The NISQ Complexity of Collision Finding*

Yassine Hamoudi† Qipeng Liu‡ Makrand Sinha§

Last update: February 28, 2024

Abstract

Collision-resistant hashing, a fundamental primitive in modern cryptography, ensures that there is no efficient way to find distinct inputs that produce the same hash value. This property underpins the security of various cryptographic applications, making it crucial to understand its complexity. The complexity of this problem is well-understood in the classical setting and $\Theta(N^{1/2})$ queries are needed to find a collision. However, the advent of quantum computing has introduced new challenges since quantum adversaries — equipped with the power of quantum queries — can find collisions much more efficiently. Brassard, Høyer and Tapp [BHT98] and Aaronson and Shi [AS04] established that full-scale quantum adversaries require $\Theta(N^{1/3})$ queries to find a collision, prompting a need for longer hash outputs, which impacts efficiency in terms of the key lengths needed for security.

This paper explores the implications of quantum attacks in the Noisy-Intermediate Scale Quantum (NISQ) era. In this work, we investigate three different models for NISQ algorithms and achieve *tight bounds for all of them*:

1. A hybrid algorithm making adaptive quantum or classical queries but with a limited quantum query budget, or
2. A quantum algorithm with access to a noisy oracle, subject to a dephasing or depolarizing channel, or
3. A hybrid algorithm with an upper bound on its maximum quantum depth; *i.e.* a classical algorithm aided by low-depth quantum circuits.

In fact, our results handle all regimes between NISQ and full-scale quantum computers. Previously, only results for the preimage search problem were known for these models (by Sun and Zheng [SZ19], Rosmanis [Ros22; Ros23], Chen, Cotler, Huang and Li [CCHL23]) while nothing was known about the collision finding problem.

Along with our main results, we develop an information-theoretic framework for recording query transcripts of quantum-classical algorithms. The main feature of this framework is that it allows us to record queries in two incompatible bases — classical queries in the standard basis and quantum queries in the Fourier basis — consistently. 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 for recording quantum queries. We demonstrate its applicability by giving simpler proofs of the optimal lower bounds for NISQ preimage search and by showing optimal lower bounds for NISQ collision finding.

*A previous version of this paper, which only covered model 1, was titled "Quantum-Classical Tradeoffs in the Random Oracle Model" [HLS22].

†Université de Bordeaux, CNRS, LaBRI, ys.hamoudi@gmail.com.

‡University of California at San Diego, qipengliu0@gmail.com.

§University of Illinois at Urbana-Champaign, msinha@illinois.edu.

1 Introduction

In modern cryptography, collision-resistant hashing stands as a cornerstone, providing countless cryptographic protocols and systems. Collision resistance refers to the intractability of recovering two distinct inputs that produce the same hash value. Collision resistance is crucial to establishing the security of many cryptographic applications, including digital signatures [KL07], Merkle trees [Mer89], zero-knowledge proofs/arguments [BG09], and many more. Thus, understanding collision resistance (or the complexity of collision finding) is particularly important to understand the security of these cryptographic applications.

The so-called generic attacks or black-box query model has received a lot of attention in understanding the security of various cryptographic primitives. In this model, when working with hash functions, an algorithm can only take advantage of the input-output behavior of the function, but does not have access to its actual implementation or other side-information. This approach not only provides simpler proof techniques, but indeed effectively encapsulates real-world attack scenarios. Classically, the complexity of collision finding in the black-box model is well understood. For instance, when employing an ideal hash function, denoted as $F : [M] \to [N]$, the best possible attack needs to make $\Omega(\sqrt{N})$ queries to the hash function to find a collision pair with high probability[1], aligning with the upper bound implied by the Birthday problem. In practical applications, it is imperative that adversaries with limited resources, typically no more than 2^{128} units of computational time, are unable to find a collision. This requirement necessitates a minimum output length of at least 256 bits. As an illustrative example, the latest addition to the Secure Hash Algorithm family of standards, SHA3-256, as released by NIST, frequently finds use in such applications.

The emergence of quantum computing requires us to significantly reevaluate existing cryptography since quantum adversaries can be much more powerful. In the quantum black-box model, *quantum queries*, i.e. the ability to access in superposition the values of a black-box function [BW02] is treated as a fundamental resource. 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 collision finding, how should we set the output length such that the hash function is still collision resistant even against quantum adversaries? Brassard, Høyer and Tapp [BHT98] and Aaronson and Shi [AS04] proved that in the quantum black-box model, $\Theta(N^{1/3})$ queries are both sufficient and necessary for finding a collision. This suggests that to maintain the same level of security (i.e., secure against quantum algorithms that run in time 2^{128}), the output length of the hash function needs to be extended to $3 \times 128 = 384$. Consequently, this adjustment in output length has affected storage requirements and the overall efficiency of various cryptographic protocols. However, as we are in the noisy-intermediate scale quantum (NISQ) era, quantum computation is noisy and quantum memory is short-lived, we ask the following question:

Should we sacrifice efficiency for potential quantum attacks, especially in the NISQ era?

The question above has a natural motivation stemming from practice. In particular, various constraints on near-term quantum hardware often necessitate the use of classical processing in addition to quantum operations. For instance, in certain scenarios, it might not be feasible that superposition queries could be made to the entire input, or the cost of making such queries might be prohibitive. Furthermore, the depth of possible quantum computation in near-term devices is also limited since the decoherence effects accumulate, thus additional classical processing is warranted to fully utilize the capabilities of such devices.

Motivated by the above considerations, in this paper, we investigate the limitations of NISQ algorithms for collision finding, as well as introduce a general technique/framework for proving lower bounds in the NISQ era. Using the new framework, along with the lower bounds for

[1] We remark that for typical applications the parameter M satisfies $M = \Omega(N)$.

collision finding, we also give simpler and unified proofs of several results on preimage finding by Sun and Zheng [SZ19], Rosmanis [Ros22; Ros23], and Chen, Cotler, Huang and Li [CCHL23].

1.1 Contributions

We first present our contributions on the limitations of NISQ collision finding.

Collision Finding (Section 6). The problem is to find a pair of elements $x \neq y \in [M]$ that evaluate to the same value $F(x) = F(y)$, given a uniformly random function $F : [M] \to [N]$. Classically, a tight bound $\Theta(c^2/N)$ for the optimal success probability is easily proved for this problem, where c is the number of classical queries. When a full-scale quantum computer with q quantum queries is available, one can use the so-called BHT algorithm [BHT98] to find a collision pair with probability $O(q^3/N)$ (assuming $M = \Omega(N^{2/3})$). However, this algorithm requires q quantum queries, meaning no noise or upper bounds on quantum depth were considered for implementing the algorithm, leaving the potential quantum speed-up elusive in the NISQ era. Towards resolving this issue, we propose three different models for NISQ algorithms and show tight bounds for each of these models.

Model 1. Bounded Quantum Queries. In this model, we consider a quantum algorithm that only has limited access to its quantum capabilities: namely, an upper bound on the number of quantum queries, denoted by q. Additionally, the algorithm can make (potentially significantly more) c classical queries. This model is closely related to "d-QC model" discussed in the line of work [CCL23; CM20; AGS22; HG22], where d quantum queries are interleaved with classical queries. Rosmanis [Ros22] proved a tight bound for preimage search in this model, and posed an open question on collision finding. We answer this question below:

Theorem 6.1, first bullet. *The optimal success probability of an 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.*

Our bound is tight when $M = \Omega(N^{2/3})$ because of the following variant of the BHT algorithm: the first $c + \lceil q/2 \rceil$ queries are classical[2] and are used to collect distinct $(x, F(x))$ pairs. If there is a collision among these values the algorithm terminates. Otherwise, the remaining $\lfloor q/2 \rfloor$ quantum queries are used to run Grover's search on the rest of F, where an element x is marked if its image $F(x)$ occurs among the collected pairs. This algorithm stops working for small domains of size $M = O(N^{2/3})$, as is the case for the BHT algorithm. In fact, we conjecture that the optimal bound is $\Theta((c^2 + q^3)/N)$ when $M = \Theta(\sqrt{N})$ (which is the regime of the Element Distinctness problem). We also note that $M > N$ is safe to assume for most cryptographic applications.

Model 2. Noisy Quantum Queries. In the second model, we consider noisy quantum machines, whose only noise comes from quantum queries to the hash function. More explicitly, we assume each quantum query to the hash function is affected by a dephasing noise $b \in (0, 1]$: with probability $1 - b$, it is a quantum query; otherwise (with probability b), it is a classical query. We ignore all other noises in this model and only pose constraints on oracle queries.

Theorem 6.1, second bullet. *The optimal success probability of an algorithm making t noisy queries with dephasing noise $b \in [\frac{1}{t}, 1]$ for solving the Collision Finding problem is $\Theta(t^2/(bN))$. There is a matching hybrid algorithm that achieves asymptotically the same success probability.*

In the above theorem statement, we only consider $b \geq \frac{1}{t}$, as when b is sufficiently small, t noisy queries are already very likely to be all quantum. Our bound is tight when $M = \Omega(N^{2/3})$ due to

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

the following variant of the BHT algorithm. First, make $t/2$ classical queries to collect distinct $(x, F(x))$ pairs (note that a noisy query can be made purely classical by simply measuring both the input and output registers). Next, run bt independent instances of Grover's search, each using $1/(2b)$ noisy queries, and try to find a collision within the collected pairs. As there are only $1/(2b)$ noisy queries, each instance is a purely quantum algorithm with high probability. Thus, each instance succeeds with probability $\Omega(1/(2b)^2 \cdot t/(2N)) = \Omega(t/(b^2N))$. Consequently, this algorithm succeeds with probability $\Omega(bt \cdot t/(b^2N)) = \Omega(t^2/(bN))$.

Model 3. Bounded Quantum Depth. In this model, we consider a quantum algorithm that is almost classical, but has access to quantum helper subroutines that have bounded depth d. In other words, the collection of algorithms in this model can be modeled as $\mathsf{BPP}^{\mathsf{QNC}_d}$. This model captures a significant NISQ scenario where we have access to arbitrary polynomial-time randomized classical algorithms, but all usable quantum machines are vulnerable to noise and completely collapse after a certain period of time. This model is the "d-CQ model" discussed in the line of work [CCL23; CM20; AGS22; HG22].

Theorem 6.1, third bullet. *The optimal success probability of an algorithm making t quantum queries with bounded depth $d \leq t$ for solving the Collision Finding problem is $\Theta(dt^2/N)$. There is a matching algorithm that achieves asymptotically the same success probability.*

The tightness of the bound follows from a similar algorithm to the one in model 2 when $b = 1/d$.

Our results are proven using a new information-theoretic framework that we call the hybrid compressed oracle. We next provide a high-level description of this framework.

Hybrid Compressed Oracle (Section 4). The main technical contribution of this work is a new information-theoretic 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. As the name suggests, our framework is an extension of the compressed oracle technique of Zhandry [Zha19]. This part of our work broadly fits under the long-term goal in complexity theory to develop general lower-bound techniques that characterize the *tradeoffs* between the number of queries and other computational resources. For instance, prior works have studied the interplay between quantum queries and memory space [KŠW07; AŠW09; HM23], circuit depth [SZ19; CCL23; CM20; AGS22; HG22; CH22], parallel computation [Zal99; GR04; JMW17; AHU19; CFHL21; BLZ21], proof size [Aar12; ST23; 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 however.

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. The classical variant of the method records a *query transcript* representing the knowledge gained by an algorithm (the "attacker") on the input and on an intuitive level uses it to argue that the algorithm does not record enough information via these queries to succeed. However, 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 first extend Zhandry's construction to support recording both classical and quantum queries. This is not as easy as it may seem since it requires merging two ways of recording on distinct bases (the standard and the Fourier basis). Our solution relies on replacing the original classical and quantum 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 perfectly simulates the behavior of the original algorithm (Proposition 4.2).

We then further extend our framework to record *mixtures* of the classical and quantum oracles. Such mixtures capture the model where a quantum query can collapse into a classical one because of dephasing noise. We handle this setting by interpolating between the two types of recording that happen when the query is purely classical or quantum. Our simulation is again indistinguishable from the viewpoint of the algorithm. Furthermore, we demonstrate a close connection between a mixture that puts probability $b \in (0, 1]$ on the classical oracle and the model where the quantum depth is bounded by $1/b$. The latter amounts to a complete collapse of the quantum memory after every $1/b$ quantum queries. We show that, when replacing each quantum query with the aforementioned mixture and removing the depth constraint, the success probability of the algorithm is barely changed. Hence, the depth-bounded model can be analyzed in our framework using the appropriate interpolation parameter. A more detailed technical overview of our framework is provided in Section 2.2.

Apart from proving NISQ lower bounds for collision finding, we also demonstrate the applicability of our framework by proving NISQ lower bounds for preimage search in all three models. These lower bounds were previously shown by [SZ19; CCHL23; Ros22; Ros23] and we are able to give unified and simplified proofs of these results.

Preimage Search (Section 5). The preimage search concerns the problem of finding a preimage $x \in [M]$ 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, first bullet. *The optimal success probability of an 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.

Sun and Zheng [SZ19], Chen, Cotler, Huang and Li [CCHL23] and Rosmanis [Ros23] also considered the case of hybrid algorithms that make noisy queries or have bounded depth. We also recover these results using the hybrid compressed oracle framework.

Theorem 5.1, second bullet. *The optimal success probability of an algorithm making t noisy queries with dephasing noise $b \in [1/t, 1]$ for solving the Preimage Search problem is $\Theta(t/(bN))$. There is a matching algorithm that achieves asymptotically the same success probability.*

Theorem 5.1, third bullet. *The optimal success probability of an algorithm making t quantum queries with bounded depth $d \leq t$ for solving the Preimage Search problem is $\Theta(dt/N)$. There is a matching hybrid algorithm that achieves asymptotically the same success probability.*

1.2 Related Work

Query Complexity Lower Bounds. There are two main systematic techniques for proving lower bounds in quantum query complexity: the polynomial [BBC+01] and the adversary [Amb02]

methods. A different information-theoretic method, called the compressed oracle technique, was recently introduced by Zhandry [Zha19]. This method is useful in proving lower bounds for search problems when the superposition queries are made to a *uniformly random* function, a setting that is often used to model various cryptographic scenarios, and is commonly called *the random oracle model* in the cryptography literature. The compressed oracle technique has led to new and simpler lower bounds for certain search problems (e.g. [LZ19a; HM23; 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, use ad-hoc methods that are tailor-made for the specific problem being studied.

Lower Bounds for Hybrid and NISQ Algorithms. As mentioned before, in a recent work, Rosmanis [Ros22] characterized the optimal success probability of solving the preimage search problem, although not in the random oracle model. The proof techniques are specific to the search problem and inspired by a lower bound for Grover's search with quantum faulty oracles by Regev and Schiff [RS08].

Another related line of work [CCL23; CM20; AGS22; HG22; CH22] proves lower bounds for hybrid algorithms in the so-called "d-QC model" where d quantum queries are interleaved with polynomially (in the number of input qubits) many classical queries. This model is akin to small-depth *measurement-based quantum computation*, where measurement outcomes are classically processed to select subsequent quantum gates and is encompassed by our hybrid quantum-classical query model when the number of quantum queries is bounded by d. This model is captured by the first hybrid model with a bound on the number of quantum queries. The aforementioned works show that certain carefully constructed variants of Glued-Trees and Simons problems require a large quantum depth. For the preimage search problem, Sun and Zheng [SZ19], Chen, Cotler, Huang and Li [CCHL23] and Rosmanis [Ros23] also considered the case of hybrid algorithms that make noisy queries or have bounded depth, as mentioned above.

In post-quantum cryptography, several works [JST21; ABKM22] 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 does not seem generalizable to the proof of more general hybrid results.

2 Technical Overview

2.1 Overview of the Compressed Oracle

First 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 (or database) 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[3] unitary:

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

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.

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 Hermitian unitary operation S that 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 it 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.

[3]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.

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 is initially 0 and increases by at most $O(1/\sqrt{N})$ after each query and thus

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

We stress out that the compressed encoding is just a technique for proving lower bounds in the real random oracle model. An algorithm will never encounter the compressed symbol $\perp$ in practice, as the simulation is statistically indistinguishable from the real world.

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 that make both quantum and classical queries. In fact, we consider an even more general scenario where each query can behave as a superposition of the quantum and classical oracles according to some interpolation parameter. This setting allows us to capture a wide variety of NISQ models based on noisy oracles and depth-bounded quantum algorithms.

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 take 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 (un)compression 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 classical/quantum queries (Model 1). With the above framework, we give an alternative lower-bound proof for the search problem against hybrid algorithms that use c classical and q quantum queries (when $c = 0$ or $q = 0$ we recover the usual quantum or classical bounds). As remarked before, this was first shown by Rosmanis [Ros22] with a proof tailored for the search problem. Although there are some similarities between his 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's 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 making a classical query, we show that the total progress defined as

$$\Psi_t = \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$$

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 than $\|\Pi_{\mathrm{C}}|\phi\rangle\|^2$, the state $\Pi_{\mathrm{C}}|\phi'\rangle$ consists of three parts:

1. $|\phi_1\rangle$: This corresponds to the basis states that 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 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

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

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 at least $\delta_{\mathrm{Q}\to\mathrm{C}}$ due to a similar reason. Thus, we conclude that after a classical query, Ψ_t increases by at most $O(1/N)$ (in fact, $O(1/N) - \delta_{\mathrm{Q}\to\mathrm{C}}$ but we do not need that refinement here). 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 at most $\Psi_{c+q} = O\big(\frac{c+q^2}{N}\big)$.

Lower Bound for Preimage search with interpolated queries (Model 2). We adapt the above proof to the case where each query is a mixture of the classical and quantum oracles (instead of being purely classical or quantum). For simplicity, we assume that all queries have the same probability $b \in (0, 1]$ of being classical, which is equivalent to making quantum queries affected by dephasing noise b.

The success probability of Grover's search using t such queries is $\Omega((1-b)^t t^2/N)$ since the probability that all queries are quantum is $(1-b)^t$. This is nearly optimal when the noise is sufficiently small $b \leq 1/t$, as noiseless algorithms succeed with probability $O(t^2/N)$ anyway.

However, when $b \geq 1/t$, a better algorithm consists of running $\lfloor bt \rfloor$ independent instances of Grover's search, each using $\lfloor 1/b \rfloor$ queries, to succeed with probability $\Omega(bt \cdot 1/(b^2 N)) = \Omega(t/(bN))$.

We show that the above algorithm is optimal by tracking the same progress measure Ψ_t as before, but now making interpolated queries. One can immediately apply the analysis of the previous paragraph to show that the progress increases by at most $O((1-b)\sqrt{\Psi_t/N} + 1/N)$ after each query. This is however not sufficient to conclude that $\Psi_t = O(t/(bN))$. The proof involves refining the analysis of how the quantum progress changes after a query. We consider the exact value $\delta_{\mathrm{Q}\to\overline{\mathrm{Q}}} = \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi'\rangle\|^2$ by which it decreases when making a classical query. Since it is at least the amount $\delta_{\mathrm{Q}\to\mathrm{C}}$ transferred to the classical progress, we obtain that Ψ_t increases by at most $O(1/N) - \delta_{\mathrm{Q}\to\overline{\mathrm{Q}}}$ after a classical query. On the other hand, we show that the quantum progress increases by at most $O(\sqrt{\delta_{\mathrm{Q}\to\overline{\mathrm{Q}}}/N} + 1/N)$ when making a quantum query, which is sometimes smaller than the quantity $O(\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|/\sqrt{N} + 1/N)$ used to analyze the model 1. Overall, by interpolating between the two oracles, we conclude that Ψ_t increases by

$$O\Big((1-b)\sqrt{\delta_{\mathrm{Q}\to\overline{\mathrm{Q}}}/N} - b \cdot \delta_{\mathrm{Q}\to\overline{\mathrm{Q}}} + 1/N\Big) = O(1/(bN))$$

after each interpolated query, since the function $Z \mapsto (1-b)Z/\sqrt{N} - bZ^2 + 1/N$ is at most $O(1/(bN))$. Hence the success probability after t queries is at most $\Psi_t = O\big(\frac{t}{bN}\big)$.

Lower Bound for Preimage search with bounded depth (Model 3). At first sight, the bounded-depth model is more subtle to analyze since it concerns all the memory of the algorithm (which has to decohere every d queries), instead of only the query registers. We do not know if a variant of the hybrid compressed oracle can capture this property optimally. Instead, we aim to relax that model to focus the analysis on the query registers. A first attempt could be to only decohere the latter registers, which amounts imposing a classical query every d quantum queries. This is however a very weak constraint, since an algorithm can swap the query registers with garbage qubits before and after making the classical queries to avoid the decoherence. Our solution is to instead show that a depth-bounded algorithm can always be simulated by an algorithm – in model 2 – where each query is classical with probability $b = 1/d$. Intuitively, this amounts to "spread out" the decoherence occurring every d queries (in the bounded-depth model) into a smaller probability $1/d$ of decohering *only* the query registers but at *every* query. The details of the reduction are provided in Proposition 3.4. Plugging the parameter $b = 1/d$ in the above bound established in model 2, we immediately obtain that the success probability after t queries in the bounded-depth model is at most $O\big(\frac{dt}{N}\big)$. This is easily shown to be optimal.

Lower Bounds for Collision Finding. The intuition behind the proof for the collision lower bounds 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.

We only sketch the lower bound in model 1, where c queries are classical and q queries are quantum. The lower bounds in the two other models build upon these ideas in a similar way to what is discussed above for preimage search.

The proof consists again of bounding 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:

$$\Delta_{\mathrm{C}} \leq 2\delta_{\mathrm{H}\to\mathrm{C}} + O\Big(\frac{t}{N}\Big),$$
$$\Delta_{\mathrm{H}\cdot\overline{\mathrm{C}}} \leq -\delta_{\mathrm{H}\to\mathrm{C}} + 2\delta_{\mathrm{Q}\to\mathrm{H}} + O\Big(\frac{t}{N}\Big),$$
$$\Delta_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} \leq -\delta_{\mathrm{Q}\to\mathrm{H}} + O\left(\sqrt{\frac{t\cdot\delta_{\mathrm{H}\to\mathrm{C}}}{N}}\right).$$

Using these facts, we prove that the following potential

$$\Psi_t := \|\Pi_{\mathrm{C}}|\phi\rangle\|^2 + 3\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 7\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2,$$

which upper bounds the total progress, always increases as follows: $\sqrt{\Psi_t} \leq \sqrt{\Psi_{t-1}} + O\Big(\sqrt{\frac{t}{N}}\Big)$ if the t-th query is quantum and $\Psi_t \leq \Psi_{t-1} + O\big(\frac{t}{N}\big)$ 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 $\Psi_{c+q} = O\Big(\frac{c^2+cq^2+q^3}{N}\Big)$.

3 Hybrid Random Oracle Model

Below we define a computational model that captures hybrid algorithms that make both classical and quantum queries to a random function (which we also refer to as a random oracle for consistency with the compressed oracle framework). We also note that our model captures the QC model [CCL23], a generalized model for measurement-based quantum computation, as a special case.[4]

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 $x \in [M]$.
- Phase register $\mathcal{P}$ holding $p \in [N]$.
- Workspace register $\mathcal{W}$ holding $w \in \{0,1\}^*$ (the size of the register may increase during the computation as we allow appending new qubits to it).

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

[4] 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.

Quantum Phase Oracle. We define the quantum oracle $\mathcal{O}_0^D$ as the unitary operator acting on the memory of the algorithm as follows.

$$\mathcal{O}_0^D : |x, p, w\rangle_{\mathcal{A}} \mapsto \omega_N^{pD(x)} |x, p, w\rangle_{\mathcal{A}} \quad \text{where} \quad \omega_N = e^{\frac{2\mathbf{i}\pi}{N}}.$$

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 $\mathcal{H} = \mathcal{H}_1 \cdots \mathcal{H}_t$ where the c-th subregister $\mathcal{H}_c$ is used to purify the c-th classical query (there are at most t queries in total) and stores a value in $([M] \times [N]) \cup \{\star\}$. The initial state of that register is $|\star, \ldots, \star\rangle_{\mathcal{H}}$. The classical oracle $\mathcal{O}_1^D$ is defined as the unitary operator acting as follows

$$\begin{aligned} \mathcal{O}_1^D \quad &: \quad |x, p, w\rangle_{\mathcal{A}} |(x_1, y_1), \ldots, (x_c, y_c), \star, \ldots, \star\rangle_{\mathcal{H}} \\ &\mapsto \quad \omega_N^{pD(x)} |x, p, w\rangle_{\mathcal{A}} |(x_1, y_1), \ldots, (x_c, y_c), (x, D(x)), \star, \ldots, \star\rangle_{\mathcal{H}}. \end{aligned}$$

Since we only care about a bounded number of t queries, the above oracle can easily be made a unitary. For convenience, we denote the list $((x_1, y_1), \ldots, (x_c, y_c), \star, \ldots, \star)$ by H and we say $x \in H$ if and only if there exists $1 \leq i \leq c$ such that $x_i = x$. We use the following shorthand for appending a new pair (x, y) to H.

Definition 3.1 ($H_{x \leftarrow y}$)**.** Given a history $H = ((x_1, y_1), \ldots, (x_c, y_c), \star, \ldots, \star)$ with at least one star entry, we define

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

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

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 $y \neq y'$. We also let $\mathscr{H}$ denote the set of all possible histories H.

Hybrid Oracle. We extend the above definitions by allowing for probabilistic choices between the two oracles. This is represented by a channel that applies the quantum oracle $\mathcal{O}_0^D$ with probability $1 - b$, for some $b \in [0, 1]$, and applies the classical oracle $\mathcal{O}_1^D$ otherwise. Additionally, we assume that the algorithm is provided with a query type bit (or "flag") indicating which oracle has been applied. We represent this operation by an isometry $\mathcal{O}_b^D$ acting as

$$\mathcal{O}_b^D : |x, p, w\rangle_{\mathcal{A}} |H\rangle_{\mathcal{H}} \mapsto \omega_N^{pD(x)} |x, p\rangle_{\mathcal{X}\mathcal{P}} \Big(\sqrt{1-b} \cdot |w0\rangle_{\mathcal{W}} |H\rangle_{\mathcal{H}} + \sqrt{b} \cdot |w1\rangle_{\mathcal{H}} |H_{x \leftarrow D(x)}\rangle_{\mathcal{H}} \Big)$$

where the bit appended to the workspace w indicates the nature of the oracle. We recover the quantum and classical oracles when $b = 0$ and $b = 1$ respectively (ignoring the query type bit). We will use $b \notin \{0, 1\}$ in the analysis of noisy and bounded-depth quantum algorithms.

Hybrid Algorithm. An algorithm with t queries is defined as a sequence $U_0, \ldots, U_t$ of unitary transformations acting on the memory register $\mathcal{A}$ and a list of real numbers $b(1), \ldots, b(t) \in [0, 1]$ that specifies which interpolation parameter is used at each query. The state $|\psi_t^D\rangle$ of the algorithm after t queries is

$$|\psi_t^D\rangle = U_t \, \mathcal{O}_{b(t)}^D \, U_{t-1} \cdots U_1 \, \mathcal{O}_{b(1)}^D \, U_0 \, (|0\rangle_{\mathcal{A}} |\star, \ldots, \star\rangle_{\mathcal{H}}). \tag{3.1}$$

The function D is chosen uniformly at random from the set $\{D : [M] \to [N]\}$. We model that by adding another purification register (the *database*) $\mathcal{D} = \mathcal{D}_0 \dots \mathcal{D}_{M-1}$ where each subregister $\mathcal{D}_x$ for $x \in [M]$ holds a value $D(x) \in [N]$ and we define the following joint state,

$$|\psi_t\rangle = \frac{1}{N^{M/2}} \sum_{D \in [N]^M} |\psi_t^D\rangle_{\mathcal{AH}} \otimes |D\rangle_{\mathcal{D}} = U_t \, \mathcal{O}_{b(t)} \, U_{t-1} \cdots U_1 \, \mathcal{O}_{b(1)} \, U_0 \, |\psi_0\rangle, \tag{3.2}$$

where $\mathcal{O}_b := \sum_D \mathcal{O}_b^D \otimes |D\rangle\langle D|_{\mathcal{D}}$ and $|\psi_0\rangle := |0\rangle_{\mathcal{A}} \otimes |\star, \cdots, \star\rangle_{\mathcal{H}} \otimes \frac{1}{N^{M/2}} \sum_D |D\rangle_{\mathcal{D}}$.

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 $(x_1, \dots, x_k) \in [M]^k$ with $k \leq 2$, by making k extra classical queries, we may assume that all the indices $x_1, \dots, x_k$ are in the history register at the end.

3.1 Models for NISQ Algorithms

We describe the three models of NISQ quantum query complexity than can be analyzed in our framework of hybrid algorithms and state some of their properties.

Model 1. Bounded Quantum Queries and Adaptiveness. We first consider the case of algorithms that make only two types of queries: quantum queries and classical queries (i.e. $b \in \{0, 1\}$). Here, one can consider two types of algorithms: static or adaptive. A "static" algorithm fixes the order of which type of queries to make before it interacts with the oracle. An "adaptive" algorithm adaptively chooses the query type for each individual query, as long as the total number of quantum (and classical) queries is unchanged.

Below, we present a theorem, as a special case of [DFH22, Theorem 1], showing that any hybrid algorithm can be assumed to be static without loss of generality.

Theorem 3.2. *In the hybrid random oracle model, for any adaptive hybrid quantum algorithm making at most q quantum queries and c classical, there exists a static hybrid algorithm making at most $2q$ quantum queries and $2c$ classical queries such that their outputs are always identical.*

Given the above theorem, we will only consider lower bounds for static algorithms in the rest of the paper.

Before we move on, we give some intuition on why Theorem 3.2 holds. For fixed c, q, there exists a sequence $b^* = b_1^* b_2^* \cdots b_{2c+2q}^* \in \{0, 1\}^{2c+2q}$ with exactly $2c$ elements being 1, such that every $b = b_1, \cdots, b_{c+q} \in \{0, 1\}^{c+q}$ is a subsequence of b^*. This was proved in [DFH22, Lemma 1]; we ignore the proof and refer interested readers to [DFH22] for full details. Assuming the statement about the existence of such a sequence is true, a static hybrid algorithm just picks the fixed sequence b^* and every time it makes the next query, it checks if the current query type in b^* is equal to the next query type in b. If yes, it makes the query; otherwise, it makes a junk query (for example, regardless of the query type, querying on input 0 classically and discarding both the input and output). This strategy results in identical behavior of the static hybrid algorithm and any adaptive hybrid algorithm.

Model 2. Noisy Quantum Queries. We next consider the case of algorithms that have access to a noisy quantum oracle with noise level $b \in [0, 1]$. We define this model using the mixed state representation ρ of the memory of an algorithm (over the registers $\mathcal{XPW}$) and the channel $\mathcal{N}_{\mathcal{XP}}$ that dephases the index and phase registers (i.e. $\mathcal{N}_{\mathcal{XP}}(\rho) = \sum_{x,p}(|x, p\rangle\langle x, p| \otimes \mathbb{I}_{\mathcal{W}})\rho(|x, p\rangle\langle x, p| \otimes \mathbb{I}_{\mathcal{W}})$). The noisy oracle is represented by the channel

$$\mathcal{N}_b^D : \rho \mapsto (1 - b) \cdot \mathcal{O}_0^D \rho \mathcal{O}_0^D \otimes |0\rangle\langle 0| + b \cdot \mathcal{N}_{\mathcal{XP}}\big(\mathcal{O}_0^D \rho \mathcal{O}_0^D\big) \otimes |1\rangle\langle 1|. \tag{3.3}$$

This channel dephases the query registers after each quantum query with probability $b \in [0,1]$ and appends a "noise flag" qubit indicating whether the dephasing occurred. The state of the algorithm after t queries is defined recursively as $\rho_0^D = |0,0,0\rangle\langle 0,0,0|$ and $\rho_t^D = U_t \mathcal{N}_b^D(\rho_{t-1}^D) U_t^\dagger$ where U_t is the unitary operator applied by the algorithm after the t-th query. One can observe that the hybrid oracle $\mathcal{O}_b^D$ is a purification of the noise channel $\mathcal{N}_b^D$, where the environment is enacted by the history register $\mathcal{H}$.

Fact 3.3. *Let $|\psi_t^D\rangle$ be the state defined in Equation (3.1) for a given sequence of unitaries $U_0, \ldots, U_t$ and hybrid oracles $\mathcal{O}_{b(1)}^D, \ldots, \mathcal{O}_{b(t)}^D$. Let ρ_t^D be the state obtained by applying the same sequence of unitaries and replacing each oracle $\mathcal{O}_{b(i)}^D$ with $\mathcal{N}_{b(i)}^D$. Then, $\rho_t^D = \mathrm{Tr}_{\mathcal{H}}(|\psi_t^D\rangle\langle\psi_t^D|)$.*

This fact implies that the complexity of solving any problem using noisy quantum oracles is captured by the above model of hybrid algorithms. We will use this connection to derive the complexity of the preimage search and collision finding problems with noisy oracles.

Notice that our model is particularly versatile for proving hardness results (as is the goal in the present paper). Indeed, it can simulate algorithms that do not have access to the noise flag (just ignore the flag), algorithms that are subject to depolarizing noise (measure the flag qubit and depolarize the state on purpose when it is 1) and algorithms whose entire memory is subject to noise. Hence, our lower bounds apply to these models as well.

Model 3. Bounded Quantum Depth. Finally, we consider the model of bounded-depth quantum computation where the entire system decoheres periodically. Given a depth parameter d, this amounts to applying the channel $\mathcal{N}_{\mathcal{XPW}}$ that dephases all the memory (i.e. $\mathcal{N}_{\mathcal{XPW}}(\rho) = \sum_{x,p,w} |x,p,w\rangle\langle x,p,w|\rho|x,p,w\rangle\langle x,p,w|$) every d queries. The state of the algorithm can again be defined recursively as $\rho_0^D = |0,0,0\rangle\langle 0,0,0|$, $\rho_t^D = U_t \mathcal{N}_{\mathcal{XPW}}\big(\mathcal{O}_0^D \rho_{t-1}^D \mathcal{O}_0^D\big) U_t^\dagger$ if t is a multiple of d, and $\rho_t^D = U_t \mathcal{O}_0^D \rho_{t-1}^D \mathcal{O}_0^D U_t^\dagger$ otherwise. This captures the scenario where a classical computer has access to a quantum computer of depth d and performs t queries in total, which is also known as the d-CQ scheme [CCL23; CM20].

We show that any d-depth algorithm can be simulated by an unbounded-depth algorithm that uses the hybrid oracle $\mathcal{O}_{1/d}$ without increasing the query complexity significantly. Intuitively, the interpolation parameter $1/d$ is sufficiently small so that d calls to the hybrid oracle will behave almost as d calls to the quantum oracle.

Proposition 3.4. *Fix any d-depth algorithm that makes t quantum queries in total. Then, there exists an algorithm in the hybrid model that makes at most $2t$ queries* in expectation *to the oracle $\mathcal{O}_{1/d}$ and outputs the same outcome as the bounded-depth algorithm.*

Proof. It is sufficient to explain how to simulate a sequence of d quantum queries using at most $2d$ queries in expectation to the hybrid oracle $\mathcal{O}_{1/d}$. The proposition follows by applying this simulation to the $\lceil t/d \rceil$ sequences of queries occurring between the applications of the channel $\mathcal{N}_{\mathcal{XPW}}$ in the bounded-depth model.

Consider an algorithm making d queries to a quantum oracle $\mathcal{O}_0^D$. Suppose that we instead use the hybrid oracle $\mathcal{O}_{1/d}^D$ and measure after each query whether the query type bit is 0 – indicating that the query is quantum. If it is not 0, we restart the simulation (the initial memory is classical, hence it can be cloned to restart as many times as needed). The algorithm stops once it obtains a sequence of d consecutive 0 (which will perfectly simulate the bounded-depth algorithm). Since each query is quantum with probability $1 - 1/d$, the expected number of calls to $\mathcal{O}_{1/d}^D$ corresponds to the number of coin flips needed to get d consecutive heads when a coin has probability $1 - 1/d$ of coming up heads. This is equal to $((1-1/d)^{-d} - 1)d \leq 2d$. □

We can easily modify the above algorithm to make exactly $4t$ queries to $\mathcal{O}_{1/d}$ and succeeds in doing the simulation with probability at least $1/2$. This leads to the following corollary for deriving lower bounds in the depth-bounded model.

Corollary 3.5. *Let $\sigma(t,b)$ denote the optimal success probability for solving a given problem using t queries to the oracle $\mathcal{O}_b$ where $b \in (0,1]$. Then, the optimal success probability for solving the same problem using t quantum queries in the bounded-depth model with depth $d = \lceil 1/b \rceil$ is at most $2\sigma(4t,b)$.*

While this reduction may not be tight in general, we show in this paper that it provides optimal bounds (up to constant factors) for the preimage search and collision finding problems.

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 $|\perp, \dots, \perp\rangle_{\mathcal{D}}$. 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 $|\hat{p}\rangle_{\mathcal{D}_x} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} \omega_N^{py} |y\rangle_{\mathcal{D}_x}$ for $p = 0, \dots, N-1$, denote the Fourier basis states and let S_x be the unitary operator acting on $\mathcal{D}_x$ such that

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

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

$$S_{x,H} = \begin{cases} \mathbb{I} & \text{if } x \in H \\ S_x & \text{otherwise.} \end{cases} \tag{4.1}$$

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

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

The hybrid compressed oracle $\mathcal{R}_b$ is defined as follows,

$$\mathcal{R}_b = S\mathcal{O}_b S \quad \text{where} \quad \mathcal{O}_b = \sum_{D \in (\{\perp\} \cup [N])^M} \mathcal{O}_b^D \otimes |D\rangle\langle D|_{\mathcal{D}},$$

for $b \in [0,1]$. The idea behind these definitions is that, for any basis state $|x,p,w\rangle_{\mathcal{A}} |H,D\rangle_{\mathcal{HD}}$:

- 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 $\mathcal{R}_0$ only acts on the register $\mathcal{H}$ as control. We provide an alternative definition to $\mathcal{R}_0$ and $\mathcal{R}_1$ 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

$$|\phi_t\rangle = U_t\,\mathcal{R}_{b(t)}\,U_{t-1}\,\cdots\,U_1\,\mathcal{R}_{b(1)}\,U_0\,(|0\rangle_{\mathcal{A}}|\star,\ldots,\star\rangle_{\mathcal{H}}|\perp,\ldots,\perp\rangle_{\mathcal{D}}). \tag{4.2}$$

Following from Equation (4.2), we define the initial state $|\phi_0\rangle = |0\rangle_{\mathcal{A}} \otimes |\star,\cdots,\star\rangle_{\mathcal{H}} \otimes |\perp,\ldots,\perp\rangle_{\mathcal{D}}$.

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 $\mathcal{D}_x$. Observe that $S_{\mathsf{all}}|\phi_0\rangle = |\psi_0\rangle$. We also have the following proposition:

Proposition 4.1. *$\mathcal{R}_b = S\mathcal{O}_bS = S_{\mathsf{all}}\mathcal{O}_bS_{\mathsf{all}}$ for all $b \in [0,1]$.*

Proof. This is because for $|x,p,w\rangle_{\mathcal{A}}$, the oracle $\mathcal{O}_b$ acts as identity on the registers $\mathcal{D}_{<x}$ and $\mathcal{D}_{>x}$. Therefore, for every $x' \neq x$, we have that $S_{x'}$ in the left multiplication with S_{all} cancels with $S_{x'}$ in the right multiplication with 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 (3.2) and $|\phi_t\rangle$ from (4.2) 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 (4.2), the left-hand side is equal to

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

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 last line uses that S_{all} is Hermitian, unitary and satisfies $S_{\mathsf{all}}|\phi_0\rangle = |\psi_0\rangle$. □

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

Definition 4.3 (History-Database Consistent State)**.** Given an integer t, we say that (H,D) is a *history-database t-consistent pair* it it has the following properties:

1. (Database size) The database satisfies $D(x) \neq \perp$ for at most t different values of x.
2. (History size) The history is of the form $H = ((x_1,y_1),\ldots,(x_c,y_c),\star,\ldots,\star)$ where $x_1,\ldots,x_c \in [M]$ and $y_1,\ldots,y_c \in \{\perp\} \cup [N]$ for some $c \leq t$.

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 let $\mathbb{H}_t$ denote the vector space spanned by all basis state $|x, p, w\rangle_{\mathcal{A}}|H, D\rangle_{\mathcal{HD}}$ where (H, D) is history-database t-consistent. We say that a basis state is *history-database consistent* if it is in $\mathbb{H}_t$ for some integer t.

The reader may 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 t queries in the compressed oracle model satisfies $|\phi_t\rangle \in \mathbb{H}_t$.*

Proof. We check the four properties stated in Definition 4.3. The first property follows from the fact that each 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 (4.1), 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 $\omega_N = e^{\frac{2\mathbf{i}\pi}{N}}$ as ω. We also adopt the following notation to modify one entry of a database (we recall that for a history H the notation $H_{x \leftarrow y}$ is used for appending (x, y) to the list).

Definition 4.5 ($D_{x \leftarrow y}$)**.** 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 by

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

The next lemmas 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, the database remains unchanged apart from an added phase.

Lemma 4.6 (Quantum Query $\mathcal{R}_0$)**.** *Let $|x,p,w\rangle|H,D\rangle$ be a history-database consistent basis state. Then, $\mathcal{R}_0$ maps this state to $|x,p,w0\rangle|H\rangle|\varphi\rangle$ where the state $|\varphi\rangle$ of the database register is*

$$\cdot\ \omega^{pD(x)}|D\rangle \qquad (\text{if } H(x)\neq\star \text{ or } p=0)$$

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

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

Lemma 4.7 (Classical Query $\mathcal{R}_1$)**.** *Let $|x,p,w\rangle|H,D\rangle$ be a history-database consistent basis state. Then, $\mathcal{R}_1$ maps this state to $|x,p,w1\rangle|\varphi\rangle$ where the state $|\varphi\rangle$ of the history-database registers is*

$$\cdot\ \omega^{pD(x)}|H_{x\leftarrow D(x)},D\rangle \qquad (\text{if } H(x)\neq\star)$$

$$\cdot\ \sum_{y\in[N]}\frac{\omega^{py}}{\sqrt{N}}|H_{x\leftarrow y},D_{x\leftarrow y}\rangle \qquad (\text{if } H(x)=\star,\ D(x)=\perp)$$

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

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 a 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 $|x,p,w\rangle_{\mathcal{A}}|H,D\rangle_{\mathcal{HD}}$. We define the projection

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

over all basis states satisfying 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 $|\phi\rangle$, a real $b\in[0,1]$ and a projector Π over $\mathcal{AHD}$, we define

$$\Delta_b(\Pi,|\phi\rangle)=\|\Pi\mathcal{R}_b|\phi\rangle\|^2-\|\Pi|\phi\rangle\|^2\quad\text{and}\quad\Gamma_b(\Pi,|\phi\rangle)=\frac{\|\Pi\mathcal{R}_b(\mathbb{I}-\Pi)|\phi\rangle\|^2}{\|(\mathbb{I}-\Pi)|\phi\rangle\|^2},$$

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

The quantity $\Delta_b(\Pi, |\phi\rangle) \in [-1, 1]$ represents the increase in norm of the projection onto Π after applying a hybrid query $\mathcal{R}_b$. These will be used as a measure of progress later in the proofs.

The quantity $\Gamma_b(\Pi, |\phi\rangle) \in [0, 1]$ tracks the amplitude that moves after making a query from a subspace to its orthogonal complement. In particular, if $\Gamma_b(\Pi, |\phi\rangle) \leq \gamma$, then we have that $\|\Pi\mathcal{R}_b(\mathbb{I} - \Pi)|\phi\rangle\|^2 \leq \gamma\|(\mathbb{I} - \Pi)|\phi\rangle\|^2$. In this paper, we only consider projectors Π_{P} for some predicates P. In such cases, we can equivalently write

$$\Gamma_b(\Pi_{\mathrm{P}}, |\phi\rangle) = \frac{\|\Pi_{\mathrm{P}}\mathcal{R}_b\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2}{\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2}.$$

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 notion of "database property" 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)**.** Let $\mathrm{P} : (H, D) \mapsto \{\textsc{False}, \textsc{True}\}$ be a predicate function over all history-database pairs. We say that it is a *history-database predicate* if for every true-pair $(H, D) \in \mathrm{P}^{-1}(\textsc{True})$,

- (Consistent) The pair (H, D) is history-database consistent (see Definition 4.3).
- (History Invariant) For every list H' such that (H', D) is history-database consistent and $H(x') = H'(x')$ for all $x' \in [M]$, we have $(H', D) \in \mathrm{P}^{-1}(\textsc{True})$.
- (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 $(H, D') \in \mathrm{P}^{-1}(\textsc{True})$.

By extension, we say that $\mathrm{P} : (x, p, w, H, D) \mapsto \{\textsc{False}, \textsc{True}\}$ is a history-database predicate if it does not depend on (x, p, w) and its restriction to (H, D) satisfies the above properties.

The next lemmas bound the progress overlap Γ_0 (resp. Γ_1) in terms of the probability γ 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 6.9), 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, t be an integer and $\gamma \in [0, 1]$ be a real parameter. Suppose that, for every false-state $(H, D) \in \mathrm{P}^{-1}(\textsc{False}) \cap \mathbb{H}_t$ where $D(x) = \perp$, the probability to make the predicate true by replacing $D(x)$ with a random value y is at most*

$$\Pr_{y \leftarrow [N]}\left[(H, D_{x \leftarrow y}) \in \mathrm{P}^{-1}(\textsc{True})\right] \leq \gamma. \tag{4.3}$$

Then, the quantum progress overlap is at most $\Gamma_0(\Pi_{\mathrm{P}}, |\phi\rangle) \leq 10\gamma$ for all $|\phi\rangle \in \mathbb{H}_t$.

The adaptation of the above lemma to the classical query case requires making one extra assumption stated in Equation (4.5) 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, t be an integer and $\gamma \in [0, 1]$ be a real parameter. Suppose that, for every false-state $(H, D) \in$*

$\mathrm{P}^{-1}(\textsc{False}) \cap \mathbb{H}_t$ *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*

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

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

$$(H, D) \in \mathrm{P}^{-1}(\textsc{False}) \quad \Rightarrow \quad (H_{x \leftarrow D(x)}, D) \in \mathrm{P}^{-1}(\textsc{False}). \tag{4.5}$$

Then, the classical progress overlap is at most $\Gamma_1(\Pi_{\mathrm{P}}, |\phi\rangle) \leq 2\gamma$ *for all* $|\phi\rangle \in \mathbb{H}_t$*.*

Note that γ will often depend on the maximum number t of values contained in the database and in the history. Moreover, if Lemmas 4.12 and 4.13 hold with parameters γ_0 and γ_1 respectively, then the progress interpolates as $\Gamma_b(\Pi_{\mathrm{P}}, |\phi\rangle) \leq 10(1-b)\gamma_0 + 2b\gamma_1$.

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. *The success probability of finding a zero preimage, in a uniformly random function* $D : [M] \to [N]$*, is at most*

- (Model 1.) $O\left(\frac{c+q^2}{N}\right)$ *using* q *quantum queries and* c *classical queries,*
- (Model 2.) $O\left(\frac{t}{bN}\right)$ *using* t *queries to the hybrid oracle* $\mathcal{O}_b$ *where* $1/t \leq b \leq 1$*,*
- (Model 3.) $O\left(\frac{dt}{N}\right)$ *using* t *quantum queries with bounded-depth* $1 \leq d \leq t$*.*

The above inequalities are optimal. 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 $D(x') = H(x') = 0$.
- XQ: the predicate Q holds *and* the query index x is the only zero preimage in the quantum database D that is not in the history H, i.e. $D(x) = 0$, $H(x) = \star$ and $H(x') = 0$ if $D(x') = 0$ for all $x' \neq x$.

- $\overline{\mathrm{X}}\mathrm{Q}$: the predicate Q holds but not XQ (i.e., there exists $x' \neq x$ such that $D(x') = 0$ and $H(x') = \star$).

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

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. We remark that because of the above, our hybrid compressed oracle framework avoids the need of using [Zha19, Lemma 5] that is typically needed for proofs in the usual compressed oracle framework.

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 ($b = 0$) or classical ($b = 1$) query, we show that the progress evolves as follows in terms of the quantity defined in Definition 4.10:

$$\Delta_b(\Pi, |\phi\rangle) = \|\Pi\mathcal{R}_b|\phi\rangle\|^2 - \|\Pi|\phi\rangle\|^2.$$

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

$$\Delta_0(\Pi_{\mathrm{C}}, |\phi\rangle) = 0 \quad \text{and} \quad \Delta_0(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq 2\sqrt{\frac{10}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{10}{N}.$$

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

$$\Delta_1(\Pi_{\mathrm{C}}, |\phi\rangle) \leq 2\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \delta + \frac{4}{N} \quad \text{and} \quad \Delta_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}, |\phi\rangle) = -\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \delta$$

where $\delta = \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$.

The first proposition follows from a similar (but refined) analysis of the preimage search in the compressed oracle framework of [Zha19]. The second proposition is different from the usual analysis in this framework as it shows that a classical query can also decrease the progress the algorithm has made. We shall give their proofs later. First we show how the above imply optimal lower bounds for preimage search. It suffices to prove the results in models 1 and 2 since the result in model 3 follows by that in model 2 and Corollary 3.5.

Theorem 5.5. *The progress made by any algorithm after t queries satisfies*

- (Model 1.) $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 = O\left(\frac{c+q^2}{N}\right)$ *if q queries use the quantum oracle and c queries use the classical oracle with $c + q = t$,*
- (Model 2.) $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 = O\left(\frac{t}{bN}\right)$ *if all queries use the hybrid oracle $\mathcal{O}_b$ for some $1/t \leq b \leq 1$.*

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

$$\Psi_t := \|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2.$$

Observe that $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \leq \Psi_t$[5]. We claim that the following recurrence holds for the potential Ψ_t if the t-th query is made to the oracle $\mathcal{O}_b$ with $b \in [0, 1]$:

$$\Psi_t \leq \Psi_{t-1} + \min\left(11\sqrt{\frac{\Psi_{t-1}}{N}}, \frac{90}{bN}\right) + \frac{30}{N} \tag{5.1}$$

[5]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 $\frac{1}{3}\Psi_t \leq \|\Pi_{\mathrm{Q}+\mathrm{C}}|\phi_t\rangle\|^2 \leq \Psi_t$ but we do not use this fact.

with the initial condition that $\Psi_0 = 0$. Recalling the definition of $\Delta_b(\Pi, |\phi\rangle)$, it follows from the fact $\Psi_t = \|\Pi_{\mathrm{C}}\mathcal{R}_b|\phi_{t-1}\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_b|\phi_{t-1}\rangle\|^2 = \Psi_{t-1} + \Delta_b(\Pi_{\mathrm{C}}, |\phi_{t-1}\rangle) + 3\Delta_b(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi_{t-1}\rangle)$ and Propositions 5.3 and 5.4 that

$$\begin{aligned}\Psi_t &\leq \Psi_{t-1} - b\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\|^2 + 6(1-b)\sqrt{\frac{10}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| - 2\delta b + \frac{30-26b}{N} \\ &\leq \Psi_{t-1} - b\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\|^2 + 6\sqrt{\frac{10}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| + \frac{30}{N}.\end{aligned}$$

We obtain Equation (5.1) by bounding the term $-b\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\|^2 + 6\sqrt{\frac{10}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\|$ in two different ways: (1) using that $\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| \leq \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_{t-1}\rangle\| \leq \sqrt{\Psi_{t-1}/3}$, it is at most $11\sqrt{\Psi_{t-1}/N}$, (2) using that the polynomial $-bZ^2 + 6\sqrt{\frac{10}{N}}Z$ is maximized at $Z = \sqrt{\frac{90}{b^2N}}$ when $b > 0$, it is at most $\frac{90}{bN}$.

If all queries use the same oracle $\mathcal{O}_b$, for some $b \neq 0$, then by Equation (5.1) we get

$$\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \leq \Psi_t = O\Big(\frac{t}{bN}\Big),$$

which proves the second statement in the theorem. If instead each query is either to the quantum ($b = 0$) or classical ($b = 1$) oracle then the potential increases by at most $\Psi_t - \Psi_{t-1} \leq 11\sqrt{\Psi_{t-1}/N} + 30/N$ when making a quantum query and $\Psi_t - \Psi_{t-1} \leq 120/N$ when making a classical query by Equation (5.1). We can assume that the last two inequalities are replaced with equalities as it can only increase the maximum possible value for Ψ_t. Observe in this case that the potential always increases by the same amount $120/N$ when making a classical query, whereas for quantum queries it is advantageous to first maximize the value of Ψ_{t-1}. Hence, for an algorithm making c classical and q quantum queries, the optimal strategy is to use the classical recurrence for the first c steps and the quantum recurrence afterward. In this case, it follows that for $t = q + c$ queries, 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 Propositions 5.3 and 5.4.

Proof of Proposition 5.3. The first equality is due to the fact that a quantum query $\mathcal{R}_0$ 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 $\mathcal{R}_0$ 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 $\mathcal{R}_0$. Since $\mathbb{I} = \Pi_{\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}$ and the projectors in the summation are orthogonal, the statement $\|\Pi_{\mathrm{C}}\mathcal{R}_0|\phi\rangle\| = \|\Pi_{\mathrm{C}}|\phi\rangle\|$ follows and hence $\Delta_0(\Pi_{\mathrm{C}}, |\phi\rangle) = 0$.

To see the second inequality, we have that

$$\begin{aligned}\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{C}} + \Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\leq \|\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + (\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|)^2 \\ &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2. \qquad (5.2)\end{aligned}$$

The second equality uses that $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\mathrm{C}} = 0$ since any basis state in the support of Π_{C} will remain in the support of the same projector. This is because $\mathcal{R}_0$ acts as a control on $\mathcal{H}$ and there is already a zero preimage $x \in H$ before applying $\mathcal{R}_0$. The third equality uses that

$\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle$ is orthogonal to $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$ since the former is supported over basis states $|x\rangle_{\mathcal{X}}|D\rangle_{\mathcal{D}}$ containing a zero preimage in D not equal to x, whereas the latter can only contain the preimage x. The last two lines uses the triangle inequality and the fact that $\|\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2+\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2=\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$.

To bound the term $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$ in (5.2), 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, $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|\leq\|\Pi_{\mathrm{Q}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}}\Pi_{\overline{\mathrm{C}}}|\phi\rangle\|$. 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 (5.2) and rearranging, we get the desired inequality about $\Delta_0(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}},|\phi\rangle)$. □

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

$$\begin{aligned}
\|\Pi_{\mathrm{C}}\mathcal{R}_1|\phi\rangle\|^2 &= \|\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{C}}+\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2\\
&= \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}|\phi\rangle\|^2+\|\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2\\
&= \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}|\phi\rangle\|^2+\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2+\|\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2\\
&\leq \|\Pi_{\mathrm{C}}|\phi\rangle\|^2+\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2+2\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2+2\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2. \qquad (5.3)
\end{aligned}$$

The second equality in the above sequence follows since $\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}|\phi\rangle$ is orthogonal to $\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$. This can be seen from the fact that the history register $\mathcal{H}$ in $\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}|\phi\rangle$ is supported over basis states $|H\rangle_{\mathcal{H}}$ where the first c entries of H contains a zero preimage. Therefore, it is orthogonal to $\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$. Similarly, the third equality uses that $\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle$ is orthogonal to $\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle$ since the latter is supported over basis states $|x\rangle_{\mathcal{X}}|D\rangle_{\mathcal{D}}$ where the only possible zero preimage in D is x. 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 any states $|a\rangle$ and $|b\rangle$.

Since $\mathrm{Q}+\mathrm{C}$ is a history-database predicate satisfying Equation (4.5), we can use Lemma 4.13 to bound the last term in Equation (5.3). It gives us that for $\gamma=\frac{1}{N}$,

$$\Gamma_1(\Pi_{\mathrm{Q}+\mathrm{C}},|\phi\rangle)\leq 2\gamma \implies \|\Pi_{\mathrm{Q}+\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\leq 2\gamma\|\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\leq\frac{2}{N}$$

and $\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\leq\|\Pi_{\mathrm{Q}+\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$. Recalling Definition 4.10, we thus have shown that

$$\Delta_1(\Pi_{\mathrm{C}},|\phi\rangle)\leq 2\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2+\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2+\frac{4}{N},$$

proving the first inequality in the statement of the proposition.

The second equality is relatively straightforward:

$$\begin{aligned}
\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_1|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{C}}+\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2\\
&= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\\
&= \|\Pi_{\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\\
&= \|\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2-\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2\\
&= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2-\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2-\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2,
\end{aligned}$$

where the second line is true as $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{C}}+\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{C}}})=0$. This holds since a classical query $\mathcal{R}_1$ 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 the state $\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}|\phi\rangle$ must necessarily contain a zero preimage in the database (by the predicate $\overline{\mathrm{X}}\mathrm{Q}$). The last two lines use that $\Pi_{\mathrm{C}}+\Pi_{\overline{\mathrm{C}}}=\mathbb{I}$ and $\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{C}}}=\Pi_{\mathrm{Q}\cdot\overline{\mathrm{C}}}$ where the projectors in each sum are orthogonal. □

6 Collision Finding

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

Theorem 6.1. *The success probability of finding a colliding pair, in a uniformly random function $D : [M] \to [N]$, is at most*

- (Model 1.) $O\left(\frac{c^2+cq^2+q^3}{N}\right)$ *using q quantum queries and c classical queries,*
- (Model 2.) $O\left(\frac{t^2}{bN}\right)$ *using t queries to the hybrid oracle $\mathcal{O}_b$ where $1/t \leq b \leq 1$,*
- (Model 3.) $O\left(\frac{dt^2}{N}\right)$ *using t quantum queries with bounded-depth $1 \leq d \leq t$.*

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 and 6.4.

6.1 Progress Measure

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 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).
- XQ: the predicate Q holds *and* the query index x is contained in every quantum collision.
- XH: the predicate H holds *and* the query index is contained in every hybrid collision *and* the query index is not in the history.
- $\overline{\text{X}}$Q (resp. $\overline{\text{X}}$H): the predicate Q (resp. H) holds, but not XQ (resp. XH).

Note that XQ + $\overline{\text{X}}$Q = Q and XH + $\overline{\text{X}}$H = H. Furthermore, the predicate $\overline{\text{X}}$Q is equivalent to the existence of a quantum collision not containing the query index. The last four predicates are the only ones that depend on the value x contained in the index register. The other predicates depend only on the history-database (H, D).

We will combine the above predicates into the potential

$$\Psi(|\phi\rangle) = \|\Pi_{\text{C}}|\phi\rangle\|^2 + 3\|\Pi_{\text{H}\cdot\overline{\text{C}}}|\phi\rangle\|^2 + 7\|\Pi_{\text{Q}\cdot\overline{\text{H}}\cdot\overline{\text{C}}}|\phi\rangle\|^2$$

that allows for bounding the probability $\|\Pi_{\text{Q+H+C}}|\phi\rangle\|^2 = \|\Pi_{\text{C}}|\phi\rangle\|^2 + \|\Pi_{\text{H}\cdot\overline{\text{C}}}|\phi\rangle\|^2 + \|\Pi_{\text{Q}\cdot\overline{\text{H}}\cdot\overline{\text{C}}}|\phi\rangle\|^2$ of recording any type of collision.

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 $\|\Pi_{\mathrm{Q+H+C}}|\phi_t\rangle\|^2$ of recording any type of collision is an upper bound on the success probability. Since a direct bound on this quantity is difficult to obtain, we instead analyze the three predicates C, $\mathrm{H}\cdot\overline{\mathrm{C}}$, $\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}$ separately, and later combine them into a bound on the potential $\Psi(|\phi_t\rangle)$.

We first show that performing a quantum query incurs the following progress increases.

Lemma 6.4 (Progress Measure, Quantum Query)**.** *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ are at most,*

$$\begin{aligned}
\Delta_0(\Pi_{\mathrm{C}}, |\phi\rangle) &= 0\,,\\
\Delta_0(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\le 2\sqrt{\frac{10t}{N}}\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{10t}{N}\,,\\
\Delta_0(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\le \sqrt{\frac{8t}{N}}\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + 2\sqrt{\frac{20t}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{20t}{N}\,.
\end{aligned}$$

Recall that, by Definition 4.10, the quantity $\Delta_0(\Pi_{\mathrm{P}}, |\phi\rangle) \in [-1, 1]$ for a predicate P represents the progress increase $\Delta_0(\Pi_{\mathrm{P}}, |\phi\rangle) = \|\Pi_{\mathrm{P}}\mathcal{R}_0|\phi\rangle\|^2 - \|\Pi_{\mathrm{P}}|\phi\rangle\|^2$ 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 t/N since it must collide with one of the at most t 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 increase when the query is classical.

Lemma 6.5 (Progress Measure, Classical Query)**.** *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$ with norm at most 1, the progress caused by one classical query on $|\phi\rangle$ are at most,*

$$\begin{aligned}
\Delta_1(\Pi_{\mathrm{C}}, |\phi\rangle) &\le 2\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \delta_1 + \frac{4t}{N}\,,\\
\Delta_1(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\le -\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \delta_1 + 2\delta_2 + \frac{12t}{N}\,,\\
\Delta_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) &\le \sqrt{\frac{2t}{N}}\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\| - \|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \delta_2
\end{aligned}$$

where $\delta_1 = \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ and $\delta_2 = \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$.

The negative terms on the right-hand side represent the amount of progress transferred by one classical query between different progress measures. Note that, as a simple case, if an algorithm makes only classical queries then there can be no hybrid or quantum collision, hence $\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| = \|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\| = 0$ and the above inequalities simplify to $\Delta_1(\Pi_{\mathrm{C}}, |\phi_t\rangle) = \|\Pi_{\mathrm{C}}\mathcal{R}_1|\phi_t\rangle\|^2 - \|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 \le 4t/N$. Thus, we recover the birthday bound $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 = O(t^2/N)$ after t classical queries.

We now combine the two lemmas to bound the potential increase under applying the hybrid compressed oracle $\mathcal{R}_b$.

Proposition 6.6. *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$ with norm at most 1, upon applying the hybrid compressed oracle $\mathcal{R}_b$, the potential increases by at most*

$$\Psi(\mathcal{R}_b|\phi\rangle) \le \Psi(|\phi\rangle) + \min\left(81\sqrt{\frac{t\cdot\Psi(|\phi\rangle)}{N}},\ \frac{1641t}{bN}\right) + \frac{170t}{N} \tag{6.1}$$

for all $b \in [0, 1]$.

Proof. We start by proving

$$\Psi(\mathcal{R}_b|\phi\rangle) \leq \Psi(|\phi\rangle) - b\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 81\sqrt{\frac{t}{N}}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{170t}{N} \tag{6.2}$$

for all $b \in [0,1]$. By combining Lemmas 6.4 and 6.5 with the fact that

$$\begin{aligned}\Psi(\mathcal{R}_b|\phi\rangle) &= (1-b)\Psi(\mathcal{R}_0|\phi\rangle) + b\Psi(\mathcal{R}_1|\phi\rangle)\\ &= \Psi(|\phi\rangle) + \Delta_b(\Pi_{\mathrm{C}}, |\phi\rangle) + 3\Delta_b(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) + 7\Delta_b(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle),\end{aligned}$$

we have that

$$\begin{aligned}\Psi(\mathcal{R}_b|\phi\rangle) \leq \Psi(|\phi\rangle) &- b(\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2)\\ &+ 40\sqrt{\frac{t}{N}}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + 70\sqrt{\frac{t}{N}}\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{170t}{N}.\end{aligned}$$

Equation (6.2) follows by observing that

$$\begin{aligned}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 &= \|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2, \text{ and}\\ 40\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + 70\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| &\leq \sqrt{40^2+70^2}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|,\end{aligned}$$

where the last inequality follows from Cauchy–Schwarz.

Finally, the proposition is derived from Equation (6.2) and the fact that

$$\begin{aligned}-b\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 81\sqrt{\frac{t}{N}}&\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|\\ &\leq \min\{81\sqrt{\frac{t}{N}}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}+\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|, \frac{1641t}{bN}\}\\ &\leq \min\{81\sqrt{\frac{t}{N}\cdot\Psi(|\phi\rangle)}, \frac{1641t}{bN}\}\end{aligned}$$

since the polynomial $-bZ^2 + 81\sqrt{\frac{t}{N}}Z$ is maximized at $Z = 81\sqrt{\frac{t}{4b^2N}}$. □

Finally, we can prove our main theorem by tuning the interpolation coefficient b.

Proof of Theorem 6.1. We first consider the case of hybrid algorithms that only make classical or quantum queries (model 1). We want to upper bound the probability that an algorithm outputs a collision pair after $t = c + q$ queries, of which c are classical and q are quantum. Fix any such algorithm and let $|\phi_t\rangle$ denote its state as defined in Equation (4.2). We can always assume, at the cost of doing two extra classical queries, that the output is contained in the history register. Hence, the success probability of the algorithm is upper bounded by the probability $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2$ of having recorded a classical collision. We now prove the upper bound $\|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 = O((c^2 + cq^2 + q^3)/N)$ that matches our theorem. For that, we consider the potential after t queries defined as

$$\Psi_t := \|\Pi_{\mathrm{C}}|\phi_t\rangle\|^2 + 3\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2 + 7\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi_t\rangle\|^2.$$

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. By Proposition 6.6, at each query, the potential increases by at most,

$$\Psi_t \leq \begin{cases}\left(\sqrt{\Psi_{t-1}} + 41\sqrt{\frac{t-1}{N}}\right)^2 & \text{if the } t\text{-th query is quantum } (b=0),\\ \Psi_{t-1} + \frac{1811(t-1)}{N} & \text{if the } t\text{-th query is classical } (b=1).\end{cases}$$

The maximum increase permitted by the above two inequalities is achieved when all the classical queries are performed first. Thus, we conclude that

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

We now study the case of algorithms that make t queries to the same hybrid oracle $\mathcal{O}_b$ where $b > 0$ (model 2). By using the same definition of Ψ_t as above, together with Proposition 6.6, we obtain that

$$\Psi_t = O\left(\frac{t^2}{bN}\right)$$

since each query increases the potential by at most $O(t/(bN))$.

Finally, the case of bounded-depth algorithms (model 3) follows by the result in model 2 and Corollary 3.5. □

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 $\mathbb{H}_t$ of consistent states:*

$$\Pi_{\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\mathrm{C}},\ \Pi_{\mathrm{C}}\mathcal{R}_0\Pi_{\overline{\mathrm{C}}},\ \Pi_{\mathrm{Q}\cdot\mathrm{H}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}},\ \Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{H}}$$

and

$$\Pi_{\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{C}},\ \Pi_{\mathrm{Q}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}},\ \Pi_{\overline{\mathrm{Q}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}},\ \Pi_{\overline{\mathrm{H}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}}\,.$$

For any states $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{H}_t$ and basis-state predicate P, the following vectors are orthogonal:

$$\Pi_{\mathrm{P}}\mathcal{R}_b\Pi_{\overline{\mathrm{X}}\mathrm{Q}}|\phi_1\rangle \perp \mathcal{R}_b(\Pi_{\overline{\mathrm{Q}}} + \Pi_{\mathrm{X}\mathrm{Q}})|\phi_2\rangle \quad \textit{and} \quad \Pi_{\mathrm{P}}\mathcal{R}_b\Pi_{\overline{\mathrm{X}}\mathrm{H}}|\phi_1\rangle \perp \mathcal{R}_b(\Pi_{\overline{\mathrm{H}}} + \Pi_{\mathrm{X}\mathrm{H}})|\phi_2\rangle.$$

for $b \in \{0,1\}$.

Proof. The statement follows by simple applications of Lemmas 4.6 and 4.7.

We detail the proof of the equality $\Pi_{\mathrm{Q}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}} = 0$. 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 $\mathcal{R}_1|x,p,w,H,D\rangle$ must be identical to (H,D) except possibly on the value x. Furthermore, since x must be in the history after the classical query (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 sketch the proof of $\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}}|\phi_1\rangle \perp \mathcal{R}_1\Pi_{\overline{\mathrm{H}}}|\phi_2\rangle$. Every basis state in the support of $\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}}|\phi_1\rangle$ has a hybrid collision that does not contain the query index. On the other hand, none of the basis states in the support of $\mathcal{R}_1\Pi_{\overline{\mathrm{H}}}|\phi_2\rangle$ satisfy this property since the only possible hybrid collisions must contain the index on which $\mathcal{R}_1$ is queried. Hence, $\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}}|\phi_1\rangle \perp \mathcal{R}_1\Pi_{\overline{\mathrm{H}}}|\phi_2\rangle$. Finally, applying Π_{P} does not change the orthogonality property since it can only remove basis states from the support of these states. □

We now analyze the effect of quantum and classical queries on the progress overlaps $\Gamma_0(\Pi,|\phi\rangle), \Gamma_1(\Pi,|\phi\rangle) \in [0,1]$ for different projectors Π. Recall that, by Definition 4.10, these numbers give the relative amplitude that moves from the support of $\mathbb{I}-\Pi$ to the support of Π after making a query, i.e. $\Gamma_b(\Pi,|\phi\rangle) = \|\Pi\mathcal{R}_b(\mathbb{I}-\Pi)|\phi\rangle\|^2 / \|(\mathbb{I}-\Pi)|\phi\rangle\|^2$. Notice that Fact 6.7 already shows that $\Gamma_0(\Pi_{\mathrm{C}},|\phi\rangle) = \Gamma_0(\Pi_{\overline{\mathrm{C}}},|\phi\rangle) = \Gamma_1(\Pi_{\overline{\mathrm{C}}},|\phi\rangle) = 0$.

Lemma 6.8. *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$, the progress overlap caused by one quantum query on $|\phi\rangle$ are at most,*

$$\Gamma_0(\Pi_{\mathrm{Q}}, |\phi\rangle) \leq \frac{10t}{N}\,, \qquad (6.3) \qquad \Gamma_0(\Pi_{\mathrm{Q+H}}, |\phi\rangle) \leq \frac{10t}{N}\,, \qquad (6.4)$$

$$\Gamma_0(\Pi_{\mathrm{H}}, |\phi\rangle) \leq \frac{10t}{N}\,, \qquad (6.5)$$

and the progress overlap caused by one classical query on $|\phi\rangle$ are,

$$\Gamma_1(\Pi_{\mathrm{Q}}, |\phi\rangle) = 0\,, \qquad (6.6) \qquad \Gamma_1(\Pi_{\mathrm{Q+H}}, |\phi\rangle) \leq \frac{2t}{N}\,. \qquad (6.7)$$

Proof. The inequalities for quantum queries follow from Lemma 4.12 as $\mathrm{Q}, \mathrm{Q}+\mathrm{H}$ and H are history-database predicates (Definition 4.11) with the γ parameters being t/N. Similarly, for classical queries, the two inequalities follow from Lemma 4.13 with the γ parameters being 0 and t/N respectively. □

Finally, we give four inequalities that do not follow from Lemmas 4.12 and 4.13. Equations (6.8) and (6.10) 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 (6.9) 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 (6.11) overcomes the fact that the predicate $\mathrm{H}+\mathrm{C}$ does not satisfy the condition stated in Equation (4.5).

Lemma 6.9. *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$, we have*

$$\Gamma_0(\Pi_{\overline{\mathrm{H+C}}}, |\phi\rangle) \leq \frac{10t}{N}\,, \qquad (6.8) \qquad \|\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \frac{t}{N}\cdot\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2\,, \qquad (6.9)$$

$$\Gamma_1(\Pi_{\overline{\mathrm{H+C}}}, |\phi\rangle) \leq \frac{2t}{N}\,, \qquad (6.10) \qquad \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2 \leq \frac{2t}{N}\cdot\|\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2\,. \qquad (6.11)$$

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

6.4 Progress Increase Lemmas

In this section, we analyze the progress measures for: (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.

Lemma 6.4 (Progress Measure, Quantum Query). *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$ with norm at most 1, the progress caused by one quantum query on $|\phi\rangle$ satisfies*

$$\Delta_0(\Pi_{\mathrm{C}}, |\phi\rangle) = 0\,, \qquad (6.12)$$

$$\Delta_0(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq 2\sqrt{\frac{10t}{N}}\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{10t}{N}\,, \qquad (6.13)$$

$$\Delta_0(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \leq \sqrt{\frac{8t}{N}}\|\Pi_{\mathrm{XH}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + 2\sqrt{\frac{20t}{N}}\|\Pi_{\mathrm{XQ}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \frac{20t}{N}\,. \qquad (6.14)$$

Proof of Equation (6.12). We have $\|\Pi_{\mathrm{C}}\mathcal{R}_0|\phi\rangle\|^2 = \|\Pi_{\mathrm{C}}\mathcal{R}_0\Pi_{\mathrm{C}}|\phi\rangle\|^2 = \|\Pi_{\mathrm{C}}|\phi\rangle\|^2$ since $\mathbb{I} = \Pi_{\mathrm{C}} + \Pi_{\overline{\mathrm{C}}}$ and $\Pi_{\mathrm{C}}\mathcal{R}_0\Pi_{\overline{\mathrm{C}}} = \Pi_{\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\mathrm{C}} = 0$ by Fact 6.7. □

Proof of Equation (6.13). We use the decomposition $\mathbb{I} = \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}$. By Fact 6.7, $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\mathrm{C}} = 0$ and the states $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle = \Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{H}}\Pi_{\overline{\mathrm{C}}}|\phi\rangle$ and $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}+\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle = \Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{X}\mathrm{H}} + \Pi_{\overline{\mathrm{H}}})\Pi_{\overline{\mathrm{C}}}|\phi\rangle$ are orthogonal. Therefore,

$$\begin{aligned}
\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0|\phi\rangle\|^2 &= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}})|\phi\rangle\|^2 \\
&= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\
&\le \|\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + (\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{H}}\mathcal{R}_0\Pi_{\overline{\mathrm{H}}}|\phi\rangle\|)^2 \\
&= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{H}}\mathcal{R}_0\Pi_{\overline{\mathrm{H}}}|\phi\rangle\| + \|\Pi_{\mathrm{H}}\mathcal{R}_0\Pi_{\overline{\mathrm{H}}}|\phi\rangle\|^2
\end{aligned}$$

where the third line uses the triangle inequality, and the last line uses that $\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 = \|\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$. Finally, $\|\Pi_{\mathrm{H}}\mathcal{R}_0\Pi_{\overline{\mathrm{H}}}|\phi\rangle\|^2 \le 10t/N$ by Equation (6.5). □

Proof of Equation (6.14). We use the decomposition $\mathbb{I} = \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}$. By Fact 6.7, $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}) = 0$ and the states $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle$ and $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle$ are orthogonal. Therefore,

$$\begin{aligned}
&\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0|\phi\rangle\|^2 \\
&\quad= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}})|\phi\rangle\|^2 \\
&\quad\le \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0(\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_0\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \\
&\quad\le \|\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + (\|\Pi_{\mathrm{Q}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| + \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|)^2 + 3\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \\
&\quad= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \cdot \|\Pi_{\mathrm{Q}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\| + \|\Pi_{\mathrm{Q}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\|^2 + 3\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|
\end{aligned}$$

where the second line uses the identity $\|a+b\|^2 \le \|a\|^2 + 3\|b\|$ when $\|a\|, \|b\| \le 1$, the third line uses the triangle inequality and the last line uses that $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 = \|\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|$. Finally, $\|\Pi_{\mathrm{Q}}\mathcal{R}_0\Pi_{\overline{\mathrm{Q}}}|\phi\rangle\|^2 \le 10t/N$ by Equation (6.3) and $\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \le (10t/N)\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ by Equation (6.8). □

We now analyze the case of classical queries.

Lemma 6.5 (Progress Measure, Classical Query). *Given an integer t and a state $|\phi\rangle \in \mathbb{H}_t$ with norm at most 1, the progress caused by one classical query on $|\phi\rangle$ are at most,*

$$\Delta_1(\Pi_{\mathrm{C}}, |\phi\rangle) \le 2\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \delta_1 + \frac{4t}{N}\,, \tag{6.15}$$

$$\Delta_1(\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \le -\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \delta_1 + 2\delta_2 + \frac{12t}{N}\,, \tag{6.16}$$

$$\Delta_1(\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}, |\phi\rangle) \le \sqrt{\frac{2t}{N}}\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| - \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \delta_2 \tag{6.17}$$

where $\delta_1 = \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ and $\delta_2 = \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$.

Proof of Equation (6.15). We use the decomposition $\mathbb{I} = \Pi_{\mathrm{C}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$. By Fact 6.7, the states $\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}|\phi\rangle$, $\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle$ and $\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle$ are orthogonal. Therefore,

$$\begin{aligned}
\|\Pi_{\mathrm{C}}\mathcal{R}_1|\phi\rangle\|^2 &= \|\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{C}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})\|^2 \\
&= \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\mathrm{C}}\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\
&\le \|\Pi_{\mathrm{C}}\|^2 + \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + 2\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2
\end{aligned}$$

where the last line uses the identity $\|a+b\|^2 \le 2\|a\|^2 + 2\|b\|^2$. Finally, $\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \le 2t/N$ by Equation (6.11). □

Proof of Equation (6.16). We use the decomposition $\mathbb{I} = \Pi_{\mathrm{C}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$. By Fact 6.7, $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{C}} = 0$ and the states $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle$ and $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle$ are orthogonal. Therefore,

$$\begin{aligned}\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1|\phi\rangle\|^2 &= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &= \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 - \|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2\end{aligned}$$

where the second line uses that $\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 - \|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 = \|\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 - \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 = \|\Pi_{\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2 = \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}}\|^2$ since $\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} = 0$ by Fact 6.7. It remains to bound $\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2$. We further decompose $\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$ into $\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} = \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}$ and observe that $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle$ and $\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle$ are orthogonal by Fact 6.7. Hence,

$$\begin{aligned}&\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\quad\le 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\quad= 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\quad\le 2\|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 2\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + \frac{12t}{N}\end{aligned}$$

where the last line uses the triangle inequality and Equations (6.7) and (6.9) on $\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \le (\|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| + \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}})|\phi\rangle\|)^2 \le (1+\sqrt{2})^2 t/N$. □

Proof of Equation (6.17). We use the decomposition $\mathbb{I} = \Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}$. By Fact 6.7, $\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\overline{\mathrm{Q}}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\overline{\mathrm{X}}\mathrm{H}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}}) = 0$. Therefore,

$$\begin{aligned}\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1|\phi\rangle\|^2 &= \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1(\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}})|\phi\rangle\|^2 \\ &\le \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\| \\ &\le \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 + 3\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|\end{aligned}$$

where the last line uses $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \le \|(\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} + \Pi_{\mathrm{C}})\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 = \|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{X}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 - \|\Pi_{\mathrm{H}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\overline{\mathrm{X}}\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$. Finally, $\|\Pi_{\mathrm{Q}\cdot\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2 \le (2t/N)\|\Pi_{\mathrm{X}\mathrm{H}\cdot\overline{\mathrm{C}}}|\phi\rangle\|^2$ by Equation (6.10). □

Acknowledgements

The authors would like to thank Ansis Rosmanis for fruitful discussions and for sharing a draft of his work on noisy oracles [Ros23]. The authors are also grateful to the anonymous referees for their valuable comments and suggestions which helped to improve the paper. Part of this work was supported by the Simons Institute through Simons-Berkeley Postdoctoral Fellowships.

References

[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. 4).

[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 p. 6).

[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. 3, 4, 6).

[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. 4).

[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. 4).

[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. 5).

[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 (EUROCRYPT)*. 2020, pp. 788–817 (cit. on p. 6).

[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 pp. 1, 2).

[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. 4).

[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. 5).

[BG09] B. Barak and O. Goldreich. "Universal Arguments and their Applications". In: *SIAM Journal on Computing* 38.5 (2009), pp. 1661–1694 (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. 6).

[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. 1–3).

[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. 4).

[BV97] E. Bernstein and U. V. Vazirani. "Quantum Complexity Theory". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1411–1473 (cit. on p. 2).

[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. 2).

[CCHL23] S. Chen, J. Cotler, H.-Y. Huang, and J. Li. "The Complexity of NISQ". In: *Nature Communications* 14.1 (2023), p. 6001 (cit. on pp. 1, 3, 5, 6).

[CCL23] N.-H. Chia, K.-M. Chung, and C.-Y. Lai. "On the Need for Large Quantum Depth". In: *Journal of the ACM* 70.1 (2023) (cit. on pp. 3, 4, 6, 11, 14).

[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. 4, 19).

[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. 4).

[CH22] N.-H. Chia and S.-H. Hung. *Classical Verification of Quantum Depth*. arXiv:2205.04656 [quant-ph]. 2022 (cit. on pp. 4, 6).

[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. 4).

[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. 3, 4, 6, 14).

[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. 6, 19).

[CMSZ19] J. Czajkowski, C. Majenz, C. Schaffner, and S. Zur. *Quantum Lazy Sampling and Game-Playing Proofs for Quantum Indifferentiability*. arXiv:1904.11477 [quant-ph]. 2019 (cit. on p. 6).

[DFH22] J. Don, S. Fehr, and Y.-H. Huang. "Adaptive Versus Static Multi-oracle Algorithms, and Quantum Security of a Split-Key PRF". In: *Proceedings of the 20th Conference on Theory of Cryptography (TCC)*. 2022, pp. 33–51 (cit. on p. 13).

[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. 2).

[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. 4).

[GR04] L. K. Grover and J. Radhakrishnan. *Quantum Search for Multiple Items using Parallel Queries*. arXiv:quant-ph/0407217. 2004 (cit. on p. 4).

[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 p. 5).

[HG22] A. Hasegawa and F. L. Gall. "An Optimal Oracle Separation of Classical and Quantum Hybrid Schemes". In: *Proceedings of the 33rd International Symposium on Algorithms and Computation (ISAAC)*. 2022, 6:1–6:14 (cit. on pp. 3, 4, 6).

[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. 6).

[HLS22] Y. Hamoudi, Q. Liu, and M. Sinha. *Quantum-Classical Tradeoffs in the Random Oracle Model*. arXiv:2211.12954v1 [quant-ph]. 2022 (cit. on p. 1).

[HM23] Y. Hamoudi and F. Magniez. "Quantum Time–Space Tradeoff for Finding Multiple Collision Pairs". In: *ACM Transactions on Computation Theory* 15.1–2 (2023) (cit. on pp. 4, 6).

[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. 4).

[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. 4).

[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 p. 6).

[KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. 1st. Chapman & Hall/CRC, 2007 (cit. on p. 2).

[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. 4).

[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. 6).

[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. 6).

[Mer89] R. C. Merkle. "A Certified Digital Signature". In: *Proceedings of the 9th International Conference on the Theory and Applications of Cryptology (CRYPTO)*. 1989, pp. 347–363 (cit. on p. 2).

[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. 4).

[Ros21] A. Rosmanis. *Tight Bounds for Inverting Permutations via Compressed Oracle Arguments*. arXiv:2103.08975 [quant-ph]. 2021 (cit. on p. 6).

[Ros22] A. Rosmanis. *Hybrid Quantum-Classical Search Algorithms*. arXiv:2202.11443 [quant-ph]. 2022 (cit. on pp. 1, 3, 5, 6, 8).

[Ros23] A. Rosmanis. *Quantum Search with Noisy Oracle*. arXiv:2309.14944 [quant-ph]. 2023 (cit. on pp. 1, 3, 5, 6, 30).

[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. 6).

[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. 2).

[Sim97] D. R. Simon. "On the Power of Quantum Computation". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1474–1483 (cit. on p. 2).

[ST23] A. A. Sherstov and J. Thaler. "Vanishing-Error Approximate Degree and QMA Complexity". In: *Chicago Journal of Theoretical Computer Science* 2023.3 (2023) (cit. on p. 4).

[SZ19] X. Sun and Y. Zheng. *Hybrid Decision Trees: Longer Quantum Time is Strictly More Powerful*. arXiv:1911.13091 [cs.CC]. 2019 (cit. on pp. 1, 3–6).

[Zal99] C. Zalka. "Grover's Quantum Searching Algorithm is Optimal". In: *Physical Review A* 60 (1999), pp. 2746–2751 (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. 4, 6, 19, 21).

A Missing Proofs for Section 4 (Hybrid Compressed Oracle)

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 $\mathcal{R}_0 = S\mathcal{O}_0 S$ appends $|0\rangle$ to the workspace register and 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 in $\mathcal{D}_x$. 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

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

Applying $\mathcal{O}_0$ 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 again 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 $|H\rangle_{\mathcal{H}} = |(x_1, y_1), \ldots, (x_c, y_c), \star, \ldots, \star\rangle_{\mathcal{H}}$, for some integer c, denote the value contained in the history register. The operator $\mathcal{R}_1 = S\mathcal{O}_1 S$ appends $|1\rangle$ to the workspace register and acts as a control on all registers except $\mathcal{H}_{c+1}\mathcal{D}_x$, which contain $|\star, z\rangle_{\mathcal{H}_{c+1}\mathcal{D}_x}$ for some $z = D(x) \neq \perp$. Similarly as in the above proof of Lemma 4.6, after applying the first two operators $\mathcal{O}_1 S$, 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 $\mathcal{O}_1$). Finally, applying S 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 $\Pi_{\overline{\mathrm{P}}}|\phi\rangle = \sum_{x,p,w,H,D} \alpha_{x,p,w,H,D}|x, p, w\rangle|H, D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ 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 $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \leq 2\gamma \cdot \|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2$. 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 $|x, p, w, H, D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) = \star$ and $D(x) = \perp$.
- Π_2: all basis states $|x, p, w, H, D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) = \star$ and $D(x) \neq \perp$.
- Π_3: all basis states $|x, p, w, H, D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x) \neq \star$.

Below, we prove the inequalities $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_1|\phi\rangle\|^2 \leq \gamma\|\Pi_1|\phi\rangle\|^2$, $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\|^2 \leq \gamma\|\Pi_2|\phi\rangle\|^2$ and $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_3|\phi\rangle\| = 0$. Hence, by the triangle inequality and Cauchy–Schwarz inequality, we conclude that

$$\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \leq (\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_1|\phi\rangle\| + \|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\| + \|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_3|\phi\rangle\|)^2 \leq 2\gamma\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2.$$

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

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_1|\phi\rangle\|^2 &= \left\|\Pi_{\mathrm{P}}\mathcal{R}_1 \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp}} \alpha_{x,p,w,H,D}|x,p,w\rangle|H,D\rangle\right\|^2 \\
&= \left\|\Pi_{\mathrm{P}} \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp}} \alpha_{x,p,w,H,D}|x,p,w1\rangle\left(\sum_{y\in[N]}\frac{\omega^{py}}{\sqrt{N}}|H_{x\leftarrow y},D_{x\leftarrow y}\rangle\right)\right\|^2 \\
&= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\left[(H_{x\leftarrow y},D_{x\leftarrow y})\in \mathrm{P}^{-1}(\textsc{True})\right] \\
&\leq \gamma\|\Pi_1|\phi\rangle\|^2.
\end{aligned}$$

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 (4.4).

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 $D(x) = \perp$ 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 (4.5). Hence, we have

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\|^2 &= \left\|\Pi_{\mathrm{P}}\mathcal{R}_1 \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} \alpha_{x,p,w,H,D}|x,p,w\rangle|H,D\rangle\right\|^2 \\
&= \left\|\Pi_{\mathrm{P}} \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} \sum_{y\in[N]} \alpha_{x,p,w,H,D}\frac{\omega^{py}}{N}|x,p,w1\rangle|H_{x\leftarrow y},D_{x\leftarrow y}\rangle\right\|^2.
\end{aligned}$$

Next, observe that for any two tuples $(x,p,w,H,D_{x\leftarrow\perp},y) \neq (x',p',w',H',D'_{x'\leftarrow\perp},y')$, the basis states $|x,p,w1\rangle|H_{x\leftarrow y},D_{x\leftarrow y}\rangle$ and $|x',p',w'1\rangle|H'_{x'\leftarrow y'},D'_{x'\leftarrow y'}\rangle$ must be orthogonal. Thus, we can exploit this orthogonality property to simplify the above expression as follows.

$$\begin{aligned}
\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y}} \left\|\Pi_{\mathrm{P}}\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{py}}{N}|x,p,w1\rangle|H_{x\leftarrow y},D\rangle\right\|^2 \\
&= \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{P}(H_{x\leftarrow y},D)=\textsc{True}}} \left|\sum_{z\in[N]}\alpha_{x,p,w,H,D_{x\leftarrow z}}\frac{\omega^{py}}{N}\right|^2.
\end{aligned}$$

Applying the Cauchy–Schwarz inequality, we have

$$\begin{aligned}\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\|^2 &\le \sum_{\substack{x,p,w,H,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{P}(H_{x\leftarrow y},D)=\textsc{True}}} \sum_{z\in[N]} \frac{|\alpha_{x,p,w,H,D_{x\leftarrow z}}|^2}{N}\\ &= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} \left(\sum_{y\in[N]:\mathrm{P}(H_{x\leftarrow y},D_{x\leftarrow y})=\textsc{True}} \frac{|\alpha_{x,p,w,H,D}|^2}{N}\right)\\ &= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)\neq\perp}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\left[(H_{x\leftarrow y},D_{x\leftarrow y})\in \mathrm{P}^{-1}(\textsc{True})\right].\end{aligned}$$

Finally, for each $|x,p,w,H,D\rangle$ in the support of Π_2, we must have $\mathrm{P}(H,D_{x\leftarrow\perp}) = \textsc{False}$ by the database monotone property (see Definition 4.11). Hence, by Equation (4.4), the above inequality implies that $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_2|\phi\rangle\|^2 \le \gamma\cdot\|\Pi_2|\phi\rangle\|^2$.

Analysis of Π_3. By Lemma 4.7, the operator $\mathcal{R}_1$ maps any state $|x,p,w\rangle|H,D\rangle \in \mathrm{supp}(\Pi_3)$ to $\omega^{pD(x)}|x,p,w1\rangle|H_{x\leftarrow D(x)},D\rangle$ 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 $\mathrm{P}(H_{x\leftarrow D(x)},D) = \textsc{False}$ and $\|\Pi_{\mathrm{P}}\mathcal{R}_1\Pi_3|\phi\rangle\| = 0$. □

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 $\Pi_{\overline{\mathrm{P}}}|\phi\rangle = \sum_{x,p,w,H,D}\alpha_{x,p,w,H,D}|x,p,w\rangle|H,D\rangle \in \mathbb{H}_t\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$. We will prove that $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \le 10\gamma\cdot\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2$. 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 $|x,p,w,H,D\rangle\in\mathbb{H}_t\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)=\star$, $D(x)=\perp$, $p\neq 0$.
- Π_2: all basis states $|x,p,w,H,D\rangle\in\mathbb{H}_t\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)=\star$, $D(x)\neq\perp$, $p\neq 0$.
- Π_3: all basis states $|x,p,w,H,D\rangle\in\mathbb{H}_t\cap\mathrm{supp}(\Pi_{\overline{\mathrm{P}}})$ such that $H(x)\neq\star$ or $p=0$.

Below, we prove that $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_1|\phi\rangle\|^2 \le \gamma\|\Pi_1|\phi\rangle\|^2$, $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_2|\phi\rangle\|^2 \le 9\gamma\|\Pi_2|\phi\rangle\|^2$ and $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_3|\phi\rangle\| = 0$. Hence, by the triangle and Cauchy–Schwarz inequalities, we conclude that $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2 \le 10\gamma\cdot\|\Pi_{\overline{\mathrm{P}}}|\phi\rangle\|^2$.

Analysis of Π_1. The effect of applying $\mathcal{R}_0$ 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

$$\begin{aligned}\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_1|\phi\rangle\|^2 &= \sum_{\substack{x,p,w,H,D:\\ H(x)=\star,D(x)=\perp,p\neq 0}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\left[(H,D_{x\leftarrow y})\in\mathrm{P}^{-1}(\textsc{True})\right]\\ &\le \gamma\|\Pi_1|\phi\rangle\|^2.\end{aligned}$$

where the second line is by Equation (4.3).

Analysis of Π_2. The effect of applying $\mathcal{R}_0$ on a basis state in the support of Π_2 is described in the third item of Lemma 4.6. By using the bound $|1-\omega^{pD(x)}-\omega^{py}|\leq 3$ 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

$$\begin{aligned}\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_2|\phi\rangle\|^2 &\leq 9 \sum_{\substack{x,p,w,H,D:\\ H(x)=\star, D(x)\neq\perp, p\neq 0}} |\alpha_{x,p,w,H,D}|^2 \cdot \Pr_{y\leftarrow[N]}\left[(H, D_{x\leftarrow y})\in \mathrm{P}^{-1}(\textsc{True})\right]\\ &\leq 9\gamma\|\Pi_2|\phi\rangle\|^2.\end{aligned}$$

where the second line is by Equation (4.3).

Analysis of Π_3. By the first item in Lemma 4.6, the operator $\mathcal{R}_0$ maps any basis state in the support of Π_3 to itself, up to a phase factor. Thus, we have $\|\Pi_{\mathrm{P}}\mathcal{R}_0\Pi_3|\phi\rangle\| = 0$. □

B Missing Proofs for Section 6 (Collision Finding)

In this section, we prove the following lemma:

Lemma 6.9 (Restated). *Given an integer t and a state $|\phi\rangle\in\mathbb{H}_t$, we have*

$$\Gamma_0(\Pi_{\overline{\mathrm{H+C}}},|\phi\rangle)\leq\frac{10t}{N}, \quad (6.8) \qquad \|\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2\leq\frac{t}{N}\cdot\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2, \quad (6.9)$$

$$\Gamma_1(\Pi_{\overline{\mathrm{H+C}}},|\phi\rangle)\leq\frac{2t}{N}, \quad (6.10) \qquad \|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2\leq\frac{2t}{N}\cdot\|\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2. \quad (6.11)$$

We will use the following simple fact about the predicate XH.

Fact B.1. *For any basis state $|x,p,w,H,B,D\rangle$ satisfying the predicate* XH*, 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 X and 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 X). □

Since the proofs of Equations (6.8) to (6.11) share strong similarities with those of Lemmas 4.6 and 4.7, we skip some details in the calculation below.

Proof of Equation (6.8). We first claim that it is sufficient to show that

$$\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}|\phi\rangle\|^2\leq\frac{10t}{N}\cdot\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2. \quad (B.1)$$

Indeed, $\Pi_{\overline{\mathrm{H+C}}}\mathcal{R}_0\Pi_{\mathrm{H+C}}|\phi\rangle = \Pi_{\overline{\mathrm{H+C}}}\mathcal{R}_0\Pi_{\mathrm{XH}}\Pi_{\mathrm{H+C}}|\phi\rangle$ by Fact 6.7. Thus, using Equation (B.1), we conclude that $\|\Pi_{\overline{\mathrm{H+C}}}\mathcal{R}_0\Pi_{\mathrm{H+C}}|\phi\rangle\|^2\leq\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}\Pi_{\mathrm{H+C}}|\phi\rangle\|^2\leq\frac{10t}{N}\cdot\|\Pi_{\mathrm{H+C}}|\phi\rangle\|^2$.

We now prove Equation (B.1). Let $\Pi_{\mathrm{XH}}|\phi\rangle=\sum_{x,p,w,H,B,D}\alpha_{x,p,w,H,B,D}|x,p,w,H,B,D\rangle\in\mathbb{H}_t\cap\mathrm{supp}(\Pi_{\mathrm{XH}})$. 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 B.1, it implies that the post-query state is given by the third item of Lemma 4.6,

$$\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}|\phi\rangle = \Pi_{\overline{\mathrm{H}}}\sum_{x,p,w,H,B,D}\alpha_{x,p,w,H,B,D}|x,p,w,H,B_{\leftarrow 0}\rangle\Bigg(\frac{\omega^{pD(x)}}{\sqrt{N}}|D_{x\leftarrow\perp}\rangle + \sum_{y\in[N]}\frac{1-\omega^{pD(x)}-\omega^{py}}{N}|D_{x\leftarrow y}\rangle\Bigg).$$

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

$$\begin{aligned}
&\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \\
&= \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star,D(x)=\perp}}\left\|\Pi_{\overline{\mathrm{H}}}\sum_{z\in[N]}\alpha_{x,p,w,H,B,D_{x\leftarrow z}}\frac{\omega^{pz}}{\sqrt{N}}|x,p,w\rangle|H,B_{\leftarrow 0},D\rangle\right\|^2 \\
&\quad+\sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N],H(x)=\star,D(x)=y}}\left\|\Pi_{\overline{\mathrm{H}}}\sum_{z\in[N]}\alpha_{x,p,w,H,B,D_{x\leftarrow z}}\frac{1-\omega^{pz}-\omega^{py}}{N}|x,p,w\rangle|H,B_{\leftarrow 0},D\rangle\right\|^2 \\
&= \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star,D(x)=\perp,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}}\left|\sum_{z\in[N]}\alpha_{x,p,w,H,B,D_{x\leftarrow z}}\frac{\omega^{pz}}{\sqrt{N}}\right|^2 \\
&\quad+\sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}}\left|\sum_{z\in[N]}\alpha_{x,p,w,H,B,D_{x\leftarrow z}}\frac{1-\omega^{pz}-\omega^{py}}{N}\right|^2.
\end{aligned}$$

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

$$\begin{aligned}
&\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \\
&\leq \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star,D(x)=\perp,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}}\left(\sum_{z\in[N]}|\alpha_{x,p,w,H,B,D_{x\leftarrow z}}|^2\right)\Pr_{z\leftarrow[N]}[\mathrm{H}(x,p,w,H,B,D_{x\leftarrow z})=\textsc{True}] \\
&+\sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N],H(x)=\star,D(x)=y,\\ \mathrm{H}(x,p,w,H,B,D_{x\leftarrow\perp})=\textsc{False}}}\frac{9}{N}\left(\sum_{z\in[N]}|\alpha_{x,p,w,H,B,D_{x\leftarrow z}}|^2\right)\Pr_{z\leftarrow[N]}[\mathrm{H}(x,p,w,H,B,D_{x\leftarrow z})=\textsc{True}] \\
&= \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star,D(x)=\perp,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}}10\left(\sum_{z\in[N]}|\alpha_{x,p,w,H,B,D_{x\leftarrow z}}|^2\right)\Pr_{z\leftarrow[N]}[\mathrm{H}(x,p,w,H,B,D_{x\leftarrow z})=\textsc{True}]
\end{aligned}$$

where we used that the non-zero amplitudes $\alpha_{x,p,w,H,B,D_{x\leftarrow z}}$ must satisfy $\mathrm{H}(x,p,w,H,B,D_{x\leftarrow z}) = \textsc{True}$ (since $\Pi_{\mathrm{XH}}|\phi\rangle \in \mathrm{supp}(\Pi_{\mathrm{H}})$), 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 $\Pi_{\mathrm{XH}}|\phi\rangle$ is supported over basis states whose history register contains at most t non-$\star$ entries, the probability to create a hybrid collision by adding one value to the database is at most $\Pr_{z\leftarrow[N]}[\mathrm{H}(x,p,w,H,B,D_{x\leftarrow z})=\textsc{True}] \leq t/N$. We conclude that, $\|\Pi_{\overline{\mathrm{H}}}\mathcal{R}_0\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \frac{10t}{N}\sum_{x,p,w,H,B,D}|\alpha_{x,p,w,H,B,D}|^2 = \frac{10t}{N}\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2$. □

Proof of Equation (6.10). Similarly to the above proof, by Fact 6.7, it is sufficient to show that

$$\|\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \frac{10t}{N}\cdot\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \tag{B.2}$$

where we keep the predicate $\overline{\mathrm{C}}$ 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 $\Pi_{\mathrm{XH}}|\phi\rangle = \sum_{x,p,w,H,B,D} \alpha_{x,p,w,H,B,D}|x,p,w,H,B,D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\mathrm{XH}})$. By Fact B.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

$$\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle = \Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}} \sum_{x,p,w,H,B,D} \alpha_{x,p,w,H,B,D}|x,p,w\rangle \Bigg(\frac{1}{\sqrt{N}}|H_{x\leftarrow\perp}, B_{\leftarrow 1}, D_{x\leftarrow\perp}\rangle - \sum_{y\in[N]} \frac{\omega^{py}}{N}|H_{x\leftarrow y}, B_{\leftarrow 1}, D_{x\leftarrow y}\rangle \Bigg).$$

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

$$\|\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star, D(x)=\perp,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}} \left| \sum_{z\in[N]} \alpha_{x,p,w,H,B,D_{x\leftarrow z}} \frac{1}{\sqrt{N}} \right|^2 + \sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N], H(x)=\star, D(x)=y,\\ \mathrm{H}(x,p,w,H,B,D)=\textsc{False}}} \left| \sum_{z\in[N]} \alpha_{x,p,w,H,B,D_{x\leftarrow z}} \frac{\omega^{py}}{N} \right|^2.$$

Hence, we can conclude in the same way as in the proof of Equation (6.8) by using Cauchy–Schwarz inequality, which gives that $\|\Pi_{\overline{\mathrm{H}}\cdot\overline{\mathrm{C}}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \frac{2t}{N}\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2$. □

Proof of Equation (6.9). Let us denote $\Pi_{\mathrm{XH}}|\phi\rangle = \sum_{x,p,w,H,B,D} \alpha_{x,p,w,H,B,D}|x,p,w,H,B,D\rangle \in \mathbb{H}_t \cap \mathrm{supp}(\Pi_{\mathrm{XH}})$. By Fact B.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

$$\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle = -\Pi_{\mathrm{H}} \sum_{x,p,w,H,B,D} \alpha_{x,p,w,H,B,D}|x,p,w\rangle \sum_{y\in[N]} \frac{\omega^{py}}{N}|H_{x\leftarrow y}, B_{\leftarrow 1}, D_{x\leftarrow y}\rangle.$$

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

$$\|\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 = \sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N], H(x)=\star, D(x)=y}} \left\| \Pi_{\mathrm{H}} \sum_{z\in[N]} \alpha_{x,p,w,H,B,D_{x\leftarrow z}} \frac{\omega^{py}}{N}|x,p,w\rangle|H_{x\leftarrow y}, B_{\leftarrow 1}, D\rangle \right\|^2 = \sum_{\substack{x,p,w,H,B,D,y:\\ y\in[N], H(x)=\star, D(x)=y,\\ \mathrm{H}(x,p,w,H_{x\leftarrow y},B,D)=\textsc{True}}} \left| \sum_{z\in[N]} \frac{\alpha_{x,p,w,H,B,D_{x\leftarrow z}}}{N} \right|^2.$$

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

$$\|\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \sum_{\substack{x,p,w,H,B,D:\\ H(x)=\star, D(x)\neq\perp}} |\alpha_{x,p,w,H,B,D}|^2 \cdot \Pr_{y\leftarrow[N]}[\mathrm{H}(x,p,w,H_{x\leftarrow y},B,D_{x\leftarrow y}) = \textsc{True}].$$

For each (H,D) in the above state, D contains at most t entries different from $\perp$ (by definition of $\mathbb{H}_t$). 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 $\Pr_{y\leftarrow[N]}[\mathrm{H}(x,p,w,H_{x\leftarrow y},B,D_{x\leftarrow y}) = \textsc{True}] \leq t/N$. We conclude that $\|\Pi_{\mathrm{H}}\mathcal{R}_1\Pi_{\mathrm{XH}}|\phi\rangle\|^2 \leq \frac{t}{N}\|\Pi_{\mathrm{XH}}|\phi\rangle\|^2$. □

Proof of Equation (6.11). The proof is almost identical to that of Lemma 4.13. The reason for which we cannot apply this lemma directly to the predicate $\mathrm{H}+\mathrm{C}$ is because it does not satisfy the condition stated in Equation (4.5). 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* $|x, p, w, H, B, D\rangle$ *is not in the support of* Π_{P} *then* $|x, p, w, H_{x\leftarrow D(x)}, B, D\rangle$ *will not be either.* This statement is wrong for the predicate $\mathrm{P} = \mathrm{H} + \mathrm{C}$ (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* $|x, p, w, H, B, D\rangle$ *is not in the support of* $\Pi_{\mathrm{H+C}}$ *then* $|x, p, w, H_{x\leftarrow D(x)}, B, D\rangle$ *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 $\|\Pi_{\mathrm{C}}\mathcal{R}_1\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2 \leq \frac{2t}{N} \cdot \|\Pi_{\overline{\mathrm{H+C}}}|\phi\rangle\|^2$. □