A note on pseudorandom unitaries in polylog depth

Hsin-Yuan Huang, Fermi Ma

September 16, 2024

Abstract

In this note, we give a simple construction of pseudorandom unitaries that can be implemented in poly log depth on all-to-all-connected quantum circuits consisting of two-qubit gates assuming hardness of Learning with Errors (LWE).

The purpose of this note is to provide a fix to pseudorandom unitary results based on the Luby-Rackoff construction for creating pseudorandom permutation P from pseudorandom functions. This note is part of an ongoing research project studying the minimum time to form strong pseudorandom unitaries and its connection to scrambling. This note is intended to remain unpublished, with the majority of its content to be incorporated into a forthcoming manuscript.

1 A known issue in the pseudorandomness literature

We begin by describing a known issue in the pseudorandomness literature.

In Section 2.8 of Ref. [1], the authors use the claim that the 4-round Luby-Rackoff construction forms a quantum-secure pseudorandom permutation [2] to show that quantum-secure in-place pseudorandom permutations P can be constructed in QNC^1_f assuming the quantum hardness of learning with errors (LWE). From this result, one immediately obtain that the PFC construction for pseudorandom unitaries proposed in [3] can be created in QNC^1_f assuming hardness of LWE.

Unfortunately, the claim that 4-round Luby-Rackoff construction forms a quantum-secure pseudorandom permutations [2] contain flaws in the proof; see Footnote 3 of [4]. Furthermore, even if the flaws in [2] are fixed, Ref. [2] studied the XOR pseudorandom permutations rather than the in-place pseudorandom permutations. The quantum security of XOR pseudorandom permutations, with query only to the forward direction but not the inverse, do not imply the quantum security of in-place pseudorandom permutations. As a result, it is unknown if pseudorandom unitaries can be created in QNC^1_f assuming hardness of LWE.

Hsin-Yuan Huang thanks Daniel Liang for raising this important caveat in the pseudorandomness literature. Daniel Liang has learned these issues from Soumik Ghosh.

2 A simple construction of pseudorandom unitaries

Let n be the number of qubits and $N \coloneqq 2^n$. We begin by defining the following components:

- $f_0 : \{0,1\}^n \to \{1,-1\}$, a random function mapping n-bit strings to random binary phase.
- $f_1, f_2 : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, two independent random functions operating on $(n/2)$-bit strings.

2.1 Feistel network

Our construction utilizes a simple variant of the Feistel network, also known as the Luby-Rackoff construction. For a function f, we define the *Left* and *Right* Luby-Rackoff construction as follows:

$$\mathsf{L}_f(x_L\|x_R) \coloneqq (x_L \oplus f(x_R))\|x_R, \tag{2.1}$$
$$\mathsf{R}_f(x_L\|x_R) \coloneqq x_L\|(x_R \oplus f(x_L)), \tag{2.2}$$

where $x = x_L\|x_R \in \{0,1\}^n$, and $\|$ denotes bitstring concatenation.

2.2 Quantum oracles

We define the following n-qubit quantum oracles:

$$\mathcal{O}^{f_0} \coloneqq \sum_{x\in\{0,1\}^n} f_0(x)\,|x\rangle\langle x|\,, \tag{2.3}$$
$$\mathcal{O}^{\mathsf{L},f} \coloneqq \sum_{x\in\{0,1\}^n} |\mathsf{L}_f(x)\rangle\langle x|\,, \tag{2.4}$$
$$\mathcal{O}^{\mathsf{R},f} \coloneqq \sum_{x\in\{0,1\}^n} |\mathsf{R}_f(x)\rangle\langle x|\,. \tag{2.5}$$

2.3 Construction

Let G be an n-qubit random unitary sampled independently from a unitary 2-design, such as a random Clifford circuit. Our n-qubit pseudorandom unitary U is constructed as follows:

$$U \coloneqq \mathcal{O}^{\mathsf{R},f_2} \cdot \mathcal{O}^{f_0} \cdot \mathcal{O}^{\mathsf{L},f_1} \cdot G. \tag{2.6}$$

This constructions satisfies the following when f_0, f_1, f_2 are fully random functions.

Theorem 1 (Indistinguishability)**.** *Let n be the number of qubits. Any algorithm $\mathcal{A}$ that queries an n-qubit unitary U for $t = 2^{o(n)}$ times can only distinguish between (1) $U = \mathcal{O}^{\mathsf{R},f_2} \cdot \mathcal{O}^{f_0} \cdot \mathcal{O}^{\mathsf{L},f_1} \cdot G$ and (2) U is a Haar-random unitary with a negligible probability.*

Assuming quantum subexponential hardness of LWE, we can take the functions f_0, f_1, f_2 to be pseudorandom functions secure against subexponential-time quantum adversary. Furthermore, as shown in Ref. [5], the classical functions f_0, f_1, f_2 can all be implemented using log-depth classical circuits NC^1. Hence, the n-qubit oracles $\mathcal{O}^{f_0}, \mathcal{O}^{\mathsf{L},f_1}$ and $\mathcal{O}^{\mathsf{R},f_2}$ can all be implemented in $\mathsf{QNC}^1_f \subseteq \mathsf{QNC}$. Together, the n-qubit unitary U can be implemented in QNC, i.e., $\operatorname{poly}\log n$ depth quantum circuits. When instantiated with pseudorandom function, Theorem 1 implies that U is a pseudorandom unitary secure against subexponential-time quantum adversary.

3 Preliminaries

For completeness, the Preliminaries section is adapted from our work proving the conjecture regarding the existence of pseudorandom unitaries [6].

3.1 Notation

For simplicity, we consider the number of qubits n to be even. We note that our results naturally generalize to odd n by considering left side to have one more bit than the right side similar to how Feistel network handles odd-size bitstrings.

- Throughout this paper, we write $N \coloneqq 2^n$, where n represents the number of qubits.
- Let $[N] \coloneqq \{1, \ldots, N\}$ denote the set of integers from 1 to N.
- We identify $[N]$ with $\{0,1\}^n$ by associating each integer $i \in [N]$ with the string $x \in \{0,1\}^n$ corresponding to the binary representation of $i-1$.
- For any integer $1 \leq t \leq N$, let $[N]^t_{\text{dist}}$ denote the set of length-t sequences of distinct integers from 1 to N, i.e.,

$$[N]^t_{\text{dist}} \coloneqq \{(x_1, \ldots, x_t) \in [N]^t : x_i \neq x_j \text{ for all } i \neq j\}. \tag{3.1}$$

- For $t = 0$, $[N]^t_{\text{dist}} \coloneqq \{()\}$ is a set with a single element () denoting a length-0 sequence.
- For a pure state $|\psi\rangle$, we sometimes denote ψ as the density matrix $|\psi\rangle\langle\psi|$.
- We identify $[N^{1/2}]$ with $\{0,1\}^{n/2}$ by associating each integer $i \in [N^{1/2}]$ with the string $x \in \{0,1\}^{n/2}$ corresponding to the binary representation of $i-1$.
- Let $x \in \{0,1\}^n$ be an n-bit string. We define:
  - $x_L \coloneqq x[1 : n/2]$, (the left half of x, i.e., the first $n/2$ bits)
  - $x_R \coloneqq x[n/2+1 : n]$, (the right half of x, i.e., the last $n/2$ bits)

  such that $x = x_L \| x_R$, where $\|$ denotes concatenation.
- Given a set $X = \{x_1, \ldots, x_t\}$ with $x_i \in \{0,1\}^n$. We define $X_L \coloneqq \{x_{1,L}, \ldots, x_{t,L}\}$ to be the set of the left half strings and $X_R \coloneqq \{x_{1,R}, \ldots, x_{t,R}\}$ to be the set of the right half strings.
- Given an n-qubit register A. We denote register $\mathsf{A_L}$ to be the left half of A, which consists of $n/2$ qubits, and $\mathsf{A_R}$ to be the right half of A.

3.2 Oracle adversary

In the context of quantum cryptography, we often analyze the security of systems against adversaries with oracle access. We define such oracle adversaries as follows:

Definition 1 (Oracle adversary)**.** *An oracle adversary $\mathcal{A}$ is a quantum algorithm that makes queries to an oracle $\mathcal{O}$ that acts on the first n qubits of the adversary's space, which we call the A register. The adversary also has an m-qubit ancillary space, which we call the B register. A t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}), \ldots, A^{(t)}_{\mathsf{AB}})$.*

Definition 2 (Adversary view after t queries)**.** *Given a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$, we define the adversary's view after t queries as:*

$$|\mathcal{A}^{\mathcal{O}}_t\rangle_{\mathsf{AB}} \coloneqq \prod_{i=1}^{t} \left(\mathcal{O}_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}}\,. \tag{3.2}$$

Here, $\mathcal{O}$ represents the n-qubit oracle, and $A^{(i)}_{\mathsf{AB}}$ is the unitary operation applied by the adversary between the $(i-1)$-th and i-th oracle queries. For an arbitrary t, we denote as $|\mathcal{A}^{\mathcal{O}}\rangle_{\mathsf{AB}}$.

The adversary's view corresponds to the entire state of the adversary's system after making t queries to the oracle.

3.3 Pseudorandom unitaries

A pseudorandom unitary is a unitary operation that can be efficiently implemented but is computationally indistinguishable from a Haar-random unitary. This notion is formalized in [3, 7, 8] focusing on polynomial-time adversary. Here, we present a definition of pseudorandom unitary secure against $t(n)$-time adversaries. In some applications, e.g., in proving the hardness of recognizing topological phases of matter [9], we would like consider pseudorandom unitary secure against subexponential-time adversary, which will be covered by the following definition.

Definition 3 (Pseudorandom unitary secure against $t(n)$-time adversary)**.** *A sequence $\{\mathcal{U}_n\}_{n\in\mathbb{N}}$ of distributions over n-qubit unitary $\mathcal{U}_n = \{U_{\mathsf{key}}\}_{\mathsf{key}\in\mathcal{K}_n}$ with the key space $\mathcal{K}_n$ is a pseudorandom unitary secure against any $t(n)$-time adversary if it satisfies the following.*

- ***Efficient computation:*** *There exists a* $\mathrm{poly}(n)$*-time quantum algorithm that implements the n-qubit unitary U_{key} for all $\mathsf{key} \in \mathcal{K}_n$.*
- ***Indistinguishability from Haar:*** *Any oracle adversary $\mathcal{A}$ that runs in time $\leq t(n)$, queries an n-qubit oracle $\mathcal{O}$ for any number of times, and measures a two-outcome observable $D_{\mathcal{A}}$ with eigenvalues $\{0,1\}$ after the queries satisfies*

$$\left| \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathcal{U}_n} \mathrm{Tr}\left(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}}\rangle\langle\mathcal{A}^{\mathcal{O}}|_{\mathsf{AB}} \right) - \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_{\mathrm{Haar}}} \mathrm{Tr}\left(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}}\rangle\langle\mathcal{A}^{\mathcal{O}}|_{\mathsf{AB}} \right) \right| \leq \mathrm{negl}(n), \tag{3.3}$$

where μ_{Haar} is the Haar measure and $\mathrm{negl}(n)$ *denotes any negligible function.*

The difference between the observable expectation value on the adversary's view after querying n-qubit oracle $\mathcal{O}$ sampled from $\mathcal{U}_n$ and from μ_{Haar} is the advantage of the adversary $\mathcal{A}$.

This definition captures several important aspects of pseudorandom unitaries. The first condition *Efficient computation* ensures that each unitary in the family can be implemented efficiently, i.e., with a quantum circuit of polynomial size. This is crucial for practical applications in quantum computing and cryptography. The second condition *Indistinguishability from Haar* formalizes the notion that no efficient quantum algorithm (adversary) can distinguish between a unitary drawn from the pseudorandom family and a Haar-random unitary. This is quantified by the probability of outputting 1 after measuring the observable $D_{\mathcal{A}}$ after the queries.

3.4 The Haar measure and unitary t-designs

The Haar measure over the unitary group is defined below.

Definition 4 (Haar measure)**.** *Given the number of qubits n, the Haar measure over the n-qubit unitary group $U(2^n)$ is the unique probability measure μ on $U(2^n)$ that is:*

1. *Left-invariant: For any measurable set $S \subseteq U(2^n)$ and any $V \in U(2^n)$, $\mu(VS) = \mu(S)$.*
2. *Right-invariant: For any measurable set $S \subseteq U(2^n)$ and any $V \in U(2^n)$, $\mu(SV) = \mu(S)$.*
3. *Normalized: $\mu(U(2^n)) = 1$.*

The Haar measure provides a notion of uniform distribution over the unitary group.

Because a random unitary sampled according to the Haar measure requires exponential many gates to implement, one typically works with distributions that only matches the first t moments of the Haar measure. Such distributions are known as unitary t-designs. The formal definition of (exact) unitary t-design is given as follows.

Definition 5 (Unitary t-design)**.** *Given the number of qubits n, a distribution $\mathcal{U}$ on n-qubit unitaries is an exact unitary t-design if*

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}}[U^{\otimes t}\otimes U^{\dagger,\otimes t}] = \int_{U(2^n)} U^{\otimes t}\otimes U^{\dagger,\otimes t} d\mu(U), \tag{3.4}$$

where μ is the Haar measure over the unitary group $U(2^n)$.

To formally define symmetric subspace, we need to define permutation operators. Permutation operators rearrange the subsystems of a quantum state according to a given permutation π.

Definition 6 (Permutation operator)**.** *For any permutation $\pi \in \mathsf{Sym}_t$, let S_π be a unitary that acts on $(\mathbb{C}^N)^t$ as follows:*

$$S_\pi : |x_1,\ldots,x_t\rangle \mapsto |x_{\pi^{-1}(1)},\ldots,x_{\pi^{-1}(t)}\rangle\,. \tag{3.5}$$

3.5 Twirling channel

Twirling channels are used to average quantum states or operations over a set of unitary transformations, effectively creating a more symmetric or invariant representation. In this subsection, we focus on the two-fold twirling channel, which is defined using unitary 2-designs. Unitary 2-designs are distributions over unitary operators that reproduce the statistical properties of the full unitary group up to the second moment.

We begin by defining the two-fold twirling channel.

Lemma 3.1 (2-fold twirling channel for unitary 2-design; [10, 11])**.** *Let $\mathcal{U}$ be a unitary 2-design on a N-dimensional Hilbert space $\mathcal{H}$. The two-fold twirling channel $\mathcal{T}_2$ with respect to $\mathcal{U}$ is defined as:*

$$\mathcal{T}_2(X) = \mathop{\mathbb{E}}_{U\leftarrow\mathcal{U}}[(U^\dagger\otimes U^\dagger)X(U\otimes U)] \tag{3.6}$$

where X is an operator on $\mathcal{H}\otimes\mathcal{H}$. The action of $\mathcal{T}_2$ on X can be expressed as:

$$\mathcal{T}_2(X) = \frac{2}{N(N+1)}\operatorname{Tr}(\Pi^{\mathsf{sym}}X)\cdot\Pi^{\mathsf{sym}} + \frac{2}{N(N-1)}\operatorname{Tr}(\Pi^{\mathsf{asym}}X)\cdot\Pi^{\mathsf{asym}}, \tag{3.7}$$

where $\Pi^{\mathsf{sym}} = \frac{1}{2}(\mathsf{Id}+\mathsf{Swap})$ and $\Pi^{\mathsf{asym}} = \frac{1}{2}(\mathsf{Id}-\mathsf{Swap})$ are the projectors onto the symmetric and antisymmetric subspaces respectively and Swap is the swap operator.

Notation 1 (Half-equality projector)**.** *We define the following half-equality projectors $\Pi^{\mathsf{eq},\mathsf{L}}_{\mathsf{AB}}, \Pi^{\mathsf{eq},\mathsf{R}}_{\mathsf{AB}}$ over two n-qubit registers A,B,*

$$\Pi^{\mathsf{eq},\mathsf{L}}_{\mathsf{AB}} := \sum_{x\in[N^{1/2}]} |x\rangle\langle x|_{\mathsf{A_L}}\otimes\mathsf{Id}_{\mathsf{A_R}}\otimes|x\rangle\langle x|_{\mathsf{B_L}}\otimes\mathsf{Id}_{\mathsf{B_R}}, \tag{3.8}$$

$$\Pi^{\mathsf{eq},\mathsf{R}}_{\mathsf{AB}} := \sum_{x\in[N^{1/2}]} \mathsf{Id}_{\mathsf{A_L}}\otimes|x\rangle\langle x|_{\mathsf{A_R}}\otimes\mathsf{Id}_{\mathsf{B_L}}\otimes|x\rangle\langle x|_{\mathsf{B_R}}\,. \tag{3.9}$$

Lemma 3.2 (Twirled half-equality projectors)**.** *Let $\mathcal{U}$ be a unitary 2-design on an n-qubit Hilbert space $\mathcal{H}$, where $N = 2^n$. We have*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathcal{U}}[(U^\dagger_{\mathsf{A}}\otimes U^\dagger_{\mathsf{B}})\Pi^{\mathsf{eq},\mathsf{R}}_{\mathsf{AB}}(U_{\mathsf{A}}\otimes U_{\mathsf{B}})] = \frac{N^{3/2}-1}{N^2-1}\mathsf{Id}_{\mathsf{AB}} + \frac{N-N^{1/2}}{N^2-1}\mathsf{Swap}_{\mathsf{AB}}\,. \tag{3.10}$$

Proof. We begin by applying the twirling channel in Lemma 3.1 to $\Pi^{\mathsf{eq},\mathsf{R}}$:

$$\mathcal{T}_2(\Pi^{\mathsf{eq},\mathsf{R}}) = \frac{2}{N(N+1)} \operatorname{Tr}\Big(\Pi^{\mathsf{sym}}\Pi^{\mathsf{eq},\mathsf{R}}\Big) \cdot \Pi^{\mathsf{sym}} + \frac{2}{N(N-1)} \operatorname{Tr}\Big(\Pi^{\mathsf{asym}}\Pi^{\mathsf{eq},\mathsf{R}}\Big) \cdot \Pi^{\mathsf{asym}} \tag{3.11}$$

To evaluate this, we need to calculate $\operatorname{Tr}\big(\Pi^{\mathsf{sym}}\Pi^{\mathsf{eq},\mathsf{R}}\big)$ and $\operatorname{Tr}\big(\Pi^{\mathsf{asym}}\Pi^{\mathsf{eq},\mathsf{R}}\big)$:

$$\operatorname{Tr}\Big(\Pi^{\mathsf{sym}}\Pi^{\mathsf{eq},\mathsf{R}}\Big) = \frac{1}{2}\operatorname{Tr}\Big((\mathsf{Id}+\mathsf{Swap})\Pi^{\mathsf{eq},\mathsf{R}}\Big) = \frac{1}{2}(N^{3/2}+N) \tag{3.12}$$

$$\operatorname{Tr}\Big(\Pi^{\mathsf{asym}}\Pi^{\mathsf{eq},\mathsf{R}}\Big) = \frac{1}{2}\operatorname{Tr}\Big((\mathsf{Id}-\mathsf{Swap})\Pi^{\mathsf{eq},\mathsf{R}}\Big) = \frac{1}{2}(N^{3/2}-N) \tag{3.13}$$

Substituting these values into the twirling channel formula:

$$\mathcal{T}_2(\Pi^{\mathsf{eq},\mathsf{R}}) = \frac{2}{N(N+1)} \cdot \frac{N^{3/2}+N}{2} \cdot \Pi^{\mathsf{sym}} + \frac{2}{N(N-1)} \cdot \frac{N^{3/2}-N}{2} \cdot \Pi^{\mathsf{asym}} \tag{3.14}$$

$$= \frac{N^{1/2}+1}{N+1}\Pi^{\mathsf{sym}} + \frac{N^{1/2}-1}{N-1}\Pi^{\mathsf{asym}} = \frac{N^{3/2}-1}{N^2-1}\mathsf{Id} + \frac{N-N^{1/2}}{N^2-1}\,\mathsf{Swap}\,. \tag{3.15}$$

This completes the proof of this lemma. □

3.6 Path-recording framework

We review the path-recording framework proposed in [6] for constructing various types of path-recording oracles PR.

3.6.1 Relation states

To state the path-recording oracle, we need the following definitions.

Notation 2 (X,Y registers)**.** *For all $1 \le t \le N$, let X_t be a register associated with the $(N+1)$-dimensional Hilbert space $\mathcal{H}_{\mathsf{X}_t}$ spanned by the states $\{|x\rangle\}_{x\in[N]} \cup |\perp\rangle$. The registers Y_t for $1 \le t \le N$ are defined identically. Let X,Y be the registers associated with the Hilbert spaces*

$$\mathcal{H}_{\mathsf{X}} \coloneqq \bigotimes_{1\le t\le N} \mathcal{H}_{\mathsf{X}_t} \quad \text{and} \quad \mathcal{H}_{\mathsf{Y}} \coloneqq \bigotimes_{1\le t\le N} \mathcal{H}_{\mathsf{Y}_t}. \tag{3.16}$$

Notation 3 (Extended unitaries)**.** *When applying an n-qubit unitary U to a state $|\psi\rangle \in \mathcal{H}_{\mathsf{X}_t}$, we extend the unitary U to act as $|\perp\rangle\langle\perp| + U$, though we will simply write this operator as U.*

Notation 4 (Length-t states)**.** *We use the notation*

$$|x_1,\dots,x_t\rangle_{\mathsf{X}} \coloneqq |x_1\rangle_{\mathsf{X}_1} \cdots |x_t\rangle_{\mathsf{X}_t} |\perp\rangle_{\mathsf{X}_{t+1}} \cdots |\perp\rangle_{\mathsf{X}_N}, \tag{3.17}$$

for all $0 \le t \le N$ and $x_1,\dots,x_t \in [N]$.

Notation 5 (Relation states)**.** *For $0 \le t \le N$ and a size-t relation $R = \{(x_1,y_1),\dots,(x_t,y_t)\}$, define the corresponding relation state to be the unit vector*

$$|R\rangle_{\mathsf{XY}} \coloneqq \frac{1}{\sqrt{\gamma_R}} \sum_{\pi\in\mathsf{Sym}_t} S_\pi |x_1,\dots,x_t\rangle_{\mathsf{X}} \otimes S_\pi |y_1,\dots,y_t\rangle_{\mathsf{Y}}, \tag{3.18}$$

where the normalizing factor is

$$\gamma_R \coloneqq t! \cdot \sum_{x,y\in[N]} \Big(\sum_{i=1}^{t} \delta_{(x_i,y_i)=(x,y)}\Big)!. \tag{3.19}$$

For any relation R, define the sets $\mathrm{Dom}(R) \coloneqq \{x : \exists y \in [N] \text{ s.t.} (x,y) \in R\}$ *and* $\mathrm{Im}(R) \coloneqq \{y : \exists x \in [N] \text{ s.t.} (x,y) \in R\}$. *Note that the state* $|\{\}\rangle_{\mathsf{XY}}$ *corresponding to the empty set equals*

$$|\{\}\rangle_{\mathsf{XY}} = |\perp\rangle_{\mathsf{X}_1} \cdots |\perp\rangle_{\mathsf{X}_N} |\perp\rangle_{\mathsf{Y}_1} \cdots |\perp\rangle_{\mathsf{Y}_N} . \tag{3.20}$$

Notation 6 (The set of all relation states)**.** *Let $\mathfrak{R}_t$ be the set of all relations R of size t. Let $\mathfrak{R} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t$ be the set of all relations R of size $0 \le t \le N$.*

Claim 1 (Orthonormality of the relation states; see [6])**.** $\{|R\rangle_{\mathsf{XY}}\}_{R\in\mathfrak{R}}$ *forms an orthonormal basis.*

The path-recording oracle acts naturally on the following restricted sets of relations.

Notation 7 (Distinct sets of relations)**.** *Define the following restricted sets of relations:*

- *Let $\mathfrak{R}_t^{\mathsf{inj}}$ be the set of all* injective *relations, i.e., relations $R = \{(x_1,y_1),\ldots,(x_t,y_t)\}$ of size t, where $(y_1,\ldots,y_t) \in [N]^t_{\mathrm{dist}}$. Let $\mathfrak{R}^{\mathsf{inj}} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t^{\mathsf{inj}}$.*
- *Let $\mathfrak{R}_t^{\mathsf{bij}}$ be the set of all* bijective *relations, i.e., relations $R = \{(x_1,y_1),\ldots,(x_t,y_t)\}$ of size t, where $(x_1,\ldots,x_t) \in [N]^t_{\mathrm{dist}}$ and $(y_1,\ldots,y_t) \in [N]^t_{\mathrm{dist}}$. Let $\mathfrak{R}^{\mathsf{bij}} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t^{\mathsf{bij}}$.*

For relations $R = \{(x_1,y_1),\ldots,(x_t,y_t)\}$ where the tuples are all distinct, i.e., $(x_i,y_i) \neq (x_j,y_j)$ when $i \neq j$, the normalization factor is simply $1/\sqrt{t!}$, i.e.,

$$|R\rangle_{\mathsf{XY}} = \frac{1}{\sqrt{t!}} \sum_{\pi\in\mathsf{Sym}_t} S_\pi |x_1,\ldots,x_t\rangle_{\mathsf{X}} \otimes S_\pi |y_1,\ldots,y_t\rangle_{\mathsf{Y}} . \tag{3.21}$$

Note that any relation $R \in \mathfrak{R}^{\mathsf{inj}}$ or $R \in \mathfrak{R}^{\mathsf{bij}}$ satisfies this condition.

3.6.2 Restricted subset of relations

We will define a modified path-recording oracle via the path-recording framework [6]. To develop this modified path-recording oracle, we need to consider a restricted subset of $\mathfrak{R}_t^{\mathsf{inj}}$.

- $t_{\max} = N^{1/2}$ sets the maximum size of the relations.
- $\mathfrak{S}_t^{\mathsf{inj}}$ is the set of all injective relations $R = \{(x_i,y_i)\}_{i=1}^t$ with $y_{1,L},\ldots,y_{t,L} \in [N^{1/2}]^t_{\mathrm{dist}}$.
- $\mathfrak{S}^{\mathsf{inj}} \coloneqq \cup_{t=0}^{t_{\max}} \mathfrak{S}_t^{\mathsf{inj}}$.

It is not hard to see that this restricted set $\mathfrak{S}^{\mathsf{inj}}$ of relations satisfies the following two conditions.

Definition 7 (Consistency)**.** *We say the set $\mathfrak{S}^{\mathsf{inj}}$ of relations is consistent if*

$$\forall (x_1,\ldots,x_t) \in [N]^t, \quad \exists (y_1,\ldots,y_t) \in [N]^t, \tag{3.22}$$

$$\text{such that} \quad \{(x_i,y_i)\}_{i=1}^t \in \mathfrak{S}^{\mathsf{inj}}. \tag{3.23}$$

Furthermore, if $\{(x_i,y_i)\}_{i=1}^t \in \mathfrak{S}^{\mathsf{inj}}$, then for any $0 \le \tau \le t$, $\{(x_i,y_i)\}_{i=1}^\tau \in \mathfrak{S}^{\mathsf{inj}}$.

Definition 8 (Uniform growth)**.** *We say the set $\mathfrak{S}^{\mathsf{inj}}$ of relations satisfies the uniform growth constraint if for all $0 \le t < t_{\max}$, there exists $\mathcal{Z}_t \ge 1$, such that for all $x \in [N]$ and $R \in \mathfrak{S}_t^{\mathsf{inj}}$,*

$$\mathcal{Z}_t = \sum_{\substack{y\in[N],\,\text{s.t.}\\ R\cup\{(x,y)\}\in\mathfrak{S}_{t+1}^{\mathsf{inj}}}} 1. \tag{3.24}$$

3.6.3 $\mathfrak{S}^{\mathsf{inj}}$-restricted path-recording oracle

For the set $\mathfrak{S}^{\mathsf{inj}}$ of relations defined here, we have $\mathcal{Z}_t = (N - N^{1/2}t)$.

We now recall the definition of the $\mathfrak{S}^{\mathsf{inj}}$-restricted path-recording oracle from [6].

Definition 9 ($\mathfrak{S}^{\mathsf{inj}}$-restricted path-recording oracle)**.** *Given any consistent set $\mathfrak{S}^{\mathsf{inj}}$ of relations that satisfies uniform growth. The $\mathfrak{S}^{\mathsf{inj}}$-restricted path-recording oracle $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ is a linear map*

$$\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}}) : \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}} \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}} \tag{3.25}$$

defined as follows. For all $0 \leq t < t_{\max}$, $R \in \mathfrak{S}^{\mathsf{inj}}_t$, and $x \in [N]$,

$$\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}}) : |x\rangle_{\mathsf{A}} |R\rangle_{\mathsf{XY}} \mapsto \frac{1}{\sqrt{\mathcal{Z}_{|R|}}} \sum_{\substack{y\in[N],\\ R\cup\{(x,y)\}\in\mathfrak{S}^{\mathsf{inj}}_{t+1}}} |y\rangle_{\mathsf{A}} |R\cup\{(x,y)\}\rangle_{\mathsf{XY}} . \tag{3.26}$$

Next, we define the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state, which represents the global state after an adversary has queried the $\mathfrak{S}^{\mathsf{inj}}$-restricted path-recording oracle multiple times.

Definition 10 (G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state)**.** *Given a consistent set $\mathfrak{S}^{\mathsf{inj}}$, an n-qubit unitary G and a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \ldots, A^{(t)}_{\mathsf{AB}})$, the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state is*

$$|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} \coloneqq \prod_{i=1}^{t} \left(\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}}) \cdot G_{\mathsf{A}} \cdot U^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{XY}} . \tag{3.27}$$

Fact 1 (Explicit form of the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state)**.** *Given a consistent set $\mathfrak{S}^{\mathsf{inj}}$ of relations that satisfies uniform growth. We can expand the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state after t queries to obtain*

$$|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} = \sqrt{\prod_{i=0}^{t-1} \frac{1}{\mathcal{Z}_i}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t\\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}\\ R=\{(x_i,y_i)\}_{i=1}^t\in\mathfrak{S}^{\mathsf{inj}}_t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot U^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}}\right] \otimes |R\rangle_{\mathsf{XY}} . \tag{3.28}$$

We state two important lemmas about the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state proven in [6].

Lemma 3.3 (G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state has unit norm; See [6])**.** *For any consistent set $\mathfrak{S}^{\mathsf{inj}}$ of relations, any adversary $\mathcal{A}$ making $t \leq t_{\max}$ queries to an n-qubit oracle, and any n-qubit unitary G, the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state $|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}}$ has unit norm.*

Lemma 3.4 (Right unitary invariance; See [6])**.** *Given a consistent set $\mathfrak{S}^{\mathsf{inj}}$ of relations that satisfies uniform growth. For any n-qubit unitary G, we have*

$$|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} = (G_{\mathsf{X}_1} \otimes \ldots \otimes G_{\mathsf{X}_t}) |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}\rangle_{\mathsf{ABXY}} . \tag{3.29}$$

A central theorem proven in [6] is that the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state is an approximate purification of any algorithm that queries a Haar-random unitary many times.

Theorem 2 ($\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ is indistinguishable from Haar random; see [6])**.** *Given a consistent set $\mathfrak{S}^{\mathsf{inj}}$ of relations that satisfies uniform growth. Let $\mathcal{A}$ be a t-query oracle adversary. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu(\mathcal{U}(N))} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}| , \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}|_{\mathsf{ABXY}}\right)\right) \tag{3.30}$$

$$\leq \frac{2t(t-1)}{N+1} + 2\left(1 - \prod_{i=0}^{t-1} \mathcal{Z}_i \cdot \frac{(N-t)!}{N!}\right) . \tag{3.31}$$

Using $\mathcal{Z}_i = N(1 - iN^{-1/2})$ for the set $\mathfrak{S}^{\mathsf{inj}}$ of relations defined in this work, we have

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu(\mathcal{U}(N))} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|\,, \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}|_{\mathsf{ABXY}}\right)\right) \tag{3.32}$$

$$\leq \frac{2t(t-1)}{N+1} + 2\left(1 - \prod_{i=0}^{t-1} \mathcal{Z}_i \cdot \frac{(N-t)!}{N!}\right) \leq \frac{3t(t-1)}{N^{1/2}}. \tag{3.33}$$

3.6.4 Enhanced gentle measurement lemma

The following lemma will be useful for bounding the distance between a pair of mixed states whose purifications are related by a projection that acts only on the purifying register. When applicable, this lemma gives a quadratically improved bound over the standard gentle measurement lemma.

Lemma 3.5 (Enhanced gentle measurement lemma; See [6])**.** *Let ρ_{CD} be a density matrix on registers C, D and let Π_{CD} be a projector of the form $\Pi_{\mathsf{CD}} = \mathsf{Id}_{\mathsf{C}} \otimes \Pi'_{\mathsf{D}}$ where Π'_{D} is a projector that acts on register D. Then the following holds,*

$$\|\mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}}) - \mathrm{Tr}_{\mathsf{D}}(\Pi_{\mathsf{CD}} \cdot \rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{CD}})\|_1 = 1 - \mathrm{Tr}(\Pi_{\mathsf{CD}} \cdot \rho_{\mathsf{CD}}). \tag{3.34}$$

4 Proof of Theorem 1

4.1 Restriction to a special distinct subspace

Definition 11 (Projection on Register X)**.** *We define the projector,*

$$\Pi_{\mathsf{X}}^{\mathsf{XRdist}} = \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ \text{s.t. } (x_{1,R},\ldots,x_{t,R})\in[N^{1/2}]^t_{\mathrm{dist}}}} |x_1,\ldots,x_t\rangle\langle x_1,\ldots,x_t|_{\mathsf{X}}\,. \tag{4.1}$$

Note that for any $(y_1,\ldots,y_t) \in [N]^t$ such that $(y_{1,L},\ldots,y_{t,L}) \in [N^{1/2}]^t_{\mathrm{dist}}$, we have $(y_1,\ldots,y_t) \in [N]^t_{\mathrm{dist}}$. When we apply the projector to the G-rotated $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state, we obtain

$$\Pi_{\mathsf{X}}^{\mathsf{XRdist}} |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} \tag{4.2}$$

$$= \sqrt{\frac{1}{N^t}\prod_{i=0}^{t-1}\frac{1}{1-i/N^{1/2}}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t \\ R=\{(x_1,y_1),\ldots,(x_t,y_t)\} \\ \text{s.t. } (x_{1,R},\ldots,x_{t,R})\in[N^{1/2}]^t_{\mathrm{dist}} \\ \text{and } (y_{1,L},\ldots,y_{t,L})\in[N^{1/2}]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot U^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes |R\rangle_{\mathsf{XY}}\,. \tag{4.3}$$

We now analyze the norm of the projected state.

Lemma 4.1. *Given $t < N^{1/2}$ and a unitary 2-design $\mathcal{D}$. The projected state has norm bounded by,*

$$\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}| \Pi_{\mathsf{X}}^{\mathsf{XRdist}} |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} \geq 1 - \frac{t^2}{N^{1/2}}. \tag{4.4}$$

Proof. From Lemma 3.4,, we have

$$\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}| \Pi_{\mathsf{X}}^{\mathsf{XRdist}} |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABXY}} = \langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}| G_{\mathsf{X}}^{\dagger,\otimes t} \Pi_{\mathsf{X}}^{\mathsf{XRdist}} G_{\mathsf{X}}^{\otimes t} |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}\rangle_{\mathsf{ABXY}}\,. \tag{4.5}$$

To bound this quantity, note that we have

$$\mathsf{Id} - \Pi_{\mathsf{X}}^{\mathsf{XRdist}} \leq \sum_{1\leq i<j\leq t} \Pi_{\mathsf{X}_i\mathsf{X}_j}^{\mathsf{eq},\mathsf{R}}, \tag{4.6}$$

where $\leq$ is the PSD order. Hence, using Lemma 3.2, we have

$$1 - \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \langle \mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})} | \, G_{\mathsf{X}}^{\dagger,\otimes t} \Pi_{\mathsf{X}}^{\mathsf{XRdist}} G_{\mathsf{X}}^{\otimes t} \, | \mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})} \rangle_{\mathsf{ABXY}} \tag{4.7}$$

$$\leq \sum_{1\leq i<j\leq t} \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} (G_{\mathsf{X}_i} \otimes G_{\mathsf{X}_j})^\dagger \cdot \Pi_{\mathsf{X}_i\mathsf{X}_j}^{\mathsf{eq},\mathsf{R}} \cdot (G_{\mathsf{X}_i} \otimes G_{\mathsf{X}_j}) \cdot |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}\rangle\langle \mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})}|_{\mathsf{ABXY}} \right) \tag{4.8}$$

$$\leq \frac{t(t-1)}{2} \cdot \left(\frac{N^{3/2}-1}{N^2-1} + \frac{N-N^{1/2}}{N^2-1} \right) \leq \frac{t^2}{N^{1/2}}. \tag{4.9}$$

This concludes the proof of this lemma. □

4.2 Purification of our construction

Given an n-qubit unitary G and a t-query adversary $\mathcal{A}$ specified by a t-tuple of $(n+m)$-qubit unitaries $(A_{\mathsf{AB}}^{(1)}), \ldots, A_{\mathsf{AB}}^{(t)})$ with $t < N^{1/2}$. When $\mathcal{A}$ queries our constructed n-qubit oracle,

$$\mathcal{O}^{f_0,f_1,f_2} \cdot G := \mathcal{O}^{\mathsf{R},f_2} \cdot \mathcal{O}^{f_0} \cdot \mathcal{O}^{\mathsf{L},f_1} \cdot G, \tag{4.10}$$

for random functions $f_0 : [N] \mapsto \{\pm 1\}$, $f_1, f_2 : [N^{1/2}] \mapsto [N^{1/2}]$, we can purify the randomness in the functions by defining the global state,

$$|\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} := \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot C_{\mathsf{A}} \cdot U_{\mathsf{AB}}^{(i)} \right) |0\rangle_{\mathsf{AB}} \right]$$

$$\otimes \frac{1}{\sqrt{2^N}} \sum_{f_0:[N]\mapsto\{\pm1\}} \left(\prod_{i=1}^{t} f_0(y_{i,L} \| x_{i,R}) \right) |f_0\rangle_{\mathsf{F}_0} \tag{4.11}$$

$$\otimes \frac{1}{\sqrt{N^{N^{1/2}/2}}} \sum_{f_1:[N^{1/2}]\mapsto[N^{1/2}]} \left(\prod_{i=1}^{t} \delta_{x_{i,L}\oplus f_1(x_{i,R})=y_{i,L}} \right) |f_1\rangle_{\mathsf{F}_1} \tag{4.12}$$

$$\otimes \frac{1}{\sqrt{N^{N^{1/2}/2}}} \sum_{f_2:[N^{1/2}]\mapsto[N^{1/2}]} \left(\prod_{i=1}^{t} \delta_{x_{i,R}\oplus f_2(y_{i,L})=y_{i,R}} \right) |f_2\rangle_{\mathsf{F}_2}, \tag{4.13}$$

where register F_0 is used to store a function mapping from $[N]$ to $\{\pm 1\}$, register F_1 and F_2 are used to store a function mapping from $[N^{1/2}]$ to $[N^{1/2}]$, and for two bitstrings x, x', $\delta_{x=x'}$ is 1 if the two bitstrings are equal and 0 otherwise.

After tracing out the purifying registers $\mathsf{F}_0, \mathsf{F}_1, \mathsf{F}_2$, the resulting density matrix on register A, B is equal to the density matrix

$$\mathop{\mathbb{E}}_{f_0,f_1,f_2} |\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}\rangle\langle\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}|_{\mathsf{AB}}, \tag{4.14}$$

where the functions f_0, f_1, f_2 are sampled uniformly at random.

Fact 2 (Purification of our construction)**.** *For any n-qubit unitary G, we have*

$$\mathrm{Tr}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \left[\; |\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{RFLO}\cdot G}|_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} \; \right] = \mathop{\mathbb{E}}_{f_0,f_1,f_2} \left[\; |\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}\rangle\langle\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}|_{\mathsf{AB}} \; \right]. \tag{4.15}$$

Proof. The proof follows from the definition of $\mathcal{O}^{f_0}, \mathcal{O}^{\mathsf{L},f_1}, \mathcal{O}^{\mathsf{R},f_2}$. □

We consider a relation to be a multiset of tuples. We consider each tuple to be a pair of bitstrings (x, y) for $x, y \in [N]$. Hence, a relation is given by $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ with $(x_1, \ldots, x_t) \in [N]^t$ and $(y_1, \ldots, y_t) \in [N]^t$.

Definition 12 (F^3-relation state)**.** *For any $0 \le t \le N^{1/2}$ and relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ with $(x_1, \ldots, x_t) \in [N]^t, (y_1, \ldots, y_t) \in [N]^t$, we define the F^3-relation state to be*

$$|\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \coloneqq \frac{1}{\sqrt{2^N}} \sum_{f_0:[N]\mapsto\{\pm1\}} \left(\prod_{i=1}^{t} f_0(y_{i,L}\|x_{i,R})\right) |f_0\rangle_{\mathsf{F}_0} \tag{4.16}$$

$$\otimes \frac{1}{\sqrt{N^{N^{1/2}/2}}} \sum_{f_1:[N^{1/2}]\mapsto[N^{1/2}]} \left(\prod_{i=1}^{t} \delta_{x_{i,L}\oplus f_1(x_{i,R})=y_{i,L}}\right) |f_1\rangle_{\mathsf{F}_1} \tag{4.17}$$

$$\otimes \frac{1}{\sqrt{N^{N^{1/2}/2}}} \sum_{f_2:[N^{1/2}]\mapsto[N^{1/2}]} \left(\prod_{i=1}^{t} \delta_{x_{i,R}\oplus f_2(y_{i,L})=y_{i,R}}\right) |f_2\rangle_{\mathsf{F}_2}\,, \tag{4.18}$$

which depends only on the relation R but not the ordering of $(x_1, y_1), \ldots, (x_t, y_t)$. The $\widetilde{\cdot}$ denotes that $|\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}$ is an unnormalized pure state, possibly with norm 0.

Fact 3 (Inner products between relations)**.** *Given $0 \le t \le N^{1/2}$. For any $R, R' \in \mathfrak{R}_t^{\mathrm{dist}}$, we have*

$$\langle\widetilde{\phi}_{R'}|\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} = \frac{1}{N^t} \cdot \delta_{R=R'}. \tag{4.19}$$

For any $R \in \mathfrak{R}_t^{\mathrm{dist}}$ and $R' \in \mathfrak{R}_t$, we have

$$\langle\widetilde{\phi}_{R'}|\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} = 0. \tag{4.20}$$

Proof. This fact can be easily shown by evaluating the inner product explicitly. □

From this basic fact, we can present the following two definitions.

Definition 13 (Unit-norm F^3-relation state)**.** *Given $0 \le t \le N^{1/2}$. For all $R \in \mathfrak{R}_t^{\mathrm{dist}}$, we define the normalized F^3-relation state,*

$$|\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \coloneqq \sqrt{N^t}\,|\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}\,, \tag{4.21}$$

where $|\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}$ has unit norm.

Definition 14 (Distinct relation projectors)**.** *Given $0 \le t \le N^{1/2}$. We define the projector to the subspace formed by size-t distinct F^3-relation states,*

$$\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \coloneqq \sum_{R\in\mathfrak{R}_t^{\mathrm{dist}}} |\phi_R\rangle\langle\phi_R|\,. \tag{4.22}$$

Fact 4 (Alternative formulation of the purified state)**.** *Given $0 \le t \le N^{1/2}$. We have*

$$|\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} = \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t\\(y_1,\ldots,y_t)\in[N]^t\\R=\{(x_1,y_1),\ldots,(x_t,y_t)\}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot C_{\mathsf{A}}\cdot U^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes |\widetilde{\phi}_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}\,. \tag{4.23}$$

Furthermore, after projecting to the subspace of distinct relations, we have

$$\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \left|\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\right\rangle_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} \tag{4.24}$$

$$= \frac{1}{\sqrt{N^t}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t \\ R=\{(x_1,y_1),\ldots,(x_t,y_t)\} \\ \text{s.t. } (x_{1,R},\ldots,x_{t,R})\in[N^{1/2}]^t_{\mathrm{dist}} \\ \text{and } (y_{1,L},\ldots,y_{t,L})\in[N^{1/2}]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot C_{\mathsf{A}}\cdot U^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes |\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}. \tag{4.25}$$

Proof. This fact follows immediately from Fact 3, Definition 13, and Definition 14. □

By comparing the result obtained in this lemma to the projected $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ state,

$$\Pi^{\mathsf{XRdist}}_{\mathsf{X}} \left|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\right\rangle_{\mathsf{ABXY}} \tag{4.26}$$

$$= \frac{1}{\sqrt{N^t}}\sqrt{\prod_{i=0}^{t-1}\frac{1}{1-i/N^{1/2}}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t \\ R=\{(x_1,y_1),\ldots,(x_t,y_t)\} \\ \text{s.t. } (x_{1,R},\ldots,x_{t,R})\in[N^{1/2}]^t_{\mathrm{dist}} \\ \text{and } (y_{1,L},\ldots,y_{t,L})\in[N^{1/2}]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot G_{\mathsf{A}}\cdot U^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes |R\rangle_{\mathsf{XY}}. \tag{4.27}$$

we see that they are almost the same up to (1) the slight difference in the factor in front and (2) the difference between $|\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}$ and $|R\rangle_{\mathsf{XY}}$. We can address Point (2) using the following fact.

Fact 5 (Compressing F^3-relation states to relation states)**.** *Given $0 \le t \le N^{1/2}$. There exists a linear map $\mathsf{Compress}_t$ from register $\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2$ to register X,Y, such that*

$$\mathsf{Compress}_t \left|\phi_R\right\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} = |R\rangle_{\mathsf{XY}}, \tag{4.28}$$

for all relation $R \in \mathfrak{R}^{\mathrm{dist}}_t$ and $\mathsf{Compress}_t$ is an isometry in the subspace $\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}$.

Proof. This follows immediately from Fact 3 that $\langle\phi_{R'}|\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} = \delta_{R=R'} = \langle R'|R\rangle_{\mathsf{XY}}$. □

By combining all these facts, we obtain the following lemma.

Lemma 4.2 (Relating $\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})$ and RFLO)**.** *We have*

$$\mathrm{Tr}_{\mathsf{X},\mathsf{Y}}\left[\,\Pi^{\mathsf{XRdist}}_{\mathsf{X}}\cdot\left|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\right\rangle\!\!\left\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\right|_{\mathsf{ABXY}}\cdot\Pi^{\mathsf{XRdist}}_{\mathsf{X}}\,\right] \tag{4.29}$$

$$= \prod_{i=0}^{t-1}\left(\frac{1}{1-i/N^{1/2}}\right)\cdot\mathrm{Tr}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}\left[\,\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}\cdot\left|\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\right\rangle\!\!\left\langle\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\right|_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2}\cdot\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}\,\right]. \tag{4.30}$$

Proof. From Fact 5, we have

$$\Pi^{\mathsf{XRdist}}_{\mathsf{X}}\left|\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\right\rangle_{\mathsf{ABXY}} = \mathsf{Compress}_t\cdot\sqrt{\prod_{i=0}^{t-1}\left(\frac{1}{1-i/N^{1/2}}\right)}\cdot \tag{4.31}$$

$$\sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t \\ R=\{(x_1,y_1),\ldots,(x_t,y_t)\} \\ \text{s.t. } (x_{1,R},\ldots,x_{t,R})\in[N^{1/2}]^t_{\mathrm{dist}} \\ \text{and } (y_{1,L},\ldots,y_{t,L})\in[N^{1/2}]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot G_{\mathsf{A}}\cdot U^{(i)}_{\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes |\phi_R\rangle_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \tag{4.32}$$

$$= \mathsf{Compress}_t \cdot \sqrt{\prod_{i=0}^{t-1}\left(\frac{1}{1-i/N^{1/2}}\right)} \cdot \Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} |\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2}. \tag{4.33}$$

Because $\mathsf{Compress}_t$ is an isometry in the subspace $\Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2}$, we have obtained this lemma. □

4.3 Full proof

Proof of Theorem 1. Consider any unitary 2-design $\mathcal{D}$. We compare the following states,

$$\rho^{(1)} := \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_{\mathrm{Haar}}} \left[\, |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}} \,\right] \tag{4.34}$$

$$\rho^{(2)} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathrm{Tr}_{\mathsf{X},\mathsf{Y}} \left[\, |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}|_{\mathsf{ABXY}} \,\right] \tag{4.35}$$

$$\rho^{(3)} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathrm{Tr}_{\mathsf{X},\mathsf{Y}} \left[\, \Pi_{\mathsf{X}}^{\mathsf{XRdist}} \cdot |\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}(\mathfrak{S}^{\mathsf{inj}})\cdot G}|_{\mathsf{ABXY}} \cdot \Pi_{\mathsf{X}}^{\mathsf{XRdist}} \,\right] \tag{4.36}$$

$$\rho^{(4)} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathrm{Tr}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \left[\, \Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \cdot |\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{RFLO}\cdot G}|_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} \cdot \Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \,\right] \tag{4.37}$$

$$\rho^{(5)} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathrm{Tr}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \left[\, |\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{RFLO}\cdot G}|_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} \,\right] \tag{4.38}$$

$$\rho^{(6)} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathop{\mathbb{E}}_{f_0,f_1,f_2} |\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}\rangle\langle\mathcal{A}^{\mathcal{O}^{f_0,f_1,f_2}\cdot G}|_{\mathsf{AB}}. \tag{4.39}$$

All of these matrices are over register A,B and are PSD. However, they are not necessarily trace one. $\rho^{(1)}$ is when the adversary $\mathcal{A}$ access Haar-random unitaries. $\rho^{(6)}$ is when the adversary $\mathcal{A}$ access our random unitary construction $\mathcal{O}^{f_0,f_1,f_2}\cdot G := \mathcal{O}^{\mathsf{R},f_2}\cdot\mathcal{O}^{f_0}\cdot\mathcal{O}^{\mathsf{L},f_1}\cdot G$. From Fact 2, we have $\rho^{(5)} = \rho^{(6)}$. By triangle inequality, we can bound the distance between $\rho^{(1)}$ and $\rho^{(6)}$ by the following,

$$\|\rho^{(1)} - \rho^{(6)}\|_1 \le \|\rho^{(1)} - \rho^{(2)}\|_1 + \|\rho^{(2)} - \rho^{(3)}\|_1 + \|\rho^{(3)} - \rho^{(4)}\|_1 + \|\rho^{(4)} - \rho^{(5)}\|_1. \tag{4.40}$$

$\|\rho^{(1)} - \rho^{(2)}\|_1$ is at most $\frac{3t^2}{N^{1/2}}$ using Eq. (3.33) obtained from Theorem 2. $\|\rho^{(2)} - \rho^{(3)}\|_1$ is at most $\frac{t^2}{N^{1/2}}$ using Lemma 3.5 and Lemma 4.1. $\|\rho^{(3)} - \rho^{(4)}\|_1$ can be bounded using Lemma 4.2,

$$\|\rho^{(3)} - \rho^{(4)}\|_1 \le \left|1 - \prod_{i=0}^{t-1}\left(1 - i/N^{1/2}\right)\right| \cdot \|\rho^{(3)}\|_1 \le \frac{0.5t^2}{N^{1/2}}. \tag{4.41}$$

Bounding $\|\rho^{(4)} - \rho^{(5)}\|_1$ is slightly more complicated and requires using Lemma 3.5, Lemma 4.1, and Lemma 4.2. We have the following,

$$\|\rho^{(4)} - \rho^{(5)}\|_1 \le 1 - \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \mathrm{Tr}\left[\, \Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \cdot |\mathcal{A}_t^{\mathsf{RFLO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{RFLO}\cdot G}|_{\mathsf{ABF}_0\mathsf{F}_1\mathsf{F}_2} \cdot \Pi^{\mathsf{F}^3\,\mathrm{dist},t}_{\mathsf{F}_0,\mathsf{F}_1,\mathsf{F}_2} \,\right] \tag{4.42}$$

$$= 1 - \prod_{i=0}^{t-1}\left(1 - i/N^{1/2}\right) \cdot \mathrm{Tr}\left[\rho^{(3)}\right] \tag{4.43}$$

$$\le \left(1 - \prod_{i=0}^{t-1}\left(1 - i/N^{1/2}\right)\right) + \left(1 - \mathrm{Tr}\left[\rho^{(3)}\right]\right) \tag{4.44}$$

$$\le \frac{0.5t^2}{N^{1/2}} + \frac{t^2}{N^{1/2}} = \frac{1.5t^2}{N^{1/2}}. \tag{4.45}$$

The first line uses Lemma 3.5. The second line uses Lemma 4.2. The third line uses the inequality $1 - ab \le (1-a) + (1-b)$ for any $a, b \in [0,1]$. The fourth line uses Eq. (4.41) and Lemma 4.1. By

aggregating all inequalities, we obtain

$$\|\rho^{(1)} - \rho^{(6)}\|_1 \leq \frac{3t^2}{N^{1/2}} + \frac{t^2}{N^{1/2}} + \frac{0.5t^2}{N^{1/2}} + \frac{1.5t^2}{N^{1/2}} \leq \frac{6t^2}{N^{1/2}}, \tag{4.46}$$

which is negligible in n for any $t = 2^{o(n)}$ since $N = 2^n$. □

References

[1] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum pseudoentanglement. *arXiv preprint arXiv:2211.00747 v2*, 2022.

[2] Akinori Hosoyamada and Tetsu Iwata. 4-round luby-rackoff construction is a qprp. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 145–174. Springer, 2019.

[3] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. *arXiv preprint arXiv:2404.12647*, 2024.

[4] Dominique Unruh. Towards compressed permutation oracles. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 369–400. Springer, 2023.

[5] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–737. Springer, 2012.

[6] Fermi Ma and Hsin-Yuan Huang. Pseudorandom unitaries. *Upcoming*, 2024.

[7] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[8] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and pseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751*, 2024.

[9] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *arXiv preprint arXiv:2407.07754*, 2024.

[10] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(1):012304, 2009.

[11] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.