Quantum-Classical Tradeoffs in the Random Oracle Model

Yassine Hamoudi* Qipeng Liu† Makrand Sinha‡

Simons Institute and UC Berkeley

Last update: November 23, 2022

Abstract

We study tradeoffs between quantum and classical queries for hybrid algorithms that have black-box access to a random oracle. Although there are several established techniques for proving query lower bounds for both quantum and classical algorithms, there is no such widely applicable technique for hybrid algorithms and the optimal tradeoffs for many fundamental problems are still unknown — an optimal tradeoff for the search problem was only shown recently by Rosmanis [Ros22], although not in the random oracle model. For another fundamental problem, collision finding, the optimal tradeoff was not known.

In this work, we develop a framework for recording a query transcript for quantum-classical algorithms that represents the knowledge gained by the algorithm. The main feature of this framework is to allow us to record queries in two incompatible bases — classical queries in the standard basis and quantum queries in the Fourier basis — in a consistent way. We call the framework the *hybrid compressed oracle* as it naturally interpolates between the classical way of recording queries and the *compressed oracle* framework of Zhandry [Zha19] for recording quantum queries. We demonstrate its applicability by giving a simpler proof of the optimal quantum-classical tradeoff for search and by showing an optimal tradeoff for collision finding.

1 Introduction

A central question in quantum information theory is to understand the essence of quantum *speedups*. The quantum Fourier transform has, for instance, long been recognized as one of the jewels of quantum algorithm design [Sim97; BV97; Sho97; Kit95; BHMT02]. Another fundamental resource is the access to *quantum queries*, which is the ability to access in superposition the values of a black-box function [BW02]. This idealized input model gave rise to the early quantum algorithms by Deutsch and Jozsa [DJ92], Simon [Sim97] (paving the way for Shor's factoring algorithm [Sho97]), and Bernstein and Vazirani [BV97]. For certain problems (such as parity learning [BV97] or Forrelation [AA18]), a *single* quantum query turns out to be sufficient to outperform any classical query algorithm by an exponential factor. Yet, for other problems such as preimage search [Gro97] or collision finding [BHT98], the best-known algorithms make intensive use of superposition queries to speed up the computation. Could it be the case that a single or a few quantum queries (together with many classical ones) suffice for solving these problems with the same efficiency? While a negative answer has been given recently for preimage search by Rosmanis [Ros22], this question remains largely unaddressed by current lower-bound techniques. Furthermore, the quantum query complexity model assumes that one can make superposition

*ys.hamoudi@gmail.com. Supported by the Simons Institute and DOE NQISRC QSA grant #FP00010905.

†qipengliu0@gmail.com. Supported in part by the Simons Institute for the Theory of Computing, through a Quantum Postdoctoral Fellowship, by the DARPA SIEVE-VESPA grant Np.HR00112020023 and by the NSF QLCI program through grant number OMA-2016245.

‡makrand@berkeley.edu. Supported by a Simons-Berkeley Postdoctoral Fellowship.

queries to the entire input. This may not translate to some practical scenarios, for instance, if some parts of the input cannot be accessed in superposition or only at a prohibitive cost. Could this model be amended to make it more realistic and amenable to near-term applications, while still obtaining quantum speedups?

This paper addresses some aspects of the above-mentioned questions through the scope of *quantum-classical query tradeoffs*. We investigate the limitations of an idealized quantum computer equipped with two query interfaces: one providing superposition access to the input, the other being only classical. Our main contribution is the design of a new lower-bound framework that captures the progress made towards solving a problem when the numbers of available quantum and classical queries are bounded. Our construction is an extension of the compressed oracle technique of Zhandry [Zha19]. In the second part of our paper, we illustrate the power of this framework by solving the open question raised in [Ros22] on the optimal quantum-classical tradeoffs for the *collision finding* problem. We further motivate the study of the hybrid quantum-classical query model by listing below four scenarios where it shows its relevance.

Post-Quantum Cryptography. The advent of quantum computation has led to rethinking the security of well-established cryptographic schemes. Boneh et al. [BDF+11] advocated that a quantum attacker shall be able to evaluate (pseudo)random functions in superposition, presuming, for instance, that it gets access to their code. While this model (known as the Quantum Random Oracle Model, or QROM) provides a high level of security, it is sometimes unrealistic to assume that a full quantum query interface is exposed to the attacker [HS18; BHN+19]. A potentially weaker access model is the hybrid model where, given a random function or permutation f and a private key K, quantum access is granted to the unkeyed primitive f but only classical access to the keyed one $f(K,.)$. Few security proofs have been established in this setting [JST21; ABKM22; ABK+22]. The hybrid compressed oracle described in our work can help analyze such a scenario.

Quantum Resource Estimates. In concrete applications, the resource estimates of a black-box algorithm (such as Grover's search [Gro97] or BHT collision finding [BHT98]) have to take into account the cost of implementing each query. Oftentimes, significant overheads are expected for simulating quantum queries compared to classical ones. This is the case, for instance, when applying Grover's algorithm to AES key recovery [GLRS16; JNRV20] or preimage attacks on SHA-2 and SHA-3 [ADG+17]. Hence, faster implementations would result from the discovery of algorithms that use fewer quantum queries without increasing the number of classical queries much. Our work limits the possibility of finding such algorithms (in the Hybrid Random Oracle Model) for the preimage search and collision finding problems.

Bounded Quantum Depth. The accumulation of decoherence effects in near-term quantum computers requires limiting the depth of computation. While this may not be an obstacle to implementing the quantum Fourier transform [CW00] for instance, certain oracular problems have been shown recently to require a large quantum depth [CCL20; CM20; AGS22; HG22; CH22]. Some of these results are stated in the so-called "QC model", where a d-depth quantum circuit is interleaved with layers of polynomial-time classical computation. This model is akin to small-depth *measurement-based quantum computation*, where measurement outcomes are classically processed to select subsequent quantum gates. It is also encompassed by our hybrid quantum-classical query model when the number of quantum queries is bounded by d.

Hybrid Lower-Bound Techniques. A long-term goal in complexity theory is finding lower-bound techniques that characterize the *tradeoffs* between the number of queries and other computational resources. This is particularly relevant in scenarios where the query complexity may not be the most prohibitive constraint. For instance, prior works have studied the interplay between quantum queries and memory space [KŠW07; AŠW09; HM21], circuit depth [SZ19; CCL20; CM20; AGS22; HG22; CH22], parallel computation [Zal99; GR04; JMW17; AHU19; CFHL21; BLZ21], proof size [Aar12; ST19; AKKT20], advice size [NABT15; HXY19; CLQ20; CGLQ20; GLLZ21], among others. These results are often tailored to the problems at hand and do not provide general lower-bound frameworks. In particular, the complexity of collision finding is notoriously open in most of these models [Aar12; HM21]. The techniques deployed in our work may shed light on other set-ups where the computational resources are partly classical.

1.1 Related work

The study of quantum query complexity is dominated by two lower-bound techniques: the polynomial [BBC+01] and the adversary [Amb02] methods. The compressed oracle technique, recently introduced by Zhandry [Zha19], led to new and simpler lower bounds for certain search problems (e.g. [LZ19a; HM21; Ros21]) and security proofs in post-quantum cryptography (e.g. [HI19; LZ19b; CMS19; CMSZ19; BHH+19; AMRS20]). While the classical counterparts of these methods are often easy to manipulate, it is generally unknown how to adapt them to the hybrid setting. Indeed, the only prior works concerning the hybrid quantum-classical query model, that we are aware of, are tailor-made to some specific problems. Notably, Rosmanis [Ros22] characterized the optimal success probability of solving the preimage search problem, using techniques inspired by a lower bound from Regev and Schiff [RS08] for quantum faulty oracles, although the proof is not in the random oracle model.

Another recent line of work [JST21; ABKM22; ABK+22] studied the post-quantum security of the Even-Mansour and FX constructions when the attacker has quantum access to the underlying block cipher and classical access to the keyed primitive. These results are based on new "reprogramming" lemmas for analyzing the advantage of distinguishing between two oracles that differ in some specific way. Additionally, [JST21] introduced a variant of the compressed oracle for recording both classical and quantum queries *in the Fourier domain*. It allows the authors to argue that, for a variant of the FX construction, the classical and quantum queries can be (approximately) treated as acting on disjoint domains. This method seems nevertheless unadapted to the proof of more general hybrid results.

1.2 Contributions

We develop a new lower-bound framework, called the *hybrid compressed oracle*, for analyzing the success probability of hybrid algorithms that perform a mix of quantum and classical queries. We provide a high-level description of this framework below and present the main applications studied in our paper to illustrate its power.

Hybrid Compressed Oracle (Section 4). Our hybrid lower-bound framework departs from a recent method introduced by Zhandry [Zha19], called the *compressed oracle* (see Section 2.1), that quantizes the classical *lazy sampling* technique. These methods aim to record a *query transcript* representing the knowledge gained by an algorithm (the "attacker") on the input. Unless classically, the recording of quantum queries is a blurry task to define due to the no-cloning theorem and the superposition input access. Some important features of Zhandry's solution to these problems are the construction of a quantum query transcript in the Fourier domain, and the ability for the attacker to erase the transcript (for instance, by running its algorithm in reverse). We extend this construction to support recording both classical and quantum queries. This is not as easy as it may seem since it requires merging two recordings on distinct bases (the standard and the Fourier basis). Our solution relies on replacing the original classical and query operators with two "recording query operators" (Section 4.1) that maintain a consistent classical-quantum query transcript throughout the execution of the algorithm (Proposition 4.4). In the extreme cases where all the queries are classical or quantum, our framework recovers the classical lazy sampling and the quantum compressed oracle techniques, respectively. Moreover, as in previous work, our hybrid recording is undetectable by an attacker (Proposition 4.2); therefore, it perfectly simulates a hybrid random oracle and completely preserves an attacker's behavior. A more detailed technical overview of this framework is provided in Section 2.2.

Preimage Search (Section 5). Our first application concerns the problem of finding a preimage[1] $x \in [M]$ satisfying $F(x) = 0$ given a uniformly random function $F : [M] \to [N]$. The optimal success probability for solving this problem is $\Theta(c/N)$ with c classical queries, or $\Theta(q^2/N)$ with q quantum queries by using Grover's algorithm [Gro97]. Rosmanis [Ros22], using a proof tailored to the search problem, showed that no hybrid algorithm can interpolate between these two cases efficiently. Here, we give a simpler proof of the same result using the hybrid compressed oracle framework.

Theorem 5.1 (Informal)**.** *The optimal success probability of a hybrid algorithm making q quantum and c classical queries for solving the Preimage Search problem is $\Theta((c + q^2)/N)$.*

The proof relies on a simple application of our hybrid compressed oracle framework, where the progress made towards finding a preimage is represented as the probability of measuring a classical-quantum query transcript containing such a preimage. The central argument in our analysis, that allows us to overcome the $O((c + q)^2/N)$ upper bound derived from the original compressed oracle, is a refinement of certain triangle inequalities when a classical query is made.

Collision Finding (Section 6). Our second application concerns the problem of finding a pair of elements $x \neq y \in [M]$ that evaluate to the same value $F(x) = F(y)$, given a uniformly random function $F : [M] \to [N]$. The optimal success probability for solving this problem is $\Theta(c^2/N)$ with c classical queries (by the birthday paradox), or $\Theta(q^3/N)$ with q quantum queries (the lower bound is using the BHT algorithm [BHT98], while the upper bound on the success probability follows from the compressed oracle method in [Zha19][2]).

Unlike preimage search, here we show that the optimal hybrid strategy does not always consist of running the optimal classical and quantum algorithms separately. This resolves an open question posed in [Ros22].

Theorem 6.1 (Informal)**.** *The optimal success probability of a hybrid algorithm making q quantum and c classical queries for solving the Collision Finding problem is $\Theta((c^2 + cq^2 + q^3)/N)$. There is a matching hybrid algorithm that achieves asymptotically the same success probability.*

The upper bound is proven using our hybrid compressed oracle framework. Our bound is tight because of the following variant of the BHT algorithm: the first $c + q/2$ queries are classical[3] and are used to collect distinct $(x, F(x))$ pairs. The rest of the $q/2$ queries are then used to run Grover's search algorithm to find a collision.

The proof of the upper bound above is significantly more involved than for the preimage search problem. It requires introducing the concepts of "quantum", "classical", and "hybrid" collisions, depending on whether the two elements of a colliding pair (x, y) are recorded in the quantum transcript, the classical transcript, or split between the two. This requires several measures of progress in the analysis to track what types of collisions are being recorded.

[1] Here we write $[m]$ to denote the set $\{0, 1, \ldots, m - 1\}$ for $m \in \mathbb{N}$.

[2] We also note that a lower bound on the query complexity was already established in earlier works [AS04; Zha15]

[3] The first $q/2$ quantum queries are also used to make classical queries.

2 Technical Overview

2.1 Overview of the Compressed Oracle

Here we give a detailed overview of the compressed oracle framework [Zha19]. As mentioned before, this framework gives an information-theoretic method that is useful in proving lower bounds against quantum algorithms that get black-box query access to a uniformly random function $F : [M] \to [N]$. The framework allows one to store a compressed encoding of the uniformly random function conditioned on the knowledge gained from the queries.

To illustrate the framework, we first consider the case of classical and quantum algorithms separately and then discuss the ideas involved in extending the framework to the setting of hybrid algorithms. For pedagogical reasons, we shall primarily focus on the preimage search problem as a running example and use D (instead of F) to denote a uniformly random function henceforth.

Classical Algorithms. Let us first consider classical query algorithms for the search problem. After c classical queries at most c entries of the uniformly random function D can be assumed to be fixed, since the entries that have not been queried are still uniformly random in $[N]$. This observation allows one to model the random function D as being generated by *lazy sampling*: we may think of a location $x \in [M]$ that has not been queried to be marked with a special symbol $\perp$ and whenever that location is queried for the first time, $D(x)$ is replaced with a uniformly random value in $[N]$. In other words, after c queries, we store a compressed encoding of D where only c locations are fixed, and others are compressed to a special symbol $\perp$. Whenever a query is made to a location that is still compressed, it is uncompressed and replaced by a uniformly random value. It follows that if after c queries we have not seen a zero preimage, then the probability of seeing a zero preimage in the next query is $1/N$. Thus the probability of success after t queries, denoted p_t, satisfies $p_{t+1} \leq p_t + 1/N$ and is bounded by c/N after c queries.

Quantum Algorithms. The compressed oracle framework quantizes the lazy sampling idea and allows one to define a compressed encoding of a random function that works well with quantum queries. Unlike the classical case, quantum information can not be cloned and could be forgotten, so some care needs to be taken in defining this compressed encoding. Consider a quantum algorithm that has an index register $\mathcal{X}$, a phase register $\mathcal{P}$, a workspace register $\mathcal{W}$ and has black-box access to a uniformly random function D via the following phase[4] unitary:

$$\mathcal{O}_D^Q : |x, p, w\rangle \mapsto \omega_N^{pD(x)} |x, p, w\rangle \quad \text{where} \quad \omega_N = e^{\frac{2i\pi}{N}}.$$

A quantum algorithm starts with the all-zero state $|0, 0, 0\rangle$ and applies arbitrary unitaries interleaved with phase queries. For a fixed $D : [M] \to [N]$, the state of the algorithm at any point is some arbitrary state $|\psi_D\rangle$. After averaging over uniformly random D, the state is the mixed state $\mathbb{E}_D[|\psi_D\rangle\langle\psi_D|]$ and it will be more convenient for us to work with a purification of this state. We add a purification register $\mathcal{D} = \mathcal{D}_0 \cdots \mathcal{D}_{M-1}$ where the subregister $\mathcal{D}_x$ for $x \in [M]$ holds a value $D(x) \in [N]$ and we refer to it as the database register. Then, the state

$$\frac{1}{N^{M/2}} \sum_{D \in [N]^M} |\psi_D\rangle \otimes |D\rangle_{\mathcal{D}}$$

is a purification, as after tracing out $\mathcal{D}$ we obtain the same mixed state as before. Note that in the above encoding, the database register is never altered during the run of the algorithm.

[4] Note that the value of $D(x)$ is returned in the phase of the complex state and p is an additional control register. This kind of query is usually called a *phase query* in the literature. There is another standard way of defining a quantum query by a unitary that maps $|x, p, w\rangle$ to $|x, p \oplus D(x), w\rangle$. The two kinds of queries are equivalent up to a unitary transformation, and we focus on phase queries as they work better with our framework.

Motivated by the classical case, we would like to have a compressed encoding of the random function D. For this, we extend the range of D to allow for a compressed symbol $\perp$ and define compression and uncompression operations that act on the database register $\mathcal{D}$ whenever a query is made. In particular, let $D : [M] \to \{\perp\} \cup [N]$ and extend the register $\mathcal{D}_x$ so that it can now also hold the value $\perp$. The initial state of the register $\mathcal{D}$ (at the beginning of the algorithm) is $|\perp, \ldots, \perp\rangle_{\mathcal{D}}$, which corresponds to a completely compressed database. We also define a unitary operation S which is controlled on the index register $\mathcal{X}$ and uncompresses an entry that is $\perp$: if the index register is $|x\rangle_{\mathcal{X}}$ and the database register is $|\perp\rangle_{\mathcal{D}_x}$, then it is mapped to $\frac{1}{\sqrt{N}} \sum_{y \in [N]} |y\rangle_{\mathcal{D}_x}$ while the compress operation $S^\dagger$ maps the last state back to $|\perp\rangle_{\mathcal{D}_x}$ (for details on how to unitarily implement this, see Section 4). Before a quantum query, the database is uncompressed by applying S and after the query it is compressed again by applying $S^\dagger$.

With the above framework, one can prove a lower bound for the preimage search problem against any quantum algorithm by following a similar template as in the classical case. In particular, the probability p_t of succeeding after t queries is essentially the *squared* norm of the projection of the state at time t onto the subspace spanned by databases $|D\rangle_{\mathcal{D}}$ that contain a zero preimage. One can show that the norm of this projection increases by at most $O(1/\sqrt{N})$ after each query and thus

$$\sqrt{p_{t+1}} \leq \sqrt{p_t} + O\left(\frac{1}{\sqrt{N}}\right) \implies p_q = O\left(\frac{q^2}{N}\right).$$

2.2 Overview of the Hybrid Compressed Oracle

One of the main contributions of this work is to extend the compressed oracle framework to the setting of hybrid algorithms which make both quantum and classical queries. Since a quantum query can always simulate a classical query, one could hope to analyze such algorithms using the compressed oracle framework for quantum algorithms above. However, it is not straightforward in such an analysis to capture that classical queries do not create additional interference. In fact, such attempts run into significant technical difficulties.

Here we start from first principles and define another purification compatible with both classical and quantum queries and that allows us to store a compressed encoding of the random function D conditioned on the queries made by the algorithm. There are two main principles behind the new purification that takes into account the classical nature of the queries:

Measurement Classical queries can be measured, so we add an additional history register $\mathcal{H}$ that records all the classical queries $(x, D(x))$. The contents of a recorded query in this register are never changed.

Consistency We define compression and uncompression operations for the database $\mathcal{D}$ conditioned on the history. In particular, under the standard compressed oracle framework $|y\rangle_{\mathcal{D}_x}$ can be changed during compression/uncompression if the index register contains $|x\rangle_{\mathcal{X}}$, which captures the fact that quantum algorithms could forget information. However, in the new purification, if $(x, D(x))$ is in the history, which happens if x has been queried classically, then the register $\mathcal{D}_x$ is never compressed or uncompressed again.

Lower Bound for Preimage search. With the above framework, we give an alternative lower-bound proof for the search problem against any hybrid algorithm. As remarked before, this was first shown by Rosmanis [Ros22] with a proof tailored for the search problem. Although there are some similarities between that approach and ours, the proof using the hybrid compressed oracle framework follows in a more principled way, is arguably simpler and works in the random oracle model.

To prove the lower bound, we again bound the probability p_t of succeeding after t queries. To do this, we now keep track of whether there is a zero preimage in the classical history or in the quantum database: let $|\phi\rangle$ be the current joint state of all registers, we define Π_{C} as the projector on the span of the basis state where the classical history $\mathcal{H}$ contains a zero preimage and $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}$ as the projector on those basis states where there is a zero preimage in the quantum database $\mathcal{D}$ but none in the history. The norms $\|\Pi_{\mathrm{C}}|\phi\rangle\|$ and $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$ can be considered the classical and quantum progress respectively.

We show that after a quantum query, the quantum progress $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$ increases by $O(1/\sqrt{N})$ as in the completely quantum case while the classical progress $\|\Pi_{\mathrm{C}}|\phi\rangle\|$ does not change. However, under a classical query, the classical progress could increase by a much larger amount, but only at the cost of decreasing the quantum progress. As an example, consider a hybrid algorithm that creates a superposition over all preimages of zero by performing Grover search, then measures its internal register to get a random preimage x and finally makes a classical query on x. Clearly, before the only classical query, we have $\|\Pi_{\mathrm{C}}|\phi\rangle\| = 0$ and $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \approx 1$ but right after the query, $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$ becomes almost zero whereas $\|\Pi_{\mathrm{C}}|\phi\rangle\| \approx 1$.

This phenomenon does not appear when the algorithm is purely classical or quantum. Nonetheless, upon doing a classical query, we show that the total progress defined as $\Psi_t = \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ increases by at most $O(1/N)$, behaving as in the classical case. Note that Ψ_t upper bounds the total probability of having a preimage in either the database or the classical history.

More precisely, let $|\phi'\rangle$ be the resulting quantum state after a classical query is made. Although $\|\Pi_{\mathrm{C}}|\phi'\rangle\|^2$ can be much larger that $\|\Pi_{\mathrm{C}}|\phi\rangle\|^2$, the state $\Pi_{\mathrm{C}}|\phi'\rangle$ consists of three parts:

1. $|\phi_1\rangle$: This corresponds to the basis states which already contained a zero preimage in their history register prior to the last classical query. The squared norm of this part can be bounded by $\|\Pi_{\mathrm{C}}|\phi\rangle\|^2$.

2. $|\phi_2\rangle$: This corresponds to the basis states where there was no zero preimage either in the history or the database (prior to the classical query) and the classical query sampled a new zero preimage. The squared norm of this term is roughly equal to at most $1/N$.

3. $|\phi_3\rangle$: The last part consists of the basis states where there was at least one zero preimage in the database but none in the history (prior to the classical query) and the classical query either sampled a new preimage or "moved" one from the quantum database to the classical history. We denote the squared norm of $|\phi_3\rangle$ by $\delta_{\mathrm{Q}\to\mathrm{C}}$ (denoting the amplitude that moved from $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}$ to Π_{C}). This exactly captures the scenario mentioned in the above example using Grover's search.

On a high level, we show that $\Pi_{\mathrm{C}}|\phi'\rangle = |\phi_1\rangle + |\phi_2\rangle + |\phi_3\rangle$ and $|\phi_1\rangle$ is also orthogonal to $|\phi_2\rangle$ and $|\phi_3\rangle$. Thus, we have that

$$\|\Pi_{\mathrm{C}}|\phi'\rangle\|^2 \;=\; \||\phi_1\rangle\|^2 + \||\phi_2\rangle + |\phi_3\rangle\|^2 \;\le\; \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 2\||\phi_2\rangle\|^2 + 2\||\phi_3\rangle\|^2.$$

The increase $\|\Pi_{\mathrm{C}}|\phi'\rangle\|^2 - \|\Pi_{\mathrm{C}}|\phi\rangle\|^2$ is then $O(\frac{1}{N}) + 2\delta_{\mathrm{Q}\to\mathrm{C}}$. On the other hand, $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ will decrease by $\delta_{\mathrm{Q}\to\mathrm{C}}$ due to a similar reason. Thus, we conclude that after a classical query, Ψ_t increases by at most $O(1/N)$. Combined with the fact that a quantum query increases $\sqrt{\Psi_t}$ by $O(1/\sqrt{N})$, this shows that the success probability after c classical and q quantum queries is $O\big(\frac{c+q^2}{N}\big)$.

Lower Bound for Collision Finding. The intuition behind the proof for the collision lower bound is similar to that for the search problem. However, the details are quite involved because of one crucial difference. For the preimage search problem, the preimage is either in the history $\mathcal{H}$ or only in the quantum database $\mathcal{D}$, allowing us to define classical and quantum measures of progress. For the collision finding problem, there could also be *hybrid collisions*, meaning a colliding pair (x, x') where x is in the history while x' is only in the database $\mathcal{D}$. This makes the proof substantially more involved, as one also needs to keep track of other progress measures for such hybrid collisions.

To prove the lower bound, we again bound the probability p_t of finding a collision after t queries. To do this, we now keep track of whether there is a classical, hybrid, or quantum collision. We define various projectors onto the span of basis states containing such collisions and use these as measures of classical, hybrid, or quantum progress.

Similar to the case of preimage search, a quantum query can only increase all these measures of progress by a small amount, but a classical query might increase some of them by a large amount while decreasing others at the same time. We are able to show how much amplitude is transferred onto the subspace spanned by basis states containing classical, hybrid or quantum collisions after making a quantum or classical query.

To be more precise, we define three projectors: $\Pi_{\mathrm{C}}, \Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, \Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$. The support of Π_{C} consists of the span of all basis states whose classical history contains a collision. We similarly define $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}$ for hybrid collisions only (no classical collisions) and $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$ for quantum collisions only (no hybrid or classical collisions). Similar to our discussion on preimage search, a classical query can move a large amplitude from $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}$ to Π_{C}, or from $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$ to $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}$. This is more complicated than the case of preimage search, as there is a hierarchy of three projectors, instead of two in the prior case — let $|\phi\rangle$ be the current state and let $\Delta_{\mathrm{C}}, \Delta_{\mathrm{H}\cdot\overline{\mathrm{C}}}, \Delta_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$ be the increment in the squared norms $\|\Pi_{\mathrm{C}}|\phi\rangle\|^2, \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2, \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ after a classical query is made. By a refinement of certain triangle inequalities, we show that:

$$\begin{aligned}
\Delta_{\mathrm{C}} &\leq 2\delta_{\mathrm{H}\to\mathrm{C}} + O\left(\frac{c}{N}\right),\\
\Delta_{\mathrm{H}\cdot\overline{\mathrm{C}}} &\leq -\delta_{\mathrm{H}\to\mathrm{C}} + 2\delta_{\mathrm{Q}\to\mathrm{H}} + O\left(\frac{q^2}{N}\right),\\
\Delta_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} &\leq -\delta_{\mathrm{Q}\to\mathrm{H}} + O\left(\frac{cq^4+\sqrt{cq^9}}{N^2}\right).
\end{aligned}$$

Using these facts, we prove that the following potential

$$\Psi_t := \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 4\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2,$$

which upper bounds the total progress always increases as follows: $\sqrt{\Psi_t} \leq \sqrt{\Psi_{t-1}} + O\Big(\sqrt{\frac{c+q}{N}}\Big)$ if the t-th query is quantum and $\Psi_t \leq \Psi_{t-1} + O\Big(\frac{c+q^2}{N} + \frac{cq^4+\sqrt{cq^9}}{N^2}\Big)$ if the t-th query is classical. Overall, this shows that the success probability of finding a collision after c classical and q quantum queries is at most $\Psi_{c+q} \leq O\Big(\frac{c^2+cq^2+q^3}{N}\Big)$.

3 Hybrid Random Oracle Model

Below we define a computational model that captures hybrid algorithms which make both classical and quantum queries to a random oracle. We also note that our model captures the QC model [CCL20], a generalized model for measurement-based quantum computation, as a special case.[5]

Memory. The memory of an algorithm accessing an oracle $D : [M] \to [N]$ is made of three quantum registers defined as follows:

- Index register $\mathcal{X}$ holding $x \in [M]$.

[5]In the QC model, there are $2q$ rounds of computation where in the even numbered rounds, c/q classical queries are made, and in the odd numbered round, one quantum query is made followed by a (possibly partial) measurement. The measurements can be deferred till the end using ancilla qubits.

- Phase register $\mathcal{P}$ holding $p \in [N]$.
- Workspace register $\mathcal{W}$ holding $w \in \{0,1\}^s$ where s is an (arbitrarily large) integer fixed in advance.

We represent a basis state in the corresponding Hilbert space as $|x,p,w\rangle_{\mathcal{A}}$, where $\mathcal{A}$ is a shorthand for the registers $\mathcal{XPW}$ on which the algorithm operates. The initial state of the memory is the all-zero basis state $|0,0,0\rangle_{\mathcal{A}}$.

Quantum Phase Oracle. We define the quantum oracle $\mathcal{O}_D^Q$ as the unitary operator acting on the memory of the algorithm as follows.

$$\mathcal{O}_D^Q : |x,p,w\rangle_{\mathcal{A}} \mapsto \omega_N^{pD(x)} |x,p,w\rangle_{\mathcal{A}} \quad \text{where} \quad \omega_N = e^{\frac{2i\pi}{N}}.$$

Note that this oracle returns the value $D(x)$ in the phase but it is equivalent to the standard oracle that maps $|x,p,w\rangle_{\mathcal{A}}$ to $|x,p \oplus D(x),w\rangle_{\mathcal{A}}$ up to a unitary transformation.

Classical Oracle. A classical oracle query is defined as a query to the standard oracle that maps $|x,p,w\rangle_{\mathcal{A}}$ to $|x,p \oplus D(x),w\rangle_{\mathcal{A}}$ followed by a measurement on the index register $\mathcal{X}$ and phase register $\mathcal{P}$. Since we are working with phase oracles for convenience, we define them in the following way, equivalent to the above up to a unitary transformation.

We add a *history* register $\mathcal{H} = \mathcal{H}_1 \cdots \mathcal{H}_c$ where the i-th subregister $\mathcal{H}_i$ is used to purify the i-th classical query (there are c classical queries in total) and stores a value in $([M] \times [N]) \cup \{\star\}$. The classical oracle $\mathcal{O}_D^C$ is defined as the unitary operator acting as follows

$$\begin{aligned} \mathcal{O}_D^C \quad : \quad & |x,p,w\rangle_{\mathcal{A}} |(x_1,y_1),\ldots,(x_i,y_i),\star,\ldots,\star\rangle_{\mathcal{H}} \\ \mapsto \quad & \omega_N^{pD(x)} |x,p,w\rangle_{\mathcal{A}} |(x_1,y_1),\ldots,(x_i,y_i),(x,D(x)),\star,\ldots,\star\rangle_{\mathcal{H}}. \end{aligned}$$

Since we only care about a bounded number of c classical queries, the above oracle can be easily made a unitary. For convenience, we denote the list $((x_1,y_1),\ldots,(x_i,y_i),\star,\ldots,\star)$ by H and we say $x \in H$ if and only if there exists $1 \leq j \leq i$ such that $x_j = x$. Let $\mathscr{H}$ be the set of all possible H. Sometimes, we will identify the above list with a function $H : [M] \to [N] \cup \{\star\}$ if there are no ambiguous pairs, i.e. no pairs of the form (x,y) and (x,y') where $y \neq y'$. The initial state of the history register is $|\star,\ldots,\star\rangle_{\mathcal{H}}$.

Hybrid Algorithm. An algorithm with q quantum and c classical queries is defined as a sequence $U_0,\ldots,U_{c+q}$ of unitary transformations acting on the memory register $\mathcal{A}$ and a function $\ell : \{1,\ldots,c+q\} \to \{C,Q\}$ with exactly q preimages of Q that specifies which queries are quantum versus classical. The state $|\psi_t^D\rangle$ of the algorithm after t queries is

$$|\psi_t^D\rangle = U_t \, \mathcal{O}_D^{\ell(t)} \, U_{t-1} \cdots U_1 \, \mathcal{O}_D^{\ell(1)} \, U_0 \left(|0\rangle_{\mathcal{A}} |\star,\ldots,\star\rangle_{\mathcal{H}}\right)$$

where the quantum phase oracle $\mathcal{O}_D^Q$ has been extended to act as the identity on $\mathcal{H}$. The oracle D is chosen uniformly at random from the set of functions $\{D : [M] \to [N]\}$. We model that by adding a purification register (the *database*) $\mathcal{D} = \mathcal{D}_0 \ldots \mathcal{D}_{M-1}$ where each subregister $\mathcal{D}_x$ for $x \in [M]$ holds a value $D(x) \in [N]$ and we define the following joint state,

$$|\psi_t\rangle = \frac{1}{N^{M/2}} \sum_{D \in [N]^M} |\psi_t^D\rangle_{\mathcal{AH}} \otimes |D\rangle_{\mathcal{D}} = U_t \, \mathcal{O}_D^{\ell(t)} \, U_{t-1} \cdots U_1 \, \mathcal{O}_D^{\ell(1)} \, U_0 \, |\psi_0\rangle, \tag{3.1}$$

where $|\psi_0\rangle := |0\rangle_{\mathcal{A}} \otimes |\star,\cdots,\star\rangle_{\mathcal{H}} \otimes \frac{1}{N^{M/2}} \sum_{D \in [N]^M} |D\rangle_{\mathcal{D}}$.

Output. The output of a hybrid algorithm is obtained by performing a computational basis measurement on the final state $|\psi_t\rangle$ where we measure a designated part of the workspace register $\mathcal{W}$. Since in this paper the output is always a tuple $(x_1, \ldots, x_k) \in [M]^k$ with $k \leq 2$, by making k extra classical queries, we may always assume that all the output indices $x_1, \ldots, x_k$ are in the history register at the end.

4 Hybrid Compressed Oracle

In this section, we define the hybrid compressed oracle framework and prove some of its main properties. We also describe general results for constructing and analyzing progress measures in this framework.

4.1 Construction

We start by defining the compressed encoding of the database that will be compatible with the history register. For this, we first augment the alphabet used for the database register such that $\mathcal{D}_x$ can now hold $D(x) \in \{\perp\} \cup [N]$ and with the convention that $\omega_N^{pD(x)} = 1$ if $D(x) = \perp$. The initial state of the database is defined to be $|\perp, \ldots, \perp\rangle_{\mathcal{D}}$. We also augment the alphabet of the history register so it can also store tuples of the form $(x, \perp)$ where $x \in [M]$. We say that $x \in H$ if there is a tuple of the form $(x, y) \in H$ where $y \in \{\perp\} \cup [N]$. Note that if there are no ambiguous pairs in the list, we can identify H as a function mapping $[M]$ to $\{\perp, \star\} \cup [N]$ with the extended alphabet (we will prove in Proposition 4.4 that such a property always holds in practice).

Next, we define the uncompression operator S. Let

$$|\hat{p}\rangle_{\mathcal{D}_x} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} \omega_N^{py} |y\rangle_{\mathcal{D}_x} \quad \text{for } p = 0, \ldots, N-1, \tag{4.1}$$

denote the Fourier basis states and let S_x be the unitary operator acting on $\mathcal{D}_x$ such that

$$S_x : \begin{cases} |\perp\rangle_{\mathcal{D}_x} & \longmapsto \; |\hat{0}\rangle_{\mathcal{D}_x} \\ |\hat{0}\rangle_{\mathcal{D}_x} & \longmapsto \; |\perp\rangle_{\mathcal{D}_x} \\ |\hat{p}\rangle_{\mathcal{D}_x} & \longmapsto \; |\hat{p}\rangle_{\mathcal{D}_x} \quad \text{for } p = 1, \ldots, N-1. \end{cases}$$

Note that $S_x = S_x^\dagger$. We now define a controlled unitary $S_{x,H}$ acting on $\mathcal{D}_x$ and $\mathcal{H}$:

$$S_{x,H} := \begin{cases} \mathbb{I} & \text{if } x \in H \\ S_x & \text{otherwise.} \end{cases} \tag{4.2}$$

Define the unitary operator S acting on $\mathcal{AHD}$ such that:

$$S = \sum_{x \in [M], H \in \mathscr{H}} |x\rangle\langle x|_{\mathcal{X}} \otimes \mathbb{I}_{\mathcal{PW}} \otimes |H\rangle\langle H|_{\mathcal{H}} \otimes (\mathbb{I}_{\mathcal{D}_0 \ldots \mathcal{D}_{x-1}} \otimes S_{x,H} \otimes \mathbb{I}_{\mathcal{D}_{x+1} \ldots \mathcal{D}_{M-1}}).$$

The quantum and classical compressed oracles $\mathcal{R}^Q$ and $\mathcal{R}^C$ are defined as follows,

$$\mathcal{R}^Q = S^\dagger \mathcal{O}^Q S \quad \text{and} \quad \mathcal{R}^C = S^\dagger \mathcal{O}^C S,$$

where we let $\mathcal{O}^Q := \sum_{D \in (\{\perp\} \cup [N])^M} \mathcal{O}_D^Q \otimes |D\rangle\langle D|_{\mathcal{D}}$ and $\mathcal{O}^C := \sum_{D \in (\{\perp\} \cup [N])^M} \mathcal{O}_C^Q \otimes |D\rangle\langle D|_{\mathcal{D}}$. The idea behind these definitions is that, for any basis state $|x, p, w\rangle_{\mathcal{A}} |H\rangle_{\mathcal{H}} |D\rangle_{\mathcal{D}}$:

- If the queried input satisfies $x \in H$, it means that x has been queried classically before; then we stop (un)compressing $\mathcal{D}_x$, and it behaves like a regular phase oracle on input x.

- Otherwise $x \notin H$, then $\mathcal{D}_x$ is simulated as a compressed oracle.

In particular, note that the quantum compressed oracle $\mathcal{R}^Q$ only acts on the register $\mathcal{H}$ as control. We provide an alternative definition to $\mathcal{R}^Q$ and $\mathcal{R}^C$ in Section 4.3 that makes these observations more formal. Finally, the joint state $|\phi_t\rangle$ of the algorithm and the oracle after t queries in the compressed oracle model is defined as

$$|\phi_t\rangle = U_t\, \mathcal{R}^{\ell(t)}\, U_{t-1} \cdots U_1\, \mathcal{R}^{\ell(1)}\, U_0\, (|0\rangle_{\mathcal{A}} |\star, \dots, \star\rangle_{\mathcal{H}} |\bot, \dots, \bot\rangle_{\mathcal{D}}). \tag{4.3}$$

Following from Equation (4.3), we define the initial state $|\phi_0\rangle = |0\rangle_{\mathcal{A}} \otimes |\star, \cdots, \star\rangle_{\mathcal{H}} \otimes |\bot, \dots, \bot\rangle_{\mathcal{D}}$.

4.2 Structural Properties

Indistinguishability. We show that the compression and uncompression operations behave as intended. For this, we will need some auxiliary definitions and lemmas. Let us define the unitary operator S_{all} that applies $S_{x,H}$ on every $\mathcal{D}_x$:

$$S_{\mathsf{all}} = \sum_{H \in \mathscr{H}} \mathbb{I}_{\mathcal{XPW}} \otimes |H\rangle\langle H|_{\mathcal{H}} \otimes (S_{0,H} \otimes S_{2,H} \otimes \cdots \otimes S_{M-1,H}).$$

In other words, we uncompress every entry of $\mathcal{D}$ (that is not in H) instead of only $\mathcal{D}_x$. One fact about S_{all} is that $S_{\mathsf{all}}|\phi_0\rangle = |\psi_0\rangle$. We have the following proposition about S_{all}:

Proposition 4.1. $\mathcal{R}^Q = S^\dagger \mathcal{O}^Q S = S_{\mathsf{all}}^\dagger \mathcal{O}^Q S_{\mathsf{all}}$ *and* $\mathcal{R}^C = S^\dagger \mathcal{O}^C S = S_{\mathsf{all}}^\dagger \mathcal{O}^C S_{\mathsf{all}}$.

Proof. This is because for $|x,p,w\rangle_{\mathcal{A}}$, the unitaries $\mathcal{O}^C$ and $\mathcal{O}^Q$ act as identity on the registers $\mathcal{D}_{<x}$ and $\mathcal{D}_{>x}$. Therefore, for every $x' \neq x$, we have that $S_{x'}^\dagger$ in $S_{\mathsf{all}}^\dagger$ cancels with $S_{x'}$ in S_{all}. □

The next proposition shows that $|\phi_t\rangle$ in the compressed oracle framework can be viewed as a compressed encoding of the state $|\psi_t\rangle$.

Proposition 4.2 (Indistinguishability)**.** *The states $|\psi_t\rangle$ from (3.1) and $|\phi_t\rangle$ from (4.3) satisfy*

$$S_{\mathsf{all}}|\phi_t\rangle = |\psi_t\rangle.$$

In particular, the two states are identical when we trace out the database register.

Proof. Using (4.3), the left-hand side is equal to

$$\begin{aligned}
S_{\mathsf{all}}\,|\phi_t\rangle &= S_{\mathsf{all}}\, U_t\, \mathcal{R}^{\ell(t)}\, U_{t-1} \cdots U_1\, \mathcal{R}^{\ell(1)}\, U_0\, |\phi_0\rangle \\
&= S_{\mathsf{all}}\, U_t\, (S_{\mathsf{all}}^\dagger \mathcal{O}^{\ell(t)} S_{\mathsf{all}})\, U_{t-1} \cdots U_1\, (S_{\mathsf{all}}^\dagger \mathcal{O}^{\ell(1)} S_{\mathsf{all}})\, U_0\, |\phi_0\rangle \\
&= (S_{\mathsf{all}}\, S_{\mathsf{all}}^\dagger)\, U_t\, \mathcal{O}^{\ell(t)} (S_{\mathsf{all}}\, S_{\mathsf{all}}^\dagger)\, U_{t-1} \cdots U_1\, \mathcal{O}^{\ell(1)}\, U_0\, S_{\mathsf{all}}\, |\phi_0\rangle \\
&= U_t\, \mathcal{O}^{\ell(t)}\, U_{t-1} \cdots U_1\, \mathcal{O}^{\ell(1)}\, U_0\, S_{\mathsf{all}}\, |\phi_0\rangle \\
&= U_t\, \mathcal{O}^{\ell(t)}\, U_{t-1} \cdots U_1\, \mathcal{O}^{\ell(1)}\, U_0\, |\psi_0\rangle \\
&= |\psi_t\rangle.
\end{aligned}$$

The second line follows from Proposition 4.1. The third line is true because U_i only operates on $\mathcal{A}$ and commutes with S_{all} (which only operates on $\mathcal{HD}$). Finally, the fourth line comes from the fact that $S_{\mathsf{all}}|\phi_0\rangle = |\psi_0\rangle$. □

Consistency. We aim at characterizing what basis states can be in the support of $|\phi_t\rangle$. For that, we introduce the following vector space $\mathbb{H}_{c,q}$ spanned by *consistent states*.

Definition 4.3 (History-Database Consistent State)**.** Given two integers c and q, we let $\mathbb{H}_{c,q}$ denote the vector space spanned by the basis states $|x, p, w\rangle_{\mathcal{A}}|H\rangle_{\mathcal{H}}|D\rangle_{\mathcal{D}}$ satisfying the following:

1. (Database size) The database satisfies $D(x) \neq \perp$ for at most q different values of x.
2. (History size) The history register is of the form $|H\rangle = |(x_1, y_1), \ldots, (x_c, y_c), \star, \ldots, \star\rangle$ where $x_1, \ldots, x_c \in [M]$ and $y_1, \ldots, y_c \in \{\perp\} \cup [N]$.
3. (Uniqueness) We can identify the history with a function $H : [M] \to \{\star, \perp\} \cup [N]$ where $H(x_j) = y_j$ for all $j \in \{1, 2, \cdots c\}$ (meaning no two pairs in the history can differ on the second coordinate only) and $H(x) = \star$ for $x \notin \{x_1, \ldots, x_c\}$.
4. (Equality) The database coincides with the history on non-$\star$ values, meaning that $H(x) \neq \star$ implies $D(x) = H(x)$.

We say that a basis state is *history-database consistent* if it is in $\mathbb{H}_{c,q}$ for some non-negative integers c and q.

Notice that the consistency of a basis state is a property that depends only on H and D. The reader may also wonder why we allow the history register to contain $(x, \perp)$ in the above definition since such a case shall not occur in $|\psi_t\rangle$ and $|\phi_t\rangle$ because of Proposition 4.2. This is only to provide more flexibility in further analysis. We now prove that $|\phi_t\rangle$ is supported over consistent basis states only.

Proposition 4.4 (Consistency)**.** *Any state $|\phi_t\rangle$ obtained after c classical queries and q quantum queries in the compressed oracle model, where $t = c + q$, satisfies $|\phi_t\rangle \in \mathbb{H}_{c,q}$.*

Proof. We check the four properties stated in Definition 4.3. The first property follows from the fact that each quantum query can increase the number of non-$\perp$ entries in D by at most 1. For the second and third properties, we note that they hold for $|\psi_t\rangle$ and, by Proposition 4.2, the states $|\psi_t\rangle$ and $|\phi_t\rangle$ have the same reduced density matrix over $\mathcal{H}$. Finally, the fourth property holds for $|\psi_t\rangle$ since $H(x) \neq \star$ implies that $D(x) = H(x)$. By Proposition 4.2 and Equation (4.2), for any x such that $H(x) \neq \star$, the unitary S_{all} acts like an identity on $\mathcal{D}_x$. Therefore, the same holds for $|\phi_t\rangle$ as well. □

Because of the above proposition, it suffices to only consider history-database consistent basis states while analyzing any algorithm and we shall tacitly assume that this is the case in any of the proofs that follow.

4.3 Sampling and Resampling

In this section, we prove that the compressed oracle follows a similar behavior as the classical lazy-sampling strategy, namely the sampling of each input coordinate is delayed until it gets queried. There are some crucial differences yet, due to the reversibility of quantum computation. In particular, a coordinate can get "resampled" to a different value with a small probability.

In the rest of the paper, we abbreviate the root of unity $\omega_N = e^{\frac{2i\pi}{N}}$ as ω. We also adopt the following notations to modify one entry of a database or history.

Definition 4.5 ($D_{x \leftarrow y}$ and $H_{x \leftarrow y}$)**.** Let $(x, y) \in [M] \times (\{\perp\} \cup [N])$. Given $D : [M] \to \{\perp\} \cup [N]$, we define the database $D_{x \leftarrow y}$ over the same domain as D such that

$$D_{x \leftarrow y}(x') = \begin{cases} y & \text{if } x' = x, \\ D(x') & \text{if } x' \neq x. \end{cases}$$

Given a history $H = ((x_1, y_1), \ldots, (x_k, y_k), \star, \ldots, \star)$ with at least one $\star$ entry, we define

$$H_{x \leftarrow y} = ((x_1, y_1), \ldots, (x_k, y_k), (x, y), \star, \ldots, \star)$$

where the leftmost star has been replaced with (x, y).

The two lemmas below describe what happens to the history and database when making a quantum or classical query. Among all the cases described below, the most interesting one is when the query is made at an index x that is in the database but not in the history (i.e. $D(x) \neq \perp$ and $H(x) = \star$): up to a small resampling error state, the database remains unchanged apart from an added phase.

Lemma 4.6 (Quantum Query)**.** *Let $|x, p, w, H, D\rangle$ be a history-database consistent basis state. Then, $\mathcal{R}^Q$ acts as a control on $|x, p, w\rangle|H\rangle$ and maps the database register $|D\rangle$ to*

- $\omega^{pD(x)}|D\rangle$ (if $H(x) \neq \star$ or $p = 0$)
- $\sum_{y \in [N]} \frac{\omega^{py}}{\sqrt{N}}|D_{x \leftarrow y}\rangle$ (if $H(x) = \star$, $D(x) = \perp$, $p \neq 0$)
- $\omega^{pD(x)}|D\rangle + \frac{\omega^{pD(x)}}{\sqrt{N}}|D_{x \leftarrow \perp}\rangle + \sum_{y \in [N]} \frac{1 - \omega^{pD(x)} - \omega^{py}}{N}|D_{x \leftarrow y}\rangle$ (if $H(x) = \star$, $D(x) \neq \perp$, $p \neq 0$)

Lemma 4.7 (Classical Query)**.** *Let $|x, p, w, H, D\rangle$ be a history-database consistent basis state. Then, $\mathcal{R}^C$ acts as a control on $|x, p, w\rangle$ and maps the history and database registers $|H, D\rangle$ to*

- $\omega^{pD(x)}|H_{x \leftarrow D(x)}, D\rangle$ (if $H(x) \neq \star$)
- $\sum_{y \in [N]} \frac{\omega^{py}}{\sqrt{N}}|H_{x \leftarrow y}, D_{x \leftarrow y}\rangle$ (if $H(x) = \star$, $D(x) = \perp$)
- $\omega^{pD(x)}|H_{x \leftarrow D(x)}, D\rangle + \frac{1}{\sqrt{N}}|H_{x \leftarrow \perp}, D_{x \leftarrow \perp}\rangle - \sum_{y \in [N]} \frac{\omega^{py}}{N}|H_{x \leftarrow y}, D_{x \leftarrow y}\rangle$ (if $H(x) = \star$, $D(x) \neq \perp$)

In the above lemmas, when x is not in the history but is in the database, after making a quantum or classical query, most likely $D(x)$ remains unchanged (corresponding to the $|D\rangle$ term), but there is a small probability that $D(x)$ gets removed (corresponding to the $|D_{x \leftarrow \perp}\rangle$ term) or resampled (corresponding to an equal superposition of $|D_{x \leftarrow y}\rangle$ over y). We call the first term "unchanged term" (the database does not get updated), the second term "removed term" (the outcome on x gets removed) and the last one "resampled term" in both items above. The proofs can be found in Appendix A.1.

4.4 Progress Measures

All progress measures studied in this paper will be expressed in terms of the norm of the projection onto basis states satisfying certain predicates.

Definition 4.8 (Basis-State Predicate)**.** Let $\mathrm{P} : (x, p, w, H, D) \mapsto \{\textsc{False}, \textsc{True}\}$ be a predicate function over all basis states $|x, p, w\rangle_{\mathcal{A}}|H\rangle_{\mathcal{H}}|D\rangle_{\mathcal{D}}$. Then, we define the projector

$$\Pi_{\mathrm{P}} = \sum_{(x,p,w,H,D) \in \mathrm{P}^{-1}(\textsc{True})} |x, p, w, H, D\rangle\langle x, p, w, H, D|$$

that projects over all basis states satisfying the predicate P. We let $\overline{\mathrm{P}}$ denote the *negation* of P and, given two predicates P_1 and P_2, we let $\mathrm{P}_1 \cdot \mathrm{P}_2$ denote their *conjunction* and $\mathrm{P}_1 + \mathrm{P}_2$ denote their *disjunction*.

Fact 4.9. *Let* P_1 *and* P_2 *be two basis-state predicates. Then, the projections* Π_{P_1} *and* Π_{P_2} *are commuting operators. We have* $\Pi_{\overline{\mathrm{P}_1}} = \mathbb{I} - \Pi_{\mathrm{P}_1}$, $\Pi_{\mathrm{P}_1 \cdot \mathrm{P}_2} = \Pi_{\mathrm{P}_1}\Pi_{\mathrm{P}_2}$ *and* $\Pi_{\mathrm{P}_1+\mathrm{P}_2} = \Pi_{\mathrm{P}_1} + \Pi_{\mathrm{P}_2} - \Pi_{\mathrm{P}_1}\Pi_{\mathrm{P}_2}$. *Moreover,* $P_1 \Rightarrow P_2$ *if and only if* $\Pi_{\mathrm{P}_1} \preceq \Pi_{\mathrm{P}_2}$, *where* $\preceq$ *is the Loewner order.*

Most of the predicates considered in this paper will in fact depend only on the values of H and D (a few predicates will also depend on the query index x).

We define the following general notions of progress measure and overlap.

Definition 4.10 (Progress Measure and Progress Overlap)**.** Given a state $|\phi\rangle$ and a projector Π over $\mathcal{AHD}$, we define

$$\Delta^Q(\Pi, |\phi\rangle) = \|\Pi\mathcal{R}^Q|\phi\rangle\| - \|\Pi|\phi\rangle\| \quad \text{and} \quad \Gamma^Q(\Pi, |\phi\rangle) = \frac{\|\Pi\mathcal{R}^Q(\mathbb{I} - \Pi)|\phi\rangle\|}{\|(\mathbb{I} - \Pi)|\phi\rangle\|},$$

$$\Delta^C(\Pi, |\phi\rangle) = \|\Pi\mathcal{R}^C|\phi\rangle\|^2 - \|\Pi|\phi\rangle\|^2 \quad \text{and} \quad \Gamma^C(\Pi, |\phi\rangle) = \frac{\|\Pi\mathcal{R}^C(\mathbb{I} - \Pi)|\phi\rangle\|^2}{\|(\mathbb{I} - \Pi)|\phi\rangle\|^2},$$

with the convention that $\Gamma^Q(\Pi, |\phi\rangle) = \Gamma^C(\Pi, |\phi\rangle) = 0$ if $\|(\mathbb{I} - \Pi)|\phi\rangle\| = 0$.

The quantities $\Delta^Q(\Pi, |\phi\rangle), \Delta^C(\Pi, |\phi\rangle) \in [-1, 1]$ represent the increase in the norm (resp. squared norm) of the projection onto Π after applying a quantum (resp. classical query). These will be used as a measure of quantum and classical progress later in the proofs.

The quantities $\Gamma^Q(\Pi, |\phi\rangle), \Gamma^C(\Pi, |\phi\rangle) \in [0, 1]$ track the amplitude that moves after making a quantum or classical query from a subspace to its orthogonal complement. In particular, if $\Gamma^Q(\Pi, |\phi\rangle) \le \gamma$, then we have that $\|\Pi\mathcal{R}^Q(\mathbb{I} - \Pi)|\phi\rangle\| \le \gamma\|(\mathbb{I} - \Pi)|\phi\rangle\|$ and we get a similar relation for the squared norm if $\Gamma^C(\Pi, |\phi\rangle) \le \gamma$. In this paper, we only consider projectors Π_{P} for some predicates P. In such cases, we can equivalently write

$$\Gamma^Q(\Pi_{\mathrm{P}}, |\phi\rangle) = \frac{\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|}{\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|} \quad \text{and} \quad \Gamma^C(\Pi_{\mathrm{P}}, |\phi\rangle) = \frac{\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2}{\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2}.$$

Next, we give two general lemmas that bound how much increase a single classical or quantum query can have towards a target history–database pair. These lemmas will apply when the predicate satisfies the following definition, which is similar to the database properties introduced in [CMS19; CFHL21]. One difference in our definition is that we need to take the classical history into account.

Definition 4.11 (History-Database Predicate)**.** We say that a basis-state predicate P is a *history-database predicate* if, for every true-state $(x, p, w, H, D) \in \mathrm{P}^{-1}(\textsc{True})$,

- (Consistent) The state $|x, p, w, H, D\rangle$ is consistent (see Definition 4.3).
- (History Invariant) For every list $H' \in \mathscr{H}$ with no ambiguous pair, if H and H' represent the same function (i.e. $H(x') = H'(x')$ for all $x' \in [M]$) then $(x, p, w, H', D) \in \mathrm{P}^{-1}(\textsc{True})$.
- (Database Monotone) For every database D' that is obtained by replacing a $\perp$ in D with another value (i.e. $D = D'_{x' \leftarrow \perp}$ for some $x' \in [M]$), we have $(x, p, w, H, D') \in \mathrm{P}^{-1}(\textsc{True})$.

The next lemmas bound the progress overlap Γ^Q (resp. Γ^C) in terms of the probability that a history-database predicate becomes true when a new uniformly random value y is added to the database (resp. database and history). We first provide the lemma for quantum queries, which follows the ideas used in previous work, starting from [Zha19]. Then we state the lemma for classical queries, which is new, but the core argument in the proof is similar. These results encompass most, although not all (see Lemma 6.10), of the progress overlap bounds needed in subsequent applications. The proofs can be found in Appendix A.2.

Lemma 4.12 (Progress Overlap, Quantum Query)**.** *Let* P *be a history-database predicate,* c *and* q *be two non-negative integers and* $\gamma \in [0,1]$ *be a real parameter. Suppose that, for every false-state* $(x,p,w,H,D) \in \mathrm{P}^{-1}(\textsc{False}) \cap \mathbb{H}_{c,q}$ *where* $D(x) = \perp$*, the probability to make the predicate true by replacing* $D(x)$ *with a random value* y *is at most*

$$\Pr_{y \leftarrow [N]}\left[(x,p,w,H,D_{x\leftarrow y}) \in \mathrm{P}^{-1}(\textsc{True})\right] \leq \gamma. \tag{4.4}$$

Then, the quantum progress overlap is at most $\Gamma^{Q}(\Pi_{\mathrm{P}}, |\phi\rangle) \leq \sqrt{10\gamma}$ *for all* $|\phi\rangle \in \mathbb{H}_{c,q}$.

The adaptation of the above lemma to the classical query case requires making one extra assumption stated in Equation (4.6) below. This condition rules out predicates that can become true by simply copying a value from the database to the history.

Lemma 4.13 (Progress Overlap, Classical Query)**.** *Let* P *be a history-database predicate,* c *and* q *be two non-negative integers and* $\gamma \in [0,1]$ *be a real parameter. Suppose that, for every false-state* $(x,p,w,H,D) \in \mathrm{P}^{-1}(\textsc{False}) \cap \mathbb{H}_{c,q}$ *where* $D(x) = \perp$*, the probability to make the predicate true by replacing* $H(x)$ *and* $D(x)$ *with the same random value* y *is at most*

$$\Pr_{y \leftarrow [N]}\left[(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y}) \in \mathrm{P}^{-1}(\textsc{True})\right] \leq \gamma. \tag{4.5}$$

Assume further that, for every false-state $(x,p,w,H,D) \in \mathrm{P}^{-1}(\textsc{False})$*, the predicate does not become true when* $(x, D(x))$ *is appended to the history, i.e.*

$$\mathrm{P}(x,p,w,H,D) = \textsc{False} \quad \Rightarrow \quad \mathrm{P}(x,p,w,H_{x\leftarrow D(x)},D) = \textsc{False}. \tag{4.6}$$

Then, the classical progress overlap is at most $\Gamma^{C}(\Pi_{\mathrm{P}}, |\phi\rangle) \leq 2\gamma$ *for all* $|\phi\rangle \in \mathbb{H}_{c,q}$.

Finally, we state some simple facts that will be used frequently throughout the paper.

Fact 4.14. *Let* $|\phi\rangle, |\phi'\rangle$ *be two states defined over the registers* $\mathcal{AHD}$*. Let* U *be a unitary operator over* $\mathcal{A}$*. Let* Π, Π' *be two projectors over* $\mathcal{AHD}$*. Then,*

- *(Monotonicity) If* $\Pi \preceq \Pi'$ *then* $\Pi \cdot \Pi' = \Pi' \cdot \Pi = \Pi$.
- *(Commutativity) If* $\Pi = \mathbb{I}_{\mathcal{A}} \otimes \Pi_{\mathcal{HD}}$ *for some projector* $\Pi_{\mathcal{HD}}$ *then* $\|\Pi U|\phi\rangle\| = \|\Pi|\phi\rangle\|$.
- *(Sub-multiplicativity)* $\|\Pi|\phi\rangle\| \leq \||\phi\rangle\|$.

5 Preimage Search

In this section, we prove the lower bound for preimage search against hybrid algorithms.

Theorem 5.1. *For any quantum algorithm that makes at most* q *quantum oracle queries and* c *classical oracle queries, given a uniformly random function* $D : [M] \to [N]$*, its success probability of finding a zero preimage is at most* $O((c+q^2)/N)$.

The proof proceeds as mentioned in the technical overview — we will define a notion of quantum and classical progress to keep track of the success probability of the algorithm after each query. To formally define these measures, we now give a series of predicates that characterize whether the history or the database contains a zero preimage:

Definition 5.2. The following predicates evaluate a basis state $|x,p,w,H,D\rangle$ to $\textsc{True}$ if and only if it is history-database consistent (see Definition 4.3) and satisfies the next conditions:

- Q: there exists a zero preimage in the quantum database D that is not in the history H, i.e. x' such that $D(x') = 0$ and $H(x') = \star$.

- C: there exists a zero preimage in the classical history H, i.e. x' such that $H(x')=0$. Note that for any history-database consistent basis state $(x',y) \in H$ implies $D(x')=y$, and thus if C is true, then there exists x' such that $D(x')=H(x')=0$.

We shall also use negations, conjunctions and disjunctions of the above predicates as well.

To prove the lower bound, we first note that the squared norm $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2$ is an upper bound on the success probability of the algorithm after the last query since we can assume that the final output is always in the history register (by making one extra classical query at the end) and hence also in the database. To keep track of the progress of the algorithm, we will need more fine-grained control and for this we keep track of the change in the quantities $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|$ and $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|$ which can be thought of as classical and (purely) quantum progress respectively. Initially, both quantities are equal to zero. Each time the algorithm makes a quantum or classical query, we show that the progress evolves as follows in terms of the quantities defined in Definition 4.10:

$$\Delta^Q(\Pi,|\phi\rangle) = \|\Pi\mathcal{R}^Q|\phi\rangle\| - \|\Pi|\phi\rangle\|,$$
$$\Delta^C(\Pi,|\phi\rangle) = \|\Pi\mathcal{R}^C|\phi\rangle\|^2 - \|\Pi|\phi\rangle\|^2.$$

Proposition 5.3 (Progress after a quantum query)**.** *Given two integers c,q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ are at most,*

$$\Delta^Q(\Pi_{\mathrm{C}},|\phi\rangle) = 0 \quad \textit{and} \quad \Delta^Q(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}},|\phi\rangle) \le \sqrt{\frac{10}{N}}.$$

Proposition 5.4 (Progress after a classical query)**.** *Given two integers c,q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ are at most,*

$$\Delta^C(\Pi_{\mathrm{C}},|\phi\rangle) \le\ 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2 + \frac{4}{N} \quad \textit{and} \quad \Delta^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}},|\phi\rangle) \le -\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2.$$

The first proposition is standard and its proof is deferred to Appendix B. The second proposition is different from the usual analysis in the compressed oracle framework as it shows that a classical query can also decrease the progress the algorithm has made. We shall give its proof later. First we show how the above implies an optimal lower bound for preimage search.

Theorem 5.5. *The progress made by any algorithm after $t=q+c$ queries, of which q are quantum and c are classical, satisfies*

$$\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \le O\left(\frac{c+q^2}{N}\right).$$

Proof. It will be more convenient to keep track of the potential

$$\Psi_t := \|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 + 2\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2.$$

Observe that $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \le \Psi_t$[6]. We claim that the following recurrence holds for the potential Ψ_t:

$$\Psi_t \le O\left(\sqrt{\Psi_{t-1}} + \frac{7}{\sqrt{N}}\right)^2 \text{ if quantum query at time } t, \tag{5.1}$$
$$\Psi_t \le \Psi_{t-1} + \frac{4}{N} \qquad \text{if classical query at time } t,$$

[6]In fact, since $\Pi_{\mathrm{C}} + \Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} = \Pi_{\mathrm{Q}+\mathrm{C}}$ where the projectors in the sum are orthogonal, we also have that $\frac{1}{2}\Psi_t \le \|\Pi_{\mathrm{Q}+\mathrm{C}}|\phi_t\rangle\|^2 \le \Psi_t$ but we do not use this fact.

with the initial condition that $\Psi_0 = 0$. Recalling the definition of $\Delta^Q(\Pi, |\phi\rangle)$, the first inequality follows from Proposition 5.3 (and the fact that $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| \leq \sqrt{\Psi_{t-1}}$) since

$$\begin{aligned}\Psi_t &\leq \|\Pi_{\mathrm{C}}|\phi_{t-1}\rangle\|^2 + 2O\left(\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| + \sqrt{\frac{10}{N}}\right)^2 \\ &\leq \Psi_{t-1} + 4\sqrt{\frac{10}{N}}\cdot\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| + \frac{20}{N} \ \leq O\left(\sqrt{\Psi_{t-1}} + \frac{7}{\sqrt{N}}\right)^2,\end{aligned}$$

while the second inequality follows directly from Proposition 5.4.

In the rest of the argument, we will assume that the inequalities in Equation (5.1) are replaced with equalities as it can only increase the maximum possible value for Ψ_t. Observe now that the progress always increases by the same amount $\Psi_t - \Psi_{t-1} = 4/N$ when making a classical query, whereas for quantum queries it is advantageous to maximize the value of Ψ_{t-1} since $\Psi_t - \Psi_{t-1} = 14\sqrt{\Psi_{t-1}/N} + 49/N$. Hence, the optimal strategy is to use the classical recurrence for the first c steps and the quantum recurrence afterward. In this case, if there are q quantum and c classical queries, it follows that for $t = q + c$, we have that

$$\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \leq \Psi_t = O\left(\frac{c+q^2}{N}\right). \qquad \square$$

To complete the proof, we now prove Proposition 5.4.

Proof of Proposition 5.4. Towards proving the first inequality in the statement of the proposition, we have that

$$\begin{aligned}\|\Pi_{\mathrm{C}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{C}}\mathcal{R}^C(\Pi_{\mathrm{C}} + \Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{C}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\leq \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2.\end{aligned}$$

The second equality in the above sequence follows since $\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{C}}|\phi\rangle$ is orthogonal to $\Pi_{\mathrm{C}}\mathcal{R}^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$. This can be seen from the fact that the history register $\mathcal{H}$ in $\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{C}}|\phi\rangle$ is supported over basis states $|H\rangle_{\mathcal{H}}$ where the first c entries of H contains a zero pre-image. Therefore, it is orthogonal to $\Pi_{\mathrm{C}}\mathcal{R}^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$. The last inequality follows from Fact 4.14 and the fact that $\||a\rangle + |b\rangle\|^2 \leq 2\||a\rangle\|^2 + 2\||b\rangle\|^2$ for unnormalized states $|a\rangle$ and $|b\rangle$.

Since C is a history-database predicate satisfying Equation (4.6), we can use Lemma 4.13 to bound the last term. It gives us that for some $\gamma \leq \frac{1}{N}$,

$$\Gamma^C(\Pi_{\mathrm{C}}, \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle) \leq 2\gamma \implies \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq 2\gamma\|\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq \frac{2}{N}.$$

Recalling Definition 4.10, we thus have shown that

$$\Delta^C(\Pi_{\mathrm{C}}, |\phi\rangle) \leq 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \frac{4}{N},$$

proving the first inequality in the statement of the proposition.

The second inequality is relatively straightforward:

$$\begin{aligned}\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^C(\Pi_{\mathrm{C}} + \Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{Q}+\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \\ &\leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2,\end{aligned}$$

where the second line is true as $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^C(\Pi_{\mathrm{C}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}) = 0$. This holds since a classical query $\mathcal{R}^C$ can not remove a zero preimage from H or lead to a zero preimage in the database that is not in the classical history as well. The third line follows since $\Pi_{\mathrm{C}} + \Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} = \Pi_{\mathrm{Q}+\mathrm{C}}$ where the projectors Π_{C} and $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}$ are orthogonal, while the last line follows from Fact 4.14. Recalling Definition 4.10, rearranging the above gives us the desired statement. □

6 Collision Finding

In this section, we prove our main theorem on hybrid collision-finding algorithms:

Theorem 6.1. *For any quantum algorithm that makes at most q quantum oracle queries and c classical oracle queries, given a uniformly random function $D : [M] \to [N]$, its success probability of finding a colliding pair is at most $O((c^2 + cq^2 + q^3)/N)$.*

The section is organized as follows. The progress measures needed for the proof of the above theorem are introduced in Section 6.1. The main part of the proof is contained in Section 6.2. It uses some auxiliary lemmas whose demonstrations are deferred to Sections 6.3 to 6.5.

6.1 Progress Measures

We define three types of collision pairs that can be recorded by a hybrid compressed oracle.

Definition 6.2 (Collision Type)**.** Given a history-database consistent pair (H, D), we say that it contains a collision if there exist two values $x_1 \neq x_2$ such that $D(x_1) = D(x_2) \neq \perp$. Additionally, if $x_1, x_2 \notin H$ the collision is said to be *quantum*, if $x_1, x_2 \in H$ it is said to be *classical* and if $x_1 \notin H$, $x_2 \in H$ it is said to be *hybrid*.

We now give a series of predicates that characterize what types of collisions have been recorded in a basis state. Later on, we will combine these predicates together to define the different measures of progress needed in our proofs.

Definition 6.3. The following predicates evaluate a basis state $|x, p, w, H, D\rangle$ to TRUE if and only if it is history-database consistent (see Definition 4.3) and satisfies the next conditions:

- Q, H, C: there is respectively at least one quantum, one hybrid or one classical collision contained in (H, D).
- Q_2: there are at least two quantum collisions contained in (H, D).
- X: the query index is not in the history (i.e. $x \notin H$) and it is contained in every hybrid collision (i.e. if $D(x_1) = D(x_2)$ and $x_1 \notin H$, $x_2 \in H$ then $x = x_1$).

Note that among all the predicates defined above, X is the only one that depends on the value x contained in the query register. The other predicates depend only on the history-database (H, D).

6.2 Main Result

We now turn to the proof of Theorem 6.1, delaying auxiliary lemmas to later sections. First, it is simple to argue that, for a t-query algorithm computing a state $|\phi_t\rangle$ in the hybrid compressed oracle model, the probability $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2$ to have recorded a *classical* collision is an upper bound on the success probability. Hence, the core of our proof is to show that this recording probability is at most $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \leq O((c^2 + cq^2 + q^3)/N)$ when c-out-of-t queries are classical and q-out-of-t are quantum. Since a direct bound on this quantity is difficult to obtain, we decompose its analysis into simpler measures of progress. First, in Section 6.4, we prove the next upper bounds on the probability of having recorded a *quantum* collision, or both a *quantum* collision and a *hybrid* collision.

Proposition 6.4. *Any state $|\phi_{c+q}\rangle$ obtained after c classical and q quantum queries in the hybrid compressed oracle model satisfies,*

$$\|\Pi_{\mathrm{Q}}|\phi_{c+q}\rangle\|^2 \leq O\left(\frac{q^3}{N}\right) \quad \text{and} \quad \|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi_{c+q}\rangle\|^2 \leq O\left(\frac{cq^5+q^6}{N^2}\right).$$

The first inequality corresponds to the optimal success probability for solving collision finding when all the queries are quantum, its proof is a simple adaptation of [Zha19]. For the second inequality, it will be easier to consider the more general predicate $\mathrm{Q}_2 + \mathrm{Q}\cdot\mathrm{H} = (\mathrm{Q}+\mathrm{H})\cdot\mathrm{Q}$ that allows replacing the hybrid collision with a second quantum collision. Intuitively, one can satisfy this predicate by finding one quantum collision with probability $O(q^3/N)$, and finding one quantum or hybrid collision with probability $O((cq^2+q^3)/N)$. It turns out that the probability of satisfying the predicate $\mathrm{Q}_2 + \mathrm{Q}\cdot\mathrm{H}$ essentially behaves like the product of these two probabilities which gives us the second inequality.

Next, in Section 6.5, we turn to the more complicated task of recording *classical* collisions. We consider the progress measures corresponding to the three predicates C, $\mathrm{H}\cdot\overline{\mathrm{C}}$ and $\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}$. We first show that performing a quantum query incurs the following progress increases.

Lemma 6.5 (Progress Measure, Quantum Query)**.** *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ are at most,*

$$\Delta^Q(\Pi_{\mathrm{C}}, |\phi\rangle) = 0\,, \qquad \Delta^Q(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq \sqrt{\frac{10c}{N}}\,, \qquad \Delta^Q(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq \sqrt{\frac{20(c+q)}{N}}\,.$$

Recall that, by Definition 4.10, the quantity $\Delta^Q(\Pi_{\mathrm{P}}, |\phi\rangle) \in [-1,1]$ for a predicate P corresponds to the progress difference $\Delta^Q(\Pi_{\mathrm{P}}, |\phi\rangle) = \|\Pi_{\mathrm{P}}\mathcal{R}^Q|\phi\rangle\| - \|\Pi_{\mathrm{P}}|\phi\rangle\|$ when doing a quantum query. Hence, the first equality reflects the fact that a quantum query cannot create or destroy a classical collision. The second inequality is based on the observation that, when adding a random value to the database, the probability that it creates a hybrid collision is at most c/N since it must collide with one of the c values contained in the history. The third inequality is slightly more involved since it must also take into account the case of *removing* a hybrid collision from the history-database.

We next look at the progress measures when the query is instead classical. Recall that the difference $\Delta^C(\Pi_{\mathrm{P}}, |\phi\rangle) = \|\Pi_{\mathrm{P}}\mathcal{R}^C|\phi\rangle\|^2 - \|\Pi_{\mathrm{P}}|\phi\rangle\|^2$ is defined with respect to the squared norm.

Lemma 6.6 (Progress Measure, Classical Query)**.** *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one classical query on $|\phi\rangle$ are at most,*

$$\begin{aligned}
\Delta^C(\Pi_{\mathrm{C}}, |\phi\rangle) &\leq 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \frac{4c}{N}\,, \\
\Delta^C(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\leq -\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\sqrt{\frac{q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \frac{7q}{N}\,, \\
\Delta^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\leq -\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \sqrt{\frac{8c}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\| + \frac{2c}{N}\,.
\end{aligned}$$

The above inequalities are more involved and are the core of our proof. The two negative terms on the right-hand side represent the exact amount of progress transferred by one classical query between different progress measures. Note that, as a simple case, if an algorithm makes no quantum query then the inequalities simplify to $\Delta^C(\Pi_{\mathrm{C}}, |\phi\rangle) = \|\Pi_{\mathrm{C}}\mathcal{R}^C|\phi_{c+1}\rangle\|^2 - \|\Pi_{\mathrm{C}}|\phi_c\rangle\|^2 \leq \frac{4c}{N}$ and we recover the classical success probability $\|\Pi_{\mathrm{C}}|\phi_c\rangle\|^2 \leq O(c^2/N)$ for collision finding.

Finally, we are ready to prove our main theorem by using the above three results.

Proof of Theorem 6.1. Fix any hybrid algorithm and let $|\phi_t\rangle$ denote the state, described in Equation (4.3), that is obtained after t queries in the hybrid compressed oracle model. We want to upper bound the probability that after $t = c + q$ queries, of which c queries are classical and q queries are quantum, the algorithm outputs a correct collision pair. We can always assume, at the cost of doing two extra classical queries, that the two output values are also contained in the history register. Hence, the success probability of the algorithm is upper bounded by the probability $\|\Pi_{\mathrm{C}}|\phi_{c+q}\rangle\|^2$ of having registered a collision pair in the history register.

We now prove the upper bound on $\|\Pi_{\mathrm{C}}|\phi_{c+q}\rangle\|^2$ that matches our theorem. For that, we define the following progress measure after t queries,

$$\Psi_t = \|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2 + 4\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2. \tag{6.1}$$

Note that Ψ_{c+q} is larger than $\|\Pi_{\mathrm{C}}|\phi_{c+q}\rangle\|^2$, hence it suffices to bound the former quantity. Our proof is by induction on t. Initially, $\Psi_0 = 0$ since the history and database registers of $|\phi_0\rangle$ are empty by definition. Let us now consider $t < c + q$. If the $(t+1)$-th query is a quantum query, then the progress increases by at most,

$$\begin{aligned}
\Psi_{t+1} &\leq \big(\|\Pi_{\mathrm{C}}|\phi_t\rangle\| + \Delta^Q(\Pi_{\mathrm{C}}, |\phi_t\rangle)\big)^2 + 2\big(\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| + \Delta^Q(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi_t\rangle)\big)^2 \\
&\quad + 4\big(\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| + \Delta^Q(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi_t\rangle)\big)^2 \\
&\leq \Psi_t + 4\sqrt{\frac{10c}{N}}\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| + 8\sqrt{\frac{20(c+q)}{N}}\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| + \frac{100c + 80q}{N} \\
&\leq \left(\sqrt{\Psi_t} + 10\sqrt{\frac{c+q}{N}}\right)^2
\end{aligned}$$

where the first inequality is by Definition 4.10 and the second inequality is by Lemma 6.5. If the $(t+1)$-th query is instead classical, the progress increases by at most,

$$\begin{aligned}
\Psi_{t+1} &\leq \Psi_t + \Delta^C(\Pi_{\mathrm{C}}, |\phi_t\rangle) + 2\Delta^C(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi_t\rangle) + 4\Delta^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi_t\rangle) \\
&\leq \Psi_t + 4\sqrt{\frac{q}{N}}\|\Pi_{\mathrm{Q}}|\phi_t\rangle\| + \sqrt{\frac{128c}{N}}\|\Pi_{\mathrm{Q}}|\phi_t\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi_t\rangle\| + \frac{12c + 14q}{N} \\
&\leq \Psi_t + O\left(\frac{c+q^2}{N} + \frac{cq^4 + \sqrt{cq^9}}{N^2}\right)
\end{aligned}$$

where the first inequality is again by Definition 4.10, the second inequality is by Lemma 6.6 and the last inequality is by Proposition 6.4.

Finally, one can observe that the maximum progress permitted by the above two inequalities is achieved when all the classical queries are performed first. Thus, we conclude that

$$\Psi_{c+q} \leq O\left(c \cdot \left(\frac{c+q^2}{N} + \frac{cq^4 + \sqrt{cq^9}}{N^2}\right) + q^2 \cdot \frac{c+q}{N}\right) \leq O\left(\frac{c^2 + cq^2 + q^3}{N}\right).$$

□

6.3 Progress Overlap Lemmas

In this section, we prove several simple lemmas that upper bound the progress overlap when making one classical or quantum query. Roughly speaking, these quantities correspond to the probability of recording new collisions in the history-database register when a new coordinate of the input is revealed by a query.

We first give a central fact that will be used throughout the next sections. It describes certain subspaces that remain orthogonal after applying one (classical or quantum) query to them.

Fact 6.7. *The following linear maps are equal to zero over the subspace $\mathbb{H}_{c,q}$ of consistent states:*

$$\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}},\ \Pi_{\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{C}},\ \Pi_{\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\mathrm{C}},\ \Pi_{\mathrm{C}}\mathcal{R}^Q\Pi_{\overline{\mathrm{C}}},\ \Pi_{\mathrm{Q}_2}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}},\ \Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}},\ \Pi_{\overline{\mathrm{H}}}\mathcal{R}^Q\Pi_{\overline{\mathrm{X}}\cdot\mathrm{H}}.$$

For any states $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{H}_{c,q}$, the following vectors are orthogonal:

$$\mathcal{R}^C \Pi_{\overline{\mathrm{X}\cdot\mathrm{H}}} |\phi_1\rangle \perp \mathcal{R}^C \Pi_{\overline{\mathrm{H}}} |\phi_2\rangle \quad \textit{and} \quad \mathcal{R}^C \Pi_{\overline{\mathrm{C}}} |\phi_1\rangle \perp \mathcal{R}^C \Pi_{\mathrm{C}} |\phi_2\rangle\,.$$

Proof. The statement follows by simple applications of Lemmas 4.6 and 4.7. We detail the proof of the first equality $\Pi_{\mathrm{Q}} \mathcal{R}^C \Pi_{\overline{\mathrm{Q}}} = 0$. Consider any basis state $|x, p, w, H, D\rangle \in \mathrm{supp}(\Pi_{\overline{\mathrm{Q}}})$. By Lemma 4.7, every history-database (H', D') contained in the support of the post-query state $\mathcal{R}^C |x, p, w, H, D\rangle$ must be identical to (H, D) except possibly on the value x. Furthermore, since x is in the history (i.e. $H'(x) \neq \star$), it cannot contribute to any quantum collision in (H', D'). Thus, no quantum collision can be contained in (H', D'). □

We now analyze the effect of quantum queries on the progress overlap $\Gamma^Q(\Pi, |\phi\rangle) \in [0, 1]$ for different projectors Π. Recall that, by Definition 4.10, this value is defined as the number satisfying $\Gamma^Q(\Pi, |\phi\rangle) = \|\Pi \mathcal{R}^Q (\mathbb{I} - \Pi)|\phi\rangle\| / \|(\mathbb{I} - \Pi)|\phi\rangle\|$. In colloquial terms, this number gives the relative amplitude that moves from the support of $\mathbb{I} - \Pi$ to the support of Π after making a quantum query. Notice that Fact 6.7 already shows that $\Gamma^Q(\Pi_{\mathrm{C}}, |\phi\rangle) = \Gamma^Q(\Pi_{\overline{\mathrm{C}}}, |\phi\rangle) = 0$.

Lemma 6.8. *Given two integers c and q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$, the progress overlap caused by one quantum query on $|\phi\rangle$ are at most,*

$$\Gamma^Q(\Pi_{\mathrm{Q}}, |\phi\rangle) \leq \sqrt{\frac{10q}{N}}\,, \qquad (6.2) \qquad\qquad \Gamma^Q(\Pi_{\mathrm{Q}+\mathrm{H}}, |\phi\rangle) \leq \sqrt{\frac{10(c+q)}{N}}\,, \qquad (6.3)$$

$$\Gamma^Q(\Pi_{\mathrm{Q}_2}, |\phi\rangle) \leq \sqrt{\frac{10q}{N}}\,, \qquad (6.4) \qquad\qquad \Gamma^Q(\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}, |\phi\rangle) \leq \sqrt{\frac{10(c+q)}{N}}\,, \qquad (6.5)$$

$$\Gamma^Q(\Pi_{\mathrm{H}}, |\phi\rangle) \leq \sqrt{\frac{10c}{N}}\,. \qquad (6.6)$$

Proof. The five inequalities follow from Lemma 4.12 as $\mathrm{Q}, \mathrm{Q}_2, \mathrm{H}, \mathrm{Q}+\mathrm{H}, \mathrm{Q}_2 + \mathrm{Q}\cdot\mathrm{H}$ are history-database predicates (Definition 4.11) and the corresponding γ parameters are $q/N, q/N, c/N, (c+q)/N, (c+q)/N$ respectively. □

We prove a similar statement for classical queries. Note that the value $\Gamma^C(\Pi, |\phi\rangle)$ is defined with respect to the squared norm, that is, $\Gamma^C(\Pi, |\phi\rangle) = \|\Pi \mathcal{R}^C (\mathbb{I} - \Pi)|\phi\rangle\|^2 / \|(\mathbb{I} - \Pi)|\phi\rangle\|^2$.

Lemma 6.9. *Given two integers c and q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$, the progress overlap caused by one classical query on $|\phi\rangle$ are at most,*

$$\Gamma^C(\Pi_{\mathrm{Q}}, |\phi\rangle) = 0\,, \qquad (6.7) \qquad\qquad \Gamma^C(\Pi_{\mathrm{Q}+\mathrm{H}}, |\phi\rangle) \leq \frac{2q}{N}\,, \qquad (6.8)$$

$$\Gamma^C(\Pi_{\mathrm{Q}_2}, |\phi\rangle) = 0\,, \qquad (6.9) \qquad\qquad \Gamma^C(\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}, |\phi\rangle) \leq \frac{2q}{N}\,. \qquad (6.10)$$

Proof. The four inequalities follow from Lemma 4.13 as $\mathrm{Q}, \mathrm{Q}_2, \mathrm{Q}+\mathrm{H}, \mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}$ are history-database predicates (Definition 4.11) with the corresponding γ parameters being $0, 0, q/N, q/N$ respectively, and they satisfy the condition of Equation (4.6). □

Finally, we give four inequalities that do not follow from Lemmas 4.12 and 4.13. Equations (6.11) and (6.13) below upper bound the progress made towards *removing* all hybrid and classical collisions from the history-database, which is not a database monotone property (see Definition 4.11). The purpose of Equation (6.12) is to upper bound the probability that a classical query transfers the query index x from one hybrid collision to a *different* hybrid collision. Finally, Equation (6.14) overcomes the fact that the predicate $\mathrm{H}+\mathrm{C}$ does not satisfy the condition stated in Equation (4.6).

Lemma 6.10. *Given two integers c and q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$, we have*

$$\Gamma^Q(\Pi_{\overline{\mathrm{H+C}}}, |\phi\rangle) \leq \sqrt{\frac{10c}{N}}\,, \quad (6.11) \qquad \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{X\cdot H}}|\phi\rangle\|^2 \leq \frac{q}{N}\cdot\|\Pi_{\mathrm{X\cdot H}}|\phi\rangle\|^2\,, \quad (6.12)$$

$$\Gamma^C(\Pi_{\overline{\mathrm{H+C}}}, |\phi\rangle) \leq \frac{2c}{N}\,, \quad (6.13) \qquad \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2 \leq \frac{2c}{N}\cdot\|\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2\,. \quad (6.14)$$

The proofs of these equations use similar ideas to those of Lemmas 4.12 and 4.13. They are deferred to Appendix C.

6.4 Quantum and Hybrid Collisions

The objective of this section is to upper bound the probability of having recorded *quantum* or *hybrid* collisions after a certain number of classical and quantum queries have been made. This is a prerequisite for analyzing the recording of *classical* collisions in the next section, which will be a more involved task. Here, we show the following proposition.

Proposition 6.4 (Restated)**.** *Any state $|\phi_{c+q}\rangle$ obtained after c classical and q quantum queries in the hybrid compressed oracle model satisfies,*

$$\|\Pi_{\mathrm{Q}}|\phi_{c+q}\rangle\|^2 \leq O\left(\frac{q^3}{N}\right) \quad \text{and} \quad \|\Pi_{\mathrm{Q\cdot H}}|\phi_{c+q}\rangle\|^2 \leq O\left(\frac{cq^5+q^6}{N^2}\right).$$

The proof requires analyzing as intermediate measures of progress the projections on Π_{Q_2}, $\Pi_{\mathrm{Q+H}}$ and $\Pi_{\mathrm{Q_2+Q\cdot H}}$ as well. We start by upper bounding the quantum progress Δ^Q (see Definition 4.10) when doing one quantum query.

Lemma 6.11 (Progress Measure, Quantum Query)**.** *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ satisfies*

$$\Delta^Q(\Pi_{\mathrm{Q}}, |\phi\rangle) \leq \sqrt{\frac{10q}{N}}\,, \tag{6.15}$$

$$\Delta^Q(\Pi_{\mathrm{Q}_2}, |\phi\rangle) \leq \sqrt{\frac{10q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\|\,, \tag{6.16}$$

$$\Delta^Q(\Pi_{\mathrm{Q+H}}, |\phi\rangle) \leq \sqrt{\frac{10(c+q)}{N}}\,, \tag{6.17}$$

$$\Delta^Q(\Pi_{\mathrm{Q_2+Q\cdot H}}, |\phi\rangle) \leq \sqrt{\frac{10(c+q)}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \sqrt{\frac{10q}{N}}\|\Pi_{\mathrm{H}}|\phi\rangle\|\,. \tag{6.18}$$

Proof. The four inequalities follow by repeated applications of Facts 4.9, 4.14 and 6.7, Lemma 6.8 and the triangle inequality.

Equation (6.15). We have $\|\Pi_{\mathrm{Q}}\mathcal{R}^Q|\phi\rangle\| = \|\Pi_{\mathrm{Q}}\mathcal{R}^Q(\Pi_{\mathrm{Q}}+\Pi_{\overline{\mathrm{Q}}})|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}}|\phi\rangle\| + \sqrt{\frac{10q}{N}}$, where the last step is by Equation (6.2).

Equation (6.16). We have $\|\Pi_{\mathrm{Q}_2}\mathcal{R}^Q|\phi\rangle\| = \|\Pi_{\mathrm{Q}_2}\mathcal{R}^Q(\Pi_{\mathrm{Q}_2} + \Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}} + \Pi_{\overline{\mathrm{Q}}})|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}_2}|\phi\rangle\| + \|\Pi_{\mathrm{Q}_2}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}}|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}_2}|\phi\rangle\| + \sqrt{\frac{10q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\|$, where the second step uses that $\Pi_{\mathrm{Q}_2}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}} = 0$ (Fact 6.7) and the last step is by Equation (6.4) and the fact that $\|\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}}|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}}|\phi\rangle\|$.

Equation (6.17). We have $\|\Pi_{\mathrm{Q+H}}\mathcal{R}^Q|\phi\rangle\| = \|\Pi_{\mathrm{Q+H}}\mathcal{R}^Q(\Pi_{\mathrm{Q+H}} + \Pi_{\overline{\mathrm{Q+H}}})|\phi\rangle\| \leq \|\Pi_{\mathrm{Q+H}}|\phi\rangle\| + \|\Pi_{\mathrm{Q+H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q+H}}}|\phi\rangle\| \leq \|\Pi_{\mathrm{Q+H}}|\phi\rangle\| + \sqrt{\frac{10(c+q)}{N}}$, where the last step is by Equation (6.3).

Equation (6.18). We have

$$\begin{aligned}\|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^Q|\phi\rangle\| &= \|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^Q\big(\Pi_{\mathrm{Q_2+Q\cdot H}} + \Pi_{\overline{\mathrm{Q_2}}\cdot\overline{\mathrm{H}}}\Pi_{\mathrm{Q}} + \Pi_{\overline{\mathrm{Q}}}\Pi_{\mathrm{H}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\big)|\phi\rangle\| \\ &\leq \|\Pi_{\mathrm{Q_2+Q\cdot H}}|\phi\rangle\| + \|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q_2}}\cdot\overline{\mathrm{H}}}\Pi_{\mathrm{Q}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}}\Pi_{\mathrm{H}}|\phi\rangle\| \\ &\leq \|\Pi_{\mathrm{Q_2+Q\cdot H}}|\phi\rangle\| + \sqrt{\frac{10(c+q)}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \sqrt{\frac{10q}{N}}\|\Pi_{\mathrm{H}}|\phi\rangle\|\end{aligned}$$

where the second step uses the triangle inequality and Fact 6.7 (since $\Pi_{\mathrm{Q}_2}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}}$ and $\Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}$ are zero on the subspace $\mathbb{H}_{c,q}$, it implies that $\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}$ is also zero on $\mathbb{H}_{c,q}$). The last step uses Equation (6.5) to bound the middle term (noting that $\Pi_{\overline{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}}\Pi_{\overline{\mathrm{Q}_2}\cdot\overline{\mathrm{H}}}\Pi_{\mathrm{Q}} = \Pi_{\overline{\mathrm{Q}_2}\cdot\overline{\mathrm{H}}}\Pi_{\mathrm{Q}}$) and Equation (6.2) to bound the last term. □

We similarly analyze the classical progress Δ^C when doing one classical query.

Lemma 6.12 (Progress Measure, Classical Query)**.** *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one classical query on $|\phi\rangle$ are at most,*

$$\Delta^C(\Pi_{\mathrm{Q}}, |\phi\rangle) \le 0\,, \quad (6.19) \qquad \Delta^C(\Pi_{\mathrm{Q}+\mathrm{H}}, |\phi\rangle) \le \sqrt{\frac{8q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \frac{5q}{N}\,, \quad (6.20)$$

$$\Delta^C(\Pi_{\mathrm{Q}_2}, |\phi\rangle) \le 0\,, \quad (6.21) \quad \Delta^C(\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}, |\phi\rangle) \le \frac{5q}{N}\|\Pi_{\mathrm{Q}}|\phi\rangle\|^2 + \sqrt{\frac{3q}{N}}\|\Pi_{\mathrm{Q}_2}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}}|\phi\rangle\|\,. \quad (6.22)$$

Proof. The four inequalities follow by repeated applications of Facts 4.9, 4.14 and 6.7, Lemma 6.9, the triangle inequality and the Cauchy–Schwarz inequality.

Equations (6.19) *and* (6.21). Since $\|\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| = \|\Pi_{\mathrm{Q}_2}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}_2}}|\phi\rangle\| = 0$ by Fact 6.7, we have $\|\Pi_{\mathrm{Q}}\mathcal{R}^C|\phi\rangle\|^2 = \|\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\mathrm{Q}}|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q}}|\phi\rangle\|^2$ and $\|\Pi_{\mathrm{Q}_2}\mathcal{R}^C|\phi\rangle\|^2 = \|\Pi_{\mathrm{Q}_2}\mathcal{R}^C\Pi_{\mathrm{Q}_2}|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q}_2}|\phi\rangle\|^2$.

Equation (6.20). We first expand the norm $\|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C|\phi\rangle\|^2$ using the identity $\||a\rangle + |b\rangle\|^2 \le \||a\rangle\|^2 + \||b\rangle\|^2 + 2|\langle a|b\rangle|$ for unnormalized states $|a\rangle$ and $|b\rangle$,

$$\begin{aligned}
\|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C(\Pi_{\mathrm{Q}+\mathrm{H}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}})|\phi\rangle\|^2 \\
&= \|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{Q}+\mathrm{H}}|\phi\rangle + \Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\|^2 \\
&\le \|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{Q}+\mathrm{H}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\|^2 + 2|\langle\phi|\,\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle| \\
&\le \|\Pi_{\mathrm{Q}+\mathrm{H}}|\phi\rangle\|^2 + \frac{2q}{N} + 2|\langle\phi|\,\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle|
\end{aligned}$$

where the second line uses that $\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle = 0$ by Fact 6.7, the third line uses that $\Pi_{\mathrm{H}} \cdot \Pi_{\mathrm{Q}+\mathrm{H}} = \Pi_{\mathrm{H}}$ and the last line is by Equation (6.8).

Next, we consider the inner product term. Observe first that,

$$\langle\phi|\,\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle = \langle\phi|\,\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle + \langle\phi|\,\Pi_{\overline{\mathrm{Q}}\cdot\mathrm{X}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle \quad (6.23)$$

since $\Pi_{\mathrm{Q}+\mathrm{H}} = \Pi_{\mathrm{Q}} + \Pi_{\overline{\mathrm{Q}}\cdot\mathrm{X}\cdot\mathrm{H}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{X}}\cdot\mathrm{H}}$ and $\mathcal{R}^C\Pi_{\overline{\mathrm{X}}\cdot\mathrm{H}}|\phi_1\rangle \perp \mathcal{R}^C\Pi_{\overline{\mathrm{H}}}|\phi_2\rangle$ by Fact 6.7. The first term in the right-hand side of Equation (6.23) is at most $|\langle\phi|\,\Pi_{\mathrm{Q}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle| \le \|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\| \le \|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\| \le \sqrt{\frac{2q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\|$ by Cauchy–Schwarz inequality, the fact that $\Pi_{\mathrm{H}} \preceq \Pi_{\mathrm{Q}+\mathrm{H}}$ and Equation (6.8) (noting that $\Pi_{\overline{\mathrm{Q}+\mathrm{H}}} = \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}$). The second term is at most $|\langle\phi|\,\Pi_{\overline{\mathrm{Q}}\cdot\mathrm{X}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}\,|\phi\rangle| \le \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\mathrm{X}\cdot\mathrm{H}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\| \le \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{X}\cdot\mathrm{H}} \cdot \Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}+\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}}|\phi\rangle\| \le \frac{\sqrt{2}q}{N}$ by Cauchy–Schwarz inequality and Equations (6.8) and (6.12). This concludes the proof of Equation (6.20).

Equation (6.22). Following a similar reasoning as above, we have

$$\begin{aligned}
\|\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle + \Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}}|\phi\rangle\|^2 \\
&\le \|\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\|^2 + \frac{2q}{N}\|\Pi_{\mathrm{Q}}|\phi\rangle\|^2 + 2|\langle\phi|\,\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}}\,|\phi\rangle|
\end{aligned}$$

where we used Equation (6.10) and the fact that $\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}} = \Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}} = \Pi_{\mathrm{Q}} \cdot \Pi_{\overline{\mathrm{H}}}$ on $\mathbb{H}_{c,q}$ to upper bound

$$\|\Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}}|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q}_2+\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}_2}}\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}}|\phi\rangle\|^2 \le \frac{2q}{N}\|\Pi_{\mathrm{Q}}|\phi\rangle\|^2.$$

Next, we have

$$\langle\phi|\,\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^C\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot\overline{H}}}\,|\phi\rangle = \langle\phi|\,(\Pi_{\mathrm{Q_2}}+\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot X\cdot H}})\mathcal{R}^C\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot\overline{H}}}\,|\phi\rangle. \tag{6.24}$$

using that $\Pi_{\mathrm{Q_2+Q\cdot H}} = \Pi_{\mathrm{Q_2}} + \Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot X\cdot H}} + \Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot\overline{X}\cdot H}}$ and $\mathcal{R}^C\Pi_{\mathrm{\overline{X}\cdot H}}|\phi_1\rangle \perp \mathcal{R}^C\Pi_{\overline{\mathrm{H}}}|\phi_2\rangle$ by Fact 6.7. Finally, by Cauchy–Schwarz inequality, the right-hand side of Equation (6.24) is at most $\|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C(\Pi_{\mathrm{Q_2}}+\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot X\cdot H}})|\phi\rangle\|\cdot\|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot\overline{H}}}|\phi\rangle\|$. The first factor is at most $\|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C(\Pi_{\mathrm{Q_2}}+\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot X\cdot H}})|\phi\rangle\| \le \|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\mathrm{Q_2}}|\phi\rangle\| + \|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{X\cdot H}}\Pi_{\mathrm{Q}}|\phi\rangle\| \le \|\Pi_{\mathrm{Q_2}}|\phi\rangle\| + \sqrt{\frac{q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\|$ by the triangle inequality and Equation (6.12) (using that $\|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{X\cdot H}}\Pi_{\mathrm{Q}}|\phi\rangle\| = \|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{X\cdot H}}\Pi_{\mathrm{Q}}|\phi\rangle\|$ by Fact 6.7 and $\|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{X\cdot H}}\Pi_{\mathrm{Q}}|\phi\rangle\| \le \|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{X\cdot H}}\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q}}|\phi\rangle\|$). The second factor is bounded similarly as $\|\Pi_{\mathrm{Q\cdot H}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q_2}}}\Pi_{\mathrm{Q\cdot\overline{H}}}|\phi\rangle\| \le \sqrt{\frac{2q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\|$ by Equation (6.10). □

We conclude this section with the proof of our main proposition.

Proof of Proposition 6.4. The proof is done by induction on the number of queries, unfolding the inequalities of Lemmas 6.11 and 6.12. First,

$$\|\Pi_{\mathrm{Q}}|\phi_{c+q}\rangle\|^2 \le O\left(\frac{q^3}{N}\right) \quad\text{and}\quad \|\Pi_{\mathrm{Q_2}}|\phi_{c+q}\rangle\|^2 \le O\left(\frac{q^6}{N^2}\right), \tag{6.25}$$

using Equation (6.15) and Equation (6.16) respectively. Next, using Equation (6.17), we have that $\|\Pi_{\mathrm{Q+H}}\mathcal{R}^Q|\phi\rangle\| \le \|\Pi_{\mathrm{Q+H}}|\phi\rangle\| + O\left(\sqrt{\frac{c+q}{N}}\right)$ and using Equations (6.20) and (6.25), we have that $\|\Pi_{\mathrm{Q+H}}\mathcal{R}^C|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q+H}}|\phi\rangle\|^2 + O\left(\frac{q^2}{N}\right)$, which gives

$$\|\Pi_{\mathrm{Q+H}}|\phi_{c+q}\rangle\|^2 \le O\left(\frac{cq^2+q^3}{N}\right). \tag{6.26}$$

Finally, $\|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^Q|\phi\rangle\| \le \|\Pi_{\mathrm{Q_2+Q\cdot H}}|\phi\rangle\| + O\left(\frac{\sqrt{cq^3+q^4}}{N}\right)$ (using Equations (6.18), (6.25) and (6.26) together with the fact that $\|\Pi_{\mathrm{H}}|\phi\rangle\| \le \|\Pi_{\mathrm{Q+H}}|\phi\rangle\|$) and $\|\Pi_{\mathrm{Q_2+Q\cdot H}}\mathcal{R}^C|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q_2+Q\cdot H}}|\phi\rangle\|^2 + O\left(\frac{q^5}{N^2}\right)$ using Equations (6.22) and (6.25), which gives

$$\|\Pi_{\mathrm{Q\cdot H}}|\phi\rangle\|^2 \le \|\Pi_{\mathrm{Q_2+Q\cdot H}}|\phi\rangle\|^2 \le O\left(\frac{cq^5}{N^2} + \frac{cq^5+q^6}{N^2}\right) \le O\left(\frac{cq^5+q^6}{N^2}\right). \qquad \square$$

6.5 Classical Collisions

In this section, we give progress measures on three projections: (1) finding a classical collision, (2) finding a hybrid collision but no classical ones and (3) finding quantum collisions only. We start with the case of quantum queries, which is simpler to analyze.

Lemma 6.5 (Progress Measure, Quantum Query). *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ satisfies*

$$\Delta^Q(\Pi_{\mathrm{C}}, |\phi\rangle) = 0\,, \tag{6.27}$$

$$\Delta^Q(\Pi_{\mathrm{H\cdot\overline{C}}}, |\phi\rangle) \le \sqrt{\frac{10c}{N}}\,, \tag{6.28}$$

$$\Delta^Q(\Pi_{\mathrm{Q\cdot\overline{H}\cdot\overline{C}}}, |\phi\rangle) \le \sqrt{\frac{20(c+q)}{N}}\,. \tag{6.29}$$

Proof. Equation (6.27) follows directly from Fact 6.7. Equation (6.28) is obtained by applying the triangle inequality, Fact 6.7 and Equation (6.6): $\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q|\phi\rangle\| = \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}})|\phi\rangle\| \leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{H}}\mathcal{R}^Q\Pi_{\overline{\mathrm{H}}}|\phi\rangle\| \leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \sqrt{\frac{10c}{N}}$. Similarly, for Equation (6.29), we have $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q|\phi\rangle\| = \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{Q}\cdot\mathrm{H}} + \Pi_{\overline{\mathrm{Q}}})|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\overline{\mathrm{H}}}\mathcal{R}^Q\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| \leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \sqrt{\frac{10c}{N}} + \sqrt{\frac{10q}{N}}$ by using Equations (6.2) and (6.11). $\square$

We now analyze the case of classical queries.

Lemma 6.6 (Progress Measure, Classical Query). *Given two integers c, q and a state $|\phi\rangle \in \mathbb{H}_{c,q}$ with norm at most 1, the progress caused by one classical query on $|\phi\rangle$ are at most,*

$$\Delta^C(\Pi_{\mathrm{C}}, |\phi\rangle) \leq 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \frac{4c}{N}, \tag{6.30}$$

$$\Delta^C(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq -\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\sqrt{\frac{q}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \frac{7q}{N}, \tag{6.31}$$

$$\Delta^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq -\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \sqrt{\frac{8c}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\| + \frac{2c}{N}. \tag{6.32}$$

Proof. The four inequalities follow by repeated applications of Facts 4.9, 4.14 and Fact 6.7, Lemma 6.9, the triangle inequality and the Cauchy–Schwarz inequality.

Equation (6.30). The states $\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{C}}|\phi\rangle$ and $\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{C}}}|\phi\rangle$ are orthogonal by Fact 6.7. Therefore, $\|\Pi_{\mathrm{C}}\mathcal{R}^C|\phi\rangle\|^2 = \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{C}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|^2$. We upper bound the last term using the triangle inequality and Equation (6.14) (noting that $\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} = \Pi_{\overline{\mathrm{H}+\mathrm{C}}}$):

$$\begin{aligned}\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|^2 &= \|\Pi_{\mathrm{C}}\mathcal{R}^C(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\leq 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq 2\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + \frac{4c}{N}.\end{aligned}$$

Equation (6.31). We have the following inequalities,

$$\begin{aligned}\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2|\langle\phi|\,\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\,|\phi\rangle| \\ &\leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2|\langle\phi|\,\Pi_{\mathrm{X}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\,|\phi\rangle|\end{aligned} \tag{6.33}$$

where Fact 6.7 has been used at the first and third lines. We now bound each of the three terms separately. The first one is at most

$$\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$$

since $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}} \preceq \mathbb{I}$ and $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}$, Π_{C} are orthogonal. For the second term in Equation (6.33), by the triangle inequality and Equation (6.8),

$$\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \leq 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \frac{4q}{N}.$$

Finally, for the last term in Equation (6.33), we have

$$\begin{aligned}|\langle\phi|\,\Pi_{\mathrm{X}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\,|\phi\rangle| &\leq \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{X}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \\ &\leq \sqrt{\frac{q}{N}} \cdot \left(\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|\right) \\ &\leq \sqrt{\frac{q}{N}} \cdot \left(\|\Pi_{\mathrm{Q}}|\phi\rangle\| + \sqrt{\frac{2q}{N}}\right)\end{aligned}$$

where the first line is by the Cauchy–Schwarz inequality, the second line is by Equation (6.12) and the triangle inequality, and the last line is by Equation (6.8). By adding the three inequalities together, this concludes the proof of Equation (6.31).

Equation (6.32). We first have $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C|\phi\rangle = \Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle$ by Fact 6.7. Thus, using the identity $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} = \Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{Q}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}$,

$$\begin{aligned}
\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{Q}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\
&\leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \\
&\quad + \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \\
&\leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \sqrt{\frac{2c}{N}}\|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\| + \frac{2c}{N} \\
&\leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}^C\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \sqrt{\frac{8c}{N}}\|\Pi_{\mathrm{Q}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\mathrm{H}}|\phi\rangle\| + \frac{2c}{N}.
\end{aligned}$$

where the second line uses the Cauchy–Schwarz inequality, the second inequality is by Equation (6.13) and the last line follows by $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}} \preceq \mathbb{I}$ and $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$, $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}$ are orthogonal. □

References

[AA18] S. Aaronson and A. Ambainis. "Forrelation: A Problem That Optimally Separates Quantum from Classical Computing". In: *SIAM Journal on Computing* 47.3 (2018), 982–)1038 (cit. on p. 1).

[Aar12] S. Aaronson. "Impossibility of Succinct Quantum Proofs for Collision-Freeness". In: *Quantum Information & Computation* 12.1–2 (2012), pp. 21–28 (cit. on p. 3).

[ABK+22] G. Alagic, C. Bai, J. Katz, C. Majenz, and P. Struck. *Post-Quantum Security of the (Tweakable) FX Construction, and Applications*. Cryptology ePrint Archive, Paper 2022/1097. https://eprint.iacr.org/2022/1097. 2022 (cit. on pp. 2, 3).

[ABKM22] G. Alagic, C. Bai, J. Katz, and C. Majenz. "Post-Quantum Security of the Even-Mansour Cipher". In: *Proceedings of the 41st International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2022, pp. 458–487 (cit. on pp. 2, 3).

[ADG+17] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck. "Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3". In: *Proceedings of the 24th Conference on Selected Areas in Cryptography (SAC)*. 2017, pp. 317–337 (cit. on p. 2).

[AGS22] A. S. Arora, A. Gheorghiu, and U. Singh. *Oracle Separations of Hybrid Quantum-Classical Circuits*. arXiv:2201.01904 [quant-ph]. 2022 (cit. on pp. 2, 3).

[AHU19] A. Ambainis, M. Hamburg, and D. Unruh. "Quantum Security Proofs Using Semi-classical Oracles". In: *Proceedings of the 39th International Cryptology Conference (CRYPTO)*. 2019, pp. 269–295 (cit. on p. 3).

[AKKT20] S. Aaronson, R. Kothari, W. Kretschmer, and J. Thaler. "Quantum Lower Bounds for Approximate Counting via Laurent Polynomials". In: *Proceedings of the 35th Computational Complexity Conference (CCC)*. 2020 (cit. on p. 3).

[Amb02] A. Ambainis. "Quantum Lower Bounds by Quantum Arguments". In: *Journal of Computer and System Sciences* 64.4 (2002), pp. 750–767 (cit. on p. 3).

[AMRS20] G. Alagic, C. Majenz, A. Russell, and F. Song. "Quantum-Access-Secure Message Authentication via Blind-Unforgeability". In: *Proceedings of the 39th International Conference on the Theory and Applications of Cryptographic Techniques (EURO-CRYPT)*. 2020, pp. 788–817 (cit. on p. 3).

[AS04] S. Aaronson and Y. Shi. "Quantum Lower Bounds for the Collision and the Element Distinctness Problems". In: *Journal of the ACM* 51.4 (2004), pp. 595–605 (cit. on p. 4).

[AŠW09] A. Ambainis, R. Špalek, and R. de Wolf. "A New Quantum Lower Bound Method, with Applications to Direct Product Theorems and Time-Space Tradeoffs". In: *Algorithmica* 55.3 (2009), pp. 422–461 (cit. on p. 3).

[BBC+01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. "Quantum Lower Bounds by Polynomials". In: *Journal of the ACM* 48.4 (2001), pp. 778–797 (cit. on p. 3).

[BDF+11] D. Boneh, O. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. "Random Oracles in a Quantum World". In: *Proceedings of the 17th International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*. 2011, pp. 41–69 (cit. on p. 2).

[BHH+19] N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, and E. Persichetti. "Tighter Proofs of CCA Security in the Quantum Random Oracle Model". In: *Proceedings of the 17th Conference on Theory of Cryptography (TCC)*. 2019, pp. 61–90 (cit. on p. 3).

[BHMT02] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. "Quantum Amplitude Amplification and Estimation". In: *Contemporary Mathematics* 305 (2002), pp. 53–74 (cit. on p. 1).

[BHN+19] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher. "Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm". In: *Proceedings of the 25th International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*. 2019, pp. 552–583 (cit. on p. 2).

[BHT98] G. Brassard, P. Høyer, and A. Tapp. "Quantum Cryptanalysis of Hash and Claw-Free Functions". In: *Proceedings of the 3rd Latin American Symposium on Theoretical Informatics (LATIN)*. 1998, pp. 163–169 (cit. on pp. 1, 2, 4).

[BLZ21] J. Blocki, S. Lee, and S. Zhou. "On the Security of Proofs of Sequential Work in a Post-Quantum World". In: *Proceedings of the 2nd Conference on Information-Theoretic Cryptography (ITC)*. 2021, 22:1–22:27 (cit. on p. 3).

[BV97] E. Bernstein and U. V. Vazirani. "Quantum Complexity Theory". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1411–1473 (cit. on p. 1).

[BW02] H. Buhrman and R. de Wolf. "Complexity Measures and Decision Tree Complexity: A Survey". In: *Theoretical Computer Science* 288.1 (2002), pp. 21–43 (cit. on p. 1).

[CCL20] N.-H. Chia, K.-M. Chung, and C.-Y. Lai. "On the Need for Large Quantum Depth". In: *Proceedings of the 52nd Symposium on Theory of Computing (STOC)*. 2020, pp. 902–915 (cit. on pp. 2, 3, 8).

[CFHL21] K.-M. Chung, S. Fehr, Y.-H. Huang, and T.-N. Liao. "On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work". In: *Proceedings of the 40th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2021, pp. 598–629 (cit. on pp. 3, 14).

[CGLQ20] K.-M. Chung, S. Guo, Q. Liu, and L. Qian. "Tight Quantum Time-Space Tradeoffs for Function Inversion". In: *Proceedings of the 61st Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 673–684 (cit. on p. 3).

[CH22] N.-H. Chia and S.-H. Hung. *Classical Verification of Quantum Depth*. arXiv: 2205.04656 [quant-ph]. 2022 (cit. on pp. 2, 3).

[CLQ20] K.-M. Chung, T.-N. Liao, and L. Qian. "Lower Bounds for Function Inversion with Quantum Advice". In: *Proceedings of the 1st Conference on Information-Theoretic Cryptography (ITC)*. 2020, 8:1–8:15 (cit. on p. 3).

[CM20] M. Coudron and S. Menda. "Computations with Greater Quantum Depth Are Strictly More Powerful (Relative to an Oracle)". In: *Proceedings of the 52nd Symposium on Theory of Computing (STOC)*. 2020, pp. 889–901 (cit. on pp. 2, 3).

[CMS19] A. Chiesa, P. Manohar, and N. Spooner. "Succinct Arguments in the Quantum Random Oracle Model". In: *Proceedings of the 17th Conference on Theory of Cryptography (TCC)*. 2019, pp. 1–29 (cit. on pp. 3, 14).

[CMSZ19] J. Czajkowski, C. Majenz, C. Schaffner, and S. Zur. *Quantum Lazy Sampling and Game-Playing Proofs for Quantum Indifferentiability*. `arXiv:1904.11477v1 [quant-ph]`. 2019 (cit. on p. 3).

[CW00] R. Cleve and J. Watrous. "Fast Parallel Circuits for the Quantum Fourier Transform". In: *Proceedings of the 41st Symposium on Foundations of Computer Science (FOCS)*. 2000, pp. 526–536 (cit. on p. 2).

[DJ92] D. Deutsch and R. Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society of London Series A* 439.1907 (1992), pp. 553–558 (cit. on p. 1).

[GLLZ21] S. Guo, Q. Li, Q. Liu, and J. Zhang. "Unifying Presampling via Concentration Bounds". In: *Proceedings of the 19th Conference on Theory of Cryptography (TCC)*. 2021, pp. 177–208 (cit. on p. 3).

[GLRS16] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt. "Applying Grover's Algorithm to AES: Quantum Resource Estimates". In: *Proceedings of the 7th International Workshop on Post-Quantum Cryptography (PQCrypto)*. 2016, pp. 29–43 (cit. on p. 2).

[GR04] L. K. Grover and J. Radhakrishnan. *Quantum Search for Multiple Items using Parallel Queries*. `arXiv:quant-ph/0407217`. 2004 (cit. on p. 3).

[Gro97] L. K. Grover. "Quantum Mechanics Helps in Searching for a Needle in a Haystack". In: *Physical Review Letters* 79.2 (1997), pp. 325–328 (cit. on pp. 1, 2, 4).

[HG22] A. Hasegawa and F. L. Gall. *An Optimal Oracle Separation of Classical and Quantum Hybrid Schemes*. `arXiv:2205.04633 [quant-ph]`. 2022 (cit. on pp. 2, 3).

[HI19] A. Hosoyamada and T. Iwata. "4-Round Luby-Rackoff Construction is a qPRP". In: *Proceedings of the 25th International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*. 2019, pp. 145–174 (cit. on p. 3).

[HM21] Y. Hamoudi and F. Magniez. "Quantum Time-Space Tradeoff for Finding Multiple Collision Pairs". In: *Proceedings of the 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*. 2021, 1:1–1:21 (cit. on p. 3).

[HS18] A. Hosoyamada and Y. Sasaki. "Cryptanalysis Against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations". In: *Proceedings of the Topics in Cryptology – CT-RSA 2018*. 2018, pp. 198–218 (cit. on p. 2).

[HXY19] M. Hhan, K. Xagawa, and T. Yamakawa. "Quantum Random Oracle Model with Auxiliary Input". In: *Proceedings of the 25th International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT)*. 2019, pp. 584–614 (cit. on p. 3).

[JMW17] S. Jeffery, F. Magniez, and R. de Wolf. "Optimal Parallel Quantum Query Algorithms". In: *Algorithmica* 79.2 (2017), pp. 509–529 (cit. on p. 3).

[JNRV20] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC". In: *Proceedings of the 39th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2020, pp. 280–310 (cit. on p. 2).

[JST21] J. Jaeger, F. Song, and S. Tessaro. "Quantum Key-Length Extension". In: *Proceedings of the 19th Conference on Theory of Cryptography (TCC)*. 2021, pp. 209–239 (cit. on pp. 2, 3).

[Kit95] A. Kitaev. *Quantum Measurements and the Abelian Stabilizer Problem*. `arXiv:quant-ph/9511026`. 1995 (cit. on p. 1).

[KŠW07] H. Klauck, R. Špalek, and R. de Wolf. "Quantum and Classical Strong Direct Product Theorems and Optimal Time-Space Tradeoffs". In: *SIAM Journal on Computing* 36.5 (2007), pp. 1472–1493 (cit. on p. 3).

[LZ19a] Q. Liu and M. Zhandry. "On Finding Quantum Multi-collisions". In: *Proceedings of the 38th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2019, pp. 189–218 (cit. on p. 3).

[LZ19b] Q. Liu and M. Zhandry. "Revisiting Post-Quantum Fiat-Shamir". In: *Proceedings of the 39th International Cryptology Conference (CRYPTO)*. 2019, pp. 326–355 (cit. on p. 3).

[NABT15] A. Nayebi, S. Aaronson, A. Belovs, and L. Trevisan. "Quantum Lower Bound for Inverting a Permutation with Advice". In: *Quantum Information & Computation* 15.11&12 (2015), pp. 901–913 (cit. on p. 3).

[Ros21] A. Rosmanis. *Tight Bounds for Inverting Permutations via Compressed Oracle Arguments*. `arXiv:2103.08975 [quant-ph]`. 2021 (cit. on p. 3).

[Ros22] A. Rosmanis. *Hybrid Quantum-Classical Search Algorithms*. `arXiv:2202.11443 [quant-ph]`. 2022 (cit. on pp. 1–4, 6).

[RS08] O. Regev and L. Schiff. "Impossibility of a Quantum Speed-Up with a Faulty Oracle". In: *Proceedings of the 35th International Colloquium on Automata, Languages, and Programming (ICALP)*. 2008, pp. 773–781 (cit. on p. 3).

[Sho97] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509 (cit. on p. 1).

[Sim97] D. R. Simon. "On the Power of Quantum Computation". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1474–1483 (cit. on p. 1).

[ST19] A. A. Sherstov and J. Thaler. *Vanishing-Error Approximate Degree and QMA Complexity*. `arXiv:1909.07498 [cs.CC]`. 2019 (cit. on p. 3).

[SZ19] X. Sun and Y. Zheng. *Hybrid Decision Trees: Longer Quantum Time is Strictly More Powerful*. `arXiv:1911.13091 [cs.CC]`. 2019 (cit. on p. 3).

[Zal99] C. Zalka. "Grover's Quantum Searching Algorithm is Optimal". In: *Physical Review A* 60 (1999), pp. 2746–2751 (cit. on p. 3).

[Zha15] M. 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. 4).

[Zha19] M. Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *Proceedings of the 39th International Cryptology Conference (CRYPTO)*. 2019, pp. 239–268 (cit. on pp. 1–5, 14, 19).

A Missing Proofs for Section 4

A.1 Resampling Lemma (Lemmas 4.6 and 4.7)

Proof of Lemma 4.6. We only prove the third item, corresponding to $H(x) = \star$, $D(x) \neq \perp$, $p \neq 0$, as it is the most involved of the three. The operator $\mathcal{R}^Q = S^\dagger \mathcal{O}^Q S$ acts as a control on all registers except $\mathcal{D}_x$, which contains the x-th entry of the database. Let $z = D(x) \neq \perp$ be the value contained in the register $\mathcal{D}_x$. Writing $|z\rangle = \frac{1}{\sqrt{N}} \sum_{p \in [N]} \omega^{-pz} |\hat{p}\rangle$ in the Fourier basis, we can see that S maps $|z\rangle_{\mathcal{D}_x}$ to

$$\frac{1}{\sqrt{N}} \sum_{p \in [N]} \omega^{-pz} |\hat{p}\rangle + \frac{1}{\sqrt{N}} |\perp\rangle - \frac{1}{\sqrt{N}} |\hat{0}\rangle = |z\rangle + \frac{1}{\sqrt{N}} |\perp\rangle - \frac{1}{N} \sum_{y \in [N]} |y\rangle,$$

while acting as control on the other registers. Applying $\mathcal{O}^Q$ to the above state, we get

$$\omega^{pz} |z\rangle + \frac{1}{\sqrt{N}} |\perp\rangle - \frac{1}{N} \sum_{y \in [N]} \omega^{py} |y\rangle = \frac{\omega^{pz}}{\sqrt{N}} \sum_{p' \in [N]} \omega^{-p'z} |\hat{p}'\rangle + \frac{1}{\sqrt{N}} |\perp\rangle - \frac{1}{\sqrt{N}} |\hat{p}\rangle.$$

Applying $S^\dagger$ to the above and simplifying we get

$$\frac{\omega^{pz}}{\sqrt{N}} \sum_{p' \in [N]} \omega^{-p'z} |\hat{p}'\rangle + \frac{\omega^{pz}}{\sqrt{N}} |\perp\rangle + \frac{1 - \omega^{pz}}{\sqrt{N}} |\hat{0}\rangle - \frac{1}{\sqrt{N}} |\hat{p}\rangle = \omega^{pz} |z\rangle + \frac{\omega^{pz}}{\sqrt{N}} |\perp\rangle + \sum_{y \in [N]} \frac{1 - \omega^{pz} - \omega^{py}}{N} |y\rangle.$$

thus proving the third item. □

Proof of Lemma 4.7. We only prove the third item, corresponding to $H(x) = \star$, $D(x) \neq \perp$. Let $|H\rangle_{\mathcal{H}} = |(x_1, y_1), \ldots, (x_i, y_i), \star, \ldots, \star\rangle_{\mathcal{H}}$, for some integer i, denote the value contained in the history register. The operator $\mathcal{R}^C = S^\dagger \mathcal{O}^C S$ acts as a control on all registers except $\mathcal{H}_{i+1}\mathcal{D}_x$, which contain $|\star, z\rangle_{\mathcal{H}_{i+1}\mathcal{D}_x}$ for some $z = D(x) \neq \perp$. Similarly as in the above proof of Lemma 4.6, after applying the first two operators $\mathcal{O}^C S$, this state gets mapped to

$$\omega^{pz} |(x, z), z\rangle + \frac{1}{\sqrt{N}} |(x, \perp), \perp\rangle - \frac{1}{N} \sum_{y \in [N]} \omega^{py} |(x, y), y\rangle.$$

where the value contained in the database register $\mathcal{D}_x$ has been appended to the history (by definition of a the classical query operator $\mathcal{O}^C$). Finally, applying $S^\dagger$ to the above state does nothing since the query index x is now contained in the history. □

A.2 Progress Overlap Lemmas (Lemmas 4.12 and 4.13)

We first give the proof for Lemma 4.13 (classical query) as it differs the most from previous work on the compressed oracle. The proof will be next adapted for Lemma 4.12 (quantum query).

Proof of Lemma 4.13. Let $\Pi_{\overline{\mathrm{P}}} |\phi\rangle = \sum_{x,p,w,H,D} \alpha_{x,p,w,H,D} |x, p, w\rangle |H\rangle |D\rangle \in \mathbb{H}_{c,q} \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ be any state supported over consistent basis-states evaluating the predicate P to false. We show that, after making a classical query, the probability of satisfying P is at most $\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_{\overline{\mathrm{P}}} |\phi\rangle\|^2 \leq 2\gamma \cdot \|\Pi_{\overline{\mathrm{P}}} |\phi\rangle\|^2$. We define three projections Π_1, Π_2, Π_3 such that $\Pi_1 + \Pi_2 + \Pi_3 = \Pi_{\overline{\mathrm{P}}}$.

- Π_1: all basis states $|x, p, w, H, D\rangle \in \mathbb{H}_{c,q} \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) = \star$ and $D(x) = \perp$.
- Π_2: all basis states $|x, p, w, H, D\rangle \in \mathbb{H}_{c,q} \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) = \star$ and $D(x) \neq \perp$.
- Π_3: all basis states $|x, p, w, H, D\rangle \in \mathbb{H}_{c,q} \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) \neq \star$.

Below, we prove the inequalities $\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_1 |\phi\rangle\|^2 \leq \gamma \|\Pi_1 |\phi\rangle\|^2$, $\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_2 |\phi\rangle\|^2 \leq \gamma \|\Pi_2 |\phi\rangle\|^2$ and $\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_3 |\phi\rangle\| = 0$. Hence, by the triangle inequality and Cauchy–Schwarz inequality, we conclude that

$$\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_{\overline{\mathrm{P}}} |\phi\rangle\|^2 \leq \left(\|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_1 |\phi\rangle\| + \|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_2 |\phi\rangle\| + \|\Pi_{\mathrm{P}} \mathcal{R}^C \Pi_3 |\phi\rangle\| \right)^2 \leq 2\gamma \|\Pi_{\overline{\mathrm{P}}} |\phi\rangle\|^2.$$

Analysis of Π_1. The projection Π_1 corresponds to *sampling* a new outcome at x. We have

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_1|\phi\rangle\|^2 &= \Bigg\|\Pi_{\mathrm{P}}\mathcal{R}^C \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\bot}} \alpha_{x,p,w,H,D}|x,p,w\rangle|H\rangle|D\rangle\Bigg\|^2 \\
&= \Bigg\|\Pi_{\mathrm{P}} \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\bot}} \alpha_{x,p,w,H,D}|x,p,w\rangle\Bigg(\sum_{y\in[N]}\frac{\omega^{py}}{\sqrt{N}}|H_{x\leftarrow y}\rangle|D_{x\leftarrow y}\rangle\Bigg)\Bigg\|^2 \\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\bot}} |\alpha_{x,p,w,H,D}|^2\cdot \Pr_{y\leftarrow[N]}\big[(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y})\in \mathrm{P}^{-1}(\textsc{True})\big] \\
&\le \gamma\|\Pi_1|\phi\rangle\|^2.
\end{aligned}$$

The first line is by definition of Π_1. The second line is by Lemma 4.7. The third line uses the orthogonality of the basis states. Finally, the last line is by Equation (4.5).

Analysis of Π_2. The projection Π_2 corresponds to *resampling* a new outcome at index x (see the third item of Lemma 4.7). There are three components and the only states that may be in the support of Π_{P} after the query is done are those for which $D(x)$ is resampled to a different value $y \neq D(x)$. Indeed, the other two cases are where $D(x) = \bot$ gets removed or $D(x)$ remains unchanged in the database. The former case cannot make the predicate true because of the database monotone property (Definition 4.11), the latter case cannot either because of the condition stated in Equation (4.6). Hence, we have

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_2|\phi\rangle\|^2 &= \Bigg\|\Pi_{\mathrm{P}}\mathcal{R}^C \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\bot}} \alpha_{x,p,w,H,D}|x,p,w\rangle|H\rangle|D\rangle\Bigg\|^2 \\
&= \Bigg\|\Pi_{\mathrm{P}} \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\bot}} \sum_{y\in[N]} \alpha_{x,p,w,H,D}\frac{\omega^{py}}{N}|x,p,w\rangle|H_{x\leftarrow y}\rangle|D_{x\leftarrow y}\rangle\Bigg\|^2.
\end{aligned}$$

Next, observe that for any two distinct tuples $(x,p,w,H,D_{x\leftarrow\bot},y) \neq (x',p',w',H',D'_{x'\leftarrow\bot},y')$, the basis states $|x,p,w\rangle|H_{x\leftarrow y}\rangle|D_{x\leftarrow y}\rangle$ and $|x',p',w'\rangle|H'_{x'\leftarrow y'}\rangle|D'_{x'\leftarrow y'}\rangle$ must be orthogonal. Thus, we can exploit this orthogonality property to simplify the above expression as follows.

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_2|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y}} \Bigg\|\Pi_{\mathrm{P}}\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{py}}{N}|x,p,w\rangle|H_{x\leftarrow y}\rangle|D\rangle\Bigg\|^2 \\
&= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{P}(x,p,w,H_{x\leftarrow y},D)=\textsc{True}}} \Bigg|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{py}}{N}\Bigg|^2.
\end{aligned}$$

Applying the Cauchy–Schwarz inequality, we have

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_2|\phi\rangle\|^2 &\leq \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{P}(x,p,w,H_{x\leftarrow y},D)=\textsc{True}}} \sum_{z\in[N]} \frac{|\alpha_{x,p,w,H,D_{x\leftarrow z}}|^2}{N}\\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} \left(\sum_{y\in[N]:\mathrm{P}(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y})=\textsc{True}} \frac{|\alpha_{x,p,w,H,D}|^2}{N}\right)\\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\big[(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y})\in\mathrm{P}^{-1}(\textsc{True})\big].
\end{aligned}$$

Finally, for each $|x,p,w,H,D\rangle$ in the support of Π_2, we must have $\mathrm{P}(x,p,w,H,D_{x\leftarrow\perp}) = \textsc{False}$ by the database monotone property (see Definition 4.11). Hence, by Equation (4.5), the above inequality implies that $\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_2|\phi\rangle\|^2 \leq \gamma\cdot\|\Pi_2|\phi\rangle\|^2$.

Analysis of Π_3. By Lemma 4.7, the operator $\mathcal{R}^C$ maps any state $|x,p,w\rangle|H\rangle|D\rangle\in\mathrm{supp}(\Pi_3)$ to $\omega^{pD(x)}|x,p,w\rangle|H_{x\leftarrow D(x)}\rangle|D\rangle$ since $H(x)\neq\star$. Moreover, H and $H_{x\leftarrow D(x)}$ have the same function representation (since the initial state is history-database consistent). Thus, by the history invariant property (see Definition 4.11), we have $\mathrm{P}(x,p,w,H_{x\leftarrow D(x)},D)=\textsc{False}$ and $\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_3|\phi\rangle\| = 0$. □

The proof of Lemma 4.12 is similar to the above one, the main difference being that quantum queries do not act on the history register.

Proof of Lemma 4.12. Let $\Pi_{\overline{\mathrm{P}}}|\phi\rangle = \sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w\rangle|H\rangle|D\rangle \in \mathbb{H}_{c,q}\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$. We will prove that $\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \leq 10\gamma\cdot\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2$. We first define three projections Π_1,Π_2,Π_3 such that $\Pi_1+\Pi_2+\Pi_3=\Pi_{\overline{\mathrm{P}}}$.

- Π_1: all basis states $|x,p,w,H,D\rangle\in\mathbb{H}_{c,q}\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)=\star$, $D(x)=\perp$, $p\neq 0$.
- Π_2: all basis states $|x,p,w,H,D\rangle\in\mathbb{H}_{c,q}\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)=\star$, $D(x)\neq\perp$, $p\neq 0$.
- Π_3: all basis states $|x,p,w,H,D\rangle\in\mathbb{H}_{c,q}\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)\neq\star$ or $p=0$.

Below, we prove that $\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_1|\phi\rangle\|^2 \leq \gamma\|\Pi_1|\phi\rangle\|^2$, $\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_2|\phi\rangle\|^2 \leq 9\gamma\|\Pi_2|\phi\rangle\|^2$ and $\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_3|\phi\rangle\| = 0$. Hence, by the triangle and Cauchy–Schwarz inequalities, we conclude that $\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \leq 10\gamma\cdot\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2$.

Analysis of Π_1. The effect of applying $\mathcal{R}^Q$ on a basis state in the support of Π_1 is described in the second item of Lemma 4.6. Similarly to the analysis of Π_1 in the proof of Lemma 4.13, we deduce that

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_1|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,p\neq 0}} |\alpha_{x,p,w,H,D}|^2\cdot\Pr_{y\leftarrow[N]}\big[(x,p,w,H,D_{x\leftarrow y})\in\mathrm{P}^{-1}(\textsc{True})\big]\\
&\leq \gamma\|\Pi_1|\phi\rangle\|^2.
\end{aligned}$$

where the second line is by Equation (4.4).

Analysis of Π_2. The effect of applying $\mathcal{R}^Q$ on a basis state in the support of Π_2 is described in the third item of Lemma 4.6. By using the bound $|1-\omega^{pD(x)}-\omega^{py}|\le 3$ on the term displayed there, we can follow a similar analysis as in the proof of Lemma 4.13 for Π_2 and deduce that

$$\begin{aligned}\|\Pi_{\mathrm{P}}\mathcal{R}^Q\Pi_2|\phi\rangle\|^2 &\le 9\sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp,p\neq 0}}|\alpha_{x,p,w,H,D}|^2\cdot\Pr_{y\leftarrow[N]}\left[(x,p,w,H,D_{x\leftarrow y})\in\mathrm{P}^{-1}(\textsc{True})\right]\\ &\le 9\gamma\|\Pi_2|\phi\rangle\|^2.\end{aligned}$$

where the second line is by Equation (4.4).

Analysis of Π_3. By the first item in Lemma 4.6, the operator $\mathcal{R}^Q$ maps any basis state in the support of Π_3 to itself, up to a phase factor. Thus, we have $\|\Pi_{\mathrm{P}}\mathcal{R}^C\Pi_3|\phi\rangle\|=0$. $\square$

B Missing Proofs for Section 5

Proof of Proposition 5.3. The first equality is due to the fact that a quantum query $\mathcal{R}^Q$ only uses the register $\mathcal{H}$ as a control. Thus, for any basis state in the support of the projector $\Pi_{\overline{\mathrm{C}}}$, which does not contain a zero preimage in H by definition, the state after applying the quantum query $\mathcal{R}^Q$ will still not contain a zero preimage in H and thus be orthogonal to the support of Π_{C}. On the other hand, a basis state in the support of Π_{C} contains a zero preimage in H and remains in the support even after applying $\mathcal{R}^Q$. Since $\mathbb{I}=\Pi_{\overline{\mathrm{C}}}+\Pi_{\mathrm{C}}$ and the projectors in the summation are orthogonal, the statement $\|\Pi_{\mathrm{C}}\mathcal{R}^Q|\phi\rangle\|=\|\Pi_{\mathrm{C}}|\phi\rangle\|$ follows and hence $\Delta^Q(\Pi_{\mathrm{C}},|\phi\rangle)=0$.

To see the second inequality, we consider the basis states in the support of the orthogonal projectors $\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}},\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}$, and Π_{C} separately. We have, by the triangle inequality,

$$\begin{aligned}\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q|\phi\rangle\| &\le \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|+\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|+\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\mathrm{C}}|\phi\rangle\|\\ &\le \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|+\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|,\end{aligned}\tag{B.1}$$

where the last term on the right-hand side in the first inequality is zero since any basis state in the support of Π_{C} will remain in the support of the same projector. This is because $\mathcal{R}^Q$ acts as a control on $\mathcal{H}$ and there is already a zero preimage $x\in H$ before applying $\mathcal{R}^Q$. Thus, $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\mathrm{C}}=0$.

To bound the term $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$, we use that $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}=\Pi_{\overline{\mathrm{C}}}\cdot\Pi_{\mathrm{Q}}$ and $\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}=\Pi_{\overline{\mathrm{Q}}}\cdot\Pi_{\overline{\mathrm{C}}}$ and thus, $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|\le\|\Pi_{\mathrm{Q}}\mathcal{R}^Q\Pi_{\overline{\mathrm{Q}}}\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|$. Since Q is a history-database predicate, we can apply Lemma 4.12 to bound the above by $\sqrt{\frac{10}{N}}\|\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|$. Plugging this into (B.1) and rearranging, we get the desired inequality about $\Delta^Q(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}},|\phi\rangle)$. $\square$

C Missing Proofs for Section 6

In this section, we prove the following lemma:

Lemma 6.10 (Restated)**.** *Given two integers c and q and a state $|\phi\rangle\in\mathbb{H}_{c,q}$, we have*

$$\Gamma^Q(\Pi_{\overline{\mathrm{H}+\mathrm{C}}},|\phi\rangle)\le\sqrt{\frac{10c}{N}}\,,\tag{6.11}$$

$$\|\Pi_{\mathrm{H}}\mathcal{R}^C\Pi_{\mathrm{X}\cdot\mathrm{H}}|\phi\rangle\|^2\le\frac{q}{N}\cdot\|\Pi_{\mathrm{X}\cdot\mathrm{H}}|\phi\rangle\|^2\,,\tag{6.12}$$

$$\Gamma^C(\Pi_{\overline{\mathrm{H}+\mathrm{C}}},|\phi\rangle)\le\frac{2c}{N}\,,\tag{6.13}$$

$$\|\Pi_{\mathrm{C}}\mathcal{R}^C\Pi_{\overline{\mathrm{H}+\mathrm{C}}}|\phi\rangle\|^2\le\frac{2c}{N}\cdot\|\Pi_{\overline{\mathrm{H}+\mathrm{C}}}|\phi\rangle\|^2\,.\tag{6.14}$$

We will use the following simple fact about the predicate $\mathrm{X}\cdot\mathrm{H}$.

Fact C.1. *For any basis state $|x,p,w,H,D\rangle$ satisfying the predicate $\mathrm{X}\cdot\mathrm{H}$, we have*

1. The query index x is in the database but not in the history, that is $D(x) \neq \perp$ and $H(x) = \star$.

2. There is no hybrid collision in $(H, D_{x\leftarrow\perp})$.

3. The query index x does not belong to a quantum collision.

Proof. The first two items are immediate by definition of $\textsc{x}$ and $\textsc{h}$. For the last item, if x was in a quantum collision then, since it also belongs to a hybrid collision, there would exist a second hybrid collision that does not contain x (which contradicts $\textsc{x}$). $\square$

Since the proofs of Equations (6.11) to (6.14) share strong similarities with those of Lemmas 4.6 and 4.7, we skip some details in the calculation below.

Proof of Equation (6.11). We first claim that it is sufficient to show that

$$\|\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \leq \frac{10c}{N}\cdot\|\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2. \tag{C.1}$$

Indeed, $\Pi_{\overline{\textsc{h}+\textsc{c}}}\mathcal{R}^Q\Pi_{\textsc{h}+\textsc{c}}|\phi\rangle = \Pi_{\overline{\textsc{h}+\textsc{c}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}\Pi_{\textsc{h}+\textsc{c}}|\phi\rangle$ by Fact 6.7. Thus, using Equation (C.1), we conclude that $\|\Pi_{\overline{\textsc{h}+\textsc{c}}}\mathcal{R}^Q\Pi_{\textsc{h}+\textsc{c}}|\phi\rangle\|^2 \leq \|\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}\Pi_{\textsc{h}+\textsc{c}}|\phi\rangle\|^2 \leq \frac{10c}{N}\cdot\|\Pi_{\textsc{h}+\textsc{c}}|\phi\rangle\|^2$.

We now prove Equation (C.1). Let $\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle = \sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w,H,D\rangle \in \mathbb{H}_{c,q} \cap \mathrm{supp}(\Pi_{\textsc{x}\cdot\textsc{h}})$. Notice that if the phase register contains $p = 0$ then doing a quantum query on such a state will not modify (H, D). Hence, we only need to consider the basis states for which $p \neq 0$. Together with Fact C.1, it implies that the post-query state is given by the third item of Lemma 4.6,

$$\begin{aligned}
&\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle \\
&= \Pi_{\overline{\textsc{h}}}\sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w,H\rangle\left(\frac{\omega^{pD(x)}}{\sqrt{N}}|D_{x\leftarrow\perp}\rangle + \sum_{y\in[N]}\frac{1-\omega^{pD(x)}-\omega^{py}}{N}|D_{x\leftarrow y}\rangle\right).
\end{aligned}$$

Next, using the orthogonality between basis states, the norm of the above state is equal to,

$$\begin{aligned}
\|\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp}}\left\|\Pi_{\overline{\textsc{h}}}\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{pz}}{\sqrt{N}}|x,p,w\rangle|H\rangle|D\rangle\right\|^2 \\
&\quad+ \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y}}\left\|\Pi_{\overline{\textsc{h}}}\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{1-\omega^{pz}-\omega^{py}}{N}|x,p,w\rangle|H\rangle|D\rangle\right\|^2 \\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}}\left|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{pz}}{\sqrt{N}}\right|^2 \\
&\quad+ \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}}\left|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{1-\omega^{pz}-\omega^{py}}{N}\right|^2.
\end{aligned}$$

By the Cauchy–Schwarz inequality, the above term is at most

$$\begin{aligned}
&\|\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \\
&\leq \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}} \Big(\sum_{z\in[N]}|\alpha_{x,p,w,H,D_{x\leftarrow z}}|^2\Big) \Pr_{z\leftarrow[N]}\big[(x,p,w,H,D_{x\leftarrow z})\in \textsc{h}^{-1}(\textsc{True})\big] \\
&\quad + \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \textsc{h}(x,p,w,H,D_{x\leftarrow\perp})=\textsc{False}}} \frac{9}{N}\Big(\sum_{z\in[N]}|\alpha_{x,p,w,H,D_{x\leftarrow z}}|^2\Big) \Pr_{z\leftarrow[N]}\big[(x,p,w,H,D_{x\leftarrow z})\in \textsc{h}^{-1}(\textsc{True})\big] \\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}} 10\Big(\sum_{z\in[N]}|\alpha_{x,p,w,H,D_{x\leftarrow z}}|^2\Big) \Pr_{z\leftarrow[N]}\big[(x,p,w,H,D_{x\leftarrow z})\in \textsc{h}^{-1}(\textsc{True})\big]
\end{aligned}$$

where we used that the non-zero amplitudes $\alpha_{x,p,w,H,D_{x\leftarrow z}}$ must satisfy $(x,p,w,H,D_{x\leftarrow z})\in \textsc{h}^{-1}(\textsc{True})$ (since $\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle \in \mathrm{supp}(\Pi_{\textsc{h}})$), we extended the range of the second summation to all pairs (H,D) that contain no hybrid collision in $(H,D_{x\leftarrow\perp})$ and we used that $|1-\omega^{pz}-\omega^{py}|\leq 3$.

Finally, since $\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle$ is supported over basis states whose history register contains at most c non-$\star$ entries, the probability to create a hybrid collision by adding one value to the database is at most $\Pr_{z\leftarrow[N]}\big[(x,p,w,H,D_{x\leftarrow z})\in \textsc{h}^{-1}(\textsc{True})\big]\leq c/N$. We conclude that, $\|\Pi_{\overline{\textsc{h}}}\mathcal{R}^Q\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \leq \frac{10c}{N}\sum_{x,p,w,H,D}|\alpha_{x,p,w,H,D}|^2 = \frac{10c}{N}\|\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2$. □

Proof of Equation (6.13). Similarly to the above proof, by Fact 6.7, it is sufficient to show that

$$\|\Pi_{\overline{\textsc{h}}\cdot\overline{\textsc{c}}}\mathcal{R}^C\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \leq \frac{10c}{N}\cdot\|\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \tag{C.2}$$

where we keep the predicate $\overline{\textsc{c}}$ on the left-hand side to rule out the case where the classical query transforms the hybrid collision into a classical collision (the inequality would not hold without this predicate).

Let $\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle = \sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w,H,D\rangle \in \mathbb{H}_{c,q}\cap\mathrm{supp}(\Pi_{\textsc{x}\cdot\textsc{h}})$. By Fact C.1, the effect of doing a classical query on this state is given by the third item of Lemma 4.7. Since we must not have classical collisions, we can ignore the $|H_{x\leftarrow D(x)},D\rangle$ term therein, which gives

$$\begin{aligned}
&\Pi_{\overline{\textsc{h}}\cdot\overline{\textsc{c}}}\mathcal{R}^C\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle \\
&= \Pi_{\overline{\textsc{h}}\cdot\overline{\textsc{c}}}\sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w\rangle\Big(\frac{1}{\sqrt{N}}|H_{x\leftarrow\perp},D_{x\leftarrow\perp}\rangle - \sum_{y\in[N]}\frac{\omega^{py}}{N}|H_{x\leftarrow y},D_{x\leftarrow y}\rangle\Big).
\end{aligned}$$

Next, using the orthogonality between basis states, the norm of the above state is at most,

$$\begin{aligned}
\|\Pi_{\overline{\textsc{h}}\cdot\overline{\textsc{c}}}\mathcal{R}^C\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \leq &\sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}}\Big|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{1}{\sqrt{N}}\Big|^2 \\
&+ \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \textsc{h}(x,p,w,H,D)=\textsc{False}}}\Big|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{py}}{N}\Big|^2.
\end{aligned}$$

Hence, we can conclude in the same way as in the proof of Equation (6.11) by using Cauchy–Schwarz inequality, which gives that $\|\Pi_{\overline{\textsc{h}}\cdot\overline{\textsc{c}}}\mathcal{R}^C\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2 \leq \frac{2c}{N}\|\Pi_{\textsc{x}\cdot\textsc{h}}|\phi\rangle\|^2$. □

Proof of Equation (6.12). Let $\Pi_{\text{X}\cdot\text{H}}|\phi\rangle = \sum_{x,p,w,H,D} \alpha_{x,p,w,H,D}|x,p,w,H,D\rangle \in \mathbb{H}_{c,q} \cap \text{supp}(\Pi_{\text{X}\cdot\text{H}})$. By Fact C.1, the effect of doing a classical query on this state is given by the third item of Lemma 4.7. Moreover, the only terms therein that can lead to a hybrid collision are those for which $D(x)$ gets replaced with a new value y, which gives

$$\Pi_{\text{H}}\mathcal{R}^C\Pi_{\text{X}\cdot\text{H}}|\phi\rangle = -\Pi_{\text{H}} \sum_{x,p,w,H,D} \alpha_{x,p,w,H,D}|x,p,w\rangle \sum_{y\in[N]} \frac{\omega^{py}}{N}|H_{x\leftarrow y}\rangle|D_{x\leftarrow y}\rangle.$$

Next, using the orthogonality between basis states, the norm of the above state is equal to,

$$\begin{aligned}\|\Pi_{\text{H}}\mathcal{R}^C\Pi_{\text{X}\cdot\text{H}}|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y}} \left\|\Pi_{\text{H}} \sum_{z\in[N]} \alpha_{x,p,w,H,D_{x\leftarrow z}} \frac{\omega^{py}}{N}|x,p,w\rangle|H_{x\leftarrow y}\rangle|D\rangle\right\|^2 \\ &= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \text{H}(x,p,w,H_{x\leftarrow y},D)=\text{True}}} \left|\sum_{z\in[N]} \frac{\alpha_{x,p,w,H,D_{x\leftarrow z}}}{N}\right|^2.\end{aligned}$$

Applying the Cauchy–Schwarz inequality and rearranging the expression, we have

$$\|\Pi_{\text{H}}\mathcal{R}^C\Pi_{\text{X}\cdot\text{H}}|\phi\rangle\|^2 \le \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\big[(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y}) \in \text{H}^{-1}(\text{True})\big].$$

For each (H,D) in the above state, D contains at most q entries different from $\perp$ (by definition of $\mathbb{H}_{c,q}$). Moreover, there is exactly one hybrid collision in (H,D) and this collision contains x. Hence, the probability to still have a hybrid collision when $D(x)$ is replaced with a random $y \in [N]$ is at most $\Pr_{y\leftarrow[N]}\big[(x,p,w,H_{x\leftarrow y},D_{x\leftarrow y}) \in \text{H}^{-1}(\text{True})\big] \le q/N$. We conclude that $\|\Pi_{\text{H}}\mathcal{R}^C\Pi_{\text{X}\cdot\text{H}}|\phi\rangle\|^2 \le \frac{q}{N}\|\Pi_{\text{X}\cdot\text{H}}|\phi\rangle\|^2$. □

Proof of Equation (6.14). The proof is almost identical to that of Lemma 4.13. The reason for which we cannot apply this lemma directly to the predicate H + C is because it does not satisfy the condition stated in Equation (4.6). Nevertheless, the latter equation is only needed in analyzing the projector Π_2 in the proof of Lemma 4.13, where it is used to argue that *if a basis state* $|x,p,w,H,D\rangle$ *is not in the support of* Π_{P} *then* $|x,p,w,H_{x\leftarrow D(x)},D\rangle$ *will not be either*. This statement is wrong for the predicate $\text{P} = \text{H} + \text{C}$ (indeed, if x is contained in a quantum collision then $(H_{x\leftarrow D(x)},D)$ will contain a hybrid collision). However, *if a basis state* $|x,p,w,H,D\rangle$ *is not in the support of* $\Pi_{\text{H+C}}$ *then* $|x,p,w,H_{x\leftarrow D(x)},D\rangle$ *will not be in the support of* Π_{C}. Hence, we can carry out the same argument as in the original proof if we replace the outer projector Π_{P} with Π_{C}. This leads to $\|\Pi_{\text{C}}\mathcal{R}^C\Pi_{\overline{\text{H+C}}}|\phi\rangle\|^2 \le \frac{2c}{N} \cdot \|\Pi_{\overline{\text{H+C}}}|\phi\rangle\|^2$. □