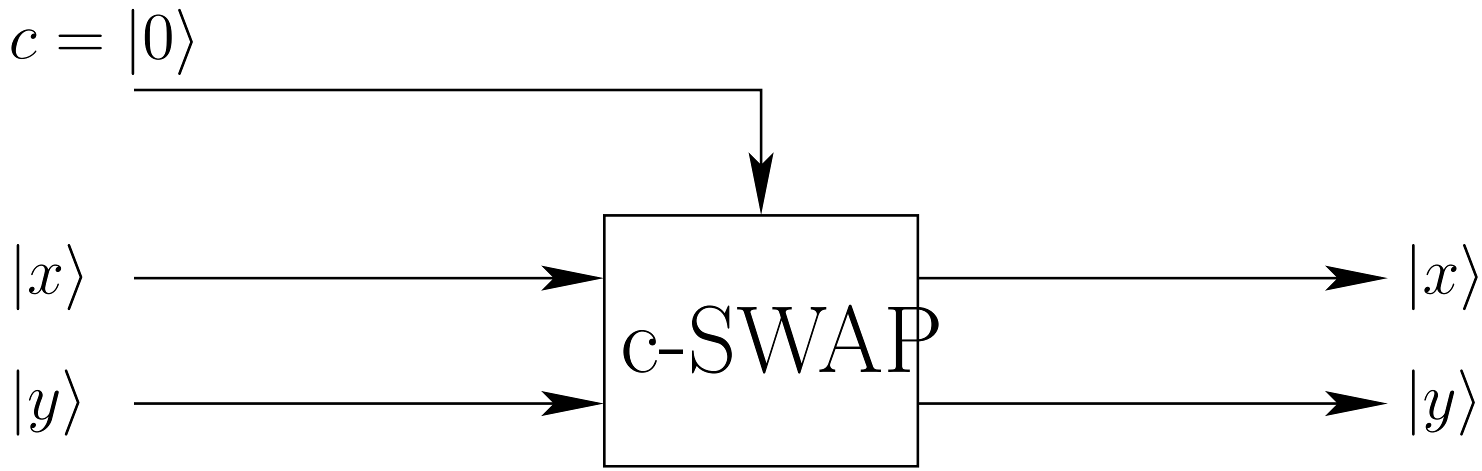

$|0\rangle$
H
$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
H
$|0\rangle$

What is H? (2)

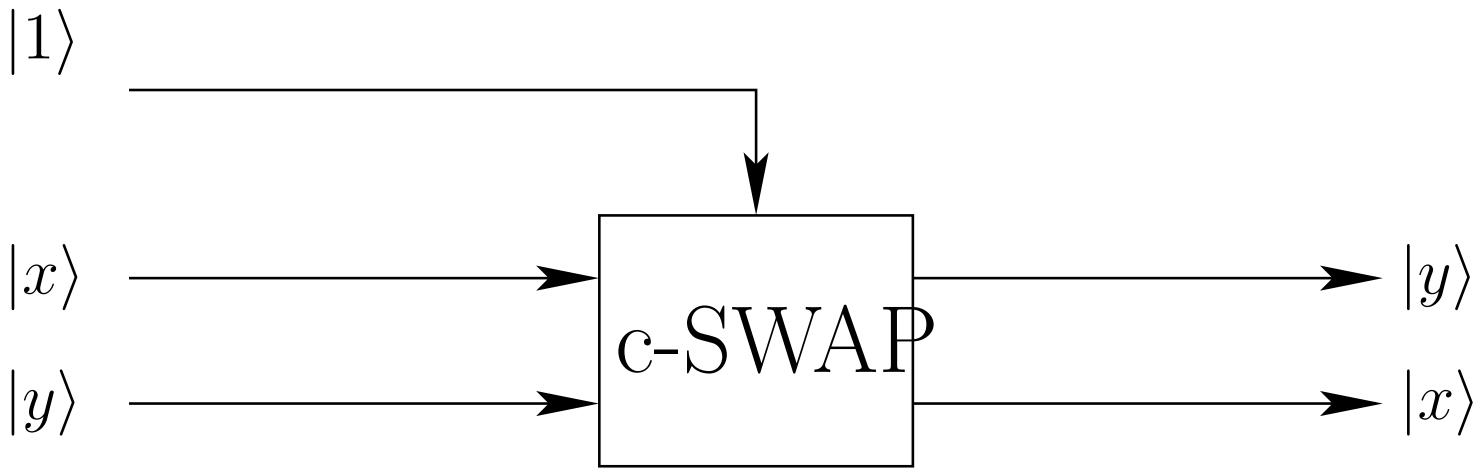


$|1\rangle$
H
$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
H
$|1\rangle$

What is c-SWAP? (1)

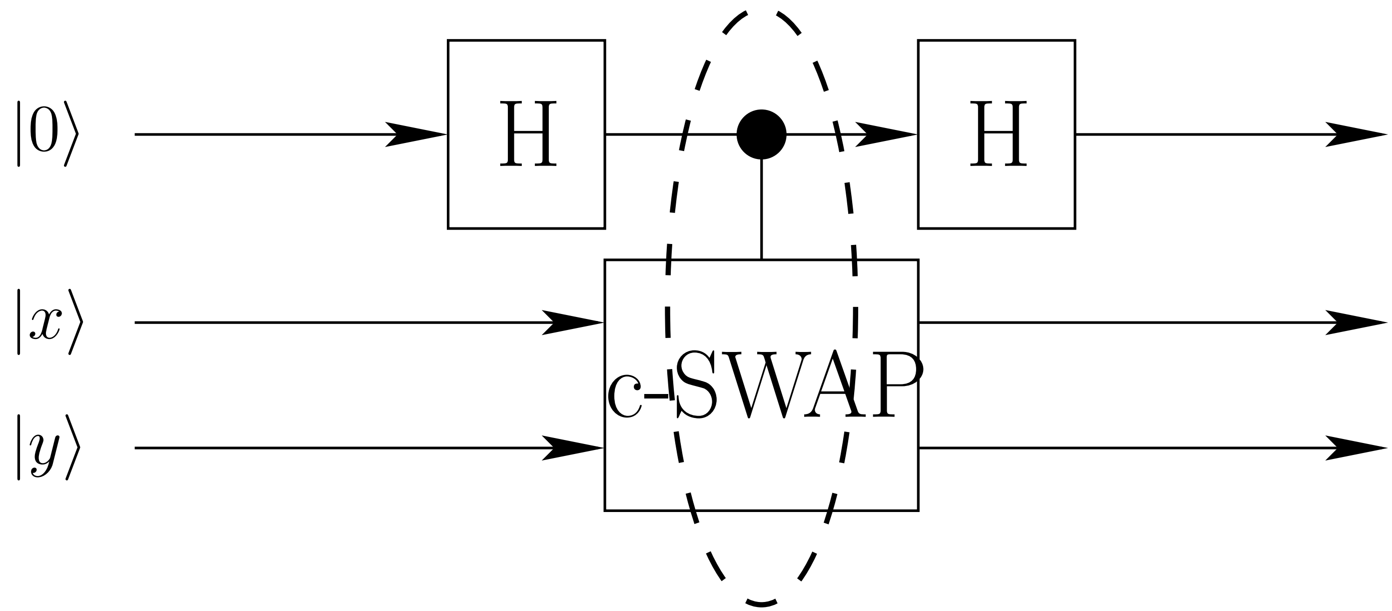


What is c-SWAP? (2)



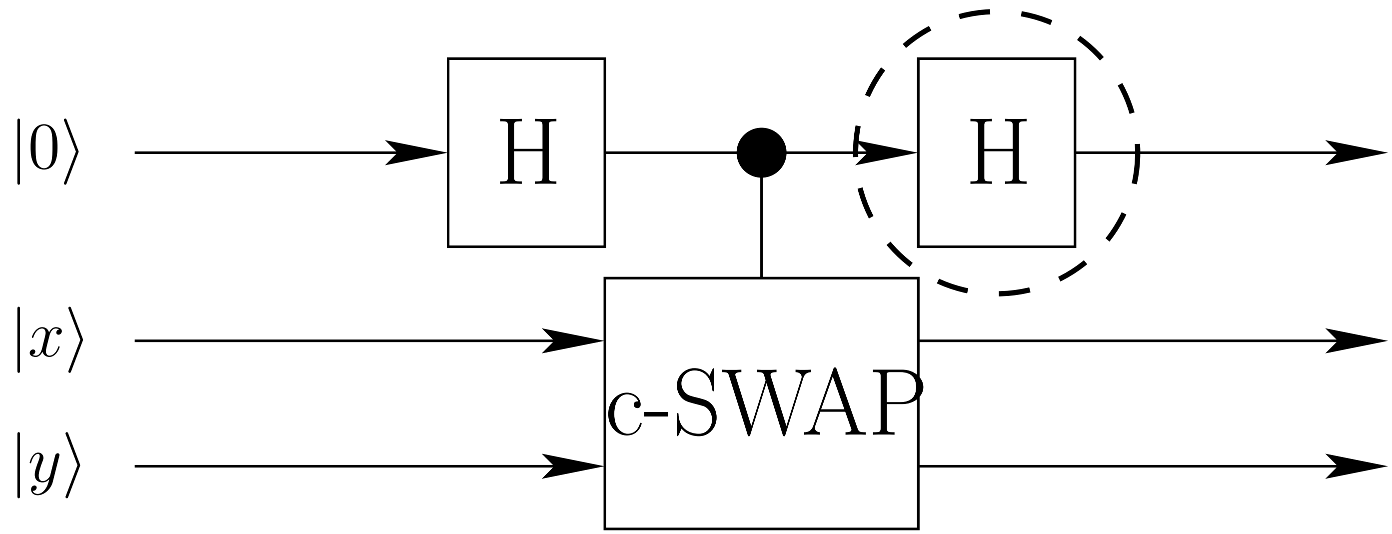
Stage 1

$$|0\rangle \otimes |x\rangle \otimes |y\rangle \longrightarrow \frac{1}{\sqrt{2}}\,|0\rangle \otimes |x\rangle \otimes |y\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \otimes |y\rangle \otimes |x\rangle \quad (5)$$



Stage 2

$$
\begin{aligned}
(5) \quad \longrightarrow \quad & \frac{1}{2}(|0\rangle + |1\rangle) \otimes |x\rangle \otimes |y\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |y\rangle \otimes |x\rangle \\
= \quad & \frac{1}{2}\,|0\rangle \otimes (|x\rangle \otimes |y\rangle + |y\rangle \otimes |x\rangle) + \frac{1}{2}\,|1\rangle \otimes (|x\rangle \otimes |y\rangle - |y\rangle \otimes |x\rangle) \\
= \quad & (2)
\end{aligned}
$$



Stage 3

Referee R regards $|0\rangle$ as $x = y$, $|1\rangle$ as $x \neq y$.

Apply the Projection operation $P_{|0\rangle}$ to

$$(2) = \frac{1}{2}\,|0\rangle\otimes(|x\rangle\otimes|y\rangle+|y\rangle\otimes|x\rangle)+\frac{1}{2}\,|1\rangle\otimes(|x\rangle\otimes|y\rangle-|y\rangle\otimes|x\rangle),$$

then

$$\begin{aligned} P_{|0\rangle}(2) &= |\mathbf{0}\rangle\left(\frac{1}{2}(\langle x|\otimes\langle y|+\langle y|\otimes\langle x|)\frac{1}{2}(|x\rangle\otimes|y\rangle+|y\rangle\otimes|x\rangle)\right) \\ &= |\mathbf{0}\rangle\left(\frac{1}{2}(1+|\,\langle x\,|\,y\rangle\,|^2)\right). \end{aligned}$$

Stage 3 (Cont.)

Thus,

$$\frac{1}{2}(1+|\langle x|y\rangle|^2)\begin{cases}=1, & x=y;\\ \leq \frac{1}{2}(1+\varepsilon^2), & x\neq y.\end{cases} \tag{6}$$

EQ_ε(x,y) Protocol in $\mathcal{M}$ – Analysis

Figure 6: What is sent by Bob – classical vs quantum

EQ_ε(x,y) Protocol in $\mathcal{M}$ – Analysis

Comparison

- Classically Bob sends j and $E_{*,j}(y)$: $\lg n + c\sqrt{n}$ bits ($\Theta(\sqrt{n})$ de facto).
- Quantumly Bob sends $|y\rangle$: $O(\lg n)$ qubits.

Reduce error

- – Can we reduce the one side error $\boldsymbol{\epsilon} \triangleq \frac{1}{2}(1+\varepsilon^2)$?
  - Naively, repeat the protocol k times, we have an error bound $(\frac{1+\varepsilon^2}{2})^k$.
- Moreover it can be reduced to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$.
- But it cannot be less than $\frac{1}{4}(\frac{1+\varepsilon}{2})^{2k}$.

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (0)

Idea:

- Know fact:

$$\langle x \,|\, y \rangle \leq \varepsilon \tag{7}$$

- Duplicate $|x\rangle$ and $|y\rangle$ k times respectively we have $|X\rangle \triangleq |x\rangle^{(k)}$ and $|Y\rangle \triangleq |y\rangle^{(k)}$.

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (1)

Prepare two kinds of quantum registers

- Permutation register $|P\rangle$.
- Data register $|D\rangle \triangleq |XY\rangle$.

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (2)

Permutation register $|s\rangle$:

- Defined by the permutition group S_{2k} for $\sigma_s \in S_{2k}$.
  (**Note** $s = 0$: the index of identity permutition)
- Define $C = |S_{2k}|$
- Initially, we prepare $|s\rangle = |0\rangle^{(C)}$.

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (3)

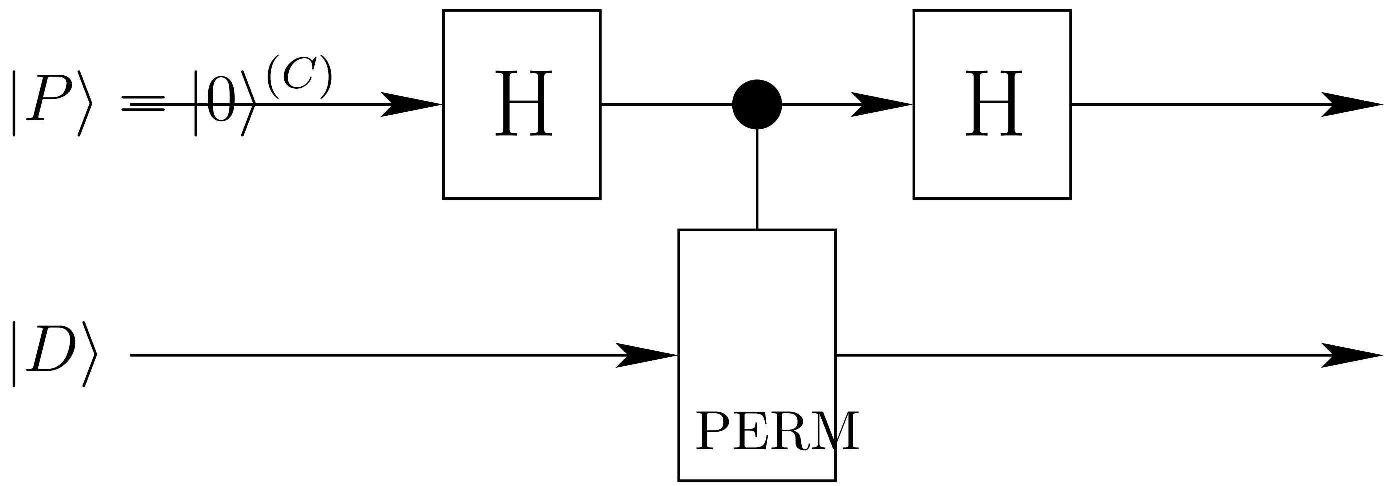


Figure 7: The algorithm for reducing err to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ $(|D\rangle = |XY\rangle = |x\rangle^{(k)} |y\rangle^{(k)})$

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (4)

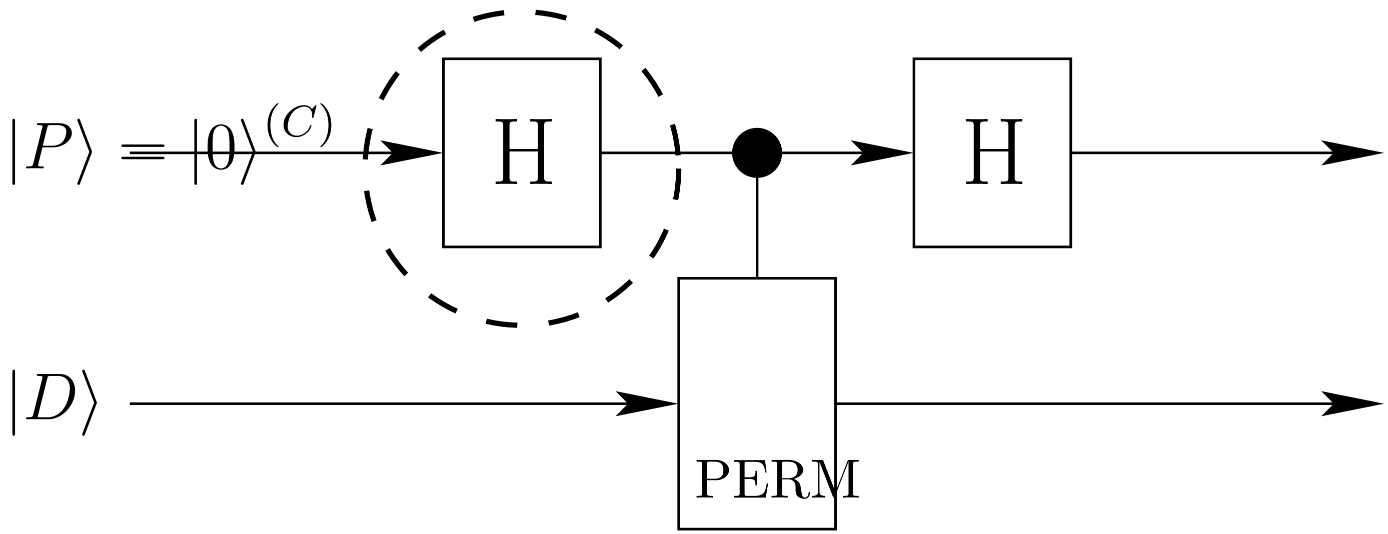
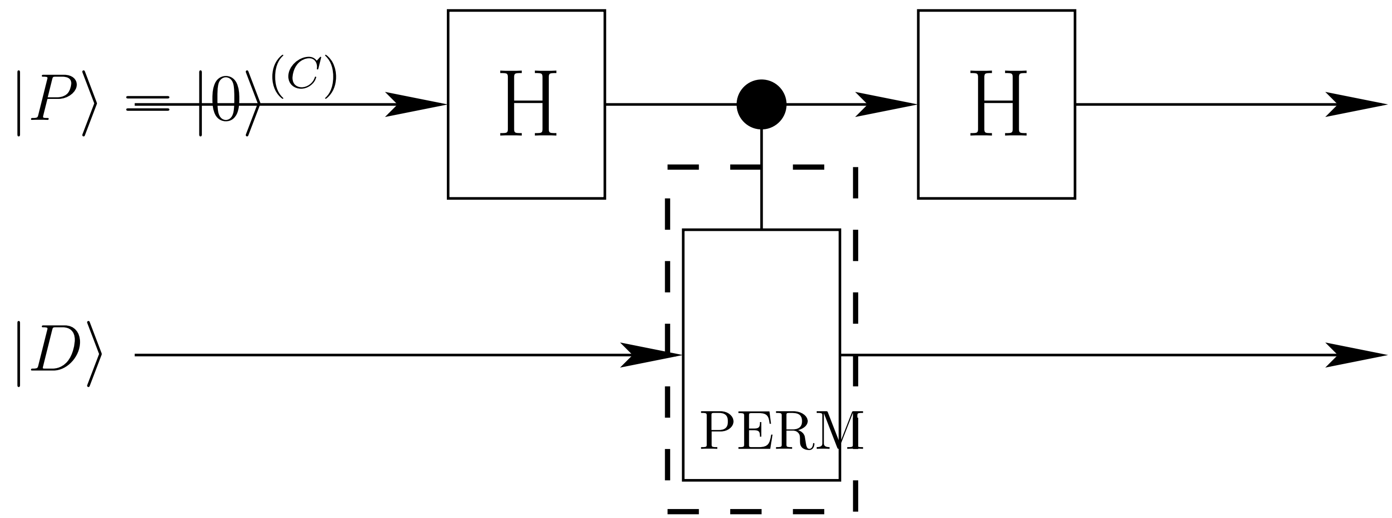


Figure 8: $|P\rangle = \frac{1}{\sqrt{C}} \sum_{s=0}^{C-1} |s\rangle$: generate all possible permutation uniformly

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (5)



$$
\begin{aligned}
|P\rangle \otimes |D\rangle &= \frac{1}{\sqrt{C}} \sum_{s=0}^{C-1} |s\rangle \otimes \sigma_s(|D\rangle) \\
&= \frac{1}{\sqrt{C}} \sum_{s=0}^{C-1} |s\rangle \otimes |\sigma_s(D)\rangle \qquad (8)
\end{aligned}
$$

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (6)

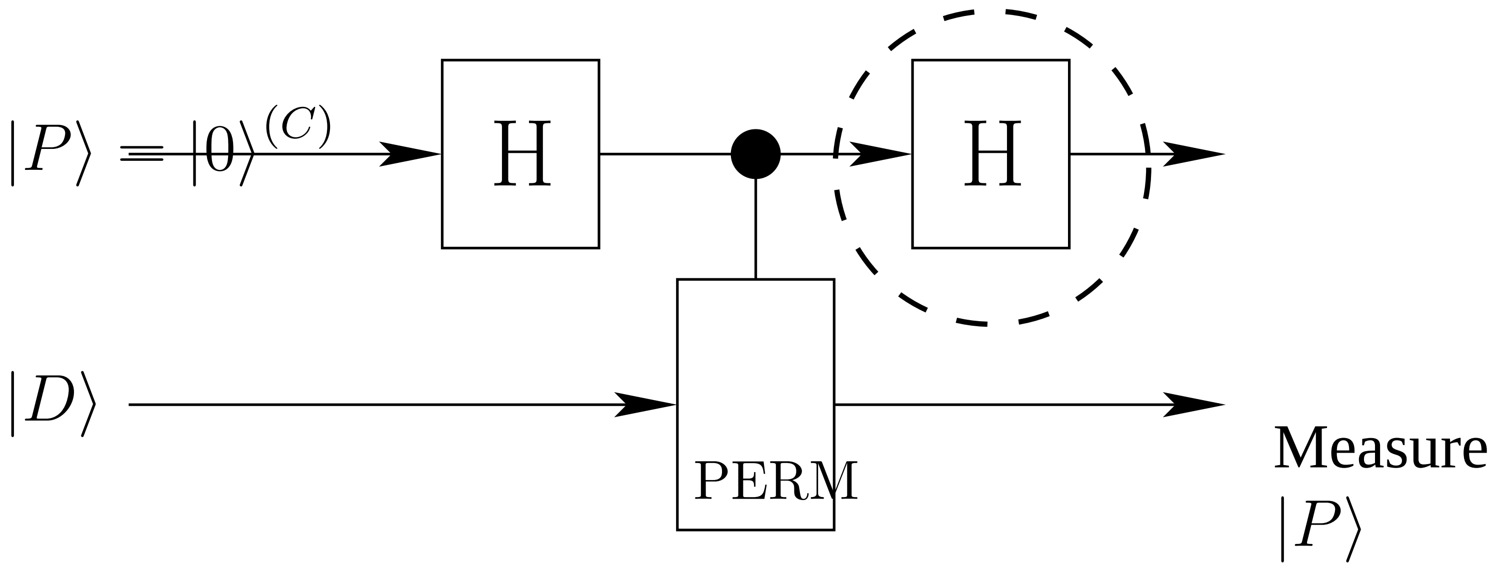


Figure 9: We only care whether $|P\rangle = |0\rangle^{(C)}$ thus measure the permutation register

$$
\begin{aligned}
|P\rangle \otimes |D\rangle &= (\langle 0|^{(C)} \, H^{(C)} \otimes I)(8) \\
&= \frac{1}{\sqrt{C}} \sum_{s=0}^{C-1} \langle 0|^{(C)} \, H^{(C)} \, |s\rangle \otimes |\sigma_s(D)\rangle \\
&= \frac{1}{\sqrt{C}} \sum_{s=0}^{C-1} \left(\frac{1}{\sqrt{C}} \sum_{t=0}^{C-1} \langle t|\right) |s\rangle \otimes |\sigma_s(D)\rangle \\
&= \frac{1}{C} \sum_{s=0}^{C-1} |s\rangle \otimes |\sigma_s(D)\rangle \qquad (9)
\end{aligned}
$$

$$
\langle 0|^{(C)} \, (9) = \frac{1}{C} \sum_{s=0}^{C-1} |\sigma_s(D)\rangle \qquad (10)
$$

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (7)

The probability that we measure $|P\rangle = |0\rangle^{(C)}$ is

$$(10)^{\dagger}(10) = (\frac{1}{C}\sum_{t=0}^{C-1} \langle\sigma_t(D)|)(\frac{1}{C}\sum_{s=0}^{C-1} |\sigma_s(D)\rangle)$$

$$= \frac{1}{C^2}\sum_{t=0}^{C-1}\sum_{s=0}^{C-1} \langle\sigma_t(D)\,|\,\sigma_s(D)\rangle = \frac{1}{C^2}\sum_{t=0}^{C-1}\sum_{s=0}^{C-1} \langle D|\,\sigma_t^{-1}\sigma_s\,|D\rangle$$

$$= \frac{1}{C^2}\sum_{s=0}^{C-1} \langle D|\, C\sigma_s(|D\rangle)$$

$$= \frac{1}{C}\sum_{s=0}^{C-1} \langle D|\,\sigma_s(|D\rangle) = \frac{1}{C}\sum_{s=0}^{C-1} \langle x|^{(k)}\,\langle y|^{(k)}\,\sigma_s(|x\rangle^{(k)}\,|y\rangle^{(k)}) \quad (11)$$

Reduce to $\sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k}$ (8)

Because $\langle x \,|\, y \rangle \le \varepsilon$ and $C = |S_{2k}| = (2k)!$, we have

$$(11) = \frac{1}{C}\sum_{s=0}^{C-1} \langle x|^{(k)} \langle y|^{(k)} \sigma_s(|x\rangle^{(k)} |y\rangle^{(k)})$$

$$\le \frac{(k!)^2}{(2k)!}\sum_{i=0}^{k}(\binom{k}{i}\varepsilon^i)^2 \le \frac{(k!)^2}{(2k)!}(1+\varepsilon)^{2k} \le \sqrt{\pi k}(\frac{1+\varepsilon}{2})^{2k} \quad (12)$$

Cannot be smaller than $\frac{1}{4}(\frac{1+\varepsilon}{2})^{2k}$ (1)

Extremal case:

- $|\phi\rangle = |x_1\rangle^{(k)}\,|y_1\rangle^{(k)}$ and $|\psi\rangle = |x_2\rangle^{(k)}\,|y_2\rangle^{(k)}$
- Set $\cos(\theta) = \langle x_2\,|\,y_2\rangle \stackrel{\Delta}{=} \varepsilon$, $|x_1\rangle = |0\rangle$, $|y_1\rangle = |0\rangle$;
  $|x_2\rangle = \cos(\frac{\theta}{2})\,|0\rangle + \sin(\frac{\theta}{2})\,|1\rangle$,
  $|y_2\rangle = \cos(\frac{\theta}{2})\,|0\rangle - \sin(\frac{\theta}{2})\,|1\rangle$.
- $\langle\phi\,|\,\psi\rangle = \cos^{2k}(\frac{\theta}{2}) = (\frac{1+\cos(\theta)}{2})^k = (\frac{1+\varepsilon}{2})^k \stackrel{\Delta}{=} \cos(\beta)$

Cannot be smaller than $\frac{1}{4}(\frac{1+\varepsilon}{2})^{2k}$ (2)

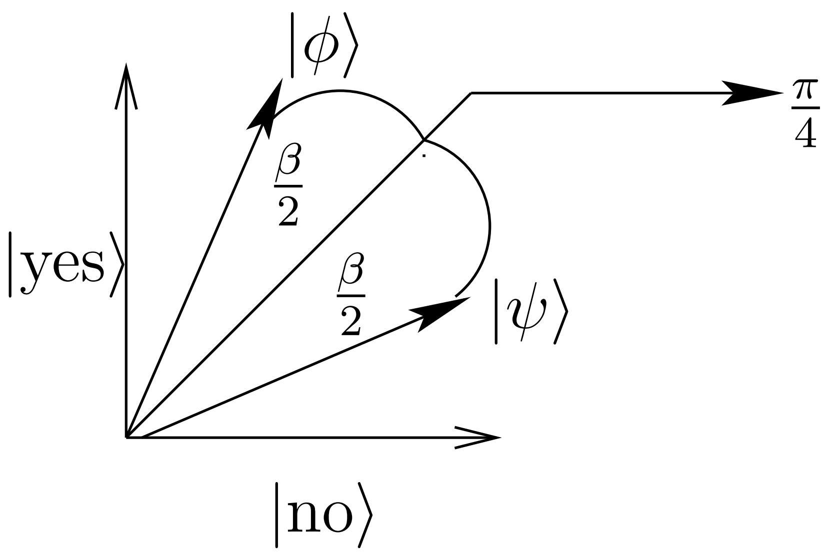


Figure 10: Indistinguishable case for $|\phi\rangle$ and $|\psi\rangle$

Cannot be smaller than $\frac{1}{4}(\frac{1+\varepsilon}{2})^{2k}$ (3)

- $|\text{yes}\rangle$: $|\phi\rangle$ and $|\psi\rangle$ are the same.
  $|\text{no}\rangle$: $|\phi\rangle$ and $|\psi\rangle$ are different.

$$\begin{aligned} &\mathbf{Pr}[\text{Answer yes when different}] \\ &+\mathbf{Pr}[\text{Answer no when the same}] \\ &= \frac{1}{2}\sin^2(\frac{\pi}{4}-\frac{\beta}{2}) + \frac{1}{2}\sin^2(\frac{\pi}{4}-\frac{\beta}{2}) \\ &= \frac{1-\sin(\beta)}{2} \geq \frac{1}{4}\cos^2(\beta) = \frac{1}{4}(\frac{1+\varepsilon}{2})^{2k} \end{aligned} \tag{13}$$

Cryptography

Goldreich Levin Theorem

- OWF: one-way function $f : \{0,1\}^n \rightarrow \{0,1\}^n$
- HCP: hardcore predicate $h : \{0,1\}^n \rightarrow \{0,1\}$
- Predicting a HCP is as hard as inverting a OWF.
- We only care about the efficeincy of the reduction from OWF to HCP.

Main Results

The efficeincy of the reduction:

- **Classical world:** $\Omega(\frac{\delta n}{\varepsilon^2})$
- **Quantum world:** $O(\frac{1}{\varepsilon})$

Modified Reduction/Problem:

- **EQ** query corresponds to computing $(b, x) \triangleq (f(a), x)$.
- **IP** query corresponds to computing $h(a, x) \triangleq a \cdot x$.

The Problem

- **Input**: $a \in \{0,1\}^n$
  (given but kept confidential in a black box.)
- **Output**: a (rechieve it from the black box!)
- **Allowed operations**: black-box queries only.
- **Goal**: determine a with a minimun number of black-box queries.

Classical black boxes

1. **IP**. for a set $S(\subseteq \{0,1\}^n)$ which satisfies $|S| \geq (0.5+\varepsilon)2^n$:

$$\mathbf{IP}(x) \triangleq \begin{cases} a \cdot x, & x \in S; \\ \overline{a \cdot x}, & x \notin S. \end{cases}$$

   Alternative speaking, $\mathbf{Pr}_{x\in\{0,1\}^n}[\mathbf{IP}(x) = a \cdot x] \geq 0.5 + \varepsilon$

2. **EQ**.

$$\mathbf{EQ}(x) \triangleq \begin{cases} 1, & x = a; \\ 0, & x \neq a. \end{cases}$$

Classical Theorem

Given

- success probability: $\delta(> 0)$ and
- $\varepsilon \geq \sqrt{n}2^{-\frac{n}{3}}$.

We should determine a by

- at lease $2^{\frac{n}{2}}$ **EQ** queries; or
- $\Omega(\frac{\delta n}{\varepsilon^2})$ **IP** queries.

From randomized to deterministic

- Let
  - $\mathcal{I}$: the set of all possible inputs;
    p: chosen distribution of all possible algorithms;
    R_ε: a randomized algorithm with err prob ε.
  - $\mathcal{A}$: the set of all possible algorithms.
    q: chosen distribution of all possible inputs;
    $D_{2\varepsilon}$: a deterministic algorithm with err prob 2ε.

  Then we have

$$2 \max_{I \in \mathcal{I}} \mathbf{E}_p[R_\varepsilon] \geq \min_{A \in \mathcal{A}} \mathbf{E}_q[D_{2\varepsilon}] \tag{14}$$

From randomized to deterministic

- a deterministic algorithm with **error** inputs can lower bounded corresponding randomized ones.
- That's the reason we define **IP** which might have error string in.

Classical black box algorithm

- Do **IP** queries for m times first.
- Then do **EQ** queries for $2^{\frac{n}{2}}$ times.
- Analyze the conditional mutual information about a:
  - Lower bound: determined by **IP** queries.
  - Upper bound: determined by **EQ** queries.
- estimate m from the conditional mutual information about a.

$H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

$H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$:

- *the quality of information* on the input $a \in \{0,1\}^n$ (which corresponds to the random variable $\boldsymbol{A}$) we gained after applying m queries.
- $\boldsymbol{Y}_i$: the $\{0,1\}$-valued random variable corresponding to the output of the i-th time **IP** query.

Conditional and Joint Entropy

- Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ are two random variables, then
- **Conditional Entropy**:

$$H(\boldsymbol{X}|\boldsymbol{Y}) \triangleq -\sum_{y\in\boldsymbol{Y}} \mathbf{Pr}[y] \sum_{x\in\boldsymbol{X}} \mathbf{Pr}[x|y] \lg(\mathbf{Pr}[x|y]) \quad (15)$$

$$= H(\boldsymbol{X},\boldsymbol{Y}) - H(\boldsymbol{Y}) \quad (16)$$

- **Joint Entropy**:

$$H(\boldsymbol{X},\boldsymbol{Y}) \triangleq \left(-\sum_{y\in\boldsymbol{Y}} \sum_{x\in\boldsymbol{X}} \mathbf{Pr}[x,y] \lg(\mathbf{Pr}[x,y])\right) \quad (17)$$

$$= H(\boldsymbol{X}) + H(\boldsymbol{Y}|\boldsymbol{X}) \quad (18)$$

Compute $H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

Let $\boldsymbol{Y}^{m-1} \triangleq \{\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}\}$, then

$$\begin{aligned}
& H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m) \\
\triangleq \quad & \underline{\underline{H(\boldsymbol{A}|\boldsymbol{Y}^{m-1}, \boldsymbol{Y}_m)}} \\
= \quad & \underline{\underline{H(\boldsymbol{A}, \boldsymbol{Y}^{m-1}, \boldsymbol{Y}_m) - H(\boldsymbol{Y}^{m-1}, \boldsymbol{Y}_m)}} \\
= \quad & \left(H(\boldsymbol{Y}_m|\boldsymbol{A}, \boldsymbol{Y}^{m-1}) + \boxed{H(\boldsymbol{A}, \boldsymbol{Y}^{m-1})}\right) \\
- \quad & \left(H(\boldsymbol{Y}_m|\boldsymbol{Y}^{m-1}) + H(\boldsymbol{Y}^{m-1})\right) \\
= \quad & \left(H(\boldsymbol{Y}_m|\boldsymbol{A}, \boldsymbol{Y}^{m-1}) + \boxed{H(\boldsymbol{A}|\boldsymbol{Y}^{m-1}) + H(\boldsymbol{Y}^{m-1})}\right) \\
- \quad & \left(H(\boldsymbol{Y}_m|\boldsymbol{Y}^{m-1}) + H(\boldsymbol{Y}^{m-1})\right) \\
= \quad & H(\boldsymbol{Y}_m|\boldsymbol{A}, \boldsymbol{Y}^{m-1}) + H(\boldsymbol{A}|\boldsymbol{Y}^{m-1}) - H(\boldsymbol{Y}_m|\boldsymbol{Y}^{m-1}) \qquad (19)
\end{aligned}$$

Compute $H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

Thus (19) can be spreaded as follows:

$$
\begin{aligned}
H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_m) &= H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}) \\
&+ H(\boldsymbol{Y}_m|\boldsymbol{A}, \boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}) \\
&- H(\boldsymbol{Y}_m|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}) \\
H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}) &= H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-2}) \\
&+ H(\boldsymbol{Y}_{m-1}|\boldsymbol{A}, \boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-2}) \\
&- H(\boldsymbol{Y}_{m-1}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-2}) \\
H(\boldsymbol{A}|\boldsymbol{Y}_1, \boldsymbol{Y}_2) &= H(\boldsymbol{A}|\boldsymbol{Y}_1) + H(\boldsymbol{Y}_2|\boldsymbol{A}, \boldsymbol{Y}_1) \\
&- H(\boldsymbol{Y}_2|\boldsymbol{Y}_1) \\
H(\boldsymbol{A}|\boldsymbol{Y}_1) &= H(\boldsymbol{A}) + H(\boldsymbol{Y}_1|\boldsymbol{A})
\end{aligned}
$$

Compute $H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

Recursively plug the above equations into (19), we have

$$\begin{aligned} H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_m) &= H(\boldsymbol{A}) + \sum_{\imath=1}^{m} H(\boldsymbol{Y}_i|\boldsymbol{A}, \boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{\imath-1}) \\ &- \sum_{\imath=1}^{m} H(\boldsymbol{Y}_i|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{i-1}) \\ &\triangleq (\mathfrak{X}) + (\mathfrak{Y}) - (\mathfrak{Z}) \qquad (20) \end{aligned}$$

We will analyze the above terms.

Analyze ($\mathfrak{X}$)

Because $\boldsymbol{A}$ is a random variable (which corresponds to the input a of our algorithm) uniformly chosen from $\{0,1\}^n$, it's trivial that

$$
\begin{aligned}
(\mathfrak{X}) \triangleq H(A) &= -\sum_{a\in\{0,1\}^n} \mathbf{Pr}[a]\lg(\mathbf{Pr}[a]) \\
&= -2^n\frac{1}{2^n}\lg(\frac{1}{2^n}) = n \qquad (21)
\end{aligned}
$$

Analyze ($\mathfrak{Y}$): algorithm IPQuery

IPQuery(m)

$U \leftarrow \{0,1\}^n$

$S \leftarrow$ NIL, $\overline{S} \leftarrow$ NIL

$j \leftarrow 0$

for $i \leftarrow 1$ **to** m

do $x \in_R U$

    w.p. $((0.5+\varepsilon)2^n - j)/(2^n - (i-1))$

        do $S \leftarrow S \cup x$

            $j \leftarrow j+1$

        or $\overline{S} \leftarrow \overline{S} \cup x$

    $U \leftarrow U \setminus \{x\}$

Analyze ($\mathfrak{Y}$)

- S can be regarded as the *success* set $\{x \mid \mathbf{IP}(x) = a \cdot x\}$ and
  $\overline{S}$ as the *fail* set $\{x \mid \mathbf{IP}(x) = \overline{a \cdot x}\}$.
- Let $\mathfrak{p}_i$ be the probability that x is put into the *success* set at the i-th query, then

$$0.5 - 2\varepsilon \le \frac{(0.5+\varepsilon)2^n - (i-1)}{2^n - (i-1)} \le \mathfrak{p}_i \le \frac{(0.5+\varepsilon)2^n}{2^n - (i-1)} \le 0.5 + 2\varepsilon \tag{22}$$

Analyze ($\mathfrak{Y}$)

Thus, the information on the output of the i-th query (when *a and the information on the output of previous queries* are known) has a lower bound determined by (22) because $H(p)$ is **convex** for $p \in [0, 1]$, **max** when $p = 0.5$.

Analyze ($\mathfrak{Y}$)

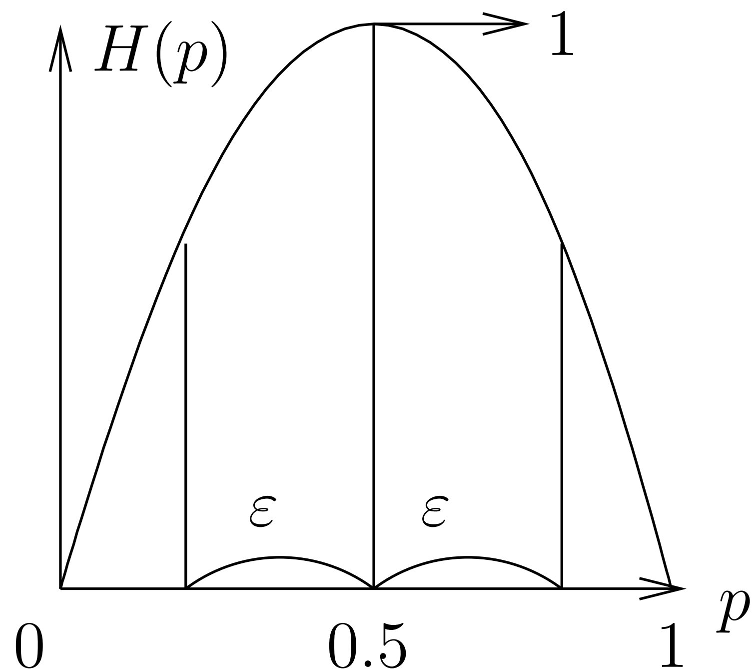


Figure 11: $H(p)$ is **convex** for $p \in [0, 1]$

Analyze $(\mathfrak{Y})$

That is

$$
\begin{aligned}
& H(\boldsymbol{Y}_i|\boldsymbol{A}, \boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{\imath-1}) \\
\geq \quad & H(0.5 - 2\varepsilon) \ (\equiv H(0.5 + 2\varepsilon)) \\
\triangleq \quad & -(0.5 - 2\varepsilon)\lg(0.5 - 2\varepsilon) - (0.5 + 2\varepsilon)\lg(0.5 + 2\varepsilon) \\
\geq \quad & 1 - \frac{16}{\ln 2}\varepsilon^2 \ \text{(Taylor expansion)}
\end{aligned}
$$

$$
(\mathfrak{Y}) = \sum_{\imath=1}^{m} H(\boldsymbol{Y}_i|\boldsymbol{A}, \boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{\imath-1}) \quad \geq \quad (1 - \frac{16}{\ln 2}\varepsilon^2)m \tag{23}
$$

Analyze ($\mathfrak{Z}$)

Because $\boldsymbol{Y}_i$ is a random variable chosen from $\{0, 1\}$ (which corresponds to the output y_i after the ith query) and the entropy of an 1-bit string is *at most* 1, we have

$$H(\boldsymbol{Y}_i|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{i-1}) \leq 1$$

$$\Longrightarrow (\mathfrak{Z}) \triangleq \sum_{\imath=1}^{m} H(\boldsymbol{Y}_i|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{i-1}) \leq m \qquad (24)$$

Lower bound of $H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

Substituting (21), (23) and (24) into (20), we have

$$\begin{aligned} H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_m) &\triangleq (\mathfrak{X}) + (\mathfrak{Y}) - (\mathfrak{Z}) \\ &\geq (n) + \left((1 - \frac{16}{\ln 2}\varepsilon^2)m\right) - (m) \\ &= n - \left(\frac{16}{\ln 2}\varepsilon^2\right) m \qquad (25) \end{aligned}$$

Two tuned parameters

- the number of **EQ** queries: $2^{-\frac{n}{2}}$
- the upper bound of ε: $\delta\sqrt{n}2^{-\frac{n}{3}}$

Upper bound of $H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m)$

Achieve maximum entropy when $\delta(> 0)$ is fixed:

- $2^{n/2}$ elements each have EQUAL probability $\frac{\delta}{2^{n/2}}$.
- $2^n - 2^{n/2}$ elements each have EQUAL probability $\frac{1-\delta}{2^n - 2^{n/2}}$.

Therefore,

$$\begin{aligned}
& H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m) \\
\leq\ & H(\underbrace{\frac{\delta}{2^{n/2}}, \cdots, \frac{\delta}{2^{n/2}}}_{2^{n/2}}, \underbrace{\frac{1-\delta}{2^n - 2^{n/2}}, \cdots, \frac{1-\delta}{2^n - 2^{n/2}}}_{2^n - 2^{n/2}}) \\
=\ & \delta \lg(2^{n/2}) + H(\delta) + (1-\delta) \lg(2^n - 2^{n/2}) \\
<\ & \delta n/2 + 1 + (1-\delta)n = n - \delta n/2 + 1 \qquad (26)
\end{aligned}$$

Estimate m: the number of queries to IP

Combine (25) with (26), we have

$$n - \left(\frac{16}{\ln 2}\varepsilon^2\right) m \leq H(\boldsymbol{A}|\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_{m-1}, \boldsymbol{Y}_m) < n - \frac{\delta n}{2} + 1$$

Finally,

$$m > \frac{\delta n - 2}{32\varepsilon^2} \ln 2 \in \Omega(\frac{\delta n}{\varepsilon^2}) \tag{27}$$

The Problem in quantum model

- **Input**: $a \in \{0,1\}^n$
  (given but kept confidential in a black box.)
- **Output**: a (rechieve it from the black box!)
- **Allowed operations**: quantum black-box queries only.
- **Goal**: determine a with a minimun number of quantum black-box queries.

Quantum black boxes

- U_{IP}:

$$U_{IP} \overbrace{|x\rangle}^{n\text{ qubits}} \boxed{|0^m\rangle} \overbrace{|o\rangle}^{1\text{ qubit}}$$

$$\triangleq \quad |x\rangle \boxed{(\alpha_x |v_x\rangle |a \cdot x\rangle + \beta_x |w_x\rangle |\overline{a \cdot x}\rangle)} |o\rangle$$

$$\frac{1}{2^n}\left(\sum_{x\in\{0,1\}^n} \alpha_x^2\right) \geq \frac{1}{2} + \varepsilon, \quad \frac{1}{2^n}\left(\sum_{x\in\{0,1\}^n} \beta_x^2\right) \leq \frac{1}{2} - \varepsilon$$

- U_{EQ}:

$$U_{EQ}\,|x\rangle\,\left|0^{m-1}\right\rangle\,\overbrace{|b\rangle}^{\text{1 qubit}}\,|o\rangle = \begin{cases} |x\rangle\,\left|0^{m-1}\right\rangle\,\left|\bar{b}\right\rangle\,|o\rangle\,, & x = a; \\ |x\rangle\,\left|0^{m-1}\right\rangle\,|b\rangle\,|o\rangle\,, & x \neq a. \end{cases}$$

What is U_{EQ}?

For $x, a \in \{0,1\}^n$ and $b \in \{0,1\}$,

- if $|\mathbf{a}\rangle\,|\mathbf{0}\rangle$ is in the form of a 2^{n+1}-dimention column vector $\overrightarrow{e_K}$ [a],
  then U_{EQ} can be represented as the following $2^{n+1} \times 2^{n+1}$ matrix: (for the first 0 in the frame box $\boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}}$ is located at (K, K))

[a] For $i \in \{1, 2, \ldots, 2^{n+1}\}$, $\overrightarrow{e_K}_i =$ **1** (if $i = K$) or **0** (otherwise).

$$\begin{pmatrix} 1 &&&&&&& \\ & \ddots &&&&&& \\ && \ddots &&&&& \\ &&& 1 &&&& \\ &&&& \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} &&& \\ &&&&& 1 && \\ &&&&&& \ddots & \\ &&&&&&& 1 \end{pmatrix}$$

The circuit C

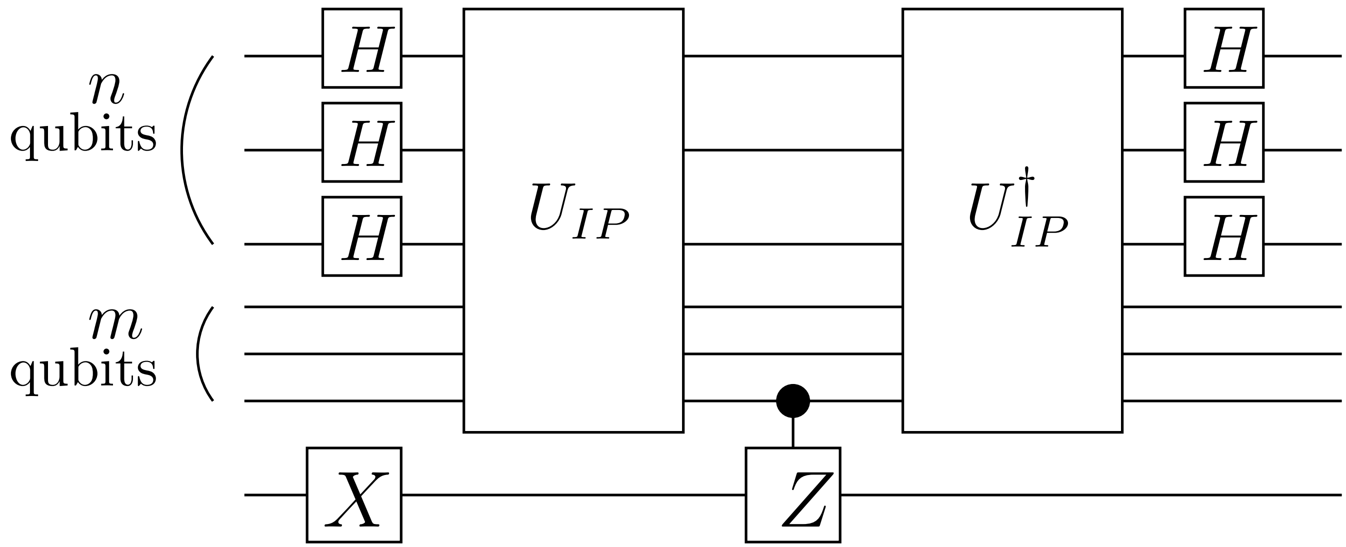


Figure 12: The circuit C

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

GOAL

- Circuit input: $|0^n, 0^m, 0\rangle$.
- Ideal output: $|a, 0^m, 1\rangle$, actual output: $C\,|0^n, 0^m, 0\rangle$.
- Prove that

$$\begin{aligned} \langle a, 0^m, 1| \cdot C\,|0^n, 0^m, 0\rangle &\geq 2\varepsilon, \text{ or} \\ |\langle a, 0^m, 1| \cdot C\,|0^n, 0^m, 0\rangle|^2 &\geq 4\varepsilon^2 \end{aligned}$$

- Thus when repeating the quantum algorithm[a] for $O(\frac{1}{\varepsilon^2})$ times, the input a can be found w.h.p.

[a] That is, feed $|0^n, 0^m\ 0\rangle$ into the circuit C

Decompose C

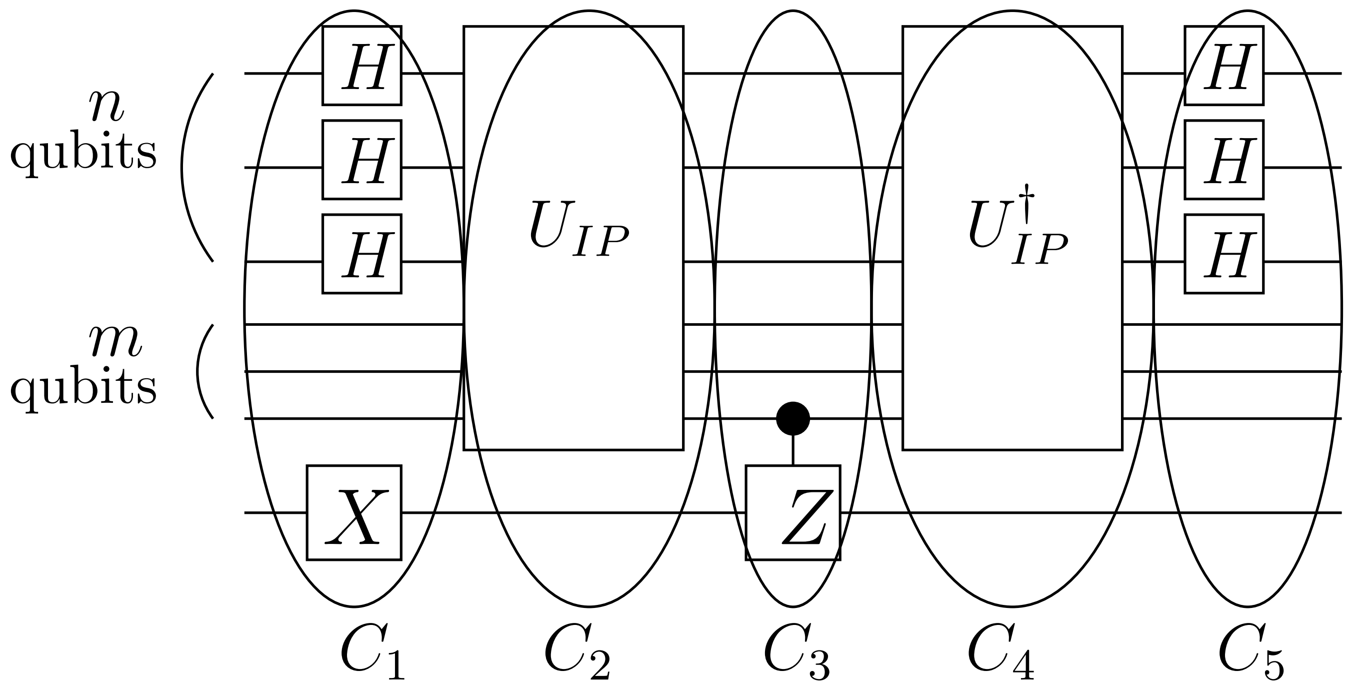


Figure 13: Decompose C

GOAL in detail

$$
\begin{aligned}
& \langle a, 0^m, 1| \cdot \boxed{C} \, |0^n, 0^m, 0\rangle \\
= \; & \langle a, 0^m, 1| \cdot \boxed{C_5 C_4 C_3 C_2 C_1} \, |0^n, 0^m, 0\rangle \\
= \; & \boxed{C_4^{-1} C_5^{-1}} \, \langle a, 0^m, 1| \cdot \boxed{C_3 C_2 C_1} \, |0^n, 0^m, 0\rangle \\
= \; & \boxed{C_4^{-1} C_5^{-1} \, \langle a| \, \langle 0^m| \, \langle 1|} \cdot \boxed{C_3 C_2 C_1 \, |0^n\rangle \, |0^m\rangle \, |0\rangle} \\
= \; & (\mathfrak{A}) \cdot (\mathfrak{B}) \geq 2\varepsilon
\end{aligned} \tag{28}
$$

Compute ($\mathfrak{B}$): stage C_1

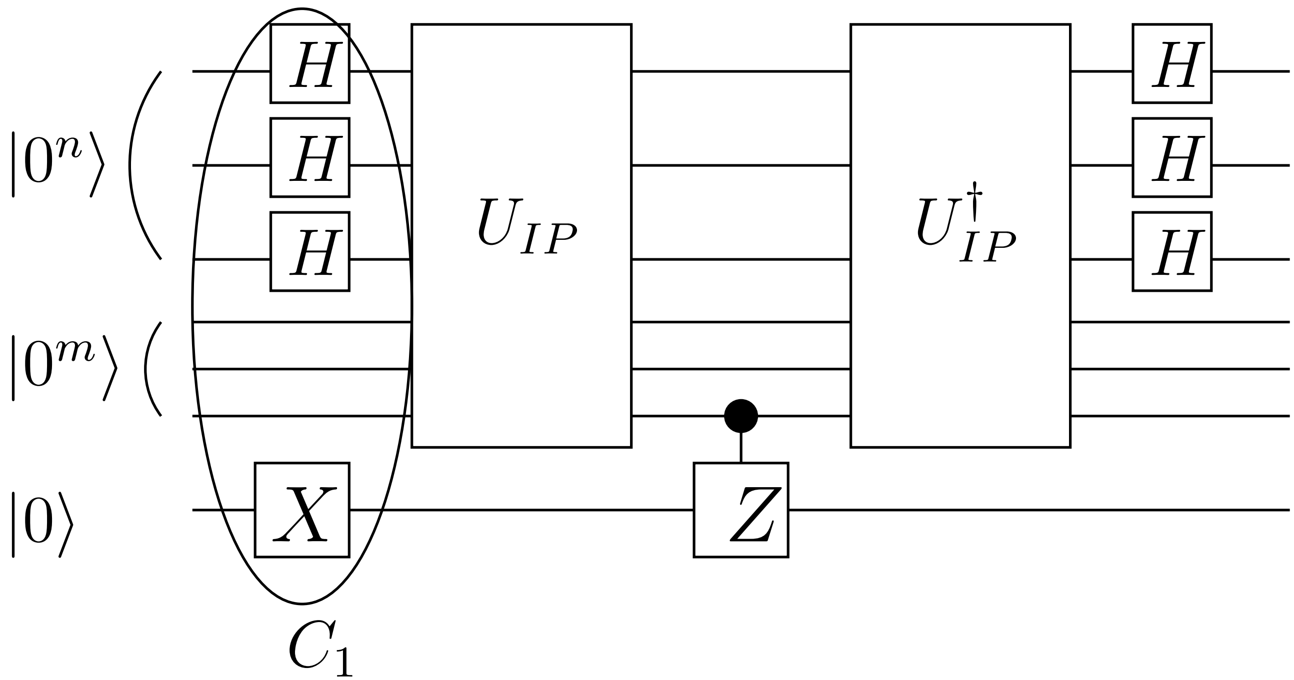


Figure 14: Apply H to the first n qubits and NOT to the last qubit.

$$
\begin{aligned}
& \boxed{C_1 \left|0^n\right\rangle} \left|0^m\right\rangle \left|\mathbf{0}\right\rangle \\
= \quad & \boxed{\tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x \in \{0,1\}^n} \left|x\right\rangle} \left|0^m\right\rangle \left|\mathbf{1}\right\rangle
\end{aligned} \tag{29}
$$

Compute ($\mathfrak{B}$): stage C_2

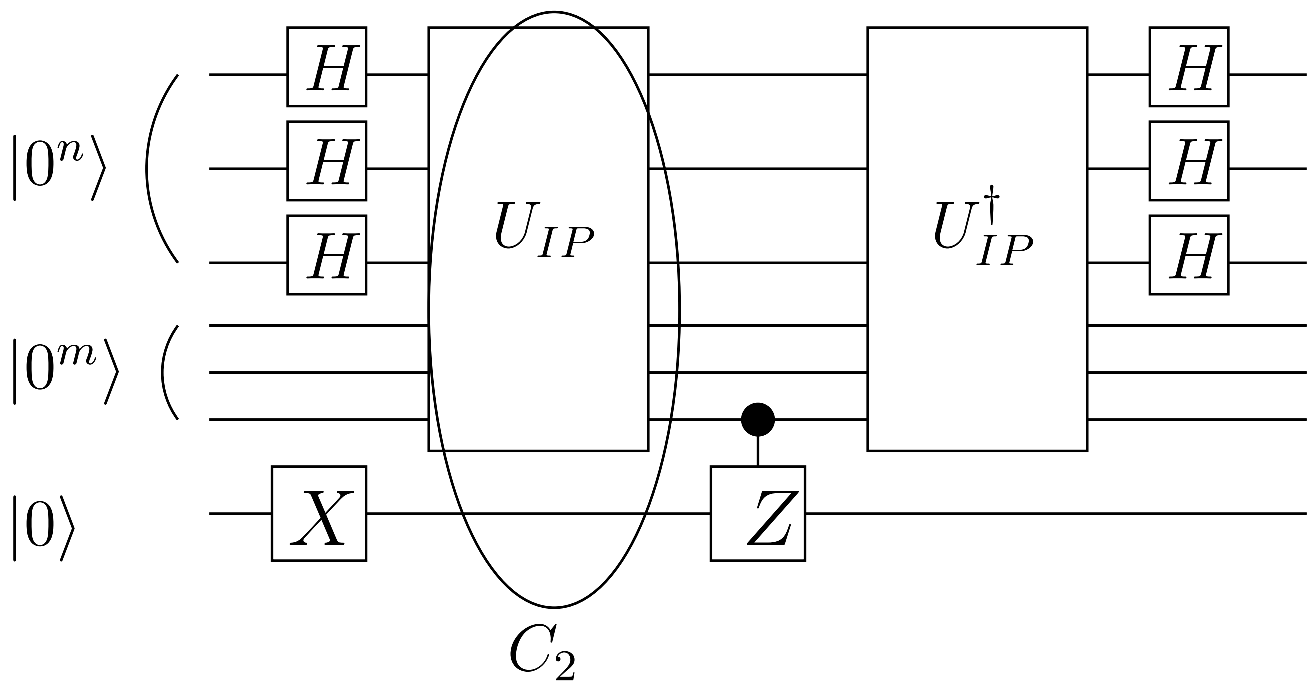


Figure 15: Apply U_{IP} to the first $n+m$ qubits.

$$
\begin{aligned}
C_2(29) &= C_2 \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \boxed{|0^m\rangle} |1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \boxed{(\alpha_x |v_x\rangle |a \cdot x\rangle + \beta_x |w_x\rangle |\overline{a \cdot x}\rangle)} |1\rangle
\end{aligned} \tag{30}
$$

Compute ($\mathfrak{B}$): stage C_3

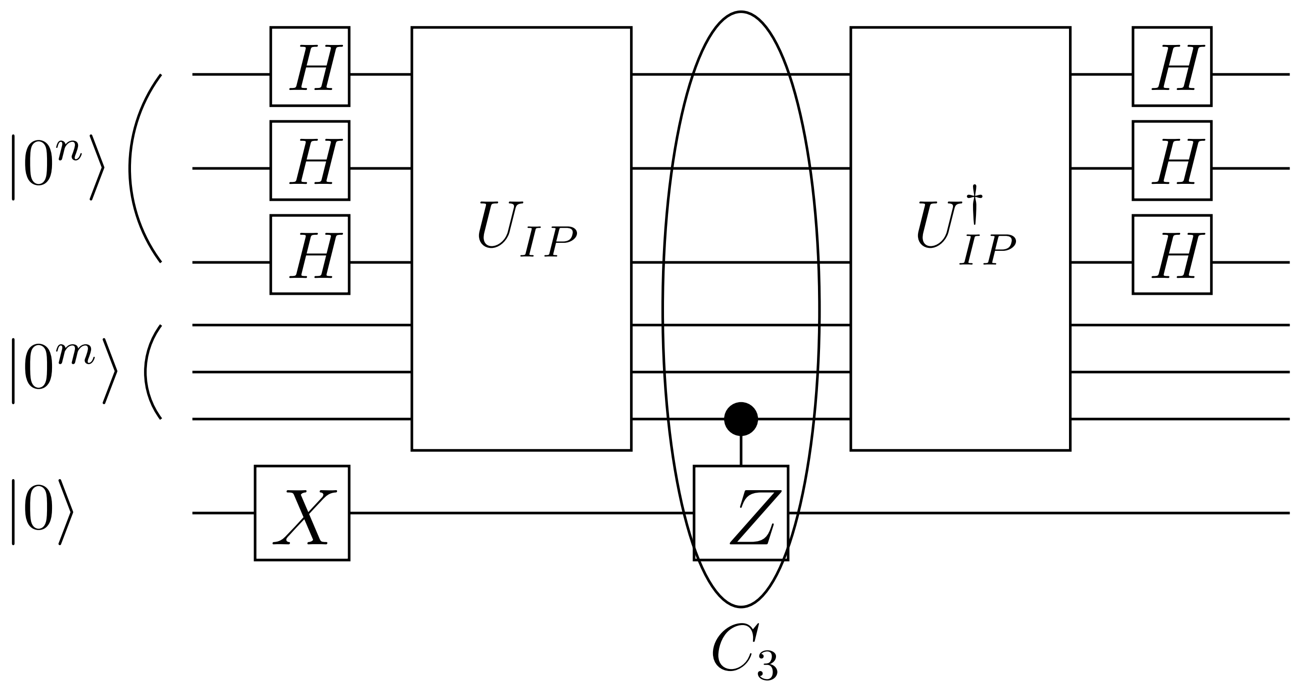


Figure 16: Apply controlled-Z to the last 2 qubits.

$$
\begin{aligned}
& C_3(30) \\
= \quad & C_3 \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \boxed{\left(\alpha_x |v_x\rangle |a \cdot x\rangle + \beta_x |w_x\rangle |\overline{a \cdot x}\rangle\right)} |1\rangle \\
= \quad & \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \underline{\left(\alpha_x (-1)^{a \cdot x} |v_x\rangle |a \cdot x\rangle\right)} |1\rangle \\
+ \quad & \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \underline{\left(\beta_x (-1)^{\overline{a \cdot x}} |w_x\rangle |\overline{a \cdot x}\rangle\right)} |1\rangle \\
= \quad & \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \boxed{(-1)^{a \cdot x}} |x\rangle \underline{\left(\alpha_x |v_x\rangle |a \cdot x\rangle\right)} |1\rangle \\
\boxed{-} \quad & \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \boxed{(-1)^{a \cdot x}} |x\rangle \underline{\left(\beta_x |w_x\rangle |\overline{a \cdot x}\rangle\right)} |1\rangle \\
= \quad & (\mathfrak{B}) \qquad (31)
\end{aligned}
$$

Compute ($\mathfrak{A}$): stage C_5

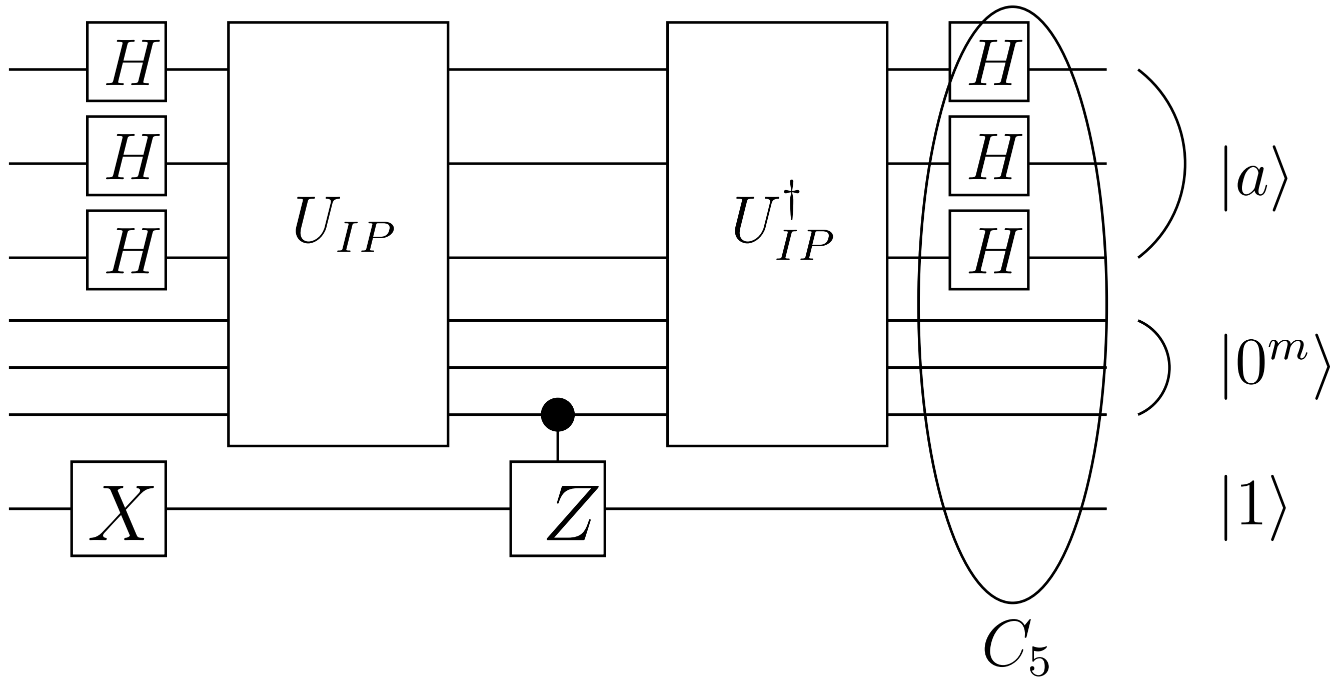


Figure 17: Apply H to the first n qubits.

$$\underline{C_5^{-1}\left|a\right\rangle}\left|0^m\right\rangle\left|1\right\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \left(\underline{(-1)^{a\cdot x}\left|x\right\rangle}\left|0^m\right\rangle\left|1\right\rangle\right) \tag{32}$$

Compute ($\mathfrak{A}$): stage C_4

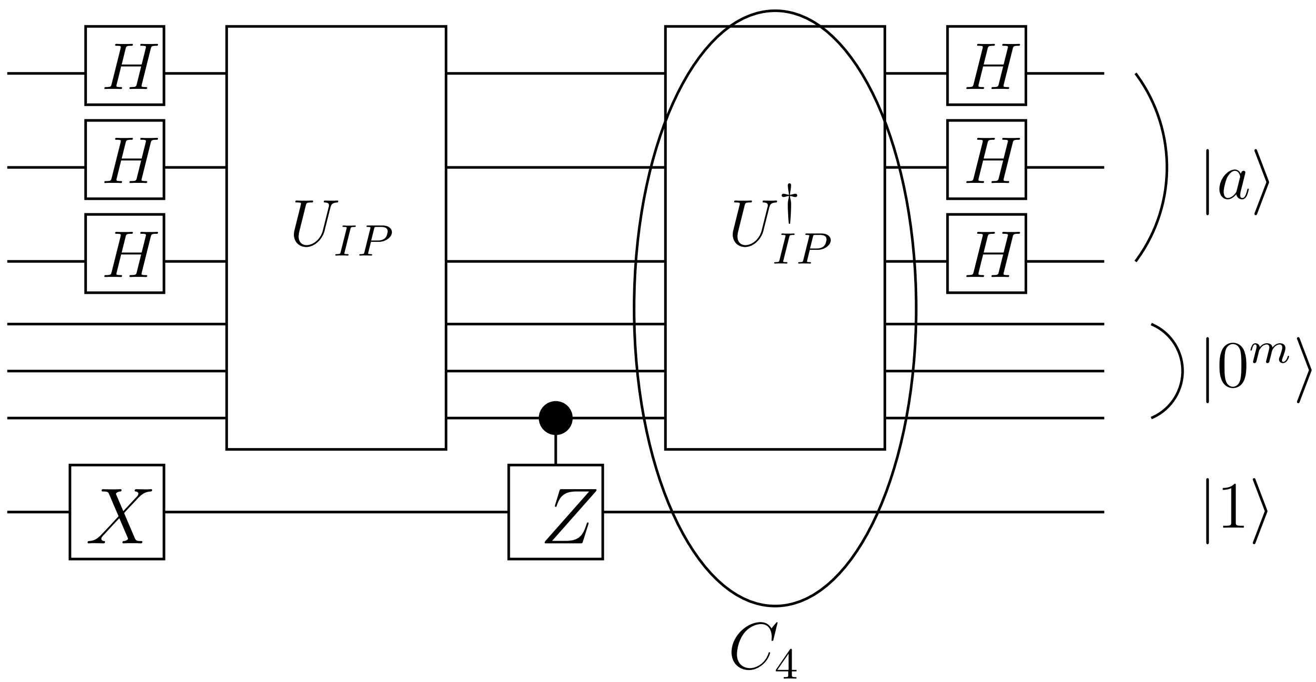


Figure 18: Apply U_{IP}^{-1} to the first $n+m$ qubits.

$$
\begin{aligned}
& C_4^{-1}(32) \\
= \quad & C_4^{-1}\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}\left((-1)^{a\cdot x}\left|x\right\rangle\left|0^m\right\rangle\left|1\right\rangle\right) \\
= \quad & \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}\left|x\right\rangle\underline{\left(\alpha_x\left|v_x\right\rangle\left|a\cdot x\right\rangle\right)}\left|1\right\rangle \\
\boxed{+} \quad & \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{a\cdot x}\left|x\right\rangle\underline{\left(\beta_x\left|w_x\right\rangle\left|\overline{a\cdot x}\right\rangle\right)}\left|1\right\rangle \\
= \quad & (\mathfrak{A}^{-1}) \qquad (33)
\end{aligned}
$$

Compute $(\mathfrak{A}) \cdot (\mathfrak{B})$: warmup!

$$(\mathfrak{A}) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \alpha_x \underline{((-1)^{a \cdot x} |x\rangle |v_x\rangle |a \cdot x\rangle |1\rangle)}$$

$$\boxed{+} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \beta_x \underline{((-1)^{a \cdot x} |x\rangle |w_x\rangle |\overline{a \cdot x}\rangle |1\rangle)}$$

$$(\mathfrak{B}) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \alpha_x \underline{((-1)^{a \cdot x} |x\rangle |v_x\rangle |a \cdot x\rangle |1\rangle)}$$

$$\boxed{-} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \beta_x \underline{((-1)^{a \cdot x} |x\rangle |w_x\rangle |\overline{a \cdot x}\rangle |1\rangle)}$$

Compute $(\mathfrak{A}) \cdot (\mathfrak{B})$

$$
\begin{aligned}
& (\mathfrak{A}) \cdot (\mathfrak{B}) \\
= \quad & \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \left(\alpha_x^2 - \beta_x^2\right) \\
= \quad & \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \alpha_x^2 \right) - \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \beta_x^2 \right) \\
\geq \quad & \left(\frac{1}{2} + \varepsilon \right) - \left(\frac{1}{2} - \varepsilon \right) = 2\varepsilon
\end{aligned} \tag{34}
$$

Boosting: achieve the GOAL in another way

- Previously known: repeat the quantum algorithm for $O(\varepsilon^{-\mathbf{2}})$ times.
- More effeciently: do the quantum algorithm once then apply the boosting algorithm:

$$Q \triangleq -C(U_0 \otimes I)C^{-1}(U_a \otimes I)$$

for $O(\varepsilon^{-\mathbf{1}})$ times. That is, compute $Q^{(t)} \cdot (C\,|0^n, 0^m, 0\rangle)$ for $t = O(\varepsilon^{-\mathbf{1}})$.

$$Q = -C(U_0 \otimes I)C^{-1}(U_a \otimes I)$$

- Revise C s.t. $(\langle a, 0^m, 1|) \cdot (C\,|0^n, 0^m, 0\rangle) \equiv 2\varepsilon$.
- U_a or U_0: apply to **the first** n **qubit**.
- I: apply to **the last** $m+1$ **qubits**.
- U_a:

$$U_a\,|x\rangle \triangleq \begin{cases} |x\rangle & x \neq a, \\ -\,|x\rangle & x = a. \end{cases}$$

  Alternative speaking, $U_a = I - 2\,|a\rangle\langle a|$.
- U_0: a kind of U_a when $a = 0^n$.

$$(U_a \otimes I) \xrightarrow{\text{drop } I} U_a$$

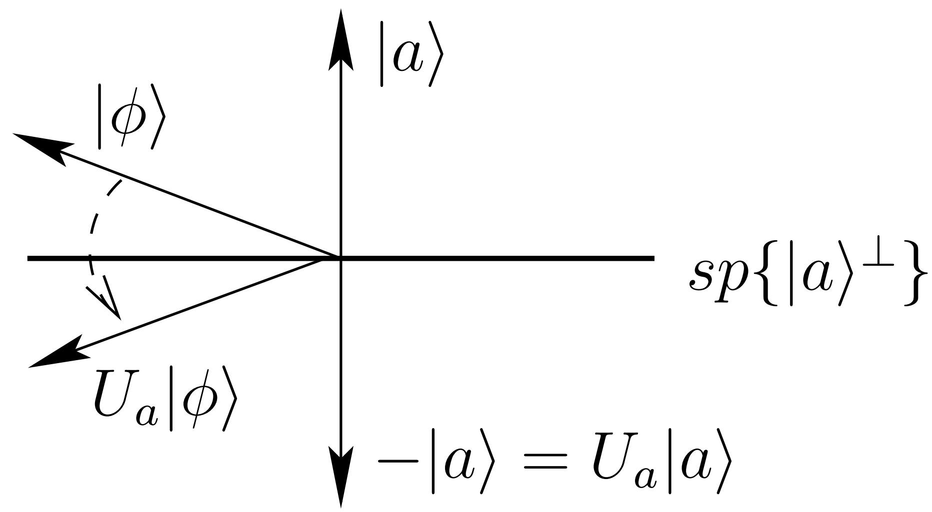


Figure 19: U_a: **refection** in the hyperplane $sp\{|a\rangle^{\perp}\}$

.

$C(U_0 \otimes I)C^{-1} = U_{C|0^n,z\rangle}$

- For $z \in \{0,1\}^{m+1}$:

$$\left(C(U_0 \otimes I)C^{-1}\right) \cdot \underline{C\,|0^n, z\rangle}$$
$$= C(U_0 \otimes I)\left(C^{-1}C\right)|0^n, z\rangle \quad = \quad \boxed{CU_0\,|0^n, z\rangle}$$
$$= \boxed{C\left(-\,|0^n, z\rangle\right)} \quad = \quad -C\,|0^n, z\rangle \qquad (35)$$

- For $y \in \{0,1\}^n$ and $y \neq 0^n$:

$$\left(C(U_0 \otimes I)C^{-1}\right) \cdot \underline{C\,|y, z\rangle} \quad = \quad C(U_0 \otimes I)\left(C^{-1}C\right)|y, z\rangle$$
$$= \boxed{CU_0\,|y, z\rangle} \quad = \quad \boxed{C\,|y, z\rangle} \qquad (36)$$

- Thus, $\boldsymbol{C}(U_{\mathbf{0}} \otimes I)\boldsymbol{C}^{-1} = U_{\underline{\boldsymbol{C}|\mathbf{0}^n,z\rangle}}$

$$-\boldsymbol{C}(U_{\mathbf{0}} \otimes I)\boldsymbol{C}^{-1} = -U_{\boldsymbol{C}|\mathbf{0}^n,z\rangle}$$

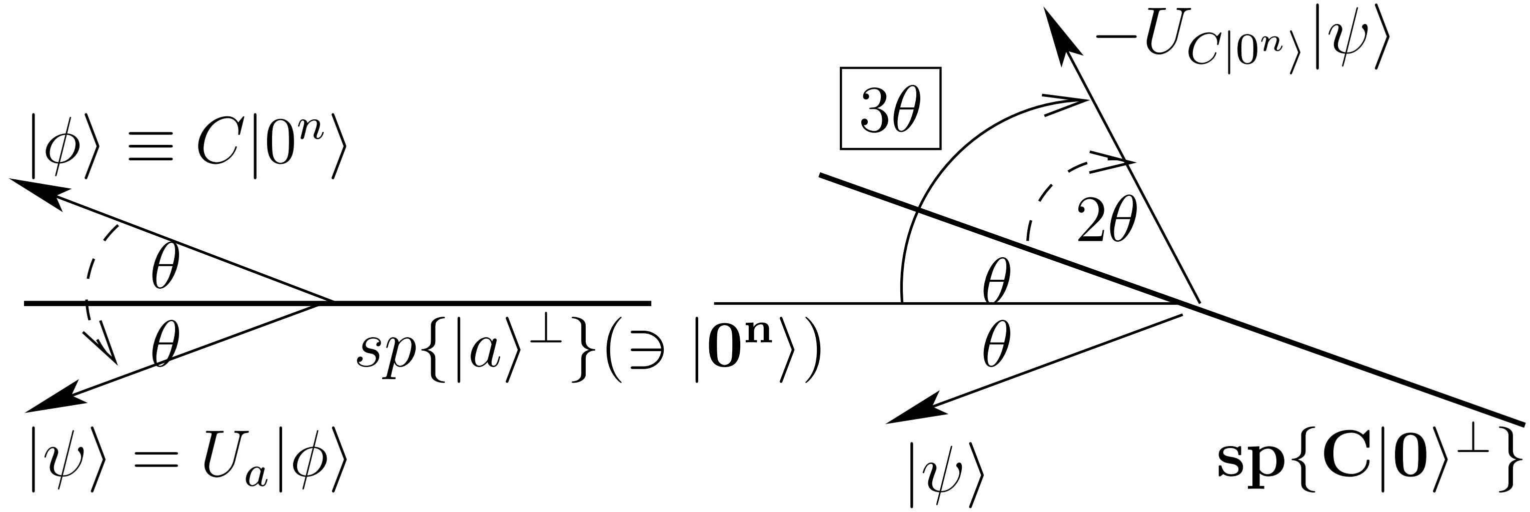


Figure 20: $-U_{C|0^n\rangle}$: **rotate** $|\phi\rangle$ **to alternative direction**.

- Recall that $Q = -C(U_0 \otimes I)C^{-1}(U_a \otimes I)$
- After querying Q for k times, $|0^n\rangle$ rotates by $(2k+1)\theta$.

Ratate towards $|a\rangle$

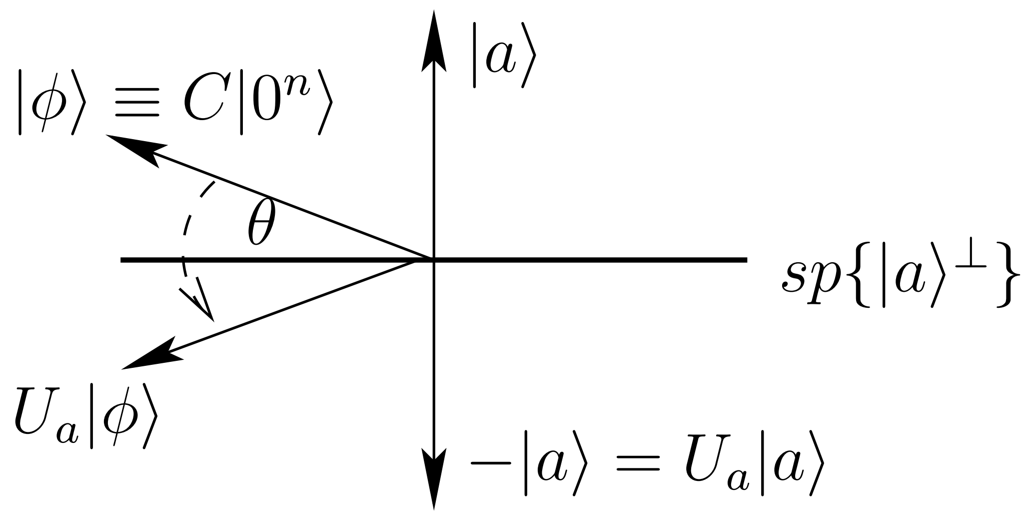


Figure 21: $\theta \equiv \sin^{-1}(\langle a| \cdot C\,|0^n\rangle) = \sin^{-1}(2\varepsilon)$

Boost the probability that $|a\rangle$ happens

- When $\sin((2k+1)\theta) = 1$, $Q^{(k)}\,|0^n, 0^m, 0\rangle = |a, 0^m, 1\rangle$.
- The minimun k which satisfies

$$\sin((2k+1)\theta) = 1 \quad \Longleftrightarrow \quad (2k+1)\theta = \frac{\pi}{2} \tag{37}$$

  is $\frac{\pi - \sin^{-1}(2\varepsilon)}{2\sin^{-1}(2\varepsilon)}$.

- Because $\sin^{-1}(2\varepsilon) \geq 2\varepsilon$ holds for small ε, we can estimate that

$$k = \frac{\pi - \sin^{-1}(2\varepsilon)}{2\sin^{-1}(2\varepsilon)} \leq \frac{\pi - 2\varepsilon}{2 \cdot 2\varepsilon} = \frac{\pi}{4\varepsilon} - \frac{1}{2} \in \underline{\underline{O(\frac{1}{\varepsilon})}}$$