Parallel Kac's Walk Generates PRU

Chuhan Lu[1], Minglong Qin[2], Fang Song[3], Penghui Yao[4,5], and Mingnan Zhao[4]

[1] Department of Computer Science, Rice University, USA
cl308@rice.edu
[2] Centre for Quantum Technologies, National University of Singapore, Singapore
mlqin6@gmail.com
[3] Computer Science Department, Portland State University, USA
fang.song@pdx.edu
[4] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
phyao1985@gmail.com, mingnanzh@gmail.com
[5] Hefei National Laboratory, Hefei 230088, China

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 [MH25].

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+26], 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 permutations (PRPs) and pseudorandom generators (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, GTB23, JMW23, BM24]. Ji, Liu and Song further introduced the concept of *pseudorandom unitaries* (PRUs), which

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 work has 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], and pseudorandom scramblers [LQS+26].

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 [MH25] 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+26], 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 the 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 the 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 an initial unit vector sequentially. Pillai and Smith [PS17] showed a tight $\Theta(N \log N)$ mixing time for Kac's walk on an N-dimensional unit sphere.

Lu, Qin, Song, Yao and Zhao [LQS+26] introduced a variant called *parallel Kac's walk*. It randomly samples a random matching among all N computational basis elements, say $\{(|i_1\rangle, |j_1\rangle), \ldots, (|i_{N/2}\rangle, |j_{N/2}\rangle)\}$, 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 (pseudo)random state. This is formalized as a primitive called *(pseudo)random state scrambler* in [LQS+26]. It was left open in their paper whether 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 (Main Theorem, Informal). *The distribution of the unitary corresponding to an $O(n)$-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 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+26] 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. Note that 2-designs, such as random Clifford, can also project states onto distinct block subspaces. However, parallel Kac's walk alone is not known to form a 2-design, and hence this does not help us build a PRU purely based on the parallel Kac's walk. Therefore, we instead directly prove that the parallel Kac's walk suffices for this purpose by an unexpected application of a random scrambling property established in [LQS+26].

In the second phase, we adapt the techniques in [MH25]. A key ingredient in their method is the path-recording oracle of [MH25], which was designed so that it behaves indistinguishably from both the (purified) PF and Haar random distribution as long as the queries are restricted to tuples of distinct elements (a.k.a. the distinct subspace). In our case, because of the 2×2 block diagonal structure of the random rotations in parallel Kac's walk, we instead need to work with the distinct block subspace as indicated earlier. We thus design a variant path-recording oracle tailored to the distinct block subspace structure, and show that it serves as an effective bridge to reason about the indistinguishability of one-round parallel Kac's walk and Haar random unitary when restricting queries in the distinct block subspace. This also illustrates the versatility of the path-recording technique and provides a template for further extension.

1.2 Discussions

As far as we are aware, existing provably-secure constructions of PRU all follow the PFC paradigm. For example, Schuster, Haferkamp and Huang [SHH25]

developed a "gluing" lemma which can compose $\omega(\log n)$-qubit PRU by a two-layer brickwork into an n-qubit PRU. However, prior to our construction, the only instantiation of the small $\omega(\log n)$-qubit PRU would be by PFC. More recently in [CSBH25], it was observed that the (pseudo-)random permutation P in the PFC construction can be substituted by a two-round Luby-Rackoff Feistel network, and several PRU constructions with reduced depth were obtained. This can be seen as a further refinement of the PFC paradigm. Our Kac-walk based PRU hence gives the first secure construction that explores a new route drastically deviating from the PFC style.[6]

While our PRU construction does not provide efficiency advantages over the PFC construction, there are potential benefits in other regards. First, it is usually valuable to have multiple candidates for a primitive available, to cater to 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 construction consists of repetitions of this basic module. Finally, since PRUs are the quantum analogue of pseudorandom permutations (i.e., block ciphers), our PRU is also reminiscent of the famous Feistel network and variants in practical block ciphers such as AES, where a basic unit is iterated in multiple rounds to achieve desirable security properties.

The construction and analysis in our work also shed new light on designing PRU and quantum pseudorandomness more broadly. From the perspective of appropriate path-recording oracles, one can argue that PF in the PFC construction and one-round parallel Kac's walk are already indistinguishable from Haar random unitary under respective restrictions on the adversary's queries. Thus to obtain a full-fledged PRU, we can prepend to it a "filter" (random Clifford/2-design C or $O(n)$-round parallel Kac's walk) to enforce the restriction. Alternatively, we can view both PF and one-round parallel Kac's walk as a "randomness-compiler": as long as the initial object (random Clifford/2-design C in PFC or $O(n)$-round leading parallel Kac's walk) admits some well-specified "benign" randomizing property (e.g., approximating Haar under some twirling operation), composing with PF or one-round parallel Kac's walk will convert it to a PRU. We distill such claims in the main body, which would be useful in building more PRUs and other quantum (pseudo-)random objects. For example, one can immediately obtain a host of new PRU constructions, such as an arbitrary 2-design or random-state scrambler followed by one-round parallel Kac's walk.

Some open questions naturally follow from the above discussion. 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 analogy we draw between our construction and

[6] An earlier version of [BHHP25] claimed a proof for a variant of a candidate PRU proposed in [JLS18], but a bug was found and the claim was retracted later.

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. On a more technical note, [LQS+26] identifies a strong *dispersing* property of the parallel Kac's walk. Does this property carry over 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. Finally, can Kac's walk lead to pseudorandom operations on other groups? In particular, since Kac's walk also arises on SO(N) [Jan01, Mas03, Jan03, CCL03, Oli09, PS18, PS26], it would be interesting to investigate whether it yields other pseudorandom operations, such as pseudorandom orthogonal operators.

Acknowledgment. This work was done while Chuhan Lu was at Portland State University. 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 the National Natural Science Foundation of China (Grant Nos. 62332009 and 12347104), the Quantum Science and Technology—National Science and Technology Major Project (Grant No. 2021ZD0302901), the NSFC/RGC Joint Research Scheme (Grant No. 12461160276), the Natural Science Foundation of Jiangsu Province (No. BK20243060), the Fundamental and Interdisciplinary Disciplines Breakthrough Plan of the Ministry of Education of China (No. JYB2025XDXM118), the "111 Center" (No. B26023), and the Fundamental Research Funds for the Central Universities (Grant No. 2026300376).

Organization. The remainder of the paper is organized as follows. Section 2 introduces the notation and cryptographic preliminaries. Section 3 proves the projection lemma into the distinct block subspace. Section 4 presents the parallel Kac's walk construction and proves its adaptive security. Section 5 extends the analysis to inverse queries and proves strong security. Deferred proofs are given in the appendix.

2 Preliminaries

2.1 Notation

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,

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

We also need the following lemmas:

Lemma 2 ([MH25, Lemma 2.2]). *Let ρ_{CD} be a density matrix on registers C, D and let Π_{CD} be a projector of the form $\Pi_{\mathsf{CD}} = \mathsf{Id}_{\mathsf{C}} \otimes \Pi'_{\mathsf{D}}$, where Π'_{D} is a projector that acts on register D. Then*

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

Lemma 3 (Gentle Measurement Lemma [MH25, Lemma 2.3]). *Let $|\psi\rangle$ be a quantum state, $U_1, \ldots, U_t$ be unitary operators, and $\Pi_1, \ldots, \Pi_t$ be projectors. We have*

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

2.2 Adversary with Access to Oracle

We adopt the model for adversaries with oracle access in [MH25].

Definition 4 (Adversary with Access to Oracle). *An adversary $\mathcal{A}$ with oracle access is a quantum algorithm which queries an oracle $\mathcal{O}$ on its first n-qubit register A without knowing the description of $\mathcal{O}$. The adversary owns an additional m-qubit ancillary register, 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

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

We also allow the adversary $\mathcal{A}$ to make both forward queries (i.e., to $\mathcal{O}$) and inverse queries (i.e., to $\mathcal{O}^\dagger$). In this case, a t-query adversary $\mathcal{A}$ is specified by

a t-tuple of unitaries $(A_{\mathsf{AB}}^{(1)}, \cdots, A_{\mathsf{AB}}^{(t)})$ and a Boolean string $b \in \{0,1\}^t$. The view of the adversary after all the queries is

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

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

Definition 5 (Computational Indistinguishability). *We say two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over $\mathrm{U}(N)$ are computationally indistinguishable if for any $\mathrm{poly}(n)$-time adversary $\mathcal{A}$ with oracle access who makes $t = \mathrm{poly}(n)$ queries,*

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

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 $\mathfrak{R} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t$ be the set of all relations with size at most N. For $R \in \mathfrak{R}_t$, the corresponding *relation state* is defined by

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

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 $\gamma_R \coloneqq t! \cdot \sum_{x,y \in \{0,1\}^n} \left(\sum_{i=1}^{t} \delta_{(x_i, y_i) = (x,y)} \right)!$.

Fact 6. $\{|R\rangle_{\mathsf{XY}}\}_{R \in \mathfrak{R}}$ *forms an orthogonal basis.*

We further introduce additional notation for later use. Let $\mathfrak{R}_t^{\mathsf{yDB}}$ be the set of all size-t relations $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ such that $(y_1, \ldots, y_t) \in \mathsf{DB}_t$. Let $\mathfrak{R}^{\mathrm{yDB}} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t^{\mathsf{yDB}}$. Let $\mathfrak{R}_t^{\mathsf{DB}}$ 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 $\mathfrak{R}^{\mathrm{DB}} \coloneqq \cup_{t=0}^{N} \mathfrak{R}_t^{\mathsf{DB}}$. For any relation R, define

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

2.4 Cryptography

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

Definition 7 (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 8 (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 [Son17, Zha25].

Definition 9 (Random State Scrambler [LQS+26]). *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 if for any n-qubit pure state $|\phi\rangle$ and $\ell \in \mathrm{poly}(n)$,*

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

*We call a random unitary K sampled from such distribution an ϵ-random state scrambler (ϵ-*RSS*).*

Definition 10 (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

This section shows 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*. We define the projector onto the distinct block subspace as follows.

Definition 11 (Distinct Block subspaces). *Let $0 \leq t \leq N$, and let*

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

Lemma 12. *Let $0 \leq t \leq N$, and let $\mathcal{R}$ be a distribution over $\mathrm{U}(N)$ such that for $K \leftarrow \mathcal{R}$, $K^\dagger$ is an ϵ-RSS with $\epsilon = O\left(\frac{1}{N^2}\right)$. Define $\mathcal{D}$ to be the distribution that samples $G = PK$ where $P \leftarrow \mathcal{S}_N$ is a random permutation unitary and $K \leftarrow \mathcal{R}$. For any state ρ on an nt-qubit register $\mathsf{X} = (\mathsf{X}_1, ..., \mathsf{X}_t)$ together with another arbitrary register, we have*

$$\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\Pi^{(t)}_{\mathsf{X}} \cdot G^{\otimes t}_{\mathsf{X}} \rho G^{\otimes t,\dagger}_{\mathsf{X}}\right)\right] \geq 1 - O\left(\frac{t^2}{N}\right) \quad .$$

Proof. Using the cyclic property of trace and then the definition of $\Pi^{(t)}$,

$$\begin{aligned}\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\Pi^{(t)}_{\mathsf{X}} \cdot G^{\otimes t}_{\mathsf{X}} \rho G^{\otimes t,\dagger}_{\mathsf{X}}\right)\right] &= \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[G^{\otimes t,\dagger}_{\mathsf{X}} \cdot \Pi^{(t)}_{\mathsf{X}} \cdot G^{\otimes t}_{\mathsf{X}} \cdot \rho\right]\right) \\ &= \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[G^{\otimes t,\dagger}_{\mathsf{X}} \cdot \sum_{x\in\mathsf{DB}_t} |x\rangle\langle x|_{\mathsf{X}} \cdot G^{\otimes t}_{\mathsf{X}} \cdot \rho\right]\right) \quad . \end{aligned} \tag{2}$$

Now define $\rho_{\mathsf{X}_1,\ldots,\mathsf{X}_t} := \mathrm{Tr}_{-(\mathsf{X}_1,\ldots,\mathsf{X}_t)}(\rho)$, where $\mathrm{Tr}_{-(\mathsf{X}_1,\ldots,\mathsf{X}_t)}$ represents tracing out all registers except $\mathsf{X}_1,\ldots,\mathsf{X}_t$. Then Eq. (2) can be rewritten as

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

This implies:

$$\begin{aligned}1 - \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\Pi^{(t)}_{\mathsf{X}} \cdot G^{\otimes t}_{\mathsf{X}} \rho G^{\otimes t,\dagger}_{\mathsf{X}}\right)\right] \\ = \mathrm{Tr}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[G^{\otimes t,\dagger} \cdot \sum_{x\in\{0,1\}^{nt}\setminus\mathsf{DB}_t} |x\rangle\langle x| \cdot G^{\otimes t} \cdot \rho_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right]\right) \quad . \end{aligned} \tag{3}$$

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

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

And we have

$$\sum_{x\in\{0,1\}^{nt}\setminus \mathsf{DB}_t} |x\rangle\!\langle x|_{\mathsf{X}_1,\ldots,\mathsf{X}_t} \preceq \sum_{1\le i<j\le t} \Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j} + \Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j} \ , \tag{4}$$

where $\preceq$ represents the positive semidefinite order; $\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}$ is the equality projector on registers X_i and X_j; and $\Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}$ is the flip-first-bit projector on registers X_i and X_j. Combining Eq. (3) and the inequality Eq. (4):

$$\begin{aligned}
&1 - \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\Pi^{(t)}_{\mathsf{X}}\cdot G^{\otimes t}_{\mathsf{X}}\rho G^{\otimes t,\dagger}_{\mathsf{X}}\right)\right] \\
\le &\sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(G^{\otimes t,\dagger}\cdot\left(\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}+\Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right)\cdot G^{\otimes t}\cdot\rho_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right)\right] \\
= &\sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\left(G^{\dagger}_{\mathsf{X}_i}\otimes G^{\dagger}_{\mathsf{X}_j}\right)\cdot\left(\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}+\Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right)\cdot\left(G_{\mathsf{X}_i}\otimes G_{\mathsf{X}_j}\right)\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \\
= &\sum_{1\le i<j\le t} \mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N\\K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\begin{array}{c}\left((PK)^{\dagger}_{\mathsf{X}_i}\otimes(PK)^{\dagger}_{\mathsf{X}_j}\right)\cdot\left(\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}+\Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\right)\\ \cdot\left(PK_{\mathsf{X}_i}\otimes PK_{\mathsf{X}_j}\right)\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\end{array}\right)\right] \ ,
\end{aligned} \tag{5}$$

where the part inside of the summation of Eq. (5) can be rewritten as the sum of the following two terms:

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

$$\mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N\\K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left((PK)^{\dagger}_{\mathsf{X}_i}\otimes(PK)^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{ffb}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(PK_{\mathsf{X}_i}\otimes PK_{\mathsf{X}_j}\right)\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \ . \tag{7}$$

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

$$\begin{aligned}
(6) &= \mathop{\mathbb{E}}_{\substack{P\leftarrow\mathcal{S}_N\\K\leftarrow\mathcal{R}}}\left[\mathrm{Tr}\left(\left(K^{\dagger}_{\mathsf{X}_i}\otimes K^{\dagger}_{\mathsf{X}_j}\right)\left(P^{\dagger}_{\mathsf{X}_i}\otimes P^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(P_{\mathsf{X}_i}\otimes P_{\mathsf{X}_j}\right)\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\right)\right] \\
&= \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\mathrm{Tr}\left(\left(K^{\dagger}_{\mathsf{X}_i}\otimes K^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\cdot\rho_{\mathsf{X}_1,\ldots,\mathsf{X}_t}\right)\right] \ .
\end{aligned}$$

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

$$(6) \le \left\| \mathop{\mathbb{E}}_{K\leftarrow\mathcal{R}}\left[\left(K^{\dagger}_{\mathsf{X}_i}\otimes K^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(K_{\mathsf{X}_i}\otimes K_{\mathsf{X}_j}\right)\right]\right\|_{\infty} \ .$$

By the triangle inequality, we have

$$\begin{aligned}
(6) \le &\left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U^{\dagger}_{\mathsf{X}_i}\otimes U^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(U_{\mathsf{X}_i}\otimes U_{\mathsf{X}_j}\right)\right]\right\|_{\infty} \\
&+ \left\| \mathop{\mathbb{E}}_{U\leftarrow\mu}\left[\left(U^{\dagger}_{\mathsf{X}_i}\otimes U^{\dagger}_{\mathsf{X}_j}\right)\cdot\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot\left(U_{\mathsf{X}_i}\otimes U_{\mathsf{X}_j}\right)\right]\right.
\end{aligned}$$

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

where we use the property 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 $\mathbb{E}_{U\leftarrow\mu}\left[\left(U^{\dagger}\otimes U^{\dagger}\right)\cdot|x,x\rangle\langle x,x|\cdot\left(U\otimes U\right)\right]=\mathbb{E}_{|\psi\rangle\leftarrow\mu}[|\psi,\psi\rangle\langle\psi,\psi|]$ and the operator norm is $\frac{2}{N(N+1)}$ [Har13, Proposition 6]. Thus, we have

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

Next, we attempt to bound (7):

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

Since both Eqs. (6) and (7) are upper bounded by $O\left(N^{-1}\right)$, by substituting into Eq. (5) and using a union bound on all i and j, we have

$$
1-\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)}\cdot G_{\mathsf{X}}^{\otimes t}\rho G_{\mathsf{X}}^{\otimes t,\dagger}\right)\right]\le O\left(\frac{t^2}{N}\right)\ . \qquad \square
$$

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

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

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

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

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+26].

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 13. *$\mathsf{HP}_{n,T}$ is a distribution over $\mathrm{U}(N)$ which can be sampled 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* $\mathsf{Kac} = \prod_{i=1}^{T} (H_{f_i} \cdot P_{\sigma_i})$.

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 14. *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 between two adjacent hybrids is bounded by

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

where the second inequality is from the triangle inequality and the last inequality is from Lemma 19 in [LQS+26]. Thus, we have that by the triangle inequality,

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

□

It is proved in [LQS+26] 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+26, Theorem 10].

Theorem 15. *Let* $T = 30n$ *and* $d = 5n$. *Then the distribution* $\mathsf{HP}_{n,T}$ *is an* ϵ-RSS *distribution on* $\mathrm{U}(N)$ *with* $\epsilon = O\left(\frac{1}{N^2}\right)$. *Moreover, if* $\mathsf{Kac} \leftarrow \mathsf{HP}_{n,T}$, *then* $\mathsf{Kac}^\dagger$ *is also an* ϵ-RSS *with* $\epsilon = O\left(\frac{1}{N^2}\right)$. [7]

[7] The second statement follows from the observation that $\mathsf{Kac}^\dagger$ contains enough steps of the parallel Kac's walk.

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:

Theorem 16. *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 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 then consists of three steps:

- We begin by establishing a purification of the adversary's view state when making queries to the random unitary $H_f \cdot P_\sigma$. Specifically, we introduce two environment registers, H and P, which record the function f and the 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 the adversary's registers and the 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 a path-recording oracle PR, where PR is defined in Definition 23. 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, we will introduce the purified function-permutation oracle HPO in Section 4.2 and the path-recording oracle in Section 4.3. We then explain how to connect the actions of HPO and PR by introducing an isometry $\mathsf{Compress}$ in Section 4.4. Lastly, we prove the main result in Section 4.5.

4.2 The Purified Function-Permutation Oracle

To analyze the behavior of querying $H_f \cdot P_\sigma$, we employ a purified oracle.

Definition 17 (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*

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

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

Fact 18. *For any adversary* $\mathcal{A}$ *holding the register* A*, the following two oracles 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*

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

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:

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

where the view state is

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

and the view of the same adversary $\mathcal{A}$ who makes t queries to the oracle HPO and the unitary G:

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

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 18 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.

HP-Relation States We define the following relation states on H and P.

Definition 19 (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 $x^{\oplus 1} = \overline{x}$ 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.

For the set $\mathfrak{R}^{\mathrm{DB}}$ of restricted relations, the corresponding relation states form an orthogonal basis, whose proof is given in Appendix A.

Lemma 20. *$\{|\phi_R\rangle\}_{R\in\mathfrak{R}^{\mathrm{DB}}}$ forms a set of orthogonal vectors.*

Action of HPO Using the HP-relation states, the action of the HPO oracle is described by the following lemma.

Lemma 21. *For $0 \le t \le N$, $x \in \{0,1\}^n$ 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

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

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

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

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

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

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

$$H_f |\sigma(x)\rangle = \left(\sum_{y\in\{0,1\}^n, b\in\{0,1\}} \langle y| H_f |y^{\oplus b}\rangle \, |y\rangle\langle y^{\oplus b}| \right) \cdot \left(\sum_{y\in\{0,1\}^n} \delta_{y=\sigma(x)} |y\rangle \right)$$

$$= \sum_{y\in\{0,1\}^n, b\in\{0,1\}} \langle y|\, H_f\, |y^{\oplus b}\rangle\, \delta_{y^{\oplus b}=\sigma(x)}\, |y\rangle \quad .$$

Inserting this into (9), we have

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

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

Corollary 22. *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 $\mathcal{A}$ has finished all the queries to be*

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

Then we have:

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

4.3 The Path-Recording Oracle PR

We now present the definition of our new path-recording oracle PR, which is similar to that in [MH25]. The difference is that each time we query on x, our oracle PR samples a $y \notin \mathrm{BIm}(R)$ whose block differs from the blocks of all previous y's in R.

Definition 23 (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 $R \in \mathfrak{R}^{\mathrm{DB}}$,

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

Fact 24. *For an n-qubit unitary operator G and a t-query adversary $\mathcal{A}$ with query access to $\mathsf{PR}\cdot G$, define the state after $\mathcal{A}$ has finished all the queries to be*

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

Then we have:

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

Similar to [MH25, Lemma 4.3], our new path-recording oracle has the *right invariance* property, whose proof is given in Appendix B.

Lemma 25 (Right invariance property). *For an arbitrary n-qubit unitary operator G, we have that*

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

Moreover, if the oracle PR is preceded by a random scrambler and a random permutation, then the adversary's record lies almost entirely in the desired *distinct block subspace*.

Lemma 26. *Let $\mathcal{R}$ be a distribution over $\mathrm{U}(N)$ such that for $K\leftarrow\mathcal{R}$, $K^\dagger$ is an ϵ-RSS with $\epsilon = O\left(\frac{1}{N^2}\right)$. Define $\mathcal{D}$ to be the distribution that samples $G = PK$ where $P\leftarrow\mathcal{S}_N$ is a random permutation unitary and $K\leftarrow\mathcal{R}$. Let*

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

then

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

Proof. By Lemma 25, we can rewrite $\rho^{\mathcal{D}}$ as

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

Then by Lemma 12, we have

$$\begin{aligned}
&\mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)}\cdot\rho_{\mathsf{ABXY}}^{\mathcal{D}}\right)\\
&= \mathrm{Tr}\left(\Pi_{\mathsf{X}}^{(t)}\cdot\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t})\cdot|A_t^{\mathsf{PR}}\rangle\langle A_t^{\mathsf{PR}}|_{\mathsf{ABXY}}\cdot(G_{\mathsf{X}_1}\otimes\ldots\otimes G_{\mathsf{X}_t})^\dagger\right]\right)\\
&\geq 1 - O\left(\frac{t^2}{N}\right) \quad .
\end{aligned}$$

□

4.4 Connecting HPO and PR via Compress Isometry

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 27. *We define an isometry* $\mathsf{Compress} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{H}} \to \mathcal{H}_{\mathsf{X}} \otimes \mathcal{H}_{\mathsf{Y}}$ *as:*

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

Lemma 28. *Define the projector onto the* distinct block subspace *of* HP*-relation states by*

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

We have that for every n-qubit unitary G,

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

Proof. By Corollary 22, it is easy to see that

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

By Fact 24, we have

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

Therefore, we observe that

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

where

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

Using the above lemma, we show that for a suitably sampled unitary G, an adversary's views before and after applying the projector $\widetilde{\Pi}^{(t)}_{\mathsf{HP}}$ are close.

Lemma 29. *Let $\mathcal{R}$ be a distribution over $\mathrm{U}(N)$ such that for $K \leftarrow \mathcal{R}$, $K^\dagger$ is an ϵ-RSS 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. Write*

$$\sigma := \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{HPO} \cdot G} \rangle\langle \mathcal{A}_t^{\mathsf{HPO} \cdot G}|_{\mathsf{ABHP}} \right] \quad .$$

Then we have

$$\left\| \mathrm{Tr}_{\mathsf{HP}}(\sigma) - \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot \sigma \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \right) \right\|_1 = O\left(\frac{t^2}{N} \right) \quad .$$

Proof. We first apply Lemma 2:

$$\left\| \mathrm{Tr}_{\mathsf{HP}}(\sigma) - \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot \sigma \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \right) \right\|_1 = 1 - \mathrm{Tr}\left(\widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot \sigma \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \right) \quad .$$

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

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

where the second equality uses Lemma 28 and the last uses Lemma 26. □

4.5 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 30. *Let $\mathcal{R}$ be a distribution over $\mathrm{U}(N)$ such that for $K \leftarrow \mathcal{R}$, $K^\dagger$ is an ϵ-RSS 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*

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

Proof. We start by defining the following states:

$$\begin{aligned}
\rho_0 &= \mathop{\mathbb{E}}_{H_f P_\sigma \leftarrow \mathsf{HP}_{n,1}, G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{H_f P_\sigma G} \rangle\langle \mathcal{A}_t^{H_f P_\sigma G}| \right] \\
\rho_1 &= \mathrm{Tr}_{\mathsf{HP}}\left(\mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{HPO} \cdot G} \rangle\langle \mathcal{A}_t^{\mathsf{HPO} \cdot G}|_{\mathsf{ABHP}} \right] \right) \\
\rho_2 &= \mathrm{Tr}_{\mathsf{HP}}\left(\widetilde{\Pi}_{\mathsf{HP}}^{(t)} \cdot \mathop{\mathbb{E}}_{G \leftarrow \mathcal{D}} \left[|\mathcal{A}_t^{\mathsf{HPO} \cdot G} \rangle\langle \mathcal{A}_t^{\mathsf{HPO} \cdot G}|_{\mathsf{ABHP}} \right] \cdot \widetilde{\Pi}_{\mathsf{HP}}^{(t)} \right)
\end{aligned}$$

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

$$\rho_4 = \mathrm{Tr}_{\mathsf{XY}}\left(\mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}}\right]\right) \qquad \rho_5 = \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}}\right)$$

By Fact 18, $\rho_0 = \rho_1$. By Lemma 29, $\|\rho_1 - \rho_2\|_1 \le O\left(\frac{t^2}{N}\right)$. By Lemma 28 and the fact that Compress acts only on the environment register, we have that $\|\rho_2 - \rho_3\|_1 = O\left(\frac{t^2}{N}\right)$. By Lemma 26 and Lemma 2, $\|\rho_3 - \rho_4\|_1 \le O\left(\frac{t^2}{N}\right)$. Finally,

$$\begin{aligned}\rho_4 &= \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle\langle\mathcal{A}_t^{\mathsf{PR}\cdot G}|_{\mathsf{ABXY}}\right)\right] \\ &= \mathop{\mathbb{E}}_{G\leftarrow\mathcal{D}}\left[\mathrm{Tr}_{\mathsf{XY}}\left(G_{\mathsf{X}}^{\otimes t}\cdot|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}}\cdot G_{\mathsf{X}}^{\otimes t,\dagger}\right)\right] = \mathrm{Tr}_{\mathsf{XY}}\left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|_{\mathsf{ABXY}}\right) = \rho_5 \ ,\end{aligned}$$

where the second equality follows from Lemma 25. Combining the above bounds with the triangle inequality proves the lemma. □

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

Proof of Theorem 16. 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,

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

Since Kac is sampled from $\mathsf{HP}_{n,T}$ and $S \leftarrow \mathcal{S}_N$, by Theorem 15 and Lemma 30,

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

Now substitute Kac with a Haar random unitary U and we have

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

Since U is a 0-RSS and $S \leftarrow \mathcal{S}_N$, we have that by Lemma 30

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

Then by the triangle inequality, we have

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

This proves the theorem. □

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 31. *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 14 and Theorem 16, 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. □

A closer look at our analysis actually reveals a more general and abstract statement. Namely, given a distribution over unitaries, we identify a property which approximates Haar random unitary under a specific twirling operation. As soon as this property holds, composing it with a single step of the parallel Kac's walk would produce a PRU. This readily implies a number of instantiations and can help mechanize the design of PRU.

Theorem 32. *Let* V *be an* n*-qubit unitary sampled from the distribution* $\mathsf{HP}_{n,1}$ *(i.e., a single step of parallel Kac's walk). Let* $\Pi^{\mathsf{eq}} := \sum_{x\in\{0,1\}^n} |x,x\rangle\langle x,x|$*. Suppose a unitary* K *is sampled from a distribution* $\mathcal{R}$ *over* $\mathrm{U}(N)$ *such that*

$$\left\| \mathop{\mathbb{E}}_{K} \left[(K\otimes K)^\dagger \cdot \Pi^{\mathsf{eq}} \cdot (K\otimes K) \right] \right\|_\infty \leq \delta \ .$$

Then, for any adversary making at most t *queries,* VK *is indistinguishable from a Haar random unitary except with advantage at most* $O(t^2\delta + t^2/N)$*. Some examples of instantiations of* K *are below.*

- K *is a* δ*-approximate unitary* 2*-design, or*
- $K^\dagger$ *is an* $O(\delta/N)$-RSS*. For instance, for* $K \leftarrow \mathsf{HP}_{n,T=30n}$*,* $K^\dagger$ *has the same distribution, and hence satisfies it.*

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

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

Theorem 33 ($\mathsf{HP}_{n,2T+1}$ is a statistical strong-PRU). *Let* $\mathcal{A}$ *be a* t*-query oracle adversary performing both forward and inverse queries to oracle* $\mathcal{O}$*, and let* $\mathsf{HP}_{n,2T+1}$ *be defined as in Definition 13 with* $T = 30n$ *and* $d = 5n$*. Then*

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

This theorem establishes the statistical strong security. Assuming post-quantum secure OWFs, it then implies the existence of computationally strong PRUs. The proof of this theorem follows a similar routine to Theorem 16:

- 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 $D \cdot \mathsf{HPO} \cdot C$ and querying a path-recording oracle V introduced in Section 5.3. Here C and D are sampled from either $\mathsf{HP}_{n,T}$ or Haar distribution μ to ensure that the environment state is mostly within the distinct block subspace. We require two unitary operators to achieve this purpose, as the adversary can make both forward and inverse queries.
– Finally, we apply the above indistinguishability result to two cases. If $C, D \leftarrow \mathsf{HP}_{n,T}$, then querying $D \cdot \mathsf{HPO} \cdot C$ is equivalent to querying $\mathcal{O} \leftarrow \mathsf{HP}_{n,2T+1}$. On the other hand, if $C, D \leftarrow \mu$, then querying $D \cdot \mathsf{HPO} \cdot C$ is equivalent to querying $\mathcal{O} \leftarrow \mu$. Hence, both query cases can be reduced to the same path-recording oracle V, and Theorem 33 follows from the triangle inequality.

Similarly to Theorem 32, we can distill from our proof a stronger security condition for a distribution of unitaries, which approximates Haar random unitary under a larger family of twirling operations. Composing such a distribution of unitaries with an additional round of parallel Kac's walk yields a strong PRU.

Theorem 34. *Let V be an n-qubit unitary sampled from the distribution $\mathsf{HP}_{n,1}$. Define $\Pi^{\mathsf{eq}} := \sum_{x\in\{0,1\}^n} |x,x\rangle\langle x,x|$ and $\Pi^{\mathsf{EPR}} := \frac{1}{N}\sum_{x,y\in\{0,1\}^n} |x,x\rangle\langle y,y|$. Suppose K is sampled from a distribution $\mathcal{R}$ over $\mathrm{U}(N)$ such that*

$$\left\| \mathop{\mathbb{E}}_{K} \left[A \cdot \Pi^{\mathsf{eq}} \cdot A^\dagger \right] \right\|_\infty \leq \delta \quad \text{for all } A \in \{K \otimes K, (K \otimes K)^\dagger\} \ ,$$

and

$$\left\| \mathop{\mathbb{E}}_{K} \left[B \cdot (\Pi^{\mathsf{eq}} - \Pi^{\mathsf{EPR}}) \cdot B^\dagger \right] \right\|_\infty \leq \delta \quad \text{for all } B \in \{K \otimes \overline{K}, (K \otimes \overline{K})^\dagger\} \ .$$

Then, for any adversary making at most t forward and inverse queries, $K_2 V K_1$, with $K_1, K_2 \leftarrow \mathcal{R}$ independently, is indistinguishable from a Haar random unitary except with advantage at most $O(t^2 \cdot (\delta + 1/\sqrt{N})^{1/4})$. Concretely, the following are examples of instantiations of K.

– *K is a δ-approximate unitary 2-design, or*
– *$K \leftarrow \mathsf{HP}_{n,T=30n}$ is an $O(n)$-round parallel Kac's walk.*

Below, we first extend the HPO oracle and the HP-relation states to handle 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 an intermediate operator to connect the action of HPO and the path-recording oracle V defined in Section 5.3. Finally, we prove Theorem 33 in Section 5.4.

5.1 Action of HPO Oracle and Its Inverse

We start by adding inverse query to the HPO oracle.

Definition 35 (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*

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

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

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

As in Fact 18, querying $H_f \cdot P_\sigma$ and querying HPO are identical in the adversary's view:

Fact 36. *For any adversary* $\mathcal{A}$ *holding the register* A*, the following two oracles 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 37 (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*

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

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

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

Lemma 39. *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 C.

5.2 Partial Path-Recording Oracle W

We first introduce some relevant notation from [MH25]. 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 an 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 $(M_{\le t,\mathsf{LR}})^{\dagger}$. For any unitary U, define $U^{\otimes *} := \sum_{t=0}^{\infty} U^{\otimes t}$.

Definition 40. *Let L, R be 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

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

Thus

$$W^\dagger \cdot W = W^{L,\dagger} \cdot W^L + W^R \cdot W^{R,\dagger} \ . \tag{10}$$

Therefore $W \cdot W^\dagger \cdot W = W$, which implies W is a partial isometry.

Notation 41. *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* $\mathrm{Im}\,(G)$.

Up to the partial isometry $\mathsf{Compress} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{L}} \otimes \mathcal{H}_{\mathsf{R}}$ defined by

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

the oracle W is an approximate restriction of HPO:

Lemma 42. *For $0 \le t < N$,*

$$\left\| W_{\le t} - \mathsf{Compress} \cdot \mathsf{HPO} \cdot \mathsf{Compress}^\dagger \cdot \Pi^{\mathrm{Dom}(W)} \cdot \Pi_{\le t} \right\|_\infty \le \frac{2t}{N-t} \ , \tag{11}$$

$$\left\| (W^\dagger)_{\le t} - \mathsf{Compress} \cdot \mathsf{HPO}^\dagger \cdot \mathsf{Compress}^\dagger \cdot \Pi^{\mathrm{Im}(W)} \cdot \Pi_{\le t} \right\|_\infty \le \frac{2t}{N-t} \ . \tag{12}$$

Proof. We will prove Eq. (11), and Eq. (12) follows from a symmetric argument. Denote

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

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

and

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

Then by Eq. (10), $X = X^L + X^{R,\dagger}$. To prove Eq. (11), it suffices to prove

$$\left\| W^L_{\le t} - X^L \right\|_\infty \le \frac{t}{N-t} \quad \text{and} \quad \left\| (W^{R,\dagger})_{\le t} - X^{R,\dagger} \right\|_\infty \le \frac{t}{N-t} \ . \tag{13}$$

Next, we prove the first inequality in Eq. (13). The other inequality follows from a symmetric argument. For L, R such that $L \cup R \in \mathfrak{R}^{\mathrm{DB}}$ and $|L \cup R| \le t$, and $x \in \{0,1\}^n$ such that $x \notin \mathrm{BDom}\,(L \cup R)$, we have

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

and

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

Then for such x, L, R, we have

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

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

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

This completes the proof. □

5.3 Path-Recording Oracle V

Definition 43. *Let $L, R\in\mathfrak{R}$. We define operators V^L and V^R to be the linear maps such that for $x\in\{0,1\}^n$,*

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

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

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

The path-recording oracle V is defined to be

$$V = V^L\cdot(\mathbb{1}-V^R\cdot V^{R,\dagger})+(\mathbb{1}-V^L\cdot V^{L,\dagger})\cdot V^{R,\dagger} \ . \tag{14}$$

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.,

$$V^L \cdot \Pi^{\mathrm{Dom}(W^L)} = W^L \quad \text{and} \quad \Pi^{\mathrm{Im}(W^R)} \cdot V^R = W^R \ . \tag{15}$$

Also, we have

$$W^L \cdot V^R = W^R \cdot V^L = 0 \ . \tag{16}$$

Claim 44. *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, which is true if and only if $(\mathbb{1} - V^R \cdot V^{R,\dagger}) \cdot V^{L,\dagger} \cdot V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger})$ is a projector. It suffices to show that $V^{L,\dagger} \cdot V^L$ and $V^R \cdot V^{R,\dagger}$ commute. By the definition of V^L, $V^{L,\dagger} \cdot V^L = \mathbb{1}_{\mathsf{A}} \otimes \Pi_{\leq N-1,\mathsf{LR}}$. 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 $\mathbb{1}_{\mathsf{A}} \otimes \Pi_{\leq N-1,\mathsf{LR}}$. Moreover, we know that $(\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ is also a partial isometry by a similar argument.

To show that V is a partial isometry, we then show that the domains of $V^L \cdot (\mathbb{1} - V^R \cdot V^{R,\dagger})$ and $(\mathbb{1} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ are orthogonal. Indeed, these domains lie within the subspaces $\mathbb{1} - \Pi^{\mathrm{Im}(V^R)}$ and $\Pi^{\mathrm{Im}(V^R)}$, respectively, and are therefore orthogonal. □

We formalize the fact that W is a restriction of V in the following lemma.

Lemma 45.

$$W = V \cdot \Pi^{\mathrm{Dom}(W)} \ , \tag{17}$$

$$W^\dagger = V^\dagger \cdot \Pi^{\mathrm{Im}(W)} \ . \tag{18}$$

Proof. To prove Eq. (17), it suffices to show that

$$W^L = V \cdot \Pi^{\mathrm{Dom}(W^L)} \ , \tag{19}$$

$$W^{R,\dagger} = V \cdot \Pi^{\mathrm{Im}(W^R)} \ . \tag{20}$$

By Eq. (10), Eq. (17) can be obtained by summing these two equations.

We now prove Eq. (19). By Eq. (14), 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. (16), we have

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

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. (15).

It remains to prove Eq. (20). By Eq. (14), 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. (15) and Eq. (16), we have

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

The proof of Eq. (18) follows from a similar argument. □

Two-sided Unitary Invariance The modified path-recording oracle V also admits an approximate two-sided unitary invariance as in [MH25, Section 8.3]. We state it below and provide the proof in Appendix D.

Definition 46. *For any two n-qubit unitaries C and D, define*

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

Lemma 47. *For any two n-qubit unitaries C and D, and for an integer $0 \leq t \leq N-1$,*

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

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

5.4 Main Proof

We are now prepared to prove Theorem 33, which demonstrates the strong security of our construction $\mathsf{HP}_{n,2T+1}$. We first show that our construction is indistinguishable from the path-recording oracle V.

Lemma 48 ($\mathsf{HP}_{n,2T+1}$ 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 13 with $T = 30n$ and $d = 5n$, and V be defined as in Definition 43. Then*

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

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

Lemma 49 (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*

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

In the following sections, we provide the details of the main lemma Lemma 48. 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 59). Lemma 49 follows from a similar argument. Finally, by applying the triangle inequality to Lemma 48 and Lemma 49, we conclude the proof of Theorem 33 at the end of this section.

V* Is Indistinguishable from *W Our goal here is to establish that even if the adversary can make queries from both directions, the path-recording oracle V is indistinguishable from $D \cdot W \cdot C$ for $C, D \leftarrow \mathcal{D}$, as long as $\mathcal{D}$ is one of the following two distributions:

Definition 50. *We define two distributions of unitaries:*

- $\mathcal{D}_1$*: 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 introduce some notation. Let

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

Definition 51 (Controlled C, D and Q). *Define the following operators:*

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

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

We then define the quantum states after querying the twirled-W and V.

Definition 52 (Purification of Twirled-W). *We define the adversary state* $|\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$ *after the* i*-th query to twirled-*W *as follows:*

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

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

where

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

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

– *For* $1 \le i \le t$,

$$|\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \coloneqq \Big((1-b_i)\cdot(\mathsf{cD}\cdot W\cdot \mathsf{cC}) + b_i\cdot(\mathsf{cD}\cdot W\cdot \mathsf{cC})^\dagger\Big)\cdot A_i\cdot|\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle$$

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

Definition 53 (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* $i = 0$,

$$|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} \coloneqq |0^n0^m\rangle_{\mathsf{AB}}\,|\{\}\rangle_{\mathsf{L}}\,|\{\}\rangle_{\mathsf{R}}$$

– *For* $1 \le i \le t$,

$$|\mathcal{A}_i^V\rangle_{\mathsf{ABLR}} \coloneqq \big((1-b_i)\cdot V + b_i\cdot V^\dagger\big)\cdot A_i\cdot|\mathcal{A}_{i-1}^V\rangle$$

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

Fact 54 (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 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 55 (Spaces containing purified states)**.** *By definition, 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* $\Pi_{\le t}^{\mathfrak{R}^2}$*.*

We now state the following claim, which shows that the state produced by twirled-W is almost the same as that from V, up to a local unitary transformation acting only on the registers LRCD. The proof of this claim follows a similar argument to that of [MH25, Claim 18], with the full details provided in Appendix E.

Claim 56. *For any integer* $t \ge 0$*, and* $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ *as defined in Definition 50*

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

Now, we are ready to prove the indistinguishability between oracles V and twirled W.

Lemma 57. *For any* $0 \le t < N$ *and* $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ *as defined in Definition 50,*

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

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

$$\begin{aligned}
&\mathrm{TD}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}, \mathsf{cQ}_{\mathsf{LRCD}}\cdot\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}}\otimes|\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}}\right)\cdot\mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right)^2\\
&\le \left\||\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLR}} - \mathsf{cQ}_{\mathsf{LRCD}}\cdot\left(|\mathcal{A}_t^V\rangle_{\mathsf{ABLR}}\otimes|\mathsf{init}(\mathcal{D})_{\mathsf{CD}}\rangle\right)\right\|_2^2
\end{aligned}$$

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

Since unitary cQ only acts on registers $\mathsf{L}, \mathsf{R}, \mathsf{C}, \mathsf{D}$,

$$
\begin{aligned}
&\mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \right), \mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \right) \right) \\
&= \mathrm{TD}\Bigg(\mathrm{Tr}_{-\mathsf{AB}} \left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}} \right), \\
&\qquad\qquad \mathrm{Tr}_{-\mathsf{AB}} \left(\mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}} \right) \cdot \mathsf{cQ}_{\mathsf{LRCD}}^{\dagger} \right) \Bigg) \\
&\leq \mathrm{TD}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}, \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathcal{D})\rangle\langle\mathsf{init}(\mathcal{D})|_{\mathsf{CD}} \right) \cdot \mathsf{cQ}_{\mathsf{LRCD}}^{\dagger} \right) \\
&\leq \frac{9t}{N^{1/8}} \ .
\end{aligned}
$$

□

Claim 56 also gives a bound on the norm of $|\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}$.

Lemma 58. *For any $0 \leq t < N$ and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 50, we have*

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

Proof. We have

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

where the first inequality uses the fact that $|\mathcal{A}_t^{V}\rangle$ has norm at most 1, the second one is from the Cauchy-Schwarz inequality, and the last one is from Claim 56. □

***W* Is Indistinguishable from HPO** In this section, we show that after twirling, adversaries cannot distinguish the HPO oracle from W (Lemma 63). We first define the purification of twirled-HPO oracle and then connect it with twirled-W (Definition 52) via some projection.

Definition 59 (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 $i = 0$,*

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

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

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

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

– *For $1 \le i \le t$,*

$$|\mathcal{A}_i^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}} \coloneqq \Big((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{HPO}\cdot\mathsf{cC}) + b_i\cdot(\mathsf{cD}\cdot\mathsf{HPO}\cdot\mathsf{cC})^\dagger\Big)\cdot A_i\cdot|\mathcal{A}_{i-1}^{\mathsf{HPO},\mathcal{D}}\rangle$$

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

Definition 60. *Define the projectors*

$$\widetilde{\Pi}^{\mathrm{Dom}(W)} \coloneqq \mathsf{Compress}^\dagger \cdot \Pi^{\mathrm{Dom}(W)} \cdot \mathsf{Compress}\ ,$$
$$\widetilde{\Pi}^{\mathrm{Im}(W)} \coloneqq \mathsf{Compress}^\dagger \cdot \Pi^{\mathrm{Im}(W)} \cdot \mathsf{Compress}\ .$$

Definition 61 (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 $i = 0$, $|\mathcal{A}_0^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle \coloneqq |\mathcal{A}_0^{\mathsf{HPO},\mathcal{D}}\rangle$*
– *For $1 \le i \le t$,*

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

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

Claim 62. *For all integers $0 \le t \le N/2$,*

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

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

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

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

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

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}
&\left\| |\mathcal{A}_i^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress}_{\mathsf{HP}} \cdot |\mathcal{A}_i^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 \\
= &\left\| \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}} \right. \\
&\qquad \left. - \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{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 \\
= &\left\| \mathsf{cD} \cdot W_{\le i-1} \cdot \mathsf{cC} \cdot A_i \, |\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} \right. \\
&\qquad \left. - \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{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 \\
\le &\left\| \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}} \right. \\
&\qquad \left. - \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{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 + \frac{2i-2}{N-i+1} \\
= &\left\| \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}} \right. \\
&\qquad \left. - \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{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 + \frac{2i-2}{N-i+1} \\
\le &\left\| |\mathcal{A}_{i-1}^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - \mathsf{Compress} \cdot |\mathcal{A}_{i-1}^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle \right\|_2 + \frac{4i}{N} \\
\le &\frac{2i(i-1)}{N} + \frac{4i}{N} \quad = \frac{2i(i+1)}{N} \ ,
\end{aligned}$$

where the first inequality is by Lemma 42 and the last one is by induction. □

We are ready to prove the indistinguishability between oracles W and HPO:

Lemma 63. *For all integers $0 \le t \le N$, and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 50*

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

Proof. Recall the state $|\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}$ defined in Definition 61. By the triangle inequality, we have

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

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

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 $\left\||\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 = 1$ and $\left\||\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \le 1$. Since $\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \le 2\,\||u\rangle - |v\rangle\|_2$ for $\|u\|_2 \le 1$ and $\|v\|_2 \le 1$, we have

$$\begin{aligned}
(\star) &\le \mathrm{TD}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABLRCD}}, |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}|_{\mathsf{ABHPCD}}\right) \\
&\le \left\||\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle_{\mathsf{ABLRCD}} - |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \\
&\le t \cdot \sqrt{1 - \left\||\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2^2} ,
\end{aligned} \tag{21}$$

where the last inequality is from the gentle measurement lemma in Lemma 3. Notice that, since Compress is an isometry, we have

$$\begin{aligned}
\left\||\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 &= \left\|\mathsf{Compress} \cdot |\mathcal{A}_t^{\widetilde{\mathsf{HPO}},\mathcal{D}}\rangle_{\mathsf{ABHPCD}}\right\|_2 \\
&\ge \left\||\mathcal{A}_t^{W,\mathcal{D}}\rangle_{\mathsf{ABLRCD}}\right\|_2 - \frac{2t(t+1)}{N} \\
&\ge 1 - \frac{38t^2}{N^{1/4}} - \frac{2t(t+1)}{N} \\
&\ge 1 - \frac{40t(t+1)}{N^{1/4}} ,
\end{aligned} \tag{22}$$

where the first inequality is from the triangle inequality and Claim 62, and the second one is from Lemma 58. Combining Eqs. (21) and (22), we have

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

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

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

$$\leq \frac{2t(t+1)}{N} \ ,$$

where the second inequality is from the fact that $\| |u\rangle\langle u| - |v\rangle\langle v| \|_1 \leq 2 \| |u\rangle - |v\rangle \|_2$ for $\|u\|_2 \leq 1$ and $\|v\|_2 \leq 1$, and the last one is from Claim 62. □

The Strong Security of HPO Now, we complete the main proof of Theorem 33 by mainly establishing Lemma 48 and Lemma 49 that both our construction and Haar distribution are indistinguishable from V.

Proof of Lemma 48. Consider $\mathcal{D} = \mathcal{D}_2$ defined in Definition 50. First, due to the perfect indistinguishability between the standard oracle and its purified version (Fact 18),

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

And, from Lemma 57, we get

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

Then, according to Lemma 63, we have

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

Thus, via the triangle inequality, we show:

$$\begin{aligned}&\mathrm{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{HP}_{n,2T+1}}\left[|\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}\right], \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right) \\ &= \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABHPCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right) \\ &\leq \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right)\right) \\ &\quad + \mathrm{TD}\left(\mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}\rangle\langle\mathcal{A}_t^{\mathsf{HPO},\mathcal{D}}|_{\mathsf{ABLRCD}}\right), \mathrm{Tr}_{-\mathsf{AB}}\left(|\mathcal{A}_t^{W,\mathcal{D}}\rangle\langle\mathcal{A}_t^{W,\mathcal{D}}|_{\mathsf{ABLRCD}}\right)\right) \\ &\leq \frac{11t^2+20t}{N^{1/8}} \ .\end{aligned}$$

□

The argument above also proves Lemma 49 by considering $\mathcal{D} = \mathcal{D}_1$ as defined in Definition 50. Therefore, combining Lemma 48 and Lemma 49 yields Theorem 33. We can finally conclude that our construction, based on parallel Kac's walk, satisfies strong security against adversaries making inverse queries.

Theorem 64. *By replacing random functions and random permutations with their post-quantum secure pseudorandom counterparts in the sampling procedure of* $\widehat{\mathsf{HP}}_{n,2T+1}$ *where* $T = 30n$ *and* $d = 5n$*, we obtain a strong* PRU.

References

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

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In *Theory of Cryptography Conference – TCC 2022*, pages 237–265. Springer, 2022.

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

[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*, Leibniz International Proceedings in Informatics (LIPIcs), pages 63:1–63:2. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.

[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.

[BHHP25] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states. In Bill Fefferman, editor, *20th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2025)*, volume 350 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:18, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BM24] Zvika Brakerski and Nir Magrafta. Real-valued somewhat-pseudorandom unitaries. In *Theory of Cryptography Conference – TCC 2024*, pages 36–59. Springer, 2024.

[BS19] Zvika Brakerski and Omri Shmueli. (Pseudo) random quantum states with binary phase. In *Theory of Cryptography Conference – TCC 2019*, pages 229–250. Springer, 2019.

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

[CCL03] Eric A. Carlen, Mario C. Carvalho, and Michael Loss. Determination of the spectral gap for Kac's master equation and related stochastic evolution. *Acta Mathematica*, 191(1):1–54, Mar 2003.

[CSBH25] Laura Cui, Thomas Schuster, Fernando Brandao, and Hsin-Yuan Huang. Unitary designs in nearly optimal depth. arXiv:2507.06216, 2025.

[GTB23] Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states. arXiv:2312.09206, 2023.

[Har13] Aram W. Harrow. The church of the symmetric subspace. arXiv:1308.6595, 2013.

[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.

[Jan01] Elise Janvresse. Spectral gap for Kac's model of Boltzmann equation. *The Annals of Probability*, 29(1):288–304, 2001.

[Jan03] Elise Janvresse. Bounds on semigroups of random rotations on SO(n). *Theory of Probability & Its Applications*, 47(3):526–532, 2003.

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

[JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Pseudorandom and pseudoentangled states from subset states. arXiv:2312.15285, 2023.

[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.

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

[LQS+26] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. *SIAM Journal on Computing*, 55(4):787–850, 2026.

[Mas03] David K. Maslen. The eigenvalues of Kac's master equation. *Mathematische Zeitschrift*, 243(2):291–331, Feb 2003.

[MH25] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing – STOC 2025*, pages 806–809, 2025. Full paper at arXiv preprint arXiv:2410.10116.

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

[Oli09] Roberto Imbuzeiro Oliveira. On the convergence to equilibrium of Kac's random walk on matrices. *The Annals of Applied Probability*, 19(3):1200–1231, 2009.

[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.

[PS18] Natesh S. Pillai and Aaron Smith. On the mixing time of Kac's walk and other high-dimensional Gibbs samplers with constraints. *The Annals of Probability*, 46(4):2345–2399, 2018.

[PS26] Natesh S. Pillai and Aaron Smith. Kac's walk on rotation matrices mixes in $n^2 \log n$ steps. arXiv:2604.23828, 2026.

[SHH25] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *Science*, 389(6755):92–96, 2025.

[Son17] Fang Song. Quantum-secure pseudorandom permutations, 2017. Blog post: https://qcc.fangsong.info/2017-06-quantumprp.

[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.

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

[Zha25] Mark Zhandry. A note on quantum-secure PRPs. *Quantum*, 9:1696, April 2025.

A Proof of Lemma 20

Lemma 20. $\{|\phi_R\rangle\}_{R\in\mathfrak{R}^{\mathrm{DB}}}$ *forms a set of orthogonal vectors.*

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

Lemma 62. *For any* $x \in \{0,1\}^n$,

1. $\mathbb{E}_f[\langle x| H_f |x\rangle] = \mathbb{E}_f[\langle x| H_f |\bar{x}\rangle] = 0$;
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. Note that $\langle x| H_f |x\rangle = \mathrm{e}^{\mathrm{i}\alpha_y}\cos\theta_y$ and $\langle x| H_f |\bar{x}\rangle = -\mathrm{e}^{\mathrm{i}\beta_y}\sin\theta_y$. Item 1 holds, since $\mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}\alpha_y}\right] = \mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}\beta_y}\right] = 0$
2. Note that $\overline{\langle x| H_f |x\rangle}\,\langle x| H_f |\bar{x}\rangle = -\mathrm{e}^{\mathrm{i}(\beta_y-\alpha_y)}\sin\theta_y\cos\theta_y$. Item 2 holds, since $\mathbb{E}_f\left[\mathrm{e}^{\mathrm{i}(\beta_y-\alpha_y)}\right] = 0$.
3. Note that $\overline{\langle x| H_f |x\rangle}\,\langle \bar{x}| H_f |\bar{x}\rangle = \mathrm{e}^{-2\mathrm{i}\alpha_y}\cos^2\theta_y$ and $\overline{\langle x| H_f |\bar{x}\rangle}\,\langle \bar{x}| H_f |x\rangle = -\mathrm{e}^{-2\mathrm{i}\beta_y}\sin^2\theta_y$. 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 20. Consider two relations $R, S \in \mathfrak{R}^{\mathrm{DB}}$, where $R = \{(x_1, y_1), \ldots, (x_{|R|}, y_{|R|})\}$ and $S = \left\{(x'_1, y'_1), \ldots, (x'_{|S|}, y'_{|S|})\right\}$. By Lemma 62 item 1, if $|R| \neq |S|$, then $\langle\phi_R|\phi_S\rangle = 0$. So we may assume $|R| = |S| = t$. Then

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

There are two cases to consider:

– $R = S$. Then by Lemma 62 item 2 and the fact that

$$|\langle x| H_f |x\rangle|^2 + |\langle x| H_f |\bar{x}\rangle|^2 = 1$$

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 62 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 62 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 62 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 62 item 1, $\langle \phi_R | \phi_S \rangle = 0$. □

B Right Invariance Property

Lemma 25. *For an arbitrary n-qubit unitary operator G, we have that*

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

Proof. We have trivial identities for registers A and $\mathsf{X} = \mathsf{X}_1, \ldots, \mathsf{X}_t$.

$$\sum_{z \in \{0,1\}^n} |z\rangle\langle z|_{\mathsf{A}} = \mathsf{Id}_{\mathsf{A}} \tag{23}$$

$$\sum_{z \in \{0,1\}^n} |z\rangle\langle z|_{\mathsf{X}_i} = \mathsf{Id}_{\mathsf{X}_i} \ , \quad \forall i \in [t] \ . \tag{24}$$

For an arbitrary n-qubit unitary G and any $x, z \in \{0,1\}^n$, we trivially have the following scalar equality:

$$\langle x|_{\mathsf{A}} G_{\mathsf{A}} |z\rangle_{\mathsf{A}} = \langle x|_{\mathsf{X}_i} G_{\mathsf{X}_i} |z\rangle_{\mathsf{X}_i} \ . \tag{25}$$

Thus, we have

$$\begin{aligned}
\sum_{x \in \{0,1\}^n} |x\rangle_{\mathsf{X}_i} \otimes \langle x|_{\mathsf{A}} G_{\mathsf{A}} &= \sum_{x \in \{0,1\}^n} \left(|x\rangle_{\mathsf{X}_i} \otimes \langle x|_{\mathsf{A}} G_{\mathsf{A}} \left(\sum_{z \in \{0,1\}^n} |z\rangle\langle z|_{\mathsf{A}} \right) \right) \\
&= \sum_{x,z} |x\rangle_{\mathsf{X}_i} \otimes \left(\langle x|_{\mathsf{A}} G_{\mathsf{A}} |z\rangle_{\mathsf{A}} \right) \langle z|_{\mathsf{A}} \\
&= \sum_{x,z} |x\rangle_{\mathsf{X}_i} \otimes \left(\langle x|_{\mathsf{X}_i} G_{\mathsf{X}_i} |z\rangle_{\mathsf{X}_i} \right) \langle z|_{\mathsf{A}} \\
&= \sum_{x,z} \left(|x\rangle\langle x|_{\mathsf{X}_i} G_{\mathsf{X}_i} |z\rangle_{\mathsf{X}_i} \right) \otimes \langle z|_{\mathsf{A}} \\
&= \sum_{z} G_{\mathsf{X}_i} |z\rangle_{\mathsf{X}_i} \otimes \langle z|_{\mathsf{A}}
\end{aligned}$$

$$= \sum_{x\in\{0,1\}^n} G_{\mathsf{X}_i} |x\rangle_{\mathsf{X}_i} \otimes \langle x|_{\mathsf{A}} \quad , \tag{26}$$

where we apply (23) in the first equality, (25) in the third equality, (24) in the fifth equality, and simply relabel the variable in the last equality. Using this identity on each register X_i, we can rewrite the expression of Fact 24 as follows. For simplicity, let $\alpha_{N,t} = \sqrt{\prod_{i=0}^{t-1} \frac{1}{(N-2i)}}$. Then we have

$$\begin{aligned}
&|\mathcal{A}_t^{\mathsf{PR}\cdot G}\rangle_{\mathsf{ABXY}} \\
&= \alpha_{N,t} \cdot \sum_{\substack{(x_1,\ldots,x_t)\in(\{0,1\}^n)^t \\ (y_1,\ldots,y_t)\in \mathsf{DB}_t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}\right] \otimes |\{(x_i,y_i)\}_{i=1}^t\rangle_{\mathsf{XY}} \\
&= \alpha_{N,t} \cdot \sum_{\substack{(x_1,\ldots,x_t)\in(\{0,1\}^n)^t \\ (y_1,\ldots,y_t)\in \mathsf{DB}_t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}\right] \otimes \\
&\frac{1}{\sqrt{t!}} \sum_{\sigma\in S_t} (S_\sigma |x_1,\ldots,x_t\rangle_{\mathsf{X}}) \otimes (S_\sigma |y_1,\ldots,y_t\rangle_{\mathsf{Y}}) \qquad (27) \\
&= \alpha_{N,t} \cdot \sum_{\substack{(x_1,\ldots,x_t)\in(\{0,1\}^n)^t \\ (y_1,\ldots,y_t)\in \mathsf{DB}_t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot A_{\mathsf{AB}}^{(i)}\right) |0\rangle_{\mathsf{AB}}\right] \otimes \\
&\frac{1}{\sqrt{t!}} \sum_{\sigma\in S_t} \left(S_\sigma \cdot \left(G_{\mathsf{X}_1} |x_1\rangle_{\mathsf{X}_1} \otimes \ldots \otimes G_{\mathsf{X}_t} |x_t\rangle_{\mathsf{X}_t}\right)\right) \otimes (S_\sigma |y_1,\ldots,y_t\rangle_{\mathsf{Y}}) \qquad (28) \\
&= (G_{\mathsf{X}_1} \otimes \ldots \otimes G_{\mathsf{X}_t}) \cdot |\mathcal{A}_t^{\mathsf{PR}}\rangle_{\mathsf{ABXY}} \quad , \qquad (29)
\end{aligned}$$

where in (27), we rewrite the relation state on registers XY, using the fact that γ_R in (1) simplifies to $t!$ when all y_i in the set are distinct. We then apply (26) to obtain (28), and (29) follows from the fact that $(G_{\mathsf{X}_1} \otimes \cdots \otimes G_{\mathsf{X}_t})$ performs an identical operation on all t registers. □

C Proofs of Lemma 38 and Lemma 39

C.1 Proof of Lemma 38

Lemma 38. $\{|\phi_{L,R}\rangle\}_{L,R:L\cup R\in\mathfrak{R}^{\mathrm{DB}}}$ *forms a set of orthonormal vectors.*

Proof. Let $L = \{(x_1,y_1),\ldots,(x_l,y_l)\} \in \mathfrak{R}_l$, $R = \{(x'_1,y'_1),\ldots,(x'_r,y'_r)\} \in \mathfrak{R}_r$, $S = \{(x^*_1,y^*_1),\ldots,(x^*_s,y^*_s)\} \in \mathfrak{R}_l$, and $T = \left\{(x_1^{\triangle},y_1^{\triangle}),\ldots,(x_t^{\triangle},y_t^{\triangle})\right\} \in \mathfrak{R}_t$ 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,

$$\langle\phi_{L,R}|\phi_{S,T}\rangle = \frac{1}{2^{3d(n-1)}(N-l-r)!}\sum_{f,\sigma}\sum_{\substack{b,b^*\in\{0,1\}^l\\ b',b^\triangle\in\{0,1\}^r}}\prod_{i=1}^{l}\langle y_i^{\oplus b_i}|H_f^\dagger|y_i\rangle\delta_{y_i^{\oplus b_i}=\sigma(x_i)}$$
$$\cdot\prod_{i=1}^{r}\langle y_i'|H_f|{y_i'}^{\oplus b_i'}\rangle\delta_{{y_i'}^{\oplus b_i'}=\sigma(x_i')}\cdot\prod_{i=1}^{l}\langle y_i^*|H_f|{y_i^*}^{\oplus b_i^*}\rangle\delta_{{y^*}_i^{\oplus b_i^*}=\sigma(x_i^*)}$$
$$\cdot\prod_{i=1}^{r}\langle {y_i}^{\triangle\oplus b_i^\triangle}\mid H_f^\dagger\mid {y^\triangle}_i\rangle\,\delta_{{y_i}^{\triangle\oplus b_i^\triangle}=\sigma(x_i^\triangle)}\quad . \tag{30}$$

Case 1: $L = S = \{(x_1, y_1), \ldots, (x_l, y_l)\}$ *and* $R = T = \{(x_1', y_1'), \ldots, (x_r', y_r')\}$. Note that

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

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

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

$$= \mathop{\mathbb{E}}_{f}\Bigg[\frac{1}{(N-l-r)!}\sum_{\substack{b\in\{0,1\}^l\\ b'\in\{0,1\}^r}}\prod_{i=1}^{l}\langle y_i^{\oplus b_i}|H_f^\dagger|y_i\rangle\langle y_i|H_f|y_i^{\oplus b_i}\rangle$$

$$\cdot\prod_{i=1}^{r}\langle y_i'|H_f|y_i'^{\oplus b_i'}\rangle\langle y_i'^{\oplus b_i'}|H_f^\dagger|y_i'\rangle\cdot\sum_{\sigma}\prod_{i=1}^{l}\delta_{y_i^{\oplus b_i}=\sigma(x_i)}\cdot\prod_{i=1}^{r}\delta_{y_i'^{\oplus b_i'}=\sigma(x_i')}\Bigg]\ .$$

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,

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

Then, we have

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

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

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

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

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

- **Case 2.2:** $\mathrm{BIm}\,(L\cup R) = \mathrm{BIm}\,(S\cup T)$.
  - **Case 2.2.1:** $\mathrm{BIm}\,(L)\neq\mathrm{BIm}\,(S)$. Without loss of generality, we assume that y_1 and $\overline{y_1}$ are not in S. This means $y_1\in\left\{y_1^{\triangle},\ldots,y_t^{\triangle}\right\}$ or $\overline{y_1}\in\left\{y_1^{\triangle},\ldots,y_t^{\triangle}\right\}$.

* Suppose that $y_1 \in \left\{y_1^{\triangle}, \ldots, y_t^{\triangle}\right\}$. 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. (30) 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. (30) 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 $\overline{y_1} \in \left\{y_1^{\triangle}, \ldots, y_t^{\triangle}\right\}$. 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. (30) 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. (30) 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 2.2.2:** $\mathrm{BIm}(L) = \mathrm{BIm}(S)$. This means $\mathrm{BIm}(R) = \mathrm{BIm}(T)$ as well.
  * **Case 2.2.2.1:** $\{y_1, \ldots, y_l\} \neq \{y_1^*, \ldots, y_s^*\}$. 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. (30) 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. (30) 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 2.2.2.2:** $\{y_1', \ldots, y_r'\} \neq \left\{y_1^{\triangle}, \ldots, y_t^{\triangle}\right\}$. Similar to Case 2.2.2.1, we have $\langle \phi_{L,R} | \phi_{S,T} \rangle = 0$.

* **Case 2.2.2.3:** $\{y_1,\ldots,y_l\}=\{y_1^*,\ldots,y_s^*\}$ 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. (30) is zero when $b_1=b_1^*$. It is not hard to check $\langle\phi_{L,R}|\phi_{S,T}\rangle=0$, since

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

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

C.2 Proof of Lemma 39

Lemma 39. *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 $x\in\{0,1\}^n$*

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

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 21, we know

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

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

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

$$= \frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i|H_f|y_i^{\oplus b_i}\rangle \delta_{y_i^{\oplus b_i}=\sigma(x_i)}$$

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

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

Similarly, we have

$$\mathsf{HPO}_{\mathsf{AHP}}^\dagger |y\rangle_{\mathsf{A}} |\phi_{L,R}\rangle_{\mathsf{HP}}$$

$$= \frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i|H_f|y_i^{\oplus b_i}\rangle \delta_{y_i^{\oplus b_i}=\sigma(x_i)}$$

$$\prod_{i=1}^{r} \langle {y'}_i^{\oplus b'_i}|H_f^\dagger|y'_i\rangle \delta_{{y'}_i^{\oplus b'_i}=\sigma(x'_i)} \cdot \mathsf{HPO}_{\mathsf{AHP}}^\dagger |y\rangle_{\mathsf{A}} |f\rangle_{\mathsf{H}} |\sigma\rangle_{\mathsf{P}}$$

$$= \frac{1}{\sqrt{2^{3d(n-1)}(N-l-r)!}} \sum_{f,\sigma} \sum_{\substack{b\in\{0,1\}^l \\ b'\in\{0,1\}^r}} \prod_{i=1}^{l} \langle y_i|H_f|y_i^{\oplus b_i}\rangle \delta_{y_i^{\oplus b_i}=\sigma(x_i)}$$

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

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

D Approximate Two-Side Unitary Invariance

We will show that the path-recording oracle V defined in Definition 43 satisfies an approximate unitary invariance property in this section. Formally, we have

Lemma 47. *For any two n-qubit unitaries C and D, and any integer $0 \le t \le N-1$,*

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

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

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 [MH25, Section 10.1] that have exact two-side unitary invariance property. We first give the definition of E^L and E^R.

Definition 63. *E^L and E^R are linear maps on register* A, L *and* R *such that*

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

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

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 64 (Claim 20 in [MH25]). *For any two n-qubit unitaries C and D,*

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

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 65. *For any integer* $0\le t\le N-1$,

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

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

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

we have

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

Note that

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

$$+ \underbrace{\sum_{\substack{x\in\{0,1\}^n \\ L,R\in\mathfrak{R} \text{ s.t. } |L\cup R|\le t}} \alpha_{x,L,R} \sum_{\substack{y\in\{0,1\}^n \\ y\in \mathrm{BIm}(L\cup R)}} \left(-\frac{\sqrt{\mathrm{num}(L,(x,y))+1}}{\sqrt{N}}\right) |y\rangle\,|L\cup\{(x,y)\}\rangle\,|R\rangle}_{|v\rangle} \ .$$

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

$$\left\|V^L_{\le t}\,|\psi\rangle - E^L_{\le t}\,|\psi\rangle\right\|_2^2 = \langle u|u\rangle + \langle v|v\rangle \ .$$

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

Notice that we can rewrite $|u\rangle$ as

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

Thus, by the Cauchy–Schwarz inequality, we have

$$\langle u|u\rangle \le \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:\left|L'\cup R\right|\le t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} |\alpha_{x,L,R}|^2 \right) \cdot A_{y,L',R} \ ,$$

where

$$A_{y,L',R} \coloneqq \sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{BIm}(L\cup R)}} \left(\frac{1}{\sqrt{N-|\mathrm{BIm}\,(L\cup R)|}} - \frac{1}{\sqrt{N}} \right)^2 \ .$$

For $A_{y,L',R}$, we have

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

where the first inequality follows from the fact that, for nonnegative real numbers $a \geq b$, one has $\sqrt{a} - \sqrt{b} \leq \sqrt{a-b}$. The second inequality uses the following observation: once y, L', R are fixed, the number of summands satisfying $L' = L \cup \{(x,y)\}$ and $y \notin \mathrm{BIm}(L \cup R)$ is at most $t+1$, and $|\mathrm{BIm}(L' \cup R)| = |\mathrm{BIm}(L \cup R)| + 2$. Therefore,

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

where the last inequality follows from $|\mathrm{BIm}(L \cup R)| \leq 2t$.

As for $|v\rangle$, notice that we can rewrite it as

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

By the Cauchy–Schwarz inequality, we have

$$\langle v|v\rangle \leq \sum_{\substack{y\in\{0,1\}^n \\ L',R\in\mathfrak{R}:\left|L'\cup R\right|\leq t+1}} \left(\sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} |\alpha_{x,L,R}|^2 \right) \cdot B_{y,L',R} \ ,$$

where

$$B_{y,L',R} \coloneqq \sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \frac{\mathrm{num}(L,(x,y))+1}{N} \ .$$

For $B_{y,L',R}$, we have

$$B_{y,L',R} = \sum_{\substack{x\in\{0,1\}^n, L\in\mathfrak{R}: \\ L'=L\cup\{(x,y)\}, \\ y\in \mathrm{BIm}(L\cup R)}} \frac{\mathrm{num}(L',(x,y))}{N} \leq \frac{\sum_{x\in\{0,1\}^n} \mathrm{num}(L',(x,y))}{N} \leq \frac{t+1}{N} \ ,$$

where the last inequality follows because, for fixed y, $\sum_{x\in\{0,1\}^n} \mathrm{num}(L',(x,y))$ is precisely the number of occurrences of y in L', which is at most $t+1$. Therefore,

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

□

Next, we prove the main lemma in this section.

Proof of Lemma 47. To prove

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

it is equivalent to show

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

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

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

For (a), by the unitary invariance of operator E^L (Lemma 64) and the triangle inequality, we have

$$(a) \le \left\| D_{\mathsf{A}} \cdot V^L_{\le t} \cdot C_{\mathsf{A}} - D_{\mathsf{A}} \cdot E^L_{\le t} \cdot C_{\mathsf{A}} \right\|_\infty$$

$$
\begin{aligned}
&\quad + \left\| Q[C,D]_{\mathsf{LR}} \cdot E^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_\infty \\
&\leq\ 2 \left\| V^L_{\leq t} - E^L_{\leq t} \right\|_\infty \leq\ 4\sqrt{\frac{t(t+1)}{N}}\ .
\end{aligned}
$$

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

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

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

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

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,

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

The other inequality in Lemma 47 follows from a similar argument. □

E Proof of Claim 56

We first need a twirling lemma. Recall that

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

Lemma 66 (Twirling). *Let $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 50. For an integer $0 \le t \le N/4$, we have*

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

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

The proof of this twirling lemma is deferred to Appendix F. Now, we proceed to prove Claim 56.

Claim 56. *For any integer $t \ge 0$ and $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 50*

$$\mathrm{Re}\left[\langle \mathcal{A}^{W,\mathcal{D}}_t |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}^V_t\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \right] \ge 1 - \frac{38t^2}{N^{1/4}} \ .$$

Proof by induction.. For the base case $t = 0$, by Definition 51, Definition 52 and Definition 53, we have

$$\begin{aligned} \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}^V_0\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) &= \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|0^n 0^m\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{L}} |\{\}\rangle_{\mathsf{R}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \\ &= |0^n 0^m\rangle_{\mathsf{AB}} |\{\}\rangle_{\mathsf{L}} |\{\}\rangle_{\mathsf{R}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \\ &= |\mathcal{A}^{W,\mathcal{D}}_0\rangle_{\mathsf{ABLRCD}} \ . \end{aligned}$$

Thus, the base case holds: $\mathrm{Re}\left[\langle \mathcal{A}^{W,\mathcal{D}}_0 |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}^V_0\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) \right] = 1$.

Assuming the claim holds for some $t \ge 0$, we now prove it for $t+1$. Since 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,

$$\begin{aligned} |\mathcal{A}^{W,\mathcal{D}}_{t+1}\rangle_{\mathsf{ABLRCD}} &= (\mathsf{cD} \cdot W \cdot \mathsf{cC}) \cdot A_{t+1} \cdot |\mathcal{A}^{W,\mathcal{D}}_t\rangle \\ \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}^V_{t+1}\rangle_{\mathsf{ABLR}} |\mathsf{init}(\mathcal{D})\rangle_{\mathsf{CD}} \right) &= \mathsf{cQ} \cdot \left(V \cdot A_{t+1} \cdot |\mathcal{A}^V_t\rangle |\mathsf{init}(\mathcal{D})\rangle \right) \end{aligned}$$

which gives

$$\begin{aligned} &\mathrm{Re}\left[\langle \mathcal{A}^{W,\mathcal{D}}_{t+1}| \cdot \mathsf{cQ} \cdot \left(|\mathcal{A}^V_{t+1}\rangle |\mathsf{init}(\mathcal{D})\rangle \right) \right] \\ &= \mathrm{Re}\left[\langle \mathcal{A}^{W,\mathcal{D}}_t| \cdot A^\dagger_{t+1} \cdot \mathsf{cC}^\dagger \cdot W^\dagger \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot \left(V \cdot A_{t+1} \cdot |\mathcal{A}^V_t\rangle |\mathsf{init}(\mathcal{D})\rangle \right) \right] \qquad (31) \\ &= \mathrm{Re}\left[\langle \mathcal{A}^{W,\mathcal{D}}_t| \cdot A^\dagger_{t+1} \cdot \mathsf{cC}^\dagger \cdot W^\dagger_{\le t} \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot V_{\le t} \cdot A_{t+1} \cdot |\mathcal{A}^V_t\rangle |\mathsf{init}(\mathcal{D})\rangle \right] , \end{aligned}$$

because of Fact 55. 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 (31) $= (*) + (**)$ where

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

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

We first lower bound $(**)$:

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

The first inequality follows from Fact 54, 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 47. To bound $(*)$, we first utilize the properties of W and V to derive:

$$\begin{aligned}
W_{\le t}^{\dagger} \cdot V_{\le t} &= (W \cdot \Pi_{\le t})^{\dagger} \cdot V \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot W^{\dagger} \cdot V \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot \Pi^{\mathrm{Dom}(W)} \cdot \Pi_{\le t} \\
&= \Pi_{\le t} \cdot \left(\Pi^{\mathrm{DB}} - \left(\Pi^{\mathrm{DB}} - \Pi^{\mathrm{Dom}(W)}\right)\right) \cdot \Pi_{\le t} \\
&= \Pi_{\le t}^{\mathrm{DB}} - \left(\Pi_{\le t}^{\mathrm{DB}} - \Pi_{\le t}^{\mathrm{Dom}(W)}\right) .
\end{aligned} \tag{32}$$

Then, we can rewrite $(*) = (\triangle) - (\triangle\triangle)$ using Eq. (32) where:

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

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

Thus, to bound $(*)$ we need to separately bound $(\triangle)$ and $(\triangle\triangle)$. First, in $(\triangle)$ 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

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

Then we will upper-bound $(\triangle\triangle)$:

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

where the last line follows from Lemma 66.

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

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

F A Twirling Lemma

In this section, we prove Lemma 66. We first analyze $\Pi_{\mathsf{LR}}^{\mathrm{Dom}(W)}$ and $\Pi_{\mathsf{LR}}^{\mathrm{Im}(W)}$ and then give the proof.

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

We need some notation:

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

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

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

We have the following lemma:

Lemma 67.

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

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

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

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

Recall the operator E^R in Definition 63. It is not hard to check

$$W^R_{l,r} = \frac{\sqrt{N}}{\sqrt{N-2l-2r}} \cdot \Pi^{\mathrm{DB}}_{l,r+1,\mathsf{LR}} \cdot E^R_{l,r} \ .$$

Therefore,

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

where the second inequality is from [MH25, Eq. (11.26)]. □

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

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

It is evident that

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

Now we define

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

Then we have

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

We will need the following lemma when proving Lemma 66.

Lemma 68. *For non-negative l, r such that $l + r < N/2$,*

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

where

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

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

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

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

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

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

where

$$
\lambda \coloneqq \left\| \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Delta_i \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} - \Delta_i \cdot \Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Delta_i \right\|_\infty \quad ,
$$

and $\Delta_i \coloneqq \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$. Thus, we are left to show that λ is bounded by $2\sqrt{\frac{2(l+r)}{N}}$. Notice that

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

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 $\Pi^{\mathrm{db}}_{l,r,\mathsf{LR}} \cdot \Pi^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$ is

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

Here, $x \in \{0,1\}^{nl}$, $x' \in \{0,1\}^{n(r-1)}$, $y \in \{0,1\}^{nl}$, $y' \in \{0,1\}^{nr}$ and $T_{x,x'}$ denotes the set of all binary strings that do not belong to the same block as any string in x and x'. Similarly, $\mathit{\Pi}^{\mathrm{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \cdot \mathit{\Pi}^{\mathrm{db}}_{l,r,\mathsf{LR}}$ is

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

Then, we have

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

Therefore,

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

Notice that

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

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 $\||\phi\rangle\langle\psi| - |\psi\rangle\langle\phi|\|_\infty = 1$. Therefore,

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

F.2 Proof of Lemma 66

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

Lemma 69 (Claim 2 in [MH25]). *Let $\mathcal{D}$ be the Haar measure over $\mathrm{U}(N)$. We have*

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

Before proving Lemma 66, we prove a lemma that will assist in our argument.

Lemma 70. *Let $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ as defined in Definition 50. 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 68 and the triangle inequality, we have

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

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

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 $\frac{1}{N^2}-\mathsf{RSS}$ 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,

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

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

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

$$
\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes\overline{C})^\dagger \cdot |x,x\rangle\langle x,x| \cdot (C\otimes\overline{C}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes\overline{U})^\dagger \cdot |x,x\rangle\langle x,x| \cdot (U\otimes\overline{U}) \right] \right\|_\infty \le \frac{4}{N^2} \ . \tag{33}
$$

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

$$
\left\| \mathop{\mathbb{E}}_{C} \left[(C\otimes\overline{C})^\dagger \cdot |x,x\rangle\langle x,x| \cdot (C\otimes\overline{C}) \right] - \mathop{\mathbb{E}}_{U\leftarrow\mu} \left[(U\otimes\overline{U})^\dagger \cdot |x,x\rangle\langle x,x| \cdot (U\otimes\overline{U}) \right] \right\|_\infty
$$

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

From [LQS+26, Theorem 4], we know that there is a joint distribution γ among $|u\rangle$ and $|v\rangle$ such that $\mathbb{E}_\gamma[\||u\rangle - |v\rangle\|_2] \leq \frac{1}{N^2}$. Therefore, we have

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

This establishes Eq. (33). From Eq. (33), Lemma 69 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

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

□

We are now ready to prove Lemma 66. We restate the lemma here.

Lemma 66. *For an integer* $0 \le t \le N/4$ *and* $\mathcal{D} \in \{\mathcal{D}_1, \mathcal{D}_2\}$ *as defined in Definition 50, we have*

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

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

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

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

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

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

where the equality holds because $\Pi^{\mathrm{db}}_{\le t,\mathsf{LR}}$ and $J^{\mathrm{Dom}(W)}_{\le t,\mathsf{LR}}$ are block diagonal with respect to l and r. Then from Lemma 70, we have

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathcal{D}} \left[(C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{DB}}_{\le t,\mathsf{LR}} - \Pi^{\mathrm{Dom}(W)}_{\le t,\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right] \right\|_\infty \\
\le &\max_{\substack{l,r\ge 0 \\ l+r\le t}} \frac{4l+r}{N-1} + \frac{7rN}{N-2l-2r+2} \cdot \sqrt{\frac{2(l+r)}{N}} \\
\le &\max_{\substack{l,r\ge 0 \\ l+r\le t}} \frac{3l+t}{N-1} + \frac{7rN}{N-2t+2} \cdot \sqrt{\frac{2t}{N}} \\
\le &\frac{t}{N-1} + \frac{7tN}{N-2t+2} \cdot \sqrt{\frac{2t}{N}} \le \frac{8tN}{N-2t+2} \cdot \sqrt{\frac{2t}{N}} \le 16t \cdot \sqrt{\frac{2t}{N}} \ ,
\end{aligned}$$

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