Parallel Kac's Walk Generates PRU

Chuhan Lu[*] Minglong Qin[†] Fang Song[‡] Penghui Yao[§¶]
Mingnan Zhao[‖]

June 10, 2025

Abstract

Ma and Huang recently proved that the PFC construction, introduced by Metger, Poremba, Sinha and Yuen [MPSY24], gives an adaptive-secure pseudorandom unitary family (PRU). Their proof developed a new *path recording* technique [MH24].

In this work, we show that a linear number of sequential repetitions of the *parallel Kac's Walk*, introduced by Lu, Qin, Song, Yao and Zhao [LQS+24], also forms an adaptive-secure PRU, confirming a conjecture therein. Moreover, it additionally satisfies strong security against adversaries making inverse queries. This gives an alternative PRU construction, and provides another instance demonstrating the power of the path recording technique. We also discuss some further simplifications and implications.

1 Introduction

Pseudorandomness is a fundamental concept in cryptography. The basic pseudorandom objects, including pseudorandom functions (PRFs), pseudorandom permutation (PRPs), pseudorandom generator (PRGs), have served as primitives in modern classical cryptography.

Pseudorandom objects in quantum information have witnessed increasing influences in recent years. The first example is *pseudorandom states* (PRSs), introduced by Ji, Liu and Song [JLS18], which are a set of states that can be prepared by polynomial-sized quantum circuits and look indistinguishable from Haar random states for any polynomial-time quantum distinguisher. They gave the first construction of PRSs. PRSs have found applications in various areas including quantum cryptography [AQY22], quantum learning theory [HBC+22] and quantum gravity [BFV20, YE25]. Since their work, a number of different constructions have been discovered [BS19, BM25, GTB23, JMW24]. Ji, Liu and Song further introduced the concept of *pseudorandom unitaries* (PRUs), which

[*]Computer Science Department, Portland State University, USA. Email: chuhan@pdx.edu.
[†]Centre for Quantum Technologies, National University of Singapore, Singapore. Email: mlqin6@gmail.com.
[‡]Computer Science Department, Portland State University, USA. Email: crissong@gmail.com.
[§]State Key Laboratory for Novel Software Technology, New Cornerstone Science Laboratory, Nanjing University, Nanjing 210023, China. Email: phyao1985@gmail.com.
[¶]Hefei National Laboratory, Hefei 230088, China.
[‖]State Key Laboratory for Novel Software Technology, New Cornerstone Science Laboratory, Nanjing University, Nanjing 210023, China. Email: mingnanzh@gmail.com.

are ensembles of unitaries that are efficient to implement, but are indistinguishable from Haar random unitaries by any quantum polynomial-time distinguisher. The construction of PRU turns out to be challenging and a large body of works have been devoted to constructing pseudorandom objects that partially realize PRU's functions. Examples include scalable pseudorandom states [BS20], pseudorandom function-like quantum state generators [AGQY22], pseudorandom isometries [AGKL24], pseudorandom scramblers [LQS+24].

A giant leap was achieved by Metger, Poremba, Sinha and Yuen [MPSY24] where a pseudorandom unitary family is constructed against *non-adaptive* adversaries. Their construction is a PFC ensemble, where the circuits sequentially apply a uniformly random Clifford gate, a diagonal unitary with a (pseudorandom) random phase $f : \{0,1\}^n \to \{-1,1\}$, and then a (pseudorandom) permutation matrix on n-qubit computational basis states. Soon after, Ma and Huang in their very recent work [MH24] proved that PFC ensembles are indeed secure against *adaptive* adversaries as well, provably establishing the feasibility of PRU for the first time.

1.1 Main result

In this work, we carry on the exciting advancement on PRU lately. We show that the *parallel Kac's walk* construction, introduced in [LQS+24], also produces an *adaptive-secure* PRU. The original *Kac's walk*, introduced by Kac [Kac56] in 1956, is a random walk on unitary groups, which has been extensively studied by mathematical physicists. Kac's walk has also found applications in construction of polynomial designs [BHH16] and memory-optimal dimension reduction [JPS+22]. To put it in the language of quantum computing, in one step of Kac's walk, the algorithm randomly selects two elements of computational basis $\{|i\rangle, |j\rangle\}$ and implements a random 2×2 unitary in the space spanned by these two basis elements. Kac's walk can also be viewed as a random walk on a unit sphere, where all the random unitaries sampled by the walk are applied to a initial unit vector, sequentially. Pillai and Smith [PS17] showed a tight $\Theta(N \log N)$ mixing time for the Kac's walk on an N-dimensional unit sphere.

Lu, Qin, Song, Yao and Zhao [LQS+24] introduced a variant called *parallel Kac's walk*. It randomly samples a random matching, say $\{(|i_1\rangle, |j_1\rangle), \ldots, (|i_{N/2}\rangle, |j_{N/2}\rangle)\}$, among all N computational basis elements, which is done in a single step via a random permutation of all basis elements. For each pair $(|i\rangle, |j\rangle)$, the algorithm implements a 2×2 Haar random unitary. By replacing the random functions and random permutations with their quantum-secure pseudorandom counterparts, one obtains an efficient implementation of one step of the parallel Kac's walk. It was shown that a parallel Kac's walk reduces the mixing time by a factor N. Consequently, $O(\log N)$ steps of parallel Kac's walk, which is linear in the number of qubits n, map any input pure state to a family of pseudorandom states. It was left open in their paper if such a construction can generate a PRU. In this paper, we show an affirmative answer that *linear* steps of parallel Kac's walk indeed form a PRU.

Theorem 1.1 (Main Theorem, Informal)**.** *The distribution of the unitary corresponding to a $O(n)$-step random parallel Kac's walk is computationally indistinguishable from Haar distribution against adaptive adversaries. Moreover, without asymptotically increasing the number of steps, it also remains secure against adversaries capable of making inverse queries.*

Proof overview. The entire proof comprises two phases. First we show that $O(n)$ iterations of parallel Kac's walk effectively project the adversary's state to what we term the *distinct block subspace*. We divide $\{0,1\}^n$ into $N/2$ blocks, each containing two bit strings. We define $(x_1, \ldots, x_t) \in (\{0,1\}^n)^t$ to be in the distinct block subspace if they belong to different blocks. Once the state is promised to reside in the distinct block subspace, the second phase employs a single step of parallel Kac's walk to ensure that the entire construction is indistinguishable from a Haar random unitary.

More specifically, in the initial phase, we leverage the random state scrambling property of parallel Kac's walk as introduced in [LQS+24] to ensure that the adversary's state is approximately in the *distinct subspace* after $O(n)$ steps. To further show the projection into the distinct block subspace, imagine inserting an additional random permutation that does not affect the construction (since every iteration inherently includes a random permutation). Given that the adversary's state already resides in the distinct subspace, applying a random permutation will cause it to fall into the distinct block subspace with high probability. Noting that 2-designs, such as random Cliffords, can also project states onto distinct block subspaces, one approach would be to show that the parallel Kac's walk alone forms a 2-design—as our goal is to build a PRU purely based on the parallel Kac's walk—which, however, was unknown prior to this work. Therefore, we instead directly prove that the parallel Kac's walk suffices for this purpose.

In the second phase of the proof, we borrow the techniques in [MH24]. It consists of three steps: (1) we establish a straightforward purification of the adversary's output state using a large environment register; (2) we compress the environment register so as to make the environment state conform to the *relation state*, which is feasible under the condition that the adversary's state resides in the distinct block subspace; (3) we employ the path-recording technique. In the final step, we can apply the *right invariance* property of the path-recording oracle as the state in the environment register resembles the relation state. This effectively shifts the adaptive queries to the environment register without altering the state. Since the queries are redirected to the environment, they do not affect the adversary's state, regardless of whether they stem from parallel Kac's walk or Haar measure.

1.2 Discussions

While our PRU construction does not provide efficiency advantages over the PFC construction [MPSY24, MH24], there are potential benefits in other regards. First, it is usually valuable to have multiple candidates for a primitive available, to cater different use cases and to mitigate the risk in case of unexpected vulnerabilities in some candidates. It is also preferable in cryptography, for practical implementation concerns, to base the construction on as few primitives as possible. For instance, the popular HMAC instantiates the Hash-then-MAC paradigm using hash functions only as opposed to the vanilla instantiation by a hash function and a MAC scheme separately. We can view each step of the parallel Kac's walk as a basic module and then the PRU just constitutes repetitions of this basic module. In another recent work, Schuster, Haferkamp and Huang [SHH24] exhibited an alternate construction of PRU which glues together $\omega(\log n)$-qubit pseudorandom unitaries in a two-layer brickwork manner. Here each small pseudorandom unitary can also be viewed as a basic module. However, we still do not know the construction of small pseudorandom unitaries other than PFC. Finally, since PRUs are the quantum analogue of pseudorandom permutations (i.e., block ciphers), our PRU is also reminiscent of the famous

Luby-Rackoff construction and variants in practical block ciphers such as AES, where a basic unit is iterated in multiple rounds to achieve desirable security properties.

The discussion above naturally leads to a few open questions. Can we reduce the number of rounds of the parallel Kac's walk, ideally to constant rounds? This appears difficult with the current analysis, and new techniques may be needed. Following the analogue we draw between our construction and classical constructions of block ciphers à la Feistel network, it is worth exploring quantum analogues of the wide variations on Feistel network (e.g., unbalanced Luby-Rackoff). Can our construction be further simplified? Can we replace all i.i.d. random rotations in one step of parallel Kac's walk by the same random rotation? Recent research on orthogonal repeated averaging, which is a simplified Kac's walk, alludes to an affirmative answer. The other possible simplification is replacing the PRPs in the construction by random local permutations, like practical architecture of DES[2]-brickwork circuits. If both simplifications were plausible, we would obtain a construction of local random circuits, which is also a PRU, answering a longstanding open problem in quantum complexity theory. A more technical note, [LQS+24] identifies a strong *dispersing* property of the parallel Kac's walk, does it pass along and equip our PRU with additional properties? This is both interesting for the sake of Kac's walk and possible applications of the resulting PRU.

Acknowledgment. CL and FS were supported by the US National Science Foundation grants CCF-2054758 (CAREER) and CCF-2224131. MQ was supported by the National Research Foundation, Singapore through the National Quantum Office, hosted in A*STAR, under its Centre for Quantum Technologies Funding Initiative (S24Q2d0009). PY and MZ were supported by National Natural Science Foundation of China (Grant No. 62332009 and 12347104), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302901), NSFC/RGC Joint Research Scheme (Grant No. 12461160276), Natural Science Foundation of Jiangsu Province (Grant No. BK20243060) and the New Cornerstone Science Foundation.

2 Preliminaries

2.1 Notations

Unless stated otherwise, we use n to denote the number of qubits and $N = 2^n$ to denote the dimension. We denote the set of unitaries of dimension N by $\mathrm{U}(N)$. The symbol μ represents the Haar random distribution over quantum states or unitaries, depending on the context. For finite sets $\mathcal{X}$ and $\mathcal{Y}$, we use $\mathcal{X}^{\mathcal{Y}}$ to denote the set of all functions $\{f : \mathcal{X} \to \mathcal{Y}\}$. We generally refer to the permutation group over elements in set $\mathcal{X}$ as $\mathcal{S}_{\mathcal{X}}$. We often write $\mathcal{S}_N$ instead of $\mathcal{S}_{\{0,1\}^n}$ to denote the permutation group over elements in $\{0,1\}^n$. In the context of unitary matrices, $\mathcal{S}_N$ refers to the group of permutation unitaries of dimension N, and $S \leftarrow \mathcal{S}_N$ indicates sampling a permutation unitary uniformly at random. Given two density operators ρ, η, the trace distance between them is $\mathrm{TD}(\rho, \eta) = \|\rho - \eta\|_1$.

For $x \in \{0,1\}^n$, we define $\mathrm{val}(x) = \sum_{i=1}^{n} 2^{-i} x_i$ and use $\overline{x} \in \{0,1\}^n$ to denote the binary string obtained by flipping the first bit of x. We divide the set $\{0,1\}^n$ into 2^{n-1} blocks according to the suffix of each string. For any $x, y \in \{0,1\}^n$, we say that x and y belong to the same block if x and y share the same suffix of length $n-1$ (i.e., $x_2 = y_2, \ldots, x_n = y_n$). Conversely, we say that x and

y are in *distinct blocks* if they have different suffixes. For $t \in \mathbb{N}$, we use DB_t to denote the set of all t-tuples consisting of strings from distinct blocks. That is,

$$\mathsf{DB}_t := \left\{(x_1, \ldots, x_t) \in (\{0,1\}^n)^t : \forall\, i \neq j,\ x_i \text{ and } x_j \text{ are in distinct blocks}\right\}.$$

We also need the following lemmas:

Lemma 2.1. *[MH24, Lemma 2.2] Let ρ_{CD} be a density matrix on registers C, D and let Π_{CD} be a projector of the form $\Pi_{\mathsf{CD}} = \mathrm{Id}_{\mathsf{C}} \otimes \Pi'_{\mathsf{D}}$, where Π'_{D} is a projector that acts on register D. Then*

$$\mathrm{TD}\left(\mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}}), \mathrm{Tr}_{\mathsf{D}}\left(\Pi_{\mathsf{CD}} \cdot \rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{CD}}\right)\right) = 1 - \mathrm{Tr}\left(\Pi_{\mathsf{CD}} \rho_{\mathsf{CD}}\right).$$

Lemma 2.2 (Gentle Measurement Lemma)**.** *[MH24, Lemma 2.3] Let $|\psi\rangle$ be a quantum state, $U_1, \ldots, U_t$ are unitary operators, and $\Pi_1, \ldots, \Pi_t$ are projectors. We have*

$$\left\| U_t \cdots U_1 |\psi\rangle - \Pi_t U_t \cdots \Pi_1 U_1 |\psi\rangle \right\|_2 \leq t \cdot \sqrt{1 - \left\| \Pi_t U_t \cdots \Pi_1 U_1 |\psi\rangle \right\|_2^2}\ .$$

2.2 Adversary with Access to Oracle

We adopt the model for adversaries with oracle access in [MH24].

Definition 2.3 (Adversary with Access to Oracle)**.** *An adversary $\mathcal{A}$ with oracle access is a quantum algorithm which queries an oracle O on its first n-qubit register A without knowing the description of O. The adversary own another ancillary register of m-qubit, denoted by B.*

A t-query adversary $\mathcal{A}$ with oracle access is specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \cdots, A^{(t)}_{\mathsf{AB}})$. The view of the adversary after all the queries is

$$|\mathcal{A}^O_t\rangle_{\mathsf{AB}} := \prod_{i=1}^{t} \left(O_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}}\ .$$

We also allow adversary $\mathcal{A}$ make both forward queries (i.e., to O) and inverse queries (i.e., to $O^\dagger$). In this case, a t-query adversary $\mathcal{A}$ is specified by a t-tuple of unitaries $(A^{(1)}_{\mathsf{AB}}, \cdots, A^{(t)}_{\mathsf{AB}})$ and a Boolean string $b \in \{0,1\}^t$. The view of the adversary after all the queries is

$$|\mathcal{A}^O_t\rangle_{\mathsf{AB}} := \prod_{i=1}^{t} \left(\left((1-b_i) \cdot O + b_i \cdot O^\dagger\right)_{\mathsf{A}} \cdot A^{(i)}_{\mathsf{AB}}\right) |0\rangle_{\mathsf{AB}}\ .$$

Unless otherwise specified, we assume that the adversary makes only forward queries.

Definition 2.4 (Computational Indistinguishibility)**.** *We say two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over $\mathrm{U}(N)$ is computationally indistinguishable if for any $\mathrm{poly}(n)$-time adversary $\mathcal{A}$ with oracle access who makes $t = \mathrm{poly}(n)$ queries, we have*

$$\left| \Pr_{U \sim \mathcal{D}_1}\left[\mathcal{A}^U \text{ outputs } 1.\right] - \Pr_{V \sim \mathcal{D}_2}\left[\mathcal{A}^V \text{ outputs } 1.\right] \right| = \mathrm{negl}(n)\ .$$

2.3 Relation States

For $t \in \mathbb{N}$, $\mathfrak{R}_t$ represents the set of all size-t relations $R = \{(x_1, y_1), \ldots, (x_t, y_t)\} \subseteq \{0,1\}^n \times \{0,1\}^n$. We allow the relations to be a multiset. And let $\mathfrak{R} := \cup_{t=0}^{N} \mathfrak{R}_t$ be the set of all relations with size at most N. For $R \in \mathfrak{R}_t$, the corresponding *relation state* is defined by

$$|R\rangle_{\mathsf{XY}} := \frac{1}{\gamma_R} \sum_{\sigma \in \mathcal{S}_t} S_\sigma \, |x_1, \ldots, x_t\rangle_{\mathsf{X}} \otimes S_\sigma \, |y_1, \ldots, y_t\rangle_{\mathsf{Y}} \quad ,$$

where S_σ is a permutation operator on $\left(\mathbb{C}^{2^n}\right)^{\otimes t}$ defined as

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

and the normalizer is given by $\gamma_R := t! \cdot \sum_{x,y \in \{0,1\}^n} \left(\sum_{i=1}^{t} \delta_{(x_i,y_i)=(x,y)}\right)!$.

Fact 2.5. *$\{|R\rangle_{\mathsf{XY}}\}_{R \in \mathfrak{R}}$ forms an orthogonal basis.*

Let $\mathfrak{R}_t^{\text{yDB}}$ be the set of all size-t relations $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ such that $(y_1, \ldots, y_t) \in \mathrm{DB}_t$. Let $\mathfrak{R}^{\text{yDB}} := \cup_{t=0}^{N} \mathfrak{R}_t^{\text{yDB}}$. Let $\mathfrak{R}_t^{\text{DB}}$ be the set of all size-t relations $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ such that both $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ are in DB_t. Let $\mathfrak{R}^{\text{DB}} := \cup_{t=0}^{N} \mathfrak{R}_t^{\text{DB}}$.

For any relation R, define

$$\begin{aligned}
\mathrm{Dom}\,(R) &:= \{x : \exists y \in \{0,1\}^n \text{ s.t. } (x,y) \in R\}\,, \\
\mathrm{Im}\,(R) &:= \{y : \exists x \in \{0,1\}^n \text{ s.t. } (x,y) \in R\}\,, \\
\mathrm{BDom}\,(R) &:= \{x : \exists y \in \{0,1\}^n \text{ s.t. } (x,y) \in R \text{ or } (\bar{x},y) \in R\} \\
\mathrm{BIm}\,(R) &:= \{y : \exists x \in \{0,1\}^n \text{ s.t. } (x,y) \in R \text{ or } (x,\bar{y}) \in R\}\,.
\end{aligned}$$

We will use a similar path-recording oracle to that of [MH24]. The difference is that every time we query on x, the new path-recording oracle PR samples a $y \in \mathrm{BIm}\,(R)$ whose block differs from all previous blocks in R.

Definition 2.6 (Path-Recording Oracle)**.** *The path-recording oracle* PR *is a linear map*

$$\mathsf{PR} : \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}} \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}}$$

defined as follows. For all $x \in \{0,1\}^n$ and $R \in \mathfrak{R}^{\text{DB}}$,

$$\mathsf{PR} : |x\rangle_{\mathsf{A}} \, |R\rangle_{\mathsf{XY}} \to \frac{1}{\sqrt{N - 2\,|R|}} \sum_{\substack{y \in \{0,1\}^n, \\ y \notin \mathrm{BIm}(R)}} |y\rangle_{\mathsf{A}} \, |R \cup \{(x,y)\}\rangle_{\mathsf{XY}}$$

Fact 2.7. *For an arbitrary n-qubit unitary operator G and a t-query adversary $\mathcal{A}$ with query access to $\mathsf{PR} \cdot G$, define the state after $\mathcal{A}$ finishing all the queries to be*

$$|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABXY}} := \prod_{i=1}^{t} \left(\mathsf{PR} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} \, |\{\}\rangle_{\mathsf{XY}} \quad .$$

Then we have:

$$|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABHP}} = \sqrt{\prod_{i=0}^{t-1} \frac{1}{(N-2i)}} \sum_{\substack{(x_1,\ldots,x_t) \in (\{0,1\}^n)^t \\ (y_1,\ldots,y_t) \in \mathrm{DB}_t}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} \, |\{(x_i,y_i)\}_{i=1}^{t}\rangle_{\mathsf{XY}} \quad .$$

Similar to [MH24, Lemma 4.3], the path-recording oracle has the *right invariance* property.

Lemma 2.8. *For an arbitrary n-qubit unitary operator G, we have that*

$$|\mathcal{A}_t^{\mathrm{PR}\cdot G}\rangle_{\mathsf{ABXY}} = \left(G_{\mathsf{X}_1} \otimes \ldots \otimes G_{\mathsf{X}_t}\right) \cdot |\mathcal{A}_t^{\mathrm{PR}}\rangle_{\mathsf{ABXY}} \quad .$$

We define the projector operator of *distinct block subspace* as follows

Definition 2.9 (Distinct Block subspaces on register X with length t)**.** *Given $0 \leq t \leq N$. Let*

$$\Pi_{\mathsf{X}}^{(t)} := \sum_{(x_1,\ldots,x_t)\in \mathsf{DB}_t} |x_1,\ldots,x_t\rangle\langle x_1,\ldots,x_t|_{\mathsf{X}} \quad .$$

2.4 Cryptopgraphy

In this section, we will review various definitions and results in cryptography. Throughout this work, λ denotes a security parameter.

Definition 2.10 (Quantum-Secure Pseudorandom Function)**.** *Let $\mathcal{K}, \mathcal{X}$ and $\mathcal{Y}$ be the key space, the domain and range, all implicitly depending on the security parameter λ. A keyed family of functions $\{\mathsf{PRF}_k : \mathcal{X} \to \mathcal{Y}\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom function (*QPRF*) if the following two conditions hold:*

1. ***Efficient generation.*** *PRF_k is polynomial-time computable on a classical computer.*
2. ***Pseudorandomness.*** *For any polynomial-time quantum oracle algorithm $\mathcal{A}$, PRF_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random function $f \leftarrow \mathcal{Y}^{\mathcal{X}}$ in the sense that:*

$$\left| \Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{\mathsf{PRF}_k}\left(1^\lambda\right) = 1\right] - \Pr_{f\leftarrow\mathcal{Y}^{\mathcal{X}}}\left[\mathcal{A}^{f}\left(1^\lambda\right) = 1\right] \right| = \mathrm{negl}(\lambda) \quad .$$

Definition 2.11 (Quantum-Secure Pseudorandom Permutation)**.** *Let $\mathcal{K}$ be the key space, and $\mathcal{X}$ be both the domain and range, implicitly depending on the security parameter λ. A keyed family of permutations $\{\mathsf{PRP}_k \in \mathcal{S}_{\mathcal{X}}\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom permutation (*QPRP*) if the following two conditions hold:*

1. ***(Efficient generation).*** *PRP_k and PRP_k^{-1} are polynomial-time computable on a classical computer.*
2. ***(Pseudorandomness).*** *For any polynomial-time quantum oracle algorithm $\mathcal{A}$, PRP_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random permutation $\sigma \leftarrow \mathcal{S}_{\mathcal{X}}$ in the sense that:*

$$\left| \Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{\mathsf{PRP}_k,\mathsf{PRP}_k^{-1}}\left(1^\lambda\right) = 1\right] - \Pr_{\sigma\leftarrow S_{\mathcal{X}}}\left[\mathcal{A}^{\sigma,\sigma^{-1}}\left(1^\lambda\right) = 1\right] \right| = \mathrm{negl}(\lambda) \quad .$$

Under the assumption that post-quantum one-way functions exist, Zhandry proved the existence of QPRFs [Zha21]. QPRPs can be constructed from QPRFs efficiently [Zha16].

Definition 2.12 (Random State Scrambler with error ϵ)**.** *For $n \in \mathbb{N}$, let $\mathcal{D}$ be a distribution over $\mathrm{U}(N)$. We say $\mathcal{D}$ is a* random state scrambler distribution *with error ϵ (ϵ-*RSS*) if for any n-qubit pure state $|\phi\rangle$ and $\ell \in \mathrm{poly}(n)$,*

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{K\leftarrow\mathcal{D}}\left[K^{\otimes\ell}\,|\phi\rangle\langle\phi|^{\otimes\ell}\,K^{\otimes\ell,\dagger}\right], \mathop{\mathbb{E}}_{|\psi\rangle\in\mu}\left[|\psi\rangle\langle\psi|^{\otimes\ell}\right]\right) \leq \epsilon.$$

Definition 2.13 (Pseudorandom Unitary Operator)**.** *For $n \in \mathbb{N}$, let $\mathcal{D}$ be a distribution over $\mathrm{U}(N)$. We say $\mathcal{D}$ is a* pseudorandom unitary distribution *(*PRU*) if*

- *$\mathcal{D}$ can be sampled in $\mathrm{poly}(n)$ time;*
- *$\mathcal{D}$ is computationally indistinguishable from Haar random over $\mathrm{U}(N)$.*

3 Projecting into Distinct Block Subspace

In this section, we demonstrate that applying an RSS operator followed by a random permutation to any state results in a state that is mostly within the distinct block subspace.

Lemma 3.1. *For any ϵ-RSS distribution $\mathcal{R}$ on $\mathrm{U}(N)$ with $\epsilon = O\left(\frac{1}{N^2}\right)$, define $\mathcal{D}$ to be a distribution that samples $G = PK$ where $P \leftarrow \mathcal{S}_N$ is a random permutation unitary and $K \leftarrow \mathcal{R}$. Let*

$$\rho^{\mathcal{D}} := \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[|\mathcal{A}_t^{\mathrm{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathrm{PR}\cdot G}|_{\mathsf{ABXY}}\right],$$

then

$$\mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)}\cdot\rho^{\mathcal{D}}_{\mathsf{ABXY}}\right) \geq 1 - O\left(\frac{t^2}{N}\right).$$

Proof. By Lemma 2.8, we can rewrite $\rho^{\mathcal{D}}$ as

$$\rho^{\mathcal{D}} = \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)\cdot|A_t^{\mathrm{PR}}\rangle\langle A_t^{\mathrm{PR}}|_{\mathsf{ABXY}}\cdot\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)^{\dagger}\right]$$

Then, using the cyclic property of trace and then the definition of $\Pi_{\mathsf{X}}^{(t)}$

$$\begin{aligned}\mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)}\cdot\rho^{\mathcal{D}}_{\mathsf{ABXY}}\right) =& \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)^{\dagger}\cdot\Pi_{\mathsf{X}}^{(t)}\cdot\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)\cdot|A_t^{\mathrm{PR}}\rangle\langle A_t^{\mathrm{PR}}|_{\mathsf{ABXY}}\right]\right)\\ =& \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\begin{array}{c}\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)^{\dagger}\cdot\sum_{x\in\mathsf{DB}_t}|x\rangle\langle x|_{\mathsf{X}_1,\cdots,\mathsf{X}_t}\\ \cdot\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)\cdot|A_t^{\mathrm{PR}}\rangle\langle A_t^{\mathrm{PR}}|_{\mathsf{ABXY}}\end{array}\right]\right)\end{aligned} \tag{1}$$

Now, defining

$$\sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t} := \mathrm{Tr}_{-(\mathsf{X}_1,\ldots,\mathsf{X}_t)}\,|A_t^{\mathrm{PR}}\rangle\langle A_t^{\mathrm{PR}}|_{\mathsf{ABXY}}$$

where $\mathrm{Tr}_{-(\mathsf{X}_1,\ldots,\mathsf{X}_t)}$ represents tracing out all registers except $X_1,\ldots,X_t$. Then Eq. (1) can be rewritten as

$$\mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)^{\dagger}\cdot\sum_{x\in\mathsf{DB}_t}|x\rangle\langle x|_{\mathsf{X}_1,\cdots,\mathsf{X}_t}\cdot\left(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t}\right)\cdot\sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right]\right)$$

To simplify the notation, we write

$$\mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)} \cdot \rho_{\mathsf{ABXY}}^{\mathcal{D}}\right) = \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[G^{\otimes t,\dagger} \cdot \sum_{x\in \mathrm{DB}_t} |x\rangle\langle x|_{\mathsf{X}_1,\cdots,\mathsf{X}_t} \cdot G^{\otimes t} \cdot \sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right]\right)$$

This implies:

$$1 - \mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)} \cdot \rho_{\mathsf{ABXY}}^{\mathcal{D}}\right) = \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[G^{\otimes t,\dagger} \cdot \sum_{x\in \{0,1\}^{nt}\setminus \mathrm{DB}_t} |x\rangle\langle x|_{\mathsf{X}_1,\cdots,\mathsf{X}_t} \cdot G^{\otimes t} \cdot \sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right]\right) \tag{2}$$

We can see that the set $\{0,1\}^{nt}\setminus \mathrm{DB}_t$ includes all t-tuples where (a) $\exists i \neq j$ s.t. $x_i = x_j$ or (b) $\exists$i $\neq j$ s.t. $x_i = \bar{x}_j$ where $\bar{x}_j$ flips the first bit of x_j. We further define two projectors to capture these two situations:

$$\Pi^{\mathrm{eq}} = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes |x\rangle\langle x|$$

$$\Pi^{\mathrm{ffb}} = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes |\bar{x}\rangle\langle \bar{x}|$$

And we have

$$\sum_{x\in\{0,1\}^{nt}\setminus \mathrm{DB}_t} |x\rangle\langle x|_{\mathsf{X}_1,\ldots,\mathsf{X}_t} \preceq \sum_{1\le i<j\le t} \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} + \Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j} \tag{3}$$

where $\preceq$ represents the positive semidefinite order; $\Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}$ is the equality projector on register X_i, X_j; and $\Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}$ is the flip-first-bit projector on register X_i, X_j. Combining Eq.(2) and the inequality Eq.(3):

$$\begin{aligned}
1 - \mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)} \cdot \rho_{\mathsf{ABXY}}^{\mathcal{D}}\right) &\le \sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(G^{\otimes t,\dagger} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} + \Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right) \cdot G^{\otimes t} \cdot \sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right)\right] \\
&= \sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\left(G^{\dagger}_{\mathsf{X}_i} \otimes G^{\dagger}_{\mathsf{X}_j}\right) \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} + \Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right) \cdot \left(G_{\mathsf{X}_i} \otimes G_{\mathsf{X}_j}\right) \cdot \sigma_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \\
&= \sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N \\ K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\begin{array}{c}\left((PK)^{\dagger}_{\mathsf{X}_i} \otimes (PK)^{\dagger}_{\mathsf{X}_j}\right) \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} + \Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right) \\ \cdot \left(PK_{\mathsf{X}_i} \otimes PK_{\mathsf{X}_j}\right) \cdot \sigma_{\mathsf{X}_i,\mathsf{X}_j}\end{array}\right)\right]
\end{aligned} \tag{4}$$

where the part inside of the summation of Eq.(4) can be rewritten as the sum of the following two terms:

$$\mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N \\ K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left((PK)^{\dagger}_{\mathsf{X}_i} \otimes (PK)^{\dagger}_{\mathsf{X}_j}\right) \cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} \cdot \left(PK_{\mathsf{X}_i} \otimes PK_{\mathsf{X}_j}\right) \cdot \sigma_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \tag{5}$$

$$\mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N \\ K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left((PK)^{\dagger}_{\mathsf{X}_i} \otimes (PK)^{\dagger}_{\mathsf{X}_j}\right) \cdot \Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j} \cdot \left(PK_{\mathsf{X}_i} \otimes PK_{\mathsf{X}_j}\right) \cdot \sigma_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \tag{6}$$

We will bound these two terms one by one. First, note that for any permutation matrix P, $(P^{\dagger} \otimes P^{\dagger}) \cdot \Pi^{\mathrm{eq}} \cdot (P \otimes P) = \Pi^{\mathrm{eq}}$. Therefore, we have

$$(5) = \mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N \\ K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left(K^{\dagger}_{\mathsf{X}_i} \otimes K^{\dagger}_{\mathsf{X}_j}\right)\left(P^{\dagger}_{\mathsf{X}_i} \otimes P^{\dagger}_{\mathsf{X}_j}\right) \cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j} \cdot \left(P_{\mathsf{X}_i} \otimes P_{\mathsf{X}_j}\right)\left(K_{\mathsf{X}_i} \otimes K_{\mathsf{X}_j}\right) \cdot \sigma_{\mathsf{X}_i,\mathsf{X}_j}\right)\right]$$

$$= \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\mathrm{Tr}\left(\left(K_{\mathsf{X}_i}^\dagger \otimes K_{\mathsf{X}_j}^\dagger\right)\cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\cdot \sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right)\right]$$

Then, since $\sigma_{\mathsf{X}_1,\ldots,\mathsf{X}_t}$ is a density operator, we have

$$(5) \le \left\| \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\left(K_{\mathsf{X}_i}^\dagger \otimes K_{\mathsf{X}_j}^\dagger\right)\cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\right]\right\|_\infty$$

By the triangle inequality, we have

$$\begin{aligned}
(5) \le& \left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U_{\mathsf{X}_i}^\dagger \otimes U_{\mathsf{X}_j}^\dagger\right)\cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(U_{\mathsf{X}_i}\otimes U_{\mathsf{X}_j}\right)\right]\right\|_\infty \\
&+ \left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U_{\mathsf{X}_i}^\dagger \otimes U_{\mathsf{X}_j}^\dagger\right)\cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(U_{\mathsf{X}_i}\otimes U_{\mathsf{X}_j}\right)\right] - \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\left(K_{\mathsf{X}_i}^\dagger \otimes K_{\mathsf{X}_j}^\dagger\right)\cdot \Pi^{\mathrm{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\right]\right\|_\infty \\
\le& \sum_{x\in\{0,1\}^n}\left(\left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U^\dagger\otimes U^\dagger\right)\cdot |x,x\rangle\langle x,x|\cdot(U\otimes U)\right]\right\|_\infty\right. \\
&\left.+ \left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U^\dagger\otimes U^\dagger\right)\cdot |x,x\rangle\langle x,x|\cdot(U\otimes U)\right] - \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\left(K^\dagger\otimes K^\dagger\right)\cdot |x,x\rangle\langle x,x|\cdot(K\otimes K)\right]\right\|_\infty\right) \\
\le& \sum_{x\in\{0,1\}^n}\left(\left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U^\dagger\otimes U^\dagger\right)\cdot |x,x\rangle\langle x,x|\cdot(U\otimes U)\right]\right\|_\infty + O\left(\frac{1}{N^2}\right)\right) \qquad (7)
\end{aligned}$$

where we use the propery of $O\left(\frac{1}{N^2}\right)$ – RSS to derive the last inequality. Since $U|x\rangle$ is a Haar random state, we have $\mathbb{E}_{U\leftarrow\mu}\left[\left(U^\dagger\otimes U^\dagger\right)\cdot|x,x\rangle\langle x,x|\cdot(U\otimes U)\right] = \mathbb{E}_{|\psi\rangle\leftarrow\mu}[|\psi,\psi\rangle\langle\psi,\psi|]$ and the operator norm is $\frac{2}{N(N+1)}$ [Har13, Proposition 6]. Thus,

$$\begin{aligned}
(5) \le& \sum_{x\in\{0,1\}^n}\left(\left\| \mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mu}[|\psi,\psi\rangle\langle\psi,\psi|]\right\|_\infty + O\left(\frac{1}{N^2}\right)\right) \\
\le& N\cdot\left(\frac{2}{N(N+1)} + O\left(\frac{1}{N^2}\right)\right) = O\left(N^{-1}\right)
\end{aligned}$$

Next, we attempt to bound (6):

$$\begin{aligned}
(6) =& \mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N\\K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left(K_{\mathsf{X}_i}^\dagger\otimes K_{\mathsf{X}_j}^\dagger\right)\left(P_{\mathsf{X}_i}^\dagger\otimes P_{\mathsf{X}_j}^\dagger\right)\cdot\Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(P_{\mathsf{X}_i}\otimes P_{\mathsf{X}_j}\right)\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\cdot\sigma_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \\
\le& \left\| \mathop{\mathbb{E}}_{P\leftarrow\mathcal{S}_N}\left[\left(P_{\mathsf{X}_i}^\dagger\otimes P_{\mathsf{X}_j}^\dagger\right)\cdot\Pi^{\mathrm{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(P_{\mathsf{X}_i}\otimes P_{\mathsf{X}_j}\right)\right]\right\|_\infty \\
\le& \sum_{x\in\{0,1\}^n}\left\|\mathop{\mathbb{E}}_P\left[(P\otimes P)^\dagger\cdot|x,\bar{x}\rangle\langle x,\bar{x}|\cdot(P\otimes P)\right]\right\|_\infty \\
=& \sum_{x\in\{0,1\}^n}\left\|\frac{1}{N(N-1)}\sum_{z\neq y}|z,y\rangle\langle z,y|\right\|_\infty \\
=& \frac{1}{N-1}
\end{aligned}$$

Since both Eq. (5) and (6) are upper bounded by $O\left(N^{-1}\right)$, by substituting into (4) and using union bound on all i and j, we have

$$1 - \mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)} \cdot \rho_{\mathsf{ABXY}}^{\mathcal{D}}\right) \leq O\left(\frac{t^2}{N}\right)$$

□

4 PRU from Parallel Kac's Walk

In this section, we introduce our construction for PRU which is inspired by parallel Kac's walk. Our construction is simply to repeat the parallel Kac's walk.

4.1 The $\mathsf{HP}_{n,T}$ distribution

Our construction is based on *parallel Kac's walk*, a random walk on unit vectors within Hilbert spaces. A single step of parallel Kac's walk can be simulated by firstly sampling a random function $f : \{0,1\}^{n-1} \to \{0,1\}^{3d}$ and a random permutation $\sigma : \{0,1\}^n \to \{0,1\}^n$, and then applying two unitary operators P_σ and H_f in sequence. The unitary P_σ is the permutation matrix defined by

$$P_\sigma = \sum_{x \in \{0,1\}^n} |\sigma(x)\rangle\langle x| \quad .$$

The unitary P_σ will pair the 2^n computational basis up according to their images after the permutation σ. More specifically, the basis $|x\rangle$ and $|z\rangle$ are paired up iff $\sigma(x)$ and $\sigma(z)$ share the same suffix of length $n-1$, and each pair can be identified by its unique suffix. The unitary H_f then applies independent 2×2 Haar random unitaries on all pairs in the following way:

1. for every $y \in \{0,1\}^{n-1}$, we first parse $f(y) = f_\alpha(y) \| f_\beta(y) \| f_\theta(y)$ such that $f_\alpha(y)$, $f_\beta(y)$, $f_\theta(y) \in \{0,1\}^d$,
2. calculate three angles

$$\theta_y = \arcsin\left(\sqrt{\mathrm{val}(f_\theta(y))}\right) \quad , \quad \alpha_y = 2\pi \cdot \mathrm{val}(f_\alpha(y)) \quad , \quad \beta_y = 2\pi \cdot \mathrm{val}\big(f_\beta(y)\big) \quad ,$$

3. apply $U(\alpha_y, \beta_y, \theta_y) = \begin{bmatrix} e^{\mathrm{i}\alpha_y}\cos(\theta_y) & -e^{\mathrm{i}\beta_y}\sin(\theta_y) \\ e^{-\mathrm{i}\beta_y}\sin(\theta_y) & e^{-\mathrm{i}\alpha_y}\cos(\theta_y) \end{bmatrix}$ on the pair with suffix y.

The expression for H_f is

$$\sum_{y \in \{0,1\}^{n-1}} \begin{pmatrix} \mathrm{e}^{\mathrm{i}\left(\frac{\alpha_y+\beta_y}{2}\right)} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\left(\frac{\alpha_y+\beta_y}{2}\right)} \end{pmatrix} \begin{pmatrix} \cos\theta_y & -\sin\theta_y \\ \sin\theta_y & \cos\theta_y \end{pmatrix} \begin{pmatrix} \mathrm{e}^{\mathrm{i}\left(\frac{\alpha_y-\beta_y}{2}\right)} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\left(\frac{\alpha_y-\beta_y}{2}\right)} \end{pmatrix} \otimes |y\rangle\langle y| \quad , \tag{8}$$

where $U(\alpha_y, \beta_y, \theta_y)$ is decomposed into a product of three matrices. The unitary H_f can be approximated by a polynomial time implementable unitary $\widehat{H}_f$ satisfying that $\|H_f - \widehat{H}_f\|_\infty$ is sufficiently small [LQS+24].

Our construction for PRU is simply to repeat the parallel Kac's walk. We define two distributions over $\mathrm{U}(N)$, denoted by $\mathsf{HP}_{n,T}$ and $\widehat{\mathsf{HP}}_{n,T}$:

Definition 4.1. $\mathsf{HP}_{n,T}$ *is a distribution over* $\mathrm{U}(N)$ *which can be sample via the following procedure:*

- *sample* T *uniformly random functions* $f_1, \ldots, f_T : \{0,1\}^{n-1} \to \{0,1\}^{3d}$*, and* T *uniformly random permutations* $\sigma_1, \ldots, \sigma_T : \{0,1\}^n \to \{0,1\}^n$*,*
- *output the unitary* $\mathsf{Kac} = \prod_{i=1}^{T} \left(H_{f_i} \cdot P_{\sigma_i}\right)$*.*

Similarly, we define the distribution $\widehat{\mathsf{HP}}_{n,T}$ *by substituting* H_f *with* $\widehat{H}_f$*, and we denote the unitary sampled according to* $\widehat{\mathsf{HP}}_{n,T}$ *as* $\widehat{\mathsf{Kac}}$*.*

These two distributions are indistinguishable by any polynomial-time quantum adversary.

Lemma 4.2. *For* $T = \mathrm{poly}(n)$ *and* $d = 5n$*,* $\widehat{\mathsf{HP}}_{n,T}$ *is computationally indistinguishable from* $\mathsf{HP}_{n,T}$*.*

Proof. Consider the views $|\mathcal{A}_t^{\mathsf{Kac}}\rangle_{\mathsf{AB}}$ and $|\mathcal{A}_t^{\widehat{\mathsf{Kac}}}\rangle_{\mathsf{AB}}$ of a t-query adversary $\mathcal{A}$ with oracle access to Kac and $\widehat{\mathsf{Kac}}$ respectively. It is sufficient to show that the trace distance between these two states is negligible. To this end, we define the following hybrids: for $0 \le j \le t$,

$$|\varphi_j\rangle = \prod_{k=1}^{j} \left(\widehat{\mathsf{Kac}}_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) \prod_{j=k+1}^{t} \cdot \left(\mathsf{Kac}_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} \quad .$$

It is evident that $|\varphi_0\rangle = |\mathcal{A}_t^{\mathsf{Kac}}\rangle_{\mathsf{AB}}$ and $|\varphi_t\rangle = |\mathcal{A}_t^{\widehat{\mathsf{Kac}}}\rangle_{\mathsf{AB}}$, and the trace distance with two adjacent hybrids is bounded by

$$\begin{aligned}\left\| |\varphi_j\rangle\langle\varphi_j| - |\varphi_{j+1}\rangle\langle\varphi_{j+1}| \right\|_1 &\le \|\Pi_{i=1}^{T} \left(H_{f_i} \cdot P_{\sigma_i}\right) - \Pi_{i=1}^{T} \left(\widehat{H}_{f_i} \cdot P_{\sigma_i}\right) \|_\infty \\ &\le \Sigma_{i=1}^{T} \|H_{f_i} - \widehat{H}_{f_i}\|_\infty \le 8\pi \cdot 2^{-d} \cdot T = \mathrm{negl}(n) \quad ,\end{aligned}$$

where the second inequality is from the triangle inequality and the last inequality is from Lemma 19 in [LQS+24]. Thus, we have that by the triangle inequality,

$$\begin{aligned}&\left\| \mathop{\mathbb{E}}_{\mathsf{Kac} \leftarrow \mathsf{HP}_{n,T}} \left[|\mathcal{A}_t^{\mathsf{Kac}}\rangle\langle\mathcal{A}_t^{\mathsf{Kac}}|\right] - \mathop{\mathbb{E}}_{\widehat{\mathsf{Kac}} \leftarrow \widehat{\mathsf{HP}}_{n,T}} \left[|\mathcal{A}_t^{\widehat{\mathsf{Kac}}}\rangle\langle\mathcal{A}_t^{\widehat{\mathsf{Kac}}}|\right] \right\|_1 \\ \le \sum_{j=0}^{t-1} &\left\| \mathbb{E}\left[|\varphi_j\rangle\langle\varphi_j|\right] - \mathbb{E}\left[|\varphi_{j+1}\rangle\langle\varphi_{j+1}|\right] \right\|_1 \le t \cdot 8\pi \cdot 2^{-d} \cdot T = \mathrm{negl}(n) \quad .\end{aligned}$$

□

It is proved in [LQS+24] that with large enough T and d, the distribution $\mathsf{HP}_{n,T}$ is an RSS distribution. Formally, we have the following theorem by adjusting the parameters used in [LQS+24, Theorem 10].

Theorem 4.3. *For* $T = 30n$ *and* $d = 5n$*,* $\mathsf{HP}_{n,T}$ *is an* ϵ*-RSS distribution on* $\mathrm{U}(N)$ *with* $\epsilon = O\left(\frac{1}{N^2}\right)$*.*

In this work, we will prove that adding one more step of parallel Kac's walk results in a distribution that is close to Haar random. Our main result is as follows:

Theorem 4.4. *For $T = 30n$ and $d = 5n$, $\mathsf{HP}_{n,T+1}$ is computationally indistinguishable from Haar distribution.*

We view the procedure of sampling a unitary operator from $\mathsf{HP}_{n,T+1}$ as three stages:

1. sample a unitary operator Kac from $\mathsf{HP}_{n,T}$;
2. sample a unitary operator $H_f \cdot P_\sigma$ from $\mathsf{HP}_{n,1}$ corresponding to a random permutation $\sigma \in S_N$ and a random function $f : \{0,1\}^{n-1} \to \{0,1\}^{3d}$;
3. output $H_f \cdot P_\sigma \cdot \mathsf{Kac}$.

The proof of this theorem consists of three steps:

- We begin by establishing a purification of the adversary's view state when making queries to random unitary $H_f \cdot P_\sigma$. Specifically, we introduce two environment registers, H and P, which record function f and permutation σ being utilized. From the adversary's perspective, making queries to $H_f \cdot P_\sigma$ is equivalent to querying a *purified function-permutation oracle* HPO that acts on both adversary's registers and environment registers.
- Next, we demonstrate that as long as G is a random unitary sampled from an RSS distribution, the adversary cannot distinguish between making queries to $\mathsf{HPO} \cdot G$ and making queries to PR, where PR is the oracle defined in Definition 2.6. The key insight in this step is that if the environment state resides in the distinct block subspace, we can identify an isometry acting on the environment that connects the behaviors of HPO and PR. The random unitary G ensures that the environment state is nearly within the distinct block subspace.
- Let U be sampled from Haar distribution μ. Since both $\mathsf{HP}_{n,T}$ and μ are RSS distributions, we can conclude that oracle $\mathsf{HPO} \cdot \mathsf{Kac}$ and $\mathsf{HPO} \cdot U$ are both indistinguishable from the oracle PR to the adversary. Thus, $\mathsf{HPO} \cdot \mathsf{Kac}$ and $\mathsf{HPO} \cdot U$ are indistinguishable from each other. This implies that making queries to $H_f \cdot P_\sigma \cdot \mathsf{Kac}$ and $H_f \cdot P_\sigma \cdot U$ are indistinguishable as well. These two unitary operators correspond to $\mathsf{HP}_{n,T+1}$ and Haar distribution, respectively.

In the following sections, we will elucidate the purification process and introduce the purified function-permutation oracle HPO in Section 4.2. We then explain how to connect the actions of HPO and PR by introducing an isometry Compress in Section 4.3. Lastly, we prove the main result in Section 4.4.

4.2 The Purified Function-Permutation Oracle

To analysis the behavior of making queries to $H_f \cdot P_\sigma$, we employ a purified oracle similar to [MH24].

Definition 4.5 (Purified Function-Permutation Oracle)**.** *The* purified function-permutation oracle HPO *is a unitary on registers* A, H *and* P, *where*

- H *is a register with Hilbert space* $\mathcal{H}_{\mathsf{H}}$ *spanned by the orthogonal states* $|f\rangle$ *for all* $f \in \{0,1\}^{n-1} \to \{0,1\}^{3d}$,
- P *is a register with Hilbert space* $\mathcal{H}_{\mathsf{P}}$ *spanned by the orthogonal states* $|\sigma\rangle$ *for all* $\sigma \in \mathcal{S}_N$.

The unitary operator HPO *acts as*

$$\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} := \left(H_f P_\sigma\right)_{\mathsf{A}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} = H_{f_{\mathsf{A}}} |\sigma(x)\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \quad .$$

In the adversary's view, querying $H_f \cdot P_\sigma$ and querying HPO are identical in the following sense:

Fact 4.6. *For any adversary* $\mathcal{A}$ *holding the register* A*, the following two oracle are perfectly indistinguishable:*

- *Sample uniformly random* $\sigma \in S_N$ *and* $f : \{0,1\}^{n-1} \to \{0,1\}^{3d}$*. On each query, apply* $H_f P_\sigma$ *on register* A.
- *Initialize registers* H *and* P *in the state*

$$|\phi_{\{\}}\rangle := \frac{1}{\sqrt{2^{3d(n-1)}}} \sum_{f:\{0,1\}^{n-1}\to\{0,1\}^{3d}} |f\rangle_{\mathsf{H}} \otimes \frac{1}{\sqrt{N!}} \sum_{\sigma\in S_N} |\sigma\rangle_{\mathsf{P}} \quad .$$

  On each query, apply HPO *on registers* A, H *and* P.

Consider the view of an adversary $\mathcal{A}$ who makes t queries to the oracle $H_f \cdot P_\sigma \cdot G$ where G is an arbitrary unitary operator:

$$\rho_0 := \mathop{\mathbb{E}}_{H_f P_\sigma} \left[|\mathcal{A}_t^{H_f P_\sigma G}\rangle\langle\mathcal{A}_t^{H_f P_\sigma G}|_{\mathsf{AB}} \right]$$

where the view state is

$$|\mathcal{A}_t^{H_f P_\sigma G}\rangle_{\mathsf{AB}} = \prod_{i=1}^{t} \left(\left(H_f P_\sigma G\right)_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)} \right) |0\rangle_{\mathsf{AB}}$$

and the view of the same adversary A who makes t queries to the oracle HPO and the unitary G:

$$\rho_1 := \mathrm{Tr}_{\mathsf{HP}} \left(|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{HPO}\cdot G}|_{\mathsf{ABHP}} \right)$$

where the view state is

$$|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle_{\mathsf{ABHP}} = \prod_{i=1}^{t} \left(\mathsf{HPO}_{\mathsf{AHP}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)} \right) |0\rangle_{\mathsf{AB}} |\phi_{\{\}}\rangle_{\mathsf{HP}} \quad ,$$

Fact 4.6 states that $\rho_0 = \rho_1$. This enables us to analyze the purified state instead of the original mixed state. The action of the purified function-permutation oracle on the purified state can be better understood by introducing HP-relation states on registers H and P.

4.2.1 HP-Relation States

We define the following relation states on register H and P.

Definition 4.7 (HP-Relation States). *For $0 \le t \le N$ and a size-t relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\} \in \mathfrak{R}_t$, we define*

$$|\phi_R\rangle_{\mathsf{HP}} \coloneqq \frac{1}{\sqrt{2^{3d(n-1)}(N-t)!}} \sum_{f,\sigma} \sum_{b\in\{0,1\}^t} \prod_{i=1}^{t} \langle y_i| H_f |y_i^{\oplus b_i}\rangle \, \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \, |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}}$$

where $x^{\oplus 0} = x$ and $x^{\oplus 1} = \bar{x}$ for any $x \in \{0,1\}^n$, and $\delta_{y=x}$ is an indicator that equals 1 iff strings x and y are identical in every coordinate.

When considering a set of restricted relations, the corresponding relation states forms an orthogonal basis.

Lemma 4.8. *$\{|\phi_R\rangle\}_{R\in\mathfrak{R}^{\mathrm{DB}}}$ forms a set of orthogonal vectors.*

Before proving this lemma, we show some properties of H_f:

Lemma 4.9. *For any $x \in \{0,1\}^n$,*

1. $\mathbb{E}_f\left[\langle x| H_f |x\rangle\right] = \mathbb{E}_f\left[\langle x| H_f |\bar{x}\rangle\right] = 0$;
2. $\mathbb{E}_f\left[\overline{\langle x| H_f |x\rangle}\, \langle x| H_f |\bar{x}\rangle\right] = 0$;
3. $\mathbb{E}_f\left[\overline{\langle x| H_f |x\rangle}\, \langle \bar{x}| H_f |\bar{x}\rangle\right] = \mathbb{E}_f\left[\overline{\langle x| H_f |\bar{x}\rangle}\, \langle \bar{x}| H_f |x\rangle\right] = 0$.

Proof. By Eq. (8), if $x = 0y$ for some $y \in \{0,1\}^{n-1}$, then

1. $$\langle x| H_f |x\rangle = \mathrm{e}^{\mathrm{i}\alpha_y} \cos\theta_y \quad \text{and} \quad \langle x| H_f |\bar{x}\rangle = -\mathrm{e}^{\mathrm{i}\beta_y} \sin\theta_y.$$
   Since $\mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}\alpha_y}\right] = \mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}\beta_y}\right] = 0$, item 1 holds.

2. $$\overline{\langle x| H_f |x\rangle}\, \langle x| H_f |\bar{x}\rangle = -\mathrm{e}^{\mathrm{i}(\beta_y-\alpha_y)} \sin\theta_y \cos\theta_y.$$
   Since $\mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}(\beta_y-\alpha_y)}\right] = 0$, item 2 holds.

3. $$\overline{\langle x| H_f |x\rangle}\, \langle \bar{x}| H_f |\bar{x}\rangle = \mathrm{e}^{-2\mathrm{i}\alpha_y} \cos^2\theta_y \quad \text{and} \quad \overline{\langle x| H_f |\bar{x}\rangle}\, \langle \bar{x}| H_f |x\rangle = -\mathrm{e}^{-2\mathrm{i}\beta_y} \sin^2\theta_y.$$
   Since $\mathbb{E}_f\left[\mathrm{e}^{-2\mathrm{i}\alpha_y}\right] = \mathbb{E}_f\left[\mathrm{e}^{-2\mathrm{i}\beta_y}\right] = 0$, item 3 holds.

The case when $x = 1y$ can be argued similarly. □

Proof of Lemma 4.8. Consider two relations $R, S \in \mathfrak{R}^{\mathrm{DB}}$, where $R = \{(x_1, y_1), \ldots, (x_{|R|}, y_{|R|})\}$ and $S = \{(x'_1, y'_1), \ldots, (x'_{|S|}, y'_{|S|})\}$. By Lemma 4.9 item 1, if $|R| \neq |S|$, then $\langle \phi_R | \phi_S \rangle = 0$. So we may assume $|R| = |S| = t$. Then

$$\langle \phi_R | \phi_S \rangle = \frac{1}{2^{3d(n-1)}(N-t)!} \sum_{f,\sigma} \sum_{b,b' \in \{0,1\}^t} \prod_{i=1}^{t} \overline{\langle y_i | H_f | y_i^{\oplus b_i} \rangle} \delta_{y_i^{\oplus b_i} = \sigma(x_i)} \langle y'_i | H_f | (y'_i)^{\oplus b'_i} \rangle \delta_{(y'_i)^{\oplus b'_i} = \sigma(x'_i)}.$$

There are two cases to consider:

- $R = S$. Then by Lemma 4.9 item 2 and the fact that $\left|\langle x | H_f | x \rangle\right|^2 + \left|\langle x | H_f | \bar{x} \rangle\right|^2 = 1$ for all $x \in \{0,1\}^n$, it is not hard to check that $\langle \phi_R | \phi_S \rangle = 1$.
- $R \neq S$. Now we consider three sub-cases:
  - $\mathrm{Im}(R) = \mathrm{Im}(S)$, then $\mathrm{Dom}(R) \neq \mathrm{Dom}(S)$. Without loss of generality, we can assume that $y_i = y'_i$ for all $i \in [t]$. Fix i such that $x_i \neq x'_i$. For all $b_i, b'_i \in \{0,1\}$, if $b_i = b'_i$, then for all σ, $\delta_{y_i^{\oplus b_i} = \sigma(x_i)} \delta_{(y'_i)^{\oplus b'_i} = \sigma(x'_i)} = 0$; if $b_i \neq b'_i$, then by Lemma 4.9 item 2,
    $$\sum_f \overline{\langle y_i | H_f | y_i^{\oplus b_i} \rangle} \langle y'_i | H_f | (y'_i)^{\oplus b'_i} \rangle = 0.$$
    Both cases imply $\langle \phi_R | \phi_S \rangle = 0$.
  - $\mathrm{Im}(R) \neq \mathrm{Im}(S)$ and $\mathrm{BIm}(R) = \mathrm{BIm}(S)$. Without loss of generality, we can assume that there exists $i \in [t]$ such that $y'_i = \overline{y_i}$. If $b_i = b'_i$, then by Lemma 4.9 item 3,
    $$\sum_f \overline{\langle y_i | H_f | y_i^{\oplus b_i} \rangle} \langle y'_i | H_f | (y'_i)^{\oplus b'_i} \rangle = 0;$$
    if $b_i \neq b'_i$, then by Lemma 4.9 item 2,
    $$\sum_f \overline{\langle y_i | H_f | y_i^{\oplus b_i} \rangle} \langle y'_i | H_f | (y'_i)^{\oplus b'_i} \rangle = 0.$$
    Both cases imply $\langle \phi_R | \phi_S \rangle = 0$.
  - $\mathrm{BIm}(R) \neq \mathrm{BIm}(S)$. By Lemma 4.9 item 1, $\langle \phi_R | \phi_S \rangle = 0$.

□

4.2.2 Action of HPO

Using the relation states defined in the previous section, the action of HPO oracle is described by the following lemma:

Lemma 4.10. *For $0 \leq t \leq N$, $x \in \{0,1\}^n$ and a size-t relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\} \in \mathfrak{R}_t$, we have*

$$\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |\phi_R\rangle_{\mathsf{HP}} = \frac{1}{\sqrt{N-t}} \sum_{y \in \{0,1\}^n} |y\rangle_{\mathsf{A}} \otimes |\phi_{R \cup \{x,y\}}\rangle_{\mathsf{HP}} \quad .$$

Proof. Expanding the definitions, we have

$$\begin{aligned}&\mathsf{HPO}_{\mathsf{AHP}}\left|x\right\rangle_{\mathsf{A}}\left|\phi_R\right\rangle_{\mathsf{HP}}\\=&\frac{1}{\sqrt{2^{3d(n-1)}(N-t)!}}\sum_{f,\sigma}\sum_{b\in\{0,1\}^t}\prod_{i=1}^{t}\left\langle y_i\right|H_f\left|y_i^{\oplus b_i}\right\rangle\delta_{y_i^{\oplus b_i}=\sigma(x_i)}H_f\left|\sigma(x)\right\rangle_{\mathsf{A}}\left|f\right\rangle_{\mathsf{H}}\left|\sigma\right\rangle_{\mathsf{P}}\end{aligned}\tag{9}$$

Note that for a fix $f:\{0,1\}^{n-1}\to\{0,1\}^{3d}$, the matrix H_f can be expressed as

$$H_f=\sum_{y,y'\in\{0,1\}^n}\left\langle y\right|H_f\left|y'\right\rangle\left|y\right\rangle\!\left\langle y'\right|$$

and $\left\langle y\right|H_f\left|y'\right\rangle=0$ if y and y' are not in the same block. Therefore, we can write H_f as

$$H_f=\sum_{y\in\{0,1\}^n,b\in\{0,1\}}\left\langle y\right|H_f\left|y^{\oplus b}\right\rangle\left|y\right\rangle\!\left\langle y^{\oplus b}\right|\quad.$$

And we can write $\left|\sigma(x)\right\rangle$ as $\sum_{y\in\{0,1\}^n}\delta_{y=\sigma(x)}\left|y\right\rangle$. Therefore, we have

$$\begin{aligned}H_f\left|\sigma(x)\right\rangle&=\left(\sum_{y\in\{0,1\}^n,b\in\{0,1\}}\left\langle y\right|H_f\left|y^{\oplus b}\right\rangle\left|y\right\rangle\!\left\langle y^{\oplus b}\right|\right)\cdot\left(\sum_{y\in\{0,1\}^n}\delta_{y=\sigma(x)}\left|y\right\rangle\right)\\&=\sum_{y\in\{0,1\}^n,b\in\{0,1\}}\left\langle y\right|H_f\left|y^{\oplus b}\right\rangle\delta_{y^{\oplus b}=\sigma(x)}\left|y\right\rangle\quad.\end{aligned}$$

Inserting this into (9), we have

$$\begin{aligned}&\mathsf{HPO}_{\mathsf{AHP}}\left|x\right\rangle_{\mathsf{A}}\left|\phi_R\right\rangle_{\mathsf{HP}}=\\&\frac{1}{\sqrt{N-t}}\sum_{y_{t+1}\in\{0,1\}^n}\left|y_{t+1}\right\rangle_{\mathsf{A}}\otimes\frac{1}{\sqrt{2^{3d(n-1)}(N-t-1)!}}\sum_{f,\sigma}\sum_{b\in\{0,1\}^{t+1}}\prod_{i=1}^{t+1}\left\langle y_i\right|H_f\left|y_i^{\oplus b_i}\right\rangle\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\left|f\right\rangle_{\mathsf{H}}\left|\sigma\right\rangle_{\mathsf{P}}\\&=\frac{1}{\sqrt{N-t}}\sum_{y_{t+1}\in\{0,1\}^n}\left|y_{t+1}\right\rangle_{\mathsf{A}}\otimes\left|\phi_{R\cup\{x,y_{t+1}\}}\right\rangle_{\mathsf{HP}}\quad.\end{aligned}$$

□

By expanding HPO, we can then rewrite the view state of an adversary A with query access to the oracle HPO and the unitary G in terms of HP-relation states:

Corollary 4.11. *For an arbitrary n-qubit unitary operator G and a t-query adversary $\mathcal{A}$ with query access to* $\mathsf{HPO}\cdot G$*, define the state after $\mathcal{A}$ finishing all the queries to be*

$$\left|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\right\rangle_{\mathsf{ABHP}}:=\prod_{i=1}^{t}\left(\mathsf{HPO}_{\mathsf{AHP}}\cdot G_{\mathsf{A}}\cdot A_{\mathsf{AB}}^{(i)}\right)\left|0\right\rangle_{\mathsf{AB}}\left|\phi_{\{\}}\right\rangle_{\mathsf{HP}}\quad.$$

Then we have:

$$\left|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\right\rangle_{\mathsf{ABHP}}=\sqrt{\frac{(N-t)!}{N!}}\sum_{\substack{(x_1,\ldots,x_t)\in(\{0,1\}^n)^t\\(y_1,\ldots,y_t)\in(\{0,1\}^n)^t}}\prod_{i=1}^{t}\left(\left|y_i\right\rangle\!\left\langle x_i\right|_{\mathsf{A}}\cdot G_{\mathsf{A}}\cdot A_{\mathsf{AB}}^{(i)}\right)\left|0\right\rangle_{\mathsf{AB}}\left|\phi_{\{(x_i,y_i)\}_{i=1}^t}\right\rangle_{\mathsf{HP}}$$

4.3 Connecting HPO and PR via Compress Isometry

Recall the path-recording oracle PR we introduce earlier, acting on registers A, X and Y, and the state after $\mathcal{A}$'s queries to $\mathsf{PR} \cdot G$:

$$|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABXY}} = \prod_{i=1}^{t} \left(\mathsf{PR} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{XY}}$$
$$= \sqrt{\prod_{i=0}^{t-1} \frac{1}{(N-2i)}} \sum_{\substack{(x_1,\ldots,x_t)\in(\{0,1\}^n)^t \\ (y_1,\ldots,y_t)\in\mathsf{DB}_t}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} |\{(x_i,y_i)\}_{i=1}^{t}\rangle_{\mathsf{XY}} \ .$$

By defining the following isometry, we are able to connect the behavior of the purified function-permutation oracle HPO and the path-recording oracle PR.

Definition 4.12. *We define an isometry, denoted* $\mathsf{Compress} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}}$*, as:*

$$\mathsf{Compress} := \sum_{R\in\mathfrak{R}^{\mathsf{DB}}} |R\rangle\langle\phi_R| \ .$$

Lemma 4.13. *Define the* distinct block subspace projector *for* HPO*-relation states as*

$$\widetilde{\Pi}_{\mathsf{HP}}^{(t)} := \sum_{R\in\mathfrak{R}_t^{\mathsf{DB}}} |\phi_R\rangle\langle\phi_R| \ .$$

We have that for all n-qubit unitaries G,

$$\mathsf{Compress} \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle_{\mathsf{ABHP}} = \left(1 + O\left(\frac{t^2}{N}\right)\right) \Pi_{\mathsf{X}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABXY}} \ .$$

Proof. By Corollary 4.11, it is easy to see that

$$\mathsf{Compress} \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle_{\mathsf{ABHP}}$$
$$= \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in\mathsf{DB}_t \\ (y_1,\ldots,y_t)\in\mathsf{DB}_t}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} |\{(x_i,y_i)\}_{i=1}^{t}\rangle_{\mathsf{HP}} \ . \tag{10}$$

By Fact 2.7, we have

$$\Pi_{\mathsf{X}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABXY}}$$
$$= \sqrt{\prod_{i=0}^{t-1} \frac{1}{(N-2i)}} \sum_{\substack{(x_1,\ldots,x_t)\in\mathsf{DB}_t \\ (y_1,\ldots,y_t)\in\mathsf{DB}_t}} \prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}} |\{(x_i,y_i)\}_{i=1}^{t}\rangle_{\mathsf{XY}} \ . \tag{11}$$

Therefore we observe that

$$\mathsf{Compress} \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle = \rho \cdot \Pi_{\mathsf{X}}^{(t)} \cdot |\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle$$

where

$$\rho = \sqrt{\prod_{i=0}^{t-1} \frac{N-i}{N-2i}} = \sqrt{\prod_{i=0}^{t-1} \left(1 + \frac{i}{N-2i}\right)} = 1 + O\left(\frac{t^2}{N}\right) \quad .$$

□

With the above lemma, we are able to argue that the views before and after the projection $\widetilde{\Pi}^{(t)}_{\mathsf{HP}}$ of an adversary are close if we sample G according to some distribution.

Lemma 4.14. *For any ϵ-RSS distribution $\mathcal{R}$ on $\mathrm{U}(N)$ with $\epsilon = O\left(\frac{1}{N^2}\right)$, define $\mathcal{D}$ to be a distribution that samples $G = SK$ where $S \leftarrow \mathcal{S}_N$ and $K \leftarrow \mathcal{R}$. Let $\mathcal{A}$ be a t-query oracle adversary. Then we have*

$$\left\| \mathrm{Tr}_{\mathsf{HP}}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \right) - \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \right) \right\|_1 = O\left(\frac{t^2}{N}\right) \quad .$$

Proof. We first apply Lemma 2.1:

$$\left\| \mathrm{Tr}_{\mathsf{HP}}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \right) - \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \right) \right\|_1 = 1 - \mathrm{Tr}\left(\widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \right] \right).$$

Notice that $\widetilde{\Pi}^{(t)}_{\mathsf{HP}} = \mathrm{Compress}^\dagger \cdot \mathrm{Compress} \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}}$. Therefore

$$\begin{aligned}
&\left\| \mathrm{Tr}_{\mathsf{HP}}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \right) - \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \right) \right\|_1 \\
&= 1 - \mathrm{Tr}\left(\mathrm{Compress} \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}^{(t)}_{\mathsf{HP}} \cdot \mathrm{Compress}^\dagger \right) \\
&= 1 - \left(1 + O\left(\frac{t^2}{N}\right)\right) \mathrm{Tr}\left(\Pi^{(t)}_{\mathsf{X}} \cdot \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{\mathrm{HPO}\cdot G} \rangle\langle \mathcal{A}_t^{\mathrm{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \right) = O\left(\frac{t^2}{N}\right) \quad ,
\end{aligned}$$

where the second equality is from Lemma 4.13 and the last one is from Lemma 3.1. □

4.4 Computational Indistinguishability of $\mathsf{HP}_{n,T+1}$

We first show that if G consists of an RSS and a random permutation, then the view of an adversary when making queries to $H_f P_\sigma G$ is nearly the view it will see when making queries to the path-recording oracle PR.

Lemma 4.15. *For any ϵ-RSS distribution $\mathcal{R}$ on $\mathrm{U}(N)$ with $\epsilon = O\left(\frac{1}{N^2}\right)$, define $\mathcal{D}$ to be a distribution that samples $G = SK$ where $S \leftarrow \mathcal{S}_N$ and $K \leftarrow \mathcal{R}$. Let $\mathcal{A}$ be a t-query oracle adversary. Then*

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{H_f P_\sigma \leftarrow \mathsf{HP}_{n,1}, G\leftarrow\mathcal{D}} \left[|\mathcal{A}_t^{H_f P_\sigma G} \rangle\langle \mathcal{A}_t^{H_f P_\sigma G}| \right], \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathrm{PR}} \rangle\langle \mathcal{A}_t^{\mathrm{PR}}|_{\mathsf{ABXY}} \right) \right) = O\left(\frac{t^2}{N}\right)$$

Proof. We start with defining the following states:

$$\rho_0 = \mathop{\mathbb{E}}_{H_f P_\sigma \leftarrow \mathsf{HP}_{n,1}, G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{H_f P_\sigma G}\rangle\langle\mathcal{A}_t^{H_f P_\sigma G}| \right]$$

$$\rho_1 = \mathrm{Tr}_{\mathsf{HP}} \left(\mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \right)$$

$$\rho_2 = \mathrm{Tr}_{\mathsf{HP}} \left(\widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{HPO}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{HPO}\cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \right)$$

$$\rho_3 = \mathrm{Tr}_{\mathsf{XY}} \left(\Pi_{\mathsf{X}}^{(t)} \cdot \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}} \right] \cdot \Pi_{\mathsf{X}}^{(t)} \right)$$

$$\rho_4 = \mathrm{Tr}_{\mathsf{XY}} \left(\mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}} \right] \right)$$

$$\rho_5 = \mathrm{Tr}_{\mathsf{XY}} \left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}} \right)$$

By Fact 4.6, $\rho_0 = \rho_1$. By Lemma 4.14, $\|\rho_1 - \rho_2\|_1 \le O\left(\frac{t^2}{N}\right)$. And we have that $\|\rho_2 - \rho_3\|_1 = O\left(\frac{t^2}{N}\right)$ by Lemma 4.13 and the fact that Compress is applied only on the environment register. By Lemma 3.1 and Lemma 2.1, $\|\rho_3 - \rho_4\|_1 \le O\left(\frac{t^2}{N}\right)$. $\rho_4 = \rho_5$ since

$$\begin{aligned}
\mathrm{Tr}_{\mathsf{XY}} \left(\mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}} \right] \right) &= \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[\mathrm{Tr}_{\mathsf{XY}} \left(|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}} \right) \right] \\
&= \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[\mathrm{Tr}_{\mathsf{XY}} \left(G_{\mathsf{X}}^{\otimes t} \cdot |\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}} \cdot G_{\mathsf{X}}^{\otimes t,\dagger} \right) \right] \\
&= \mathrm{Tr}_{\mathsf{XY}} \left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}} \right) \quad ,
\end{aligned}$$

where the second equality is from Lemma 2.8. □

We now prove that the distribution $\mathsf{HP}_{n,T+1}$ is computationally indistinguishable from Haar distribution.

Proof of Theorem 4.4. Consider an adversary $\mathcal{A}$ who makes $t = \mathrm{poly}(n)$ queries. Note that the distribution of $H_f \cdot P_\sigma \cdot \mathsf{Kac}$ is the same as the distribution of $H_f \cdot P_\sigma \cdot S \cdot \mathsf{Kac}$ where we add a random permutation matrix $S \leftarrow \mathcal{S}_N$. Therefore, we have

$$\mathop{\mathbb{E}}_{H_f P_\sigma \mathsf{Kac}} \left[|\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}\rangle\langle\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}| \right] = \mathop{\mathbb{E}}_{H_f P_\sigma S \mathsf{Kac}} \left[|\mathcal{A}_t^{H_f P_\sigma S \mathsf{Kac}}\rangle\langle\mathcal{A}_t^{H_f P_\sigma S \mathsf{Kac}}| \right] \quad .$$

Since Kac is sampled from an ϵ-RSS distribution with $\epsilon = O\left(\frac{1}{N^2}\right)$ and S is a random permutation matrix, we have by Lemma 4.15

$$\mathsf{TD} \left(\mathop{\mathbb{E}}_{H_f P_\sigma \mathsf{Kac}} \left[|\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}\rangle\langle\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}| \right], \mathrm{Tr}_{\mathsf{XY}} \left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}} \right) \right) = O\left(\frac{t^2}{N}\right) \quad .$$

Now we substitute the unitary Kac with a Haar random unitary U. We have the following relationship:

$$\mathop{\mathbb{E}}_{U}\left[|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|\right] = \mathop{\mathbb{E}}_{H_f P_\sigma S U}\left[|\mathcal{A}_t^{H_f P_\sigma S U}\rangle\langle\mathcal{A}_t^{H_f P_\sigma S U}|\right] \quad .$$

Since the Haar distribution is a 0-RSS distribution and S is a random permutation matrix, we have by Lemma 4.15

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U}\left[|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|\right], \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}}\right)\right) = O\left(\frac{t^2}{N}\right) \quad .$$

Then by the triangle inequality, we have

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U}\left[|\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|\right], \mathop{\mathbb{E}}_{H_f P_\sigma \mathsf{Kac}}\left[|\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}\rangle\langle\mathcal{A}_t^{H_f P_\sigma \mathsf{Kac}}|\right]\right) = O\left(\frac{t^2}{N}\right) = \mathrm{negl}(n) \quad .$$

□

Our construction of PRU based on parallel Kac's walk is to use QPRF and QPRP when sampling from $\widehat{\mathsf{HP}}_{n,T+1}$.

Theorem 4.16. *By replacing random functions and random permutations with their post-quantum secure pseudorandom counterparts in the sampling procedure of $\widehat{\mathsf{HP}}_{n,T+1}$ where $T = 30n$ and $d = 5n$, we obtain a* PRU.

Proof. By the post-quantum security of QPRP and QPRF, Lemma 4.2 and Theorem 4.4, the new distribution is computationally indistinguishable from Haar distribution. This new distribution can be sampled in polynomial time since QPRP and QPRF can be sampled efficiently.

□

5 Showing the strong security of $\mathsf{HP}_{n,2T+1}$

We further show that our construction, based on Kac's walk, also achieves the strong security when adversaries are granted query access to the inverse unitary. Formally,

Theorem 5.1 ($\mathsf{HP}_{n,2T+1}$ is a statistical strong-PRU)**.** *Let $\mathcal{A}$ be a t-query oracle adversary capable of performing both forward and inverse queries to oracle $\mathcal{O}$, and let $\mathsf{HP}_{n,2T+1}$ be defined as in Definition 4.1 with $T = 30n$ and $d = 5n$. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}\right], \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu}\left[|\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}\right]\right) \leq \frac{2t(11t+20)}{N^{1/8}}. \tag{12}$$

This theorem establishes the statistical strong security. Then, assuming the existence of post-quantum secure OWFs, we infer the existence of computationally strong PRUs. The proof of this theorem follows a similar routine as Theorem 4.4:

- We first use the purification to establish that making queries to $H_f \cdot P_\sigma$ is equivalent to querying HPO.
- We then show that the adversary cannot distinguish between making queries to $D \cdot \mathrm{HPO} \cdot C$ and querying a path-recording oracle V introduced in Section 5.3. Here C and D are sampled from either $\mathrm{HP}_{n,T}$ or Haar distribution μ to ensure that the environment state is mostly within the distinct block subspace. We require two unitary operator to achieve this purpose, as the adversary can make both forward and inverse query.
- If C and D are sampled from $\mathrm{HP}_{n,T}$, querying $D \cdot \mathrm{HPO} \cdot C$ corresponds to querying O such that $O \leftarrow \mathrm{HP}_{n,2T+1}$. On the other hand, if C and D are sampled from μ, querying $D \cdot \mathrm{HPO} \cdot C$ corresponds to querying O such that $O \leftarrow \mu$.

In the following sections, we first extend the HPO oracle and the HP-relation states to handle with inverse queries and describe the action of HPO using the HP-relation states in Section 5.1. Then, we introduce a partial path-recording oracle W in Section 5.2 as a intermediate operator to connect the action of HPO and the path-recording oracle V defined in Section 5.3. Finally, we prove Theorem 5.1 in Section 5.4.

5.1 Action of HPO oracle and its inverse

We first add inverse query to the HPO oracle.

Definition 5.2 (Purified Function-Permutation Oracle)**.** *The* purified function permutation oracle HPO *is a unitary on registers* A, H *and* P*, where*

- H *is a register with Hilbert space* $\mathcal{H}_{\mathsf{H}}$ *spanned by the orthogonal states* $|f\rangle$ *for all* $f \in \{0,1\}^{n-1} \to \{0,1\}^{3d}$,
- P *is a register with Hilbert space* $\mathcal{H}_{\mathsf{P}}$ *spanned by the orthogonal states* $|\sigma\rangle$ *for all* $\sigma \in \mathcal{S}_N$.

The unitary operator HPO *acts as*

$$\mathrm{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} := \left(H_f P_\sigma\right)_{\mathsf{A}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \quad ,$$

and $\mathrm{HPO}^\dagger$ *acts as*

$$\mathrm{HPO}^\dagger_{\mathsf{AHP}} |y\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} = \left(H_f P_\sigma\right)^\dagger_{\mathsf{A}} |y\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \quad ,$$

Similar to Fact 4.6, querying $H_f \cdot P_\sigma$ and querying HPO are identical in the adversary's view:

Fact 5.3. *For any adversary* $\mathcal{A}$ *holding the register* A*, the following two oracle are perfectly indistinguishable:*

- *Sample uniformly random* $\sigma \in S_N$ *and* $f : \{0,1\}^{n-1} \to \{0,1\}^{3d}$*. On each forward query, apply* $H_f P_\sigma$ *(*$(H_f P_\sigma)^\dagger$*, if it is an inverse query) on register* A*.*

- *Initialize registers* H *and* P *in the state*

$$|\phi_{\{\}}\rangle := \frac{1}{\sqrt{2^{3d(n-1)}}} \sum_{f:\{0,1\}^{n-1}\to\{0,1\}^{3d}} |f\rangle_{\mathsf{H}} \otimes \frac{1}{\sqrt{N!}} \sum_{\sigma\in S_N} |\sigma\rangle_{\mathsf{P}} \quad .$$

On each forward query, apply HPO *(*$\mathsf{HPO}^\dagger$*, if it is an inverse query) on registers* A, H *and* P.

The HP-relation states are modified in the following way.

Definition 5.4 (HP-Relation States). *For two integers* l *and* r *such that* $0 \le l + r \le N$*, and two relations* $L = \{(x_1, y_1), \ldots, (x_l, y_l)\} \in \mathfrak{R}_l$ *and* $R = \{(x'_1, y'_1), \ldots, (x'_r, y'_r)\} \in \mathfrak{R}_r$*, we define*

$$|\phi_{L,R}\rangle_{\mathsf{HP}} := \frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i| H_f |y_i^{\oplus b_i}\rangle \, \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \prod_{i=1}^{r} \langle y'^{\oplus b'_i}_i| H_f^\dagger |y'_i\rangle \, \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \quad .$$

where $x^{\oplus 0} = x$ *and* $x^{\oplus 1} = \overline{x}$ *for any* $x \in \{0,1\}^n$*, and* $\delta_{y=x}$ *is an indicator that equals* 1 *iff strings* x *and* y *are identical in every coordinate.*

The HP-relation states are orthonormal if we require $L \cup R \in \mathfrak{R}^{\mathrm{DB}}$.

Lemma 5.5. $\{|\phi_{L,R}\rangle\}_{L,R:L\cup R\in\mathfrak{R}^{\mathrm{DB}}}$ *forms a set of orthonormal vectors.*

Intuitively, the action of HPO is to add query pair (x, y) into the set L, while the action of $\mathsf{HPO}^\dagger$ is to add query pair (x, y) into the set R.

Lemma 5.6. *For two integers* l *and* r *such that* $0 \le l+r \le N$*, and two relations* $L = \{(x_1, y_1), \ldots, (x_l, y_l)\} \in \mathfrak{R}_l$ *and* $R = \{(x'_1, y'_1), \ldots, (x'_r, y'_r)\} \in \mathfrak{R}_r$*, we have for* $x \in \{0,1\}^n$

$$\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}} = \frac{1}{\sqrt{N-l-r}} \sum_{y\in\{0,1\}^n} |y\rangle_{\mathsf{A}} \otimes |\phi_{L\cup\{x,y\},R}\rangle_{\mathsf{HP}} \quad .$$

Similarly, we have for $y \in \{0,1\}^n$

$$\mathsf{HPO}^\dagger_{\mathsf{AHP}} |y\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}} = \frac{1}{\sqrt{N-l-r}} \sum_{x\in\{0,1\}^n} |x\rangle_{\mathsf{A}} \otimes |\phi_{L,R\cup\{x,y\}}\rangle_{\mathsf{HP}} \quad .$$

We provide the proofs of the above two lemmas in Appendix A.

5.2 Partial path-recording oracle W

We first introduce the variable-length registers along with some relevant notations from [MH24].

For $t \in \mathbb{N}$, the register $\mathsf{R}^{(t)} := \left(\mathsf{R}_{\mathsf{X}}^{(t)}, \mathsf{R}_{\mathsf{Y}}^{(t)}\right)$ is defined with the Hilbert space

$$\mathcal{H}_{\mathsf{R}^{(t)}} := \mathcal{H}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \otimes \mathcal{H}_{\mathsf{R}_{\mathsf{Y}}^{(t)}} := \left(\mathbb{C}^N\right)^{\otimes t} \otimes \left(\mathbb{C}^N\right)^{\otimes t} \quad .$$

Note that $\mathsf{R}_{\mathsf{X}}^{(t)}$ and $\mathsf{R}_{\mathsf{Y}}^{(t)}$ both consist of t registers with Hilbert space $\mathbb{C}^N$. For $i \le t$, let $\mathsf{R}_{\mathsf{X},i}^{(t)}$ denote the i-th register in $\mathsf{R}_{\mathsf{X}}^{(t)}$, and $\mathsf{R}_{\mathsf{Y},i}^{(t)}$ denote the i-th register in $\mathsf{R}_{\mathsf{Y}}^{(t)}$. The register R is defined with the infinite dimensional Hilbert space $\mathcal{H}_{\mathsf{R}} := \bigoplus_{t\ge 0} \mathcal{H}_{\mathsf{R}^{(t)}}$. And the register L is defined in the same way.

For integers $l, r \ge 0$, $\Pi_{l,r,\mathsf{LR}}$ is the projector onto the Hilbert space $\mathcal{H}_{\mathsf{L}^{(l)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$. For $t \ge 0$, $\Pi_{\le t,\mathsf{LR}}$ is the projector onto the Hilbert space $\bigoplus_{l,r\ge 0: l+r\le t} \mathcal{H}_{\mathsf{L}^{(l)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$. For a operator M_{LR}, $M_{l,r,\mathsf{LR}} := M_{\mathsf{LR}} \cdot \Pi_{l,r,\mathsf{LR}}$, $M_{\le t,\mathsf{LR}} := M_{\mathsf{LR}} \cdot \Pi_{\le t,\mathsf{LR}}$, and $M^{\dagger}_{\le t,\mathsf{LR}}$ is $\left(M_{\le t,\mathsf{LR}}\right)^{\dagger}$. For any unitary U, define $U^{\otimes *} := \sum_{t=0}^{\infty} U^{\otimes t}$.

Definition 5.7 (Definition of W)**.** *Let L, R such that $L \cup R \in \mathfrak{R}^{\mathrm{DB}}$. We define operators W^L and W^R to be the linear maps such that for $x \in \{0,1\}^n$ and $x \notin \mathrm{BDom}\,(L \cup R)$*

$$W^L |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - 2|L \cup R|}} \sum_{\substack{y\in\{0,1\}^n \\ y\notin \mathrm{BIm}(L\cup R)}} |y\rangle_{\mathsf{A}} \otimes |L \cup \{x,y\}\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}} \quad ,$$

and for $y \in \{0,1\}^n$ and $y \notin \mathrm{BIm}\,(L \cup R)$

$$W^R |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - 2|L \cup R|}} \sum_{\substack{x\in\{0,1\}^n \\ x\notin \mathrm{BDom}(L\cup R)}} |x\rangle_{\mathsf{A}} \otimes |L\rangle_{\mathsf{L}} \otimes |R \cup \{x,y\}\rangle_{\mathsf{R}} \quad .$$

The partial path-recording oracle W is defined as $W = W^L + W^{R,\dagger}$.

By the above definition, it is easy to verify that W^L and W^R are partial isometries, and that

$$W^L W^R = W^{R,\dagger} W^{L,\dagger} = 0. \tag{13}$$

Thus

$$W^{\dagger} W = W^{L,\dagger} W^L + W^R W^{R,\dagger}. \tag{14}$$

Therefore $WW^{\dagger}W = W$, which implies W is a partial isometry.

Notation 5.8. *For a partial isometry G, let $\Pi^{\mathrm{Dom}(G)} = G^{\dagger} \cdot G$ and $\Pi^{\mathrm{Im}(G)} = G \cdot G^{\dagger}$ denote the orthogonal projectors onto $\mathrm{Dom}\,(G)$ and $\mathrm{Im}\,(G)$.*

W is a restriction of HPO up to a partial isometry defined as follows.

Definition 5.9. *We define a partial isometry, denoted $\mathsf{Compress} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{L}} \otimes \mathcal{H}_{\mathsf{R}}$, as:*

$$\mathsf{Compress} := \sum_{L\cup R \in \mathfrak{R}^{\mathrm{DB}}} \left(|L\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}}\right) \langle \phi_{L,R}|_{\mathsf{PF}} \,.$$

Lemma 5.10. *For $0 \le t < N$,*

$$\left\| W_{\le t} - \mathsf{Compress} \cdot \mathsf{HPO} \cdot \mathsf{Compress}^{\dagger} \cdot \Pi^{\mathrm{Dom}(W)} \cdot \Pi_{\le t} \right\|_{\infty} \le \frac{2t}{N-t}, \tag{15}$$

$$\left\| (W^{\dagger})_{\le t} - \mathsf{Compress} \cdot \mathsf{HPO}^{\dagger} \cdot \mathsf{Compress}^{\dagger} \cdot \Pi^{\mathrm{Im}(W)} \cdot \Pi_{\le t} \right\|_{\infty} \le \frac{2t}{N-t}. \tag{16}$$

Proof. We will prove Eq. (15), and Eq. (16) follows from a symmetric argument. Denote

$$X = \text{Compress} \cdot \text{HPO} \cdot \text{Compress}^\dagger \cdot \Pi^{\text{Dom}(W)} \cdot \Pi_{\le t},$$

$$X^L = \text{Compress} \cdot \text{HPO} \cdot \text{Compress}^\dagger \cdot \Pi^{\text{Dom}(W^L)} \cdot \Pi_{\le t}$$

and

$$X^R = \Pi_{\le t} \cdot \Pi^{\text{Im}(W^R)} \cdot \text{Compress} \cdot \text{HPO}^\dagger \cdot \text{Compress}^\dagger.$$

Then by Eq. (14), $X = X^L + X^{R,\dagger}$. To prove Eq. (15), it suffices to prove

$$\left\|W^L_{\le t} - X^L\right\|_\infty \le \frac{t}{N-t} \quad \text{and} \quad \left\|(W^{R,\dagger})_{\le t} - X^{R,\dagger}\right\|_\infty \le \frac{t}{N-t}. \tag{17}$$

Next, we prove the first inequality in Eq. (17). The other inequality follows from a symmetric argument. For L, R such that $L \cup R \in \mathfrak{R}^{\text{DB}}$ and $|L \cup R| \le t$, and $x \in \{0,1\}^n$ such that $x \notin \text{BDom}(L \cup R)$, we have

$$X^L |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in \{0,1\}^n \\ y \notin \text{BIm}(L \cup R)}} |y\rangle_{\mathsf{A}} \otimes |L \cup \{x,y\}\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}} \quad ,$$

and

$$W^L_{\le t} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - 2|L \cup R|}} \sum_{\substack{y \in \{0,1\}^n \\ y \notin \text{BIm}(L \cup R)}} |y\rangle_{\mathsf{A}} \otimes |L \cup \{x,y\}\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}} \quad .$$

Then for such x, L, R, we have

$$\begin{aligned}
&\left\|\left(W^L_{\le t} - X^L\right) |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}\right\|_2 \\
&= \left\|\left(\frac{1}{\sqrt{N - |L \cup R|}} - \frac{1}{\sqrt{N - 2|L \cup R|}}\right) \sum_{\substack{y \in \{0,1\}^n \\ y \notin \text{BIm}(L \cup R)}} |y\rangle_{\mathsf{A}} \otimes |L \cup \{x,y\}\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}}\right\|_2 \\
&= \sqrt{\left(\frac{1}{\sqrt{N - |L \cup R|}} - \frac{1}{\sqrt{N - 2|L \cup R|}}\right)^2 (N - 2|L \cup R|)} \\
&= 1 - \sqrt{1 - \frac{|L \cup R|}{N - |L \cup R|}} \\
&\le \frac{|L \cup R|}{N - |L \cup R|}.
\end{aligned}$$

Note that for other x, L, R, $X^L |x\rangle |L\rangle |R\rangle = W^L |x\rangle |L\rangle |R\rangle = 0$. Therefore,

$$\left\|W^L_{\le t} - X^L\right\|_\infty = \sup_{\substack{x,L,R: \\ L \cup R \in \mathfrak{R}^{\text{DB}}, |L \cup R| \le t \\ x \notin \text{BDom}(L \cup R)}} \left\|\left(W^L_{\le t} - X^L\right) |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}\right\|_2 \le \frac{t}{N-t}.$$

□

5.3 Path-recording oracle V

Definition 5.11 (Definition of V). *Let $L, R \in \mathfrak{R}$. We define operators V^L and V^R to be the linear maps such that for $x \in \{0,1\}^n$*

$$V^L |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - |\mathrm{BIm}(L \cup R)|}} \sum_{\substack{y \in \{0,1\}^n \\ y \notin \mathrm{BIm}(L \cup R)}} |y\rangle_{\mathsf{A}} \otimes |L \cup \{x, y\}\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}} \quad ,$$

and for $y \in \{0,1\}^n$

$$V^R |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \frac{1}{\sqrt{N - |\mathrm{BDom}(L \cup R)|}} \sum_{\substack{x \in \{0,1\}^n \\ x \notin \mathrm{BDom}(L \cup R)}} |x\rangle_{\mathsf{A}} \otimes |L\rangle_{\mathsf{L}} \otimes |R \cup \{x, y\}\rangle_{\mathsf{R}} \quad .$$

The path-recording oracle V is defined to be

$$V = V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger}) + (\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger} \quad . \tag{18}$$

By the above definition, it is easy to verify that V^L and V^R are partial isometries, and that $V^L(V^R)$ differs from $W^L(W^R)$ by only a projection, i.e.,

$$V^L \cdot \Pi^{\mathrm{Dom}(W^L)} = W^L \quad \text{and} \quad \Pi^{\mathrm{Im}(W^R)} \cdot V^R = W^R. \tag{19}$$

Also, we have

$$W^L \cdot V^R = W^R \cdot V^L = 0. \tag{20}$$

Claim 5.12. *V is a partial isometry.*

Proof. We first show that $V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger})$ is a partial isometry. This is true if and only if $(\mathbb{1} - V^R \cdot V^{R,\dagger}) \cdot V^{L,\dagger} V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger})$ is a projector. It suffices to show that $V^{L,\dagger} V^L$ and $V^R \cdot V^{R,\dagger}$ commute. By the definition of V^L, $V^{L,\dagger} V^L = \mathbb{1}_{\mathsf{A}} \otimes \Pi_{\leq N-1,\mathsf{LR}}$. Since $V^R \cdot V^{R,\dagger}$ takes states in $\Pi_{\leq i+1,\mathsf{LR}}$ to $\Pi_{\leq i+1,\mathsf{LR}}$ (for $0 \leq i \leq N-1$), it commutes with $\mathbb{1}_{\mathsf{A}} \otimes \Pi_{\leq N-1,\mathsf{LR}}$. Using a symmetric argument, we can conclude that $(\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ is also a partial isometry.

To show V is a partial isometry, it suffices to show that $V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger})$ and $(\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ are orthogonal. This is true since V^L and V^R are partial isometries:

$$(\mathbb{1} - V^R \cdot V^{R,\dagger}) V^R = 0 \quad \text{and} \quad V^{L,\dagger} (\mathbb{1} - V^L \cdot V^{L,\dagger}) = 0.$$

□

Note that W is a restriction of V.

Lemma 5.13.

$$W = V \cdot \Pi^{\mathrm{Dom}(W)}, \tag{21}$$

$$W^\dagger = V^\dagger \cdot \Pi^{\mathrm{Im}(W)}. \tag{22}$$

Proof. To prove Eq. (21), it suffices to show that

$$W^L = V \cdot \Pi^{\mathrm{Dom}(W^L)}, \tag{23}$$

$$W^{R,\dagger} = V \cdot \Pi^{\mathrm{Im}(W^R)}. \tag{24}$$

By Eq. (14), Eq. (21) can be obtained by summing these two equations.

We now prove Eq. (23). By Eq. (18), we have

$$V \cdot \Pi^{\mathrm{Dom}(W^L)} = \left(V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger}) + (\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}\right) \cdot \Pi^{\mathrm{Dom}(W^L)}.$$

By Eq. (20), we have

$$V^{R,\dagger} \cdot \Pi^{\mathrm{Dom}(W^L)} = V^{R,\dagger} W^{L,\dagger} W^L = 0,$$

where the last equality follows from Eq. (20). Thus

$$V \cdot \Pi^{\mathrm{Dom}(W^L)} = V^L \cdot \Pi^{\mathrm{Dom}(W^L)} = W^L,$$

where the second equality follows from Eq. (19).

It remains to prove Eq. (24). By Eq. (18), we have

$$V \cdot \Pi^{\mathrm{Im}(W^R)} = \left(V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger}) + (\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}\right) \cdot \Pi^{\mathrm{Im}(W^R)}.$$

By the definition of V^R and W^R, we have that $\mathrm{Im}(W^R) \subseteq \mathrm{Im}(V^R)$. Thus

$$(\mathbb{1} - V^R \cdot V^{R,\dagger})\Pi^{\mathrm{Im}(W^R)} = \Pi^{\mathrm{Im}(W^R)} - \Pi^{\mathrm{Im}(V^R)}\Pi^{\mathrm{Im}(W^R)} = 0.$$

At last, by Eq. (19) and Eq. (20), we have

$$(\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger} \cdot \Pi^{\mathrm{Im}(W^R)} = (\mathbb{1} - V^L \cdot V^{L,\dagger}) W^{R,\dagger} = W^{R,\dagger}.$$

□

5.3.1 Two-sided unitary invariance

The modified path-recording oracle V also has an approximate two-sided unitary invariance property as in [MH24, Section 8.3]. Recall the notation in [MH24].

Definition 5.14. *For any two n-qubit unitary C and D, define*

$$Q[C, D] := (C \otimes D^T)_{\mathsf{L}}^{\otimes *} \otimes (\overline{C} \otimes D^\dagger)_{\mathsf{R}}^{\otimes *} \quad .$$

Formally, we have the following lemma.

Lemma 5.15. *For any two n-qubit unitary C and D, and any integer $0 \le t \le N-1$,*

$$\|D_{\mathsf{A}} \cdot V_{\le t} \cdot C_{\mathsf{A}} \cdot Q[C, D]_{\mathsf{LR}} - Q[C, D]_{\mathsf{LR}} \cdot V_{\le t}\|_\infty \le 32\sqrt{\frac{t(t+1)}{N}} \quad ,$$

$$\left\|C_{\mathsf{A}}^\dagger \cdot (V^\dagger)_{\le t} \cdot D_{\mathsf{A}}^\dagger \cdot Q[C, D]_{\mathsf{LR}} - Q[C, D]_{\mathsf{LR}} \cdot (V^\dagger)_{\le t}\right\|_\infty \le 32\sqrt{\frac{t(t+1)}{N}} \quad .$$

The proof of this lemma is similar to that of Claim 16 in [MH24, Section 8.3]. We provide the proof in the Appendix B.

5.4 Main proof

We are now prepared to prove Theorem 5.1, which demonstrate the strong security of our construction $\mathsf{HP}_{n,2T+1}$. We repeat the theorem here.

Theorem 5.1. *Let $\mathcal{A}$ be a t-query oracle adversary capable of performing both forward and inverse queries to oracle O, and let $\mathsf{HP}_{n,2T+1}$ be defined as in Definition 4.1 with $T = 30n$ and $d = 5n$. Then*

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{O\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^O\rangle\langle\mathcal{A}_t^O|_{\mathsf{AB}}\right], \mathop{\mathbb{E}}_{O\leftarrow\mu}\left[|\mathcal{A}_t^O\rangle\langle\mathcal{A}_t^O|_{\mathsf{AB}}\right]\right) \le \frac{2t(11t+20)}{N^{1/8}} \quad . \tag{25}$$

To prove Theorem 5.1 we first show that our construction is indistinguishable from the path-recording oracle V, as stated in the following lemma:

Lemma 5.16 ($\mathsf{HP}_{n,2T+1}$ is indistinguishable from V)**.** *Let $\mathcal{A}$ be a t-query oracle adversary capable of performing both forward and inverse queries. Let $\mathsf{HP}_{n,2T+1}$ be defined as in Definition 4.1 with $T = 30n$ and $d = 5n$, and V be defined as in Definition 5.11. Then*

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{O\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^O\rangle\langle\mathcal{A}_t^O|_{\mathsf{AB}}\right], \mathrm{Tr}_{\mathsf{LR}}\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}}\right)\right) \le \frac{t(11t+20)}{N^{1/8}} \quad . \tag{26}$$

Then, we show the Haar random unitary is indistinguishable from V as well:

Lemma 5.17 (V is indistinguishable from Haar random unitaries)**.** *Let $\mathcal{A}$ be a t-query oracle adversary capable of performing both forward and inverse queries. Then*

$$\mathrm{TD}\left(\mathop{\mathbb{E}}_{O\leftarrow\mu}\left[|\mathcal{A}_t^O\rangle\langle\mathcal{A}_t^O|_{\mathsf{AB}}\right], \mathrm{Tr}_{\mathsf{LR}}\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}}\right)\right) \le \frac{t(11t+20)}{N^{1/8}} \quad . \tag{27}$$

Finally, by applying the triangular inequality to Lemma 5.16 and Lemma 5.17, we conclude the proof of Theorem 5.1 in Subsection 5.4.3.

In the following sections, we provide the details of proving the main lemma Lemma 5.16. The proof is structured as follows: first, we demonstrate that V is indistinguishable from the twirled partial path-recording oracle W; then, we show that the twirled W is indistinguishable from the twirled purified HPO oracle (Definition 5.2) that is equivalent to $\mathsf{HP}_{n,2T+1}$ as stated in Fact 4.6. Lemma 5.17 follows from a similar argument.

5.4.1 V is indistinguishable from W

In this section, we mainly prove that even if the adversary can make queries from both directions, the path-recording oracle V is indistinguishable to $D \cdot W \cdot C$ for $C, D \leftarrow \mathcal{D}$, where $\mathcal{D}$ is one of the following two distributions:

Definition 5.18.

- *$\mathcal{D}_1$: sample two independent unitary operators C and D from Haar measure on $\mathrm{U}(N)$, and output C and D,*

- *$\mathcal{D}_2$: sample independent C' and D from $\mathsf{HP}_{n,T}$ with $T = 30n$ and $d = 5n$, and a random permutation matrix P. Output $C = P \cdot C'$ and D.*

We first need a twirling lemma. Let

$$\Pi_{\mathsf{LR}}^{\mathrm{DB}} := \sum_{L,R:L\cup R\in\mathfrak{R}^{\mathrm{DB}}} |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}} \quad , \quad \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} := \sum_{L,R\in\mathfrak{R}} |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}} \quad .$$

Lemma 5.19 (Twirling). *Let $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18. For integer $0 \le t \le N/4$, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi_{\le t,\mathsf{LR}}^{\mathrm{DB}} - \Pi_{\le t,\mathsf{LR}}^{\mathrm{Dom}(W)} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \le 16t \cdot \sqrt{\frac{2t}{N}} \quad ,$$

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}} \left[(D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi_{\le t,\mathsf{LR}}^{\mathrm{DB}} - \Pi_{\le t,\mathsf{LR}}^{\mathrm{Im}(W)} \right) \cdot (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \le 16t \cdot \sqrt{\frac{2t}{N}} \quad .$$

The proof of this twirling lemma is deferred to Appendix C.

Definition 5.20 (Controlled C, D and Q). *Define the following operators:*

$$\mathrm{cC} := \int_C C_{\mathsf{A}} \otimes |C\rangle\langle C|_{\mathsf{C}} \,, \quad \mathrm{cD} := \int_D D_{\mathsf{A}} \otimes |D\rangle\langle D|_{\mathsf{D}} \,, \quad \mathrm{cQ} := Q[C,D]_{\mathsf{LR}} \otimes |C\rangle\langle C|_{\mathsf{C}} \otimes |D\rangle\langle D|_{\mathsf{D}} \,,$$

where $Q[C,D] := (C \otimes D^T)_{\mathsf{L}}^{\otimes *} \otimes (\overline{C} \otimes D^\dagger)_{\mathsf{R}}^{\otimes *}$.

Definition 5.21 (Purification of Twirled-W). *Define the adversary state $|\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$ after the i-th query to twirled-W as follows:*

- *For $i = 0$,*

$$|\mathcal{A}_0^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} := |0^n 0^m\rangle_{\mathsf{AB}} \, |\{\}\rangle_{\mathsf{L}} \, |\{\}\rangle_{\mathsf{R}} \, |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \tag{28}$$

  where

$$|\mathsf{init}(\mathcal{D})\rangle := \int_{C,D} \sqrt{d\mu_{\mathcal{D}}(C) d\mu_{\mathcal{D}}(D)} \, |C\rangle_{\mathsf{C}} \, |D\rangle_{\mathsf{D}}$$

  is the initial purification on registers C, D set up for $C, D \leftarrow \mathcal{D}$; and $\mu_{\mathcal{D}}(\cdot)$ denote the probability measure of unitaries sampled from the distribution $\mathcal{D}$.

- *For $1 \le i \le t$,*

$$|\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} := \left((1-b_i) \cdot (\mathrm{cD} \cdot W \cdot \mathrm{cC}) + b_i \cdot (\mathrm{cD} \cdot W \cdot \mathrm{cC})^\dagger \right) \cdot A_i \cdot |\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle \tag{29}$$

  where $b_i \in \{0,1\}$ indicates that the adversary makes a forward/backward query in the i-th step.

Definition 5.22 (Purification of V). *Define the adversary state $|\mathcal{A}_i^V\rangle_{\mathsf{ABLR}}$ after the i-th query to oracle V as follows:*

- *For $i = 0$,*
$$|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} := |0^n 0^m\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{L}} |\{\}\rangle_{\mathsf{R}} \tag{30}$$
- *For $1 \le i \le t$,*
$$|\mathcal{A}_i^V\rangle_{\mathsf{ABLR}} := \left((1 - b_i) \cdot V + b_i \cdot V^\dagger\right) \cdot A_i \cdot |\mathcal{A}_{i-1}^V\rangle \tag{31}$$
where $b_i \in \{0, 1\}$ indicates that the adversary makes a forward/backward query in the i-th step.

Fact 5.23 (Norm of the purified states). *For any $t \ge 0$, $|\mathcal{A}_t^{W,\mathcal{D}}\rangle$ and $|\mathcal{A}_t^V\rangle$ both have a norm of at most 1, since W and V are partial isometries, meaning that applying $W, W^\dagger, V$ or $V^\dagger$ is equivalent to a projection followed by a unitary operation.*

Fact 5.24 (Spaces containing puried states). *For any $t \ge 0$, $|\mathcal{A}_t^{W,\mathcal{D}}\rangle$ lies in the image of $\Pi_{\le t}^{\mathrm{DB}}$, and $|\mathcal{A}_t^V\rangle$ lies in the image of $\Pi_{\le t}^{\Re^2}$, follwing their definitions.*

Now, we proceed to demonstrate the main claim in the proof of Lemma 5.27.

Claim 5.25. *For any integer $t \ge 0$, and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18*
$$\mathrm{Re}\left[\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^V\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}\right)\right] \ge 1 - \frac{38t^2}{N^{1/4}} \ . \tag{32}$$

Proof by induction. For the base case $t = 0$, following the Definition 5.20, 5.21 and 5.22, we have
$$\begin{aligned}
\mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}\right) &= \mathsf{cQ}_{\mathsf{LRCD}} \cdot (|0^n 0^m\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{L}} |\{\}\rangle_{\mathsf{R}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}) \\
&= |0^n 0^m\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{L}} |\{\}\rangle_{\mathsf{R}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \\
&= |\mathcal{A}_0^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}
\end{aligned}$$
Thus, the base case holds: $\mathrm{Re}\left[\langle\mathcal{A}_0^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}\right)\right] = 1$.

Assuming the claim holds for some $t \ge 0$, we now prove it for $t + 1$. Due to the argument is symmetric, we assume the $(t + 1)$-th query is a forward query, i.e. $b_{t+1} = 0$, without loss of generality. Thus,
$$\begin{aligned}
|\mathcal{A}_{t+1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} &= (\mathsf{cD} \cdot W \cdot \mathsf{cC}) \cdot A_{t+1} \cdot |\mathcal{A}_t^{W,\mathcal{D}}\rangle \\
\mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_{t+1}^V\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}\right) &= \mathsf{cQ} \cdot \left(V \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle |\mathsf{init}(\mathcal{D})\rangle\right)
\end{aligned}$$
derives
$$\begin{aligned}
&\mathrm{Re}\left[\langle\mathcal{A}_{t+1}^{W,\mathcal{D}}| \cdot \mathsf{cQ} \cdot \left(|\mathcal{A}_{t+1}^V\rangle |\mathsf{init}(\mathcal{D})\rangle\right)\right] \\
&= \mathrm{Re}\left[\langle\mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W^\dagger \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot \left(V \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle |\mathsf{init}(\mathcal{D})\rangle\right)\right] \\
&= \mathrm{Re}\left[\langle\mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot V_{\le t} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle |\mathsf{init}(\mathcal{D})\rangle\right],
\end{aligned} \tag{33}$$

because of Fact 5.24. Recall the notation $W_{\le t} = W \cdot \Pi_{\le t}$ and $V_{\le t} = V \cdot \Pi_{\le t}$. Then, via rewriting

$$\mathsf{cQ} \cdot V_{\le t} = \mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ} + \left(\mathsf{cQ} \cdot V_{\le t} - \mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ}\right)$$

we further rewrite (33) = (∗) + (∗∗) where

$$(*) = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right],$$

$$(**) = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot \mathsf{cD}^\dagger \cdot \left(\mathsf{cQ} \cdot V_{\le t} - \mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ}\right) \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right]$$

We first lower bound (∗∗):

$$\begin{aligned}
(**) &\ge -\left\|\left(\mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ} - \mathsf{cQ} \cdot V_{\le t}\right)\right\|_\infty \\
&\ge -\left\|\sum_{C,D} \left(D_A \cdot V_{\le t} \cdot C_A \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\le t}\right) \otimes |C,D\rangle\langle C,D|\right\|_\infty \\
&\ge -\max_{C,D} \|D_A \cdot V_{\le t} \cdot C_A \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\le t}\|_\infty \\
&\ge -32\sqrt{\frac{t(t+1)}{N}}
\end{aligned} \tag{34}$$

The first inequality follows from Fact 5.23, ensuring that the norm of $\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot \mathsf{cD}^\dagger$ and $A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle$ are at most 1. The last inequality follows from Lemma 5.15. To bound (∗), we first utilizes the properties of W and V to derive:

$$\begin{aligned}
W_{\le t}^\dagger \cdot V_{\le t} &= (W \cdot \Pi_{\le t})^\dagger \cdot V \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot W^\dagger \cdot V \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot \Pi^{\mathrm{Dom}(W)} \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot \left(\Pi^{\mathrm{DB}} - \left(\Pi^{\mathrm{DB}} - \Pi^{\mathrm{Dom}(W)}\right)\right) \cdot \Pi_{\le t} \\
&= \Pi_{\le t}^{\mathrm{DB}} - \left(\Pi_{\le t}^{\mathrm{DB}} - \Pi_{\le t}^{\mathrm{Dom}(W)}\right)
\end{aligned} \tag{35}$$

Then, we can rewrite (∗) = (△) − (△△) using (35) where:

$$(\triangle) = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \Pi_{\le t}^{\mathrm{DB}} \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right], \tag{36}$$

$$(\triangle\triangle) = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \left(\Pi_{\le t}^{\mathrm{DB}} - \Pi_{\le t}^{\mathrm{Dom}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right]. \tag{37}$$

Thus, to bound (∗) we need to separately bound (△) and (△△). First, in (△) we have:

$$\begin{aligned}
\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \Pi_{\le t}^{\mathrm{DB}} &= \langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot \Pi_{\le t}^{\mathrm{DB}} \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \\
&= \langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger
\end{aligned}$$

Thus, by the inductive hypothesis, we have

$$\begin{aligned}(\triangle) &= \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right] \\ &= \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot \mathsf{cQ} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right] \\ &\geq 1 - \frac{38t^2}{N^{1/4}} \ .\end{aligned} \tag{38}$$

Then we will uper bound $(\triangle\triangle)$:

$$\begin{aligned}(\triangle\triangle) &\leq \left|\langle \mathcal{A}_t^{W,\mathcal{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \left(\Pi_{\leq t}^{\mathrm{DB}} - \Pi_{\leq t}^{\mathrm{Dom}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right| \\ &\leq \max_{\substack{|u\rangle \in \mathcal{H}_{\mathsf{ABLRCD}} : \||u\rangle\|_2 \leq 1 \\ |v\rangle \in \mathcal{H}_{\mathsf{ABLR}} : \||v\rangle\|_2 \leq 1}} \left|\langle u| \cdot \left(\Pi_{\leq t}^{\mathrm{DB}} - \Pi_{\leq t}^{\mathrm{Dom}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot |v\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right| \\ &= \left(\max_{\substack{|v\rangle \in \mathcal{H}_{\mathsf{ABLR}} : \\ \||v\rangle\|_2 \leq 1}} \langle v| \, \langle \mathsf{init}(\mathcal{D})| \cdot \mathsf{cQ}^\dagger \cdot \mathsf{cC}^\dagger \cdot \left(\Pi_{\leq t}^{\mathrm{DB}} - \Pi_{\leq t}^{\mathrm{Dom}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot |v\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right)^{1/2} \\ &= \left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \left(\Pi_{\leq t}^{\mathrm{DB}} - \Pi_{\leq t}^{\mathrm{Dom}(W)}\right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty^{1/2} \\ &\leq \left(16t\sqrt{\frac{2t}{N}}\right)^{1/2} \leq \frac{6t^{3/4}}{N^{1/4}}\end{aligned}$$

where the last line follows from Lemma 5.19.

Now, putting everything together we show the claim for $t+1$ to conclude:

$$\begin{aligned}\mathrm{Re}\left[\langle \mathcal{A}_{t+1}^{W,\mathcal{D}}| \cdot \mathsf{cQ} \cdot \left(|\mathcal{A}_{t+1}^V\rangle \, |\mathsf{init}(\mathcal{D})\rangle\right)\right] &= (*) + (**) \\ &\geq (*) - 32\sqrt{\frac{t(t+1)}{N}} \\ &\geq (\triangle) - (\triangle\triangle) - 32\sqrt{\frac{t(t+1)}{N}} \\ &\geq 1 - \frac{38t^2}{N^{1/4}} - \frac{6t^{3/4}}{N^{1/4}} - 32\sqrt{\frac{t(t+1)}{N}} \\ &\leq 1 - \frac{1}{N^{1/4}}\left(38t^2 + 6t^{3/4} + 32\frac{\sqrt{t(t+1)}}{N^{1/4}}\right) \\ &\leq 1 - \frac{1}{N^{1/4}}\left(38t^2 + 6t + 32(t+1)\right) \\ &\geq 1 - \frac{38(t+1)^2}{N^{1/4}} \ .\end{aligned}$$

□

This claim also gives a bound on the norm of $|\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$:

Lemma 5.26. *For any $0 \le t < N$ and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18, we have*

$$\left\| |\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \right\|_2 \ge 1 - \frac{38t^2}{N^{1/4}} \ .$$

Proof. We have

$$\begin{aligned}
\left\| |\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \right\|_2^2 &= \langle \mathcal{A}_t^{W,\mathcal{D}} | \mathcal{A}_t^{W,\mathcal{D}} \rangle \\
&\ge \langle \mathcal{A}_t^{W,\mathcal{D}} | \mathcal{A}_t^{W,\mathcal{D}} \rangle \cdot \langle \mathcal{A}_t^{V} | \mathcal{A}_t^{V} \rangle \\
&= \langle \mathcal{A}_t^{W,\mathcal{D}} | \mathcal{A}_t^{W,\mathcal{D}} \rangle \cdot \left(\langle \mathcal{A}_t^{V}| \langle \mathsf{init}(\mathcal{D})| \right) \mathrm{cQ}^\dagger \cdot \mathrm{cQ} \cdot \left(|\mathcal{A}_t^{V}\rangle |\mathsf{init}(\mathcal{D})\rangle \right) \\
&\ge \left| \langle \mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \cdot \mathrm{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \right|^2 \\
&\ge \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \cdot \mathrm{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \right]^2 \\
&\ge \left(1 - \frac{38t^2}{N^{1/4}} \right)^2 \ ,
\end{aligned}$$

where the first inequality is from the fact that $|\mathcal{A}_t^V\rangle$ has norm at most 1, the second one is from Cauchy-Schwarz inequality, and the last one is from Claim 5.25. □

Now, we are ready to prove the indistinguishability between oracles V and twirled W via proving the following lemma:

Lemma 5.27. *For any $0 \le t < N$ and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18, we have*

$$\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \right), \mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \right) \right) \le \frac{9t}{N^{1/8}} \ . \tag{39}$$

Proof. Using the fact that $\| |u\rangle\langle u| - |v\rangle\langle v| \|_1 \le 2 \| |u\rangle - |v\rangle \|_2$, we have

$$\begin{aligned}
&\mathrm{TD}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}, \mathrm{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}} \right) \cdot \mathrm{cQ}_{\mathsf{LRCD}}^\dagger \right)^2 \\
\le &\left\| |\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLR}} - \mathrm{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathcal{D})_{\mathsf{CD}}\rangle \right) \right\|_2^2 \\
= &\langle \mathcal{A}_t^{W,\mathcal{D}} \mid \mathcal{A}_t^{W,\mathcal{D}} \rangle + \langle \mathcal{A}_t^{V} \mid \mathcal{A}_t^{V} \rangle - 2\mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \cdot \mathrm{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \right] \\
\le &2 - 2 \cdot \left(1 - \frac{38t^2}{N^{1/4}} \right) = \frac{76t^2}{N^{1/4}} \ .
\end{aligned}$$

Since unitary cQ only acts on registers L, R, C, D,

$$\begin{aligned}
&\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \right), \mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \right) \right) \\
= &\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \right), \right.
\end{aligned}$$

$$\mathrm{Tr}_{-\mathsf{AB}}\left(\mathsf{cQ}_{\mathsf{LRCD}}\cdot\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}}\otimes|\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}}\right)\cdot\mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right)\right)$$

$$\leq \mathrm{TD}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}, \mathsf{cQ}_{\mathsf{LRCD}}\cdot\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}}\otimes|\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}}\right)\cdot\mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right)$$

$$\leq \frac{9t}{N^{1/8}}\ .$$

□

5.4.2 W is indistinguishable from HPO

In this section, we mainly shows that after twirling, adversaries cannot differentiate from HPO oracle to W (Lemma 5.32). We first define the purification of twirled-HPO oracle and then connect it with twirled-W (Definition 5.21) via some projection.

Definition 5.28 (Purification of twirled-HPO)**.** *Define the adversary state* $|\mathcal{A}_i^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}$ *after the* i*-th query to twirled-*HPO *as follows:*

- *For* $i=0$*,*

$$|\mathcal{A}_0^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}} := |0^n0^m\rangle_{\mathsf{AB}}\,|+_f\rangle_{\mathsf{H}}\,|+_\sigma\rangle_{\mathsf{P}}\,|\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \tag{40}$$

  where $|+_f\rangle_{\mathsf{H}}$ *and* $|+_\sigma\rangle_{\mathsf{P}}$ *are the uniform superposition over all permutations and functions respectively, and*

$$|\mathsf{init}(\mathcal{D})\rangle := \int_{C,D}\sqrt{d\mu_{\mathcal{D}}(C)d\mu_{\mathcal{D}}(D)}\,|C\rangle_{\mathsf{C}}\,|D\rangle_{\mathsf{D}}$$

  is the initial purification on registers C, D *set up for* $C,D\leftarrow\mathcal{D}$*; and* $\mu_{\mathcal{D}}(\cdot)$ *denote the probability measure of unitaries sampled from the distribution* $\mathcal{D}$*.*

- *For* $1\leq i\leq t$*,*

$$|\mathcal{A}_i^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}} := \left((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{HPO}\cdot\mathsf{cC})+b_i\cdot(\mathsf{cD}\cdot\mathsf{HPO}\cdot\mathsf{cC})^\dagger\right)\cdot A_i\cdot|\mathcal{A}_{i-1}^{\mathsf{HPO},\mathcal{D}}\rangle \tag{41}$$

  where $b_i\in\{0,1\}$ *indicates that the adversary makes a forward/backward query in the* i*-th step.*

Definition 5.29. *Define the projectors*

$$\widetilde{\Pi}^{\mathrm{Dom}(W)} := \mathsf{Compress}^\dagger\cdot\Pi^{\mathrm{Dom}(W)}\cdot\mathsf{Compress}, \tag{42}$$

$$\widetilde{\Pi}^{\mathrm{Im}(W)} := \mathsf{Compress}^\dagger\cdot\Pi^{\mathrm{Im}(W)}\cdot\mathsf{Compress}. \tag{43}$$

Definition 5.30 (Purification of twirled-projected-HPO)**.** *Define the adversary state* $|\mathcal{A}_i^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}$ *after the* i*-th query to twirled-*HPO *with projection:*

- *For* $i=0$*,* $|\mathcal{A}_0^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle := |\mathcal{A}_0^{\mathsf{HPO},\mathcal{D}}\rangle$

- *For* $1 \le i \le t$,

$$|\mathcal{A}_i^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle := \Big((1-b_i)\cdot\Big(\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\Big) + b_i\cdot\Big(\mathsf{cD}\cdot\widetilde{\Pi}^{\mathrm{Im}(W)}\cdot\mathsf{HPO}\cdot\mathsf{cC}\Big)^{\dagger}\Big)\cdot A_i\cdot|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \tag{44}$$

  where $b_i \in \{0,1\}$ *indicates that the adversary makes a forward/backward query in the* i*-th step.*

Claim 5.31. *For all integer* $0 \le t \le N/2$,

$$\Big\| |\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}_{\mathsf{HP}}\cdot|\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 \le \frac{2t(t+1)}{N} \quad .$$

Proof by induction. First, we check the claim is true for the base case $t = 0$:

$$\begin{aligned}\mathsf{Compress}_{\mathsf{HP}}\cdot|\mathcal{A}_0^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle &= \mathsf{Compress}_{\mathsf{HP}}\cdot|\mathcal{A}_0^{\mathrm{HPO},\mathcal{D}}\rangle \\ &= \mathsf{Compress}_{\mathsf{HP}}\cdot\big(|0^n0^m\rangle_{\mathsf{AB}}\,|+_f\rangle_{\mathsf{H}}\,|+_\sigma\rangle_{\mathsf{P}}\,|\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}}\big) \\ &= |0^n0^m\rangle_{\mathsf{AB}}\,|\{\}\rangle_{\mathsf{H}}\,|\{\}\rangle_{\mathsf{P}}\,|\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} = |\mathcal{A}_t^{W,\mathcal{D}}\rangle\end{aligned}$$

Next, assuming the claim for case $(i-1)$, we will show the case i. W.l.o.g we assume $b_i = 0$, then

$$\begin{aligned}(\star) &:= \Big\| |\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}_{\mathsf{HP}}\cdot|\mathcal{A}_i^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 \\ &= \Big\| \mathsf{cD}\cdot W\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 .\end{aligned}$$

Note that $|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$ lies in the image of $\Pi_{\le i-1}$. Thus, $\Pi_{\le i-1}\cdot|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} = |\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$. Therefore, we have

$$\begin{aligned}&(\star)\\ =\ &\Big\| \mathsf{cD}\cdot W\cdot\mathsf{cC}\cdot A_i\cdot\Pi_{\le i-1}\cdot|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 \\ =\ &\Big\| \mathsf{cD}\cdot W_{\le i-1}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 \\ \overset{(*)}{\le}\ &\Big\| \mathsf{cD}\cdot\mathsf{Compress}\cdot\mathsf{HPO}\cdot\mathsf{Compress}^{\dagger}\cdot\Pi^{\mathrm{Dom}(W)}\cdot\Pi_{\le i-1}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \\ &\qquad -\mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 + \frac{2i-2}{N-i+1} \\ =\ &\Big\| \mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\cdot\mathsf{Compress}^{\dagger}\cdot|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \\ &\qquad -\mathsf{Compress}\cdot\mathsf{cD}\cdot\mathsf{HPO}\cdot\widetilde{\Pi}^{\mathrm{Dom}(W)}\cdot\mathsf{cC}\cdot A_i\,|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 + \frac{2i-2}{N-i+1} \\ \le\ &\Big\| |\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}\cdot|\mathcal{A}_{i-1}^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle \Big\|_2 + \frac{4i}{N} \\ \overset{(**)}{\le}\ &\frac{2i(i-1)}{N} + \frac{4i}{N} \quad = \frac{2i(i+1)}{N},\end{aligned}$$

where $(*)$ is by Lemma 5.10 and $(**)$ is by induction. □

Now, we are ready to prove the indistinguishability between oracles W and HPO:

Lemma 5.32. *For all integers $0 \le t \le N$, and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18*

$$\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}|_{\mathsf{ABLR}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right) \le \frac{11t(t+1)}{N^{1/8}} \ .$$

Proof. Recall the state $|\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}$ defined in Definition 5.30. By the triangle inequality, we have

$$\begin{aligned}
&\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}|_{\mathsf{ABLR}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right) \\
\le\ & \underbrace{\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}|_{\mathsf{ABLR}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}}\right)\right)}_{(\star)} \\
&+ \underbrace{\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right)}_{(*)} \ .
\end{aligned}$$

It suffices to show that

$$(\star) \le \frac{9t(t+1)}{N^{1/8}} \ , \quad \text{and} \quad (*) \le \frac{2t(t+1)}{N} \ .$$

We first bound term $(\star)$. Since HPO and Compress are isometries, we have $\left\||\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 = 1$ and $\left\||\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \le 1$. Using the fact that $\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \le 2\,\||u\rangle - |v\rangle\|_2$ for $\|u\|_2 \le 1$ and $\|v\|_2 \le 1$, we have

$$\begin{aligned}
(\star) &\le \mathrm{TD}\left(|\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}|_{\mathsf{ABLR}}, |\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}}\right) \\
&\le \left\||\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle_{\mathsf{ABLR}} - |\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \\
&\le t \cdot \sqrt{1 - \left\||\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2^2} \ , \qquad (45)
\end{aligned}$$

where the last inequality is from the gentle measurement lemma in Lemma 2.2. Notice that, since Compress is an isometry, we have

$$\begin{aligned}
\left\||\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 &= \left\|\mathsf{Compress} \cdot |\mathcal{A}_t^{\widetilde{\mathrm{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \\
&\ge \left\||\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}\right\|_2 - \frac{2t(t+1)}{N} \\
&\ge 1 - \frac{38t^2}{N^{1/4}} - \frac{2t(t+1)}{N} \\
&\ge 1 - \frac{40t(t+1)}{N^{1/4}} \ , \qquad (46)
\end{aligned}$$

where the first inequality is from the triangle inequality and Claim 5.31, and the second one is from Lemma 5.26. Combing Eq. (45). and. Eq. (46), we have

$$(\star) \le t \cdot \sqrt{1 - \left(1 - \frac{40t(t+1)}{N^{1/4}}\right)^2} \le t \cdot \sqrt{\frac{80t(t+1)}{N^{1/4}}} \le \frac{9t(t+1)}{N^{1/8}} \quad .$$

As for term $(*)$, note that Compress acts on environment registers. We have

$$\begin{aligned}
&(*)\\
&= \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(\mathsf{Compress} \cdot |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}} \cdot \mathsf{Compress}^\dagger\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right)\\
&\le \mathrm{TD}\left(\mathsf{Compress} \cdot |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}} \cdot \mathsf{Compress}^\dagger, |\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\\
&\le \left\|\mathsf{Compress} \cdot |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}} - |\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}\right\|_2\\
&\le \frac{2t(t+1)}{N},
\end{aligned}$$

where the second inequality follows from the fact that $\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \le 2\||u\rangle - |v\rangle\|_2$ for $\|u\|_2 \le 1$ and $\|v\|_2 \le 1$, and the last one is from Claim 5.31. □

5.4.3 The Strong Security of HPO

Now, we complete the main proof of Theorem 5.1 by mainly establishing Lemma 5.16 and Lemma 5.17 that both our construction and Haar distribution are indistinguishable from V.

Proof of Lemma 5.16. Consider $\mathcal{D} = \mathcal{D}_2$ defined in Definition 5.18. First, due to the perfect indistinguishability between the standard oracle and its purified version (Fact 5.3),

$$\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABHPCD}}\right) = \mathop{\mathbb{E}}_{\substack{H_f P_\sigma\\ C,D\leftarrow\mathcal{D}}}\left[|\mathcal{A}_t^{DH_fP_\sigma C}\rangle\langle\mathcal{A}_t^{DH_fP_\sigma C}|_{\mathsf{AB}}\right] = \mathop{\mathbb{E}}_{O\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^{O}\rangle\langle\mathcal{A}_t^{O}|_{\mathsf{AB}}\right] \quad .$$

And, from Lemma 5.27, we get

$$\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right) \le \frac{9t}{N^{1/8}} \quad .$$

Then, according to Lemma 5.32, we have

$$\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABLR}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right) \le \frac{11t(t+1)}{N^{1/8}} \quad .$$

Thus, via triangle inequality, we show:

$$\begin{aligned}
&\mathrm{TD}\left(\mathop{\mathbb{E}}_{O\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^{O}\rangle\langle\mathcal{A}_t^{O}|_{\mathsf{AB}}\right], \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right)\\
&= \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABHPCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&\leq \mathrm{TD}\Big(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\Big) \\
&\quad + \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathrm{HPO},\mathcal{D}}|_{\mathsf{ABLR}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right) \\
&\leq \frac{11t^2+20t}{N^{1/8}} \quad .
\end{aligned}
$$

□

The argument above also proves Lemma 5.17 by considering $\mathcal{D} = \mathcal{D}_1$ as defined in Definition 5.18. Therefore, combining Lemma 5.16 and Lemma 5.17, we ultimately derive Theorem 5.1.

References

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. In *Advances in Cryptology – EUROCRYPT 2024*, pages 226–254, Cham, 2024. Springer Nature Switzerland. 2

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography*, pages 237–265, Cham, 2022. Springer Nature Switzerland. 2

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2022*, pages 208–236. Springer, 2022. 1

[BFV20] Adam Bouland, Bill Fefferman, and Umesh Vazirani. Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality. In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, volume 151 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 63:1–63:2. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. 1

[BHH16] Fernando G.S.L. Brandão, Aram W. Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346:397–434, 2016. 2

[BM25] Zvika Brakerski and Nir Magrafta. Real-valued somewhat-pseudorandom unitaries. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography*, pages 36–59, Cham, 2025. Springer Nature Switzerland. 1

[BS19] Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*, pages 229–250, Cham, 2019. Springer International Publishing. 1

[BS20] Zvika Brakerski and Omri Shmueli. Scalable pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2020*, pages 417–440. Springer, 2020. 2

[GTB23] Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states. 2023. https://arxiv.org/abs/2312.09206. 1

[Har13] Aram W. Harrow. The church of the symmetric subspace, 2013. https://arxiv.org/abs/1308.6595. 10

[HBC+22] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, and Jarrod R. McClean. Quantum advantage in learning from experiments. *Science*, 376(6598):1182–1186, 2022. 1

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology – CRYPTO 2018*, pages 126–152. Springer, 2018. 1

[JMW24] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Pseudorandom and pseudoentangled states from subset states. 2024. https://arxiv.org/abs/2312.15285. 1

[JPS+22] Vishesh Jain, Natesh S. Pillai, Ashwin Sah, Mehtaab Sawhney, and Aaron Smith. Fast and memory-optimal dimension reduction using Kac's walk. *The Annals of Applied Probability*, 32(5):4038 – 4064, 2022. 2

[Kac56] Mark Kac. Foundations of kinetic theory. In *Third Berkeley symposium on mathematical statistics and probability*, volume 3, pages 171–197, 1956. 2

[LQS+24] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography*, pages 3–35, Cham, 2024. Springer Nature Switzerland. 1, 2, 3, 4, 11, 12, 57

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries, 2024. https://arxiv.org/abs/2410.10116. 1, 2, 3, 5, 6, 7, 13, 23, 27, 45, 46, 52, 55

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 485–492, 2024. 1, 2, 3

[PS17] Natesh S Pillai and Aaron Smith. Kac's walk on n-sphere mixes in $n \log n$ steps. *The Annals of Applied Probability*, 27(1):631–650, 2017. 2

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth, 2024. https://arxiv.org/abs/2407.07754. 3

[YE25] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems. *Journal of High Energy Physics*, 2025(3):1–65, 2025. 1

[Zha16] Mark Zhandry. A note on quantum-secure PRPs. Cryptology ePrint Archive, Paper 2016/1076, 2016. 7

[Zha21] Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), 2021. 7

A Proofs of Lemma 5.5 and Lemma 5.6

A.1 Proof of Lemma 5.5

Lemma 5.5. $\left\{|\phi_{L,R}\rangle\right\}_{L,R:L\cup R\in\mathfrak{R}^{\mathrm{DB}}}$ *forms a set of orthonormal vectors.*

Proof. Let $L=\{(x_1,y_1),\ldots,(x_l,y_l)\}\in\mathfrak{R}_l$, $R=\left\{(x'_1,y'_1),\ldots,(x'_r,y'_r)\right\}\in\mathfrak{R}_r$, $S=\left\{(x^*_1,y^*_1),\ldots,(x^*_s,y^*_s)\right\}\in\mathfrak{R}_l$, and $T=\left\{(x^\triangle_1,y^\triangle_1),\ldots,(x^\triangle_t,y^\triangle_t)\right\}\in\mathfrak{R}_t$ such that $L\cup R\in\mathfrak{R}^{\mathrm{DB}}$ and $S\cup T\in\mathfrak{R}^{\mathrm{DB}}$. We need to prove:

- $\langle\phi_{L,R}|\phi_{S,T}\rangle=1$, if $L=S$ and $R=T$;
- $\langle\phi_{L,R}|\phi_{S,T}\rangle=0$, otherwise.

Here,

$$\begin{aligned}&\langle\phi_{L,R}|\phi_{S,T}\rangle\\=&\frac{1}{2^{3d(n-1)}(N-l-r)!}\sum_{f,\sigma}\sum_{\substack{b,b^*\in\{0,1\}^l\\ b',b^\triangle\in\{0,1\}^r}}\prod_{i=1}^{l}\langle y_i^{\oplus b_i}|\,H_f^\dagger\,|y_i\rangle\,\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\langle y'_i|\,H_f\,|y'^{\oplus b'_i}_i\rangle\,\delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)}\\&\qquad\cdot\prod_{i=1}^{l}\langle y^*_i|\,H_f\,|y^{*\oplus b^*_i}_i\rangle\,\delta_{y^{*\oplus b^*_i}_i=\sigma(x^*_i)}\cdot\prod_{i=1}^{r}\langle y^{\triangle\oplus b^\triangle_i}_i|\,H_f^\dagger\,|y^\triangle_i\rangle\,\delta_{y^{\triangle\oplus b^\triangle_i}_i=\sigma(x^\triangle_i)}\end{aligned}\tag{47}$$

Case 1: $L=S=\{(x_1,y_1),\ldots,(x_l,y_l)\}$ **and** $R=T=\left\{(x'_1,y'_1),\ldots,(x'_r,y'_r)\right\}$**.** Note that

$$\begin{aligned}&\langle\phi_{L,R}|\phi_{S,T}\rangle\\=&\frac{1}{2^{3d(n-1)}(N-l-r)!}\sum_{f,\sigma}\sum_{\substack{b,b^*\in\{0,1\}^l\\ b',b^\triangle\in\{0,1\}^r}}\prod_{i=1}^{l}\langle y_i^{\oplus b_i}|\,H_f^\dagger\,|y_i\rangle\,\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\langle y'_i|\,H_f\,|y'^{\oplus b'_i}_i\rangle\,\delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)}\\&\qquad\cdot\prod_{i=1}^{l}\langle y_i|\,H_f\,|y_i^{\oplus b^*_i}\rangle\,\delta_{y_i^{\oplus b^*_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\langle y'^{\oplus b^\triangle_i}_i|\,H_f^\dagger\,|y'_i\rangle\,\delta_{y'^{\oplus b^\triangle_i}_i=\sigma(x'_i)}\end{aligned}$$

If $b_i\neq b^*_i$, then $\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\delta_{y_i^{\oplus b^*_i}=\sigma(x_i)}=0$. Similarly, if $b'_i\neq b^\triangle_i$, then $\delta_{y_i^{\oplus b'_i}=\sigma(x_i)}\cdot\delta_{y_i^{\oplus b^\triangle_i}=\sigma(x_i)}=0$. Therefore, the term in the summation is zero whenever $b\neq b^*$ or $b'\neq b^\triangle$. Thus,

$$\begin{aligned}&\langle\phi_{L,R}|\phi_{S,T}\rangle\\=&\frac{1}{2^{3d(n-1)}(N-l-r)!}\sum_{f,\sigma}\sum_{\substack{b\in\{0,1\}^l\\ b'\in\{0,1\}^r}}\prod_{i=1}^{l}\langle y_i^{\oplus b_i}|\,H_f^\dagger\,|y_i\rangle\,\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\langle y'_i|\,H_f\,|y'^{\oplus b'_i}_i\rangle\,\delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)}\\&\qquad\cdot\prod_{i=1}^{l}\langle y_i|\,H_f\,|y_i^{\oplus b_i}\rangle\,\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\langle y'^{\oplus b_i}_i|\,H_f^\dagger\,|y'_i\rangle\,\delta_{y'^{\oplus b_i}_i=\sigma(x'_i)}\end{aligned}$$

$$= \frac{1}{2^{3d(n-1)}(N-l-r)!} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i^{\oplus b_i}| H_f^\dagger |y_i\rangle \langle y_i| H_f |y_i^{\oplus b_i}\rangle \prod_{i=1}^{r} \langle y'_i| H_f |y'^{\oplus b'_i}_i\rangle \langle y'^{\oplus b_i}_i| H_f^\dagger |y'_i\rangle$$
$$\cdot \prod_{i=1}^{l} \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \cdot \prod_{i=1}^{r} \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)}$$
$$= \mathop{\mathbb{E}}_{f}\Bigg[\frac{1}{(N-l-r)!} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i^{\oplus b_i}| H_f^\dagger |y_i\rangle \langle y_i| H_f |y_i^{\oplus b_i}\rangle \prod_{i=1}^{r} \langle y'_i| H_f |y'^{\oplus b'_i}_i\rangle \langle y'^{\oplus b_i}_i| H_f^\dagger |y'_i\rangle$$
$$\cdot \sum_{\sigma} \prod_{i=1}^{l} \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \cdot \prod_{i=1}^{r} \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)} \Bigg]$$

For fixed b, b', $y_i^{\oplus b_i}$ and $y'^{\oplus b_i}_i$ are distinct since y_i and y'_i are from different blocks. Moreover, x_i and x'_i are distinct. Thus,

$$\sum_{\sigma} \prod_{i=1}^{l} \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \cdot \prod_{i=1}^{r} \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)} = (N-l-r)! \ .$$

Then, we have

$$\begin{aligned}
&\langle \phi_{L,R}|\phi_{S,T}\rangle \\
&= \mathop{\mathbb{E}}_{f}\Bigg[\sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i^{\oplus b_i}| H_f^\dagger |y_i\rangle \langle y_i| H_f |y_i^{\oplus b_i}\rangle \prod_{i=1}^{r} \langle y'_i| H_f |y'^{\oplus b'_i}_i\rangle \langle y'^{\oplus b_i}_i| H_f^\dagger |y'_i\rangle \Bigg] \\
&= \prod_{i=1}^{l} \mathop{\mathbb{E}}_{f}\Bigg[\sum_{b_i\in\{0,1\}} \langle y_i^{\oplus b_i}| H_f^\dagger |y_i\rangle \langle y_i| H_f |y_i^{\oplus b_i}\rangle \Bigg] \cdot \prod_{i=1}^{r} \mathop{\mathbb{E}}_{f}\Bigg[\sum_{b'_i\in\{0,1\}} \langle y'_i| H_f |y'^{\oplus b'_i}_i\rangle \langle y'^{\oplus b_i}_i| H_f^\dagger |y'_i\rangle \Bigg]
\end{aligned}$$

Note that for $y \in \{0,1\}^n$,

$$\mathop{\mathbb{E}}_{f}\Big[\langle y| H_f |y\rangle \langle y| H_f^\dagger |y\rangle + \langle y| H_f |\bar{y}\rangle \langle \bar{y}| H_f^\dagger |y\rangle \Big] = 1 \ .$$

Therefore, we have $\langle \phi_{L,R}|\phi_{S,T}\rangle = 1$.

Case 2: $L \neq S$ or $R \neq T$.

- **Case 2.1:** $\mathrm{BIm}(L \cup R) \neq \mathrm{BIm}(S \cup T)$. Without loss of generality, we assume that there exists a y such that $y \in \{y_1, \ldots, y_l, y'_1, \ldots, y'_r\}$ and $y \notin \mathrm{BIm}(S \cup T)$. It is easy to check $\langle \phi_{L,R}|\phi_{S,T}\rangle = 0$, since

$$\mathop{\mathbb{E}}_{f}\Big[\langle y| H_f^\dagger |y\rangle \Big] = \mathop{\mathbb{E}}_{f}\Big[\langle \bar{y}| H_f^\dagger |y\rangle \Big] = \mathop{\mathbb{E}}_{f}\Big[\langle y| H_f |y\rangle \Big] = \mathop{\mathbb{E}}_{f}\Big[\langle y| H_f |\bar{y}\rangle \Big] = 0 \ .$$

- **Case 2.1:** $\mathrm{BIm}(L \cup R) = \mathrm{BIm}(S \cup T)$.

- **Case 2.1.1:** $\mathrm{BIm}(L) \neq \mathrm{BIm}(S)$. Without loss of generality, we assume that y_1 and $\overline{y_1}$ are not in S. This means $y_1 \in \{y_1^\triangle, \ldots, y_t^\triangle\}$ or $\overline{y_1} \in \{y_1^\triangle, \ldots, y_t^\triangle\}$.
  - Suppose that $y_1 \in \{y_1^\triangle, \ldots, y_t^\triangle\}$. Without loss of generality, we can assume $y_1 = y_1^\triangle$. We have two cases:
    - $x_1 = x_1^\triangle$. In this case, the term in the summation in Eq. (47) is zero when $b_1 \neq b_1^\triangle$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle y_1^\triangle| H_f^\dagger |y_1^\triangle\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle \overline{y_1^\triangle}| H_f^\dagger |y_1^\triangle\rangle\right] = 0 \ .$$
    - $x_1 \neq x_1^\triangle$. In this case, the term in the summation in Eq. (47) is zero when $b_1 = b_1^\triangle$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle \overline{y_1^\triangle}| H_f^\dagger |y_1^\triangle\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle y_1^\triangle| H_f^\dagger |y_1^\triangle\rangle\right] = 0 \ .$$
  - Suppose that $\overline{y_1} \in \{y_1^\triangle, \ldots, y_t^\triangle\}$. Without loss of generality, we can assume $\overline{y_1} = y_1^\triangle$. We have two cases:
    - $x_1 = x_1^\triangle$. In this case, the term in the summation in Eq. (47) is zero when $b_1 = b_1^\triangle$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle \overline{y_1^\triangle}| H_f^\dagger |y_1^\triangle\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle y_1^\triangle| H_f^\dagger |y_1^\triangle\rangle\right] = 0 \ .$$
    - $x_1 \neq x_1^\triangle$. In this case, the term in the summation in Eq. (47) is zero when $b_1 \neq b_1^\triangle$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle y_1^\triangle| H_f^\dagger |y_1^\triangle\rangle + \langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle \overline{y_1^\triangle}| H_f^\dagger |y_1^\triangle\rangle\right] = 0 \ .$$
- **Case 2.1.2:** $\mathrm{BIm}(L) = \mathrm{BIm}(S)$. This means $\mathrm{BIm}(R) = \mathrm{BIm}(T)$ as well.
  - **Case 2.1.2.1:** $\{y_1, \ldots, y_l\} \neq \{y_1^*, \ldots, y_s^*\}$. Without loss of generality, we can assume $y_1 = \overline{y_1^*}$. We have two cases:
    - $x_1 = x_1^*$. In this case, the term in the summation in Eq. (47) is zero when $b_1 = b_1^*$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |\overline{y_1^*}\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |y_1^*\rangle\right] = 0 \ .$$
    - $x_1 \neq x_1^*$. In this case, the term in the summation in Eq. (47) is zero when $b_1 \neq b_1^*$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since
$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |y_1^*\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |\overline{y_1^*}\rangle\right] = 0 \ .$$
  - **Case 2.1.2.2:** $\{y_1', \ldots, y_r'\} \neq \{y_1^\triangle, \ldots, y_t^\triangle\}$. Similar to Case 2.1.2.1, we have $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$.
  - **Case 2.1.2.2:** $\{y_1, \ldots, y_l\} = \{y_1^*, \ldots, y_s^*\}$ and $\{y_1', \ldots, y_r'\} = \{y_1^\triangle, \ldots, y_t^\triangle\}$.

- Suppose $L \neq S$. Then there exist $(x, y) \in L$ and $(x^*, y) \in S$ such that $x \neq x^*$. Without loss of generality, we can assume $y_1 = y_1^*$ and $x_1 \neq x_1^*$. In this case, the term in the summation in Eq. (47) is zero when $b_1 = b_1^*$. It is not hard to check $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$, since

$$\mathop{\mathbb{E}}_{f}\left[\langle y_1| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |\overline{y_1^*}\rangle\right] = \mathop{\mathbb{E}}_{f}\left[\langle \overline{y_1}| H_f^\dagger |y_1\rangle \langle y_1^*| H_f |y_1^*\rangle\right] = 0 \ .$$

- Suppose $R \neq T$. Similarly, we have $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$.

□

A.2 Proof of Lemma 5.6

Lemma 5.6. *For two integers l and r such that $0 \leq l+r \leq N$, and two relations $L = \{(x_1, y_1), \ldots, (x_l, y_l)\} \in \mathfrak{R}_l$ and $R = \{(x'_1, y'_1), \ldots, (x'_r, y'_r)\} \in \mathfrak{R}_r$, we have for $x \in \{0,1\}^n$*

$$\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}} = \frac{1}{\sqrt{N-l-r}} \sum_{y \in \{0,1\}^n} |y\rangle_{\mathsf{A}} \otimes |\phi_{L \cup \{x,y\},R}\rangle_{\mathsf{HP}} \ .$$

Similarly, we have for $y \in \{0,1\}^n$

$$\mathsf{HPO}^\dagger_{\mathsf{AHP}} |y\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}} = \frac{1}{\sqrt{N-l-r}} \sum_{x \in \{0,1\}^n} |x\rangle_{\mathsf{A}} \otimes |\phi_{L,R \cup \{x,y\}}\rangle_{\mathsf{HP}} \ .$$

Proof. In the proof of Lemma 4.10, we know

$$\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} = H_{f\,\mathsf{A}} |\sigma(x)\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} = \sum_{y \in \{0,1\}^n, b \in \{0,1\}} \langle y| H_f |y^{\oplus b}\rangle \, \delta_{y^{\oplus b} = \sigma(x)} |y\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \ .$$

Similarly, for $\mathsf{HPO}^\dagger$ we have

$$\mathsf{HPO}^\dagger_{\mathsf{AHP}} |y\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} = \sum_{x \in \{0,1\}^n, b \in \{0,1\}} \langle y^{\oplus b}| H_f^\dagger |y\rangle \, \delta_{y^{\oplus b} = \sigma(x)} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \ .$$

Then, we have

$$\begin{aligned}
&\mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}} \\
=&\frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b \in \{0,1\}^l \\ b' \in \{0,1\}^r}} \prod_{i=1}^{l} \langle y_i| H_f |y_i^{\oplus b_i}\rangle \, \delta_{y_i^{\oplus b_i} = \sigma(x_i)} \prod_{i=1}^{r} \langle y'^{\oplus b'_i}_i| H_f^\dagger |y'_i\rangle \, \delta_{y'^{\oplus b'_i}_i = \sigma(x'_i)} \\
&\qquad \cdot \mathsf{HPO}_{\mathsf{AHP}} |x\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}} \\
=&\frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b \in \{0,1\}^l \\ b' \in \{0,1\}^r}} \prod_{i=1}^{l} \langle y_i| H_f |y_i^{\oplus b_i}\rangle \, \delta_{y_i^{\oplus b_i} = \sigma(x_i)} \prod_{i=1}^{r} \langle y'^{\oplus b'_i}_i| H_f^\dagger |y'_i\rangle \, \delta_{y'^{\oplus b'_i}_i = \sigma(x'_i)}
\end{aligned}$$

$$\cdot \sum_{y\in\{0,1\}^n, b\in\{0,1\}} \langle y|\, H_f\, |y^{\oplus b}\rangle\, \delta_{y^{\oplus b}=\sigma(x)}\, |y\rangle_{\mathsf{A}}\, |f\rangle_{\mathsf{H}}\, |\sigma\rangle_{\mathsf{P}}$$

$$= \frac{1}{\sqrt{N-l-r}} \sum_{y\in\{0,1\}^n} |y\rangle_{\mathsf{A}} \otimes |\phi_{L\cup\{x,y\},R}\rangle_{\mathsf{HP}} \quad .$$

Similarly, we have

$$\begin{aligned}
&\mathsf{HPO}^{\dagger}_{\mathsf{AHP}}\, |x\rangle_{\mathsf{A}}\, |\phi_{L,R}\rangle_{\mathsf{HP}} \\
=&\frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i|\, H_f\, |y_i^{\oplus b_i}\rangle\, \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \prod_{i=1}^{r} \langle y'^{\oplus b'_i}_i|\, H_f^{\dagger}\, |y'_i\rangle\, \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)} \\
&\qquad \cdot \mathsf{HPO}^{\dagger}_{\mathsf{AHP}}\, |x\rangle_{\mathsf{A}}\, |f\rangle_{\mathsf{H}}\, |\sigma\rangle_{\mathsf{P}} \\
=&\frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i|\, H_f\, |y_i^{\oplus b_i}\rangle\, \delta_{y_i^{\oplus b_i}=\sigma(x_i)} \prod_{i=1}^{r} \langle y'^{\oplus b'_i}_i|\, H_f^{\dagger}\, |y'_i\rangle\, \delta_{y'^{\oplus b'_i}_i=\sigma(x'_i)} \\
&\qquad \cdot \sum_{x\in\{0,1\}^n, b\in\{0,1\}} \langle y^{\oplus b}|\, H_f^{\dagger}\, |y\rangle\, \delta_{y^{\oplus b}=\sigma(x)}\, |x\rangle_{\mathsf{A}}\, |f\rangle_{\mathsf{H}}\, |\sigma\rangle_{\mathsf{P}} \\
=&\frac{1}{\sqrt{N-l-r}} \sum_{x\in\{0,1\}^n} |x\rangle_{\mathsf{A}} \otimes |\phi_{L,R\cup\{x,y\}}\rangle_{\mathsf{HP}} \quad .
\end{aligned}$$

□

B Approximate Two-Side Unitary Invariance

We will show that the path-recording oracle V defined in Definition 5.11 satisfies an approximate unitary invariance property in this section. Formally, we have

Lemma 5.15. *For any two n-qubit unitary C and D, and any integer $0 \le t \le N-1$,*

$$\|D_{\mathsf{A}} \cdot V_{\le t} \cdot C_{\mathsf{A}} \cdot Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\le t}\|_{\infty} \le 32\sqrt{\frac{t(t+1)}{N}} \quad ,$$

$$\left\|C^{\dagger}_{\mathsf{A}} \cdot (V^{\dagger})_{\le t} \cdot D^{\dagger}_{\mathsf{A}} \cdot Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{\dagger})_{\le t}\right\|_{\infty} \le 32\sqrt{\frac{t(t+1)}{N}} \quad .$$

This lemma is proved by showing the closeness between V^L and E^L as well as V^R and E^R where E^L and E^R are operators introduced in [MH24, Section 10.1] that have exact two-side unitary invariance property. We first give the definition of E^L and E^R.

Definition B.1. *E^L and E^R are linear maps on register* A, L *and* R *such that*

$$E^L := \frac{1}{\sqrt{N}} \sum_{x,y\in\{0,1\}^n} |y\rangle\langle x|_{\mathsf{A}} \otimes \sum_{L\in\mathfrak{R}} \sqrt{\mathrm{num}(L,(x,y))+1} \cdot |L\cup\{(x,y)\}\rangle\langle L|_{\mathsf{L}} \otimes \sum_{R\in\mathfrak{R}} |R\rangle\langle R|_{\mathsf{R}} \quad ,$$

$$E^R := \frac{1}{\sqrt{N}} \sum_{x,y\in\{0,1\}^n} |y\rangle\langle x|_{\mathsf{A}} \otimes \sum_{L\in\mathfrak{R}} |L\rangle\langle L|_{\mathsf{L}} \otimes \sum_{R\in\mathfrak{R}} \sqrt{\mathrm{num}(R,(x,y))+1}\cdot |R\cup\{(x,y)\}\rangle\langle R|_{\mathsf{R}} \quad .$$

Here, $\mathrm{num}(L,(x,y))$ *is the number of times that* (x,y) *appears in* L*.*

E^L and E^R satisfy the exact unitary invariance:

Lemma B.2 (Claim 20 in [MH24])**.** *For any two n-qubit unitary* C *and* D*,*

$$D_{\mathsf{A}}\cdot E^L\cdot C_{\mathsf{A}} = Q[C,D]_{\mathsf{LR}}\cdot E^L\cdot Q[C,D]^\dagger_{\mathsf{LR}} \quad ,$$
$$D_{\mathsf{A}}\cdot E^R\cdot C_{\mathsf{A}} = Q[C,D]_{\mathsf{LR}}\cdot E^R\cdot Q[C,D]^\dagger_{\mathsf{LR}} \quad .$$

The approximate unitary invariance of V arises from the property that V^L and V^R are very close to E^L and E^R in operator norm respectively. That is,

Lemma B.3. *For any integer* $0\le t\le N-1$*,*

$$\left\|V^L_{\le t}-E^L_{\le t}\right\|_\infty \le \sqrt{\frac{4t(t+1)}{N}} \quad ,$$
$$\left\|V^R_{\le t}-E^R_{\le t}\right\|_\infty \le \sqrt{\frac{4t(t+1)}{N}} \quad .$$

Proof. We demonstrate that V^L and E^L are close in operator norm, and a similar argument shows that the proximity between V^R and E^R holds as well. It is sufficient to show that for any state

$$|\psi\rangle = \sum_{\substack{x\in\{0,1\}^n\\ L,R\in\mathfrak{R}\text{ s.t. }|L\cup R|\le t}} \alpha_{x,L,R}\,|x\rangle_{\mathsf{A}}\,|L\rangle_{\mathsf{L}}\,|R\rangle_{\mathsf{R}} \quad ,$$

we have

$$\left\|V^L_{\le t}|\psi\rangle - E^L_{\le t}|\psi\rangle\right\|_2 \le \sqrt{\frac{4t(t+1)}{N}} \quad .$$

Note that

$$\begin{aligned}
&V^L_{\le t}|\psi\rangle - E^L_{\le t}|\psi\rangle \\
&= \sum_{\substack{x\in\{0,1\}^n\\ L,R\in\mathfrak{R}\text{ s.t. }|L\cup R|\le t}} \alpha_{x,L,R} \sum_{y\in\{0,1\}^n} \left(\frac{\delta_{y\notin \mathrm{BIm}(L\cup R)}}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{\sqrt{\mathrm{num}(L,(x,y))+1}}{\sqrt{N}}\right)|y\rangle\,|L\cup\{(x,y)\}\rangle\,|R\rangle \\
&= \underbrace{\sum_{\substack{x\in\{0,1\}^n\\ L,R\in\mathfrak{R}\text{ s.t. }|L\cup R|\le t}} \alpha_{x,L,R} \sum_{\substack{y\in\{0,1\}^n\\ y\notin\mathrm{BIm}(L\cup R)}} \left(\frac{1}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{1}{\sqrt{N}}\right)|y\rangle\,|L\cup\{(x,y)\}\rangle\,|R\rangle}_{|u\rangle} \\
&\quad + \underbrace{\sum_{\substack{x\in\{0,1\}^n\\ L,R\in\mathfrak{R}\text{ s.t. }|L\cup R|\le t}} \alpha_{x,L,R} \sum_{\substack{y\in\{0,1\}^n\\ y\in\mathrm{BIm}(L\cup R)}} \left(-\frac{\sqrt{\mathrm{num}(L,(x,y))+1}}{\sqrt{N}}\right)|y\rangle\,|L\cup\{(x,y)\}\rangle\,|R\rangle}_{|v\rangle} \quad .
\end{aligned}$$

Since $|u\rangle$ and $|v\rangle$ are orthogonal, we have

$$\left\|V_{\leq t}^{L}|\psi\rangle - E_{\leq t}^{L}|\psi\rangle\right\|_2^2 = \langle u|u\rangle + \langle v|v\rangle \quad .$$

Therefore, it is left to show $\langle u|u\rangle \leq \frac{2t(t+1)}{N}$ and $\langle v|v\rangle \leq \frac{2t(t+1)}{N}$.

Notice that

$$|u\rangle = \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \alpha_{x,L,R} \left(\frac{1}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{1}{\sqrt{N}} \right) \right) |y\rangle\,|L'\rangle\,|R\rangle \quad .$$

So we have

$$\begin{aligned}
\langle u|u\rangle &= \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left| \sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \alpha_{x,L,R} \left(\frac{1}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{1}{\sqrt{N}} \right) \right|^2 \\
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left(\frac{1}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{1}{\sqrt{N}} \right)^2 \right) \\
&= \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left(\frac{\sqrt{N}-\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}}{\sqrt{N(N-|\mathrm{BIm}\,(L\cup R)|)}} \right)^2 \right) \\
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \frac{|\mathrm{BIm}\,(L\cup R)|}{N(N-|\mathrm{BIm}\,(L\cup R)|)} \right) \\
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \cdot \left(\frac{(t+1)(|\mathrm{BIm}\,(L'\cup R)|-2)}{N(N-|\mathrm{BIm}\,(L'\cup R)|+2)} \right)
\end{aligned}$$

$$
\begin{aligned}
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \cdot \frac{(t+1)\left|\mathrm{BIm}\left(L\cup R\right)\right|}{N(N-\left|\mathrm{BIm}\left(L\cup R\right)\right|)} \right) \\
&\leq \sum_{\substack{x\in\{0,1\}^n \\ L,R\in\mathfrak{R} \text{ s.t. } |L\cup R|\leq t}} \left|\alpha_{x,L,R}\right|^2 \cdot \left(\sum_{y\in\{0,1\}^n} \delta_{y\notin \mathrm{BIm}(L\cup R)} \right) \cdot \frac{(t+1)\left|\mathrm{BIm}\left(L\cup R\right)\right|}{N(N-\left|\mathrm{BIm}\left(L\cup R\right)\right|)} \\
&\leq \frac{(t+1)2t}{N} \ ,
\end{aligned}
$$

where the first inequality is from Cauchy-Schwarz inequality, the second inequality holds because $\sqrt{a}-\sqrt{b}\leq\sqrt{a-b}$ for non-negative a,b, the third inequality is from that fact that there are at most $t+1$ terms in the third summation and $|\mathrm{BIm}\left(L'\cup R\right)|=|\mathrm{BIm}\left(L\cup R\right)|+2$ and the last one is from $|\mathrm{BIm}\left(L\cup R\right)|\leq 2t$.

As for $|v\rangle$, notice that

$$
|v\rangle = \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \alpha_{x,L,R} \left(-\frac{\sqrt{\mathrm{num}(L,(x,y))+1}}{\sqrt{N}} \right) \right) |y\rangle\,|L'\rangle\,|R\rangle
$$

So we have

$$
\begin{aligned}
\langle v|v\rangle &= \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left| \sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \alpha_{x,L,R} \left(-\frac{\sqrt{\mathrm{num}(L,(x,y))+1}}{\sqrt{N}} \right) \right|^2 \\
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \frac{\mathrm{num}(L,(x,y))+1}{N} \right) \\
&= \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \frac{\mathrm{num}(L',(x,y))}{N} \right)
\end{aligned}
$$

$$
\begin{aligned}
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \left(\frac{\sum_{x\in\{0,1\}^n} \mathrm{num}(L',(x,y))}{N} \right) \\
&\leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:|L'\cup R|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \left|\alpha_{x,L,R}\right|^2 \right) \cdot \frac{t+1}{N} \\
&= \sum_{\substack{x\in\{0,1\}^n \\ L,R\in\mathfrak{R} \text{ s.t. } |L\cup R|\leq t}} \left|\alpha_{x,L,R}\right|^2 \cdot \left(\sum_{y\in\{0,1\}^n} \delta_{y\in \mathrm{BIm}(L\cup R)} \right) \cdot \frac{t+1}{N} \\
&\leq \frac{2t(t+1)}{N} \ ,
\end{aligned}
$$

where the first inequality is from Cauchy-Schwarz inequality, and the third inequality is from that fact that for a fixed y, $\sum_{x\in\{0,1\}^n} \mathrm{num}(L',(x,y))$ is the number of times that y appears in L' which is at most $t+1$. □

Next, we prove the main lemma in this section.

Proof of Lemma 5.15. To prove

$$
\|D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} \cdot Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t}\|_\infty \leq 32\sqrt{\frac{t(t+1)}{N}} \ ,
$$

it is equivalent to show

$$
\left\| D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty \leq 32\sqrt{\frac{t(t+1)}{N}} \ .
$$

By the triangle inequality and expanding the definition of operator V, we have

$$
\begin{aligned}
&\left\| D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty \\
&\leq \underbrace{\left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty}_{(a)} \\
&\quad + \underbrace{\left\| D_{\mathsf{A}} \cdot \left(V^L \cdot V^R \cdot V^{R,\dagger}\right)_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot \left(V^L \cdot V^R \cdot V^{R,\dagger}\right)_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty}_{(b)} \\
&\quad + \underbrace{\left\| D_{\mathsf{A}} \cdot \left(V^{R,\dagger}\right)_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot \left(V^{R,\dagger}\right)_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty}_{(c)}
\end{aligned}
$$

$$+\underbrace{\left\|D_{\mathsf{A}}\cdot\left(V^{L}\cdot V^{L,\dagger}\cdot V^{R,\dagger}\right)_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot\left(V^{L}\cdot V^{L,\dagger}\cdot V^{R,\dagger}\right)_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}}_{(d)}\ .$$

For (a), by the unitary invariance of operator E^L (Lemma B.2) and the triangle inequality, we have

$$\begin{aligned}(a)&\leq\left\|D_{\mathsf{A}}\cdot V_{\leq t}^{L}\cdot C_{\mathsf{A}}-D_{\mathsf{A}}\cdot E_{\leq t}^{L}\cdot C_{\mathsf{A}}\right\|_{\infty}+\left\|Q[C,D]_{\mathsf{LR}}\cdot E_{\leq t}^{L}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}^{L}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&\leq 2\left\|V_{\leq t}^{L}-E_{\leq t}^{L}\right\|_{\infty}\leq 4\sqrt{\frac{t(t+1)}{N}}\ .\end{aligned}$$

For (b), notice that $\left(V^{L}\cdot V^{R}\cdot V^{R,\dagger}\right)_{\leq t}=V_{\leq t}^{L}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}$. Therefore, we have

$$\begin{aligned}&(b)\\&=\left\|D_{\mathsf{A}}\cdot V_{\leq t}^{L}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}^{L}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&=\left\|D_{\mathsf{A}}\cdot V_{\leq t}^{L}\cdot C_{\mathsf{A}}\cdot C_{\mathsf{A}}^{\dagger}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}^{L}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\cdot Q[C,D]_{\mathsf{LR}}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&\leq\left\|D_{\mathsf{A}}\cdot V_{\leq t}^{L}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}^{L}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&\quad+\left\|C_{\mathsf{A}}^{\dagger}\cdot\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\ .\end{aligned}$$

The first term is exactly (a) which is bounded by $4\sqrt{\frac{t(t+1)}{N}}$. As for the second one, note that $\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}=V_{\leq t-1}^{R}\cdot V_{\leq t-1}^{R,\dagger}$, we have

$$\begin{aligned}&\left\|C^{\dagger}\cdot_{\mathsf{A}}\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot\left(V^{R}\cdot V^{R,\dagger}\right)_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&=\left\|C_{\mathsf{A}}^{\dagger}\cdot V_{\leq t-1}^{R}\cdot V_{\leq t-1}^{R,\dagger}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t-1}^{R}\cdot V_{\leq t-1}^{R,\dagger}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&\leq\left\|C_{\mathsf{A}}^{\dagger}\cdot V_{\leq t-1}^{R}\cdot D_{\mathsf{A}}^{\dagger}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t-1}^{R}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}+\left\|D_{\mathsf{A}}\cdot V_{\leq t-1}^{R,\dagger}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t-1}^{R,\dagger}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\\&\leq 8\sqrt{\frac{t(t+1)}{N}}\ ,\end{aligned}$$

where the last inequality follows from a similar argument as (a). Then, we have $(b)\leq 12\sqrt{\frac{t(t+1)}{N}}$. Similarly, we obtain $(c)\leq 4\sqrt{\frac{t(t+1)}{N}}$ and $(d)\leq 12\sqrt{\frac{t(t+1)}{N}}$. Thus,

$$\left\|D_{\mathsf{A}}\cdot V_{\leq t}\cdot C_{\mathsf{A}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}\cdot Q[C,D]_{\mathsf{LR}}^{\dagger}\right\|_{\infty}\leq 32\sqrt{\frac{t(t+1)}{N}}\ .$$

The other inequality in Lemma 5.15 follows from a similar argument. □

C A Twirling Lemma

In this section, we prove Lemma 5.19, we first analyze $\Pi_{\mathsf{LR}}^{\mathrm{Dom}(W)}$ and $\Pi_{\mathsf{LR}}^{\mathrm{Im}(W)}$ and then give the proof.

C.1 Properties of $\Pi^{\mathrm{Dom}(W)}$ and $\Pi^{\mathrm{Im}(W)}$

We need some notations:

$$\Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}} := \sum_{\substack{L,R\in\mathfrak{R}\\ x\notin \mathrm{BDom}(L\cup R)}} |x\rangle\!\langle x|_{\mathsf{A}} \otimes |L\rangle\!\langle L|_{\mathsf{L}} \otimes |R\rangle\!\langle R|_{\mathsf{R}} \quad ,$$

$$\Pi^{\notin\mathrm{Im}}_{\mathsf{ALR}} := \sum_{\substack{L,R\in\mathfrak{R}\\ y\notin \mathrm{BIm}(L\cup R)}} |y\rangle\!\langle y|_{\mathsf{A}} \otimes |L\rangle\!\langle L|_{\mathsf{L}} \otimes |R\rangle\!\langle R|_{\mathsf{R}} \quad ,$$

$$\Pi^{\mathrm{EPR}} := \frac{1}{N} \sum_{x,y\in\{0,1\}^n} |x,x\rangle\!\langle y,y| \quad .$$

We have the following lemma:

Lemma C.1.

$$\Pi^{\mathrm{Dom}(W)}_{\mathsf{LR}} = \Pi^{\mathrm{DB}}_{\mathsf{LR}} \cdot \left(\Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}} + \sum_{\substack{l,r\geq 0\\ l+r<N/2}} \frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{DB}}_{\mathsf{LR}} \quad ,$$

$$\Pi^{\mathrm{Im}(W)}_{\mathsf{LR}} = \Pi^{\mathrm{DB}}_{\mathsf{LR}} \cdot \left(\Pi^{\notin\mathrm{Im}}_{\mathsf{ALR}} + \sum_{\substack{l,r\geq 0\\ l+r<N/2}} \frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{R}} \otimes \sum_{i\in[r+1]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{L}^{(r+1)}_{\mathsf{Y},i}} \right) \cdot \Pi^{\mathrm{DB}}_{\mathsf{LR}} \quad .$$

Here, $\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{X,i}}$ *denotes the operator that acts on* A *and* $\mathsf{R}^{(r+1)}$ *such that it applies* Π^{EPR} *to* $\mathsf{A},\mathsf{R}^{(r+1)}_{X,i}$*, while applying identity to the remainder of* $\mathsf{R}^{(r+1)}$*.*

Proof. We show the first equality, and the other one follows from a similar argument. Note that $\Pi^{\mathrm{Dom}(W)} = \Pi^{\mathrm{Dom}(W^L)} + \Pi^{\mathrm{Im}(W^R)}$. So, it is sufficient to show

$$\Pi^{\mathrm{Dom}(W^L)} = \Pi^{\mathrm{DB}}_{\mathsf{LR}} \cdot \Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}} \cdot \Pi^{\mathrm{DB}}_{\mathsf{LR}} \quad ,$$

$$\Pi^{\mathrm{Im}(W^R)} = \Pi^{\mathrm{DB}}_{\mathsf{LR}} \cdot \left(\sum_{\substack{l,r\geq 0\\ l+r<N/2}} \frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{DB}}_{\mathsf{LR}} \quad .$$

It is easy to see that

$$\Pi^{\mathrm{Dom}(W^L)} = \sum_{\substack{L\cup R\in\mathfrak{R}^{\mathrm{DB}}\\ x\notin\mathrm{Dom}(L\cup R)}} |x\rangle\!\langle x|_{\mathsf{A}} \otimes |L\rangle\!\langle L|_{\mathsf{L}} \otimes |R\rangle\!\langle R|_{\mathsf{R}} = \Pi^{\mathrm{DB}}_{\mathsf{LR}} \cdot \Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}} \cdot \Pi^{\mathrm{DB}}_{\mathsf{LR}} \quad .$$

We now turn to proving the second equality. By definition of W^R, we know

$$\Pi^{\mathrm{Im}(W^R)} = W^R \cdot W^{R,\dagger} = W^R \cdot \sum_{\substack{l,r\geq 0,\\ l+r<N/2}} \Pi_{l,r,\mathsf{LR}} \cdot W^{R,\dagger} = \sum_{\substack{l,r\geq 0,\\ l+r<N/2}} W^R_{l,r} \cdot W^{R,\dagger}_{l,r} \quad .$$

Therefore, we are left to show

$$W_{l,r}^{R} \cdot W_{l,r}^{R,\dagger} = \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \cdot \left(\frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r+1)}}^{\mathrm{EPR}} \right) \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \ .$$

Recall the operator E^R in Definition B.1, it is not hard to check

$$W_{l,r}^{R} = \frac{\sqrt{N}}{\sqrt{N-2l-2r}} \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \cdot E_{l,r}^{R} \ .$$

Therefore,

$$\begin{aligned} W_{l,r}^{R} \cdot W_{l,r}^{R,\dagger} &= \frac{N}{N-2l-2r} \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \cdot E_{l,r}^{R} \cdot E_{l,r}^{R,\dagger} \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \\ &= \frac{N}{N-2l-2r} \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \cdot \left(\Pi_{l,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r+1)}}^{\mathrm{EPR}} \right) \cdot \Pi_{l,r+1,\mathsf{LR}}^{\mathrm{DB}} \ , \end{aligned}$$

where the second inequality is from [MH24, Eq. (11.26)]. □

For $l, r \geq 0$, we define

$$\begin{aligned} \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} &:= \sum_{L,R\in\mathfrak{R}} |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}} \ , \\ \Pi_{l,r,\mathsf{LR}}^{\mathrm{db}} &:= \sum_{\substack{(x_1,\cdots,x_l,x'_1,\cdots,x'_l)\in \mathrm{DB}_{l+r} \\ (y_1,\cdots,y_l,y'_1,\cdots,y'_l)\in \mathrm{DB}_{l+r}}} |x_1,\cdots,x_l,y_1,\cdots,y_l\rangle\langle x_1,\cdots,x_l,y_1,\cdots,y_l|_{\mathsf{L}} \\ &\qquad \otimes |x'_1,\cdots,x'_r,y'_1,\cdots,y'_r\rangle\langle x'_1,\cdots,x'_r,y'_1,\cdots,y'_r|_{\mathsf{R}} \ , \\ \Pi_{\mathsf{LR}}^{\mathrm{db}} &:= \sum_{\substack{l,r\geq 0 \\ l+r\leq N}} \Pi_{l,r,\mathsf{LR}}^{\mathrm{db}} \ . \end{aligned}$$

It is evident that

$$\Pi_{\mathsf{LR}}^{\mathrm{DB}} = \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \cdot \Pi_{\mathsf{LR}}^{\mathrm{db}} = \Pi_{\mathsf{LR}}^{\mathrm{db}} \cdot \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \ .$$

Now we define

$$J_{\mathsf{LR}}^{\mathrm{Dom}(W)} := \Pi_{\mathsf{LR}}^{\mathrm{db}} \cdot \left(\Pi_{\mathsf{ALR}}^{\notin\mathrm{Dom}} + \sum_{\substack{l,r\geq 0 \\ l+r<N/2}} \frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r+1)}}^{\mathrm{EPR}} \right) \cdot \Pi_{\mathsf{LR}}^{\mathrm{db}} \ ,$$

$$J_{\mathsf{LR}}^{\mathrm{Im}(W)} := \Pi_{\mathsf{LR}}^{\mathrm{db}} \cdot \left(\Pi_{\mathsf{ALR}}^{\notin\mathrm{Im}} + \sum_{\substack{l,r\geq 0 \\ l+r<N/2}} \frac{N}{N-2l-2r} \cdot \Pi_{l,\mathsf{R}} \otimes \sum_{i\in[r+1]} \Pi_{\mathsf{A},\mathsf{L}_{\mathsf{Y},i}^{(r+1)}}^{\mathrm{EPR}} \right) \cdot \Pi_{\mathsf{LR}}^{\mathrm{db}} \ .$$

Then we have

$$\begin{aligned} \Pi_{\mathsf{LR}}^{\mathrm{Dom}(W)} &= \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \cdot J_{\mathsf{LR}}^{\mathrm{Dom}(W)} \cdot \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \ , \\ \Pi_{\mathsf{LR}}^{\mathrm{Im}(W)} &= \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \cdot J_{\mathsf{LR}}^{\mathrm{Im}(W)} \cdot \Pi_{\mathsf{LR}}^{\mathfrak{R}^2} \ . \end{aligned}$$

We will need the following lemma when proving Lemma 5.19.

Lemma C.2. *For non-negative l, r such that $l + r < N/2$,*

$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}}$$
$$\preceq \sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \left(\left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) + 2\sqrt{\frac{2(l+r)}{N}} \cdot \mathbb{1}_{\mathsf{ALR}} \right) ,$$
$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Im}(W)}_{l,r,\mathsf{LR}}$$
$$\preceq \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{Y},i}} + \sum_{i\in[r]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{Y},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{Y},i}} + \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \left(\left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{Y},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{Y},i}} \right) + 2\sqrt{\frac{2(l+r)}{N}} \cdot \mathbb{1}_{\mathsf{ALR}} \right) .$$

Proof. We prove the first inequality, and the other one follows from a similar argument. Notice that

$$J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}} = \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\notin\mathrm{Dom}}_{l,r,\mathsf{ALR}} + \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}$$

Therefore, we have

$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}}$$
$$= \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi_{l,r,\mathsf{LR}} - \Pi^{\notin\mathrm{Dom}}_{l,r,\mathsf{ALR}} - \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}$$
$$\preceq \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}$$

where

$$\Pi^{\mathrm{eq}} = \sum_{x\in\{0,1\}^n} |x\rangle\!\rangle x| \otimes |x\rangle\!\rangle x| \quad ,$$
$$\Pi^{\mathrm{ffb}} = \sum_{x\in\{0,1\}^n} |x\rangle\!\rangle x| \otimes |\bar{x}\rangle\!\rangle \bar{x}| \quad .$$

Since Π^{eq}, Π^{ffb} and $\Pi^{\mathrm{db}}_{l,r}$ commute with each other, we have

$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}}$$
$$\preceq \sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\sum_{i\in[r]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}$$
$$\preceq \sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}$$
$$\preceq \sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$$
$$+ \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \left(\left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) + \lambda \cdot \mathbb{1}_{\mathsf{ALR}} \right)$$

$$\leq \sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} + \sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \frac{N}{N-2l-2r+2} \cdot \sum_{i\in[r]} \left(\left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) + \lambda \cdot \mathbb{1}_{\mathsf{ALR}} \right) \quad ,$$

where

$$\lambda := \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right\|_\infty \quad .$$

Thus, we are left to show λ is bounded by $2\sqrt{\frac{2(l+r)}{N}}$. Notice that

$$\begin{aligned}
\lambda &\leq \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \right\|_\infty \\
&+ \left\| \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right\|_\infty \\
&= \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right)^2 \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \right\|_\infty \\
&+ \left\| \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \Pi^{\mathrm{db}^2}_{l,r,\mathsf{LR}} \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right\|_\infty \\
&\leq 2 \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) - \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \right\|_\infty \\
&= 2 \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \right\|_\infty \quad .
\end{aligned}$$

So, it suffices to prove that

$$\left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \right\|_\infty \leq \sqrt{\frac{2(l+r)}{N}} \quad .$$

If $r = 0$, this holds trivially. From now on, we assume $r \geq 1$. Note that

$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} = \sum_{\substack{(x,x')\in \mathsf{DB}_{l+r-1} \\ (y,y')\in \mathsf{DB}_{l+r}}} |x,y\rangle\langle x,y|_{\mathsf{L}} \otimes |x',y'\rangle\langle x',y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},i}} \otimes \frac{1}{N} \sum_{\substack{z\in T_{x,x'} \\ w\in\{0,1\}^n}} |z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \quad .$$

Here, $x \in \{0,1\}^{nl}$, $x' \in \{0,1\}^{n(r-1)}$, $y, y' \in \{0,1\}^{nr}$ and $T_{x,x'}$ denotes the set of all binary strings that do not belong to the same block with any string in x and x'. Similarly, we have

$$\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} = \sum_{\substack{(x,x')\in \mathsf{DB}_{l+r-1} \\ (y,y')\in \mathsf{DB}_{l+r}}} |x,y\rangle\langle x,y|_{\mathsf{L}} \otimes |x',y'\rangle\langle x',y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},i}} \otimes \frac{1}{N} \sum_{\substack{w\in T_{x,x'} \\ z\in\{0,1\}^n}} |z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \quad .$$

Then, we have

$$\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} = \sum_{\substack{(x,x')\in \mathsf{DB}_{l+r-1} \\ (y,y')\in \mathsf{DB}_{l+r}}} |x,y\rangle\langle x,y|_{\mathsf{L}} \otimes |x',y'\rangle\langle x',y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},i}} \otimes$$

$$\left(\frac{1}{N}\sum_{\substack{z\in T_{x,x'}\\ w\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\frac{1}{N}\sum_{\substack{w\in T_{x,x'}\\ z\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\right)\quad.$$

Therefore,

$$\left\|\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}\cdot\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\cdot\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}\right\|_\infty\le\max_{x,x'}\left\|\frac{1}{N}\sum_{\substack{z\in T_{x,x'}\\ w\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\frac{1}{N}\sum_{\substack{w\in T_{x,x'}\\ z\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\right\|_\infty\quad.$$

Notice that

$$\begin{aligned}&\left\|\frac{1}{N}\sum_{\substack{z\in T_{x,x'}\\ w\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\frac{1}{N}\sum_{\substack{w\in T_{x,x'}\\ z\in\{0,1\}^n}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\right\|_\infty\\ =&\left\|\frac{1}{N}\sum_{\substack{z\in T_{x,x'}\\ w\notin T_{x,x'}}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\frac{1}{N}\sum_{\substack{w\in T_{x,x'}\\ z\notin T_{x,x'}}}|z,z\rangle\langle w,w|_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\right\|_\infty\\ =&\frac{\sqrt{(N-2l-2r+2)(2l+2r-2)}}{N}\left\||\phi\rangle\langle\psi|-|\psi\rangle\langle\phi|\right\|_\infty\quad,\end{aligned}$$

where

$$|\phi\rangle:=\frac{1}{\sqrt{N-2l-2r+2}}\sum_{z\in T_{x,x'}}|z,z\rangle\quad\text{and}\quad|\psi\rangle:=\frac{1}{\sqrt{2l+2r-2}}\sum_{z\notin T_{x,x'}}|z,z\rangle\quad.$$

Since $|\phi\rangle$ and $|\psi\rangle$ are orthogonal, it is not hard to see that $\left\||\phi\rangle\langle\psi|-|\psi\rangle\langle\phi|\right\|_\infty=1$. Therefore,

$$\left\|\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}\cdot\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}-\Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}}\cdot\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}}\right\|_\infty\le\frac{\sqrt{(N-2l-2r+2)(2l+2r-2)}}{N}\le\sqrt{\frac{2(l+r)}{N}}\quad.$$

□

C.2 Proof of Lemma 5.19

We need the following property of twirling with Haar random unitary.

Lemma C.3 (Claim 2 in [MH24]). *Let $\mathcal{D}$ be the Haar measure over $\mathrm{U}(N)$. We have*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathcal{D}}\left[\left(U\otimes\overline{U}\right)^\dagger\cdot\Pi^{\mathrm{eq}}\cdot\left(U\otimes\overline{U}\right)\right]=\Pi^{\mathrm{EPR}}+\frac{1}{N+1}\left(\mathbb{1}-\Pi^{\mathrm{EPR}}\right)\quad.$$

Before proving Lemma 5.19, we prove a lemma that will assist in our argument.

Lemma C.4. *Let $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18. We have for non-negative l, r*

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \le \frac{4l+r}{N-1} + \frac{7rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \,,$$

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}} \left[(D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Im}(W)}_{l,r,\mathsf{LR}} \right) \cdot (D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \le \frac{l+4r}{N-1} + \frac{7lN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \,.$$

Proof. We show the first inequality for $\mathcal{D} = \mathcal{D}_2$ and the rest inequalities follow from a similar argument. From Lemma C.2 and the triangle inequality, we have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
\le &\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[l]} \Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
&+ \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[l]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{L}^{(l)}_{\mathsf{X},i}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
&+ \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[r]} \Pi^{\mathrm{ffb}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
&+ \frac{N}{N-2l-2r+2} \cdot \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[r]} \left(\Pi^{\mathrm{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
&+ \frac{2rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \\
\le &\, l \cdot \sum_{x\in\{0,1\}^n} \underbrace{\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes C)^\dagger \cdot |x,x\rangle\langle x,x| \cdot (C\otimes C) \right] \right\|_\infty}_{(1)} + l \cdot \sum_{x\in\{0,1\}^n} \underbrace{\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes C)^\dagger \cdot |x,\bar{x}\rangle\langle x,\bar{x}| \cdot (C\otimes C) \right] \right\|_\infty}_{(2)} \\
&+ r \cdot \sum_{x\in\{0,1\}^n} \underbrace{\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes \bar{C})^\dagger \cdot |x,\bar{x}\rangle\langle x,\bar{x}| \cdot (C\otimes \bar{C}) \right] \right\|_\infty}_{(3)} \\
&+ \frac{rN}{N-2l-2r+2} \cdot \underbrace{\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes \bar{C})^\dagger \cdot \left(\Pi^{\mathrm{eq}} - \Pi^{\mathrm{EPR}} \right) \cdot (C\otimes \bar{C}) \right] \right\|_\infty}_{(4)} + \frac{2rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \,.
\end{aligned}$$

For (1), notice that $C^\dagger$ is equivalent to a T-step parallel Kac's walk followed by an independent

random permutation, which means $C^\dagger$ is drawn from a $\frac{1}{N^2}$ − RSS distribution. Thus, we have

$$(1) \le \left\| \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes U)\cdot |x,x\rangle\langle x,x|\cdot (U\otimes U)^\dagger \right] \right\|_\infty + \frac{1}{N^2} = \frac{2}{N(N+1)} + \frac{1}{N^2} \ .$$

For (2), notice that $C^\dagger = C'^\dagger \cdot P^\dagger$. So,

$$(2) \le \left\| \mathop{\mathbb{E}}_{P} \left[(P\otimes P)^\dagger \cdot |x,\bar{x}\rangle\langle x,\bar{x}|\cdot (P\otimes P) \right] \right\|_\infty = \left\| \frac{1}{N(N-1)} \sum_{x\neq y} |x,y\rangle\langle x,y| \right\|_\infty = \frac{1}{N(N-1)} \ .$$

Similarly, we have $(3) \le \frac{1}{N(N-1)}$.

We now give an upper bound on (4). We first prove that for any $x \in \{0,1\}^n$

$$\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes \overline{C})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (C\otimes \overline{C}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes \overline{U})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (U\otimes \overline{U}) \right] \right\|_\infty \le \frac{4}{N^2} \ . \quad (48)$$

Notice that $C^\dagger$ is equivalent to a T-step parallel Kac's walk followed by a random permutation P'. Let $|u\rangle$ be the random state after T steps of parallel Kac's walk starting at $|x\rangle\langle x|$, and $|v\rangle$ be the Haar random state. We have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes \overline{C})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (C\otimes \overline{C}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes \overline{U})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (U\otimes \overline{U}) \right] \right\|_\infty \\
\le &\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes \overline{C})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (C\otimes \overline{C}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes \overline{U})^\dagger \cdot |x,x\rangle\langle x,x|\cdot (U\otimes \overline{U}) \right] \right\|_1 \\
\le &\left\| \mathop{\mathbb{E}}_{P',|u\rangle} \left[\left(P'\otimes \overline{P'}\right) \left(|u\rangle\langle u|\otimes \overline{|u\rangle\langle u|}\right) \left(P'\otimes \overline{P'}\right)^\dagger \right] - \mathop{\mathbb{E}}_{P',|v\rangle} \left[\left(P'\otimes \overline{P'}\right) \left(|v\rangle\langle v|\otimes \overline{|v\rangle\langle v|}\right) \left(P'\otimes \overline{P'}\right)^\dagger \right] \right\|_1 \\
\le &\left\| \mathop{\mathbb{E}}_{|u\rangle} \left[|u\rangle\langle u|\otimes \overline{|u\rangle\langle u|} \right] - \mathop{\mathbb{E}}_{|v\rangle} \left[|v\rangle\langle v|\otimes \overline{|v\rangle\langle v|} \right] \right\|_1 \ .
\end{aligned}$$

From [LQS+24, Theorem 4], we know that there is a joint distribution γ among $|u\rangle$ and $|v\rangle$ such that $\mathbb{E}_\gamma[\||u\rangle - |v\rangle\|_2] \le \frac{1}{N^2}$. Therefore, we have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{|u\rangle} \left[|u\rangle\langle u|\otimes \overline{|u\rangle\langle u|} \right] - \mathop{\mathbb{E}}_{|v\rangle} \left[|v\rangle\langle v|\otimes \overline{|v\rangle\langle v|} \right] \right\|_1 \\
= &\left\| \mathop{\mathbb{E}}_{\gamma} \left[|u\rangle\langle u|\otimes \overline{|u\rangle\langle u|} - |v\rangle\langle v|\otimes \overline{|v\rangle\langle v|} \right] \right\|_1 \\
\le &\left\| \mathop{\mathbb{E}}_{\gamma} \left[|u\rangle\langle u|\otimes \overline{|u\rangle\langle u|} - |v\rangle\langle v|\otimes \overline{|u\rangle\langle u|} \right] \right\|_1 + \left\| \mathop{\mathbb{E}}_{\gamma} \left[|v\rangle\langle v|\otimes \overline{|u\rangle\langle u|} - |v\rangle\langle v|\otimes \overline{|v\rangle\langle v|} \right] \right\|_1 \\
\le &\mathop{\mathbb{E}}_{\gamma} \left[\left\| |u\rangle\langle u|\otimes \overline{|u\rangle\langle u|} - |v\rangle\langle v|\otimes \overline{|u\rangle\langle u|} \right\|_1 \right] + \mathop{\mathbb{E}}_{\gamma} \left[\left\| |v\rangle\langle v|\otimes \overline{|u\rangle\langle u|} - |v\rangle\langle v|\otimes \overline{|v\rangle\langle v|} \right\|_1 \right] \\
= &2\cdot \mathop{\mathbb{E}}_{\gamma} [\||u\rangle\langle u| - |v\rangle\langle v|\|_1] \\
\le &2\cdot \left(\mathop{\mathbb{E}}_{\gamma} [\||u\rangle \left(\langle u| - \langle v|\right)\|_1 + \|\left(|u\rangle - |v\rangle\right)\langle v|\|_1] \right) \\
\le &4\cdot \mathop{\mathbb{E}}_{\gamma} [\||u\rangle - |v\rangle\|_2] \le \frac{4}{N^2} \ .
\end{aligned}$$

This establishes Eq. (48). From Eq. (48), Lemma C.3 and the fact that $(U \otimes \overline{U})^\dagger \cdot \Pi^{\mathrm{EPR}} \cdot (U \otimes \overline{U}) = \Pi^{\mathrm{EPR}}$ for any unitary U, we have

$$(4) \leq \left\| \mathop{\mathbb{E}}_{U \leftarrow \mu} \left[(U \otimes \overline{U})^\dagger \cdot \left(\Pi^{\mathrm{eq}} - \Pi^{\mathrm{EPR}} \right) \cdot (U \otimes \overline{U}) \right] \right\|_\infty + \frac{4}{N} \leq \frac{1}{N+1} + \frac{4}{N} \leq \frac{5}{N} \ .$$

Therefore, we have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}_2} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
\leq & \frac{2l}{N+1} + \frac{l}{N} + \frac{l}{N-1} + \frac{r}{N-1} + \frac{5r}{N-2l-2r+2} + \frac{2rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \\
\leq & \frac{4l+r}{N-1} + \frac{7rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \ .
\end{aligned}$$

□

We are now ready to prove Lemma 5.19. We restate the lemma here.

Lemma 5.19. *For integer $0 \leq t \leq N/4$ and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 5.18, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{DB}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \leq 16t \cdot \sqrt{\frac{2t}{N}} \ ,$$

$$\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{DB}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Im}(W)}_{\leq t,\mathsf{LR}} \right) \cdot (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \leq 16t \cdot \sqrt{\frac{2t}{N}} \ .$$

Proof. We prove the first inequality and the other one is from a similar argument. Note that

$$\Pi^{\mathrm{DB}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} = \Pi^{\Re^2}_{\mathsf{LR}} \cdot \left(\Pi^{\mathrm{db}}_{\leq t,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} \right) \cdot \Pi^{\Re^2}_{\mathsf{LR}} \ ,$$

and $\Pi^{\Re^2}$ commutes with $Q[C,D]_{\mathsf{LR}}$ since $\Pi^{\Re^2}$ is the sum of projectors onto the symmetric subspaces. We have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{DB}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
\leq & \left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{\leq t,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
= & \max_{\substack{l,r \geq 0 \\ l+r \leq t}} \left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - J^{\mathrm{Dom}(W)}_{l,r,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \ ,
\end{aligned}$$

where the equality holds because $\Pi^{\mathrm{db}}_{\leq t,\mathsf{LR}}$ and $J^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}}$ are block diagonal with repect to l and r. Then from Lemma C.4, we have

$$\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{DB}}_{\leq t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\leq t,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty$$

$$
\begin{aligned}
&\leq \max_{\substack{l,r\geq 0\\ l+r\leq t}} \quad \frac{4l+r}{N-1} + \frac{7rN}{N-2l-2r+2}\cdot\sqrt{\frac{2(l+r)}{N}} \\
&\leq \max_{\substack{l,r\geq 0\\ l+r\leq t}} \quad \frac{3l+t}{N-1} + \frac{7rN}{N-2t+2}\cdot\sqrt{\frac{2t}{N}} \\
&\leq \frac{t}{N-1} + \frac{7tN}{N-2t+2}\cdot\sqrt{\frac{2t}{N}} \leq \frac{8tN}{N-2t+2}\cdot\sqrt{\frac{2t}{N}} \leq 16t\cdot\sqrt{\frac{2t}{N}} \ ,
\end{aligned}
$$

where the second inequality is from $l + r \leq t$, the third inequality holds since the maximal value is achieved at $r = t$, and the last one is from $t \leq N/4$. □