How to Construct Random Unitaries

Fermi Ma* Hsin-Yuan Huang†

Abstract

The existence of pseudorandom unitaries (PRUs)—efficient quantum circuits that are computationally indistinguishable from Haar-random unitaries—has been a central open question, with significant implications for cryptography, complexity theory, and fundamental physics. In this work, we close this question by proving that PRUs exist, assuming that any quantum-secure one-way function exists. We establish this result for both (1) the standard notion of PRUs, which are secure against any efficient adversary that makes queries to the unitary U, and (2) a stronger notion of PRUs, which are secure even against adversaries that can query both the unitary U and its inverse $U^\dagger$. In the process, we prove that any algorithm that makes queries to a Haar-random unitary can be *efficiently* simulated on a quantum computer, up to inverse-exponential trace distance.

*Simons Institute & UC Berkeley. Email: fermima1@gmail.com

†Google Quantum AI, Caltech, & MIT. This work was conducted while Hsin-Yuan Huang was visiting the Simons Institute for the Theory of Computing. Email: hsinyuan@google.com, hsinyuan@caltech.edu

Contents

1 Introduction **1**
- 1.1 Our results . . . 1
- 1.2 Our techniques . . . 1
- 1.3 Acknowledgments . . . 4

2 Preliminaries **4**
- 2.1 Relations and variable-length registers . . . 5
  - 2.1.1 Variable-length registers . . . 6
  - 2.1.2 Pairs of variable-length registers . . . 7
- 2.2 The Haar measure, unitary t-designs, and twirling channels . . . 7
- 2.3 Oracle adversaries . . . 10
- 2.4 Pseudorandom unitaries . . . 11
- 2.5 Useful lemmas . . . 11

I Standard PRUs **13**

3 The purified permutation-function oracle **13**
- 3.1 Orthonormality of the pf-relation states . . . 14
- 3.2 How pfO acts on the pf-relation states . . . 15

4 The path-recording oracle V **16**
- 4.1 Defining V . . . 16
- 4.2 Right unitary invariance . . . 18
- 4.3 Relating V to pfO . . . 20

5 The PRU proof **22**
- 5.1 Setup . . . 22
- 5.2 Proof of Lemma 5.1 . . . 23

II Strong PRUs **24**

6 The purified permutation-function oracle **24**
- 6.1 Orthonormality of the pf-relation states . . . 25
- 6.2 How pfO acts on the pf-relation states . . . 26

7 The partial path-recording oracle W **27**
- 7.1 Defining W^L and W^R . . . 28
- 7.2 Defining W . . . 29

8 The path-recording oracle V **30**
- 8.1 Defining V^L and V^R . . . 31
- 8.2 Defining V . . . 32
- 8.3 Two-sided unitary invariance . . . 32
- 8.4 W is a restriction of V . . . 33

9 The strong PRU proof **35**
- 9.1 Setup . . . 35

9.2 V is indistinguishable from twirled W . . . 36
9.3 Twirled W and twirled pfO are indistinguishable . . . 41
9.4 Proof of Lemma 9.1 . . . 43

10 Proof of Claim 16 **44**
10.1 Defining E^L and E^R . . . 44
10.2 Approximate unitary invariance of V^L and V^R . . . 46

11 Proof of Lemma 9.2 **52**
11.1 The domain and image of W . . . 52
11.2 An operator upper bound . . . 55
11.3 An intermediate lemma on 2-design twirling . . . 60
11.4 Finishing the proof of Lemma 9.2 . . . 61

III Appendices **66**

A Efficient circuit implementation of path-recording oracle **66**
A.1 Implementing relation states . . . 66
A.2 Implementing forward queries . . . 66
A.3 Implementing forward and inverse queries . . . 67

B The path-recording framework **68**
B.1 Defining $V(\mathcal{S}^{\mathsf{inj}})$ and the $V(\mathcal{S}^{\mathsf{inj}})$ state . . . 69
B.2 $V(\mathcal{S}^{\mathsf{inj}})$ is a partial isometry . . . 70
B.3 $V(\mathcal{S}^{\mathsf{inj}})$ is right unitary invariant . . . 71
B.4 Relation between $V(\mathcal{S}^{\mathsf{inj}})$ and V state . . . 72
B.5 $V(\mathcal{S}^{\mathsf{inj}})$ is indistinguishable from Haar random unitaries . . . 72

C An elementary proof of the gluing lemma **73**

1 Introduction

This paper resolves the question: can efficient quantum circuits behave like truly random unitaries? Specifically, we prove that *pseudorandom unitaries* (PRUs) exist assuming the existence of any quantum-secure one-way function. First proposed by Ji, Liu, and Song in 2017 [JLS17], a PRU is the unitary analogue of a pseudorandom function (PRF) [GGM86]. A PRU consists of a family of efficiently computable quantum circuits with the guarantee that no polynomial-time quantum algorithm can distinguish between queries to a unitary sampled from the PRU family and a unitary sampled from the Haar measure.

Random unitaries play an essential role throughout quantum information science, arising in quantum algorithms, quantum supremacy experiments, quantum learning, cryptographic protocols, and much more [HLSW04, KLR+08, AAB+19, BFNV19, HKP20, AQY22, HKT+22, EFH+22, HBC+22, Mov23, KQST23, LMW24]. In physics, highly chaotic systems such as black holes are often modeled as Haar-random unitary transformations [CGAH+17, NVH18, CHJLY17, KTP20, CSM+23]. However, this approach has a fundamental problem: Haar-random unitaries are inherently unphysical, requiring exponential complexity to even specify. The notion of a PRU offers a tantalizing solution: efficient circuits that are as good as Haar-random. In fact, the idea that PRUs are a more accurate model of black hole dynamics is behind recent advances in fundamental physics [KTP20, YE23, EFL+24].

Despite considerable interest, the question of whether PRUs actually *exist* has remained open. In the past couple of years, a series of works has established that weaker notions are possible [LQS+23, BM24, HBK23, MPSY24, AGKL24]. For example, [MPSY24, CBB+24] constructed *non-adaptive* PRUs, which are secure against restricted adversaries that makes all of their queries *at once* in parallel. While these works represent important progress, the broader goal remains elusive, and constructing a PRU remains one of the central challenges in quantum cryptography.

1.1 Our results

In this work, we give the first proof that PRUs exist.

Theorem 1. *PRUs exist assuming the existence of any quantum-secure one-way function.*

In fact, we go one step further. Theorem 1 is about PRUs that satisfy the original definition of [JLS18], which are secure against adversaries that can query an oracle for U, but *not* the inverse unitary $U^\dagger$. We therefore define *strong PRUs*, which are indistinguishable from Haar-random even to adverasaries that can query both U and $U^\dagger$. Our second main result builds strong PRUs from one-way functions.[1]

Theorem 2. *Strong PRUs exist assuming the existence of any quantum-secure one-way function.*

While Theorem 2 technically subsumes Theorem 1, the proof of Theorem 2 is significantly more involved. Since Theorem 1 may suffice for many applications, we present them separately. By establishing the existence of PRUs, our work provides the foundation for new avenues of research in quantum computation, cryptography, and fundamental physics.

1.2 Our techniques

We achieve our results on PRUs by proving that any quantum oracle algorithm $\mathcal{A}^U$ that queries an n-qubit Haar-random unitary U can be *efficiently simulated* with a remarkably simple procedure:

1. Initialize an external register E to the state $|\varnothing\rangle$, where $\varnothing$ denotes the empty set. (**Aside:** When we write a set inside a ket, e.g., $|S\rangle_{\mathsf{E}}$, we are simply using the set S as a label for a unit vector. The inner product $\langle R|S\rangle$ equals 1 if $R = S$ and 0 otherwise.)

[1] The notion of strong PRUs is also discussed in [MPSY24] as an open question.

2. Run the oracle algorithm $\mathcal{A}$, replacing each query to U with the following linear map:

$$V : |x\rangle\,|S\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{2^n - |S|}} \sum_{\substack{y\in\{0,1\}^n:\\ y\notin S_Y}} |y\rangle\,|S\cup\{(x,y)\}\rangle_{\mathsf{E}}\,, \tag{1.1}$$

where S_Y denotes the set of all y such that $(x,y)\in S$ for some x. In words, V maps x to a uniform superposition over $y\in\{0,1\}^n$, except those that already appear in S, and simultaneously "records" (x,y) by inserting it into S. We refer to V as the *path-recording oracle*.

We prove that the following mixed states have trace distance $O(t^2/2^n)$:

- $\mathbb{E}_U\,|\mathcal{A}^U\rangle\langle\mathcal{A}^U|$, the state of $\mathcal{A}$ after t queries to a Haar-random unitary U, where $|\mathcal{A}^U\rangle \coloneqq U\cdot A_t\cdots U\cdot A_1\,|0\rangle$ denotes the state of the algorithm after t queries to U, and $|0\rangle$ denotes an arbitrary initial state.
- $\mathrm{Tr}_{\mathsf{E}}(\,|\mathcal{A}^V\rangle\langle\mathcal{A}^V|)$, where $|\mathcal{A}^V\rangle_{\mathsf{AE}} \coloneqq V\cdot A_t\cdot\cdots V\cdot A_1\,|0\rangle\,|\varnothing\rangle_{\mathsf{E}}$ denotes the global state of the algorithm and the external register E after t queries to V.

Despite the extensive literature on Haar-random unitaries, to the best of our knowledge, this "path-recording" characterization was not known before.[2][3] Furthermore, it is easy to show that V can be efficiently implemented on a quantum computer; see Appendix A. This establishes the following fact:

Any algorithm that queries a Haar-random unitary can be efficiently simulated on a quantum computer up to inverse-exponential trace distance.

As we now explain, this new path-recording perspective is the key to our PRU proof.

How to construct PRUs. The main technical step in our PRU proof is to show that a t-query oracle algorithm $\mathcal{A}$ can only distinguish between

- $P_\pi\cdot F_f\cdot C$, where $P_\pi=\sum_x |\pi(x)\rangle\langle x|$ for a random permutation $\pi\leftarrow S_{2^n}$, $F_f=\sum_x(-1)^{f(x)}\,|x\rangle\langle x|$ for a random function $f\leftarrow\{0,1\}^{2^n}$, and C is a random n-qubit Clifford.[4]
- a Haar-random n-qubit unitary U,

with probability $1/2+t^2/2^n$.

Our proof works by *purifying* the randomness of the PRU. Ignoring C for now, suppose we initialize an external register to the uniform superposition $\propto\sum_{\pi\in S_{2^n}}|\pi\rangle\otimes\sum_{f\in\{0,1\}^{2^n}}|f\rangle$ over all permutations π and functions f. In this view, a query to a random $P_\pi\cdot F_f$ is equivalent to a query to a fixed unitary that applies $P_\pi\cdot F_f$ controlled on $|\pi\rangle\,|f\rangle$, i.e., the map

$$|x\rangle\otimes|\pi,f\rangle\mapsto(-1)^{f(x)}\cdot|\pi(x)\rangle\otimes|\pi,f\rangle\,. \tag{1.2}$$

Equivalently, we can view this map as sending x to a superposition over all y, while simultaneously multiplying the purifying register by the coefficient $\delta_{\pi(x)=y}\cdot(-1)^{f(x)}$:

$$|x\rangle\otimes|\pi,f\rangle\mapsto\sum_{y\in\{0,1\}^n}|y\rangle\otimes\Big(\delta_{\pi(x)=y}\cdot(-1)^{f(x)}\cdot|\pi,f\rangle\Big). \tag{1.3}$$

[2] We note that [AMR20] proves that there *exists* a space-efficient (but otherwise inefficient) way to exactly simulate Haar-random unitaries. Moreover, their proof is non-constructive, i.e., they do not give a simulator.

[3] This can also be viewed as an analog of Zhandry's compressed oracles for Haar-random unitaries [Zha19].

[4] This PFC construction was introduced by [MPSY24], who proved security against *non-adaptive* adversaries, i.e., adversaries that make all of their oracle queries at once, in parallel.

After t queries to the purified $P_\pi \cdot F_f$, the global state including the purifying registers is (proportional to) a sum of terms

$$|y_t\rangle\langle x_t| \cdot A_t \cdots |y_1\rangle\langle x_1| \cdot A_1 \, |0^n\rangle \otimes \underbrace{\sum_{\pi \in S_{2^n}} |\pi, f\rangle \cdot \delta_{\pi(x_1)=y_1} \cdots \delta_{\pi(x_t)=y_t} \cdot (-1)^{f(x_1)+\cdots+f(x_t)}}_{\propto |\mathsf{pf}_{\{(x_1,y_1),\ldots,(x_t,y_t)\}}\rangle}, \tag{1.4}$$

over all possible $x_1, y_1, \ldots, x_t, y_t \in \{0,1\}^n$, i.e., over all *Feynman paths*.

Crucially, when all the $x_1, \ldots, x_t$ are distinct, these $|\mathsf{pf}_{\{(x_1,y_1),\ldots,(x_t,y_t)\}}\rangle$ states are orthogonal and is isometric to $|\{(x_1,y_1),\ldots,(x_t,y_t)\}\rangle$. Since the algorithm is not given the purifying registers, a query to a random $P_\pi \cdot F_f$ is *identical* to a query to the path-recording oracle V described earlier—except on paths where there is a collision among the inputs $x_1, \ldots, x_t$.

This is where C comes in. We prove that V satisfies a key property: for any n-qubit unitary C,

$$(V \cdot C) \cdot A_t \cdots (V \cdot C) \cdot A_1 \, |0^n\rangle \, |\varnothing\rangle_{\mathsf{E}} = ((C \otimes \mathsf{Id})^{\otimes t})_{\mathsf{E}} \cdot V \cdot A_t \cdots V \cdot A_1 \, |0^n\rangle \, |\varnothing\rangle_{\mathsf{E}} \, . \tag{1.5}$$

This says that applying C to the **adversary's register** before each query to V is equivalent to applying C to each x_i in the **purifying register** $|\{(x_1,y_1),\ldots,(x_t,y_t)\}\rangle$. When C is sampled from any 2-design, the randomness of C ensures there are no collisions in the $x_1, \ldots, x_t$ with overwhelming probability. Consequently, we show that queries to V are indistinguishable from queries to $P_\pi \cdot F_f \cdot C$, as long as C is sampled from *any* 2-design. By instantiating the 2-design to be either (1) a random Clifford or (2) a Haar-random unitary, we show that both $P_\pi \cdot F_f \cdot C$ and Haar-random unitaries are indistinguishable from V, and thus, from each other.

Strong PRUs and a symmetrized path-recording oracle $\widetilde{V}$. To obtain strong PRUs, we use the construction: $D \cdot P_\pi \cdot F_f \cdot C$, where D, C are both random n-qubit Cliffords, P_π is the same as before, and F_f is a random q-ary phase (for any $q \geq 3$). By analyzing the purification of $P_\pi \cdot F_f$, we show that when $\mathcal{A}$ makes forward and inverse queries, the purifying registers, viewed in the right basis, "record" information from *two Feynman paths*: one set S^{for} consists of (x,y) tuples corresponding to the forward queries, and another set S^{inv} of tuples (x,y) corresponds to the inverse queries. Whereas each query in the standard PRU proof always inserts a tuple (x,y) into the set S, when both forward and inverse queries are allowed, the effect is more intricate:

- A forward query will sometimes add a tuple to S^{for}, but other times delete a tuple from S^{inv}.
- An inverse query will sometimes add a tuple to S^{inv}, but other times delete a tuple from S^{for}.

We prove that this behavior corresponds to a more general "symmetrized" path recording oracle $\widetilde{V}$. Moreover, as long as D, C are sampled from any 2-design, the adversary cannot distinguish between queries to $D \cdot P_\pi \cdot F_f \cdot C$ and queries to $\widetilde{V}$, and using similar reasoning as the standard PRU proof, conclude both of the following (1) strong PRUs exist and (2) $\widetilde{V}$ is indistinguishable from Haar-random even under inverse queries. As we show in Appendix A, $\widetilde{V}$ can also be implemented efficiently, and consequently any algorithm that makes *forward and inverse* queries to a Haar-random unitary can also be simulated to inverse exponential error.

Our proof leverages the following property of 2-designs: if one samples C from a 2-design and applies $C \otimes \overline{C}$ to any state (where $\overline{C}$ denotes the complex conjugate), then with overwhelmingly high probability, the result is either (a) a pair of distinct elements, or (b) the maximally entangled state. At a very high level, the fact that there are two kinds of outcomes after twirling by $C \otimes \overline{C}$ is related to how the purification "decides" whether it should add or delete a tuple (x,y).

We remark that the strong PRU proof is significantly more involved than standard PRU proof, and the reader may find it beneficial to start with the standard PRU proof.

A new approach to random unitaries. More broadly, the path-recording oracle unlocks a new way to proving theorems about random unitaries. Before this work, analyzing mixed states such as $\mathbb{E}_U |\mathrm{Adv}^U\rangle\langle\mathrm{Adv}^U|$ often necessitated the use of Weingarten calculus, involving intricate asymptotic bounds on Weingarten functions through sophisticated combinatorial and representation-theoretic calculations. Our approach circumvents this complexity entirely.[5]

We demonstrate the power of this approach by giving an elementary proof of the "gluing lemma" recently proven by [SHH24]. This lemma states that if two Haar-random unitaries U_1 and U_2 *overlap*, with U_1 acting on systems A, B and U_2 on B, C (where B has a super-logarithmic number of qubits), then queries to $U_2 \cdot U_1$ are indistinguishable from queries to a larger Haar-random unitary U acting on $\mathsf{A}, \mathsf{B}, \mathsf{C}$. Using this lemma (and our Theorem 1), [SHH24] constructed low-depth PRUs secure against forward queries. However, their proof of the gluing lemma is highly technical, relying on careful representation-theoretic analysis and tight bounds on Weingarten functions.

The path-recording oracle yields an elementary proof of the gluing lemma (see Part III). The key insight is to replace the Haar-random unitaries with path-recording oracles. This reduces to showing that the composition of two independent path-recording oracles $V_2 \cdot V_1$, where V_1 acts on $(\mathsf{A}, \mathsf{B}, \mathsf{E}_1)$ and V_2 acts on $(\mathsf{B}, \mathsf{C}, \mathsf{E}_2)$, approximates a single path-recording oracle V acting on $(\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{E})$.

Given the central role of random unitaries in physics and quantum computing, we expect the path-recording framework to have broad applications in the future.

1.3 Acknowledgments

Special thanks to John Wright for many helpful suggestions and extensive discussions at every stage of this project, and to Ewin Tang for providing significant feedback on the manuscript. We also thank Thiago Bergamaschi, John Bostanci, Adam Bouland, Chi-Fang (Anthony) Chen, Lijie Chen, Tudor Giurgica-Tiron, Jeongwan Haah, Jonas Haferkamp, William Kretschmer, Alex Lombardi, Tony Metger, Thomas Schuster, Joseph Slote, Xinyu (Norah) Tan, Umesh Vazirani, Henry Yuen, and Mark Zhandry for valuable discussions and feedback.

Fermi Ma is supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. Hsin-Yuan Huang acknowledges the visiting position at Center for Theoretical Physics, MIT. This work was conducted while both authors were at the Simons Institute for the Theory of Computing, supported by DOE QSA grant FP00010905.

2 Preliminaries

This section establishes basic notation, definitions, and lemmas that we use throughout the paper.

Notation. We write $N \coloneqq 2^n$, where n typically denotes the number of qubits. We write $[N] \coloneqq \{1, \ldots, N\}$ to denote the set of integers from 1 to N, and we will identify $[N]$ with $\{0,1\}^n$ by associating each integer $i \in [N]$ with the string $x \in \{0,1\}^n$ corresponding to the binary representation of $i-1$. For any integer $1 \le t \le N$, let $[N]^t_{\mathrm{dist}}$ denote the set of length-t sequences of distinct integers from 1 to N, i.e.,

$$[N]^t_{\mathrm{dist}} \coloneqq \{(x_1, \ldots, x_t) \in [N]^t : x_i \neq x_j \text{ for all } i \neq j\}. \tag{2.1}$$

[5] Alternatively, one can view our technique as deriving a simplified and approximate version of the Weingarten calculus from purely elementary arguments.

For $t = 0$, we adopt the convention that $[N]^t_{\text{dist}} \coloneqq \{()\}$ is a set with a single element () denoting a length-0 sequence. For any permutation $\pi \in \mathsf{Sym}_t$, let S_π be a unitary that acts on $(\mathbb{C}^N)^t$ as follows:

$$S_\pi : |x_1, \ldots, x_t\rangle \mapsto |x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(t)}\rangle . \tag{2.2}$$

Quantum registers. We use capital sans-serif letters to label quantum registers. For a register A, the associated Hilbert space is denoted $\mathcal{H}_\mathsf{A}$. When a quantum state is supported on multiple registers, such as (A, B), this means that $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. To clarify which systems a state is defined on, we sometimes include the register labels as subscripts in dark gray sans-serif font, e.g., $|\psi\rangle_{\mathsf{AB}}$. If a linear operator U acts only on subsystem A, we may write this as U_A. Such an operator can be extended to a larger system by acting trivially on other registers; for example, $(U_\mathsf{A} \otimes \mathsf{Id}_\mathsf{B}) \cdot |\psi\rangle_{\mathsf{AB}}$. To reduce notational clutter, we often omit the "$\otimes\mathsf{Id}_\mathsf{B}$" and simply write $U_\mathsf{A} \cdot |\psi\rangle_{\mathsf{AB}}$. Similarly, when summing operators that act on different registers, such as U_A and V_{AB}, we write $U_\mathsf{A} + V_{\mathsf{AB}}$ to mean $U_\mathsf{A} \otimes \mathsf{Id}_\mathsf{B} + V_{\mathsf{AB}}$.

Given a projector Π acting on register A, we say that a state $|\psi\rangle \in \mathcal{H}_\mathsf{A}$ is in the image of Π if $\Pi |\psi\rangle = |\psi\rangle$. For a state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, we similarly say that $|\psi\rangle$ is in the image of Π_A if $\Pi_\mathsf{A} |\psi\rangle_{\mathsf{AB}} = (\Pi_\mathsf{A} \otimes \mathsf{Id}_\mathsf{B}) \cdot |\psi\rangle_{\mathsf{AB}} = |\psi\rangle_{\mathsf{AB}}$.

Given a state $|\psi\rangle$ on systems (A, B), we denote the partial trace over system B as $\mathrm{Tr}_\mathsf{B}(|\psi\rangle\langle\psi|)$. Occasionally, we will write this as $\mathrm{Tr}_{-\mathsf{A}}(|\psi\rangle\langle\psi|)$, where the minus sign indicates tracing out all systems except A.

2.1 Relations and variable-length registers

Fix a choice of $N = 2^n$. A relation R is defined as a *multiset* $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ of ordered pairs $(x_i, y_i) \in [N]^2$. This definition deviates slightly from the standard notion of a relation, which is typically an ordinary set of ordered pairs without repeated elements. The *size* of the relation refers to the number of ordered pairs in the relation, including multiplicities. We denote this by $|R|$, as the size corresponds to the cardinality of R as a multiset.

Definition 1. *Let $\mathcal{R}$ denote the infinite set of all relations R. For any $t \geq 0$, let $\mathcal{R}_t$ denote the set of all size-t relations.*

Definition 2. *For a relation R, we use $\mathrm{Dom}(R)$ to denote the set*

$$\mathrm{Dom}(R) = \{x : x \in [N], \exists y \ s.t. (x, y) \in R\}, \tag{2.3}$$

and $\mathrm{Im}(R)$ to denote the set

$$\mathrm{Im}(R) = \{y : y \in [N], \exists x \ s.t. (x, y) \in R\}. \tag{2.4}$$

Note that while R may be a multi-set, $\mathrm{Dom}(R)$ and $\mathrm{Im}(R)$ are ordinary sets, i.e., they will not have repeated elements.

Each relation $R \in \mathcal{R}$ is associated with a *relation state* $|R\rangle$, defined as follows.

Notation 1 (Relation states)**.** *For a relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, define the corresponding relation state $|R\rangle$ to be the state*

$$|R\rangle \coloneqq \frac{\sum_{\pi \in \mathsf{Sym}_t} |x_{\pi(1)}, y_{\pi(1)}, \ldots, x_{\pi(t)}, y_{\pi(t)}\rangle}{\sqrt{t! \cdot \sum_{(x,y) \in [N]^2} \mathsf{num}(R, (x, y))!}}. \tag{2.5}$$

where $\mathsf{num}(R, (x, y))$ denotes the number of times the tuple (x, y) appears in R.

An elementary counting argument yields the following result.

Fact 1. *For any relation $R \in \mathcal{R}$, the state $|R\rangle$ is a unit vector.*

The relation states $|R\rangle$ for $R \in \mathcal{R}_t$ can also be viewed as the standard basis for the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes t}$. Note that this is only true because we allow for multi-set relations. Specifically, if $\Pi_{\mathsf{sym}}^{N^2,t}$ denotes the projector onto the symmetric subspace of $(\mathbb{C}^{N^2})^{\otimes t}$, we have the equality

$$\Pi_{\mathsf{sym}}^{N^2,t} = \sum_{R \in \mathcal{R}_t} |R\rangle\langle R| \,. \tag{2.6}$$

However, we will typically use the following notation to refer to this projector.

Notation 2. *For any integer $t \geq 0$, we define*

$$\Pi_t^{\mathcal{R}} \coloneqq \sum_{R \in \mathcal{R}: |R| = t} |R\rangle\langle R| = \Pi_{\mathsf{sym}}^{N^2,t}. \tag{2.7}$$

Notation 3 (Restricted sets of relations)**.** *Define the following restricted sets of relations:*

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

If the tuples in a relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ are distinct, i.e., $(x_i, y_i) \neq (x_j, y_j)$ for $i \neq j$, the normalization factor simplifies to $1/\sqrt{t!}$, i.e.,

$$|R\rangle = \frac{1}{\sqrt{t!}} \sum_{\pi \in \mathsf{Sym}_t} |x_{\pi(1)}, y_{\pi(1)}, \ldots, x_{\pi(t)}, y_{\pi(t)}\rangle \,. \tag{2.8}$$

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

In both Parts I and II, we will consider linear maps that send superpositions of $|R\rangle$ for $R \in \mathcal{R}_t$ to superpositions of $|R'\rangle$ for $R' \in \mathcal{R}_{t+1}$. This motivates the definition of *variable-length registers*.

2.1.1 Variable-length registers

For every integer $t \geq 0$ let $\mathsf{R}^{(t)}$ be a register associated with the Hilbert space $\mathcal{H}_{\mathsf{R}^{(t)}} \coloneqq (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes t}$. Let R be a register corresponding to the infinite dimensional Hilbert space

$$\mathcal{H}_{\mathsf{R}} \coloneqq \bigoplus_{t=0}^{\infty} \mathcal{H}_{\mathsf{R}^{(t)}} = \bigoplus_{t=0}^{\infty} (\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes t}. \tag{2.9}$$

When $t = 0$, the space $(\mathbb{C}^N \otimes \mathbb{C}^N)^{\otimes 0} = \mathbb{C}$ is a one-dimensional Hilbert space. Thus, $\mathcal{H}_{\mathsf{R}^{(t)}}$ is spanned by the states $|x_1, y_1, \ldots, x_t, y_t\rangle$ where $x_i, y_i \in [N]$. Note that the relation states $|R\rangle$ for $R \in \mathcal{R}_t$ span the symmetric subspace of $\mathcal{H}_{\mathsf{R}^{(t)}}$.

We will sometimes divide up the $\mathsf{R}^{(t)}$ register into $\mathsf{R}^{(t)} \coloneqq (\mathsf{R}_{\mathsf{X}}^{(t)}, \mathsf{R}_{\mathsf{Y}}^{(t)})$ where $\mathsf{R}_{\mathsf{X}}^{(t)}$ refers to the registers containing $|x_1, \ldots, x_t\rangle$ and $\mathsf{R}_{\mathsf{Y}}^{(t)}$ refers to the registers containing $|y_1, \ldots, y_t\rangle$. We denote $\mathsf{R}^{(t)}\mathsf{X}, i$ as the register containing $|x_i\rangle$ and $\mathsf{R}^{(t)}\mathsf{Y}, i$ as the register containing $|y_i\rangle$. Following our convention for defining the length/size of a relation R, we say that a state $|x_1, y_1, \ldots, x_t, y_t\rangle$ has length/size t. Two states of different lengths are orthogonal by definition, since $\mathcal{H}_{\mathsf{R}}$ is a direct sum $\bigoplus_{t=0}^{\infty} \mathcal{H}_{\mathsf{R}^{(t)}}$.

Notation 4 (Extending fixed-length operators to variable-length)**.** *For any operator O defined on the fixed-size Hilbert space $\mathcal{H}_{\mathsf{R}^{(t)}}$, we abuse notation by using O to also refer to its extension on all of $\mathcal{H}_{\mathsf{R}}$. The extended operator is the direct sum of O and the 0 operator on $\mathcal{H}_{\mathsf{R}^{(t')}}$ for all $t' \neq t$.*

Hence, if two operators O_1 and O_2 act on $\mathcal{H}_{\mathsf{R}^{(t)}}$ and $\mathcal{H}_{\mathsf{R}^{(t')}}$, respectively, then $O_1 + O_2$ is the sum of their extensions over all of $\mathcal{H}_{\mathsf{R}}$. We can now define the projector $\Pi^{\mathcal{R}}$ that projects onto the span of all relation states.

Notation 5. *We define the projector*

$$\Pi^{\mathcal{R}} \coloneqq \sum_{t=0}^{\infty} \Pi_t^{\mathcal{R}} = \sum_{R \in \mathcal{R}} |R\rangle\langle R|\,, \tag{2.10}$$

that projects onto the span of all relation states $|R\rangle$ for all $R \in \mathcal{R}$.

Finally, we introduce the notion of variable-length tensor powers, which will be useful to describe applying an operator to each $|x_i, y_i\rangle$ in a state $|x_1, y_1, \ldots, x_t, y_t\rangle$, in settings where t is not explicitly known.

Notation 6 (Variable-length tensor powers)**.** *For any unitary $U \in \mathcal{U}(N^2)$, let*

$$U^{\otimes *} \coloneqq \sum_{t=0}^{\infty} U^{\otimes t} \tag{2.11}$$

be a unitary that acts on the Hilbert space $\mathcal{H}_{\mathsf{R}}$.

2.1.2 Pairs of variable-length registers

In Part II, we will consider states of the form $|L\rangle_{\mathsf{L}}\,|R\rangle_{\mathsf{R}}$, where $|L\rangle$ and $|R\rangle$ are both relation states, and L is another variable-length register defined analogously to R. Throughout Part II, we will use the following definitions.

Notation 7 (Fixed-length projectors)**.** *For any integers $\ell, r \geq 0$, let $\Pi_{\ell,r}$ denote the projector acting on $\mathcal{H}_{\mathsf{L}} \otimes \mathcal{H}_{\mathsf{R}}$ that projects onto the fixed-length Hilbert space $\mathcal{H}_{\mathsf{L}^{(\ell)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$.*

Notation 8 (Maximum-length projectors)**.** *For any integer $t \geq 0$, let $\Pi_{\leq t}$ denote the projector acting on $\mathcal{H}_{\mathsf{L}} \otimes \mathcal{H}_{\mathsf{R}}$ onto the Hilbert space $\bigoplus_{\ell,r\geq 0:\ell+r\leq t} \mathcal{H}_{\mathsf{L}^{(\ell)}} \otimes \mathcal{H}_{\mathsf{R}^{(r)}}$.*

Notation 9 (Length-restricted operators)**.** *For any operator B that acts on the variable-length registers R and R, let $B_{\ell,r} \coloneqq B \cdot \Pi_{\ell,r}$ denote the restriction of B to input states where registers R and R have lengths ℓ and r. Let $B_{\leq t} \coloneqq B \cdot \Pi_{\leq t}$ denote the restriction of B to inputs states where the combined length of L and R is at most t.*

Note that, with this notation, $(B{\leq}\, t)^\dagger$ does not necessarily equal $(B^\dagger)_{\leq t}$. We adopt the convention that $B^\dagger_{\leq t}$ refers to $(B_{\leq t})^\dagger$.

2.2 The Haar measure, unitary t-designs, and twirling channels

Definition 3 (Haar measure)**.** *The Haar measure over the n-qubit unitary group $\mathcal{U}(2^n)$ is the unique probability measure μ on $\mathcal{U}(2^n)$ that is:*

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

2. *Right-invariant: For any measurable set* $S \subseteq \mathcal{U}(2^n)$ *and any* $V \in \mathcal{U}(2^n)$, $\mu(SV) = \mu(S)$.

3. *Normalized:* $\mu(\mathcal{U}(2^n)) = 1$.

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

We will refer to the Haar measure as μ_{Haar}.

Definition 4 (Unitary t-design)**.** *A distribution* $\mathfrak{D}$ *on* n*-qubit unitaries is a unitary* t*-design if*

$$\mathop{\mathbb{E}}_{U\sim\mathfrak{D}}[U^{\otimes t}\otimes U^{\dagger,\otimes t}] = \int_{\mathcal{U}(2^n)} U^{\otimes t}\otimes U^{\dagger,\otimes t} d\mu(U), \tag{2.12}$$

where μ *is the Haar measure over the unitary group* $\mathcal{U}(2^n)$.

Notation 10. *Define the equality projector*

$$\Pi^{\mathsf{eq}} = \sum_{x\in[N]} |x\rangle\langle x| \otimes |x\rangle\langle x| . \tag{2.13}$$

In the following, when we write $\mathbb{E}_\psi$ and $\mathbb{E}_U$ without any specified distribution, we always refer to the uniform distribution over pure states and the Haar measure over unitary groups, respectively. We will use the following standard fact about Haar-random states and the symmetric subspace.

Fact 2. *The expectation over Haar measure satisfies*

$$\mathop{\mathbb{E}}_{\psi\leftarrow\mathbb{C}^N} |\psi\rangle\langle\psi|^{\otimes 2} = \frac{\Pi^{N,2}_{\mathsf{sym}}}{\mathrm{Tr}\left(\Pi^{N,2}_{\mathsf{sym}}\right)} = \frac{\Pi^{N,2}_{\mathsf{sym}}}{\binom{N+1}{2}}, \tag{2.14}$$

where $\Pi^{N,k}_{\mathsf{sym}}$ *is the projector onto the symmetric subspace of* $(\mathbb{C}^N)^{\otimes k}$.

We will use the following elementary claim about unitary 2-designs in Parts I and II.

Claim 1 (Standard twirling)**.** *For any* n*-qubit unitary* 2*-design* $\mathfrak{D}$*,*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}}\left[(U\otimes U)^\dagger\cdot\Pi^{\mathsf{eq}}\cdot(U\otimes U)\right] = \frac{2}{N+1}\cdot\Pi^{N,2}_{\mathsf{sym}}. \tag{2.15}$$

Proof.

$$\begin{aligned}
\mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}}\left[(U^\dagger\otimes U^\dagger)\cdot\Pi^{\mathsf{eq}}\cdot(U\otimes U)\right] &= \mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}}\sum_{x\in[N]} U^\dagger|x\rangle\langle x|U\otimes U^\dagger|x\rangle\langle x|U && \text{(definition of } \Pi^{\mathsf{eq}}\text{)}\\
&= \mathop{\mathbb{E}}_{U}\sum_{x\in[N]} U^\dagger|x\rangle\langle x|U\otimes U^\dagger|x\rangle\langle x|U && (\mathfrak{D} \text{ is a 2-design})\\
&= N\cdot\mathop{\mathbb{E}}_{\psi}|\psi\rangle\langle\psi|\otimes|\psi\rangle\langle\psi| && (U^\dagger|x\rangle \text{ is a Haar-random state})\\
&= \frac{2}{N+1}\cdot\Pi^{N,2}_{\mathsf{sym}}. && \text{(Fact 2)}
\end{aligned}$$

□

From the above claim, we immediately obtain the following lemma, which was also also used by [MPSY24] to construct *non-adaptive* PRUs.

Lemma 2.1 (Twirling into the distinct subspace)**.** *Given two integers $n, t > 0$. Define the distinct subspace projector acting on nt qubits as follows,*

$$\Pi^{\text{dist}} \coloneqq \sum_{(x_1,\ldots,x_t)\in[N]^t_{\text{dist}}} |x_1\rangle\langle x_1| \otimes \ldots \otimes |x_t\rangle\langle x_t| \,. \tag{2.16}$$

For any n-qubit unitary 2-design $\mathfrak{D}$ and any state ρ on at least nt qubits, we have

$$\operatorname{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}}(\Pi^{\text{dist}}\otimes \mathsf{Id})\cdot(C^{\otimes t}\otimes \mathsf{Id})\cdot\rho\cdot(C^{\dagger,\otimes t}\otimes \mathsf{Id})\cdot(\Pi^{\text{dist}}\otimes \mathsf{Id})\right) \geq 1-\frac{t(t-1)}{N+1}. \tag{2.17}$$

Proof. From the definition of the distinct subspace projector, we have

$$\mathsf{Id}-\Pi^{\text{dist}} = \sum_{(x_1,\ldots,x_t)\in[N]^t\setminus[N]^t_{\text{dist}}} |x_1,\ldots,x_t\rangle\langle x_1,\ldots,x_t| \,. \tag{2.18}$$

Because for any $(x_1,\ldots,x_t)\in[N]^t\setminus[N]^t_{\text{dist}}$, there exists $i\neq j$, such that $x_i = x_j$, we have

$$\sum_{(x_1,\ldots,x_t)\in[N]^t\setminus[N]^t_{\text{dist}}} |x_1,\ldots,x_t\rangle\langle x_1,\ldots,x_t| \preceq \sum_{1\leq i<j\leq t} \Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}, \tag{2.19}$$

where $\preceq$ here denotes the PSD order and $\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}$ is the equality projector in Eq. (2.13) on the i-th and j-th n-qubit register $\mathsf{X}_i,\mathsf{X}_j$. This implies the following:

$$1-\operatorname{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}}(\Pi^{\text{dist}}\otimes \mathsf{Id})\cdot(C^{\otimes t}\otimes \mathsf{Id})\cdot\rho\cdot(C^{\dagger,\otimes t}\otimes \mathsf{Id})\cdot(\Pi^{\text{dist}}\otimes \mathsf{Id})\right) \tag{2.20}$$

$$= 1-\operatorname{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}}(\Pi^{\text{dist}}\otimes \mathsf{Id})\cdot(C^{\otimes t}\otimes \mathsf{Id})\cdot\rho\cdot(C^{\dagger,\otimes t}\otimes \mathsf{Id})\right) \tag{2.21}$$

$$= \operatorname{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}}\left(\sum_{(x_1,\ldots,x_t)\in[N]^t\setminus[N]^t_{\text{dist}}} |x_1,\ldots,x_t\rangle\langle x_1,\ldots,x_t|\otimes \mathsf{Id}\right)\cdot(C^{\otimes t}\otimes \mathsf{Id})\cdot\rho\cdot(C^{\dagger,\otimes t}\otimes \mathsf{Id})\right) \tag{2.22}$$

$$\leq \sum_{1\leq i<j\leq t} \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \operatorname{Tr}\left((\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\otimes \mathsf{Id})\cdot(C^{\otimes t}\otimes \mathsf{Id})\cdot\rho\cdot(C^{\dagger,\otimes t}\otimes \mathsf{Id})\right) \tag{2.23}$$

$$= \sum_{1\leq i<j\leq t} \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \operatorname{Tr}\left(\Pi^{\mathsf{eq}}_{\mathsf{X}_i,\mathsf{X}_j}\cdot C^{\otimes 2}\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\cdot C^{\dagger,\otimes 2}\right) \qquad (\text{where } \rho_{\mathsf{X}_i,\mathsf{X}_j} \coloneqq \operatorname{Tr}_{-\mathsf{X}_i,\mathsf{X}_j}(\rho))$$

$$= \sum_{1\leq i<j\leq t} \frac{2}{N+1}\operatorname{Tr}\left(\Pi^{N,2}_{\mathsf{sym}}\cdot\rho_{\mathsf{X}_i,\mathsf{X}_j}\right) \leq \sum_{1\leq i<j\leq t}\frac{2}{N+1} = \frac{t(t-1)}{N}. \tag{2.24}$$

This completes the proof. □

The following claim will only be used in Part II.

Notation 11. *Let*

$$|\mathsf{EPR}_N\rangle \coloneqq \frac{1}{\sqrt{N}}\sum_{x\in[N]} |x\rangle\,|x\rangle \,. \tag{2.25}$$

Claim 2 (Mixed twirling)**.** *For any n-qubit unitary 2-design $\mathfrak{D}$,*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}}\left[(U\otimes\overline{U})^\dagger\cdot\Pi^{\mathsf{eq}}\cdot(U\otimes\overline{U})\right] = |\mathsf{EPR}_N\rangle\langle\mathsf{EPR}_N| + \frac{1}{N+1}(\mathsf{Id}-|\mathsf{EPR}_N\rangle\langle\mathsf{EPR}_N|). \tag{2.26}$$

Proof. Label the registers that U and $\overline{U}$ act on as A and B respectively. For any operator X acting on A, B, define the partial transpose as

$$X^{T_B} = \Big(\sum_{i,j,k,\ell} X_{ijkl} \, |i\rangle\langle j|_A \otimes |k\rangle\langle \ell|_B \Big)^{T_B} = \sum_{i,j,k,\ell} X_{ijkl} \, |i\rangle\langle j|_A \otimes |\ell\rangle\langle k|_B \, . \tag{2.27}$$

We will use the identity

$$(U \otimes \overline{U})^\dagger \cdot X \cdot (U \otimes \overline{U}) = \Big((U \otimes U)^\dagger \cdot X^{T_B} \cdot (U \otimes U) \Big)^{T_B} . \tag{2.28}$$

Since $(\Pi^{\mathsf{eq}})^{T_B} = \Pi^{\mathsf{eq}}$,

$$\mathop{\mathbb{E}}_{U \leftarrow \mathfrak{D}} (U \otimes \overline{U})^\dagger \cdot \Pi^{\mathsf{eq}} \cdot (U \otimes \overline{U}) \tag{2.29}$$

$$= \Big(\mathop{\mathbb{E}}_{U \leftarrow \mathfrak{D}} (U \otimes U)^\dagger \cdot \Pi^{\mathsf{eq}} \cdot (U \otimes U) \Big)^{T_B} \tag{2.30}$$

$$= \Big(\frac{2}{N+1} \cdot \Pi^{N,2}_{\mathsf{sym}} \Big)^{T_B} \qquad \text{(by Claim 1)}$$

$$= \frac{2}{N+1} \cdot \left(\sum_{x \in [N]} |xx\rangle\langle xx| + \sum_{x,y \in [N], x<y} \Big(\frac{|xy\rangle + |yx\rangle}{\sqrt{2}} \Big) \Big(\frac{\langle xy| + \langle yx|}{\sqrt{2}} \Big) \right)^{T_B} \tag{2.31}$$

$$= \frac{2}{N+1} \cdot \left(\sum_{x \in [N]} |xx\rangle\langle xx| + \frac{1}{2} \sum_{x,y \in [N], x<y} \Big(|xy\rangle\langle xy| + |xy\rangle\langle yx| + |yx\rangle\langle xy| + |yx\rangle\langle yx| \Big) \right)^{T_B} \tag{2.32}$$

$$= \frac{2}{N+1} \cdot \left(\sum_{x \in [N]} |xx\rangle\langle xx| + \frac{1}{2} \sum_{x,y \in [N], x<y} \Big(|xy\rangle\langle xy| + |xx\rangle\langle yy| + |yy\rangle\langle xx| + |yx\rangle\langle yx| \Big) \right) \tag{2.33}$$

$$= \frac{2}{N+1} \cdot \left(\frac{1}{2} \sum_{x,y \in [N]} |xx\rangle\langle yy| + \frac{1}{2} \sum_{x,y \in [N]} |xy\rangle\langle xy| \right) \tag{2.34}$$

$$= \frac{1}{N+1} \cdot \mathsf{Id} + \frac{N}{N+1} |\mathsf{EPR}_N\rangle\langle \mathsf{EPR}_N| \tag{2.35}$$

$$= |\mathsf{EPR}_N\rangle\langle \mathsf{EPR}_N| + \frac{1}{N+1} (\mathsf{Id} - |\mathsf{EPR}_N\rangle\langle \mathsf{EPR}_N|). \tag{2.36}$$

This completes the proof. □

2.3 Oracle adversaries

We first define oracle adversaries that make only forward queries to an n-qubit unitary oracle $\mathcal{O}$. This definition will be used exclusively in Part I.

Definition 5 (Oracle adversaries with forward queries, used in Part I)**.** *A t-query oracle adversary $\mathcal{A}$ that makes only forward queries is parameterized by a sequence of $(n+m)$-qubit unitaries $(A_1, \ldots, A_t)$, which act on registers (A, B), where A is the n-qubit query register and B is an m-qubit ancilla. We assume without loss of generality that the adversary's initial state is $|0^{n+m}\rangle_{\mathsf{AB}}$. The state of the algorithm after t queries to $\mathcal{O}$ is*

$$|\mathcal{A}^{\mathcal{O}}_t\rangle_{\mathsf{AB}} \coloneqq \prod_{i=1}^{t} \Big(\mathcal{O}_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0^{n+m}\rangle_{\mathsf{AB}} \, . \tag{2.37}$$

We also define an oracle adversary that can make both forward and inverse queries to an n-qubit unitary oracle $\mathcal{O}$. This definition will be used exclusively in Part II.

Definition 6 (Oracle adversaries with forward and inverse queries, used in Part II)**.** *A t-query oracle adversary $\mathcal{A}$ that makes both forward and inverse queries is parameterized by*

- *a sequence of $(n+m)$-qubit unitaries $(A_1, \ldots, A_t)$, which act on registers (A, B), where A is the n-qubit query register and B is an m-qubit ancilla, and*
- *a sequence of bits $(b_1, \ldots, b_t)$ where $b_i = 0$ means that the adversary's ith oracle query is to $\mathcal{O}$, and $b_i = 1$ means that query is to $\mathcal{O}^\dagger$.*

We assume without loss of generality that the adversary's initial state is $|0^{n+m}\rangle_{\mathsf{AB}}$. The state of the algorithm after t queries to $\mathcal{O}$ is

$$|\mathcal{A}_t^{\mathcal{O}}\rangle_{\mathsf{AB}} \coloneqq \prod_{i=1}^{t} \left(\left((1-b_i) \cdot \mathcal{O}_{\mathsf{A}} + b_i \cdot \mathcal{O}_{\mathsf{A}}^\dagger \right) \cdot A_{i,\mathsf{AB}} \right) |0^{n+m}\rangle_{\mathsf{AB}} \,. \tag{2.38}$$

2.4 Pseudorandom unitaries

Definition 7 (pseudorandom unitaries)**.** *We say $\{\mathcal{U}_n\}_{n\in\mathbb{N}}$ is a secure PRU if, for all $n \in \mathbb{N}$, $\mathcal{U}_n = \{U_k\}_{k\in\mathcal{K}_n}$ is a set of n-qubit unitaries where $\mathcal{K}_n$ denotes the keyspace, satisfying the following:*

- ***Efficient computation:*** *There exists a $\mathrm{poly}(n)$-time quantum algorithm that implements the n-qubit unitary U_k for all $k \in \mathcal{K}_n$.*
- ***Indistinguishability from Haar:*** *For any oracle adversary $\mathcal{A}$ that runs in time $\mathrm{poly}(n)$ (the runtime is the total number of gates that $\mathcal{A}$ uses, counting oracle gates as 1), and measures a two-outcome observable $D_{\mathcal{A}}$ with eigenvalues $\{0,1\}$ after the queries, we have*

$$\left| \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathcal{U}_n} \mathrm{Tr}\left(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}}\rangle\langle\mathcal{A}^{\mathcal{O}}|_{\mathsf{AB}} \right) - \mathop{\mathbb{E}}_{\mathcal{O}\sim\mathsf{Haar}} \mathrm{Tr}\left(D_{\mathcal{A}} \cdot |\mathcal{A}^{\mathcal{O}}\rangle\langle\mathcal{A}^{\mathcal{O}}|_{\mathsf{AB}} \right) \right| \leq \mathsf{negl}(n), \tag{2.39}$$

  where $\mathsf{negl}(n)$ is any function that is $o(1/n^c)$ for all $c > 0$.

*A **standard PRU** (i.e., the original [JLS18] notion) is one where indistinguishability holds against oracle adversaries that only make forward queries to $\mathcal{O}$. A **strong PRU** is one where indistinguishability holds against oracle adversaries that make both forward and inverse queries to $\mathcal{O}$.*

2.5 Useful lemmas

The following lemma will be used in Part I to bound the distance between a pair of mixed states who purifications are related by a projection that acts only on the purifying register.

Lemma 2.2. *Let ρ_{CD} be a density matrix on registers C, D and let Π_{D} be a projector that acts on register D. Then*

$$\|\mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}}) - \mathrm{Tr}_{\mathsf{D}}(\Pi_{\mathsf{D}} \cdot \rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{D}})\|_1 = 1 - \mathrm{Tr}(\Pi_{\mathsf{D}} \cdot \rho_{\mathsf{CD}}). \tag{2.40}$$

Proof. We can decompose $\mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}})$ as follows:

$$\begin{aligned} \mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}}) &= \mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{D}}) + \mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}} \cdot (\mathsf{Id} - \Pi_{\mathsf{D}})) && (2.41) \\ &= \mathrm{Tr}_{\mathsf{D}}(\Pi_{\mathsf{D}} \cdot \rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{D}}) + \mathrm{Tr}_{\mathsf{D}}((\mathsf{Id} - \Pi_{\mathsf{D}}) \cdot \rho_{\mathsf{CD}} \cdot (\mathsf{Id} - \Pi_{\mathsf{D}})) && (2.42) \end{aligned}$$

where the second equality uses the fact that $\Pi_{\mathsf{D}} = \mathsf{Id}_{\mathsf{C}} \otimes \Pi'_{\mathsf{D}}$, which allows us to invoke the cyclic property of Tr_{D}. Using Eq. (2.42), we have

$$\begin{aligned}
&\|\mathrm{Tr}_{\mathsf{D}}(\rho_{\mathsf{CD}}) - \mathrm{Tr}_{\mathsf{D}}(\Pi_{\mathsf{D}} \cdot \rho_{\mathsf{CD}} \cdot \Pi_{\mathsf{D}})\|_1 && (2.43)\\
&= \|\mathrm{Tr}_{\mathsf{D}}((\mathsf{Id} - \Pi_{\mathsf{D}}) \cdot \rho_{\mathsf{CD}} \cdot (\mathsf{Id} - \Pi_{\mathsf{D}}))\|_1 && (2.44)\\
&= \mathrm{Tr}((\mathsf{Id} - \Pi_{\mathsf{D}}) \cdot \rho_{\mathsf{CD}} \cdot (\mathsf{Id} - \Pi_{\mathsf{D}})) && (\text{since } \|M\|_1 = \mathrm{Tr}(M) \text{ for PSD } M)\\
&= \mathrm{Tr}((\mathsf{Id} - \Pi_{\mathsf{D}}) \cdot \rho_{\mathsf{CD}}) && (2.45)\\
&= 1 - \mathrm{Tr}(\Pi_{\mathsf{D}} \cdot \rho_{\mathsf{CD}}). && (2.46)
\end{aligned}$$

□

We will use the following "sequential" gentle measurement lemma in Part II.

Lemma 2.3 (sequential gentle measurement)**.** *Let $|\psi\rangle$ be a normalized state, $P_1, \ldots, P_t$ be projectors, and $U_1, \ldots, U_t$ be unitaries.*

$$\|U_t \ldots U_1 |\psi\rangle - P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2 \leq t\sqrt{1 - \|P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2^2}. \tag{2.47}$$

To prove this, we will need the following version of the standard gentle measurement lemma.

Lemma 2.4 (gentle measurement)**.** *For any projector Π and sub-normalized state $|\psi\rangle$ satisfying $\langle\psi|\psi\rangle \leq 1$, we have*

$$\|(\mathsf{Id} - \Pi)|\psi\rangle\|_2 \leq \sqrt{1 - \|\Pi|\psi\rangle\|_2^2}. \tag{2.48}$$

Proof of Lemma 2.4. By direct expansion, we have

$$\||\psi\rangle - \Pi|\psi\rangle\|_2^2 = \langle\psi|(\mathsf{Id} - \Pi)|\psi\rangle = \langle\psi|\psi\rangle - \langle\psi|\Pi|\psi\rangle \leq 1 - \|\Pi|\psi\rangle\|_2^2. \tag{2.49}$$

□

Proof of Lemma 2.3. We prove this lemma by induction. For $t = 0$, we have $\||\psi\rangle - |\psi\rangle\|_2 = 0 = 1 - \||\psi\rangle\|_2^2$. So the base case holds. Suppose the inductive hypothesis holds for $t-1$, i.e.,

$$\begin{aligned}
\|U_{t-1} \ldots U_1 |\psi\rangle - P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2 &\leq (t-1)\sqrt{1 - \|P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2^2} && (2.50)\\
&= (t-1)\sqrt{1 - \|U_t P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2^2} && (2.51)\\
&\leq (t-1)\sqrt{1 - \|P_t U_t P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2^2}. && (2.52)
\end{aligned}$$

The second line uses the unitary invariance of $\|\cdot\|_2$. The third line uses the fact that P_t is a projector and hence cannot increase the norm. We can use the unitary invariance of $\|\cdot\|_2$ to obtain

$$\|U_{t-1} \ldots U_1 |\psi\rangle - P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2 = \|U_t \ldots U_1 |\psi\rangle - U_t P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2. \tag{2.53}$$

Next we use Lemma 2.4 to obtain

$$\|(\mathsf{Id} - P_t) U_t P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2 \leq \sqrt{1 - \|P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2^2}. \tag{2.54}$$

Together, we have

$$\begin{aligned}
&\|U_t \ldots U_1 |\psi\rangle - P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2 && (2.55)\\
&\leq \|U_{t-1} \ldots U_1 |\psi\rangle - P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2 + \|(\mathsf{Id} - P_t) U_t P_{t-1} U_{t-1} \ldots P_1 U_1 |\psi\rangle\|_2 && (2.56)\\
&\leq (t-1)\sqrt{1 - \|P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2^2} + \sqrt{1 - \|P_t U_t \ldots P_1 U_1 |\psi\rangle\|_2^2}. && (2.57)
\end{aligned}$$

This concludes the proof. □

Part I
Standard PRUs

The goal of Part I is to construct standard PRUs (i.e., the definition of [JLS18]), which are secure against adversaries that only make forward queries to the unitary oracle.

3 The purified permutation-function oracle

In this section, we analyze the view of an adversary that makes forward queries to an oracle for $P_\pi \cdot F_f$, for uniformly random $\pi \leftarrow \mathsf{Sym}_N$ and $f \leftarrow \{0,1\}^N$. These operators are defined as

$$P_\pi \coloneqq \sum_{x\in[N]} |\pi(x)\rangle\langle x| \quad \text{and} \quad F_f \coloneqq \sum_{x\in[N]} (-1)^{f(x)} |x\rangle\langle x| \,. \tag{3.1}$$

Our first step will be to consider a purification of the adversary's state where the randomness of π and f is replaced by the uniform superposition

$$\frac{1}{\sqrt{N!}} \sum_{\pi\in\mathsf{Sym}_N} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f\in\{0,1\}^N} |f\rangle_{\mathsf{F}} \,, \tag{3.2}$$

and each query is implemented by the purified permutation-function oracle pfO, which applies $P_\pi \cdot F_f$ controlled on $|\pi\rangle\,|f\rangle$.

Definition 8 (purified permutation-function oracle)**.** *The purified permutation-function oracle* pfO *is a unitary acting on registers* $\mathsf{A},\mathsf{P},\mathsf{F}$*, where*

- P *is a register associated with the Hilbert space* $\mathcal{H}_{\mathsf{P}}$*, defined to be the span of the orthonormal states* $|\pi\rangle$ *for all* $\pi \in \mathsf{Sym}_N$*.*
- F *is a register associated with the Hilbert space* $\mathcal{H}_{\mathsf{F}}$*, defined to be the span of the orthonormal states* $|f\rangle$ *for all* $f \in \{0,1\}^N$*.*

The unitary pfO *is defined to act as follows:*

$$\mathsf{pfO}_{\mathsf{APF}} |x\rangle_{\mathsf{A}}\, |\pi\rangle_{\mathsf{P}}\, |f\rangle_{\mathsf{F}} \coloneqq (-1)^{f(x)} |\pi(x)\rangle_{\mathsf{A}}\, |\pi\rangle_{\mathsf{P}}\, |f\rangle_{\mathsf{F}} \,, \tag{3.3}$$

for all $x \in [N], \pi \in \mathsf{Sym}_N$*, and* $f \in \{0,1\}^N$*.*

When P and F are initialized to the uniform superposition over permutations and functions respectively, the view of an adversary that queries the pfO is equivalent to the view of an adversary that queries the standard oracle $P_\pi \cdot F_f$, for uniformly random $\pi \leftarrow \mathsf{Sym}_N$ and $f \leftarrow \{0,1\}^N$.

Claim 3 (Equivalence of the purified and standard oracles)**.** *For any oracle adversary* $\mathcal{A}$*, the following oracle instantiations are perfectly indistinguishable:*

- *(Queries to a random* $P_\pi \cdot F_f$*) Sample a uniformly random* $\pi \leftarrow \mathsf{Sym}_N, f \leftarrow \{0,1\}^N$*. On each query, apply* $P_\pi \cdot F_f$ *to register* A*.*
- *(Queries to* pfO*) Initialize registers* P,F *to* $\frac{1}{\sqrt{N!}} \sum_{\pi\in\mathsf{Sym}_N} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f\in\{0,1\}^N} |f\rangle_{\mathsf{F}}$*. At each query, apply* pfO *to registers* $\mathsf{A},\mathsf{P},\mathsf{F}$*.*

Proof. Since the adversary's view does not contain the P, F registers, the adversary's view in the second case is unchanged if the P, F registers are measured at the end. Since pfO is controlled on the P, F registers, the queries to pfO commute with the measurement of the P, F registers. Hence, measuring the P, F registers at the end produces the same view as measuring at the beginning, which is equivalent to the first case. □

The key to understanding the oracle pfO is to consider how it acts on the following "pf-relation states", defined below.

Definition 9 (pf-relation state)**.** *For $0 \le t \le N$ and $R = \{(x_1, y_1), \ldots, (x_t, y_t)\} \in \mathcal{R}_t$, let*

$$|\mathsf{pf}_R\rangle_{\mathsf{PF}} \coloneqq \frac{1}{\sqrt{(N-t)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} |f\rangle_{\mathsf{F}}, \tag{3.4}$$

where $\delta_{\pi,R}$ is an indicator variable that equals 1 if $\pi(x) = y$ for all $(x, y) \in R$, and is 0 otherwise.

Note that for $t = 0$ and $R = \varnothing$, the pf-relation state $|\mathsf{pf}_\varnothing\rangle_{\mathsf{PF}}$ is the uniform superposition over all permutations $\pi \in \mathsf{Sym}_N$ and all functions $f \in \{0,1\}^N$,

$$|\mathsf{pf}_\varnothing\rangle_{\mathsf{PF}} \coloneqq \frac{1}{\sqrt{N!}} \sum_{\pi \in \mathsf{Sym}_N} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} |f\rangle_{\mathsf{F}}. \tag{3.5}$$

3.1 Orthonormality of the pf-relation states

Claim 4 (Orthonormality of the distinct sets of pf-relation states)**.** $\{|\mathsf{pf}_R\rangle\}_{R \in \mathcal{R}^{\mathsf{bij}}}$ *forms a set of orthonormal vectors.*

Proof of Claim 4. We first recall the definition of $|\mathsf{pf}_R\rangle$:

$$|\mathsf{pf}_R\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{(N-t)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} |f\rangle_{\mathsf{F}}. \tag{3.6}$$

For $x \in [N]$, let $e_x \in \{0,1\}^N$ denote the N-dimensional vector that has a 1 in the x-th position, and is 0 everywhere else. Then by writing $f(x)$ as $f(x) = f \cdot e_x$, we get

$$\frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} |f\rangle_{\mathsf{F}} = \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f \cdot (e_{x_1}+\cdots+e_{x_t})} |f\rangle_{\mathsf{F}} \tag{3.7}$$

$$= H^{\otimes N} |e_{x_1} + \cdots + e_{x_t} \pmod 2\rangle_{\mathsf{F}}. \tag{3.8}$$

When $x_1, \ldots, x_t$ are distinct, $e_{x_1} + \cdots + e_{x_t} \pmod 2$ is a vector in $\{0,1\}^N$ whose x-th entry is 1 if $x \in \{x_1, \ldots, x_t\}$, and 0 otherwise. Since this is simply the indicator vector for the set $\{x_1, \ldots, x_t\}$, there exists an isometry that maps

$$\frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} |f\rangle_{\mathsf{F}} \mapsto |\{x_1, \ldots, x_t\}\rangle. \tag{3.9}$$

Applying this to the F register of $|\mathsf{pf}_R\rangle$, this tells us there is an isometry M such that for all $R \in \mathcal{R}^{\mathsf{bij}}$,

$$M : |\mathsf{pf}_R\rangle \mapsto \frac{1}{\sqrt{(N-t)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R} |\pi\rangle_{\mathsf{P}} \otimes |\{x_1, \ldots, x_t\}\rangle. \tag{3.10}$$

Consider $R, S \in \mathcal{R}^{\mathsf{bij}}$, where $R = \{(x_1, y_1), \ldots, (x_{|R|}, y_{|R|})\}$ and $S = \{(x'_1, y'_1), \ldots, (x'_{|S|}, y'_{|S|})\}$.

$$\langle \mathsf{pf}_R | \mathsf{pf}_S \rangle = \langle \mathsf{pf}_R | \, M^\dagger \cdot M \, | \mathsf{pf}_S \rangle \tag{3.11}$$

$$= \frac{1}{\sqrt{(N-|R|)!(N-|S|)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R} \cdot \delta_{\pi,S} \, \langle \{x_1, \ldots, x_{|R|}\} | \{x'_1, \ldots, x'_{|S|}\} \rangle \, . \tag{3.12}$$

This expression is equal to zero if $\mathrm{Dom}(R) \neq \mathrm{Dom}(S)$ due to the $\langle \{x_1, \ldots, x_{|R|}\} | \{x'_1, \ldots, x'_{|S|}\} \rangle$ term. Thus, it remains to consider R, S such that $\mathrm{Dom}(R) = \mathrm{Dom}(S)$. This means that $|R| = |S|$ and thus Eq. (3.12) simplifies to

$$\frac{1}{(N-|R|)!} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R} \cdot \delta_{\pi,S}. \tag{3.13}$$

There are two cases to consider:

- In the first case, $R \neq S$. Then there exists x, y, y' such that $(x, y) \in R$, $(x, y') \in S$, and $y \neq y'$. But then the above expression will be 0, since there are no permutations π satisfying both $\pi(x) = y$ and $\pi(x) = y'$.
- In the other case, $R = S$. Then the sum is over all permutations P such that $\pi(x) = y$ for all $(x, y) \in R$. There are $(N - |R|)!$ such permutations, and so in this case the sum becomes 1.

This completes the proof. □

3.2 How pfO acts on the pf-relation states

Claim 5 (Action of pfO on pf-relation states)**.** *For $0 \leq t < N$, $R \in \mathcal{R}_t$ and $x \in [N]$,*

$$\mathsf{pfO} \, |x\rangle_{\mathsf{A}} \, |\mathsf{pf}_R\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{N-|R|}} \sum_{y \in [N]} |y\rangle_{\mathsf{A}} \, |\mathsf{pf}_{R \cup \{(x,y)\}}\rangle_{\mathsf{PF}} \, . \tag{3.14}$$

Proof of Claim 5. From the definitions of pfO and $|\mathsf{pf}_R\rangle$ (Eq. (3.3) and Eq. (3.4)), we have

$$\mathsf{pfO} \, |x\rangle_{\mathsf{A}} \, |\mathsf{pf}_R\rangle_{\mathsf{PF}}$$

$$= \sum_{\pi \in \mathsf{Sym}_N} (-1)^{f(x)} \, |\pi(x)\rangle_{\mathsf{A}} \frac{1}{\sqrt{(N-t)!}} \delta_{\pi,R} \, |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} \, |f\rangle_{\mathsf{F}} \, . \tag{3.15}$$

We now rewrite the right-hand side of Eq. (3.15) using the substitution $|\pi(x)\rangle = \sum_{y \in [N]} \delta_{\pi(x)=y} \, |y\rangle$. This gives

$$(3.15) = \sum_{\pi \in \mathsf{Sym}_N} (-1)^{f(x)} \sum_{y \in [N]} \delta_{\pi,\{(x,y)\}} \, |y\rangle_{\mathsf{A}} \frac{1}{\sqrt{(N-t)!}} \delta_{\pi,R} \, |\pi\rangle_{\mathsf{P}}$$

$$\otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} \, |f\rangle_{\mathsf{F}} \, . \tag{3.16}$$

Since $\delta_{\pi,R} \cdot \delta_{\pi,\{(x,y)\}} = \delta_{\pi,R\cup\{(x,y)\}}$, we can rearrange the expression to get

$$(3.16) = \frac{1}{\sqrt{N-t}} \sum_{y \in [N]} |y\rangle_{\mathsf{A}} \frac{1}{\sqrt{(N-t-1)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,R\cup\{(x,y)\}} \, |\pi\rangle$$

$$\otimes \frac{1}{\sqrt{2^N}} \sum_{f\in\{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)+f(x)} |f\rangle_{\mathsf{F}} \tag{3.17}$$

$$= \frac{1}{\sqrt{N-t}} \sum_{y\in[N]} |y\rangle_{\mathsf{A}} \, |\mathsf{pf}_{R\cup\{(x,y)\}}\rangle_{\mathsf{PF}} \,, \tag{3.18}$$

which completes the proof. □

4 The path-recording oracle V

In this section, we define the *path-recording oracle*. The path-recording oracle V acts on an n-qubit query register A held by the adversary, as well as a variable-length relation R containing a relation state $|R\rangle$ (see Section 2.1). In section Section 4.3, we connect the path-recording oracle V to the pfO oracle. In Appendix A.2, we sketch how to implement V efficiently.

4.1 Defining V

Definition 10 (Path-recording oracle)**.** *The path-recording oracle V is a linear map $V : \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}} \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}}$ defined as follows. For all $x \in [N]$ and $R \in \mathcal{R}^{\mathsf{inj}}$ such that $|R| < N$,*

$$V : |x\rangle_{\mathsf{A}} \, |R\rangle_{\mathsf{R}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}} \, |R\cup\{(x,y)\}\rangle_{\mathsf{R}} \,. \tag{4.1}$$

Note that $R\cup\{(x,y)\} \in \mathcal{R}^{\mathsf{inj}}$ since $y \notin \mathrm{Im}(R)$.

Lemma 4.1 (Partial isometry)**.** *The path-recording oracle V is an isometry on the subspace of $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}}$ spanned by the states $|x\rangle \, |R\rangle$ for $x \in [N]$ and $R \in \mathcal{R}^{\mathsf{inj}}$ such that $|R| < N$.*

Proof of Lemma 4.1. To prove that V is an isometry on the specified subspace, it suffices to show that for all $x, x' \in [N]$ and $R, R' \in \mathcal{R}^{\mathsf{inj}}$ with $|R|, |R'| < N$,

$$\langle x'|_{\mathsf{A}} \, \langle R'|_{\mathsf{R}} \, V^\dagger \cdot V \, |x\rangle_{\mathsf{A}} \, |R\rangle_{\mathsf{R}} = \langle x'|x\rangle_{\mathsf{A}} \cdot \langle R'|R\rangle_{\mathsf{R}} \,. \tag{4.2}$$

We proceed by considering two cases:

- **Case 1:** $|R| \neq |R'|$. $V \, |x\rangle_{\mathsf{A}} \, |R\rangle_{\mathsf{R}}$ and $V \, |x'\rangle_{\mathsf{A}} \, |R'\rangle_{\mathsf{R}}$ are orthogonal because, by the definition of V, these two states are supported on relation states of different sizes. Therefore, the left-hand side of Eq. (4.2) is zero, which equals the right-hand side, since $\langle R'|R\rangle_{\mathsf{R}} = 0$ for $|R| \neq |R'|$.
- **Case 2:** $|R| = |R'| = t$ for some $0 \leq t \leq N-1$. In this case, we expand the left-hand side:

$$\begin{aligned} &\langle x'|_{\mathsf{A}} \, \langle R'|_{\mathsf{R}} \, V^\dagger \cdot V \, |x\rangle_{\mathsf{A}} \, |R\rangle_{\mathsf{R}} \\ &= \left(\frac{1}{\sqrt{N-t}} \sum_{\substack{y'\in[N],\\ y'\notin \mathrm{Im}(R')}} \langle y'|_{\mathsf{A}} \, \langle R'\cup\{(x',y')\}|_{\mathsf{R}} \right) \cdot \left(\frac{1}{\sqrt{N-t}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}} \, |R\cup\{(x,y)\}\rangle_{\mathsf{R}} \right) \end{aligned} \tag{4.3}$$

$$= \frac{1}{N-t} \sum_{\substack{y\in[N]\\ y\notin \mathrm{Im}(R')\cup\mathrm{Im}(R)}} \langle R'\cup\{(x',y)\}|R\cup\{(x,y)\}\rangle_{\mathsf{R}} \tag{4.4}$$

  Now, we consider two sub-cases:

– **Case 2a:** $(x, R) \neq (x', R')$. For $y \notin \mathrm{Im}(R) \cup \mathrm{Im}(R')$, the term $\langle R' \cup \{(x', y)\} | R \cup \{(x, y)\} \rangle_{\mathsf{R}}$ is always zero because either $x \neq x'$ or $R \neq R'$. Therefore, Eq. (4.4) is equal to zero, which matches the right-hand side of the original equation.

– **Case 2b:** $(x, R) = (x', R')$. In this case, we have:

$$(4.4) = \frac{1}{N-t} \sum_{y \in [N] \setminus \mathrm{Im}(R)} \langle R \cup \{(x, y)\} | R \cup \{(x, y)\} \rangle_{\mathsf{R}} \tag{4.5}$$

$$= \frac{1}{N-t} \cdot (N-t) \cdot 1 = 1, \tag{4.6}$$

which again matches the right-hand side of the original equation.

This shows that Eq. (4.2) holds in all cases, completing the proof. □

Next, we define the state $|\mathcal{A}_t^V\rangle_{\mathsf{ABR}}$ to be the state of the state of the entire system after the adversary has made t queries to the path recording oracle, with the R register initialized to $|\varnothing\rangle$, the state associated with the empty set.

Definition 11. *Given a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A_{1,\mathsf{AB}}, \ldots, A_{t,\mathsf{AB}})$, define the state*

$$|\mathcal{A}_t^V\rangle_{\mathsf{ABR}} \coloneqq \prod_{i=1}^{t} \left(V \cdot A_{i,\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \, |\varnothing\rangle_{\mathsf{R}} \,. \tag{4.7}$$

In fact, it will be useful to define a version of this state in which an arbitrary n-qubit unitary G is applied to the adversary's query register A before each query to V.

Definition 12. *Given an n-qubit unitary G and a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A_{1,\mathsf{AB}}, \ldots, A_{t,\mathsf{AB}})$, define the state*

$$|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}} \coloneqq \prod_{i=1}^{t} \left(V \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \, |\varnothing\rangle_{\mathsf{R}} \,. \tag{4.8}$$

One consequence of Lemma 4.1 is that $|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$ has unit norm as long as $t \leq N$.

Lemma 4.2 ($|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$ has unit norm)**.** *For any adversary $\mathcal{A}$ making $t \leq N$ forward queries, and any n-qubit unitary G, $|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$ has unit norm.*

Proof of Lemma 4.2. We say that a state on registers $(\mathsf{A}, \mathsf{B}, \mathsf{R})$ is supported on $\mathcal{R}^{\mathsf{inj}}$ if the state is contained in the span of $|x\rangle_{\mathsf{A}} \, |z\rangle_{\mathsf{B}} \, |R\rangle_{\mathsf{R}}$ for $R \in \mathcal{R}^{\mathsf{inj}}$ and any x, z. We will prove by induction on t that for all $0 \leq t \leq N$, $|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$ is a unit-norm state supported on $\mathcal{R}_t^{\mathsf{inj}}$.

Base case ($t = 0$): $|\mathcal{A}_0^{V \cdot G}\rangle = |0\rangle_{\mathsf{AB}} \, |\varnothing\rangle_{\mathsf{R}}$. This state clearly has unit norm, and $|\varnothing\rangle_{\mathsf{R}} \in \mathcal{R}_0^{\mathsf{inj}}$, so the claim holds for $t = 0$.

Inductive step: Assume the claim is true for some $0 \leq t < N$, i.e., $|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$ is a unit-norm state supported on $\mathcal{R}_t^{\mathsf{inj}}$. We will prove that it must hold for $t + 1$. By definition, we have:

$$|\mathcal{A}_{t+1}^{V \cdot G}\rangle = V \cdot G_{\mathsf{A}} \cdot A_{t+1,\mathsf{AB}} \, |\mathcal{A}_t^{V \cdot G}\rangle \tag{4.9}$$

This state is unit norm because:

1. $G_{\mathsf{A}} \cdot A_{t+1,\mathsf{AB}}$ is a unitary that acts only on the A and B registers, and so $G_{\mathsf{A}} \cdot A_{t+1,\mathsf{AB}} \, |\mathcal{A}_t^{V \cdot G}\rangle$ is still a unit-norm state supported on $\mathcal{R}_t^{\mathsf{inj}}$.

2. By Lemma 4.1, V is an isometry on states supported on $\mathcal{R}_t^{\mathsf{inj}}$. Moreover, the definition of V, ensures that it maps states supported on $\mathcal{R}_t^{\mathsf{inj}}$ to states supported on $\mathcal{R}_{t+1}^{\mathsf{inj}}$ for $0 \leq t < N$. Thus, $|\Psi_{t+1}^G\rangle$ is a unit-norm state supported on $\mathcal{R}_{t+1}^{\mathsf{inj}}$.

Hence, for all $0 \leq t \leq N$, $|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}}$ is a unit-norm state supported on $\mathcal{R}_t^{\mathsf{inj}}$. □

4.2 Right unitary invariance

Our next step is to prove that V satisfies *right unitary invariance*: for any unitary G, queries to $V \cdot G_{\mathsf{A}}$ are perfectly indistinguishable from queries to V, from the point of view of the adversary who cannot access the purifying register R. This is captured by the following lemma.

Lemma 4.3 (Right unitary invariance)**.** *For any n-qubit unitary G, we have*

$$|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}} = (G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}})\,|\mathcal{A}_t^{V}\rangle_{\mathsf{ABR}}\,. \tag{4.10}$$

Note that

$$\begin{aligned}
&\mathrm{Tr}_{\mathsf{R}}(\,|\mathcal{A}_t^{V\cdot G}\rangle\langle\mathcal{A}_t^{V\cdot G}|_{\mathsf{ABR}}) \\
&= \mathrm{Tr}_{\mathsf{R}}((G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}})\,|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\,(G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}})^\dagger) && \text{(by Lemma 4.3)} \\
&= \mathrm{Tr}_{\mathsf{R}}(\,|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}), && \text{(by the cyclic property of } \mathrm{Tr}_{\mathsf{R}})
\end{aligned}$$

where the first line corresponds to the adversary's view after making t queries to $V \cdot G_{\mathsf{A}}$, and the last line corresponds to its view after making t queries to V.

Fact 3 (Explicit form)**.** *From the definition of V and $|R\rangle_{\mathsf{R}}$, we can expand out $|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}}$ to obtain*

$$|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}} = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t} \Big(\,|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}}\Big)\,|0\rangle_{\mathsf{AB}}\right] \otimes |\{(x_i,y_i)\}_{i=1}^t\rangle_{\mathsf{R}} \tag{4.11}$$

$$\begin{aligned}
&= \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t} \Big(\,|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}}\Big)\,|0\rangle_{\mathsf{AB}}\right] \\
&\otimes \frac{1}{\sqrt{t!}} \sum_{\pi\in\mathsf{Sym}_t} \left(S_\pi\,|x_1\rangle_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \ldots |x_t\rangle_{\mathsf{R}_{\mathsf{X},t}^{(t)}}\right) \otimes \left(S_\pi\,|y_1\rangle_{\mathsf{R}_{\mathsf{Y},1}^{(t)}} \ldots |y_t\rangle_{\mathsf{R}_{\mathsf{Y},t}^{(t)}}\right),
\end{aligned} \tag{4.12}$$

Proof of Lemma 4.3. Our proof will use the following trivial identities for registers A and $(\mathsf{R}_{\mathsf{X},i}^{(t)})_{i\in[N]}$:

$$\sum_{z\in[N]} |z\rangle\langle z|_{\mathsf{A}} = \mathsf{Id}_{\mathsf{A}}, \tag{4.13}$$

$$\sum_{z\in[N]} |z\rangle\langle z|_{\mathsf{R}_{\mathsf{X},i}^{(t)}} = \mathsf{Id}_{\mathsf{R}_{\mathsf{X},i}^{(t)}}. \tag{4.14}$$

For any n-qubit unitary G and $x, z \in [N]$, we have

$$\langle x|_{\mathsf{A}}\,G_{\mathsf{A}}\,|z\rangle_{\mathsf{A}} = \langle x|_{\mathsf{R}_{\mathsf{X},i}^{(t)}}\,G_{\mathsf{R}_{\mathsf{X},i}^{(t)}}\,|z\rangle_{\mathsf{R}_{\mathsf{X},i}^{(t)}}\,. \tag{4.15}$$

Therefore, we have

$$\begin{aligned}
\sum_{x\in[N]} |x\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}} \otimes \langle x|_{\mathsf{A}}\, G_{\mathsf{A}} &= \sum_{x,z\in[N]} |x\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}} \otimes (\langle x|_{\mathsf{A}}\, G_{\mathsf{A}}\, |z\rangle_{\mathsf{A}})\ \langle z|_{\mathsf{A}} && \text{(Using Eq. (4.13))}\\
&= \sum_{x,z\in[N]} |x\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}} \otimes \left(\langle x|_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, G_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, |z\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\right) \langle z|_{\mathsf{A}} && \text{(Using Eq. (4.15))}\\
&= \sum_{x,z\in[N]} \left(|x\rangle\langle x|_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, G_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, |z\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\right) \otimes \langle z|_{\mathsf{A}} && (4.16)\\
&= \sum_{z\in[N]} G_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, |z\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}} \otimes \langle z|_{\mathsf{A}} && \text{(Using Eq. (4.14))}\\
&= \sum_{x\in[N]} G_{\mathsf{R}^{(t)}_{\mathsf{X},i}}\, |x\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},i}} \otimes \langle x|_{\mathsf{A}}\,. && \text{(Relabeling } z \text{ with } x)
\end{aligned}$$

Applying the above identity to registers $\mathsf{R}^{(t)}_{\mathsf{X},1},\ldots,\mathsf{R}^{(t)}_{\mathsf{X},t}$ to Fact 3 yields

$$|\mathcal{A}^{V\cdot G}_t\rangle = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t\\(y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle_{\mathsf{A}} \otimes \langle x_i|_{\mathsf{A}}\, G_{\mathsf{A}}\cdot A_{i,\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes \tag{4.17}$$

$$\frac{1}{\sqrt{t!}} \sum_{\pi\in\mathsf{Sym}_t} \left(S_\pi\, |x_1\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \ldots |x_t\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},t}}\right) \otimes \left(S_\pi\, |y_1\rangle_{\mathsf{R}^{(t)}_{\mathsf{Y},1}} \ldots |y_t\rangle_{\mathsf{R}^{(t)}_{\mathsf{Y},t}}\right) \tag{4.18}$$

$$= \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t\\(y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot A_{i,\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right] \otimes \tag{4.19}$$

$$\frac{1}{\sqrt{t!}} \sum_{\pi\in\mathsf{Sym}_t} \left(S_\pi\, G_{\mathsf{R}^{(t)}_{\mathsf{X},1}}\, |x_1\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \ldots G_{\mathsf{R}^{(t)}_{\mathsf{X},t}}\, |x_t\rangle_{\mathsf{R}^{(t)}_{\mathsf{X},t}}\right) \otimes \left(S_\pi\, |y_1\rangle_{\mathsf{R}^{(t)}_{\mathsf{Y},1}} \ldots |y_t\rangle_{\mathsf{R}^{(t)}_{\mathsf{Y},t}}\right) \tag{4.20}$$

$$= (G_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \otimes \ldots \otimes G_{\mathsf{R}^{(t)}_{\mathsf{X},t}})\, |\mathcal{A}^{V}_t\rangle \tag{4.21}$$

The last line follows from the fact that $(G_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \otimes \ldots \otimes G_{\mathsf{R}^{(t)}_{\mathsf{X},t}})$ acts identically on all t registers, so

$$S_\pi \cdot (G_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \otimes \ldots \otimes G_{\mathsf{R}^{(t)}_{\mathsf{X},t}}) = (G_{\mathsf{R}^{(t)}_{\mathsf{X},1}} \otimes \ldots \otimes G_{\mathsf{R}^{(t)}_{\mathsf{X},t}}) \cdot S_\pi. \tag{4.22}$$

This concludes the proof. □

Corollary 4.1 (Trace distance between original state and the projected state)**.**

$$\left\| \mathrm{Tr}_{\mathsf{R}}\left(\Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}^{V\cdot C}_t\rangle\langle\mathcal{A}^{V\cdot C}_t|_{\mathsf{ABR}} \cdot \Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\right) - \mathrm{Tr}_{\mathsf{R}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}^{V\cdot C}_t\rangle\langle\mathcal{A}^{V\cdot C}_t|_{\mathsf{ABR}}\right)\right\|_1 \le \frac{t(t-1)}{N+1}. \tag{4.23}$$

Proof. The trace distance can be bounded as follows,

$$\left\| \mathrm{Tr}_{\mathsf{R}}\left(\Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}^{V\cdot C}_t\rangle\langle\mathcal{A}^{V\cdot C}_t|_{\mathsf{ABR}} \cdot \Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\right) - \mathrm{Tr}_{\mathsf{R}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}^{V\cdot C}_t\rangle\langle\mathcal{A}^{V\cdot C}_t|_{\mathsf{ABR}}\right)\right\|_1 \tag{4.24}$$

$$= 1 - \mathrm{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X} \cdot |\mathcal{A}^{V\cdot C}_t\rangle\langle\mathcal{A}^{V\cdot C}_t|_{\mathsf{ABR}} \cdot \Pi^{\mathrm{dist}}_{\mathsf{R}^{(t)}_X}\right) \qquad \text{(Lemma 2.2)}$$

$$= 1 - \mathrm{Tr}\left(\mathop{\mathbb{E}}_{C \leftarrow \mathfrak{D}} \Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot C^{\otimes t}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot |\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABPF}} \cdot C^{\otimes t}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot \Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \right) \qquad \text{(By Lemma 4.3)}$$

$$\leq \frac{t(t-1)}{N+1}, \qquad \text{(By Lemma 2.1)}$$

which completes the proof of this corollary. □

4.3 Relating V to pfO

We now connect the path-recording oracle V to the pfO oracle defined previously. We begin by defining the pfO analog of $|\mathcal{A}_t^{V \cdot G}\rangle_{\mathsf{ABR}}$.

Definition 13. *Given an n-qubit unitary G and a t-query adversary $\mathcal{A}$ specified by a t-tuple of unitaries $(A_{1,\mathsf{AB}}, \ldots, A_{t,\mathsf{AB}})$, define*

$$|\mathcal{A}_t^{\mathsf{pfO} \cdot G}\rangle_{\mathsf{ABPF}} := \prod_{i=1}^{t} \left(\mathsf{pfO} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \, |\mathsf{pf}_{\varnothing}\rangle_{\mathsf{PF}} \,. \tag{4.25}$$

Recall that

$$|\mathsf{pf}_{\varnothing}\rangle_{\mathsf{PF}} := \frac{1}{\sqrt{N!}} \sum_{\pi \in \mathsf{Sym}_N} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} |f\rangle_{\mathsf{F}} \,. \tag{4.26}$$

We can expand the definition of $|\mathcal{A}_t^{\mathsf{pfO} \cdot G}\rangle_{\mathsf{ABPF}}$ to obtain the following.

Fact 4 (Explicit form of $|\mathcal{A}_t^{\mathsf{pfO} \cdot G}\rangle_{\mathsf{ABPF}}$)**.**

$$|\mathcal{A}_t^{\mathsf{pfO} \cdot G}\rangle_{\mathsf{ABPF}} = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t) \in [N]^t \\ (y_1,\ldots,y_t) \in [N]^t}} \left[\prod_{i=1}^{t} \left(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \right) |0\rangle_{\mathsf{AB}} \right] \otimes |\mathsf{pf}_{\{(x_i,y_i)\}_{i=1}^t}\rangle_{\mathsf{PF}} \,. \tag{4.27}$$

While the state $|\mathsf{pf}_{\{(x_i,y_i)\}_{i=1}^t}\rangle$ is supported on an exponential number of qubits, we can compress the environment using the following linear operator Comp. By Claim 4, Comp is a partial isometry. Intuitively, Comp "compresses" the state $|\mathsf{pf}_R\rangle$, which requires an exponential number of qubits n, to $|R\rangle$, which is only as big as the size of the relation.

Definition 14. *Define $\mathsf{Comp} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{R}}$ to be*

$$\mathsf{Comp} := \sum_{R \in \mathcal{R}^{\mathsf{bij}}} |R\rangle\langle \mathsf{pf}_R| \tag{4.28}$$

Next, we will use Comp to relate the path-recording oracle V to the purified permutation-function oracle. To do so, we will need to define the following projectors.

Definition 15 (Distinct subspace projector)**.** *Given $0 \leq t \leq N$. Let*

$$\Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} := \sum_{(x_1,\ldots,x_t) \in [N]^t_{\mathrm{dist}}} |x_1\rangle\langle x_1|_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes |x_t\rangle\langle x_t|_{\mathsf{R}_{\mathsf{X},t}^{(t)}} \,. \tag{4.29}$$

Definition 16 (Distinct subspace projector for pf-relation states)**.** *Let*

$$\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} := \sum_{\substack{R \in \mathcal{R}^{\mathsf{bij}}, \\ |R| = t}} |\mathsf{pf}_R\rangle\langle \mathsf{pf}_R| \,. \tag{4.30}$$

Lemma 4.4 (Relating V and pfO states)**.** *For all n-qubit unitaries G,*

$$\mathsf{Comp} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot |\mathcal{A}_t^{\mathsf{pfO}\cdot G}\rangle_{\mathsf{ABPF}} = \Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot |\mathcal{A}_t^{V\cdot G}\rangle \tag{4.31}$$

Proof. By Fact 3, we have

$$|\mathcal{A}_t^{V\cdot G}\rangle = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t} \Big(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0\rangle_{\mathsf{AB}}\right] \otimes |\{(x_i,y_i)\}_{i=1}^t\rangle_{\mathsf{R}} \,. \tag{4.32}$$

Applying $\Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}}$ to this state selects the terms corresponding to $(x_1,\ldots,x_t)\in[N]^t_{\mathrm{dist}}$:

$$\Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot |\mathcal{A}_t^{V\cdot G}\rangle = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t_{\mathrm{dist}} \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t} \Big(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0\rangle_{\mathsf{AB}}\right] \otimes |\{(x_i,y_i)\}_{i=1}^t\rangle_{\mathsf{R}} \,. \tag{4.33}$$

By Fact 4,

$$|\mathcal{A}_t^{\mathsf{pfO}\cdot G}\rangle_{\mathsf{ABPF}} = \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t}} \left[\prod_{i=1}^{t} \Big(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0\rangle_{\mathsf{AB}}\right] \otimes |\mathsf{pf}_{\{(x_i,y_i)\}_{i=1}^t}\rangle_{\mathsf{PF}} \,. \tag{4.34}$$

Applying $\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}$ selects the terms corresponding to $(x_1,\ldots,x_t)\in[N]^t_{\mathrm{dist}}$ and $(y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}$:

$$\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot |\mathcal{A}_t^{\mathsf{pfO}\cdot G}\rangle_{\mathsf{ABPF}} \tag{4.35}$$

$$= \sqrt{\frac{(N-t)!}{N!}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t_{\mathrm{dist}} \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}}}} \left[\prod_{i=1}^{t} \Big(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0\rangle_{\mathsf{AB}}\right] \otimes |\mathsf{pf}_{\{(x_i,y_i)\}_{i=1}^t}\rangle_{\mathsf{PF}} \,. \tag{4.36}$$

Since Comp maps $|\mathsf{pf}_R\rangle$ to $|R\rangle$ for all $R\in\mathcal{R}^{\mathsf{bij}}$, applying Comp to the right-hand side of Eq. (4.36) yields the right-hand side of Eq. (4.33), which proves the claim. □

Corollary 4.2 (Trace distance between original state and the projected state)**.**

$$\left\| \mathrm{Tr}_{\mathsf{PF}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \right) - \mathrm{Tr}_{\mathsf{PF}}\left(\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \right) \right\|_1 \leq \frac{t(t-1)}{N+1}. \tag{4.37}$$

Proof. By Lemma 2.2, we have

$$\left\| \mathrm{Tr}_{\mathsf{PF}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \right) - \mathrm{Tr}_{\mathsf{PF}}\left(\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \right) \right\|_1$$

$$= 1 - \mathrm{Tr}\left(\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \right) \tag{4.38}$$

Next, observe that $\widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} = \mathsf{Comp}^\dagger \cdot \mathsf{Comp} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}$ since

$$\mathsf{Comp}^\dagger \cdot \mathsf{Comp} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \tag{4.39}$$

$$= \Big(\sum_{R\in\mathcal{R}^{\mathsf{bij}}} |\mathsf{pf}_R\rangle\langle R| \Big) \cdot \Big(\sum_{R\in\mathcal{R}^{\mathsf{bij}}} |R\rangle\langle \mathsf{pf}_R| \Big) \cdot \Big(\sum_{\substack{R\in\mathcal{R}^{\mathsf{bij}},\\ |R|=t}} |\mathsf{pf}_R\rangle\langle \mathsf{pf}_R| \Big) \tag{4.40}$$

$$= \sum_{\substack{R\in\mathcal{R}^{\mathsf{bij}},\\ |R|=t}} |\mathsf{pf}_R\rangle\langle \mathsf{pf}_R| = \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}}. \tag{4.41}$$

By plugging this identity into (4.38), we get

$$(4.38) = 1 - \mathrm{Tr}\left(\mathsf{Comp}^\dagger \cdot \mathsf{Comp} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \right) \tag{4.42}$$

$$= 1 - \mathrm{Tr}\left(\mathsf{Comp} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}^{\mathrm{dist}}_{\mathsf{PF}} \cdot \mathsf{Comp}^\dagger \right) \tag{4.43}$$

$$= 1 - \mathrm{Tr}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \Pi^{\mathrm{dist}}_{\mathsf{R}_{\mathsf{X}}^{(t)}} \cdot |\mathcal{A}_t^{V\cdot C}\rangle\langle\mathcal{A}_t^{V\cdot C}|_{\mathsf{ABR}} \cdot \Pi^{\mathrm{dist}}_{\mathsf{R}_{X}^{(t)}} \right) \qquad \text{(By Lemma 4.4)}$$

$$\leq \frac{t(t-1)}{N+1}, \qquad \text{(By Corollary 4.1)}$$

which completes the proof. □

5 The PRU proof

5.1 Setup

We define a distribution over n-qubit unitaries parameterized by any n-qubit unitary 2-design $\mathfrak{D}$.

Definition 17 ($\mathsf{PRU}(\mathfrak{D})$ distribution)**.** *Let $\mathfrak{D}$ be a distribution supported on $\mathcal{U}(N)$. The distribution $\mathsf{PF}(\mathfrak{D})$ is defined as follows:*

1. *Sample a uniformly random permutation $\pi \leftarrow \mathsf{Sym}_N$, a uniformly random $f \leftarrow \{0,1\}^N$, and a uniformly random n-qubit unitary $C \leftarrow \mathfrak{D}$.*
2. *Output the unitary $\mathcal{O} := P_\pi \cdot F_f \cdot C$.*

The goal of this section is to prove the following theorem.

Theorem 3 ($\mathsf{PF}(\mathfrak{D})$ is indistinguishable from Haar-random)**.** *Let $\mathcal{A}$ be a t-query oracle adversary that only makes forward queries, and let $\mathfrak{D}$ be an exact unitary 2-design. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{PF}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|, \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}| \right) \leq \frac{4t(t-1)}{N+1} \tag{5.1}$$

Since quantum-secure pseudorandom permutations and pseudorandom functions exist assuming one-way functions [Zha16, Zha21], the existence of computationally-secure PRU follows immediately from Theorem 3.

Theorem 4. *If quantum-secure one-way functions exist, then pseudorandom unitaries exist.*

The main technical component of the proof of Theorem 3 is the following lemma.

Lemma 5.1 ($\mathsf{PRU}(\mathfrak{D})$ is indistinguishable from V)**.** *Let $\mathcal{A}$ be a t-query oracle adversary and let $\mathfrak{D}$ be an exact unitary 2-design. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{PF}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|, \ \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}} \right) \right) \leq \frac{2t(t-1)}{N+1} \tag{5.2}$$

Lemma 5.1 implies Theorem 3. Lemma 5.1 implies Theorem 3 by the following argument. We can instantiate $\mathfrak{D} = \mu_{\mathsf{Haar}}$, i.e., $\mathfrak{D}$ outputs a Haar-random n-qubit unitary. Then the output of $\mathsf{PRU}(\mathfrak{D}) = \mathsf{PRU}(\mu_{\mathsf{Haar}})$ is $P_\pi \cdot F_f \cdot C$ for random π, f and Haar-random C. By invariance of the Haar measure, this is exactly the same as outputting a Haar-random unitary. Thus, we have the following corollary of Lemma 5.1.

Theorem 5 (V is indistinguishable from Haar random)**.** *Let $\mathcal{A}$ be a t-query oracle adversary. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\sim\mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|, \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\right)\right) \leq \frac{2t(t-1)}{N+1} \tag{5.3}$$

Theorem 3 follows from combining Lemma 5.1 and Theorem 5 using the triangle inequality. It remains to prove Lemma 5.1.

5.2 Proof of Lemma 5.1

Proof of Lemma 5.1. We will use a hybrid argument. Define the mixed states

$$\rho_0^{(\mathfrak{D})} \coloneqq \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{PF}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}| \tag{5.4}$$

$$\rho_1^{(\mathfrak{D})} \coloneqq \mathrm{Tr}_{\mathsf{PF}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}}\right) \tag{5.5}$$

$$\rho_2^{(\mathfrak{D})} \coloneqq \mathrm{Tr}_{\mathsf{PF}}\left(\widetilde{\Pi}_{\mathsf{PF}}^{\mathrm{dist}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{\mathsf{pfO}\cdot C}\rangle\langle\mathcal{A}_t^{\mathsf{pfO}\cdot C}|_{\mathsf{ABPF}} \cdot \widetilde{\Pi}_{\mathsf{PF}}^{\mathrm{dist}}\right) \tag{5.6}$$

$$\rho_3^{(\mathfrak{D})} \coloneqq \mathrm{Tr}_{\mathsf{R}}\left(\Pi_{\mathsf{R}_X^{(t)}}^{\mathrm{dist}} \cdot \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{V\cdot C}\rangle\langle\mathcal{A}_t^{V\cdot C}|_{\mathsf{ABR}} \cdot \Pi_{\mathsf{R}_X^{(t)}}^{\mathrm{dist}}\right) \tag{5.7}$$

$$\rho_4^{(\mathfrak{D})} \coloneqq \mathrm{Tr}_{\mathsf{R}}\left(\mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} |\mathcal{A}_t^{V\cdot C}\rangle\langle\mathcal{A}_t^{V\cdot C}|_{\mathsf{ABR}}\right) \tag{5.8}$$

$$\rho_5 \coloneqq \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\right). \tag{5.9}$$

We argue indistinguishability between each consecutive pair of mixed states:

- $\rho_0^{(\mathfrak{D})} = \rho_1^{(\mathfrak{D})}$ by Claim 3.
- $\|\rho_1^{(\mathfrak{D})} - \rho_2^{(\mathfrak{D})}\|_1 \leq t(t-1)/(N+1)$ by Corollary 4.2.
- $\rho_2^{(\mathfrak{D})} = \rho_3^{(\mathfrak{D})}$, since by Lemma 4.4, these are two mixed states whose purifications are related by the Comp isometry, which only acts on the purifying register.
- $\|\rho_3^{(\mathfrak{D})} - \rho_4^{(\mathfrak{D})}\|_1 \leq t(t-1)/(N+1)$ by Corollary 4.1.
- $\rho_4^{(\mathfrak{D})} = \rho_5^{(\mathfrak{D})}$ since

$$\rho_4^{(\mathfrak{D})} = \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V\cdot C}\rangle\langle\mathcal{A}_t^{V\cdot C}|_{\mathsf{ABR}}\right) = \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\right) = \rho_5, \tag{5.10}$$

  where the second equality follows from Lemma 4.3, which states that for any C, $|\mathcal{A}_t^{V\cdot C}\rangle\langle\mathcal{A}_t^{V\cdot C}|$ and $|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|$ are related by a unitary on the purifying register.

Using the triangle inequality, we obtain Eq. (5.2), which completes the proof. □

Part II
Strong PRUs

The goal of Part II is to construct strong PRUs, which are secure against adversaries that make both forward and inverse queries to the unitary oracle. It is important to note that several operators that were defined in Part I, including $\mathsf{pfO}, \mathsf{Comp}$ and V, will be have new definitions in Part II.

6 The purified permutation-function oracle

In this section, we analyze the view of an adversary that makes queries to an oracle $P_\pi \cdot F_f$, for uniformly random $\pi \leftarrow \mathsf{Sym}_N$ and a random **ternary** function $f \leftarrow \{0,1,2\}^N$. We will do this by analyzing the *purified permutation-function permutation* oracle, which uses a purification of π and f.

Definition 18 (Purified permutation-function oracle)**.** *The purified permutation-function oracle* pfO *is a unitary acting on registers* $\mathsf{A}, \mathsf{P}, \mathsf{F}$*, where*

- P *is a register associated with the Hilbert space* $\mathcal{H}_\mathsf{P}$*, defined to be the span of the orthonormal states* $|\pi\rangle$ *for all* $\pi \in \mathsf{Sym}_N$*.*
- F *is a register associated with the Hilbert space* $\mathcal{H}_\mathsf{F}$*, defined to be the span of the orthonormal states* $|f\rangle$ *for all* $f \in \{0,1,2\}^N$*.*

The unitary pfO *is defined to act as follows:*

$$\mathsf{pfO}_{\mathsf{APF}} |x\rangle_\mathsf{A} |\pi\rangle_\mathsf{P} |f\rangle_\mathsf{F} := \omega_3^{f(x)} |\pi(x)\rangle_\mathsf{A} |\pi\rangle_\mathsf{P} |f\rangle_\mathsf{F}, \tag{6.1}$$

$$= \sum_{y\in[N]} |y\rangle_\mathsf{A} \delta_{\pi(x)=y} |\pi\rangle \omega_3^{f(x)} |f\rangle, \tag{6.2}$$

for all $x \in [N], \pi \in \mathsf{Sym}_N$*, and* $f \in \{0,1,2\}^N$*. Here,* $\omega_3 = \exp(2\pi i/3)$*.*

The action of $\mathsf{pfO}^\dagger$ is

$$\mathsf{pfO}^\dagger |y\rangle_\mathsf{A} |\pi\rangle |f\rangle = \sum_{x\in[N]} |x\rangle_\mathsf{A} \delta_{\pi(x)=y} |\pi\rangle \omega_3^{-f(x)} |f\rangle. \tag{6.3}$$

The view of an adversary that queries the purified oracle is equivalent to the view of an adversary that queries the standard oracle $P_\pi \cdot F_f$, for uniformly random $\pi \leftarrow \mathsf{Sym}_N$ and $f \leftarrow \{0,1,2\}^N$.

Claim 6 (Equivalence of purified and standard oracles)**.** *For any oracle adversary* $\mathcal{A}$*, the following oracle instantiations are perfectly indistinguishable:*

- *(Queries to a random* $P_\pi \cdot F_f$*) Sample a uniformly random* $\pi \leftarrow \mathsf{Sym}_N, f \leftarrow \{0,1,2\}^N$*. On each query, apply* $P_\pi \cdot F_f$ *to register* A*.*
- *(Queries to* pfO*) Initialize registers* P, F *to* $\frac{1}{\sqrt{N!}} \sum_{\pi\in\mathsf{Sym}_N} |\pi\rangle_\mathsf{P} \otimes \frac{1}{\sqrt{2^N}} \sum_{f\in\{0,1,2\}^N} |f\rangle_\mathsf{F}$*. At each query, apply* pfO *to registers* $\mathsf{A}, \mathsf{P}, \mathsf{F}$*.*

The proof is the same as the proof of Claim 3 in Part I.

Next, we define the following states on the P, F registers.

Definition 19 (pf-relation state)**.** *For $L = \{(x_1, y_1), \ldots, (x_\ell, y_\ell)\} \in \mathcal{R}_\ell$ and $R = \{(x'_1, y'_1), \ldots, (x'_r, y'_r)\} \in \mathcal{R}_r$, where ℓ and r are non-negative integers such that $\ell + r \le N$, let*

$$|\mathsf{pf}_{L,R}\rangle \coloneqq \frac{1}{\sqrt{(N-\ell-r)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi, L\cup R} |\pi\rangle \frac{1}{\sqrt{3^N}} \sum_{f \in \{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)-(f(x'_1)+\cdots+f(x'_r))} |f\rangle\,, \quad (6.4)$$

where $\delta_{\pi,L\cup R}$ is an indicator variable that equals 1 if $\pi(x) = y$ for all $(x, y) \in L\cup R$, and is 0 otherwise.

Note that when $\ell = r = 0$, i.e., $L = R = \varnothing$ are both the empty relation, the pf-relation state $|\mathsf{pf}_{\varnothing,\varnothing}\rangle_{\mathsf{PF}}$ is the uniform superposition over all permutations $\pi \in \mathsf{Sym}_N$ and all ternary functions $f \in \{0, 1, 2\}^N$,

$$|\mathsf{pf}_{\varnothing,\varnothing}\rangle_{\mathsf{PF}} \coloneqq \frac{1}{\sqrt{N!}} \sum_{\pi \in \mathsf{Sym}_N} |\pi\rangle_{\mathsf{P}} \otimes \frac{1}{\sqrt{3^N}} \sum_{f \in \{0,1\}^N} |f\rangle_{\mathsf{F}}\,. \quad (6.5)$$

Recall that a relation R is *bijective* if and only if $|\mathrm{Im}(R)| = |\mathrm{Dom}(R)| = |R|$. Equivalently, writing $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, R is bijective if $x_1, \ldots, x_t$ are all distinct, and $y_1, \ldots, y_t$ are also all distinct.

Definition 20. *Let $\mathcal{R}^{2,\mathrm{dist}}$ be the set of all ordered pairs of relations $(L, R) \in \mathcal{R}^2$ where $L \cup R$ is a bijective relation.*

6.1 Orthonormality of the pf-relation states

Claim 7 (Orthonormality of pf-relation states)**.** *$\{|\mathsf{pf}_{L,R}\rangle\}_{(L,R)\in\mathcal{R}^{2,\mathrm{dist}}}$ is an orthonormal set of vectors.*

Proof of Claim 7. For $x \in [N]$, let $e_x \in \{0, 1, 2\}^N$ denote the N-dimensional vector that has a 1 in the x-th position, and is 0 everywhere else. Then by writing $f(x)$ as $f(x) = f \cdot e_x$, we get

$$\frac{1}{\sqrt{3^N}} \sum_{f \in \{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)-(f(x'_1)+\cdots f(x'_r))} |f\rangle_{\mathsf{F}} \quad (6.6)$$

$$= \frac{1}{\sqrt{3^N}} \sum_{f \in \{0,1,2\}^N} \omega_3^{f\cdot(e_{x_1}+\cdots+e_{x_\ell})-f\cdot(e_{x'_1}+\cdots+e_{x'_r})} |f\rangle_{\mathsf{F}} \quad (6.7)$$

$$= \mathsf{QFT}_3^{\otimes N} |(e_{x_1} + \cdots + e_{x_\ell}) - (e_{x'_1} + \cdots + e_{x'_r}) \pmod 3\rangle_{\mathsf{F}}\,, \quad (6.8)$$

where QFT_3 denotes the 3-ary quantum Fourier transform. When $\{x_1, \ldots, x_\ell, x'_1, \ldots, x'_r\}$ are all distinct, there is a bijection between $(e_{x_1}+\cdots+e_{x_\ell})-(e_{x'_1}+\cdots+e_{x'_r})$ and the sets $\{x_1, \ldots, x_\ell\}, \{x'_1, \ldots, x'_r\}$: the first set corresponds to the indices where the vector is 1, and the second set is the indices where the vector is $-1 \equiv 2 \pmod 3$. Thus, there is an isometry that maps

$$\frac{1}{\sqrt{3^N}} \sum_{f \in \{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)-(f(x'_1)+\cdots f(x'_r))} |f\rangle_{\mathsf{F}} \mapsto |\{x_1, \ldots, x_\ell\}\rangle\, |\{x'_1, \ldots, x'_r\}\rangle\,, \quad (6.9)$$

whenever $\{x_1, \ldots, x_\ell, x'_1, \ldots, x'_r\}$ are all distinct. Thus, for any $L = \{(x_1, y_1), \ldots, (x_\ell, y_\ell)\}$, $R = \{(x'_1, y'_1), \ldots, (x'_r, y'_r)\}$ where $L \cup R$ is a bijective relation, applying this isometry to the F register of $|\mathsf{pf}_{L,R}\rangle$ yields

$$|\mathsf{pf}_{L,R}\rangle \mapsto \frac{1}{\sqrt{(N-\ell-r)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi,L\cup R} |\pi\rangle_{\mathsf{P}} \otimes |\{x_1, \ldots, x_\ell\}\rangle\, |\{x'_1, \ldots, x'_r\}\rangle\,. \quad (6.10)$$

Next, we can apply an isometry that, controlled on $|\pi\rangle$, sends each x_i to the tuple $(x_i, \pi(x_i)) = (x_i, y_i)$. The result is

$$\frac{1}{\sqrt{(N-\ell-r)!}} \sum_{\pi \in \mathsf{Sym}_N} \delta_{\pi, L\cup R} \, |\pi\rangle_{\mathsf{P}} \otimes |\{(x_1,y_1),\dots,(x_\ell,y_\ell)\}\rangle \, |\{(x'_1,y'_1),\dots,(x'_r,y'_r)\}\rangle \,. \tag{6.11}$$

Finally, controlled on the last two registers, we can uncompute the superposition on the P register. The result is

$$|\{(x_1,y_1),\dots,(x_\ell,y_\ell)\}\rangle \, |\{(x'_1,y'_1),\dots,(x'_r,y'_r)\}\rangle = |L\rangle \, |R\rangle \,. \tag{6.12}$$

This completes the proof. □

Definition 21. *Define the partial isometry* $\mathsf{Comp} : \mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{F}} \to \mathcal{H}_{\mathsf{L}} \otimes \mathcal{H}_{\mathsf{R}}$ *to be*

$$\mathsf{Comp} := \sum_{(L,R)\in\mathcal{R}^{2,\mathrm{dist}}} |L\rangle_{\mathsf{L}} \otimes |R\rangle_{\mathsf{R}} \cdot \langle \mathsf{pf}_R|_{\mathsf{PF}} \tag{6.13}$$

Here, L and R are variable-length registers as defined in Section 2.1. Note that Comp is a partial isometry by Claim 7.

6.2 How pfO acts on the pf-relation states

Claim 8 (Action of pfO)**.** *For any* $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$ *and* $x \in [N]$ *such that* $x \notin \mathrm{Dom}(L\cup R)$*, we have*

$$\mathsf{pfO} \, |x\rangle_{\mathsf{A}} \, |\mathsf{pf}_{L,R}\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{N-|L\cup R|}} \sum_{\substack{y\in[N]:\\ y\notin \mathrm{Im}(L\cup R)}} |y\rangle_{\mathsf{A}} \, |\mathsf{pf}_{L\cup\{(x,y)\},R}\rangle_{\mathsf{PF}} \,. \tag{6.14}$$

Similarly, for any $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$ *and* $y \in [N]$ *such that* $y \notin \mathrm{Im}(L\cup R)$*, we have*

$$\mathsf{pfO}^\dagger \, |y\rangle_{\mathsf{A}} \, |\mathsf{pf}_{L,R}\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{N-|L\cup R|}} \sum_{\substack{x\in[N]:\\ x\notin \mathrm{Dom}(L\cup R)}} |x\rangle_{\mathsf{A}} \, |\mathsf{pf}_{L,R\cup\{(x,y)\}}\rangle_{\mathsf{PF}} \,. \tag{6.15}$$

Proof of Claim 8. Recall that

$$\mathsf{pfO}_{\mathsf{APF}} \, |x\rangle_{\mathsf{A}} \, |\pi\rangle_{\mathsf{P}} \, |f\rangle_{\mathsf{F}} = \sum_{y\in[N]} |y\rangle_{\mathsf{A}} \, \delta_{\pi(x)=y} \, |\pi\rangle \, \omega_3^{f(x)} \, |f\rangle \,. \tag{6.16}$$

Let us write $L = \{(x_1,y_1),\dots,(x_\ell,y_\ell)\}$ and $R = \{(x'_1,y'_1),\dots,(x'_r,y'_r)\}$. Then

$$|\mathsf{pf}_{L,R}\rangle_{\mathsf{PF}} = \frac{1}{\sqrt{(N-\ell-r)!}} \sum_{\pi\in\mathsf{Sym}_N} \delta_{\pi,L\cup R} \, |\pi\rangle_{\mathsf{P}} \, \frac{1}{\sqrt{3^N}} \sum_{f\in\{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)-f(x'_1)-\cdots-f(x'_r))} \, |f\rangle_{\mathsf{F}} \,, \tag{6.17}$$

Thus, we have

$$\begin{aligned} &\mathsf{pfO}_{\mathsf{APF}} \, |x\rangle_{\mathsf{A}} \, |\mathsf{pf}_{L,R}\rangle_{\mathsf{PF}} \\ &= \sum_{y\in[N]} |y\rangle_{\mathsf{A}} \, \frac{1}{\sqrt{(N-\ell-r)!}} \sum_{\pi\in\mathsf{Sym}_N} \delta_{\pi(x)=y} \cdot \delta_{\pi,L\cup R} \, |\pi\rangle_{\mathsf{P}} \end{aligned} \tag{6.18}$$

$$\frac{1}{\sqrt{3^N}} \sum_{f\in\{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)+f(x)-f(x'_1)-\cdots-f(x'_r))} \left|f\right\rangle_{\mathsf{F}}. \tag{6.19}$$

In this sum, $|y\rangle$ has a coefficient of 0 whenever $y \in \mathrm{Im}(L \cup R)$, since in that case the constraints that $\delta_{\pi,L\cup R}$ and $\delta_{\pi(x)=y}$ are impossible to satisfy since $x \notin \mathrm{Dom}(L\cup R)$, and thus satisfying both constraints would require y to have two different preimages under the permutation π. We can therefore rewrite the above sum as

$$\mathsf{pfO}_{\mathsf{APF}} \left|x\right\rangle_{\mathsf{A}} \left|\mathsf{pf}_{L,R}\right\rangle_{\mathsf{PF}} \tag{6.20}$$

$$= \frac{1}{\sqrt{N-\ell-r}} \sum_{\substack{y\in[N]:\\ y\notin\mathrm{Im}(L\cup R)}} \left|y\right\rangle_{\mathsf{A}} \frac{1}{\sqrt{(N-\ell-1-r)!}} \sum_{\pi\in\mathsf{Sym}_N} \delta_{\pi,L\cup\{(x,y)\}\cup R} \left|\pi\right\rangle_{\mathsf{P}}$$

$$\frac{1}{\sqrt{3^N}} \sum_{f\in\{0,1,2\}^N} \omega_3^{f(x_1)+\cdots+f(x_\ell)+f(x)-f(x'_1)-\cdots-f(x'_r))} \left|f\right\rangle_{\mathsf{F}} \tag{6.21}$$

$$= \frac{1}{\sqrt{N-\ell-r}} \sum_{y\in[N]} \left|y\right\rangle_{\mathsf{A}} \left|\mathsf{pf}_{L\cup\{(x,y)\},R}\right\rangle_{\mathsf{PF}}. \tag{6.22}$$

This completes the proof of Eq. (6.14). Since $\mathsf{pfO}^\dagger$ applies the map

$$\mathsf{pfO}^\dagger \left|y\right\rangle_{\mathsf{A}} \left|\pi\right\rangle \left|f\right\rangle = \sum_{x\in[N]} \left|x\right\rangle_{\mathsf{A}} \delta_{\pi(x)=y} \left|\pi\right\rangle \omega_3^{-f(x)} \left|f\right\rangle, \tag{6.23}$$

the proof for Eq. (6.15) follows by a symmetric argument. □

7 The partial path-recording oracle W

In the previous section, we proved Claim 8, which partially characterizes how the unitaries pfO and $\mathsf{pfO}^\dagger$ act in terms of states $\left|x\right\rangle_{\mathsf{A}} \left|\mathsf{pf}_{L,R}\right\rangle_{\mathsf{PF}}$. We also proved that there exists an isometry Comp that maps $\left|\mathsf{pf}_{L,R}\right\rangle_{\mathsf{PF}}$ to $\left|L\right\rangle_{\mathsf{L}} \left|R\right\rangle_{\mathsf{R}}$ for all pairs of relations L, R such that their union $L \cup R$ is a bijective relation. In this section, we will define a linear operator W that we call the *partial path recording oracle*. This W operator, up to isometry, implements a restricted version of the pfO operator. In particular, we have the following.

- On states of the form $\left|x\right\rangle_{\mathsf{A}} \left|L\right\rangle_{\mathsf{L}} \left|R\right\rangle_{\mathsf{R}}$ such that $L \cup R$ is a bijection and $x \notin \mathrm{Dom}(L \cup R)$, the linear map W performs exactly the same map as pfO (up to isometry).
- On states of the form $\left|y\right\rangle_{\mathsf{A}} \left|L\right\rangle_{\mathsf{L}} \left|R\right\rangle_{\mathsf{R}}$ such that $L \cup R$ is a bijection and $y \notin \mathrm{Im}(L \cup R)$, the linear map $W^\dagger$ performs exactly the same map as $\mathsf{pfO}^\dagger$ (up to isometry).

In the above, "up to isometry" refers to the isometry Comp that maps $\left|\mathsf{pf}_{L,R}\right\rangle_{\mathsf{PF}}$ to $\left|L\right\rangle_{\mathsf{L}} \left|R\right\rangle_{\mathsf{R}}$. Formally, the registers L and R are both *variable-length* registers that store the two relations L and R. We refer the reader to Sections 2.1 and 2.1.1 in the Preliminaries section for our definitions of variable-length registers, relations, and relation states.

The role of the W operator in our proof. Looking ahead to our main proof, we will show that if C, D are sampled from any n-qubit 2-design, then an adversary (making both forward and inverse queries) cannot distinguish between an oracle that implements $D_{\mathsf{A}} \cdot \mathsf{pfO} \cdot C_{\mathsf{A}}$ and an oracle that implements $D_{\mathsf{A}} \cdot W \cdot C_{\mathsf{A}}$, except with negligible advantage. Thus, even though W only behaves

like (a compressed version of) pfO on a restricted subspace, we will show that the twirling of C, D prevents the adversary from detecting the difference.

In the next section, we will show that the W operator can also be seen as a restricted version of another linear operator V that we call the *path-recording oracle*. The connection between W and V plays a crucial role in our proof; see Section 8 for further discussion.

7.1 Defining W^L and W^R

Before we define W, we will first define helper operators W^L and W^R. The W^L operator is defined to capture the (partial) characterization of pfO given in Eq. (6.14), while W^R is defined to capture the (partial) characterization of $\mathsf{pfO}^\dagger$ given in Eq. (6.15).

Definition 22 (W^L and W^R)**.** *Define W^L to be the linear map such that for any $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$ and $x \in [N]$ such that $x \notin \mathrm{Dom}(L \cup R)$,*

$$W^L \cdot |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} \coloneqq \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{y \in [N]: \\ y \notin \mathrm{Im}(L \cup R)}} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} . \tag{7.1}$$

Similarly, define W^R be the linear map such that for any $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$ and $y \in [N]$ such that $y \notin \mathrm{Im}(L \cup R)$,

$$W^R \cdot |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} \coloneqq \frac{1}{\sqrt{N - |L \cup R|}} \sum_{\substack{x \in [N]: \\ x \notin \mathrm{Dom}(L \cup R)}} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R \cup \{(x,y)\}\rangle_{\mathsf{R}} . \tag{7.2}$$

It is useful to define the following projectors to describe the actions of W^L, W^R.

Definition 23 (Bijective-relation projectors)**.** *Define the projectors*

$$\Pi^{\mathsf{bij}}_{\mathsf{LR}} \coloneqq \sum_{(L,R) \in \mathcal{R}^{2,\mathrm{dist}}} |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}} , \qquad \Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} \coloneqq \Pi^{\mathsf{bij}}_{\mathsf{LR}} \cdot \Pi_{\le t,\mathsf{LR}} = \Pi_{\le t,\mathsf{LR}} \cdot \Pi^{\mathsf{bij}}_{\mathsf{LR}}, \tag{7.3}$$

where the projector $\Pi_{\le t,\mathsf{LR}}$ is the maximum-length projector defined in Notation 8.

By the definition of W^L and W^R, we have the following fact about the action of W^L and W^R on states with a bounded length.

Fact 5. *For any integer $i \ge 0$, W^L, W^R map states in the subspace associated to the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\le i,\mathsf{LR}}$ into the subspace associated with the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\le i+1,\mathsf{LR}}$.*

The following property follows from the relation between W^L, W^R and $\mathsf{pfO}, \mathsf{pfO}^\dagger$.

Claim 9. *W^L and W^R are both partial isometries.*

Proof. Since pfO is a unitary operator, the operator obtained by restricting the domain of pfO to the span of the states $|x\rangle |\mathsf{pf}_{L,R}\rangle$ is a partial isometry. Up to relabeling $|\mathsf{pf}_{L,R}\rangle$ as $|L,R\rangle$ (i.e., applying the partial isometry Comp), this is W^L. Similarly, $\mathsf{pfO}^\dagger$ is a unitary, and the operator obtained by restricting $\mathsf{pfO}^\dagger$ to the span of states $|y\rangle |\mathsf{pf}_{L,R}\rangle$ is a partial isometry. Up to relabeling $|\mathsf{pf}_{L,R}\rangle$ as $|L,R\rangle$, this is W^R. □

Notation 12. *For a partial isometry G, let $\mathcal{D}(G)$ and $\mathcal{I}(G)$ denote its domain and image. Let $\Pi^{\mathcal{D}(G)} = G^\dagger \cdot G$ and $\Pi^{\mathcal{I}(G)} = G \cdot G^\dagger$ denote the orthogonal projectors onto $\mathcal{D}(G)$ and $\mathcal{I}(G)$.*

Claim 10. *For all integers $t \geq 0$, $\Pi_{\leq t}$ commutes with $\Pi^{\mathcal{D}(W^L)}$, $\Pi^{\mathcal{I}(W^L)}$, $\Pi^{\mathcal{D}(W^R)}$, and $\Pi^{\mathcal{I}(W^R)}$.*

Proof. By Fact 5, $\Pi^{\mathcal{D}(W^L)} = W^{L,\dagger} \cdot W^L$ maps states from $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}}$ to $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}}$ for $t \geq 0$. This implies that $\Pi^{\mathcal{D}(W^L)}$ commutes with $\Pi_{\leq t}$ for all $t \geq 0$. By Fact 5, $\Pi^{\mathcal{I}(W^L)} = W^L \cdot W^{L,\dagger}$ maps states from $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq t+1,\mathsf{LR}}$ to $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq t+1,\mathsf{LR}}$ for $t+1 \geq 0$. This implies that $\Pi^{\mathcal{D}(W^L)}$ commutes with $\Pi_{\leq t}$ for all $t \geq 1$. Additionally, $\Pi^{\mathcal{I}(W^L)} = W^L \cdot W^{L,\dagger}$ has no support on $\Pi_{\leq 0}$, and thus it commutes with $\Pi_{\leq 0}$. By symmetric arguments, we obtain the analogous statements for W^R. □

It will be useful to state the connection between the W^L, W^R, and pfO more formally.

Fact 6. *We have*

$$W^L = \mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{D}(W^L)} = \Pi^{\mathcal{I}(W^L)} \cdot \mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger, \tag{7.4}$$

$$W^R = \mathsf{Comp} \cdot \mathsf{pfO}^\dagger \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{D}(W^R)} = \Pi^{\mathcal{I}(W^R)} \cdot \mathsf{Comp} \cdot \mathsf{pfO}^\dagger \cdot \mathsf{Comp}^\dagger. \tag{7.5}$$

7.2 Defining W

We now use W^L and W^R to define the partial path-recording oracle W.

Definition 24. *The partial path-recording oracle is the operator W defined as*

$$W \coloneqq W^L + W^{R,\dagger}. \tag{7.6}$$

From Fact 5, we immediately obtain the following fact.

Fact 7. *$\mathcal{D}(W)$, $\mathcal{I}(W)$ are subspaces of the image of $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\mathsf{LR}}$. Moreover, for any integer $i \geq 0$, W and $W^\dagger$ map states in the subspace associated to the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq i,\mathsf{LR}}$ into the subspace associated with the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\leq i+1,\mathsf{LR}}$.*

Claim 11. *W is a partial isometry.*

Proof of Claim 11. Since W^L and W^R (and hence $W^{R,\dagger}$) are partial isometries, the operator $W = W^L + W^{R,\dagger}$ is a partial isometry as long as both of the following are true:

- The subspaces $\mathcal{D}(W^L)$ and $\mathcal{D}(W^{R,\dagger}) = \mathcal{I}(W^R)$ are orthogonal, i.e., W is a sum of two partial isometries with orthogonal domains.
- The subspaces $\mathcal{I}(W^L)$ and $\mathcal{I}(W^{R,\dagger}) = \mathcal{D}(W^R)$ are orthogonal, i.e., W is a sum of two partial isometries with orthogonal images.

$\mathcal{D}(W^L)$ and $\mathcal{I}(W^R)$ are orthogonal because $\mathcal{D}(W^L)$ is only supported on states $|x\rangle\,|L\rangle\,|R\rangle$ where $x \notin \mathrm{Dom}(L \cup R)$, while $\mathcal{I}(W^R)$ is only supported on states $|x\rangle\,|L\rangle\,|R\rangle$ where $x \in \mathrm{Dom}(L \cup R)$ (this can be seen by inspecting the right-hand-side of Eq. (7.2)). A symmetric argument shows that $\mathcal{D}(W^R)$ and $\mathcal{I}(W^L)$ are also orthogonal, which completes the proof. □

In fact, our proof of Claim 11 establishes the following relationship between the domain and image of W and the domain and image of W^L and W^R.

Fact 8. *The domain and image of W are given by*

$$\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}, \tag{7.7}$$

$$\Pi^{\mathcal{I}(W)} = \Pi^{\mathcal{D}(W^R)} + \Pi^{\mathcal{I}(W^L)}. \tag{7.8}$$

Claim 12. *For all integers $t \geq 0$, $\Pi_{\leq t}$ commutes with $\Pi^{\mathcal{D}(W)}$ and $\Pi^{\mathcal{I}(W)}$.*

Proof. This follows immediately from Claim 10, which states that the projector $\Pi_{\leq t}$ commutes with the projectors $\Pi^{\mathcal{D}(W^L)}$, $\Pi^{\mathcal{I}(W^L)}$, $\Pi^{\mathcal{D}(W^R)}$, $\Pi^{\mathcal{I}(W^R)}$. □

Corollary 7.1. *For all integers $t \geq 0$, the image of $\Pi^{\mathcal{D}(W)}_{\leq t,\mathsf{ALR}}$ is a subspace of the image of $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}}$. Similarly, the image of $\Pi^{\mathcal{I}(W)}_{\leq t,\mathsf{ALR}}$ is a subspace of the image of $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathsf{bij}}_{\leq t,\mathsf{LR}}$.*

Using Fact 8, we can now establish the following relationship between W and pfO.

Claim 13 (W is a restriction of pfO up to isometry)**.** *We have*

$$W = \mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{D}(W)}, \tag{7.9}$$

$$W^\dagger = \mathsf{Comp} \cdot \mathsf{pfO}^\dagger \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{I}(W)}. \tag{7.10}$$

In words, Claim 13 says that for any state in $\mathcal{D}(W)$, the domain of W, the action of W is the same as pfO up to isometry. Additionally, it says that for any state in the image in $\mathcal{I}(W)$, the image of W, the action of $W^\dagger$ is the same as $\mathsf{pfO}^\dagger$ up to isometry.

Proof of Claim 13. We will prove the first equality, Eq. (7.9); the second equality, Eq. (7.10), follows from a symmetric argument. From Eq. (7.4) and Eq. (7.5), we have

$$\mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{D}(W^L)} = W^L, \tag{7.11}$$

$$\mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{I}(W^R)} = W^{R,\dagger}. \tag{7.12}$$

Summing Eqs. (7.11) and (7.12) yields

$$\mathsf{Comp} \cdot \mathsf{pfO} \cdot \mathsf{Comp}^\dagger \cdot (\Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}) = W^L + W^{R,\dagger}, \tag{7.13}$$

and plugging in $\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}$ from Eq. (7.7) and $W = W^L + W^{R,\dagger}$ yields Eq. (7.9). □

8 The path-recording oracle V

In the previous section, we defined a linear operator W and showed that W acts as a restricted version of pfO, up to an application of the Comp isometry. In this section, we will introduce a second linear operator V, which will satisfy a number of key properties that will be crucial for our proof. We will show that V satisfies the following properties:

- V **is indistinguishable from** W **under twirling**, i.e., for C, D sampled from any n-qubit unitary 2-design $\mathfrak{D}$, an adversary making forward and inverse queries cannot distinguish between queries to $D_\mathsf{A} \cdot V \cdot C_\mathsf{A}$ and queries to $D_\mathsf{A} \cdot W \cdot C_\mathsf{A}$.
- V **satisfies approximate unitary invariance**, which we will use to conclude the following: an adversary making forward and inverse queries cannot distinguish between queries to $D_\mathsf{A} \cdot V \cdot C_\mathsf{A}$ for C, D sampled from any n-qubit unitary 2-design $\mathfrak{D}$, and plain queries to V.[6]

We will refer to V as the *path-recording oracle*. We remark that this definition of V is different from the one given in Part I, as this V will need to be designed to handle forward and inverse queries. In Appendix A.3 we describe how to implement V efficiently.

[6]For technical reasons, our main proof will handle both of these bullets in one argument.

8.1 Defining V^L and V^R

To define V, we first introduce helper operators V^L and V^R.

Definition 25 (left and right partial isometries)**.** *Let V^L be the linear operator that acts as follows. For $x \in [N]$ and $(L, R) \in \mathcal{R}^{2,\leq N-1}$,*

$$V^L \cdot |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} := \sum_{\substack{y\in[N]:\\ y\notin \mathrm{Im}(L\cup R)}} \frac{1}{\sqrt{N - |\mathrm{Im}(L \cup R)|}} |y\rangle_{\mathsf{A}} |L \cup \{(x, y)\}\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} . \tag{8.1}$$

Define V^R to be the linear operator such that for all $y \in [N]$ and $(L, R) \in \mathcal{R}^{2,\leq N-1}$,

$$V^R \cdot |y\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} := \sum_{\substack{x\in[N]:\\ x\notin \mathrm{Dom}(L\cup R)}} \frac{1}{\sqrt{N - |\mathrm{Dom}(L \cup R)|}} |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R \cup \{(x, y)\}\rangle_{\mathsf{R}} . \tag{8.2}$$

By construction, V^L and V^R take states in $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\leq i,\mathsf{LR}}$ to $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$.

Why these definitions of V^L and V^R? On states of the form $|x\rangle |L\rangle |R\rangle$ within the domain of W^L, the operators W^L and V^L act in the same way. However, the domain of W^L is limited to states $|x\rangle |L\rangle |R\rangle$ where $L \cup R$ forms a bijection and $x \notin \mathrm{Dom}(L \cup R)$ (which also implies that $|L \cup R| \leq N-1$). On the other hand, the definition of V^L extends W^L so that it acts on all $|x\rangle |L\rangle |R\rangle$ satisfying $|L \cup R| \leq N - 1$. In particular, we have dropped the requirement that $L \cup R$ is a bijection and that $x \notin \mathrm{Dom}(L \cup R)$. An analogous relationship holds between V^R and W^R. We define these extended operators, V^L and V^R, to establish a property known as (approximate) unitary invariance (see Claim 23). Importantly, this property holds only for the extended operators V^L and V^R, and not for the original W^L and W^R operators.

Claim 14. *V^L and V^R are partial isometries.*

Proof. We will give the proof for V^L; the proof for V^R follows by a symmetric argument. V^L is a partial isometry if and only if $V^L \cdot V^{L,\dagger}$ is the orthogonal projector onto $\mathcal{D}(V^L)$. From the definition of V^L, we can see that its domain is

$$\mathcal{D}(V^L) = \mathrm{span}\{ |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} : x \in [N], (L, R) \in \mathcal{R}^{2,\leq N-1}\}. \tag{8.3}$$

It suffices to show that for all $x, x' \in [N]$, and $(L, R) \in \mathcal{R}^{2,\leq N-1}$ and $(L', R') \in \mathcal{R}^{2,\leq N-1}$ that

$$\langle x'|_{\mathsf{A}} \langle L'|_{\mathsf{L}} \langle R'|_{\mathsf{R}} \cdot V^{L,\dagger} \cdot V^L \cdot |x\rangle_{\mathsf{A}} |L\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}} = \langle x'|x\rangle_{\mathsf{A}} \langle L'|L\rangle_{\mathsf{L}} \langle R'|R\rangle_{\mathsf{R}} . \tag{8.4}$$

We can expand out the LHS as

$$\Big(\sum_{y'\notin \mathrm{Im}(L'\cup R')} \frac{\langle y'|_{\mathsf{A}} \langle L' \cup x'y'|_{\mathsf{L}} \langle R'|_{\mathsf{R}}}{\sqrt{N - |\mathrm{Im}(L' \cup R')|}} \Big) \cdot \Big(\sum_{y\notin \mathrm{Im}(L\cup R)} \frac{|y\rangle_{\mathsf{A}} |L \cup \{(x, y)\}\rangle_{\mathsf{L}} |R\rangle_{\mathsf{R}}}{\sqrt{N - |\mathrm{Im}(L \cup R)|}} \Big) \tag{8.5}$$

The summand is zero unless $y' = y$, $L' \cup x'y' = L \cup \{(x, y)\}$, and $R' = R$. Combining the first two constraints, we have $L' \cup x'y = L \cup \{(x, y)\}$. Since y does not appear in either $\mathrm{Im}(L')$ or $\mathrm{Im}(L)$, this implies $x' = x$ and $L' = L$. This means that the sum is 0 unless $x = x'$, $L = L'$ and $R = R'$. When these constraints are satisfied, the sum becomes $\sum_{y\notin \mathrm{Im}(L\cup R)} 1/(N - |\mathrm{Im}(L \cup R)|) = 1$. This completes the proof that V^L is a partial isometry. □

8.2 Defining V

Definition 26. *The path-recording oracle is the operator V defined as*

$$V = V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) + (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}. \tag{8.6}$$

By construction, V and $V^\dagger$ take states in $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathcal{R}^2}_{\leq i,\mathsf{LR}}$ to $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$ for any integer $i \geq 0$.

Why this definition of V? Recall that since we defined $W \coloneqq W^L + W^{R,\dagger}$, it might seem natural to define $V \coloneqq V^L + V^{R,\dagger}$. However, if we defined V this way, it would *not* be a partial isometry. As we showed in the proof of Claim 11, $W^L + W^{R,\dagger}$ is a partial isometry because W^L and $W^{R,\dagger}$ do not "overlap", i.e., they are partial isometries with orthogonal domains and orthogonal images . On the other hand, this is not true for V^L and $V^{R,\dagger}$. Thus, in order to ensure that V is a partial isometry, we need to "project out" the overlap between V^L and $V^{R,\dagger}$.

Claim 15. *V is a partial isometry.*

Proof. We will first show that $V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger})$ is a partial isometry. This is true if and only if $(\mathsf{Id} - V^R \cdot V^{R,\dagger}) \cdot V^{L,\dagger} \cdot V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger})$ is a projector. To show that this operator is a projector, it suffices to show that $\Pi^{\mathcal{D}(V^L)} = V^{L,\dagger} \cdot V^L$ and $\Pi^{\mathcal{I}(V^R)} = V^R \cdot V^{R,\dagger}$ commute. From the definition of V^L, its domain is the image of the projector $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathcal{R}^2}_{\leq N-1,\mathsf{LR}}$. Since V^R takes states in $\Pi^{\mathcal{R}^2}_{\leq i,\mathsf{LR}}$ to $\Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$ (for $0 \leq i \leq N-1$), it follows that $V^R \cdot V^{R,\dagger}$ takes states in $\Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$ to $\Pi^{\mathcal{R}^2}_{\leq i+1,\mathsf{LR}}$ (for $0 \leq i \leq N-1$). In particular, this means it commutes with $\mathsf{Id}_\mathsf{A} \otimes \Pi^{\mathcal{R}^2}_{\leq N-1}$. Using a symmetric argument, we can conclude that $(\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ is also a partial isometry.

Now, we just need to show that the sum of these two partial isometries is a partial isometry. It suffices to show that their domains are orthogonal and their images are orthogonal. To see that their domains are orthogonal, note that the domain of $V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger})$ is a subspace of $\mathsf{Id} - \Pi^{\mathcal{I}(V^R)}$, while the domain of $(\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}$ is a subspace of $\Pi^{\mathcal{I}(V^R)}$, and hence they are orthogonal. A symmetric argument shows their images are orthogonal. This completes the proof. □

V being a partial isometry implies that any state generated by an adversary that queries V and $V^\dagger$ will have a norm at most 1. This is an important property that will be central to our strong PRU proof. Recall that in the standard PRU proof of Part I, the path-recording oracle acts as an isometry on all states that can be generated by querying the path-recording oracle. This first property of V being a partial isometry is a relaxation of the isometric property of the standard path-recording oracle. While V is a partial isometry, we will later show that the state generated by an adversary that queries V and $V^\dagger$ will have a norm close to one for subexponential number of queries.

8.3 Two-sided unitary invariance

The path-recording oracle V satisfies an (approximate) two-sided unitary invariance property, which we state below.

Definition 27. *For any n-qubit unitary C, D, define*

$$Q[C,D] \coloneqq (C \otimes D^T)^{\otimes *}_\mathsf{L} \otimes (\overline{C} \otimes D^\dagger)^{\otimes *}_\mathsf{R}. \tag{8.7}$$

Claim 16 (two-sided unitary invariance)**.** *For any integer $0 \leq t \leq N-1$ and any pair of n-qubit unitaries C, D,*

$$\|D_\mathsf{A} \cdot V_{\leq t} \cdot C_\mathsf{A} \otimes Q[C,D]_\mathsf{LR} - Q[C,D]_\mathsf{LR} \cdot V_{\leq t}\|_{\mathrm{op}} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{8.8}$$

$$\left\| C_{\mathsf{A}}^{\dagger} \cdot (V^{\dagger})_{\leq t} \cdot D_{\mathsf{A}}^{\dagger} \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{\dagger})_{\leq t} \right\|_{\mathrm{op}} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{8.9}$$

Claim 16 is proven in Section 10. The two-sided unitary invariance of V allows us to move the random unitaries C and D acting on system register A to the purifying registers L, R.

8.4 W is a restriction of V

We now show that W is a restriction of V. First, we need the following basic facts relating W^L, W^R, V^L, and V^R that follow immediately from the definitions of these operators.

Fact 9. *We have*

- *W^L is a restriction of V^L and W^R is a restriction of V^R:*

$$W^L = V^L \cdot \Pi^{\mathcal{D}(W^L)} = \Pi^{\mathcal{I}(W^L)} \cdot V^L \tag{8.10}$$
$$W^R = V^R \cdot \Pi^{\mathcal{D}(W^R)} = \Pi^{\mathcal{I}(W^R)} \cdot V^R \tag{8.11}$$

- *The image of V^R is in the kernel of W^L, and the image of V^L is in the kernel of W^R, i.e.,*

$$W^L \cdot V^R = W^R \cdot V^L = 0, \tag{8.12}$$

Lemma 8.1. *If Π_1 and Π_2 are projectors, and $\Pi_1 = \Pi_1\Pi_2\Pi_1$ then Π_1 is a subspace of Π_2.*

Proof. Consider any normalized state $|\psi\rangle \in \Pi_1$, i.e., $\Pi_1 |\psi\rangle = |\psi\rangle$. We have the following identity,

$$1 = \langle\psi| \Pi_1 |\psi\rangle = \langle\psi| \Pi_1\Pi_2\Pi_1 |\psi\rangle = \langle\psi| \Pi_2 |\psi\rangle . \tag{8.13}$$

Because Π_2 is a projector and $\langle\psi| \Pi_2 |\psi\rangle = 1$, we have $|\psi\rangle \in \Pi_2$. □

Lemma 8.2. *Consider any partial isometries V_1, V_2. If $V_2 = V_1 \cdot \Pi^{\mathcal{D}(V_2)}$, then $\mathcal{D}(V_2)$ is a subspace of $\mathcal{D}(V_1)$. And if $V_2 = \Pi^{\mathcal{I}(V_2)} \cdot V_1$, then $\mathcal{I}(V_2)$ is a subspace of $\mathcal{I}(V_1)$.*

Proof. From $V_2 = V_1 \cdot \Pi^{\mathcal{D}(V_2)}$, we have

$$\Pi^{\mathcal{D}(V_2)} = V_2^{\dagger} \cdot V_2 = \Pi^{\mathcal{D}(V_2)} \cdot V_1^{\dagger} \cdot V_1 \cdot \Pi^{\mathcal{D}(V_2)} = \Pi^{\mathcal{D}(V_2)} \cdot \Pi^{\mathcal{D}(V_1)} \cdot \Pi^{\mathcal{D}(V_2)}. \tag{8.14}$$

Hence from Lemma 8.1, we have $\mathcal{D}(V_2)$ is a subspace of $\mathcal{D}(V_1)$.

From $V_2 = \Pi^{\mathcal{I}(V_2)} \cdot V_1$, we have

$$\Pi^{\mathcal{I}(V_2)} = V_2 \cdot V_2^{\dagger} = \Pi^{\mathcal{I}(V_2)} \cdot V_1 \cdot V_1^{\dagger} \cdot \Pi^{\mathcal{I}(V_2)} = \Pi^{\mathcal{I}(V_2)} \cdot \Pi^{\mathcal{I}(V_1)} \cdot \Pi^{\mathcal{I}(V_2)}. \tag{8.15}$$

Hence from Lemma 8.1, we have $\mathcal{I}(V_2)$ is a subspace of $\mathcal{I}(V_1)$. □

Corollary 8.1. *$\mathcal{I}(W^L)$ is a subspace of $\mathcal{I}(V^L)$. And $\mathcal{I}(W^R)$ is a subspace of $\mathcal{I}(V^R)$.*

Proof. This follows immediately from Eq. (8.10), Eq. (8.11), and Lemma 8.2. □

Claim 17 (W is a restriction of V)**.** *We have*

$$W = V \cdot \Pi^{\mathcal{D}(W)}, \tag{8.16}$$
$$W^{\dagger} = V^{\dagger} \cdot \Pi^{\mathcal{I}(W)}. \tag{8.17}$$

In words, Claim 17 says that for any state in $\mathcal{D}(W)$, the domain of W, the action of W is the same as V. Additionally, it says that for any state in the image in $\mathcal{I}(W)$, the image of W, the action of $W^\dagger$ is the same as $V^\dagger$.

Proof of Claim 17. To prove Eq. (8.16), it suffices to show that

$$V \cdot \Pi^{\mathcal{D}(W^L)} = W^L, \tag{8.18}$$

$$V \cdot \Pi^{\mathcal{I}(W^R)} = W^{R,\dagger}. \tag{8.19}$$

This is because summing these two equations gives

$$V \cdot (\Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}) = W^L + W^{R,\dagger}, \tag{8.20}$$

and plugging in $\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}$ from Eq. (7.7) and $W = W^L + W^{R,\dagger}$ yields Eq. (8.16). It remains to prove Eqs. (8.18) and (8.19).

- **Proof of Eq. (8.18).** By the definition of V, we have

$$V \cdot \Pi^{\mathcal{D}(W^L)} = \left(V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) + (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}\right) \cdot \Pi^{\mathcal{D}(W^L)}. \tag{8.21}$$

  Note that $V^{R,\dagger} \cdot \Pi^{D(W^L)} = V^{R,\dagger} \cdot W^{L,\dagger} \cdot W^L = (W^L \cdot V^R)^\dagger \cdot W^L = 0$, where the final equality uses Eq. (8.12). Thus,

$$V \cdot \Pi^{\mathcal{D}(W^L)} = V^L \cdot \Pi^{\mathcal{D}(W^L)} = W^L, \tag{8.22}$$

  where the second equality follows from Eq. (8.10).

- **Proof of Eq. (8.19).** By the definition of V,

$$V \cdot \Pi^{\mathcal{I}(W^R)} = \left(V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) + (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}\right) \cdot \Pi^{\mathcal{I}(W^R)}. \tag{8.23}$$

  Since $\mathcal{I}(W^R)$ is a subspace of $\mathcal{I}(V^R)$ by Corollary 8.1, we have $V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) \cdot \Pi^{\mathcal{I}(W^R)} = 0$. Next, we have $V^{R,\dagger} \cdot \Pi^{\mathcal{I}(W^R)} = (\Pi^{\mathcal{I}(W^R)} \cdot V^R)^\dagger = W^{R,\dagger}$ by Eq. (8.11). Thus, we have

$$V \cdot \Pi^{\mathcal{I}(W^R)} = (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot W^{R,\dagger} \tag{8.24}$$

$$= W^{R,\dagger} - V^L \cdot V^{L,\dagger} \cdot W^{R,\dagger} \tag{8.25}$$

$$= W^{R,\dagger}, \tag{8.26}$$

  where the last equality uses the fact that $V^{L,\dagger} \cdot W^{R,\dagger} = (W^R \cdot V^L)^\dagger = 0$ from Eq. (8.12).

This completes the proof of Eq. (8.16). The proof of Eq. (8.17) follows by a symmetric argument. □

Corollary 8.2. *$\Pi^{\mathcal{D}(W)}$ is a subspace of $\Pi^{\mathcal{D}(V)}$. And $\Pi^{\mathcal{I}(W)}$ is a subspace of $\Pi^{\mathcal{I}(V)}$.*

Proof. This follows immediately from Claim 17 and Lemma 8.2. □

Corollary 8.3. *We have*

$$W^\dagger \cdot V = \Pi^{\mathcal{D}(W)} \tag{8.27}$$

$$W \cdot V^\dagger = \Pi^{\mathcal{I}(W)}. \tag{8.28}$$

Proof. From $W = V \cdot \Pi^{\mathcal{D}(W)}$, we can multiply $V^\dagger$ on the left of both sides to obtain

$$V^\dagger \cdot W = V^\dagger \cdot V \cdot \Pi^{\mathcal{D}(W)}. \tag{8.29}$$

Using $V^\dagger \cdot V = \Pi^{\mathcal{D}(V)}$, we have

$$V^\dagger \cdot W = \Pi^{\mathcal{D}(V)} \cdot \Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W)}, \tag{8.30}$$

since $\Pi^{\mathcal{D}(W)}$ is a subspace of $\Pi^{\mathcal{D}(V)}$ from Corollary 8.2. Taking dagger yields $W^\dagger \cdot V = \Pi^{\mathcal{D}(W)}$.

From $W^\dagger = V^\dagger \cdot \Pi^{\mathcal{I}(W)}$, we can multiply V on the left of both sides to obtain

$$V \cdot W^\dagger = V \cdot V^\dagger \cdot \Pi^{\mathcal{I}(W)}. \tag{8.31}$$

Using $V \cdot V^\dagger = \Pi^{\mathcal{I}(V)}$, we have

$$V \cdot W^\dagger = \Pi^{\mathcal{I}(V)} \cdot \Pi^{\mathcal{I}(W)} = \Pi^{\mathcal{I}(W)}, \tag{8.32}$$

since $\Pi^{\mathcal{I}(W)}$ is a subspace of $\Pi^{\mathcal{I}(V)}$ from Corollary 8.2. Taking dagger yields $W \cdot V^\dagger = \Pi^{\mathcal{I}(W)}$. □

9 The strong PRU proof

9.1 Setup

We define a distribution over n-qubit unitaries parameterized by any n-qubit unitary 2-design $\mathfrak{D}$.

Definition 28 ($\mathsf{sPRU}(\mathfrak{D})$ distribution)**.** *For any distribution $\mathfrak{D}$ supported on $\mathcal{U}(N)$, define the distribution $\mathsf{sPRU}(\mathfrak{D})$ as follows:*

1. *Sample a uniformly random permutation $\pi \leftarrow \mathsf{Sym}_N$, a uniformly random $f \leftarrow \{0,1,2\}^N$, and two independently sampled n-qubit unitaries $C, D \leftarrow \mathfrak{D}$. Following the definitions in Section 6,*

$$F_f := \sum_{x \in [N]} e^{2\pi \cdot f(x) \cdot i/3} |x\rangle\langle x| \quad \text{and} \quad P_\pi := \sum_{x \in [N]} |\pi(x)\rangle\langle x| . \tag{9.1}$$

2. *Output the n-qubit unitary $\mathcal{O} := D \cdot P_\pi \cdot F_f \cdot C$.*

The goal of this section is to prove the following theorem.

Theorem 6 ($\mathsf{sPRU}(\mathfrak{D})$ is a statistical strong PRU)**.** *Let $\mathcal{A}$ be a t-query oracle adversary that can perform forward and inverse queries and let $\mathfrak{D}$ be an exact unitary 2-design. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O} \leftarrow \mathsf{sPRU}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}} , \mathop{\mathbb{E}}_{\mathcal{O} \leftarrow \mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}} \right) \leq \frac{18t(t+1)}{N^{1/8}} \tag{9.2}$$

Since quantum-secure pseudorandom permutations and pseudorandom functions exist assuming one-way functions by [Zha16, Zha21], the existence of computationally-secure strong PRUs follows immediately from Theorem 6.

Theorem 7. *If quantum-secure one-way functions exist, then strong pseudorandom unitaries exist.*

The main technical component of the proof of Theorem 6 is Lemma 9.1, which relates the PRU adversary to an adversary that queries the path-recording oracle V, defined previously in Section 8. Recall that V is a partial isometry that acts on registers $(\mathsf{A}, \mathsf{L}, \mathsf{R})$, where L and R are variable-length registers. Initially, L and R are both initialized to the length-0 state $|\varnothing\rangle$. To state Lemma 9.1, we will need the following definition.

Definition 29 (the global state after queries to V)**.** *For a t-query oracle adversary $\mathcal{A}$ that can perform forward and inverse queries and any $0 \le i \le t$, let*

$$|\mathcal{A}_i^V\rangle_{\mathsf{ABLR}} := \prod_{i=1}^{t} \left(\left((1-b_i) \cdot V_{\mathsf{ALR}} + b_i \cdot V_{\mathsf{ALR}}^\dagger \right) \cdot A_{i,\mathsf{AB}} \right) |0^{n+m}\rangle_{\mathsf{AB}} \otimes |\varnothing\rangle_{\mathsf{L}} \, |\varnothing\rangle_{\mathsf{R}} \tag{9.3}$$

denote the global state on registers $\mathsf{A}, \mathsf{B}, \mathsf{L}, \mathsf{R}$ after $\mathcal{A}$ makes i queries to V.

Lemma 9.1 ($\mathsf{sPRU}(\mathfrak{D})$ is indistinguishable from V)**.** *Let $\mathfrak{D}$ be any exact unitary 2-design. For any t-query oracle adversary $\mathcal{A}$,*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O} \leftarrow \mathsf{sPRU}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}, \ \mathrm{Tr}_{\mathsf{LR}}\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}} \right) \right) \le \frac{9t(t+1)}{N^{1/8}} \tag{9.4}$$

Lemma 9.1 implies Theorem 6. Lemma 9.1 implies Theorem 6 by the following argument. We can instantiate $\mathfrak{D} = \mu_{\mathsf{Haar}}$, i.e., $\mathfrak{D}$ outputs a Haar-random n-qubit unitary. Then the output of $\mathsf{sPRU}(\mathfrak{D}) = \mathsf{sPRU}(\mu_{\mathsf{Haar}})$ is $D \cdot P_\pi \cdot F_f \cdot C$ for random π, f and Haar-random D and C. By invariance of the Haar measure, this is exactly the same as outputting a Haar-random unitary. Thus, we have the following corollary of Lemma 9.1.

Theorem 8 (V is indistinguishable from a Haar-random unitary)**.** *Let $\mathcal{A}$ be a t-query oracle adversary that can perform forward and inverse queries. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O} \leftarrow \mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}, \ \mathrm{Tr}_{\mathsf{LR}}\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABLR}} \right) \right) \le \frac{9t(t+1)}{N^{1/8}}. \tag{9.5}$$

Theorem 6 follows from combining Lemma 9.1 and Theorem 8 using the triangle inequality. The remainder of this section is devoted to proving Lemma 9.1.

9.2 V is indistinguishable from twirled W

Our first step towards proving Lemma 9.1 is to prove that an oracle adversary $\mathcal{A}$ that makes both forward and inverse queries cannot distinguish whether its query is implemented by the path-recording oracle V (Definition 26), or as $D \cdot W \cdot C$ where $C, D \leftarrow \mathfrak{D}$ are sampled from a 2-design, and W is the *partial* path-recording oracle (Definition 24).

We will require the following definitions. Let C and D be a pair of registers that each contain the *description* of an n-qubit unitary. These registers will be part of the purification and will not be in the adversary's view.

Definition 30. *For any distribution $\mathfrak{D}$ over n-qubit unitaries, define the state*

$$|\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} := \int_{C,D} \sqrt{d\mu_{\mathfrak{D}}(C) d\mu_{\mathfrak{D}}(D)} \, |C\rangle_{\mathsf{C}} \otimes |D\rangle_{\mathsf{D}}, \tag{9.6}$$

where $\mu_{\mathfrak{D}}(C)$ is the probability measure for which C is sampled from $\mathfrak{D}$.

Recall from Definition 27 that for any pair of n-qubit unitaries C, D, the operator $Q[C,D]_{\mathsf{LR}}$ is defined as

$$Q[C,D] := (C \otimes D^T)_{\mathsf{L}}^{\otimes *} \otimes (\overline{C} \otimes D^\dagger)_{\mathsf{R}}^{\otimes *}. \tag{9.7}$$

Definition 31 (Controlled C, D and Q)**.** *Define the following operators*

$$\mathsf{cC} \coloneqq \int_C C_{\mathsf{A}} \otimes |C\rangle\langle C|_{\mathsf{C}}\,, \quad \mathsf{cD} \coloneqq \int_D D_{\mathsf{A}} \otimes |D\rangle\langle D|_{\mathsf{D}}\,, \tag{9.8}$$

$$\mathsf{cQ} \coloneqq \int_{C,D} Q[C,D]_{\mathsf{L},\mathsf{R}} \otimes |C\rangle\langle C|_{\mathsf{C}} \otimes |D\rangle\langle D|_{\mathsf{D}}\,. \tag{9.9}$$

We now state a key lemma that we will need for our proof.

Lemma 9.2 (Twirling)**.** *For any unitary 2-design $\mathfrak{D}$, and any integer $0 \le t \le N-1$, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} - \Pi^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}}\right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \le 6t\sqrt{\frac{t}{N}}, \tag{9.10}$$

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} - \Pi^{\mathcal{I}(W)}_{\le t,\mathsf{ALR}}\right) \cdot (D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \le 6t\sqrt{\frac{t}{N}}, \tag{9.11}$$

Note that in the statement of Lemma 9.2, $\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}}$ is shorthand for $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}}$, and thus the operators inside the $\|\cdot\|_{\mathrm{op}}$ act on $\mathsf{A},\mathsf{L},\mathsf{R}$. We prove Lemma 9.2 in Section 11.

Next, we define the following adversary states.

Definition 32 (Twirled-W purification)**.** *Define the states $|\mathcal{A}^{W,\mathfrak{D}}_i\rangle_{\mathsf{ABLRCD}}$ as follows:*

$$|\mathcal{A}^{W,\mathfrak{D}}_0\rangle \coloneqq |0^n\rangle_{\mathsf{A}}\, |0^m\rangle_{\mathsf{B}}\, |\varnothing\rangle_{\mathsf{L}}\, |\varnothing\rangle_{\mathsf{R}}\, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}}\,, \tag{9.12}$$

$$\text{For} \quad i = 1,\dots,t: \quad |\mathcal{A}^{W,\mathfrak{D}}_i\rangle \coloneqq \Big((1-b_i)\cdot(\mathsf{cD}\cdot W\cdot \mathsf{cC}) + b_i\cdot(\mathsf{cD}\cdot W\cdot \mathsf{cC})^\dagger\Big)\cdot A_i\cdot |\mathcal{A}^{W,\mathfrak{D}}_{i-1}\rangle\,. \tag{9.13}$$

For contrast, let us recall the definition of $|\mathcal{A}^V_i\rangle$.

Definition 33 (V purification)**.** *Define the states $|\mathcal{A}^V_i\rangle_{\mathsf{ABLR}}$ for $0 \le i \le t$ as follows:*

$$|\mathcal{A}^V_0\rangle \coloneqq |0^n\rangle_{\mathsf{A}}\, |\varnothing\rangle_{\mathsf{L}}\, |\varnothing\rangle_{\mathsf{R}}\,, \tag{9.14}$$

$$\text{For} \quad i = 1,\dots,t: \quad |\mathcal{A}^V_i\rangle \coloneqq \Big((1-b_i)\cdot V + b_i\cdot V^\dagger\Big)\cdot A_i\cdot |\mathcal{A}^V_{i-1}\rangle\,. \tag{9.15}$$

Note that because $b_i \in \{0,1\}$, in the construction of these purified states, one either queries V, $\mathsf{cD}\cdot W\cdot\mathsf{cC}$ for $b_i = 0$ or $V^\dagger$, $(\mathsf{cD}\cdot W\cdot\mathsf{cC})^\dagger$ for $b_i = 1$. Because W and V are partial isometries from Claim 11 and Claim 15, $W, W^\dagger, V, V^\dagger$ are all equal to applying a projector followed by a unitary. Hence, $|\mathcal{A}^V_t\rangle$, $|\mathcal{A}^{W,\mathfrak{D}}_t\rangle$ are both states with norm at most 1.

Fact 10 (Norm of the purified states)**.** *For any $t \ge 0$, $|\mathcal{A}^V_t\rangle$, $|\mathcal{A}^{W,\mathfrak{D}}_t\rangle$ both have norm at most 1.*

Furthermore, from Definition 26, V and $V^\dagger$ take states in the subspace associated with the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\le i,\mathsf{LR}}$ to the the subspace associated with the projector $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathcal{R}^2}_{\le i+1,\mathsf{LR}}$. Hence, after t queries in total to V and $V^\dagger$, we have $|\mathcal{A}^V_t\rangle$ is in the image of $\Pi^{\mathcal{R}^2}_{\le t}$. Similarly, from Fact 7, W and $W^\dagger$ map states in $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\le i,\mathsf{LR}}$ to $\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathsf{bij}}_{\le i+1,\mathsf{LR}}$. Hence, after t queries to W and $W^\dagger$, we have $|\mathcal{A}^{W,\mathfrak{D}}_t\rangle$ is in the image of $\Pi^{\mathsf{bij}}_{\le t}$. We collect these two basic properties in Fact 11.

Fact 11 (Spaces that the purified states are in)**.** *For any $t \ge 0$, we have the following guarantees:*

- *$|\mathcal{A}^V_t\rangle$ is in the image of $\Pi^{\mathcal{R}^2}_{\le t}$.*
- *$|\mathcal{A}^{W,\mathfrak{D}}_t\rangle$ is in the image of $\Pi^{\mathsf{bij}}_{\le t}$.*

The main technical claim of this subsection is the following.

Claim 18. *For any integer $t \geq 0$,*

$$\mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}} |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^V\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \right] \geq 1 - \frac{35t^2}{N^{1/4}} \tag{9.16}$$

Proof of Claim 18. We prove this claim by induction. When $t = 0$, we have

$$\mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) = \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|0^n\rangle_{\mathsf{A}} \, |\varnothing\rangle_{\mathsf{L}} \, |\varnothing\rangle_{\mathsf{R}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \tag{9.17}$$

$$= |0^n\rangle_{\mathsf{A}} \, |\varnothing\rangle_{\mathsf{L}} \, |\varnothing\rangle_{\mathsf{R}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \tag{9.18}$$

$$= |A_0^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}}\,, \tag{9.19}$$

where the first equality is by the definition of $|\mathcal{A}_0^V\rangle$ (Definition 33), the second is because cQ acts as identity on $|\varnothing\rangle_{\mathsf{L}} \, |\varnothing\rangle_{\mathsf{R}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{LR}}$, and the third equality is the definition of $|\mathcal{A}_0^{W,\mathfrak{D}}\rangle$ (Definition 32). This implies that

$$\mathrm{Re}\left[\langle \mathcal{A}_0^{W,\mathfrak{D}} |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_0^V\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \right] = 1, \tag{9.20}$$

so the base case holds.

For the inductive step, assume that

$$\mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}} |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^V\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \right] \geq 1 - \frac{35t^2}{N^{1/4}} \tag{9.21}$$

for some integer $t \geq 0$. We will prove that the claim holds for $t + 1$. To simplify notation, let us assume that the adversary makes a forward query at step $t + 1$, i.e., $b_{t+1} = 0$; this is without loss of generality because the argument is symmetric if the adversary makes an inverse query at step $t + 1$. We have

$$|\mathcal{A}_{t+1}^{W,\mathfrak{D}}\rangle = \mathsf{cD} \cdot W \cdot \mathsf{cC} \cdot A_{t+1} \cdot \, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\,, \tag{9.22}$$

$$\mathsf{cQ} \cdot \left(|\mathcal{A}_{t+1}^V\rangle \, |\mathsf{init}(\mathfrak{D})\rangle \right) = \mathsf{cQ} \cdot V \cdot A_{t+1} \cdot \, |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathfrak{D})\rangle \tag{9.23}$$

and thus

$$\mathrm{Re}\left[\langle \mathcal{A}_{t+1}^{W,\mathfrak{D}} | \cdot \mathsf{cQ} \cdot \left(|\mathcal{A}_{t+1}^V\rangle \, |\mathsf{init}(\mathfrak{D})\rangle \right) \right] \tag{9.24}$$

$$= \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}} | \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W^\dagger \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot V \cdot A_{t+1} \cdot \, |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathfrak{D})\rangle \right] \tag{9.25}$$

By Fact 11, the states $|\mathcal{A}_t^{W,\mathfrak{D}}\rangle$ and $|\mathcal{A}_t^V\rangle$ are both in the image of $\Pi_{\leq t}$. Following Notation 9, we write $W_{\leq t} = W \cdot \Pi_{\leq t}$ and $V_{\leq t} = V \cdot \Pi_{\leq t}$. We can then rewrite (9.25) as

$$(9.25) = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}} | \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\leq t}^\dagger \cdot \mathsf{cD}^\dagger \cdot \mathsf{cQ} \cdot V_{\leq t} \cdot A_{t+1} \cdot \, |\mathcal{A}_t^V\rangle \, |\mathsf{init}(\mathfrak{D})\rangle \right] \tag{9.26}$$

Next, we will write $\mathsf{cQ} \cdot V_{\leq t}$ as

$$\mathsf{cQ} \cdot V_{\leq t} = \mathsf{cD} \cdot V_{\leq t} \cdot \mathsf{cC} \cdot \mathsf{cQ}. + \left(\mathsf{cQ} \cdot V_{\leq t} - \mathsf{cD} \cdot V_{\leq t} \cdot \mathsf{cC} \cdot \mathsf{cQ} \right) \tag{9.27}$$

This allows us to rewrite (9.26) as

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

$$+ \operatorname{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot \mathsf{cD}^\dagger \cdot \Big(\mathsf{cQ} \cdot V_{\le t} - \mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ}\Big) \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle \right]. \tag{9.28}$$

We can lower bound the second term in the sum as follows. We know that $A_{t+1} \cdot |\mathcal{A}_t^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle$ and $\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot \mathsf{cD}^\dagger$ have at most unit norm by Fact 10 and the fact that $A_{t+1}, \mathsf{cC}, \mathsf{cD}, W_{\le t}^\dagger$ all have operator norm at most 1 (since $W_{\le t}^\dagger = (W \cdot \Pi_{\le t})^\dagger$ and W is a partial isometry by Claim 11). Then by Claim 16, the second term can be lower bounded by

$$- \left\| \Big(\mathsf{cD} \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ} - \mathsf{cQ} \cdot V_{\le t}\Big) \right\|_{\mathrm{op}} \tag{9.29}$$

$$- \left\| \sum_{C,D} \Big(D_{\mathsf{A}} \cdot V_{\le t} \cdot C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\le t} \Big) \otimes |C,D\rangle\langle C,D| \right\|_{\mathrm{op}} \tag{9.30}$$

$$- \max_{C,D} \left\| D_{\mathsf{A}} \cdot V_{\le t} \cdot C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\le t} \right\|_{\mathrm{op}} \tag{9.31}$$

$$\ge -16\sqrt{\frac{2t(t+1)}{N}}. \qquad \text{(by Claim 16)} \tag{9.32}$$

Combining this bound with the sequence of equalities (9.24) = (9.25) = (9.26) = (9.28), we get

$$\operatorname{Re}\left[\langle \mathcal{A}_{t+1}^{W,\mathfrak{D}}| \cdot \mathsf{cQ} \cdot \Big(|\mathcal{A}_{t+1}^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle \Big) \right] \tag{9.33}$$

$$\ge \underbrace{\operatorname{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot W_{\le t}^\dagger \cdot V_{\le t} \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle \right]}_{:=\gamma_t} - 16\sqrt{\frac{2t(t+1)}{N}}. \tag{9.34}$$

Next we can use properties of the W and V operators to rewrite

$$W_{\le t}^\dagger \cdot V_{\le t} = \Big(W \cdot \Pi_{\le t}\Big)^\dagger \cdot V \cdot \Pi_{\le t} \tag{9.35}$$

$$= \Pi_{\le t} \cdot W^\dagger \cdot V \cdot \Pi_{\le t} \tag{9.36}$$

$$= \Pi_{\le t} \cdot \Pi^{\mathcal{D}(W)} \cdot \Pi_{\le t} \qquad \text{(by Corollary 8.3)} \tag{9.37}$$

$$= \Pi_{\le t} \cdot \Big(\Pi^{\mathsf{bij}} - (\Pi^{\mathsf{bij}} - \Pi^{\mathcal{D}(W)})\Big) \cdot \Pi_{\le t} \tag{9.38}$$

$$= \Pi_{\le t}^{\mathsf{bij}} - \Big(\Pi_{\le t}^{\mathsf{bij}} - \Pi_{\le t}^{\mathcal{D}(W)}\Big) \qquad \text{(Definition 23 and Claim 12)} \tag{9.39}$$

Plugging this into γ_t, we get

$$\gamma_t = \underbrace{\operatorname{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \Pi_{\le t}^{\mathsf{bij}} \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle \right]}_{:=\alpha_t} \tag{9.40}$$

$$- \underbrace{\operatorname{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \Big(\Pi_{\le t}^{\mathsf{bij}} - \Pi_{\le t}^{\mathcal{D}(W)}\Big) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle\ |\mathsf{init}(\mathfrak{D})\rangle \right]}_{:=\beta_t} \tag{9.41}$$

Bounding α_t. Observe that

$$\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \Pi_{\le t}^{\mathsf{bij}} \tag{9.42}$$

$$= \langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot \Pi_{\le t}^{\mathsf{bij}} \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \qquad (\ \Pi_{\le t,\mathsf{LR}}^{\mathsf{bij}} \text{ commutes with } (A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger)_{\mathsf{A}}) \tag{9.43}$$

$$= \langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger. \qquad \text{(by Fact 11)}$$

Thus,

$$\alpha_t = \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot \mathsf{cQ} \cdot |\mathcal{A}_t^V\rangle \ |\mathsf{init}(\mathfrak{D})\rangle \right] \geq 1 - \frac{35t^2}{N^{1/4}}, \tag{9.40}$$

by the inductive hypothesis.

Bounding β_t. We will lower bound $-\beta_t$ by upper bounding β_t:

$$\beta_t \leq \left| \langle \mathcal{A}_t^{W,\mathfrak{D}}| \cdot A_{t+1}^\dagger \cdot \mathsf{cC}^\dagger \cdot \left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot A_{t+1} \cdot |\mathcal{A}_t^V\rangle \ |\mathsf{init}(\mathfrak{D})\rangle \right| \tag{9.41}$$

$$\leq \max_{\substack{|u\rangle \in \mathcal{H}_{\mathsf{ABLRCD}}: \||u\rangle\|_2 \leq 1 \\ |v\rangle \in \mathcal{H}_{\mathsf{ABLR}}: \||v\rangle\|_2 \leq 1}} \left| \langle u| \cdot \left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot |v\rangle \ |\mathsf{init}(\mathfrak{D})\rangle \right|, \tag{9.42}$$

$$= \left(\max_{\substack{|v\rangle \in \mathcal{H}_{\mathsf{ABLR}}: \\ \||v\rangle\|_2 \leq 1}} \langle v| \ \langle \mathsf{init}(\mathfrak{D})| \cdot \mathsf{cQ}^\dagger \cdot \mathsf{cC}^\dagger \cdot \left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right) \cdot \mathsf{cC} \cdot \mathsf{cQ} \cdot |v\rangle \ |\mathsf{init}(\mathfrak{D})\rangle \right)^{1/2} \tag{9.43}$$

$$= \left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}}^{1/2} \tag{9.44}$$

$$\leq \left(6t\sqrt{\frac{t}{N}}\right)^{1/2} \leq \frac{3t^{3/4}}{N^{1/4}} \tag{9.45}$$

where:

- the first inequality uses the fact that $\mathrm{Re}(z) \leq |z|$,
- the second inequality holds because $\mathsf{cC} \cdot A_{t+1} \cdot |\mathcal{A}_t^{W,\mathfrak{D}}\rangle \in \mathcal{H}_{\mathsf{ABLRCD}}$ and $A_{t+1} \cdot |\mathcal{A}_t^V\rangle \in \mathcal{H}_{\mathsf{ABLR}}$ both have at most unit norm,
- the third line uses the fact that

$$\max_{\substack{|u\rangle: \||u\rangle\|_2 \leq 1, \\ |v\rangle: \||v\rangle\|_2 \leq 1}} |\langle u| \cdot M \cdot |v\rangle| = \left(\max_{|v\rangle: \||v\rangle\|_2 \leq 1} \langle v| \cdot M^\dagger \cdot M \cdot |v\rangle \right)^{1/2}, \tag{9.46}$$

  and the fact that $\left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right)^\dagger \cdot \left(\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}\right) = \Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}$, since $\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}$ is a projector.[7]
- the fourth line follows from the definitions of $|\mathsf{init}(\mathfrak{D})\rangle, \mathsf{cC}, \mathsf{cQ}$ (Definitions 30 and 31),
- and the last line follows from Lemma 9.2.

Note that in the fourth line, we can drop the B register since the operator inside the $\|\cdot\|_{\mathrm{op}}$ acts as identity on B. Putting everything together, we have

$$\mathrm{Re}\left[\langle \mathcal{A}_{t+1}^{W,\mathfrak{D}}| \cdot \mathsf{cQ} \cdot \left(|\mathcal{A}_{t+1}^V\rangle \ |\mathsf{init}(\mathfrak{D})\rangle \right) \right] \geq \alpha_t - \beta_t - 16\sqrt{\frac{2t(t+1)}{N}} \tag{9.47}$$

[7] By Fact 7, $\Pi^{\mathsf{bij}} - \Pi^{\mathcal{D}(W)}$ is a projector. By Claim 12, $\Pi^{\mathcal{D}(W)}$ commutes with $\Pi_{\leq t}$ and by Claim 12, Π^{bij} commutes with $\Pi_{\leq t}$ by Definition 23. Recall the fact that if Π_1 and Π_2 are projectors such that $[\Pi_1, \Pi_2] = 0$, then $\Pi_1 \cdot \Pi_2$ is a projector. Thus, since $\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)} = (\Pi^{\mathsf{bij}} - \Pi^{\mathcal{D}(W)}) \cdot \Pi_{\leq t}$, we have that $\Pi_{\leq t}^{\mathsf{bij}} - \Pi_{\leq t}^{\mathcal{D}(W)}$ is a projector.

$$\geq 1 - \frac{35t^2}{N^{1/4}} - \frac{3t^{3/4}}{N^{1/4}} - 16\sqrt{\frac{2t(t+1)}{N}} \tag{9.48}$$

$$\geq 1 - \frac{1}{N^{1/4}} \cdot \left(35t^2 + 3t^{3/4} + 16 \cdot \frac{2t}{N^{1/4}}\right) \tag{9.49}$$

$$\geq 1 - \frac{1}{N^{1/4}} \cdot \left(35t^2 + 35t\right) \tag{9.50}$$

$$\geq 1 - \frac{35(t+1)^2}{N^{1/4}}, \tag{9.51}$$

which establishes the claim for $t+1$. This concludes the proof. □

Lemma 9.3. *For any $0 \leq t < N$ and any unitary 2-design $\mathfrak{D}$, we have*

$$\mathsf{TD}(\mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}, \mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}) \leq \frac{9t}{N^{1/8}}. \tag{9.52}$$

Proof. Using the fact that $|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}}$ and $|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}}$ are subnormalized states from Fact 10 and that $\mathsf{TD}(|u\rangle\langle u|, |v\rangle\langle v|) \leq \| |u\rangle - |v\rangle \|_2$ for subnormalized states $|u\rangle, |v\rangle$, we have

$$\mathsf{TD}\left(|\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}, \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathfrak{D})\rangle\langle\mathsf{init}(\mathfrak{D})|_{\mathsf{CD}}\right) \cdot \mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right)^2 \tag{9.53}$$

$$\leq \left\| |\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLR}} - \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}}\right) \right\|_2^2 \tag{9.54}$$

$$= \langle\mathcal{A}_t^{W,\mathfrak{D}}|\mathcal{A}_t^{W,\mathfrak{D}}\rangle + \langle\mathcal{A}_t^{V}|\mathcal{A}_t^{V}\rangle - 2\,\mathrm{Re}\left[\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}}\right)\right] \tag{9.55}$$

$$\leq 2 - 2 \cdot (1 - \frac{35t^2}{N^{1/4}}) = \frac{70t^2}{N^{1/4}}. \qquad \text{(Using Claim 18)}$$

Therefore, using the fact that $\mathsf{cQ}_{\mathsf{LRCD}}$ acts only on $\mathsf{L}, \mathsf{R}, \mathsf{C}, \mathsf{D}$ and $\mathsf{cQ}_{\mathsf{LRCD}}$ is a unitary, we obtain

$$\mathsf{TD}(\mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}, \mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}) \tag{9.56}$$

$$= \mathsf{TD}\Big(\mathrm{Tr}_{-\mathsf{AB}}\, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}, \mathrm{Tr}_{-\mathsf{AB}}\left[\mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathfrak{D})\rangle\langle\mathsf{init}(\mathfrak{D})|_{\mathsf{CD}}\right) \cdot \mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right]\Big) \tag{9.57}$$

$$\leq \mathsf{TD}\left(|\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}, \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \otimes |\mathsf{init}(\mathfrak{D})\rangle\langle\mathsf{init}(\mathfrak{D})|_{\mathsf{CD}}\right) \cdot \mathsf{cQ}_{\mathsf{LRCD}}^\dagger\right) \tag{9.58}$$

$$\leq \sqrt{\frac{70t^2}{N^{1/4}}} \leq \frac{9t}{N^{1/8}}. \tag{9.59}$$

This completes the proof. □

9.3 Twirled W and twirled pfO are indistinguishable

Let $|+_{N!}\rangle_{\mathsf{P}}$ and $|+_{3^N}\rangle_{\mathsf{F}}$ denote the uniform superposition over all permutations and functions, respectively. We define the follow state obtained by querying twirled pfO.

Definition 34 (Twirled pfO purification)**.** *Let*

$$|\mathcal{A}_0^{\mathsf{pfO},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}} := |0^n\rangle_{\mathsf{A}}\, |0^m\rangle_{\mathsf{B}}\, |+_{N!}\rangle_{\mathsf{P}}\, |+_{3^N}\rangle_{\mathsf{F}}\, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}}, \tag{9.60}$$

For $1 \leq i \leq t$, define

$$|\mathcal{A}_i^{\mathsf{pfO},\mathfrak{D}}\rangle := \left((1-b_i) \cdot (\mathsf{cD} \cdot \mathsf{pfO} \cdot \mathsf{cC}) + b_i \cdot (\mathsf{cD} \cdot \mathsf{pfO} \cdot \mathsf{cC})^\dagger\right) \cdot A_i \cdot |\mathcal{A}_{i-1}^{\mathsf{pfO},\mathfrak{D}}\rangle. \tag{9.61}$$

To connect twirled W and twirled pfO, we need to define the following projections.

Definition 35. *Define the projectors*

$$\widetilde{\Pi}^{\mathcal{D}(W)} \coloneqq \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{D}(W)} \cdot \mathsf{Comp}, \tag{9.62}$$

$$\widetilde{\Pi}^{\mathcal{I}(W)} \coloneqq \mathsf{Comp}^\dagger \cdot \Pi^{\mathcal{I}(W)} \cdot \mathsf{Comp}. \tag{9.63}$$

We define the following state obtained by querying twirled pfO, but depending on whether forward or inverse query (determined by b_i) is made, we will add a projector.

Definition 36 (Twirled projected pfO purification)**.** *Let* $|\mathcal{A}_0^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle \coloneqq |\mathcal{A}_0^{\mathsf{pfO},\mathfrak{D}}\rangle$*. For* $1 \le i \le t$*, define*

$$|\mathcal{A}_i^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle \coloneqq \Big((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{pfO}\cdot\widetilde{\Pi}^{\mathcal{D}(W)}\cdot\mathsf{cC}) + b_i\cdot(\mathsf{cC}^\dagger\cdot\mathsf{pfO}^\dagger\cdot\widetilde{\Pi}^{\mathcal{I}(W)}\cdot\mathsf{cD}^\dagger)\Big)\cdot A_i\cdot|\mathcal{A}_{i-1}^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle\,. \tag{9.64}$$

Claim 19. *For all integers* $0 \le t \le N$*,*

$$|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} = \mathsf{Comp}\cdot|\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}}\,. \tag{9.65}$$

Proof. We prove this using induction. The base case $t=0$ follows from the fact that

$$\mathsf{Comp}\cdot|+_{N!}\rangle_{\mathsf{P}}\,|+_{3^N}\rangle_{\mathsf{F}} = |\varnothing\rangle_{\mathsf{L}}\,|\varnothing\rangle_{\mathsf{R}}\,. \tag{9.66}$$

If $|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} = \mathsf{Comp}\cdot|\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}}$ for $t>0$, then we have

$$|\mathcal{A}_{t+1}^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} \tag{9.67}$$

$$= \Big((1-b_i)\cdot(\mathsf{cD}\cdot W\cdot\mathsf{cC}) + b_i\cdot(\mathsf{cD}\cdot W\cdot\mathsf{cC})^\dagger\Big)\cdot A_i\cdot|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} \tag{9.68}$$

$$\begin{aligned}= \Big((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{Comp}\cdot\mathsf{pfO}\cdot\mathsf{Comp}^\dagger\cdot\Pi^{\mathcal{D}(W)}\cdot\mathsf{cC}) \\ + b_i\cdot(\mathsf{cC}^\dagger\cdot\mathsf{Comp}\cdot\mathsf{pfO}^\dagger\cdot\mathsf{Comp}^\dagger\cdot\Pi^{\mathcal{I}(W)}\cdot\mathsf{cD}^\dagger)\Big)\cdot A_i\cdot|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} \qquad \text{(Using Claim 13)}\end{aligned}$$

$$\begin{aligned}= \mathsf{Comp}\cdot\Big((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{pfO}\cdot\widetilde{\Pi}^{\mathcal{D}(W)}\cdot\mathsf{cC}) \\ + b_i\cdot\mathsf{cC}^\dagger\cdot\mathsf{pfO}^\dagger\cdot\widetilde{\Pi}^{\mathcal{I}(W)}\cdot\mathsf{cD}^\dagger\Big)\cdot A_i\cdot\mathsf{Comp}^\dagger\cdot|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}}\end{aligned} \tag{9.69}$$

$$\begin{aligned}= \mathsf{Comp}\cdot\Big((1-b_i)\cdot(\mathsf{cD}\cdot\mathsf{pfO}\cdot\widetilde{\Pi}^{\mathcal{D}(W)}\cdot\mathsf{cC}) \\ + b_i\cdot\mathsf{cC}^\dagger\cdot\mathsf{pfO}^\dagger\cdot\widetilde{\Pi}^{\mathcal{I}(W)}\cdot\mathsf{cD}^\dagger\Big)\cdot A_i\cdot|\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}} \qquad \text{(inductive hypothesis)}\end{aligned}$$

$$= \mathsf{Comp}\cdot|\mathcal{A}_{t+1}^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}}\,. \tag{9.70}$$

This concludes the proof. □

Lemma 9.4 (Norm bound)**.** *For any* $0 \le t < N$ *and any unitary 2-design* $\mathfrak{D}$*, we have*

$$1 \ge \langle\mathcal{A}_t^{W,\mathfrak{D}}|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} \ge 1 - \frac{70t^2}{N^{1/4}}. \tag{9.71}$$

Proof. We can utilize the following bounds,

$$\langle\mathcal{A}_t^{W,\mathfrak{D}}|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}} \tag{9.72}$$

$$\ge \langle\mathcal{A}_t^{W,\mathfrak{D}}|\mathcal{A}_t^{W,\mathfrak{D}}\rangle_{\mathsf{ABLRCD}}\cdot\langle\mathcal{A}_t^{V}|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \qquad (\langle\mathcal{A}_t^{V}|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \le 1 \text{ from Fact 10})$$

$$= \langle \mathcal{A}_t^{W,\mathfrak{D}} | \mathcal{A}_t^{W,\mathfrak{D}} \rangle_{\mathsf{ABLRCD}} \cdot \left(\langle \mathcal{A}_t^{V} |_{\mathsf{ABLR}} \, \langle \mathsf{init}(\mathfrak{D})|_{\mathsf{CD}} \right) \cdot \mathsf{cQ}^\dagger \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \tag{9.73}$$

$$\geq \left| \langle \mathcal{A}_t^{W,\mathfrak{D}} |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \right|^2 \qquad \text{(Cauchy-Schwarz inequality)}$$

$$\geq \mathrm{Re}\left[\langle \mathcal{A}_t^{W,\mathfrak{D}} |_{\mathsf{ABLRCD}} \cdot \mathsf{cQ}_{\mathsf{LRCD}} \cdot \left(|\mathcal{A}_t^{V}\rangle_{\mathsf{ABLR}} \, |\mathsf{init}(\mathfrak{D})\rangle_{\mathsf{CD}} \right) \right]^2 \tag{9.74}$$

$$\geq (1 - \frac{35t^2}{N^{1/4}})^2 \geq 1 - \frac{70t^2}{N^{1/4}}, \qquad \text{(Using Claim 18)}$$

which completes the proof. □

Lemma 9.5. *For all integers* $0 \leq t \leq N$,

$$\mathsf{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}} , \mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}} \right) \leq \frac{9t^2}{N^{1/8}}. \tag{9.75}$$

Proof. Because Comp acts on registers P, F and maps to L, R, we have

$$\mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}} = \mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}|_{\mathsf{ABPFCD}} . \tag{9.76}$$

Because pfO is an isometry, $|\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}}$ has norm 1. Furthermore, from Claim 19, because Comp is an isometry, we have

$$\langle \mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}} | \mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}} \rangle_{\mathsf{ABPFCD}} = \left\langle \mathcal{A}_t^{W,\mathfrak{D}} \middle| \mathcal{A}_t^{W,\mathfrak{D}} \right\rangle_{\mathsf{ABLRCD}} \leq 1. \tag{9.77}$$

Together, we can obtain the following,

$$\mathsf{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}} , \mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}} \right) \tag{9.78}$$

$$= \mathsf{TD}\left(\mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}} , \mathrm{Tr}_{-\mathsf{AB}} \, |\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}|_{\mathsf{ABPFCD}} \right) \tag{9.79}$$

$$\leq \mathsf{TD}\left(|\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}} , |\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}|_{\mathsf{ABPFCD}} \right) \tag{9.80}$$

$$\leq \left\| |\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}} - |\mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}}\rangle_{\mathsf{ABPFCD}} \right\|_2 \qquad (\tfrac{1}{2}\left\|uu^\dagger - vv^\dagger\right\|_{\mathrm{tr}} \leq \|u-v\|_2 \text{ if } \|u\|_2, \|v\|_2 \leq 1)$$

$$\leq t \cdot \sqrt{1 - \left\langle \mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}} \middle| \mathcal{A}_t^{\widetilde{\mathsf{pfO}},\mathfrak{D}} \right\rangle_{\mathsf{ABPFCD}}} \qquad \text{(Lemma 2.3 on sequential gentle measurement)}$$

$$= t \cdot \sqrt{1 - \left\langle \mathcal{A}_t^{W,\mathfrak{D}} \middle| \mathcal{A}_t^{W,\mathfrak{D}} \right\rangle_{\mathsf{ABLRCD}}} \qquad \text{(Claim 19)}$$

$$\leq t \cdot \sqrt{\frac{70t^2}{N^{1/4}}} \leq \frac{9t^2}{N^{1/8}}. \qquad \text{(Lemma 9.4)}$$

This concludes the proof. □

9.4 Proof of Lemma 9.1

From Claim 6, we have

$$\mathrm{Tr}_{\mathsf{PFCD}} \, |\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}} = \mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{sPRU}(\mathfrak{D})} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}} . \tag{9.81}$$

From Lemma 9.3, we have

$$\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{LRCD}} \, |\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}} , \mathrm{Tr}_{\mathsf{LR}} \, |\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}} \right) \leq \frac{9t}{N^{1/8}}. \tag{9.82}$$

From Lemma 9.5, we have

$$\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{PFCD}}\,|\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}}\,,\mathrm{Tr}_{\mathsf{LRCD}}\,|\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}\right)\leq\frac{9t^2}{N^{1/8}}. \tag{9.83}$$

By triangle inequality, we have

$$\begin{aligned}
&\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mathsf{sPRU}(\mathfrak{D})}|\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}|_{\mathsf{AB}}\,,\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right) && (9.84)\\
&=\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{PFCD}}\,|\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}}\,,\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right) && (9.85)\\
&\leq\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{PFCD}}\,|\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}\rangle\langle\mathcal{A}_t^{\mathsf{pfO},\mathfrak{D}}|_{\mathsf{ABPFCD}}\,,\mathrm{Tr}_{\mathsf{LRCD}}\,|\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}\right)\\
&+\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{LRCD}}\,|\mathcal{A}_t^{W,\mathfrak{D}}\rangle\langle\mathcal{A}_t^{W,\mathfrak{D}}|_{\mathsf{ABLRCD}}\,,\mathrm{Tr}_{\mathsf{LR}}\,|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABLR}}\right) && (9.86)\\
&\leq\frac{9t(t+1)}{N^{1/8}}. && (9.87)
\end{aligned}$$

This completes the proof of Lemma 9.1.

10 Proof of Claim 16

In this section, we prove Claim 16, which states that the symmetric path recording oracle V is approximately unitary invariant. For convenience, we restate the lemma below:

Lemma 10.1 (Claim 16, restated)**.** *For any $0\leq t<N$, and any pair of n-qubit unitaries C,D, we have*

$$\|D_{\mathsf{A}}\cdot V_{\leq t}\cdot C_{\mathsf{A}}\otimes Q[C,D]_{\mathsf{LR}}-Q[C,D]_{\mathsf{LR}}\cdot V_{\leq t}\|_{\mathrm{op}}\leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{10.1}$$

$$\left\|C_{\mathsf{A}}^{\dagger}\cdot(V^{\dagger})_{\leq t}\cdot D_{\mathsf{A}}^{\dagger}\otimes Q[C,D]_{\mathsf{LR}}-Q[C,D]_{\mathsf{LR}}\cdot(V^{\dagger})_{\leq t}\right\|_{\mathrm{op}}\leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{10.2}$$

To prove this lemma, we will define a pair of operators E^L and E^R that satisfy *exact* unitary invariance. We will then prove that E^L is close in operator norm to V^L, and that E^R is close in operator norm to E^R. By combining these guarantees, we will show that V^L and V^R satisfy approximate unitary invariance, which we will use to prove that V satisfies approximate unitary invariance.

10.1 Defining E^L and E^R

Definition 37. *Define the operator E^L and E^R that act on registers $\mathsf{A},\mathsf{L},\mathsf{R}$ as follows:*

$$E^L:=\frac{1}{\sqrt{N}}\sum_{x,y\in[N]}|y\rangle\langle x|_{\mathsf{A}}\otimes\sum_{L\in\mathcal{R}}\sqrt{\mathsf{num}(L,(x,y))+1}\cdot\,|L\cup\{(x,y)\}\rangle\langle L|_{\mathsf{L}}\otimes\sum_{R\in\mathcal{R}}|R\rangle\langle R|_{\mathsf{R}}\,. \tag{10.3}$$

$$E^R:=\frac{1}{\sqrt{N}}\sum_{x,y\in[N]}|x\rangle\langle y|_{\mathsf{A}}\otimes\sum_{L\in\mathcal{R}}|L\rangle\langle L|_{\mathsf{L}}\otimes\sum_{R\in\mathcal{R}}\sqrt{\mathsf{num}(R,(x,y))+1}\cdot\,|R\cup\{(x,y)\}\rangle\langle R|_{\mathsf{R}}\,. \tag{10.4}$$

We will show that E^L and E^R satisfies the following unitary invariance property. To state the property, recall that we define the operator $Q[C,D]$ as follows:

Definition 38 (Definition 27, restated)**.** *For any pair of n-qubit unitaries C, D, define*

$$Q[C,D] \coloneqq (C \otimes D^T)^{\otimes *}_{\mathsf{L}} \otimes (\overline{C} \otimes D^\dagger)^{\otimes *}_{\mathsf{R}}. \tag{10.5}$$

Claim 20 (Exact unitary invariance of E^L and E^R)**.** *For any pair of n qubit unitaries C, D, we have*

$$D_{\mathsf{A}} \cdot E^L_{\mathsf{ALR}} \cdot C_{\mathsf{A}} = Q[C,D]_{\mathsf{LR}} \cdot E^L_{\mathsf{ALR}} \cdot Q[C,D]^\dagger_{\mathsf{LR}}, \tag{10.6}$$

$$C^\dagger_{\mathsf{A}} \cdot E^R_{\mathsf{ALR}} \cdot D^\dagger_{\mathsf{A}} = Q[C,D]_{\mathsf{LR}} \cdot E^R_{\mathsf{ALR}} \cdot Q[C,D]^\dagger_{\mathsf{LR}}, \tag{10.7}$$

To prove Claim 20, it will be useful to have the following alternative expressions for E^L and E^R.

Claim 21 (Alternative form of E^L and E^R)**.** *The E^L operator can also be written as*

$$E^L = \frac{1}{\sqrt{N}} \sum_{x,y \in [N]} |y\rangle\langle x|_{\mathsf{A}} \otimes \sum_{\ell \geq 0} \Pi^{\mathcal{R}}_{\ell+1,\mathsf{L}} \cdot \left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right)_{\mathsf{L}} \otimes \Pi^{\mathcal{R}}_{\mathsf{R}}. \tag{10.8}$$

$$E^R = \frac{1}{\sqrt{N}} \sum_{x,y \in [N]} |x\rangle\langle y|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\mathsf{L}} \otimes \sum_{r \geq 0} \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \cdot \left(\sqrt{r+1} \cdot |x,y\rangle \otimes \Pi_r\right)_{\mathsf{R}}. \tag{10.9}$$

Here Π_ℓ denotes the projector onto the span of length-ℓ states $|x_1, y_1, \ldots, x_\ell, y_\ell\rangle$, and $(|x,y\rangle \otimes \Pi_\ell)_{\mathsf{L}}$ is the linear operator that maps

$$(|x,y\rangle \otimes \Pi_\ell)_{\mathsf{L}} \cdot |x_1, y_1, \ldots, x_\ell, y_\ell\rangle = |x, y, x_1, y_1, \ldots, x_\ell, y_\ell\rangle. \tag{10.10}$$

Proof. We will prove the statement for E^L, and the proof for E^R will be symmetric. To establish (10.3) = (10.8), we need to prove that for all $(x,y) \in [N]^2$ and $\ell \geq 0$,

$$\sum_{L \in \mathcal{R}_\ell} \sqrt{\mathsf{num}(L,(x,y))+1} \cdot |L \cup \{(x,y)\}\rangle\langle L|_{\mathsf{L}} = \Pi^{\mathcal{R}}_{\ell+1,\mathsf{L}} \cdot \left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right)_{\mathsf{L}}. \tag{10.11}$$

Since $\Pi^{\mathcal{R}}_{\ell+1} = \sum_{R \in \mathcal{R}_{\ell+1}} |R\rangle\langle R|$ (Notation 5), we can write the right-hand side of Eq. (10.11) as

$$\sum_{L \in \mathcal{R}_{\ell+1}} |L\rangle\langle L| \cdot \left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right)_{\mathsf{R}} \tag{10.12}$$

$$= \sum_{L \in \mathcal{R}_\ell} |L \cup \{(x,y)\}\rangle\langle L \cup \{(x,y)\}| \cdot \left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right)_{\mathsf{R}}. \tag{10.13}$$

Therefore, we need to prove that for all $\ell \geq 0$ and $L \in \mathcal{R}_\ell$ that

$$\langle L \cup \{(x,y)\}| \cdot \left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right) = \sqrt{\mathsf{num}(L,(x,y))} \cdot \langle L|. \tag{10.14}$$

To see this, note that $\langle L \cup \{(x,y)\}|$ is a superposition over all permutations of the elements of $L \cup \{(x,y)\}$, and thus when we right multiply by $\left(\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi_\ell\right)$, the resulting state is proportional to $\langle L|$. To compute the proportionality constant, note that a

$$\frac{\binom{\ell-1}{\mathsf{num}(L,(x,y))-1}}{\binom{\ell}{\mathsf{num}(L,(x,y))}} = \frac{\mathsf{num}(L,(x,y))}{\ell} \tag{10.15}$$

fraction of the permutations of the elements of $L \cup \{(x,y)\}$ will have (x,y) in the left-most slot. Thus,

$$\langle L \cup \{(x,y)\}| \cdot \left(|x,y\rangle \otimes \Pi_\ell\right) = \frac{\sqrt{\mathsf{num}(L,(x,y))}}{\sqrt{\ell+1}} \cdot \langle L|, \tag{10.16}$$

which gives Eq. (10.14) when we multiply by $\sqrt{\ell+1}$. □

We can use Claim 21 to prove exact unitary invariance of E^L and E^R (Claim 20).

Proof of Claim 20. To prove Eq. (10.6), it suffices to prove that

$$D_{\mathsf{A}} \cdot E^L_{\mathsf{ALR}} \cdot C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}} = Q[C,D]_{\mathsf{LR}} \cdot E^L_{\mathsf{ALR}}. \tag{10.17}$$

Recall that

$$Q[C,D]_{\mathsf{LR}} = (C \otimes D^T)^{\otimes *}_{\mathsf{L}} \otimes (\overline{C} \otimes D^\dagger)^{\otimes *}_{\mathsf{R}}. \tag{10.18}$$

Expanding the left-hand-side using the definition of $Q[C,D]$ and the expression for E given by Claim 21, we have

$$\begin{aligned}
&D_{\mathsf{A}} \cdot E^L_{\mathsf{ALR}} \cdot C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}} && (10.19)\\
&= \frac{1}{\sqrt{N}} \sum_{x,y\in[N]} D_{\mathsf{A}} \cdot |y\rangle\langle x|_{\mathsf{A}} \cdot C_{\mathsf{A}} \otimes \sum_{\ell\geq 0} \Pi^{\mathcal{R}}_{\ell+1,\mathsf{L}} \cdot (\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}}) \cdot (C \otimes D^T)^{\otimes \ell}_{\mathsf{L}} && (10.20)\\
&\quad \otimes \Pi^{\mathcal{R}}_{\mathsf{R}} \cdot (\overline{C} \otimes D^\dagger)^{\otimes *}_{\mathsf{R}} && (10.21)\\
&= \frac{1}{\sqrt{N}} \sum_{x,y\in[N]} |y\rangle\langle x|_{\mathsf{A}} \otimes \sum_{\ell\geq 0} \Pi^{\mathcal{R}}_{\ell+1,\mathsf{L}} \cdot (C \otimes D^T)^{\otimes \ell+1}_{\mathsf{L}} \cdot (\sqrt{\ell+1} \cdot |x,y\rangle \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}}) && (10.22)\\
&\quad \otimes (\overline{C} \otimes D^\dagger)^{\otimes *}_{\mathsf{R}} \cdot \Pi^{\mathcal{R}}_{\mathsf{R}} && (10.23)\\
&= Q[C,D]_{\mathsf{LR}} \cdot E^L_{\mathsf{ALR}} && (10.24)
\end{aligned}$$

A similar argument works for E^R_{ALR} to establish Eq. (10.7). □

10.2 Approximate unitary invariance of V^L and V^R

We now prove approximate unitary invariance of the operators V^L and V^R. The key step is the following lemma, which relates these operators to E^L and E^R.

Recall that for an operator M acting on registers L, R, the notation $M_{\leq t} = M \cdot \Pi_{\leq t,\mathsf{LR}}$ refers to the restriction of the operator M to states where the combined length of the L and R components is at most t.

Claim 22. *For any positive integer t,*

$$\left\|V^L_{\leq t} - E^L_{\leq t}\right\|_{\mathrm{op}} \leq \sqrt{\frac{2t(t+1)}{N}} \quad \textit{and} \quad \left\|V^R_{\leq t} - E^R_{\leq t}\right\|_{\mathrm{op}} \leq \sqrt{\frac{2t(t+1)}{N}}. \tag{10.25}$$

Proof. We will only prove this for $V^L_{\leq t}$, as the proof for $V^R_{\leq t}$ is analogous. Let $|\psi\rangle_{\mathsf{ALR}}$ be an arbitrary unit-norm state in the image of $\mathsf{Id}_{\mathsf{A}} \otimes \Pi_{\leq t,\mathsf{LR}}$. In particular,

$$|\psi\rangle_{\mathsf{ALR}} = \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \alpha_{x,L,R} \, |x\rangle_{\mathsf{A}} \, |L\rangle_{\mathsf{L}} \, |R\rangle_{\mathsf{R}}. \tag{10.26}$$

where $\alpha_{x,L,R}$ is zero whenever $|L \cup R| > t$. It suffices to show that for any such $|\psi\rangle$,

$$\left\|V^L |\psi\rangle - E^L_{\mathsf{ALR}} |\psi\rangle\right\|_{\mathrm{op}} \leq \sqrt{\frac{2t(t+1)}{N}}. \tag{10.27}$$

Expanding out $V^L |\psi\rangle$, we get

$$V^L |\psi\rangle = \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \frac{\alpha_{x,L,R}}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} \sum_{\substack{y\in[N]:\\ y\notin\mathrm{Im}(L\cup R)}} |y\rangle\ |L\cup\{(x,y)\}\rangle\ |R\rangle\,. \tag{10.28}$$

Expanding out $E^L_{\mathsf{ALR}} |\psi\rangle_{\mathsf{ALR}}$, we get

$$E^L_{\mathsf{ALR}} |\psi\rangle = \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \frac{\alpha_{x,L,R}}{\sqrt{N}} \sum_{y\in[N]} |y\rangle \sqrt{\mathsf{num}(L,(x,y))+1}\cdot\ |L\cup\{(x,y)\}\rangle\ |R\rangle \tag{10.29}$$

Then we have

$$V^L_{\mathsf{ALR}} |\psi\rangle - E^L_{\mathsf{ALR}} |\psi\rangle \tag{10.30}$$

$$= \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \alpha_{x,L,R} \sum_{y\in[N]} |y\rangle\ |L\cup\{(x,y)\}\rangle\ |R\rangle \left(\frac{\delta_{y\notin\mathrm{Im}(L\cup R)}}{\sqrt{N-|L\cup R|}} - \frac{\sqrt{\mathsf{num}(L,(x,y))+1}}{\sqrt{N}}\right) \tag{10.31}$$

$$= \underbrace{\sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \alpha_{x,L,R} \sum_{\substack{y\in[N]:\\ y\notin\mathrm{Im}(L\cup R)}} |y\rangle\ |L\cup\{(x,y)\}\rangle\ |R\rangle \left(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}}\right)}_{:=|v\rangle}$$

$$+ \underbrace{\sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} \alpha_{x,L,R} \sum_{y\in\mathrm{Im}(L\cup R)} |y\rangle\ |L\cup\{(x,y)\}\rangle\ |R\rangle \left(-\frac{\sqrt{\mathsf{num}(L,(x,y))+1}}{\sqrt{N}}\right)}_{:=|w\rangle}. \tag{10.32}$$

Note that $|v\rangle$ and $|w\rangle$ are orthogonal, since $|v\rangle$ is a superposition of states $|y\rangle\ |L'\rangle\ |R\rangle$ where y is in $\mathrm{Im}(L'\cup R)$ exactly once, while $|w\rangle$ is a superposition of states $|y\rangle\ |L'\rangle\ |R\rangle$ where y is in $\mathrm{Im}(L'\cup R)$ at least twice. Thus,

$$\left\| V^L_{\mathsf{ALR}} |\psi\rangle - E^L_{\mathsf{ALR}} |\psi\rangle \right\|^2 = \langle v|v\rangle + \langle w|w\rangle \tag{10.33}$$

Bounding $\langle v|v\rangle$. By changing the order of summation, we can rewrite $|v\rangle$ as

$$|v\rangle = \sum_{\substack{y\in[N],\\(L',R)\in\mathcal{R}^2}} |y\rangle\ |L'\rangle\ |R\rangle \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R)}} \alpha_{x,L,R}\Big(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}}\Big)\right), \tag{10.34}$$

and thus

$$\langle v|v\rangle = \sum_{\substack{y\in[N],\\(L',R)\in\mathcal{R}^2}} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R)}} \alpha_{x,L,R}\Big(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}}\Big)\right)^2 \tag{10.35}$$

$$\leq \sum_{\substack{y\in[N],\\(L',R)\in\mathcal{R}^2}} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R)}} |\alpha_{x,L,R}|^2 \right) \cdot \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R)}} \Big(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}}\Big)^2 \right), \tag{10.36}$$

where the last inequality is by Cauchy-Schwarz. We can bound the summand by writing

$$\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin \mathrm{Im}(L\cup R)}} \Big(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}}-\frac{1}{\sqrt{N}}\Big)^2 = \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin \mathrm{Im}(L\cup R)}} \Big(\frac{\sqrt{N}-\sqrt{N-|\mathrm{Im}(L\cup R)|}}{\sqrt{N(N-|\mathrm{Im}(L\cup R)|)}}\Big)^2 \tag{10.37}$$

$$\leq \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin \mathrm{Im}(L\cup R)}} \Big(\frac{\sqrt{|\mathrm{Im}(L\cup R)|}}{\sqrt{N(N-|\mathrm{Im}(L\cup R)|)}}\Big)^2$$

(since $\sqrt{a}-\sqrt{b}\leq\sqrt{a-b}$ when $a\geq b\geq 0$)

$$= \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin \mathrm{Im}(L\cup R)}} \frac{|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)} \tag{10.38}$$

$$\leq \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)} \tag{10.39}$$

where the last inequality uses the fact that for any fixed L', there are at most $|L|+1$ choices of (x,L) that can satisfy $L'=L\cup\{(x,y)\}$. Thus,

$$\langle v|v\rangle \leq \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)}\cdot \sum_{\substack{y\in[N],\\ (L',R)\in\mathcal{R}^2}} \Bigg(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin \mathrm{Im}(L\cup R)}} |\alpha_{x,L,R}|^2\Bigg) \tag{10.40}$$

$$= \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)}\cdot \sum_{\substack{x\in[N],\\ (L,R)\in\mathcal{R}^2}} |\alpha_{x,L,R}|^2\cdot\Big(\sum_{y\in[N]}\delta_{y\notin \mathrm{Im}(L\cup R)}\Big) \tag{10.41}$$

$$\leq \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N}\cdot \sum_{\substack{x\in[N],\\ (L,R)\in\mathcal{R}^2}} |\alpha_{x,L,R}|^2 = \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N}. \tag{10.42}$$

Bounding $\langle w|w\rangle$. By changing the order of summation, we can rewrite $|w\rangle$ as

$$|w\rangle = \sum_{\substack{y\in[N],\\ (L',R)\in\mathcal{R}^2}} |y\rangle\ |L'\rangle\ |R\rangle\Bigg(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in \mathrm{Im}(L\cup R)}} \alpha_{x,L,R}\Big(-\frac{\sqrt{\mathsf{num}(L,(x,y))+1}}{\sqrt{N}}\Big)\Bigg). \tag{10.43}$$

Thus,

$$\langle w|w\rangle = \sum_{\substack{y\in[N],\\ (L',R)\in\mathcal{R}^2}} \Bigg|\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in \mathrm{Im}(L\cup R)}} \alpha_{x,L,R}\Big(-\frac{\sqrt{\mathsf{num}(L,(x,y))+1}}{\sqrt{N}}\Big)\Bigg|^2 \tag{10.44}$$

$$\leq \sum_{\substack{y\in[N],\\ (L',R)\in\mathcal{R}^2}} \Bigg(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in \mathrm{Im}(L\cup R)}} |\alpha_{x,L,R}|^2\Bigg)\cdot\Bigg(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in \mathrm{Im}(L\cup R)}} \frac{\mathsf{num}(L,(x,y))+1}{N}\Bigg)$$

(by Cauchy-Schwarz)

$$\leq \sum_{\substack{y\in[N],\\(L',R)\in\mathcal{R}^2}} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in\mathrm{Im}(L\cup R)}} |\alpha_{x,L,R}|^2 \right) \cdot \frac{(|L|+1)}{N}, \tag{10.45}$$

where we have used the fact that for any y, L', we have the upper bound

$$\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in\mathrm{Im}(L\cup R)}} \mathsf{num}(L,(x,y)) + 1 \leq |L|+1, \tag{10.46}$$

since each tuple in L' increases the value of $\mathsf{num}(L,(x,y))$ by 1 for at most one x. Thus,

$$\langle w|w\rangle = \frac{|L|+1}{N} \cdot \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} |\alpha_{x,L,R}|^2 \cdot \Big(\sum_{y\in[N]} \delta_{y\in\mathrm{Im}(L\cup R)} \Big) \tag{10.47}$$

$$\leq \frac{(|L|+1)\cdot|\,\mathrm{Im}(L\cup R)|}{N} \cdot \sum_{\substack{x\in[N],\\(L,R)\in\mathcal{R}^2}} |\alpha_{x,L,R}|^2 = \frac{(|L|+1)\cdot|\,\mathrm{Im}(L\cup R)|}{N}. \tag{10.48}$$

Putting everything together, we have that for all $|\psi\rangle_{\mathsf{ALR}}$ in the image of $\mathsf{Id}_{\mathsf{A}}\Pi_{\leq t,\mathsf{LR}}$,

$$\left\| V^L_{\mathsf{ALR}} |\psi\rangle - E^L_{\mathsf{ALR}} |\psi\rangle \right\| \leq \sqrt{\frac{2(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N}} \leq \sqrt{\frac{2t(t+1)}{N}}, \tag{10.49}$$

since $|\mathrm{Im}(L\cup R)| \leq t$ and $|L|+1 \leq t+1$. This completes the claim. □

Claim 23. *For any positive integer t, and any pair of n-qubit unitaries C, D, we have*

$$\left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_{\mathrm{op}} \leq 2 \cdot \sqrt{\frac{2t(t+1)}{N}} \tag{10.50}$$

$$\left\| D_{\mathsf{A}} \cdot V^{R,\dagger}_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^{R,\dagger}_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_{\mathrm{op}} \leq 2 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.51}$$

Proof. We first prove Eq. (10.50). Using Claim 20 together and the triangle inequality, we have

$$\left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_{\mathrm{op}} \tag{10.52}$$

$$\leq \left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} - D_{\mathsf{A}} \cdot E^L_{\leq t} \cdot C_{\mathsf{A}} \right\|_{\mathrm{op}} + \left\| Q[C,D]_{\mathsf{LR}} \cdot E^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^\dagger_{\mathsf{LR}} \right\|_{\mathrm{op}} \tag{10.53}$$

$$\leq 2 \cdot \left\| V^L_{\leq t} - E^L_{\leq t} \right\|_{\mathrm{op}} \qquad \text{(by unitary invariance of } \|\cdot\|_{\mathrm{op}}\text{)}$$

$$\leq 2 \cdot \sqrt{\frac{2t(t+1)}{N}}. \qquad \text{(by Claim 22)}$$

Eq. (10.51) follows from a symmetric argument. □

Note that with our convention that $M_{\leq t} = M \cdot \Pi_{\leq t}$, the operator $M^\dagger_{\leq t} = (M\cdot\Pi_{\leq t})^\dagger = \Pi_{\leq t}\cdot M^\dagger$ is not the same as $(M^\dagger)_{\leq t} = M^\dagger \cdot \Pi_{\leq t}$. However, since our V^L and V^R operators map $\Pi_{\leq t}$ to $\Pi_{\leq t+1}$, we have the following identities,

$$(V^{L,\dagger})_{\leq t} = V^{L,\dagger}\cdot\Pi_{\leq t} = \Pi_{\leq t-1}\cdot V^{L,\dagger} = V^{L,\dagger}_{\leq t-1} \tag{10.54}$$

$$(V^{R,\dagger})_{\le t} = V^{R,\dagger} \cdot \Pi_{\le t} = \Pi_{\le t-1} \cdot V^{R,\dagger} = V^{R,\dagger}_{\le t-1}. \tag{10.55}$$

As a consequence, Eq. (10.51) also holds for the "mis-parenthesized" version. In particular, for any positive integer t and any C, D, we have

$$\left\| D_{\mathsf{A}} \cdot (V^{R,\dagger})_{\le t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{R,\dagger})_{\le t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\mathrm{op}} \le 2 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.56}$$

To prove the approximate unitary invariance of V, we need to utilize the following basic lemma.

Lemma 10.2. *Given any operators A, B, A', B' with operator norm bounded above by one, we have*

$$\left\| A \cdot B - A' \cdot B' \right\|_{\mathrm{op}} \le \left\| A - A' \right\|_{\mathrm{op}} + \left\| B - B' \right\|_{\mathrm{op}}. \tag{10.57}$$

Proof. We can prove this lemma via triangle inequality,

$$\begin{aligned} \left\| A \cdot B - A' \cdot B' \right\|_{\mathrm{op}} &\le \left\| A \cdot B - A' \cdot B \right\|_{\mathrm{op}} + \left\| A' \cdot B - A' \cdot B' \right\|_{\mathrm{op}} && (10.58)\\ &\le \left\| A - A' \right\|_{\mathrm{op}} \cdot \|B\|_{\mathrm{op}} + \left\| A' \right\|_{\mathrm{op}} \cdot \left\| B - B' \right\|_{\mathrm{op}} && (10.59)\\ &\le \left\| A - A' \right\|_{\mathrm{op}} + \left\| B - B' \right\|_{\mathrm{op}}. && (10.60) \end{aligned}$$

This completes the proof. □

We start by proving the approximate unitary invariance for the projectors $V^L \cdot V^{L,\dagger}$ and $V^R \cdot V^{R,\dagger}$.

Claim 24. *For any positive integer t, and any pair of n-qubit unitaries C, D, we have*

$$\left\| D_{\mathsf{A}} \cdot \left(V^L \cdot V^{L,\dagger} \right)_{\le t} \cdot D^{\dagger}_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot \left(V^L \cdot V^{L,\dagger} \right)_{\le t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\mathrm{op}} \le 4 \cdot \sqrt{\frac{2t(t+1)}{N}} \tag{10.61}$$

$$\left\| C^{\dagger}_{\mathsf{A}} \cdot \left(V^R \cdot V^{R,\dagger} \right)_{\le t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot \left(V^R \cdot V^{R,\dagger} \right)_{\le t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\mathrm{op}} \le 4 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.62}$$

Proof. By the definition of V^L, we have $(V^L \cdot V^{L,\dagger})_{\le t} = V^L_{\le t-1} \cdot V^{L,\dagger}_{\le t-1}$. We have

$$\begin{aligned} &\left\| D_{\mathsf{A}} \cdot V^L_{\le t-1} \cdot V^{L,\dagger}_{\le t-1} \cdot D^{\dagger}_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\le t-1} \cdot V^{L,\dagger}_{\le t-1} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\mathrm{op}} && (10.63)\\ &= \Bigg\| \left(D_{\mathsf{A}} \cdot V^L_{\le t-1} \cdot C_{\mathsf{A}} \right) \cdot \left(C^{\dagger}_{\mathsf{A}} \cdot V^{L,\dagger}_{\le t-1} \cdot D^{\dagger}_{\mathsf{A}} \right)\\ &\quad - \left(Q[C,D]_{\mathsf{LR}} \cdot V^L_{\le t-1} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right) \cdot \left(Q[C,D]_{\mathsf{LR}} \cdot V^{L,\dagger}_{\le t-1} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right) \Bigg\|_{\mathrm{op}} && (10.64)\\ &\le \left\| \left(D_{\mathsf{A}} \cdot V^L_{\le t-1} \cdot C_{\mathsf{A}} \right) - \left(Q[C,D]_{\mathsf{LR}} \cdot V^L_{\le t-1} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right) \right\|_{\mathrm{op}}\\ &\quad + \left\| \left(C^{\dagger}_{\mathsf{A}} \cdot V^{L,\dagger}_{\le t-1} \cdot D^{\dagger}_{\mathsf{A}} \right) - \left(Q[C,D]_{\mathsf{LR}} \cdot V^{L,\dagger}_{\le t-1} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right) \right\|_{\mathrm{op}} && \text{(by Lemma 10.2)}\\ &\le 4 \cdot \sqrt{\frac{2t(t+1)}{N}} && \text{(by Claim 23)} \end{aligned}$$

The statement for V^R can be proven similarly. This concludes the proof of this claim. □

We can now prove approximate invariance of V (Claim 16). By unitary invariance of $\|\cdot\|_{\text{op}}$ we can restate lemma Claim 16 as follows.

Lemma 10.3 (Claim 16, restated)**.** *For any positive integer t, and any pair of n-qubit unitaries C, D, we have*

$$\left\| D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{10.65}$$

$$\left\| C^{\dagger}_{\mathsf{A}} \cdot (V^{\dagger})_{\leq t} \cdot D^{\dagger}_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \leq 16\sqrt{\frac{2t(t+1)}{N}}, \tag{10.66}$$

Proof. We will prove the first inequality, as the second follows from a symmetric argument. From the definition of V, we have

$$V = V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) + (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}. \tag{10.67}$$

From the definitions of $\Pi_{\leq t}$, V^L, and V^R, we note that

$$(V^L \cdot V^R \cdot V^{R,\dagger})_{\leq t} = V^L_{\leq t} \cdot (V^R \cdot V^{R,\dagger})_{\leq t}, \tag{10.68}$$

$$(V^L \cdot V^{L,\dagger} \cdot V^{R,\dagger})_{\leq t} = (V^L \cdot V^{L,\dagger})_{\leq t} \cdot (V^{R,\dagger})_{\leq t}. \tag{10.69}$$

Using this fact and the definition of V, we can apply the triangle inequality to obtain,

$$\left\| D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \tag{10.70}$$

$$\leq \left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \tag{10.71}$$

$$+ \left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \tag{10.72}$$

$$+ \left\| D_{\mathsf{A}} \cdot (V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{R,\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \tag{10.73}$$

$$+ \left\| D_{\mathsf{A}} \cdot (V^L \cdot V^{L,\dagger})_{\leq t} \cdot (V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot (V^L \cdot V^{L,\dagger})_{\leq t} \cdot (V^{R,\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}}. \tag{10.74}$$

We now bound each of the four terms. The first term Eq. (10.71) is bounded above by $2 \cdot \sqrt{\frac{2t(t+1)}{N}}$ from Eq. (10.50). The third term Eq. (10.73) is also bounded above by $2 \cdot \sqrt{\frac{2t(t+1)}{N}}$ from Eq. (10.56). The second and fourth terms Eq. (10.72), Eq. (10.74) require the use of Lemma 10.2. Hence, we can bound the second term Eq. (10.72) as follows,

$$\left\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \right\|_{\text{op}} \tag{10.75}$$

$$= \Big\| D_{\mathsf{A}} \cdot V^L_{\leq t} \cdot C_{\mathsf{A}} \cdot C^{\dagger}_{\mathsf{A}} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}}$$

$$- Q[C,D]_{\mathsf{LR}} \cdot V^L_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \cdot Q[C,D]_{\mathsf{LR}} \cdot (V^R \cdot V^{R,\dagger})_{\leq t} \cdot Q[C,D]^{\dagger}_{\mathsf{LR}} \Big\|_{\text{op}} \tag{10.76}$$

$$\leq \left\| D_{\mathsf{A}} \cdot V_{\leq t}^{L} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t}^{L} \cdot Q[C,D]_{\mathsf{LR}}^{\dagger} \right\|_{\mathrm{op}} \tag{10.77}$$

$$+ \left\| C_{\mathsf{A}}^{\dagger} \cdot (V^{R} \cdot V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot (V^{R} \cdot V^{R,\dagger})_{\leq t} \cdot Q[C,D]_{\mathsf{LR}}^{\dagger} \right\|_{\mathrm{op}}, \tag{10.78}$$

$$\leq 6 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.79}$$

where we used the fact that Eq. (10.77) is bounded above by $2 \cdot \sqrt{\frac{2t(t+1)}{N}}$ from Eq. (10.50) and Eq. (10.78) is bounded above by $4 \cdot \sqrt{\frac{2t(t+1)}{N}}$ from Eq. (10.62). Similarly, we can bound the fourth term given Eq. (10.74) using the same argument to obtain

$$\left\| D_{\mathsf{A}} \cdot V_{\leq t}^{L} \cdot (V^{R} \cdot V^{R,\dagger})_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t}^{L} \cdot (V^{R} \cdot V^{R,\dagger})_{\leq t} \cdot Q[C,D]_{\mathsf{LR}}^{\dagger} \right\|_{\mathrm{op}} \leq 6 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.80}$$

Combining the bounds on the four terms, we obtain

$$\left\| D_{\mathsf{A}} \cdot V_{\leq t} \cdot C_{\mathsf{A}} - Q[C,D]_{\mathsf{LR}} \cdot V_{\leq t} \cdot Q[C,D]_{\mathsf{LR}}^{\dagger} \right\|_{\mathrm{op}} \leq 16 \cdot \sqrt{\frac{2t(t+1)}{N}}. \tag{10.81}$$

This completes the proof of the approximate unitary invariance of V. □

11 Proof of Lemma 9.2

In this section, we prove Lemma 9.2. For convenience, we restate the lemma below.

Lemma 11.1 (Lemma 9.2, restated)**.** *For any unitary 2-design $\mathfrak{D}$ and integer $0 \leq t \leq N-1$, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^{\dagger} \cdot \left(\Pi_{\leq t,\mathsf{LR}}^{\mathsf{bij}} - \Pi_{\leq t,\mathsf{ALR}}^{\mathcal{D}(W)} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \leq 6t\sqrt{\frac{t}{N}}, \tag{11.1}$$

$$\left\| \mathop{\mathbb{E}}_{C,D \leftarrow \mathfrak{D}} (D_{\mathsf{A}}^{\dagger} \otimes Q[C,D]_{\mathsf{LR}})^{\dagger} \cdot \left(\Pi_{\leq t,\mathsf{LR}}^{\mathsf{bij}} - \Pi_{\leq t,\mathsf{ALR}}^{\mathcal{I}(W)} \right) \cdot (D_{\mathsf{A}}^{\dagger} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \leq 6t\sqrt{\frac{t}{N}}, \tag{11.2}$$

In the above expressions, $\Pi_{\leq t,\mathsf{LR}}^{\mathsf{bij}}$ is shorthand for $\mathsf{Id}_{\mathsf{A}} \otimes \Pi_{\leq t,\mathsf{LR}}^{\mathsf{bij}}$, and thus the operators inside the $\|\cdot\|_{\mathrm{op}}$ act on $\mathsf{A}, \mathsf{L}, \mathsf{R}$.

11.1 The domain and image of W

In order to prove Lemma 11.1, we will first need to give an explicit characterization of the projectors $\Pi^{\mathcal{D}(W)}$ and $\Pi^{\mathcal{I}(W)}$.

Definition 39. *Let*

$$\Pi^{\notin \mathrm{Dom}} := \sum_{\substack{(L,R) \in \mathcal{R}^2, \\ x \notin \mathrm{Dom}(L \cup R)}} |x\rangle\langle x|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}} \tag{11.3}$$

$$\Pi^{\notin \mathrm{Im}} := \sum_{\substack{(L,R) \in \mathcal{R}^2, \\ y \notin \mathrm{Im}(L \cup R)}} |y\rangle\langle y|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{L}} \otimes |R\rangle\langle R|_{\mathsf{R}}. \tag{11.4}$$

Definition 40. *Let*

$$\Pi^{\mathsf{EPR}} \coloneqq |\mathsf{EPR}_N\rangle\langle\mathsf{EPR}_N| = \Big(\frac{1}{\sqrt{N}}\sum_{x\in[N]}|x\rangle\,|x\rangle\Big)\cdot\Big(\frac{1}{\sqrt{N}}\sum_{y\in[N]}\langle y|\,\langle y|\Big). \tag{11.5}$$

Notation 13. *We use the notation* $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$ *for the projector on registers* $\mathsf{A},\mathsf{R}^{(r)}$ *that applies* Π^{EPR} *to the registers* A, $\mathsf{R}^{(r)}_{\mathsf{X},i}$ *(where* $i\in[r]$*), and acts as identity on the rest of* $\mathsf{R}^{(r)}$*. The same notation applies for* $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}}$*.*

Fact 12. *The projectors* $\Pi^{\mathcal{R}^2}_{\mathsf{LR}}$ *and* $\Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}}$ *commute, and moreover*

$$\Pi^{\mathsf{bij}}_{\mathsf{LR}} = \Pi^{\mathcal{R}^2}_{\mathsf{LR}}\cdot\Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \tag{11.6}$$

Claim 25.

$$\Pi^{\mathcal{D}(W)} = \Pi^{\mathsf{bij}}_{\mathsf{LR}}\cdot\left(\Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}} + \sum_{\substack{\ell,r\geq 0:\\ \ell+r<N}}\frac{N}{N-\ell-r}\Pi_{\ell,\mathsf{L}}\otimes\sum_{i\in[r+1]}\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right)\cdot\Pi^{\mathsf{bij}}_{\mathsf{LR}} \tag{11.7}$$

$$\Pi^{\mathcal{I}(W)} = \Pi^{\mathsf{bij}}_{\mathsf{LR}}\cdot\left(\Pi^{\notin\mathrm{Im}}_{\mathsf{ALR}} + \sum_{\substack{\ell,r\geq 0:\\ \ell+r<N}}\frac{N}{N-\ell-r}\Pi_{r,\mathsf{R}}\otimes\sum_{i\in[\ell+1]}\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell+1)}_{\mathsf{Y},i}}\right)\cdot\Pi^{\mathsf{bij}}_{\mathsf{LR}} \tag{11.8}$$

Proof. By Fact 8,

$$\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{D}(W^L)} + \Pi^{\mathcal{I}(W^R)}. \tag{11.9}$$

To prove Eq. (11.7), it suffices to prove

$$\Pi^{\mathcal{D}(W^L)} = \Pi^{\mathsf{bij}}_{\mathsf{LR}}\cdot\Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}}\cdot\Pi^{\mathsf{bij}}_{\mathsf{LR}} \tag{11.10}$$

$$\Pi^{\mathcal{I}(W^R)} = \Pi^{\mathsf{bij}}_{\mathsf{LR}}\cdot\left(\sum_{\substack{\ell,r\geq 0:\\ \ell+r<N}}\frac{N}{N-\ell-r}\Pi_{\ell,\mathsf{L}}\otimes\sum_{i\in[r+1]}\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right)\cdot\Pi^{\mathsf{bij}}_{\mathsf{LR}} \tag{11.11}$$

Proof of Eq. (11.10). From the definition of W^L, its domain is the image of the projector

$$\Pi^{\mathcal{D}(W^L)} = \sum_{\substack{(L,R)\in\mathcal{R}^{2,\mathrm{dist}},\\ x\notin\mathrm{Dom}(L,R)}}|x\rangle\langle x|_{\mathsf{A}}\otimes|L\rangle\langle L|_{\mathsf{L}}\otimes|R\rangle\langle R|_{\mathsf{R}} \tag{11.12}$$

$$= \left(\sum_{(L,R)\in\mathcal{R}^{2,\mathrm{dist}}}|L\rangle\langle L|_{\mathsf{L}}\otimes|R\rangle\langle R|_{\mathsf{R}}\right)\cdot\left(\sum_{\substack{(L,R)\in\mathcal{R}^{2},\\ x\notin\mathrm{Dom}(L\cup R)}}|x\rangle\langle x|_{\mathsf{A}}\otimes|L\rangle\langle L|_{\mathsf{L}}\otimes|R\rangle\langle R|_{\mathsf{R}}\right)$$
$$\cdot\left(\sum_{(L,R)\in\mathcal{R}^{2,\mathrm{dist}}}|L\rangle\langle L|_{\mathsf{L}}\otimes|R\rangle\langle R|_{\mathsf{R}}\right) \tag{11.13}$$

$$= \Pi^{\mathsf{bij}}_{\mathsf{LR}}\cdot\Pi^{\notin\mathrm{Dom}}_{\mathsf{ALR}}\cdot\Pi^{\mathsf{bij}}_{\mathsf{LR}}. \tag{11.14}$$

Proof of Eq. (11.11). We can expand out

$$\Pi^{\mathcal{I}(W^R)} = W^R \cdot W^{R,\dagger} = W^R \cdot \sum_{\substack{\ell,r\geq 0,\\ \ell+r<N}} \Pi_{\ell,r,\mathsf{LR}} \cdot W^{R,\dagger} \tag{11.15}$$

$$= \sum_{\substack{\ell,r\geq 0,\\ \ell+r<N}} W^R_{\ell,r} \cdot W^{R,\dagger}_{\ell,r} \tag{11.16}$$

where the second equality uses the fact that the domain of W^R is contained in the image of the projector $\sum_{\ell,r\geq 0,\ell+r<N} \Pi_{\ell,r,\mathsf{LR}}$, i.e., W^R is only defined on states where the L and R registers have sizes $\ell, r \geq 0$ where $\ell + r < N$. Thus, it suffices to prove that for all $\ell, r \geq 0$ such that $\ell + r < N$ that

$$W^R_{\ell,r} \cdot W^{R,\dagger}_{\ell,r} = \frac{N}{N-\ell-r} \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}} \cdot \left(\Pi_{\ell,\mathsf{L}} \otimes \sum_{i\in[r+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}}, \tag{11.17}$$

where we use our notational convention that for an operator B acting on a variable-length registers L, R, the operator $B_{\ell,r} = B \cdot \Pi_{\ell,r,\mathsf{LR}}$ is the restriction of B to states where the L register is length ℓ and the R register is length r.

We will do this by relating W^R to the E^R operator defined in Definition 37. From the definition of W^R in Definition 22, we immediately have:

$$W^R_{\ell,r} \coloneqq \frac{1}{\sqrt{N-\ell-r}} \sum_{\substack{(L,R)\in\mathcal{R}^{2,\mathrm{dist}},\\ |L|=\ell,|R|=r,\\ x\notin \mathrm{Dom}(L\cup R),\\ y\notin \mathrm{Im}(L\cup R)}} |x\rangle\langle y|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{L}} \otimes |R\cup\{(x,y)\}\rangle\langle R|_{\mathsf{R}} \tag{11.18}$$

Using Eq. (10.4) for E^R, we have

$$E^R_{\ell,r} = \frac{1}{\sqrt{N}} \sum_{\substack{(L,R)\in\mathcal{R}^{2},\\ |L|=\ell,|R|=r,\\ x,y\in[N]}} \sqrt{\mathsf{num}(R,(x,y))+1} \cdot |x\rangle\langle y|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{L}} \otimes |R\cup\{(x,y)\}\rangle\langle R|_{\mathsf{R}} \tag{11.19}$$

By inspection, we can see that

$$W^R_{\ell,r} = \frac{\sqrt{N}}{\sqrt{N-\ell-r}} \cdot \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}} \cdot E^R_{\ell,r}, \tag{11.20}$$

since multiplying by Π_{bij} restricts the sum in Eq. (11.19) to x, y, L, R such that $(L,R) \in \mathcal{R}^{2,\mathrm{dist}}$, $y \notin \mathrm{Im}(L\cup R)$, and and $x \notin \mathrm{Dom}(L\cup R)$, and for all such x, y, L, R, we have $\sqrt{\mathsf{num}(R,(x,y))+1} = 1$. Now, recall from Eq. (10.9) in Claim 21 that $E^R_{\ell,r}$ can be also be written as

$$E^R_{\ell,r} = \frac{1}{\sqrt{N}} \sum_{x,y\in[N]} |x\rangle\langle y|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}} \otimes \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \cdot \left(\sqrt{r+1} \cdot |x,y\rangle \otimes \Pi_r \right)_{\mathsf{R}}. \tag{11.21}$$

And thus, we have the following expression for $E^R_{\ell,r}$

$$E^R_{\ell,r} \cdot E^{R,\dagger}_{\ell,r} \tag{11.22}$$
$$= \left(\frac{1}{\sqrt{N}} \sum_{x,y\in[N]} |x\rangle\langle y|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}} \otimes \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \cdot \left(\sqrt{r+1} \cdot |x,y\rangle \otimes \Pi_r \right)_{\mathsf{R}} \right)$$

$$\cdot \left(\frac{1}{\sqrt{N}} \sum_{x',y' \in [N]} |y'\rangle\langle x'|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}} \otimes \left(\sqrt{r+1} \cdot \langle x', y'| \otimes \Pi_r\right)_{\mathsf{R}} \cdot \Pi^{\mathcal{R}}_{r+1,\mathsf{R}}\right) \tag{11.23}$$

$$= \frac{1}{N} \sum_{x,x' \in [N]} |x\rangle\langle x'|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}} \otimes \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \cdot \left((r+1) \cdot |x\rangle\langle x'|_{\mathsf{R}^{(r+1)}_{\mathsf{X},1}} \otimes \sum_y |y\rangle\langle y|_{\mathsf{R}^{(r+1)}_{\mathsf{Y},1}} \otimes \Pi_r\right)_{\mathsf{R}} \cdot \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \tag{11.24}$$

$$= \frac{1}{N} \sum_{x,x' \in [N]} |x\rangle\langle x'|_{\mathsf{A}} \otimes \Pi^{\mathcal{R}}_{\ell,\mathsf{L}} \otimes \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \cdot \left(\sum_{i \in [r+1]} |x\rangle\langle x'|_{\mathsf{R}^{(r+1)}_{\mathsf{X},i}} \otimes \sum_y |y\rangle\langle y|_{\mathsf{R}^{(r+1)}_{\mathsf{Y},i}} \otimes \Pi_r\right)_{\mathsf{R}} \cdot \Pi^{\mathcal{R}}_{r+1,\mathsf{R}} \tag{11.25}$$

$$= \Pi^{\mathcal{R}^2}_{\ell,r+1,\mathsf{LR}} \cdot \left(\Pi_{\ell,\mathsf{L}} \otimes \sum_{i \in [r+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathcal{R}^2}_{\ell,r+1,\mathsf{LR}}. \tag{11.26}$$

And thus, combining this with Eq. (11.20), we obtain

$$W^R_{\ell,r} \cdot W^{R,\dagger}_{\ell,r} \tag{11.27}$$

$$= \frac{N}{N-\ell-r} \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}} \cdot \left(\Pi^{\mathcal{R}^2}_{\ell,r+1,\mathsf{LR}} \cdot \left(\Pi_{\ell,\mathsf{L}} \otimes \sum_{i \in [r+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathcal{R}^2}_{\ell,r+1,\mathsf{LR}}\right) \cdot \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}} \tag{11.28}$$

$$= \frac{N}{N-\ell-r} \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}} \cdot \left(\Pi_{\ell,\mathsf{L}} \otimes \sum_{i \in [r+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathsf{bij}}_{\ell,r+1,\mathsf{LR}}. \tag{11.29}$$

This concludes the proof. □

Definition 41. *Define*

$$P^{\mathcal{D}(W)}_{\mathsf{ALR}} = \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \cdot \left(\Pi^{\not\in \mathrm{Dom}}_{\mathsf{ALR}} + \sum_{\substack{\ell,r \geq 0: \\ \ell+r<N}} \frac{N}{N-\ell-r} \Pi_{\ell,\mathsf{L}} \otimes \sum_{i \in [r+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r+1)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \tag{11.30}$$

$$P^{\mathcal{I}(W)}_{\mathsf{ALR}} = \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \cdot \left(\Pi^{\not\in \mathrm{Dom}}_{\mathsf{ALR}} + \sum_{\substack{\ell,r \geq 0: \\ \ell+r<N}} \frac{N}{N-\ell-r} \Pi_{r,\mathsf{R}} \otimes \sum_{i \in [\ell+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell+1)}_{\mathsf{Y},i}}\right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \tag{11.31}$$

Combining Claim 25, Definition 41, and Fact 12, we have the following corollary.

Corollary 11.1.

$$\Pi^{\mathcal{D}(W)} = \Pi^{\mathcal{R}^2} \cdot P^{\mathcal{D}(W)} \cdot \Pi^{\mathcal{R}^2} \tag{11.32}$$

$$\Pi^{\mathcal{I}(W)} = \Pi^{\mathcal{R}^2} \cdot P^{\mathcal{I}(W)} \cdot \Pi^{\mathcal{R}^2} \tag{11.33}$$

11.2 An operator upper bound

Claim 26. *For any non-negative integers ℓ, r,*

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}} \preceq \frac{N}{N-\ell-r+1} \left(\sum_{i \in [\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} + \sum_{i \in [r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) + 2r\sqrt{\frac{\ell+r}{N}} \mathsf{Id}_{\mathsf{ALR}}\right) \tag{11.34}$$

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - P^{\mathcal{I}(W)}_{\ell,r,\mathsf{ALR}} \preceq \frac{N}{N-\ell-r+1} \left(\sum_{i \in [r]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{Y},i}} + \sum_{i \in [\ell]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}}\right) + 2\ell\sqrt{\frac{\ell+r}{N}} \mathsf{Id}_{\mathsf{ALR}}\right) \tag{11.35}$$

Proof. We will prove the first inequality, and the second will follow from a symmetric argument. We begin by writing out $P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}}$ as

$$P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}} = \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \cdot \left(\Pi^{\not\in \mathrm{Dom}}_{\mathsf{ALR}} + \sum_{\substack{\ell',r' \geq 0: \\ \ell'+r'<N}} \frac{N}{N-\ell'-r'} \Pi_{\ell',\mathsf{L}} \otimes \sum_{i \in [r'+1]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r'+1)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \cdot \Pi_{\ell,r,\mathsf{LR}} \tag{11.36}$$

$$= \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\not\in \mathrm{Dom}}_{\ell,r,\mathsf{ALR}} + \frac{N}{N-\ell-r+1} \Pi_{\ell,\mathsf{L}} \otimes \sum_{i \in [r]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}, \tag{11.37}$$

where the second equality uses the fact that $\Pi_{\ell,r,\mathsf{LR}}$ commutes with every other projector in the above expression. Note that in the special case where $r = 0$, the above expression simplifies to

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\not\in \mathrm{Dom}}_{\ell,r,\mathsf{ALR}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}. \tag{11.38}$$

Next, we use our expression for $P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}}$ to expand out

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}} = \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi_{\ell,r,\mathsf{LR}} - \Pi^{\not\in \mathrm{Dom}}_{\ell,r,\mathsf{ALR}} - \frac{N}{N-\ell-r+1} \sum_{i \in [r]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}. \tag{11.39}$$

Using the definition of $\Pi^{\not\in \mathrm{Dom}}_{\ell,r}$, we have

$$\Pi_{\ell,r,\mathsf{LR}} - \Pi^{\not\in \mathrm{Dom}}_{\ell,r,\mathsf{ALR}} \preceq \sum_{i \in [\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} + \sum_{i \in [r]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}. \tag{11.40}$$

This inequality holds because any state in the image of $\Pi_{\ell,r,\mathsf{LR}} - \Pi^{\not\in \mathrm{Dom}}$ must have a collision between the A register and at least one of the registers $\{\mathsf{L}^{(\ell)}_{\mathsf{X},i}\}_{i\in[\ell]} \cup \{\mathsf{R}^{(r)}_{\mathsf{X},i}\}_{i\in[r]}$, and will therefore be in the image of at least one of the projectors on the right-hand-side. Plugging this inequality into Eq. (11.39), we have

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - P^{\mathcal{D}(W)}_{\ell,r,\mathsf{ALR}} \tag{11.41}$$

$$\preceq \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\sum_{i \in [\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} + \sum_{i \in [r]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \frac{N}{N-\ell-r+1} \sum_{i \in [r]} \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \tag{11.42}$$

$$\preceq \frac{N}{N-\ell-r+1} \underbrace{\left(\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\sum_{i \in [\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \right)}_{\mathrm{Term}_1}$$

$$+ \frac{N}{N-\ell-r+1} \underbrace{\left(\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\sum_{i \in [r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \right)}_{\mathrm{Term}_2}. \tag{11.43}$$

Comparing (11.43) to the right-hand side of Eq. (11.34), it suffices to prove that:

$$\mathrm{Term}_1 \preceq \sum_{i \in [\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}}, \tag{11.44}$$

$$\mathrm{Term}_2 \preceq \sum_{i \in [r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) + 2r \sqrt{\frac{\ell+r}{N}} \mathsf{Id}_{\mathsf{ALR}}. \tag{11.45}$$

Bounding the first term. To prove Eq. (11.44), it suffices to prove for each $i \in [\ell]$,

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \preceq \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}}. \tag{11.46}$$

This holds because $\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}}$ commutes with $\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ (since both are diagonal in the standard basis) and thus:

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} = \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \preceq \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \cdot \Pi_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} = \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}}. \tag{11.47}$$

Bounding the second term. To prove Eq. (11.45), it suffices to prove for each $i \in [r]$,

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \preceq \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) + 2\sqrt{\frac{\ell+r}{N}}\mathsf{Id}_{\mathsf{ALR}} \tag{11.48}$$

Note that $\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ and $\left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right)$ do not commute, so we cannot simply apply the argument we used to bound the first term. However, these two operators *almost* commute. In particular,

$$\left\|\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) - \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}\right\|_{\mathrm{op}} \leq \sqrt{\frac{\ell+r}{N}}. \tag{11.49}$$

We prove Eq. (11.49) in Claim 27, which follows this proof. To simplify notation for the following steps, let us write $A \coloneqq \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ and $B \coloneqq \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$. Note that B is a projector because $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$ projects onto a subspace of the image of $\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$.

Using the definition of operator norm, we have

$$A \cdot B \cdot A - B \cdot A \cdot B \preceq \|A \cdot B \cdot A - B \cdot A \cdot B\|_{\mathrm{op}} \cdot \mathsf{Id}. \tag{11.50}$$

Adding $B \cdot A \cdot B$ to both sides, we get

$$\begin{aligned} A \cdot B \cdot A &\preceq B \cdot A \cdot B + \|A \cdot B \cdot A - B \cdot A \cdot B\|_{\mathrm{op}} \cdot \mathsf{Id} && (11.51)\\ &\preceq B + \|A \cdot B \cdot A - B \cdot A \cdot B\|_{\mathrm{op}} \cdot \mathsf{Id}, && (11.52) \end{aligned}$$

where the second inequality uses the fact that $B \cdot A \cdot B \preceq B \cdot \mathsf{Id} \cdot B = B$ for projectors A and B. Now,

$$\begin{aligned} \|A \cdot B \cdot A - B \cdot A \cdot B\|_{\mathrm{op}} &\leq \|A \cdot B \cdot A - A \cdot B \cdot A \cdot B\|_{\mathrm{op}} + \|A \cdot B \cdot A \cdot B - B \cdot A \cdot B\|_{\mathrm{op}} \\ &\qquad\qquad \text{(triangle inequality)} \\ &= \|A \cdot B \cdot (B \cdot A - A \cdot B)\|_{\mathrm{op}} + \|(A \cdot B - B \cdot A) \cdot A \cdot B\|_{\mathrm{op}} \\ &\qquad\qquad \text{(since } A^2 = A \text{ and } B^2 = B\text{)} \\ &\leq \|A \cdot B\|_{\mathrm{op}} \cdot \|B \cdot A - A \cdot B\|_{\mathrm{op}} + \|A \cdot B - B \cdot A\|_{\mathrm{op}} \cdot \|A \cdot B\|_{\mathrm{op}} && (11.53)\\ &\leq \|B \cdot A - A \cdot B\|_{\mathrm{op}} + \|A \cdot B - B \cdot A\|_{\mathrm{op}} && (11.54)\\ &\leq 2\sqrt{\frac{\ell+r}{N}} && \text{(by Claim 27)} \end{aligned}$$

Plugging this inequality into Eq. (11.52), and plugging in $A = \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ and $B = \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}$ yields Eq. (11.48). This completes the proof. □

We now prove Claim 27, which we used in the previous proof.

Claim 27. *For any integers $\ell, r \geq 0$ such that $\ell + r \leq N$ and any index $i \in [r]$ (if such an i exists[8]), we have*

$$\left\| \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) - \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \right\|_{\mathrm{op}} \leq \sqrt{\frac{\ell + r}{N}}. \tag{11.55}$$

Similarly, for any integers $\ell, r \geq 0$ such that $\ell + r \leq N$, and any index $i \in [\ell]$ (if such an i exists), we have

$$\left\| \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}} \right) - \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{Y},i}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \right\|_{\mathrm{op}} \leq \sqrt{\frac{\ell + r}{N}}. \tag{11.56}$$

Proof. We will prove the first inequality, and the second will follow from a symmetric argument. Assume without loss of generality that $i = 1$. Since $\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ and $\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}}$ commute,

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \right) - \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \right) \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \tag{11.57}$$

$$= \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}}. \tag{11.58}$$

We will write down an explicit expression for the operator $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} - \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}}$, which we will then use to bound the operator norm.

We can expand out $\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$ as

$$\Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}} = \sum_{\substack{(x,x') \in [N]^{\ell+r}_{\mathrm{dist}}, \\ (y,y') \in [N]^{\ell+r}_{\mathrm{dist}}}} |x,y\rangle\langle x,y|_{\mathsf{L}^{(\ell)}} \otimes |x',y'\rangle\langle x',y'|_{\mathsf{R}^{(r)}}, \tag{11.59}$$

where in the above sum, $x, y \in [N]^\ell$, $x', y' \in [N]^r$, and $|x,y\rangle_{\mathsf{L}^{(\ell)}} = |x_1, y_1, \ldots, x_\ell, y_\ell\rangle_{\mathsf{L}^{(\ell)}}$.

We can then expand out

$$(\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \tag{11.60}$$

$$= \left(\sum_{\substack{(x,x') \in [N]^{\ell+r}_{\mathrm{dist}}, \\ (y,y') \in [N]^{\ell+r}_{\mathrm{dist}}}} |x,y\rangle\langle x,y|_{\mathsf{L}^{(\ell)}} \otimes |x',y'\rangle\langle x',y'|_{\mathsf{R}^{(r)}} \right) \cdot \left(\frac{1}{N} \sum_{u,v \in [N]} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} \right) \tag{11.61}$$

$$= \sum_{\substack{(x,x'_{[2,r]}) \in [N]^{\ell+r-1}_{\mathrm{dist}}, \\ (y,y') \in [N]^{\ell+r}_{\mathrm{dist}}}} |x,y\rangle\langle x,y|_{\mathsf{L}^{(\ell)}} \otimes |x'_{[2:r]},y'\rangle\langle x'_{[2:r]},y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},1}} \otimes \frac{1}{N} \sum_{\substack{v \in [N], \\ u \notin \{x, x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}}, \tag{11.62}$$

where $x'_{[2,r]} \in [N]^{r-1}$, the notation $u \notin \{x, x'_{[2,r]}\}$ means u must be distinct from each element of x and $x'_{[2,r]}$, and $\mathsf{R} \setminus \mathsf{R}^{(r)}_{\mathsf{X},1}$ refers to all of the registers $\mathsf{R} = (\mathsf{R}^{(r)}_{\mathsf{X},1}, \mathsf{R}^{(r)}_{\mathsf{Y}_1}, \ldots, \mathsf{R}^{(r)}_{\mathsf{X},r}, \mathsf{R}^{(r)}_{\mathsf{Y}_r})$ *except* for $\mathsf{R}^{(r)}_{\mathsf{X},1}$.

[8] Note that $[r] \coloneqq \{1, 2, \ldots, r\}$, so no i exists when $r = 0$. But in this case, the bound is trivially satisfied.

Next, to get an explicit expression for $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}$, we can just take the conjugate transpose of Eq. (11.62). By exploiting symmetry, we can write the result in such a way that it looks nearly identical to (11.62), except for the part highlighted in red.

$$\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot (\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) \tag{11.63}$$

$$= \sum_{\substack{(x,x'_{[2,r]})\in[N]^{\ell+r-1}_{\mathrm{dist}},\\ (y,y')\in[N]^{\ell+r}_{\mathrm{dist}}}} |x,y\rangle\langle x,y|_{\mathsf{L}^{(\ell)}} \otimes |x'_{[2:r]},y'\rangle\langle x'_{[2:r]},y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},1}} \otimes \frac{1}{N} \sum_{\substack{u\in[N],\\ v\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}}. \tag{11.64}$$

Subtracting (11.62) from (11.64), we get

$$\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot (\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) - (\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \tag{11.65}$$

$$= \sum_{\substack{(x,x'_{[2,r]})\in[N]^{\ell+r-1}_{\mathrm{dist}},\\ (y,y')\in[N]^{\ell+r}_{\mathrm{dist}}}} |x,y\rangle\langle x,y|_{\mathsf{L}^{(\ell)}} \otimes |x'_{[2:r]},y'\rangle\langle x'_{[2:r]},y'|_{\mathsf{R}\setminus\mathsf{R}^{(r)}_{\mathsf{X},1}}$$

$$\otimes \frac{1}{N} \sum_{\substack{u\in[N],\\ v\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} - \frac{1}{N} \sum_{\substack{v\in[N],\\ u\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}}. \tag{11.66}$$

Since this is a block diagonal matrix with blocks indexed by $x, y, x'_{[2:r]}, y'$, the operator norm is

$$\left\| \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \cdot (\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) - (\mathsf{Id}_{\mathsf{A}} \otimes \Pi^{\mathrm{dist}_{X,Y}}_{\ell,r,\mathsf{LR}}) \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},1}} \right\|_{\mathrm{op}} \tag{11.67}$$

$$= \max_{\substack{(x,x'_{[2,r]})\in[N]^{\ell+r-1}_{\mathrm{dist}},\\ (y,y')\in[N]^{\ell+r}_{\mathrm{dist}}}} \left\| \frac{1}{N} \sum_{\substack{u\in[N],\\ v\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} - \frac{1}{N} \sum_{\substack{v\in[N],\\ u\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} \right\|_{\mathrm{op}}. \tag{11.68}$$

Fix any choice of $(x, x'_{[2,r]}) \in [N]^{\ell+r-1}_{\mathrm{dist}}, (y, y') \in [N]^{\ell+r}_{\mathrm{dist}}$. We can rewrite

$$\frac{1}{N} \sum_{\substack{u\in[N],\\ v\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} - \frac{1}{N} \sum_{\substack{v\in[N],\\ u\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} \tag{11.69}$$

$$= \frac{1}{N} \sum_{\substack{u\in\{x,x'_{[2,r]}\},\\ v\notin\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} - \frac{1}{N} \sum_{\substack{u\notin\{x,x'_{[2,r]}\},\\ v\in\{x,x'_{[2,r]}\}}} |u\rangle\langle v|_{\mathsf{A}} \otimes |u\rangle\langle v|_{\mathsf{R}^{(r)}_{\mathsf{X},1}} \tag{11.70}$$

$$= \frac{\sqrt{(N-r-\ell+1)(r+\ell-1)}}{N} \Big(|\phi\rangle\langle\psi| - |\psi\rangle\langle\phi| \Big), \tag{11.71}$$

where $|\psi\rangle$ and $|\phi\rangle$ are the following vectors

$$|\psi\rangle := \frac{1}{\sqrt{N-r-\ell+1}} \sum_{u\notin\{x,x'_{[2,r]}\}} |u\rangle_{\mathsf{A}} \, |u\rangle_{\mathsf{R}^{(r)}_{\mathsf{X},1}}, \tag{11.72}$$

$$|\phi\rangle := \frac{1}{\sqrt{r+\ell-1}} \sum_{u\in\{x,x'_{[2,r]}\}} |u\rangle_{\mathsf{A}} \, |u\rangle_{\mathsf{R}^{(r)}_{\mathsf{X},1}}, \tag{11.73}$$

Note that if $r = 1$ and $\ell = 0$, these vectors have norm 0 and we are done. For all other choices of $r \geq 1$, $\ell \geq 0$ such that $r + \ell \leq N$, these are orthogonal unit vectors, and thus $|\psi\rangle\langle\phi| - |\phi\rangle\langle\psi|$ has operator norm 1. It follows that the overall operator norm is at most

$$\frac{\sqrt{(N-r-\ell+1)(r+\ell-1)}}{N} \leq \sqrt{\frac{\ell+r}{N}}. \tag{11.74}$$

which completes the proof. □

11.3 An intermediate lemma on 2-design twirling

Claim 28 (Twirling)**.** *For any unitary 2-design $\mathfrak{D}$ and any non-negative integers ℓ, r,*

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} + \sum_{i\in[r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}}$$
$$\leq \frac{2\ell + r}{N+1}, \tag{11.75}$$

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[r]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} + \sum_{i\in[\ell]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \right) \right) \cdot (D^\dagger_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}}$$
$$\leq \frac{2r + \ell}{N+1}. \tag{11.76}$$

Before we prove Claim 28, let us recall the following claims that were proven in the preliminaries.

Claim 29 (Claim 1, restated)**.** *For any n-qubit unitary 2-design $\mathfrak{D}$,*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}} \left[(U\otimes U)^\dagger \cdot \Pi^{\mathsf{eq}} \cdot (U \otimes U) \right] = \frac{2}{N+1} \cdot \Pi^{N,2}_{\mathsf{sym}}. \tag{11.77}$$

Claim 30 (Claim 2, restated)**.** *For any n-qubit unitary 2-design $\mathfrak{D}$,*

$$\mathop{\mathbb{E}}_{U\leftarrow\mathfrak{D}} \left[(U\otimes \overline{U})^\dagger \cdot \left(\Pi^{\mathsf{eq}} - \Pi^{\mathsf{EPR}} \right) \cdot (U \otimes \overline{U}) \right] = \frac{1}{N+1} \cdot (\mathsf{Id} - \Pi^{\mathsf{EPR}}). \tag{11.78}$$

Proof of Claim 28. We prove the first inequality, and the proof for the second one is symmetric. By the triangle inequality,

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} + \sum_{i\in[r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \tag{11.79}$$

$$\leq \sum_{i\in[\ell]} \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}}$$
$$+ \sum_{i\in[r]} \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \tag{11.80}$$

Plugging in

$$Q[C,D]_{\mathsf{LR}} = (C \otimes D^T)^{\otimes *}_{\mathsf{L}} \otimes (\overline{C} \otimes D^\dagger)^{\otimes *}_{\mathsf{R}}, \tag{11.81}$$

we can rewrite (11.80) as

$$\begin{aligned}(11.80) &= \sum_{i\in[\ell]} \left\| \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes C_{\mathsf{L}_{\mathsf{X},i}^{(\ell)}})^\dagger \cdot \Pi^{\mathsf{eq}}_{\mathsf{L}_{\mathsf{X},i}^{(\ell)}} \cdot (C_{\mathsf{A}} \otimes C_{\mathsf{A},\mathsf{L}_{\mathsf{X},i}^{(\ell)}}) \right\|_{\mathrm{op}} \\ &\quad + \sum_{i\in[r]} \left\| \mathop{\mathbb{E}}_{C\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes \overline{C}_{\mathsf{R}_{\mathsf{X},i}^{(r)}})^\dagger \cdot \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}_{\mathsf{X},i}^{(r)}} \right) \cdot (C_{\mathsf{A}} \otimes \overline{C}_{\mathsf{R}_{\mathsf{X},i}^{(r)}}) \right\|_{\mathrm{op}} \qquad (11.82) \\ &\le \frac{2\ell}{N+1} + \frac{r}{N+1}. \qquad \text{(by Claims 1 and 2)}\end{aligned}$$

This completes the proof. □

11.4 Finishing the proof of Lemma 9.2

We now prove Lemma 9.2, which we state again for convenience.

Lemma 11.2 (Lemma 9.2, restated)**.** *For any unitary 2-design $\mathfrak{D}$ and integer $0 \le t \le N/2$, we have*

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} - \Pi^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \le 6t\sqrt{\frac{t}{N}}, \qquad (11.83)$$

$$\left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} - \Pi^{\mathcal{I}(W)}_{\le t,\mathsf{ALR}} \right) \cdot (D_{\mathsf{A}}^\dagger \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \le 6t\sqrt{\frac{t}{N}}, \qquad (11.84)$$

Proof. Using Fact 12 and Corollary 11.1, we have

$$\Pi^{\mathsf{bij}}_{\mathsf{LR}} = \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\mathsf{LR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}}, \qquad (11.85)$$

$$\Pi^{\mathcal{D}(W)}_{\mathsf{ALR}} = \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot P^{\mathcal{D}(W)}_{\mathsf{ALR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}}, \qquad (11.86)$$

Since $\Pi^{\mathcal{R}^2}$ commutes with $\Pi_{\le t}$, this implies

$$\Pi^{\mathsf{bij}}_{\le t,\mathsf{LR}} = \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\le t,\mathsf{LR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}}, \qquad (11.87)$$

$$\Pi^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} = \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot P^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}}. \qquad (11.88)$$

Plugging this into the left-hand side of Eq. (11.83), we get

$$= \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot \Pi^{\mathrm{dist}_{X,Y}}_{\le t,\mathsf{LR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}} - \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot P^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} \qquad (11.89)$$

$$= \left\| \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \cdot \left(\mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{dist}_{X,Y}}_{\le t,\mathsf{LR}} - P^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right) \cdot \Pi^{\mathcal{R}^2}_{\mathsf{LR}} \right\|_{\mathrm{op}} \qquad (11.90)$$

$$\le \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi^{\mathrm{dist}_{X,Y}}_{\le t,\mathsf{LR}} - P^{\mathcal{D}(W)}_{\le t,\mathsf{ALR}} \right) \cdot (C_{\mathsf{A}} \otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}}, \qquad (11.91)$$

where the second equality follows from the fact that $\Pi^{\mathcal{R}^2}_{\mathsf{LR}}$ commutes with $Q[C,D]_{\mathsf{LR}}$, and the inequality uses the fact that $\|\Pi \cdot M \cdot \Pi\|_{\mathrm{op}} \le \|M\|_{\mathrm{op}}$ for any projector Π.

Next, we use the fact that the operators $\Pi_{\leq t}^{\mathrm{dist}_{X,Y}}$ and $P_{\leq t,\mathsf{ALR}}^{\mathcal{D}(W)}$ are block diagonal with respect to $\{\Pi_{\ell,r,\mathsf{LR}}\}_{\ell,r\geq 0}$ (recall that $\Pi_{\ell,r}$ denotes the projector that restricts the registers L and R to have lengths ℓ and r, respectively), i.e., they map the image of $\Pi_{\ell,r}$ to the image of $\Pi_{\ell,r}$. Thus,

$$
\begin{aligned}
(11.91) &= \max_{\substack{\ell,r\geq 0:\\ \ell+r\leq t}} \left\| \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}}\otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\Pi_{\ell,r,\mathsf{LR}}^{\mathrm{dist}_{X,Y}} - P_{\ell,r,\mathsf{ALR}}^{\mathcal{D}(W)}\right) \cdot (C_{\mathsf{A}}\otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} && (11.92)\\
&\leq \max_{\substack{\ell,r\geq 0:\\ \ell+r\leq t}} \left\| \frac{N}{N-\ell-r+1} \cdot \mathop{\mathbb{E}}_{C,D\leftarrow\mathfrak{D}} (C_{\mathsf{A}}\otimes Q[C,D]_{\mathsf{LR}})^\dagger \cdot \left(\sum_{i\in[\ell]} \Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{L}^{(\ell)}_{\mathsf{X},i}} \right.\right.\\
&\quad \left.\left. + \sum_{i\in[r]} \left(\Pi^{\mathsf{eq}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}} - \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{R}^{(r)}_{\mathsf{X},i}}\right) + 2r\sqrt{\frac{\ell+r}{N}}\mathsf{Id}_{\mathsf{ALR}} \right) \cdot (C_{\mathsf{A}}\otimes Q[C,D]_{\mathsf{LR}}) \right\|_{\mathrm{op}} && \text{(by Claim 26)}\\
&\leq \max_{\substack{\ell,r\geq 0:\\ \ell+r\leq t}} \frac{N}{N-\ell-r+1} \cdot \left(\frac{2\ell+r}{N+1} + 2r\sqrt{\frac{\ell+r}{N}} \right). && \text{(by Claim 28 and the triangle inequality)}
\end{aligned}
$$

This expression is maximized by setting $r=t$ and $\ell=0$, which yields a final upper bound of

$$
\frac{N}{N-t+1}\cdot\left(\frac{t}{N+1}+2t\sqrt{\frac{t}{N}}\right) \leq \frac{N}{N-t}\cdot\left(3t\sqrt{\frac{t}{N}}\right) \leq 6t\sqrt{\frac{t}{N}} \tag{11.93}
$$

where the last inequality uses the assumption that $t\leq N/2$. □

References

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[AGKL24] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin. Pseudorandom isometries. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 226–254. Springer, 2024.

[AMR20] Gorjan Alagic, Christian Majenz, and Alexander Russell. Efficient simulation of random states and random unitaries. In *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III 39*, pages 759–787. Springer, 2020.

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

[BFNV19] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019.

[BM24] Zvika Brakerski and Nir Magrafta. Real-valued somewhat-pseudorandom unitaries. *arXiv preprint arXiv:2403.16704*, 2024.

[CBB+24] Chi-Fang Chen, Adam Bouland, Fernando GSL Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and spseudorandom unitaries from permutations. *arXiv preprint arXiv:2404.16751*, 2024.

[CGAH+17] Jordan S Cotler, Guy Gur-Ari, Masanori Hanada, Joseph Polchinski, Phil Saad, Stephen H Shenker, Douglas Stanford, Alexandre Streicher, and Masaki Tezuka. Black holes and random matrices. *Journal of High Energy Physics*, 2017(5):1–54, 2017.

[CHJLY17] Jordan Cotler, Nicholas Hunter-Jones, Junyu Liu, and Beni Yoshida. Chaos, complexity, and random matrices. *Journal of High Energy Physics*, 2017(11):1–60, 2017.

[CSM+23] Joonhee Choi, Adam L Shaw, Ivaylo S Madjarov, Xin Xie, Ran Finkelstein, Jacob P Covey, Jordan S Cotler, Daniel K Mark, Hsin-Yuan Huang, Anant Kale, et al. Preparing random states and benchmarking with many-body quantum chaos. *Nature*, 613(7944):468–473, 2023.

[EFH+22] Andreas Elben, Steven T Flammia, Hsin-Yuan Huang, Richard Kueng, John Preskill, Benoît Vermersch, and Peter Zoller. The randomized measurement toolbox. *arXiv preprint arXiv:2203.11374*, 2022.

[EFL+24] Netta Engelhardt, Åsmund Folkestad, Adam Levine, Evita Verheijden, and Lisa Yang. Cryptographic censorship. *arXiv preprint arXiv:2402.03425*, 2024.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM (JACM)*, 33(4):792–807, 1986.

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

[HBK23] Tobias Haug, Kishor Bharti, and Dax Enshan Koh. Pseudorandom unitaries are neither real nor sparse nor noise-robust. *arXiv preprint arXiv:2306.11677*, 2023.

[HKP20] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nat. Phys.*, 16, 2020.

[HKT+22] Hsin-Yuan Huang, Richard Kueng, Giacomo Torlai, Victor V Albert, and John Preskill. Provably efficient machine learning for quantum many-body problems. *Science*, 377(6613):eabk3333, 2022.

[HLSW04] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250:371–391, 2004.

[JLS17] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom states, non-cloning theorems and quantum money. *arXiv preprint arXiv:1711.00385*, 2017.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[KLR+08] Emanuel Knill, Dietrich Leibfried, Rolf Reichle, Joe Britton, R Brad Blakestad, John D Jost, Chris Langer, Roee Ozeri, Signe Seidelin, and David J Wineland. Randomized benchmarking of quantum gates. *Physical Review A—Atomic, Molecular, and Optical Physics*, 77(1):012307, 2008.

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1589–1602, 2023.

[KTP20] Isaac Kim, Eugene Tang, and John Preskill. The ghost in the radiation: Robust encodings of the black hole interior. *Journal of High Energy Physics*, 2020(6):1–65, 2020.

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 979–990, 2024.

[LQS+23] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers. *arXiv preprint arXiv:2309.08941*, 2023.

[Mov23] Ramis Movassagh. The hardness of random quantum circuits. *Nature Physics*, 19(11):1719–1724, 2023.

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. *arXiv preprint arXiv:2404.12647*, 2024.

[NVH18] Adam Nahum, Sagar Vijay, and Jeongwan Haah. Operator spreading in random unitary circuits. *Physical Review X*, 8(2):021014, 2018.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *arXiv preprint arXiv:2407.07754*, 2024.

[YE23] Lisa Yang and Netta Engelhardt. The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems. *arXiv preprint arXiv:2302.11013*, 2023.

[Zha16] Mark Zhandry. A note on quantum-secure prps. *arXiv preprint arXiv:1611.05564*, 2016.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 239–268. Springer, 2019.

[Zha21] Mark Zhandry. How to construct quantum random functions. *Journal of the ACM (JACM)*, 68(5):1–43, 2021.

Part III
Appendices

A Efficient circuit implementation of path-recording oracle

We briefly describe how to efficiently implement the path-recording oracles on a quantum computer to simulate forward and inverse queries of a Haar-random unitary up to inverse-exponential error.

A.1 Implementing relation states

There are multiple ways to implement the relation state $|R\rangle$ for a relation R. We describe one simple approach. We represent $|R\rangle$ using $|R|$ $2n$-qubit registers by sorting the tuples $(x, y) \in [N]^2$ in the relation R. For example, consider R, we can store $|R\rangle$ on a quantum computer as

$$|x_1\rangle\ |y_1\rangle \dots |x_{|R|}\rangle\ |y_{|R|}\rangle\,, \tag{A.1}$$

where $R = \{(x_i, y_i)\}_{i=1}^{|R|}$ and $(x_1, y_1) \le \dots \le (x_{|R|}, y_{|R|})$. Here, $(x, y) \le (x', y')$ denotes the lexicographical ordering, which means either (a) $x < x'$ or (b) $x = x'$ and $y \le y'$.

A.2 Implementing forward queries

In Section 4, we defined a (standard) path-recording oracle V that simulates forward (but not inverse) queries to a Haar-random unitary. In this subsection, we describe how to implement this linear map efficiently.

Definition 42. *[Definition 10, repeated] The path-recording oracle V is a linear map $V : \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}} \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}}$ defined as follows. For all $x \in [N]$ and injective relations $R \in \mathcal{R}^{\mathsf{inj}}$ such that $|R| < N$,*

$$V :\ |x\rangle_{\mathsf{A}}\ |R\rangle_{\mathsf{R}} \mapsto \frac{1}{\sqrt{N - |R|}} \sum_{\substack{y \in [N],\\ y \notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}}\ |R \cup \{(x, y)\}\rangle_{\mathsf{R}}\,. \tag{A.2}$$

We briefly sketch how to implement V on an input $|x\rangle\ |R\rangle$.

Input: a state of the form $|x\rangle\ |R\rangle$.

1. The first step is to perform the map

$$|x\rangle\ |R\rangle \mapsto \frac{1}{\sqrt{N - |R|}} \sum_{\substack{y \in [N],\\ y \notin \mathrm{Im}(R)}} |y\rangle\ |x\rangle\ |R\rangle\,. \tag{A.3}$$

   This can be done as follows:

   (a) First, prepare a new register containing a uniform superposition over $\{1, 2, \dots, N - |R|\}$.

   (b) Next, observe that given $y_1 \le \dots \le y_{|R|}$ (which are stored in subregisters of $|R\rangle$), there is an efficiently computable bijection f from $\{1, 2, \dots, N - |R|\}$ to the set $\{y : y \in [N], y \notin \mathrm{Im}(R)\}$: on input x, compute the number n_x of elements y_i in the list $(y_1, \dots, y_{|R|})$ such that $x \ge y_i$, and output $x + n_x$. Using a similar algorithm, we can also compute f^{-1} efficiently.

   This allows us to efficiently compute f *in place*. Applying this to the uniform superposition over $\{1, 2, \dots, N - |R|\}$ produces the desired superposition.

2. Next, compute the function that maps (y, x, R) to $R \cup \{(x, y)\}$ (where R and $R \cup \{(x, y)\}$ are represented as sorted lists of ordered pairs). This step corresponds to the map

$$\frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle\,|x\rangle\,|R\rangle \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle\,|x\rangle\,|R\rangle\,|R\cup\{(x,y)\}\rangle\,. \tag{A.4}$$

3. Finally, use the $|y\rangle\,|R\cup\{(x,y)\}\rangle$ register to uncompute the $|x\rangle\,|R\rangle$ registers; note that x, R can be uniquely computed from $y, R\cup\{(x,y)\}$, since y is guaranteed to be outside $\mathrm{Im}(R)$. This corresponds to the map

$$\frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle\,|x\rangle\,|R\rangle\,|R\cup\{(x,y)\}\rangle \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle\,|R\cup\{(x,y)\}\rangle\,, \tag{A.5}$$

which corresponds to the output of V.

A.3 Implementing forward and inverse queries

In Section 8, we defined a (symmetric) path-recording oracle V that simulates both forward and inverse queries to a Haar-random unitary. In this subsection, we describe how to implement this linear map efficiently. Recall that this linear map V is defined in terms of two helper linear maps V^L and V^R.

Definition 43 (left and right partial isometries)**.** *[Definition 25, repeated] Let V^L be the linear operator that acts as follows. For $x \in [N]$ and $(L, R) \in \mathcal{R}^{2,\le N-1}$,*

$$V^L \cdot |x\rangle_{\mathsf{A}}\,|L\rangle_{\mathsf{L}}\,|R\rangle_{\mathsf{R}} := \sum_{\substack{y\in[N]:\\ y\notin \mathrm{Im}(L\cup R)}} \frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}}\,|y\rangle_{\mathsf{A}}\,|L\cup\{(x,y)\}\rangle_{\mathsf{L}}\,|R\rangle_{\mathsf{R}}\,. \tag{A.6}$$

Define V^R to be the linear operator such that for all $y \in [N]$ and $(L, R) \in \mathcal{R}^{2,\le N-1}$,

$$V^R \cdot |y\rangle_{\mathsf{A}}\,|L\rangle_{\mathsf{L}}\,|R\rangle_{\mathsf{R}} := \sum_{\substack{x\in[N]:\\ x\notin \mathrm{Dom}(L\cup R)}} \frac{1}{\sqrt{N-|\mathrm{Dom}(L\cup R)|}}\,|x\rangle_{\mathsf{A}}\,|L\rangle_{\mathsf{L}}\,|R\cup\{(x,y)\}\rangle_{\mathsf{R}}\,. \tag{A.7}$$

Efficient implementation of forward queries to V^L and V^R can be done similarly to Appendix A.2. Now, let U^L denote the efficient unitary implicit in the procedure described in Appendix A.2, which satisfies the guarantee that $U^L\,|x\rangle\,|R\rangle\,|0^m\rangle = (V^L\,|x\rangle\,|R\rangle)\otimes|0^{m'}\rangle$, where m and m' denotes the number of ancilla qubits in the input and output respectively. Define U^R similarly. Technically, the number of ancillas depends on the size of L and R. However, we can always assume that the sizes of L and R are upper bounded by the number of queries so far, and so we can also use this to bound the size of the ancillas needed to implement the t-th query.

Implementing $V^{L,\dagger}, V^{R,\dagger}$ Since we can efficiently implement U^L, we can also implement its inverse $U^{L,\dagger}$. Note that on states of the form $|\psi\rangle\,|0^{m'}\rangle$, where $|\psi\rangle$ is in the image of V^L, applying $U^{L,\dagger}$ produces the output state $(V^{L,\dagger}\,|\psi\rangle)\,|0^m\rangle$. Thus, we can use $U^{L,\dagger}$ to implement $V^{L,\dagger}$.

Implementing coherent measurements on $V^L \cdot V^{L,\dagger}$ and $V^R \cdot V^{R,\dagger}$ Before we describe how we implement V, we will need to describe how to perform measurements corresponding to the projectors $V^L \cdot V^{L,\dagger}$ and $V^R \cdot V^{R,\dagger}$. In fact, we will need to implement these measurements coherently, i.e., apply the unitary that computes the binary measurement outcome onto an external qubit. This can be done as follows (for simplicity, we only describe the procedure for implementing the coherent $V^L \cdot V^{L,\dagger}$ measurement, as the coherent $V^R \cdot V^{R,\dagger}$ measurement is symmetric).

Input: a state $|\psi\rangle = \sum_{x,L,R} \alpha_{x,L,R} |x\rangle\ |L\rangle\ |R\rangle$.

1. Add m' ancillary qubits $|0^{m'}\rangle$ and then apply $U^{L,\dagger}$.
2. Initialize a new one-qubit register to $|0\rangle_{\mathsf{B}}$. Controlled on the last m qubits of the rest of the state (i.e., all registers except for B) being 0^m, apply a Pauli X to the B register. By definition of $U^{L,\dagger}$, this Pauli X is applied if and only if the original input state was in the image of $V^L \cdot V^{L,\dagger}$.
3. Apply U^L to the non-B registers.

Now, recall the definition of V.

Definition 44. *The symmetric path-recording oracle is the operator V defined as*

$$V = V^L \cdot (\mathsf{Id} - V^R \cdot V^{R,\dagger}) + (\mathsf{Id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}. \tag{A.8}$$

We sketch an implementation of a forward query to the symmetric path-recording oracle V. The inverse query is symmetric by swapping L and R.

Input: a state $|\psi\rangle = \sum_{x,L,R} \alpha_{x,L,R} |x\rangle\ |L\rangle\ |R\rangle$.

1. Add two ancilla qubits initialized at $|0\rangle$ to obtain $|0\rangle\ |0\rangle\ |\psi\rangle$.
2. Implement coherent measurement $V^R \cdot V^{R,\dagger}$, writing the outcome onto the first ancilla qubit.
3. Apply the following controlled operation:
   - Controlled on the first ancilla qubit being 1, apply V^L.
   - Controlled on the first ancilla qubit being 0, apply $V^{R,\dagger}$. Then, apply the coherent measurement $V^L \cdot V^{L,\dagger}$, writing the outcome onto the second ancilla qubit.
4. Measure the second ancilla qubit, and abort if the outcome is 1.
5. Apply the coherent measurement of $V^L \cdot V^{L,\dagger}$ with the outcome applied onto the first ancilla qubit.
6. Trace out the remaining ancilla qubit (the first one), which is guaranteed to be $|0\rangle$.

B The path-recording framework

In this section, we develop a mathematical framework by generalizing the path-recording oracle introduced in Section 4. This new framework enables one to develop modified versions of path-recording oracle in which the set of relations that the oracle uses is restricted to a subset $\mathcal{S}^{\mathsf{inj}} \subseteq \mathcal{R}^{\mathsf{inj}}$ of the set of all injective relations. This mathematical framework offers flexibility for establishing indistinguishability from Haar-random unitary via the path-recording oracle.

To develop the path-recording framework, we define the following notations.

- $t_{\max}$ is an integer between 1 and N sets the maximum size of the relations. This integer also sets the limit on how many queries we can make to the path-recording oracle. In the canonical path-recording oracle introduced in Section 4.1, $t_{\max}$ is equal to N.
- $\mathcal{S}_t^{\mathsf{inj}}$ is a subset of all the injective relations $\mathcal{R}_t^{\mathsf{inj}}$ of size t for any $0 \le t \le t_{\max}$. In particular, we require the subset for the maximum t to be non-empty: $|\mathcal{S}_{t_{\max}}^{\mathsf{inj}}| \ge 1$.
- $\mathcal{S}^{\mathsf{inj}} \coloneqq \cup_{t=0}^{t_{\max}} \mathcal{S}_t^{\mathsf{inj}}$. The set $\mathcal{S}$ restricts the relations that the path-recording oracle could use.

We define the following two constraints on the restricted set $\mathcal{S}^{\mathsf{inj}}$.

Definition 45 (Consistency)**.** *We say the set $\mathcal{S}^{\mathsf{inj}}$ of relations is consistent if*

$$\forall (x_1, \ldots, x_t) \in [N]^t, \quad \exists (y_1, \ldots, y_t) \in [N]^t, \tag{B.1}$$

$$\text{such that} \quad \{(x_i, y_i)\}_{i=1}^t \in \mathcal{S}^{\mathsf{inj}}. \tag{B.2}$$

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

The *consistency constraint* ensures that all possible $(x_1, \ldots, x_t) \in [N]^t$ are valid. This is central for path-recording oracle because the adversary algorithm can choose the inputs $x_1, \ldots, x_t$ arbitrarily. The constraint also ensures that all relations in $\mathcal{S}^{\mathsf{inj}}$ are "meaningful" because they can all be obtained by adding in each tuple (x_i, y_i) one by one while maintaining in the restricted subset $\mathcal{S}^{\mathsf{inj}}$.

Definition 46 (Uniform growth)**.** *We say the set $\mathcal{S}^{\mathsf{inj}}$ of relations satisfies the uniform growth constraint if for all $0 \le t < t_{\max}$, there exists $\mathcal{Z}_t \ge 1$, such that for all $x \in [N]$ and $R \in \mathcal{S}_t^{\mathsf{inj}}$,*

$$\mathcal{Z}_t = \sum_{\substack{y \in [N], \text{ s.t.} \\ R \cup \{(x,y)\} \in \mathcal{S}_{t+1}^{\mathsf{inj}}}} 1. \tag{B.3}$$

The *uniform growth constraint* ensures the number of y that can be used to grow the relation R by by size one is uniform across all $x \in [N]$ and all relations R of the same size. We illustrate these two constraints with the following examples.

- $\mathcal{S}^{\mathsf{inj}}$ contains all relations where the first k bits in $y_1, \ldots, y_t \in [N]$ are distinct. In this case, $t_{\max} = 2^k$. Furthermore, $\mathcal{S}^{\mathsf{inj}}$ is consistent and satisfies the uniform growth constraint.
- $\mathcal{S}^{\mathsf{inj}}$ contains all relations R where $R = \{(x_i, x_i)\}_{i=1}^{|R|}$. In this case, $t_{\max} = N$. And $\mathcal{S}^{\mathsf{inj}}$ is consistent and satisfies the uniform growth constraint.
- $\mathcal{S}^{\mathsf{inj}} = \{R \in \mathcal{R}^{\mathsf{inj}} \mid |R| = N\}$. In this case, $t_{\max} = N$. However, $\mathcal{S}^{\mathsf{inj}}$ is not consistent and does not satisfy the uniform growth constraint because it violates $\mathcal{Z}_t \ge 1$.

For any consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations, we have $\varnothing \in \mathcal{S}^{\mathsf{inj}}$ because we can take $\tau = 0$ in Definition 45 for any relation $R \in \mathcal{S}^{\mathsf{inj}}$ to obtain that $\varnothing \in \mathcal{S}^{\mathsf{inj}}$.

B.1 Defining $V(\mathcal{S}^{\mathsf{inj}})$ and the $V(\mathcal{S}^{\mathsf{inj}})$ state

We now define the behavior of the $\mathcal{S}^{\mathsf{inj}}$-restricted path-recording oracle.

Definition 47 ($\mathcal{S}^{\mathsf{inj}}$-restricted path-recording oracle)**.** *Given any consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations. The $\mathcal{S}^{\mathsf{inj}}$-restricted path-recording oracle $V(\mathcal{S}^{\mathsf{inj}})$ is a linear map*

$$V(\mathcal{S}^{\mathsf{inj}}) : \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}} \to \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}} \tag{B.4}$$

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

$$V(\mathcal{S}^{\mathsf{inj}}) : |x\rangle_{\mathsf{A}} |R\rangle_{\mathsf{R}} \mapsto \frac{1}{\sqrt{\mathcal{Z}_{x,R}}} \sum_{\substack{y\in[N],\\ R\cup\{(x,y)\}\in\mathcal{S}^{\mathsf{inj}}_{t+1}}} |y\rangle_{\mathsf{A}} |R\cup\{(x,y)\}\rangle_{\mathsf{R}}\,, \tag{B.5}$$

The normalization factor $\mathcal{Z}_{x,R}$ is given by

$$\mathcal{Z}_{x,R} \coloneqq \sum_{\substack{y\in[N],\\ R\cup\{(x,y)\}\in\mathcal{S}^{\mathsf{inj}}_{t+1}}} 1 \ge 1, \tag{B.6}$$

where the last inequality follows from the consistency constraint that for any $(x_1,\dots,x_t) \in [N]^t$, there exists $(y_1,\dots,y_t) \in [N]^t$, such that $\{(x_i,y_i)\}_{i=1}^t \in \mathcal{S}^{\mathsf{inj}}$.

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

Definition 48 (G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state)**.** *Given a consistent set $\mathcal{S}^{\mathsf{inj}}$, an n-qubit unitary G and a t-query adversary $\mathcal{A}$ with forward queries specified by a t-tuple of unitaries $(A_{1,\mathsf{AB}},\dots,A_{t,\mathsf{AB}})$, the G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state is*

$$|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}} \coloneqq \prod_{i=1}^{t} \Big(V(\mathcal{S}^{\mathsf{inj}}) \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}}\Big) |0\rangle_{\mathsf{AB}} |\varnothing\rangle_{\mathsf{R}}\,. \tag{B.7}$$

The G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state $|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}}$ is the state of the entire system after the adversary has made t queries to $V(\mathcal{S}^{\mathsf{inj}}) \cdot G$, and includes the adversary's query register (A), auxiliary register (B), and the purifying registers (R), after t queries to the oracle.

B.2 $V(\mathcal{S}^{\mathsf{inj}})$ is a partial isometry

A crucial property of the G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state is that it maintains unit norm up to $t_{\max}$ queries. We formalize this in the following lemma:

Lemma B.1 (G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state has unit norm)**.** *For any consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations, any adversary $\mathcal{A}$ making $t \le t_{\max}$ forward queries to an n-qubit oracle, and any n-qubit unitary G, the G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state $|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}}$ has unit norm.*

To prove this lemma, we first need to establish that the $\mathcal{S}^{\mathsf{inj}}$-restricted path-recording oracle $V(\mathcal{S}^{\mathsf{inj}})$ acts as a partial isometry on certain states. This is formalized in the following lemma:

Lemma B.2 (Partial Isometry)**.** *For any consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations, the $\mathcal{S}^{\mathsf{inj}}$-restricted path-recording oracle $V(\mathcal{S}^{\mathsf{inj}})$ is an isometry on the subspace of $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{R}}$ spanned by the states $|x\rangle |R\rangle$ for $x \in [N]$ and $R \in \mathcal{S}^{\mathsf{inj}}$ such that $|R| < t_{\max}$.*

Proof of Lemma B.2. To prove that $V(\mathcal{S}^{\mathsf{inj}})$ is an isometry on the specified subspace, it suffices to show that for all $x, x' \in [N]$ and $R, R' \in \mathcal{S}^{\mathsf{inj}}$ with $|R|, |R'| < t_{\max}$,

$$\langle x'|_{\mathsf{A}} \langle R'|_{\mathsf{R}} V(\mathcal{S}^{\mathsf{inj}})^\dagger \cdot V(\mathcal{S}^{\mathsf{inj}}) |x\rangle_{\mathsf{A}} |R\rangle_{\mathsf{R}} = \langle x'|x\rangle_{\mathsf{A}} \cdot \langle R'|R\rangle_{\mathsf{R}} . \tag{B.8}$$

The proof proceeds in the same way as the proof of Lemma 4.1 after one notes the fact that the normalization factor $\mathcal{Z}x, R \geq 1$ from the consistency of the set $\mathcal{S}^{\mathsf{inj}}$. □

We can now prove Lemma B.1.

Proof of Lemma B.1. Note that $\mathcal{S}^{\mathsf{inj}}$ is consistent implies $\varnothing \in \mathcal{S}_0^{\mathsf{inj}}$. Hence, we can use Lemma B.2 to establish this lemma via the same mathematical induction as the proof of Lemma 4.2. □

B.3 $V(\mathcal{S}^{\mathsf{inj}})$ is right unitary invariant

So far, we have not used the uniform growth constraint. To show that $V(\mathcal{S}^{\mathsf{inj}})$ is (exactly) right unitary invariant, we need to utilize the uniform growth constraint.

Lemma B.3 (Right unitary invariance)**.** *Given a consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations that satisfies the uniform growth constraint. For any n-qubit unitary G, we have*

$$|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}} = (G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}}) |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle_{\mathsf{ABR}} . \tag{B.9}$$

Lemma B.3 implies right unitary invariance since

$$\begin{aligned}
&\mathrm{Tr}_{\mathsf{R}}(\, |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle\langle \mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}|_{\mathsf{ABR}}) \\
&= \mathrm{Tr}_{\mathsf{R}}((G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}}) |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle \mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}} (G_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \otimes \ldots \otimes G_{\mathsf{R}_{\mathsf{X},t}^{(t)}})^\dagger) && \text{(by Lemma B.3)} \\
&= \mathrm{Tr}_{\mathsf{R}}(\, |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle \mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}). && \text{(by the cyclic property of } \mathrm{Tr}_{\mathsf{R}})
\end{aligned}$$

The first line corresponds to the adversary's view after making t queries to $V(\mathcal{S}^{\mathsf{inj}}) \cdot G_{\mathsf{A}}$, while the last line corresponds to its view after making t queries to $V(\mathcal{S}^{\mathsf{inj}})$.

Fact 13 (Explicit form of the G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ state)**.** *Given a consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations that satisfies the uniform growth constraint. The definition of $V(\mathcal{S}^{\mathsf{inj}})$ and $|R\rangle_{\mathsf{R}}$ enable us to expand the $V(\mathcal{S}^{\mathsf{inj}})$ state after t queries to obtain*

$$|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}} = \sqrt{\prod_{i=0}^{t-1} \frac{1}{\mathcal{Z}_i}} \sum_{\substack{(x_1,\ldots,x_t)\in[N]^t \\ (y_1,\ldots,y_t)\in[N]^t_{\mathrm{dist}} \\ R=\{(x_i,y_i)\}_{i=1}^t \in \mathcal{S}_t^{\mathsf{inj}}}} \left[\prod_{i=1}^{t} \Big(|y_i\rangle\langle x_i|_{\mathsf{A}} \cdot G_{\mathsf{A}} \cdot A_{i,\mathsf{AB}} \Big) |0\rangle_{\mathsf{AB}} \right] \otimes |R\rangle_{\mathsf{R}} \tag{B.10}$$

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

$$\otimes \frac{1}{\sqrt{t!}} \sum_{\pi\in\mathsf{Sym}_t} \left(R_\pi |x_1\rangle_{\mathsf{R}_{\mathsf{X},1}^{(t)}} \ldots |x_t\rangle_{\mathsf{R}_{\mathsf{X},t}^{(t)}} \right) \otimes \left(R_\pi |y_1\rangle_{\mathsf{R}_{\mathsf{Y},1}^{(t)}} \ldots |y_t\rangle_{\mathsf{R}_{\mathsf{Y},t}^{(t)}} \right) . \tag{B.11}$$

Proof of Lemma B.3. By utilizing Fact 13 instead of Fact 3, we can prove this lemma in the same way as the proof of Lemma 4.3. □

B.4 Relation between $V(\mathcal{S}^{\mathsf{inj}})$ and V state

Using the states $|R\rangle_{\mathsf{R}}$, we can define the following restricted subspace projector based on the restricted subspace $\Pi_{\mathsf{R}}^{\mathsf{restrict},t}$.

Definition 49 (Restricted subspace projector)**.** *For $0 \le t \le t_{\max}$, we define the size-t restricted subspace projector $\Pi_{\mathsf{R}}^{\mathsf{restrict},t}$ as follows:*

$$\Pi_{\mathsf{R}}^{\mathsf{restrict},t} := \sum_{R \in \mathcal{S}_t^{\mathsf{inj}}} |R\rangle\langle R|_{\mathsf{R}} \,. \tag{B.12}$$

The restricted subspace projector is defined as:

$$\Pi_{\mathsf{R}}^{\mathsf{restrict}} := \sum_{t=0}^{t_{\max}} \Pi_{\mathsf{R}}^{\mathsf{restrict},t}. \tag{B.13}$$

From Fact 13 and the projector defined above, we immediately obtain the following equation relating the G-rotated $V(\mathcal{S}^{\mathsf{inj}})$ and the $|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}}$s.

Fact 14 (Relation between $V(\mathcal{S}^{\mathsf{inj}})$ and V state)**.** *Given a consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations that satisfies the uniform growth constraint. For any n-qubit unitary G, we have*

$$\sqrt{\prod_{i=0}^{t-1} \mathcal{Z}_i} \cdot \sqrt{\frac{(N-t)!}{N!}} \cdot |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}} = \Pi_{\mathsf{R}}^{\mathsf{restrict}} |\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}} \,, \tag{B.14}$$

where the prefactor $\sqrt{\prod_{i=0}^{t-1} \mathcal{Z}_i} \cdot \sqrt{\frac{(N-t)!}{N!}}$ is between 0 and 1 because the $V(\mathcal{S}^{\mathsf{inj}})$ state $|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})\cdot G}\rangle_{\mathsf{ABR}}$ has unit norm and the projected V state $\Pi_{\mathsf{R}}^{\mathsf{restrict}} |\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}}$ has norm at most one.

B.5 $V(\mathcal{S}^{\mathsf{inj}})$ is indistinguishable from Haar random unitaries

When the restricted set $\mathcal{S}^{\mathsf{inj}}$ of relations has a large enough growth, then $V(\mathcal{S}^{\mathsf{inj}})$ is indistinguishable from Haar-random unitaries. This is formally captured by the following theorem.

Theorem 9 ($V(\mathcal{S}^{\mathsf{inj}})$ is indistinguishable from Haar random)**.** *Given a consistent set $\mathcal{S}^{\mathsf{inj}}$ of relations that satisfies the uniform growth constraint. Let $\mathcal{A}$ be a t-query oracle adversary with forward queries. Then*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}| \,, \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right) \tag{B.15}$$

$$\le \frac{2t(t-1)}{N+1} + 2\left(1 - \prod_{i=0}^{t-1} \mathcal{Z}_i \cdot \frac{(N-t)!}{N!}\right). \tag{B.16}$$

Proof. Using Theorem 5 and triangle inequality, we have

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{\mathcal{O}\leftarrow\mu_{\mathsf{Haar}}} |\mathcal{A}_t^{\mathcal{O}}\rangle\langle\mathcal{A}_t^{\mathcal{O}}| \,, \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right) \tag{B.17}$$

$$\le \frac{2t(t-1)}{N+1} + \mathsf{TD}\left(\mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\right), \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right). \tag{B.18}$$

We can bound the second term as follows,

$$\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V}\rangle\langle\mathcal{A}_t^{V}|_{\mathsf{ABR}}\right), \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right) \tag{B.19}$$

$$\leq \mathsf{TD}\left(\mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^V\rangle\langle\mathcal{A}_t^V|_{\mathsf{ABR}}\right), \mathrm{Tr}_{\mathsf{R}}\left(\Pi_{\mathsf{R}}^{\mathsf{restrict}}|\mathcal{A}_t^{V\cdot G}\rangle\langle\mathcal{A}_t^{V\cdot G}|_{\mathsf{ABR}}\Pi_{\mathsf{R}}^{\mathsf{restrict}}\right)\right) \tag{B.20}$$

$$+\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{R}}\left(\Pi_{\mathsf{R}}^{\mathsf{restrict}}|\mathcal{A}_t^{V\cdot G}\rangle\langle\mathcal{A}_t^{V\cdot G}|_{\mathsf{ABR}}\Pi_{\mathsf{R}}^{\mathsf{restrict}}\right), \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right). \tag{B.21}$$

Using Lemma 2.2 and Fact 14, Eq. (B.20) is equal to

$$1 - \langle\mathcal{A}_t^{V\cdot G}|\Pi_{\mathsf{R}}^{\mathsf{restrict}}|\mathcal{A}_t^{V\cdot G}\rangle_{\mathsf{ABR}} = \left(1 - \prod_{i=0}^{t-1}\mathcal{Z}_i\cdot\frac{(N-t)!}{N!}\right). \tag{B.22}$$

Again, using Fact 14, Eq. (B.21) is equal to

$$\mathsf{TD}\left(\prod_{i=0}^{t-1}\mathcal{Z}_i\cdot\frac{(N-t)!}{N!}\cdot\mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right), \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}})}|_{\mathsf{ABR}}\right)\right) \tag{B.23}$$

$$= \left(1 - \prod_{i=0}^{t-1}\mathcal{Z}_i\cdot\frac{(N-t)!}{N!}\right). \tag{B.24}$$

Together, we obtained the stated result. □

C An elementary proof of the gluing lemma

In this section, we show how to use the path-recording framework to establish an elementary proof of the gluing lemma recently shown in [SHH24]. The proof in [SHH24] makes use of representation theory and Weingarten calculus. Here, we present an elementary proof using the path-recording framework for analyzing Haar-random unitaries.

The gluing lemma presented in [SHH24] shows that the composition of two Haar-random unitaries on system $\mathsf{A}_1\mathsf{A}_2$ and $\mathsf{A}_2\mathsf{A}_3$ that overlap only on a small number of qubits is indistinguishable from a Haar-random unitary on the entire system $\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3$.

Theorem 10 (Gluing two Haar-random unitaries)**.** *Consider three systems $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3$ of qubits with $\mathsf{A} = \mathsf{A}_1\mathsf{A}_2\mathsf{A}_3$. Let $|\mathsf{A}_1|, |\mathsf{A}_2|, |\mathsf{A}_3|$ denote the number of qubits in each system. Let $U_{\mathsf{A}_1\mathsf{A}_2}, U_{\mathsf{A}_2\mathsf{A}_3}, U_{\mathsf{A}}$ be Haar-random unitaries on system $\mathsf{A}_1\mathsf{A}_2, \mathsf{A}_2\mathsf{A}_3, \mathsf{A}$, respectively. We have*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U_{\mathsf{A}_1\mathsf{A}_2}, U_{\mathsf{A}_2\mathsf{A}_3}}|\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}U_{\mathsf{A}_2\mathsf{A}_3}}\rangle\langle\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}U_{\mathsf{A}_2\mathsf{A}_3}}|, \mathop{\mathbb{E}}_{U_{\mathsf{A}}}|\mathcal{A}_t^{U_{\mathsf{A}}}\rangle\langle\mathcal{A}_t^{U_{\mathsf{A}}}|\right) \leq \frac{9t(t-1)}{2^{|\mathsf{A}_2|}}. \tag{C.1}$$

Proof. We approximate the three Haar-random unitaries $U_{\mathsf{A}_1\mathsf{A}_2}, U_{\mathsf{A}_2\mathsf{A}_3}, U_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}$ by three restricted sets $\mathcal{S}^{\mathsf{inj}}_{\mathsf{A}_1\mathsf{A}_2}, \mathcal{S}^{\mathsf{inj(D)}}_{\mathsf{A}_2\mathsf{A}_3}, \mathcal{S}^{\mathsf{inj(CD)}}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}$ of relations. The three subsets of injective relations are given as follows.

- $\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2}$: Injective relations R over system $\mathsf{A}_1\mathsf{A}_2$ such that the system A_2 part of elements in the image $\mathrm{Im}(R)$ are distinct, i.e., given $\mathrm{Im}(R) = \{y_1, \ldots, y_{|R|}\}$, $y_{i,\mathsf{A}_2} \neq y_{j,\mathsf{A}_2}$ for all $i \neq j$.
- $\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3}$: Injective relations R over system $\mathsf{A}_2\mathsf{A}_3$ such that the system A_2 part of elements in the image $\mathrm{Im}(R)$ are distinct.
- $\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}$: Injective relations R over system $\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3$ such that the system $\mathsf{A}_1\mathsf{A}_2$ part of elements in the image $\mathrm{Im}(R)$ are distinct.

Here, given a bitstring y, we denote y_{A_2} to be the substring corresponding to bits in A_2. It is not hard to see that these restricted sets is consistent and satisfies the uniform growth constraint. We

consider the path recording oracle $V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2})$ to act on system $\mathsf{A}_1, \mathsf{A}_2, \mathsf{R}_1$, the oracle $V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})$ to act on system $\mathsf{A}_2, \mathsf{A}_3, \mathsf{R}_2$, and the oracle $V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})$ to act on system $\mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3, \mathsf{R}_3$. Let

$$\rho_1 \coloneqq \mathop{\mathbb{E}}_{U_{\mathsf{A}_1\mathsf{A}_2}, U_{\mathsf{A}_2\mathsf{A}_3}} |\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}U_{\mathsf{A}_2\mathsf{A}_3}}\rangle\langle\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}U_{\mathsf{A}_2\mathsf{A}_3}}|, \tag{C.2}$$

$$\rho_2 \coloneqq \mathop{\mathbb{E}}_{U_{\mathsf{A}_1\mathsf{A}_2}} \mathrm{Tr}_{\mathsf{R}_1} |\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}\rangle\langle\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2}V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}|, \tag{C.3}$$

$$\rho_3 \coloneqq \mathrm{Tr}_{\mathsf{R}_1}\mathrm{Tr}_{\mathsf{R}_2} |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}|, \tag{C.4}$$

$$\rho_4 \coloneqq \mathrm{Tr}_{\mathsf{R}_3} |\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}|, \tag{C.5}$$

$$\rho_5 \coloneqq \mathop{\mathbb{E}}_{U_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}} |\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}}\rangle\langle\mathcal{A}_t^{U_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}}|. \tag{C.6}$$

Using Theorem 9 and properly computing the normalization factor $\mathcal{Z}_t$, we have

$$\mathsf{TD}(\rho_1,\rho_2) \le \frac{2t(t-1)}{2^{|\mathsf{A}_2|+|\mathsf{A}_3|}} + 2\left(1 - \prod_{i=0}^{t-1}(2^{|\mathsf{A}_2|+|\mathsf{A}_3|} - i2^{|\mathsf{A}_3|})\cdot\frac{(2^{|\mathsf{A}_2|+|\mathsf{A}_3|}-t)!}{(2^{|\mathsf{A}_2|+|\mathsf{A}_3|})!}\right), \tag{C.7}$$

$$\le \frac{2t(t-1)}{2^{|\mathsf{A}_2|+|\mathsf{A}_3|}} + 2\left(1 - \prod_{i=0}^{t-1}\left(1 - i2^{-|\mathsf{A}_2|}\right)\right) \le \frac{2t(t-1)}{2^{|\mathsf{A}_2|+|\mathsf{A}_3|}} + \frac{t(t-1)}{2^{|\mathsf{A}_2|}} \le \frac{3t(t-1)}{2^{|\mathsf{A}_2|}}. \tag{C.8}$$

Similarly, we have

$$\mathsf{TD}(\rho_2,\rho_3) \le \frac{2t(t-1)}{2^{|\mathsf{A}_1|+|\mathsf{A}_2|}} + 2\left(1 - \prod_{i=0}^{t-1}(2^{|\mathsf{A}_1|+|\mathsf{A}_2|} - i2^{|A_1|})\cdot\frac{(2^{|\mathsf{A}_1|+|\mathsf{A}_2|}-t)!}{(2^{|\mathsf{A}_1|+|\mathsf{A}_2|})!}\right) \le \frac{3t(t-1)}{2^{|\mathsf{A}_2|}}, \tag{C.9}$$

$$\mathsf{TD}(\rho_4,\rho_5) \le \frac{2t(t-1)}{2^{|\mathsf{A}|}} + 2\left(1 - \prod_{i=0}^{t-1}(2^{|\mathsf{A}|} - i2^{|\mathsf{A}_1|+|\mathsf{A}_3|})\cdot\frac{(2^{|\mathsf{A}|}-t)!}{(2^{|\mathsf{A}|})!}\right) \le \frac{3t(t-1)}{2^{|\mathsf{A}_2|}}. \tag{C.10}$$

Finally, we show that $\rho_3 = \rho_4$. Let $x||y$ denote bitstring concatenation. Using the definition of the restricted subsets of injective relations, the explicit form of the purified state in Fact 13 yields

$$|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}\rangle_{\mathsf{ABR}_1\mathsf{R}_2} = \sqrt{\prod_{i=0}^{t-1}\frac{1}{2^{|\mathsf{A}_2|+|\mathsf{A}_3|} - i2^{|\mathsf{A}_3|}}}\cdot\sqrt{\prod_{i=0}^{t-1}\frac{1}{2^{|\mathsf{A}_1|+|\mathsf{A}_2|} - i2^{|\mathsf{A}_1|}}}. \tag{C.11}$$

$$\sum_{\substack{(x_1,\ldots,x_t)\in[2^{|A|}]^t\\(y_1,\ldots,y_t)\in[2^{|A|}]^t_{\mathrm{dist}}\\(z_1,\ldots,z_t)\in[2^{|A_2|}]^t_{\mathrm{dist}}\\\text{s.t. }(y_{1,A_2},\ldots,y_{t,A_2})\in[2^{|A_2|}]^t_{\mathrm{dist}}\\R=\{(x_{i,A_2}||x_{i,A_3},z_{i,A_2}||y_{i,A_3})\}_{i=1}^t\in\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3}\\S=\{(x_{i,A_1}||z_{i,A_2},y_{i,A_1}||y_{i,A_2})\}_{i=1}^t\in\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2}}} \left[\prod_{i=1}^{t}\left(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot A_{i,\mathsf{AB}}\right)|0\rangle_{\mathsf{AB}}\right]\otimes|R\rangle_{\mathsf{R}_1}\otimes|S\rangle_{\mathsf{R}_2}, \tag{C.12}$$

and, similarly, Fact 13 also yields

$$|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}\rangle_{\mathsf{ABR}_3} = \sqrt{\prod_{i=0}^{t-1}\frac{1}{2^{|\mathsf{A}|} - i2^{|\mathsf{A}_1|+|\mathsf{A}_3|}}}. \tag{C.13}$$

$$\sum_{\substack{(x_1,\ldots,x_t)\in[2^{|A|}]^t\\(y_1,\ldots,y_t)\in[2^{|A|}]^t_{\mathrm{dist}}\\ \text{s.t. } (y_{1,A_2},\ldots,y_{t,A_2})\in[2^{|A_2|}]^t_{\mathrm{dist}}\\ T=\{(x_i,y_i)\}_{i=1}^t\in\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3}}} \left[\prod_{i=1}^{t}\Big(|y_i\rangle\langle x_i|_{\mathsf{A}}\cdot A_{i,\mathsf{AB}}\Big)|0\rangle_{\mathsf{AB}}\right]\otimes|T\rangle_{\mathsf{R}_3}. \tag{C.14}$$

We define a linear map $\mathsf{Uncompress}$ that maps registers R_3 to registers $\mathsf{R}_1,\mathsf{R}_2$. For any $T=\{(x_i,y_i)\}_{i=1}^t$ such that $(x_1,\ldots,x_t)\in[2^{|A|}]^t$, $(y_1,\ldots,y_t)\in[2^{|A|}]^t_{\mathrm{dist}}$, and $(y_{1,A_2},\ldots,y_{t,A_2})\in[2^{|A_2|}]^t_{\mathrm{dist}}$, the linear map $\mathsf{Uncompress}$ acts as

$$\mathsf{Uncompress}\,|T\rangle_{\mathsf{R}_3}\coloneqq\sqrt{\prod_{i=0}^{t-1}\frac{1}{2^{|\mathsf{A}_2|}-i}}\sum_{\substack{(z_1,\ldots,z_t)\in[2^{|A_2|}]^t_{\mathrm{dist}}\\ \text{s.t. } R=\{(x_{i,A_2}||x_{i,A_3},z_{i,A_2}||y_{i,A_3})\}_{i=1}^t\\ S=\{(x_{i,A_1}||z_{i,A_2},y_{i,A_1}||y_{i,A_2})\}_{i=1}^t}}|R\rangle_{\mathsf{R}_1}\,|S\rangle_{\mathsf{R}_2}. \tag{C.15}$$

One can directly check that $\mathsf{Uncompress}$ is a partial isometry and $|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}\rangle_{\mathsf{ABR}_3}$ is in the domain of $\mathsf{Uncompress}$ by construction. Furthermore, by definition, we have

$$\mathsf{Uncompress}\,|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}\rangle_{\mathsf{ABR}_3}=|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}\rangle_{\mathsf{ABR}_1\mathsf{R}_2}. \tag{C.16}$$

Because $\mathsf{Uncompress}$ acts isometric in its domain, we have

$$\rho_3=\mathrm{Tr}_{\mathsf{R}_1}\mathrm{Tr}_{\mathsf{R}_2}\,|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}}_{\mathsf{A}_1\mathsf{A}_2})V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_2\mathsf{A}_3})}| \tag{C.17}$$

$$=\mathrm{Tr}_{\mathsf{R}_3}\,|\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}\rangle\langle\mathcal{A}_t^{V(\mathcal{S}^{\mathsf{inj}(\mathsf{A}_2)}_{\mathsf{A}_1\mathsf{A}_2\mathsf{A}_3})}|=\rho_4. \tag{C.18}$$

Together, by a series of triangle inequality, we have

$$\mathsf{TD}(\rho_1,\rho_5)\le\mathsf{TD}(\rho_1,\rho_2)+\mathsf{TD}(\rho_2,\rho_3)+\mathsf{TD}(\rho_4,\rho_5)\le\frac{9t(t-1)}{2^{|\mathsf{A}_2|}}, \tag{C.19}$$

which concludes the proof of this theorem by noting the definition of ρ_1 and ρ_5. □

As shown in [SHH24], one can iteratively apply the gluing lemma to glue many small Haar-random unitaries over small number of qubits into a pseudorandom unitary on the entire system. If we have an n-qubit system A that is separated into consecutive subsystems $\mathsf{A}_1,\ldots,\mathsf{A}_{2m}$, we can glue together small Haar-random unitaries $U_{\mathsf{A}_1\mathsf{A}_2},U_{\mathsf{A}_2\mathsf{A}_3},\ldots$ as follows,

$$U_{\mathsf{glued}}\coloneqq\prod_{k=0}^{m-1}(U_{\mathsf{A}_{2+2k}\mathsf{A}_{3+2k}})\prod_{k=0}^{m-1}(U_{\mathsf{A}_{1+2k}\mathsf{A}_{2+2k}}). \tag{C.20}$$

Using triangle inequality, the trace distance between a t-query adversary output state that queries U_{glued} versus Haar-random unitary is upper bounded by

$$2m\cdot\frac{9t(t-1)}{2^{\min_{i\in[2m]}|\mathsf{A}_i|}}. \tag{C.21}$$

If each subsystem is of size $\omega(\log n)$, then the glued unitary U_{glued} will be a pseudorandom unitary secure against poly(n)-time adversary. This can be seen by noting that a poly(n)-time adversary can

only make $t = \mathrm{poly}(n)$ queries, so the trace distance between the adversary state querying U_{glued} and Haar-random unitary is upper bounded by

$$2m \cdot \frac{9t(t-1)}{2^{\min_{i\in[2m]} |\mathsf{A}_i|}} \leq \frac{\mathrm{poly}(n)}{2^{\omega(\log n)}} = \mathrm{negl}(n). \tag{C.22}$$

By replacing the small Haar-random unitaries over $\omega(\log n)$ qubits with small pseudorandom unitaries secure against subexponential adversary, one can show that the glued unitary U is an n-qubit pseudorandom unitary secure against $\mathrm{poly}(n)$-time adversary.

Assuming the subexponential hardness of LWE [Reg09], we have proved that a pseudorandom unitary secure against subexponential adversary can be generated in polynomial-depth on any circuit geometry using the PFC construction, including a 1D geometry. Hence, an n-qubit pseudorandom unitary secure against polynomial adversary can be generated in $\mathrm{poly}\log(n)$ depth on any circuit geometry. This work fills in the gap in [SHH24] that assumes the PFC construction forms a pseudorandom unitary under LWE hardness to rigorously establish the surprising fact that pseudorandom unitaries can be generated in extremely low depth under standard cryptographic assumptions.