Gluing Random Unitaries with Inverses and Applications to Strong Pseudorandom Unitaries*

Prabhanjan Ananth† UCSB
John Bostanci‡ Columbia
Aditya Gulati§ UCSB
Yao-Ting Lin¶ UCSB

Abstract

Gluing theorem for random unitaries [Schuster, Haferkamp, Huang, QIP 2025] have found numerous applications, including designing low depth random unitaries [Schuster, Haferkamp, Huang, QIP 2025], random unitaries in QAC0 [Foxman, Parham, Vasconcelos, Yuen'25] and generically shortening the key length of pseudorandom unitaries [Ananth, Bostanci, Gulati, Lin EUROCRYPT'25]. We present an alternate method of combining Haar random unitaries from the gluing lemma from [Schuster, Haferkamp, Huang, QIP 2025] that is secure against adversaries with inverse query access to the joined unitary. As a consequence, we show for the first time that strong pseudorandom unitaries can generically have their length extended, and can be constructed using only $O(n^{1/c})$ bits of randomness, for any constant c, if any family of strong pseudorandom unitaries exists.

*A preliminary version, merging this paper and [ABGL25a], appears in the proceedings of the *45th Annual International Cryptology Conference* (CRYPTO 2025) under the title "Pseudorandom Unitaries in the Haar Random Oracle Model" [ABGL25b]. This is Part II of the full version.

†prabhanjan@cs.ucsb.edu
‡johnb@cs.columbia.edu
§adityagulati@ucsb.edu
¶yao-ting_lin@ucsb.edu

Contents

1 Introduction **3**
- 1.1 Our Results . . . 3

2 Technical Overview **4**
- 2.1 Interpreting and Generalizing Ma-Huang's Path Recording Framework. . . . 4
- 2.2 The Strong Gluing Theorem and Its Purification . . . 6
- 2.3 Analyzing Purification of Querying V^{glued} . . . 7
- 2.4 Simulating the Larger Haar Unitary . . . 11
  - 2.4.1 Bounding "Progress Measure" . . . 14

3 Preliminaries **14**
- 3.1 Notation . . . 15
- 3.2 Cryptographic Primitives . . . 15
- 3.3 Useful Lemmas . . . 16

4 Path Recording and its Variants **16**
- 4.1 Interpreting the Path Recording Framework . . . 16
- 4.2 A Generalization of the Path-Recording Framework . . . 18
- 4.3 Modified Path Recording . . . 18

5 Glued Haar Unitary and its Purification **19**
- 5.1 Glued Haar Unitary Construction . . . 19
- 5.2 Glued Path Recording . . . 19
- 5.3 Modified Glued Path Recording . . . 21

6 Structure of Purification for W^{glued} **23**
- 6.1 Graph associated with the Database . . . 23
- 6.2 Analyzing Structure of the Graph . . . 24
- 6.3 Parametrizing Good Graphs . . . 24
- 6.4 Defining Good Auxiliary States . . . 25
- 6.5 Subspaces of Π^{Good} . . . 26
- 6.6 Action of W^{glued} on states in Π^{Good} . . . 28
- 6.7 Purification of W^{glued} is Good . . . 29

7 Strong Gluing Theorem **29**
- 7.1 Proof of Theorem 7.1 . . . 29
- 7.2 Defining $\mathcal{O}_{\mathsf{comp}}$ . . . 31
- 7.3 Proof of Theorem 7.4: Closeness between $\mathbf{H}_3$ and $\mathbf{H}_4$ . . . 32
- 7.4 Proof of Theorem 7.8: Closeness of the Oracle Queries . . . 33

8 Stretching Strong Pseudorandom Unitaries **34**

A Proof of Theorem 4.3 **39**

B Glued Path Recording **42**

C Proofs of Section 6.5 **43**

D Proofs of Section 6.6 **48**

E Proofs of Section 7.4 **50**

1 Introduction

Random unitaries are fundamental objects that find applications across diverse areas of quantum information science, including quantum algorithm benchmarking [KLR+08], quantum machine learning [HCP23], quantum cryptography [JLS18; GJMZ23; AGKL24; BHHP24], quantum chaos [GQY+24; Liu18] and quantum gravity [CGH+17]. Their utility stems from their ability to model generic quantum processes and serve as building blocks for various quantum protocols. Random unitaries are inherently complex objects—they require exponentially sized descriptions in general. To circumvent this complexity, researchers have developed the concepts of t-designs [AE07] and pseudorandom unitaries (PRUs) [JLS18], which can efficiently approximate the statistical properties of truly random unitaries for many applications.

Understanding the resources needed to implement random unitaries, t-designs and pseudorandom unitaries has been an important problem. Recently, a remarkable work by Schuster, Haferkamp and Huang [SHH24] presented a construction of random unitaries in extremely low depth. Specifically, they showed that pseudorandom unitaries can be constructed in logarithmic depth. The core contribution of their work is the gluing theorem which informally states the following: suppose we have two random unitaries U_1, U_2 such that U_1 acts on registers $\mathbf{A}, \mathbf{B}$ and unitaries U_2 acts on registers $\mathbf{B}, \mathbf{C}$ then $U_1 U_2$ approximately computes a random unitary on registers $\mathbf{A}, \mathbf{B}$ and $\mathbf{C}$ as long as $\mathbf{B}$ is sufficiently large enough. The gluing theorem has been proven to be quite useful in many applications:

- In the same work, Schuster et al. [SHH24] applied the gluing theorem recursively to construct random unitaries in logarithmic depth.
- Foxman, Parham, Vasconcelos, Yuen [FPVY25] used the gluing theorem to demonstrate that pseudorandom unitaries can be approximately implemented in $\mathsf{QAC0}$.
- Ananth, Bostanci, Gulati and, Lin [ABGL24] used the gluing theorem to show that any pseudorandom unitary can be converted into another pseudorandom unitary with the key length to be much smaller than the output length.

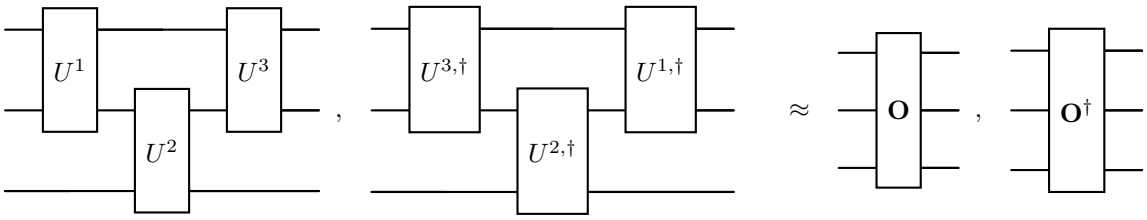
The disadvantage of the above gluing theorem is that the closeness to the joining random unitary does not hold if additionally oracle access to the inverse of the glued unitary is provided. In many applications, giving both forward and inverse access is important. As noted in [FPVY25], to determine lightcones, entanglement entropy and displacement amplitudes, access to the inverse is required. Having a gluing theorem that holds *even with inverse access* could have powerful applications; we call such a gluing theorem, a *strong* gluing theorem. As an example, [FPVY25] showed that the non-existence of strong gluing theorem (with certain properties) would imply that $\mathsf{PARITY} \notin \mathsf{QAC0}$, settling a major open problem in quantum complexity theory.

1.1 Our Results

We present for the first time a strong gluing theorem for random unitaries.

Theorem 1.1 (Strong gluing of random unitaries)**.** *Let U^1, U^2, and U^3 be three Haar random unitaries on n qubits, and A, C be registers of length $n - \lambda$ qubits, and B be a register of λ qubits, for $\lambda = \Omega(\log^{1+\epsilon}(n))$. Then no polynomial-query adversary can distinguish between $U^1_{\mathsf{AB}} V^2_{\mathsf{BC}} W^3_{\mathsf{AB}}$ and a Haar random unitary on* ABC even given inverse access *except with probability* $\mathsf{negl}(n)$.

We note that our strong gluing theorem is incomparable to the gluing lemma of [SHH24]. The strong gluing theorem uses a different construction, and applies to Haar random unitaries with inverse access, but does *not* get the same depth savings that the gluing lemma achieves. This is perhaps to be expected, as in the stronger query model with inverse access any two-layer construction is impossible. Hence, we end-up with the following three-layer construction:



Combining Theorem 1.1 with the construction of strong PRUs in the quantum Haar random oracle model [ABGL25b], we show how to shrink keys of strong PRUs for free: given a single sample of a PRU, denoted by U, we can sample $O(\log^{1+\epsilon}(n))$ additional bits of randomness to get sample access to two additional instances of a strong PRU, V, and W. Then we can join those instances to form a new strong PRU family that acts on (roughly) double the qubits. Recursively applying this strategy to the new, larger PRU, we can stretch to any arbitrary polynomial output length, giving us the following corollary.

Corollary 1.2 (Key-stretched strong PRUs)**.** *If there exists a family of strong PRUs in the plain model, then for every constant c, there exists a family of strong PRUs acting on n qubits with keys of length $O(n^{1/c})$.*

Interestingly, our strong gluing theorem implies that the existence of strong PRUs (in plain model) implies the existence of strong PRUs with linear depth (in plain model). In particular, given any strong PRU family that has depth $O(n^d)$ for some constant d, we can construct a strong PRU family with depth almost linear (i.e. $O(n^{1+1/c})$ for any constant c).

Corollary 1.3. *If there exists a family of strong PRUs in the plain model, then for every constant c, there exists a family of strong PRUs acting on n qubits with depth $O(n^{1+1/c})$.*

Beyond these results, we develop a number of mathematical tools and results useful for analyzing Haar random unitaries and modeling states using the path-recording isometries from [MH24].

2 Technical Overview

We structure the overview of our proof in the following steps: First, we will interpret Path Recording as a purification to queries to Haar unitaries and give a way to generalise it. Then we give a construction of gluing Haar unitaries and give a purification for this similar to Path Recording. Then we study the structure of this purification of glued Haar unitaries. Finally, using insights into the structure of the purification of glued Haar unitaries, we will define an operator that maps this purification to the purification of a single larger Haar unitary. We then by a query-by-query analysis show that the glued Haar unitaries is indistinguishable from a larger Haar unitary.

2.1 Interpreting and Generalizing Ma-Huang's Path Recording Framework.

Before we recall the isometries described by [MH24], we first set up some notation. A relation R is defined as a *multiset* $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$ of ordered pairs $(x_i, y_i) \in [N] \times [N]$, for some $N \in \mathbb{N}$. For any relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, we say that R is $\mathcal{D}$*-distinct* if the first coordinates of all elements are distinct, and *injective* or $\mathcal{I}$*-distinct* if the second coordinates are distinct. For a relation R, we use $\mathrm{Dom}(R)$ to denote the *set* $\mathrm{Dom}(R) := \{x : x \in [N], \exists y \text{ s.t. } (x, y) \in R\}$ and $\mathrm{Im}(R)$ to denote the *set* $\mathrm{Im}(R) := \{y : y \in [N], \exists x \text{ s.t. } (x, y) \in R\}$. For any relation $R = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, we use R^{-1} to denote the relation $R^{-1} := \{(y_1, x_1), \ldots, (y_t, x_t)\}$ obtained by swapping the coordinates of all elements in R. [1]

[1] For an $\mathcal{I}$-distinct or $\mathcal{D}$-distinct relation $L = \{(x_1, y_1), \ldots, (x_t, y_t)\}$, the corresponding *relation state* $|L\rangle$ is defined to be

$$|L\rangle := \frac{1}{\sqrt{t!}} \sum_{\pi \in \mathsf{Sym}_t} |x_{\pi^{-1}(1)}\rangle |y_{\pi^{-1}(1)}\rangle \ldots |x_{\pi^{-1}(t)}\rangle |y_{\pi^{-1}(t)}\rangle.$$

In [MH24], relation states are defined for arbitrary relations, whereas we will not require them in this work.

To understand the path recording framework in [MH24], we start by thinking about what querying a Haar unitary looks like. We start by thinking about only forward queries to the Haar unitary. Since a Haar unitary is highly scrambling, a single query to a Haar unitary on any state returns a maximally mixed state. [MH24] notices that given half of a maximally entangled state, it looks like a maximally mixed state.
Even on multiple queries to a Haar unitary, it acts almost like returning maximally mixed states except that if the query is made on the same state, the output should pass the swap test and while on orthogonal states, the result should be orthogonal (pass swap test with only half probability). Hence, even while returning a maximally mixed state, we want to associate these to the input. [MH24] proposes the following: On any input, create a maximally entangled pair, return one half of this pair in the query register and save the other half in the purification register labeled by the input. Formally, define the following operator: for any injective relations R,

$$\mathsf{PR} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{R}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{y \notin \mathrm{Im}(R)} |y\rangle_{\mathsf{A}}|R \cup \{(x,y)\}\rangle_{\mathsf{R}}.$$

[MH24] shows in essence that querying PR simulated querying a Haar unitary. Notice that this seems to follow our intuition, as we can see that $|y\rangle$ returned in the query register is almost maximally entanged with a $|y\rangle$ in the purification register.
To extend this to both forward and inverse queries to the Haar unitary, we can think of the following intuition: The forward and backward queries to a Haar unitary look almost like independent Haar unitaries except if an inverse query is made on the output of a forward query, we should invert the forward query. In purification sense, we can do this as follows: Instantiate almost independent purification for forward and inverse queries. When an inverse query is made, check if the input is the output of a forward query (which looks like being maximally entagled with the purification), if it is, invert the query (which looks like returning the label). Else apply the independent Haar unitary corresponding to the inverse query. To formalise this, we do the following:
We define the following two operators (which are also partial isometries) such that for any relations L, R,

$$V_L : |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R^{-1})|}} \sum_{y \notin \mathrm{Im}(L\cup R^{-1})} |y\rangle_{\mathsf{A}}|L \cup \{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

$$V_R : |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{N-|\mathrm{Dom}(L\cup R^{-1})|}} \sum_{y \notin \mathrm{Dom}(L\cup R^{-1})} |y\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R \cup \{(x,y)\}\rangle_{\mathsf{T}}.$$

We define the following projector:

$$\Pi^L = V_L V_L^\dagger$$
$$\Pi^R = V_R V_R^\dagger$$

Using V_L and V_R, they define the following partial isometry:

$$V = \Pi^L \cdot V_L \cdot (I - \Pi^R) + (I - \Pi^L) \cdot V_R^\dagger \cdot \Pi^R.$$

They then showed that oracle access to a Haar random unitary U and its inverse $U^\dagger$ can be simulated by V and $V^\dagger$, respectively. In more detail, consider any oracle algorithm $\mathcal{A}$ described by a sequence of unitaries $(A_1, B_1, \ldots, A_t, B_t)$ such that $\mathcal{A}$ alternatively makes t forward queries and t inverse queries. Namely, the final state of $\mathcal{A}$ with oracle access to (fixed) $U, U^\dagger$ is denoted by

$$|\mathcal{A}_t^{U,U^\dagger}\rangle_{\mathsf{AB}} := \prod_{i=1}^{t} \left(U^\dagger B_i U A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}},$$

where A is the adversary's query register, B is the adversary's auxiliary register, and each A_i and B_i acts on AB. They then consider the final joint state of $\mathcal{A}$ and the purification after interacting with $V, V^\dagger$:

$$|\mathcal{A}_t^{V,V^\dagger}\rangle_{\mathsf{ABST}} := \prod_{i=1}^{t} \left(V^\dagger B_i V A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}.$$

[MH24] showed that ρ_{Haar} is $O(t^2/N^{1/8})$-close in trace distance to ρ_{MH}, where

$$\rho_{\mathsf{Haar}} := \mathop{\mathbb{E}}_{U\sim\mu_n}\left[|\mathcal{A}_t^{U,U^\dagger}\rangle\langle\mathcal{A}_t^{U,U^\dagger}|_{\mathsf{AB}}\right] \quad \text{and} \quad \rho_{\mathsf{MH}} := \mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|_{\mathsf{ABST}}\right),$$

and μ_n denotes the Haar measure over n-qubit unitaries and $N = 2^n$. We discuss the above in more detail in Section 4.1.

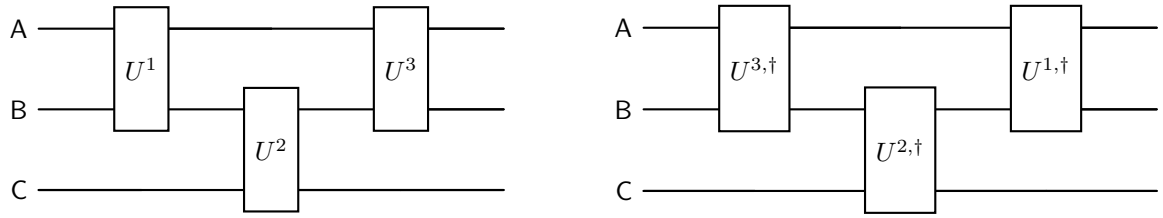
We give a generalisation of Path recording framework with the following intuition. The main idea is that in most applications of Path Recording, we don't want the maximal entanglement over all strings, and want some conditions on what strings are part of the maximal entanglement. We generally want this condition to depend on the current state, the input and some auxiliary information. We notice that as long as this condition doesn't eliminate too many strings, we find the resulting operator still simulates a Haar unitary well. We formalise how to do this in Section 4.2.

2.2 The Strong Gluing Theorem and Its Purification

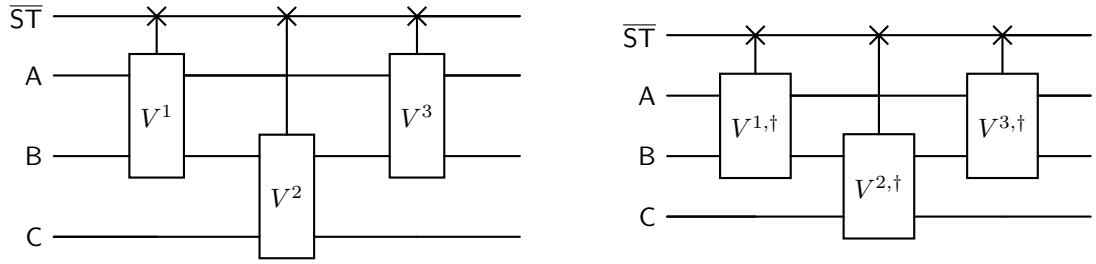
In our main result, we show that for three Haar random unitaries, U^1, U^2, and U^3, applying them in a shifted brickwork pattern, overlapping on some register B, yields an ensemble that is indistinguishable from a larger Haar random unitary to any adversary, with inverse access, making $\mathsf{poly}(|\mathsf{B}|)$ queries. That is, let $|\mathsf{A}|, |\mathsf{C}| = n$ and $|\mathsf{B}| = \lambda$, then

$$\mathop{\mathbb{E}}_{U^1,U^2,U^3\sim\mu_{n+\lambda}}\left[\mathcal{A}^{U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}},(U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}})^\dagger}\right] \approx \mathop{\mathbb{E}}_{O\sim\mu_{2n+\lambda}}\left[\mathcal{A}^{O_{\mathsf{ABC}},O^\dagger_{\mathsf{ABC}}}\right].$$

We start by writing the two oracles the adversary has access to, i.e. $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$.



The associated trivial purification using Path recording looks like the following:



Where $\overline{\mathsf{ST}}$ denotes the concatenation of the databases associated with the three Path Recording Framework (i.e. $\overline{\mathsf{ST}} = \mathsf{S}_1\mathsf{T}_1\mathsf{S}_2\mathsf{T}_2\mathsf{S}_3\mathsf{T}_3$).

Notice that the output of V^1 in the above is partially fed into V^2. Hence, if V^1 outputs one half of a maximally entangled state while saving the other half in L_1, then when this is fed into V^2, V^2 checks if the query is maximally entangled with anything in R_2, then because of monogamy of entanglement, since the query register is maximally entangled with something in L_1, it cannot be maximally entangled with something in R_2. Formally, this means

$$\|V_R^{2,\dagger}V_L^1\|_{\mathrm{op}} = \mathsf{negl}(\lambda).$$

Similarly,

$$\|V_R^{3,\dagger} V_L^2\|_{\text{op}} = \mathsf{negl}(\lambda).$$

Analyzing these, we get that the construction in effect does one of four operations. To see what these are, we start by stating the purified isometry.
We start by defining some projectors that correspond to checking entanglements (similar to Π^R in case of Path Recording):

$$\begin{aligned}
\Pi^{R,1} &= V_R^1 V_R^{1,\dagger} \\
\Pi^{R,12} &= V_R^1 V_R^2 V_R^{2,\dagger} V_R^{1,\dagger} \\
\Pi^{R,123} &= V_R^1 V_R^2 V_R^3 V_R^{3,\dagger} V_R^{2,\dagger} V_R^{1,\dagger}
\end{aligned}$$

Similarly, we define similar projectors in the opposite direction (similar to Π^L in case of Path Recording):

$$\begin{aligned}
\Pi^{L,3} &= V_L^3 V_L^{3,\dagger} \\
\Pi^{L,32} &= V_L^3 V_L^2 V_L^{2,\dagger} V_L^{3,\dagger} \\
\Pi^{L,321} &= V_L^3 V_L^2 V_L^1 V_L^{1,\dagger} V_L^{2,\dagger} V_L^{3,\dagger}
\end{aligned}$$

Then with these in mind, we define the glued purification as follows:

$$\begin{aligned}
V^{\mathsf{glued}} = &\left(\Pi^{L,321}\right) \cdot V_L^3 \cdot V_L^2 \cdot V_L^1 \cdot \left(I - \Pi^{R,1}\right) \\
&+ \left(\Pi^{L,32} - \Pi^{L,321}\right) \cdot V_L^3 \cdot V_L^2 \cdot V_R^{1,\dagger} \cdot \left(\Pi^{R,1} - \Pi^{R,12}\right) \\
&+ \left(\Pi^{L,3} - \Pi^{L,32}\right) \cdot V_L^3 \cdot V_R^{2,\dagger} \cdot V_R^{1,\dagger} \cdot \left(\Pi^{R,12} - \Pi^{R,123}\right) \\
&+ \left(I - \Pi^{L,3}\right) \cdot V_R^{3,\dagger} \cdot V_R^{2,\dagger} \cdot V_R^{1,\dagger} \cdot \left(\Pi^{R,123}\right)
\end{aligned}$$

Operationally, the V^{glued} works as follows:

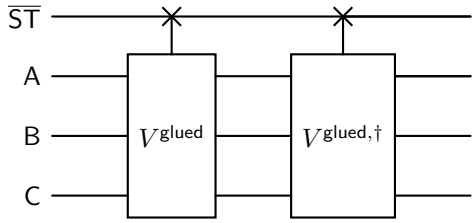
- Check if the query register is in the output of $V_R^1 \cdot V_R^2 \cdot V_R^3$, if it is, invert these queries.
- Else, check if the query register is in the output of $V_R^1 \cdot V_R^2$, if it is, invert these queries and apply V_L^3.
- Else, check if the query register is in the output of V_R^1, if it is, invert this query and apply $V_L^3 \cdot V_L^2$.
- Else, apply $V_L^3 \cdot V_L^2 \cdot V_L^1$.

We show that querying the glued Haar unitary can be purified to querying V^{glued} and $V^{\mathsf{glued},\dagger}$. Notice that V^{glued} looks very similar to path recording, in the way that it checks how the query register is entangled to the purification, and depending on how it is entangled, does some operation (which is deleting some entangled pairs or adds some entangled pairs). We discuss this purification in more detail and provide proofs in Section 5.2.

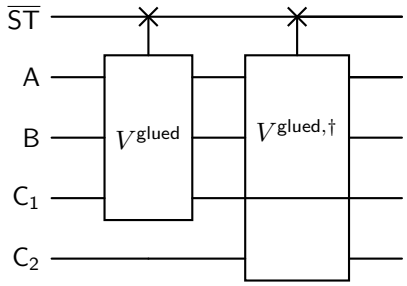
2.3 Analyzing Purification of Querying V^{glued}

Next, we try to study the structure of purification of querying V^{glued}. We know that V^{glued} and $V^{\mathsf{glued},\dagger}$ have different actions depending on how the query register is entangled with the purification. Notice that $V^{\mathsf{glued},\dagger}$ just acts as adding three entangled pairs unless the query the first part of the query is entangled with the L_3 database. If it is entanged, we have a different action. To see how these actions behave, we look at the following example: Let we just look at what happens if we query V^{glued} followed by $V^{\mathsf{glued},\dagger}$.

Example 1:

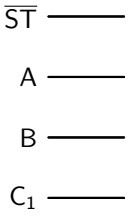


Example 2:

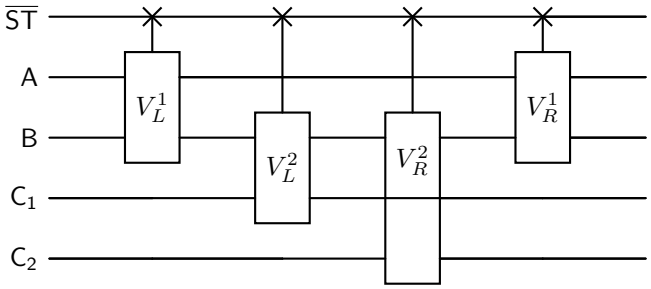


Looking at the operational definition of V^{glued} and $V^{\mathsf{glued},\dagger}$, we can simplify the above as:

Example 1:

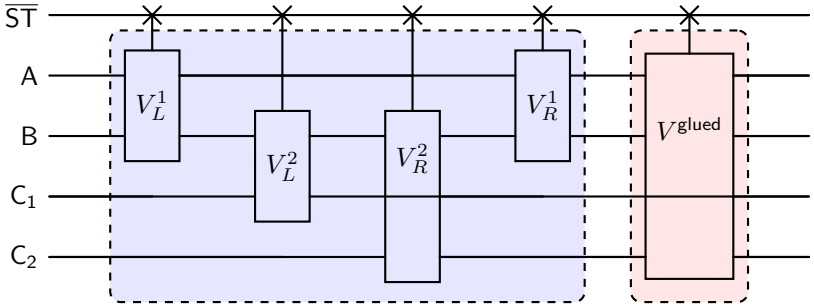


Example 2:

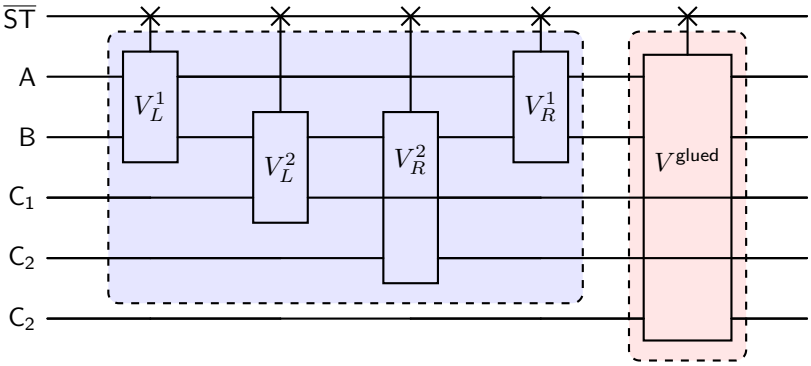


Notice next, if we query V^{glued} on Example 2, unless the V^{glued} matches up on AB, V^{glued} just adds 3 new entangled pairs. The more interesting case is when V^{glued} matches up on AB. This can again be seen as two cases, either the C register also matches up or it doesn't. Let's analyse these examples:

Example 2a:

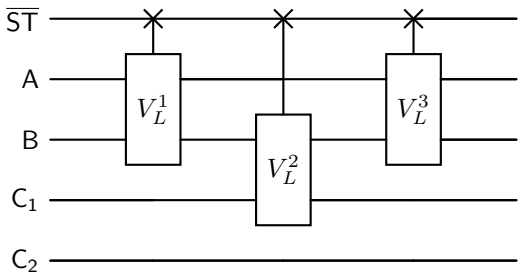


Example 2b:

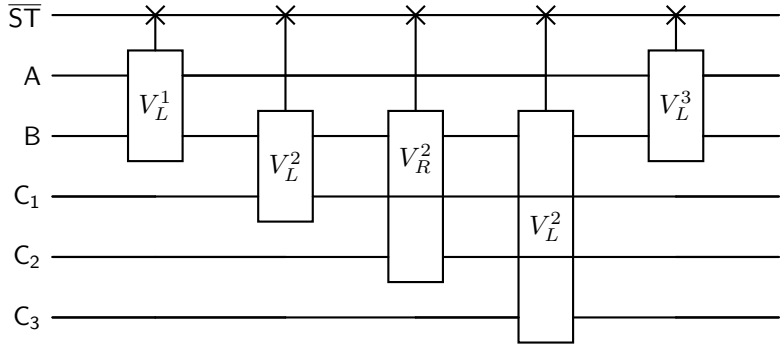


Again, expanding by definition of V^{glued}, we simplify as follows:

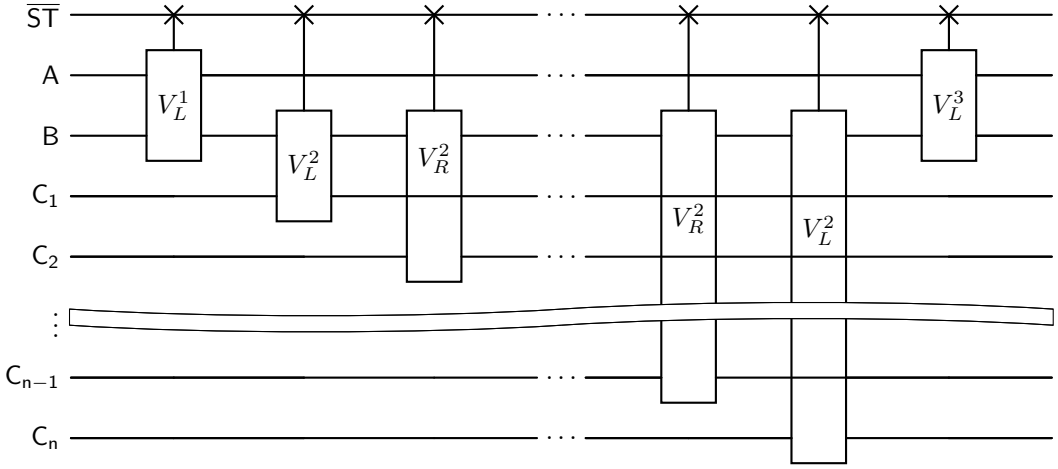
Example 2a:



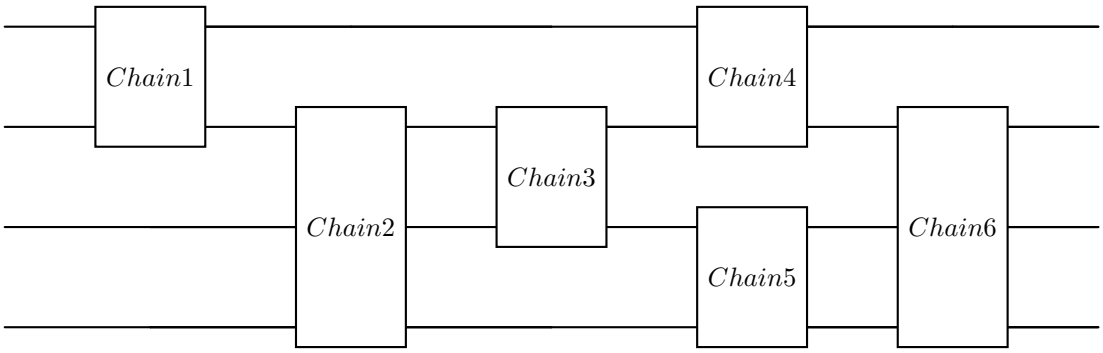
Example 2b:



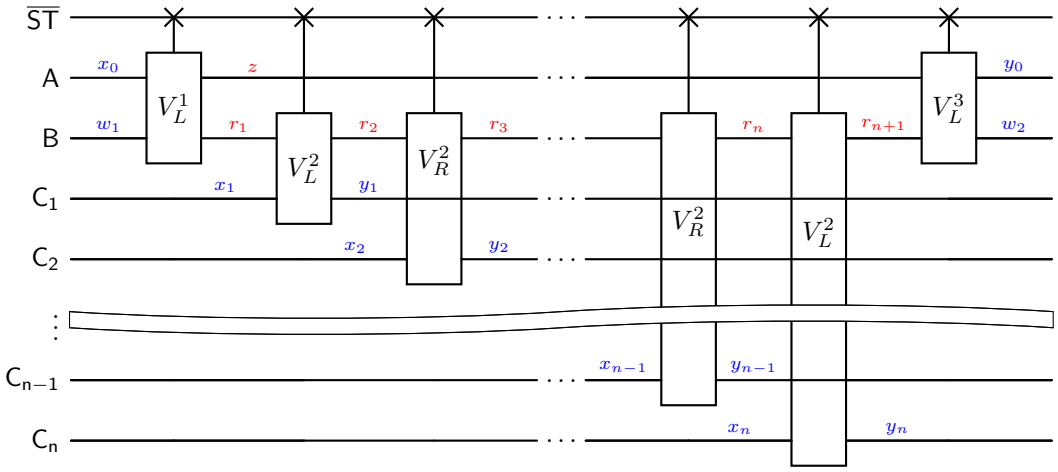
Notice that Example 2a is just equivalent to a single query to the first oracle. Exmple 2b has multiple unitaries chained together. Notice in all of the above two properties maintained. First, the register A which has only two gates applied to it (the first, e.g. V_L^1 and the last, e.g. V_L^3). Second, the register B has all gates applied to it. Whenever a wire is the output of V_L^i or V_R^i, it is a maximally entangled state, half of which is stored in the purification. Whenever a wire is the input of V_L^i or V_R^i, it is saved in the purification. Hence, all wire on register B creates a maximally entagled pair between two databases in the purification register. Similarly, the wire on A creates a maximally entagled pair between two databases in the purification register. Notice that we could extend the above example further to get multiple chained isometries. Pictorially, this looks as follows:



Thinking of the above as a "chain" of unitaries. Then we want to imagine any adversary's circuit as some "chains" strung together. We give an example below:



We want to formalise the intuition above, any adversary querying the oracles can be broken as multiple chains. To formalise the above intuition, start labeling the wires as follows:



Recalling the properties from before, we have the all isometries are applied to B, only the first and last isometry are applied to A and the labels in *red* are the maximally entangled pairs that only exist in the purification. Then on the above labels, the database register looks as follows:

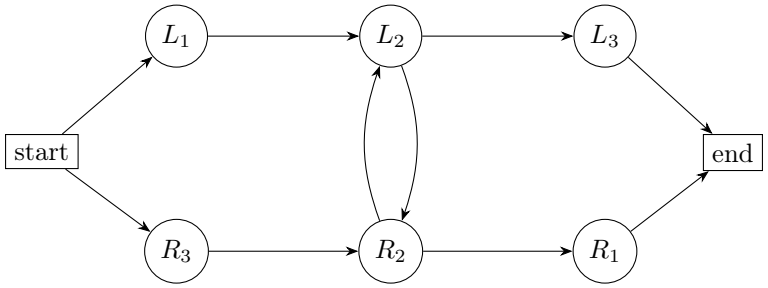
$$
\begin{aligned}
&|\{(x_0||w_1, z||r_1)\}\rangle_{\mathsf{S}_1}|\{\}\rangle_{\mathsf{T}_1} \\
&\otimes |\{(r_1||x_1, r_2||y_1), \ldots, (r_n||x_n, r_{n+1}||y_n)\}\rangle_{\mathsf{S}_2} \\
&\otimes |\{(r_2||x_2, r_3||y_2), \ldots, (r_{n-1}||x_{n-1}, r_n||y_{n-1})\}\rangle_{\mathsf{T}_2} \\
&\otimes |\{(z||r_{n+1}, y_0||w_2)\}\rangle_{\mathsf{S}_3}|\{\}\rangle_{\mathsf{T}_3}
\end{aligned}
$$

A better way to think about this database is modeling it as a graph. To do this, we do the following:

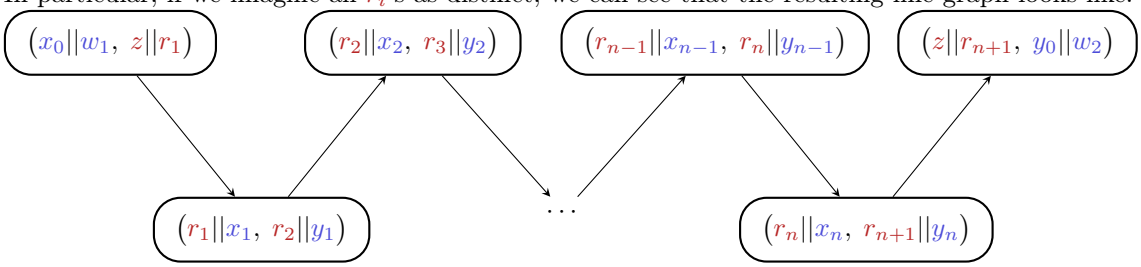
- **Defining Vertices**: For each tuple in the database, we add a vertex in the graph labelled by the touple.
- **Adding Edges from L_1 to L_2**: For any vertices v_1 coming from L_1, say the label of this vertex is $(x||w, z||r)$, and any vertex v_2 coming from L_2, say the label of this vertex is $(r'||x', \tilde{r}'||y')$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $r = r'$.
- **Adding Edges from L_2 to R_2**: For any vertices v_1 coming from L_2, say the label of this vertex is $(r||x, \tilde{r}||y)$, and any vertex v_2 coming from R_2, say the label of this vertex is $(r'||x', \tilde{r}'||y')$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $\tilde{r} = r'$.
- **Adding Edges from R_2 to L_2**: For any vertices v_1 coming from R_2, say the label of this vertex is $(r||x, \tilde{r}||y)$, and any vertex v_2 coming from L_2, say the label of this vertex is $(r'||x', \tilde{r}'||y')$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $\tilde{r} = r'$.

- **Adding Edges from L_2 to L_3**: For any vertices v_1 coming from L_2, say the label of this vertex is $(r||x, \tilde{r}||y)$, and any vertex v_2 coming from L_3, say the label of this vertex is $(z||r', y'||w)$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $\tilde{r} = r'$.
- **Adding Edges from R_3 to R_2**: For any vertices v_1 coming from R_3, say the label of this vertex is $(x||w, z||r)$, and any vertex v_2 coming from R_2, say the label of this vertex is $(r'||x', \tilde{r}'||y')$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $r = r'$. (These edges don't arise in the chain we look at in this example, but chains starting from $U_3^\dagger$ instead of U_1).
- **Adding Edges from R_2 to R_1**: For any vertices v_1 coming from R_2, say the label of this vertex is $(r||x, \tilde{r}||y)$, and any vertex v_2 coming from R_1, say the label of this vertex is $(z||r', y'||w)$. We add an edge from v_1 to v_2 if the vertices are "corelated", i.e. $\tilde{r} = r'$. (These edges don't arise in the chain we look at in this example, but chains ending from $U_1^\dagger$ instead of U_3).

Drawing edge structure, we get edges of the following form:



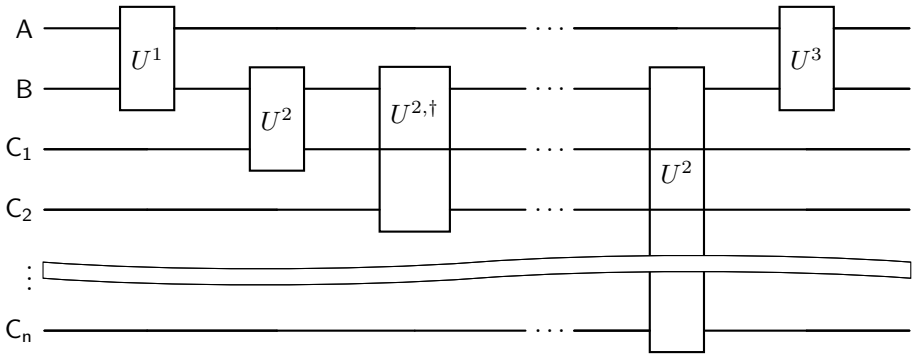
In particular, if we imagine all r_i's as distinct, we can see that the resulting line graph looks like:



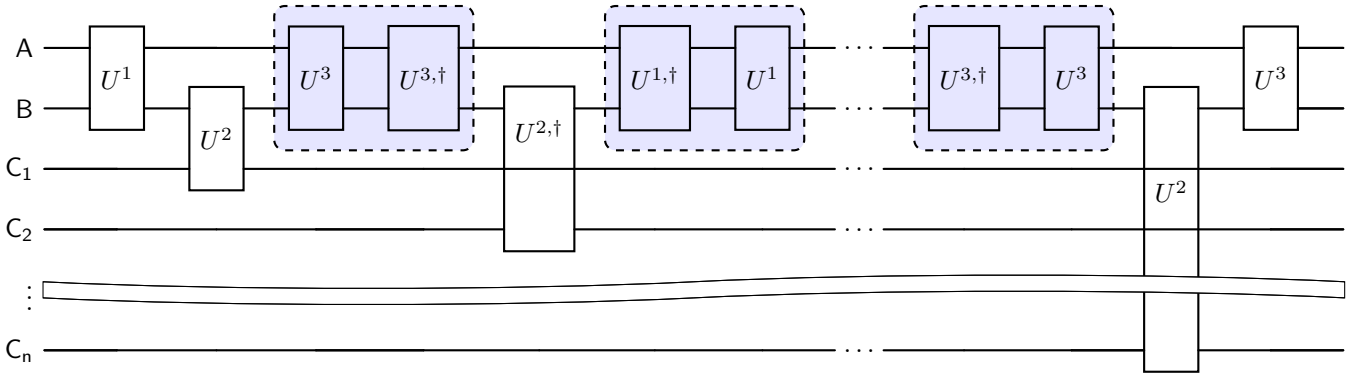
If we imagine any adversary's circuit as some "chains" strung together (recall the example from before), then corresponding to each chain, we get a disjoint line graph, and the database register corresponds to the union of databases corresponding to these disjoint line graphs. Also notice that all the labels in *red* are maximally entangled pairs which exist fully in the purification register. Hence, given the *blue* labels, we can completely identify the purification states. We refer the reader to Section 6 to see how we formalise the above.

2.4 Simulating the Larger Haar Unitary

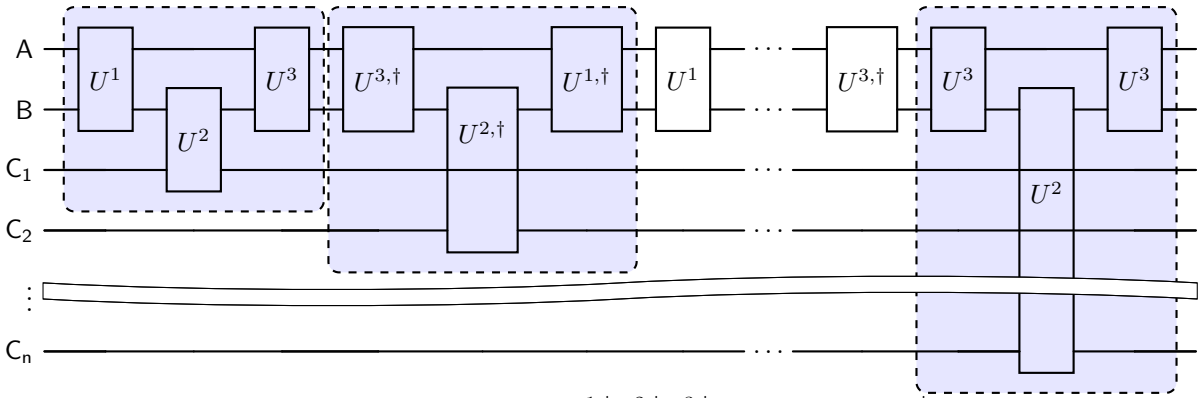
Now that we know that the adversary's query structure can be broken into disjoint chains. To see how to simulate the larger Haar unitary, we will first see what a single disjoint chain looks like and then see what a corresponding database register looks like. To start, we again consider a chain as example:



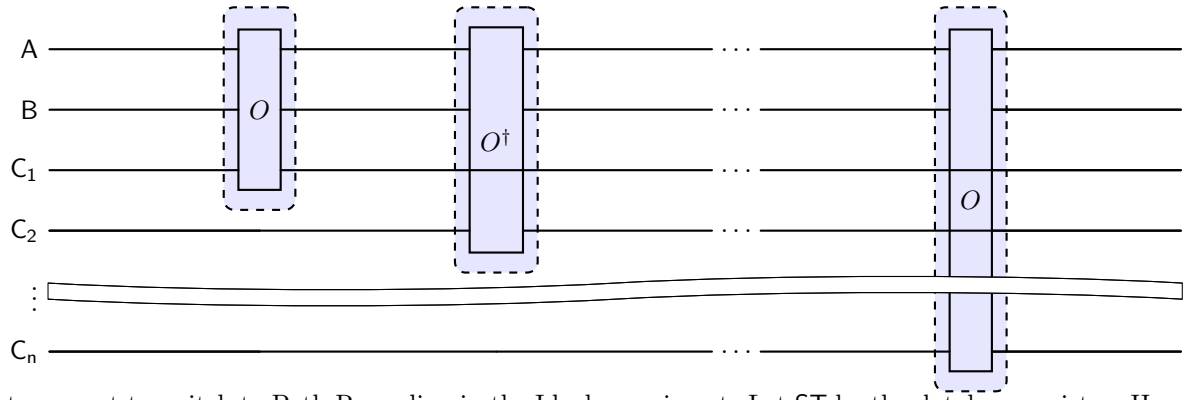
We know that in the Ideal experiment, we replace $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$ with O_{ABC} and $O^\dagger_{\mathsf{ABC}}$, respectively. To do this, we insert dummy unitaries in the abvoe chain. Particularly, we insert a $U^3U^{3,\dagger}$ between U^2 and $U^{2,\dagger}$ and we insert a $U^{1,\dagger}U^1$ between $U^{2,\dagger}$ and U^2. Then the above chain looks like:



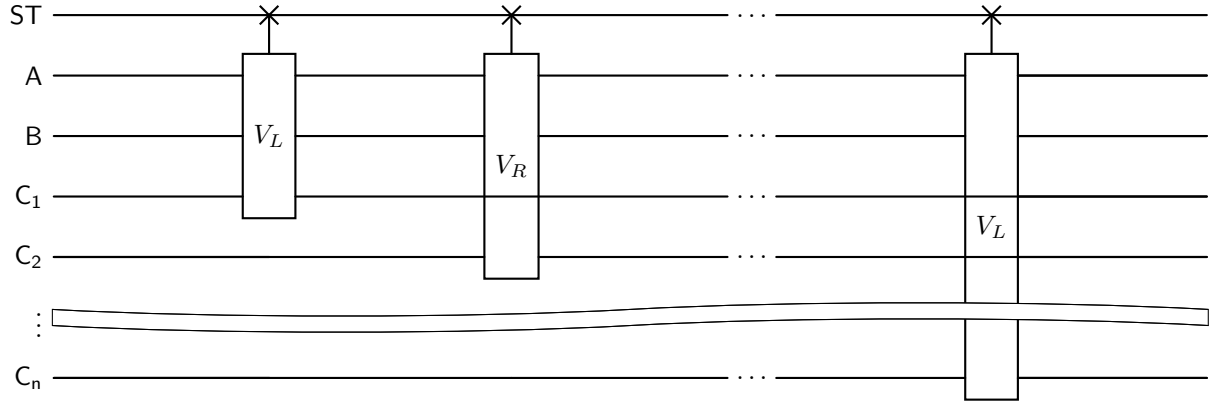
Notice that doing this, each component of the chain can be seen as queries to $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$. In particular, the chain looks like alternating queries to $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$. Hence, our example looks as follows:



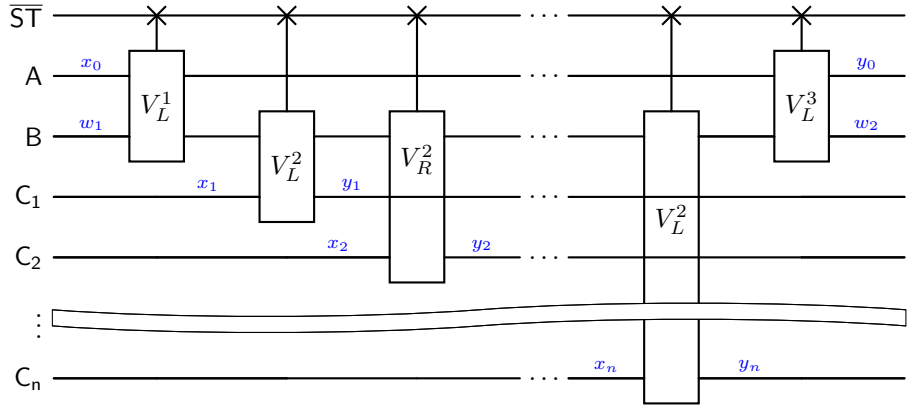
In the Ideal experiment, we replace $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$ with O_{ABC} and $O^\dagger_{\mathsf{ABC}}$, respectively. Hence, the chain becomes alternating queries to O_{ABC} and $O^\dagger_{\mathsf{ABC}}$. Hence, our example looks as follows:



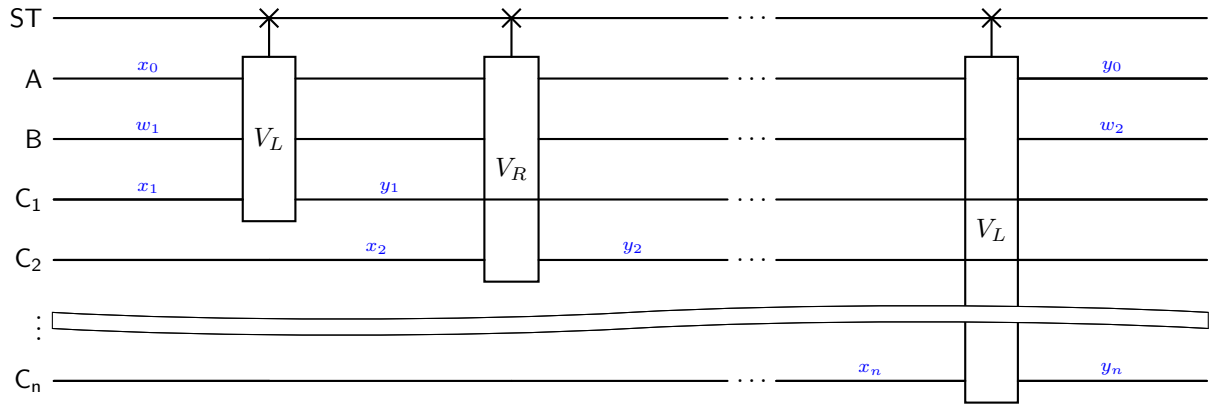
Next we want to switch to Path Recording in the Ideal experiment. Let ST be the database register. Hence, we switch O_{ABC} with V_L and $O^\dagger_{\mathsf{ABC}}$ with V_R. Hence, our example looks like:



To show that the Ideal experiment is close to the Real experiment, we define a simulator isometry that maps the database register in the Real case to the database register in the Ideal case. To see what this isometry looks like, we first add labels to both the experiments. Recalling the *blue* labels for the Real experiment as below:



Recall that the purification state can completely be identified by the *blue* labels. Similarly, we add these labels to the Ideal experiment as below:



Notice that in the above we skip the intermediate labels on the AB, this is because these are again maximally entangeled pairs completely existing in the database register. Finally, analyzing the database state from the Ideal experiment above and the real experiment from before we can define the simulator isometry (we call this isometry $\mathcal{O}_{\mathsf{comp}}$). To see how this is formally defined, we refer the reader to Section 7.2.

2.4.1 Bounding "Progress Measure"

The main challenge in demonstrating that $\mathcal{O}_{\mathsf{comp}}$ approximately maps the state in the real case close to the one in the ideal case is the difficulty of obtaining a simple closed-form expression, as was possible in the inverseless setting (see [MH24], Appendix C). Instead, we draw inspiration from the query-by-query analysis approach in the literature of the quantum random oracle model [Zha19; DFMS22]. Specifically, we do query-by-query analysis via defining the *progress measure* as the adversary's distinguishing advantage after each query.

A key step in our analysis is to show that, for any state $|\psi\rangle$ (generated using the real oracles), the process of first simulating the ideal database and then making a query to a ideal oracle (e.g., V^{fwd}) is close to making a query to a corresponding real oracle (e.g., $V^{3,\mathsf{fwd}}V^{2,\mathsf{fwd}}V^{1,\mathsf{fwd}}$) first and then simulating the database. Formally, we show that the following two states are close:

$$V\mathcal{O}_{\mathsf{comp}}|\psi\rangle \quad \text{and} \quad \mathcal{O}_{\mathsf{comp}}V^{\mathsf{glued}}|\psi\rangle\,,$$

which we establish by proving that the operator norm bound

$$\|(V\mathcal{O}_{\mathsf{comp}} - \mathcal{O}_{\mathsf{comp}}V^{\mathsf{glued}})\Pi_{\leq t}\|_{\mathrm{op}} = \mathsf{negl}(n)\,,$$

where $\Pi_{\leq t}$ denotes the projector acting on the database register that checks that the database is of poly-size. Similarly, we extend this argument to show inverse queries too, i.e.

$$\|(V^{\dagger}\mathcal{O}_{\mathsf{comp}} - \mathcal{O}_{\mathsf{comp}}V^{\mathsf{glued},\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = \mathsf{negl}(n)$$

To show this, we first show this in each of the subspaces and combine them to get the final result. Details for this can be found in Section 7.4. By establishing these bounds, we can inductively analyze the adversary's distinguishing advantage after each query (for details, see Section 7.3). Hence, we show that $\mathcal{O}_{\mathsf{comp}}$ approximately maps the state in the real case to the one in the ideal case.

3 Preliminaries

We denote the security parameter by λ. We assume that the reader is familiar with fundamentals of quantum computing, otherwise readers can refer to [NC10]. We refer to $\mathsf{negl}(\cdot)$ to be a negligible function.

3.1 Notation

Indexing and sets We use the notation $[n]$ to refer to the set $\{1, \ldots, n\}$. For a string $x \in \{0,1\}^{n+m}$, let $x_{[1:n]}$ to denote the first n bits of x. For $N, \ell \in \mathbb{N}$, we let $N^{\downarrow \ell} = \prod_{i=0}^{\ell-1}(N-i)$.

Sets and set operators For two binary strings of the same length a, b, we define $a \oplus b$ to be the xor of the two strings. For a set of binary strings A and a binary string b, we define the set $A \oplus b := \{a \oplus b \mid a \in A\}$. For two sets of same length binary strings A and B, we define the set $A \oplus B := \{a \oplus b \mid a \in A, b \in B\}$.

Set products and the symmetric group We use Sym_t to refer to the symmetric group over t elements (i.e. the group of all permutations of t elements). Given a set A and $t \in \mathbb{N}$, we use the notation A^t to denote the t-fold Cartesian product of A, and the notation A^t_{dist} to denote distinct subspace of A^t, i.e. the vectors in A^t, $\vec{y} = (y_1, \ldots, y_t)$, such that for all $i \neq j$, $y_i \neq y_j$. We also define the set $\{\vec{x}\} := \bigcup_{i \in [t]} \{x_i\}$.

Quantum states and distances A register R is a named finite-dimensional Hilbert space. If A and B are registers, then AB denotes the tensor product of the two associated Hilbert spaces. We denote by $\mathcal{D}(\mathsf{R})$ the density matrices over register R. For $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathsf{AB})$, we let $\mathrm{Tr}_{\mathsf{B}}(\rho_{\mathsf{AB}}) \in \mathcal{D}(\mathsf{A})$ denote the reduced density matrix that results from taking the partial trace over B. We denote by $\mathsf{TD}(\rho, \rho') = \frac{1}{2}\|\rho - \rho'\|_1$ the trace distance between ρ and ρ', where $\|X\|_1 = \mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$ is the trace norm. For two pure (and possibly subnormalized) states $|\psi\rangle$ and $|\phi\rangle$, we use $\mathsf{TD}(|\psi\rangle, |\phi\rangle)$ as a shorthand for $\mathsf{TD}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|)$. We also say that $A \preceq B$ if $B - A$ is a positive semi-definite matrix. For positive integers $t, d \in \mathbb{N}$ and a permutation $\sigma \in \mathsf{Sym}_t$, we let $P_d(\sigma)$ be the d^t-dimensional unitary that acts on registers $\mathsf{R}_1, \ldots, \mathsf{R}_t$ by permuting the registers according to σ. That is,

$$P_d(\sigma)|x_1\rangle_{\mathsf{R}_1} \otimes \cdots \otimes |x_t\rangle_{\mathsf{R}_t} := |x_{\sigma^{-1}(1)}\rangle_{\mathsf{R}_1} \otimes \cdots \otimes |x_{\sigma^{-1}(t)}\rangle_{\mathsf{R}_t}$$

for all $(x_1, \ldots, x_t) \in [d]^t$. We denote by $\mathcal{H}_n$ the Haar distribution over n-qubit states, and μ_n the Haar measure over n-qubit unitaries (i.e. the unique left and right invariant measure).

Relations Relations are an important part of the path recording framework, here we define relations between sets, as well as what it means to be injective and to take the inverse of a relation.

Definition 3.1 (Relation)**.** *A relation between two finite sets X and Y is a* multiset *of tuples $\{(x_i, y_i)\}_{i \in [t]}$ with $x_i \in X$ and $y_i \in Y$ for all $i \in [t]$.*

Definition 3.2 (Dom(R) and Im(R))**.** *For a relation $R = \{(x_i, y_i)\}_{i=1}^t$, define* $\mathrm{Dom}(R) = \{x_i\}_{i \in [t]}$ *and* $\mathrm{Im}(R) = \{y_i\}_{i \in [t]}$.

Definition 3.3 (Inverse of a relation)**.** *The inverse of a relation $R = \{(x_i, y_i)\}_{i=1}^t$ is the relation from Y to X defined by $R^{-1} = \{(y_i, x_i)\}_{i=1}^t$*

Definition 3.4 (Substrings)**.** *Given a string $x \in \{0,1\}^{2n+\lambda}$, let $x^{\mathfrak{l}(n)}$, $x^{\mathfrak{m}(\lambda)}$, and $x^{\mathfrak{r}(n)}$ represent the substring on the first n, middle λ, and final n bits respectively, so that $x = x^{\mathfrak{l}(n)}||x^{\mathfrak{m}(\lambda)}||x^{\mathfrak{r}(n)}$. Also define $\mathfrak{l}(\cdot)$, $\mathfrak{r}(\cdot)$ and $\mathfrak{m}(\cdot)$ for vectors and sets of strings as follows, let $S = \{x_i\}_{i \in [t]}$, then $S^{\mathfrak{l}(n)} = \{x_i^{\mathfrak{l}(n)}\}_{i \in [t]}$ and let $\overrightarrow{x} = (x_1, \ldots, x_t)$, then $\overrightarrow{x^{\mathfrak{l}(n)}} = (x_1^{\mathfrak{l}(n)}, \ldots, x_t^{\mathfrak{l}(n)})$.*[2]

3.2 Cryptographic Primitives

In this section, we define strong pseudorandom unitaries (strong PRU) [JLS18], which are the quantum equivalent of a pseudorandom function, in that an adversary can not distinguish the strong PRU from a truly Haar random unitary, even with inverse access to both.

[2]Let $\mathfrak{l}(\cdot)$, $\mathfrak{r}(\cdot)$ and $\mathfrak{m}(\cdot)$ can be defined on strings of other lengths too as first, last and middle substring of some length.

Definition 3.5 (Strong pseudorandom unitaries)**.** *We say that a quantum polynomial-size circuit G is a strong pseudorandom unitary if for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that for all λ,*

$$\left| \Pr_{k\leftarrow\{0,1\}^\lambda}\left[1 \leftarrow \mathcal{A}_\lambda^{G_\lambda(k),G_\lambda(k)^\dagger}\right] - \Pr_{\mathcal{U}\leftarrow\mu_{n(\lambda)}}\left[1 \leftarrow \mathcal{A}_\lambda^{\mathcal{U},\mathcal{U}^\dagger}\right]\right| \leq \epsilon(\lambda)\,.$$

In the QHROM*, both G_λ and $\mathcal{A}_\lambda$ have oracle access to an additional family of unitaries $\{U_\lambda\}_{\lambda\in\mathbb{N}}$ sampled from the Haar measure on λ qubits, and their inverses.*

3.3 Useful Lemmas

Here we present useful quantum lemmas that should be familiar to a reader well versed in quantum computation.

Lemma 3.6. *For any operator A and vector $|\psi\rangle$, $\||A|\psi\rangle\|_2 \leq \|A\|_{\mathrm{op}}\||\psi\rangle\|_2$.*

Lemma 3.7. *Let A be an operator and $\mathcal{B}$ be an orthonormal basis of the domain of A. If $A|i\rangle$ is orthogonal to $A|j\rangle$ for all $|i\rangle \neq |j\rangle \in \mathcal{B}$, then $\|A\|_{\mathrm{op}} = \max_{|i\rangle\in\mathcal{B}} \|A|i\rangle\|_2$.*

Lemma 3.8. *Let Π_1 and Π_2 be two projectors, then Π_1 and Π_2 commute if and only if their product is a projector.*

4 Path Recording and its Variants

In this section, we recall the path recording framework from [MH24]. We give a relatively more general way of looking at path recording and a general theorem for working with path recording. Finally, we define a variant of path recording that we will use throughout this paper.

4.1 Interpreting the Path Recording Framework

Here we recall the path recording framework from [MH24]. The path recording framework was defined as a purification of querying a Haar unitary.
We will start by stating and interpreting how to "simulate" just forward queries to a Haar unitary. Define the following operator: for any injective relations R,

$$\mathsf{PR} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{R}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{y\notin \mathrm{Im}(R)} |y\rangle_{\mathsf{A}}|R\cup\{(x,y)\}\rangle_{\mathsf{R}}.$$

[MH24] gives the following theorem that, in essence, shows that PR simulates forward queries to a Haar unitary.

Theorem 4.1 ([MH24, Theorem 5])**.** *For any t-query algorithm $\mathcal{A} = (A_1,\dots,A_t)$,*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U\sim\mu_n} |\mathcal{A}_t^U\rangle\langle\mathcal{A}_t^U|, \mathrm{Tr}_{\mathsf{R}}\left(|\mathcal{A}_t^{\mathsf{PR}}\rangle\langle\mathcal{A}_t^{\mathsf{PR}}|\right)\right) \leq O\left(\frac{t^2}{N^{1/2}}\right),$$

where $N = 2^n, |\mathcal{A}_t^U\rangle = \prod_{i=1}^t (UA_i)\,|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}$ and $|\mathcal{A}_t^{\mathsf{PR}}\rangle = \prod_{i=1}^t (\mathsf{PR}A_i)\,|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{R}}$.

To understand how PR works, we must first understand what querying a Haar unitary looks like. In general, querying a Haar unitary on any state gives a maximally mixed state. To understand how PR does this, we first notice that if you have a maximally entangled state $\frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle_{\mathsf{A}}|x\rangle_{\mathsf{B}}$ on two registers A and B, then if you only have access to one of these registers A or B, the state looks maximally mixed. PR uses this property to answer queries to a Haar unitary. In particular, on a query to PR, it saves the input in the

purification register and creates a maximally entangled pair, saves one half in the purification register (with the label as the input), and returns the other half as output on the query register.
The above idea works almost perfectly, except the operation we define above is not "reversible" (i.e. isn't an isometry or physically realizable). To fix this, we define PR as only creating an almost maximally entangled state and returns a half in the query register while saving the other in the purification register (labeled by the input) in a way that the operation is still "reversible".
Next [MH24] extends this idea to both forward and inverse queries to the Haar unitary. Define the following two operators: for any relations L, R,

$$V_L : |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{N - |\operatorname{Im}(L \cup R^{-1})|}} \sum_{y \notin \operatorname{Im}(L \cup R^{-1})} |y\rangle_{\mathsf{A}}|L \cup \{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

$$V_R : |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{N - |\operatorname{Im}(R \cup L^{-1})|}} \sum_{y \notin \operatorname{Im}(R \cup L^{-1})} |y\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R \cup \{(x,y)\}\rangle_{\mathsf{T}}.$$

Using V_L and V_R, they define the following partial isometry:

$$V = V_L \cdot (I - V_R \cdot V_R^\dagger) + (I - V_L \cdot V_L^\dagger) \cdot V_R^\dagger.$$

Theorem 4.2 ([MH24, Theorem 8])**.** *For any $2t$-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U \sim \mu_n} |\mathcal{A}_t^{U,U^\dagger}\rangle\langle\mathcal{A}_t^{U,U^\dagger}|, \operatorname{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|\right)\right) \leq O\left(\frac{t^2}{N^{1/8}}\right),$$

where $N = 2^n$, $|\mathcal{A}_t^{U,U^\dagger}\rangle = \prod_{i=1}^t \left(U^\dagger B_i U A_i\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}$ and $|\mathcal{A}_t^{V,V^\dagger}\rangle = \prod_{i=1}^t \left(V^\dagger B_i V A_i\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$.

To understand how V works, we use the following intuition: given access to the Haar unitary and its inverse, this almost looks like two independent Haar unitaries except if the inverse is queried on the output of a forward query, one must reverse the forward query. To do this, we can think of instantiating two independent forward query oracles V_L and V_R, except whenever the inverse oracle is queried, first we check if the input is entangled with something in the purification of V_L (i.e. was the output of V_L), if it is, return the associated label, else, just act as a forward query to V_R. Again, to make the above operator "reversible" (i.e. an isometry), we restrict how the "almost" maximally entangled state is defined.
Another way of looking at the above operation V that maps well to our intuition is the following: First define the following two projectors (as the projectors that check entanglement between the query register and the database register corresponding to V_L (and V_R, respectively)):

$$\Pi^L = V_L \cdot V_L^\dagger$$
$$\Pi^R = V_R \cdot V_R^\dagger$$

Then we can see that V can be written as

$$V = \Pi^L \cdot V_L \cdot (I - \Pi^R) + (I - \Pi^L) \cdot V_R^\dagger \cdot \Pi^R$$
$$V^\dagger = \Pi^R \cdot V_R \cdot (I - \Pi^L) + (I - \Pi^R) \cdot V_L^\dagger \cdot \Pi^L$$

Hence operationally, we interpret V as two branches:

- If the query register is maximally entangled with the database of V_R, apply $V_R^\dagger$,
- Else apply V_L.

In the above, we can think of first checking what subspace a query lies in and then applying the operation depending on this subspace.

4.2 A Generalization of the Path-Recording Framework

In this section, we will define a generalization of the Path-Recording Framework. The main intuition behind this generalization is that when applying V_L or V_R, one doesn't necessarily need a maximally entangled state, just a state with "enough" entanglement. Consider the following operation: Let V_L acts on some query register A and some purification register ST, and added an entry in the database saved in the register S. Then an operation V_L^f action on some query register A and some purification register ST and an ancilla register B, is close to V_L where f acts on ABST and outputs a "large enough" subset of $[N] \setminus \mathrm{Im}(S)$ over which we create the highly entangled state.
Formally, we define the following two operators:

$$V_L^{f_L}|x\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} = \frac{1}{\sqrt{|f_L(x,z,L,R)|}} \sum_{y \in f_L(x,z,L,R)} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L \cup \{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}}$$

$$V_R^{f_R}|x\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} = \frac{1}{\sqrt{|f_R(x,z,L,R)|}} \sum_{y \in f_R(x,z,L,R)} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\rangle_{\mathsf{S}}|R \cup \{(x,y)\}\rangle_{\mathsf{T}}$$

where for all x, z, L, R, $f_L(x,z,L,R) \subseteq [N] \setminus \mathrm{Im}(L)$ and $f_R(x,z,L,R) \subseteq [N] \setminus \mathrm{Im}(R)$.
Using above, we can define V^{f_L,f_R} as

$$V^{f_L,f_R} = V_L^{f_L} \cdot (I - V_R^{f_R} \cdot V_R^{f_R,\dagger}) + (I - V_L^{f_L} \cdot V_L^{f_L,\dagger}) \cdot V_R^{f_R,\dagger}.$$

Then we can show that as long as f_L and f_R give large enough subsets, to a poly query algorithm, V and V^{f_L,f_R} are indistinguishable. Formally, we have the following:

Lemma 4.3 (Generalized Path-Recording)**.** *Let f_L and f_R be functions such that for all x, z, L, R, $|L|+|R| \leq t$,*

$$\begin{aligned} f_L(x,z,L,R) &\subseteq [N] \setminus \mathrm{Im}(L) \\ f_R(x,z,L,R) &\subseteq [N] \setminus \mathrm{Im}(R) \\ \frac{|N - |f_L(x,z,L,R)| - t|}{|f_L(x,z,L,R)|} &\leq \delta \\ \frac{|N - |f_R(x,z,L,R)| - t|}{|f_R(x,z,L,R)|} &\leq \delta, \end{aligned}$$

For any $2t$-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,

$$\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}\rangle\langle\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}|\right), \mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|\right)\right) \leq 16t\sqrt{2\cdot(t+1)\cdot\delta},$$

where,

$$|\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}\rangle = \prod_{i=1}^{t} \left(V^{f_L,f_R,\dagger} B_i V^{f_L,f_R} A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$$

$$|\mathcal{A}_t^{V,V^\dagger}\rangle = \prod_{i=1}^{t} \left(V^\dagger B_i V A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$$

The proof of the above lemma is provided in Section A.

4.3 Modified Path Recording

In this subsection, we define a specific restriction on path recording that we will use later in the proof. We define the following restricted path recording operator as:

$$W_L^{\mathfrak{m}(\lambda)} : |x\rangle_{\mathsf{ABC}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathfrak{m}(\lambda)}|)}} \sum_{y : y^{\mathfrak{m}(\lambda)} \notin \mathrm{Im}(L\cup R)^{\mathfrak{m}(\lambda)}} |y\rangle_{\mathsf{ABC}}|L \cup \{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

$$W_R^{\mathfrak{m}(\lambda)} : |x\rangle_{\mathsf{ABC}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{2^{2n}(2^\lambda - |\operatorname{Im}(L\cup R)^{\mathfrak{m}(\lambda)}|)}} \sum_{y:y^{\mathfrak{m}(\lambda)}\notin \operatorname{Im}(L\cup R)^{\mathfrak{m}(\lambda)}} |y\rangle_{\mathsf{ABC}}|L\rangle_{\mathsf{S}}|R\cup\{(x,y)\}\rangle_{\mathsf{T}}.$$

Finally, define:

$$W^{\mathfrak{m}(\lambda)} = W_L^{\mathfrak{m}(\lambda)} \cdot (I - W_R^{\mathfrak{m}(\lambda)} \cdot W_R^{\mathfrak{m}(\lambda),\dagger}) + (I - W_L^{\mathfrak{m}(\lambda)} \cdot W_L^{\mathfrak{m}(\lambda),\dagger}) \cdot W_R^{\mathfrak{m}(\lambda),\dagger}$$

Then from Theorem 4.3, we have the following lemma.

Lemma 4.4. *For any $2t$-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,*

$$\mathsf{TD}\Big(\operatorname{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{W^{\mathfrak{m}(\lambda)},W^{\mathfrak{m}(\lambda),\dagger}}\rangle\langle\mathcal{A}_t^{W^{\mathfrak{m}(\lambda)},W^{\mathfrak{m}(\lambda),\dagger}}|\right), \operatorname{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|\right)\Big) \le O\left(\sqrt{\frac{t^3}{2^\lambda}}\right),$$

where $|\mathsf{ABC}| = 2n+\lambda$, $|\mathcal{A}_t^{W^{\mathfrak{m}(\lambda)},W^{\mathfrak{m}(\lambda),\dagger}}\rangle = \prod_{i=1}^t \left(W^{\mathfrak{m}(\lambda),\dagger} B_i W^{\mathfrak{m}(\lambda)} A_i\right)|0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$ and $|\mathcal{A}_t^{V,V^\dagger}\rangle = \prod_{i=1}^t \left(V^\dagger B_i V A_i\right)|0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$.

5 Glued Haar Unitary and its Purification

In this section, we present our glued Haar random unitary construction. We study an operation that acts on a purification register and mimics as if querying a glued Haar random unitary construction (similar to how path recording mimics a single Haar unitary). We'll call this operator the Glued Path Recording operator. Similar to how Path Recording has different actions on two different subspaces, Glued Path Recording has different actions on four different subspaces.

We start by looking at the naive way to achieve this by just replacing each Haar unitary in the glued construction with an instance of Path Recording Instance. Next, we will define a modification of the Path Recording oracle that is easier to work with in the proof. Finally, we define the four subspaces of interest and, using these subspaces, we define an operator that acts as the Glued Path Recording.

5.1 Glued Haar Unitary Construction

In this section, we present our construction of the Glued Haar Unitary. Let U^1, U^2 and U^3 be unitaries acting on $n+\lambda$ qubits, then we define the glued construction $G(U^1, U^2, U^3)$ acting on $2n+\lambda$ qubits as:

$$G(U^1, U^2, U^3)_{\mathsf{ABC}} = U^3_{\mathsf{AB}} \cdot U^2_{\mathsf{BC}} \cdot U^1_{\mathsf{AB}}$$

where $|\mathsf{A}| = |\mathsf{C}| = n$, $|\mathsf{B}| = \lambda$.

Throughout this paper, we show that an if U_1, U_2 and U_3 were sampled from the Haar distribution, then no poly query algorithm can distinguish between $G(U^1, U^2, U^3)$ and its inverse from a Haar random untary O and its inverse (where O acts on $2n+\lambda$ qubits).

We start by studying a purification of the construction $G(U^1, U^2, U^3)$. Notice that one can always just purify U^1, U^2, and U^3 individually using Path Recording. While this is a valid purification, it seems hard to work with. We give a more intuitive purification of the above construction in the next section.

5.2 Glued Path Recording

To get a more intuitive purification of the glued Haar unitary construction, we first look at how the construction behaves. Let we make a query to the construction, then we know, from the discussion in Section 4.1, that if this query is a previous output of U^1 (which in the purified view looks like checking entanglement), then U^1 inverts this query; else U^1 returns an extremely scrambled state.

Notice that the output of U^1 is (partially) fed into U^2. U^2 performs a similar check to see if the query is a previous output of U^2 or not. Interestingly, notice that if U^1 was returning an extremely scrambled state, then this state would almost certainly not be the output of a previous query to U^2.

To look at this in the purified view, if U^1 created a new maximally entangled pair and returns one half in the query register and saves the other half in the first database register, then when U^2 checks if this state is maximally entangled with something in the second database, this check almost always fails because by monogamy of entanglement we know that if the query register is maximally entangled with something in the first database, it cannot be maximally entangled with anything in the second database.
To formalise this intuition, we start defining some operations similar to path recording. In particular, corresponding to U^1 (and U^2 and U^3, respectively), we define a pair of operations (V_L^1, V_R^1) (and (V_L^2, V_R^2) and (V_L^3, V_R^3), respectively) where (V_L^1, V_R^1) (and (V_L^2, V_R^2) and (V_L^3, V_R^3), respectively) have corresponding purification registers $\mathsf{S_1T_1}$ (and $\mathsf{S_2T_2}$ and $\mathsf{S_3T_3}$, respectively).
Now we define some projectors that correspond to checking entanglements (similar to Π^R in Section 4.1):

$$\begin{aligned}\Pi^{R,1} &= V_R^1 V_R^{1,\dagger}\\ \Pi^{R,12} &= V_R^1 V_R^2 V_R^{2,\dagger} V_R^{1,\dagger}\\ \Pi^{R,123} &= V_R^1 V_R^2 V_R^3 V_R^{3,\dagger} V_R^{2,\dagger} V_R^{1,\dagger}\end{aligned}$$

Similarly, we define similar projectors in the opposite direction (similar to Π^L in Section 4.1):

$$\begin{aligned}\Pi^{L,3} &= V_L^3 V_L^{3,\dagger}\\ \Pi^{L,32} &= V_L^3 V_L^2 V_L^{2,\dagger} V_L^{3,\dagger}\\ \Pi^{L,321} &= V_L^3 V_L^2 V_L^1 V_L^{1,\dagger} V_L^{2,\dagger} V_L^{3,\dagger}\end{aligned}$$

Then with these in mind, we define the glued purification as follows:

$$\begin{aligned}V^{\mathsf{glued}} = &\left(\Pi^{L,321}\right)\cdot V_L^3\cdot V_L^2\cdot V_L^1\cdot\left(I-\Pi^{R,1}\right)\\ &+\left(\Pi^{L,32}-\Pi^{L,321}\right)\cdot V_L^3\cdot V_L^2\cdot V_R^{1,\dagger}\cdot\left(\Pi^{R,1}-\Pi^{R,12}\right)\\ &+\left(\Pi^{L,3}-\Pi^{L,32}\right)\cdot V_L^3\cdot V_R^{2,\dagger}\cdot V_R^{1,\dagger}\cdot\left(\Pi^{R,12}-\Pi^{R,123}\right)\\ &+\left(I-\Pi^{L,3}\right)\cdot V_R^{3,\dagger}\cdot V_R^{2,\dagger}\cdot V_R^{1,\dagger}\cdot\left(\Pi^{R,123}\right)\end{aligned}$$

Operationally, the V^{glued} works as follows:

- Check if the query register is in the output of $V_R^1\cdot V_R^2\cdot V_R^3$, if it is, invert these queries.
- Else, check if the query register is in the output of $V_R^1\cdot V_R^2$, if it is, invert these queries and apply V_L^3.
- Else, check if the query register is in the output of V_R^1, if it is, invert this query and apply $V_L^3\cdot V_L^2$.
- Else, apply $V_L^3\cdot V_L^2\cdot V_L^1$.

One can see that V^{glued} has a structure that is similar to path recording while also following the intuition stated at the beginning. In fact using the intuition from the discussion above, we formally show the following:

Lemma 5.1. *For any $2t$-query algorithm $\mathcal{A}=(A_1,B_1,\ldots,A_t,B_t)$,*

$$\left\||\mathcal{A}^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}}-|\mathcal{A}^{V^3V^2V^1,(V^3V^2V^1)^\dagger}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}}\right\|_2=O\left(\frac{t^3}{2^\lambda}\right).$$

where $\overline{\mathsf{ST}}=\mathsf{S_1S_2S_3T_1T_2T_3}$, $|\mathsf{ABC}|=2n+\lambda$,

$$|\mathcal{A}_t^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle=\prod_{i=1}^{t}\left(V^{\mathsf{glued},\dagger}B_iV^{\mathsf{glued}}A_i\right)|0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}|\varnothing\rangle_{\mathsf{S_1}}|\varnothing\rangle_{\mathsf{T_1}}|\varnothing\rangle_{\mathsf{S_2}}|\varnothing\rangle_{\mathsf{T_2}}|\varnothing\rangle_{\mathsf{S_3}}|\varnothing\rangle_{\mathsf{T_3}}$$

and $|\mathcal{A}^{V^3V^2V^1,(V^3V^2V^1)^\dagger}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}}$ is defined similarly.

The proof of the above lemma is provided in Section B.

5.3 Modified Glued Path Recording

In this subsection, we define a specific restriction on the glued path recording that we will use later in the proof. We define the following restricted glued path recording operator as:
We first define the following

$$\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)=\mathrm{Im}(L_1\cup R_3)^{\mathfrak{r}(\lambda)}\bigcup\mathrm{Im}(L_2\cup R_2)^{\mathfrak{l}(\lambda)}\bigcup\mathrm{Dom}(L_2\cup R_2)^{\mathfrak{l}(\lambda)},$$

and

$$\mathrm{Im}_2^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)=\mathrm{Im}(L_3\cup R_1)^{\mathfrak{r}(\lambda)}.$$

Next, we define the following partial isometries:

$$\begin{aligned}
&V_L^{(1),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{r}(\lambda)}\notin\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|y\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}\\
&\qquad\otimes|L_1\cup\{(x^{\mathfrak{l}(n+\lambda)},y)\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&V_R^{(1),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_2^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{r}(\lambda)}\notin\mathrm{Im}_2^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|y\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}\\
&\qquad\otimes|L_1\rangle_{\mathsf{S}_1}|R_1\cup\{(x^{\mathfrak{l}(n+\lambda)},y)\}\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&V_L^{(2),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{l}(\lambda)}\notin\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|x^{\mathfrak{l}(n)}\rangle_{\mathsf{A}}|y\rangle_{\mathsf{BC}}\\
&\qquad\otimes|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\cup\{(x^{\mathfrak{r}(n+\lambda)},y)\}\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&V_R^{(2),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{l}(\lambda)}\notin\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|x^{\mathfrak{l}(n)}\rangle_{\mathsf{A}}|y\rangle_{\mathsf{BC}}\\
&\qquad\otimes|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\cup\{(x^{\mathfrak{r}(n+\lambda)},y)\}\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&V_L^{(3),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_2^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{r}(\lambda)}\notin\mathrm{Im}_2^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|y\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}\\
&\qquad\otimes|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\cup\{(x^{\mathfrak{l}(n+\lambda)},y)\}\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&V_R^{(3),\mathsf{mid}}|x\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\rangle_{\mathsf{T}_3}\\
&\quad=\frac{1}{\sqrt{2^n(2^\lambda-|\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)|)}}\sum_{\substack{y:\\ y^{\mathfrak{r}(\lambda)}\notin\mathrm{Im}_1^{\mathsf{mid}}(L_1,L_2,L_3,R_1,R_2,R_3)}}|y\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}\\
&\qquad\otimes|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|L_3\rangle_{\mathsf{S}_3}|R_3\cup\{(x^{\mathfrak{l}(n+\lambda)},y)\}\rangle_{\mathsf{T}_3}
\end{aligned}$$

We know by Theorem A.2 that for $i \in \{1,2,3\}$ and $X \in \{L,R\}$,

$$\|(V_X^i - V_X^{(i),\mathsf{mid}})\Pi_{\leq t}\|_{\mathrm{op}} = O\left(\sqrt{\frac{t^2}{2^\lambda}}\right).$$

The reason the above operators are defined this way will become clear in the next section. Basically, querying glued path recording using the above operators results in a mbetter-structuredured purification. We next define the modified path recording with the above operator.
Now we define some projectors that correspond to checking entanglements (similar to Section 5.2):

$$\begin{aligned}
\Pi^{\mathcal{R},1} &= V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \\
\Pi^{\mathcal{R},12} &= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
\Pi^{\mathcal{R},123} &= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}
\end{aligned}$$

Similarly, we define similar projectors in the opposite direction (similar to Section 5.2):

$$\begin{aligned}
\Pi^{\mathcal{L},3} &= V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} \\
\Pi^{\mathcal{R},32} &= V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger} V_L^{(3),\mathsf{mid},\dagger} \\
\Pi^{\mathcal{L},321} &= V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} V_L^{(2),\mathsf{mid},\dagger} V_L^{(3),\mathsf{mid},\dagger}
\end{aligned}$$

Then with these in mind, we define the glued purification as follows:

$$\begin{aligned}
W^{\mathsf{glued}} = &\left(\Pi^{\mathcal{L},321}\right) \cdot V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_L^{(1),\mathsf{mid}} \cdot \left(I - \Pi^{\mathcal{R},1}\right) \\
&+ \left(\Pi^{\mathcal{L},32} - \Pi^{\mathcal{L},321}\right) \cdot V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_R^{(1),\mathsf{mid},\dagger} \cdot \left(\Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12}\right) \\
&+ \left(\Pi^{\mathcal{L},3} - \Pi^{\mathcal{L},32}\right) \cdot V_L^{(3),\mathsf{mid}} \cdot V_R^{(2),\mathsf{mid},\dagger} \cdot V_R^{(1),\mathsf{mid},\dagger} \cdot \left(\Pi^{\mathcal{R},12} - \Pi^{\mathcal{R},123}\right) \\
&+ \left(I - \Pi^{\mathcal{L},3}\right) \cdot V_R^{(3),\mathsf{mid},\dagger} \cdot V_R^{(2),\mathsf{mid},\dagger} \cdot V_R^{(1),\mathsf{mid},\dagger} \cdot \left(\Pi^{\mathcal{R},123}\right)
\end{aligned}$$

Then we have the following:

Lemma 5.2. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

$$\left\| |\mathcal{A}^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}} - |\mathcal{A}^{W^{\mathsf{glued}},W^{\mathsf{glued},\dagger}}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}} \right\|_2 = O\left(\sqrt{\frac{t^4}{2^\lambda}}\right),$$

where $\overline{\mathsf{ST}} = \mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3$.

For ease of notation, we define the following projectors:

$$\begin{aligned}
\Pi^{\mathsf{I},1} &= I - \Pi^{\mathcal{R},1} \\
\Pi^{\mathsf{I},2} &= \Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12} \\
\Pi^{\mathsf{I},3} &= \Pi^{\mathcal{R},12} - \Pi^{\mathcal{R},123} \\
\Pi^{\mathsf{I},4} &= \Pi^{\mathcal{R},123}
\end{aligned}$$

6 Structure of Purification for W^{glued}

In this section, our main goal would be to understand the structure of purification when using glued path recording. To do this, we start by showing how the purification can be associated to a graph, how this graph is structured and can be parametrized. We then use these graphs to define "good" states. Once we have defined the good states, we study intersection of good states and the subspaces defined with respect to glued path recording. Finally, we show that querying glued path recording only leads to good states.
The main intuition behind studying the structure is the following: Looking at the operational definition of V^{glued} in Section 5.2, we can see that the queries can only be done in certain patterns. In particular, any output of V_L^2 is partially fed as input to a V_L^3. Similarly, whenever we try to invert V_L^3 (i.e. apply $V_L^{3,\dagger}$), it is followed by either inverting V_L^2 (i.e. apply $V_L^{2,\dagger}$) or applying V_R^2. We associate a graph with the database to keep track of these correlations (i.e. keep track of when the output of some operator is part fed as the input to another operation).

6.1 Graph associated with the Database

To study the structure of the purification when querying W^{glued} and $W^{\mathsf{glued},\dagger}$, we start by associating a graph to the database in the purification. To do this, we associate a vertex for each entry in the database. We label these vertices with the tuple in the database as well as what database it came from. Formally we do the following: Given $(L_1, L_2, L_3, R_1, R_2, R_3)$, we define the following vertex set:

$$\begin{aligned}
V_{L_1} &= \{(\mathfrak{l}_1, x, y) | (x, y) \in L_1\} \\
V_{L_2} &= \{(\mathfrak{l}_2, x, y) | (x, y) \in L_2\} \\
V_{L_3} &= \{(\mathfrak{l}_3, x, y) | (x, y) \in L_3\} \\
V_{R_1} &= \{(\mathfrak{r}_1, x, y) | (x, y) \in R_1\} \\
V_{R_2} &= \{(\mathfrak{r}_2, x, y) | (x, y) \in R_2\} \\
V_{R_3} &= \{(\mathfrak{r}_3, x, y) | (x, y) \in R_3\}\,.
\end{aligned}$$

Next we want to add edges to the graph. We add edges where we suspect that the output of a given query was partially fed as input to another query. Looking back at the operational definition of V^{glued} (in Section 5.2), we see that in some operations correlate various enties in this form. We define directed edges between such tuples as follows:

$$\begin{aligned}
E_{L_1L_2} &= \{(v_1, v_2) | v_1 = (\mathfrak{l}_1, x_1, y_1) \in V_{L_1}, v_2 = (\mathfrak{l}_2, x_2, y_2) \in V_{L_2}, {y_1}^{\mathfrak{r}(\lambda)} = {x_2}^{\mathfrak{l}(\lambda)}\} \\
E_{L_2L_3} &= \{(v_1, v_2) | v_1 = (\mathfrak{l}_2, x_1, y_1) \in V_{L_2}, v_2 = (\mathfrak{l}_3, x_2, y_2) \in V_{L_3}, {y_1}^{\mathfrak{l}(\lambda)} = {x_2}^{\mathfrak{r}(\lambda)}\} \\
E_{R_3R_2} &= \{(v_1, v_2) | v_1 = (\mathfrak{r}_3, x_1, y_1) \in V_{R_3}, v_2 = (\mathfrak{r}_2, x_2, y_2) \in V_{R_2}, {y_1}^{\mathfrak{r}(\lambda)} = {x_2}^{\mathfrak{l}(\lambda)}\} \\
E_{R_2R_1} &= \{(v_1, v_2) | v_1 = (\mathfrak{r}_2, x_1, y_1) \in V_{R_2}, v_2 = (\mathfrak{r}_1, x_2, y_2) \in V_{R_1}, {y_1}^{\mathfrak{l}(\lambda)} = {x_2}^{\mathfrak{r}(\lambda)}\} \\
E_{L_2R_2} &= \{(v_1, v_2) | v_1 = (\mathfrak{l}_2, x_1, y_1) \in V_{L_2}, v_2 = (\mathfrak{r}_2, x_2, y_2) \in V_{R_2}, {y_1}^{\mathfrak{l}(\lambda)} = {x_2}^{\mathfrak{l}(\lambda)}\} \\
E_{R_2L_2} &= \{(v_1, v_2) | v_1 = (\mathfrak{r}_2, x_1, y_1) \in V_{R_2}, v_2 = (\mathfrak{l}_2, x_2, y_2) \in V_{L_2}, {y_1}^{\mathfrak{l}(\lambda)} = {x_2}^{\mathfrak{l}(\lambda)}\}\,.
\end{aligned}$$

Finally, we this gives us the graph:

$$\begin{aligned}
V(L_1, L_2, L_3, R_1, R_2, R_3) &= \bigcup_{i=1}^{3} (V_{L_i} \cup V_{R_i}) \\
E(L_1, L_2, L_3, R_1, R_2, R_3) &= \bigcup_{i=1}^{2} \left(E_{L_iL_{i+1}} \cup E_{R_{i+1}R_i}\right) \cup E_{L_2R_2} \cup E_{R_2L_2} \\
G(L_1, L_2, L_3, R_1, R_2, R_3) &= (V(L_1, L_2, L_3, R_1, R_2, R_3), E(L_1, L_2, L_3, R_1, R_2, R_3))
\end{aligned}$$

6.2 Analyzing Structure of the Graph

Next we try to study the structure of this graph associated with the database. We know that we added an edge at every instance where we suspect that an output from some operator was partially fed into another operator as the input. Next, we will try to see "chains" of multiple operators where the output of one is fed as input to another. These would look like a path in the associated graph.
A path in the graph to a sequence of connected vertices $(v_1, v_2, \ldots, v_n)$ with edges (v_i, v_{i+1}). A graph is a line graph if all the vertices in the graph form a path and all edges in the graph are just part of the path. We say a graph is a linear forest if it is a disjoint union of line graphs. For any linear forest, let $\mathcal{P}(G)$ be the set of disjoint line graphs. For any $p \in \mathcal{P}(G)$, let $\mathsf{len}(p)$ denote the number of edges in p.
Looking back at the operational description of V^{glued}, operations always start with either V_L^1 or V_R^3. Similarly, operations always end with either V_L^3 or V_R^1. Hence, we can classify the lines in the linear forest associated to the database. Formally, we define the following classes of Line Graphs in G.

Definition 6.1 (Classes of Line Graphs in G)**.** *Given a collection of relations, $\vec{L} = (L_1, L_2, L_3), \vec{R} = (R_1, R_2, R_3)$, define the following sets:*

$$\mathcal{P}_{LL}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}(G(L_1, L_2, L_3, R_1, R_2, R_3)) | p_{\mathsf{start}} \in L_1, p_{\mathsf{end}} \in L_3\}$$
$$\mathcal{P}_{LR}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}(G(L_1, L_2, L_3, R_1, R_2, R_3)) | p_{\mathsf{start}} \in L_1, p_{\mathsf{end}} \in R_1\}$$
$$\mathcal{P}_{RL}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}(G(L_1, L_2, L_3, R_1, R_2, R_3)) | p_{\mathsf{start}} \in R_3, p_{\mathsf{end}} \in L_3\}$$
$$\mathcal{P}_{RR}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}(G(L_1, L_2, L_3, R_1, R_2, R_3)) | p_{\mathsf{start}} \in R_3, p_{\mathsf{end}} \in R_1\}$$

Next, notice that while part of the output of V_L^1 is fed into V_L^2, the other part of the output is fed to the last operator in the path. We refer the reader to figures in the Section 2.3. We formalise this to define good line in graphs:

Definition 6.2 (Good lines in G)**.** *Given a collection of relations, $\vec{L} = (L_1, L_2, L_3), \vec{R} = (R_1, R_2, R_3)$, define the following subsets of $\{\mathcal{P}_{LL}, \mathcal{P}_{LR}, \mathcal{P}_{RL}, \mathcal{P}_{RR}\}$:*

$$\mathcal{P}_{LL}^{\text{good}}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}_{LL}(\vec{L}, \vec{R}) \mid p_{\mathsf{start}} = (\mathfrak{l}_1, x_1, y_1), p_{\mathsf{end}} = (\mathfrak{l}_3, x_2, y_2), y_1^{\mathfrak{l}(n)} = x_2^{\mathfrak{l}(n)}\}$$
$$\mathcal{P}_{LR}^{\text{good}}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}_{LR}(\vec{L}, \vec{R}) \mid p_{\mathsf{start}} = (\mathfrak{l}_1, x_1, y_1), p_{\mathsf{end}} = (\mathfrak{r}_1, x_2, y_2), y_1^{\mathfrak{l}(n)} = x_2^{\mathfrak{l}(n)}\}$$
$$\mathcal{P}_{RL}^{\text{good}}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}_{RL}(\vec{L}, \vec{R}) \mid p_{\mathsf{start}} = (\mathfrak{r}_3, x_1, y_1), p_{\mathsf{end}} = (\mathfrak{l}_3, x_2, y_2), y_1^{\mathfrak{l}(n)} = x_2^{\mathfrak{l}(n)}\}$$
$$\mathcal{P}_{RR}^{\text{good}}(\vec{L}, \vec{R}) = \{p \in \mathcal{P}_{RR}(\vec{L}, \vec{R}) \mid p_{\mathsf{start}} = (\mathfrak{r}_3, x_1, y_1), p_{\mathsf{end}} = (\mathfrak{r}_1, x_2, y_2), y_1^{\mathfrak{l}(n)} = x_2^{\mathfrak{l}(n)}\}.$$

Next we can define a graph as good as graphs which are made of good line graphs.

Definition 6.3 (Good graphs)**.** *Given $L_1, L_2, L_3, R_1, R_2, R_3$, we say $G(L_1, L_2, L_3, R_1, R_2, R_3)$ is "good" if:*

1. *$G(L_1, L_2, L_3, R_1, R_2, R_3)$ is a linear forest.*
2. *All lines in $G(L_1, L_2, L_3, R_1, R_2, R_3)$ are either $\mathcal{P}_{LL}^{\text{good}}$, $\mathcal{P}_{LR}^{\text{good}}$, $\mathcal{P}_{RL}^{\text{good}}$ or $\mathcal{P}_{RR}^{\text{good}}$.*

6.3 Parametrizing Good Graphs

Now that we have a highly structured graph associated to the database, we try to define some notation to look at these graphs. We start by defining a parametrized form of good line graphs. We know that in good line graphs, part of the output label at any vertex is repeated in the adjacent vertex. We label these by r_i. We also know that the first and the last vector also share part of the label, we denote this with z. The other labels are made by x_i and y_i along with w_1, w_2. We refer the reader to figures in the Section 2.3. We formalise this representation below.

Definition 6.4 (Good line graph parametrization)**.** *Let p be a line in $\mathcal{P}_{LL}^{\text{good}}(\vec{L},\vec{R})$ for some collection $\vec{L}$ and $\vec{R}$, then we can write the line p as follows:*

$$p = \{(\mathfrak{l}_1, x_0||w_1, z||r_1), (\mathfrak{l}_2, r_1||x_1, r_2||y_1), (\mathfrak{r}_2, r_2||x_2, r_3||y_2), \ldots, (\mathfrak{l}_2, r_n||x_n, r_{n+1}||y_n), (\mathfrak{l}_3, z||r_{n+1}, y_0||w_2)\}\,.$$

Then we define the function

$$\mathfrak{p}(\mathcal{LL}, \vec{x}, \vec{y}, w_1, w_2, \vec{r}, z) = p\,,$$

where $\vec{x}$, $\vec{y}$ are $\mathsf{len}(p)$-length vectors of $n-\lambda$ bit strings, and $\vec{r}$ is a $\mathsf{len}(p)$-length vector of λ bit strings.

We similarly define the functions $\mathfrak{p}$ with the first index $\mathcal{LR}$, $\mathcal{RL}$ and $\mathcal{RR}$ for paths in $\mathcal{P}_{LR}^{\text{good}}(\vec{L},\vec{R})$, $\mathcal{P}_{RL}^{\text{good}}(\vec{L},\vec{R})$ and $\mathcal{P}_{RR}^{\text{good}}(\vec{L},\vec{R})$, respectively.
We extend the above formalization to a "good" graph (i.e. a disjoint union of good line graphs). We define the following parametrized representations of "good" graphs:

Definition 6.5 (Good graph parametrization)**.** *Given any "good" graph G, we define the following representation: Let*

$$G = \bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \left(\bigcup_i p_i^{XY} \right)$$

where $p_i^{\mathcal{LL}} = \mathfrak{p}(\mathcal{LL}, \overrightarrow{x^{\mathcal{LL},i}}, \overrightarrow{y^{\mathcal{LL},i}}, w_1^{\mathcal{LL},i}, w_2^{\mathcal{LL},i}, \overrightarrow{r^{\mathcal{LL},i}}, z^{\mathcal{LL},i})$, and similarly $p_i^{\mathcal{LR}}$, $p_i^{\mathcal{RL}}$ and $p_i^{\mathcal{RR}}$. Then we define $\overline{\mathcal{G}}$ as:

$$G = \overline{\mathcal{G}} \left(\bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \left(\bigcup_i \{(XY, \overrightarrow{x^{XY,i}}, \overrightarrow{y^{XY,i}}, w_1^{XY,i}, w_2^{XY,i}, \overrightarrow{r^{XY,i}}, z^{XY,i})\} \right) \right).$$

6.4 Defining Good Auxiliary States

Next we associate even more structure with the database state. In particular, we notice that the internal labels for each line graph (i.e. the $\overrightarrow{r}$'s and $\overrightarrow{z}$'s) exist as maximally entangled pairs, with one half in the output labels with respect to some operators and the other half in the input labels with respect to some other operator. These maximally entangled pairs can be sampled later and added into the database state. Formally, given some partial description of line graphs (i.e. all parameters except the $\overrightarrow{r}$'s and $\overrightarrow{z}$'s), we can sample the rest of the parameters and create a superposition over these. We will call these partial descriptions of line graphs a "state structure parameter".
We start by defining some notation to help us formalize the above intuition. We define "state structure parameter" notation as the following four sets:

- $S_{\mathcal{LL}} = \{\mathfrak{q}_i^{\mathcal{LL}}\}_i$, where $\mathfrak{q}_i^{\mathcal{LL}} = (\mathcal{LL}, \overrightarrow{x^{\mathcal{LL},i}}, \overrightarrow{y^{\mathcal{LL},i}}, w_1^{\mathcal{LL},i}, w_2^{\mathcal{LL},i})$ and $|\overrightarrow{x^{\mathcal{LL},i}}| = |\overrightarrow{y^{\mathcal{LL},i}}|$.
- $S_{\mathcal{LR}} = \{\mathfrak{q}_i^{\mathcal{LR}}\}_i$, where $\mathfrak{q}_i^{\mathcal{LR}} = (\mathcal{LR}, \overrightarrow{x^{\mathcal{LR},i}}, \overrightarrow{y^{\mathcal{LR},i}}, w_1^{\mathcal{LR},i}, w_2^{\mathcal{LR},i})$ and $|\overrightarrow{x^{\mathcal{LR},i}}| = |\overrightarrow{y^{\mathcal{LR},i}}|$.
- $S_{\mathcal{RL}} = \{\mathfrak{q}_i^{\mathcal{RL}}\}_i$, where $\mathfrak{q}_i^{\mathcal{RL}} = (\mathcal{RL}, \overrightarrow{x^{\mathcal{RL},i}}, \overrightarrow{y^{\mathcal{RL},i}}, w_1^{\mathcal{RL},i}, w_2^{\mathcal{RL},i})$ and $|\overrightarrow{x^{\mathcal{RL},i}}| = |\overrightarrow{y^{\mathcal{RL},i}}|$.
- $S_{\mathcal{RR}} = \{\mathfrak{q}_i^{\mathcal{RR}}\}_i$, where $\mathfrak{q}_i^{\mathcal{RR}} = (\mathcal{RR}, \overrightarrow{x^{\mathcal{RR},i}}, \overrightarrow{y^{\mathcal{RR},i}}, w_1^{\mathcal{RR},i}, w_2^{\mathcal{RR},i})$ and $|\overrightarrow{x^{\mathcal{RR},i}}| = |\overrightarrow{y^{\mathcal{RR},i}}|$.

Before defining the notation to study "good states", we define the following helper functions for "state structure parameter":

Definition 6.6. *Given a state structure parameter $\overline{S}$, with $\overline{S} = \bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} S_{XY}$ and $S_{\mathcal{LL}} = \{\mathfrak{q}_i^{\mathcal{LL}}\}_i$, $S_{\mathcal{LR}} = \{\mathfrak{q}_i^{\mathcal{LR}}\}_i$, $S_{\mathcal{RL}} = \{\mathfrak{q}_i^{\mathcal{RL}}\}_i$ and $S_{\mathcal{RR}} = \{\mathfrak{q}_i^{\mathcal{RR}}\}_i$. Define:*

- *For $X, Y \in \{\mathcal{L},\mathcal{R}\}$, $\mathsf{len}(S_{XY}) = \sum_{i\in|S_{XY}|} \mathsf{len}(\overrightarrow{x^{XY,i}})$ and $\mathsf{len}(\overline{S}) = \sum_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \mathsf{len}(S_{XY})$.*

- *For* $X, Y \in \{\mathcal{L}, \mathcal{R}\}$, $\mathsf{count}(S_{XY}) = |S_{XY}|$ *and* $\mathsf{count}(\overline{S}) = \sum_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \mathsf{count}(S_{XY})$.
- $\mathrm{Im}(\overline{S}) = \{w_2^{XY,i} | X, Y \in \{\mathcal{L}, \mathcal{R}\}, i\}$.

Before defining "Good States", we first impose an extra condition on state structure parameters.

Definition 6.7 (Good State Structure Parameter)**.** *Given a state parameter* $\overline{S}$*, with* $\overline{S} = \overline{S} = \bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} S_{XY}$ *and* $S_{\mathcal{LL}} = \{\mathfrak{q}_i^{\mathcal{LL}}\}_i$, $S_{\mathcal{LR}} = \{\mathfrak{q}_i^{\mathcal{LR}}\}_i$, $S_{\mathcal{RL}} = \{\mathfrak{q}_i^{\mathcal{RL}}\}_i$ *and* $S_{\mathcal{RR}} = \{\mathfrak{q}_i^{\mathcal{RR}}\}_i$*. We say* $\overline{S}$ *is a good state parameter if* $|\mathrm{Im}(\overline{S})| = \mathsf{count}(\overline{S})$.

Finally, we define "good states":

Definition 6.8 (Good States)**.** *Given* $\overline{S} = \bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} S_{XY}$ *with* $S_{\mathcal{LL}} = \{(\mathcal{LL}, \overrightarrow{x^{\mathcal{LL},i}}, \overrightarrow{y^{\mathcal{LL},i}}, w_1^{\mathcal{LL},i}, w_2^{\mathcal{LL},i})\}_i$ *and similarly* $S_{\mathcal{LR}}$, $S_{\mathcal{RL}}$ *and* $S_{\mathcal{RR}}$ *with* $a = \mathsf{count}(\overline{S})$ *and* $b = \mathsf{len}(\overline{S})$*. Let, for* $X, Y \in \{\mathcal{L}, \mathcal{R}\}$, $z^{XY,i} \in \{0,1\}^\lambda$ *and* $\{\overrightarrow{r^{XY,i}}\}_{X,Y,i} \in \{0,1\}^{bn}_{\mathrm{dist}}$*. Say* $Z = \{z^{XY,i}\}_{X,Y,i}$ *and* $R = \{\overrightarrow{r^{XY,i}}\}_{X,Y,i}$*. Define* $\mathbb{G}$ *as the following notation:*

$$\mathbb{G}(\overline{S}, R, Z) = \overline{\mathcal{G}}\Bigg(\bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \{(XY, \overrightarrow{x^{XY,i}}, \overrightarrow{y^{XY,i}}, w_1^{XY,i}, w_2^{XY,i}, \overrightarrow{r^{XY,i}}, z^{XY,i})\}_i\Bigg)$$

Then we define the following state (defining notation $\mathfrak{G}$*):*

$$|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}} = \frac{1}{\sqrt{2^{an}(2^\lambda)\dots(2^\lambda - b + 1)}} \sum_{\substack{Z\in\{0,1\}^{an} \\ R\in\left(\{0,1\}^\lambda\right)^b_{\mathrm{dist}}}} |\mathbb{G}\left(\overline{S}, R, Z\right)\rangle_{\overline{\mathsf{ST}}},$$

where $|\mathbb{G}\left(\overline{S}, R, Z\right)\rangle_{\overline{\mathsf{ST}}}$ *denotes the* $|L_1\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|L_3\rangle_{\mathsf{S}_3}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|R_3\rangle_{\mathsf{T}_3}$ *corresponding to the* $\mathbb{G}\left(\overline{S}, R, Z\right)$.

Next, we define the projector on these good state as below:

Definition 6.9 (Good Projector)**.** *Define "good" projector as follows:*

$$\Pi^{\mathsf{Good}} = \sum_{\substack{\overline{S} \\ \overline{S} \text{ is good}}} |\mathfrak{G}(\overline{S})\rangle\langle\mathfrak{G}(\overline{S})|$$

6.5 Subspaces of Π^{Good}

Now that we have defined this projector Π^{Good}, we want to say that any algorithm querying V^{glued}, the purification mostly lies in the subspace defined by Π^{Good}. Before we approach this, know from Section 5.2, V^{glued} has different operations on different subspaces. We show how these subspaces behave with Π^{Good}. In particular, we know that V^{glued} has different operations on subspaces defined by projectors $\Pi^{\mathcal{R},1}$, $\Pi^{\mathcal{R},12}$ and $\Pi^{\mathcal{R},123}$. In particular, we show that $\Pi^{\mathcal{R},1}$, $\Pi^{\mathcal{R},12}$ and $\Pi^{\mathcal{R},123}$ commute with Π^{Good}.
From Theorem 3.8, we know that two projectors commute if and only if their product is a projector. Hence, to show that $\Pi^{\mathcal{R},1}$, $\Pi^{\mathcal{R},12}$ and $\Pi^{\mathcal{R},123}$ commute with Π^{Good}, we show that their product is a projector. To define these projectors, we first define the following vectors:

- Let $\overline{S'}$ be a good state parameter, let $X \in \{\mathcal{L}, \mathcal{R}\}$, $t \in \mathbb{N}$, $\overrightarrow{x} \in \{0,1\}^{(t+1)n}$ and $\overrightarrow{y} \in \{0,1\}^{tn}$ and $w_1 \in \{0,1\}^\lambda$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathsf{I},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle = \frac{1}{\sqrt{2^n(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ w'_2\in\left(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S'})\right)}} |y'_0, w'_2, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y'_0||\overrightarrow{y}, w_1, w'_2)\})\rangle_{\mathsf{ABS}\overline{\mathsf{ST}}}.$$

- Let $\overline{S'}$ be a good state parameter, let $t \in \mathbb{N}$, $X \in \{\mathcal{L}, \mathcal{R}\}$, $\overrightarrow{x} \in \{0,1\}^{(t+2)n}$ and $\overrightarrow{y} \in \{0,1\}^{tn}$ and $w \in \{0,1\}^{\lambda}$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle = \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ y'_1\in\{0,1\}^n \\ w'_2\in(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'}))}} |y'_0, w'_2, y'_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y'_0||\overrightarrow{y}||y'_1, w_1, w'_2)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}.$$

- Let $\overline{S'}$ be a good state parameter, let $\overrightarrow{x} \in \{0,1\}^{2n}$ and $w \in \{0,1\}^{\lambda}$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathfrak{l},3}_{\overline{S'},\overrightarrow{x},w_1}\rangle = \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ y'_1\in\{0,1\}^n \\ w'_2\in(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'}))}} |y'_0, w'_2, y'_1, \mathfrak{G}(\overline{S'} \cup \{(\mathcal{R}\mathcal{R}, \overrightarrow{x}, (y'_0, y'_1), w_1, w'_2)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}.$$

Notice that the above states defined are norm 1 and orthogonal.
The way to think about these states is the following:

- The space spanned by $|\chi^{\mathfrak{l},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle$ are the "Good" states in the image of $V_R^{(1),\mathsf{mid}}$ (i.e. in $\Pi^{\mathcal{R},1}$).
- The space spanned by $|\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle$ are the "Good" states in the image of $V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}$ (i.e. in $\Pi^{\mathcal{R},12}$).
- The space spanned by $|\chi^{\mathfrak{l},3}_{\overline{S'},\overrightarrow{x},w_1}\rangle$ are the "Good" states in the image of $V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}V_R^{(3),\mathsf{mid}}$ (i.e. in $\Pi^{\mathcal{R},123}$).

Similar to above, we also define $|\chi^{\mathfrak{r},i}\rangle$ as:

- Let $\overline{S'}$ be a good state parameter, let $X \in \{\mathcal{L}, \mathcal{R}\}$, $t \in \mathbb{N}$, $\overrightarrow{x} \in \{0,1\}^{(t+1)n}$ and $\overrightarrow{y} \in \{0,1\}^{tn}$ and $w_1 \in \{0,1\}^{\lambda}$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathfrak{r},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle = \frac{1}{\sqrt{2^n(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ w'_2\in(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'}))}} |y'_0, w'_2, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x}, y'_0||\overrightarrow{y}, w_1, w'_2)\})\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}.$$

- Let $\overline{S'}$ be a good state parameter, let $t \in \mathbb{N}$, $X \in \{\mathcal{L}, \mathcal{R}\}$, $\overrightarrow{x} \in \{0,1\}^{(t+2)n}$ and $\overrightarrow{y} \in \{0,1\}^{tn}$ and $w \in \{0,1\}^{\lambda}$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathfrak{r},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle = \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ y'_1\in\{0,1\}^n \\ w'_2\in(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'}))}} |y'_0, w'_2, y'_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x}, y'_0||\overrightarrow{y}||y'_1, w_1, w'_2)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}.$$

- Let $\overline{S'}$ be a good state parameter, let $\overrightarrow{x} \in \{0,1\}^{2n}$ and $w \in \{0,1\}^{\lambda}$, let $a = \mathsf{count}(\overline{S'})$, define

$$|\chi^{\mathfrak{r},3}_{\overline{S'},\overrightarrow{x},w_1}\rangle = \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \sum_{\substack{y'_0\in\{0,1\}^n \\ y'_1\in\{0,1\}^n \\ w'_2\in(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'}))}} |y'_0, w'_2, y'_1, \mathfrak{G}(\overline{S'} \cup \{(\mathcal{L}\mathcal{L}, \overrightarrow{x}, (y'_0, y'_1), w_1, w'_2)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}.$$

Finally, we have the following lemmas that formalize that $|\chi^i\rangle$'s span $\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},i}$:

Lemma 6.10. *We have the following:*

$$\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},1} = \sum_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1} |\chi^{\mathfrak{l},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathfrak{l},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}|$$

Lemma 6.11. *We have the following:*

$$\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},12} = \sum_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1} |\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}|$$

Lemma 6.12. *We have the following:*

$$\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},123} = \sum_{\overline{S'},\overrightarrow{x},w_1} |\chi^{\mathfrak{l},3}_{\overline{S'},\overrightarrow{x},w_1}\rangle\langle\chi^{\mathfrak{l},3}_{\overline{S'},\overrightarrow{x},w_1}|$$

Similar to above, we have $\Pi^{\mathsf{Good}}\Pi^{\mathcal{L},i}$ as a projector on space spanned by $|\chi^{\mathfrak{r},i}\rangle$. We give proofs for the above lemmas in Section C.

6.6 Action of W^{glued} on states in Π^{Good}

Now finally we can start talking about the action of W^{glued} on states in Π^{Good}. In particular, we want to show that querying W^{glued} on a state in Π^{Good} gives us states in Π^{Good}. Recall that:

$$\begin{aligned}
W^{\mathsf{glued}} = &\left(\Pi^{\mathcal{L},321}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_L^{(2),\mathsf{mid}}\cdot V_L^{(1),\mathsf{mid}}\cdot\left(I-\Pi^{\mathcal{R},1}\right)\\
&+\left(\Pi^{\mathcal{L},32}-\Pi^{\mathcal{L},321}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_L^{(2),\mathsf{mid}}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},1}-\Pi^{\mathcal{R},12}\right)\\
&+\left(\Pi^{\mathcal{L},3}-\Pi^{\mathcal{L},32}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_R^{(2),\mathsf{mid},\dagger}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},12}-\Pi^{\mathcal{R},123}\right)\\
&+\left(I-\Pi^{\mathcal{L},3}\right)\cdot V_R^{(3),\mathsf{mid},\dagger}\cdot V_R^{(2),\mathsf{mid},\dagger}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},123}\right)
\end{aligned}$$

Recall that from the previous section, we know exactly how to characterize good states in the four branches. In particular, we know that these states in various branches are spanned by $|\chi^{\mathfrak{l},i}\rangle$. We show the action of W^{glued} on $|\chi^{\mathfrak{l},i}\rangle$. In particular, we show the following:

Lemma 6.13. *Let $\overline{S}$ be some good state parameter and $x_0, x_1 \in \{0,1\}^n$, $w_1 \in \{0,1\}^\lambda$. Then we have the following:*

$$\begin{aligned}
V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}V_R^{(3),\mathsf{mid}}|x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle &= |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle\\
V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}|x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle &= |\chi^{\mathfrak{r},3}_{\overline{S},(x_0,x_1),w_1}\rangle
\end{aligned}$$

Lemma 6.14. *Let $\overline{S'}$ be a good state parameter, let $X \in \{\mathcal{L},\mathcal{R}\}$, $t \in \mathbb{N}$, $\overrightarrow{x} \in \{0,1\}^{(t+1)n}$ and $\overrightarrow{y} \in \{0,1\}^{tn}$, $x_0 \in \{0,1\}^n$ and $w_1 \in \{0,1\}^\lambda$. Then we have the following:*

$$\begin{aligned}
V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}V_L^{(3),\mathsf{mid},\dagger}|\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}} &= |\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_R^{(1),\mathsf{mid},\dagger}|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}} &= |\chi^{\mathfrak{r},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

We provide the proofs of the above lemmas in Section D. Finally, now since we understand the action of W^{glued} on basis states of the subspaces, we show that applying W^{glued} on good states gives good states. Formally, we show the following lemma:

Lemma 6.15. *Let $|\phi\rangle$ be some state such that $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$, then $(I-\Pi^{\mathsf{Good}})W^{\mathsf{glued}}|\phi\rangle = 0$.*

The proof of the above lemma is in Section D. Symmetrically, we can also get the lemma below.

Lemma 6.16. *Let $|\phi\rangle$ be some state such that $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$, then $(I-\Pi^{\mathsf{Good}})W^{\mathsf{glued},\dagger}|\phi\rangle = 0$.*

6.7 Purification of W^{glued} is Good

Let $\mathcal{A}$ denote a $2t$-query algorithm. For any unitaries U, define

$$|\mathcal{A}^{U,U^\dagger}\rangle = \prod_{i=1}^{t}\left(U^\dagger_{\mathsf{ABC}}B_iU_{\mathsf{ABC}}A_i\right)|0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}.$$

Lemma 6.17. *Let $\mathcal{A}$ denote a $2t$-query algorithm. Define*

$$|\psi\rangle = |\mathcal{A}^{W^{\mathsf{glued}},W^{\mathsf{glued},\dagger}}\rangle$$
$$|\phi\rangle = |\mathcal{A}^{\Pi^{\mathsf{Good}}W^{\mathsf{glued}},\Pi^{\mathsf{Good}}W^{\mathsf{glued},\dagger}}\rangle$$

Then

$$|\psi\rangle = |\phi\rangle$$

We get the above by Theorems 6.15 and 6.16.

7 Strong Gluing Theorem

In this section, we finally prove the Strong Gluing Theorem. We start by reducing the large Haar Unitary to the modified path recording and the glued construction to the modified glued path recording. Next we define an operator that simulates the purification in the large path recording from the purification in the gluing construction. To do this, we do a query-by-query analysis.
We now state the main result of this section.

Theorem 7.1 (Strong gluing of random unitaries)**.** *Let $\mathsf{A},\mathsf{B},\mathsf{C}$ be registers, and U^1_{AB}, U^2_{BC}, and U^3_{AB} be Haar random unitaries on $n+\lambda$ qubits, with B being λ qubits. Then for any t-query adversary $\mathcal{A}^{(\cdot)}$, the following holds*

$$\mathsf{TD}\left(\mathop{\mathbb{E}}_{U^1,U^2,U^3\leftarrow\mu_n}\left[|\mathcal{A}^{U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}},(U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}})^\dagger}\rangle\langle\mathcal{A}^{U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}},(U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}})^\dagger}|\right],\mathop{\mathbb{E}}_{O\leftarrow\mu_{2n-\lambda}}\left[|\mathcal{A}^{O_{\mathsf{ABC}},O^\dagger_{\mathsf{ABC}}}\rangle\langle\mathcal{A}^{O_{\mathsf{ABC}},O^\dagger_{\mathsf{ABC}}}|\right]\right)$$
$$= O\left(\frac{t^2}{2^{\lambda/2}}+\frac{t^3}{2^{\lambda}}+\frac{t^3}{2^{(n+\lambda)/8}}\right).$$

7.1 Proof of Theorem 7.1

Let $\mathcal{A}$ denote a strong PRU adversary. For any unitaries U, define

$$|\mathcal{A}^{U,U^\dagger}\rangle = \prod_{i=1}^{t}\left(U^\dagger_{\mathsf{ABC}}B_iU_{\mathsf{ABC}}A_i\right)|0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}.$$

We define the following hybrids (changes are denoted in red):

Hybrid $\mathbf{H}_1$: Define:

$$|u_1(O)\rangle = |\mathcal{A}^{O_{\mathsf{ABC}},O^\dagger_{\mathsf{ABC}}}\rangle.$$

Output

$$\mathop{\mathbb{E}}_{O\sim\mu_{2n+\lambda}}\left[|u_1(O)\rangle\langle u_1(O)|\right].$$

Hybrid $\mathbf{H}_2$: Define:

$$|u_2\rangle = |\mathcal{A}^{V,V^\dagger}\rangle,$$

where $V, V^\dagger$ acts on the registers ABCST and registers S and T are initialised as $|\varnothing\rangle$. Output

$$\mathrm{Tr}_{\mathsf{ST}}\left(|u_2\rangle\langle u_2|\right).$$

Hybrid $\mathbf{H}_3$: Define

$$|u_3\rangle = |\mathcal{A}^{W^{\mathrm{m}(\lambda)},W^{\mathrm{m}(\lambda),\dagger}}\rangle,$$

where $W^{\mathsf{fwd}}, W^{\mathsf{inv}}$ acts on the registers ABCST and registers S and T are initialised as $|\varnothing\rangle$. Output

$$\mathrm{Tr}_{\mathsf{ST}}\left(|u_3\rangle\langle u_3|\right).$$

Hybrid $\mathbf{H}_4$: Define

$$|u_4\rangle = |\mathcal{A}^{\Pi^{\mathsf{Good}}W^{\mathsf{glued}},\Pi^{\mathsf{Good}}W^{\mathsf{glued},\dagger}}\rangle,$$

where $\Pi^{\mathsf{Good}}W^{\mathsf{glued}}, \Pi^{\mathsf{Good}}W^{\mathsf{glued},\dagger}$ acts on the registers $\mathsf{ABCS}_1\mathsf{T}_1\mathsf{S}_2\mathsf{T}_2\mathsf{S}_3\mathsf{T}_3$ and registers S_i and T_i are initialised as $|\varnothing\rangle$ for $i \in [3]$. Output

$$\mathrm{Tr}_{\mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3}\left(|u_4\rangle\langle u_4|\right).$$

Hybrid $\mathbf{H}_5$: Define

$$|u_5\rangle = |\mathcal{A}^{W^{\mathsf{glued}},W^{\mathsf{glued},\dagger}}\rangle,$$

where $W^{\mathsf{glued}}, W^{\mathsf{glued},\dagger}$ acts on the registers $\mathsf{ABCS}_1\mathsf{T}_1\mathsf{S}_2\mathsf{T}_2\mathsf{S}_3\mathsf{T}_3$ and registers S_i and T_i are initialised as $|\varnothing\rangle$ for $i \in [3]$. Output

$$\mathrm{Tr}_{\mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3}\left(|u_5\rangle\langle u_5|\right).$$

Hybrid $\mathbf{H}_6$: Define

$$|u_6\rangle = |\mathcal{A}^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle,$$

where $V^{\mathsf{glued}}, V^{\mathsf{glued},\dagger}$ acts on the registers $\mathsf{ABCS}_1\mathsf{T}_1\mathsf{S}_2\mathsf{T}_2\mathsf{S}_3\mathsf{T}_3$ and registers S_i and T_i are initialised as $|\varnothing\rangle$ for $i \in [3]$. Output

$$\mathrm{Tr}_{\mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3}\left(|u_6\rangle\langle u_6|\right).$$

Hybrid $\mathbf{H}_7$: Define

$$|u_7(U^1,U^2,U^3)\rangle = |\mathcal{A}^{U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}},(U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}})^\dagger}\rangle.$$

Output

$$\mathop{\mathbb{E}}_{U_1,U_2,U_3\sim\mu_{n+\lambda}}\left[|u_7(U^1,U^2,U^3)\rangle\langle u_7(U^1,U^2,U^3)|\right].$$

Statistical Indistinguishability of Hybrids. We prove the closeness as follows:

Claim 7.2. *The trace distance between* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *is* $O\left(\frac{t^3}{N^{1/8}}\right)$.

Proof. By Theorem 4.2. □

Claim 7.3. *The trace distance between* $\mathbf{H}_2$ *and* $\mathbf{H}_3$ *is* $O\left(\sqrt{\frac{t^4}{2^\lambda}}\right)$.

Proof. By Theorem 4.4. □

Claim 7.4. *The trace distance between* $\mathbf{H}_3$ *and* $\mathbf{H}_4$ *is* $O\left(\frac{t^3}{2^\lambda}\right)$.

Proving Theorem 7.4 is the main technical step of this section. We begin by defining $\mathcal{O}_{\mathsf{comp}}$ in Section 7.2, which we then use to prove Theorem 7.4 in Section 7.3.

Claim 7.5. *The trace distance between* $\mathbf{H}_4$ *and* $\mathbf{H}_5$ *is* 0.

Proof. By Theorem 6.17. □

Claim 7.6. *The trace distance between* $\mathbf{H}_5$ *and* $\mathbf{H}_6$ *is* $O\left(\sqrt{\frac{t^4}{2^\lambda}}\right)$.

Proof. By Theorem 5.2. □

Claim 7.7. *The trace distance between* $\mathbf{H}_6$ *and* $\mathbf{H}_5$ *is* $O\left(\frac{t^3}{2^\lambda} + \frac{t^3}{2^{(n+\lambda)/8}}\right)$.

Proof. By Theorem 5.1 and Theorem 4.2. □

7.2 Defining $\mathcal{O}_{\mathsf{comp}}$

In this section, we will define $\mathcal{O}_{\mathsf{comp}}$, which maps the purification from querying $\Pi^{\mathsf{Good}}W^{\mathsf{glued}}$ to purification of $W^{\mathsf{m}(\lambda)}$. We know that the purification of $\Pi^{\mathsf{Good}}W^{\mathsf{glued}}$ is in the good subspace, hence is in the span of $|\mathfrak{G}(\overline{S})\rangle$. We start by thinking about what $\mathcal{O}_{\mathsf{comp}}$ should do for a single $|\mathfrak{G}(\overline{S})\rangle$.
The intuition towards defining $\mathcal{O}_{\mathsf{comp}}$ is the following: Given any path $\mathfrak{q} \in \overline{S}$, we know that it signifies multiple interweaving queries to $V_X^{(i),\mathsf{mid}}$ with outputs from one being partially fed as input into the next. We define $\mathcal{O}_{\mathsf{comp}}$ to convert these interweaving queries to $W^{\mathsf{m}(\lambda)}$ and $W^{\mathsf{m}(\lambda),\dagger}$. We refer the reader to figures in the Section 2.4.
Again, when we have interweaving queries to $W^{\mathsf{m}(\lambda)}$ and $W^{\mathsf{m}(\lambda),\dagger}$, we see that the output of one feeding into the exists as a maximally entangled pair between the two databases (similar to Section 6.4). Hence, we can sample these maximally entangled pairs and append them to a state structure parameter. Let's denote these by $\overrightarrow{u}$ and $\overrightarrow{v}$.
Formally, we define comp as below: Given $\mathfrak{q} = (\mathcal{LL}, \overrightarrow{x^{LL}}, \overrightarrow{y^{LL}}, w_1^{LL}, w_2^{LL}) \in \overline{S}$ with $\mathsf{len}(\mathfrak{q}) > 2$, then define for $\overrightarrow{u^{LL}} \in \{0,1\}^{(\mathsf{len}(\mathfrak{q})-1)n}, \overrightarrow{v^{LL}} \in \{0,1\}^{(\mathsf{len}(\mathfrak{q})-1)\lambda}$

$$
\begin{aligned}
&|\mathsf{comp}(\mathfrak{q}, \overrightarrow{u^{LL}}, \overrightarrow{v^{LL}})\rangle = \\
&\quad \big|\{(x_0^{LL}||w_1^{LL}||x_1^{LL}, u_1^{LL}||v_1^{LL}||y_1^{LL}), (u_2^{LL}||v_2^{LL}||x_3^{LL}, u_3^{LL}||v_3^{LL}||y_3^{LL}), \\
&\qquad \ldots, (u_{n-3}^{LL}||v_{n-3}^{LL}||x_{n-2}^{LL}, u_{n-2}^{LL}||v_{n-2}^{LL}||y_{n-2}^{LL}), (u_{n-1}^{LL}||v_{n-1}^{LL}||x_{n-1}^{LL}, y_0^{LL}||w_2^{LL}||y_{n-1}^{LL})\}\big\rangle \\
&\qquad \otimes |\{(u_1^{LL}||v_1^{LL}||x_2^{LL}, u_2^{LL}||v_2^{LL}||y_2^{LL}), \ldots, (u_{n-2}^{LL}||v_{n-2}^{LL}||x_{n-1}^{LL}, u_{n-1}^{LL}||v_{n-1}^{LL}||y_{n-1}^{LL})\}\rangle
\end{aligned}
$$

On any $\mathfrak{q} = (\mathcal{LL}, \overrightarrow{x^{LL}}, \overrightarrow{y^{LL}}, w_1^{LL}, w_2^{LL}) \in \overline{S}$ with $\mathsf{len}(\mathfrak{q}) = 2$, $\overrightarrow{u^{LL}} = (), \overrightarrow{v^{LL}} = ()$, then define

$$|\mathsf{comp}(\mathfrak{q}, \overrightarrow{u^{LL}}, \overrightarrow{v^{LL}})\rangle = |\{(x_0^{LL}||w_1^{LL}||x_1^{LL}, y_0^{LL}||w_2^{LL}||y_1^{LL})\}\rangle|\emptyset\rangle$$

We think of $\overrightarrow{u^{LL}}$ and $\overrightarrow{v^{LL}}$ the simulated A and B.
Similarly, define comp on $\mathfrak{q}$ with first element $\mathcal{LR}, \mathcal{RL}$ and $\mathcal{RR}$. Next, we define an operation that takes $\overline{S}$, a set of $\overrightarrow{u}$'s and $\overrightarrow{v}$'s, and give a combined database:
Formally, let $\overline{S}$ with $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$. Let $\mathcal{U} = \{\overrightarrow{u^i}\}_i \in \{0,1\}^{(b-a)n}$ and $\mathcal{V} = \{\overrightarrow{v^i}\}_i \in \{0,1\}^{(b-a)\lambda}$, then define

$$|\mathbb{F}(\overline{S}, \mathcal{U}, \mathcal{V})\rangle = |\bigcup_{\mathfrak{q}_i \in \overline{S}} \mathsf{comp}(\mathfrak{q}_i, \overrightarrow{u^i}, \overrightarrow{v^i})\rangle$$

Finally, we define $\mathcal{O}_{\mathsf{comp}}$

$$\mathcal{O}_{\mathsf{comp}}|\mathfrak{G}(\overline{S})\rangle = \frac{1}{\sqrt{2^{(b-a)n}\left((2^\lambda - a)\dots(2^\lambda - b + 1)\right)}} \sum_{\substack{\mathcal{U}\in\{0,1\}^{(b-a)n} \\ \mathcal{V}\in(\{0,1\}^\lambda\setminus \mathrm{Im}(\overline{S}))^{b-a}_{\mathrm{dist}}}} |\mathbb{F}(\overline{S},\mathcal{U},\mathcal{V})\rangle$$

We define the notation $\mathfrak{F}$ as

$$\mathcal{O}_{\mathsf{comp}}|\mathfrak{G}(\overline{S})\rangle = |\mathfrak{F}(\overline{S})\rangle$$

Then we prove that for each query, $\mathcal{O}_{\mathsf{comp}}$ simulates the database, i.e. we prove the following:

Lemma 7.8. *For any integer $t \geq 0$,*

- *Forward query:*

$$\left\| \left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi_{\leq t}\right\|_{\mathrm{op}} = O(t^2/2^\lambda)$$

- *Inverse query:*

$$\left\| \left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued},\dagger} - W^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi_{\leq t}\right\|_{\mathrm{op}} = O(t^2/2^\lambda)$$

We prove the above in Section 7.4 but before that we will finish proving Theorem 7.4 in Section 7.3 using Theorem 7.8.

7.3 Proof of Theorem 7.4: Closeness between $\mathbf{H}_3$ and $\mathbf{H}_4$

Denote the initial joint state in $\mathbf{H}_3$ by

$$|\psi_0\rangle := |0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}.$$

For $i \in [2t]$, denote the joint state right after the i-th query by

$$|\psi_i\rangle := \begin{cases} W^{\mathfrak{m}(\lambda)}A_{(i+1)/2}|\psi_{i-1}\rangle & , \text{if } i \equiv 1 \bmod 2 \\ W^{\mathfrak{m}(\lambda),\dagger}B_{i/2}|\psi_{i-1}\rangle & , \text{if } i \equiv 0 \bmod 2. \end{cases}$$

The output of $\mathbf{H}_3$ is

$$\mathrm{Tr}_{\mathsf{ST}}\left(|\psi_{2t}\rangle\langle\psi_{2t}|\right).$$

Similarly, denote the initial joint state in $\mathbf{H}_4$ by

$$|\phi_0\rangle := |0\rangle_{\mathsf{ABC}}|0\rangle_{\mathsf{D}}|\varnothing\rangle_{\mathsf{S}_1}|\varnothing\rangle_{\mathsf{T}_1}|\varnothing\rangle_{\mathsf{S}_2}|\varnothing\rangle_{\mathsf{T}_2}|\varnothing\rangle_{\mathsf{S}_3}|\varnothing\rangle_{\mathsf{T}_3}.$$

For $i \in [2t]$, denote the joint state right after the i-th query by

$$|\phi_i\rangle := \begin{cases} \Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2}|\phi_{i-1}\rangle & , \text{if } i \equiv 1 \bmod 2 \\ \Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}inv}}B_{i/2}|\phi_{i-1}\rangle & , \text{if } i \equiv 0 \bmod 2. \end{cases}$$

The output of $\mathbf{H}_4$ is

$$\mathrm{Tr}_{\mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3}\left(|\phi_{2t}\rangle\langle\phi_{2t}|\right).$$

We prove the following claim by induction: for $i \in [2t]$, $\|\mathcal{O}_{\mathsf{comp}}|\phi_i\rangle - |\psi_i\rangle\|_2 = O(i^3/2^\lambda)$.

- Base case: $\mathcal{O}_{\mathsf{comp}}|\phi_0\rangle = |\psi_0\rangle$.
- Induction hypothesis: Suppose $\|\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - |\psi_{i-1}\rangle\|_2 = O((i-1)^3/2^\lambda)$.

Consider the following two cases:

Case 1: i is odd:

$$
\begin{aligned}
&\|\mathcal{O}_{\mathsf{comp}}|\phi_i\rangle - |\psi_i\rangle\|_2 \\
=&\|\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2}|\phi_{i-1}\rangle - W^{\mathfrak{m}(\lambda)}A_{(i+1)/2}|\psi_{i-1}\rangle\|_2 \\
&\qquad\qquad\qquad

Lemma 7.11. *For any integer $t \geq 0$,*

$$\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\leq t} \|_{\mathrm{op}} = O(t^2/2^\lambda)$$

Lemma 7.12. *For any integer $t \geq 0$,*

$$\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\leq t} \|_{\mathrm{op}} = O(t^2/2^\lambda)$$

We give proofs of the above lemmas in Section E.
We restate Theorem 7.8 for convenience.

Lemma 7.13 (Theorem 7.8, restated)**.** *For any integer $t \geq 0$,*

- *Forward query:*

$$\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi_{\leq t} \|_{\mathrm{op}} = O(t^2/2^\lambda)$$

- *Inverse query:*

$$\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}} - W^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi_{\leq t} \|_{\mathrm{op}} = O(t^2/2^\lambda)$$

Proof. We prove the lemma for forward queries and we get it for inverse queries symmetrically. We want to show

$$\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi_{\leq t} \|_{\mathrm{op}} = O(t^2/2^\lambda).$$

First, notice that $\sum_{i=1}^{4} \Pi^{\mathfrak{l},i} = I$. Hence, we get

$$\begin{aligned}
\gamma =& \| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi_{\leq t} \|_{\mathrm{op}} \\
=& \| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \left(\sum_{i=1}^{4} \Pi^{\mathfrak{l},i} \right) \Pi_{\leq t} \|_{\mathrm{op}} \\
=& \| \sum_{i=1}^{4} \left(\left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},i} \right) \Pi_{\leq t} \|_{\mathrm{op}} \\
\leq & \sum_{i=1}^{4} \| \left(\left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},i} \right) \Pi_{\leq t} \|_{\mathrm{op}} \\
=& O(t^2/2^\lambda)
\end{aligned}$$

Where the fouth line is by triangle inequality, and fifth line is by Theorems 7.9 to 7.12. □

8 Stretching Strong Pseudorandom Unitaries

Now we show how to apply our results to get nearly linear depth and to stretch the length of *any* strong pseudorandom unitary, relative to its key size.

To prove that we can stretch the keys in a PRU family, we start by recalling the following result from [ABGL25b],

Theorem 8.1. *For any $f(n) = \omega(\log n)$, $k_1, k_2, k_3 \in \{0,1\}^{f(n)}$, define*

$$G^U(k_1 || k_2 || k_3) := (X^{k_3} \otimes I_{n-f(n)}) U (X^{k_2} \otimes I_{n-f(n)}) U (X^{k_1} \otimes I_{n-f(n)}),$$

where U is an n-qubit unitary. Then $\{G_U(k_1||k_2||k_3)\}_{k_1,k_2,k_3 \in \{0,1\}^{f(n)}}$ is a strong PRU in the QHROM.

At a high level, from a single instance of a strong pseudorandom unitary for a key k, and 9 random strings of length $O(\log^2(n))$, we can create three additional instances of a strong pseudorandom unitaries, that are random even relative to the original instance of the pseudorandom unitary, by applying the construction above thrice. Then we can apply the strong gluing theorem to join these three pseudorandom unitaries into a strong pseudorandom unitary acting on a larger input. Formally, we have the following theorem.

Theorem 8.2 (Stretching a strong PRU)**.** *Let $\{\mathsf{PRU}_{\lambda,k}\}_{\lambda\in\mathbb{N},k\in\{0,1\}^\lambda}$ be a strong pseudorandom unitary family with keys of size λ acting on $t(\lambda)$ many qubits. Then there exists a family of strong pseudorandom unitaries $\{\mathsf{StretchPRU}_{\lambda,k\in\{0,1\}^{\lambda+9\log^2(\lambda)}}\}$ with keys of length $\lambda+9\log^2(\lambda)$ that acts on $2t(\lambda)-\log^2(\lambda)$ qubits.*

Proof of Theorem 8.2. Let $k_1||\ldots||k_9$ be a string of length $9\log^2(\lambda)$ where each k_i is length $\log^2(\lambda)$. Then consider the following construction of $\mathsf{StretchPRU}$ on registers ABC, where A is $t(\lambda)-\log^2(\lambda)$ qubits, B is $\log^2(\lambda)$ qubits, and C is $t(\lambda)-\log^2(\lambda)$ qubits.

$$\mathsf{StretchPRU}_{k||k_1||\ldots||k_9} = (X^{k_1}\mathsf{PRU}_k X^{k_2}\mathsf{PRU}_k X^{k_3})_{\mathsf{AB}}(X^{k_4}\mathsf{PRU}_k X^{k_5}\mathsf{PRU}_k X^{k_6})_{\mathsf{BC}}(X^{k_7}\mathsf{PRU}_k X^{k_8}\mathsf{PRU}_k X^{k_9})_{\mathsf{AB}}\,.$$

Let $\mathsf{Stretch}_{k_1||\ldots||k_9}(U)$ be the same construction, except that PRU_k is replaced with a unitary U. Then by the definition of a strong pseudo-random unitary, we have the following for all polynomial-time adversaries $\mathcal{A}$.

$$\left|\Pr_{k||k_1||\ldots||k_9\leftarrow\{0,1\}^{\lambda+9\log^2(\lambda)}}\left[\top\leftarrow\mathcal{A}^{\mathsf{StretchPRU}_{k||k_1||\ldots||k_9},\mathsf{StretchPRU}^\dagger_{k||k_1||\ldots||k_9}}\right] - \Pr_{\substack{U\leftarrow\mu_{t(\lambda)}\\ k_1||\ldots||k_9\leftarrow\{0,1\}^{9\log^2(\lambda)}}}\left[\top\leftarrow\mathcal{A}^{\mathsf{Stretch}_{k_1||\ldots||k_9}(U),\left(\mathsf{Stretch}_{k_1||\ldots||k_9}(U)\right)^\dagger}\right]\right| \leq \mathsf{negl}(\lambda)\,.$$

From Theorem 8.1, applied three times, we have the following bound:

$$\left|\Pr_{\substack{U\leftarrow\mu_{t(\lambda)}\\ k_1||\ldots||k_9\leftarrow\{0,1\}^{9\log^2(\lambda)}}}\left[\top\leftarrow\mathcal{A}^{\mathsf{Stretch}_{k_1||\ldots||k_9}(U),\left(\mathsf{Stretch}_{k_1||\ldots||k_9}(U)\right)^\dagger}\right] - \Pr_{U',V,W\leftarrow\mu_{t(\lambda)}}\left[\top\leftarrow\mathcal{A}^{U'VW,(U'VW)^\dagger}\right]\right| \leq \mathsf{negl}(\lambda)\,.$$

Finally, applying Theorem 7.1, we have the following:

$$\left|\Pr_{U',V,W\leftarrow\mu_{t(\lambda)}}\left[\top\leftarrow\mathcal{A}^{U'VW,(U'VW)^\dagger}\right] - \Pr_{O\leftarrow\mu_{2t(\lambda)-\log^2(\lambda)}}\left[\top\leftarrow\mathcal{A}^{O,O^\dagger}\right]\right| \leq \mathsf{negl}(\lambda)\,.$$

Applying the triangle inequality, the construction of $\mathsf{StretchPRU}$ is indistinguishable from a large Haar random unitary on $2t(\lambda)-\log^2(\lambda)$ qubits. □

Corollary 8.3 (Strong pseudorandom unitaries with small keys)**.** *If there exists a family of strong pseudorandom unitaries, then for every constant c there exists a strong pseudorandom unitary family such that*

1. *The key size is $\lambda+9c\log^3(\lambda)$.*
2. *The pseudorandom unitary family acts on $\lambda^c(t(\lambda)-\log^2(\lambda))+\log^2(\lambda)$ qubits.*

Proof of Theorem 8.3. We recursively apply the previous theorem $c\log(\lambda)$ many times. Each time, we need $9\log^2(\lambda)$ additional bits of randomness, and we double (minus $9\log^2(\lambda)$) the output length of the strong pseudorandom unitary. Thus, after performing this transformation recursively n times, our output length is

$$2^n t(\lambda) - 2^{n-1}\cdot 9\log^2(\lambda) - 2^{n-2}\cdot 9\log^2(\lambda) - \ldots - 9\log^2(\lambda) = 2^n(t(\lambda) - 9\log^2(\lambda))\,.$$

This setting $n = c\log(\lambda)$, we get the desired key length and output length. Note that this requires running the original strong pseudorandom unitary $O(\lambda^c)$ times, which is polynomial in λ for constant c. □

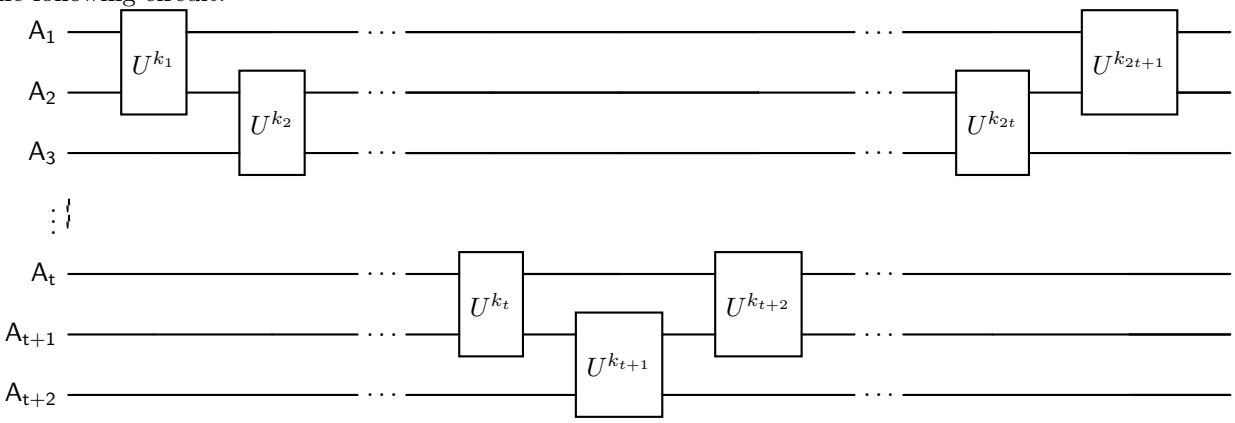
Rescaling so that $\lambda \leftarrow \lambda + 9c\log^3(\lambda)$, we have that there is a family of strong pseudo-random unitaries with keys of length λ and output size roughly λ^c.

Next, we prove that our strong gluing theorem implies that strong PRUs exist at near linear depth.

Corollary 8.4 (Shortening a super-linear depth PRU)**.** *If there exists a family of strong pseudorandom unitaries, then for every constant c there exists a family of strong pseudorandom unitaries with depth $O(n^{1+1/c})$.*

Proof. Let $\mathcal{G} = \{\mathcal{G}^n\}_{n\in\mathbb{N}}$ denote a strong pseudorandom unitary family with $\mathcal{G}^n$ denoting the unitaries with input length n. Let $\mathcal{K}^n$ denote the set of keys assoicated with $\mathcal{G}^n$. By the definition of strong pseudorandom unitaries, the depth of any circuit in $\mathcal{G}^n$ is asymptotically bounded by a polynomial in n, the input size. Let c_1 be a constant such that the depth of the family of strong pseudorandom unitaries is asymptotically bounded by $O(n^{c_1})$.

Then circuits in $\mathcal{G}^{n^{1/(c_1\cdot c)}}$ are strong PRUs on input length $n^{1/(c_1\cdot c)}$ qubits, whose depth is bounded by $O(n^{1/c})$. Then for any $t \in \mathsf{poly}(n)$, we sample some $k_1, \ldots, k_{2t+1} \leftarrow \mathcal{K}^{n^{1/(c_1\cdot c)}}$. We arrange $U^{k_1}, \ldots, U^{k_{2t+1}}$ in the following circuit:



In the above, $|A_i| = n^{1/(c_1\cdot c)}/2$. Notice that the above circuit is on input size $(t+2)\cdot n^{1/(c_1\cdot c)}/2$ that has depth $(2t+1)\cdot O(n^{1/c})$. Let $t = O(n)$, we have a family of circuits on input length $O(n)$ that has depth $O(n^{1+1/c})$.

We prove sampling $k_1, \ldots, k_{2t+1} \leftarrow \mathcal{K}^{n^{1/(c_1\cdot c)}}$ and arranging as above gives us a family of strong PRUs with input length $O(n)$ that has depth $O(n^{1+1/c})$. To prove that the above circuit is a PRU, we start by applying the strong gluing theorem on the middle three unitaries (i.e. $U^{k_t}U^{k_{t+1}}U^{k_{t+2}}$) and replacing it with a larger Haar unitary (say V_1). Next, we apply the strong gluing theorem on the new middle three unitaries (i.e. $U^{k_{t-1}}V_1U^{k_{t+3}}$) and replacing it with a larger Haar unitary (say V_2). Repeating this process a total of t times gives us a single large Haar unitary. □

Acknowledgments

PA, AG and YTL are supported by the National Science Foundation under the grants FET-2329938, CAREER-2341004 and, FET-2530160.

References

[ABGL24] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. "Pseudorandomness in the (inverseless) haar random oracle model". In: *arXiv preprint arXiv:2410.19320* (2024) (cit. on p. 3).

[ABGL25a] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. "Pseudorandom Unitaries in the Haar Random Oracle Model". In: *arXiv preprint arXiv:2509.24432* (2025) (cit. on p. 1).

[ABGL25b] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. "Pseudorandom Unitaries in the Haar Random Oracle Model". In: *Annual International Cryptology Conference*. Springer. 2025, pp. 301–333 (cit. on pp. 1, 4, 34).

[AE07] Andris Ambainis and Joseph Emerson. "Quantum t-designs: t-wise independence in the quantum world". In: *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007, pp. 129–140 (cit. on p. 3).

[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*. Springer. 2024, pp. 226–254 (cit. on p. 3).

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. "Efficient Quantum Pseudorandomness from Hamiltonian Phase States". In: *arXiv preprint arXiv:2410.08073* (2024) (cit. on p. 3).

[CGH+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". In: *Journal of High Energy Physics* 2017.5 (2017), pp. 1–54 (cit. on p. 3).

[DFMS22] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Online-extractability in the quantum random-oracle model". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2022, pp. 677–706 (cit. on p. 14).

[FPVY25] Ben Foxman, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. "Random Unitaries in Constant (Quantum) Time". In: *arXiv preprint arXiv:2508.11487* (2025) (cit. on p. 3).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to quantum states". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1579–1588 (cit. on p. 3).

[GQY+24] Andi Gu, Yihui Quek, Susanne Yelin, Jens Eisert, and Lorenzo Leone. "Simulating quantum chaos without chaos". In: *arXiv preprint arXiv:2410.18196* (2024) (cit. on p. 3).

[HCP23] Hsin-Yuan Huang, Sitan Chen, and John Preskill. "Learning to predict arbitrary quantum processes". In: *PRX Quantum* 4.4 (2023), p. 040337 (cit. on p. 3).

[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*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5 (cit. on pp. 3, 15).

[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". In: *Physical Review A—Atomic, Molecular, and Optical Physics* 77.1 (2008), p. 012307 (cit. on p. 3).

[Liu18] Junyu Liu. "Spectral form factors and late time quantum chaos". In: *Physical Review D* 98.8 (2018), p. 086026 (cit. on p. 3).

[MH24] Fermi Ma and Hsin-Yuan Huang. *How to Construct Random Unitaries*. 2024. arXiv: 2410.10116 [quant-ph]. URL: https://arxiv.org/abs/2410.10116 (cit. on pp. 4–6, 14, 16, 17, 39).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667 (cit. on p. 14).

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. "Random unitaries in extremely low depth". In: *arXiv preprint arXiv:2407.07754* (2024) (cit. on p. 3).

[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*. Springer. 2019, pp. 239–268 (cit. on p. 14).

A Proof of Theorem 4.3

We start by proving that $V_L^{f_L}$ is close to V_L and $V_R^{f_R}$ is close to V_R.

Lemma A.1. *For any integer $t \geq 0$,*

$$\|(V_L - V_L^{f_L})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{2\cdot(t+1)\cdot\delta} \quad \textit{and} \quad \|(V_R - V_R^{f_R})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{2\cdot(t+1)\cdot\delta}.$$

Proof. Consider an arbitrary (normalized) state in the support of $\Pi_{\leq t}$

$$|\psi\rangle_{\mathsf{ABST}} = \sum_{x,z,L,R} \alpha_{x,z,L,R}|x\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

where $\alpha_{x,z,L,R} = 0$ whenever $|L \cup R| > t$. Then

$$V_L|\psi\rangle_{\mathsf{ABST}} = \sum_{x,z,L,R} \frac{\alpha_{x,z,L,R}}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} \sum_{y\notin \operatorname{Im}(L\cup R^{-1})} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

and

$$V_L^{f_L}|\psi\rangle_{\mathsf{ABST}} = \sum_{x,z,L,R} \frac{\alpha_{x,z,L,R}}{\sqrt{|f_L(x,z,L,R)|}} \sum_{y\in f_L(x,z,L,R)} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}}.$$

Subtracting,

$$\begin{aligned}
&(V_L - V_L^{f_L})|\psi\rangle_{\mathsf{ABST}} \\
&= \sum_{x,z,L,R} \alpha_{x,z,L,R} \sum_{\substack{y: y\in f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \\
&\qquad \underbrace{\times\left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{|f_L(x,z,L,R)|}}\right)}_{|v\rangle} \\
&\quad + \underbrace{\sum_{x,z,L,R} \alpha_{x,z,L,R} \sum_{\substack{y: y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}}\right)}_{|w_1\rangle} \\
&\quad + \underbrace{\sum_{x,z,L,R} \alpha_{x,z,L,R} \sum_{\substack{y: y\in f_L(x,z,L,R)\\ y\in \operatorname{Im}(L\cup R^{-1})}} |y\rangle_{\mathsf{A}}|z\rangle_{\mathsf{B}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \left(-\frac{1}{\sqrt{|f_L(x,z,L,R)|}}\right)}_{|w_2\rangle}.
\end{aligned}$$

Note that $|w_1\rangle$, $|w_2\rangle$ and $|v\rangle$ are orthogonal. Thus,

$$\left\|(V_L - V_L^{f_L})|\psi\rangle_{\mathsf{ABST}}\right\|_2^2 = \langle v|v\rangle + \langle w_1|w_1\rangle + \langle w_2|w_2\rangle$$

Bounding $\langle v|v\rangle$. Similar to [MH24], by changing the order of summation, we can rewrite $|v\rangle$ as

$$|v\rangle = \sum_{y,z,L',R} |y\rangle|z\rangle|L'\rangle|R\rangle \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} \alpha_{x,z,L,R}\left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{|f_L(x,z,L,R)|}}\right)\right),$$

and thus

$$\langle v|v\rangle = \sum_{y,z,L',R} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \alpha_{x,z,L,R} \left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{|f_L(x,z,L,R)|}} \right) \right)^2$$

$$\leq \sum_{y,z,L',R} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} |\alpha_{x,z,L,R}|^2 \right)$$

$$\times \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{|f_L(x,z,L,R)|}} \right)^2 \right),$$

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

$$\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{|f_L(x,z,L,R)|}} \right)^2$$

$$= \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{\sqrt{|f_L(x,z,L,R)|} - \sqrt{2^n - |\operatorname{Im}(L\cup R^{-1})|}}{\sqrt{|f_L(x,z,L,R)|(2^n - |\operatorname{Im}(L\cup R^{-1})|)}} \right)^2$$

$$\leq \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{\sqrt{|2^n - |\operatorname{Im}(L\cup R^{-1})| - |f_L(x,z,L,R)||}}{\sqrt{|f_L(x,z,L,R)|(2^n - |\operatorname{Im}(L\cup R^{-1})|)}} \right)^2$$

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

$$\leq \frac{(|L|+1)\cdot \left|2^n - |\operatorname{Im}(L\cup R^{-1})| - |f_L(x,z,L,R)|\right|}{|f_L(x,z,L,R)|(2^n - |\operatorname{Im}(L\cup R^{-1})|)}$$

$$\leq \delta \cdot \frac{(|L|+1)}{(2^n - |\operatorname{Im}(L\cup R^{-1})|)}$$

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,

$$\begin{aligned}
\langle v|v\rangle &\le \delta \cdot \frac{(|L|+1)}{(2^n - |\operatorname{Im}(L \cup R^{-1})|)} \cdot \sum_{y,z,L',R} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\in f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} |\alpha_{x,z,L,R}|^2 \right) \\
&= \delta \cdot \frac{(|L|+1)}{(2^n - |\operatorname{Im}(L \cup R^{-1})|)} \cdot \sum_{x,z,L,R} |\alpha_{x,z,L,R}|^2 \cdot \left(\sum_{y\in\{0,1\}^{2n+\lambda}} \mathbb{1}(y \in f_L(x,z,L,R)) \mathbb{1}(y \notin \operatorname{Im}(L \cup R^{-1})) \right) \\
&\le \delta \cdot (|L|+1) \cdot \sum_{x,z,L,R} |\alpha_{x,z,L,R}|^2 = \delta \cdot (|L|+1).
\end{aligned}$$

Bounding $\langle w_1|w_1\rangle$. We know that

$$\begin{aligned}
|w_1\rangle &= \sum_{x,z,L,R} \alpha_{x,z,L,R} \sum_{\substack{y: y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} |y\rangle_{\mathsf{A}} |z\rangle_{\mathsf{B}} |L \cup \{(x,y)\}\rangle_{\mathsf{S}} |R\rangle_{\mathsf{T}} \left(\frac{1}{\sqrt{2^n - |\operatorname{Im}(L \cup R^{-1})|}} \right) \\
&= \sum_{y,z,(L',R)} |y\rangle|z\rangle|L'\rangle|R\rangle \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} \left(\frac{\alpha_{x,z,L,R}}{\sqrt{2^n - |\operatorname{Im}(L \cup R^{-1})|}} \right)
\end{aligned}$$

Then

$$\begin{aligned}
\langle w_1|w_1\rangle &= \sum_{y,z,(L',R)} \left| \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} \frac{\alpha_{x,z,L,R}}{\sqrt{2^n - |\operatorname{Im}(L \cup R^{-1})|}} \right|^2 \le \sum_{y,z,(L',R)} \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} \frac{|\alpha_{x,z,L,R}|^2}{2^n - |\operatorname{Im}(L \cup R^{-1})|} \\
&= \sum_{x,z,L,R} \frac{|\alpha_{x,z,L,R}|^2}{2^n - |\operatorname{Im}(L \cup R^{-1})|} \left(\sum_{\substack{y: y\notin f_L(x,z,L,R)\\ y\notin \operatorname{Im}(L\cup R^{-1})}} 1 \right) \le \sum_{x,z,L,R} \frac{(2^n - |f_L(x,z,L,R)|)\,|\alpha_{x,z,L,R}|^2}{2^n - |\operatorname{Im}(L \cup R^{-1})|} \\
&\le \frac{\delta}{\delta+1} \sum_{x,z,L,R} |\alpha_{x,z,L,R}|^2 = \frac{\delta}{\delta+1} \le \delta
\end{aligned}$$

Similarly, we also have

$$\langle w_2|w_2\rangle \le \sum_{x,z,L,R} \frac{t\,|\alpha_{x,z,L,R}|^2}{|f_L(x,z,L,R)|} \le t \cdot \delta.$$

Hence, it holds that

$$\|(V_L - W_L^{\mathsf{m}(\lambda)})\Pi_{\le t}\|_{\mathrm{op}} \le \sqrt{2 \cdot (t+1) \cdot \delta}.$$

By a symmetric argument, we have

$$\|(V_R - W_R^{\mathsf{m}(\lambda)})\Pi_{\le t}\|_{\mathrm{op}} \le \sqrt{2 \cdot (t+1) \cdot \delta}. \qquad \square$$

Then by applying triangle inequality multiple times, we have:

Lemma A.2. *For any integer $t \geq 0$,*

$$\|(V - V^{f_L,f_R})\Pi_{\leq t}\|_{\mathrm{op}} \leq 8\sqrt{2 \cdot (t+1) \cdot \delta}.$$

Finally, by bounding each query distance by δ, we get the following:

Lemma A.3 (Generalized Path-Recording (restated))**.** *Let f_L and f_R be functions such that for all x, z, L, R, $|L| + |R| \leq t$,*

$$\begin{aligned} f_L(x,z,L,R) &\subseteq [N] \setminus \mathrm{Im}(L) \\ f_R(x,z,L,R) &\subseteq [N] \setminus \mathrm{Im}(R) \\ \frac{|N - |f_L(x,z,L,R)| - t|}{|f_L(x,z,L,R)|} &\leq \delta \\ \frac{|N - |f_R(x,z,L,R)| - t|}{|f_R(x,z,L,R)|} &\leq \delta, \end{aligned}$$

For any $2t$-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,

$$\mathsf{TD}\Big(\mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}\rangle\langle\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}|\right), \mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|\right)\Big) \leq 16t\sqrt{2 \cdot (t+1) \cdot \delta},$$

where,

$$\begin{aligned} |\mathcal{A}_t^{V^{f_L,f_R},V^{f_L,f_R,\dagger}}\rangle &= \prod_{i=1}^{t} \left(V^{f_L,f_R,\dagger} B_i V^{f_L,f_R} A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}} \\ |\mathcal{A}_t^{V,V^\dagger}\rangle &= \prod_{i=1}^{t} \left(V^\dagger B_i V A_i\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}} \end{aligned}$$

B Glued Path Recording

We want to show that querying $V^3V^2V^1$ is close to querying V^{glued}. We start by formalising the intuition we had about monogamy of entanglement by proving the following lemma:

Lemma B.1. *Let V_L^1 be such that it acts on $\mathsf{ABS_1T_1}$ and V_R^2 be such that it acts on $\mathsf{BCS_2T_2}$, then*

$$\|V_L^{1,\dagger} V_R^2 \Pi_{\leq t}\|_{\mathrm{op}} \leq O\left(\frac{t^2}{2^\lambda}\right).$$

Proof. Let

$$|\psi\rangle = \sum_{x,L_1,L_2,R_1,R_2} \alpha_{xL_1L_2R_1R_2} |x\rangle_{\mathsf{ABC}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2}.$$

Then let $|\chi\rangle = V_L^{1,\dagger} V_R^2 |\psi\rangle$

$$\begin{aligned} |\chi\rangle &= \sum_{y,L_1,L_2,R_1,R_2} \alpha_{yL_1L_2R_1R_2} V_L^{1,\dagger} V_R^2 |y\rangle_{\mathsf{ABC}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} \\ &= \frac{1}{\sqrt{2^{n+\lambda}}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x \notin \mathrm{Dom}(L \cup R^{-1})}} \alpha_{yL_1L_2R_1R_2} V_L^{1,\dagger} |y^{\mathfrak{l}(n)}\rangle_{\mathsf{A}} |x\rangle_{\mathsf{BC}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2 \cup \{(y^{\mathfrak{r}(n+\lambda)}, x)\}\rangle_{\mathsf{T}_2} \end{aligned}$$

$$= \frac{1}{2^{n+\lambda}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x\notin \mathrm{Dom}(L_2\cup R_2^{-1}) \\ z:(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\in L_1}} \alpha_{yL_1L_2R_1R_2} |z\rangle_{\mathsf{AB}} |x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}} |L_1 \setminus \{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2 \cup \{(y^{\mathfrak{r}(n+\lambda)},x)\}\rangle_{\mathsf{T}_2}$$

$$= \frac{1}{2^{n+\lambda}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x\notin \mathrm{Dom}(L_2\cup R_2) \\ z:(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\in L_1}} \alpha_{yL_1L_2R_1R_2} |z\rangle_{\mathsf{AB}} |x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}} |L_1 \setminus \{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2 \cup \{(y^{\mathfrak{r}(n+\lambda)},x)\}\rangle_{\mathsf{T}_2}$$

$$= \frac{1}{2^{n+\lambda}} \sum_{x,y,z,L_1',L_2,R_1,R_2'} \alpha_{yL_1'\cup\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}L_2R_1R_2'\setminus\{(y^{\mathfrak{r}(n+\lambda)},x)\}} |z\rangle_{\mathsf{AB}} |x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}} |L_1'\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2'\rangle_{\mathsf{T}_2}$$

Then $\||\chi\rangle\|_2^2 = \langle\chi|\chi\rangle$,

$$\begin{aligned}
\||\chi\rangle\|_2^2 &= \frac{1}{2^{2(n+\lambda)}} \sum_{z,x^{\mathfrak{r}(n)},L_1',R_1,L_2,R_2'} \left| \sum_{y^{\mathfrak{l}(n)},y^{\mathfrak{r}(n+\lambda)},x^{\mathfrak{l}(\lambda)}} \alpha_{yL_1'\cup\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}L_2R_1R_2'\setminus\{(x,y^{\mathfrak{r}(n+\lambda)})\}} \right|^2 \\
&\le \frac{t^2 2^{2n}}{2^{2(n+\lambda)}} \sum_{z,x^{\mathfrak{r}(n)},L_1',R_1,L_2,R_2'} \sum_{y^{\mathfrak{l}(n)},y^{\mathfrak{r}(n+\lambda)},x^{\mathfrak{l}(\lambda)}} \left| \alpha_{yL_1'\cup\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}L_2R_1R_2'\setminus\{(x,y^{\mathfrak{r}(n+\lambda)})\}} \right|^2 \\
&\le \frac{t^4}{2^{2\lambda}}
\end{aligned}$$

Hence

$$\|V_L^{1,\dagger} V_R^2 \Pi_{\le t}\|_{\mathrm{op}} \le \frac{t^2}{2^\lambda}.$$

□

Lemma B.2. *Let V^{glued} be defined as before, then*

$$\|(V^{\mathsf{glued}} - V^3V^2V^1)\Pi_{\le t}\|_{\mathrm{op}} \le O\left(\frac{t^2}{2^\lambda}\right).$$

The above lemma gives us the following:

Lemma B.3 (Theorem 5.1 restated)**.** *For any $2t$-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,*

$$\left\| |\mathcal{A}^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}} - |\mathcal{A}^{V^3V^2V^1,(V^3V^2V^1)^\dagger}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}} \right\|_2 = O\left(\frac{t^3}{2^\lambda}\right).$$

where $\overline{\mathsf{ST}} = \mathsf{S}_1\mathsf{S}_2\mathsf{S}_3\mathsf{T}_1\mathsf{T}_2\mathsf{T}_3$, $|\mathsf{ABC}| = 2n+\lambda$,

$$|\mathcal{A}_t^{V^{\mathsf{glued}},V^{\mathsf{glued},\dagger}}\rangle = \prod_{i=1}^{t} \left(V^{\mathsf{glued},\dagger} B_i V^{\mathsf{glued}} A_i\right) |0\rangle_{\mathsf{ABC}} |0\rangle_{\mathsf{D}} |\varnothing\rangle_{\mathsf{S}_1} |\varnothing\rangle_{\mathsf{T}_1} |\varnothing\rangle_{\mathsf{S}_2} |\varnothing\rangle_{\mathsf{T}_2} |\varnothing\rangle_{\mathsf{S}_3} |\varnothing\rangle_{\mathsf{T}_3}$$

and $|\mathcal{A}^{V^3V^2V^1,(V^3V^2V^1)^\dagger}\rangle_{\mathsf{ABCD}\overline{\mathsf{ST}}}$ is defined similarly.

C Proofs of Section 6.5

Proof of Theorem 6.10. Fix some $y, w, \overline{S}$ where $\overline{S}$ is good and $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$. We start by looking at what

$$|\psi_{y,w,\overline{S}}\rangle = \Pi^{\mathcal{R},1} |y\rangle_{\mathsf{A}} |w\rangle_{\mathsf{B}} |\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}},$$

Then we have the following:

$$\begin{aligned}|\psi_{y,w,\overline{S}}\rangle =&\Pi^{\mathcal{R},1}|y\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}}\\ =&\frac{1}{\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^{\lambda}-i+1)}}\sum_{\substack{Z\in\{0,1\}^{an}\\ R\in\left(\{0,1\}^{\lambda}\right)^{b}_{\mathrm{dist}}}}\Pi^{\mathcal{R},1}|y\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|\mathbb{G}\left(\overline{S},R,Z\right)\rangle_{\overline{\mathsf{ST}}}\end{aligned}$$

Notice that the above is zero if there's no line in $\mathbb{G}\left(\overline{S},R,Z\right)$ of the form $(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w,\overrightarrow{r},z)$ for some $X\in\{\mathcal{L},\mathcal{R}\}$ and $\overrightarrow{x},\overrightarrow{y},w_1,w_2,\overrightarrow{r},z$. That is that $\overline{S}=\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w)\}$.Then the above looks like:

$$\begin{aligned}|\psi_{y,w,\overline{S}}\rangle =&\frac{1}{\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^{\lambda}-i+1)}}\sum_{\substack{Z'\in\{0,1\}^{(a-1)n}\\ R'\in\left(\{0,1\}^{\lambda}\right)\cup\{w\}\right)^{b-|\overrightarrow{x}|}_{\mathrm{dist}}\\ z\in\{0,1\}^{n}\\ \overrightarrow{r}\in\left(\{0,1\}^{\lambda}\setminus R'\right)^{|\overrightarrow{x}|}_{\mathrm{dist}}}}\Pi^{\mathcal{R},1}|y\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}\\ &\times|\mathbb{G}\left(\overline{S'},R',Z'\right)\cup\{(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w,\overrightarrow{r},z)\}\rangle_{\overline{\mathsf{ST}}}\\ =&\frac{1}{2^n(2^{\lambda}-a+1)\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^{\lambda}-i+1)}}\sum_{\substack{Z'\in\{0,1\}^{(a-1)n}\\ R'\in\left(\{0,1\}^{\lambda}\right)^{b-|\overrightarrow{x}|}_{\mathrm{dist}}\\ z\in\{0,1\}^{n}\\ \overrightarrow{r}\in\left(\{0,1\}^{\lambda}\setminus R'\right)^{|\overrightarrow{x}|}_{\mathrm{dist}}\\ y'\in\{0,1\}^{n}\\ w'\in\left(\{0,1\}^{\lambda}\setminus\mathrm{Im}(\overline{S'})\right)}}|y'\rangle_{\mathsf{A}}|w'\rangle_{\mathsf{B}}\\ &\times|\mathbb{G}\left(\overline{S'},R',Z'\right)\cup\{(X\mathcal{R},\overrightarrow{x},y'||\overrightarrow{y},w_1,w',\overrightarrow{r},z)\}\rangle_{\overline{\mathsf{ST}}}\\ =&\frac{1}{2^n(2^{\lambda}-a+1)\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^{\lambda}-i+1)}}\sum_{\substack{y'\in\{0,1\}^{n}\\ w'\in\left(\{0,1\}^{\lambda}\setminus\mathrm{Im}(\overline{S'})\right)\\ Z\in\{0,1\}^{an}\\ R\in\left(\{0,1\}^{\lambda}\right)^{b}_{\mathrm{dist}}}}|y'\rangle_{\mathsf{A}}|w'\rangle_{\mathsf{B}}\\ &\times|\mathbb{G}\left(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y'||\overrightarrow{y},w_1,w')\},R,Z\right)\rangle_{\overline{\mathsf{ST}}}\\ =&\frac{1}{\sqrt{2^n(2^{\lambda}-a+1)}}\underbrace{\frac{1}{\sqrt{2^n(2^{\lambda}-a+1)}}\sum_{\substack{y'\in\{0,1\}^{n}\\ w'\in\left(\{0,1\}^{\lambda}\setminus\mathrm{Im}(\overline{S'})\right)}}|y',w',\mathfrak{G}(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y'||\overrightarrow{y},w_1,w')\})\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}}_{|\chi^{\mathfrak{l},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle}\end{aligned}$$

Finally, to understand $\Pi^{\mathcal{R},1}\Pi^{\mathsf{Good}}$, we expanding the projector Π^{Good}:

$$\begin{aligned}\Pi^{\mathcal{R},1}\Pi^{\mathsf{Good}} =&\Pi^{\mathcal{R},1}\sum_{\substack{y,w,\overline{S}\\ \overline{S}\text{ is good}}}|y,w,\mathfrak{G}(\overline{S})\rangle\langle y,w,\mathfrak{G}(\overline{S})|_{\mathsf{AB}\overline{\mathsf{ST}}}\\ =&\sum_{\substack{y,w,\overline{S}\\ \overline{S}\text{ is good}}}\Pi^{\mathcal{R},1}|y,w,\mathfrak{G}(\overline{S})\rangle\langle y,w,\mathfrak{G}(\overline{S})|_{\mathsf{AB}\overline{\mathsf{ST}}}\\ =&\sum_{\substack{y,w\\ X,\overrightarrow{x},\overrightarrow{y},w_1,\overline{S'}\\ w\in\{0,1\}^{\lambda}\setminus\mathrm{Im}(\overline{S'})}}\Pi^{\mathcal{R},1}|y,w,\mathfrak{G}(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w)\})\rangle\langle y,w,\mathfrak{G}(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w)\})|_{\mathsf{AB}\overline{\mathsf{ST}}}\end{aligned}$$

$$= \sum_{\substack{y,w \\ X,\overrightarrow{x},\overrightarrow{y},w_1,\overline{S'} \\ w\in\{0,1\}^\lambda\setminus \mathrm{Im}(\overline{S'})}} \frac{1}{\sqrt{2^n(2^\lambda-a+1)}} |\chi^{\mathsf{f},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle y,w,\mathfrak{G}(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y||\overrightarrow{y},w_1,w)\})|_{\mathsf{AB}\overline{\mathsf{ST}}}$$
$$= \sum_{X,\overrightarrow{x},\overrightarrow{y},w_1,\overline{S'}} |\chi^{\mathsf{f},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathsf{f},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}|_{\mathsf{AB}\overline{\mathsf{ST}}}$$

Hence,

$$\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},1} = \sum_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1} |\chi^{\mathsf{f},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathsf{f},1}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}|$$

□

Proof of Theorem 6.11. Fix some $y_0, w, y_1, \overline{S}$ where $\overline{S}$ is good and $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$. We start by looking at what

$$|\psi_{y_0,w,y_1,\overline{S}}\rangle = \Pi^{\mathcal{R},12}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}},$$

Then we have the following:

$$\begin{aligned}|\psi_{y_0,w,y_1,\overline{S}}\rangle =& \Pi^{\mathcal{R},12}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}} \\ =& \frac{1}{\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^\lambda-i+1)}} \sum_{\substack{Z\in\{0,1\}^{an} \\ R\in\left(\{0,1\}^\lambda\right)^b_{\mathrm{dist}}}} \Pi^{\mathcal{R},12}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathbb{G}\left(\overline{S},R,Z\right)\rangle_{\overline{\mathsf{ST}}}\end{aligned}$$

Notice that the above is zero if there's no line in $\mathbb{G}\left(\overline{S},R,Z\right)$ of the form $(X\mathcal{R},\overrightarrow{x},y_0||\overrightarrow{y}||y_1,w_1,w,\overrightarrow{r},z)$ for some $X\in\{\mathcal{L},\mathcal{R}\}$ and $\overrightarrow{x},\overrightarrow{y},w_1,\overrightarrow{r},z$. That is that $\overline{S}=\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y_0||\overrightarrow{y}||y_1,w_1,w)\}$.Then the above looks like:

$$\begin{aligned}|\psi_{y_0,w,y_1,\overline{S}}\rangle =& \frac{1}{\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^\lambda-i+1)}} \sum_{\substack{Z'\in\{0,1\}^{(a-1)n} \\ R'\in\left(\{0,1\}^\lambda)\cup\{w\}\right)^{b-|\overrightarrow{x}|}_{\mathrm{dist}} \\ z\in\{0,1\}^n \\ \overrightarrow{r}\in\left(\{0,1\}^\lambda\setminus R'\right)^{|\overrightarrow{x}|}_{\mathrm{dist}}}} \Pi^{\mathcal{R},12}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}} \\ &\times|\mathbb{G}\left(\overline{S'},R',Z'\right)\cup\{(X\mathcal{R},\overrightarrow{x},y_0||\overrightarrow{y}||y_1,w_1,w,\overrightarrow{r},z)\}\rangle_{\overline{\mathsf{ST}}} \\ =& \frac{1}{2^{2n}(2^\lambda-a+1)\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^\lambda-i+1)}} \sum_{\substack{Z'\in\{0,1\}^{(a-1)n} \\ R'\in\left(\{0,1\}^\lambda\right)^{b-|\overrightarrow{x}|}_{\mathrm{dist}} \\ z\in\{0,1\}^n \\ \overrightarrow{r}\in\left(\{0,1\}^\lambda\setminus R'\right)^{|\overrightarrow{x}|}_{\mathrm{dist}} \\ y_0'\in\{0,1\}^n \\ w'\in\left(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S'})\right) \\ y_1'\in\{0,1\}^n}} |y_0'\rangle_{\mathsf{A}}|w'\rangle_{\mathsf{B}}|y_1'\rangle_{\mathsf{A}} \\ &\times|\mathbb{G}\left(\overline{S'},R',Z'\right)\cup\{(X\mathcal{R},\overrightarrow{x},y_0'||\overrightarrow{y}||y_1',w_1,w',\overrightarrow{r},z)\}\rangle_{\overline{\mathsf{ST}}} \\ =& \frac{1}{2^{2n}(2^\lambda-a+1)\sqrt{2^{an}\cdot\Pi_{i=1}^{b}(2^\lambda-i+1)}} \sum_{\substack{y_0'\in\{0,1\}^n \\ w'\in\left(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S'})\right) \\ y_1'\in\{0,1\}^n \\ Z\in\{0,1\}^{an} \\ R\in\left(\{0,1\}^\lambda\right)^b_{\mathrm{dist}}}} |y_0'\rangle_{\mathsf{A}}|w'\rangle_{\mathsf{B}}|y_1'\rangle_{\mathsf{C}} \\ &\times|\mathbb{G}\left(\overline{S'}\cup\{(X\mathcal{R},\overrightarrow{x},y_0'||\overrightarrow{y}||y_1',w_1,w')\},R,Z\right)\rangle_{\overline{\mathsf{ST}}}\end{aligned}$$

$$= \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \underbrace{\sum_{\substack{y_0' \in \{0,1\}^n \\ w' \in \left(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})\right) \\ y_1' \in \{0,1\}^n}} |y_0', w', y_1', \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y_0' || \overrightarrow{y} || y_1', w_1, w')\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}}_{|\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}\rangle}$$

Finally, to understand $\Pi^{\mathcal{R},12}\Pi^{\mathsf{Good}}$, we expanding the projector Π^{Good}:

$$\begin{aligned}
\Pi^{\mathcal{R},12}\Pi^{\mathsf{Good}} =& \Pi^{\mathcal{R},12} \sum_{\substack{y_0, w, y_1, \overline{S} \\ \overline{S} \text{ is good}}} |y_0, w, y_1, \mathfrak{G}(\overline{S})\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1, \overline{S} \\ \overline{S} \text{ is good}}} \Pi^{\mathcal{R},12} |y_0, w, y_1, \mathfrak{G}(\overline{S})\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1 \\ X, \overrightarrow{x}, \overrightarrow{y}, w_1, \overline{S'} \\ w \in \{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})}} \Pi^{\mathcal{R},12} |y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y_0 || \overrightarrow{y} || y_1, w_1, w)\})\rangle \\
& \times \langle y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y_0 || \overrightarrow{y} || y_1, w_1, w)\})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1 \\ X, \overrightarrow{x}, \overrightarrow{y}, w_1, \overline{S'} \\ w \in \{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})}} \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} |\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{R}, \overrightarrow{x}, y_0 || \overrightarrow{y} || y_1, w_1, w)\})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{X, \overrightarrow{x}, \overrightarrow{y}, w_1, \overline{S'}} |\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}\rangle\langle\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}|_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

Hence,

$$\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},12} = \sum_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1} |\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}\rangle\langle\chi^{\mathsf{f},2}_{\overline{S'}, X, \overrightarrow{x}, \overrightarrow{y}, w_1}|$$

□

Proof of Theorem 6.12. Fix some $y_0, w, y_1, \overline{S}$ where $\overline{S}$ is good and $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$. We start by looking at what

$$|\psi_{y_0, w, y_1, \overline{S}}\rangle = \Pi^{\mathcal{R},123}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}},$$

Then we have the following:

$$\begin{aligned}
|\psi_{y_0, w, y_1, \overline{S}}\rangle =& \Pi^{\mathcal{R},123}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}} \\
=& \frac{1}{\sqrt{2^{an} \cdot \Pi_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{Z \in \{0,1\}^{an} \\ R \in \left(\{0,1\}^\lambda\right)^b_{\mathrm{dist}}}} \Pi^{\mathcal{R},123}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathbb{G}\left(\overline{S}, R, Z\right)\rangle_{\overline{\mathsf{ST}}}
\end{aligned}$$

Notice that the above is zero if there's no line in $\mathbb{G}\left(\overline{S}, R, Z\right)$ of the form $(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w, \overrightarrow{r}, z)$ for some $\overrightarrow{x}, w_1, \overrightarrow{r}, z$. That is that $\overline{S} = \overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w)\}$.Then the above looks like:

$$|\psi_{y_0, w, y_1, \overline{S}}\rangle = \frac{1}{\sqrt{2^{an} \cdot \Pi_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{Z' \in \{0,1\}^{(a-1)n} \\ R' \in \left(\{0,1\}^\lambda) \cup \{w\}\right)^{b-2}_{\mathrm{dist}} \\ z \in \{0,1\}^n \\ \overrightarrow{r} \in \left(\{0,1\}^\lambda \setminus R'\right)^2_{\mathrm{dist}}}} \Pi^{\mathcal{R},123}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}$$

$$
\begin{aligned}
&\times |\mathbb{G}\left(\overline{S'}, R', Z'\right) \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w, \overrightarrow{r}, z)\}\rangle_{\overline{\mathsf{ST}}} \\
=&\frac{1}{2^{2n}(2^\lambda - a + 1)\sqrt{2^{an} \cdot \Pi_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{Z' \in \{0,1\}^{(a-1)n} \\ R' \in \left(\{0,1\}^\lambda\right)^{b-2}_{\mathrm{dist}} \\ z \in \{0,1\}^n \\ \overrightarrow{r} \in \left(\{0,1\}^\lambda \setminus R'\right)^{2}_{\mathrm{dist}} \\ y_0' \in \{0,1\}^n \\ w' \in \left(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})\right) \\ y_1' \in \{0,1\}^n}} |y_0'\rangle_{\mathsf{A}} |w'\rangle_{\mathsf{B}} |y_1'\rangle_{\mathsf{A}} \\
&\times |\mathbb{G}\left(\overline{S'}, R', Z'\right) \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0', y_1'), w_1, w', \overrightarrow{r}, z)\}\rangle_{\overline{\mathsf{ST}}} \\
=&\frac{1}{2^{2n}(2^\lambda - a + 1)\sqrt{2^{an} \cdot \Pi_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{y_0' \in \{0,1\}^n \\ w' \in \left(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})\right) \\ y_1' \in \{0,1\}^n \\ Z \in \{0,1\}^{an} \\ R \in \left(\{0,1\}^\lambda\right)^{b}_{\mathrm{dist}}}} |y_0'\rangle_{\mathsf{A}} |w'\rangle_{\mathsf{B}} |y_1'\rangle_{\mathsf{C}} \\
&\times |\mathbb{G}\left(\overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0', y_1'), w_1, w')\}, R, Z\right)\rangle_{\overline{\mathsf{ST}}} \\
=&\frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \underbrace{\sum_{\substack{y_0' \in \{0,1\}^n \\ w' \in \left(\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})\right) \\ y_1' \in \{0,1\}^n}} |y_0', w', y_1', \mathfrak{G}(\overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0', y_1'), w_1, w')\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}}_{|\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}\rangle}
\end{aligned}
$$

Finally, to understand $\Pi^{\mathcal{R},123}\Pi^{\mathsf{Good}}$, we expanding the projector Π^{Good}:

$$
\begin{aligned}
\Pi^{\mathcal{R},123}\Pi^{\mathsf{Good}} =&\Pi^{\mathcal{R},123} \sum_{\substack{y_0, w, y_1, \overline{S} \\ \overline{S} \text{ is good}}} |y_0, w, y_1, \mathfrak{G}(\overline{S})\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1, \overline{S} \\ \overline{S} \text{ is good}}} \Pi^{\mathcal{R},123} |y_0, w, y_1, \mathfrak{G}(\overline{S})\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1 \\ \overrightarrow{x}, w_1, \overline{S'} \\ w \in \{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})}} \Pi^{\mathcal{R},123} |y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w)\})\rangle \\
&\times \langle y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w)\})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\substack{y_0, w, y_1 \\ \overrightarrow{x}, w_1, \overline{S'} \\ w \in \{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})}} \frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} |\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}\rangle\langle y_0, w, y_1, \mathfrak{G}(\overline{S'} \cup \{(\mathcal{RR}, \overrightarrow{x}, (y_0, y_1), w_1, w)\})|_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \sum_{\overrightarrow{x}, w_1, \overline{S'}} |\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}\rangle\langle\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}|_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}
$$

Hence,

$$
\Pi^{\mathsf{Good}}\Pi^{\mathcal{R},123} = \sum_{\overline{S'}, \overrightarrow{x}, w_1} |\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}\rangle\langle\chi^{\mathfrak{l},3}_{\overline{S'}, \overrightarrow{x}, w_1}|
$$

□

D Proofs of Section 6.6

Proof of Theorem 6.13. Recall that we want to analyse:

$$|\phi\rangle = V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle$$

In the below calculation, we don't explicitly write the normalisation, and can be verified.

$$\begin{aligned}
|\phi\rangle &= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle \\
&= \sum_{\substack{Z\in\{0,1\}^{an} \\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}}}} V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathbb{G}(\overline{S},R,Z)\rangle \\
&= \sum_{\substack{Z\in\{0,1\}^{an} \\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}} \\ (r_1,r_2)\in(\{0,1\}^\lambda\setminus R)^2_{\mathrm{dist}} \\ z\in\{0,1\}^n \\ y_0,y_1\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathbb{G}(\overline{S},R,Z)\cup\mathfrak{p}(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2,(r_1,r_2),z)\rangle \\
&= \sum_{\substack{Z\cup\{z\}\in\{0,1\}^{(a+1)n} \\ R\cup\{(r_1,r_2)\}\in(\{0,1\}^\lambda)^{b_2}_{\mathrm{dist}} \\ y_0,y_1\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathbb{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2)\},R\cup\{(r_1,r_2)\},Z\cup\{z\})\rangle \\
&= \sum_{\substack{y_0,y_1\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathfrak{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2)\})\rangle \\
&= |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle
\end{aligned}$$

Hence, we have

$$V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle = |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle$$

□

Proof of Theorem 6.14. Recall that we want to analyse:

$$|\phi\rangle = V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} |\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}}$$

In the below calculation, we don't explicitly write the normalisation, and can be verified.

$$\begin{aligned}
|\phi\rangle &= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} |\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \\
&= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} \sum_{\substack{y_0\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0,w_2,\mathfrak{G}(\overline{S}\cup\{(XL,\overrightarrow{x},y_0||\overrightarrow{y},w_1,w_2)\})\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \\
&= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} \sum_{\substack{y_0\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}) \\ Z\in\{0,1\}^{an} \\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}} \\ z\in\{0,1\}^n \\ \overrightarrow{r}\in(\{0,1\}^\lambda\setminus R)^{a'}_{\mathrm{dist}}}} |y_0,w_2,\mathbb{G}(\overline{S}\cup\{(XL,\overrightarrow{x},y_0||\overrightarrow{y},w_1,w_2)\},R\cup\{\overrightarrow{r}\},Z\cup\{z\})\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}}
\end{aligned}$$

$$= \sum_{\substack{y_0\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus \mathrm{Im}(\overline{S}) \\ y_1\in\{0,1\}^n \\ Z\in\{0,1\}^{an} \\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}} \\ z\in\{0,1\}^n \\ \overrightarrow{r}\in(\{0,1\}^\lambda\setminus R)^{a'}_{\mathrm{dist}} \\ r\in\{0,1\}^\lambda\setminus R\cup\{\overrightarrow{r}\}}} |y_0,w_2,y_1\mathbb{G}(\overline{S}\cup\{(XR,\overrightarrow{x}||x',y_0||\overrightarrow{y}||y_1,w_1,w_2)\},R\cup\{\overrightarrow{r}||r\},Z\cup\{z\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

$$= \sum_{\substack{y_0\in\{0,1\}^n \\ w_2\in\{0,1\}^\lambda\setminus \mathrm{Im}(\overline{S}) \\ y_1\in\{0,1\}^n}} |y_0,w_2,y_1\mathfrak{G}(\overline{S}\cup\{(XR,\overrightarrow{x}||x',y_0||\overrightarrow{y}||y_1,w_1,w_2)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

$$= |\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Hence, we have

$$V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}V_L^{(3),\mathsf{mid},\dagger}|\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}} = |\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

□

Proof of Theorem 6.15. Recall that:

$$\begin{aligned}
W^{\mathsf{glued}} = &\left(\Pi^{\mathcal{L},321}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_L^{(2),\mathsf{mid}}\cdot V_L^{(1),\mathsf{mid}}\cdot\left(I-\Pi^{\mathcal{R},1}\right)\\
&+\left(\Pi^{\mathcal{L},32}-\Pi^{\mathcal{L},321}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_L^{(2),\mathsf{mid}}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},1}-\Pi^{\mathcal{R},12}\right)\\
&+\left(\Pi^{\mathcal{L},3}-\Pi^{\mathcal{L},32}\right)\cdot V_L^{(3),\mathsf{mid}}\cdot V_R^{(2),\mathsf{mid},\dagger}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},12}-\Pi^{\mathcal{R},123}\right)\\
&+\left(I-\Pi^{\mathcal{L},3}\right)\cdot V_R^{(3),\mathsf{mid},\dagger}\cdot V_R^{(2),\mathsf{mid},\dagger}\cdot V_R^{(1),\mathsf{mid},\dagger}\cdot\left(\Pi^{\mathcal{R},123}\right)
\end{aligned}$$

We know $|\phi\rangle = \Pi^{\mathsf{Good}}|\phi\rangle$. Then we also have the following:

$$\begin{aligned}
\left(I-\Pi^{\mathcal{R},1}\right)|\phi\rangle &= \left(I-\Pi^{\mathcal{R},1}\right)\Pi^{\mathsf{Good}}|\phi\rangle\\
&= \Pi^{\mathsf{Good}}\left(I-\Pi^{\mathcal{R},1}\right)|\phi\rangle
\end{aligned}$$

Similarly, we have:

$$\begin{aligned}
\underbrace{\left(I-\Pi^{\mathcal{R},1}\right)|\phi\rangle}_{|\phi_1\rangle} &= \Pi^{\mathsf{Good}}\left(I-\Pi^{\mathcal{R},1}\right)|\phi\rangle\\
\underbrace{\left(\Pi^{\mathcal{R},1}-\Pi^{\mathcal{R},12}\right)|\phi\rangle}_{|\phi_2\rangle} &= \Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{R},1}-\Pi^{\mathcal{R},12}\right)|\phi\rangle\\
\underbrace{\left(\Pi^{\mathcal{R},12}-\Pi^{\mathcal{R},123}\right)|\phi\rangle}_{|\phi_3\rangle} &= \Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{R},12}-\Pi^{\mathcal{R},123}\right)|\phi\rangle\\
\underbrace{\left(\Pi^{\mathcal{R},123}\right)|\phi\rangle}_{|\phi_4\rangle} &= \Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{R},123}\right)|\phi\rangle
\end{aligned}$$

And we have $|\phi\rangle = \sum_{i\in[4]}|\phi_i\rangle$. Then for $i\in[4]$, we compute that $\Pi^{\mathsf{Good}}W^{\mathsf{glued}}|\phi_i\rangle - W^{\mathsf{glued}}|\phi_i\rangle$. We start by computing the above for $|\phi_1\rangle$.

$$W^{\mathsf{glued}}|\phi_1\rangle = W^{\mathsf{glued}}\left(I-\Pi^{\mathcal{R},1}\right)|\phi_1\rangle$$

$$= \left(\Pi^{\mathcal{L},321}\right) \cdot V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_L^{(1),\mathsf{mid}} \left(I - \Pi^{\mathcal{R},1}\right) |\phi_1\rangle$$

Notice that Π^{Good} commutes with $\Pi^{\mathcal{L},321}$. Also, since $|\phi_1\rangle$ is in the subspace Π^{Good}, we can write it as a superposition over $|x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle$. Then by Theorem 6.13, we get that $V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_L^{(1),\mathsf{mid}}$ on $|\phi_1\rangle$ is in Π^{Good}. Hence, we get $(I - \Pi^{\mathsf{Good}})W^{\mathsf{glued}}|\phi_1\rangle = 0$.
Next, we compute the above for $|\phi_2\rangle$.

$$\begin{aligned} W^{\mathsf{glued}}|\phi_2\rangle &= W^{\mathsf{glued}} \left(\Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12}\right) |\phi_2\rangle \\ &= \left(\Pi^{\mathcal{L},32} - \Pi^{\mathcal{L},321}\right) \cdot V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_R^{(1),\mathsf{mid},\dagger} \left(\Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12}\right) |\phi_2\rangle \end{aligned}$$

Notice that Π^{Good} commutes with $\Pi^{\mathcal{L},32} - \Pi^{\mathcal{L},321}$. Also, since $|\phi_1\rangle$ is in the subspace $\Pi^{\mathcal{R},1}\Pi^{\mathsf{Good}}$, by Theorem 6.10, we can write it as a superposition over $|\chi^{1}_{\overline{S'},\overrightarrow{x},\overrightarrow{y},w_1}\rangle|x'\rangle$. Then by Theorem 6.14, we get that $V_L^{(3),\mathsf{mid}} \cdot V_L^{(2),\mathsf{mid}} \cdot V_R^{(1),\mathsf{mid},\dagger}$ on $|\phi_2\rangle$ is in Π^{Good}. Hence, we get $(I - \Pi^{\mathsf{Good}})W^{\mathsf{glued}}|\phi_2\rangle = 0$.
Similarly by, we have for $i \in \{3,4\}$, $(I - \Pi^{\mathsf{Good}})W^{\mathsf{glued}}|\phi_i\rangle = 0$. Hence, we get $(I - \Pi^{\mathsf{Good}})W^{\mathsf{glued}}|\phi\rangle = 0$. □

E Proofs of Section 7.4

Lemma E.1. *We have the following:*

$$\|\mathcal{O}_{\mathsf{comp}}^{\dagger} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi_{\le t} - \left(\sum_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1} |\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}| \right) \Pi_{\le t}\|_{\mathrm{op}} = O(t^2/2^{\lambda})$$

The proof of the above is similar to Theorem 6.10.
Notice that Theorem 6.11, we have

$$\sum_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1} |\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle\langle\chi^{\mathfrak{l},2}_{\overline{S'},X,\overrightarrow{x},\overrightarrow{y},w_1}| = \Pi^{\mathsf{Good}} \Pi^{cR,12}.$$

Notice that

$$\Pi^{cR,12}\Pi^{\mathfrak{l},1} = \Pi^{cR,12}\Pi^{\mathfrak{l},2} = 0,$$
$$\Pi^{cR,12}\Pi^{\mathfrak{l},3} = \Pi^{\mathfrak{l},3}$$

and

$$\Pi^{cR,12}\Pi^{\mathfrak{l},4} = \Pi^{\mathfrak{l},4}$$

Then we can see how $\Pi^{\mathfrak{l},i}$ behaves with the above projector. In particular, we have the following:

Lemma E.2. *We have the following:*

$$\|\mathcal{O}_{\mathsf{comp}}^{\dagger} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\le t}\|_{\mathrm{op}} = O(t^2/2^{\lambda})$$

Lemma E.3. *We have the following:*

$$\|\mathcal{O}_{\mathsf{comp}}^{\dagger} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t}\|_{\mathrm{op}} = O(t^2/2^{\lambda})$$

Lemma E.4. *We have the following:*

$$\|\mathcal{O}_{\mathsf{comp}}^{\dagger} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\le t} - \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\le t}\|_{\mathrm{op}} = O(t^2/2^{\lambda})$$

Lemma E.5. *We have the following:*

$$\|\mathcal{O}_{\mathsf{comp}}^{\dagger} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} - \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t}\|_{\mathrm{op}} = O(t^2/2^{\lambda})$$

Proof of Theorem 7.9. We recall that we want to estimate:

$$\begin{aligned}
\gamma &= \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\leq \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued}} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\quad + \left\| W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\quad + \left\| W_L^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\leq \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} \Pi^{\mathfrak{l},1} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} + O(t^2/2^\lambda) \\
&\leq \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}} + O(t^2/2^\lambda)
\end{aligned}$$

Where the second line is by triangle inequality, and the third line is by Theorem E.2, and the fourth line is true because $\Pi^{\mathfrak{l},1} = \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \right)$ and $\Pi^{\mathfrak{l},1} \Pi^{\mathsf{Good}} = \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1}$. Next, we compute

$$\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\leq t} \right\|_{\mathrm{op}}.$$

We know that the subspace represented by Π^{Good} is spanned by $|x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle$ for $x_0, x_1 \in \{0,1\}^n$, $w_1 \in \{0,1\}^\lambda$ and $\overline{S}$ is some good state parameter. Let $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$.

Computing $\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle$: We start by computing:

$$\begin{aligned}
|\phi_1\rangle =& \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle \\
=& \mathcal{O}_{\mathsf{comp}} |\chi^{\mathfrak{l},3}_{\mathfrak{G}(\overline{S}),(x_0,x_1)w_1}\rangle \\
=& \mathcal{O}_{\mathsf{comp}} \frac{1}{2^n \sqrt{2^\lambda - a}} \sum_{\substack{y_1,y_0 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))}} |y_0, w, y_1, \mathfrak{G}(\overline{S} \cup \{(\mathcal{LL}, (x_0,x_1), (y_0,y_1), w_1, w)\})\rangle \\
=& \frac{1}{2^n \sqrt{2^\lambda - a}} \sum_{\substack{y_1,y_0 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))}} |y_0, w, y_1, \mathfrak{F}(\overline{S} \cup \{(\mathcal{LL}, (x_0,x_1), (y_0,y_1), w_1, w)\})\rangle
\end{aligned}$$

Where the second line is by Theorem 6.13.

Computing $W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle$ We start by computing:

$$\begin{aligned}
|\phi_2\rangle =& W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle \\
=& W_L^{\mathfrak{m}(\lambda)} |x_0, w_1, x_1, \mathfrak{F}(\overline{S})\rangle \\
=& W_L^{\mathfrak{m}(\lambda)} \frac{1}{\sqrt{2^{(b-a)n} \left((2^\lambda - a) \dots (2^\lambda - b + 1)\right)}} \sum_{\substack{\mathcal{U} \in \{0,1\}^{(b-a)n} \\ \mathcal{V} \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))^{b-a}_{\mathrm{dist}}}} |x_0, w_1, x_1, \mathbb{F}(\overline{S}, \mathcal{U}, \mathcal{V})\rangle \\
=& \frac{1}{\sqrt{2^{(b-a)n} \left((2^\lambda - a) \dots (2^\lambda - b + 1)\right)}} \sum_{\substack{\mathcal{U} \in \{0,1\}^{(b-a)n} \\ \mathcal{V} \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))^{b-a}_{\mathrm{dist}}}} \sum_{\substack{y_1,y_0 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus (\mathrm{Im}(\overline{S}) \cup \mathcal{V}))}}
\end{aligned}$$

$$
\begin{aligned}
&\times \frac{1}{2^n\sqrt{2^\lambda - b}}|y_0, w, y_1, \mathbb{F}(\overline{S}, \mathcal{U}, \mathcal{V}) \cup (\{(x_0||w_1||x_1, y_0||w||y_1)\},)\rangle \\
=&\frac{1}{2^n\sqrt{2^{(b-a)n}\left((2^\lambda - a)\dots(2^\lambda - b)\right)}} \sum_{\substack{y_1, y_0 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus (\mathrm{Im}(\overline{S}))) \\ \mathcal{U} \in \{0,1\}^{(b-a)n} \\ \mathcal{V} \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}) \cup \{w\})^{b-a}_{\mathrm{dist}}}} \\
&\times |y_0, w, y_1, \mathbb{F}(\overline{S} \cup \{(\mathcal{LL}, (x_0, x_1), (y_0, y_1), w_1, w)\}, \mathcal{U}, \mathcal{V})\rangle \\
=&\frac{1}{2^n\sqrt{2^\lambda - a}} \sum_{\substack{y_1, y_0 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))}} |y_0, w, y_1, \mathfrak{F}(\overline{S} \cup \{(\mathcal{LL}, (x_0, x_1), (y_0, y_1), w_1, w)\})\rangle
\end{aligned}
$$

Hence, we have $|\phi_1\rangle = |\phi_2\rangle$. Since the subspace represented by Π^{Good} is spanned by $|x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle$, hence

$$
\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\le t} \right\|_{\mathrm{op}} = 0.
$$

Finally, we get

$$
\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},1} \Pi_{\le t} \right\|_{\mathrm{op}} = O(t^2/2^\lambda)
$$

□

Proof of Theorem 7.10. We recall that we want to estimate:

$$
\begin{aligned}
\gamma =& \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
\le& \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&+ \left\| W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&+ \left\| W_L^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
\le& \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \left(\Pi^{\mathcal{L},32} - \Pi^{\mathcal{L},321} \right) V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&+ O(t^2/2^\lambda)
\end{aligned}
$$

Where the second line is by triangle inequality, and the third line is by Theorem E.3. Also notice that $\Pi^{\mathcal{L},321} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \Pi^{\mathsf{Good}} = 0$. Hence, we have

$$
\gamma = \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} + O(t^2/2^\lambda)
$$

Next, we compute

$$
\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} - W_L^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}}
$$

We know by Theorem 6.10 that the subspace represented by $\Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2}$ is spanned by $|\chi^{\mathfrak{l},1}_{\overline{S},X,\vec{x},\vec{y},w_1}\rangle_{\mathsf{ABS\overline{ST}}} |x'\rangle_{\mathsf{CS}}$.

Computing $\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_R^{(1),\mathsf{mid},\dagger}|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}$: We start by computing:

$$\begin{aligned}
|\phi_1\rangle =&\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_R^{(1),\mathsf{mid},\dagger}\left(|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}\right)\\
=&\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}|\chi^{\mathfrak{r},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\mathcal{O}_{\mathsf{comp}}|\chi^{\mathfrak{r},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\mathcal{O}_{\mathsf{comp}}\frac{1}{2^n\sqrt{2^\lambda-a}}\sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w\in(\{0,1\}^{\lambda\setminus\mathrm{Im}(\overline{S})})}}|y_0,w,y_1,\mathfrak{G}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x}||x',y_0||\overrightarrow{y}||y_1,w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\frac{1}{2^n\sqrt{2^\lambda-a}}\sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w\in(\{0,1\}^{\lambda\setminus\mathrm{Im}(\overline{S})})}}|y_0,w,y_1,\mathfrak{F}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x}||x',y_0||\overrightarrow{y}||y_1,w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

Where the above is by Theorem 6.14.

Computing $W_L^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}$ We start by computing:

$$\begin{aligned}
|\phi_2\rangle =&W_L^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}\\
=&W_L^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\sum_{\substack{u\in\{0,1\}^n\\ v\in(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}))}}|u,v,x',\mathfrak{G}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x},\overrightarrow{y}||u,w_1,v)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&W_L^{\mathfrak{m}(\lambda)}\sum_{\substack{u\in\{0,1\}^n\\ v\in(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}))}}|u,v,x',\mathfrak{F}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x},\overrightarrow{y}||u,w_1,v)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\frac{1}{2^n\sqrt{2^\lambda-a}}\sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w\in(\{0,1\}^{\lambda\setminus\mathrm{Im}(\overline{S})})}}|y_0,w,y_1,\mathfrak{F}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x}||x',y_0||\overrightarrow{y}||y_1,w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

Hence, we have $|\phi_1\rangle=|\phi_2\rangle$. Since the subspace represented by $\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},2}$ is spanned by $|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}$, hence

$$\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_R^{(1),\mathsf{mid},\dagger}-W_L^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},2}\Pi_{\le t}\right\|_{\mathrm{op}}=0.$$

Finally, we get

$$\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}-W^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},2}\Pi_{\le t}\right\|_{\mathrm{op}}=O(t^2/2^\lambda)$$

□

Proof of Theorem 7.11. We recall that we want to estimate:

$$\begin{aligned}
\gamma=&\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}-W^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\le t}\right\|_{\mathrm{op}}\\
\le&\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}-(I-W_L^{\mathfrak{m}(\lambda)}W_L^{\mathfrak{m}(\lambda),\dagger})W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\le t}\right\|_{\mathrm{op}}\\
&+\left\|W_L^{\mathfrak{m}(\lambda)}(I-W_R^{\mathfrak{m}(\lambda)}W_R^{\mathfrak{m}(\lambda),\dagger})\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\le t}\right\|_{\mathrm{op}}\\
\le&\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{L},3}-\Pi^{\mathcal{L},32}\right)V_L^{(3),\mathsf{mid}}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}-(I-W_L^{\mathfrak{m}(\lambda)}W_L^{\mathfrak{m}(\lambda),\dagger})W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\le t}\right\|_{\mathrm{op}}\\
&+O(t^2/2^\lambda)
\end{aligned}$$

$$\leq \underbrace{\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{L},3}\right)V_L^{(3),\mathsf{mid}}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}-W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\leq t}\right\|_{\mathrm{op}}}_{\gamma_1}$$
$$+\underbrace{\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\left(\Pi^{\mathcal{L},32}\right)V_L^{(3),\mathsf{mid}}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}-(W_L^{\mathfrak{m}(\lambda)}W_L^{\mathfrak{m}(\lambda),\dagger})W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\leq t}\right\|_{\mathrm{op}}}_{\gamma_2}$$
$$+O(t^2/2^\lambda)$$

Where the second line is by triangle inequality, and the third line is by Theorem E.4, and the last line is by triangle inequality. Next, we compute γ_1 and γ_2. Before computing this, we know by Theorems 6.11 and 6.12 that the subspace represented by $\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},2}$ is spanned by $|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$s where $\mathsf{len}(\overrightarrow{x})>2$.

Computing γ_1: We start by looking at some fixed $\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1$ with $a=\mathsf{count}S$ and $b=\mathsf{len}(\overline{S})\cup\mathsf{len}(\overrightarrow{x})$. Then we will show

$$\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_L^{(3),\mathsf{mid}}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}-W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}=0$$

We start by computing the first term (call it $|\phi_1\rangle$):

$$\begin{aligned}
|\phi_1\rangle =&\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_L^{(3),\mathsf{mid}}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}|\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}\\
=&\mathcal{O}_{\mathsf{comp}}\frac{1}{\sqrt{2^n(2^\lambda-a)}}\sum_{\substack{y\in\{0,1\}^n\\ w\in(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}))}}|y,w,x',\mathfrak{G}(\overline{S}\cup\{(X\mathcal{L},\overrightarrow{x},\overrightarrow{y},w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&\frac{1}{\sqrt{2^n(2^\lambda-a)}}\sum_{\substack{y\in\{0,1\}^n\\ w\in(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}))}}|y,w,x',\mathfrak{F}(\overline{S}\cup\{(X\mathcal{L},\overrightarrow{x},\overrightarrow{y},w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

Where the above is by Theorem 6.14. Next, we compute the second term (call it $|\phi_2\rangle$):

$$\begin{aligned}
|\phi_2\rangle =&W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\
=&W_R^{\mathfrak{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\frac{1}{2^n\sqrt{2^\lambda-a}}\sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w\in(\{0,1\}\lambda\setminus\mathrm{Im}(\overline{S}))}}|y_0,w,y_1,\mathfrak{G}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x}||x',\overrightarrow{y},w_1,w)\})\rangle\\
=&W_R^{\mathfrak{m}(\lambda),\dagger}\frac{1}{2^n\sqrt{2^\lambda-a}}\sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w\in(\{0,1\}\lambda\setminus\mathrm{Im}(\overline{S}))}}|y_0,w,y_1,\mathfrak{F}(\overline{S}\cup\{(X\mathcal{R},\overrightarrow{x}||x',\overrightarrow{y},w_1,w)\})\rangle\\
=&\frac{1}{\sqrt{2^n(2^\lambda-a)}}\sum_{\substack{y\in\{0,1\}^n\\ w\in(\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S}))}}|y,w,x',\mathfrak{F}(\overline{S}\cup\{(X\mathcal{L},\overrightarrow{x},\overrightarrow{y},w_1,w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

Hence $|\phi_1\rangle=|\phi_2\rangle$. Hence, we get $\gamma_1=0$.
Similarly, we can show that $\gamma_2=O(t^2/2^\lambda)$. Hence combining, we get

$$\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}-W^{\mathfrak{m}(\lambda)}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},3}\Pi_{\leq t}\right\|_{\mathrm{op}}=O(t^2/2^\lambda).$$

□

Proof of Theorem 7.12. We recall that we want to estimate:

$$\begin{aligned}
\gamma &= \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\le \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - (I - W_L^{\mathfrak{m}(\lambda)} W_L^{\mathfrak{m}(\lambda),\dagger}) W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\quad + \left\| W_L^{\mathfrak{m}(\lambda)} (I - W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger}) \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\le \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \left(I - \Pi^{\mathcal{L},3} \right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} - (I - W_L^{\mathfrak{m}(\lambda)} W_L^{\mathfrak{m}(\lambda),\dagger}) W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\quad + O(t^2/2^\lambda) \\
&\le \underbrace{\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} - W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}}}_{\gamma_1} \\
&\quad + \underbrace{\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \left(\Pi^{\mathcal{L},3} \right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} - (W_L^{\mathfrak{m}(\lambda)} W_L^{\mathfrak{m}(\lambda),\dagger}) W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}}}_{\gamma_2} \\
&\quad + O(t^2/2^\lambda)
\end{aligned}$$

Where the second line is by triangle inequality, and the third line is by Theorem E.5, and the last line is by triangle inequality. Next, we compute γ_1 and γ_2. Before computing this, we know by Theorem 6.12 that the subspace represented by $\Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4}$ is spanned by $|\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}\mathsf{S}}$.

Computing γ_1: We start by looking at some fixed $\overline{S}, (x_0, x_1), w_1$ with $a = \mathsf{count} S$ and $b = \mathsf{len}(\overline{S})$. Then we will show

$$\left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} - W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \right) |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = 0$$

We start by computing the first term (call it $|\phi_1\rangle$):

$$\begin{aligned}
|\phi_1\rangle =& \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle \\
=& |x_0, w_1, x_1, \mathfrak{F}(\overline{S})\rangle
\end{aligned}$$

Where the above is by Theorem 6.13. Next, we compute the second term (call it $|\phi_2\rangle$):

$$\begin{aligned}
|\phi_2\rangle =& W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \frac{1}{2^n \sqrt{2^\lambda - a}} \sum_{\substack{y_0, y_1 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))}} |y_0, w, y_1, \mathfrak{G}(\overline{S} \cup \{(\mathcal{LL}, (x_0, x_1), (y_0, y_1), w_1, w)\})\rangle \\
=& W_R^{\mathfrak{m}(\lambda),\dagger} \frac{1}{2^n \sqrt{2^\lambda - a}} \sum_{\substack{y_0, y_1 \in \{0,1\}^n \\ w \in (\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S}))}} |y_0, w, y_1, \mathfrak{F}(\overline{S} \cup \{(\mathcal{LL}, (x_0, x_1), (y_0, y_1), w_1, w)\})\rangle \\
=& |x_0, w_1, x_1, \mathfrak{F}(\overline{S})\rangle
\end{aligned}$$

Hence $|\phi_1\rangle = |\phi_2\rangle$. Hence, we get $\gamma_1 = 0$.
Similarly, we can show that $\gamma_2 = O(t^2/2^\lambda)$.

Hence combining, we get

$$\left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} - W^{\mathfrak{m}(\lambda)} \mathcal{O}_{\mathsf{comp}} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},4} \Pi_{\le t} \right\|_{\mathrm{op}} = O(t^2/2^\lambda).$$

□