Pseudorandom Unitaries in the Haar Random Oracle Model[*]

Prabhanjan Ananth[†]
UCSB

John Bostanci[‡]
Columbia

Aditya Gulati[§]
UCSB

Yao-Ting Lin[¶]
UCSB

Abstract

The quantum Haar random oracle model is an idealized model where every party has access to a single Haar random unitary and its inverse. We construct strong pseudorandom unitaries in the quantum Haar random oracle model. This strictly improves upon prior works who either only prove the existence of pseudorandom unitaries in the inverseless quantum Haar random oracle model [Ananth, Bostanci, Gulati, Lin, EUROCRYPT 2025] or prove the existence of a weaker notion (implied by strong pseudorandom unitaries) in the quantum Haar random oracle model [Hhan, Yamada, 2024]. Our results also present a viable approach for building quantum pseudorandomness from random quantum circuits and analyzing pseudorandom objects in nature.

[*] A preliminary version of a merge of this paper and [ABGL25a] appears in the proceedings of *the 45th Annual International Cryptology Conference* (CRYPTO 2025) [ABGL25b]. This is Part I of the full version.

[†] prabhanjan@cs.ucsb.edu

[‡] johnb@cs.columbia.edu

[§] adityagulati@ucsb.edu

[¶] yao-ting_lin@ucsb.edu

Contents

1 Introduction

Pseudorandom unitaries [JLS18] (PRUs) are efficiently computable unitaries that satisfy the following property: any quantum polynomial time adversary cannot distinguish whether it has oracle access to a PRU or a unitary sampled from the Haar measure. They generalize the notion of t-unitary designs, wherein the number of oracle adversarial queries is upper bounded by t although there are no restrictions on the computational power of the adversary. Both t-designs and pseudorandom unitaries have played a vital role in quantum information science and its interplay with other areas. Notably, they have applications to black-hole physics, quantum benchmarking, lower bounds on space complexity in learning theory and finally, in cryptography.

Exploring the design of quantum pseudorandom primitives has been an ongoing active research direction. Kretschmer's [Kre21; KQST23] work suggests one-way functions might plausibly be a stronger assumption than PRUs. This opens the door of basing pseudorandom unitaries on weaker assumptions than one-way functions. Despite this oracle separation, actually building PRUs from one-way functions has proven a challenging problem. It was only last year that a series of works [LQS+24; AGKL24; MPSY24; ABF+24], culminating in the work of Ma and Huang [MH25], were able to finally establish the feasibility of PRUs from classical cryptographic assumptions. In particular, the concurrent works by [MPSY24; ABF+24] designed selectively secure PRUs from one-way functions and the subsequent work by [MH25] achieved the stronger adaptive security under the same assumption.

In addition to studying the relation between classical cryptography and quantum pseudorandomness, there have been two other lines of works attempting to study the properties of pseudo-random unitaries. The first line of work [BHHP25] posits a concrete quantum assumption that gives rise to PRUs, but is plausibly weaker than one-way functions.[1] However, these kinds assumptions are yet to be tested and not considered standard by the community at the moment. Another line of work studies properties of pseudorandom unitaries in idealized models. One such idealized model that has recently been garnering some interest [BFV20; CM24; ABGL25c; HY24] is the quantum Haar random oracle model (QHROM). In this model, which is a quantum analogue of the classical random oracle model, all the parties have oracle access to $U, U^\dagger$, where U is drawn from the Haar measure. This model can especially come in handy when analyzing cryptographic constructions from random circuits. Our work is geared towards understanding the feasibility of pseudorandom unitaries in the quantum Haar random oracle model.

Haar Random Oracle Model: Prior Work. The question of investigating the possibility of quantum pseudorandomness in QHROM was first initiated by Bouland, Fefferman and Vazirani [BFV20], who proposed the construction of pseudorandom state generators[2] without proof in QHROM. Recently, two independent and concurrent works [HY24; ABGL25c] made further progress and presented provably secure constructions of quantum pseudorandom primitives in QHROM. Hhan

[1] We note that in a later version of [BHHP25], the claim regarding the existence of PRUs under their proposed assumption was retracted; at present, the existence of PRUs under their assumption is currently only conjectured.

[2] Informally speaking, pseudorandom states (PRS) [JLS18] are efficiently computable states that are computationally indistinguishable from Haar random states. Importantly, the computational indistinguishability should hold even if the adversary receives many copies of the state. The existence of PRS is implied by the existence of pseudorandom unitaries.

and Yamada [HY24] showed that pseudorandom function-like state generators[3] [AQY22] exist in QHROM. Ananth, Bostanci, Gulati and, Lin [ABGL25c] showed that pseudorandom unitaries existence in a weaker variant of QHROM, referred to as inverseless quantum Haar random oracle model (iQHROM). In this variant, all the parties receive oracle access to only the Haar unitary U (but not its inverse). These works have left a big gap in our understanding on the existence of pseudorandom unitaries in QHROM. A priori it should not even be clear whether pseudorandom unitaries exist in QHROM (i.e., with inverses). [ABGL25c] showed that in the inverseless QHROM setting, any PRU construction making one parallel query to the Haar unitary is insecure. They also provided a matching upper bound and showed that two sequential queries suffice. In contrast, the minimum number of parallel queries needed for the existence of PRU in QHROM has not been established so far.

Why study the QHROM? Every cryptographic model should be subjected to scrutiny and the QHROM is no different. A potential criticism of the QHROM is that constructions proven secure in the QHROM often offer little to no security guarantees when these constructions are realized in the real world. It is important to note that this line of skepticism is not new and is often used to attack the classical random oracle model. While this does suggest that we need to often exercise care when using the QHROM, or its predecessor the classical random oracle model, to justify the security of cryptographic constructions, these models still offer useful insights into properties of heuristic constructions which we otherwise do not have the tools to analyze. Let us take some concrete examples. Random circuits, which are circuits composed of 1-qubit and 2-qubit Haar unitaries, are popularly used in quantum benchmarking and for quantum advantage experiments [BIS+18; BFNV19; Mov19]. While for deep enough circuits, they are commonly supposed to be indistinguishable from Haar random unitaries, it is often not clear how to reduce the security of cryptographic constructions using random circuits to concrete cryptographic assumptions. Another example is the modeling of physical processes such as black-hole dynamics. A long line of works have posited that black-holes possess information scrambling and thermalization properties similar to Haar random unitaries, but an exact formulation of black-hole dynamics has yet to be found. These kinds of situations, where scientists suspect that objects posses random-like features, but lack a complete model, are well suited to analysis in the QHROM.

Another reason to study the QHROM model is that, perhaps surprisingly, of its implications to the plain model. [ABGL25c], leveraged the result of PRU in the inverseless QHROM, to show that any PRU can be transformed into one where the key length is much shorter than the output length. To put this result in context, there have been a few works in the past that have explored the tradeoff between the output length and the key size of quantum pseudorandom primitives. Gunn, Ju, Ma and Zhandry [GJMZ23] showed that the existence of any (multi-copy) pseudorandom state generator implies the existence of a pseudorandom state generator where the output length is strictly longer than the key size, as long as the adversary receives only one copy of the state. Extending this result to achieve a transformation that preserves the number of copies is an interesting open question. Recently, Levy and Vidick [LV24] achieved some limited results in this direction but fell short of resolving the question. On the other hand, [ABGL25c] showed that in the context of forward-only pseudorandom unitaries, such a transformation – that is, generically

[3] Pseudorandom function-like states (PRFS) [AGKL24], a generalization of pseudorandom states, allows for generation of many pseudorandom states, each indexed by a binary string, using the same key. The existence of PRFS is implied by the existence of pseudorandom unitaries.

transforming a multi-query PRU into a PRU with short keys – is indeed possible.

Our Work. The overarching theme of our work and related works is to address the following question: *What are the cryptographic implications of the quantum Haar random oracle model?* This includes constructing useful cryptography, such as PRUs, in the QHROM, but also adopting insights from studying the QRHOM to get novel results in the plain model.

In this work, we construct strong pseudo-random unitaries in the QHROM.

Theorem 1.1 (PRUs in the QHROM)**.** *Strong pseudo-random unitaries exist in the quantum Haar random oracle model.*

We note that our construction of strong PRUs, presented in Section 4.1, is simple to describe, only makes two queries to the Haar random oracle, and only requires sampling $O(\log^{1+\epsilon}(n))$ bits of randomness, for any constant ϵ, to get security against all adversaries making $\mathsf{poly}(n)$ queries to the strong PRU and Haar random oracle (and their inverses).

1.1 Related Works

Quantum Pseudorandomness. Work on quantum pseudo-randomness began with the paper of [JLS18], which first defined pseudorandom states and unitaries. They also presented the first constructions of pseudo-random states from one-way functions, and presented candidate constructions of pseudo-random unitaries from one-way functions without any security proof. In the years after the paper of [JLS18], several works made progress towards building pseudo-random unitaries by considering related pseudo-random objects with security against adversaries with restricted queries [LQS+24; AGKL24; BM24].

[MPSY24] presented the first construction of non-adaptively secure pseudorandom unitaries (that is, secure against adversaries who only make a single parallel query to the PRU) via the so-called PFC ensemble, i.e. "(random) Permutation-(random) Function-(random) Clifford". Simultaneously, [CDX+24] presented an alternate construction of non-adaptively secure PRUs using random permutations. In a breakthrough paper, [MH25] proved that the PFC ensemble and related $\mathsf{C}^\dagger\mathsf{PFC}$ ensemble yielded a construction of PRUs and strong PRUs from one-way function. The paper extended the compressed oracle technique for random functions from [Zha19] to the path-recording formalism for Haar random unitaries. Since then the path-recording formalism has been used to show that the repeated $\mathsf{FHFHF}\ldots$ ensemble, originally conjectured to be a PRU in [JLS18], is secure [BHHP25]. Using the security of the PFC ensemble, combined with a novel gluing lemma, [SHH25] showed that inverseless PRUs can be formed in surprisingly low depth, assuming sub-exponential LWE.

Idealized Models in the Quantum World. The first works on idealized models in the quantum world studied the quantum random oracle model (QROM), in attempt to prove the post-quantum security of a number of classical cryptographic primitives [BDF+11; Zha15a; Zha15b; TU16; Eat17; Zha19]. In this model, parties can make superposition queries to a *classical* random function.

The quantum auxiliary state model [MNY24; Qia24], and related common Haar random state (CHRS) model [AGL24; CCS24] are models of computation in which all parties have access to an arbitrary polynomial many copies of a common quantum state. This is meant to be the quantum equivalent to the common reference string model. [MNY24; Qia24] show that quantum bit commitments exist in the quantum auxiliary state model, and both [AGL24; CCS24] show that bounded copy pseudo-random states with short keys exist in the CHRS (which in turn imply the existence of quantum bit commitments). Furthermore, [AGL24] rules out quantum cryptography with classical communication in the CHRS, and [CCS24] rule out unbounded copy pseudo-random states. More recently, these models have been used to provide oracle separations between one-way puzzles and efficiently verifiable one-way state generators and other quantum cryptographic primitives [BCN25; BMM+25]. While this idealized model provides interesting constructions of and black-box separations between primitives, the model can be problematic to instantiate in a realistic setting. For example, instantiating the model in the real world might require a complicated multi-party computation to compute a shared quantum state, or a trusted third party who can distribute copies of the state.

The quantum Haar random oracle model (QHROM) was first formally introduced in [CM24], who provided a construction of succinct commitments in the QHROM. However, [CM24] was not able to analyze the security of their construction in the QHROM. Separately, [BFV20] considered the QHROM as an idealized model of black hole scrambling, and provided a construction of pseudo-random states in the QHROM. Similar to [CM24], [BFV20] present their construction without a security proof, although they sketch how a proof might proceed. [HY24] later showed that pseudo-random states and the related pseudo-random function-like state generators exist in the QHROM. Their analysis involves heavy use of the Weingarten calculus and the approximate orthogonality of permutations. Separately, [ABGL25c] consider a modification to the QHROM called the inverseless QHROM (iQHROM). They construct forward-only PRUs in this model and provide a security proof using the path-recording formalism of [MH25]. Finally, [Kre21] considers another variant of the QHROM where all parties have access to an exponential number of Haar random unitaries. They show that in this model, pseudo-random unitaries exist but one-way functions can be broken with PSPACE computation.

2 Technical Overview

Ma-Huang's Path Recording Framework. Before we recall the isometries described by [MH25], we first set up some notation. A relation R is defined as a *multiset* $R = \{(x_1, y_1), \dots, (x_t, y_t)\}$ of ordered pairs $(x_i, y_i) \in [N] \times [N]$, for some $N \in \mathbb{N}$. For any relation $R = \{(x_1, y_1), \dots, (x_t, y_t)\}$, 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* $\mathrm{Dom}(R) := \{x \colon x \in [N], \exists\, y \text{ s.t. } (x, y) \in R\}$ and $\mathrm{Im}(R)$ to denote the *set* $\mathrm{Im}(R) := \{y \colon y \in [N], \exists\, x \text{ s.t. } (x, y) \in R\}$. We define the following two operators (which are partial isometries) such that for any relations L, R,[4]

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

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

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

In [MH25], relation states are defined for arbitrary relations, whereas we will not require them in this work.

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

Using V^L and V^R, they define the following partial isometry:

$$V = V^L\cdot(\mathrm{id}-V^R\cdot V^{R,\dagger}) + (\mathrm{id}-V^L\cdot V^{L,\dagger})\cdot V^{R,\dagger}.$$

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 $(A_1, A_2, \ldots, A_{2t})$ such that $\mathcal{A}$ alternatively makes t forward queries and t inverse queries. The final state of $\mathcal{A}$ with oracle access to (fixed) $U, U^\dagger$ is denoted by

$$|\mathcal{A}_t^{U,U^\dagger}\rangle_{\mathsf{AB}} := \prod_{i=1}^{t}\left(U^\dagger A_{2i} U A_{2i-1}\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}},$$

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

$$|\mathcal{A}_t^{V,V^\dagger}\rangle_{\mathsf{ABST}} := \prod_{i=1}^{t}\left(V^\dagger A_{2i} V A_{2i-1}\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}.$$

[MH25] showed that ρ_{Haar} is $O(t^2/N^{1/8})$-close to ρ_{MH} in trace distance, where

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

μ_n denotes the Haar measure over n-qubit unitaries and $N = 2^n$.

2.1 Strong PRUs in the QHROM

We begin with our construction of strong PRU in the QHROM. On input the security $\lambda \in \mathbb{N}$ and key $k \in \{0,1\}^{3\lambda}$, our construction is described as follows:

$$G^U(1^\lambda, k) := X^{k_3}\cdot U_\lambda \cdot X^{k_2}\cdot U_\lambda\cdot X^{k_1},$$

where U_λ is the λ-qubit Haar random oracle and the key is written as $k := k_1||k_2||k_3$, i.e., the concatenation of three λ-bit strings.

To analyze our construction, we consider an adversary $\mathcal{A}$ that has oracle access to $\mathcal{O}_1, \mathcal{O}_2$ and their respective inverses $\mathcal{O}_1^\dagger, \mathcal{O}_2^\dagger$. The adversary operates on the registers AB and is parameterized as a sequence of unitaries $\mathcal{A} = (A_1, A_2, \ldots, A_{4t})$ each acting on AB. Without loss of generality, we assume that all oracle queries are made on the register A, following a fixed sequence of interactions: first querying $\mathcal{O}_1$, then $\mathcal{O}_2$, followed by their inverses $\mathcal{O}_1^\dagger$ and $\mathcal{O}_2^\dagger$. The final state of the adversary after making t queries to each oracle is given by:

$$|\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}\rangle_{\mathsf{AB}} = \prod_{i=1}^{t}\left(\mathcal{O}_2^\dagger\cdot A_{4i}\cdot\mathcal{O}_1^\dagger\cdot A_{4i-1}\cdot\mathcal{O}_2\cdot A_{4i-2}\cdot\mathcal{O}_1\cdot A_{4i-3}\right)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}.$$

In the ideal experiment, $\mathcal{O}_1 = U_1$ and $\mathcal{O}_2 = U_2$ where U_1, U_2 are independently sampled from the Haar distribution. In the real experiment, $\mathcal{O}_1 = U$ and $\mathcal{O}_2 = G^U(1^\lambda, k)$ where U is sampled from the Haar distribution and k are sampled uniformly from $\{0,1\}^{3\lambda}$.

2.1.1 Using the Path Recording Framework

The first step in our analysis is to replace the Haar-random unitaries with *path-recording isometries*.

Ideal Experiment: In the ideal experiment, we replace the two independent Haar-random unitaries U_1 and U_2 with two corresponding *path-recording isometries* V_1 and V_2. These path-recording isometries operate on *independent databases* stored in the purification registers, denoted as (L_1, R_1) and (L_2, R_2), respectively.

Real Experiment: In the real experiment, we replace the Haar-random oracle U with a *single path-recording isometry* V. Unlike the idealized case, here the purification register maintains a *combined database* (L, R), along with the *keys* (k_1, k_2, k_3) for strong PRU construction.

Note that at the end of the computation, the purification register is traced out. Consequently, if we can construct an isometry that acts on the purification register and that maps the output of one case close to the other, then the adversary's view remains statistically indistinguishable between the two cases.[5]

2.1.2 Defining the Isometry $\mathcal{S}$

We define an approximate isometry $\mathcal{S}$ such that it acts on the purification register of the adversary in the ideal experiment and maps it close to the state in the real experiment. Specifically, $\mathcal{S}$ serves as a *merge operator*, combining two independent databases into a single unified database while simultaneously simulating keys.

Formally, $\mathcal{S}$ acts on the auxiliary registers as follows:

$$\mathcal{S} : ((L_1, R_1), (L_2, R_2)) \mapsto (L, R, k_1, k_2, k_3)$$

where:

- (L, R) is the merged database containing all recorded queries
- k_1, k_2, k_3 are simulated keys compatible with the original PRU construction.

The key challenge in defining $\mathcal{S}$ such that when it is applied to the ideal experiment, it closely mimics the real experiment, while still being an isometry (i.e., reversible). We talk more about how we define $\mathcal{S}$ such that it is reversible in Section 4.3. The rest of proof focuses on showing that $\mathcal{S}$ maps the state in the real experiment to the state in the ideal experiment.

2.1.3 Progress Measure

The main challenge in demonstrating that $\mathcal{S}$ approximately maps the state in the real experiment close to the one in the ideal experiment is the difficulty of obtaining a simple closed-form expression, as was possible in the inverseless setting (see [ABGL25c]). Instead, we draw inspiration from the query-by-query analysis approach in the literature of the quantum random oracle

[5] This is because applying an isometry on the traced out registers does not change the final state.

model [Zha19; CMS19; 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 ideal oracles), the process of first simulating the keys and then making a query to a real oracle (e.g., V) is close to making a query to a corresponding ideal oracle (e.g., V_1) first and then simulating the keys. Formally, we show that the following two states are close:

$$V\mathcal{S}|\psi\rangle \quad \text{and} \quad \mathcal{S}V_1|\psi\rangle\,,$$

which we establish by proving that the operator norm bound

$$\|(V\mathcal{S} - \mathcal{S}V_1)\Pi_{\leq t}\|_{\mathrm{op}} = \mathsf{negl}(n)\,,$$

where $\Pi_{\leq t}$ denotes the projector acting on the Hilbert spaces labeled by $\mathsf{S}_1\mathsf{T}_1\mathsf{S}_2\mathsf{T}_2$ that projects onto the space spanned by $|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}$ such that $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$ and $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$. Similarly, we extend this argument to show all the following quantities

1. $\|(V^\dagger\mathcal{S} - \mathcal{S}V_1^\dagger)\Pi_{\leq t}\|_{\mathrm{op}}$
2. $\|(X^{k_3}VX^{k_2}VX^{k_1}\mathcal{S} - \mathcal{S}V_2)\Pi_{\leq t}\|_{\mathrm{op}}$
3. $\|(X^{k_1}V^\dagger X^{k_2}V^\dagger X^{k_3}\mathcal{S} - \mathcal{S}V_2^\dagger)\Pi_{\leq t}\|_{\mathrm{op}}$

are negligible when $t(n) = \mathsf{poly}(n)$. As the main technical contribution of this work, the details can be found in Section 6 and Section 7. By establishing these bounds, we can inductively analyze the adversary's distinguishing advantage after each query (for details, see Section 4.8). Hence, we show that $\mathcal{S}$ approximately maps the state in the real experiment to the one in the ideal experiment.

2.1.4 Simplifications for the Analysis

To streamline our analysis, we introduce several simplifications that make computations more manageable. We outline some key steps below:

Leveraging Unitary Invariance of the Haar Measure: In the real experiment, we have access to two oracles: U and $X^{k_3}UX^{k_2}UX^{k_1}$, along with their inverses. These oracles are difficult to work with because the second oracle involves two calls to U and depends on all three keys, whereas the first oracle is comparatively simple. To balance the difficulty in analysis across both oracles, we use the unitary invariance of the Haar measure. Specifically, we apply the transformation

$$U \mapsto X^{k_3}UX^{k_1}$$

and redefine the key k_2 as

$$k_2 \mapsto k_1 \oplus k_2 \oplus k_3\,.$$

This effectively changes our oracle pair to $X^{k_3}UX^{k_1}$ and $UX^{k_2}U$ (along with their inverses), making the analysis easier.

Working with Non-Norm-Preserving Operators Instead of Isometries: Explicitly maintaining normalization coefficients throughout the analysis can lead to unnecessary complications, especially when we only care about asymptotic behavior. To simplify calculations, we work with non-norm-preserving (i.e., unnormalized) operators, and then establish that these operators remain close to isometries. For more details, see Section 5.

Decoupling L and R: To further simplify our framework, we modify the operators so that L and R become completely independent. Instead of using the partial isometry

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

we switch to

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

A similar transformation is applied to V^R, replacing it with F^R. The operator F is defined analogously to V. Using techniques analogous to those in [MH25], we show that these modified operators remain negligibly close to the original ones while significantly simplifying calculations (see Appendix A.1).

2.1.5 Overview of Hybrids

To prove that our strong pseudorandom unitary (PRU) construction is secure, we go through the following stages from the real experiment (an adversary querying the PRU and Haar random oracle) to the ideal experiment (an adversary querying two Haar random unitaries):

- **Real Experiment:** The adversary has oracle access to the Haar oracle and the PRU construction and their inverses:
$$\mathcal{O}_1 = U, \quad \mathcal{O}_2 = X^{k_3}UX^{k_2}UX^{k_1}.$$
- H_1**:** By leveraging the unitary invariance of the Haar measure, we equivalently define the following oracles to balance complexity:
$$\mathcal{O}_1 = X^{k_3}UX^{k_1}, \quad \mathcal{O}_2 = UX^{k_2}U.$$
- H_2**:** We replace the Haar-random unitary U with the path-recording isometry V, allowing us to track queries explicitly:
$$\mathcal{O}_1 = X^{k_3}VX^{k_1}, \quad \mathcal{O}_2 = VX^{k_2}V.$$
- H_3**:** We modify the path-recording isometry to ensure that the registers L and R are independent, making calculations simpler:
$$\mathcal{O}_1 = X^{k_3}FX^{k_1}, \quad \mathcal{O}_2 = FX^{k_2}F.$$

- H_4**:** This is where most of our technical contributions lie. We introduce $\mathcal{S}$ to transition from separate databases to a merged structure while simulating keys. We use query-by-query analysis to show closeness of the H_3 and H_4:

$$\mathcal{O}_1 = F_1, \quad \mathcal{O}_2 = F_2.$$

- H_5**:** We transition back from F_1, F_2 to standard path-recording isometries:

$$\mathcal{O}_1 = V_1, \quad \mathcal{O}_2 = V_2.$$

- **Ideal Experiment:** Finally, we switch from path-recording isometries back to independent Haar-random unitaries:

$$\mathcal{O}_1 = U_1, \quad \mathcal{O}_2 = U_2.$$

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

Sets and vectors. For $N \in \mathbb{N}$, we use the notation $[N]$ to refer to the set $\{1, 2, \ldots, N\}$. For two binary strings a, b of equal length, we define $a \oplus b$ as their bitwise XOR. For a set of binary strings $A \subseteq \{0,1\}^n$ and a binary string $b \in \{0,1\}^n$, we define

$$A \oplus b := \{\, a \oplus b \colon a \in A \,\}.$$

For two sets $A, B \subseteq \{0,1\}^n$ of binary strings, we define

$$A \oplus B := \{\, x \colon \exists a \in A, b \in B \text{ s.t. } x = a \oplus b \,\}.$$

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 $i \neq j$, $y_i \neq y_j$. For any vector $\vec{x}$, we also define the set $\{\vec{x}\} := \bigcup_{i \in [t]} \{x_i\}$. We denote the i-th coordinate of $\vec{x}$ by x_i. For an ordered set A and an element $x \in A$, we denote by $x \in_i A$ to mean x is the i-th largest element in A. For any vector $\vec{x} \in A^t$, index $i \in [t]$, and element $y \in A$, let $\vec{x}^{(i \leftarrow y)}$ denote the vector obtained by inserting y into the i-th coordinate of $\vec{x}$ and shifting all subsequent coordinates one position to the right. For any vector $\vec{x} \in A^t$ and index $i \in [t]$, let $\vec{x}_{-i}$ denote the vector obtained by deleting its i-th coordinate and shifting all subsequent coordinates one position to the left.

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. We use $\||\psi\rangle\|_2 = \sqrt{\langle\psi|\psi\rangle}$ to denote the Euclidean 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. 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).

3.2 Cryptographic Primitives

In this section, we define strong pseudo-random 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 3.1 (Adversaries with Forward and Inverse Access to Two Oracles)**.** *An adversary $\mathcal{A}$ with oracle access to two n-qubit unitaries $\mathcal{O}_1, \mathcal{O}_2$ and their inverses $\mathcal{O}_1^\dagger, \mathcal{O}_2^\dagger$ is defined as follows. $\mathcal{A}$ has n-qubit query register A and a finite-size ancilla register B, and always queries the oracles on the register A. By padding with dummy queries, we assume that the adversary queries the oracles in the order $(\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_1^\dagger, \mathcal{O}_2^\dagger)$. An adversary $\mathcal{A}$ making t queries to each oracle is parameterized by a sequence of unitaries $(A_1, A_2, \ldots, A_{4t})$ acting on AB. We denote the final state of the adversary as*

$$|\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}\rangle_{\mathsf{AB}} := \prod_{i=1}^{t}\left(\mathcal{O}_2^\dagger \cdot A_{4i} \cdot \mathcal{O}_1^\dagger \cdot A_{4i-1} \cdot \mathcal{O}_2 \cdot A_{4i-2} \cdot \mathcal{O}_1 \cdot A_{4i-3}\right) |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}.$$

Definition 3.2 (Strong Pseudorandom Unitaries)**.** *We say that $\{\mathcal{G}_\lambda\}_{\lambda\in\mathbb{N}}$ is a strong pseudorandom unitary if, for all $\lambda \in \mathbb{N}$, $\mathcal{G}_\lambda = \{G_k\}_{k\in\mathcal{K}_\lambda}$ is a set of $m(\lambda)$-qubit unitaries where $\mathcal{K}_\lambda$ denotes the key space, satisfying the following:*

1. **Efficient Computation:** *There exists a $\mathsf{poly}(\lambda)$-time quantum algorithm that implements G_k for all $k \in \mathcal{K}_\lambda$.*

2. **Indistinguishability from Haar:** *For any quantum polynomial-time oracle adversary $\mathcal{A}$, there exists a negligible function negl such that for all $\lambda \in \mathbb{N}$,*

$$\left| \Pr_{k\leftarrow\mathcal{K}_\lambda}\left[1 \leftarrow \mathcal{A}^{G_k, G_k^\dagger}(1^\lambda)\right] - \Pr_{U\leftarrow\mu_{m(\lambda)}}\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^\lambda)\right] \right| \leq \mathsf{negl}(\lambda)\,.$$

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

3.3 Useful Lemmas

Here we present some standard lemmas.

Lemma 3.3. *For any operator A and vector $|\psi\rangle$, $\|A|\psi\rangle\|_2 \leq \|A\|_{\mathrm{op}}\||\psi\rangle\|_2$.*

Lemma 3.4. *Let A be an operator and let $\mathcal{B}$ be an orthonormal basis of the domain of A. If $A|i\rangle$ is orthogonal to $A|j\rangle$ for all distinct $|i\rangle, |j\rangle \in \mathcal{B}$, then*

$$\|A\|_{\mathrm{op}} = \max_{|i\rangle\in\mathcal{B}} \|A|i\rangle\|_2.$$

Proof. For any normalized $|\psi\rangle = \sum_{|i\rangle \in \mathcal{B}} \alpha_i |i\rangle$, we have

$$\| A|\psi\rangle \|_2^2 = \| \sum_{|i\rangle \in \mathcal{B}} \alpha_i \cdot A|i\rangle \|_2^2 = \sum_{|i\rangle \in \mathcal{B}} |\alpha_i|^2 \cdot \| A|i\rangle \|_2^2 \leq \max_{|i\rangle \in \mathcal{B}} \| A|i\rangle \|_2^2. \qquad \square$$

3.4 Path-Recording Framework

We recall the path-recording framework. The following definitions are taken from [MH25] with modest changes for our purposes.

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. 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* $\mathrm{Dom}(R) := \{x \colon x \in [N], \exists\, y \text{ s.t. } (x, y) \in R\}$ and $\mathrm{Im}(R)$ to denote the *set* $\mathrm{Im}(R) := \{y \colon y \in [N], \exists\, x \text{ s.t. } (x, y) \in R\}$. For any $t \geq 0$, let $\mathcal{R}_t$ denote the set of all relations of size t. Let $\mathcal{R} := \bigcup_{i=0}^{\infty} \mathcal{R}_t$. The size of a relation refers to the number of ordered pairs in the relation, including multiplicities. We denote this by $|R|$, as the size corresponds to the cardinality of R viewed as a multiset. Let $\mathcal{R}_t^{\mathcal{I}\text{-dist}}$ be the set of all $\mathcal{I}$-distinct relations of size t. Let $\mathcal{R}_t^{\mathcal{D}\text{-dist}}$ be the set of all $\mathcal{D}$-distinct relations of size t. Let $\mathcal{R}^{\mathcal{I}\text{-dist}} := \bigcup_{i=0}^{\infty} \mathcal{R}_t^{\mathcal{I}\text{-dist}}$ and $\mathcal{R}^{\mathcal{D}\text{-dist}} := \bigcup_{i=0}^{\infty} \mathcal{R}_t^{\mathcal{D}\text{-dist}}$. Let $\mathcal{R}_{\leq t}^{\mathcal{I}\text{-dist}} := \bigcup_{i=0}^{t} \mathcal{R}_t^{\mathcal{I}\text{-dist}}$ and $\mathcal{R}_{\leq t}^{\mathcal{D}\text{-dist}} := \bigcup_{i=0}^{t} \mathcal{R}_t^{\mathcal{D}\text{-dist}}$.

Variable-length registers. For every integer $t \geq 0$, let $\mathsf{S}^{(t)}$ be a register associated with the Hilbert space

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

Let S be a register corresponding to the infinite-dimensional Hilbert space

$$\mathcal{H}_{\mathsf{S}} := \bigoplus_{t=0}^{\infty} \mathcal{H}_{\mathsf{S}}^{(t)} = \bigoplus_{t=0}^{\infty} \left(\mathbb{C}^N \otimes \mathbb{C}^N\right)^{\otimes t}.$$

When $t = 0$, the space $\left(\mathbb{C}^N \otimes \mathbb{C}^N\right)^{\otimes 0} = \mathbb{C}$ is a one-dimensional Hilbert space. Thus, $\mathcal{H}_{\mathsf{S}}^{(t)}$ is spanned by the states

$$|x_1, y_1, \ldots, x_t, y_t\rangle \qquad \text{where } x_i, y_i \in [N].$$

Note that the relation states $|R\rangle$ for $R \in \mathcal{R}_t$ span the symmetric subspace of $\mathcal{H}_{\mathsf{S}}^{(t)}$. We will sometimes divide up the register $\mathsf{S}^{(t)}$ as

$$\mathsf{S}^{(t)} := (\mathsf{S}_{\mathsf{X}}^{(t)}, \mathsf{S}_{\mathsf{Y}}^{(t)}),$$

where $\mathsf{S}_{\mathsf{X}}^{(t)}$ refers to the registers containing $|x_1, \ldots, x_t\rangle$ and $\mathsf{S}_{\mathsf{Y}}^{(t)}$ refers to the registers containing $|y_1, \ldots, y_t\rangle$. We denote $\mathsf{S}_{\mathsf{X},i}^{(t)}$ as the register containing $|x_i\rangle$ and $\mathsf{S}_{\mathsf{Y},i}^{(t)}$ as the register containing $|y_i\rangle$.

Following our convention for defining the length/size of a relation R, we say that a state $|x_1, y_1, \ldots, x_t, y_t\rangle$ has length/size t. Two states of different lengths are orthogonal by definition, since $\mathcal{H}_{\mathsf{S}}$ is a direct sum $\bigoplus_{t=0}^{\infty} \mathcal{H}_{\mathsf{S}}^{(t)}$.

Notation 3.5. *For any $L \in \mathcal{R}^{\mathcal{I}\text{-dist}} \cup \mathcal{R}^{\mathcal{D}\text{-dist}}$, define the relation state*

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

where $t := |L|$.[6] *For any integer $t \geq 0$, let $\Pi_{\leq t}$ denote the projector*[7]

$$\bigoplus_{\substack{L \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R \in \mathcal{R}^{\mathcal{D}\text{-dist}}: \\ |L|+|R| \leq t}} |L\rangle\langle L|_{\mathsf{S}} \otimes |R\rangle\langle R|_{\mathsf{T}}\,.$$

Definition 3.6 (Path-Recording Oracle, [MH25, Definitions 25 and 26])**.** *Define the following two operators (which are partial isometries). For any $x \in [N]$ and relations $L, R \in \mathcal{R}$ such that $|L| + |R| < N$,*

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

For any $y \in [N]$ and relations $L, R \in \mathcal{R}$ such that $|L| + |R| < N$,

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

Define the following operator (which is a partial isometry).

$$V := V^L \cdot (\mathrm{id} - V^R \cdot V^{R,\dagger}) + (\mathrm{id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger}.$$

Theorem 3.7 ([MH25, Theorem 8])**.** *For any integer $0 \leq t < N$ and adversary $\mathcal{A} = (A_1, \dots, A_{2t})$,*

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

where

$$|\mathcal{A}_t^{U,U^\dagger}\rangle := \prod_{i=1}^{t} \left(U^\dagger \cdot A_{2i} \cdot U \cdot A_{2i-1} \right) |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}}, \quad \textit{and}$$

$$|\mathcal{A}_t^{V,V^\dagger}\rangle := \prod_{i=1}^{t} \left(V^\dagger \cdot A_{2i} \cdot V \cdot A_{2i-1} \right) |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{S}} |\varnothing\rangle_{\mathsf{T}}.$$

We will work with the following variants of path-recording oracles throughout this work.

Definition 3.8 (Operators F^L, F^R, and F)**.** *For any $x \in [N]$, $L \in \mathcal{R}^{\mathcal{I}\text{-dist}}$ and $R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ such that $|L| + |R| < N$,*

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

[6] In [MH25], relation states are defined for arbitrary relations, whereas we will not require them in this work.

[7] We note that our definition of $\Pi_{\leq t}$ differs from that in [MH25].

For any $y \in [N]$, $L \in \mathcal{R}^{\mathcal{I}\text{-dist}}$ and $R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ such that $|L| + |R| < N$,

$$F^R \colon |y\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} \mapsto \frac{1}{\sqrt{N}} \sum_{x \notin \mathrm{Dom}(R)} |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R \cup \{(x,y)\}\rangle_{\mathsf{T}}. \tag{2}$$

Define the operator

$$F := F^L \cdot (\mathrm{id} - F^R \cdot F^{R,\dagger}) + (\mathrm{id} - F^L \cdot F^{L,\dagger}) \cdot F^{R,\dagger}. \tag{3}$$

When $N = 2^\lambda$ and $t = \mathsf{poly}(\lambda)$, we show that F is negligibly close to V in operator norm. The formal statements and their proofs can be found in Appendix A.1. Notice that F^L and F^R are *not* partial isometries. In fact, they are contractions; that is, the operator norm of $F^L, F^R, F^{L,\dagger}, F^{R,\dagger}$ are all bounded by 1. Nevertheless, they preserve orthogonality between the standard basis vectors of the domain. Formally, we have the following lemma.

Fact 3.9. *For any distinct triples $(x, L, R) \neq (x', L', R')$, the states $F^L|x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}}$ and $F^L|x'\rangle_{\mathsf{A}}|L'\rangle_{\mathsf{S}}|R'\rangle_{\mathsf{T}}$ are orthogonal. Therefore, the set of subnormalized vectors*

$$\{F^L|x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}}\}_{(x,L,R)}$$

form an orthogonal basis for the image of F^L where (x, L, R) ranges over $x \in [N], L \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ such that $|L| + |R| < N$. Similar conditions hold for F^R as well.

Their adjoint operators $F^{L,\dagger}$ and $F^{R,\dagger}$ acts as follow:

For any $y \in [N], L \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$,

$$F^{L,\dagger} \cdot |y\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} = \begin{cases} \frac{1}{\sqrt{N}}|x\rangle_{\mathsf{A}}|L \setminus \{(x,y)\}\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} & \text{if } \exists x \in [N] \text{ s.t. } (x,y) \in L \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

For any $x \in [N], L \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$,

$$F^{R,\dagger} \cdot |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R\rangle_{\mathsf{T}} = \begin{cases} \frac{1}{\sqrt{N}}|y\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}|R \setminus \{(x,y)\}\rangle_{\mathsf{T}} & \text{if } \exists y \in [N] \text{ s.t. } (x,y) \in R, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Let T be a partial isometry. It is well known that the operator $T^\dagger T$ is the orthogonal projection onto the domain of T. The domains of V^L and V^R are given by the span of all relation states. Although F^L and F^R are not partial isometries, they satisfy the following properties.

Lemma 3.10. *For any integer $t \geq 0$,*

$$\|(F^{L,\dagger}F^L - \mathrm{id})\Pi_{\leq t}\| \leq t/N \quad \textit{and} \quad \|(F^{R,\dagger}F^R - \mathrm{id})\Pi_{\leq t}\| \leq t/N.$$

The proof can be found in Appendix A.2. The following operators will be used extensively in Sections 6 and 7.

Definition 3.11 (Operators F^L_{extract} and F^R_{extract}). *Define the partial isometry F_L^{extract} such that for any $L \in \mathcal{R}^{\mathcal{I}\text{-dist}}$ and $y \notin \text{Im}(L)$,*

$$F^L_{\text{extract}} \colon |y\rangle_{\mathsf{A}}|L \cup \{(x,y)\}\rangle_{\mathsf{S}} \mapsto |y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}}, \tag{6}$$

where register A' labels a Hilbert space with the same dimension as A. Similarly, define the partial isometry F_R^{extract} such that for any $R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ and $x \notin \text{Dom}(R)$,

$$F^R_{\text{extract}} \colon |x\rangle_{\mathsf{A}}|R \cup \{(x,y)\}\rangle_{\mathsf{T}} \mapsto |x\rangle_{\mathsf{A}'}|y\rangle_{\mathsf{A}}|R\rangle_{\mathsf{T}}. \tag{7}$$

We will use the following lemma in Section 4 to bound error terms. It can be viewed as a consequence of the "monogamy of entanglement". Intuitively, after applying F^L to a state, the registers A and S_Y become "maximally entangled" (see Fact A.7). The monogamy of entanglement then implies that A and S must be nearly disentangled from T—that is, they lie almost entirely outside the image of F^R, and vice versa.

Lemma 3.12. *For any integer $t \geq 0$ and any unitary U acting non-trivially on the register A,*

$$\|F^{L,\dagger}UF^R\Pi_{\leq t}\|_{\text{op}} \leq 3\sqrt{t(t+2)/N} \quad \textit{and} \quad \|F^{R,\dagger}UF^L\Pi_{\leq t}\|_{\text{op}} \leq 3\sqrt{t(t+2)/N}\,.$$

The proof of Lemma 3.12 can be found in Appendix A.2.

4 Strong Pseudorandom Unitaries in the QHROM

4.1 Construction

Construction 4.1. *For every $\lambda \in \mathbb{N}$, let $\mathcal{K}_\lambda := \{0,1\}^{3\lambda}$ and $\mathcal{G}_\lambda = \{G_k^{\mathcal{U}}\}_{k \in \mathcal{K}_\lambda}$ denote the family of unitaries with access to the Haar random oracle $\mathcal{U} = \{U_\ell\}_{\ell \in \mathbb{N}}$, defined as follows. For every $\lambda \in \mathbb{N}$ and $k \in \mathcal{K}_\lambda$, define the λ-qubit unitary:*

$$G_k^{\mathcal{U}} := X^{k_3} \cdot U_\lambda \cdot X^{k_2} \cdot U_\lambda \cdot X^{k_1},$$

where $k = k_1 \,\|\, k_2 \,\|\, k_3$ with $k_1, k_2, k_3 \in \{0,1\}^\lambda$, and for a bitstring $s = s_1 \cdots s_\lambda$ we set $X^s := \bigotimes_{i=1}^{\lambda} X^{s_i}$ (so $X^0 = \text{id}$, $X^1 = X$).

Remark 4.2. *We observe that Construction 4.1 does not require any ancilla qubits. Moreover, it is optimal in terms of the number of sequential queries to the Haar random oracle. In particular, [ABGL25c] constructs a polynomial-query attack that breaks every non-adaptive PRU constructions in the inverseless QHROM, namely constructions that are allowed to make a single parallel query to the Haar random oracle U of the form $U^{\otimes q}$ for an arbitrary polynomial $q(\lambda)$. We observe that the same attack also applies in the QHROM.*

Theorem 4.3. *The family of unitaries defined in Construction 4.1 is a strong pseudorandom unitary in the QHROM.*

We will prove Theorem 4.3 in Section 4.2. Looking ahead, inspecting the proof shows that if we shorten the key blocks to $n(\lambda) = \omega(\log \lambda)$—that is, $k_1, k_2, k_3 \in \{0,1\}^{n(\lambda)}$—and restrict X to act on only $n(\lambda)$ qubits, the modified construction remains a strong PRU in the QHROM. This yields the following corollary.

Corollary 4.4. *Let $n(\lambda) = \omega(\log \lambda), \mathcal{K}_\lambda := \{0,1\}^{3n(\lambda)}$ for every $\lambda \in \mathbb{N}$ and $\mathcal{F}_\lambda = \{F_k^{\mathcal{U}}\}_{k \in \mathcal{K}_\lambda}$ denote the family of unitaries with access to the Haar random oracle $\mathcal{U} = \{U_\ell\}_{\ell \in \mathbb{N}}$, defined as follows. For every $\lambda \in \mathbb{N}$ and $k \in \mathcal{K}_\lambda$, define the λ-qubit unitary:*

$$F_k^{\mathcal{U}} := (X^{k_3} \otimes \mathrm{id}_{\lambda-n}) \cdot U_\lambda \cdot (X^{k_2} \otimes \mathrm{id}_{\lambda-n}) \cdot U_\lambda \cdot (X^{k_1} \otimes \mathrm{id}_{\lambda-n}),$$

where $k = k_1||k_2||k_3$ with $k_1, k_2, k_3 \in \{0,1\}^{n(\lambda)}$. Then $\{\mathcal{F}_\lambda\}_{\lambda \in \mathbb{N}}$ is a strong PRU in the QHROM.

4.2 Security Proof: Proving Theorem 4.3

Fix λ and let $N = 2^\lambda$. Consider an adversary $\mathcal{A} = (A_1, A_2, \ldots, A_{4t})$ in the strong PRU security experiment. We define the following hybrid states on registers (A, B). Although $\mathcal{A}$ has access to the Haar random oracle of all lengths, Construction 4.1 make queries only to U_λ, which is independent of the oracles of other lengths. We may, without loss of generality, assume that $\mathcal{A}$ queries only the Haar random oracle on λ qubits.

Hybrid $\mathbf{H}_1$: This is the ideal experiment. Namely, the adversary is interacting with two independent Haar random unitaries (U_1, U_2). The final state of the adversary is the following:

$$\rho_1 := \mathop{\mathbb{E}}_{U_1, U_2 \sim \mu_\lambda} \left[|\mathcal{A}_t^{U_1, U_2, U_1^\dagger, U_2^\dagger}\rangle\langle \mathcal{A}_t^{U_1, U_2, U_1^\dagger, U_2^\dagger}| \right].$$

Hybrid $\mathbf{H}_2$: Same as Hybrid $\mathbf{H}_1$ except Haar unitaries (U_1, U_2) are simulated by path-recording oracles (V_1, V_2) defined in Definition 3.6. Define the following state:

$$|\mathbf{H}_2\rangle_{\mathsf{ABS_1T_1S_2T_2}} := \prod_{i=1}^{t} \left(V_2^\dagger \cdot A_{4i} \cdot V_1^\dagger \cdot A_{4i-1} \cdot V_2 \cdot A_{4i-2} \cdot V_1 \cdot A_{4i-3} \right) |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{S_1}} |\varnothing\rangle_{\mathsf{T_1}} |\varnothing\rangle_{\mathsf{S_2}} |\varnothing\rangle_{\mathsf{T_2}},$$

where V_1 acts on the registers $\mathsf{A}, \mathsf{S_1}, \mathsf{T_1}$, and V_2 acts on the registers $\mathsf{A}, \mathsf{S_2}, \mathsf{T_2}$. Define

$$\rho_2 := \mathrm{Tr}_{\mathsf{S_1T_1S_2T_2}}(|\mathbf{H}_2\rangle\langle \mathbf{H}_2|).$$

Hybrid $\mathbf{H}_3$: Same as Hybrid $\mathbf{H}_2$ except (V_1, V_2) are replaced by (F_1, F_2) defined in Definition 3.8. Define the following state:

$$|\mathbf{H}_3\rangle_{\mathsf{ABS_1T_1S_2T_2}} := \prod_{i=1}^{t} \left(F_2^\dagger \cdot A_{4i} \cdot F_1^\dagger \cdot A_{4i-1} \cdot F_2 \cdot A_{4i-2} \cdot F_1 \cdot A_{4i-3} \right) |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{S_1}} |\varnothing\rangle_{\mathsf{T_1}} |\varnothing\rangle_{\mathsf{S_2}} |\varnothing\rangle_{\mathsf{T_2}},$$

where F_1 acts on the registers $\mathsf{A}, \mathsf{S_1}, \mathsf{T_1}$, and F_2 acts on the registers $\mathsf{A}, \mathsf{S_2}, \mathsf{T_2}$. Define

$$\rho_3 := \mathrm{Tr}_{\mathsf{S_1T_1S_2T_2}}(|\mathbf{H}_3\rangle\langle \mathbf{H}_3|).$$

Hybrid $\mathbf{H}_4$: Define the following state:

$$|\mathbf{H}_4\rangle_{\mathsf{ABSTK_1K_2K_3}} := \frac{1}{\sqrt{N^3}} \sum_{k_1,k_2,k_3 \in \{0,1\}^\lambda} \prod_{i=1}^{t} \left(F^\dagger X^{k_2} F^\dagger \cdot A_{4i} \cdot X^{k_1} F^\dagger X^{k_3} \cdot A_{4i-1} \cdot F X^{k_2} F \cdot A_{4i-2} \cdot X^{k_3} F X^{k_1} \cdot A_{4i-3} \right) \cdot |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{S}} |\varnothing\rangle_{\mathsf{T}} |k_1\rangle_{\mathsf{K_1}} |k_2\rangle_{\mathsf{K_2}} |k_3\rangle_{\mathsf{K_3}},$$

where F acts on the registers $\mathsf{A}, \mathsf{S}, \mathsf{T}$, and X^{k_j} acting on register A for $j = 1, 2, 3$. Define

$$\rho_4 := \mathrm{Tr}_{\mathsf{STK_1K_2K_3}}(|\mathbf{H}_4\rangle\langle\mathbf{H}_4|).$$

Hybrid $\mathbf{H}_5$: Same as Hybrid $\mathbf{H}_4$ except F is replaced by V. Define the following state:

$$|\mathbf{H}_5\rangle_{\mathsf{ABSTK_1K_2K_3}} := \frac{1}{\sqrt{N^3}} \sum_{k_1,k_2,k_3 \in \{0,1\}^\lambda} \prod_{i=1}^{t} \left(V^\dagger X^{k_2} V^\dagger \cdot A_{4i} \cdot X^{k_1} V^\dagger X^{k_3} \cdot A_{4i-1} \cdot V X^{k_2} V \cdot A_{4i-2} \cdot X^{k_3} V X^{k_1} \cdot A_{4i-3} \right) \cdot |0\rangle_{\mathsf{A}} |0\rangle_{\mathsf{B}} |\varnothing\rangle_{\mathsf{S}} |\varnothing\rangle_{\mathsf{T}} |k_1\rangle_{\mathsf{K_1}} |k_2\rangle_{\mathsf{K_2}} |k_3\rangle_{\mathsf{K_3}},$$

where V acts on the registers $\mathsf{A}, \mathsf{S}, \mathsf{T}$, and X^{k_j} acting on register A for $j = 1, 2, 3$. Define

$$\rho_5 := \mathrm{Tr}_{\mathsf{STK_1K_2K_3}}(|\mathbf{H}_5\rangle\langle\mathbf{H}_5|).$$

Hybrid $\mathbf{H}_6$: Same as Hybrid $\mathbf{H}_5$ except V is replaced by a λ-qubit Haar random unitary U, and no purifications are introduced. Define

$$\rho_6 := \mathop{\mathbb{E}}_{\substack{k_1,k_2,k_3 \leftarrow \{0,1\}^\lambda,\, U \sim \mu_\lambda \\ \mathcal{O}_1 \equiv X^{k_3} U X^{k_1},\, \mathcal{O}_2 \equiv U X^{k_2} U}} \left[|\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}\rangle\langle\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}| \right].$$

Hybrid $\mathbf{H}_7$: This is the real experiment. Namely, the adversary is interacting with the Haar random oracle and the strong PRU construction $G_k^{\mathcal{U}}$ defined in Construction 4.1. The final state of the adversary is

$$\rho_7 := \mathop{\mathbb{E}}_{\substack{k_1,k_2,k_3 \leftarrow \{0,1\}^\lambda,\, U \sim \mu_\lambda \\ \mathcal{O}_1 \equiv U,\, \mathcal{O}_2 \equiv X^{k_3} U X^{k_2} U X^{k_1}}} \left[|\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}\rangle\langle\mathcal{A}_t^{\mathcal{O}_1,\mathcal{O}_2,\mathcal{O}_1^\dagger,\mathcal{O}_2^\dagger}| \right].$$

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

Claim 4.5. $\mathsf{TD}(\rho_1, \rho_2) = O\left(\frac{t^2}{N^{1/8}}\right)$ *and* $\mathsf{TD}(\rho_5, \rho_6) = O\left(\frac{t^2}{N^{1/8}}\right)$.

Proof. It immediately follows from Theorem 3.7. □

Claim 4.6. $\mathsf{TD}(\rho_2, \rho_3) = O\left(\frac{t^2}{N^{1/2}}\right)$ *and* $\mathsf{TD}(\rho_4, \rho_5) = O\left(\frac{t^2}{N^{1/2}}\right)$.

Proof. It immediately follows from Lemma A.5. □

Claim 4.7. $\rho_6 = \rho_7$.

Proof. We prove a stronger result by showing that the oracles in both hybrids are identically distributed. For any fixed choice of $k_1, k_2, k_3 \in [N]$, $(U, X^{k_3}UX^{k_2}UX^{k_1})$ is identically distributed to $(X^{k_3}UX^{k_1}, X^{k_3} \cdot X^{k_3}UX^{k_1} \cdot X^{k_2} \cdot X^{k_3}UX^{k_1} \cdot X^{k_1}) = (X^{k_3}UX^{k_1}, UX^{k_1 \oplus k_2 \oplus k_3}U)$ by the unitary invariance of the Haar measure. Next, after averaging over k_2, $(X^{k_3}UX^{k_1}, UX^{k_1 \oplus k_2 \oplus k_3}U)$ is identically distributed to $(X^{k_3}UX^{k_1}, UX^{k_2}U)$ since k_2 is uniformly random and independent of U, k_1 and k_3. Finally, averaging over k_1 and k_3 completes the proof. □

Lemma 4.8. $\mathsf{TD}(\rho_3, \rho_4) = O\left(\frac{t^2}{N^{1/2}}\right)$.

Proving Lemma 4.8 is the main technical step of proving Theorem 4.3. Toward the proof, we begin by defining an approximate isometry $\mathcal{S}$ in Section 4.3, which we then use to prove Lemma 4.8 in Section 4.8.

Proof of Theorem 4.3. It immediately follows from a standard hybrid argument, Claims 4.5 to 4.7 and Lemma 4.8. □

4.3 Auxiliary Definitions

4.3.1 Overview

Our goal is to show the closeness between the adversary's final states in hybrids $\mathbf{H}_3$ and $\mathbf{H}_4$. We start by noting that in hybrid $\mathbf{H}_3$, the purification register contains two pairs of "databases" on registers $(\mathsf{S}_1, \mathsf{T}_1)$ and $(\mathsf{S}_2, \mathsf{T}_2)$, whereas in hybrid $\mathbf{H}_4$, the purification register contains a single pair of databases on registers (S, T) along with the key registers $(\mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3)$. Indeed, two quantum states are equal if their purifications are related by an isometry acting solely on the traced-out registers. Thus, it suffices to find an (approximate) isometry $\mathcal{S}$ that maps the purification registers $(\mathsf{S}_1, \mathsf{T}_1, \mathsf{S}_2, \mathsf{T}_2)$ in hybrid $\mathbf{H}_3$ to the purification registers $(\mathsf{S}, \mathsf{T}, \mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3)$ in hybrid $\mathbf{H}_4$.

Before defining $\mathcal{S}$, we present a "classical" analogue which, while not exact, serves to motivate the upcoming definitions. Suppose $\mathcal{A}$ in hybrid $\mathbf{H}_3$ makes one query x to F_1. Informally, the action of F_1 can be viewed first "sampling" a uniform $y \notin \mathrm{Im}(L_1)$, then "adding" the pair (x, y) to L_1, and finally returning y back to $\mathcal{A}$, all in superposition. On the other hand, suppose $\mathcal{A}$ in hybrid $\mathbf{H}_4$ makes one query x to $X^{k_3}FX^{k_1}$. Similarly, $(x \oplus k_1, y)$ is added to L, and $y \oplus k_3$ is returned to $\mathcal{A}$. We can relabel $y \oplus k_3 \mapsto y$ to have that $(x \oplus k_1, y \oplus k_3)$ is added to L, and y is returned to $\mathcal{A}$. Now, suppose $\mathcal{A}$ in hybrid $\mathbf{H}_3$ makes q queries to F_1, so that L_1 becomes $\{(x_1, y_1), \dots, (x_q, y_q)\}$. By inspection, the corresponding L is $\{(x_1 \oplus k_1, y_1 \oplus k_3), \dots, (x_q \oplus k_1, y_q \oplus k_3)\}$, which is identical to that of L_1 except that each element in the domain is XOR-ed with k_1, and each element in the range is XOR-ed with k_3. We refer to it as the *augmented relation of* L_1 parameterized by (k_1, k_3). We denote it by $L_1^{\ell,(k_1,k_3)}$.

Next, consider a query x to F_2 in hybrid $\mathbf{H}_3$. In this case, a uniform $y \notin \mathrm{Im}(L_2)$ is sampled, the pair (x, y) is added to L_2, and y it returned to $\mathcal{A}$, all in superposition. By contrast, in hybrid $\mathbf{H}_4$, a query x to $FX^{k_2}F$ proceeds as follows: F samples a uniform $z \notin \mathrm{Im}(L)$, adds the pair (x, z) to L, XORs z by k_2, samples a uniform $y \notin \mathrm{Im}(L)$, adds the pair $(z \oplus k_2, y)$ to L, and finally returns to $\mathcal{A}$. Similarly, suppose $\mathcal{A}$ in hybrid $\mathbf{H}_3$ makes q queries to F_2, so that L_2 becomes $\{(x_1, y_1), \dots, (x_q, y_q)\}$. The corresponding L is $\{(x_1, z_1), (z_1 \oplus k_2, y_1), \dots, (x_q, z_q), (z_q \oplus k_2, y_q)\}$, where $\vec{z} = (z_1, \dots, z_q)$ is a vector of distinct coordinates. An important observation, also noted in [ABGL25c], is that the elements are “paired” by k_2 and are referred to as *k_2-correlated pairs*. We refer to it as the *augmented relation of* L_2 parameterized by $(\vec{z}, k_2)$. We denote it by $L_2^{\ell,(\vec{z},k_2)}$.

Suppose $\mathcal{A}$ in hybrid $\mathbf{H}_3$ makes q queries to F_1 and F_2 respectively, leading to $L_1 = \{(x_1, y_1), \ldots, (x_q, y_q)\}$ and $L_2 = \{(x'_1, y'_1), \ldots, (x'_q, y'_q)\}$. Now, in order to map (L_1, L_2) to (L, k_1, k_2, k_3)[8] almost injectively, we approach is as follows. We first sample $(\vec{z}, k_1, k_2, k_3)$ and let $L = L_1^{\ell,(k_1,k_3)} \cup L_2^{\ell,(\vec{z},k_2)}$ such that one can uniquely recover (L_1, L_2) given the information of (L, k_1, k_2, k_3). Following the idea in [ABGL25c], as long as the number of k_2-correlated pairs in L is exactly q, we know that $L_2^{\ell,(\vec{z},k_2)}$ consists of the k_2-correlated pairs in L. Suppose q is polynomial. An elementary combinatorial argument shows that the fraction of “bad” keys for which unique recoverability fails is negligible.

Careful readers may notice that the previous argument does not rely on keys (k_1, k_3). Indeed, the PRU construction in the inverseless QHROM of [ABGL25c] does not use (k_1, k_3); on key k, their construction is simply UX^kU. However, when we move to the strong PRU setting, this construction is insecure–one can learn the key by sequentially querying (1) $U^\dagger$ (2) UX^kU and (3) $U^\dagger$. More generally, queries to $U^\dagger$ may lead to unintended cancellation in the databases. The role of (k_1, k_3) is precisely to prevent such event from happening. Looking ahead, when defining $\mathcal{S}$, the condition on (k_1, k_3) ensures the image and domain of $L_1^{\ell,(k_1,k_3)}$ and $L_2^{\ell,(\vec{z},k_2)}$ are distinct.

4.3.2 Graph-theoretic definitions

In this subsection, we let $N = 2^\lambda$, and use $[N]$ and $\{0,1\}^\lambda$ interchangeably. For the purposes of the proofs in later sections, it is convenient—and also intuitive—to introduce graph-theoretic languages. In particular, the following type of *directed graph* will play an important role.

Definition 4.9 (Decomposable Graphs)**.** *A directed graph G, possibly with self-loops, is* decomposable *if it contains no self-loops and no two edges share a common vertex. In addition, we can uniquely partition its vertex set into three disjoint subsets:*

- $V_{\mathsf{isolate}}(G)$*: the set of vertices with no incoming or outgoing edges*
- $V_{\mathsf{source}}(G)$*: the set of vertices with an outgoing edge*
- $V_{\mathsf{target}}(G)$*: the set of vertices with an incoming edge*

Moreover, we have $|V_{\mathsf{source}}(G)| = |V_{\mathsf{target}}(G)|$.

The following definition connects relation–key pairs to directed graphs.

Definition 4.10 (Relation-Key-Induced Graphs)**.** *For any relation L and $k \in [N]$, define the directed graphs, possibly with self-loops, $G^\ell_{L,k}$ as follows. The vertex set of $G^\ell_{L,k}$ is equal to L.*[9] *For any two vertices (x, y) and (x', y'), there is a directed edge from (x, y) to (x', y') if and only if $x' = y \oplus k$.*

Similarly, for any relation R and $k \in [N]$, define the directed graphs, possibly with self-loops, $G^r_{R,k}$ as follows. The vertex set of $G^r_{R,k}$ is equal to R. For any two vertices (x, y) and (x', y'), there is a directed edge from (x, y) to (x', y') if and only if $y' = x \oplus k$.[10]

[8] Since R_1 and R_2 are empty, we ignore them in the exposition here.

[9] Note that L may contain repeated elements. Equivalently, one can regard the vertex set as having size $|L|$, with each vertex labeled by an element of L.

[10] Notice that this is the opposite of defining edges in $G^\ell_{L,k}$.

4.4 Augmented Relations and (Robust) Decodability

We define augmented relations mentioned in the overview below.

Definition 4.11 (Augmented Relations)**.** *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, $k_1, k_2, k_3 \in [N]$, $\vec{z}_L \in [N]^{|L_2|}_{\text{dist}}$, and $\vec{z}_R \in [N]^{|R_2|}_{\text{dist}}$, define the corresponding* augmented relations:[11]

$$L_1^{\ell,(k_1,k_3)} := \{(x \oplus k_1, y \oplus k_3) : (x,y) \in L_1\}, \tag{8}$$

$$L_2^{\ell,(k_2,\vec{z}_L)} := \{(x_i, z_{L,i}), (z_{L,i} \oplus k_2, y_i) : (x_i, y_i) \in L_2\}, \tag{9}$$

$$R_1^{r,(k_1,k_3)} := \{(x \oplus k_1, y \oplus k_3) : (x,y) \in R_1\}, \tag{10}$$

$$R_2^{r,(k_2,\vec{z}_R)} := \{(x_i, z_{R,i} \oplus k_2), (z_{R,i}, y_i) : (x_i, y_i) \in R_2\}, \tag{11}$$

where we impose an ordering on the elements of L_2 (resp., R_2) by the canonical ordering on $\mathrm{Im}(L_2)$ (resp., $\mathrm{Dom}(R_2)$). That is, we use $(x_i, y_i) \in L_2$ to indicate the element in L_2 such that y_i is the i-th largest element in $\mathrm{Im}(L_2)$, and $(x_i, y_i) \in R_2$ indicate the element in R_2 such that x_i is the i-th largest element in $\mathrm{Dom}(R_2)$.

Remark 4.12. *As expressions like $L_1^{r,(k_1,k_3)}$ or $L_1^{\ell,(k_2,\vec{z}_L)}$ never appear in this work, we omit the superscript ℓ, r in the augmented relations when it is clear from the context.*

Now, given any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, which can be viewed as a view in hybrid $\mathbf{H}_3$. We aim to map it to a view in hybrid $\mathbf{H}_4$ by:

1. sampling $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R)$ from an appropriate distribution;
2. outputting $(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}, k_1, k_2, k_3)$.

To define an (approximate) isometry $\mathcal{S}$ that performs this map coherently, we must ensure that the mapping is (almost) reversible. To this end, we proceed in two steps:

1. Define a "decoder" which, on input (L, R, k_1, k_2, k_3), outputs $(L_1, R_1, L_2, R_2, \vec{z}_L, \vec{z}_R, k_1, k_2, k_3)$.
2. For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, identify conditions on $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R)$ such that applying the decoder to $(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}, k_1, k_2, k_3)$ yields the correct $(L_1, R_1, L_2, R_2, \vec{z}_L, \vec{z}_R, k_1, k_2, k_3)$.

Definition 4.13 (Function Dec and Operator $\mathcal{D}$)**.** *The deterministic function (algorithm)* Dec *is defined as follows:*
Input: *Two relations (L, R) and $(k_1, k_2, k_3) \in [N]^3$*

1. *If G^{ℓ}_{L,k_2} is not decomposable* **or** *G^{r}_{R,k_2} is not decomposable, then output $\perp$ indicating fail.*
2. *If $V_{\mathsf{target}}(G^{\ell}_{L,k_2}) \notin \mathcal{R}^{\mathcal{I}\text{-dist}}$* **or** *$V_{\mathsf{target}}(G^{r}_{R,k_2}) \notin \mathcal{R}^{\mathcal{D}\text{-dist}}$, then output $\perp$.*
3. *Suppose*
    - $V_{\mathsf{isolate}}(G^{\ell}_{L,k_2}) = \{(a_1, b_1), \ldots, (a_s, b_s)\}$

[11] Similar to how we define relations, augmented relations are also defined as multisets.

- $V_{\mathsf{source}}(G^{\ell}_{L,k_2}) = \{(x_1, e_1), \ldots, (x_\ell, e_\ell)\}$
- $V_{\mathsf{target}}(G^{\ell}_{L,k_2}) = \{(e_1 \oplus k_2, y_1), \ldots, (e_\ell \oplus k_2, y_\ell)\}$ *such that* $y_1 < y_2 < \cdots < y_\ell$[12]
- $V_{\mathsf{isolate}}(G^{r}_{R,k_2}) = \{(c_1, d_1), \ldots, (c_t, d_t)\}$
- $V_{\mathsf{source}}(G^{r}_{R,k_2}) = \{(f_1, v_1), \ldots, (f_r, v_r)\}$
- $V_{\mathsf{target}}(G^{r}_{R,k_2}) = \{(u_1, f_1 \oplus k_2), \ldots, (u_r, f_r \oplus k_2)\}$ *such that* $u_1 < u_2 < \cdots < u_r$

4. *Let*

   - $L_{\mathsf{isolate}} := \{(a_1 \oplus k_1, b_1 \oplus k_3), \ldots, (a_s \oplus k_1, b_s \oplus k_3)\}$
   - $L_{\mathsf{pair}} := \{(x_1, y_1), \ldots, (x_\ell, y_\ell)\}$
   - $\vec{m}_L := (e_1, \ldots, e_\ell)$
   - $R_{\mathsf{isolate}} := \{(c_1 \oplus k_1, d_1 \oplus k_3), \ldots, (c_t \oplus k_1, d_t \oplus k_3)\}$
   - $R_{\mathsf{pair}} := \{(u_1, v_1), \ldots, (u_r, v_r)\}$
   - $\vec{m}_R := (f_1, \ldots, f_\ell)$

5. *If* $L_{\mathsf{isolate}} \notin \mathcal{R}^{\mathcal{I}\text{-dist}}$ **or** $L_{\mathsf{pair}} \notin \mathcal{R}^{\mathcal{I}\text{-dist}}$ **or** $R_{\mathsf{isolate}} \notin \mathcal{R}^{\mathcal{D}\text{-dist}}$ **or** $R_{\mathsf{pair}} \notin \mathcal{R}^{\mathcal{D}\text{-dist}}$ **or** $\vec{m}_L$ *has repeated coordinates* **or** $\vec{m}_R$ *has repeated coordinates, then output* $\perp$*.*

6. *If* $\mathrm{Im}(L_{\mathsf{pair}}) \cap \{\vec{m}_L\} \neq \varnothing$ **or** $\mathrm{Dom}(R_{\mathsf{pair}}) \cap \{\vec{m}_R\} \neq \varnothing$*, then output* $\perp$*.*[13]

7. *Output* $(L_{\mathsf{isolate}}, R_{\mathsf{isolate}}, L_{\mathsf{pair}}, R_{\mathsf{pair}}, \vec{m}_L, \vec{m}_R, k_1, k_2, k_3)$

We denote by $\mathcal{D}$ *the operator that performs* Dec *coherently,*[14] *and maps an input to the zero vector if* Dec *evaluates to* $\perp$ *on that input.*

Lemma 4.14 ($\mathcal{D}$ is a partial isometry)**.** *Let* $\mathrm{Supp}(\mathrm{Dec})$ *denote the set of* (L, R, k_1, k_2, k_3) *such that* $\mathrm{Dec}(L, R, k_1, k_2, k_3) \neq \perp$*. Then* Dec *is injective when restricted to* $\mathrm{Supp}(\mathrm{Dec})$*. As a corollary,* $\mathcal{D}$ *is a partial isometry.*

Proof. We prove the lemma by constructing the inverse of Dec on Supp(Dec). We denote this inverse by Enc. On input $(L_{\mathsf{isolate}}, R_{\mathsf{isolate}}, L_{\mathsf{pair}}, R_{\mathsf{pair}}, \vec{m}_L, \vec{m}_R, k_1, k_2, k_3)$, Enc outputs

$$(L_{\mathsf{isolate}}^{(k_1,k_3)} \cup L_{\mathsf{pair}}^{(k_2,\vec{m}_L)}, R_{\mathsf{isolate}}^{(k_1,k_3)} \cup R_{\mathsf{pair}}^{(k_2,\vec{m}_R)}, k_1, k_2, k_3).$$

It suffices to show that for any $(L, R, k_1, k_2, k_3) \in \mathrm{Supp}(\mathrm{Dec})$, the following holds:

$$(L, R, k_1, k_2, k_3) = \mathrm{Enc}(\mathrm{Dec}((L, R, k_1, k_2, k_3))).$$

Suppose in Step 3 of $\mathrm{Dec}(L, R, k_1, k_2, k_3)$, we have

- $V_{\mathsf{isolate}}(G^{\ell}_{L,k_2}) = \{(a_1, b_1), \ldots, (a_s, b_s)\}$
- $V_{\mathsf{source}}(G^{\ell}_{L,k_2}) = \{(x_1, e_1), \ldots, (x_\ell, e_\ell)\}$

[12] Since it passes Step 2, there exists an ordering in the image of $V_{\mathsf{target}}(G^{\ell}_{L,k_2})$.

[13] Recall that for a vector $\vec{v} = (v_1, v_2, \ldots)$, we denote the set $\bigcup_i \{v_i\}$ by $\{\vec{v}\}$.

[14] Since (k_1, k_2, k_3) is classical information, we require Dec to also output (k_1, k_2, k_3).

- $V_{\mathsf{target}}(G^{\ell}_{L,k_2}) = \{(e_1 \oplus k_2, y_1), \dots, (e_\ell \oplus k_2, y_\ell)\}$ such that $y_1 < y_2 < \cdots < y_\ell$
- $V_{\mathsf{isolate}}(G^{r}_{R,k_2}) = \{(c_1, d_1), \dots, (c_t, d_t)\}$
- $V_{\mathsf{source}}(G^{r}_{R,k_2}) = \{(f_1, v_1), \dots, (f_r, v_r)\}$
- $V_{\mathsf{target}}(G^{r}_{R,k_2}) = \{(u_1, f_1 \oplus k_2), \dots, (u_r, f_r \oplus k_2)\}$ such that $u_1 < u_2 < \cdots < u_r$,

and the input satisfies

$$\begin{aligned} L &= \{(a_1,b_1),\dots,(a_s,b_s)\} \cup \{(x_1,e_1),\dots,(x_\ell,e_\ell)\} \cup \{(e_1 \oplus k_2, y_1),\dots,(e_\ell \oplus k_2, y_\ell)\}, \\ R &= \{(c_1,d_1),\dots,(c_t,d_t)\} \cup \{(f_1,v_1),\dots,(f_r,v_r)\} \cup \{(u_1, f_1 \oplus k_2),\dots,(u_r, f_r \oplus k_2)\}. \end{aligned}$$

In Step 4 of $\mathrm{Dec}((L, R, k_1, k_2, k_3))$, we have

- $L_{\mathsf{isolate}} := \{(a_1 \oplus k_1, b_1 \oplus k_3), \dots, (a_s \oplus k_1, b_s \oplus k_3)\}$
- $L_{\mathsf{pair}} := \{(x_1, y_1), \dots, (x_\ell, y_\ell)\}$
- $\vec{m}_L := (e_1, \dots, e_\ell)$
- $R_{\mathsf{isolate}} := \{(c_1 \oplus k_1, d_1 \oplus k_3), \dots, (c_t \oplus k_1, d_t \oplus k_3)\}$
- $R_{\mathsf{pair}} := \{(u_1, v_1), \dots, (u_r, v_r)\}$
- $\vec{m}_R := (f_1, \dots, f_\ell)$.

Recall Definition 4.11. It is straightforward to verify that applying Enc to the above input yields L and R. □

Definition 4.15 (Decodability). *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, a tuple $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R)$ said to be* decodable *(with respect to (L_1, L_2, R_1, R_2)) if*

$$\mathrm{Dec}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}, k_1, k_2, k_3) = (L_1, R_1, L_2, R_2, \vec{z}_L, \vec{z}_R, k_1, k_2, k_3). \quad (12)$$

Remark 4.16. *There are cases that $\mathrm{Dec}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}, k_1, k_2, k_3) \neq \perp$ while does not match the correct $(L_1, R_1, L_2, R_2, \vec{z}_L, \vec{z}_R, k_1, k_2, k_3)$. For example, consider the case where $L_1 = \{(a, b), (b \oplus k_2, c)\}$ and $L_2 = R_1 = R_2 = \varnothing$, then Dec will output $L_{\mathsf{isolate}} = \varnothing$ and $L_{\mathsf{pair}} = \{(a, c)\}$.*

For technical reasons, we require a stronger condition than decodability. Given a decodable tuple $(L_1, L_2, R_1, R_2, \vec{z}_L, \vec{z}_R, k_1, k_2, k_3)$, we use L and R as shorthand for $L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}$ and $R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}$, respectively. In particular, we are concerned with the *robustness* of these tuples. Suppose we delete an element v from L. We are interested in whether $\mathrm{Dec}(L \setminus \{v\}, R, k_1, k_2, k_3)$ remains non-$\perp$.

Definition 4.17 (Robust Decodability). *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, a tuple $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R)$ said to be* robustly decodable *(with respect to (L_1, L_2, R_1, R_2)) if it is decodable and satisfies*

1. $\mathrm{Dec}\left(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \setminus \{v\}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}, k_1, k_2, k_3\right) \neq \perp$ *for all $v \in L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}$, and*
2. $\mathrm{Dec}\left(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}, R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)} \setminus \{u\}, k_1, k_2, k_3\right) \neq \perp$ *for all $u \in R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}$.*

In the following, we list the sufficient conditions for robustly decodable tuples and introduce the shorthands $\mathbf{z} := (\vec{z}_L, \vec{z}_R)$ and $\mathbf{k} := (k_1, k_2, k_3)$.

Lemma 4.18 (Sufficient conditions for robust decodability)**.** *Let $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$. Every 5-tuple $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \in [N] \times [N] \times [N] \times [N]^{|L_2|} \times [N]^{|R_2|}$ that satisfies all the following conditions is decodable:*

1. ***Distinctness:*** *$L_1^{(k_1,k_3)}, L_2^{(k_2,\vec{z}_L)} \in \mathcal{R}^{\mathcal{I}\text{-dist}}$ and $R_1^{(k_1,k_3)}, R_2^{(k_2,\vec{z}_R)} \in \mathcal{R}^{\mathcal{D}\text{-dist}}$*
2. ***Disjointness:*** *$\mathrm{Im}(L_1^{(k_1,k_3)}) \cap \mathrm{Im}(L_2^{(k_2,\vec{z}_L)}) = \varnothing$ and $\mathrm{Dom}(R_1^{(k_1,k_3)}) \cap \mathrm{Dom}(R_2^{(k_2,\vec{z}_R)}) = \varnothing$*
3. ***No extra k_2-correlated pairs:*** *There are exactly $|L_2|$ number of pairs $((x,y),(x',y'))$ with (x,y), $(x',y') \in L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}$ such that $x' = y \oplus k_2$, and there are exactly $|R_2|$ number of pairs $((x,y),(x',y'))$ with $(x,y),(x',y') \in R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_L)}$ such that $y' = x \oplus k_2$*

Furthermore, for all such tuples, it holds that

$$\mathcal{D}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}} = |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}. \tag{13}$$

– For $(x,y) \in L_1^{(k_1,k_3)}$,

$$\begin{aligned}\mathcal{D}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \setminus \{(x,y)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}} \\ = |L_1 \setminus \{(x \oplus k_1, y \oplus k_3)\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}.\end{aligned} \tag{14}$$

– For $(x,y) \in L_{2,\mathsf{source}}^{(k_2,\vec{z}_L)}$, suppose $i \in |L_2|$ is the index such that $y = z_{L,i}$. Let y_i denote the i-th largest element in $\mathrm{Im}(L_2)$ and x_i is the unique element such that $(x_i, y_i) \in L_2$. Then $x = x_i$ and

$$\begin{aligned}\mathcal{D}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \setminus \{(x,y)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}} \\ = |L_1 \cup \{(z_{L,i} \oplus k_2 \oplus k_1, y_i \oplus k_3)\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2 \setminus \{(x_i,y_i)\}\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}.\end{aligned} \tag{15}$$

– For $(x,y) \in L_{2,\mathsf{target}}^{(k_2,\vec{z}_L)}$, let $i \in [|L_2|]$ be the index such that y is the i-th largest element in $\mathrm{Im}(L_2)$, denoted by y_i, and let x_i be the unique value satisfying $(x_i, y_i) \in L_2$. Then $x = z_{L,i} \oplus k_2$ and

$$\begin{aligned}\mathcal{D}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \setminus \{(x,y)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}} \\ = |L_1 \cup \{(x_i \oplus k_1, z_{L,i} \oplus k_3)\}\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2 \setminus \{(x_i,y_i)\}\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}.\end{aligned} \tag{16}$$

Proof. The proof consists of two steps. First, we establish decodability. Then, by reusing the same argument, we prove the remaining part of the lemma.

Step 1: Fix the tuple. Let L be shorthand for $L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}$. Recall Definitions 4.9 and 4.10. We first show that G_{L,k_2}^{ℓ} is decomposable. The first and second conditions together imply that each vertex in G_{L,k_2}^{ℓ} has a distinct label. Next, note that from the definition of augmented relation $L_2^{(k_2,\vec{z}_L)}$ (see Definition 4.11), there are at least $|L_2|$ edges in G_{L,k_2}^{ℓ}. Together with the third condition, they imply that these $|L_2|$ edges form a perfect matching of vertices in $L_2^{(k_2,\vec{z}_L)}$. Thus, G^ℓ_{L,k_2} is decomposable. In particular, we have

$$\begin{aligned} V_{\mathsf{isolate}}(G^\ell_{L,k_2}) &= L_1^{(k_1,k_3)} \\ V_{\mathsf{source}}(G^\ell_{L,k_2}) &= \{(x,y) \in L_2^{(k_2,\vec{z}_L)} : y \in \{z_{L,1},\dots,z_{L,|L_2|}\}\} \\ V_{\mathsf{target}}(G^\ell_{L,k_2}) &= L_2^{(k_2,\vec{z}_L)} \setminus V_{\mathsf{source}}(G^\ell_{L,k_2}) \end{aligned} \tag{17}$$

By symmetry, we can show that G^r_{R,k_2} is also decomposable, so the input will pass Step 1 of Dec in Definition 4.13. Next, the first condition ensures the image of $V_{\mathsf{target}}(G^\ell_{L,k_2})$ is $\mathcal{I}$-distinct and $V_{\mathsf{target}}(G^r_{L,k_2})$ is $\mathcal{D}$-distinct, so the input will pass Step 2. By inspection, after Step 4, we obtain $L_{\mathsf{isolate}} = L_1, R_{\mathsf{isolate}} = R_1, L_{\mathsf{pair}} = L_2, R_{\mathsf{pair}} = R_2, \vec{m}_L = \vec{z}_L, \vec{m}_L = \vec{z}_R$. Finally, the first condition ensures that the input passes Steps 5 and 6. This shows that the tuple is decodable and Equation (13).

Step 2: In the view of relation-key induced graphs, deleting $v = (x,y)$ from L is equivalently as deleting v from $G^\ell_{k_2,L}$, together with all edges incident to v, that is, all edges either entering or leaving v. We denote this resulting graph by $G^\ell_{k_2,L} - v$. Suppose $v \in V_{\mathsf{isolate}}(G^\ell_{L,k_2})$ and L_1 satisfies $L_1 = L_1' \cup \{(x \oplus k_1, y \oplus k_3)\}$ for some L_1'. From Equation (17), it is not hard to verify that

$$\begin{aligned} V_{\mathsf{isolate}}(G^\ell_{L,k_2} - v) &= (L_1')^{(k_1,k_3)} \\ V_{\mathsf{source}}(G^\ell_{L,k_2} - v) &= \{(x,y) \in L_2^{(k_2,\vec{z}_L)} : y \in \{z_{L,1},\dots,z_{L,|L_2|}\}\} \\ V_{\mathsf{target}}(G^\ell_{L,k_2} - v) &= L_2^{(k_2,\vec{z}_L)} \setminus V_{\mathsf{source}}(G^\ell_{L,k_2}) \end{aligned}$$

and they pass Steps 5 and 6 of Dec. Thus, we proved Equation (14).

When $v \in V_{\mathsf{source}}(G^\ell_{L,k_2})$. Suppose $L_2 = \{(x_i,y_i)\}_{i\in[|L_2|]}$ and $L_2^{(k_2,\vec{z}_L)} = \{(x_i,z_i),(z_i \oplus k_2, y_i)\}_{i\in[|L_2|]}$. In the former case, $(x,y) = (x_{i^*}, z_{i^*})$ for some $i^* \in [|L_2|]$. As a result, the vertex $(z_{i^*} \oplus k_2, y_{i^*})$ in the graph $G^\ell_{L,k_2} - v$ becomes "unpaired". We may view $(z_{i^*} \oplus k_2, y_{i^*})$ being assigned to the isolated vertices. Namely,

$$\begin{aligned} V_{\mathsf{isolate}}(G^\ell_{L,k_2} - v) &= (L_1 \cup \{(z_{i^*} \oplus k_2 \oplus k_1, y_{i^*} \oplus k_3)\})^{(k_1,k_3)} \\ V_{\mathsf{source}}(G^\ell_{L,k_2} - v) &= \{(x_i,z_i)\}_{i\neq i^*} \\ V_{\mathsf{target}}(G^\ell_{L,k_2} - v) &= \{(z_i \oplus k_2, y_i)\}_{i\neq i^*} \end{aligned}$$

At first sight, the resulting graph remains decomposable. However, a caveat is that the newly added element $(z_{i^*} \oplus k_2 \oplus k_1,\ y_{i^*} \oplus k_3)$ may coincide with an element of L_1, which would cause Step 5 of the decoder Dec (Definition 4.13) to fail. Fortunately, Item 2 prevent this event from happening. This proves Equation (15).

Finally, if $v \in V_{\mathsf{target}}(G^\ell_{L,k_2})$, we have $(x,y) = (z_{i^*} \oplus k_2, y_{i^*})$ for some $i^* \in [|L_2|]$ and

$$\begin{aligned} V_{\mathsf{isolate}}(G^\ell_{L,k_2} - v) &= (L_1 \cup \{(x_{i^*} \oplus k_1, z_{i^*} \oplus k_3)\})^{(k_1,k_3)} \\ V_{\mathsf{source}}(G^\ell_{L,k_2} - v) &= \{(x_i,z_i)\}_{i\neq i^*} \\ V_{\mathsf{target}}(G^\ell_{L,k_2} - v) &= \{(z_i \oplus k_2, y_i)\}_{i\neq i^*}. \end{aligned}$$

Similarly, Item 2 prevent this event from happening. This proves Equation (16). □

4.5 Good Tuples and Their Combinatorial Properties

In the following, we define good tuples.

Definition 4.19 (Good tuples)**.** *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, let $\mathsf{G}\binom{L_1,L_2}{R_1,R_2}$ denote the set of 5-tuples $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \in [N] \times [N] \times [N] \times [N]^{|L_2|} \times [N]^{|R_2|}$ satisfying all the following conditions:*[15]

1. $k_1 \notin \Big(\mathrm{Dom}(L_1) \oplus \mathrm{Dom}(L_2)\Big) \cup \Big(\mathrm{Dom}(R_1) \oplus \mathrm{Dom}(R_2)\Big)$
2. $k_2 \notin \Bigg(\bigg(\Big(\mathrm{Dom}(L_1) \oplus k_1\Big) \cup \mathrm{Dom}(L_2)\bigg) \oplus \bigg(\Big(\mathrm{Im}(L_1) \oplus k_3\Big) \cup \mathrm{Im}(L_2)\bigg)\Bigg)$
   $\cup \Bigg(\bigg(\Big(\mathrm{Dom}(R_1) \oplus k_1\Big) \cup \mathrm{Dom}(R_2)\bigg) \oplus \bigg(\Big(\mathrm{Im}(R_1) \oplus k_3\Big) \cup \mathrm{Im}(R_2)\bigg)\Bigg)$
3. $k_3 \notin \Big(\mathrm{Im}(L_1) \oplus \mathrm{Im}(L_2)\Big) \cup \Big(\mathrm{Im}(R_1) \oplus \mathrm{Im}(R_2)\Big)$
4. $\vec{z}_L \in [N]^{|L_2|}_{\mathrm{dist}}$ *and* $\vec{z}_R \in [N]^{|R_2|}_{\mathrm{dist}}$
5. $\{\vec{z}_L\}$ *and* $\Big(\mathrm{Im}(L_1) \oplus k_3\Big) \cup \mathrm{Im}(L_2) \cup \Bigg(\bigg(\Big(\mathrm{Dom}(L_1) \oplus k_1\Big) \cup \mathrm{Dom}(L_2)\bigg) \oplus k_2\Bigg)$ *are disjoint.*
6. $\{\vec{z}_R\}$ *and* $\Big(\mathrm{Im}(R_1) \oplus k_3\Big) \cup \mathrm{Im}(R_2) \cup \Bigg(\bigg(\Big(\mathrm{Dom}(R_1) \oplus k_1\Big) \cup \mathrm{Dom}(R_2)\bigg) \oplus k_2\Bigg)$ *are disjoint.*

Lemma 4.20. *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, every tuple in $\mathsf{G}\binom{L_1,L_2}{R_1,R_2}$ satisfies all conditions in Lemma 4.18 and is therefore robustly decodable.*

The proof proceeds by a direct verification of all conditions and is given in Appendix B.

Remark 4.21. *Indeed, one could have alternative definitions for good tuples. In particular, we only require them to be robustly decodable and satisfy all properties introduced in the following.*

Enumerating good tuples. Here we describe how to enumerate tuples from $\mathsf{G}\binom{L_1,L_2}{R_1,R_2}$. First, for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$ and $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, we define the sets $\mathcal{B}_1(L_1, L_2, R_1, R_2)$ and $\mathcal{B}_3(L_1, L_2, R_1, R_2)$, which can be viewed as "bad k_1 and k_3":

$$\mathcal{B}_1(L_1, L_2, R_1, R_2) := \big(\mathrm{Dom}(L_1) \oplus \mathrm{Dom}(L_2)\big) \cup \big(\mathrm{Dom}(R_1) \oplus \mathrm{Dom}(R_2)\big),$$
$$\mathcal{B}_3(L_1, L_2, R_1, R_2) := \big(\mathrm{Im}(L_1) \oplus \mathrm{Im}(L_2)\big) \cup \big(\mathrm{Im}(R_1) \oplus \mathrm{Im}(R_2)\big).$$

Next, for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, and "good (k_1, k_3)" pair, namely, $k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2)$ and $k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$, define the set $\mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$ consisting of "bad k_2":

$$\mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3) := \Bigg(\bigg(\Big(\mathrm{Dom}(L_1) \oplus k_1\Big) \cup \mathrm{Dom}(L_2)\bigg) \oplus \bigg(\Big(\mathrm{Im}(L_1) \oplus k_3\Big) \cup \mathrm{Im}(L_2)\bigg)\Bigg)$$

[15] Recall that for a set $A \subseteq \{0,1\}^n$ and a string $x \in \{0,1\}^n$, we denote $A \oplus x := \{a \oplus x : a \in A\}$.

$$\cup \left(\left(\left(\mathrm{Dom}(R_1) \oplus k_1\right) \cup \mathrm{Dom}(R_2)\right) \oplus \left(\left(\mathrm{Im}(R_1) \oplus k_3\right) \cup \mathrm{Im}(R_2)\right)\right).$$

Finally, for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ and "good (k_1, k_2, k_3)" such that $k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2)$, $k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$, and $k_2 \notin \mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$, define the sets consisting of "bad $\vec{z}_L$ and $\vec{z}_R$" as

$$\mathcal{B}_L \begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix} := \Bigg\{ \vec{z}_L \in [N]^{|L_2|} : \vec{z}_L \notin [N]^{|L_2|}_{\text{dist}}$$

$$\vee\ \exists i \in [|L_2|] \text{ s.t. } z_{L,i} \in \left(\mathrm{Im}(L_1) \oplus k_3\right) \cup \mathrm{Im}(L_2) \cup \left(\left(\left(\mathrm{Dom}(L_1) \oplus k_1\right) \cup \mathrm{Dom}(L_2)\right) \oplus k_2\right)\Bigg\},$$

$$\mathcal{B}_R \begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix} := \Bigg\{ \vec{z}_R \in [N]^{|R_2|} : \vec{z}_R \notin [N]^{|R_2|}_{\text{dist}}$$

$$\vee\ \exists i \in [|R_2|] \text{ s.t. } z_{R,i} \in \left(\mathrm{Im}(R_1) \oplus k_3\right) \cup \mathrm{Im}(R_2) \cup \left(\left(\left(\mathrm{Dom}(R_1) \oplus k_1\right) \cup \mathrm{Dom}(R_2)\right) \oplus k_2\right)\Bigg\}.$$

Therefore, one can enumerate elements in $\mathsf{G}\binom{L_1, L_2}{R_1, R_2}$ by first choosing (k_1, k_3), then k_2 second, and finally $(\vec{z}_L, \vec{z}_R)$, ensuring that each choice avoids being bad. In addition, if all L_1, L_2, R_1, R_2 are all of polynomial size, then most choices of $k_1, k_2, k_3, \vec{z}_L$ and $\vec{z}_R$ are good. This is simply because the number of good keys they can eliminate is at most quadratic in the size of the relations.

Lemma 4.22. *For any integer $t \geq 0$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, the following holds.*

1. *$\mathcal{B}_1(L_1, L_2, R_1, R_2)$ and $\mathcal{B}_3(L_1, L_2, R_1, R_2)$ each occupy at most a $2t^2/N$ fraction of the universe $[N]$.*
2. *For any $k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2)$ and $k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$, the set $\mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$ occupies at most a $8t^2/N$ fraction of the universe $[N]$.*
3. *For any $k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2)$, $k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$, and $k_2 \notin \mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$, the sets $\mathcal{B}_L\begin{pmatrix} L_1, L_2 \\ R_1, R_2 \\ k_1, k_2, k_3 \end{pmatrix}$ and $\mathcal{B}_R\begin{pmatrix} L_1, L_2 \\ R_1, R_2 \\ k_1, k_2, k_3 \end{pmatrix}$ each occupy at most a $5t^2/N$ fraction of their respective universes, $[N]^{|L_2|}$ and $[N]^{|R_2|}$.*

As a corollary, all but a $22t^2/N$ fraction of the elements in $[N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$ are good tuples.

Proof. Notice that for any sets A, B, the size of the set $A \oplus B$ is at most $|A| \cdot |B|$. Thus, Item 1 follows. Items 2 and 3 can be proved in a similar manner. □

Good tuples satisfy the following property.

Lemma 4.23 (Monotonicity)**.** *For any $x \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, the following holds:*

1. *There do not exist $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \notin \mathsf{G}\binom{L_1, L_2}{R_1, R_2}$ and $y \notin \mathrm{Im}(L_1)$ such that $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \in \mathsf{G}\binom{L_1 \cup \{(x,y)\}, L_2}{R_1, R_2}$.*

2. *There do not exist* $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \notin \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$, $z \in [N]$, *and* $y \notin \mathrm{Im}(L_2)$ *such that* $(k_1, k_2, k_3, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$, *where i is the index such that y is the i-th largest element in* $\mathrm{Im}(L_2) \cup \{y\}$ *and* $\vec{z}_L^{(i\leftarrow z)}$ *denotes the vector obtained by inserting z into the i-th coordinate of* $\vec{z}_L$ *and shifting all subsequent coordinates one position to the right.*

As a corollary, for any $x \in [N], L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ *and* $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \notin \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$, *the following holds:*

1. *For every* $y \notin \mathrm{Im}(L_1)$, $\mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2} \subseteq \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$.

2. *For every* $y \notin \mathrm{Im}(L_2)$, $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$, *it holds that* $(k_1, k_2, k_3, \vec{z}_{L,-i}, \vec{z}_R) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$, *where i is the index such that y is the i-th largest element in* $\mathrm{Im}(L_2) \cup \{y\}$ *and* $\vec{z}_{L,-i}$ *denotes the vector obtained by deleting its i-th coordinate and shifting all subsequent coordinates one position to the left.*

Proof. Since $(k_1, k_2, k_3, \vec{z}_L, \vec{z}_R) \notin \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$, some condition in Definition 4.19 must be violated. To prove Item 1, simply note that the same condition remains violated after adding (x, y) to L_1. To prove Item 2, observe that the conditions in Definition 4.19 are insensitive to the ordering of $\vec{z}_L$ and $\vec{z}_R$. Thus, although inserting z into $\vec{z}_L$ changes its size and ordering, the same condition remains violated. □

The following lemmas will be used in Section 6.

Lemma 4.24. *For any* $t \geq 0, x \in [N], L_1, L_2 \in \mathcal{R}_{\leq t}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}_{\leq t}^{\mathcal{D}\text{-dist}}$, *there are at most a* $t(22t + 4)/N$ *fraction of the elements* $(\mathbf{k}, \mathbf{z}) \in [N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$ *for which no* $y \notin \mathrm{Im}(L_1)$ *satisfies* $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2}$.

Proof. Let us sample $(\mathbf{k}, \mathbf{z})$ uniformly at random from $[N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$. Define the following events

- Good: $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$
- K_1: $k_1 \in x \oplus \mathrm{Dom}(L_2)$
- K_2: $k_2 \in x \oplus k_1 \oplus \Big(\big(\mathrm{Im}(L_1) \oplus k_3 \big) \cup \mathrm{Im}(L_2) \Big)$
- Z_L: $\{\vec{z}_L\} \cap \{x \oplus k_1 \oplus k_2\} \neq \varnothing$

Suppose Good occurs, and consider the items in Definition 4.19. For there to be no y such that $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2}$, one of the conditions imposed by the addition of x to $\mathrm{Dom}(L_1)$ must be violated. These correspond to the events K_1, K_2, and Z_L. Otherwise, there always exists some y such that $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2}$. Therefore, by the union bound, the fraction of such $(\mathbf{k}, \mathbf{z})$ is at most

$$\Pr[\neg\mathsf{Good}] + \Pr[\mathsf{K}_1] + \Pr[\mathsf{K}_2] + \Pr[\mathsf{Z}_L] \leq \frac{22t^2}{N} + \frac{t}{N} + \frac{2t}{N} + \frac{t}{N} = \frac{t(22t+4)}{N},$$

where $\Pr[\mathsf{K}_1]$, $\Pr[\mathsf{K}_2]$, and $\Pr[\mathsf{Z}_L]$ are bounded by sampling k_1, k_2, and $\vec{z}_L$, respectively, at the end. □

Lemma 4.25. *For any $t \geq 0, x \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, $\mathbf{k} \in [N]^3$, $\mathbf{z} \in [N]^{|L_2|} \times [N]^{|R_2|}$, if there exists $y \notin \mathrm{Im}(L_1)$ such that $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1 \cup \{(x,y)\}, L_2}{R_1, R_2}$, then there are at most $4t$ values of $y \notin \mathrm{Im}(L_1)$ such that $(\mathbf{k}, \mathbf{z}) \notin \mathsf{G}\binom{L_1 \cup \{(x,y)\}, L_2}{R_1, R_2}$.*

Proof. Suppose there exists some $y \notin \mathrm{Im}(L_1)$ such that $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1 \cup \{(x,y)\}, L_2}{R_1, R_2}$. According to the definition of good tuples, $(\mathbf{k}, \mathbf{z})$ satisfies all conditions in Definition 4.19. Now, suppose we attempt to vary y in such a way that $(\mathbf{k}, \mathbf{z})$ violates one of the conditions. Since we are only modifying $\mathrm{Im}(L_1 \cup \{(x, y)\})$, Items 1, 4, and 6 continue to hold. We now examine Item 2. If we replace y with a different value y', the additional imposed constraint is

$$k_2 \notin \Big(\big(\mathrm{Dom}(L_1) \oplus k_1\big) \cup \mathrm{Dom}(L_2) \Big) \oplus y' \oplus k_3.$$

Thus, in order for this condition to be violated, we must have

$$y' \in \Big(\big(\mathrm{Dom}(L_1) \oplus k_1\big) \cup \mathrm{Dom}(L_2) \Big) \oplus k_2 \oplus k_3,$$

and there are at most $2t$ such values of y'. Similarly, there are at most t values of y' that violate Item 3 and at most t values of y' that violate Item 5. Hence, the total number of such y' is bounded by $4t$. □

Lemma 4.26. *For any $t \geq 0, x \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, define the following two sets:*

$$\Psi_{\ \ L_1,R_1,L_2,R_2} := \{(y, \mathbf{k}, \mathbf{z}) \colon (\mathbf{k}, \mathbf{z}) \in \mathsf{G}\left(\begin{smallmatrix} L_1, L_2, \\ R_1, R_2 \end{smallmatrix}\right), y \notin \mathrm{Im}(L_1) \cup \left(\mathrm{Im}(L_2^{(k_2, \vec{z}_L)}) \oplus k_3\right)\}$$

$$\Phi_{x,L_1,R_1,L_2,R_2} := \{(y, \mathbf{k}, \mathbf{z}) \colon y \notin \mathrm{Im}(L_1), (\mathbf{k}, \mathbf{z}) \in \mathsf{G}\left(\begin{smallmatrix} L_1 \cup \{(x,y)\}, L_2, \\ R_1, R_2 \end{smallmatrix}\right)\}.$$

Then $\Psi_{\ \ L_1,R_1,L_2,R_2} \supseteq \Phi_{x,L_1,R_1,L_2,R_2}$ and the size of their difference is at most $t(22t + 8)N^{|L_2|+|R_2|+3}$.

Proof. Consider elements in Φ_{x,L_1,R_1,L_2,R_2}. First, from Lemma 4.20 and Items 1 and 2 in Lemma 4.18, we have

$$(L_1 \cup \{(x, y)\})^{(k_1,k_3)} \in \mathcal{R}^{\mathcal{I}\text{-dist}} \quad \text{and} \quad \mathrm{Im}\left((L_1 \cup \{(x, y)\})^{(k_1,k_3)}\right) \cap \mathrm{Im}(L_2^{(k_2,\vec{z}_L)}) = \varnothing,$$

which implies $y \notin \mathrm{Im}(L_1) \cup \left(\mathrm{Im}(L_2^{(k_2,\vec{z}_L)}) \oplus k_3\right)$. Then by monotonicity (Item 1 in Lemma 4.23), we have

$$\mathsf{G}\left(\begin{smallmatrix} L_1 \cup \{(x,y)\}, L_2, \\ R_1, R_2 \end{smallmatrix}\right) \subseteq \mathsf{G}\left(\begin{smallmatrix} L_1, L_2, \\ R_1, R_2 \end{smallmatrix}\right).$$

This proves $\Psi_{\ \ L_1,R_1,L_2,R_2} \supseteq \Phi_{x,L_1,R_1,L_2,R_2}$.

Next, we bound the size of their difference. We denote by BAD the set of $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1, L_2}{R_1, R_2}$ for which no $y \notin \mathrm{Im}(L_1)$ satisfies $(\mathbf{k}, \mathbf{z}) \in \mathsf{G}\binom{L_1 \cup \{(x,y)\}, L_2}{R_1, R_2}$. By Lemma 4.24, we have

$$|\mathsf{BAD}| \leq t(22t + 4)N^{|L_2|+|R_2|+2}.$$

Now, if we enumerate $(y, \mathbf{k}, \mathbf{z})$ in $\Psi_{\ \ L_1,R_1,L_2,R_2}$, then one of the following holds:

1. If $(\mathbf{k},\mathbf{z}) \in \mathsf{BAD}$, then every $y \notin \mathrm{Im}(L_1)$ satisfies $(\mathbf{k},\mathbf{z}) \notin \mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2}$, which in turn implies $(y,\mathbf{k},\mathbf{z}) \notin \Phi_{x,L_1,R_1,L_2,R_2}$.
2. If $(\mathbf{k},\mathbf{z}) \notin \mathsf{BAD}$, then by Lemma 4.25 there are at most $4t$ values of $y \notin \mathrm{Im}(L_1)$ such that $(\mathbf{k},\mathbf{z}) \notin \mathsf{G}\binom{L_1\cup\{(x,y)\},L_2}{R_1,R_2}$. All other y satisfy $(y,\mathbf{k},\mathbf{z}) \in \Phi_{x,L_1,R_1,L_2,R_2}$.

Therefore, the size of their difference is at most

$$|\mathsf{BAD}| \cdot N + N^{|L_2|+|R_2|+3} \cdot 4t \leq t(22t+8)N^{|L_2|+|R_2|+3}. \qquad \square$$

The following lemmas will be used in Section 7.

Lemma 4.27. *For any $t \geq 0, x \in [N], L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, there are at most a $(22t^2 + 10t+1)/N$ fraction of elements $(z,\mathbf{k},\vec{z}_L,\vec{z}_R) \in [N] \times [N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$ for which no $y \notin \mathrm{Im}(L_2)$ satisfies $(\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$ where i is the index such that $y \in_i \mathrm{Im}(L_2)\cup\{y\}$.*

Proof. Let us sample $(z,\mathbf{k},\vec{z}_L,\vec{z}_R)$ uniformly at random from $[N] \times [N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$. Define the following events

- Good: $(\mathbf{k},\vec{z}_L,\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$
- K_1: $k_1 \in \mathrm{Dom}(L_1) \oplus x$
- K_2: $k_2 \in x \oplus \Big(\big(\mathrm{Im}(L_1)\oplus k_3\big) \cup \mathrm{Im}(L_2)\Big)$
- Z_L: $z \in \{\vec{z}_L\}$ **or** $x \oplus k_2 \in \{\vec{z}_L\}$ **or** $x \in \{\vec{z}_L\}$
- Z: $z \in \big(\mathrm{Im}(L_1)\oplus k_3\big) \cup \mathrm{Im}(L_2) \cup \Big(\Big(\big(\mathrm{Dom}(L_1)\oplus k_1\big) \cup \mathrm{Dom}(L_2)\Big) \oplus k_2\Big)$ **or** $z = x$

Suppose Good occurs, and consider the items in Definition 4.19. For there to be no y such that $(\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$, one of the conditions imposed by the addition of (i) x to $\mathrm{Dom}(L_1)$ or (ii) z to $\vec{z}_L$ must be violated. These correspond to the events K_1, K_2, Z_L, and Z. Otherwise, there always exists some y such that $(\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$. Therefore, by the union bound, the fraction of such $(z,\mathbf{k},\vec{z}_L,\vec{z}_R)$ is at most

$$\Pr[\neg\mathsf{Good}] + \Pr[\mathsf{K}_1] + \Pr[\mathsf{K}_2] + \Pr[\mathsf{Z}_L] + \Pr[\mathsf{Z}] \leq \frac{22t^2}{N} + \frac{t}{N} + \frac{2t}{N} + \frac{3t}{N} + \frac{4t+1}{N} = \frac{22t^2+10t+1}{N},$$

where $\Pr[\mathsf{K}_1]$, $\Pr[\mathsf{K}_2]$, $\Pr[\mathsf{Z}_L]$, and $\Pr[\mathsf{Z}]$ are bounded by sampling k_1, k_2, $\vec{z}_L$, and z, respectively, at the end. □

Lemma 4.28. *For any $t \geq 0, x \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, $\mathbf{k} \in [N]^3$, $\vec{z}_L \in [N]^{|L_2|-1}$, $z \in [N]$ and $\vec{z}_R \in [N]^{|R_2|}$, if there exists $y \notin \mathrm{Im}(L_2)$ such that $(\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$ where i is the index such that $y \in_i \mathrm{Im}(L_2)\cup\{y\}$, then there are at most $4t+1$ values of $y \notin \mathrm{Im}(L_2)$ such that $(\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R) \notin \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$ where i is the index such that $y \in_i \mathrm{Im}(L_2)\cup\{y\}$.*

Proof. Suppose there exists some $y \notin \mathrm{Im}(L_2)$ such that $(\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R) \in \mathsf{G}\binom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$. According to the definition of good tuples, $(\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R)$ satisfies all conditions in Definition 4.19. Now, suppose we attempt to vary y in such a way that $(\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R)$ violates one of the conditions. Notice that the index i might vary with the value of y because it is defined to be the index such that $y \in_i \mathrm{Im}(L_2) \cup \{y\}$. Since we are only modifying $\mathrm{Im}(L_2 \cup \{(x,y)\})$, and the conditions in Definition 4.19 depend only on the set $\{\vec{z}_L^{(i\leftarrow z)}\}$ rather than on the ordering of $\vec{z}_L^{(i\leftarrow z)}$, Items 1, 4, and 6 continue to hold. We can apply the same argument as in the proof of Lemma 4.25 to show that the total number of such y' is $4t+1$. This completes the proof. □

Lemma 4.29. *For any $x \in [N]$, $L_1, L_2 \in \mathcal{R}_{\le t}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}_{\le t}^{\mathcal{D}\text{-dist}}$, define the following two sets:*

$$\Psi_{\ L_1,R_1,L_2,R_2} := \{(y,z,\mathbf{k},\mathbf{z})\colon (\mathbf{k},\mathbf{z}) \in \mathsf{G}\tbinom{L_1,L_2}{R_1,R_2}, z, y \notin \mathrm{Im}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}), y \neq z'\}$$

$$\Phi_{x,L_1,R_1,L_2,R_2} := \{(y,z,\mathbf{k},\mathbf{z})\colon y \notin \mathrm{Im}(L_2), i \text{ s.t. } y \in_i \mathrm{Im}(L_2) \cup \{y\}, (\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R) \in \mathsf{G}\tbinom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}\}.$$

Then $\Psi_{\ L_1,R_1,L_2,R_2} \supseteq \Phi_{x,L_1,R_1,L_2,R_2}$ and the size of their difference is at most $(22t^2+14t+2)N^{|L_2|+|R_2|+4}$.

Proof. Consider elements in Φ_{x,L_1,R_1,L_2,R_2}. First, from Lemma 4.20 and Items 1 and 2 in Lemma 4.18, we have

$$(L_2 \cup \{(x,y)\})^{(k_2,\vec{z}_L^{(i\leftarrow z)})} \in \mathcal{R}^{\mathcal{I}\text{-dist}} \quad \text{and} \quad \mathrm{Im}(L_1^{(k_1,k_3)}) \cap \mathrm{Im}\left((L_2 \cup \{(x,y)\})^{(k_2,\vec{z}_L^{(i\leftarrow z)})}\right) = \varnothing,$$

which implies $z, y \notin \mathrm{Im}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}) \wedge y \neq z'$. Then by monotonicity (Item 2 in Lemma 4.23), we have

$$(\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R) \in \mathsf{G}\tbinom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2} \implies (\mathbf{k}, \vec{z}_L, \vec{z}_R) \in \mathsf{G}\tbinom{L_1,L_2}{R_1,R_2}.$$

This proves $\Psi_{\ L_1,R_1,L_2,R_2} \supseteq \Phi_{x,L_1,R_1,L_2,R_2}$.

Next, we bound the size of their difference. We denote by BAD the set of $(z,\mathbf{k},\mathbf{z}) \in [N] \times \mathsf{G}\tbinom{L_1,L_2}{R_1,R_2}$ for which no $y \notin \mathrm{Im}(L_2)$ satisfies $(\mathbf{k}, \vec{z}_L^{(i\leftarrow z)}, \vec{z}_R) \in \mathsf{G}\tbinom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$. By Lemma 4.27, we have

$$|\mathsf{BAD}| = (22t^2+10t+1)N^{|L_2|+|R_2|+3}.$$

Now, if we enumerate $(y,z,\mathbf{k},\mathbf{z})$ in $\Psi_{\ L_1,R_1,L_2,R_2}$, then one of the following holds:

1. If $(z,\mathbf{k},\mathbf{z}) \in \mathsf{BAD}$, then every $y \notin \mathrm{Im}(L_2)$ satisfies $(\mathbf{k},\mathbf{z}) \notin \mathsf{G}\tbinom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$, which in turn implies $(y,\mathbf{k},\mathbf{z}) \notin \Phi_{x,L_1,R_1,L_2,R_2}$.
2. If $(z,\mathbf{k},\mathbf{z}) \notin \mathsf{BAD}$, then by Lemma 4.28 there are at most $4t+1$ values of $y \notin \mathrm{Im}(L_2)$ for which $(\mathbf{k},\mathbf{z}) \notin \mathsf{G}\tbinom{L_1,L_2\cup\{(x,y)\}}{R_1,R_2}$. All other y satisfy $(y,\mathbf{k},\mathbf{z}) \in \Phi_{x,L_1,R_1,L_2,R_2}$.

Therefore, the size of their difference is at most

$$|\mathsf{BAD}| \cdot N + N^{|L_2|+|R_2|+4} \cdot (4t+1) \le (22t^2+14t+2)N^{|L_2|+|R_2|+4}.$$ □

4.6 Defining the Approximate Isometry $\mathcal{S}$

Before defining $\mathcal{S}$, which intuitively maps a view in hybrid $\mathbf{H}_3$ to a uniform superposition of consistent views in hybrid $\mathbf{H}_4$, we first define the following operators, which mimic each step of enumerating good tuples in the previous subsection.

Definition 4.30 (Operator $\mathcal{S}_{k_1,k_3}$)**.** *Define the operator $\mathcal{S}_{k_1,k_3}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$,*

$$\mathcal{S}_{k_1,k_3} \colon |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2} \mapsto \frac{1}{\sqrt{N^2}} \sum_{\substack{k_1 \notin \mathcal{B}_1(L_1,L_2,R_1,R_2) \\ k_3 \notin \mathcal{B}_3(L_1,L_2,R_1,R_2)}} |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_3\rangle_{\mathsf{K}_3}. \tag{18}$$

Otherwise, $\mathcal{S}_{k_1,k_3}$ maps all the other basis vectors to the zero vector.

Definition 4.31 (Operator $\mathcal{S}_{k_2}$)**.** *Define the operator $\mathcal{S}_{k_2}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}, k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2), k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$,*

$$\begin{aligned}\mathcal{S}_{k_2} \colon & |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_3\rangle_{\mathsf{K}_3} \mapsto \\ & \frac{1}{\sqrt{N}} \sum_{k_2 \notin \mathcal{B}_2(L_1,L_2,R_1,R_2,k_1,k_3)} |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}.\end{aligned} \tag{19}$$

Otherwise, $\mathcal{S}_{k_2}$ maps all the other basis vectors to the zero vector.

Definition 4.32 (Operator $\mathcal{S}_{\vec{z}}$)**.** *Define the operator $\mathcal{S}_{\vec{z}}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}, k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2), k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2), k_2 \notin \mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$,*

$$\begin{aligned}\mathcal{S}_{\vec{z}} \colon & |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3} \mapsto \\ & \frac{1}{\sqrt{N^{|L_2|+|R_2|}}} \sum_{\vec{z}_L \notin \mathcal{B}_L\begin{pmatrix}L_1,L_2,\\R_1,R_2,\\k_1,k_2,k_3\end{pmatrix}, \vec{z}_R \notin \mathcal{B}_R\begin{pmatrix}L_1,L_2,\\R_1,R_2,\\k_1,k_2,k_3\end{pmatrix}} |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\vec{z}_L\rangle_{\mathsf{Z}_\mathsf{L}}|\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}.\end{aligned} \tag{20}$$

Otherwise, $\mathcal{S}_{\vec{z}}$ maps all the other basis vectors to the zero vector.

Now, we define the operator $\mathcal{S}$.

Definition 4.33 (Operator $\mathcal{S}$)**.** *Define the operator*

$$\mathcal{S} := \mathcal{D}^\dagger \cdot \mathcal{S}_{\vec{z}} \cdot \mathcal{S}_{k_2} \cdot \mathcal{S}_{k_1,k_3}. \tag{21}$$

Note that $\mathcal{S}_{k_1,k_3}, \mathcal{S}_{k_2}, \mathcal{S}_{\vec{z}}$ are contractions, that is, their operator norms are all bounded 1. Thus, $\mathcal{S}$ is *not* a partial isometry. Importantly, the action of $\mathcal{S}$ satisfies the following.

Lemma 4.34. *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$,*

$$\begin{aligned}\mathcal{S} \colon & |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2} \mapsto \\ & \frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}} \sum_{(k_1,k_2,k_3,\vec{z}_L,\vec{z}_R) \in \mathsf{G}\begin{pmatrix}L_1,L_2\\R_1,R_2\end{pmatrix}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}.\end{aligned}$$

Proof. Recall Definitions 4.30 to 4.32, we have

$$|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2} \xmapsto{\mathcal{S}_{\vec{z}}\cdot\mathcal{S}_{k_2}\cdot\mathcal{S}_{k_1,k_3}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}}\sum_{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\vec{z}_L\rangle_{\mathsf{Z}_\mathsf{L}}|\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}.$$

From Lemma 4.20, every $(\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2}$ is decodable with respect to (L_1,R_1,L_2,R_2). Thus, $(L_1,R_1,L_2,R_2,\mathbf{k},\mathbf{z})$ is in Supp(Dec). Therefore, applying $\mathcal{D}^\dagger$ is equivalently to applying Enc, which the inverse of Dec defined in the proof of Lemma 4.14. This completes the proof. □

The following lemma will be used in Sections 6 and 7.

Lemma 4.35. *Let $\{\mathcal{P}_\tau\}_\tau$ be a collection of sets where the index τ ranges over $(y\in[N], L_1\in\mathcal{R}^{\mathcal{I}\text{-dist}}, R_1\in\mathcal{R}^{\mathcal{D}\text{-dist}}, L_2\in\mathcal{R}^{\mathcal{I}\text{-dist}}, R_2\in\mathcal{R}^{\mathcal{D}\text{-dist}})$ and $\mathcal{P}_\tau\subseteq[N]^3\times[N]^{|L_2|}\times[N]^{|R_2|}$. Define the operator*

$$\begin{aligned}\mathcal{S}^\bullet\colon\ & |y\rangle_\mathsf{A}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}\\ &\mapsto |y\rangle_\mathsf{A}\frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}}\sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2}:\\(\mathbf{k},\mathbf{z})\notin\mathcal{P}_{y,L_1,R_1,L_2,R_2}}}|L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\rangle_\mathsf{S}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_\mathsf{T}|k\rangle_\mathsf{K}.\end{aligned}$$

If there exists $\delta\geq 0$ such that for any τ,

$$\frac{\left|\mathcal{P}_{y,L_1,R_1,L_2,R_2}\cap\mathsf{G}\binom{L_1,L_2}{R_1,R_2}\right|}{N^{|L_2|+|R_2|+3}}\leq\delta,$$

then

$$\|\mathcal{S}^\bullet-\mathcal{S}\|_{\mathrm{op}}=\sqrt{\delta}.$$

Namely, $\mathcal{S}^\bullet$ is further controlled by the register A and imposes extra conditions ensuring that good tuples $(\mathbf{k},\mathbf{z})$ do not lie in some "bad set" $\mathcal{P}_\tau$. We provide the proof in Appendix A.2.

4.7 Main Lemmas

We introduce important lemmas regarding $\mathcal{S}$ below. Their proofs are deferred to further subsections. We will first use these lemmas to prove Lemma 4.8 in Section 4.8.

Lemma 4.36 ($\mathcal{S}$ is Close to a Partial Isometry)**.** *There exists a partial isometry $\widetilde{\mathcal{S}}$ such that for any integer $t\geq 0$,*

$$\|(\widetilde{\mathcal{S}}-\mathcal{S})\Pi_{\leq t}\|_{\mathrm{op}}\leq O(\sqrt{t^2/N}).$$

We provide the proof of above lemma in Section 5.

Lemma 4.37 (Closeness of the First Oracle)**.** *For any integer $t\geq 0$,*

- **Forward query:** $\|(X^{k_3}FX^{k_1}\mathcal{S}-\mathcal{S}F_1)\Pi_{\leq t}\|_{\mathrm{op}}\leq O(\sqrt{t/N})$,

- **Inverse query:** $\|(X^{k_1}F^\dagger X^{k_3}\mathcal{S} - \mathcal{S}F_1^\dagger)\Pi_{\leq t}\|_{\mathrm{op}} \leq O(\sqrt{t/N})$.

We provide the proof of above lemma in Section 6.

Lemma 4.38 (Closeness of the Second Oracle)**.** *For any integer $t \geq 0$,*

- **Forward query:** $\|(FX^{k_2}F\mathcal{S} - \mathcal{S}F_2)\Pi_{\leq t}\|_{\mathrm{op}} \leq O(t/\sqrt{N})$,
- **Inverse query:** $\|(F^\dagger X^{k_2}F^\dagger\mathcal{S} - \mathcal{S}F_2^\dagger)\Pi_{\leq t}\|_{\mathrm{op}} \leq O(t/\sqrt{N})$.

We provide the proof of above lemma in Section 7.

4.8 Statistical Closeness between $\mathbf{H}_3$ and $\mathbf{H}_4$: Proving Lemma 4.8

Now, we use the lemmas in Section 4.7 to prove Lemma 4.8. The structure of the proof is similar to the commutator-style analysis in [CMS19; DFMS22].

Proof of Lemma 4.8. We first introduce some notations. Let $|\psi_0\rangle$ denote the initial state in hybrid $\mathbf{H}_3$, i.e.,

$$|\psi_0\rangle := |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}_1}|\varnothing\rangle_{\mathsf{T}_1}|\varnothing\rangle_{\mathsf{S}_2}|\varnothing\rangle_{\mathsf{T}_2}.$$

For $i \in [4t]$, let $|\psi_i\rangle$ denote the state right after the i-th query,

$$|\psi_i\rangle := \mathcal{O}_i A_i |\psi_{i-1}\rangle,$$

where $\mathcal{O}_i$ cycles through $F_1, F_2, F_1^\dagger, F_2^\dagger$ according to i mod 4. Similarly, denote the initial state in $\mathbf{H}_4$ by

$$|\phi_0\rangle := \frac{1}{\sqrt{N^3}} \sum_{k_1,k_2,k_3 \in [N]} |0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\varnothing\rangle_{\mathsf{S}}|\varnothing\rangle_{\mathsf{T}}|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}.$$

For $i \in [4t]$, let $|\psi_i\rangle$ denote the state right after the i-th query,

$$|\phi_i\rangle := \mathcal{O}_i A_i |\phi_{i-1}\rangle,$$

where $\mathcal{O}_i$ cycles through $X^{k_3}FX^{k_1}, FX^{k_2}F, X^{k_1}F^\dagger X^{k_3}, F^\dagger X^{k_2}F^\dagger$ according to i mod 4.

Now, we prove that $\|\mathcal{S}|\psi_i\rangle - |\phi_i\rangle\|_2 = O(i^2/\sqrt{N})$ for $i \in [4t]$ by induction.

Base case ($i = 0$): $\mathcal{S}|\psi_0\rangle = |\phi_0\rangle$ holds trivially.

Induction step: Suppose $\|\mathcal{S}|\psi_{i-1}\rangle - |\phi_{i-1}\rangle\|_2 = O((i-1)^2/\sqrt{N})$. Consider the following four cases:

Case 1. $i \equiv 1$ mod 4:

$$\begin{aligned}
&\|\mathcal{S}|\psi_i\rangle - |\phi_i\rangle\|_2 \\
=&\|\mathcal{S}F_1 A_i|\psi_{i-1}\rangle - X^{k_3}FX^{k_1}A_i|\phi_{i-1}\rangle\|_2 && \text{(by expanding the definition of } |\psi_i\rangle \text{ and } |\phi_i\rangle\text{)} \\
\leq&\|\mathcal{S}F_1 A_i|\psi_{i-1}\rangle - X^{k_3}FX^{k_1}A_i\mathcal{S}|\psi_{i-1}\rangle\|_2 \\
&\qquad + \|X^{k_3}FX^{k_1}A_i\mathcal{S}|\psi_{i-1}\rangle - X^{k_3}FX^{k_1}A_i|\phi_{i-1}\rangle\|_2 && \text{(by the triangle inequality)}
\end{aligned}$$

$$\begin{aligned}
&= \|(\mathcal{S}F_i - X^{k_3}FX^{k_1}\mathcal{S})A_i|\psi_{i-1}\rangle\|_2 + \|X^{k_3}FX^{k_1}A_i(\mathcal{S}|\psi_{i-1}\rangle - |\phi_{i-1}\rangle)\|_2 && \text{(since $\mathcal{S}$ and A_i commute)}\\
&\leq \|(\mathcal{S}F_1 - X^{k_3}FX^{k_1}\mathcal{S})\Pi_{\leq t}\|_{\mathrm{op}} + \|\mathcal{S}|\psi_{i-1}\rangle - |\phi_{i-1}\rangle\|_2 && \text{(by Lemma 3.3)}\\
&= O(i^2/\sqrt{N}). && \text{(by Lemma 4.37 and the induction hypothesis)}
\end{aligned}$$

Other three cases follow from the same argument. Hence, the induction holds true. In particular, when $i = 4t$, we have

$$\|\mathcal{S}|\psi_{4t}\rangle - |\phi_{4t}\rangle\|_2 = O(t^2/\sqrt{N}). \tag{22}$$

Let $\widetilde{\mathcal{S}}$ be the partial isometry guaranteed to exist in Lemma 4.36. By the triangle inequality, Lemma 4.36, and Equation (22), we have

$$\|\widetilde{\mathcal{S}}|\psi_{4t}\rangle - |\phi_{4t}\rangle\|_2 \leq \|\widetilde{\mathcal{S}}|\psi_{4t}\rangle - \mathcal{S}|\psi_{4t}\rangle\|_2 + \|\mathcal{S}|\psi_{4t}\rangle - |\phi_{4t}\rangle\|_2 = O\left(t^2/\sqrt{N}\right). \tag{23}$$

Finally, the trace distance between the output of $\mathbf{H}_3$ and that of $\mathbf{H}_4$ satisfies

$$\begin{aligned}
&\mathsf{TD}(\rho_3, \rho_4) && (24)\\
&= \mathsf{TD}(\mathrm{Tr}_{\mathsf{S}_1\mathsf{S}_2\mathsf{T}_1\mathsf{T}_2}(|\psi_{4t}\rangle\langle\psi_{4t}|), \mathrm{Tr}_{\mathsf{STK}_1\mathsf{K}_2\mathsf{K}_3}(|\phi_{4t}\rangle\langle\phi_{4t}|))\\
&= \mathsf{TD}(\mathrm{Tr}_{\mathsf{STK}_1\mathsf{K}_2\mathsf{K}_3}(\widetilde{\mathcal{S}}|\psi_{4t}\rangle\langle\psi_{4t}|\widetilde{\mathcal{S}}^\dagger), \mathrm{Tr}_{\mathsf{STK}_1\mathsf{K}_2\mathsf{K}_3}(|\phi_{4t}\rangle\langle\phi_{4t}|)) && (25)\\
&\leq \mathsf{TD}(\widetilde{\mathcal{S}}|\psi_{4t}\rangle\langle\psi_{4t}|\widetilde{\mathcal{S}}^\dagger, |\phi_{4t}\rangle\langle\phi_{4t}|) && \text{(trace distance is non-increasing under partial trace)}\\
&\leq \|\widetilde{\mathcal{S}}|\psi_{4t}\rangle - |\phi_{4t}\rangle\|_2\\
& && \text{(the trace distance between pure states is bounded by their Euclidean distance)}\\
&= O(t^2/\sqrt{N}), && \text{(by Equation (23))}
\end{aligned}$$

where Equation (25) is because $\widetilde{\mathcal{S}}$ is a partial isometry that acts on the registers being traced out, and $|\psi_{4t}\rangle$ is in the domain of $\mathcal{S}'$. This completes the proof of Lemma 4.8. □

5 $\mathcal{S}$ is Close to a Partial Isometry: Proving Lemma 4.36

We will define the "normalized" version of $\mathcal{S}_{k_1,k_3}, \mathcal{S}_{k_2}, \mathcal{S}_{\mathcal{Z}}$ such that the coefficients match the number of terms in the sum. First, define the partial isometry $\widetilde{\mathcal{S}}_{k_1,k_3}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$,

$$\begin{aligned}
\widetilde{\mathcal{S}}_{k_1,k_3} \colon & |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}\\
&\mapsto \frac{1}{\sqrt{(N - |\mathcal{B}_1(L_1, L_2, R_1, R_2)|)(N - |\mathcal{B}_3(L_1, L_2, R_1, R_2)|)}}\\
&\qquad \times \sum_{\substack{k_1 \notin \mathcal{B}_1(L_1,L_2,R_1,R_2)\\ k_3 \notin \mathcal{B}_3(L_1,L_2,R_1,R_2)}} |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_3\rangle_{\mathsf{K}_3}.
\end{aligned}$$

Next, define the partial isometry $\widetilde{\mathcal{S}}_{k_2}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}, k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2), k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2)$,

$$\widetilde{\mathcal{S}}_{k_2} \colon |L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|k_1\rangle_{\mathsf{K}_1}|k_3\rangle_{\mathsf{K}_3}$$

$$\mapsto \frac{1}{\sqrt{N - |\mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)|}} \times \sum_{k_2 \notin \mathcal{B}_2(L_1,L_2,R_1,R_2,k_1,k_3)} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |k_1\rangle_{\mathsf{K}_1} |k_2\rangle_{\mathsf{K}_2} |k_3\rangle_{\mathsf{K}_3} .$$

Finally, define the partial isometry $\widetilde{\mathcal{S}}_{\vec{z}}$ such that for any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}, k_1 \notin \mathcal{B}_1(L_1, L_2, R_1, R_2), k_3 \notin \mathcal{B}_3(L_1, L_2, R_1, R_2), k_2 \notin \mathcal{B}_2(L_1, L_2, R_1, R_2, k_1, k_3)$,

$$\begin{aligned} \widetilde{\mathcal{S}}_{\vec{z}} \colon & |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |k_1\rangle_{\mathsf{K}_1} |k_2\rangle_{\mathsf{K}_2} |k_3\rangle_{\mathsf{K}_3} \\ & \mapsto \frac{1}{\sqrt{N^{|L_2|} - \left|\mathcal{B}_L\begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix}\right|}} \frac{1}{\sqrt{N^{|R_2|} - \left|\mathcal{B}_R\begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix}\right|}} \\ & \quad \times \sum_{\vec{z}_L \notin \mathcal{B}_L\begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix}, \vec{z}_R \notin \mathcal{B}_R\begin{pmatrix} L_1, L_2, \\ R_1, R_2, \\ k_1, k_2, k_3 \end{pmatrix}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{z}_L\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |k_1\rangle_{\mathsf{K}_1} |k_2\rangle_{\mathsf{K}_2} |k_3\rangle_{\mathsf{K}_3} . \end{aligned}$$

Lemma 5.1. *For any interger $t \geq 0$,*

$$\begin{aligned} &\|(\mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{k_1,k_3})\Pi_{\leq t}\|_{\mathrm{op}} \leq O(\sqrt{t^2/N}), \\ &\|(\mathcal{S}_{k_2} - \widetilde{\mathcal{S}}_{k_2})\Pi_{\leq t}\|_{\mathrm{op}} \leq O(\sqrt{t^2/N}), \\ &\|(\mathcal{S}_{\vec{z}} - \widetilde{\mathcal{S}}_{\vec{z}})\Pi_{\leq t}\|_{\mathrm{op}} \leq O(\sqrt{t^2/N}). \end{aligned}$$

Proof. Since $\mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{k_1,k_3}$ preserve the orthogonality of input of the form $|L_1\rangle|R_1\rangle|L_2\rangle|R_2\rangle$. Thus, by Lemma 3.4, it is suffices to maximize

$$\|(\mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{k_1,k_3})\Pi_{\leq t}|L_1\rangle|R_1\rangle|L_2\rangle|R_2\rangle\|_2.$$

This follow from Lemma 4.22 and an elementary calculation. Items 2 and 3 follow similarly. □

Proof of Lemma 4.36. Define the operator $\widetilde{\mathcal{S}} := \mathcal{D}^\dagger \cdot \widetilde{\mathcal{S}}_{\vec{z}} \cdot \widetilde{\mathcal{S}}_{k_2} \cdot \widetilde{\mathcal{S}}_{k_1,k_3}$. To see that $\widetilde{\mathcal{S}}$ is a partial isometry, one can easily verify that $\widetilde{\mathcal{S}}$ preserves the inner product between basis vectors in the domain.[16] Then we obtain

$$\begin{aligned} &\|(\mathcal{S} - \widetilde{\mathcal{S}})\Pi_{\leq t}\|_{\mathrm{op}} \\ &= \|\mathcal{D}^\dagger \cdot (\mathcal{S}_{\vec{z}} \cdot \mathcal{S}_{k_2} \cdot \mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{\vec{z}} \cdot \widetilde{\mathcal{S}}_{k_2} \cdot \widetilde{\mathcal{S}}_{k_1,k_3})\Pi_{\leq t}\|_{\mathrm{op}} \\ &= \|(\mathcal{S}_{\vec{z}} \cdot \mathcal{S}_{k_2} \cdot \mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{\vec{z}} \cdot \widetilde{\mathcal{S}}_{k_2} \cdot \widetilde{\mathcal{S}}_{k_1,k_3})\Pi_{\leq t}\|_{\mathrm{op}} && (\text{since } \|\mathcal{D}^\dagger\|_{\mathrm{op}} = \|\mathcal{D}\|_{\mathrm{op}} = 1) \\ &\leq \|(\mathcal{S}_{\vec{z}} - \widetilde{\mathcal{S}}_{\vec{z}})\Pi_{\leq t}\|_{\mathrm{op}} + \|(\mathcal{S}_{k_2} - \widetilde{\mathcal{S}}_{k_2})\Pi_{\leq t}\|_{\mathrm{op}} + \|(\mathcal{S}_{k_1,k_3} - \widetilde{\mathcal{S}}_{k_1,k_3})\Pi_{\leq t}\|_{\mathrm{op}} && (26) \\ &= O(\sqrt{t^2/N}), && (\text{by Lemma 5.1}) \end{aligned}$$

where Equation (26) uses (i) the triangle inequality; (ii) that $\Pi_{\leq t}$ commutes with each of $\mathcal{S}_{\vec{z}}, \mathcal{S}_{k_2}, \mathcal{S}_{k_1,k_3}$; (iii) that the operator norm is submultiplicative; and (iv) that $\mathcal{S}_{\vec{z}}, \mathcal{S}_{k_2}, \mathcal{S}_{k_1,k_3}$ are partial isometries (so their operator norm is 1). This completes the proof of Lemma 4.36. □

[16] In contrast to isometries, partial isometries are *not* necessarily closed under composition.

6 Closeness of the First Oracle: Proving Lemma 4.37

Our approach is through expanding oracles F_1, F_2, F as a sum of smaller terms. Then we carefully bound each pair of terms. Before proving Lemma 4.37, we first introduce several lemmas.

6.1 Closeness of F_1^L and F_1^R

Intuitively, the following lemma states the following. Suppose the adversary in hybrid $\mathbf{H}_3$ has made $t = \mathsf{poly}(\lambda)$ queries in total at the moment. Then the state obtained by applying F_1^L followed by $\mathcal{S}$ is negligibly close to the state obtained by applying $\mathcal{S}$ followed by $X^{k_3}F^LX^{k_1}$. The intuition is straightforward. If we apply F_1^L and then $\mathcal{S}$, the resulting state is entirely supported by decomposable relations with the correct number of correlated pairs, owing to the definition of $\mathcal{S}$. On the other hand, if we first apply $\mathcal{S}$, then $X^{k_3}F^LX^{k_1}$, there is a small chance that the y sampled by F^L might generate unwanted correlated pairs. Fortunately, since the relations are of polynomial size, all but a negligible fraction of y behave correctly.

Lemma 6.1 (Closeness of F_1^L and F_1^R)**.** *For any integer $t \geq 0$,*

$$\|(X^{k_3}F^LX^{k_1}\mathcal{S} - \mathcal{S}F_1^L)\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N})$$
$$\|(X^{k_1}F^RX^{k_3}\mathcal{S} - \mathcal{S}F_1^R)\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N}).$$

Proof. Fix $t \in \mathbb{N}, x \in [N], L_1, L_2 \in \mathcal{R}_{\leq t}^{\mathcal{I}\text{-dist}}$, and $R_1, R_2 \in \mathcal{R}_{\leq t}^{\mathcal{D}\text{-dist}}$. We start by calculating the following states:

$$|\psi_{x,L_1,R_1,L_2,R_2}\rangle_{\mathsf{ASTK_1K_2K_3}} := X^{k_3}F^LX^{k_1}\mathcal{S}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2},$$
$$|\phi_{x,L_1,R_1,L_2,R_2}\rangle_{\mathsf{ASTK_1K_2K_3}} := \mathcal{S}F_1^L|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}.$$

To simplify notation, we write $|\mathbf{k}\rangle_{\mathsf{K}}$ as shorthand for $|k_1\rangle_{\mathsf{K}_1}|k_2\rangle_{\mathsf{K}_2}|k_3\rangle_{\mathsf{K}_3}$, and $(\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2,}{R_1,R_2}$ as shorthand for $(k_1,k_2,k_3,\vec{z}_L,\vec{z}_R) \in \mathsf{G}\binom{L_1,L_2,}{R_1,R_2}$.

Computing $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$. Expanding the definitions of $\mathcal{S}$ and F^L, we have

$$|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}$$
$$\overset{\mathcal{S}}{\mapsto} \frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}} \sum_{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2}} |x\rangle_{\mathsf{A}}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}} \quad \text{(by Lemma 4.34)}$$
$$\xmapsto{X^{k_3}F^LX^{k_1}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2} \\ y\notin\mathrm{Im}(L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)})}} |y\oplus k_3\rangle_{\mathsf{A}}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \cup \{(x\oplus k_1, y)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}$$
$$\text{(by Equation (1))}$$
$$= \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2} \\ y\oplus k_3\notin\mathrm{Im}(L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)})}} |y\rangle_{\mathsf{A}}|L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \cup \{(x\oplus k_1, y\oplus k_3)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}$$
$$\text{(by relabeling } y \mapsto y\oplus k_3)$$

$$= \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2} \\ y\notin \mathrm{Im}(L_1)\cup\left(\mathrm{Im}(L_2^{(k_2,\vec{z}_L)})\oplus k_3\right)}} |y\rangle_{\mathsf{A}} |(L_1\cup\{(x,y)\})^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}, \tag{27}$$

where the last line is by the definition of augmented relations in Equation (8).

Computing $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$. Similarly, expanding the definitions of $\mathcal{S}$ and F_1^L, we have

$$\frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{y\notin\mathrm{Im}(L_1), \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\left(\substack{L_1\cup\{(x,y)\},L_2, \\ R_1,R_2}\right)}} |y\rangle_{\mathsf{A}} |(L_1\cup\{(x,y)\})^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}. \tag{28}$$

Orthogonality. Consider distinct (x, L_1, R_1, L_2, R_2) and $(x', L_1', R_1', L_2', R_2')$. We claim that

- $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$,
- $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$,
- $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$.

They together implies that $|\psi_{x,L_1,R_1,L_2,R_2}\rangle - |\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle - |\phi_{x',L_1',R_1',L_2',R_2'}\rangle$. Thus, by Lemma 3.4, it suffices to maximize the norm over input states of the form $|x\rangle|L_1\rangle|R_1\rangle|L_2\rangle|R_2\rangle$. To prove the claim, we define the operator

$$\mathcal{I} := X^{k_3} \cdot X^{k_1} \cdot \mathcal{D} \cdot F^L_{\mathsf{extract}} \cdot X^{k_3}$$

where the partial isometry F_L^{extract} is defined in Equation (6). Note that $\mathcal{I}$ preserves inner product between the states under consideration. To see this, we may compute the states obtained by applying $\mathcal{I}$ to them:

$$\begin{aligned}
&|\psi_{x,L_1,R_1,L_2,R_2}\rangle \\
&\xmapsto{F^L_{\mathsf{extract}}\cdot X^{k_3}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2} \\ y\notin \mathrm{Im}(L_1)\cup\left(\mathrm{Im}(L_2^{(k_2,\vec{z}_L)})\oplus k_3\right)}} |y\oplus k_3\rangle_{\mathsf{A'}} |x\oplus k_1\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}} \\
&\hspace{20em} \text{(by Equations (6) and (27))} \\
&\xmapsto{X^{k_3}\cdot X^{k_1}\cdot\mathcal{D}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2,}{R_1,R_2} \\ y\notin \mathrm{Im}(L_1)\cup\left(\mathrm{Im}(L_2^{(k_2,\vec{z}_L)})\oplus k_3\right)}} |y\rangle_{\mathsf{A'}} |x\rangle_{\mathsf{A}} |L_1\rangle_{\mathsf{S_1}} |L_2\rangle_{\mathsf{S_2}} |R_1\rangle_{\mathsf{T_1}} |R_2\rangle_{\mathsf{T_2}} |\mathbf{z}\rangle_{\mathsf{Z}} |\mathbf{k}\rangle_{\mathsf{K}},
\end{aligned} \tag{29}$$

where the last line is by Definition 4.13. From the above calculation, it is clear that $\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $\mathcal{I}|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$ whenever $(x, L_1, L_2, R_1, R_2) \neq (x', L_1', L_2', R'_1, R'_2)$. Moreover, $X^{k_3}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is in the domain of the partial isometry F_L^{extract}, and $F_L^{\mathsf{extract}} X^{k_3}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is in the domain of the partial isometry $\mathcal{D}$. Thus, $\mathcal{I}$ preserves the inner product between $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ and $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$, which implies Item 1, namely, $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$.

Similarly, we have

$$|\phi_{x,L_1,R_1,L_2,R_2}\rangle \overset{\mathcal{I}}{\mapsto} \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{y\notin \mathrm{Im}(L_1), \\ (\mathbf{k},\mathbf{z})\in \mathsf{G}\left(\substack{L_1\cup\{(x,y)\},L_2, \\ R_1,R_2}\right)}} |y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}. \tag{30}$$

Likewise, $\mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $\mathcal{I}|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$ and $\mathcal{I}$ preserves the inner product between $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ and $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$. Thus, $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$, proving Item 2. Finally, from the above calculation, we can easily conclude that $\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$ which imply that $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$, proving Item 3.

Wrap-up. According to the above argument and Lemma 3.4, it suffices to bound the maximum of

$$\| |\psi_{x,L_1,R_1,L_2,R_2}\rangle - |\phi_{x,L_1,R_1,L_2,R_2}\rangle \|_2.$$

over all $x \in [N], L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$. From the above calculation, this is equivalently reduced to bounding

$$\|\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle - \mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle\|_2.$$

Finally, by Lemma 4.26, we obtain

$$\|\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle - \mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle\|_2^2 = O(t/N).$$

This concludes the proof of Lemma 6.1. □

6.2 Closeness of $F_1^{L,\dagger}$ and $F_1^{R,\dagger}$

The following lemma implies that in $\mathbf{H}_3$, any state orthogonal to the image of F_1^L remains nearly orthogonal to the image of F^L after the action of $X^{k_3}\mathcal{S}$. Intuitively, this prevents unintended "cancellation" between oracle calls to F^L.

Lemma 6.2 (Image Lemma for F_1^L). *For any integer $t \geq 0$ and any normalized state $|\psi\rangle$ on registers* $\mathsf{A}, \mathsf{B}, \mathsf{S}_1, \mathsf{T}_1, \mathsf{S}_2, \mathsf{T}_2$ *such that $\Pi_{\leq t}|\psi\rangle = |\psi\rangle$ and $F_1^{L,\dagger}|\psi\rangle = 0$, it holds that*

$$\|F^{L,\dagger}X^{k_3}\mathcal{S}|\psi\rangle\|_2 = O(\sqrt{t/N}).$$

Proof. Suppose $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{\substack{y,b \\ L_1,L_2,R_1,R_2}} \alpha_{y,b,L_1,R_1,L_2,R_2}|y\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2},$$

where $y \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$ and $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$; recall that B is the adversary's auxiliary register, and b ranges from some finite set that we do not explicitly specify.

Zero condition. The premise implies that

$$\begin{aligned}
0 &= F_1^{L,\dagger} \cdot |\psi\rangle \\
&= F_1^{L,\dagger} \cdot \sum_{\substack{y,b\\ L_1,L_2,R_1,R_2}} \alpha_{y,b,L_1,R_1,L_2,R_2} |y\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} \\
&= \frac{1}{\sqrt{N}} \sum_{\substack{b,L_1,L_2,R_1,R_2\\ (x,y)\in L_1}} \alpha_{y,b,L_1,R_1,L_2,R_2} |x\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1 \setminus \{(x,y)\}\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2}. \qquad \text{(by Equation (4))}
\end{aligned}$$

By re-writing $L_1 = L_1' \cup \{(x,y)\}$, we obtain

$$\begin{aligned}
&\frac{1}{\sqrt{N}} \sum_{\substack{x,b\\ L_1',L_2,R_1,R_2\\ y\notin \mathrm{Im}(L_1')}} \alpha_{y,b,L_1'\cup\{(x,y)\},R_1,L_2,R_2} |x\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1'\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} \\
&= \frac{1}{\sqrt{N}} \sum_{\substack{x,b\\ L_1',L_2,R_1,R_2}} \left(\sum_{y\notin \mathrm{Im}(L_1')} \alpha_{y,b,L_1'\cup\{(x,y)\},R_1,L_2,R_2} \right) |x\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1'\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2},
\end{aligned}$$

where $x \in [N]$ and $L_1' \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\le t-1}$. Therefore, for any fixed $x \in [N]$, b, $L_1' \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\le t-1}$, $L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\le t}$, and $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\le t}$, it holds that

$$\sum_{y\notin \mathrm{Im}(L_1')} \alpha_{y,b,L_1'\cup\{(x,y)\},R_1,L_2,R_2} = 0. \tag{31}$$

Computing $F^{L,\dagger} X^{k_3} \mathcal{S} |\psi\rangle$. Next, we will compute $F^{L,\dagger} X^{k_3} \mathcal{S} |\psi\rangle$. Firstly, by Lemma 4.34, we obtain

$$|\psi\rangle \xmapsto{X^{k_3}\mathcal{S}} \sum_{\substack{y,b\\ L_1,L_2,R_1,R_2\\ (\mathbf{k},\mathbf{z})\in \mathsf{G}\binom{L_1,L_2}{R_1,R_2}}} \frac{\alpha_{y,b,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+3}}} |y \oplus k_3\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}.$$

Before we move on to apply $F^{L,\dagger}$, recall Equation (4). For the expression to be nonzero, it is necessary that $y \oplus k_3 \in L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}$. By Lemma 4.20, $L_1^{(k_1,k_3)}$ and $L_2^{(k_2,\vec{z}_L)}$ are disjoint. Therefore, $(x, y \oplus k_3)$ must belong to exactly one of the following: (i) $(x, y \oplus k_3) \in L_1^{(k_1,k_3)}$, (ii) $(x, y \oplus k_3) \in L_2^{(k_2,\vec{z}_L)}$. Define two projectors

$$\begin{aligned}
\Pi_1 &:= \sum_{\substack{(L,\mathbf{k}):\ G^{\mathcal{I}}_{L,k_2} \text{ is decomposable}\\ y\in \mathrm{Im}(V_{\mathsf{isolate}}(G^{\ell}_{L,k_2}))}} |y\rangle\langle y|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{S}} \otimes |\mathbf{k}\rangle\langle \mathbf{k}|_{\mathsf{K}}, \\
\Pi_2 &:= \sum_{\substack{(L,\mathbf{k}):\ G^{\ell}_{L,k_2} \text{ is decomposable}\\ y\in \mathrm{Im}(V_{\mathsf{target}}(G^{\ell}_{L,k_2})\cup V_{\mathsf{source}}(G^{\ell}_{L,k_2}))}} |y\rangle\langle y|_{\mathsf{A}} \otimes |L\rangle\langle L|_{\mathsf{S}} \otimes |\mathbf{k}\rangle\langle \mathbf{k}|_{\mathsf{K}}
\end{aligned}$$

Thus, it holds that

$$F^{L,\dagger} X^{k_3} \mathcal{S} |\psi\rangle = F^{L,\dagger} \Pi_1 X^{k_3} \mathcal{S} |\psi\rangle + F^{L,\dagger} \Pi_2 X^{k_3} \mathcal{S} |\psi\rangle.$$

By the triangle inequality, it suffices to the bound the norm of each term.

Bounding $F^{L,\dagger}\Pi_1 X^{k_3}\mathcal{S}|\psi\rangle$. Using Equation (4), we obtain

$$
\begin{aligned}
&F^{L,\dagger}\Pi_1 X^{k_3}\mathcal{S}|\psi\rangle \\
&= \sum_{\substack{b,L_1,L_2,R_1,R_2 \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ x,y:\ (x,y\oplus k_3)\in L_1^{(k_1,k_3)}}} \frac{\alpha_{y,b,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\setminus\{(x,y\oplus k_3)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}.
\end{aligned}
$$

Crucially, we use Lemma 4.18 to conclude that $V_{\mathsf{isolate}}\left(G^{\ell}_{L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)},k_2}\right) = L_1^{(k_1,k_3)}$. Thus, we are summing over elements in $L_1^{(k_1,k_3)}$ in the above line.

By substituting $x = x'\oplus k_1$ and using that $(\hat{x}\oplus k_1,\hat{y}\oplus k_3)\in L_1^{(k_1,k_3)}$ if and only if $(\hat{x},\hat{y})\in L_1$, we obtain

$$
\sum_{\substack{b,L_1,L_2,R_1,R_2 \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ (x',y)\in L_1}} \frac{\alpha_{y,b,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x'\oplus k_1\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|(L_1\setminus\{(x',y)\})^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}.
$$

Substituting $L_1 = L_1'\cup\{(x',y)\}$, we obtain

$$
\sum_{\substack{b,L_1',L_2,R_1,R_2 \\ x',y\notin\mathrm{Im}(L_1') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x'\oplus k_1\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|(L_1')^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}. \tag{32}
$$

We will further simplify the state. By monotonicity (Lemma 4.23), we can see that Equation (32) is in the domain of the partial isometry $\mathcal{D}$. Thus, we can equivalently evaluate the norm of $\mathcal{D}\cdot X^{k_1}\cdot F^{L,\dagger}\Pi_1 X^{k_3}\mathcal{S}|\psi\rangle$. Thus, applying $\mathcal{D}\cdot X^{k_1}$ to Equation (32), we obtain

$$
\sum_{\substack{b,L_1',L_2,R_1,R_2 \\ x',y\notin\mathrm{Im}(L_1') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x'\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1'\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}.
$$

Rearranging, we obtain

$$
\sum_{\substack{b,L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z} \\ y\notin\mathrm{Im}(L_1'):\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x'\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1'\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}, \tag{33}
$$

where $x'\in[N], k_1,k_2,k_3\in[N], \vec{z}_L\in[N]^{|L_2|}_{\mathrm{dist}}, \vec{z}_R\in[N]^{|R_2|}_{\mathrm{dist}}$ and we range over y at the end.

The squared norm of Equation (33) is

$$\sum_{\substack{b,L_1',L_2,R_1,R_2,x'\\ \mathbf{k},\mathbf{z}}} \left| \sum_{y\notin \mathrm{Im}(L_1')\colon (\mathbf{k},\mathbf{z})\in \mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}} \right|^2.$$

By Lemma 4.25, once $(L_1', L_2, R_1, R_2, x', \mathbf{k}, \mathbf{z})$ is fixed, there is either zero or at least $N - g(t)$ values of y that satisfy the condition, where $g(t) = O(t)$ is some function guaranteed by Lemma 4.25. Let BAD denote the set of tuples for which the latter case holds. We obtain

$$\sum_{b,(L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z})\in\mathsf{BAD}} \left| \sum_{y\notin \mathrm{Im}(L_1')\colon (\mathbf{k},\mathbf{z})\in \mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}} \right|^2.$$

Now, we make crucial use of the condition implied by the premise (Equation (31)) to obtain

$$\begin{aligned}
&\sum_{b,(L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z})\in\mathsf{BAD}} \left| - \sum_{y\notin \mathrm{Im}(L_1')\colon (\mathbf{k},\mathbf{z})\notin \mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}} \frac{\alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}} \right|^2 \\
= &\sum_{b,(L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z})\in\mathsf{BAD}} \frac{1}{N^{|L_2|+|R_2|+4}} \cdot \left| \sum_{y\notin \mathrm{Im}(L_1')\colon (\mathbf{k},\mathbf{z})\notin \mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}} \alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2} \right|^2. \qquad (34)
\end{aligned}$$

Using the Cauchy-Schwarz inequality and the definition of BAD to bound the number of y in the sum, we can bound Equation (34) by

$$\sum_{\substack{b,(L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z})\in\mathsf{BAD}\\ y\notin \mathrm{Im}(L_1')\colon (\mathbf{k},\mathbf{z})\notin \mathsf{G}\binom{L_1'\cup\{(x',y)\},L_2}{R_1,R_2}}} \frac{g(t)}{N^{|L_2|+|R_2|+4}} \cdot \left| \alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2} \right|^2,$$

Since we are summing over non-negative terms, by relaxing the constraints, we can bound it by

$$\sum_{\substack{b,L_1',L_2,R_1,R_2,x',\mathbf{k},\mathbf{z}\\ y\notin \mathrm{Im}(L_1')}} \frac{g(t)}{N^{|L_2|+|R_2|+4}} \cdot \left| \alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2} \right|^2.$$

By summing over $(\mathbf{k}, \mathbf{z})$, and noting that there are at most $N^{|L_2|+|R_2|+3}$ such tuples, we can bounded it by

$$\frac{g(t)}{N} \cdot \sum_{b,L_1',L_2,R_1,R_2,x',y\notin \mathrm{Im}(L_1')} \left| \alpha_{y,b,L_1'\cup\{(x',y)\},R_1,L_2,R_2} \right|^2.$$

By substituting $L = L_1' \cup \{(x', y)\}$, we obtain

$$\frac{g(t)}{N} \cdot \sum_{b,L_1,L_2,R_1,R_2,y\in \mathrm{Im}(L_1)} \left| \alpha_{y,b,L_1,R_1,L_2,R_2} \right|^2 = O(t/N)$$

by the normalization condition of $|\psi\rangle$.

Bounding $F^{L,\dagger}\Pi_2 X^{k_3}\mathcal{S}|\psi\rangle$. Recall Lemma 4.35. For any (y, L_1, R_1, L_2, R_2), define the set

$$\mathcal{P}_{y,L_1,R_1,L_2,R_2} := \{(\mathbf{k},\mathbf{z})\colon y \oplus k_3 \in \mathrm{Im}(L_2^{(k_2,\vec{z}_L)})\}.$$

By sampling k_3 at the end and the union bound, it is clear that $\mathcal{P}_{y,L_1,R_1,L_2,R_2}$ occupies at most a $2t/N$ fraction of its universe. Thus, we obtain

$$\begin{aligned}\|F^{L,\dagger}\Pi_2 X^{k_3}\mathcal{S}|\psi\rangle\|_2 &\le \|F^{L,\dagger}\Pi_2 X^{k_3}\mathcal{S}^{\bullet}|\psi\rangle\|_2 + \|F^{L,\dagger}\Pi_2 X^{k_3}(\mathcal{S}-\mathcal{S}^{\bullet})|\psi\rangle\|_2\\ &\le \|\Pi_2 X^{k_3}\mathcal{S}^{\bullet}|\psi\rangle\|_2 + \|(\mathcal{S}^{\bullet}-\mathcal{S})\Pi_{\le t}\|_{\mathrm{op}}\\ &\le O(\sqrt{t/N}).\end{aligned}$$

The first term is zero by the definitions of $\{\mathcal{P}_\tau\}_\tau$ and $\mathcal{S}^{\bullet}$. The second term is bounded by Lemma 4.35. This completes the proof of Lemma 6.2. $\square$

Lemma 6.3 (Closeness of $F_1^{L,\dagger}$ and $F_1^{R,\dagger}$)**.** *For any integer $t \ge 0$,*

$$\begin{aligned}\|(X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{L,\dagger})\Pi_{\le t}\|_{\mathrm{op}} &= O(\sqrt{t/N})\\ \|(X^{k_1}F^{R,\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} &= O(\sqrt{t/N}).\end{aligned}$$

Proof. Let $\Pi^{\mathrm{Im}(F_1^L)}$ denote the projection onto the image of F_1^L. For an arbitrary normalized state $|\psi\rangle$ on registers $\mathsf{A}, \mathsf{S}_1, \mathsf{T}_1, \mathsf{S}_2, \mathsf{T}_2$ in the subspace of $\Pi_{\le t}$, we can decompose it as

$$|\psi\rangle = \Pi^{\mathrm{Im}(F_1^L)}|\psi\rangle + (\mathrm{id} - \Pi^{\mathrm{Im}(F_1^L)})|\psi\rangle.$$

We will show the following two bounds

$$\|(X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{L,\dagger})\Pi^{\mathrm{Im}(F_1^L)}|\psi\rangle\|_2 \le O(\sqrt{t/N}) \tag{35}$$

$$\|(X^{k_1}F^{\dagger,L}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{L,\dagger})(\mathrm{id} - \Pi^{\mathrm{Im}(F_1^L)})|\psi\rangle\|_2 \le O(\sqrt{t/N}) \tag{36}$$

which then the first bound follows by the triangle inequality. Notice that $F^{L,\dagger}(\mathrm{id} - \Pi^{\mathrm{Im}(F_1^L)}) = 0$, so Equation (36) follows from Lemma 6.2. Hence, it remains to prove Equation (35). Since $\Pi^{\mathrm{Im}(F_1^L)}|\psi\rangle$ is in the image of F_1^L, there exists some state $|\phi\rangle$ such that $\Pi^{\mathrm{Im}(F_1^L)}|\psi\rangle = F_1^L|\phi\rangle$. Now, we bound Equation (35) by the triangle inequality as follows:

$$\begin{aligned}&\|(X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{L,\dagger})\Pi^{\mathrm{Im}(F_1^L)}|\psi\rangle\|_2\\ =&\|(X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{L,\dagger})F_1^L|\phi\rangle\|_2\\ \le&\|X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S}F_1^L|\phi\rangle - X^{k_1}F^{L,\dagger}F^LX^{k_1}\mathcal{S}|\phi\rangle\|_2 &(37)\\ &\qquad\qquad + \|X^{k_1}F^{L,\dagger}F^LX^{k_1}\mathcal{S}|\phi\rangle - \mathcal{S}F_1^{L,\dagger}F_1^L|\phi\rangle\|_2. &(38)\end{aligned}$$

To bound Equation (37), we have

$$\begin{aligned}&\|X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S}F_1^L|\phi\rangle - X^{k_1}F^{L,\dagger}F^LX^{k_1}\mathcal{S}|\phi\rangle\|_2\\ =&\|X^{k_1}F^{L,\dagger}X^{k_3}\mathcal{S}F_1^L|\phi\rangle - X^{k_1}F^{L,\dagger}X^{k_3}X^{k_3}F^LX^{k_1}\mathcal{S}|\phi\rangle\|_2 &\text{(since } X^{k_3}X^{k_3} = \mathrm{id})\end{aligned}$$

$$\begin{aligned}
&=\|X^{k_1}F^{L,\dagger}X^{k_3}\cdot(\mathcal{S}F_1^L - X^{k_3}F^LX^{k_1}\mathcal{S})|\phi\rangle\|_2\\
&\le\|X^{k_1}F^{L,\dagger}X^{k_3}\cdot(\mathcal{S}F_1^L - X^{k_3}F^LX^{k_1}\mathcal{S})\Pi_{\le t}\|_{\mathrm{op}}\\
&\le\|F^{L,\dagger}\|_{\mathrm{op}}\cdot\|(\mathcal{S}F_1^L - X^{k_3}F^LX^{k_1}\mathcal{S})\Pi_{\le t}\|_{\mathrm{op}} \qquad \text{(since operator norm is submultiplicative)}\\
&\le O(\sqrt{t/N}). \qquad \text{(by the fact that } F^L \text{ is a contraction and Lemma 6.1)}
\end{aligned}$$

To bound Equation (38), we first expand the terms. By Lemma 3.10, we can replace $F^{L,\dagger}F^L$ with id as follows:

$$\begin{aligned}
&\|(X^{k_1}F^{L,\dagger}F^LX^{k_1}\mathcal{S} - \mathcal{S}F_1^{L,\dagger}F_1^L)\Pi_{\le t}\|_{\mathrm{op}}\\
\le&\|(X^{k_1}F^{L,\dagger}F^LX^{k_1}\mathcal{S} - X^{k_1}X^{k_1}\mathcal{S})\Pi_{\le t}\|_{\mathrm{op}} + \|(X^{k_1}X^{k_1}\mathcal{S} - \mathcal{S}F_1^{L,\dagger}F_1^L)\Pi_{\le t}\|_{\mathrm{op}}\\
\le&\|(F^{L,\dagger}F^L - \mathrm{id})X^{k_1}\mathcal{S}\Pi_{\le t}\|_{\mathrm{op}} + \|(\mathrm{id} - F_1^{L,\dagger}F_1^L)\Pi_{\le t}\|_{\mathrm{op}}\\
\le&\|(F^{L,\dagger}F^L - \mathrm{id})\Pi_{\le 3t}\|_{\mathrm{op}} + \|(\mathrm{id} - F_1^{L,\dagger}F_1^L)\Pi_{\le t}\|_{\mathrm{op}}\\
\le&O(t/N).
\end{aligned}$$

This proves the first bound. The second bound follows symmetrically. □

6.3 Putting Things Together

Finally, we use the above lemmas to prove Lemma 4.37. We restate Lemma 4.37 for convenience.

Lemma 6.4 (Lemma 4.37, restated)**.** *For any integer $t \ge 0$,*

- **Forward query:** $\|(X^{k_3}FX^{k_1}\mathcal{S} - \mathcal{S}F_1)\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$,
- **Inverse query:** $\|(X^{k_1}F^{\dagger}X^{k_3}\mathcal{S} - \mathcal{S}F_1^{\dagger})\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$.

Proof of Lemma 4.37.
Forward query. Recall the definition of F_1:

$$\begin{aligned}
F_1 &= F_1^L\cdot(\mathrm{id} - F_1^R\cdot F_1^{R,\dagger}) + (\mathrm{id} - F_1^L\cdot F_1^{L,\dagger})\cdot F_1^{R,\dagger}\\
&= F_1^L - F_1^L\cdot F_1^R\cdot F_1^{R,\dagger} + F_1^{R,\dagger} - F_1^L\cdot F_1^{L,\dagger}\cdot F_1^{R,\dagger}.
\end{aligned}$$

Similarly, we expand $X^{k_3}FX^{k_1}$ in the following:

$$\begin{aligned}
X^{k_3}FX^{k_1} =&X^{k_3}F^L\cdot(\mathrm{id} - F^RF^{R,\dagger})X^{k_1} + X^{k_3}(\mathrm{id} - F^LF^{L,\dagger})\cdot F^{R,\dagger}X^{k_1}\\
=&X^{k_3}F^LX^{k_1} - X^{k_3}F^LF^RF^{R,\dagger}X^{k_1} + X^{k_3}F^{R,\dagger}X^{k_1} - X^{k_3}F^LF^{L,\dagger}F^{R,\dagger}X^{k_1}\\
=&X^{k_3}F^LX^{k_1} - (X^{k_3}F^LX^{k_1})(X^{k_1}F^RX^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1})\\
&+ X^{k_3}F^{R,\dagger}X^{k_1} - (X^{k_3}F_LX^{k_1})(X^{k_1}F^{L,\dagger}X^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1}).
\end{aligned}$$

By the triangle inequality, it suffices to bound each of the following terms:

$$\begin{aligned}
&\|(X^{k_3}FX^{k_1}\mathcal{S} - \mathcal{S}F_1)\Pi_{\le t}\|_{\mathrm{op}}\\
\le&\|(X^{k_3}F^LX^{k_1}\mathcal{S} - \mathcal{S}F_1^L)\Pi_{\le t}\|_{\mathrm{op}} \qquad (39)\\
+&\|((X^{k_3}F^LX^{k_1})(X^{k_1}F^RX^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1})\mathcal{S} - \mathcal{S}F_1^LF_1^RF_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} \qquad (40)
\end{aligned}$$

$$+\|(X^{k_3}F^{R,\dagger}X^{k_1}\mathcal{S} - \mathcal{S}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} \tag{41}$$
$$+\|((X^{k_3}F^{L}X^{k_1})(X^{k_1}F^{L,\dagger}X^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1})\mathcal{S} - \mathcal{S}F_1^{L}F_1^{L,\dagger}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}}. \tag{42}$$

From Lemma 6.1, we can bound Equation (39) by $O(\sqrt{t/N})$. From Lemma 6.3, we can bound Equation (41) by $O(\sqrt{t^2/N})$. To bound Equation (40), by the triangle inequality, we have

$$\begin{aligned}
&\|((X^{k_3}F^{L}X^{k_1})(X^{k_1}F^{R}X^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1})\mathcal{S} - \mathcal{S}F_1^{L}F_1^{R}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}}\\
\le&\|((X^{k_3}F^{L}X^{k_1})(X^{k_1}F^{R}X^{k_3})(X^{k_3}F^{R,\dagger}X^{k_1})\mathcal{S} - (X^{k_3}F^{L}X^{k_1})(X^{k_1}F^{R}X^{k_3})\mathcal{S}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}}\\
&\qquad + \|((X^{k_3}F^{L}X^{k_1})(X^{k_1}F^{R}X^{k_3})\mathcal{S}F_1^{R,\dagger} - (X^{k_3}F^{L}X^{k_1})\mathcal{S}F_1^{R}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}}\\
&\qquad\qquad + \|((X^{k_3}F^{L}X^{k_1})\mathcal{S}F_1^{R}F_1^{R,\dagger} - \mathcal{S}F_1^{L}F_1^{R}F_1^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}}\\
\le&O(\sqrt{t/N})
\end{aligned}$$

where we use (i) that operator norm is submultiplicative; (ii) that F^L, F^R are contractions; and (iii) Lemma 6.3, Lemma 6.1, and Lemma 6.1, in order, for the colored parts. Similarly, Equation (42) is at most $O(t/\sqrt{N})$ by Lemma 6.3, Lemma 6.3, and Lemma 6.1. Combining the above terms, we obtain

$$\|(X^{k_3}FX^{k_1}\mathcal{S} - \mathcal{S}F_1)\Pi_{\le t}\|_{\mathrm{op}} = O(\sqrt{t/N}).$$

This proves the first item of Lemma 4.37. The proof of the second item follows by symmetry. This completes the proof of Lemma 4.37. □

7 Closeness of the Second Oracle: Proving Lemma 4.38

The high-level proof strategy is similar to that in Section 6, where we bound each pair of terms separately. The main distinction is that a query to $FX^{k_2}F$ involves two calls to F, which makes the calculation more intricate. We start by listing some helpful lemmas.

7.1 Closeness of F_2^L and F_2^R

Lemma 7.1 (Closeness of F_2^L and F_2^R)**.** *For any integer $t \ge 0$,*

$$\|(F^LX^{k_2}F^L\mathcal{S} - \mathcal{S}F_2^L)\Pi_{\le t}\|_{\mathrm{op}} = O(\sqrt{t/N})$$
$$\|(F^RX^{k_2}F^R\mathcal{S} - \mathcal{S}F_2^R)\Pi_{\le t}\|_{\mathrm{op}} = O(\sqrt{t/N}).$$

Proof. Fix $t \in \mathbb{N}$, $x \in [N], L_1, L_2 \in \mathcal{R}_{\le t}^{\mathcal{I}\text{-dist}}$, and $R_1, R_2 \in \mathcal{R}_{\le t}^{\mathcal{D}\text{-dist}}$. We start by calculating the following states:

$$|\psi_{x,L_1,R_1,L_2,R_2}\rangle_{\mathsf{ASTK}} := F^LX^{k_2}F^L\mathcal{S}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2},$$
$$|\phi_{x,L_1,R_1,L_2,R_2}\rangle_{\mathsf{ASTK}} := \mathcal{S}F_2^L|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}.$$

Computing $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$. Expanding the definitions of $\mathcal{S}$ and F^L, we have

$|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}$

$$\xrightarrow{\mathcal{S}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}} \sum_{\mathsf{G}\binom{L_1,L_2}{R_1,R_2}} |x\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}} \qquad \text{(by Lemma 4.34)}$$

$$\xrightarrow{F^L} \frac{1}{\sqrt{N^{|L_2|+|R_2|+4}}} \sum_{\substack{\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ z' \notin \mathrm{Im}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)})}} |z'\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \cup \{(x,z')\}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}$$

$$\text{(by Equation (1))}$$

$$\xrightarrow{F^L X^{k_2}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ z',y \notin \mathrm{Im}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}): \\ y \neq z'}} |y\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \cup \{(x,z'),(z' \oplus k_2, y)\}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}, \tag{43}$$

where the last line is by Equation (1).

Calculating $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$. Similarly, expanding the definitions of $\mathcal{S}$ and F_2^L, we have

$$\frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{y \notin \mathrm{Im}(L_2) \\ (\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1, L_2 \cup \{(x,y)\}}{R_1,R_2}}} |y\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup (L_2 \cup \{(x,y)\})^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}. \tag{44}$$

Orthogonality. Consider distinct (x, L_1, R_1, L_2, R_2) and $(x', L_1', R_1', L_2', R_2')$. We claim that

- $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$,
- $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$,
- $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$.

They together implies that $|\psi_{x,L_1,R_1,L_2,R_2}\rangle - |\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\psi_{x',L_1',R_1',L_2',R_2'}\rangle - |\phi_{x',L_1',R_1',L_2',R_2'}\rangle$. Thus, by Lemma 3.4, it suffices to maximize the norm over input states of the form $|x\rangle|L_1\rangle|R_1\rangle|L_2\rangle|R_2\rangle$. To prove the claim, we define the operator

$$\mathcal{I} := \mathcal{D} \cdot F^L_{\mathsf{extract}} \cdot X^{k_2} \cdot F^L_{\mathsf{extract}}$$

where the partial isometry F^L_{extract} is defined in Equation (6). Note that $\mathcal{I}$ preserves inner product between the states under consideration. To see this, we may compute the states obtained by applying $\mathcal{I}$ to them:

$$|\psi_{x,L_1,R_1,L_2,R_2}\rangle \tag{45}$$

$$\xrightarrow{F^L_{\mathsf{extract}}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{(\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ z',y \notin \mathrm{Im}(L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}): \\ y \neq z'}} |y\rangle_{\mathsf{A'}} |z' \oplus k_2\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)} \cup \{(x,z')\}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}$$

$$\text{(by Equation (6))}$$

$$\xmapsto{F^L_{\mathsf{extract}} X^{k_2}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ z',y\notin \mathrm{Im}(L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}): \\ y\neq z'}} |z'\rangle_{\mathsf{A}''}|y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}$$

(by Equation (6))

$$\xmapsto{\mathcal{D}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{(\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2} \\ z',y\notin \mathrm{Im}(L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}): \\ y\neq z'}} |z'\rangle_{\mathsf{A}''}|y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|\mathbf{z}\rangle_{\mathsf{Z}}|\mathbf{k}\rangle_{\mathsf{K}}, \tag{46}$$

where the last line is by Definition 4.13 and noting that the state in the third line is entirely in the domain of $\mathcal{D}$. From the above calculation, it is clear that $\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $\mathcal{I}|\psi_{x',L_1',R_1',L_2',R_2'}\rangle$ whenever $(x,L_1,L_2,R_1,R_2)\neq(x',L_1',L_2',R'_1,R'_2)$.

Similarly, we have

$$|\phi_{x,L_1,R_1,L_2,R_2}\rangle$$
$$\xmapsto{\mathcal{I}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{y\notin\mathrm{Im}(L_2) \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\left(\substack{L_1,L_2\cup\{(x,y)\} \\ R_1,R_2}\right) \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2)\cup\{y\}}} |z_{L,i}\rangle_{\mathsf{A}''}|y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|\vec{z}_{L,-i}\rangle_{\mathsf{Z}_\mathsf{L}}|\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}}|\mathbf{k}\rangle_{\mathsf{K}}. \tag{47}$$

Note that $\vec{z}_L$ is of length $\mathrm{Im}(|L_2|)+1$. In the above expression, $i\in[|\mathrm{Im}(L_2)|+1]$ is the index such that y is the i-th largest element in $\mathrm{Im}(L_2)\cup\{y\}$; $z_{L,i}$ is the i-th coordinate of $\vec{z}_L$; and $\vec{z}_{L,-i}$ is the vector obtained by removing the i-th coordinate of $\vec{z}_L$.

By rearranging, we can express it as

$$\frac{1}{\sqrt{N^{|L_2|+|R_2|+5}}} \sum_{\substack{y\notin\mathrm{Im}(L_2),\mathbf{k},z\in[N],\vec{z}_L\in[N]^{|L_2|}_{\mathrm{dist}},\vec{z}_R\in[N]^{|R_2|}_{\mathrm{dist}}: \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2)\cup\{y\} \\ (\mathbf{k},\vec{z}_L^{(i\leftarrow z)},\vec{z}_R)\in\mathsf{G}\left(\substack{L_1,L_2\cup\{(x,y)\} \\ R_1,R_2}\right)}} |z\rangle_{\mathsf{A}''}|y\rangle_{\mathsf{A}'}|x\rangle_{\mathsf{A}}|L_1\rangle_{\mathsf{S}_1}|L_2\rangle_{\mathsf{S}_2}|R_1\rangle_{\mathsf{T}_1}|R_2\rangle_{\mathsf{T}_2}|\vec{z}_L\rangle_{\mathsf{Z}_\mathsf{L}}|\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}}|\mathbf{k}\rangle_{\mathsf{K}}, \tag{48}$$

where $\vec{z}_L^{(i\leftarrow z)}$ denotes the vector obtained by inserting z into the i-th coordinate of $\vec{z}_L$ and shifting all subsequent coordinates by one.

Likewise, $\mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $\mathcal{I}|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$ and $\mathcal{I}$ preserves the inner product between $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ and $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$. Thus, $|\phi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$, proving Item 2. Finally, from the above calculation, we can easily conclude that $\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$ which imply that $|\psi_{x,L_1,R_1,L_2,R_2}\rangle$ is orthogonal to $|\phi_{x',L_1',R_1',L_2',R_2'}\rangle$, proving Item 3.

Wrap-up. According to Lemma 3.4, it is sufficient to bound the maximum of

$$\||\psi_{x,L_1,R_1,L_2,R_2}\rangle - |\phi_{x,L_1,R_1,L_2,R_2}\rangle\|_2$$

over all $x \in [N], L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$. From the above calculation, this is equivalently reduced to bounding

$$\|\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle - \mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle\|_2.$$

Finally, we use Lemma 4.29 to bound the number of terms in Equations (46) and (48) to obtain

$$\|\mathcal{I}|\psi_{x,L_1,R_1,L_2,R_2}\rangle - \mathcal{I}|\phi_{x,L_1,R_1,L_2,R_2}\rangle\|_2^2 = O(t/N).$$

This concludes the proof of Lemma 7.1. □

7.2 Closeness of $F_2^{L,\dagger}$ and $F_2^{R,\dagger}$

Lemma 7.2 (Image Lemma for F_2^L)**.** *For any integer $t \geq 0$ and any normalized state $|\psi\rangle$ on registers* $\mathsf{A}, \mathsf{B}, \mathsf{S}_1, \mathsf{T}_1, \mathsf{S}_2, \mathsf{T}_2$ *such that $\Pi_{\leq t}|\psi\rangle = |\psi\rangle$ and $F_2^{L,\dagger}|\psi\rangle = 0$, it holds that*

$$\|F^{L,\dagger}\mathcal{S}|\psi\rangle\|_2 = O(\sqrt{t/N}).$$

Proof. Suppose $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{\substack{y,b\\ L_1,L_2,R_1,R_2}} \alpha_{y,b,L_1,R_1,L_2,R_2}|y\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2},$$

where $y \in [N]$, $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}$ and $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$; recall that B is the adversary's auxiliary register, and b ranges from some finite set that we do not explicitly specify.

Zero condition. The premise implies that

$$\begin{aligned}0 &= F_2^{L,\dagger}\cdot|\psi\rangle_{\mathsf{ABS_1T_1S_2T_2}}\\ &= F_2^{L,\dagger}\cdot \sum_{\substack{y,b\\ L_1,L_2,R_1,R_2}} \alpha_{y,b,L_1,R_1,L_2,R_2}|y\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}\\ &= \frac{1}{\sqrt{N}}\sum_{\substack{b,L_1,L_2,R_1,R_2\\ (x,y)\in L_2}} \alpha_{y,b,L_1,R_1,L_2,R_2}|x\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2\setminus\{(x,y)\}\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}. \quad \text{(by Equation (4))}\end{aligned}$$

By re-writing $L_2 = L_2' \cup \{(x,y)\}$, we obtain

$$\begin{aligned}&\frac{1}{\sqrt{N}}\sum_{\substack{x,b\\ L_1,L_2',R_1,R_2\\ y\notin \mathrm{Im}(L_2')}} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x,y)\},R_2}|x\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2'\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}\\ &= \frac{1}{\sqrt{N}}\sum_{\substack{x,b\\ L_1,L_2',R_1,R_2}}\left(\sum_{y\notin \mathrm{Im}(L_2')} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x,y)\},R_2}\right)|x\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1\rangle_{\mathsf{S}_1}|R_1\rangle_{\mathsf{T}_1}|L_2'\rangle_{\mathsf{S}_2}|R_2\rangle_{\mathsf{T}_2}.\end{aligned}$$

Hence, for any $x \in [N]$, b, and $L_1 \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t}, L_2' \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\leq t-1}, R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}_{\leq t}$, it holds that

$$\sum_{y\notin \mathrm{Im}(L_2')} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x,y)\},R_2} = 0. \tag{49}$$

Computing $F^{L,\dagger}\mathcal{S}|\psi\rangle$. Next, we will compute $F^{L,\dagger}\mathcal{S}|\psi\rangle$. Firstly, by Lemma 4.34, we obtain

$$|\psi\rangle \overset{\mathcal{S}}{\mapsto} \sum_{\substack{y,b,\\ L_1,L_2,R_1,R_2\\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2}}} \frac{\alpha_{y,b,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+3}}}|y\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}.$$

Before we move on to apply $F^{L,\dagger}$, recall Equation (4). For the expression to be nonzero, it is necessary that $y\oplus k_3 \in L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}$. By Lemma 4.18, $L_1^{(k_1,k_3)}$ and $L_2^{(k_2,\vec{z}_L)}$ are disjoint. Therefore, (x,y) must belong to exactly one of the following: (i) $(x,y)\in L_1^{(k_1,k_3)}$, (ii) $(x,y)\in L_2^{(k_2,\vec{z}_L)}$. Define two projectors

$$\Pi_1 := \sum_{\substack{(L,\mathbf{k})\colon G^{\ell}_{L,k_2}\text{ is decomposable}\\ y\in\mathrm{Im}(V_{\mathsf{isolate}}(G^{\ell}_{L,k_2})\cup V_{\mathsf{source}}(G^{\ell}_{L,k_2}))}} |y\rangle\langle y|_{\mathsf{A}}\otimes|L\rangle\langle L|_{\mathsf{S}}\otimes|\mathbf{k}\rangle\langle\mathbf{k}|_{\mathsf{K}},$$

$$\Pi_2 := \sum_{\substack{(L,\mathbf{k})\colon G^{\ell}_{L,k_2}\text{ is decomposable}\\ y\in\mathrm{Im}(V_{\mathsf{target}}(G^{\ell}_{L,k_2}))}} |y\rangle\langle y|_{\mathsf{A}}\otimes|L\rangle\langle L|_{\mathsf{S}}\otimes|\mathbf{k}\rangle\langle\mathbf{k}|_{\mathsf{K}}$$

Thus, it holds that

$$F^{L,\dagger}X^{k_3}\mathcal{S}|\psi\rangle = F^{L,\dagger}\Pi_1X^{k_3}\mathcal{S}|\psi\rangle + F^{L,\dagger}\Pi_2X^{k_3}\mathcal{S}|\psi\rangle.$$

By the triangle inequality, it suffices to the bound the norm of each term.

Bounding $F^{L,\dagger}\Pi_1\mathcal{S}|\psi\rangle$. Recall Lemma 4.35. For any (y,L_1,R_1,L_2,R_2), define the set

$$\mathcal{P}_{y,L_1,R_1,L_2,R_2} := \{(\mathbf{k},\mathbf{z})\colon y\in\mathrm{Im}(L_1^{(k_1,k_3)}\cup L_{2,\mathsf{source}}^{(k_2,\vec{z}_L)})\}.$$

By respectively sampling k_3 and $\vec{z}_L$ at the end and the union bound, it is clear that $\mathcal{P}_{y,L_1,R_1,L_2,R_2}$ occupies at most a $2t/N$ fraction of its universe. Thus, we obtain

$$\begin{aligned}\|F^{L,\dagger}\Pi_1\mathcal{S}|\psi\rangle\|_2 &\le \|F^{L,\dagger}\Pi_1\mathcal{S}^{\bullet}|\psi\rangle\|_2 + \|F^{L,\dagger}\Pi_1(\mathcal{S}-\mathcal{S}^{\bullet})|\psi\rangle\|_2\\ &\le \|\Pi_1\mathcal{S}^{\bullet}|\psi\rangle\|_2 + \|(\mathcal{S}^{\bullet}-\mathcal{S})\Pi_{\le t}\|_{\mathrm{op}}\\ &\le O(\sqrt{t/N}).\end{aligned}$$

The first term is zero by the definitions of $\{\mathcal{P}_\tau\}_\tau$ and $\mathcal{S}^{\bullet}$. The second term is bounded by Lemma 4.35

Bounding $F^{L,\dagger}\Pi_2\mathcal{S}|\psi\rangle$. Using Equation (4), we obtain

$$\begin{aligned}&F^{L,\dagger}\Pi_2\mathcal{S}|\psi\rangle\\ &= \sum_{\substack{b,L_1,L_2,R_1,R_2,\\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2}{R_1,R_2}\\ (x,y)\in L_{2,\mathsf{target}}^{(k_2,\vec{z}_L)}}} \frac{\alpha_{y,b,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+4}}}|x\rangle_{\mathsf{A}}|b\rangle_{\mathsf{B}}|L_1^{(k_1,k_3)}\cup L_2^{(k_2,\vec{z}_L)}\setminus\{(x,y)\}\rangle_{\mathsf{S}}|R_1^{(k_1,k_3)}\cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}}|\mathbf{k}\rangle_{\mathsf{K}}.\end{aligned}$$

By substituting $L_2 = L_2' \cup \{(x', y)\}$ and $x = z_{L,i} \oplus k_2$, where i is the index such that $y \in_i \mathrm{Im}(L_2') \cup \{y\}$, we obtain

$$\sum_{\substack{b,L_1,L_2',R_1,R_2 \\ x',y\notin\mathrm{Im}(L_2') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2'\cup\{(x,y)\}}{R_1,R_2} \\ i \text{ s.t. } y\in_i\mathrm{Im}(L_2')\cup\{y\}}} \frac{\alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2}}{\sqrt{N^{(|L_2'|+1)+|R_2|+4}}} |z_{L,i} \oplus k_2\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}}$$
$$\otimes |L_1^{(k_1,k_3)} \cup (L_2' \cup \{(x', y)\})^{(k_2,\vec{z}_L)} \setminus \{(z_{L,i} \oplus k_2, y)\}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}}.$$

By Lemma 4.20, the state is in the domain of the partial isometry $\mathcal{D}$. Thus, by Equation (16), we can instead calculate the norm of the following state:

$$\overset{\mathcal{D}}{\mapsto} \sum_{\substack{b,L_1,L_2',R_1,R_2 \\ x',y\notin\mathrm{Im}(L_2') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2'\cup\{(x,y)\}}{R_1,R_2} \\ i \text{ s.t. } y\in_i\mathrm{Im}(L_2')\cup\{y\}}} \frac{\alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2}}{\sqrt{N^{|L_2'|+|R_2|+5}}} |z_{L,i} \oplus k_2\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}}$$
$$\otimes |L_1 \cup \{(x' \oplus k_1, z_{L,i} \oplus k_3)\}\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2'\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{z}_{L,-i}\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |\mathbf{k}\rangle_{\mathsf{K}}.$$

We now apply the following sequence of partial isometries to simply the expression without changing the norm:

$$\xmapsto{F^L_{\mathsf{extract}} \cdot X^{k_3} \cdot X^{k_2}}$$
$$\sum_{\substack{b,L_1,L_2',R_1,R_2 \\ x',y\notin\mathrm{Im}(L_2') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2'\cup\{(x,y)\}}{R_1,R_2} \\ i \text{ s.t. } y\in_i\mathrm{Im}(L_2')\cup\{y\}}} \frac{\alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2}}{\sqrt{N^{|L_2'|+|R_2|+5}}} |z_{L,i} \oplus k_3\rangle_{\mathsf{A}'} |x' \oplus k_1\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2'\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{z}_{L,-i}\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |\mathbf{k}\rangle_{\mathsf{K}}$$

$$\xmapsto{X^{k_3} \otimes X^{k_1}}$$
$$\sum_{\substack{b,L_1,L_2',R_1,R_2 \\ x',y\notin\mathrm{Im}(L_2') \\ (\mathbf{k},\mathbf{z})\in\mathsf{G}\binom{L_1,L_2'\cup\{(x,y)\}}{R_1,R_2} \\ i \text{ s.t. } y\in_i\mathrm{Im}(L_2')\cup\{y\}}} \frac{\alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2}}{\sqrt{N^{|L_2'|+|R_2|+5}}} |z_{L,i}\rangle_{\mathsf{A}'} |x'\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2'\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{z}_{L,-i}\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |\mathbf{k}\rangle_{\mathsf{K}}.$$

By substituting $\vec{q}_L = \vec{z}_{L,-i}$, $z = z_i$, and $\vec{z}_L = \vec{q}_L^{\,(i\leftarrow z)}$, we obtain

$$\sum_{\substack{b,L_1,L_2',R_1,R_2 \\ x',y\notin\mathrm{Im}(L_2') \\ i \text{ s.t. } y\in_i\mathrm{Im}(L_2')\cup\{y\} \\ \mathbf{k},\vec{q}_L\in[N]^{|L_2'|-1},\vec{z}_R,z\in[N]: \\ (\mathbf{k},\vec{q}_L^{\,(i\leftarrow z)},\vec{z}_R)\in\mathsf{G}\binom{L_1,L_2'\cup\{(x,y)\}}{R_1,R_2}}} \frac{\alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2}}{\sqrt{N^{|L_2'|+|R_2|+5}}} |z\rangle_{\mathsf{A}'} |x'\rangle_{\mathsf{A}} |b\rangle_{\mathsf{B}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2'\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{q}_L\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |\mathbf{k}\rangle_{\mathsf{K}}.$$

We may compute its squared norm:

$$\sum_{\substack{b,L_1,L_2',R_1,R_2,x' \\ \mathbf{k},\vec{q}_L\in[N]^{|L_2'|-1},\vec{z}_R,z\in[N]}} \frac{1}{N^{|L_2'|+|R_2|+5}} \cdot \left| \sum_{\substack{y\notin \mathrm{Im}(L_2'): \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2')\cup\{y\} \\ (\mathbf{k},\vec{q}_L^{(i\leftarrow z)},\vec{z}_R)\in \mathsf{G}\left(\substack{L_1,L_2'\cup\{(x,y)\} \\ R_1,R_2}\right)}} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

By Lemma 4.28, once $(L_1', L_2, R_1, R_2, x', \mathbf{k}, \vec{q}, \vec{z}_R, z)$ is fixed, there is either zero or at least $N - g(t)$ values of y that satisfy the condition, where $g(t) = O(t)$ is some function guaranteed by Lemma 4.28. Let BAD denote the set of tuples for which the latter case holds. We obtain

$$\sum_{b,(L_1,L_2',R_1,R_2,x',\mathbf{k},\vec{q}_L,\vec{z}_R,z)\in\mathsf{Bad}} \frac{1}{N^{|L_2'|+|R_2|+5}} \cdot \left| \sum_{\substack{y\notin \mathrm{Im}(L_2'): \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2')\cup\{y\} \\ (\mathbf{k},\vec{q}_L^{(i\leftarrow z)},\vec{z}_R)\in \mathsf{G}\left(\substack{L_1,L_2'\cup\{(x,y)\} \\ R_1,R_2}\right)}} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

Now, we make crucial use of the condition implied by the premise (Equation (49)) to obtain

$$\sum_{b,(L_1,L_2',R_1,R_2,x',\mathbf{k},\vec{q}_L,\vec{z}_R,z)\in\mathsf{Bad}} \frac{1}{N^{|L_2'|+|R_2|+5}} \cdot \left| - \sum_{\substack{y\notin \mathrm{Im}(L_2'): \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2')\cup\{y\} \\ (\mathbf{k},\vec{q}_L^{(i\leftarrow z)},\vec{z}_R)\notin \mathsf{G}\left(\substack{L_1,L_2'\cup\{(x,y)\} \\ R_1,R_2}\right)}} \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

Using the Cauchy-Schwarz inequality and the definition of BAD to bound the number of y in the sum, we can bound it by

$$\sum_{\substack{b,(L_1,L_2',R_1,R_2,x',\mathbf{k},\vec{q}_L,\vec{z}_R,z)\in\mathsf{Bad}, y\notin \mathrm{Im}(L_2'): \\ i \text{ s.t. } y\in_i \mathrm{Im}(L_2')\cup\{y\} \\ (\mathbf{k},\vec{q}_L^{(i\leftarrow z)},\vec{z}_R)\notin \mathsf{G}\left(\substack{L_1,L_2'\cup\{(x,y)\} \\ R_1,R_2}\right)}} \frac{g(t)}{N^{|L_2'|+|R_2|+5}} \cdot \left| \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

Since we are summing over non-negative terms, by relaxing the constraints, we can bound it by

$$\sum_{b,L_1,L_2',R_1,R_2,x',\mathbf{k},\vec{q}_L,\vec{z}_R,z),y\notin \mathrm{Im}(L_2')} \frac{g(t)}{N^{|L_2'|+|R_2|+5}} \cdot \left| \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

By summing over $(\mathbf{k}, \vec{q}_L, \vec{z}_R, z)$, and noting that there are at most $N^{|L_2'|+|R_2|+4}$ such tuples, we can bounded it by

$$\sum_{b,x',L_1,L_2',R_1,R_2,y\notin \mathrm{Im}(L_2')} \frac{g(t)}{N} \cdot \left| \alpha_{y,b,L_1,R_1,L_2'\cup\{(x',y)\},R_2} \right|^2 .$$

By substituting $L = L_2' \cup \{(x', y)\}$, we obtain

$$\frac{g(t)}{N} \cdot \sum_{b,L_1,L_2,R_1,R_2,y\in\mathrm{Im}(L_2)} \left|\alpha_{y,b,L_1,R_1,L_2,R_2}\right|^2 = O(t/N)$$

by the normalization condition of $|\psi\rangle$.

□

Lemma 7.3 (Closeness of $F_2^{L,\dagger}$ and $F_2^{R,\dagger}$)**.** *For any integer $t \geq 0$,*

$$\begin{aligned} &\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N}) \\ &\|(F^{R,\dagger}X^{k_2}F^{R,\dagger}\mathcal{S} - \mathcal{S}F_2^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N}). \end{aligned}$$

Proof. Let $\Pi^{\mathrm{Im}(F_2^L)}$ denote the projection onto the image of F_2^L. For an arbitrary state $|\psi\rangle$ in the subspace of $\Pi_{\leq t}$, we can decompose it as

$$|\psi\rangle = \Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle + (\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)})|\psi\rangle.$$

We will show the following two bounds

$$\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle\|_2 \leq O(\sqrt{t/N}) \tag{50}$$

$$\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})(\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)})|\psi\rangle\|_2 \leq O(\sqrt{t/N}). \tag{51}$$

which then complete the proof by the triangle inequality. Notice that $F_2^{L,\dagger}(\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)}) = 0$. Thus, Equation (51) can be bounded as follows:

$$\begin{aligned} &\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})(\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)})|\psi\rangle\|_2 \\ =&\|F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S}(\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)})|\psi\rangle\|_2 \\ \leq&\|F^{L,\dagger}\mathcal{S}(\mathrm{id} - \Pi^{\mathrm{Im}(F_2^L)})|\psi\rangle\|_2 && \text{(by Lemma 3.3)} \\ \leq&O(\sqrt{t/N}). && \text{(by Lemma 7.2)} \end{aligned}$$

Hence, it suffices to bound Equation (50). Since $\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle$ is in the image of F_2^L, there exists some state $|\phi\rangle$ such that $\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle = F_2^L|\phi\rangle$. Now. we bound Equation (50) by the triangle inequality as follows:

$$\begin{aligned} &\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle\|_2 \\ =&\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^{L,\dagger})F_2^L|\phi\rangle\|_2 \\ \leq&\|(F^{L,\dagger}X^{k_2}F^{L,\dagger}\mathcal{S}F_2^L - F^{L,\dagger}X^{k_2}F^{L,\dagger}F^LX^{k_2}F^L\mathcal{S})|\phi\rangle\|_2 && (52) \\ &\qquad + \|(F^{L,\dagger}X^{k_2}F^{L,\dagger}F^LX^{k_2}F^L\mathcal{S} - \mathcal{S}F_2^{L,\dagger}F_2^L)|\phi\rangle\|_2. && (53) \end{aligned}$$

We use Lemma 7.1 and that operator norm is submultiplicative to bound Equation (52). Finally, we use Lemma 3.10 to bound Equation (53) by replacing $F^{L,\dagger}F^L$ and $F_2^{L,\dagger}F_2^L$ with the identity. This completes the proof. □

We need the following corollaries for the next subsection. The structure of the proof is similar to that of Lemma 7.3. We sketch the proof below and omit the details.

Corollary 7.4 (Closeness of $F_2^L F_2^{L,\dagger}$ and $F_2^R F_2^{R,\dagger}$)**.** *For any integer $t \geq 0$,*

$$\|(F^L F^{L,\dagger}\mathcal{S} - \mathcal{S}F_2^L F_2^{L,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N}) \quad \textit{and} \quad \|(F^R F^{R,\dagger}\mathcal{S} - \mathcal{S}F_2^R F_2^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = O(\sqrt{t/N}).$$

Proof sketch. Let $\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle = F_2^L|\phi\rangle$. We will show that

$$F^L F^{L,\dagger}\mathcal{S}\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle \approx \mathcal{S}F_2^L F_2^{L,\dagger}\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle.$$

For the left-hand side, consider the following sequence of hybrids:

$$\begin{aligned}
&F^L F^{L,\dagger}\mathcal{S}\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle \\
=&F^L F^{L,\dagger}\mathcal{S}F_2^L|\phi\rangle \\
\approx&F^L F^{L,\dagger}F^L X^{k_2}F^L\mathcal{S}|\phi\rangle && (\mathcal{S}F_2^L \approx F^L X^{k_2} F^L \mathcal{S} \text{ by Lemma 7.1}) \\
\approx&F^L X^{k_2}F^L\mathcal{S}|\phi\rangle. && (F_2^{L,\dagger}F_2^L \approx \mathrm{id} \text{ by Lemma 3.10})
\end{aligned}$$

For the right-hand side, consider the following sequence of hybrids:

$$\begin{aligned}
&\mathcal{S}F_2^L F_2^{L,\dagger}\Pi^{\mathrm{Im}(F_2^L)}|\psi\rangle \\
=&\mathcal{S}F_2^L F_2^{L,\dagger}F_2^L|\phi\rangle \\
\approx&\mathcal{S}F_2^L|\phi\rangle && (F_2^{L,\dagger}F_2^L \approx \mathrm{id} \text{ by Lemma 3.10}) \\
\approx&F^L X^{k_2}F^L\mathcal{S}|\phi\rangle. && (\mathcal{S}F_2^L \approx F^L X^{k_2} F^L \mathcal{S} \text{ by Lemma 7.1})
\end{aligned}$$

This completes the proof. □

7.3 Putting Things Together

We use the above lemmas to prove Lemma 4.38. We restate Lemma 4.38 for convenience.

Lemma 7.5 (Lemma 4.38, restated)**.** *For any integer $t \geq 0$,*

- **Forward query:** $\|(FX^{k_2}F\mathcal{S} - \mathcal{S}F_2)\Pi_{\leq t}\|_{\mathrm{op}} \leq O(t/\sqrt{N})$,
- **Inverse query:** $\|(F^\dagger X^{k_2}F^\dagger\mathcal{S} - \mathcal{S}F_2^\dagger)\Pi_{\leq t}\|_{\mathrm{op}} \leq O(t/\sqrt{N})$.

Proof of Lemma 4.38.
Forward query:. Recall the definition of F_2:

$$\begin{aligned}
F_2 &= F_2^L \cdot (\mathrm{id} - F_2^R \cdot F_2^{R,\dagger}) + (\mathrm{id} - F_2^L \cdot F_2^{L,\dagger}) \cdot F_2^{R,\dagger} \\
&= F_2^L - F_2^L \cdot F_2^R \cdot F_2^{R,\dagger} + F_2^{R,\dagger} - F_2^L \cdot F_2^{L,\dagger} \cdot F_2^{R,\dagger}.
\end{aligned} \tag{54}$$

We expand $FX^{k_2}F$ in the following way:

$$F \cdot X^{k_2} \cdot F$$

$$
\begin{aligned}
&= \Big(F^L + \underbrace{(\mathrm{id} - F^L \cdot F^R - F^L \cdot F^{L,\dagger}) \cdot F^{R,\dagger}}_{A}\Big) \cdot X^{k_2} \cdot \Big(F^{R,\dagger} + \underbrace{F^L \cdot (\mathrm{id} - F^{R,\dagger} \cdot F^R - F^{L,\dagger} \cdot F^{R,\dagger})}_{B}\Big) \\
&= F^L X^{k_2} F^{R,\dagger} + F^L X^{k_2} B + A X^{k_2} F^{R,\dagger} + AB.
\end{aligned}
$$

Here, the term AB can be viewed as a negligibly small error. Since there is $F^{R,\dagger} X^{k_2} F^L$ in the middle of AB, its operator norm is at most $O(t/\sqrt{N})$ by Lemma 3.12. Thus, it suffices to show the closeness of the remaining terms. We expand and arrange them in the following way:

$$
\begin{aligned}
& F^L X^{k_2} F^{R,\dagger} + F^L X^{k_2} B + A X^{k_2} F^{R,\dagger} \\
=& F^L X^{k_2} F^L - F^L X^{k_2} F^L F^R F^{R,\dagger} + F^{R,\dagger} X^{k_2} F^{R,\dagger} - F^L F^{L,\dagger} F^{R,\dagger} X^{k_2} F^{R,\dagger} \\
& \qquad - F^L X^{k_2} F^L F^{L,\dagger} F^{R,\dagger} + F^L (\mathrm{id} - F^R F^{R,\dagger}) X^{k_2} F^{R,\dagger}.
\end{aligned}
$$

In what follows, we will show each term in the second line is negligibly close to a corresponding term in Equation (54) in operator norm, and both terms in the third line have negligibly small operator norms. Concretely, we have the following claims, which together imply the lemma:

1. $\|(F^L X^{k_2} F^L \mathcal{S} - \mathcal{S} F_2^L)\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$
2. $\|(F^L X^{k_2} F^L F^R F^{R,\dagger} \mathcal{S} - \mathcal{S} F_2^L F_2^R F_2^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$
3. $\|(F^{R,\dagger} X^{k_2} F^{R,\dagger} \mathcal{S} - \mathcal{S} F_2^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$
4. $\|(F^L F^{L,\dagger} F^{R,\dagger} X^{k_2} F^{R,\dagger} \mathcal{S} - \mathcal{S} F_2^L F_2^{L,\dagger} F_2^{R,\dagger})\Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$
5. $\|F^L X^{k_2} F^L F^{L,\dagger} F^{R,\dagger} \mathcal{S} \Pi_{\le t}\|_{\mathrm{op}} \le O(t/\sqrt{N})$
6. $\|F^L (\mathrm{id} - F^R F^{R,\dagger}) X^{k_2} F^{R,\dagger} \mathcal{S} \Pi_{\le t}\|_{\mathrm{op}} \le O(\sqrt{t/N})$

Items 1 and 3 immediately follow from Lemmas 7.1 and 7.3, respectively. To prove Item 2, we use the following sequence of hybrids to sketch the proof:

$$
\begin{aligned}
& F^L X^{k_2} F^L F^R F^{R,\dagger} \mathcal{S} \\
\approx & F^L X^{k_2} F^L \mathcal{S} F_2^R F_2^{R,\dagger} && (F^L F^R F^{R,\dagger} \mathcal{S} \approx \mathcal{S} F_2^R F_2^{R,\dagger} \text{ by Corollary 7.4}) \\
\approx & \mathcal{S} F_2^L F_2^R F_2^{R,\dagger}. && (F^L X^{k_2} F^L \mathcal{S} \approx \mathcal{S} F_2^L \text{ by Lemma 7.1})
\end{aligned}
$$

Item 4 can be proven in a similar way using Lemma 7.3 and Corollary 7.4. To prove Item 5, we use a similar idea as in the proof of Lemma 7.3. Suppose $\Pi^{\mathrm{Im}(F_2^R)}|\psi\rangle = F_2^R|\phi\rangle$. We can bound it as follows:

$$
\begin{aligned}
& \|F^L X^{k_2} F^L F^{L,\dagger} F^{R,\dagger} \mathcal{S} \Pi^{\mathrm{Im}(F_2^R)} |\psi\rangle\|_2 \\
=& \|F^L X^{k_2} F^L F^{L,\dagger} F^{R,\dagger} \mathcal{S} F_2^R |\phi\rangle\|_2 \\
\le& \|F^L X^{k_2} F^L F^{L,\dagger} F^{R,\dagger} F^R X^{k_2} F^R \mathcal{S} |\phi\rangle\|_2 + O(\sqrt{t/N}) && (\mathcal{S} F_2^R \approx F^R X^{k_2} F^R \text{ by Lemma 7.1}) \\
\le& \|F^L X^{k_2} F^L F^{L,\dagger} X^{k_2} F^R \mathcal{S} |\phi\rangle\|_2 + O(\sqrt{t/N}) && (F^{R,\dagger} F^R \approx \mathrm{id} \text{ by Lemma 3.10}) \\
\le& \|F^{L,\dagger} X^{k_2} F^R\|_{\mathrm{op}} + O(\sqrt{t/N}) && (\text{by Lemma 3.3}) \\
\le& O(t/\sqrt{N}). && (\text{by Lemma 3.12})
\end{aligned}
$$

To prove Item 6, we use the same decomposition on $|\psi\rangle$ and obtain:

$$\begin{aligned}
&\|F^L(\mathrm{id} - F^R F^{R,\dagger}) X^{k_2} F^{R,\dagger} \mathcal{S} \Pi^{\mathrm{Im}(F_2^R)} |\psi\rangle\|_2 \\
=&\|F^L(\mathrm{id} - F^R F^{R,\dagger}) X^{k_2} F^{R,\dagger} \mathcal{S} F_2^R |\phi\rangle\|_2 \\
\le&\|F^L(\mathrm{id} - F^R F^{R,\dagger}) X^{k_2} F^{R,\dagger} F^R X^{k_2} F^R \mathcal{S} |\phi\rangle\|_2 + O(\sqrt{t/N}) && (\mathcal{S}F_2^R \approx F^R X^{k_2} F^R \text{ by Lemma 7.1}) \\
\le&\|F^L(\mathrm{id} - F^R F^{R,\dagger}) F^R \mathcal{S} |\phi\rangle\|_2 + O(\sqrt{t/N}) && (F^{R,\dagger} F^R \approx \mathrm{id} \text{ by Lemma 3.10}) \\
\le&O(\sqrt{t/N}). && (F^{R,\dagger} F^R \approx \mathrm{id} \text{ by Lemma 3.10})
\end{aligned}$$

This completes the proof. □

Acknowledgments

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

References

[ABF+24] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh V. Vazirani, Chenyi Zhang, and Zixin Zhou. "Quantum Pseudoentanglement". In: *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA*. Ed. by Venkatesan Guruswami. Vol. 287. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024, 2:1–2:21. DOI: 10.4230/LIPICS.ITCS.2024.2. URL: https://doi.org/10.4230/LIPIcs.ITCS.2024.2 (cit. on p. 3).

[ABGL25a] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. *Gluing Random Unitaries with Inverses*. In submission to QIP 2025. 2025 (cit. on p. 1).

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

[ABGL25c] Prabhanjan Ananth, John Bostanci, Aditya Gulati, and Yao-Ting Lin. "Pseudorandomness in the (inverseless) haar random oracle model". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2025, pp. 138–166 (cit. on pp. 3, 4, 6, 8, 16, 19, 20).

[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 pp. 3–5).

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. "Cryptography in the common haar state model: feasibility results and separations". In: *Theory of Cryptography Conference*. Springer. 2024, pp. 94–125 (cit. on pp. 5, 6).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. "Cryptography from pseudorandom quantum states". In: *Annual International Cryptology Conference*. Springer. 2022, pp. 208–236 (cit. on p. 4).

[BCN25] John Bostanci, Boyang Chen, and Barak Nehoran. “Oracle separation between quantum commitments and quantum one-wayness”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2025, pp. 3–22 (cit. on p. 6).

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. “Random oracles in a quantum world”. In: *Advances in Cryptology–ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings 17*. Springer. 2011, pp. 41–69 (cit. on p. 5).

[BFNV19] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. “On the complexity and verification of quantum random circuit sampling”. In: *Nature Physics* 15.2 (2019), pp. 159–163 (cit. on p. 4).

[BFV20] Adam Bouland, Bill Fefferman, and Umesh V. Vazirani. “Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)”. In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*. Ed. by Thomas Vidick. Vol. 151. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 63:1–63:2. DOI: 10.4230/LIPIcs.ITCS.2020.63 (cit. on pp. 3, 6).

[BHHP25] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. “Efficient Quantum Pseudorandomness from Hamiltonian Phase States”. In: *TQC*. Vol. 350. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025, 9:1–9:18 (cit. on pp. 3, 5).

[BIS+18] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven. “Characterizing quantum supremacy in near-term devices”. In: *Nature Physics* 14.6 (2018), pp. 595–600 (cit. on p. 4).

[BM24] Zvika Brakerski and Nir Magrafta. “Real-valued somewhat-pseudorandom unitaries”. In: *Theory of Cryptography Conference*. Springer. 2024, pp. 36–59 (cit. on p. 5).

[BMM+25] Amit Behera, Giulio Malavolta, Tomoyuki Morimae, Tamer Mour, and Takashi Yamakawa. “A new world in the depths of microcrypt: Separating OWSGs and quantum money from QEFID”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2025, pp. 23–52 (cit. on p. 6).

[CCS24] Boyang Chen, Andrea Coladangelo, and Or Sattath. “The power of a single Haar random state: constructing and separating quantum pseudorandomness”. In: *arXiv preprint arXiv:2404.03295* (2024) (cit. on pp. 5, 6).

[CDX+24] Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, Fernando G. S. L. Brandão, and Patrick Hayden. “Efficient Unitary Designs from Random Sums and Permutations”. In: *FOCS*. IEEE, 2024, pp. 476–484 (cit. on p. 5).

[CM24] Lijie Chen and Ramis Movassagh. “Quantum merkle trees”. In: *Quantum* 8 (2024), p. 1380 (cit. on pp. 3, 6).

[CMS19] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. “Succinct arguments in the quantum random oracle model”. In: *Theory of Cryptography Conference*. Springer. 2019, pp. 1–29 (cit. on pp. 9, 34).

[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 pp. 9, 34).

[Eat17] Edward Eaton. *Leighton-Micali Hash-Based Signatures in the Quantum Random-Oracle Model*. Cryptology ePrint Archive, Paper 2017/607. 2017. URL: https://eprint.iacr.org/2017/607 (cit. on p. 5).

[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. 4).

[HY24] Minki Hhan and Shogo Yamada. “Pseudorandom Function-like States from Common Haar Unitary”. In: *arXiv preprint arXiv:2411.03201* (2024) (cit. on pp. 3, 4, 6).

[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, 5, 12).

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. “Quantum cryptography in algorithmica”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1589–1602 (cit. on p. 3).

[Kre21] William Kretschmer. “Quantum Pseudorandomness and Classical Complexity”. In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*. Ed. by Min-Hsiu Hsieh. Vol. 197. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 2:1–2:20. DOI: 10.4230/LIPIcs.TQC.2021.2 (cit. on pp. 3, 6).

[LQS+24] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. “Quantum pseudorandom scramblers”. In: *Theory of Cryptography Conference*. Springer. 2024, pp. 3–35 (cit. on pp. 3, 5).

[LV24] Romi Levy and Thomas Vidick. “PRS Length Expansion”. In: *arXiv:2411.03215* (2024) (cit. on p. 4).

[MH25] Fermi Ma and Hsin-Yuan Huang. “How to construct random unitaries”. In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. 2025, pp. 806–809 (cit. on pp. 3, 5–7, 10, 13, 14, 59, 60, 63).

[MNY24] Tomoyuki Morimae, Barak Nehoran, and Takashi Yamakawa. “Unconditionally secure commitments with quantum auxiliary inputs”. In: *Annual International Cryptology Conference*. Springer. 2024, pp. 59–92 (cit. on p. 5).

[Mov19] Ramis Movassagh. “Quantum supremacy and random circuits”. In: *arXiv preprint arXiv:1909.06210* (2019) (cit. on p. 4).

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. "Simple constructions of linear-depth t-designs and pseudorandom unitaries". In: *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2024, pp. 485–492 (cit. on pp. 3, 5).

[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. 11).

[Qia24] Luowen Qian. "Unconditionally secure quantum commitments with preprocessing". In: *Annual International Cryptology Conference*. Springer. 2024, pp. 38–58 (cit. on p. 5).

[SHH25] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. "Random unitaries in extremely low depth". In: *Science* 389.6755 (2025), pp. 92–96 (cit. on p. 5).

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. "Post-quantum security of the Fujisaki-Okamoto and OAEP transforms". In: *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II 14*. Springer. 2016, pp. 192–216 (cit. on p. 5).

[Zha15a] Mark Zhandry. "A note on the quantum collision and set equality problems". In: *Quantum Information & Computation* 15.7-8 (2015), pp. 557–567 (cit. on p. 5).

[Zha15b] Mark Zhandry. "Secure identity-based encryption in the quantum random oracle model". In: *International Journal of Quantum Information* 13.04 (2015), p. 1550014 (cit. on p. 5).

[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 pp. 5, 9).

A Path-Recording with Independent Left and Right Operators

For the strong path-recording isometry defined in [MH25], the left (resp. right) isometry V^L (resp. V^R) outputs strings y (resp. x) that are in in the image (resp. domain) of *both* the left and right relation states in the purifying register. In our case, however, it will be easier to work with a similar pair of isometries that only look at their own relation state, as opposed to both relations taken together. In this section we define a pair of new isometries, F^L and F^R that are independent of each other.

A.1 Closeness to the Path-Recording Isometries

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

$$\|(V^L - F^L)\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}} \quad \textit{and} \quad \|(V^R - F^R)\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}}.$$

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

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

where $\alpha_{x,L,R} = 0$ whenever $|L|$ or $|R| > t$. Then we expand out

$$V^L|\psi\rangle_{\mathsf{AST}} = \sum_{x,L,R} \frac{\alpha_{x,L,R}}{\sqrt{N - |\operatorname{Im}(L \cup R)|}} \sum_{y \notin \operatorname{Im}(L\cup R)} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{S}} |R\rangle_{\mathsf{T}}, \text{ and}$$

$$F^L|\psi\rangle_{\mathsf{AST}} = \sum_{x,L,R} \frac{\alpha_{x,L,R}}{\sqrt{N}} \sum_{y \notin \operatorname{Im}(L)} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{S}} |R\rangle_{\mathsf{T}}.$$

Subtracting,

$$\begin{aligned}
&(V^L - F^L)|\psi\rangle_{\mathsf{AST}} \\
&\quad = \underbrace{\sum_{x,L,R} \alpha_{x,L,R} \sum_{y \notin \operatorname{Im}(L\cup R)} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{S}} |R\rangle_{\mathsf{T}} \left(\frac{1}{\sqrt{N - |\operatorname{Im}(L \cup R)|}} - \frac{1}{\sqrt{N}} \right)}_{|v\rangle} \\
&\quad + \underbrace{\sum_{x,L,R} \alpha_{x,L,R} \sum_{y \in \operatorname{Im}(R) \setminus \operatorname{Im}(L)} |y\rangle_{\mathsf{A}} |L \cup \{(x,y)\}\rangle_{\mathsf{S}} |R\rangle_{\mathsf{T}} \left(-\frac{1}{\sqrt{N}} \right)}_{|w\rangle}.
\end{aligned}$$

Note that $|w\rangle$ and $|v\rangle$ are orthogonal, since $|v\rangle$ is a superposition of states $|y\rangle|L'\rangle|R\rangle$ where y appears exactly once in $\operatorname{Im}(L')$ and does not appear in $\operatorname{Im}(R)$, while $|w\rangle$ is a superposition of states $|y\rangle|L'\rangle|R\rangle$ where y appears exactly once in both $\operatorname{Im}(L')$ and $\operatorname{Im}(R)$. Thus,

$$\left\| (V^L - F^L)|\psi\rangle \right\|_2^2 = \langle v|v\rangle + \langle w|w\rangle.$$

Bounding $\langle v|v\rangle$. Similar to [MH25], by changing the order of summation, we can rewrite $|v\rangle$ as

$$|v\rangle = \sum_{y,L',R} |y\rangle|L'\rangle|R\rangle \left(\sum_{\substack{(x,L): \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{Im}(L\cup R)}} \alpha_{x,L,R} \left(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}} \right) \right),$$

and thus

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

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

$$\begin{aligned} \sum_{\substack{(x,L): \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{Im}(L\cup R)}} \left(\frac{1}{\sqrt{N-|\mathrm{Im}(L\cup R)|}} - \frac{1}{\sqrt{N}} \right)^2 &= \sum_{\substack{(x,L): \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{Im}(L\cup R)}} \left(\frac{\sqrt{N} - \sqrt{N-|\mathrm{Im}(L\cup R)|}}{\sqrt{N(N-|\mathrm{Im}(L\cup R)|)}} \right)^2 \\ &\le \sum_{\substack{(x,L): \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{Im}(L\cup R)}} \left(\frac{\sqrt{|\mathrm{Im}(L\cup R)|}}{\sqrt{N(N-|\mathrm{Im}(L\cup R)|)}} \right)^2 \\ &\qquad \text{(since } \sqrt{a}-\sqrt{b} \le \sqrt{a-b} \text{ when } a \ge b \ge 0) \\ &= \sum_{\substack{(x,L): \\ L'=L\cup\{(x,y)\}, \\ y\notin \mathrm{Im}(L\cup R)}} \frac{|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)} \\ &\le \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)} \end{aligned}$$

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,

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

$$= \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N(N-|\mathrm{Im}(L\cup R)|)}\cdot\sum_{x,L,R}|\alpha_{x,L,R}|^2\cdot\left(\sum_{y\in[N]}\mathbb{1}(y\notin\mathrm{Im}(L\cup R))\right)$$
$$\leq \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N}\cdot\sum_{x,L,R}|\alpha_{x,L,R}|^2 = \frac{(|L|+1)\cdot|\mathrm{Im}(L\cup R)|}{N}.$$

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

$$|w\rangle = \frac{-1}{\sqrt{N}}\sum_{y,(L',R)}|y\rangle|L'\rangle|R\rangle \sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\}\\ y\in\mathrm{Im}(L\cup R)\setminus\mathrm{Im}(L)}}\alpha_{x,L,R}$$

Then

$$\langle w|w\rangle = \frac{1}{N}\sum_{y,(L',R)}\left|\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\}\\ y\in\mathrm{Im}(L\cup R)\setminus\mathrm{Im}(L)}}\alpha_{x,L,R}\right|^2 \leq \frac{1}{N}\sum_{y,(L',R)}\sum_{\substack{(x,L):\\ L'=L\cup\{(x,y)\}\\ y\in\mathrm{Im}(L\cup R)\setminus\mathrm{Im}(L)}}|\alpha_{x,L,R}|^2$$
$$= \frac{1}{N}\sum_{x,L,R}|\alpha_{x,L,R}|^2\left(\sum_{y\in\mathrm{Im}(L\cup R)\setminus\mathrm{Im}(L)}1\right) \leq \frac{t}{N}\sum_{x,L,R}|\alpha_{x,L,R}|^2 = \frac{t}{N}$$

Hence, it holds that

$$\|(V^L - F^L)\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}}.$$

By a symmetric argument, we have

$$\|(V^R - F^R)\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}}.$$ □

We have the following corollaries.

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

$$\|(V^{L,\dagger} - F^{L,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}} \quad \textit{and} \quad \|(V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}}.$$

Proof. Using the fact that $\|A\|_{\mathrm{op}} = \|A^\dagger\|_{\mathrm{op}}$ for any operator A, we have

$$\|(V^{L,\dagger} - F^{L,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} = \|\Pi_{\leq t}(V^L - F^L)\|_{\mathrm{op}}.$$

Next, since applying V^L and F^L only increase the size of each relation on the register S by one, we have

$$\Pi_{\leq t}(V^L - F^L) = (V^L - F^L)\Pi_{\leq t-1}.$$

Finally, the desired bound then follows from Lemma A.1. The second bound follows by the same argument. □

Finally, we have:

Lemma A.3. *For any integer $t \geq 0$,*

$$\|(V-F)\Pi_{\leq t}\|_{\mathrm{op}} \leq 8 \cdot \sqrt{\frac{(t+2)(t+4)}{N}}.$$

Proof. Recall the definitions

$$V = V^L \cdot (\mathrm{id} - V^R \cdot V^{R,\dagger}) + (\mathrm{id} - V^L \cdot V^{L,\dagger}) \cdot V^{R,\dagger} \quad \text{and} \quad F = F^L \cdot (\mathrm{id} - F^R \cdot F^{R,\dagger}) + (\mathrm{id} - F^L \cdot F^{L,\dagger}) \cdot F^{R,\dagger}.$$

By the triangle inequality and the above expression, we have

$$\begin{aligned}
&\|(V-F)\Pi_{\leq t}\|_{\mathrm{op}} \\
&\quad \leq \left\|(V^L - F^L)\Pi_{\leq t}\right\|_{\mathrm{op}} + \left\|(V^L V^R V^{R,\dagger} - F^L F^R F^{R,\dagger})\Pi_{\leq t}\right\|_{\mathrm{op}} \\
&\qquad + \left\|(V^L V^{L,\dagger} V^{R,\dagger} - F^L F^{L,\dagger} F^{R,\dagger})\Pi_{\leq t}\right\|_{\mathrm{op}} + \left\|(V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\right\|_{\mathrm{op}}.
\end{aligned}$$

We will bound each term in the rest of the proof. From Lemma A.1 and Corollary A.2, we can bound the first term and the last term by

$$\|(V^L - F^L)\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}} \quad \text{and} \quad \|(V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{\frac{t(t+2)}{N}}.$$

Next, by the triangle inequality, we can bound the second term by

$$\begin{aligned}
&\|(V^L V^R V^{R,\dagger} - F^L F^R F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \\
&\leq \|(V^L V^R V^{R,\dagger} - F^L V^R V^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} + \|(F^L V^R V^{R,\dagger} - F^L F^R V^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} + \|(F^L F^R V^{R,\dagger} - F^L F^R F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \\
&= \|(V^L - F^L) V^R V^{R,\dagger}\Pi_{\leq t}\|_{\mathrm{op}} + \|F^L (V^R - F^R) F^R V^{R,\dagger}\Pi_{\leq t}\|_{\mathrm{op}} + \|F^L F^R (V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}}.
\end{aligned}$$

Since applying V^R and F^R can increase the size of the relation by at most one, while applying $V_R^\dagger$ and $F_R^\dagger$ never increases it, we can bound the above sum as follows:

$$\begin{aligned}
&\leq \|(V^L - F^L)\Pi_{\leq t+1} V^R V^{R,\dagger}\Pi_{\leq t}\|_{\mathrm{op}} \\
&\qquad + \|F^L \Pi_{\leq t+2} (V^R - F^R)\Pi_{\leq t+1} F^R \Pi_{\leq t} V^{R,\dagger}\Pi_{\leq t}\|_{\mathrm{op}} \\
&\qquad\qquad + \|F^L \Pi_{\leq t+2} F^R \Pi_{\leq t+1} (V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \\
&\leq \|(V^L - F^L)\Pi_{\leq t+1}\|_{\mathrm{op}} \\
&\qquad + \|F^L \Pi_{\leq t+2}\|_{\mathrm{op}} \cdot \|(V^R - F^R)\Pi_{\leq t+1}\|_{\mathrm{op}} \cdot \|F^L \Pi_{\leq t}\|_{\mathrm{op}} \\
&\qquad\qquad + \|F^L \Pi_{\leq t+2}\|_{\mathrm{op}} \cdot \|F^R \Pi_{\leq t+1}\|_{\mathrm{op}} \cdot \|(V^{R,\dagger} - F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \\
&\hspace{20em} \text{(by submultiplicity of operator norm)} \\
&\leq 3 \cdot \sqrt{\frac{(t+2)(t+4)}{N}}.
\end{aligned}$$

(by Lemma A.1, Corollary A.2 and the fact that F^L and F^R are contractions)

Similarly, we can bound the third term by

$$\|(V^L V^{L,\dagger} V^{R,\dagger} - F^L F^{L,\dagger} F^{R,\dagger})\Pi_{\leq t}\|_{\mathrm{op}} \leq 3 \cdot \sqrt{\frac{(t+2)(t+4)}{N}}.$$

Collecting the bounds, we have

$$\|(V-F)\Pi_{\le t}\|_{\text{op}} \le 8 \cdot \sqrt{\frac{(t+2)(t+4)}{N}}$$

as desired. □

Using a symmetric argument, we also have:

Lemma A.4. *For any integer $t \ge 0$,*

$$\|(V^\dagger - F^\dagger)\Pi_{\le t}\|_{\text{op}} \le 8 \cdot \sqrt{\frac{(t+2)(t+4)}{N}}.$$

Lemma A.5. *For any adversary $\mathcal{A}$ that makes t forward queries and t inverse queries,*

$$\left\| |\mathcal{A}^{F,F^\dagger}\rangle_{\mathsf{ABST}} - |\mathcal{A}^{V,V^\dagger}\rangle_{\mathsf{ABST}} \right\|_2 = O\left(\sqrt{\frac{t^4}{N}}\right).$$

Proof. The lemma follows from Lemmas A.3 and A.4 and a sequence of hybrids that replace query to F with V one-by-one. □

A.2 Missing Proofs in Section 3.4

Lemma A.6 (Lemma 3.10, restated)**.** *For any integer $t \ge 0$,*

$$\|(F^{L,\dagger}F^L - \mathrm{id})\Pi_{\le t}\| \le t/N \quad \textit{and} \quad \|(F^{R,\dagger}F^R - \mathrm{id})\Pi_{\le t}\| \le t/N$$

Proof. For any $x, y \in [N], L \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R \in \mathcal{R}^{\mathcal{D}\text{-dist}}$ such that $|L| + |R| \le t$, from Equations (4) and (5), we have

$$F^{L,\dagger} \cdot F^L \cdot |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}} = \frac{N-|L|}{N} \cdot |x\rangle_{\mathsf{A}}|L\rangle_{\mathsf{S}} \quad \text{and} \quad F^{R,\dagger} \cdot F^R \cdot |y\rangle_{\mathsf{A}}|R\rangle_{\mathsf{T}} = \frac{N-|R|}{N} \cdot |y\rangle_{\mathsf{A}}|R\rangle_{\mathsf{T}}.$$

Therefore, by Lemma 3.3, we have

$$\|(F^{L,\dagger}F^L - \mathrm{id})\Pi_{\le t}\| = \max_{x, L \in \mathcal{R}^{\mathcal{I}\text{-dist}}_{\le t}} \frac{|L|}{N} = \frac{t}{N}.$$

The second bound follows from the same argument. □

We require the following fact, which is a consequence of [MH25, Definition 37, Claim 22, Equations (11.22) and (11.26)].

Fact A.7. *There exist operators E^L and E^R that satisfy*

- *For any $t \ge 0$, it holds that*

$$\|(V^L - E^L)\Pi_{\le t}\|_{\text{op}} \le \sqrt{t(t+2)/N} \quad \textit{and} \quad \|(V^R - E^R)\Pi_{\le t}\|_{\text{op}} \le \sqrt{t(t+2)/N}.$$

- *For any $\ell, r \geq 0$ such that $\ell + r \leq N$, it holds that*

$$E^L_{\ell,r} \cdot E^{L,\dagger}_{\ell,r} = \sum_{i \in [\ell+1]} \left(\Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \cdot \Pi_{\ell+1,\mathsf{S}} \right) \otimes \Pi_{r,\mathsf{T}}, \quad \textit{and}$$

$$E^R_{\ell,r} \cdot E^{R,\dagger}_{\ell,r} = \sum_{i \in [r+1]} \Pi_{\ell,\mathsf{S}} \otimes \left(\Pi_{r+1,\mathsf{T}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{T}^{(r+1)}_{\mathsf{X},i}} \cdot \Pi_{r+1,\mathsf{T}} \right).$$

The operators E^L and E^R satisfy the following property.

Lemma A.8. *For any integer $t \geq 0$ and any unitary U acting non-trivially on the register* A,

$$\|E^{L,\dagger} U E^R \Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{t(t+1)}/N \quad \textit{and} \quad \|E^{R,\dagger} U E^L \Pi_{\leq t}\|_{\mathrm{op}} \leq \sqrt{t(t+1)}/N\,.$$

Proof. By Lemma 3.4, we have

$$\|E^{R,\dagger} U E^L \Pi_{\leq t}\|^2_{\mathrm{op}} = \max_{0 \leq \ell, r \leq t} \|E^{R,\dagger}_{\ell+1,r-1} U E^L_{\ell,r}\|^2_{\mathrm{op}}. \tag{55}$$

We next bound the squared operator norm in the following. Using the fact $\|A\|^2_{\mathrm{op}} = \|AA^\dagger\|_{\mathrm{op}} = \|A^\dagger A\|_{\mathrm{op}}$, we have

$$\begin{aligned} (55) &= \max_{0 \leq \ell, r \leq t} \|E^{R,\dagger}_{\ell+1,r-1} U E^L_{\ell,r} \cdot E^{L,\dagger}_{\ell,r} U^\dagger E^R_{\ell+1,r}\|_{\mathrm{op}} \\ &\leq \max_{0 \leq \ell, r \leq t} \sum_{i \in [\ell+1]} \left\| E^{R,\dagger}_{\ell+1,r-1} \cdot U \cdot \left(\Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \cdot \Pi_{\ell+1,\mathsf{S}} \right) \cdot U^\dagger \cdot E^R_{\ell+1,r-1} \right\|_{\mathrm{op}}. \end{aligned} \tag{56}$$

Since U only acts non-trivially on the register A, we simplify the notation as follows:

$$(56) = \max_{0 \leq \ell, r \leq t} \sum_{i \in [\ell+1]} \left\| E^{R,\dagger}_{\ell+1,r-1} \cdot U_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \cdot U^\dagger_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot E^R_{\ell+1,r-1} \right\|_{\mathrm{op}}. \tag{57}$$

Using the facts that $\|AA^\dagger\|_{\mathrm{op}} = \|A^\dagger A\|_{\mathrm{op}}$ and $\Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}}$ is a projector, we have

$$\begin{aligned} &(57) \\ &= \max_{0 \leq \ell, r \leq t} \sum_{i \in [\ell+1]} \left\| \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \cdot U^\dagger_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot E^R_{\ell+1,r-1} \cdot E^{R,\dagger}_{\ell+1,r-1} \cdot U_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \right\|_{\mathrm{op}} \\ &\leq \max_{0 \leq \ell, r \leq t} \sum_{\substack{i \in [\ell+1] \\ j \in [r]}} \left\| \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \cdot U^\dagger_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{T}^{(r)}_{\mathsf{X},j}} \cdot U_{\mathsf{A}} \otimes \Pi_{\ell+1,\mathsf{S}} \cdot \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \Pi_{r,\mathsf{T}} \right\|_{\mathrm{op}} \end{aligned} \tag{58}$$

Thus, we have

$$\begin{aligned} (58) &= \max_{0 \leq \ell, r \leq t} \sum_{\substack{i \in [\ell+1] \\ j \in [r]}} \frac{1}{N^2} \left\| \Pi^{\mathsf{EPR}}_{\mathsf{A},\mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \otimes \left(\Pi_{r,\mathsf{T}} \cdot U^\dagger_{\mathsf{T}^{(r)}_{\mathsf{X},j}} \cdot \Pi_{\ell+1,\mathsf{T}^{(r)}_{\mathsf{X},j},\mathsf{S} \setminus \mathsf{S}^{(\ell+1)}_{\mathsf{Y},i}} \cdot U_{\mathsf{T}^{(r)}_{\mathsf{X},j}} \cdot \Pi_{r,\mathsf{T}} \right) \right\|_{\mathrm{op}} \\ &\leq \max_{0 \leq \ell, r \leq t} \frac{(\ell+1)r}{N^2} = \frac{(t+1)t}{N^2}. \end{aligned}$$

This completes the proof. □

Lemma A.9 (Lemma 3.12, restated)**.** *For any integer $t \geq 0$ and any unitary U acting non-trivially on the register A,*

$$\|F^{L,\dagger} U F^{R} \Pi_{\leq t}\|_{\mathrm{op}} \leq 3\sqrt{t(t+2)/N} \quad \textit{and} \quad \|F^{R,\dagger} U F^{L} \Pi_{\leq t}\|_{\mathrm{op}} \leq 3\sqrt{t(t+2)/N}\,.$$

Proof. It immediately follows from Lemmas A.1 and A.8 and fact A.7 together with the triangle inequality. □

Lemma A.10 (Lemma 4.35, restated)**.** *Let $\{\mathcal{P}_\tau\}_\tau$ be collection of sets where the index τ ranges over $(y \in [N], L_1 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_1 \in \mathcal{R}^{\mathcal{D}\text{-dist}}, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}})$ and $\mathcal{P}_\tau \subseteq [N]^3 \times [N]^{|L_2|} \times [N]^{|R_2|}$. Define the operator*

$$\begin{aligned}\mathcal{S}^\bullet \colon & |y\rangle_{\mathsf{A}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} \\ & \mapsto |y\rangle_{\mathsf{A}} \frac{1}{\sqrt{N^{|L_2|+|R_2|+3}}} \sum_{\substack{(\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2} : \\ (\mathbf{k},\mathbf{z}) \notin \mathcal{P}_{y,L_1,R_1,L_2,R_2}}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |k\rangle_{\mathsf{K}}.\end{aligned}$$

If there exists $\delta \geq 0$ such that for any τ,

$$\frac{\left|\mathcal{P}_{y,L_1,R_1,L_2,R_2} \cap \mathsf{G}\binom{L_1,L_2}{R_1,R_2}\right|}{N^{|L_2|+|R_2|+3}} \leq \delta,$$

then

$$\|\mathcal{S}^\bullet - \mathcal{S}\|_{\mathrm{op}} = \sqrt{\delta}.$$

Proof. For any normalized state $|\psi\rangle = \sum_{y,L_1,R_1,L_2,R_2} \alpha_{y,L_1,R_1,L_2,R_2} |y\rangle_{\mathsf{A}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2}$, we have

$$\|(\mathcal{S}^\bullet - \mathcal{S})|\psi\rangle\|_2 = \left\| \sum_{\substack{y,L_1,R_1,L_2,R_2 \\ (\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2} : \\ (\mathbf{k},\mathbf{z}) \in \mathcal{P}_{y,L_1,R_1,L_2,R_2}}} \frac{\alpha_{y,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+3}}} |y\rangle_{\mathsf{A}} |L_1^{(k_1,k_3)} \cup L_2^{(k_2,\vec{z}_L)}\rangle_{\mathsf{S}} |R_1^{(k_1,k_3)} \cup R_2^{(k_2,\vec{z}_R)}\rangle_{\mathsf{T}} |\mathbf{k}\rangle_{\mathsf{K}} \right\|_2.$$

By Lemma 4.20, we can instead apply $\mathcal{D}$ to the state and bound its squared norm as follows:

$$\begin{aligned}& \left\| \sum_{\substack{y,L_1,R_1,L_2,R_2 \\ (\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2} : \\ (\mathbf{k},\mathbf{z}) \in \mathcal{P}_{y,L_1,R_1,L_2,R_2}}} \frac{\alpha_{y,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+3}}} |y\rangle_{\mathsf{A}} |L_1\rangle_{\mathsf{S}_1} |R_1\rangle_{\mathsf{T}_1} |L_2\rangle_{\mathsf{S}_2} |R_2\rangle_{\mathsf{T}_2} |\vec{z}_L\rangle_{\mathsf{Z}_\mathsf{L}} |\vec{z}_R\rangle_{\mathsf{Z}_\mathsf{R}} |\mathbf{k}\rangle_{\mathsf{K}} \right\|_2^2 \\ & = \sum_{y,L_1,R_1,L_2,R_2} \sum_{\substack{(\mathbf{k},\mathbf{z}) \in \mathsf{G}\binom{L_1,L_2}{R_1,R_2} : \\ (\mathbf{k},\mathbf{z}) \in \mathcal{P}_{y,L_1,R_1,L_2,R_2}}} \left| \frac{\alpha_{y,L_1,R_1,L_2,R_2}}{\sqrt{N^{|L_2|+|R_2|+3}}} \right|^2 \\ & = \sum_{y,L_1,R_1,L_2,R_2} |\alpha_{y,L_1,R_1,L_2,R_2}|^2 \cdot \frac{\left|\mathcal{P}_{y,L_1,R_1,L_2,R_2} \cap \mathsf{G}\binom{L_1,L_2}{R_1,R_2}\right|}{N^{|L_2|+|R_2|+3}}\end{aligned}$$

$$\le \max_{y,L_1,R_1,L_2,R_2} \frac{\left|\mathcal{P}_{y,L_1,R_1,L_2,R_2} \cap \mathsf{G}\binom{L_1,L_2}{R_1,R_2}\right|}{N^{|L_2|+|R_2|+3}}$$
$$\le \delta. \qquad \square$$

B Missing Proofs in Section 4

B.1 Proof of Lemma 4.20

Lemma B.1 (Lemma 4.20, restated)**.** *For any $L_1, L_2 \in \mathcal{R}^{\mathcal{I}\text{-dist}}$, $R_1, R_2 \in \mathcal{R}^{\mathcal{D}\text{-dist}}$, every tuple in $\mathsf{G}\binom{L_1,L_2}{R_1,R_2}$ satisfies all conditions in Lemma 4.18 and is therefore robustly decodable.*

Proof of Lemma 4.20. Recall Definition 4.19. For convenience, we color the conditions according to the properties they enforce in the following definition: distinctness, disjointness, and no extra k_2-correlated pairs.

1. $k_1 \notin \left(\mathrm{Dom}(L_1) \oplus \mathrm{Dom}(L_2)\right) \cup \left(\mathrm{Dom}(R_1) \oplus \mathrm{Dom}(R_2)\right)$
2. $k_2 \notin \left(\left(\left(\mathrm{Dom}(L_1) \oplus k_1\right) \cup \mathrm{Dom}(L_2)\right) \oplus \left(\left(\mathrm{Im}(L_1) \oplus k_3\right) \cup \mathrm{Im}(L_2)\right)\right)$
$\cup \left(\left(\left(\mathrm{Dom}(R_1) \oplus k_1\right) \cup \mathrm{Dom}(R_2)\right) \oplus \left(\left(\mathrm{Im}(R_1) \oplus k_3\right) \cup \mathrm{Im}(R_2)\right)\right)$
3. $k_3 \notin \left(\mathrm{Im}(L_1) \oplus \mathrm{Im}(L_2)\right) \cup \left(\mathrm{Im}(R_1) \oplus \mathrm{Im}(R_2)\right)$
4. $\vec{z}_L \in [N]^{|L_2|}_{\mathrm{dist}}$ and $\vec{z}_R \in [N]^{|R_2|}_{\mathrm{dist}}$
5. $\{\vec{z}_L\}$ and $\left(\mathrm{Im}(L_1) \oplus k_3\right) \cup \mathrm{Im}(L_2) \cup \left(\left(\left(\mathrm{Dom}(L_1) \oplus k_1\right) \cup \mathrm{Dom}(L_2)\right) \oplus k_2\right)$ are disjoint.
6. $\{\vec{z}_R\}$ and $\left(\mathrm{Im}(R_1) \oplus k_3\right) \cup \mathrm{Im}(R_2) \cup \left(\left(\left(\mathrm{Dom}(R_1) \oplus k_1\right) \cup \mathrm{Dom}(R_2)\right) \oplus k_2\right)$ are disjoint.

Each condition can be verified directly. □