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 merge of this work and [ABGL25] appeared in CRYPTO 2025.

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

Contents

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.

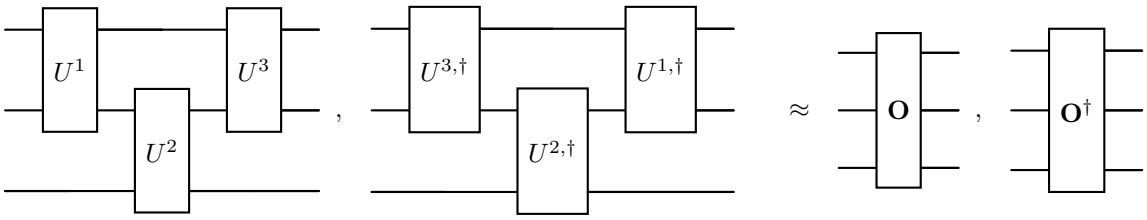
The disadvantage of the above gluing theorem is that the closeness to the joining random unitary does not hold if additionally oracle access to the inverse of the glued unitary is provided. In many applications, giving both forward and inverse access is important. As noted in [FPVY25], to determine lightcones, 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 (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 with the construction of strong PRUs in the quantum Haar random oracle model [ABGL25], 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 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 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

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. We define the following two operators (which are also partial isometries) such that for any relations L, R,[1]

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

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

[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.

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

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

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 $N = 2^n$.
For intuition, throughout this section we work with a more intuitive form of Path Recording Framework. In the technical sections, we switch work with the Path Recording Framework from [MH24]. The more intuitive form we work with is:

$$V^{\mathsf{fwd}} = V_L \cdot (I - V_R \cdot V_R^\dagger) + V_R^\dagger$$

and

$$V^{\mathsf{inv}} = V_R \cdot (I - V_L \cdot V_L^\dagger) + V_L^\dagger$$

We can think of querying V^{fwd} instead of V and V^{inv} instead of $V^\dagger$.[2] While these aren't partial isometries like the Path Recording Framework, but they capture the essence of Path Recording. For example, if we look at V^{fwd} operationally, it can be seen as the following action:

- If the input is in range of V_R, invert the V_R, i.e. delete an entry from the database R. We'll call this the "deletion branch".
- If the input is orthogonal to the range of V_R, apply V_L, i.e. add an entry from the database L. We'll call this the "addition branch".

Similarly for V^{inv}, one can again define a "deletion branch" and an "addition branch". Here, when you query some input to the addition branch, it creates an almost maximally entangled state, returns one half on the query register and appends the other half to the database register with the label as the input. The deletion branch checks if the query register is maximally entangled with something in the database register, and if it is, return the label associated with the entry in the database and deletes the maximally entangled pair.

2.1 The Strong Gluing Theorem

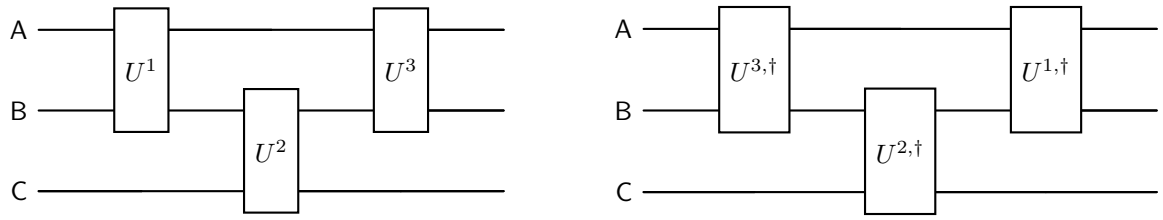
In our second main result, we show that for three Haar random unitaries, U^1, U^2, and U^3, applying them in a shifted brickwork pattern, overlapping on some register B, yields an ensemble that is indistinguishable from a larger Haar random unitary to any adversary, with inverse access, making $\mathsf{poly}(|\mathsf{B}|)$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

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

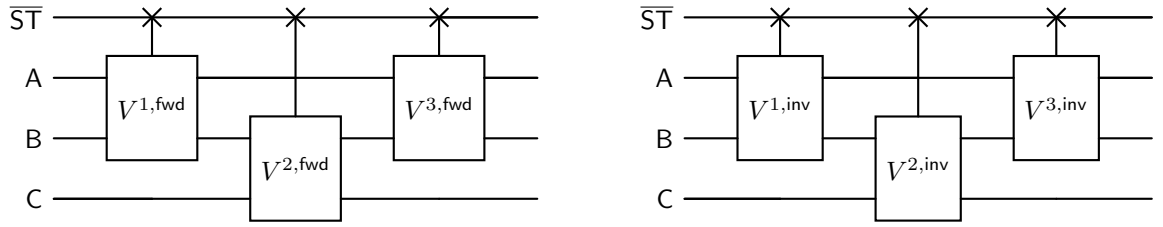
[2] Notice that we drop the $(I - V_L \cdot V_L^\dagger)$ after $V_R^\dagger$ in V to get V^{fwd}. $(I - V_L \cdot V_L^\dagger)$ can be seen as the projector that makes V a partial isometry, dropping it makes the action more intuitive to understand but for analysing formally, we include this projector in the analysis.

2.2 Construction and Path-Recording Framework

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 Path recording circuit 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 there's an "addition" and a "deletion" branch associated with each of the $V^{i,\mathsf{fwd}}$. Notice that a query to the "addition" branch of any $V^{i,\mathsf{fwd}}$ returns a state which is maximally entangled with a new entry in the corresponding S_i. Since we make queries to the $V^{i,\mathsf{fwd}}$'s sequentially (i.e. $V^{1,\mathsf{fwd}}$ then $V^{2,\mathsf{fwd}}$ then $V^{3,\mathsf{fwd}}$). Let there is a query to the addition branch on $V^{1,\mathsf{fwd}}$, then the output is maximally entangled with S_1. Then by monogamy of entanglement, this state cannot be maximally entangled with something in T_2. Note that the deletion branch of $V^{2,\mathsf{fwd}}$ checks whether the query register is maximally entagled with anything in T_2. Hence, if the "addition" branch was applied on $V^{1,\mathsf{fwd}}$, then the deletion branch on $V^{2,\mathsf{fwd}}$ has small weight. Similarly, if the "addition" branch was applied on $V^{2,\mathsf{fwd}}$, then the deletion branch on $V^{3,\mathsf{fwd}}$ has small weight. Formally, we can show that

$$\|V_R^{i+1,\dagger}V_L^i\| = \mathsf{negl}(\lambda).$$

Hence, combining the above intuition, we get that

$$\begin{aligned} V^{3,\mathsf{fwd}}V^{2,\mathsf{fwd}}V^{1,\mathsf{fwd}} \approx_{\mathrm{op}} & V_L^3V_L^2V_L^1\left(I - V_R^1V_R^{1,\dagger}\right) + V_L^3V_L^2\left(I - V_R^2V_R^{2,\dagger}\right)V_R^{1,\dagger} \\ & + V_L^3\left(I - V_R^3V_R^{3,\dagger}\right)V_R^{2,\dagger}V_R^{1,\dagger} + V_R^{3,\dagger}V_R^{2,\dagger}V_R^{1,\dagger} \end{aligned}$$

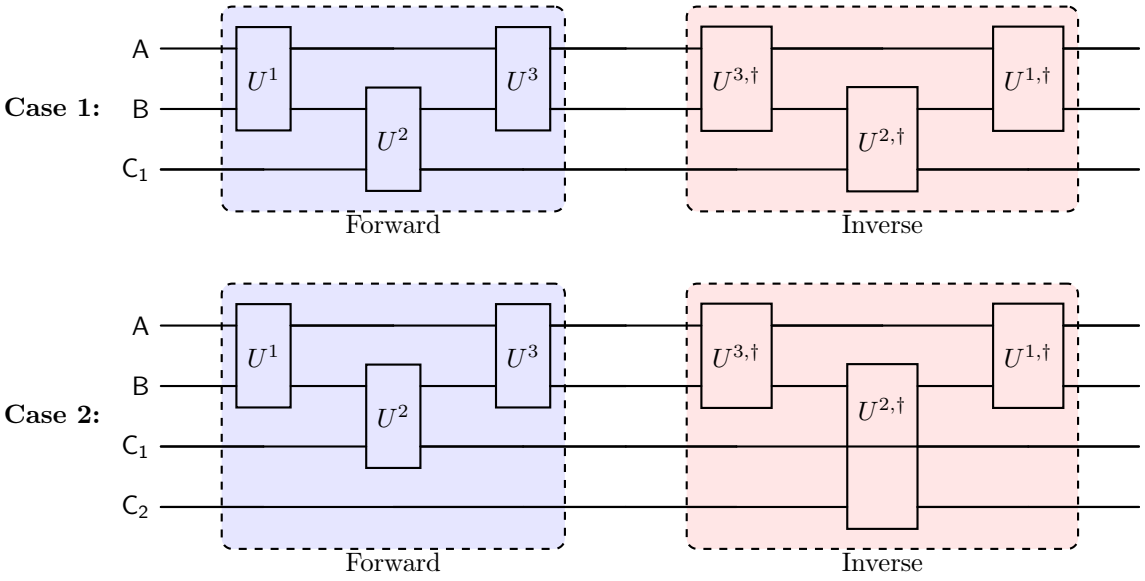
Where each of the term corresponds to a certain action. Intuitively, this can be seen as:

- **Term 1:** Corresponds to "addition" branch on $V^{1,\mathsf{fwd}}$, followed by $V^{2,\mathsf{fwd}}$, followed by $V^{3,\mathsf{fwd}}$.
- **Term 2:** Corresponds to "deletion" branch on $V^{1,\mathsf{fwd}}$, followed by "addition" branch on $V^{2,\mathsf{fwd}}$, followed by $V^{3,\mathsf{fwd}}$.
- **Term 3:** Corresponds to "deletion" branch on $V^{1,\mathsf{fwd}}$, followed by $V^{2,\mathsf{fwd}}$, followed by "addition" branch on $V^{3,\mathsf{fwd}}$.
- **Term 4:** Corresponds to "deletion" branch on $V^{1,\mathsf{fwd}}$, followed by $V^{2,\mathsf{fwd}}$, followed by $V^{3,\mathsf{fwd}}$.

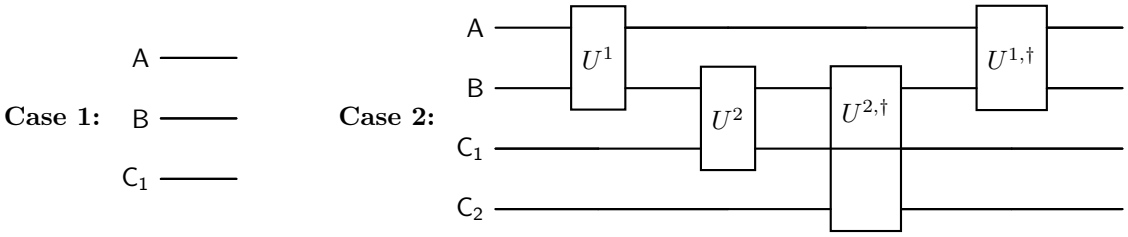
Corresponding to each of these branches, we can define four disjoint subspaces where these operations are applied. Formally, we define this approximation of Path-Recording in Section 4.1 and these subspaces in Section 4.3. Most our proofs are first done in these subspaces and then combined to get a combined result.

2.2.1 Modelling Achievable States

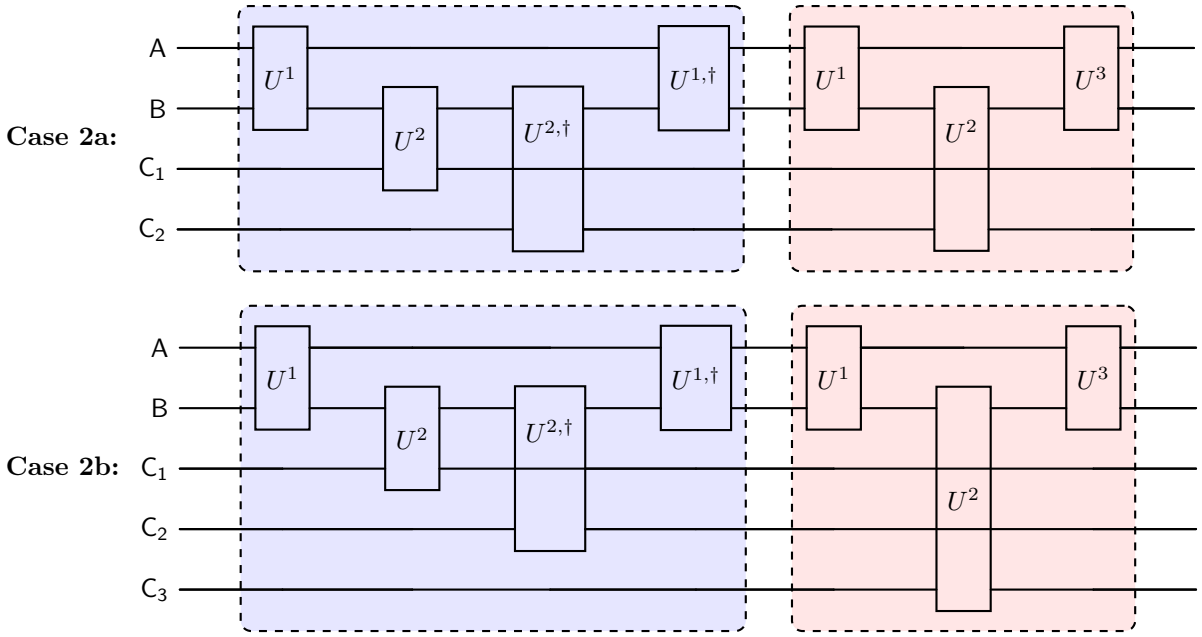
Next we try to model these states achievable by querying the Haar unitaries. Notice that in general, it is hard to invert a Haar unitary without querying its inverse. Hence, let's say the adversary wants to invert the U^3 on the output of a query to the first oracle; they can invert it by querying the second oracle with the first two registers overlapping. In this case, the third query register either has significant overlap with the third register of the state or it has less than significant overlap (for intuition purposes, we use the term significant loosely, meaning either completely or not at all). This looks like follows:



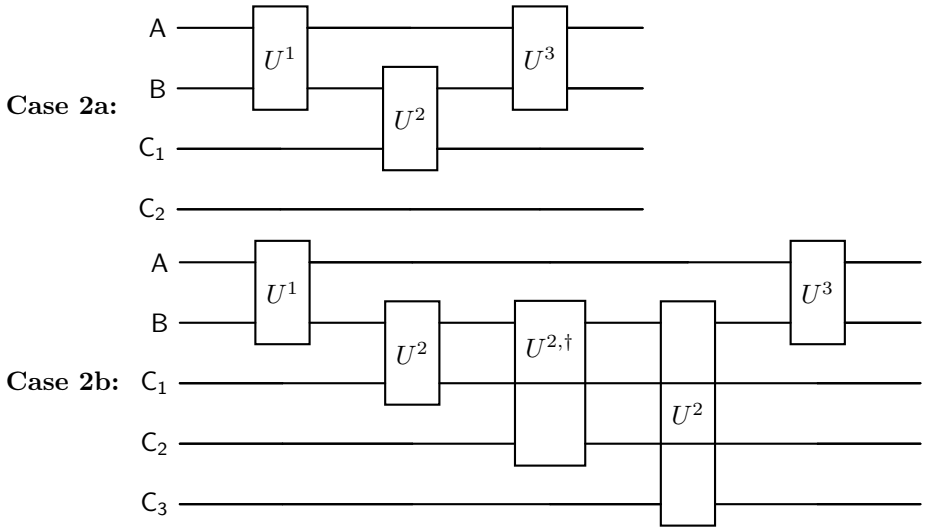
Simplifying, we get that



Notice that in trying to invert U^3, either we invert the whole glued unitary or inverts just U^3 while adding two unitaries ($U^{2,\dagger}$ and $U^{1,\dagger}$) on top. We notice two things in above. First, the register A which has only two gates applied to it (the first, i.e. U^1 and the last, i.e. $U^{1,\dagger}$). Second, the register B has all gates applied to it. Also notice that intermediate values on register A and register B are not accessible to the adversary. Finally, lets look at one more step. In particular, let's say the adversary wants to invert the $U^{1,\dagger}$ on the output of case 2 above; they can invert it by querying the first oracle with the first two registers overlapping. In this case, the third query register either has significant overlap with C_2 of the state or it has less than significant overlap (for intuition purposes, we use the term significant loosely, meaning either completely or not at all). This looks like follows:

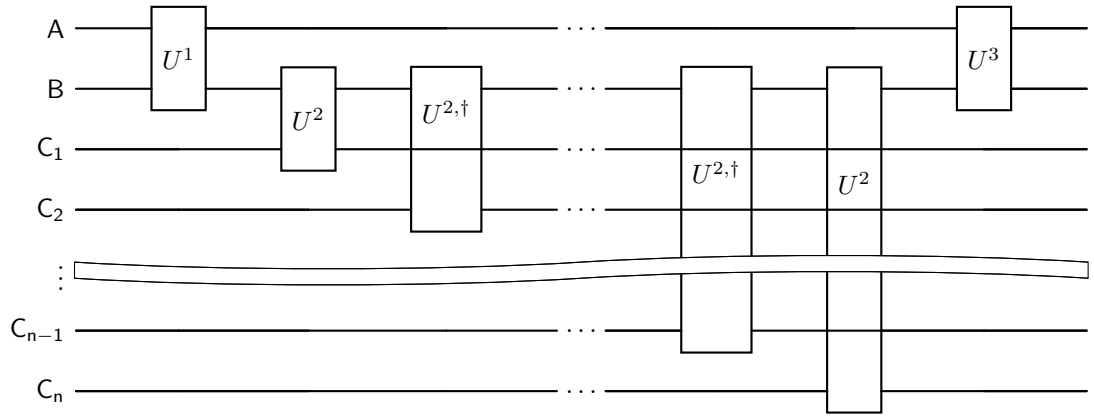


Simplifying, we get

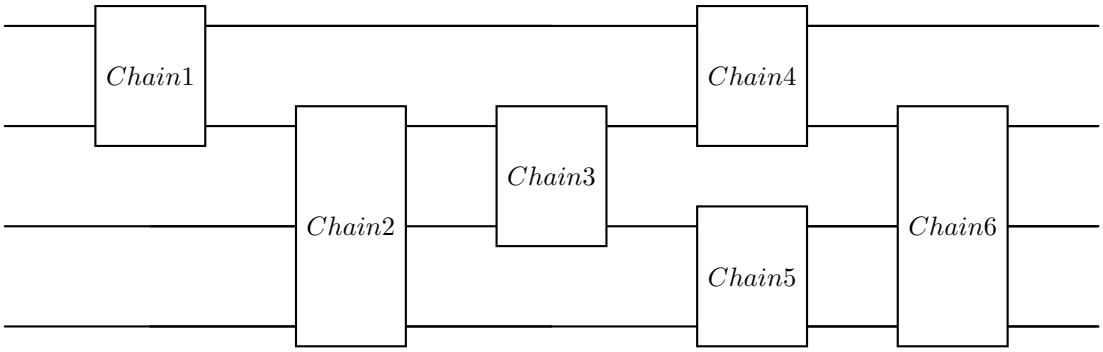


Notice that Case 2a is just equivalent to a single query to the first oracle. Case 2b has multiple unitaries chained together. Notice the similar two properties as before. First, the register A which has only two gates applied to it (the first, i.e. U^1 and the last, i.e. U^3). Second, the register B has all gates applied to it. Also notice that intermediate values on register A and register B are not accessible to the adversary.

Notice that we could start this from a call to the second oracle instead of first, in this case the first unitary in the chain is $U^{3,\dagger}$ instead of U^1 on AB. Extending the intuition, we can get chains of unitaries starting at U^1 or $U^{3,\dagger}$ on AB then multiple instances of alternating U^2 and $U^{2,\dagger}$ all passing through B (and subsequent unitary not applied to the same C_i registers), finally ending in either U^3 or $U^{1,\dagger}$ on AB. Pictorially, this looks as follows:



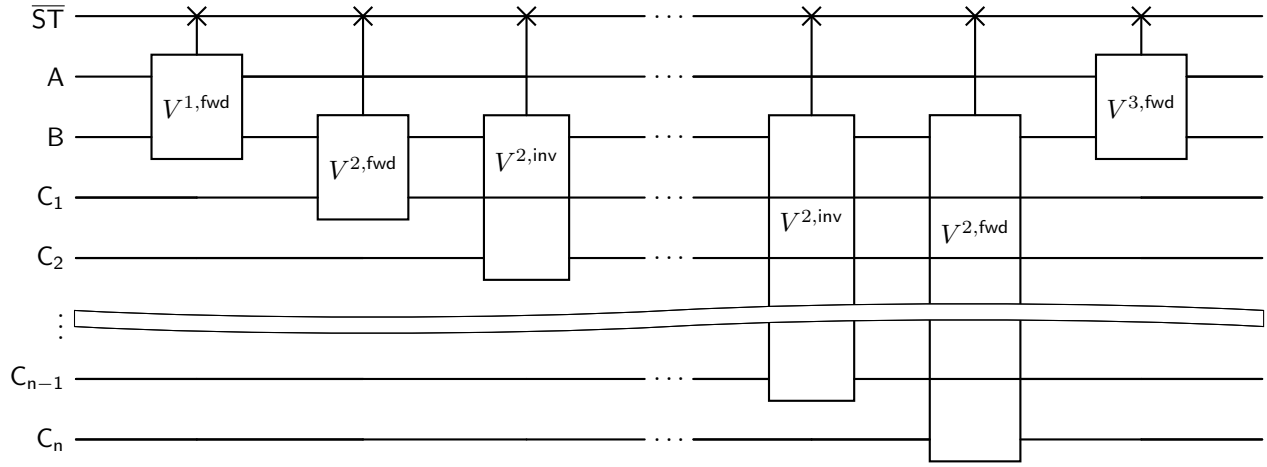
Similarly, the above could have started with $U^{3,\dagger}$ and ended with $U^{1,\dagger}$. Thinking of the above as a "chain" of unitaries. Then we want to imagine any adversary's circuit as some "chains" strung together. We give an example below:



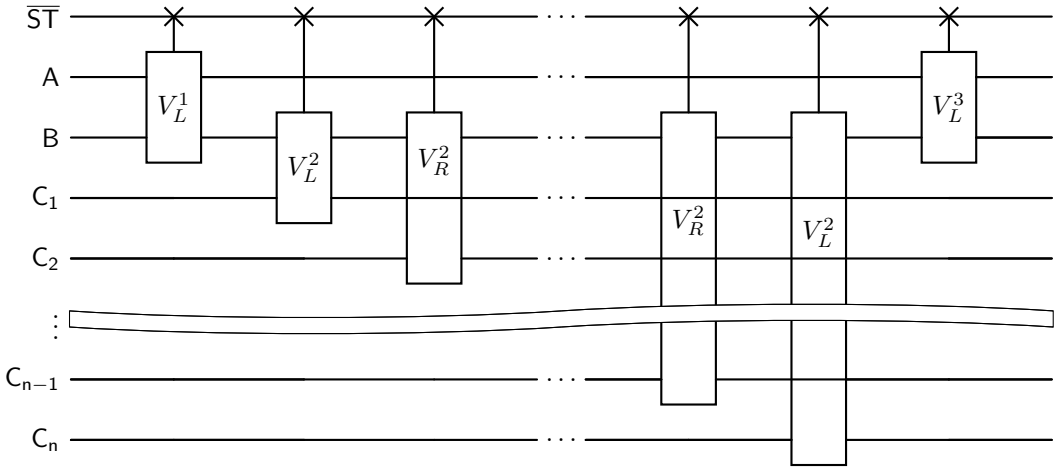
We want to formalise the intuition above, any adversary querying the oracles can be broken as multiple chains. To formalise the above intuition, we use path recording as below.

2.2.2 Using Path Recording and Formalising "Achievable States"

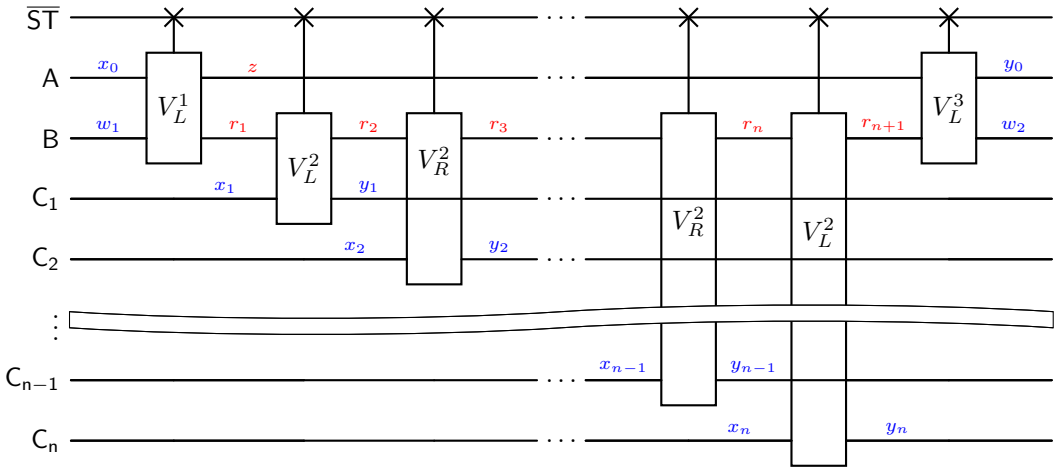
We start by considering a single chain (which starts with U^1 and ends with U^3, the other three cases can be analysed similarly). To start formalising, we start by switching Haar unitaries $(U^1, U^{1,\dagger})$, $(U^2, U^{2,\dagger})$, $(U^3, U^{3,\dagger})$ to the simplified Path Recording Isometries $(V^{1,\mathsf{fwd}}, V^{1,\mathsf{inv}})$, $(V^{2,\mathsf{fwd}}, V^{2,\mathsf{inv}})$ and $(V^{3,\mathsf{fwd}}, V^{3,\mathsf{inv}})$. Let these isometries work on purification register $\overline{\mathsf{ST}} = (\mathsf{S}_1\mathsf{T}_1, \mathsf{S}_2\mathsf{T}_2, \mathsf{S}_3\mathsf{T}_3)$. Then switching to Path Recording, a single chain looks as follows:



We first start by noticing that for the above path recording isometries, again because of monogamy of entanglement, most of their weight lies on the "addition branch" and hence only they need to be considered. Intuitively, this is because the output of the unitaries do not "line up", one should not be able to invert them. Then the above chain looks as follows:



We label the values on each wire to understand how the database register changes, 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 not visible to the adversary. Then on the above labels, the database register looks as follows:

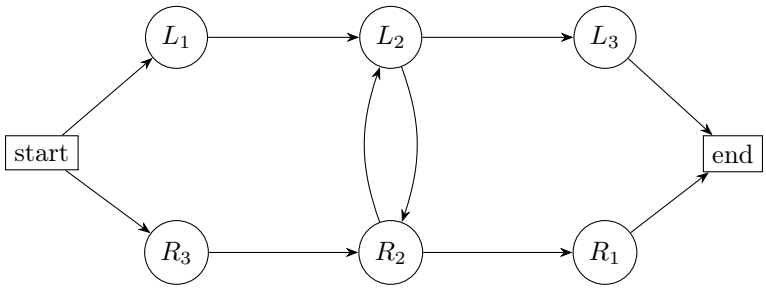
$$
\begin{aligned}
&|\{(x_0||w_1, z||r_1)\}\rangle_{\mathsf{S}_1}|\{\}\rangle_{\mathsf{T}_1} \\
&\otimes |\{(r_1||x_1, r_2||y_1), \ldots, (r_n||x_n, r_{n+1}||y_n)\}\rangle_{\mathsf{S}_2} \\
&\otimes |\{(r_2||x_2, r_3||y_2), \ldots, (r_{n-1}||x_{n-1}, r_n||y_{n-1})\}\rangle_{\mathsf{T}_2} \\
&\otimes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

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 touple 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).

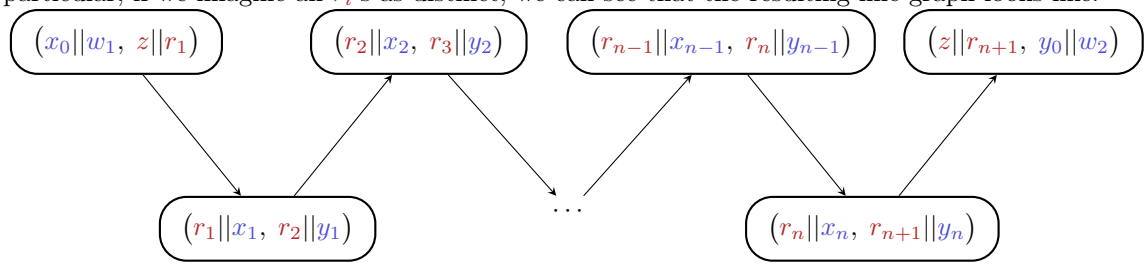
Drawing edge structure, we get edges of the following form:



Looking back at the example we had, recall that the database register looks like:

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

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



Then for notational ease, the above database/line graph can be denoted by $\mathfrak{p}_{LL}(\vec{x}, \vec{y}, w_1, w_2, \vec{r}, z)$ where $\vec{x} = (x_0, \ldots, x_n)$, $\vec{y} = (y_0, \ldots, y_n)$ and $\vec{r} = (r_0, \ldots, r_n)$. We add the "$LL$" for chains graphs starting at L_1 and ending at L_3. We can similarly define "LR", "RL" and "RR" chains. Formally, we get:

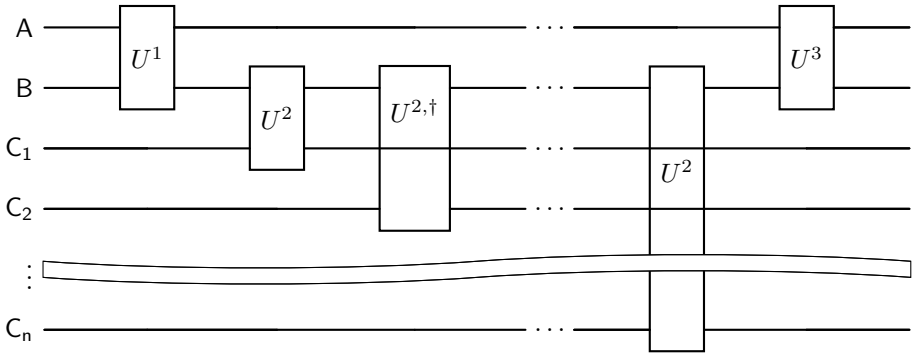
$$|\mathfrak{p}_{LL}(\vec{x}, \vec{y}, w_1, w_2, \vec{r}, z)\rangle = |\{(x_0||w_1, z||r_1)\}\rangle_{\mathsf{S}_1}|\{\}\rangle_{\mathsf{T}_1}$$

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

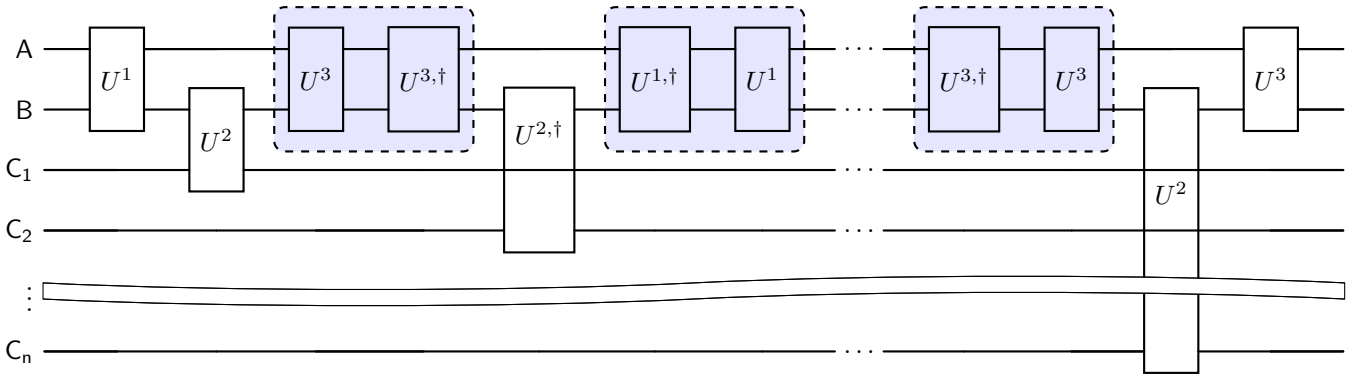
If we imagine any adversary's circuit as some "chains" strung together (recall the example from before), then corresponding to each chain, we get a disjoint line graph, and the database register corresponds to the union of databases corresponding to these disjoint line graphs.
By query-by-query analysis, we can show that for any poly-query adversary, the database register has almost all of its weight on databases corresponding to the union of databases corresponding to the disjoint line graphs. This, in spirit, shows that for any poly-query adversary, the query structure can be broken into these disjoint chains.
In fact, we can show something even stronger. Recall that we noticed that the adversary could not see the *red* labels corresponding to the line graphs. To formalise this, we can say that once you fix all the *blue* labels, the adversary's register is independent of the *red* labels. Hence, we can parametrize the adversary's state with only the *blue* labels. To see what this means formally and how we show this by query-by-query analysis, we refer the reader to Section 5.

2.2.3 Simulating the Larger Haar Unitary

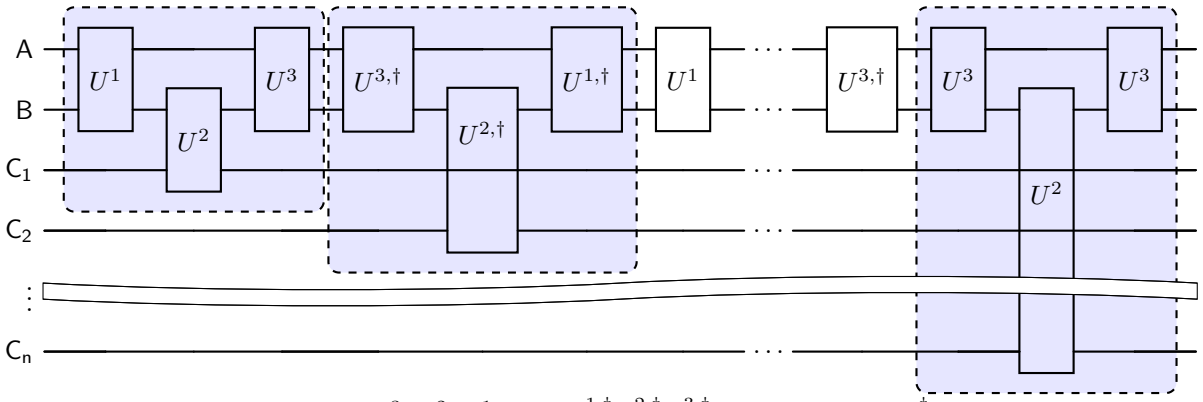
Now that we know that the adversary's query structure can be broken into disjoint chains. To seen how to simulate the larger Haar unitary, we will first see what a single disjoint chain looks like and then see what a corresponding database register looks like. To start, we again consider a chain as example:



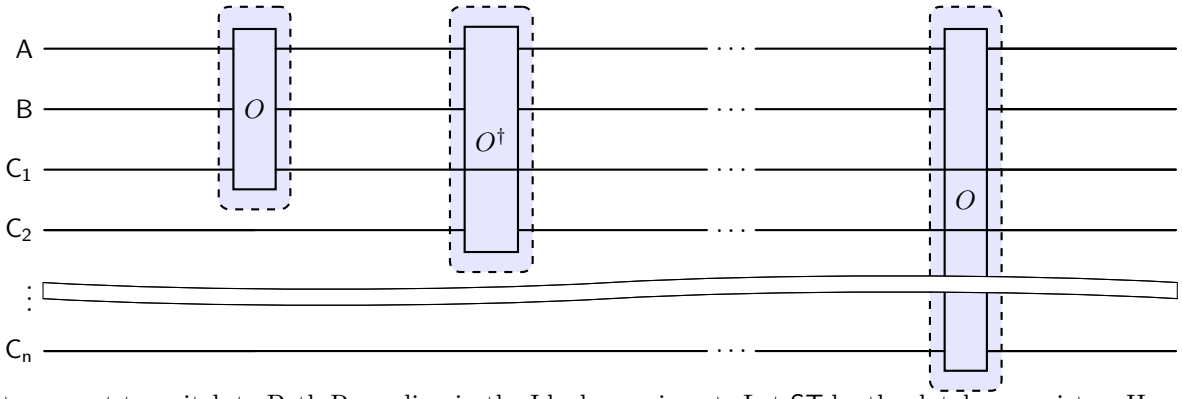
We know that in the Ideal experiment, we replace $U^3_{\mathsf{AB}} U^2_{\mathsf{BC}} U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}} U^{2,\dagger}_{\mathsf{BC}} U^{3,\dagger}_{\mathsf{AB}}$ with O_{ABC} and $O^\dagger_{\mathsf{ABC}}$, respectively. To do this, we insert dummy unitaries in the abvoe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



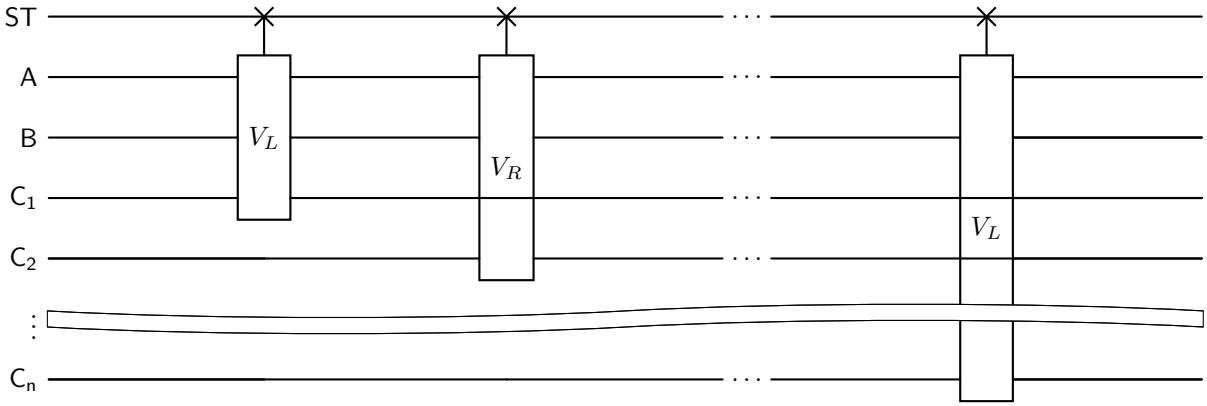
Notice that doing this, each component of the chain can be seen as queries to $U^3_{\mathsf{AB}} U^2_{\mathsf{BC}} U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}} U^{2,\dagger}_{\mathsf{BC}} U^{3,\dagger}_{\mathsf{AB}}$. In particular, the chain looks like alternating queries to $U^3_{\mathsf{AB}}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



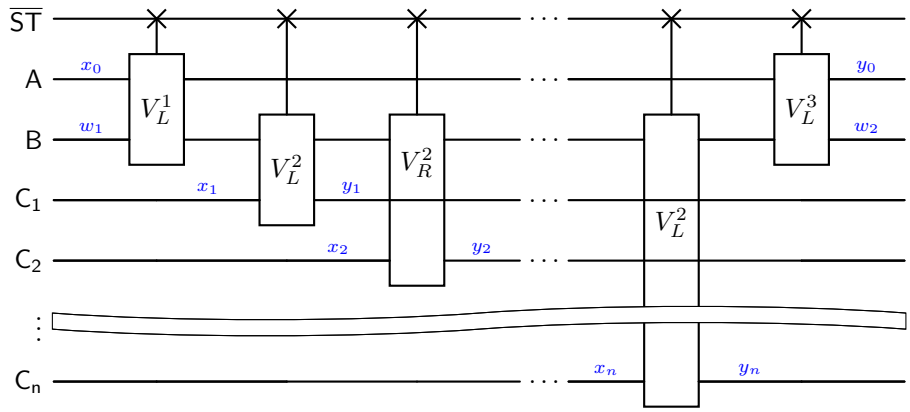
In the Ideal experiment, we replace $U^3_{\mathsf{AB}}U^2_{\mathsf{BC}}U^1_{\mathsf{AB}}$ and $U^{1,\dagger}_{\mathsf{AB}}U^{2,\dagger}_{\mathsf{BC}}U^{3,\dagger}_{\mathsf{AB}}$ with O_{ABC} and $O^\dagger_{\mathsf{ABC}}$, respectively. Hence, the chain becomes alternating queries to O_{ABC} and $O^\dagger_{\mathsf{ABC}}$.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



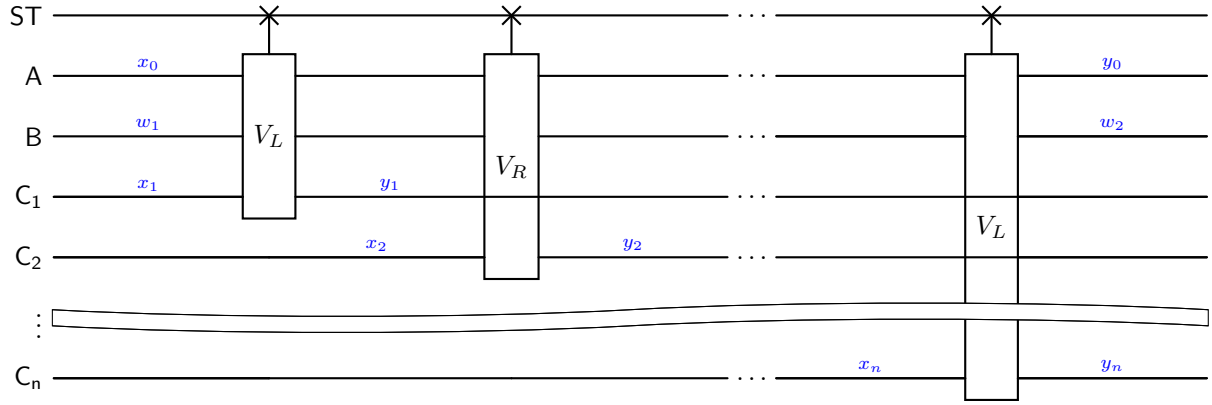
Next we want to switch to Path Recording in the Ideal experiment. Let ST be the database register. Hence, we switch O_{ABC} with V_L and $O^\dagger_{\mathsf{ABC}}$ with V_R (this is because most weight again lies on only "addition branch"). Hence, our example looks like:



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:



Notice that we skip the *red* labels in below because we showed that the adversaries state only depended on the *blue* labels. Similarly, we add these labels to the Ideal experiement as below:



Notice that in the above we skip the intermediate labels on the AB, this is because by similar analysis we can show that the adversaries state is independent of these labels. Finally, analysing 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 6.2.

2.2.4 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:

$$V^{\mathsf{fwd}}\mathcal{O}_{\mathsf{comp}}|\psi\rangle \quad \text{and} \quad \mathcal{O}_{\mathsf{comp}}V^{3,\mathsf{fwd}}V^{2,\mathsf{fwd}}V^{1,\mathsf{fwd}}|\psi\rangle\,,$$

which we establish by proving that the operator norm bound

$$\|(V^{\mathsf{fwd}}\mathcal{O}_{\mathsf{comp}} - \mathcal{O}_{\mathsf{comp}}V^3V^2V^1)\Pi_{\leq t}\|_{\mathrm{op}} = \mathsf{negl}(n)\,,$$

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.

$$\|(V^{\mathsf{inv}}\mathcal{O}_{\mathsf{comp}} - \mathcal{O}_{\mathsf{comp}}V^{1,\mathsf{inv}}V^{2,\mathsf{inv}}V^{3,\mathsf{inv}})\Pi_{\leq t}\|_{\mathrm{op}} = \mathsf{negl}(n)$$

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 6.4. By establishing these bounds, we can inductively analyze the adversary's distinguishing advantage after each query (for details, see Section 6.3). 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 4 (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 5 ($\mathrm{Dom}(R)$ and $\mathrm{Im}(R)$)**.** *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 6 (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 7 (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 $\overrightarrow{x^{\mathfrak{l}(n)}} = (x_1^{\mathfrak{l}(n)}, \ldots, x_t^{\mathfrak{l}(n)})$.*[3]

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.

Definition 8 (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 9. *For any operator A and vector $|\psi\rangle$, $\||A|\psi\rangle\|_2 \leq \|A\|_{\text{op}}\||\psi\rangle\|_2$.*

Lemma 10. *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 $\|A\|_{\text{op}} = \max_{|i\rangle\in\mathcal{B}} \|A|i\rangle\|_2$.*

Lemma 11. *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.*

3.4 Path-Recording Framework

We define the following two operators (which are also partial isometries): for any relations L, R,

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

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

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 12 ([MH24, Theorem 8])**.** *For any t-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 $|\mathcal{A}_t^{V,V^\dagger}\rangle = \prod_{i=1}^t \left(V^\dagger B_i V A_i\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}$.

[3] 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.

3.5 Restricted Path-Recording

We define the following restricted path-recording operator as:

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

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

Finally, define:

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

Lemma 13. *For any t-query algorithm $\mathcal{A} = (A_1, B_1, \ldots, A_t, B_t)$,*

$$\mathsf{TD}\left(\mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{W^{\mathfrak{m}(\lambda)},W^{\mathfrak{m}(\lambda),\dagger}}\rangle\langle\mathcal{A}_t^{W^{\mathfrak{m}(\lambda)},W^{\mathfrak{m}(\lambda),\dagger}}|\right), \mathrm{Tr}_{\mathsf{ST}}\left(|\mathcal{A}_t^{V,V^\dagger}\rangle\langle\mathcal{A}_t^{V,V^\dagger}|\right)\right) \le O\left(\sqrt{\frac{t^4}{2^\lambda}}\right),$$

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

The proof of the above lemma is provided in Appendix A

4 Glued Path-Recording

In this section, we study the variants of Path-Recording that simulates the Glued Haar unitary.

4.1 Glued Path-Recording

We define the following operators:

$$\begin{aligned}
V^{\text{glued-fwd}} =& V_L^3V_L^2V_L^1\left(I - V_R^1V_R^{1,\dagger}\right) + V_L^3V_L^2\left(I - V_R^2V_R^{2,\dagger} - V_L^1V_L^{1,\dagger}\right)V_R^{1,\dagger}\\
&+ V_L^3\left(I - V_R^3V_R^{3,\dagger} - V_L^2V_L^{2,\dagger}\right)V_R^{2,\dagger}V_R^{1,\dagger} + \left(I - V_L^3V_L^{3,\dagger}\right)V_R^{3,\dagger}V_R^{2,\dagger}V_R^{1,\dagger}\\
V^{\text{glued-inv}} =& V_R^1V_R^2V_R^3\left(I - V_L^3V_L^{3,\dagger}\right) + V_R^1V_R^2\left(I - V_L^2V_L^{2,\dagger} - V_R^3V_R^{3,\dagger}\right)V_L^{3,\dagger}\\
&+ V_R^1\left(I - V_L^1V_L^{1,\dagger} - V_R^2V_R^{2,\dagger}\right)V_L^{2,\dagger}V_L^{3,\dagger} + \left(I - V_R^1V_R^{1,\dagger}\right)V_L^{1,\dagger}V_L^{2,\dagger}V_L^{3,\dagger}
\end{aligned}$$

Then we have the following:

Lemma 14. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

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

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

4.2 Glued Restricted Path-Recording

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 define the following operator:

$$W^{\mathsf{glued\text{-}fwd}} = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}\right)$$

$$
\begin{aligned}
&+ V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} \\
&+ V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger}\right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&+ \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
W^{\mathsf{glued\text{-}inv}} =& V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) \\
&+ V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} \left(I - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger} - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger}\right) V_L^{(3),\mathsf{mid},\dagger} \\
&+ V_R^{(1),\mathsf{mid}} \left(I - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}\right) V_L^{(2),\mathsf{mid},\dagger} V_L^{(3),\mathsf{mid},\dagger} \\
&+ \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}\right) V_L^{(1),\mathsf{mid},\dagger} V_L^{(2),\mathsf{mid},\dagger} V_L^{(3),\mathsf{mid},\dagger}
\end{aligned}
$$

Then we have the following:

Lemma 15. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

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

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

The proof of the above lemma is similar to Appendix A.

4.3 Defining Forward Subspaces

We define four important subspaces:

- **Subspace 1:** Define
$$\Pi^{\mathfrak{l},1} = I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}.$$
- **Subspace 2:** Define
$$\Pi^{\mathfrak{l},2} = V_R^{(1),\mathsf{mid}} (I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid},\dagger}.$$
- **Subspace 3:** Define
$$\Pi^{\mathfrak{l},3} = V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} (I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger}) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}.$$
- **Subspace 4:** Define
$$\Pi^{\mathfrak{l},4} = V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}.$$

An alternate way to define the above subspaces, we instead define the following projectors:

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

Then notice that $\Pi^{\mathfrak{l},1} = I - \Pi^{\mathcal{R},1}$, $\Pi^{\mathfrak{l},2} = \Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12}$, $\Pi^{\mathfrak{l},3} = \Pi^{\mathcal{R},12} - \Pi^{\mathcal{R},123}$ and $\Pi^{\mathfrak{l},4} = \Pi^{\mathcal{R},123}$.
Proofs of all lemmas in this subsection are in Appendix C.
First notice the following:

Lemma 16. *Let for $i \in [4]$, $\Pi^{\mathfrak{l},i}$ be defined as above, then:*

$$\sum_{i=1}^{4} \Pi^{\mathfrak{l},i} = I$$

Lemma 17. *Let $W^{\text{glued-fwd}}$ and $\Pi^{\mathfrak{l},1}$ be defined as above, then:*

$$W^{\text{glued-fwd}}\Pi^{\mathfrak{l},1} = V_L^{(3),\text{mid}} V_L^{(2),\text{mid}} V_L^{(1),\text{mid}} \left(I - V_R^{(1),\text{mid}} V_R^{(1),\text{mid},\dagger}\right)$$

Lemma 18. *Let $W^{\text{glued-fwd}}$ and $\Pi^{\mathfrak{l},2}$ be defined as above, then:*

$$\|W^{\text{glued-fwd}}\Pi^{\mathfrak{l},2} - V_L^{(3),\text{mid}} V_L^{(2),\text{mid}} \left(I - V_R^{(2),\text{mid}} V_R^{(2),\text{mid},\dagger} - V_L^{(1),\text{mid}} V_L^{(1),\text{mid},\dagger}\right) V_R^{(1),\text{mid},\dagger}\|_{\text{op}} = O(t^2/2^\lambda)$$

Lemma 19. *Let $W^{\text{glued-fwd}}$ and $\Pi^{\mathfrak{l},3}$ be defined as above, then:*

$$\|W^{\text{glued-fwd}}\Pi^{\mathfrak{l},3} - V_L^{(3),\text{mid}} \left(I - V_R^{(3),\text{mid}} V_R^{(3),\text{mid},\dagger} - V_L^{(2),\text{mid}} V_L^{(2),\text{mid},\dagger}\right) V_R^{(2),\text{mid},\dagger} V_R^{(1),\text{mid},\dagger}\|_{\text{op}} = O(t^2/2^\lambda)$$

Lemma 20. *Let $W^{\text{glued-fwd}}$ and $\Pi^{\mathfrak{l},4}$ be defined as above, then:*

$$\|W^{\text{glued-fwd}}\Pi^{\mathfrak{l},4} - \left(I - V_L^{(3),\text{mid}} V_L^{(3),\text{mid},\dagger}\right) V_R^{(3),\text{mid},\dagger} V_R^{(2),\text{mid},\dagger} V_R^{(1),\text{mid},\dagger}\|_{\text{op}} = O(t^2/2^\lambda)$$

4.4 Defining Inverse Subspaces

Similar to above, we define four more important subspaces:

- **Subspace 1:** Define
$$\Pi^{\mathfrak{r},1} = I - V_L^{(1),\text{mid}} V_L^{(1),\text{mid},\dagger}.$$
- **Subspace 2:** Define
$$\Pi^{\mathfrak{r},2} = V_L^{(1),\text{mid}} (I - V_L^{(2),\text{mid}} V_L^{(2),\text{mid},\dagger}) V_L^{(1),\text{mid},\dagger}.$$
- **Subspace 3:** Define
$$\Pi^{\mathfrak{r},3} = V_L^{(1),\text{mid}} V_L^{(2),\text{mid}} (I - V_L^{(3),\text{mid}} V_L^{(3),\text{mid},\dagger}) V_L^{(2),\text{mid},\dagger} V_L^{(1),\text{mid},\dagger}.$$
- **Subspace 4:** Define
$$\Pi^{\mathfrak{r},4} = V_L^{(1),\text{mid}} V_L^{(2),\text{mid}} V_L^{(3),\text{mid}} V_L^{(3),\text{mid},\dagger} V_L^{(2),\text{mid},\dagger} V_L^{(1),\text{mid},\dagger}.$$

An alternate way to define the above subspaces, we instead define the following projectors:

$$\begin{aligned}
\Pi^{\mathcal{L},1} &= V_L^{(1),\text{mid}} V_L^{(1),\text{mid},\dagger} \\
\Pi^{\mathcal{L},12} &= V_L^{(1),\text{mid}} V_L^{(2),\text{mid}} V_L^{(2),\text{mid},\dagger} V_L^{(1),\text{mid},\dagger} \\
\Pi^{\mathcal{L},123} &= V_L^{(1),\text{mid}} V_L^{(2),\text{mid}} V_L^{(3),\text{mid}} V_L^{(3),\text{mid},\dagger} V_L^{(2),\text{mid},\dagger} V_L^{(1),\text{mid},\dagger}
\end{aligned}$$

Then notice that $\Pi^{\mathfrak{r},1} = I - \Pi^{\mathcal{L},1}$, $\Pi^{\mathfrak{r},2} = \Pi^{\mathcal{L},1} - \Pi^{\mathcal{L},12}$, $\Pi^{\mathfrak{r},3} = \Pi^{\mathcal{L},12} - \Pi^{\mathcal{L},123}$ and $\Pi^{\mathfrak{r},4} = \Pi^{\mathcal{L},123}$.
We have lemmas for these projectors similar to the "forward" subspaces projector.

5 Structure of Glued Path

In this section, we will study the structure of the "glued path".

5.1 Graph associated with the Path

Given $(L_1, L_2, L_3, R_1, R_2, R_3)$ we associate a vertex in the graph with each tuple in the path:

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

We define directed edges in the graph to signify the "B" ouput register being fed as an "input". Hence, we define it 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 define the graph as follows:

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

5.2 Defining Paths in the 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 its 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.
We start by characterizing the walks in G.

Definition 21 (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:*

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

Next we define "good" lines:

Definition 22 (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 $\{\mathcal{P}_{LL}, \mathcal{P}_{LR}, \mathcal{P}_{RL}, \mathcal{P}_{RR}\}$:*

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

Definition 23 (Good line 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.

5.3 Defining Good Graphs

We define "good" graphs:

Definition 24 (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 $\mathcal{P}_{RR}^{\text{good}}$.*

We define the following parametrized representations of "good" graphs:

Definition 25 (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:

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

5.4 Defining Good Auxiliary States

To define good states, we start by defining state parameter structure notation as 4 sets as follows:

- $S_{\mathcal{LL}} = \{\mathfrak{q}_i^{\mathcal{LL}}\}_i$, 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 $|\overrightarrow{x^{\mathcal{RR},i}}| = |\overrightarrow{y^{\mathcal{RR},i}}|$.

Definition 26. *Given a state 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 $\mathsf{count}(\overline{S}) = \sum_{X,Y\in\{\mathcal{L},\mathcal{R}\}} \mathsf{count}(S_{XY})$.*
- *Define $\mathrm{Im}(\overline{S}) = \{w_2^{XY,i} | X, Y \in \{\mathcal{L},\mathcal{R}\}, i\}$.*

We first define another way to parametrize graph states:

Definition 27. *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 the below:*

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

Definition 28 (Good State 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 $|\mathrm{Im}(\overline{S})| = \mathsf{count}(\overline{S})$.*

We define parametrized "good" auxiliary states:

Definition 29. *Given a good state parameter $\overline{S} = \bigcup_{X,Y\in\{\mathcal{L},\mathcal{R}\}} S_{XY}$ 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 $b = \mathsf{len}(\overline{S})$. Then we define the following state:*

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

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 $\mathbb{G}\left(\overline{S}, R, Z\right)$.

Finally, we define the following "good" projector:

Definition 30. *Define "good" projector as follows:*

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

5.5 Relation between $\Pi^{\mathsf{I},i}$ and Π^{Good}

Ideally, we want to show that $\Pi^{\mathsf{I},i}$s behave well with Π^{Good}, first step we want to show that they commute. In particular, we show instead that $\Pi^{\mathcal{R},1}$, $\Pi^{\mathcal{R},12}$ and $\Pi^{\mathcal{R},123}$ commute with Π^{Good}.
From Lemma 11, 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 need to 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

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

- 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

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

- 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

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

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

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

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

- 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

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

- 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

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

First notice that these states defined above are related to each other as follows:

Lemma 31. *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:*

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

Lemma 32. *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:*

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

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

Lemma 33. *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 34. *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 35. *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 Π^{Good} times $\Pi^{\mathcal{L},i}$ as a projector on space spanned by $|\chi^{\mathfrak{r},i}\rangle$.

5.6 Most states are "good"

We say states are "good" if applying Π^{Good} doesn't change the state much. In this subsection, we show that any state achieved by querying $V^{\mathsf{glued\text{-}fwd}}$ and $V^{\mathsf{glued\text{-}inv}}$ is "good". To do this, we start by showing that for any "good" state in the subspace associated to $\Pi^{\mathfrak{l},i}$, applying $V^{\mathsf{glued\text{-}fwd}}$ returns a good state. Formally, we show the following lemmas:

Lemma 36. *Let $|\phi\rangle$ be some state such that*

- $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$
- $\Pi^{\mathfrak{l},1}|\phi\rangle = |\phi\rangle$

Then $\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle = W^{\mathsf{glued\text{-}fwd}}|\phi\rangle$.

Lemma 37. *Let $|\phi\rangle$ be some state such that*

- $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$
- $\Pi^{\mathfrak{l},2}|\phi\rangle = |\phi\rangle$

Then $\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\|_2 = O(t^2/2^\lambda)$

Lemma 38. *Let $|\phi\rangle$ be some state such that*

- $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$

- $\Pi^{\mathsf{I},3}|\phi\rangle = |\phi\rangle$

Then $\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\|_2 = O(t^2/2^\lambda)$

Lemma 39. *Let* $|\phi\rangle$ *be some state such that*

- $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$
- $\Pi^{\mathsf{I},4}|\phi\rangle = |\phi\rangle$

Then $\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\|_2 = O(t^2/2^\lambda)$

The proofs of above lemmas are in Appendix E.

Finally, combining the above, we get the following lemma:

Lemma 40. *Let* $|\phi\rangle$ *be some state such that* $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$*, then* $\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\|_2 = O(t^2/2^\lambda)$

The proofs of above lemma is in Appendix E. Symmertically, we can also get the lemma below.

Lemma 41. *Let* $|\phi\rangle$ *be some state such that* $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$*, then* $\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}}|\phi\rangle - W^{\mathsf{glued\text{-}inv}}|\phi\rangle\|_2 = O(t^2/2^\lambda)$

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

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

Lemma 42. *Let* $\mathcal{A}$ *denote a strong PRU adversary. Define*

$$|\psi\rangle = |\mathcal{A}^{W^{\mathsf{glued\text{-}fwd}}, W^{\mathsf{glued\text{-}inv}}}\rangle$$
$$|\phi\rangle = |\mathcal{A}^{\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}, \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}}}\rangle$$

Then

$$\||\psi\rangle - |\phi\rangle\|_2 = O(t^3/2^\lambda).$$

Proof. Define

$$|\psi_0\rangle = |0\rangle_{\mathsf{ABC}} |0\rangle_{\mathsf{D}} |\varnothing\rangle_{\mathsf{S}_1} |\varnothing\rangle_{\mathsf{S}_2} |\varnothing\rangle_{\mathsf{S}_3} |\varnothing\rangle_{\mathsf{T}_1} |\varnothing\rangle_{\mathsf{T}_2} |\varnothing\rangle_{\mathsf{T}_3},$$
$$|\psi_i\rangle = \begin{cases} W^{\mathsf{glued\text{-}fwd}} A_{(i+1)/2} |\psi_{i-1}\rangle & , i \text{ is odd.} \\ W^{\mathsf{glued\text{-}inv}} B_{i/2} |\psi_{i-1}\rangle & , i \text{ is even.} \end{cases}$$

Similarly, define:

$$|\phi_0\rangle = |0\rangle_{\mathsf{ABC}} |0\rangle_{\mathsf{D}} |\varnothing\rangle_{\mathsf{S}_1} |\varnothing\rangle_{\mathsf{S}_2} |\varnothing\rangle_{\mathsf{S}_3} |\varnothing\rangle_{\mathsf{T}_1} |\varnothing\rangle_{\mathsf{T}_2} |\varnothing\rangle_{\mathsf{T}_3},$$
$$|\phi_i\rangle = \begin{cases} \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} A_{(i+1)/2} |\phi_{i-1}\rangle & , i \text{ is odd.} \\ \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}} B_{i/2} |\phi_{i-1}\rangle & , i \text{ is even.} \end{cases}$$

Notice that

$$\Pi^{\mathsf{Good}} |\phi_i\rangle = |\phi_i\rangle$$

We prove this by induction.
Base Case: $\||\phi_0\rangle - |\psi_0\rangle\|_2 = 0$.
Induction Hypothesis: $\||\phi_i\rangle - |\psi_i\rangle\|_2 = O\left(\frac{i^3}{2^\lambda}\right)$

Induction Step: We prove this for i being odd:

$$\begin{aligned}\||\psi_{i+1}\rangle - |\phi_{i+1}\rangle\|_2 &= \|W^{\text{glued-fwd}} A_{(i+1)/2}|\phi_i\rangle - \Pi^{\text{Good}} W^{\text{glued-fwd}} A_{(i+1)/2}|\psi_i\rangle\|_2 \\ &\leq \|(I - \Pi^{\text{Good}}) W^{\text{glued-fwd}} A_{(i+1)/2}|\phi_i\rangle\|_2 + O\left(\frac{i^3}{2^\lambda}\right) \\ &= O\left(\frac{(i+1)^2}{2^\lambda}\right) + O\left(\frac{i^3}{2^\lambda}\right) \\ &= O\left(\frac{(i+1)^3}{2^\lambda}\right)\end{aligned}$$

Where the second line is by induction hypothesis, and third line is by Lemma 40. Similarly, we can prove the induction step for i being even.
Then by induction we have

$$\||\psi\rangle - |\phi\rangle\|_2 = O(t^3/2^\lambda).$$

□

6 Strong Gluing of Haar Random Unitaries

We now state the main result of this section.

Theorem 43 (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*

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

6.1 Proof of Theorem 43

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

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

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

$$|u_4\rangle = |\mathcal{A}^{\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}, \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}}}\rangle,$$

where $\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}, \Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}inv}}$ 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

$$|u_5\rangle = |\mathcal{A}^{W^{\mathsf{glued\text{-}fwd}}, W^{\mathsf{glued\text{-}inv}}}\rangle,$$

where $W^{\mathsf{glued\text{-}fwd}}, W^{\mathsf{glued\text{-}inv}}$ 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

$$|u_6\rangle = |\mathcal{A}^{V^{\mathsf{glued\text{-}fwd}}, V^{\mathsf{glued\text{-}inv}}}\rangle,$$

where $V^{\mathsf{glued\text{-}fwd}}, V^{\mathsf{glued\text{-}inv}}$ 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 44. *The trace distance between* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *is* $O\left(\frac{t^3}{N^{1/8}}\right)$.

Proof. By Theorem 12. □

Claim 45. *The trace distance between* $\mathbf{H}_2$ *and* $\mathbf{H}_3$ *is* $O\left(\sqrt{\frac{t^4}{2^\lambda}}\right)$.

Proof. By Lemma 13. □

Claim 46. *The trace distance between* $\mathbf{H}_3$ *and* $\mathbf{H}_4$ *is* $O\left(\frac{t^3}{2^\lambda}\right)$.

Proving Claim 46 is the main technical step of this section. We begin by defining $\mathcal{O}_{\mathsf{comp}}$ in Section 6.2, which we then use to prove Claim 46 in Section 6.3.

Claim 47. *The trace distance between* $\mathbf{H}_4$ *and* $\mathbf{H}_5$ *is* $O\left(\frac{t^3}{2^\lambda}\right)$.

Proof. By Lemma 42. □

Claim 48. *The trace distance between* $\mathbf{H}_5$ *and* $\mathbf{H}_6$ *is* $O\left(\sqrt{\frac{t^4}{2^\lambda}}\right)$.

Proof. By Lemma 15. □

Claim 49. *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 Lemma 14. □

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

The intuition towards defining $\mathcal{O}_{\mathsf{comp}}$ is the following: Given any path $\mathfrak{q} \in \overline{S}$, you can think of $\mathcal{O}_{\mathsf{comp}}$ as interweaving forward and backward queries that share the AB register but not C_i.

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

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

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

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

Then we prove the following:

Lemma 50. *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:*

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

We prove the above in Section 6.4 but before that we will finish proving Claim 46 in Section 6.3 using Lemma 50.

6.3 Proof of Claim 46: 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

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

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:

$$\begin{aligned}
&\|\mathcal{O}_{\mathsf{comp}}|\phi_i\rangle - |\psi_i\rangle\|_2 \\
=&\|\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda)}A_{(i+1)/2}|\psi_{i-1}\rangle\|_2 \\
&\qquad\qquad \text{(by expanding the definition of } |\psi_i\rangle \text{ and } |\phi_i\rangle) \\
\le&\|\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda)}A_{(i+1)/2}\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle\|_2 \\
&+\|W^{\mathrm{m}(\lambda)}A_{(i+1)/2}\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda)}A_{(i+1)/2}|\psi_{i-1}\rangle\|_2 \qquad \text{(by the triangle inequality)} \\
=&\|(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2} - W^{\mathrm{m}(\lambda)}\mathcal{O}_{\mathsf{comp}})A_{(i+1)/2}|\phi_{i-1}\rangle\|_2 + \|W^{\mathrm{m}(\lambda)}A_{(i+1)/2}(\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - |\psi_{i-1}\rangle)\|_2 \\
&\qquad\qquad \text{(since } \mathcal{O}_{\mathsf{comp}} \text{ and } A_{(i+1)/2} \text{ commute)} \\
\le&\|(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}fwd}}A_{(i+1)/2} - W^{\mathrm{m}(\lambda)}\mathcal{O}_{\mathsf{comp}})\Pi^{\mathsf{Good}}\Pi_{\le t}\|_{\mathrm{op}} + \|\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - |\psi_{i-1}\rangle\|_2 \qquad \text{(by Lemma 9)} \\
=&O(i^2/2^\lambda) + O((i-1)^3/2^\lambda). \qquad \text{(by Lemma 50 and the induction hypothesis)} \\
=&O(i^3/2^\lambda)
\end{aligned}$$

Case 2: i is even:

$$
\begin{aligned}
&\|\mathcal{O}_{\mathsf{comp}}|\phi_i\rangle - |\psi_i\rangle\|_2 \\
=&\|\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}inv}}B_{i/2}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda),\dagger}B_{i/2}|\psi_{i-1}\rangle\|_2 \quad \text{(by expanding the definition of } |\psi_i\rangle \text{ and } |\phi_i\rangle) \\
\leq&\|\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}inv}}B_{i/2}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda),\dagger}B_{i/2}\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle\|_2 \\
&+\|W^{\mathrm{m}(\lambda),\dagger}B_{i/2}\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - W^{\mathrm{m}(\lambda),\dagger}B_{i/2}|\psi_{i-1}\rangle\|_2 \quad \text{(by the triangle inequality)} \\
=&\|(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}inv}}B_{i/2} - W^{\mathrm{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}})B_{i/2}|\phi_{i-1}\rangle\|_2 + \|W^{\mathrm{m}(\lambda),\dagger}B_{i/2}(\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - |\psi_{i-1}\rangle)\|_2 \\
&\qquad \text{(since } \mathcal{O}_{\mathsf{comp}} \text{ and } B_{i/2} \text{ commute)} \\
\leq&\|(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}W^{\mathsf{glued\text{-}inv}}B_{i/2} - W^{\mathrm{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}})\Pi^{\mathsf{Good}}\Pi_{\leq t}\|_{\mathrm{op}} + \|\mathcal{O}_{\mathsf{comp}}|\phi_{i-1}\rangle - |\psi_{i-1}\rangle\|_2 \quad \text{(by Lemma 9)} \\
=&O(i^2/2^\lambda) + O((i-1)^3/2^\lambda). \quad \text{(by Lemma 50 and the induction hypothesis)} \\
=&O(i^3/2^\lambda)
\end{aligned}
$$

6.4 Proof of Lemma 50: Closeness of the Oracle Queries

To prove Lemma 50, we first prove it in the subspaces defined by $\Pi^{\mathfrak{l},i}$. Formally, we show the following lemmas:

Lemma 51. *For any integer $t \geq 0$,*

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

Lemma 52. *For any integer $t \geq 0$,*

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

Lemma 53. *For any integer $t \geq 0$,*

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

Lemma 54. *For any integer $t \geq 0$,*

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

We give proofs of the above lemmas in Appendix F.
We restate Lemma 50 for convenience.

Lemma 55 (Lemma 50, restated)**.** *For any integer $t \geq 0$,*

- *Forward query:*

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

- *Inverse query:*

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

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

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

First, note that from Lemma 16, we know that $\sum_{i=1}^{4} \Pi^{\mathsf{I},i} = I$. Hence, we get

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

Where the fouth line is by triangle inequality, and fifth line is by Lemmas 51 to 54. □

7 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 [ABGL25],

Theorem 56. *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 57 (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 57. 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.

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

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 $\mathcal{A}$.

$$\left| \Pr_{k||k_1||\ldots||k_9 \leftarrow \{0,1\}^{\lambda + 9\log^2(\lambda)}} \left[\top \leftarrow \mathcal{A}^{\mathsf{StretchPRU}_{k||k_1||\ldots||k_9}, \mathsf{StretchPRU}^{\dagger}_{k||k_1||\ldots||k_9}} \right] \right.$$

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

From Theorem 56, applied three times, we have the following bound:

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

Finally, applying Theorem 43, 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 StretchPRU is indistinguishable from a large Haar random unitary on $2t(\lambda)-\log^2(\lambda)$ qubits. □

Corollary 58 (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 Corollary 58. 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. □

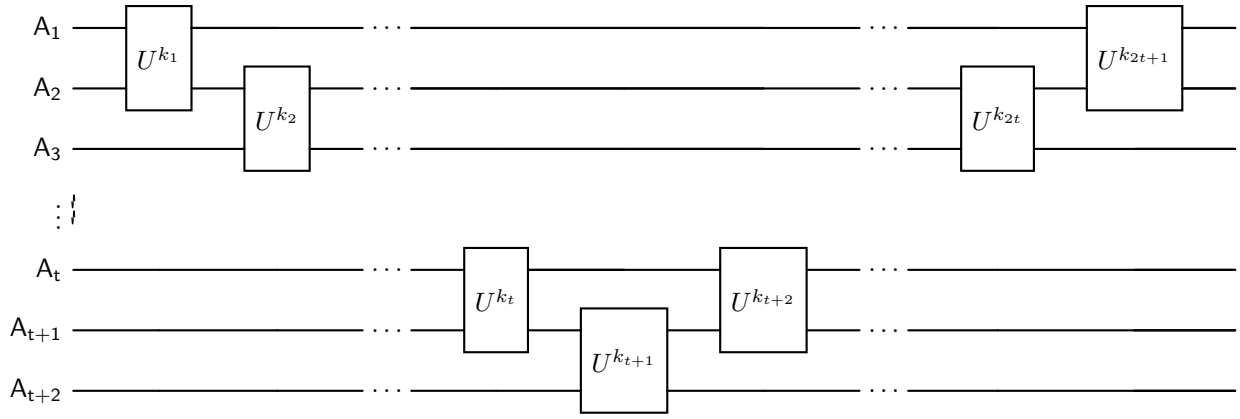
Rescaling so that $\lambda \leftarrow \lambda + 9c\log^3(\lambda)$, we have that there is a family of strong pseudo-random unitaries with keys of length λ and output size roughly λ^c.

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

Corollary 59 (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. $U^{k_{t-1}} V_1 U^{k_{t+3}}$) 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).

[ABGL25] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. "Pseudorandom Unitaries in the Haar Random Oracle Model". In: *CRYPTO*. Springer-Verlag, 2025 (cit. on pp. 1, 4, 32).

[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, 16).

[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, 5, 14, 16, 37).

[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. 15).

[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 Restricted Path-Recording

We define the following restricted Path-recording as:

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

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

We start by proving that $W_L^{\mathfrak{m}(\lambda)}$ is close to V_L.

Lemma 60. *For any integer $t \geq 0$,*

$$\|(V_L - W_L^{\mathfrak{m}(\lambda)})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{2^\lambda}} \quad \textit{and} \quad \|(V_R - W_R^{\mathfrak{m}(\lambda)})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{2^\lambda}}.$$

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

$$|\psi\rangle_{\mathsf{ABCST}} = \sum_{x,L,R} \alpha_{x,L,R}|x\rangle_{\mathsf{ABC}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}},$$

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

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

and

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

Subtracting,

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

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

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

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

$$|v\rangle = \sum_{y,L',R} |y\rangle|L'\rangle|R\rangle \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \alpha_{x,L,R} \left(\frac{1}{\sqrt{2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)}} \right) \right),$$

and thus

$$\begin{aligned}
\langle v|v\rangle &= \sum_{y,L',R} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \alpha_{x,L,R} \left(\frac{1}{\sqrt{2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)}} \right) \right)^2 \\
&\le \sum_{y,L',R} \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} |\alpha_{x,L,R}|^2 \right) \\
&\quad \times \left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{1}{\sqrt{2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)}} \right)^2 \right),
\end{aligned}$$

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

$$\begin{aligned}
&\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{1}{\sqrt{2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|}} - \frac{1}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)}} \right)^2 \\
&\qquad = \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathsf{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)} - \sqrt{2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|}}{\sqrt{2^{2n}(2^\lambda - |\mathrm{Im}(L\cup R)^{\mathsf{m}(\lambda)}|)(2^{2n+\lambda} - |\mathrm{Im}(L\cup R^{-1})|)}} \right)^2
\end{aligned}$$

$$\leq \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathtt{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}} \left(\frac{\sqrt{2^{2n}|\,\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}|}}{\sqrt{2^{2n}(2^{\lambda}-|\,\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}|)(2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|)}}\right)^2$$

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

$$\leq \frac{(|L|+1)\cdot|\,\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}|}{2^{2n+2\lambda-2}}$$

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

$$\langle v|v\rangle \leq \frac{(|L|+1)\cdot|\,\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}|}{2^{2n+2\lambda-2}}\cdot\sum_{y,L',R}\left(\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y^{\mathtt{m}(\lambda)}\notin \mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}\\ y\notin \mathrm{Im}(L\cup R^{-1})}}|\alpha_{x,L,R}|^2\right)$$

$$=\frac{(|L|+1)\cdot|\,\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}|}{2^{2n+2\lambda-2}}\cdot\sum_{x,L,R}|\alpha_{x,L,R}|^2\cdot\left(\sum_{y\in\{0,1\}^{2n+\lambda}}\mathbb{1}(y^{\mathtt{m}(\lambda)}\notin\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)})\mathbb{1}(y\notin\mathrm{Im}(L\cup R^{-1}))\right)$$

$$\leq\frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{2^{\lambda-2}}\cdot\sum_{x,L,R}|\alpha_{x,L,R}|^2=\frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{2^{\lambda-2}}.$$

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

$$|w_1\rangle=\sum_{x,L,R}\alpha_{x,L,R}\sum_{\substack{y:y\notin\mathrm{Im}(L\cup R^{-1})\\ y^{\mathtt{m}(\lambda)}\in\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}}}|y\rangle_{\mathsf{A}}|L\cup\{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}}\left(\frac{1}{\sqrt{2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|}}\right)$$

$$=\sum_{y,(L',R)}|y\rangle|L'\rangle|R\rangle\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R^{-1})\\ y^{\mathtt{m}(\lambda)}\in\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}}}\left(-\frac{\alpha_{x,L,R}}{\sqrt{2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|}}\right)$$

Then

$$\langle w_1|w_1\rangle=\sum_{y,(L',R)}\left|\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R^{-1})\\ y^{\mathtt{m}(\lambda)}\in\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}}}\frac{\alpha_{x,L,R}}{\sqrt{2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|}}\right|^2\leq\sum_{y,(L',R)}\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\},\\ y\notin\mathrm{Im}(L\cup R^{-1})\\ y^{\mathtt{m}(\lambda)}\in\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}}}\frac{|\alpha_{x,L,R}|^2}{2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|}$$

$$=\sum_{x,L,R}\frac{|\alpha_{x,L,R}|^2}{2^{2n+\lambda}-|\,\mathrm{Im}(L\cup R^{-1})|}\left(\sum_{\substack{y:y\notin\mathrm{Im}(L\cup R^{-1})\\ y^{\mathtt{m}(\lambda)}\in\mathrm{Im}(L\cup R)^{\mathtt{m}(\lambda)}}}1\right)\leq\frac{t}{2^{\lambda-1}}\sum_{x,L,R}|\alpha_{x,L,R}|^2=\frac{t}{2^{\lambda-1}}$$

Similarly, we also have

$$\langle w_2|w_2\rangle \leq \frac{t}{2^{2n+\lambda-1}}.$$

Hence, it holds that

$$\|(V_L - W_L^{\mathfrak{m}(\lambda)})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{2^\lambda}}.$$

By a symmetric argument, we have

$$\|(V_R - W_R^{\mathfrak{m}(\lambda)})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{2^\lambda}}. \qquad \square$$

Using above, we have:

Lemma 61. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

$$\left\| |\mathcal{A}^{W^{\mathsf{fwd},\mathfrak{m}(\lambda)},W^{\mathsf{inv},\mathfrak{m}(\lambda)}}\rangle_{\mathsf{ABCDST}} - |\mathcal{A}^{V^{\mathsf{fwd}},V^{\mathsf{inv}}}\rangle_{\mathsf{ABCDST}} \right\|_2 = O\left(\sqrt{\frac{t^4}{2^\lambda}}\right).$$

B Glued Path Recording

We want to show that instead of querying $V^3V^2V^1$ is close to querying V^{glued}. We start by proving the following lemma:

Lemma 62. *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*

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

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

$$\begin{aligned}
|\chi\rangle &= \sum_{y,L_1,L_2,R_1,R_2} \alpha_{yL_1L_2R_1R_2} V_L^{1,\dagger}V_R^2|y\rangle_{\mathsf{ABC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2} \\
&= \frac{1}{\sqrt{2^{n+\lambda}}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x\notin \mathrm{Dom}(L\cup R^{-1})}} \alpha_{yL_1L_2R_1R_2} V_L^{1,\dagger}|y^{\mathfrak{l}(n)}\rangle_{\mathsf{A}}|x\rangle_{\mathsf{BC}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\cup\{(y^{\mathfrak{r}(n+\lambda)},x)\}\rangle_{\mathsf{T}_2} \\
&= \frac{1}{2^{n+\lambda}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x\notin \mathrm{Dom}(L_2\cup R_2^{-1}) \\ z:(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\in L_1}} \alpha_{yL_1L_2R_1R_2}|z\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}|L_1\setminus\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\cup\{(y^{\mathfrak{r}(n+\lambda)},x)\}\rangle_{\mathsf{T}_2} \\
&= \frac{1}{2^{n+\lambda}} \sum_{\substack{y,L_1,L_2,R_1,R_2 \\ x\notin \mathrm{Dom}(L_2\cup R_2) \\ z:(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\in L_1}} \alpha_{yL_1L_2R_1R_2}|z\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}|L_1\setminus\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\cup\{(y^{\mathfrak{r}(n+\lambda)},x)\}\rangle_{\mathsf{T}_2} \\
&= \frac{1}{2^{n+\lambda}} \sum_{x,y,z,L_1',L_2,R_1,R_2'} \alpha_{yL_1'\cup\{(z,y^{\mathfrak{l}(n)}||x^{\mathfrak{l}(\lambda)})\}L_2R_1R_2'\setminus\{(y^{\mathfrak{r}(n+\lambda)},x)\}}|z\rangle_{\mathsf{AB}}|x^{\mathfrak{r}(n)}\rangle_{\mathsf{C}}|L_1'\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2'\rangle_{\mathsf{T}_2}
\end{aligned}$$

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

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

Hence

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

□

The above lemma gives us the following:

Lemma 63. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

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

C Proofs from Section 4.3

Proof of Lemma 16. Start by noticing that

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

Then adding:

$$\begin{aligned}
\sum_{i-1}^{4} \Pi^{\mathfrak{l},i} &= (I - \Pi^{\mathcal{R},1}) + (\Pi^{\mathcal{R},1} - \Pi^{\mathcal{R},12}) + (\Pi^{\mathcal{R},12} - \Pi^{\mathcal{R},123}) + (\Pi^{\mathcal{R},123}) \\
&= I
\end{aligned}$$

□

Proof of Lemma 17. Start by recalling

$$\begin{aligned}
W^{\mathsf{glued\text{-}fwd}} =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}\right) \\
&+ V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} \\
&+ V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger}\right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&+ \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}
\end{aligned}$$

and

$$\Pi^{\mathfrak{l},1} = I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}.$$

Then notice that

$$V_R^{(1),\mathsf{mid},\dagger}\Pi^{\mathfrak{l},1} = V_R^{(1),\mathsf{mid},\dagger}(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}) = 0,$$

Hence we get

$$W^{\mathsf{glued\text{-}fwd}}\Pi^{\mathfrak{l},1} = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}\right).$$

□

Proof of Lemma 18. Start by recalling

$$\begin{aligned} W^{\mathsf{glued\text{-}fwd}} =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} \left(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}\right) \\ &+ V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} \\ &+ V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger}\right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\ &+ \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \end{aligned}$$

and

$$\Pi^{\mathfrak{l},2} = V_R^{(1),\mathsf{mid}}(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid},\dagger}.$$

Then notice that

$$(I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger})\Pi^{\mathfrak{l},2} = (I - V_R^{(1),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid}} (I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid},\dagger} = 0,$$

also notice that

$$V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}\Pi^{\mathfrak{l},2} = V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid}} (I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid},\dagger} = 0$$

Hence we get

$$W^{\mathsf{glued\text{-}fwd}}\Pi^{\mathfrak{l},2} = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) (I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}) V_R^{(1),\mathsf{mid},\dagger}.$$

Then by Lemma 62 and Lemma 60, we get

$$\|W^{\mathsf{glued\text{-}fwd}}\Pi^{\mathfrak{l},2} - V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger}\|_{\mathrm{op}} = O(t^2/2^\lambda)$$

□

Proofs of Lemmas 19 and 20 are similar to above.

D Proofs from Section 5.5

Proof of Lemma 31. 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.

$$\begin{aligned} |\phi\rangle &= V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathfrak{G}(\overline{S})\rangle \\ &= \sum_{\substack{Z\in\{0,1\}^{an} \\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}}}} V_R^{(1),\mathsf{mid}} V_R^{(2),\mathsf{mid}} V_R^{(3),\mathsf{mid}} |x_0\rangle|w_1\rangle|x_1\rangle|\mathbb{G}(\overline{S}, R, Z)\rangle \end{aligned}$$

$$= \sum_{\substack{Z\in\{0,1\}^{an}\\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}}\\ (r_1,r_2)\in(\{0,1\}^\lambda\setminus R)^2_{\mathrm{dist}}\\ z\in\{0,1\}^n\\ y_0,y_1\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathbb{G}(\overline{S},R,Z)\cup\mathfrak{p}(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2,(r_1,r_2),z)\rangle$$

$$= \sum_{\substack{Z\cup\{z\}\in\{0,1\}^{(a+1)n}\\ R\cup\{(r_1,r_2)\}\in(\{0,1\}^\lambda)^{b_2}_{\mathrm{dist}}\\ y_0,y_1\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathbb{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2)\},R\cup\{(r_1,r_2)\},Z\cup\{z\})\rangle$$

$$= \sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle|w_2\rangle|y_1\rangle|\mathfrak{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w_1,w_2)\})\rangle$$

$$= |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle$$

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 Lemma 32. 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.

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

$$= V_R^{(1),\mathsf{mid}}V_R^{(2),\mathsf{mid}}V_L^{(3),\mathsf{mid},\dagger} \sum_{\substack{y_0\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0,w_2,\mathfrak{G}(\overline{S}\cup\{(XL,\overrightarrow{x},y_0||\overrightarrow{y},w_1,w_2)\})\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}$$

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

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

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

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

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 Lemma 33. 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) \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}:

$$\Pi^{\mathcal{R},1}\Pi^{\mathsf{Good}} = \Pi^{\mathcal{R},1} \sum_{\substack{y,w,\overline{S} \\ \overline{S} \text{ is good}}} |y, w, \mathfrak{G}(\overline{S})\rangle\langle y, w, \mathfrak{G}(\overline{S})|_{\mathsf{AB}\overline{\mathsf{ST}}}$$

$$= \sum_{\substack{y,w,\overline{S} \\ \overline{S} \text{ is good}}} \Pi^{\mathcal{R},1}|y,w,\mathfrak{G}(\overline{S})\rangle\langle y,w,\mathfrak{G}(\overline{S})|_{\mathsf{AB}\overline{\mathsf{ST}}}$$

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

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

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

Hence,

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

□

Proof of Lemma 34. 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:

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

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

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

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

Hence,

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

□

Proof of Lemma 35. 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:

$$
\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-2}_{\text{dist}}\\ z\in\{0,1\}^n\\ \overrightarrow{r}\in\left(\{0,1\}^\lambda\setminus R'\right)^2_{\text{dist}}}} \Pi^{\mathcal{R},123}|y_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}} \\
&\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}_{\text{dist}}\\ z\in\{0,1\}^n\\ \overrightarrow{r}\in\left(\{0,1\}^\lambda\setminus R'\right)^2_{\text{dist}}\\ y_0'\in\{0,1\}^n\\ w'\in\left(\{0,1\}^\lambda\setminus\text{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\text{Im}(\overline{S'})\right)\\ y_1'\in\{0,1\}^n\\ Z\in\{0,1\}^{an}\\ R\in\left(\{0,1\}^\lambda\right)^b_{\text{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)}} \underbrace{\frac{1}{2^n\sqrt{(2^\lambda - a + 1)}} \sum_{\substack{y_0'\in\{0,1\}^n\\ w'\in\left(\{0,1\}^\lambda\setminus\text{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^{\mathsf{I},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}:

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

$$= \sum_{\vec{x},w_1,\overline{S'}} |\chi^{\mathfrak{l},3}_{\overline{S'},\vec{x},w_1}\rangle\langle\chi^{\mathfrak{l},3}_{\overline{S'},\vec{x},w_1}|_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Hence,

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

□

E Proofs from Section 5.6

Proof of Lemma 36. Notice that from Lemma 17, $W^{\mathsf{glued\text{-}fwd}}\Pi^{\mathfrak{l},1} = V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}\Pi^{\mathfrak{l},1}$. Next, for some fixed $x_0, x_1 \in \{0,1\}^n$, $w \in \{0,1\}^\lambda$, $\overline{S}$ a good state parameter with $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$, let $|\psi\rangle = V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}|x_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}}$ then

$$\begin{aligned}
|\psi\rangle =& V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}|x_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}}\\
=& \frac{1}{\sqrt{2^{an}\prod_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{Z\in\{0,1\}^{an}\\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}}}} V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}|x_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{C}}|\mathbb{G}(\overline{S},R,Z)\rangle_{\overline{\mathsf{ST}}}\\
=& \frac{1}{\sqrt{2^{an}\prod_{i=1}^{b}(2^\lambda - i + 1)}} \sum_{\substack{Z\in\{0,1\}^{an}\\ R\in(\{0,1\}^\lambda)^b_{\mathrm{dist}}}} \frac{1}{\sqrt{2^{3n}(2^\lambda-b)(2^\lambda-b-1)(2^\lambda-a)}}\\
&\times \sum_{\substack{z,y_0,y_1\in\{0,1\}^n\\ (r_1,r_2)\in(\{0,1\}^{secp}\setminus R)^2_{\mathrm{dist}}\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle_{\mathsf{A}}|w_2\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathbb{G}(\overline{S},R,Z)\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w,w_2,(r_1,r_2),z)\}\rangle_{\overline{\mathsf{ST}}}\\
=& \frac{1}{\sqrt{2^{(a+1)n}\prod_{i=1}^{b+2}(2^\lambda - i + 1)}} \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}}}} \frac{1}{\sqrt{2^{2n}(2^\lambda-a)}}\\
&\times \sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle_{\mathsf{A}}|w_2\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathbb{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w,w_2)\},R\cup\{(r_1,r_2)\},Z\cup\{z\})\rangle_{\overline{\mathsf{ST}}}\\
=& \frac{1}{\sqrt{2^{2n}(2^\lambda-a)}} \sum_{\substack{y_0,y_1\in\{0,1\}^n\\ w_2\in\{0,1\}^\lambda\setminus\mathrm{Im}(\overline{S})}} |y_0\rangle_{\mathsf{A}}|w_2\rangle_{\mathsf{B}}|y_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S}\cup\{(\mathcal{RR},(x_0,x_1),(y_0,y_1),w,w_2)\})\rangle_{\overline{\mathsf{ST}}}\\
=& |\chi^{\mathfrak{r},3}_{\overline{S},(x_0,x_1),w}\rangle
\end{aligned}$$

Also notice that $\Pi^{\mathsf{Good}}|\phi\rangle = |\phi\rangle$, hence we can write $|\phi\rangle$ as

$$|\phi\rangle = \sum_{\substack{x_0,w,x_1\\ \overline{S}}} \alpha_{x_0,w,x_1,\overline{S}}|x_0\rangle_{\mathsf{A}}|w\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{C}}|\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}}$$

Next we try to calculate $W^{\mathsf{glued\text{-}fwd}}|\phi\rangle$, notice that since $\Pi^{\mathfrak{l},1}|\phi\rangle = |\phi\rangle$, hence

$$\begin{aligned}
W^{\mathsf{glued\text{-}fwd}}|\phi\rangle &= W^{\mathsf{glued\text{-}fwd}}\Pi^{\mathfrak{r},1}|\phi\rangle\\
&= V_L^{(3),\mathsf{mid}}V_L^{(2),\mathsf{mid}}V_L^{(1),\mathsf{mid}}\Pi^{\mathfrak{r},1}|\phi\rangle
\end{aligned}$$

$$= V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} |\phi\rangle$$

Now, substituting $|\phi\rangle = \sum_{\substack{x_0,w,x_1\\ \overline{S}}} \alpha_{x_0,w,x_1,\overline{S}} |x_0\rangle_{\mathsf{A}} |w\rangle_{\mathsf{B}} |x_1\rangle_{\mathsf{C}} |\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}}$, we get:

$$\begin{aligned} W^{\mathsf{glued\text{-}fwd}} |\phi\rangle &= \sum_{\substack{x_0,w,x_1\\ \overline{S}}} \alpha_{x_0,w,x_1,\overline{S}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_L^{(1),\mathsf{mid}} |x_0\rangle_{\mathsf{A}} |w\rangle_{\mathsf{B}} |x_1\rangle_{\mathsf{C}} |\mathfrak{G}(\overline{S})\rangle_{\overline{\mathsf{ST}}} \\ &= \sum_{\substack{x_0,w,x_1\\ \overline{S}}} \alpha_{x_0,w,x_1,\overline{S}} |\chi^{\mathfrak{r},3}_{\overline{S},(x_0,x_1),w}\rangle \end{aligned}$$

Notice that since $\Pi^{\mathsf{Good}} |\chi^{\mathfrak{r},3}_{\overline{S},(x_0,x_1),w}\rangle = |\chi^{\mathfrak{r},3}_{\overline{S},(x_0,x_1),w}\rangle$, hence we have

$$\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} |\phi\rangle = W^{\mathsf{glued\text{-}fwd}} |\phi\rangle.$$

□

Proof of Lemma 37. Notice that from Lemma 18,

$$\|W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},2} - V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} \|_{\mathrm{op}} = O(t^2/2^\lambda).$$

Next, notice that since the subspace spanned by $\Pi^{\mathfrak{l},2}_{\mathsf{ABC}\overline{\mathsf{ST}}}$ is a subspace of $\Pi^{\mathcal{R},1}_{\mathsf{AB}\overline{\mathsf{ST}}} \otimes I_{\mathsf{C}}$, and $|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$ is in the subspace spanned by $\Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2}$, we know by Lemma 33, $|\phi\rangle$ is spanned by $|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}}$s. Then let $|\phi\rangle$ is:

$$|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = \sum_{\substack{X,\overrightarrow{x},\overrightarrow{y}\\ \overline{S},w_1,x'}} \alpha_{\substack{X,\overrightarrow{x},\overrightarrow{y}\\ \overline{S},w_1,x'}} |\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}}$$

Let

$$|\phi_1\rangle = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

and

$$|\phi_2\rangle = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Then from Lemma 18, we know:

$$\|(I - \Pi^{\mathsf{Good}}) W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},2} |\phi\rangle - (I - \Pi^{\mathsf{Good}})(|\phi_1\rangle - |\phi_2\rangle)\|_2 = O(t^2/2^\lambda).$$

Hence, by triangle inequality, we have

$$\begin{aligned} \|(I - \Pi^{\mathsf{Good}}) W^{\mathsf{glued\text{-}fwd}} |\phi\rangle\|_2 \leq & O(t^2/2^\lambda) + \|(I - \Pi^{\mathsf{Good}})(|\phi_1\rangle - |\phi_2\rangle)\|_2 \\ \leq & O(t^2/2^\lambda) + \|(I - \Pi^{\mathsf{Good}})|\phi_1\rangle\|_2 + \|(I - \Pi^{\mathsf{Good}})|\phi_2\rangle\|_2 \end{aligned}$$

Computing $(I - \Pi^{\mathsf{Good}})|\phi_1\rangle$: First we simplify $|\phi_1\rangle$ as:

$$\begin{aligned} |\phi_1\rangle =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle \\ =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger}\right) V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle \\ =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \Pi^{\mathfrak{l},2} |\phi\rangle \\ =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle \end{aligned}$$

Next subtituting $|\phi\rangle$, we get:

$$\begin{aligned}
|\phi_1\rangle =& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle \\
=& V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \sum_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} \alpha_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} |\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \\
=& \sum_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} \alpha_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} V_R^{(1),\mathsf{mid},\dagger} \left(|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \right) \\
=& \sum_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} \alpha_{\substack{X,\overrightarrow{x},\overrightarrow{y} \\ \overline{S},w_1,x'}} |\chi^{\mathfrak{r},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}
\end{aligned}$$

The last line is true because

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

Finally, since $(I - \Pi^{\mathsf{Good}})|\chi^{\mathfrak{r},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle = 0$, hence, we have:

$$\|(I - \Pi^{\mathsf{Good}})|\phi_1\rangle\|_2 = 0.$$

Computing $(I - \Pi^{\mathsf{Good}})|\phi_2\rangle$: Recall how $|\phi_2\rangle$ was defined:

$$|\phi_2\rangle = V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} \right) V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

For some fixed $\overline{S}$, $\overrightarrow{x}||x$, $\overrightarrow{y}$, $X \in \{\mathcal{L}, \mathcal{R}\}$, w and x', with $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$, we compute

$$\begin{aligned}
|\psi\rangle =& V_L^{(1),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \\
=& V_L^{(1),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \frac{1}{\sqrt{2^n(2^\lambda - a)}} \sum_{\substack{y\in\{0,1\}^n \\ w\in\{0,1\}^\lambda \setminus (\mathrm{Im}(\overline{S}))}} |y, w, \mathfrak{G}(\overline{S} \cup \{(X\mathcal{R}, \overrightarrow{x}, \overrightarrow{y}||y, w_1, w)\}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}} \\
=& V_L^{(1),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \frac{1}{\sqrt{2^n(2^\lambda - a)}} \frac{1}{\sqrt{2^{an}(2^\lambda)\dots(2^\lambda - b + 1)}} \sum_{\substack{y\in\{0,1\}^n \\ w\in\{0,1\}^\lambda\setminus(\mathrm{Im}(\overline{S})) \\ R\cup\{\overrightarrow{r}||r\}\in(\{0,1\}^\lambda)^b_{\mathrm{dist}} \\ Z\cup\{z\}\in\{0,1\}^{an}}} \\
& \times |y, w, x', \mathbb{G}(\overline{S}, R, Z) \cup \mathfrak{p}(X\mathcal{R}, \overrightarrow{x}||x, \overrightarrow{y}||y, w_1, w, \overrightarrow{r}||r, z)\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& V_L^{(1),\mathsf{mid},\dagger} \frac{1}{\sqrt{2^{an}(2^\lambda)\dots(2^\lambda - b + 1)}} \sum_{\substack{R\cup\{\overrightarrow{r}||r\}\in(\{0,1\}^\lambda)^b_{\mathrm{dist}} \\ Z\cup\{z\}\in\{0,1\}^{an}}} \\
& \times |z, r, x', \mathbb{G}(\overline{S}, R, Z) \cup \mathfrak{p}(X\mathcal{R}, \overrightarrow{x}||x, \overrightarrow{y}||0, w_1, 0, \overrightarrow{r}, z) \setminus \{(\mathfrak{r}_1, z||r, 0||0)\}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} \\
=& 0
\end{aligned}$$

Where the last line is true because $\mathrm{Im}(L_1)^{\mathfrak{r}(\lambda)} \subset R \cup \{\overrightarrow{r}\}$, and $r \notin R \cup \{\overrightarrow{r}\}$. Hence, we have $|\phi_2\rangle = 0$. Hence,

$$\|(I - \Pi^{\mathsf{Good}})|\phi_2\rangle\|_2 = 0.$$

Combining, we get

$$\|(I - \Pi^{\mathsf{Good}}) W^{\mathsf{glued\text{-}fwd}} |\phi\rangle\|_2 = O(t^2/2^\lambda)$$

□

Proof of Lemma 38. Notice that from Lemma 19,

$$\|W^{\text{glued-fwd}}\Pi^{\mathfrak{l},3} - V_L^{(3),\text{mid}}\left(I - V_R^{(3),\text{mid}}V_R^{(3),\text{mid},\dagger} - V_L^{(2),\text{mid}}V_L^{(2),\text{mid},\dagger}\right)V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}\|_{\text{op}} = O(t^2/2^\lambda)$$

Next, we know by Lemma 34 and Lemma 35, $|\phi\rangle$ is spanned by $|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$s where $\mathsf{len}(\overrightarrow{x}) > 2$. We replace $\overrightarrow{x}$ with $\overrightarrow{x}||x'$ to separately look at its last element. Then let $|\phi\rangle$ is:

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

Let

$$|\phi_1\rangle = V_L^{(3),\text{mid}}\left(I - V_R^{(3),\text{mid}}V_R^{(3),\text{mid},\dagger}\right)V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

and

$$|\phi_2\rangle = V_L^{(3),\text{mid}}\left(V_L^{(2),\text{mid}}V_L^{(2),\text{mid},\dagger}\right)V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Then from Lemma 19, we know:

$$\|(I-\Pi^{\mathsf{Good}})W^{\text{glued-fwd}}\Pi^{\mathfrak{l},3}|\phi\rangle - (I-\Pi^{\mathsf{Good}})(|\phi_1\rangle - |\phi_2\rangle)\|_2 = O(t^2/2^\lambda).$$

Hence, by triangle inequality, we have

$$\begin{aligned}\|(I-\Pi^{\mathsf{Good}})W^{\text{glued-fwd}}|\phi\rangle\|_2 \leq& O(t^2/2^\lambda) + \|(I-\Pi^{\mathsf{Good}})(|\phi_1\rangle - |\phi_2\rangle)\|_2\\ \leq& O(t^2/2^\lambda) + \|(I-\Pi^{\mathsf{Good}})|\phi_1\rangle\|_2 + \|(I-\Pi^{\mathsf{Good}})|\phi_2\rangle\|_2\end{aligned}$$

Computing $(I-\Pi^{\mathsf{Good}})|\phi_1\rangle$: First we simplify $|\phi_1\rangle$ as:

$$\begin{aligned}|\phi_1\rangle =& V_L^{(3),\text{mid}}\left(I - V_R^{(3),\text{mid}}V_R^{(3),\text{mid},\dagger}\right)V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\ =& V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}V_R^{(1),\text{mid}}V_R^{(2),\text{mid}}\left(I - V_R^{(3),\text{mid}}V_R^{(3),\text{mid},\dagger}\right)V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\ =& V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}\Pi^{\mathfrak{l},3}|\phi\rangle\\ =& V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle\end{aligned}$$

Next subtituting $|\phi\rangle$, we get:

$$\begin{aligned}|\phi_1\rangle =& V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\phi\rangle\\ =& V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}\sum_{\substack{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}}\alpha_{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\ =& \sum_{\substack{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}}\alpha_{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}V_L^{(3),\text{mid}}V_R^{(2),\text{mid},\dagger}V_R^{(1),\text{mid},\dagger}|\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\\ =& \sum_{\substack{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}}\alpha_{X,\overrightarrow{x}||x'\\ \overrightarrow{y},\overline{S},w_1}|\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}}|x'\rangle_{\mathsf{C}}\end{aligned}$$

Where the last line is true because

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

Finally, since $(I-\Pi^{\mathsf{Good}})|\chi^{\mathfrak{r},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle = 0$, hence, we have:

$$\|(I-\Pi^{\mathsf{Good}})|\phi_1\rangle\|_2 = 0.$$

Computing $(I - \Pi^{\mathsf{Good}})|\phi_2\rangle$: Recall how $|\phi_2\rangle$ was defined:

$$|\phi_2\rangle = V_L^{(3),\mathsf{mid}} \left(V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger}\right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

For some fixed $\overline{S}$, $\overrightarrow{x}||x'$, $\overrightarrow{y}$, $X \in \{\mathcal{L}, \mathcal{R}\}$ and w, with $a = \mathsf{count}(\overline{S})$ and $b = \mathsf{len}(\overline{S})$, we compute

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

Notice that the above is zero if the last value in $\overrightarrow{y}$ is not x'. Now we analyse this for $\overrightarrow{y} = \overrightarrow{y'}||x'$. In this case, we get

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

Where the above equality can be checked by simple calculation. Since $|\phi_2\rangle$ is spanned my states of the above form, hence we have that $(I - \Pi^{\mathsf{Good}})|\phi_2\rangle$. Hence,

$$\|(I - \Pi^{\mathsf{Good}})|\phi_2\rangle\|_2 = 0.$$

Combining, we get

$$\|(I - \Pi^{\mathsf{Good}}) W^{\mathsf{glued\text{-}fwd}} |\phi\rangle\|_2 = O(t^2/2^\lambda)$$

□

Proof of Lemma 39. Notice that from Lemma 20,

$$\|W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},4} - \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger}\|_{\mathrm{op}} = O(t^2/2^\lambda)$$

Next, notice that since the subspace spanned by $\Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},4}$, we know by Lemma 35, $|\phi\rangle$ is spanned by $|\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$s. Then let $|\phi\rangle$ is:

$$|\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = \sum_{\overline{S},(x_0,x_1),w_1} \alpha_{\overline{S},(x_0,x_1),w_1'} |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Then notice

$$V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = \sum_{\overline{S},(x_0,x_1),w_1} \alpha_{\overline{S},(x_0,x_1),w_1'} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Hence,

$$(I - \Pi^{\mathsf{Good}}) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = \sum_{\overline{S},(x_0,x_1),w_1} \alpha_{\overline{S},(x_0,x_1),w_1'} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = 0$$

Next, for some fixed $\overline{S}, (x_0, x_1), w_1$, we compute:

$$|\psi\rangle = V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} |x_0, w_1, x_1, \mathfrak{G}(\overline{S})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

Notice that the above is zero if $\overline{S}$ does not have an element of the form $(X\mathcal{L}, \overrightarrow{x'}, \overrightarrow{y'}||x_0, w_1', w_1)$ for some $X, \overrightarrow{x'}, \overrightarrow{y'}, w_1'$. Now, we will analyse $\overline{S} = \overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x'}, \overrightarrow{y'}||x_0, w_1', w_1)\}$, with $a = \mathsf{count}(\overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x'}, \overrightarrow{y'}||x_0, w_1', w_1)\})$.

$$\begin{aligned}|\psi\rangle =& V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger} |x_0, w_1, x_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x'}, \overrightarrow{y'}||x_0, w_1', w_1)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} \\ =& \frac{1}{2^n(2^\lambda - a)} \sum_{\substack{x\in\{0,1\}^n \\ w\in\{0,1\}^\lambda \setminus \mathrm{Im}(\overline{S'})}} |x, w, x_1, \mathfrak{G}(\overline{S'} \cup \{(X\mathcal{L}, \overrightarrow{x'}, \overrightarrow{y'}||x, w_1', w)\})\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}\end{aligned}$$

Hence, we have

$$(I - \Pi^{\mathsf{Good}}) \left(I - V_L^{(3),\mathsf{mid}} V_L^{(3),\mathsf{mid},\dagger}\right) V_R^{(3),\mathsf{mid},\dagger} V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\phi\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = 0$$

Combining with Lemma 20,

$$\|(I - \Pi^{\mathsf{Good}}) W^{\mathsf{glued\text{-}fwd}} |\phi\rangle\|_2 = O(t^2/2^\lambda)$$

□

Proof of Lemma 40. We know $|\phi\rangle = \Pi^{\mathsf{Good}}|\phi\rangle$. Then for all $i \in [4]$, we have:

$$\begin{aligned}\Pi^{\mathfrak{l},i}|\phi\rangle =& \Pi^{\mathfrak{l},i}\Pi^{\mathsf{Good}}|\phi\rangle \\ =& \Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},i}|\phi\rangle\end{aligned}$$

Hence, we have $\Pi^{\mathfrak{l},i}|\phi\rangle = \Pi^{\mathsf{Good}}\Pi^{\mathfrak{l},i}|\phi\rangle$.
Then calculating

$$\begin{aligned}\gamma =& \|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\|_2 \\ =& \|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}}(\sum_{i=1}^4 \Pi^{\mathfrak{l},i})|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}(\sum_{i=1}^4 \Pi^{\mathfrak{l},i})|\phi\rangle\|_2 \\ =& \left\|\sum_{i=1}^4 \left(\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},i}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\right)\right\|_2 \\ \leq& \sum_{i=1}^4 \left\|\Pi^{\mathsf{Good}} W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},i}|\phi\rangle - W^{\mathsf{glued\text{-}fwd}}|\phi\rangle\right\|_2 \\ =& O(t^2/2^\lambda)\end{aligned}$$

where the last line if because of Lemmas 36 to 39. □

F Proofs from Section 6.4

To prove the below results, we notice the following technical lemma:

Lemma 64. *For any integer $t \geq 0$,*

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

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

Proof of Lemma 51. We recall that we want to estimate:

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

Where the second line is by triangle inequality, and the third line is by Lemma 17 and Lemma 64, 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:

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

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:

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

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

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 Lemma 52. 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}} \\
&\quad + \left\| W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le 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},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\le \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} \right) 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}} \\
&\quad + \left\| \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \left(W^{\mathsf{glued\text{-}fwd}} - V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} \right) V_R^{(1),\mathsf{mid},\dagger} \right) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \Pi_{\le t} \right\|_{\mathrm{op}} \\
&\quad + O(t^2/2^\lambda) \\
&\le \left\| \left(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} - V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} \right) 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}} \\
&\quad + O(t^2/2^\lambda)
\end{aligned}
$$

Where the second line is by triangle inequality, and the third line is by Lemma 64, and the fourth line is true by triangle inequality, and the fifth line is true by Lemma 18. Also notice that in the proof of Lemma 37 we proved that

$$
\left\| V_L^{(3),\mathsf{mid}} V_L^{(2),\mathsf{mid}} \left(V_L^{(1),\mathsf{mid}} V_L^{(1),\mathsf{mid},\dagger} \right) V_R^{(1),\mathsf{mid},\dagger} \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2} \right\|_{\mathrm{op}} = 0,
$$

Hence, we have

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

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

Where the above is true because $\Pi^{\mathfrak{l},2} = V_R^{(1),\mathsf{mid}} \left(I - V_R^{(2),\mathsf{mid}} V_R^{(2),\mathsf{mid},\dagger} \right) V_R^{(1),\mathsf{mid},\dagger}$ and $\Pi^{\mathfrak{l},2} \Pi^{\mathsf{Good}} = \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2}$. Next, we compute

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

We know by Lemma 33 that the subspace represented by $\Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},2}$ is spanned by $|\chi^{\mathfrak{l},1}_{\overline{S},X,\overrightarrow{x},\overrightarrow{y},w_1}\rangle_{\mathsf{AB}\overline{\mathsf{ST}}} |x'\rangle_{\mathsf{C}}$s.

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:

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

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

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

Finally, we get

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

□

Proof of Lemma 53. 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_{\leq t} \right\|_{\mathrm{op}} \\
&\leq \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_{\leq 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},3} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\leq \Bigg\| \Big(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger} \right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&\qquad\qquad - (I - W_L^{\mathfrak{m}(\lambda)} W_L^{\mathfrak{m}(\lambda),\dagger}) W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Big) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\leq t} \Bigg\|_{\mathrm{op}} \\
&\quad + \Bigg\| \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} \Big(V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} - V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger} \right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&\qquad\qquad - W^{\mathsf{glued\text{-}fwd}} \Pi^{\mathfrak{l},3} \Big) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\leq t} \Bigg\|_{\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},3} \Pi_{\leq t} \right\|_{\mathrm{op}} \\
&\leq \underbrace{\Bigg\| \Big(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} \right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&\qquad\qquad - W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Big) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\leq t} \Bigg\|_{\mathrm{op}}}_{\gamma_1} \\
&\quad + \underbrace{\Bigg\| \Big(\mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} \left(V_L^{(2),\mathsf{mid}} V_L^{(2),\mathsf{mid},\dagger} \right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} \\
&\qquad\qquad - (W_L^{\mathfrak{m}(\lambda)} W_L^{\mathfrak{m}(\lambda),\dagger}) W_R^{\mathfrak{m}(\lambda),\dagger} \mathcal{O}_{\mathsf{comp}} \Big) \Pi^{\mathsf{Good}} \Pi^{\mathfrak{l},3} \Pi_{\leq t} \Bigg\|_{\mathrm{op}}}_{\gamma_2} + O(t^2/2^\lambda) \\
&\quad + \underbrace{\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_{\leq t} \right\|_{\mathrm{op}}}_{\gamma_3}
\end{aligned}$$

Where the second and third line is by triangle inequality, and the last line is by Lemma 19. Next, we compute γ_1, γ_2 and γ_3. Before computing this, we know by Lemmas 34 and 35 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

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

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

$$|\phi_1\rangle = \mathcal{O}_{\mathsf{comp}} \Pi^{\mathsf{Good}} V_L^{(3),\mathsf{mid}} \left(I - V_R^{(3),\mathsf{mid}} V_R^{(3),\mathsf{mid},\dagger} \right) V_R^{(2),\mathsf{mid},\dagger} V_R^{(1),\mathsf{mid},\dagger} |\chi^{\mathfrak{l},2}_{\overline{S},X,\overrightarrow{x}||x',\overrightarrow{y},w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}}$$

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

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 $\gamma_2 = O(t^2/2^\lambda)$.

Computing γ_3: Similar to the proof of Lemma 54, we can prove that $\gamma_3 = 0$. Hence combining, we get

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

□

Proof of Lemma 54. We recall that we want to estimate:

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

$$
\begin{aligned}
&+\left\|W_L^{\mathsf{m}(\lambda)}(I-W_R^{\mathsf{m}(\lambda)}W_R^{\mathsf{m}(\lambda),\dagger})\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\Pi^{\mathsf{I},4}\Pi_{\le t}\right\|_{\mathrm{op}}\\
\le&\underbrace{\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}V_R^{(3),\mathsf{mid},\dagger}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}-W_R^{\mathsf{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathsf{I},4}\Pi_{\le t}\right\|_{\mathrm{op}}}_{\gamma_1}\\
&+\underbrace{\left\|\left(\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\left(V_L^{(3),\mathsf{mid}}V_L^{(3),\mathsf{mid},\dagger}\right)V_R^{(3),\mathsf{mid},\dagger}V_R^{(2),\mathsf{mid},\dagger}V_R^{(1),\mathsf{mid},\dagger}\right.\right.}_{\gamma_2}\\
&\qquad\underbrace{\left.\left.-(W_L^{\mathsf{m}(\lambda)}W_L^{\mathsf{m}(\lambda),\dagger})W_R^{\mathsf{m}(\lambda),\dagger}\mathcal{O}_{\mathsf{comp}}\right)\Pi^{\mathsf{Good}}\Pi^{\mathsf{I},4}\Pi_{\le t}\right\|_{\mathrm{op}}}_{\gamma_2}+O(t^2/2^\lambda)\\
&+\underbrace{\left\|W_L^{\mathsf{m}(\lambda)}(I-W_R^{\mathsf{m}(\lambda)}W_R^{\mathsf{m}(\lambda),\dagger})\mathcal{O}_{\mathsf{comp}}\Pi^{\mathsf{Good}}\Pi^{\mathsf{I},4}\Pi_{\le t}\right\|_{\mathrm{op}}}_{\gamma_3}
\end{aligned}
$$

Where the second and third line is by triangle inequality, and the last line is by Lemma 20. Next, we compute γ_1, γ_2 and γ_3. Before computing this, we know by Lemma 35 that the subspace represented by $\Pi^{\mathsf{Good}}\Pi^{\mathsf{I},4}$ is spanned by $|\chi^{\mathsf{I},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}\mathsf{S}}$.

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

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

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

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

Next, we compute the second term (call it $|\phi_2\rangle$):

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

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

Computing γ_3: Again, 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

$$(I - W_R^{\mathfrak{m}(\lambda)} W_R^{\mathfrak{m}(\lambda),\dagger}) \mathcal{O}_{\mathsf{comp}} |\chi^{\mathfrak{l},3}_{\overline{S},(x_0,x_1),w_1}\rangle_{\mathsf{ABC}\overline{\mathsf{ST}}} = 0$$

Then we have

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

Hence combining, we get

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

□