A one-query lower bound for unitary synthesis and breaking quantum cryptography

Alex Lombardi, Fermi Ma, and John Wright (2023)

arXiv preprint arXiv:2310.08870v1

November 29th, 2025

Qisca Quantum Complexity Study

윤인희

Outline

- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

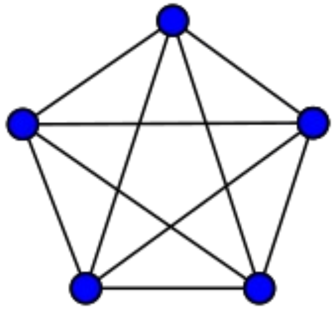
Outline

- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

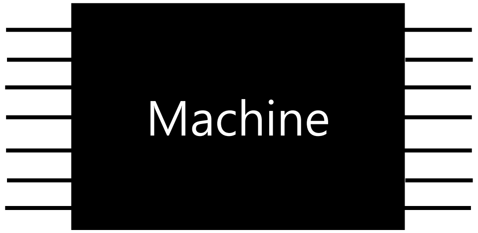
- Unitary Synthesis Problem

In Complexity theory, problems have classical inputs/outputs.

ex1) graph problem



encoding $01101\cdots$ input



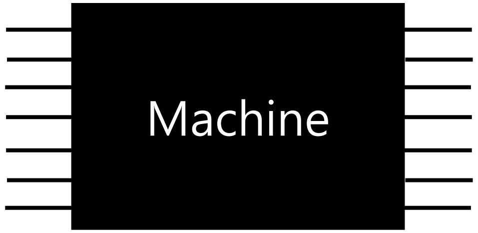
output 0 or 1

ex2) local Hamiltonian problem

Hamiltonian

$$H = \sum_{j=1}^{m} H_j$$

encoding $00111\cdots$ input



output 0 or 1

What about these quantum problems? – State tomography, State distinguishing, Error Correction, ..

Preliminaries

➔Solving a quantum problem means implementing unitary.

➔Complexity theory is about implementing functions.

To apply complexity theory, we need to **efficiently reduce** the task of implementing a unitary U to implementing a function f.

Definition (Unitary Synthesis Problem) [AK07, Aar16]

Is there a universal efficient oracle circuit $A^{(\cdot)}$ such that for any unitary U, there is a corresponding Boolean function f for which A^f implements U?

Definition 3.16 (formal version, Unitary Synthesis Problem)

Fix an error parameter $\varepsilon(n) = \frac{1}{2^{\Omega(n)}}$. Does there exist a poly(n)-query oracle circuit $A^{(\cdot)}$ computable by a poly(n)-sized quantum circuit such that for all n-qubit unitaries U, there exists a Boolean function $f: \{0,1\}^* \to \{\pm 1\}$ such that $D_\diamond\left(\Phi_{A^f}, \Phi_U\right) \leq \varepsilon(n)$?

Preliminaries

- [AK07]

For every choice of oracle f, the oracle circuit A^f is required to exactly implement an n-qubit unitary

-> In this special class, the number of distinct unitaries that a one-query oracle circuit A^f in this class ca n synthesize, is at most 4^{2^n}. (finite)

- [Ros22]

Number of oracle query to implement any n-qubit unitary U,

Upper bound : $U = O\left(2^{\frac{n}{2}}\right)$

Lower bound : None

- [Kre23]

If the Unitary Synthesis Problem is resolved in the positive,

existence of a secure PRS => $\mathrm{BPP} \neq \mathrm{NEXP}$

$\mathrm{unitaryBQP} \neq \mathrm{unitaryPSPACE}$ => $\mathrm{BPP} \neq \mathrm{NEXP}$

maybe? difficult to separate QCMA and QMA using a classical oracle

Outline

- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

The Oracle State Distinguishing Game

- single-copy PRS

Definition 5.1 (Pseudorandom state family)

Let $n: \mathbb{N} \to \mathbb{N}$ be a function and $\{|\psi_{\lambda,\mathrm{k}}\rangle\}_{k \in \{0,1\}^\lambda}$ be a family of a $n(\lambda)$-qubit quantum states for each $\lambda \in \mathbb{N}$. Thean the state family ensemble

$$\{|\psi_{\lambda,\mathrm{k}}\rangle_{k \in \{0,1\}^\lambda}\}_{\lambda \in \mathbb{N}}$$

Is a pseudorandom state (PRS) family if it has the following properties.

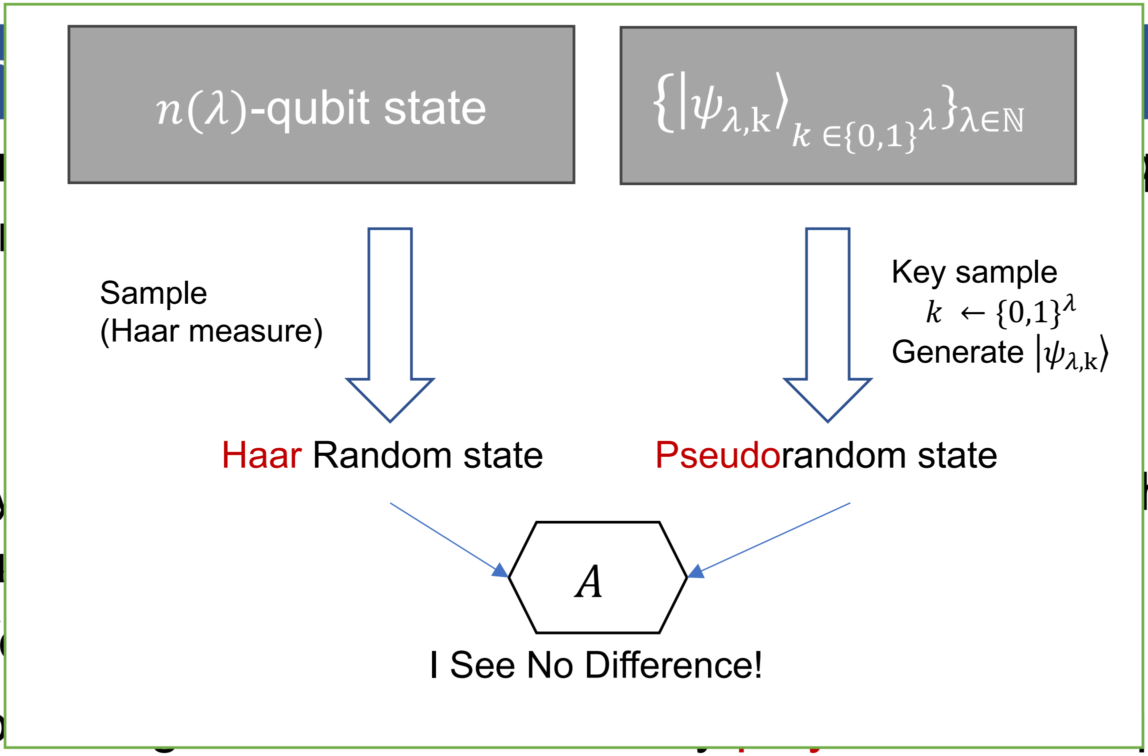
- Efficient constructability: there is a polynomial-time quantum algorithm that on input $(1^\lambda, k)$, for $k \in \{0,1\}^\lambda$, outputs $|\psi_{\lambda,\mathrm{k}}\rangle$
- Stretch: $n(\lambda) \geq \lambda + 1$, for all λ.
- Pseudorandomness: for all algorithms A described by polynomial-size quantum circuit families, we have that

$$\left|\Pr_{k \sim \{0,1\}^\lambda}\left[A\left(|\psi_{\lambda,\mathrm{k}}\rangle\right) \text{ outputs “0”}\right] - \Pr_{|\psi\rangle \sim Haar(n)}\left[A(|\psi\rangle) \text{ outputs “0”}\right]\right| \leq \mathrm{negl}(\lambda)$$

The Oracle State Distinguishing Game

- single-copy PRS

Definition 5.1 (Pseudoran



Let $n: \mathbb{N} \rightarrow \mathbb{N}$ be a functio … quantum states for each $\lambda \in \mathbb{N}$. Thean the state fa

Is a pseudorandom state

- Efficient constructability … hat on input $(1^\lambda, k)$, for $k \in \{0,1\}^\lambda$, outputs $|\psi_{\lambda,\mathrm{k}}$
- Stretch: $n(\lambda) \geq \lambda + 1$, f
- Pseudorandomness: fo … uantum circuit families, we have that

$$\left|\Pr_{k\sim\{0,1\}^\lambda}\left[A\left(|\psi_{\lambda,\mathrm{k}}\rangle\right) \text{ outputs "0"}\right] - \Pr_{|\psi\rangle\sim Haar(n)}\left[A(|\psi\rangle) \text{ outputs "0"}\right]\right| \leq \mathrm{negl}(\lambda)$$

The Oracle State Distinguishing Game

- PRS Construction

Definition 3.2 (binary phase state)

A Boolean function is function $h: \{0,1\}^n \to \{\pm 1\}$. Due to the associate between $\{0,1\}^n$ and $[N]$ ($N \coloneqq 2^n$), we will typically prefer to write such a function as $h: [N] \to \{\pm 1\}$, and we will elect to still refer to such a function as a "Boolean function". The corresponding binary phase state is

$$|\psi_h\rangle \coloneqq \frac{1}{\sqrt{N}} \sum_{x=1}^{N} h(x)\,|x\rangle$$

$$\mathbb{E}_{|\psi\rangle \sim Haar(n)}\left[|\psi\rangle\langle\psi|\right] = \mathbb{E}_h\left[|\psi_h\rangle\langle\psi_h|\right] = \mathbb{E}_{x\sim[N]}\left[|x\rangle\langle x|\right] = \frac{Id_N}{N}$$

Given that the adversary has only a single copy of the state and is limited to one query, the state ensemble is indistinguishable from a state 1-design.

So, using Haar random state is equivalent to using $|x\rangle$, where x is chosen uniformly at random from $[N]$.

$\left|\psi_{R_k}\right\rangle_{k\,\in[K]}$ is PRS, where uniformly random choice of the function family $R: [K]\times[N] \to \{\pm 1\}$

($R_k: [N] \to \{\pm 1\}$, $R \coloneqq \{R_k\}_{k\in[K]}$ $(K \ll R)$, adversary will be selected an oracle f_R which depends on R)

The Oracle State Distinguishing Game

- Oracle State Distinguishing Game (denoted $Game^R$)

$Game^R$ involves two parties, a challenger and an adversary.

Step 1.

Challenger $\xleftarrow{b}$ $\{0,1\}$

Uniformly random sample

Step 2.

If $b = 0$, Challenger $\xleftarrow{k}$ $[K]$

Generate $|\psi_{R_k}\rangle$

Uniformly random sample

If $b = 1$, Challenger $\xleftarrow{h}$ $h: \{0,1\}^n \to \{\pm 1\}$

Generate $|\psi_h\rangle$

Uniformly random sample

The Oracle State Distinguishing Game

Step 3.

Challenger → Adversary

send $|\psi_{R_k}\rangle$ or $|\psi_h\rangle$

Step 4.

Adversary → Output $b' = 0 \text{ or } 1$

Step 5.

If $b = b'$, Adversary win.

If $b \neq b'$, Adversary lose.

The Oracle State Distinguishing Game

- Relationship to the Unitary Synthesis Problem

If the Unitary Synthesis Problem is resolved in the positive,

=> for random U and any $K < N$, there exists (with high probability) a choice of f such that A^f implements the channel corresponding U.

=> For a Haar-random subspace $S = span\{U^\dagger|1\rangle, \dots, U^\dagger|K\rangle\}$,
there exists f such that A^f maps S to $span\{|1\rangle, \dots, |K\rangle\}$

$\because A^f(U^\dagger|i\rangle) \approx |i\rangle$ for all $i \in [K]$

=> If $b = 0$, $A^f\left|\psi_{R_k}\right\rangle \in span\{|1\rangle, \dots, |K\rangle\}$ (w.h.p.)

If $b = 1$, $A^f|\psi_h\rangle \notin span\{|1\rangle, \dots, |K\rangle\}$ (w.h.p.)

=> A^f can be a distinguisher between PRS and Haar random state.

=> secure PRS cannot exist.

=> In the Oralce State Distinguishing Game, the Adversary always win.

A bound on the Adversary's failure => A lower bound on the Unitary Synthesis Problem.

The Oracle State Distinguishing Game

Claim 3.17

If the maximum distinguishing advantage of any efficient t-query adversary in the oracle distinguishing game is $o(1)$, then there is no efficient t-query oracle algorithm for the Unitary Synthesis Problem on a Haar-random unitary U.

Outline

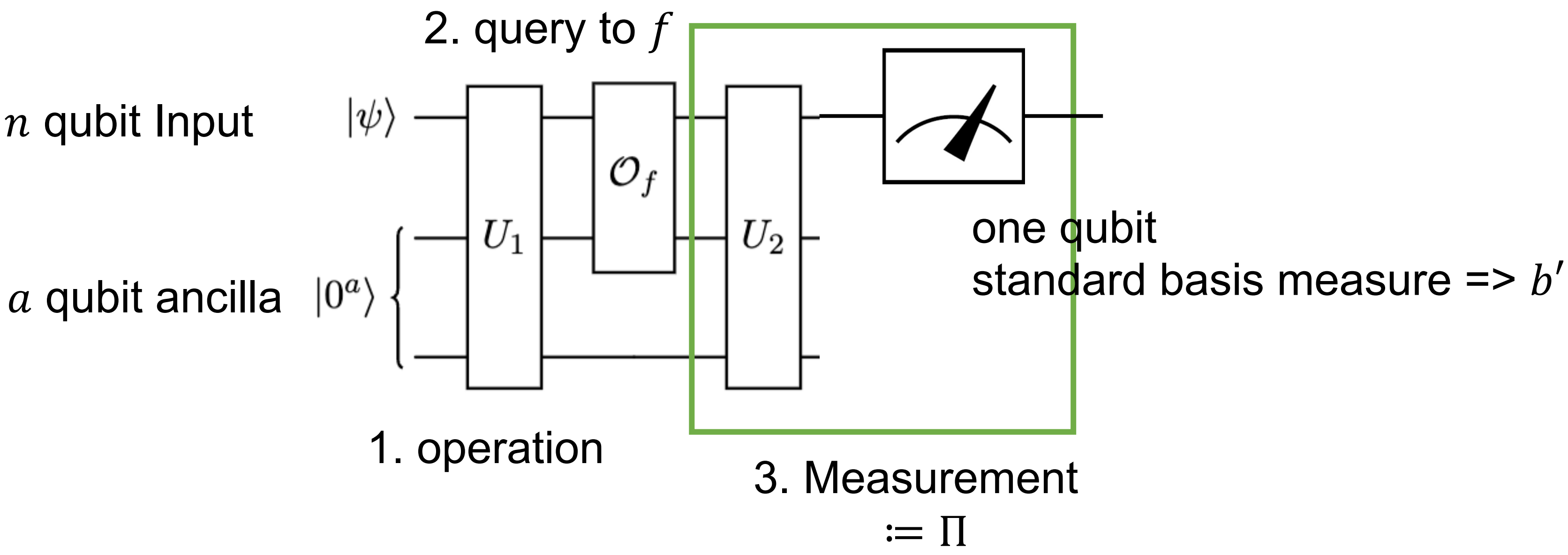
- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

Modeling the adversary

- Adversary (Definition 3.10)

$$O_f = \sum_{i=1}^{L} f(i) \cdot |i\rangle\langle i|$$

where $f:\{0,1\}^l \to \{\pm 1\}$, $2^l = L$, and O_f : $L \times L$ diagonal matrix



=> Measurement $\{\Pi, I - \Pi\}$

=>$\Pr[b' = 1] = \Pr\left[A^f(|\psi\rangle) \text{ outputs } 1\right] = \langle\psi|\langle 0|\left(\Pi O_f U_1\right)^\dagger \cdot \left(\Pi O_f U_1\right)|0\rangle|\psi\rangle$

Modeling the adversary

If $b = 0$, $\Pr[\text{adversary win}] = \Pr[b' = 0] = 1 - \mathop{\mathbb{E}}_{k\sim[K]} \Pr\left[A^f(|\psi_{R_k}\rangle) \text{ outputs } 1\right]$

If $b = 1$, $\Pr[\text{adversary win}] = \Pr[b' = 1] = \mathop{\mathbb{E}}_{h} \Pr\left[A^f(|\psi_h\rangle) \text{ outputs } 1\right]$

=> $\Pr[\text{adversary win}] = \frac{1}{2}\left(1 - \mathop{\mathbb{E}}_{k\sim[K]} \Pr\left[A^f(|\psi_{R_k}\rangle) \text{ outputs } 1\right]\right) + \frac{1}{2}\left(\mathop{\mathbb{E}}_{h} \Pr\left[A^f(|\psi_h\rangle) \text{ outputs } 1\right]\right)$

$$= \frac{1}{2} - \frac{1}{2}\left(\mathop{\mathbb{E}}_{k\sim[K]} \Pr\left[A^f(|\psi_{R_k}\rangle) \text{ outputs } 1\right] - \mathop{\mathbb{E}}_{h} \Pr\left[A^f(|\psi_h\rangle) \text{ outputs } 1\right]\right)$$

$=: \frac{1}{2} + \frac{1}{2}\Delta_{\mathrm{A}}(R|f)$ (Definition 3.12)

=> Adversary try to maximize $\Delta_{\mathrm{A}}(R|f)$

$$\Delta_{\mathrm{A}}(R) := \max_{f:[L]\to\{\pm 1\}} \left|\mathop{\mathbb{E}}_{k\sim[K]} \Pr\left[A^f(|\psi_{R_k}\rangle) \text{ outputs } 1\right] - \mathop{\mathbb{E}}_{h} \Pr\left[A^f(|\psi_h\rangle) \text{ outputs } 1\right]\right| = \max_{f:[L]\to\{\pm 1\}} \Delta_{\mathrm{A}}(R|f)$$

Finally, maximum distinguishing advantage of $A^{(\cdot)}$ on $Game_{K,N}$ is (Definition 3.13)

$$\Delta_A^{avg} := \mathop{\mathbb{E}}_{R}[\Delta_{\mathrm{A}}(R)]$$

Modeling the adversary

- Upper tail inequality for $\Delta_{\mathrm{A}}(R)$

Theorem 3.20 (Talagrand's concentration inequality)

There exists a constant $c > 0$ such that the following is true. Let $g: [-1,1]^d \to \mathbb{R}$ be a convex function with Lipschitz constant C. Let $v_1, \dots, v_d$ be independent random variables satisfying $|v_i| \leq 1$ for all $1 \leq i \leq d$. Then for $t \geq 0$,

$$\Pr[|g(v_1, \dots, v_d) - \mathbb{E}[g(v_1, \dots, v_d)]| \geq t] \leq 2 \cdot \exp\left(-c \cdot \frac{t^2}{C^2}\right)$$

For $R: [K]\times[N] \to \{\pm 1\}$, $\Delta_{\mathrm{A}}(R)$ is a convex function

and $|\Delta_{\mathrm{A}}(R) - \Delta_{\mathrm{A}}(R')| \leq \frac{2}{\sqrt{KN}} \|R - R'\|_2$. (by Lemma 3.26.)

Since each family R is mutually independent and uniformly random,

$(g = \Delta_{\mathrm{A}}, C = \frac{2}{\sqrt{KN}}, k = \varepsilon)$

then $\Pr[|\Delta_{\mathrm{A}}(R) - \Delta_A^{avg}| \geq \varepsilon] \leq 2 \cdot \exp\left(-c \cdot \frac{\varepsilon^2 KN}{4}\right)$

Modeling the adversary

- Upper tail inequality for $\Delta_{\mathrm{A}}(R)$

Theorem 3.20 (Talagrand's concentration inequality)

There exists a constant $c > 0$ such that the following is true. Let $g: [-1,1]^d \to \mathbb{R}$ be a convex function with Lipschitz constant C. Let $v_1, \ldots, v_d$ be independent random variables satisfying $|v_i| \leq 1$ for all $1 \leq i \leq d$. Then for $t > 0$

$$\Pr[\Delta_{\mathrm{A}}(R) \geq \Delta_A^{avg} + \varepsilon] \leq 4 \cdot \exp(-c\varepsilon^2 KN) \qquad \text{(Lemma 3.18)}$$

For $R: [K] \times [N]$

and $|\Delta_{\mathrm{A}}(R) - \Delta$

Since each family R is mutually independent and uniformly random,

$(g = \Delta_{\mathrm{A}},\ C = \frac{2}{\sqrt{KN}},\ k = \varepsilon)$

then $\Pr[|\Delta_{\mathrm{A}}(R) - \Delta_A^{avg}| \geq \varepsilon] \leq 2 \cdot \exp\left(-c \cdot \frac{\varepsilon^2 KN}{4}\right)$

Modeling the adversary

- Is the number of qubits used by the adversary sufficiently small?

Define isometry $V := U_1 \cdot (Id \otimes |0^a\rangle)$ where $V: \mathbb{C}^{2^n} \to \mathcal{H}_{query} \otimes \mathbb{C}^{2^{n+a-l}}$ (i.e. $U_1|\psi\rangle|0^a\rangle = V|\psi\rangle$)

=> Define $compress(V) := \sum_{z=1}^{L} |z\rangle \otimes \sqrt{M_z}$ where $M_z := V^\dagger(|z\rangle\langle z| \otimes Id_{2^a})V$ (Definition 3.30)

=> There exist isometry $T: \mathcal{H}_{query} \otimes \mathbb{C}^{2^n} \to \mathcal{H}_{query} \otimes \mathbb{C}^{2^{n+a-l}}$,

such that $T \cdot (O_f \otimes Id_{2^n}) \cdot compress(V) = (O_f \otimes Id_{2^{n+a-l}}) \cdot V$ (Lemma 3.32)

(because of matching inner product)

=> (left hand side) $compress(V): \mathbb{C}^{2^n} \to \mathcal{H}_{query} \otimes \mathbb{C}^{2^n}$ (dimension of codomain is 2^{n+l})

(right hand side) $V: \mathbb{C}^{2^n} \to \mathcal{H}_{query} \otimes \mathbb{C}^{2^{n+a-l}}$ (dimension of codomain is 2^{n+a-l})

=> An $(n+a)$-qubit oracle circuit querying O_f can be compressed to a size of $n+l$. (Lemma 3.29.)

Outline

- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

The one query lower bound and one-copy PRS

- Matrix Concentration

Theorem 4.10 (Concentration for matrix Rademacher series)

Let $x_1, \ldots, x_n$ be n independent, uniformly distributed $\{\pm 1\}$ random variables. Let $\boldsymbol{Z}$ be a $d_1 \times d_2$ complex matrix whose entries are linear combinations of the x_k's, i.e.

$$\boldsymbol{Z}_{i,j} = c_{i,j,1} \cdot x_1 + \cdots + c_{i,j,n} \cdot x_n,$$

where each $c_{i,j,k}$ is a fixed, complex number. Let $v(\boldsymbol{Z})$ be the matrix variance statistic of $\boldsymbol{Z}$, i.e.

$$v(\boldsymbol{Z}) = \max\{\left\|\mathbb{E}[\boldsymbol{Z} \cdot \boldsymbol{Z}^\dagger]\right\|_{op}, \left\|\mathbb{E}[\boldsymbol{Z}^\dagger \cdot \boldsymbol{Z}]\right\|_{op}\}$$

Then

$$\|\mathbb{E}[\boldsymbol{Z}]\|_{op} \leq \sqrt{2\ln(d_1 + d_2)} \cdot \sqrt{v(\boldsymbol{Z})}$$

Furthermore, for all $t \geq 0$,

$$\Pr\left[\|\boldsymbol{Z}\|_{op} \geq t\right] \leq (d_1 + d_2) \cdot \exp\left(-\frac{t^2}{2 \cdot v(\boldsymbol{Z})}\right)$$

The one query lower bound and one-copy PRS

First, $V = \sum_{i=1}^{2^m} \sum_{x=1}^{2^n} v_{i,x} |i\rangle\langle x| = \sum_{i=1}^{2^m} |i\rangle\langle v_i|$ $\quad (m = n + l,\ |v_i\rangle \coloneqq \sum_{x=1}^{2^n} v_{i,x}^* \, |x\rangle)$

=> $V \cdot |\psi_h\rangle = \sum_{i=1}^{2^m} |i\rangle\langle v_i|\psi_h\rangle = \sum_{i=1}^{2^m} \frac{\langle v_i|\psi_h\rangle}{\sqrt{wt_{V,i}}} \cdot \sqrt{wt_{V,i}} |i\rangle$ (by Definition 4.1., $wt_{V,i} \coloneqq \frac{\langle v_i|v_i\rangle}{2^n}$)

$= \sum_{i=1}^{2^m} \frac{\langle v_i|\psi_h\rangle}{\sqrt{wt_{V,i}}} \cdot \sqrt{wt_{V,i}} |i\rangle = \sum_{i=1}^{2^m} D_{V,h,i} \cdot \sqrt{wt_{V,i}} |i\rangle$ (by Definition 4.6. $D_{V,h,i} \coloneqq \frac{\langle v_i|\psi_h\rangle}{\sqrt{wt_{V,i}}}$)

$= D_{V,h} \cdot |wt_V\rangle$ (by Definition 4.5. $|wt_V\rangle = \sum_{i=1}^{2^m} \sqrt{wt_{V,i}} |i\rangle$

=> $\langle \psi_h | V^\dagger O_f \Pi O_f V | \psi_h \rangle = \langle wt_V | D_{V,h}^\dagger O_f \Pi O_f D_{V,h} | wt_V \rangle = \langle wt_V | O_f (D_{V,h}^\dagger \Pi D_{V,h}) O_f | wt_V \rangle$

Also, $\langle \psi_{R_k} | V^\dagger O_f \Pi O_f V | \psi_{R_k} \rangle = \langle wt_V | O_f (D_{V,R_k}^\dagger \Pi D_{V,R_k}) O_f | wt_V \rangle$

=> Let $\boldsymbol{Z} = \mathbb{E}_{k\sim[K]}[D_{V,R_k}^\dagger \Pi D_{V,R_k'}]$

by definition of R_k, if $\boldsymbol{Z}_{i,j} = c_{i,j,1} \cdot x_1 + \cdots + c_{i,j,n} \cdot x_n$, then x_i's are mutually independent and unform.

The one query lower bound and one-copy PRS

=> $\underset{R}{\mathbb{E}}[\boldsymbol{Z} \cdot \boldsymbol{Z}^\dagger] = \frac{1}{K^2}\sum_{k,k'=1}^{K} D_{V,R_k}^\dagger \Pi^2 D_{V,R'_{k'}} \preccurlyeq \frac{1}{K}\sum_{i=1}^{2^m}\left(\frac{1}{K}\sum_{k=1}^{K}\frac{\left|\langle v_i|\psi_{R_k}\rangle\right|^2}{wt_{V,i}}\right)|i\rangle\langle i| \preccurlyeq \frac{width(R)}{K} Id_{2^m}$

where $width(R) \coloneqq \max_{1\le i\le M} \frac{1}{K}\sum_{k=1}^{K}\frac{\left|\langle v_i|\psi_{R_k}\rangle\right|^2}{wt_{V,i}}$

Therefore, $\left\|\mathbb{E}[\boldsymbol{Z} \cdot \boldsymbol{Z}^\dagger]\right\|_{op} \le \frac{width(R)}{K}$

In the same way, $\left\|\mathbb{E}[\boldsymbol{Z}^\dagger \cdot \boldsymbol{Z}]\right\|_{op} \le \frac{width(R)}{K}$ => $v(\boldsymbol{Z}) \le \frac{width(R)}{K}$, $d_1 = d_2 = 2^m =: M$

by Theorem 4.10.

$$\underset{R'}{\mathbb{E}}\left[\left\|\underset{k\sim[K]}{\mathbb{E}}[D_{V,R_k}^\dagger \Pi D_{V,R'_k}]\right\|_{op}\right] \le \sqrt{2\ln(2M)} \cdot \sqrt{\frac{width(R)}{K}}$$

(Lemma 4.11.)

The one query lower bound and one-copy PRS

$$\max_{f:[L]\to\{\pm 1\}} \left| \mathbb{E}_{k\sim[K]} [\langle \psi_{R_k} | V^\dagger O_f \Pi O_f V | \psi_{R'_k} \rangle] \right|$$

$$= \max_{f:[L]\to\{\pm 1\}} \left| \langle wt_V | O_f \mathbb{E}_{k\sim[K]} \left[D^\dagger_{V,R_k} \Pi D_{V,R'_k} \right] O_f | wt_V \rangle \right|$$

$$\leq \max_{\|v\|=1} \left| \langle v | \mathbb{E}_{k\sim[K]} \left[D^\dagger_{V,R_k} \Pi D_{V,R'_k} \right] | v \rangle \right|$$

$$= \left\| \mathbb{E}_{k\sim[K]} [D^\dagger_{V,R_k} \Pi D_{V,R'_k}] \right\|_{op} \qquad \text{(Lemma 4.9.)}$$

=> By combining the two inequality,

$$\mathbb{E}_{R'} \left[\max_{f:[L]\to\{\pm 1\}} \left| \mathbb{E}_{k\sim[K]} [\langle \psi_{R_k} | V^\dagger O_f \Pi O_f V | \psi_{R'_k} \rangle] \right| \right] \leq \sqrt{2 \ln(2M)} \cdot \sqrt{\frac{width(R)}{K}}$$

=> $$\Delta_A^{avg} = \mathbb{E}_{R} \left[\max_{f:[L]\to\{\pm 1\}} \left| \mathbb{E}_{k\sim[K]} \langle \psi_{R_k} | V^\dagger O_f \Pi O_f V | \psi_{R_k} \rangle - \mathbb{E}_{h} \langle \psi_h | V^\dagger O_f \Pi O_f V | \psi_h \rangle \right| \right]$$

$$\leq 4 \cdot \mathbb{E}_{R,R'} \max_{f:[L]\to\{\pm 1\}} \left| \mathbb{E}_{k\sim[K]} [\langle \psi_{R_k} | V^\dagger O_f \Pi O_f V | \psi_{R'_k} \rangle] \right| \qquad \text{(Lemma 4.3.)}$$

The one query lower bound and one-copy PRS

=> Combining the two inequality,

$$\Delta_A^{avg} \leq 4 \cdot \mathbb{E}_R\left[\sqrt{2\ln(2M)} \cdot \sqrt{\frac{width(R)}{K}}\right] \leq 4\sqrt{\frac{2\ln(2M)}{K}} \cdot \sqrt{\mathbb{E}_R[width(R)]}$$ (by, Jensen's inequality)

=> If $width(R) \geq 1 + \alpha$,

$$\begin{aligned}\mathbb{E}_R[width(R)] &= \int_0^\infty \Pr[width(R) \geq t]\, dt \\ &= \int_0^{1+\alpha} \Pr[width(R) \geq t]\, dt + \int_{1+\alpha}^\infty \Pr[width(R) \geq t]\, dt \\ &\leq 1 + \alpha + \frac{2M}{c}\exp(-cK \cdot \alpha) \\ &= C\end{aligned}$$

(α, M, K, c are all constants, Lemma 4.16.)

=> $\Delta_A^{avg} \leq 4\sqrt{\frac{2C\ln(2M)}{K}} \leq C_1\sqrt{\frac{\ln(M)}{K}}$ (Theorem 4.17)

=> combining with $\Pr[\Delta_\mathrm{A}(R) \geq \Delta_A^{avg} + \varepsilon] \leq 4 \cdot \exp(-c\varepsilon^2 KN)$,

The one query lower bound and one-copy PRS

=> Combining the two inequality,

$$\Delta_A^{avg} \leq 4 \cdot \mathop{\mathbb{E}}_{R}\left[\sqrt{2\ln(2M)} \cdot \sqrt{\frac{width(R)}{K}}\right] \leq 4\sqrt{\frac{2\ln(2M)}{K}} \cdot \sqrt{\mathop{\mathbb{E}}_{R}[width(R)]}$$ (by, Jensen's inequality)

=> If $width(R) \geq 1 + \alpha$

$\mathop{\mathbb{E}}_{R}[width($

$=$

$\leq$

$= C$ (α, M, K, c are all constants, Lemma 4.16.)

$$\Pr[\Delta_A(R) \geq C_1\sqrt{\frac{\ln(M)}{K}} + \varepsilon] \leq 4 \cdot \exp(-C_2\varepsilon^2 KN)$$ (Theorem 4.18)

=> $\Delta_A^{avg} \leq 4\sqrt{\frac{2C\ln(2M)}{K}} \leq C_1\sqrt{\frac{\ln(M)}{K}}$ (Theorem 4.17)

=> combining with $\Pr[\Delta_A(R) \geq \Delta_A^{avg} + \varepsilon] \leq 4 \cdot \exp(-c\varepsilon^2 KN)$,

The one query lower bound and one-copy PRS

w.h.p.,

$$\Delta_{\mathrm{A}}(R) \leq O\left(\sqrt{\frac{\ln(M)}{K}}\right)$$

If $\ln(M) \ll K$, then $\Delta_{\mathrm{A}}(R) = o(1)$,

Claim 3.17

If the maximum distinguishing advantage of any efficient t-query adversary in the oracle distinguishing game is $o(1)$, then there is no efficient t-query oracle algorithm for the Unitary Synthesis Problem on a Haar-random unitary U.

The one query lower bound and one-copy PRS

w.h.p.,

$$\Delta_{\mathrm{A}}(R) \leq O\left(\sqrt{\frac{\ln(M)}{K}}\right)$$

If $\ln(M) \ll K$, then $\Delta_{\mathrm{A}}(R) = o(1)$,

Claim

If the r

disting

Synthe

Conclusion : There is no efficient 1-query oracle algorithm for the Unitary Synthesis Problem on a Haar-random unitary U.

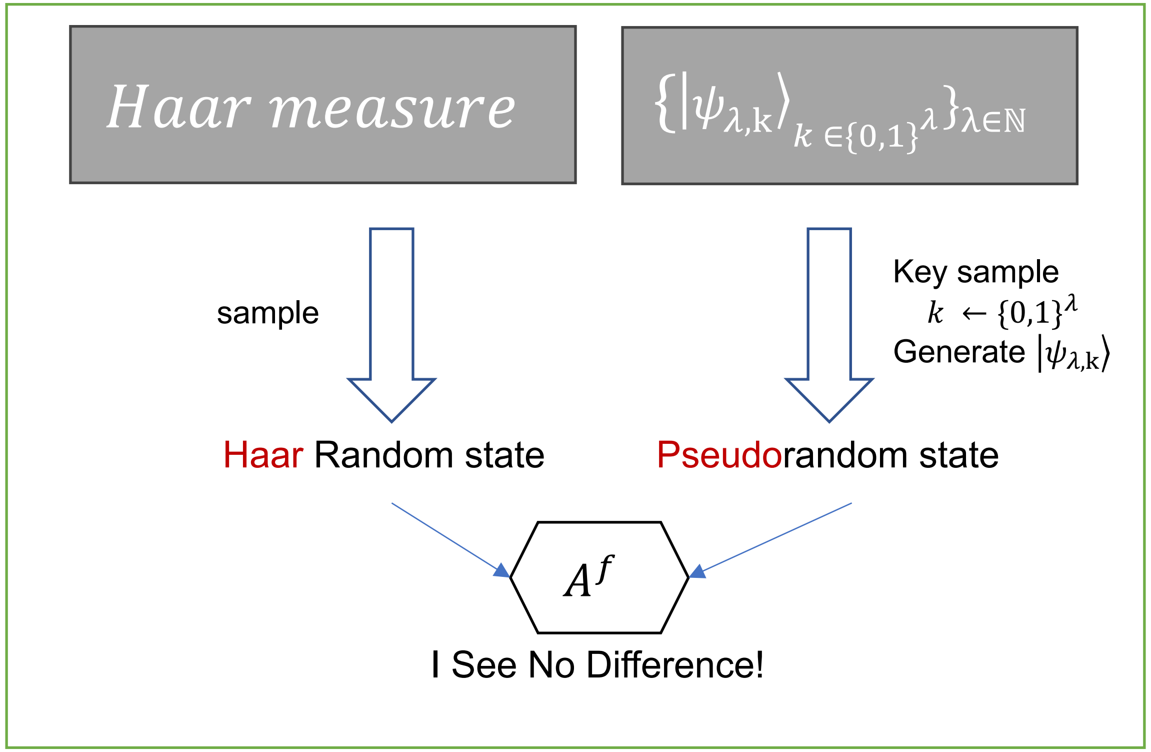
The one query lower bound and one-copy PRS

- existence of secure PRS

Any one-query algorithm A^f fails the Oracle State Distinguishing Game w.h.p.

=> By definition of PRS,

there exists a PRS secure against all one-query oracle algorithms A^f for every Boolean function f.



The one query lower bound and one-copy PRS

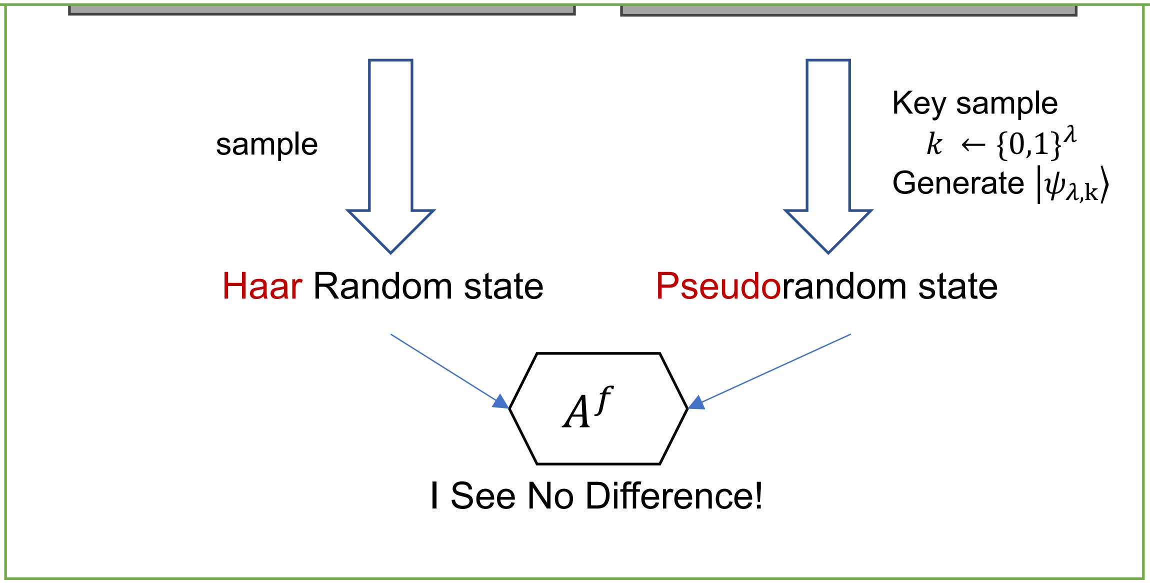
- existence of secure PRS

Any one-query algorithm A^f fails the Oracle State Distinguishing Game w.h.p.

=> By definition of PRS,

there exists a PRS secure against all one-query oracle algorithms A^f for every Boolean function f

[KQST23] Secure PRS exists with adversary A^O (classical oracle O s.t. $P^O = NP^O$)
+ without the assumption of one-way function.
This paper : Secure PRS exists with adversary A^f + without the assumption of one-way function



Outline

- Preliminaries
- The Oracle State Distinguishing Game
- Modeling the adversary
- The one query lower bound and single-copy PRS
- Future Direction

Future Direction

- 1.5-query (Conjecture 2.5.)

For any subset $S \subseteq [L]$,

$$\max_{S\subseteq[L]} \max_{f:[L]\to\{\pm 1\}} \left| \mathop{\mathbb{E}}_{k\sim[K]} \langle \psi_{R_k} | V^\dagger O_f \Pi_S O_f V | \psi_{R_k} \rangle - \mathop{\mathbb{E}}_{h} \langle \psi_h | V^\dagger O_f \Pi_S O_f V | \psi_h \rangle \right| <_? o(1)$$

where $\Pi_S \coloneqq \sum_{i\in S} \Pi_i$.

One Quantum Query O_f

➔ Projective measurement Π_S (outcome i)

➔ classical query $g: [L] \to \{0,1\}$, if $i \in S$, then $g(i) = 1$, otherwise $g(i) = 0$

- (1+ϵ)-query (Conjecture 2.6.)

For any subset $S \subseteq [L]$,

$$\max_{S\subseteq[L]} \max_{f:[L]\to\{\pm 1\}} \left| \mathop{\mathbb{E}}_{k\sim[K]} (\langle \psi_{R_k} | \otimes \langle \phi_f |) \cdot \Pi_S \cdot (|\psi_{R_k}\rangle \otimes |\phi_f\rangle) - \mathop{\mathbb{E}}_{h} (\langle \psi_h | \otimes \langle \phi_f |) \cdot \Pi_S \cdot (|\psi_h\rangle \otimes |\phi_f\rangle) \right| <_? o(1)$$

where L-outcome projective measurement $P = \{\Pi_i\}_{i\in[L]}$, $O_f V|\psi\rangle = |\psi\rangle \otimes |\phi_f\rangle$ (quantum advice $|\phi_f\rangle$)

감사합니다!