Oracle Recording for Non-Uniform Random Oracles, and its Applications

Minki Hhan[1] and Aaram Yun[2]

[1] Quantum Universe Center, Korea Institute for Advanced Study, Seoul, Korea
minkihhan@kias.re.kr
[2] Department of Cyber Security, Ewha Womans University, Seoul, Korea
aaramyun@ewha.ac.kr

Abstract. In Crypto 2019, Zhandry showed how to define compressed oracles, which record quantum superposition queries to the quantum random oracle. In this paper, we extend Zhandry's compressed oracle technique to non-uniformly distributed functions with independently sampled outputs. We define two quantum oracles CStO_D and CPhsO_D, which are indistinguishable to the non-uniform quantum random oracle where quantum access is given to a random function H whose images $H(x)$ are sampled from a probability distribution D independently for each x. We show that these compressed oracles record the adversarial quantum superposition queries. Also, we re-prove the optimality of Grover search and the collision resistance of non-uniform random functions, using our extended compressed oracle technique.

Keywords: compressed oracle, non-uniform random functions, oracle recording, quantum collsion finding, quantum random oracle, quantum search, quantum superposition query.

1 Introduction

Classically, often it is easier to prove cryptographic security in the random oracle model [6] than in the standard model, because we may exploit various useful properties of the random oracle. An adversary may make polynomially many queries, where each query examines only one point. The reduction algorithm can record these queries, and also program the random oracle to embed instances of hard problems which the reduction algorithm has to solve.

We may regard the random oracle as an idealized model of a hash function. On the other hand, in the post-quantum era, a quantum adversary may evaluate a hash function in quantum superposition. Due to this, we may say that the conventional classical random oracle model is providing insufficient capabilities to the quantum adversary. Therefore, the quantum random oracle model (QROM) was introduced in [8], where the adversary can make quantum superposition queries to the random oracle. While this gives us a better model for a hash function, at the same time, it makes proving security in the QROM harder; each query may potentially inspect exponentially many points, which makes recording and programming the quantum random oracle, not to mention doing just lazy sampling, seemingly impossible.

But, in Crypto 2019, Zhandry showed that one can in fact record the adversarial quantum random oracle queries [26]. He constructed *compressed oracles*, and showed that these compressed oracles can handle quantum random oracle queries, allowing lazy sampling and recording of the quantum queries.

The compressed oracle technique turned out to be extremely useful for proving security in the quantum random oracle model, or proving lower bounds for quantum computational problems. While there are existing proof techniques like the adversary method or the polynomial method for proving such quantum lower bounds, the proof strategy should be carefully chosen by considering the problem to show: for example, the (worst-case) collision lower bound [1] was proven years after the search lower bound, and the average-case hardness of collision [25] was taken a decade to be demonstrated. Even worse, these proofs are fairly different. On the other hand, both problems can be proven through the machinery of the compressed oracle in a systematic way, and some other, much more complex yet fundamental problems [18,10] are resolved with the help of this framework for the first time.

In this paper, we show that in fact we may define compressed oracles for *non-uniform random oracles*. Consider an arbitrary probability distribution D on $\{0,1\}^n$. Let us define a random function $H : \{0,1\}^m \to \{0,1\}^n$ by sampling $H(x)$ from D, independently for each $x \in \{0,1\}^m$. Generalizing Zhandry's results, we define two quantum oracles, CStO_D and CPhsO_D, the compressed standard oracle for D and the compressed phase oracle for D, respectively. They are indistinguishable from the quantum random oracles (with the standard interface and the phase interface) where such non-uniform random oracle H is given to the quantum adversary, and moreover they allow recording adversarial queries. Also, in order to define and use these oracles, we first formalize relevant concepts, including, quantum oracles, morphisms between them, and recordability.

As applications of these, we (re-)prove two results. The first is the optimality of the Grover search. Of course, there are many existing proofs of this [2,7,5,26] with many different formulations. Specifically, we consider the following setup: given a random boolean function $f : \{0,1\}^m \to \{0,1\}$ where each $f(x)$ is sampled so that $p = \mathbf{Pr}[f(x) = 1] \leq 1/2$, we show that the probability that a quantum adversary outputs a preimage of 1, after making at most q quantum queries, is bounded by $O(pq^2)$. This was previously proved by Hülsing et al. [17][3], using the "polynomial-like" method developed by Zhandry [24]. In comparison, we use the compressed oracle technique for non-uniform random oracles to prove this result.

The second application we have is the collision resistance of non-uniform hash functions. Suppose a non-uniform random function H is given where each point $H(x)$ is sampled from a probability distribution D over $\{0,1\}^n$ independently. What would be the success probability of a quantum adversary, which makes

[3] The proof is in the full version of their paper [16].

at most q quantum queries to H, to output a collision pair of H? In case the distribution D is uniform, Zhandry [25] showed that the probability is bounded by $O(q^3/2^n)$, which is tight in the sense that there is a matching algorithm with $q = \Theta(2^{n/3})$. Later, the uniform case is re-proved by Zhandry by using the compressed oracle technique [26].

The question is what would happen to a non-uniform random function. Of course, if the distribution is too far from uniform, then we may expect that collisions would occur more likely, and the adversary could find a collision more easily. Therefore, the min-entropy of the distribution D matters. Targhi et al. [19] showed that the collision finding probability is bounded by $O(q^{9/5}/2^{k/5})$, where k is the min-entropy of D. This was later improved to $O(nq^{5/2}/2^{k/2})$ in [13]. Then, Balogh et al. [4] improved that further to $O(q^3/2^k)$, which matches the known tight bound when the distribution is uniform. To this end, they introduce a sequence of reductions from finding a collision in a uniform random function to that of so-called flat distributions, and then again to that of non-uniform distributions.

We re-prove the same bound $O(q^3/2^k)$, again using the compressed oracle technique for non-uniform random oracles. In fact, we prove this by directly adapting Zhandry's compressed oracle proof for the uniform case to the non-uniform random oracles, but otherwise almost unchanged.

1.1 Related work

For an arbitrary function, i.e., in the worst-case analysis, [7,2,5] show the lower bound of quantum search using different techniques around 2000, which readily extended to the quantum random functions. For the collision-finding problem, Aaronson and Shi [1], followed by Ambainis [3], prove the tight lower bound a few years later. On the other hand, the collision finding lower bound for random functions is proven in the middle of 2010s in [23,25].

For the non-uniform distributions, Balogh et al. [4] show the tight lower bound for collision finding with respect to the min-entropy, following non-tight bounds proved in [20,14]. However, their strategies are to reduce the non-uniform collision from the uniform random case and are involved with multiple new concepts. We reprove this bound using a modular analysis based on the compressed oracle.

Let us summarize the properties of the original compressed oracle of Zhandry [26] for more detailed comparisons between related works.

- Compression: while the standard oracle needs exponentially many qubits to implement it, the compressed oracle essentially needs only polynomially many qubits. As more queries are made, the size of individual 'databases' in the oracle state grows, but only in proportion to the total number of queries.
- Indistinguishability: the compressed oracle is (perfectly) indistinguishable from the corresponding standard oracle. Together with compression, it allows a form of 'lazy sampling' of the standard oracle.

– Recording: the compressed oracle 'records' the standard oracle; if the adversary may correctly output some input-output pairs of the oracle, the adversary must have queried for the input, and the record can be found by measuring the oracle state. (For example, [26, Lemma 5].)

Some previous works developed compressed oracles for non-uniform functions:

– Czajkowski et al. [12] developed compressed oracles for non-uniform functions and proved so-called one-way-to-hiding lemma for compressed oracles. However, their formalization is somewhat different from others, as the initial state of the compressed oracle could be a non-zero state. They also do not rely on the recording lemma.
– Hamoudi and Magniez [15], and also Cojocaru et al. [11] developed compressed oracle tools for Bernoulli distributions and proved, among others, the lower bound for finding k marked items, which has an application to the post-quantum security of Bitcoin. They define the progress measure and track the bound of this measure by moving the standard and compressed oracles back and forth, instead of using the recordability.
– Unruh [21,22] gave some potential approaches for compressed oracles for more general functions such as permutations, though the complete construction is still elusive. One of the main difficulty is that permutations have dependent outputs, while this paper and the above-mentioned papers focus on the functions with independent outputs.

Overall, the previous studies are mostly focused on uniform random functions or Bernoulli distributions, and did not rely on recordability, resulting in the involved proofs working between standard and compressed oracles. On the other hand, we extend the compressed oracles for arbitrary distributions (with independent outputs), and formally prove the recordability, and prove the lower bounds solely focusing on the database of the compressed oracles.

2 Preliminaries

2.1 Notations and conventions

In this paper, all Hilbert spaces we use are finite dimensional.

For any finite set $\mathcal{X}$, we define $\mathcal{X}_\perp$ as $\mathcal{X} \cup \{\perp\}$, where $\perp$ is a special symbol not in $\mathcal{X}$.

For any finite sets $\mathcal{X}, \mathcal{Y}$, we define $\mathcal{Y}^{\mathcal{X}}$ as the set of all functions of form $\mathcal{X} \to \mathcal{Y}$.

Given a finite set $\mathcal{X}$, we let $\mathbb{C}[\mathcal{X}]$ to denote the Hilbert space spanned by ket vectors $|x\rangle$ of $x \in \mathcal{X}$. For any Hilbert space $\mathcal{H}$, we denote the identity operator of $\mathcal{H}$ as $I_{\mathcal{H}}$. We may omit the subscript if it is clear from the context.

For any Hilbert spaces $\mathcal{H}, \mathcal{H}'$, $L(\mathcal{H}, \mathcal{H}')$ is the set of all linear operators of form $A : \mathcal{H} \to \mathcal{H}'$. We also write $L(\mathcal{H}, \mathcal{H}')$ simply as $L(\mathcal{H})$.

A linear operator $A : \mathcal{H} \to \mathcal{H}'$ is an *isometry* if it preserves the norm: $\| A |\psi\rangle \| = \| |\psi\rangle \|$ for any $|\psi\rangle \in \mathcal{H}$. Equivalently, $A^\dagger A = I_{\mathcal{H}}$. When an isometry A maps a Hilbert space $\mathcal{H}$ to itself, we say that A is *unitary*.

We will use the notion of *quantum channels*. A quantum channel $\Phi : L(\mathcal{H}) \to L(\mathcal{H}')$ is a superoperator which is completely positive and trace preserving. When $U : \mathcal{H} \to \mathcal{H}'$ is an isometry, it induces a *unitary quantum channel* $\Phi : L(\mathcal{H}) \to L(\mathcal{H}')$ by $\Phi(A) = UAU^\dagger$. When the context is clear, we will denote this unitary channel by the symbol of the underlying isometry U as well: $U(A) = UAU^\dagger$.

When D is a probability distribution over a finite set $\mathcal{Y}$, for any $y \in \mathcal{Y}$, $D(y)$ denotes the probability of y according to the distribution D.

Also, when $\mathcal{X}$ is another finite set, $D^{\mathcal{X}}$ denotes the probability distribution of functions $f : \mathcal{X} \to \mathcal{Y}$ where for each $x \in \mathcal{X}$, $f(x)$ is sampled independently according to the distribution D. Therefore, for any $f : \mathcal{X} \to \mathcal{Y}$, we have

$$D^{\mathcal{X}}(f) = \prod_{x \in \mathcal{X}} D(f(x)).$$

For any probability distribution D, $H_\infty(D)$ denotes the *min-entropy* of D, which is defined as

$$H_\infty(D) := -\log_2 \max_x D(x).$$

2.2 Partial functions

A *partial function* is a function where some function values might be undefined. When a function value $f(x)$ is undefined, we denote that as $f(x) = \perp$. When f is a partial function from $\mathcal{X}$ to $\mathcal{Y}$, we denote that as $f : \mathcal{X} \rightharpoonup \mathcal{Y}$. In this case, we define the *domain* of f, denoted by $\mathrm{dom}(f)$, as

$$\mathrm{dom}(f) := \{x \in \mathcal{X} \mid f(x) \neq \perp\}.$$

We also define the *range* of f as

$$\mathrm{rng}(f) := \{y \in \mathcal{Y} \mid y = f(x) \text{ for some } x \in \mathrm{dom}(f)\}.$$

When $\mathcal{X} = \mathrm{dom}(f)$, the partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ is called *total*, and such a total function f can be written as $f : \mathcal{X} \to \mathcal{Y}$, as usual.

There are two equivalent ways to regard a partial function. First, we can identify a partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ with a total function $f : \mathcal{X} \to \mathcal{Y}_\perp$, with $\mathcal{Y}_\perp = \mathcal{Y} \cup \{\perp\}$, where $\perp$ is a special symbol not in $\mathcal{Y}$. In other words, we reify the undefinedness as yet another value $\perp$, and when $f(x)$ is undefined, we let $f(x) = \perp \in \mathcal{Y}_\perp$.

Another way to regard a partial function f is to identify it with its (set-theoretic) graph, which is

$$\{(x, f(x)) \mid f(x) \neq \perp\}.$$

Hence, we can apply set-theoretic notions to partial functions. For example, when f is a partial function, then $|f| = |\mathrm{dom}(f)|$. We call this quantity $|f|$ as the *rank* of f.

Also, when f and g are partial functions, then $f \subseteq g$ means that $f(x) = g(x)$ whenever $f(x) \neq \perp$ (hence, especially $g(x) \neq \perp$ in this case). When $f \subseteq g$, then we say that f is a *restriction* of g, and g is an *extension* of f.

Due to this identification of a partial function with its graph, the empty set $\emptyset$ also naturally denotes the *empty partial function*, where $\emptyset(x) = \perp$ for any x. Sometimes we will also write this empty partial function as $\perp$.

Also, we have $\mathrm{dom}(f) = \{x \mid \exists y, (x, y) \in f\}$, and $\mathrm{rng}(f) = \{y \mid \exists x, (x, y) \in f\}$.

When $f : \mathcal{X} \rightharpoonup \mathcal{Y}$, $z \in \mathcal{X}$, $y \in \mathcal{Y}$, then $f[z \to y]$ is a partial function from $\mathcal{X}$ to $\mathcal{Y}$ defined as

$$f[z \to y](x) := \begin{cases} y & \text{if } x = z, \\ f(x) & \text{if } x \neq z. \end{cases}$$

Implementation of partial functions The identification of a partial function $f : X \rightharpoonup Y$ with its graph also gives a trivial way to implement a partial function efficiently, especially when its rank is small. All we need is to write down the graph in a unique way, as a *database* of f.

For this, let us assume that the set X has a standard total order. Let $x_1, \ldots, x_r$ be all of the elements in $\mathrm{dom}(f)$, enumerated in the ascending order: $x_1 < x_2 < \cdots < x_r$. Then, the graph of f can be uniquely written as the following tuple:

$$((x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_r, f(x_r))).$$

In this way, a partial function f can be uniquely encoded, and moreover, the number of bits/qubits to represent f is proportional to its rank.

3 Quantum oracles

3.1 Definition of quantum oracles

We would like to discuss quantum oracles and that one oracle is recording other oracle. For this, we formally define a notion of quantum oracles. We want our definition to encompass all of Zhandry's purified oracles and compressed oracles, as well as the quantum random oracles. So we will give a stateful definition; the oracle maintains an internal quantum state, and the state update occurs whenever a quantum query is made. This captures what happens to Zhandry's compressed oracles.

First, let us start with defining the pure variant of a quantum oracle.

Definition 3.1. *A* pure quantum oracle *is a tuple* $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, |\mathsf{init}\rangle)$, *where* $\mathcal{I}$ *is a Hilbert space called the* interface space*,* $\mathcal{S}$ *is another Hilbert space called the* oracle state space*, and*

$$\mathsf{query} : \mathcal{I} \otimes \mathcal{S} \to \mathcal{I} \otimes \mathcal{S}$$

is a unitary operator. Finally, $|\mathsf{init}\rangle \in \mathcal{S}$ *is an element called the* initial state *of the oracle.*

The idea is that, the oracle interacts with an adversary A whose state space can be written as $\mathcal{P} \otimes \mathcal{I}$, where $\mathcal{P}$ is the private state space of A. The joint state space of the adversary and the oracle is $\mathcal{P} \otimes \mathcal{I} \otimes \mathcal{S}$, and the state is initialized as $|\mathsf{init}^P\rangle \otimes |\mathsf{init}^I\rangle \otimes |\mathsf{init}\rangle$, for some $|\mathsf{init}^P\rangle \in \mathcal{P}$ and $|\mathsf{init}^I\rangle \in \mathcal{I}$ as specified by the adversary. The adversarial computation can be written as a sequence of unitary operators $U_i : \mathcal{P} \otimes \mathcal{I} \to \mathcal{P} \otimes \mathcal{I}$ for $i = 0, \ldots, t$, and the operations $U_i \otimes I_{\mathcal{S}}$ and $I_{\mathcal{P}} \otimes \mathsf{query}$ are performed alternatingly for $i = 0, \ldots, t$.

Definition 3.2. *Let* $\mathcal{O}_1 = (\mathcal{I}_1, \mathcal{S}_1, \mathsf{query}_1, |\mathsf{init}_1\rangle)$ *and* $\mathcal{O}_2 = (\mathcal{I}_2, \mathcal{S}_2, \mathsf{query}_2, |\mathsf{init}_2\rangle)$ *be pure quantum oracles. Then, a* pure morphism $\mu : \mathcal{O}_1 \to \mathcal{O}_2$ *from* $\mathcal{O}_1$ *to* $\mathcal{O}_2$ *is a tuple* $\mu = (\mu^I, \mu^S)$ *satisfying the following.*

1. $\mu^I : \mathcal{I}_1 \to \mathcal{I}_2$ *and* $\mu^S : \mathcal{S}_1 \to \mathcal{S}_2$ *are isometries.*
2. $\mu^S |\mathsf{init}_1\rangle = |\mathsf{init}_2\rangle$.
3. *The following is a commutative diagram.*

$$\begin{tikzcd} \mathcal{I}_1 \otimes \mathcal{S}_1 \arrow[r, "\mathsf{query}_1"] \arrow[d, "\mu^I \otimes \mu^S"] & \mathcal{I}_1 \otimes \mathcal{S}_1 \arrow[d, "\mu^I \otimes \mu^S"] \\ \mathcal{I}_2 \otimes \mathcal{S}_2 \arrow[r, "\mathsf{query}_2"] & \mathcal{I}_2 \otimes \mathcal{S}_2 \end{tikzcd}$$

In other words, we have $(\mu^I \otimes \mu^S) \circ \mathsf{query}_1 = \mathsf{query}_2 \circ (\mu^I \otimes \mu^S)$.
When $\mu = (\mu^I, \mu^S)$ *is a morphism, sometimes we say* μ^I *is the* converter *of* μ*, since it provides conversion between interfaces.*

While we will mostly work with pure quantum oracles and pure morphisms between them, we do need to extend the definition such that the internal state of the oracle can be mixed. For this, we define the general notion of the quantum oracle as follows.

Definition 3.3. *A* quantum oracle *is a tuple* $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, \mathsf{init})$*, where* $\mathcal{I}$ *is a Hilbert space called the* interface space*,* $\mathcal{S}$ *is another Hilbert space called the* oracle state space*, and*

$$\mathsf{query} : \mathcal{I} \otimes \mathcal{S} \to \mathcal{I} \otimes \mathcal{S}$$

is a unitary operator. Finally, $\mathsf{init} \in L(\mathcal{S})$ *is a density operator called the* initial state *of the oracle.*

Remark 3.4. A pure quantum oracle $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, |\mathsf{init}\rangle)$ can be considered as a quantum oracle, by regarding $|\mathsf{init}\rangle\langle\mathsf{init}|$ as the initial state.

Now, let us define general morphisms between quantum oracles.

Definition 3.5. *Let* $\mathcal{O}_1 = (\mathcal{I}_1, \mathcal{S}_1, \mathsf{query}_1, \mathsf{init}_1)$ *and* $\mathcal{O}_2 = (\mathcal{I}_2, \mathcal{S}_2, \mathsf{query}_2, \mathsf{init}_2)$ *be quantum oracles. Then, a* morphism $\mu : \mathcal{O}_1 \to \mathcal{O}_2$ *from* $\mathcal{O}_1$ *to* $\mathcal{O}_2$ *is a tuple* $\mu = (\mu^I, \mu^S)$ *satisfying the following.*

1. $\mu^I : \mathcal{I}_1 \to \mathcal{I}_2$ *is an isometry, and* $\mu^S : L(\mathcal{S}_1) \to L(\mathcal{S}_2)$ *is a quantum channel.*
2. $\mu^S(\mathsf{init}_1) = \mathsf{init}_2$.

3. The following is a commutative diagram.

$$\begin{tikzcd} L(\mathcal{I}_1 \otimes \mathcal{S}_1) \arrow[r, "\mathsf{query}_1"] \arrow[d, "\mu^I \otimes \mu^S"] & L(\mathcal{I}_1 \otimes \mathcal{S}_1) \arrow[d, "\mu^I \otimes \mu^S"] \\ L(\mathcal{I}_2 \otimes \mathcal{S}_2) \arrow[r, "\mathsf{query}_2"] & L(\mathcal{I}_2 \otimes \mathcal{S}_2) \end{tikzcd}$$

Here, μ^I is the unitary quantum channel given by the isometry $\mu^I : \mathcal{I}_1 \to \mathcal{I}_2$; for any $A \in L(\mathcal{I}_1)$, we have $\mu^I(A) = \mu^I A (\mu^I)^\dagger$. Similarly, query_i is the unitary quantum channel given by the unitary operator query_i, for $i = 1, 2$. Finally, $\mu^I \otimes \mu^S$ is the product channel of two quantum channels μ^I and μ^S.

Remark 3.6. A pure morphism $\mu : \mathcal{O}_1 \to \mathcal{O}_2$ between two pure quantum oracles $\mathcal{O}_1 = (\mathcal{I}_1, \mathcal{S}_1, \mathsf{query}_1, |\mathsf{init}_1\rangle)$ and $\mathcal{O}_2 = (\mathcal{I}_2, \mathcal{S}_2, \mathsf{query}_2, |\mathsf{init}_2\rangle)$ can be considered as a morphism: the underlying isometry $\mu^S : \mathcal{S}_1 \to \mathcal{S}_2$ defines a unitary quantum channel $\mu^S : L(\mathcal{S}_1) \to L(\mathcal{S}_2)$. Since $\mu^S |\mathsf{init}_1\rangle = |\mathsf{init}_2\rangle$, we have $\mu^S(|\mathsf{init}_1\rangle\langle\mathsf{init}_1|) = \mu^S |\mathsf{init}_1\rangle\langle\mathsf{init}_1| (\mu^S)^\dagger = |\mathsf{init}_2\rangle\langle\mathsf{init}_2|$.

Also, it is straightforward to verify that the equation $\mathsf{query}_2 \circ (\mu^I \otimes \mu^S) = (\mu^I \otimes \mu^S) \circ \mathsf{query}_1$ as an equation of isometries immediately implies the same equation $\mathsf{query}_2 \circ (\mu^I \otimes \mu^S) = (\mu^I \otimes \mu^S) \circ \mathsf{query}_1$ as an equation of quantum channels.

Composition of two morphisms $\mu_1 = (\mu_1^I, \mu_1^S) : \mathcal{O}_1 \to \mathcal{O}_2$ and $\mu_2 = (\mu_2^I, \mu_2^S) : \mathcal{O}_2 \to \mathcal{O}_3$ are defined obviously: $\mu_2 \circ \mu_1 = (\mu_2^I \circ \mu_1^I, \mu_2^S \circ \mu_1^S)$. Also, for any quantum oracle $\mathcal{O}$, we have an obvious identity morphism $I_{\mathcal{O}} : \mathcal{O} \to \mathcal{O}$.

Definition 3.7. *A morphism $\mu = (\mu^I, \mu^S) : \mathcal{O}_1 \to \mathcal{O}_2$ is called an* isomorphism*, if there exists an inverse morphism $\nu : \mathcal{O}_2 \to \mathcal{O}_1$ such that $\nu \circ \mu = I_{\mathcal{O}_1}$ and $\mu \circ \nu = I_{\mathcal{O}_2}$.*

Theorem 3.8. *If there exists a morphism $\mu : \mathcal{O}_1 \to \mathcal{O}_2$, then, for any adversary A outputting an element of a finite set $\mathcal{X}$, there exists another adversary B such that the following holds.*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = x] = \mathbf{Pr}[B^{\mathcal{O}_2}() = x], \qquad \text{for any } x \in \mathcal{X}.$$

Moreover, if A makes at most q queries for some q, then B also makes at most q queries. Also, if A is an efficient quantum adversary and if the unitary map μ^I can be implemented efficiently, then B is also efficient.

Proof. Suppose that $\mathcal{O}_1 = (\mathcal{I}_1, \mathcal{S}_1, \mathsf{query}_1, \mathsf{init}_1)$, $\mathcal{O}_2 = (\mathcal{I}_2, \mathcal{S}_2, \mathsf{query}_2, \mathsf{init}_2)$, and a morphism $\mu = (\mu^I, \mu^S)$ between them are given.

Let A be an adversary interacting with $\mathcal{O}_1$ whose computation can be described by a sequence of unitary operators $U_i : \mathcal{P} \otimes \mathcal{I}_1 \to \mathcal{P} \otimes \mathcal{I}_1$ for $i = 0, \ldots, t$, with the initial state $\mathsf{init}_1^P \otimes \mathsf{init}_1^I \in L(\mathcal{P} \otimes \mathcal{I}_1)$. Also assume that the final output of A is obtained by a measurement with respect to a complete set of measurement operators $\{M_x\}_{x \in \mathcal{X}}$ on $\mathcal{P} \otimes \mathcal{I}_1$.

Then, let U'_i be the unitary operator defined by $(I \otimes \mu^I) \circ U_i \circ (I \otimes (\mu^I)^\dagger)$. Also, we define measurement operators M'_x on $\mathcal{P} \otimes \mathcal{I}_2$ by $M'_x := (I \otimes \mu^I) \circ M_x \circ (I \otimes (\mu^I)^\dagger)$ for $x \in \mathcal{X}$.

Now, let B be the adversary with the sequence $U'_0, \ldots, U'_t$, and the initial state $\mathsf{init}_2^P \otimes \mathsf{init}_2^I$, where $\mathsf{init}_2^P = \mathsf{init}_1^P$, $\mathsf{init}_2^I = \mu^I(\mathsf{init}_1^I) = \mu^I \mathsf{init}_1^I (\mu^I)^\dagger$, with the final output obtained by the measurement with respect to $\{M'_x\}_{x \in \mathcal{X}}$.

Let $\Phi_1 \in L(\mathcal{P} \otimes \mathcal{I}_1 \otimes \mathcal{S}_1)$ be the density operator representing the final state of the joint system of A and $\mathcal{O}_1$, and let $\Phi_2 \in L(\mathcal{P} \otimes \mathcal{I}_2 \otimes \mathcal{S}_2)$ be the density operator representing the final state of the joint system of B and $\mathcal{O}_2$.

Now, we can see that the following is a commutative diagram.

$$\begin{tikzcd}
L(\mathcal{P} \otimes \mathcal{I}_1 \otimes \mathcal{S}_1) \arrow[r, "U_i \otimes I"] \arrow[d, "I \otimes \mu^I \otimes \mu^S"] & L(\mathcal{P} \otimes \mathcal{I}_1 \otimes \mathcal{S}_1) \arrow[d, "I \otimes \mu^I \otimes \mu^S"] \\
L(\mathcal{P} \otimes \mathcal{I}_2 \otimes \mathcal{S}_2) \arrow[r, "U'_i \otimes I"] & L(\mathcal{P} \otimes \mathcal{I}_2 \otimes \mathcal{S}_2).
\end{tikzcd}$$

This is because we have

$$\begin{aligned}
U'_i \circ (I \otimes \mu^I) &= (I \otimes \mu^I) U_i (I \otimes (\mu^I)^\dagger)(I \otimes \mu^I) \\
&= (I \otimes \mu^I) U_i (I \otimes \ (\mu^I)^\dagger \mu^I \ ) \\
&= (I \otimes \mu^I) \circ U_i,
\end{aligned}$$

as isometries, due to the definition of U'_i, and the fact that $(\mu^I)^\dagger \mu^I = I_{\mathcal{I}_1}$, since μ^I is an isometry. This implies $U'_i \circ (I \otimes \mu^I) = (I \otimes \mu^I) \circ U_i$ as unitary channels.

Then, we have the following commutative diagram.

$$\begin{tikzcd}
* \arrow[r, "U_0 \otimes I"] \arrow[d, "I \otimes \mu^I \otimes \mu^S"] & * \arrow[r, "I \otimes \mathsf{query}_1"] \arrow[d, "I \otimes \mu^I \otimes \mu^S"] & * \arrow[r, "U_1 \otimes I"] \arrow[d, "I \otimes \mu^I \otimes \mu^S"] & * \arrow[r, "I \otimes \mathsf{query}_1"] \arrow[d, "I \otimes \mu^I \otimes \mu^S"] & \cdots \arrow[r, "U_t \otimes I"] & * \arrow[d, "I \otimes \mu^I \otimes \mu^S"] \\
* \arrow[r, "U'_0 \otimes I"] & * \arrow[r, "I \otimes \mathsf{query}_2"] & * \arrow[r, "U'_1 \otimes I"] & * \arrow[r, "I \otimes \mathsf{query}_2"] & \cdots \arrow[r, "U'_t \otimes I"] & *
\end{tikzcd}$$

So, when we chase this diagram, starting from top left, with the element $\mathsf{init}_1^P \otimes \mathsf{init}_1^I \otimes \mathsf{init}_1^O$, the diagram relates the joint states of A and $\mathcal{O}_1$, and B and $\mathcal{O}_2$. Especially, via the rightmost arrow, we can see that the final states are related as

$$\Phi_2 = (I \otimes \mu^I \otimes \mu^S)\Phi_1.$$

Then, for any $x \in \mathcal{X}$

$$\begin{aligned}
&(M'_x \otimes I)\Phi_2 \\
&= (I \otimes \mu^I \otimes I)(M_x \otimes I)(I \otimes (\mu^I)^\dagger \otimes I)(I \otimes \mu^I \otimes \mu^S)\Phi_1 \\
&= (I \otimes \mu^I \otimes I)(M_x \otimes I)(I \otimes I \otimes \mu^S)\Phi_1 \\
&= (I \otimes \mu^I \otimes \mu^S)(M_x \otimes I)\Phi_1
\end{aligned}$$

Since $I \otimes \mu^I \otimes \mu^S$ is a quantum channel, it is trace preserving.

Now, we can compute

$$\begin{aligned}
\mathbf{Pr}[B^{\mathcal{O}_2}() = x] &= \mathrm{tr}[(M'_x \otimes I)\Phi_2] \\
&= \mathrm{tr}[(I \otimes \mu^I \otimes \mu^S)(M_x \otimes I)\Phi_1] \\
&= \mathrm{tr}[(M_x \otimes I)\Phi_1] \\
&= \mathbf{Pr}[A^{\mathcal{O}_1}() = x].
\end{aligned}$$

In the above, if A is efficient and μ^I can be implemented efficiently, then U_i and M_x can be efficiently implemented. According to the construction of operators U'_i and M'_x, the adversary B is also efficient. $\square$

In case the converter μ^I of the morphism μ is bijective, we may reverse the order of the quantification in Theorem 3.8:

Corollary 3.9. *If there exists a morphism $\mu : \mathcal{O}_1 \to \mathcal{O}_2$, and if the converter μ^I of μ is bijective, then, for any adversary B outputting an element of a finite set $\mathcal{X}$, there exists another adversary A such that the following holds.*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = x] = \mathbf{Pr}[B^{\mathcal{O}_2}() = x], \qquad \text{for any } x \in \mathcal{X}.$$

Moreover, if B makes at most q queries for some q, then A also makes at most q queries. Also, if B is an efficient quantum adversary and if the unitary map μ^I can be implemented efficiently, then A is also efficient.

Proof. The proof proceeds very similar to that of Theorem 3.8: from the adversary B, we may construct the adversary A using the maps $I \otimes \mu^I$ and $I \otimes (\mu^I)^\dagger$. Since μ^I is a bijective isometry, we have $\mu^I(\mu^I)^\dagger = I_{\mathcal{I}_2}$. This can be used to prove the corollary. $\square$

Definition 3.10. *Suppose that $\mathcal{O}_1, \mathcal{O}_2$ are two quantum oracles with the same interface space $\mathcal{I}$. Suppose that there exists a morphism $\mu = (\mu^I, \mu^S) : \mathcal{O}_1 \to \mathcal{O}_2$, where the isometry μ^I is the identity operator $I_{\mathcal{I}}$ of $\mathcal{I}$, then we say that $\mathcal{O}_1$ is a* suboracle *of $\mathcal{O}_2$, and $\mathcal{O}_2$ is a* superoracle *of $\mathcal{O}_1$. In that case, the morphism μ is called an* embedding *of $\mathcal{O}_1$ into $\mathcal{O}_2$.*

Also, when $\mu = (I_{\mathcal{I}}, \mu^S) : \mathcal{O}_1 \to \mathcal{O}_2$ is an embedding, then obviously we do not have to specify $I_{\mathcal{I}}$, so we will abuse notation and simply denote the mapping μ^S as μ.

Corollary 3.11. *Let $\mathcal{O}_1, \mathcal{O}_2$ be two quantum oracles over $\mathcal{I}$. Suppose that $\mu : \mathcal{O}_1 \to \mathcal{O}_2$ is an embedding. Then, the two oracles $\mathcal{O}_1, \mathcal{O}_2$ are completely indistinguishable: for any adversary A and any possible output x, we have*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = x] = \mathbf{Pr}[A^{\mathcal{O}_2}() = x].$$

Proof. When we examine the proof of Theorem 3.8, we see that B is the same adversary as A, as μ^I is the identity operator. $\square$

3.2 Examples of quantum oracles

Now let us define a few quantum oracles that we will use. First, we define the non-uniform quantum random oracle with respect to a probability distribution D, with the standard interface. Our quantum random oracle should sample and give oracle access to a (non-uniform) random function $h : \mathcal{X} \to \mathcal{Y}$ according to the distribution $D^{\mathcal{X}}$. Therefore, the initial state of the quantum random oracle should be a mixed state $\sum_h D^{\mathcal{X}}(h) |h\rangle\langle h|$. Formalizing this, we have:

Definition 3.12 (Quantum random oracle with respect to D, standard interface). *Let $\mathcal{X} := \{0,1\}^m$, and $\mathcal{Y} := \{0,1\}^n$. Let D be a probability distribution over $\mathcal{Y}$. We define the* quantum random oracle *with respect to D with the standard interface,* $\mathsf{StQRO}_D = (\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}], \mathbb{C}[\mathcal{Y}^{\mathcal{X}}], \mathsf{query}, \mathsf{init})$ *as follows.*

The query operator is given by

$$\mathsf{query}\, |x\rangle |y\rangle \otimes |h\rangle := |x\rangle |y \oplus h(x)\rangle \otimes |h\rangle\,,$$

and the initial state init *is given by*

$$\mathsf{init} := \sum_{h \in \mathcal{Y}^{\mathcal{X}}} D^{\mathcal{X}}(h) |h\rangle\langle h|\,.$$

Similarly, we may offer the phase interface to the quantum random oracle (with respect to D):

Definition 3.13 (Quantum random oracle with respect to D, phase interface). *Let $\mathcal{X} := \{0,1\}^m$, and $\mathcal{Y} := \{0,1\}^n$. Let D be a probability distribution over $\mathcal{Y}$. We define the* quantum random oracle *with respect to D with the phase interface,* $\mathsf{PhsQRO}_D = (\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}], \mathbb{C}[\mathcal{Y}^{\mathcal{X}}], \mathsf{query}, \mathsf{init})$ *as follows.*

The query operator is given by

$$\mathsf{query}\, |x\rangle |y\rangle \otimes |h\rangle := (-1)^{y \cdot h(x)} |x\rangle |y\rangle \otimes |h\rangle\,,$$

and the initial state init *is given by*

$$\mathsf{init} := \sum_{h \in \mathcal{Y}^{\mathcal{X}}} D^{\mathcal{X}}(h) |h\rangle\langle h|\,.$$

Now, let us define Zhandry's purified quantum oracles, but generalized with respect to a probability distribution D.

Definition 3.14 (Standard oracle with respect to D). *Let $\mathcal{X} := \{0,1\}^m$, and $\mathcal{Y} := \{0,1\}^n$. Let D be a probability distribution over $\mathcal{Y}$. We define the* standard oracle *with respect to D,* $\mathsf{StO}_D = (\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}], \mathbb{C}[\mathcal{Y}^{\mathcal{X}}], \mathsf{query}, |\mathsf{init}\rangle)$ *as follows.* StO_D *is a pure quantum oracle, whose query operator is given by*

$$\mathsf{query}\, |x\rangle |y\rangle \otimes |h\rangle := |x\rangle |y \oplus h(x)\rangle \otimes |h\rangle\,,$$

and the initial state $|\mathsf{init}\rangle$ *is given by*

$$|\mathsf{init}\rangle := \sum_{h \in \mathcal{Y}^{\mathcal{X}}} \sqrt{D^{\mathcal{X}}(h)}\, |h\rangle = \sum_{h \in \mathcal{Y}^{\mathcal{X}}} \left(\prod_{x \in \mathcal{X}} \sqrt{D(h(x))} \right) |h\rangle\,.$$

As before, we may also consider the 'phase interface', which gives us the phase oracle with respect to D.

Definition 3.15 (Phase oracle with respect to D). *We define the* phase oracle *with respect to D,* $\mathsf{PhsO}_D = (\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}], \mathbb{C}[\mathcal{Y}^{\mathcal{X}}], \mathsf{query}, |\mathsf{init}\rangle)$ *as follows. This pure oracle is identical to the standard oracle* StO_D *in all aspects, except the query operator:*

The query operator of PhsO_D *is given by*

$$\mathsf{query}\,|x\rangle\,|y\rangle \otimes |h\rangle := (-1)^{y\cdot h(x)}\,|x\rangle\,|y\rangle \otimes |h\rangle\,.$$

Remark 3.16. Let us define $|\iota_D\rangle \in \mathbb{C}[\mathcal{Y}]$ as

$$|\iota_D\rangle := \sum_{y\in\mathcal{Y}} \sqrt{D(y)}\,|y\rangle\,.$$

Then the initial state of StO_D and PhsO_D is

$$\begin{aligned}
|\mathsf{init}\rangle &= \sum_{h\in\mathcal{Y}^{\mathcal{X}}} \left(\prod_{x\in\mathcal{X}} \sqrt{D(h(x))}\right) |h\rangle \\
&= \sum_{h\in\mathcal{Y}^{\mathcal{X}}} \left(\prod_{x\in\mathcal{X}} \sqrt{D(h(x))}\right) \bigotimes_{x\in\mathcal{X}} |h(x)\rangle \\
&= \bigotimes_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \sqrt{D(h)}\,|y\rangle = \bigotimes_{x\in\mathcal{X}} |\iota_D\rangle\,.
\end{aligned}$$

We will often drop D from $|\iota_D\rangle$, and write this vector just as $|\iota\rangle$.

We will often denote the query operator of a quantum oracle by the name of the quantum oracle itself, like, $\mathsf{PhsO}_D\,|x\rangle\,|y\rangle \otimes |h\rangle := (-1)^{y\cdot h(x)}\,|x\rangle\,|y\rangle \otimes |h\rangle$.

The following is a well-known fact, merely translated into this language.

Theorem 3.17. StO_D *and* PhsO_D *are isomorphic quantum oracles. Also,* StQRO_D *and* PhsQRO_D *are isomorphic quantum oracles.*

Proof. The isomorphism $\mu = (\mu^{\mathcal{I}}, \mu^{\mathcal{S}})$ from StO_D to PhsO_D (and from StQRO_D to PhsQRO_D) is simple: $\mu^{\mathcal{S}}$ is the identity operator, and $\mu^{\mathcal{I}}\,|x\rangle\,|y\rangle := |x\rangle\,H^{\otimes n}\,|y\rangle$, where $H^{\otimes n}$ is the Hadamard transformation. It can be easily verified that this μ is an isomorphism between StO_D and PhsO_D. □

Remark 3.18. Since the converter of the isomorphism between StO_D and PhsO_D is not the identity, (obviously) they are not indistinguishable oracles.

Now we can prove that StO_D and StQRO_D are completely indistinguishable, and so are PhsO_D and PhsQRO_D.

Theorem 3.19. *There are embeddings* $\mathsf{StO}_D \to \mathsf{StQRO}_D$*, and* $\mathsf{PhsO}_D \to \mathsf{PhsQRO}_D$*.*

Proof. We will show the proof for the embedding $\mathsf{StO}_D \to \mathsf{StQRO}_D$; the $\mathsf{PhsO}_D \to \mathsf{PhsQRO}_D$ case can be done essentially identically.

The embedding $\mu : \mathsf{StO}_D \to \mathsf{StQRO}_D$ is simply the 'measurement': for any $A \in L(\mathbb{C}[\mathcal{Y}^{\mathcal{X}}])$, we have

$$\mu(A) := \sum_{h \in \mathcal{Y}^{\mathcal{X}}} |h\rangle\langle h| \, A \, |h\rangle\langle h| = \sum_{h \in \mathcal{Y}^{\mathcal{X}}} \langle h|A|h\rangle \, |h\rangle\langle h| \, .$$

Recall that the initial state of StO_D is $\sum_{f\in\mathcal{Y}^{\mathcal{X}}} \sqrt{D^{\mathcal{X}}(f)}\,|f\rangle$, corresponding to the density operator

$$\rho = \left(\sum_{f \in \mathcal{Y}^{\mathcal{X}}} \sqrt{D^{\mathcal{X}}(f)}\,|f\rangle\right)\left(\sum_{g \in \mathcal{Y}^{\mathcal{X}}} \sqrt{D^{\mathcal{X}}(g)}\,\langle g|\right) = \sum_{f,g \in \mathcal{Y}^{\mathcal{X}}} \sqrt{D^{\mathcal{X}}(f)D^{\mathcal{X}}(g)}\,|f\rangle\langle g| \, .$$

Then,

$$\begin{aligned}
\mu(\rho) &= \sum_h \langle h|\rho|h\rangle \, |h\rangle\langle h| \\
&= \sum_{h,f,g} \sqrt{D^{\mathcal{X}}(f)D^{\mathcal{X}}(g)}\,\langle h|f\rangle \, \langle g|h\rangle \, |h\rangle\langle h| \\
&= \sum_h D^{\mathcal{X}}(h)\,|h\rangle\langle h| \, ,
\end{aligned}$$

which is the initial state of the quantum random oracle StQRO_D.

Also recall that StO_D and StQRO_D have the same query operator $\mathsf{query}\,|x\rangle\,|y\rangle \otimes |h\rangle := |x\rangle\,|y \oplus h(x)\rangle \otimes |h\rangle$. In order to show that μ is an embedding, we have to show that $(I \otimes \mu) \circ \mathsf{query} = \mathsf{query} \circ (I \otimes \mu)$, as quantum channels. When applied to $|xyf\rangle\langle x'y'f'|$, we have

$$\begin{aligned}
(I \otimes \mu) \circ \mathsf{query}(|xyf\rangle\langle x'y'f'|) &= (I \otimes \mu)(\mathsf{query}\,|xyf\rangle\langle x'y'f'|\,\mathsf{query}^\dagger) \\
&= (I \otimes \mu)(|x, y \oplus f(x), f\rangle\langle x', y' \oplus f'(x'), f'|) \\
&= |x, y \oplus f(x)\rangle\langle x', y' \oplus f'(x')| \otimes \mu(|f\rangle\langle f'|) \\
&= |x, y \oplus f(x)\rangle\langle x', y' \oplus f'(x')| \otimes \sum_h \langle h|f\rangle \, \langle f'|h\rangle \, |h\rangle\langle h| \, .
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\mathsf{query} \circ (I \otimes \mu)(|xyf\rangle\langle x'y'f'|) &= \mathsf{query}(|xy\rangle\langle x'y'| \otimes \mu(|f\rangle\langle f'|)) \\
&= \mathsf{query}\left(|xy\rangle\langle x'y'| \otimes \sum_h \langle h|f\rangle \, \langle f'|h\rangle \, |h\rangle\langle h|\right) \\
&= |x, y \oplus h(x)\rangle\langle x', y' \oplus h(x')| \otimes \sum_h \langle h|f\rangle \, \langle f'|h\rangle \, |h\rangle\langle h| \, .
\end{aligned}$$

We see that both are zero, when $f \neq f'$, and both are equal to

$$|x, y \oplus f(x)\rangle\langle x', y' \oplus f(x')| \otimes |f\rangle\langle f| \, ,$$

when $f = f'$. Therefore, we have $(I \otimes \mu) \circ \mathsf{query} = \mathsf{query} \circ (I \otimes \mu)$, and this shows that our $\mu : \mathsf{StO}_D \to \mathsf{StQRO}_D$ is indeed an embedding. ☐

Corollary 3.20. *For any probability distribution D, two quantum oracles StO_D and StQRO_D are completely indistinguishable, and so are PhsO_D and PhsQRO_D.*

Proof. This follows from Theorem 3.19 and Corollary 3.11. ☐

3.3 Typed oracles

In order to talk about recording an oracle, we need to be able to measure the internal state of a quantum oracle to get a (partial) function. This leads us to the following definition.

Definition 3.21. *Let $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, \mathsf{init})$ be a quantum oracle, and let $\mathcal{X}, \mathcal{Y}$ be finite sets. We say that a tuple $(\mathcal{O}, \mathbf{M})$ is a* typed oracle *of type $\mathcal{X} \to \mathcal{Y}$, if $\mathbf{M} = \{\mathsf{M}_f\}_{f:\mathcal{X} \rightharpoonup \mathcal{Y}}$ is a complete set of measurement operators of the state space $\mathcal{S}$ of $\mathcal{O}$, parametrized by partial functions $f : \mathcal{X} \rightharpoonup \mathcal{Y}$. Often, we will simply say that $\mathcal{O}$ is a typed oracle, if $\mathbf{M}$ is implicitly given by the context. $\mathbf{M}$ is called the* associated measurement operator set *of the typed oracle $\mathcal{O}$.*

When $\mathcal{O}$ is a typed oracle of type $\mathcal{X} \to \mathcal{Y}$, then we denote that as $\mathcal{O} : \mathcal{X} \to \mathcal{Y}$.

In other words, we may use the set $\mathbf{M}$ to measure the oracle state of the oracle $\mathcal{O} : \mathcal{X} \to \mathcal{Y}$, to obtain a partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$, with probability $\mathbf{Pr}[f] = \mathrm{tr}[\mathsf{M}_f \rho \mathsf{M}_f^\dagger]$, if $\rho \in L(\mathcal{S})$ is the density operator representing the oracle state. When the oracle space of $\mathcal{O}$ is measured and f is obtained as the result, we write that as $f \leftarrow \mathcal{O}$.

Definition 3.22. *Let $\mathcal{O} : \mathcal{X} \to \mathcal{Y}$ be a typed oracle, and let $\mathbf{M} = \{\mathsf{M}_f\}_{f:\mathcal{X} \rightharpoonup \mathcal{Y}}$ be the associated measurement operator set of $\mathcal{O}$. When $\mathsf{M}_f \neq 0$ implies f is total, we say that the typed oracle $\mathcal{O} : \mathcal{X} \to \mathcal{Y}$ is* total.

We will define the measurement operator sets for StQRO_D, PhsQRO_D, StO_D and PhsO_D so that they all become total typed oracles of type $\mathcal{X} \to \mathcal{Y}$, with $\mathcal{X} = \{0,1\}^m$, $\mathcal{Y} = \{0,1\}^n$: for any partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$, M_f is defined by

$$\mathsf{M}_f = \begin{cases} |f\rangle\langle f| & \text{if } f \text{ is total,} \\ 0 & \text{otherwise.} \end{cases}$$

We need the following simple lemma for StQRO_D and PhsQRO_D.

Lemma 3.23. *Consider the 'measurement' embedding $\mu : \mathsf{StO}_D \to \mathsf{StQRO}_D$ (or $\mu : \mathsf{PhsO}_D \to \mathsf{PhsQRO}_D$). For any internal oracle state ρ and any total function $f : \mathcal{X} \to \mathcal{Y}$, we have*

$$\mathrm{tr}[\mathsf{M}_f \mu(\rho) \mathsf{M}_f^\dagger] = \mathrm{tr}[\mathsf{M}_f \rho \mathsf{M}_f^\dagger].$$

Proof. In fact, we may show that $\mathsf{M}_f\mu(\rho)\mathsf{M}_f^\dagger = \mathsf{M}_f\rho\mathsf{M}_f^\dagger$.

$$\begin{aligned}\mathsf{M}_f\mu(\rho)\mathsf{M}_f^\dagger &= |f\rangle\langle f| \left(\sum_h |h\rangle\langle h|\,\rho\,|h\rangle\langle h|\right) |f\rangle\langle f| \\ &= |f\rangle\langle f|\,\rho\,|f\rangle\langle f| \\ &= \mathsf{M}_f\rho\mathsf{M}_f^\dagger. \end{aligned}$$ □

3.4 Compressed oracles

Now we define the notion of compressed oracles.

Definition 3.24. *Let $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, \mathsf{init}) : \mathcal{X} \to \mathcal{Y}$ be a quantum oracle, of type $\mathcal{X} \to \mathcal{Y}$. We say that $\mathcal{O}$ is* compressed*, if for any adversary A, when A interacts with $\mathcal{O}$, the number of qubits used to encode the oracle state is $O(q)$,when A made q quantum queries so far, at any moment. Moreover, we also require that when we measure the oracle state to get a partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ right after the qth query, we have $\mathbf{Pr}[f] = 0$ if $|f| > q$.*

Suppose $\mathcal{O}$ is compressed. If $\mathcal{O}$ is initialized and then measured immediately and a partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ is obtained, then we should have $|f| = 0$, since $\mathcal{O}$ was never queried so far. Then, $f = \perp$, the empty partial function. Due to this, when $\mathcal{O} = (\mathcal{I}, \mathcal{S}, \mathsf{query}, \mathsf{init})$ is a compressed quantum oracle, we will often write the initial state simply as $|\perp\rangle$, and say that such $\mathcal{O}$ is *null-initialized*.

3.5 Examples of compressed oracles

We are going to define two pure compressed oracles, CStO_D and CPhsO_D. For that, first we need to define the swap operator $\sigma_D : \mathbb{C}[\mathcal{Y}_\perp] \to \mathbb{C}[\mathcal{Y}_\perp]$ defined by

$$\begin{aligned} \sigma_D\,|\iota_D\rangle &:= |\perp\rangle\,, \\ \sigma_D\,|\perp\rangle &:= |\iota_D\rangle\,, \\ \sigma_D\,|\phi\rangle &:= |\phi\rangle\,, \qquad \text{if } \langle\iota_D|\phi\rangle = 0. \end{aligned}$$

Note that σ_D is a unitary, hermitian, and involutive operator. When the distribution D is clear, we would often omit D from the notation and just write σ.

Now we are ready to define CStO_D and CPhsO_D.

Definition 3.25 (Compressed standard oracle with respect to D). *Let $\mathcal{X} := \{0,1\}^m$, and $\mathcal{Y} := \{0,1\}^n$. Let D be a probability distribution over $\mathcal{Y}$. We define the* compressed standard oracle *with respect to D, $\mathsf{CStO}_D = (\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}], \mathbb{C}[\mathcal{Y}_\perp^{\mathcal{X}}], \mathsf{query}, |\perp\rangle)$ as follows.*

The query operator query *is given by*

$$\left(I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]} \otimes \bigotimes_{x\in\mathcal{X}} \sigma_D\right) \circ \mathsf{query}' \circ \left(I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]} \otimes \bigotimes_{x\in\mathcal{X}} \sigma_D\right).$$

where the operator query' *is the query operator of* StO_D*:*

$$\mathsf{query}' \left|x\right\rangle \left|y\right\rangle \otimes \left|f\right\rangle := \left|x\right\rangle \left|y \oplus f(x)\right\rangle \otimes \left|f\right\rangle .$$

In fact, we need to extend the definition of query' *by defining* $y \oplus \perp := y$ *for any* $y \in \mathcal{Y} = \{0,1\}^n$*. So* $\mathsf{query}' \left|x\right\rangle \left|y\right\rangle \left|f\right\rangle$ *is well-defined for any partial* f*.*

CStO_D *is a typed oracle of type* $\mathcal{X} \to \mathcal{Y}$*: we may define its measurement operators* M_f *parametrized by partial functions* $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ *simply by*

$$\mathsf{M}_f = \left|f\right\rangle\!\left\langle f\right| .$$

Note that $\mathsf{M}_f = \left|f\right\rangle\!\left\langle f\right| = \bigotimes_{x\in\mathcal{X}} \left|f(x)\right\rangle\!\left\langle f(x)\right|$.

Definition 3.26 (Compressed phase oracle with respect to D). *Let* $\mathcal{X}$*,* $\mathcal{Y}$*, and* D *be the same as in Definition 3.25. We define the* compressed phase oracle *with respect to* D*,* CPhsO_D *as identical in all aspects to* CStO_D*, except that.*

The query operator query *is given by*

$$\left(I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]} \otimes \bigotimes_{x\in\mathcal{X}} \sigma_D\right) \circ \mathsf{query}' \circ \left(I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]} \otimes \bigotimes_{x\in\mathcal{X}} \sigma_D\right).$$

where the operator query' *is the query operator of* PhsO_D*:*

$$\mathsf{query}' \left|x\right\rangle \left|u\right\rangle \otimes \left|f\right\rangle := (-1)^{u\cdot f(x)} \left|x\right\rangle \left|u\right\rangle \otimes \left|f\right\rangle .$$

Again, we need to extend query' *by defining* $u \cdot \perp = 0$ *for any* $y \in \mathcal{Y} = \{0,1\}^n$*.*

Just like CStO_D*,* CPhsO_D *is a typed oracle of type* $\mathcal{X} \to \mathcal{Y}$*, with measurement operators* $\mathsf{M}_f = \left|f\right\rangle\!\left\langle f\right|$ *for partial functions* $f : \mathcal{X} \rightharpoonup \mathcal{Y}$*.*

We can easily prove the following, which corresponds to Theorem 3.17.

Theorem 3.27. CStO_D *and* CPhsO_D *are isomorphic quantum oracles.*

Let us define two operators $i, e : \mathbb{C}[\mathcal{Y}] \to \mathbb{C}[\mathcal{Y}_\perp]$. First, i is the trivial embedding of Hilbert spaces:

$$i \left|y\right\rangle := \left|y\right\rangle , \qquad \text{for any } y \in \mathcal{Y}.$$

Then e is defined as

$$e := \sigma \circ i.$$

It is clear that both i and e are isometries.

Theorem 3.28. *There are pure embeddings* $\mathsf{StO}_D \to \mathsf{CStO}_D$*, and* $\mathsf{PhsO}_D \to \mathsf{CPhsO}_D$*.*

Proof. Both embeddings are given by $\bigotimes_{x\in\mathcal{X}} e$. Let query, query' be the query operators for CStO_D, StO_D, respectively. Then, the following is a commutative square:

$$\begin{tikzcd}
\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]\otimes\mathbb{C}[\mathcal{Y}^{\mathcal{X}}] \arrow[r, "\mathsf{query}'"] \arrow[d, "I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]}\otimes\bigotimes_{x\in\mathcal{X}} e"] & \mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]\otimes\mathbb{C}[\mathcal{Y}^{\mathcal{X}}] \arrow[d, "I_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]}\otimes\bigotimes_{x\in\mathcal{X}} e"] \\
\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]\otimes\mathbb{C}[\mathcal{Y}_\perp^{\mathcal{X}}] \arrow[r, "\mathsf{query}"] & \mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\mathcal{Y}]\otimes\mathbb{C}[\mathcal{Y}_\perp^{\mathcal{X}}]
\end{tikzcd}$$

This is because

$$\begin{aligned}
&\mathsf{query}(I\otimes\bigotimes_x e)\\
&=(I\otimes\bigotimes_x\sigma)\mathsf{query}'(I\otimes\bigotimes_x\sigma)(I\otimes\bigotimes_x\sigma i)\\
&=(I\otimes\bigotimes_x\sigma)\mathsf{query}'(I\otimes\bigotimes_x\sigma\sigma i)\\
&=(I\otimes\bigotimes_x\sigma)\mathsf{query}'(I\otimes\bigotimes_x i),\qquad\because\ \sigma\text{ is an involution.}
\end{aligned}$$

Note that when p is total, then $\mathsf{query}'(I\otimes\bigotimes_x i)\,|x\rangle\,|y\rangle\,|p\rangle=\mathsf{query}'\,|x\rangle\,|y\rangle\,|p\rangle=|x\rangle\,|y\oplus p(x)\rangle\,|p\rangle$, and the result still has a total function p. Therefore,

$$\mathsf{query}'\left(I\otimes\bigotimes_x i\right)=\left(I\otimes\bigotimes_x i\right)\mathsf{query}'.$$

Then,

$$\begin{aligned}
\mathsf{query}(I\otimes\bigotimes_x e)&=(I\otimes\bigotimes_x\sigma)\mathsf{query}'(I\otimes\bigotimes_x i)\\
&=(I\otimes\bigotimes_x\sigma)(I\otimes\bigotimes_x i)\mathsf{query}'\\
&=(I\otimes\bigotimes_x\sigma i)\mathsf{query}'\\
&=(I\otimes\bigotimes_x e)\mathsf{query}'.
\end{aligned}$$

Of course, the same mapping gives an embedding $\mathsf{PhsO}_D\to\mathsf{CPhsO}_D$. □

Theorem 3.28 immediately gives us the following, due to Corollary 3.11.

Corollary 3.29. *The oracles StO_D and CStO_D are completely indistinguishable, and so are the oracles PhsO_D and CPhsO_D.*

For later uses, we need to be able to compute σ and e concretely.

Lemma 3.30. *We have*

$$\sigma=I_{\mathbb{C}[\mathcal{Y}_\perp]}-(|\perp\rangle-|\iota\rangle)(\langle\perp|-\langle\iota|).$$

Proof. According to the definition of the operator σ, we see that

$$\sigma = |\bot\rangle\langle\iota| + |\iota\rangle\langle\bot| + \sum_i |\phi_i\rangle\langle\phi_i|,$$

where $|\phi_i\rangle$ are orthonormal basis vectors of $|\iota\rangle^\perp = \{|\phi\rangle \mid \langle\iota|\phi\rangle = 0\}$.

Then,

$$\begin{aligned}
\sigma &= |\bot\rangle\langle\iota| + |\iota\rangle\langle\bot| + \sum_i |\phi_i\rangle\langle\phi_i| \\
&= |\bot\rangle\langle\bot| + |\iota\rangle\langle\iota| + \sum_i |\phi_i\rangle\langle\phi_i| \\
&\quad - (|\bot\rangle\langle\bot| + |\iota\rangle\langle\iota|) + (|\bot\rangle\langle\iota| + |\iota\rangle\langle\bot|) \\
&= I - (|\bot\rangle\langle\bot| + |\iota\rangle\langle\iota|) + (|\bot\rangle\langle\iota| + |\iota\rangle\langle\bot|) \\
&= I - (|\bot\rangle - |\iota\rangle)(\langle\bot| - \langle\iota|).
\end{aligned}$$

□

Lemma 3.31. *We have*

$$e = i + (|\bot\rangle - |\iota\rangle)\langle\iota|.$$

Proof. For any $y \in \mathcal{Y}$, we have

$$\begin{aligned}
e\,|y\rangle &= \sigma i\,|y\rangle = \sigma\,|y\rangle \\
&= |y\rangle - (|\bot\rangle - |\iota\rangle)(\langle\bot| - \langle\iota|)\,|y\rangle \\
&= |y\rangle + (|\bot\rangle - |\iota\rangle)\langle\iota|y\rangle.
\end{aligned}$$

□

In fact, we need to show that CStO_D and CPhsO_D are indeed compressed. For this, we define the following operator swap. For any $|xyz\rangle \otimes |f\rangle$, we define

$$\mathsf{swap}\,|xyz\rangle \otimes |f\rangle := |xyz\rangle \otimes \left(\sigma\,|f(x)\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle\right).$$

The above notation could be somewhat confusing, but $\sigma\,|f(x)\rangle$ is in the register indexed by x, and for $w \neq x$, $|f(w)\rangle$ is in the register indexed by w.

Then,

$$\begin{aligned}
&\mathsf{swap}\,|xyz\rangle \otimes |f\rangle \\
&= |xyz\rangle \otimes \left(\sigma\,|f(x)\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle\right) \\
&= |xyz\rangle \otimes (|f(x)\rangle - (|\bot\rangle - |\iota\rangle)(\langle\bot| - \langle\iota|)\,|f(x)\rangle) \otimes \bigotimes_{w \neq x} |f(w)\rangle \\
&= |xyz\rangle \otimes \left(|f(x)\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle\right.
\end{aligned}$$

$$
\begin{aligned}
&+ \left(\langle \iota | f(x) \rangle - \langle \perp | f(x) \rangle\right) |\perp\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle \\
&- \left(\langle \iota | f(x) \rangle - \langle \perp | f(x) \rangle\right) |\iota\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle \Bigg) \\
= |xyz\rangle \otimes \Bigg(&|f\rangle + \left(\langle \iota | f(x) \rangle - \langle \perp | f(x) \rangle\right) |f[x \to \perp]\rangle \\
&- \left(\langle \iota | f(x) \rangle - \langle \perp | f(x) \rangle\right) \sum_{y'} \sqrt{D(y')}\, |f[x \to y']\rangle \Bigg)
\end{aligned}
$$

Hence, when $f(x) = \perp$,

$$
\mathsf{swap}\, |xyz\rangle \otimes |f\rangle = |xyz\rangle \otimes \sum_{y'} \sqrt{D(y')}\, |f[x \to y']\rangle \,,
$$

and when $f(x) \neq \perp$,

$$
\begin{aligned}
\mathsf{swap}\, |xyz\rangle \otimes |f\rangle = |xyz\rangle \otimes \Bigg(&|f\rangle + \sqrt{D(f(x))}\, |f[x \to \perp]\rangle \\
&- \sqrt{D(f(x))} \sum_{y'} \sqrt{D(y')}\, |f[x \to y']\rangle \Bigg)
\end{aligned}
$$

Theorem 3.32. *The quantum oracle CStO_D is compressed, and its query operator can be described as*

$$
\mathsf{swap} \circ \mathsf{query}' \circ \mathsf{swap},
$$

where query' is the query operator of StO_D, extended for $\perp$.

Similarly, we have

$$
\mathsf{CPhsO}_D = \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap},
$$

where query'' is the query operator of PhsO_D, extended for $\perp$.

Proof. Let us show this for CPhsO_D; the case for CStO_D can be proved similarly.

We have to show that $\mathsf{CPhsO}_D\, |xyzf\rangle = \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap}\, |xyzf\rangle$ for any x, y, z and f. For this, let us fix x, y and z arbitrarily. Recall that $\mathsf{query}''\, |xyzf\rangle = |xyz\rangle \otimes (-1)^{y \cdot f(x)}\, |f\rangle$, and $\mathsf{swap}\, |xyz\rangle \otimes |f\rangle := |xyz\rangle \otimes \left(\sigma\, |f(x)\rangle \otimes \bigotimes_{w \neq x} |f(w)\rangle\right)$.

Then, both query'' and swap preserve $|xyz\rangle$, and depends only on $|f\rangle$. In fact, we see that both query'' and swap only depend on the oracle register indexed by x, and acts as identity on other registers of the oracle state. Therefore, both query'' and swap, when regarded as operators on the oracle state (as we have fixed $|xyz\rangle$), commute with $I \otimes \bigotimes_{w \neq x} \sigma$, where I denotes the identity operator on the oracle register indexed by x. Then, CPhsO_D query operator, when $|xyz\rangle$ is fixed, is $(\bigotimes_w \sigma)\mathsf{query}''(\bigotimes_w \sigma)$, but then,

$$\begin{aligned}
&\mathsf{CPhsO}_D \\
&= (\bigotimes_w \sigma)\mathsf{query}''(\bigotimes_w \sigma) \\
&= (I \otimes \bigotimes_{w\neq x} \sigma) \circ \mathsf{swap} \circ \mathsf{query}'' \circ (I \otimes \bigotimes_{w\neq x} \sigma) \circ \mathsf{swap} \\
&= (I \otimes \bigotimes_{w\neq x} \sigma) \circ (I \otimes \bigotimes_{w\neq x} \sigma) \circ \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap} \\
&= (I \otimes \bigotimes_{w\neq x} \sigma\sigma) \circ \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap} \\
&= \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap}. \qquad \square
\end{aligned}$$

Now we see that CPhsO_D (and CStO_D) is indeed compressed. Consider the maximum of the rank of partial functions occurring in the oracle state right after the qth query. Since CPhsO_D is null-initialized, at the start the maximum rank is 0. For each query, since $\mathsf{CPhsO}_D = \mathsf{swap} \circ \mathsf{query}'' \circ \mathsf{swap}$, from the formula for swap we see that $\mathsf{CPhsO}_D\,|xyzf\rangle$ contains any term with larger rank than $|f|$ precisely when $f(x) = \bot$, and in that case the maximum rank is $\leq |f| + 1$. Therefore, the maximum rank of partial functions occurring in the oracle state is bounded by q, and each partial function f can be implemented efficiently as a dictionary of size $O(q)$.

4 Recordability

We want to formally define a notion of *recordability* of quantum oracles. While it could be nontrivial to capture all possible ways such recording can be done and used, one possible and natural initial attempt could be made by elevating Lemma 5 of Zhandry [26] to a definition:

Definition 4.1. *Let $\mathcal{O}, \mathcal{O}'$ be quantum oracles over the same interface space $\mathcal{I}$, and suppose that they have the same type $\mathcal{X} \to \mathcal{Y}$. Let $\mu : \mathcal{O} \to \mathcal{O}'$ be an embedding. Consider a quantum algorithm A making queries to a quantum oracle and outputting a tuple (f, z), where $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ is a partial function, and z is an auxiliary data. Let R be a relation of such tuples.*

Suppose A interacts with $\mathcal{O}$ and outputs a tuple (f, z). Assume $\mathcal{O}$ is measured afterwards: $h \leftarrow \mathcal{O}$. Let p be the probability that, (1) $R(f, z)$, and (2) $f \subseteq h$.

Similarly, let p' be the probability defined exactly like p, except that in this case A interacts with $\mathcal{O}'$. So, A outputs (f, z) after the interaction, and then $\mathcal{O}'$ is measured: $h' \leftarrow \mathcal{O}'$. Then p' is defined as the probability that, (1) $R(f, z)$ and (2) $f \subseteq h'$.

Let r_R be defined as

$$r_R := \max_f \{|f| \mid \exists z, R(f, z)\},$$

the maximum possible rank of f, which satisfies $R(f,z)$ for some z.

Then, we say that the embedding μ ε-records $\mathcal{O}$ for the relation R, if

$$\sqrt{p} \leq \sqrt{p'} + \sqrt{\varepsilon \cdot r_R}$$

holds for any such adversary A.

Remark 4.2. When the embedding $\mu : \mathcal{O} \to \mathcal{O}'$ is clear, we may simply say that the oracle $\mathcal{O}'$ ε-records the oracle $\mathcal{O}$ for R.

Example 4.3. Zhandry [26] showed in his Lemma 5 that, when we consider the uniform distribution, CStO $1/2^n$-records StO for any relation R.

Remark 4.4. One difference between our Definition 4.1 and Zhandry's Lemma 5 is that our oracles record for some particular relation R. We need this to handle the case where, for example, the codomain $\mathcal{Y}$ is small, like $\{0,1\}$. We refer to Remark 5.3 for more discussions.

We would like to show that CStO_D records StO_D in general. For this, we need a stronger, if somewhat abstract formalism for our purposes. Therefore, we will define *strong recordability.* While we believe that this definition can be generalized, here we will simply give the definition for StO_D and CStO_D (and also for PhsO_D and CPhsO_D).

Definition 4.5 (Strong recordability). *We say that* CStO_D ε-strongly records StO_D *for a relation R, if the following holds.*

$$\left\| \bigotimes_{x \in \mathrm{dom}(f)} i \, |f(x)\rangle\langle f(x)| - \bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)| \, e \right\|_F^2 \leq \varepsilon \cdot r_R,$$

for any $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ and z satisfying $R(f,z)$. Also, $\| \cdot \|_F$ is the Frobenius norm of an operator.

Similarly, we define that CPhsO_D *ε-strongly records* PhsO_D *for a relation R, if the same inequality as above holds.*

Remark 4.6. Strong recordability defined above, and also Theorem 4.8 below are influenced by Chung et al. [9], specifically Lemma 4.1 and the proof of the lemma. While their lemma is based on the Fourier transform and works for the uniform distribution, at the last step of the proof they use the Frobenius norm. We observe that in fact the Frobenius norm can be used from the start, and moreover it also works for any probability distribution D, and without the Fourier transform.

We have the following useful lemma.

Lemma 4.7. *When B, C are isometries, then for any operator A and any vector $|\Psi\rangle$, we have*

$$\|(A \otimes B) \, |\Psi\rangle \,\| = \|(A \otimes C) \, |\Psi\rangle \,\|.$$

Proof. Write $|\Psi\rangle$ in terms of an orthonormal basis of the tensor product:

$$|\Psi\rangle = \sum_{a,b} \alpha_{ab} |\phi_a\rangle |\psi_b\rangle .$$

Then,

$$\begin{aligned} \| (A \otimes B) |\Psi\rangle \|^2 &= \sum_{abcd} \overline{\alpha_{ab}} \alpha_{cd} \langle \phi_a | A^\dagger A |\phi_c\rangle \langle \psi_b | B^\dagger B |\psi_d\rangle \\ &= \sum_{abcd} \overline{\alpha_{ab}} \alpha_{cd} \langle \phi_a | A^\dagger A |\phi_c\rangle \langle \psi_b | C^\dagger C |\psi_d\rangle \\ &= \| (A \otimes C) |\Psi\rangle \|^2. \end{aligned}$$

In the above, since B, C are isometries, $B^\dagger B = C^\dagger C = I$. ☐

Now we may relate strong recordability and recordability in the following theorem. The proof is an adaptation of Corollary 4.2 of Chung et al. [9]. While the following theorem is given in terms of CStO_D and StO_D, the proof works for CPhsO_D and PhsO_D, identically.

Theorem 4.8. *ε-strong recordability implies ε-recordability.*

Proof. Let R be a relation of partial functions $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ and auxiliary data z. And let $\varepsilon > 0$ be a constant.

Suppose that $\mu = \bigotimes_x e$ ϵ-strongly records StO_D for a relation R. We need to show that μ ε-records StO_D for a relation R.

Let A be an adversary which interacts with an oracle and eventually outputs a pair (f, z), where $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ is a partial function and z is an auxiliary data, and let R be a collection of such tuples. After outputting (f, z), let us measure the rest of the internal state of the adversary and let the outcome of the measurement be w. Let $q_{f,z,w}$ be the probability that the output of A^{StO_D} is (f, z) and the measurement outcome of the rest of the state is w. And let $p_{f,z,w}$ be the probability that $h \leftarrow \mathsf{StO}_D$ satisfies $f \subseteq h$, conditioned on f, z, and w. By definition,

$$p = \sum_{(f,z)\in R, w} q_{f,z,w} p_{f,z,w}.$$

Similarly, let us define $q'_{f,z,w}$ and $p'_{f,z,w}$ to be the corresponding probabilities, when A interacts with CStO_D. Again we have

$$p' = \sum_{(f,z)\in R, w} q'_{f,z,w} p'_{f,z,w}.$$

Since μ is an embedding, by Corollary 3.11, StO_D and CStO_D are completely indistinguishable as quantum oracles, so $q'_{f,z,w} = q_{f,z,w}$.

Let $\{\mathsf{M}_f\}_{f:\mathcal{X}\rightharpoonup\mathcal{Y}}$ be the set of measurement operators for StO_D, and let $\{\mathsf{M}'_f\}_{f:\mathcal{X}\rightharpoonup\mathcal{Y}}$ be the set of measurement operators for CStO_D. Recall that $\mathsf{M}'_f = |f\rangle\langle f| = \bigotimes_{x\in\mathcal{X}} |f(x)\rangle\langle f(x)|$, and $\mathsf{M}_f = |f\rangle\langle f|$ for any total function f, and $\mathsf{M}_f = 0$ for partial functions.

Observe that when $|\Psi\rangle$ is the internal state of StO_D, post-selected for f, z, w, then

$$p_{f,z,w} = \left\| \sum_{h \supseteq f} \mathsf{M}_h |\Psi\rangle \right\|^2 = \left\| \left(\bigotimes_x i \right) \sum_{h \supseteq f} \mathsf{M}_h |\Psi\rangle \right\|^2,$$

since $\bigotimes_x i$ is an isometry. Note that

$$\begin{aligned}
\left(\bigotimes_{x \in \mathcal{X}} i \right) \sum_{h \supseteq f} \mathsf{M}_h &= \left(\bigotimes_{x \in \mathcal{X}} i \right) \sum_{h \supseteq f} \bigotimes_{x \in \mathcal{X}} |h(x)\rangle\langle h(x)| \\
&= \bigotimes_{x \in \mathrm{dom}(f)} i\, |f(x)\rangle\langle f(x)| \otimes \bigotimes_{x \notin \mathrm{dom}(f)} i \sum_{y \in \mathcal{Y}} |y\rangle\langle y| \\
&= \bigotimes_{x \in \mathrm{dom}(f)} i\, |f(x)\rangle\langle f(x)| \otimes \bigotimes_{x \notin \mathrm{dom}(f)} i.
\end{aligned}$$

So,

$$p_{f,z,w} = \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} i\, |f(x)\rangle\langle f(x)| \otimes \bigotimes_{x \notin \mathrm{dom}(f)} i \right) |\Psi\rangle \right\|^2.$$

Since $\mu = (\bigotimes_x e)$ is an embedding, we see that $\mu |\Psi\rangle$ is the corresponding oracle state of CStO_D, postselected for f, z, w. So, $p'_{f,z,w} = \| \sum_{h \supseteq f} \mathsf{M}'_h (\bigotimes_x e) |\Psi\rangle \|^2$. Similar to $p_{f,z,w}$, we can separate $\mathrm{dom}(f)$ part and the rest to get

$$p'_{f,z,w} = \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)|\, e \otimes \bigotimes_{x \notin \mathrm{dom}(f)} e \right) |\Psi\rangle \right\|^2,$$

Applying Lemma 4.7, we get

$$p'_{f,z,w} = \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)|\, e \bigotimes_{x \notin \mathrm{dom}(f)} i \right) |\Psi\rangle \right\|^2,$$

Then, we have

$$\begin{aligned}
&\sqrt{p_{f,z,w}} - \sqrt{p'_{f,z,w}} \\
&= \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} i\, |f(x)\rangle\langle f(x)| \otimes \bigotimes_{x \notin \mathrm{dom}(f)} i \right) |\Psi\rangle \right\| \\
&\qquad - \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)|\, e \otimes \bigotimes_{x \notin \mathrm{dom}(f)} i \right) |\Psi\rangle \right\| \\
&\leq \left\| \left(\bigotimes_{x \in \mathrm{dom}(f)} i\, |f(x)\rangle\langle f(x)| - \bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)|\, e \right) \otimes \left(\bigotimes_{x \notin \mathrm{dom}(f)} i \right) |\Psi\rangle \right\|
\end{aligned}$$

$$
\begin{aligned}
&\leq \left\| \left(\bigotimes_{x\in \mathrm{dom}(f)} i \left|f(x)\right\rangle\!\left\langle f(x)\right| - \bigotimes_{x\in \mathrm{dom}(f)} \left|f(x)\right\rangle\!\left\langle f(x)\right| e \right) \otimes \bigotimes_{x\notin \mathrm{dom}(f)} i \right\| \\
&\leq \left\| \bigotimes_{x\in \mathrm{dom}(f)} i \left|f(x)\right\rangle\!\left\langle f(x)\right| - \bigotimes_{x\in \mathrm{dom}(f)} \left|f(x)\right\rangle\!\left\langle f(x)\right| e \right\| \prod_{x\notin \mathrm{dom}(f)} \|i\| \\
&= \left\| \bigotimes_{x\in \mathrm{dom}(f)} i \left|f(x)\right\rangle\!\left\langle f(x)\right| - \bigotimes_{x\in \mathrm{dom}(f)} \left|f(x)\right\rangle\!\left\langle f(x)\right| e \right\| \\
&\leq \left\| \bigotimes_{x\in \mathrm{dom}(f)} i \left|f(x)\right\rangle\!\left\langle f(x)\right| - \bigotimes_{x\in \mathrm{dom}(f)} \left|f(x)\right\rangle\!\left\langle f(x)\right| e \right\|_F \\
&\leq \sqrt{\varepsilon \cdot r_R}.
\end{aligned}
$$

In the above, we have used properties of the operator norm, and the fact that the operator norm is bounded by the Frobenius norm.

Now, we have

$$
\begin{aligned}
p_{f,z,w} &\leq \left(\sqrt{p'_{f,z,w}} + \sqrt{\varepsilon \cdot r_R} \right)^2 \\
&= p'_{f,z,w} + 2\sqrt{\varepsilon \cdot r_R}\sqrt{p'_{f,z,w}} + \varepsilon \cdot r_R.
\end{aligned}
$$

Then,

$$
\begin{aligned}
p &= \sum_{(f,z)\in R,w} q_{f,z,w} p_{f,z,w} \\
&\leq \sum_{(f,z)\in R,w} q_{f,z,w} \left(p'_{f,z,w} + 2\sqrt{\varepsilon \cdot r_R}\sqrt{p'_{f,z,w}} + \varepsilon \cdot r_R \right) \\
&= \sum_{(f,z)\in R,w} q_{f,z,w} p'_{f,z,w} + 2\sqrt{\varepsilon \cdot r_R} \sum_{(f,z)\in R,w} q_{f,z,w} \sqrt{p'_{f,z,w}} \\
&\qquad + \varepsilon \cdot r_R \sum_{(f,z)\in R,w} q_{f,z,w} \\
&= p' + 2\sqrt{\varepsilon \cdot r_R} \sum_{(f,z)\in R,w} q_{f,z,w} \sqrt{p'_{f,z,w}} + \varepsilon \cdot r_R \\
&\leq p' + 2\sqrt{\varepsilon \cdot r_R} \sqrt{\sum_{(f,z)\in R,w} q_{f,z,w} p'_{f,z,w}} + \varepsilon \cdot r_R \\
&= p' + 2\sqrt{\varepsilon \cdot r_R}\sqrt{p'} + \varepsilon \cdot r_R = (\sqrt{p'} + \sqrt{\varepsilon \cdot r_R})^2.
\end{aligned}
$$

In the last inequality above, we used Jensen's inequality.

Hence,

$$
\sqrt{p} \leq \sqrt{p'} + \sqrt{\varepsilon \cdot r_R}. \qquad \square
$$

In order to prove that CStO_D strongly records StO_D, we need one additional definition.

Definition 4.9. *Let R be a relation of partial functions f and auxiliary data z. We say that R is* ε-bounded *with respect to D, if for any $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ and z, whenever $R(f,z)$ holds, then*

$$D(f(x)) \leq \varepsilon, \qquad \text{for all } x \in \mathrm{dom}(f).$$

Remark 4.10. We see that any R is $1/2^k$-bounded with respect to D, if k is the min-entropy of D, since

$$D(y) \leq \frac{1}{2^k}$$

for any $y \in \mathcal{Y}$.

Theorem 4.11. *If R is ε-bounded with respect to D, then CStO_D ε-strongly records StO_D for R, and CPhsO_D ε-strongly records PhsO_D for R.*

Proof. Fix an arbitrary partial function $f : \mathcal{X} \rightharpoonup \mathcal{Y}$ which satisfies $R(f,z)$ for some z, and let r be the rank of f. Let $\mathrm{dom}(f) = \{x_1, \ldots, x_r\}$, and $y_i := f(x_i)$.

Since $i : \mathbb{C}[\mathcal{Y}] \to \mathbb{C}[\mathcal{Y}_\perp]$ is an inclusion map, we have $i\,|y\rangle\langle y| = |y\rangle\langle y|\,i$ for any $y \in \mathcal{Y}$.

Recall that $\|A\|_F^2 = \mathrm{tr}[A^\dagger A]$ for any operator A. Then we have

$$\begin{aligned}
&\left\| \bigotimes_{x\in\mathrm{dom}(f)} i\,|f(x)\rangle\langle f(x)| - \bigotimes_{x\in\mathrm{dom}(f)} |f(x)\rangle\langle f(x)|\,e \right\|_F^2 \\
&= \left\| \bigotimes_{j=1}^{r} i\,|y_i\rangle\langle y_i| - \bigotimes_{j=1}^{r} |y_i\rangle\langle y_i|\,e \right\|_F^2 \\
&= \left\| \bigotimes_{j=1}^{r} |y_i\rangle\langle y_i|\,i - \bigotimes_{j=1}^{r} |y_i\rangle\langle y_i|\,e \right\|_F^2 \\
&= \left\| \left(\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i|\right) \left(\bigotimes_{j=1}^{r} i - \bigotimes_{j=1}^{r} e\right) \right\|_F^2
\end{aligned}$$

Rewriting the above using the trace, we get

$$\begin{aligned}
&= \mathrm{tr}\left[\left(\bigotimes_{j=1}^{r} i^\dagger - \bigotimes_{j=1}^{r} e^\dagger\right) \bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \left(\bigotimes_{j=1}^{r} i - \bigotimes_{j=1}^{r} e\right) \right] \\
&= \mathrm{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \left(\bigotimes_{j=1}^{r} i - \bigotimes_{j=1}^{r} e\right) \left(\bigotimes_{j=1}^{r} i^\dagger - \bigotimes_{j=1}^{r} e^\dagger\right) \right]
\end{aligned}$$

$$= \operatorname{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \left(\bigotimes_{j=1}^{r} ii^\dagger - \bigotimes_{j=1}^{r} ei^\dagger - \bigotimes_{j=1}^{r} ie^\dagger + \bigotimes_{j=1}^{r} ee^\dagger\right)\right]$$

$$= \operatorname{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \, ii^\dagger\right] - \operatorname{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \, ei^\dagger\right]$$

$$- \operatorname{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \, ie^\dagger\right] + \operatorname{tr}\left[\bigotimes_{j=1}^{r} |y_i\rangle\langle y_i| \, ee^\dagger\right]$$

$$= \prod_{j=1}^{r} \langle y_i| \, ii^\dagger \, |y_i\rangle - \prod_{j=1}^{r} \langle y_i| \, ei^\dagger \, |y_i\rangle - \prod_{j=1}^{r} \langle y_i| \, ie^\dagger \, |y_i\rangle + \prod_{j=1}^{r} \langle y_i| \, ee^\dagger \, |y_i\rangle .$$

Now, for any $y, z \in \mathcal{Y}$, we have $\langle z| \, i^\dagger \, |y\rangle = \overline{\langle y| \, i \, |z\rangle} = \overline{\langle y|z\rangle} = \langle z|y\rangle$. So $i^\dagger \, |y\rangle = |y\rangle$. Then, $\langle y| \, ii^\dagger \, |y\rangle = \langle y|y\rangle = 1$.

Also, we have

$$\begin{aligned}
\langle y| \, ei^\dagger \, |y\rangle &= \langle y| \, e \, |y\rangle = \langle y| \, (i + (|\bot\rangle - |\iota\rangle) \, \langle\iota|) \, |y\rangle \\
&= \langle y|y\rangle - \langle y|\iota\rangle \, \langle\iota|y\rangle = 1 - D(y), \\
\langle y| \, ie^\dagger \, |y\rangle &= \overline{\langle y| \, ei^\dagger \, |y\rangle} = \overline{1 - D(y)} = 1 - D(y), \\
\langle y| \, ee^\dagger \, |y\rangle &= \langle y| \, (i + (|\bot\rangle - |\iota\rangle) \, \langle\iota|)e^\dagger \, |y\rangle \\
&= \langle y| \, ie^\dagger \, |y\rangle - \langle y|\iota\rangle \, \langle\iota| \, e^\dagger \, |y\rangle \\
&= 1 - D(y) - \langle y|\iota\rangle \, \overline{\langle y| \, e \, |\iota\rangle} \\
&= 1 - D(y) - \langle y|\iota\rangle \, \overline{\langle y|\bot\rangle} = 1 - D(y).
\end{aligned}$$

Then,

$$\begin{aligned}
&\left\| \bigotimes_{x \in \mathrm{dom}(f)} i \, |f(x)\rangle\langle f(x)| - \bigotimes_{x \in \mathrm{dom}(f)} |f(x)\rangle\langle f(x)| \, e \right\|_F^2 \\
&= \prod_{j=1}^{r} \langle y_j| \, ii^\dagger \, |y_j\rangle - \prod_{j=1}^{r} \langle y_j| \, ei^\dagger \, |y_j\rangle - \prod_{j=1}^{r} \langle y_j| \, ie^\dagger \, |y_j\rangle + \prod_{j=1}^{r} \langle y_j| \, ee^\dagger \, |y_j\rangle \\
&= \prod_{j=1}^{r} 1 - \prod_{j=1}^{r} (1 - D(y_j)) - \prod_{j=1}^{r} (1 - D(y_j)) + \prod_{j=1}^{r} (1 - D(y_j)) \\
&= 1 - \prod_{j=1}^{r} (1 - D(y_j)) \leq \sum_{j=1}^{r} D(y_j) \\
&= \sum_{x \in \mathrm{dom}(f)} D(f(x)) \leq \sum_{x \in \mathrm{dom}(f)} \varepsilon = \varepsilon |f| \leq \varepsilon \cdot r_R.
\end{aligned}$$

□

Combining Theorem 4.8 and Theorem 4.11, we obtain:

Corollary 4.12. *Suppose D is a probability distribution over $\mathcal{Y}$. If R is ε-bounded with respect to D, then CStO_D ε-records StO_D for R, and CPhsO_D ε-records PhsO_D for R.*

Corollary 4.13. *Suppose D is a probability distribution over $\mathcal{Y}$. Suppose k is the min-entropy of D. Then, CStO_D $1/2^k$-records StO_D for any relation R, and CPhsO_D $1/2^k$-records PhsO_D for any relation R.*

5 Applications

In this section, we will apply the compressed oracle technique for non-uniform random oracles to two problems: optimality of Grover search, and collision lower bound for non-uniform random oracles.

5.1 Optimality of Grover search

First, we will give yet another proof that the quadratic speed-up of the Grover search is optimal. Specifically, we will consider a non-uniform random oracle $H : \{0,1\}^m \to \{0,1\}$, where each $H(x)$ is distributed independently according to the Bernoulli distribution B, where B be a probability distribution over $\{0,1\}$, with $B(1) = p$ and $B(0) = 1-p$ for some p satisfying $0 \leq p \leq 1/2$. We will show that the success probability of an adversary for finding a point x with $H(x) = 1$ is $O(pq^2)$.

In section 4 of [26], Zhandry gives a similar result, using the compressed oracle technique: for a uniform random oracle $H : \{0,1\}^m \to \{0,1\}^n$, the success probability for finding a point $x \in \{0,1\}^m$ with $H(x) = 0^n$ is $O(q^2/2^n)$. This corresponds to the Bernoulli distribution with $p = 1/2^n$. We generalize this to arbitrary Bernoulli parameter p, using the compressed oracle technique which we have extended to non-uniform random oracles. In fact, we may re-use Zhandry's proof almost unchanged, but applied to non-uniform compressed oracles.

Observe that it would be possible to obtain this result using only compressed oracles for uniform random oracles: approximate p in binary with sufficient precision: $p \approx d/2^n$ for some d, and analyze the success probability in finding some x with $0 \leq H(x) \leq l-1$. But, our method could be considered as more straightforward: we directly prove our results for random boolean functions with Bernoulli distribution for each point. See Remark 5.3 for more discussions about this.

Theorem 5.1. *Let B be a distribution over $\{0,1\}$ with $B(1) = p$ and $B(0) = 1-p$. Let $\mathcal{O}$ be either CStO_B or CPhsO_B. Then, for any adversary A interacting with $\mathcal{O}$, if $\mathcal{O}$ is measured after A makes q queries, the probability that the measurement outcome $f \leftarrow \mathcal{O}$ contains an element $x \in \mathcal{X}$ with $f(x) = 1$ is at most $8pq^2$.*

Proof. Since CStO_B and CPhsO_B are isomorphic, we need only to show this for CPhsO_D. Consider the joint state of the adversary and the oracle right before the adversary's jth query:

$$|\psi\rangle = \sum_{x,y,z,f} \alpha_{xyzf} |xyz\rangle \otimes |f\rangle ,$$

where $|z\rangle$ is in the work register of the adversary.

Let us define four projections P, Q, R, S as follows.

- P is the projection onto the span of $|xyzf\rangle$ where $1 \in \mathrm{rng}(f)$.
- Q is the projection onto the span of $|xyzf\rangle$ where $1 \notin \mathrm{rng}(f)$, $y = 1$, and $f(x) = \perp$.
- R is the projection onto the span of $|xyzf\rangle$ where $1 \notin \mathrm{rng}(f)$, $y = 1$, and $f(x) \neq \perp$, hence $f(x) = 0$.
- S is the projection onto the span of $|xyzf\rangle$ where $1 \notin \mathrm{rng}(f)$, and $y = 0$.

Then, $P + Q + R + S = I$. We will show that $\|P\,|\psi\rangle\,\|$ does not increase too fast, as the number of queries increases.

Suppose that $|xyzf\rangle$ is in the support of Q. In that case, $y = 1, f(x) = \perp$, and

$$\begin{aligned}
&P\,\mathsf{CPhsO}_D\,|xyzf\rangle = P\,\mathsf{swap}\,\mathsf{query}'\,\mathsf{swap}\,|xyzf\rangle \\
&= P\,\mathsf{swap}\,\mathsf{query}'\,|xyz\rangle \otimes \sum_{y'} \sqrt{D(y')}\,|f[x \to y']\rangle \\
&= P\,\mathsf{swap}\,|xyz\rangle \otimes \sum_{y'} (-1)^{y \cdot y'} \sqrt{D(y')}\,|f[x \to y']\rangle \\
&= P\,|xyz\rangle \otimes \sum_{y'} (-1)^{y'} \sqrt{D(y')} \Bigg(|f[x \to y']\rangle \\
&\qquad + \sqrt{D(y')}\,|f\rangle - \sqrt{D(y')} \sum_{y''} \sqrt{D(y'')}\,|f[x \to y'']\rangle \Bigg).
\end{aligned}$$

Since $1 \notin \mathrm{rng}(f)$, when we apply the projection P, in the above $|f\rangle$ will vanish, and only terms involving $|f[x \to 1]\rangle$ survive. In this case, $f[x \to y']$ and $f[x \to y'']$ become $f[x \to 1]$ and the corresponding coefficients $D(y')$ and $D(y'')$ collapse to p. So the above equals

$$\begin{aligned}
&-\sqrt{p} \cdot \left(1 + \left(\sum_{y'} (-1)^{y'} D(y') \right) \right) |xyz\rangle\,|f[x \to 1]\rangle \\
&= -\sqrt{p}(1 + ((1-p) - p))\,|xyz\rangle\,|f[x \to 1]\rangle \\
&= -2\sqrt{p}(1-p)\,|xyz\rangle\,|f[x \to 1]\rangle\,.
\end{aligned}$$

So, if $Q\,|\psi\rangle = \sum_{xyzf} \alpha_{xyzf}\,|xyzf\rangle$, then we have $\|Q\,|\psi\rangle\,\|^2 = \sum_{xyzf} |\alpha_{xyzf}|^2$, and

$$P\,\mathsf{CPhsO}_B\,Q\,|\psi\rangle = \sum_{xyzf} \alpha_{xyzf}(-2\sqrt{p}(1-p))\,|xyz\rangle\,|f[x \to 1]\rangle\,.$$

So,

$$\|P\,\mathsf{CPhsO}_B\,Q\,|\psi\rangle\,\|^2 = \sum_{xyzf} |\alpha_{xyzf}|^2 \cdot 4p(1-p)^2$$

$$
\begin{aligned}
&= 4p(1-p)^2 \|Q\left|\psi\right\rangle\|^2 \\
&\leq 4p\|Q\left|\psi\right\rangle\|^2.
\end{aligned}
$$

Hence, $\|P\,\mathsf{CPhsO}_B\,Q\left|\psi\right\rangle\| \leq 2\sqrt{p}\|Q\left|\psi\right\rangle\|$.

Also, suppose that $\left|xyzf\right\rangle$ is in the support of R. In that case, $y=1$, $f(x)=0$, and

$$
\begin{aligned}
&P\,\mathsf{CPhsO}_D\left|xyzf\right\rangle \\
&= P\mathsf{swap}\circ\mathsf{query}'\circ\mathsf{swap}\left|xyzf\right\rangle \\
&= P\mathsf{swap}\circ\mathsf{query}'\left|xyz\right\rangle\Bigg(\left|f\right\rangle + \sqrt{B(f(x))}\left|f[x\to\bot]\right\rangle \\
&\qquad - \sqrt{B(f(x))}\sum_w \sqrt{B(w)}\left|f[x\to w]\right\rangle\Bigg) \\
&= P\mathsf{swap}\left|xyz\right\rangle\Bigg((-1)^{1\cdot 0}\left|f\right\rangle + \sqrt{1-p}\left|f[x\to\bot]\right\rangle \\
&\qquad - \sqrt{1-p}\sum_w (-1)^{1\cdot w}\sqrt{B(w)}\left|f[x\to w]\right\rangle\Bigg) \\
&= P\mathsf{swap}\left|xyz\right\rangle(\left|f\right\rangle + \sqrt{1-p}\left|f[x\to\bot]\right\rangle \\
&\qquad - \sqrt{1-p}\sum_w (-1)^{1\cdot w}\sqrt{B(w)}\left|f[x\to w]\right\rangle) \\
&= P\left|xyz\right\rangle(\left|f\right\rangle + \sqrt{B(f(x))}\left|f[x\to\bot]\right\rangle \\
&\qquad\qquad\qquad - \sqrt{B(f(x))}\sum_w \sqrt{B(w)}\left|f[x\to w]\right\rangle \\
&\qquad + \sqrt{1-p}\sum_w \sqrt{B(w)}\left|f[x\to w]\right\rangle \\
&\qquad - \sqrt{1-p}\sum_w (-1)^w\sqrt{B(w)}(\left|f[x\to w]\right\rangle \\
&\qquad\quad + \sqrt{B(w)}\left|f[x\to\bot]\right\rangle \\
&\qquad\quad - \sqrt{B(w)}\sum_{w'}\sqrt{B(w')}\left|f[x\to w']\right\rangle))
\end{aligned}
$$

Again, when the projection P is applied, $\left|f\right\rangle, \left|f[x\to\bot]\right\rangle$ vanish, and only terms involving $\left|f[x\to 1]\right\rangle$ survive. So, the above equals

$$
\begin{aligned}
&= \left|xyz\right\rangle(-\sqrt{1-p}\sqrt{p}\left|f[x\to 1]\right\rangle \\
&\qquad + \sqrt{1-p}\sqrt{p}\left|f[x\to 1]\right\rangle \\
&\qquad - \sqrt{1-p}(-1)^1\sqrt{p}\left|f[x\to 1]\right\rangle \\
&\qquad\quad + \sqrt{1-p}\left(\sum_w (-1)^w B(w)\right)\sqrt{p}\left|f[x\to 1]\right\rangle)
\end{aligned}
$$

$$
\begin{aligned}
&= \sqrt{p(1-p)}\left(1+\sum_w (-1)^w B(w)\right) |xyz\rangle\,|f[x\to 1]\rangle \\
&= \sqrt{p(1-p)}(1+(1-p)-p)\,|xyz\rangle\,|f[x\to 1]\rangle \\
&= 2\sqrt{p(1-p)}(1-p)\,|xyz\rangle\,|f[x\to 1]\rangle\,.
\end{aligned}
$$

So, if we write $R\,|\psi\rangle = \sum_{xyzf} \alpha_{xyzf}\,|xyzf\rangle$, then $\|R\,|\psi\rangle\,\|^2 = \sum_{xyzf} |\alpha_{xyzf}|^2$, and

$$
\begin{aligned}
&P\,\mathsf{CPhsO}_B\,R\,|\psi\rangle \\
&= \sum_{xyzf} \alpha_{xyzf}(2\sqrt{p(1-p)}(1-p))\,|xyz\rangle\,|f[x\to 1]\rangle\,.
\end{aligned}
$$

So,

$$
\begin{aligned}
\|P\,\mathsf{CPhsO}_B\,R\,|\psi\rangle\,\|^2 &= \sum_{xyzf} |\alpha_{xyzf}|^2 \cdot 4p(1-p)^3 \\
&= 4p(1-p)^3\|R\,|\psi\rangle\,\|^2 \\
&\le 4p\|R\,|\psi\rangle\,\|^2.
\end{aligned}
$$

Hence, $\|P\,\mathsf{CPhsO}_B\,R\,|\psi\rangle\,\| \le 2\sqrt{p}\|R\,|\psi\rangle\,\|$.

Finally, when $|xyzf\rangle$ is in the support of S, $y=0$. In that case, query', which is $\mathsf{query}'\,|xyzf\rangle = (-1)^{y\cdot f(x)}\,|xyzf\rangle$, acts as the identity operator, when restricted to the support of S. Therefore, $\mathsf{CPhsO}_B = \mathsf{swap}\circ\mathsf{query}'\circ\mathsf{swap} = \mathsf{swap}\circ\mathsf{swap}$, which is identity since swap is involutive.

So, $\mathsf{CPhsO}_B\,S\,|\psi\rangle = S\,|\psi\rangle$. Therefore, $P\,\mathsf{CPhsO}_B\,S\,|\psi\rangle = PS\,|\psi\rangle = 0$.

Also, for any $|\psi\rangle$, we have $\|P\,\mathsf{CPhsO}_B\,P\,|\psi\rangle\,\| \le \|\,\mathsf{CPhsO}_B\,P\,|\psi\rangle\,\| = \|P\,|\psi\rangle\,\|$.

Now, for any $|\psi\rangle$,

$$
\begin{aligned}
&\|P\,\mathsf{CPhsO}_B\,|\psi\rangle\,\| \\
&\le \|P\,\mathsf{CPhsO}_B\,P\,|\psi\rangle\,\| + \|P\,\mathsf{CPhsO}_B\,Q\,|\psi\rangle\,\| \\
&\qquad + \|P\,\mathsf{CPhsO}_B\,R\,|\psi\rangle\,\| + \|P\,\mathsf{CPhsO}_B\,S\,|\psi\rangle\,\| \\
&\le \|P\,|\psi\rangle\,\| + 2\sqrt{p}(\|Q\,|\psi\rangle\,\| + \|R\,|\psi\rangle\,\|) \\
&\le \|P\,|\psi\rangle\,\| + 2\sqrt{2}\sqrt{p}.
\end{aligned}
$$

This shows that if $|\psi\rangle$ denotes the joint state right after qth query, then $\|P\,|\psi\rangle\,\| \le 2\sqrt{2}\sqrt{p}q$, since the internal state of the oracle is initialized as $f=\perp$, and each query can increase the value only by $2\sqrt{2}\sqrt{p}$. Then, the probability we want to bound is $\|P\,|\psi\rangle\,\|^2$, which is bounded by $8pq^2$. □

Corollary 5.2. *Let $\mathcal{X} = \{0,1\}^m$, $\mathcal{Y} = \{0,1\}$, and let B be a Bernoulli distribution over $\mathcal{Y}$. Let p be $B(1)$.*

Consider any quantum adversary A. When A makes q queries to the non-uniform quantum random oracle $h \leftarrow B^{\mathcal{X}}$ and outputs $x \in \mathcal{X}$, the probability that $h(x) = 1$ is at most $O(pq^2)$.

Proof. Let A' be another adversary which runs A internally until A outputs $x \in \mathcal{X}$, then outputs the partial function $f = \{(x, 1)\}$ of rank 1. Let R be a relation over partial functions such that $R(f)$ iff $f = \{(x, 1)\}$ for some $x \in \mathcal{X}$. Then, let us define three probabilities s, s', s'' as follows:

$$s := \mathbf{Pr}[f \leftarrow A'^{\mathsf{StQRO}_B}(); h \leftarrow \mathsf{StQRO}_B : h \supseteq f \wedge R(f)],$$
$$s' := \mathbf{Pr}[f \leftarrow A'^{\mathsf{StO}_B}(); h \leftarrow \mathsf{StO}_B : h \supseteq f \wedge R(f)],$$
$$s'' := \mathbf{Pr}[f \leftarrow A'^{\mathsf{CStO}_B}(); h \leftarrow \mathsf{CStO}_B : h \supseteq f \wedge R(f)]$$

We can see that s is the success probability of A which we want to bound. Also, due to Corollary 3.20 and Lemma 3.23, we have $s = s'$.

Then, by the recordability, we have

$$\sqrt{s'} \leq \sqrt{s''} + \sqrt{p},$$

as the relation R is p-bounded, and $r_R = 1$. Also, according to Theorem 5.1, s'' is bounded above by $8pq^2$. Combining, we have

$$s = s' \leq \left(\sqrt{8pq^2} + \sqrt{p}\right)^2 = O\big(pq^2\big). \qquad \square$$

Remark 5.3. In our Definition 4.1, we describe an oracle $\mathcal{O}'$ as recording another oracle $\mathcal{O}$ *for a particular relation* R. This is needed for this application. Here, when the Bernoulli parameter p is very small, $|0\rangle \in \mathbb{C}[\{0, 1\}]$ is very close to $|\iota_B\rangle \in \mathbb{C}[\{0, 1\}]$. Since $|\iota_B\rangle$ is 'compressed' back to $|\bot\rangle$ after each query, it is very likely that even if an adversary made a query for a point x and obtained $f(x) = 0$, that fact could be easily 'forgotten' by the compressed oracle. So, in general we may say that CPhsO_B does not 'record' PhsO_B very well. Also note that, when the codomain is $\{0, 1\}$, the min-entropy of any D over $\{0, 1\}$ must be at least 1/2.

(In comparison, this is not applicable for CStO or CPhsO of Zhandry, where D is uniform and $\{0, 1\}^n$ is exponentially large: all computational basis elements $|y\rangle$ for $y \in \{0, 1\}^n$ are almost orthogonal to $|\iota_D\rangle = 2^{-n/2} \sum_y |y\rangle$, so they are rarely forgotten.)

On the other hand, the state $|1\rangle$ is almost orthogonal to the initial state $|\iota_B\rangle$, so if the adversary 'has seen' $f(x) = 1$ for some x, *that* fact is not easily forgotten by the compressed oracle. Since we are interested in finding x with $f(x) = 1$ here, forgetting about 0 is all right. Indeed, according to Definition 4.9, our relation R is p-bounded, and CPhsO_B 'records' 1 without any problem.

Observe also that Zhandry formulated the optimality of Grover search as difficulty of finding a preimage of 0^n for a uniform random function $H : \{0, 1\}^m \to \{0, 1\}^n$. While the bound $O(q^2/2^n)$ for the uniform random function remains true trivially even for $n = 1$, Zhandry's Lemma 5, which claims one may switch from StO to CStO with penalty $r/2^n$ (where r is the rank of the partial function output by the adversary), would not work for $n = 1$, because $r/2^n$ is no longer negligible.

5.2 Collision lower bound for non-uniform random oracle

We will also prove that a non-uniform random oracle satisfies collision resistance, provided that the min-entropy is large.

Theorem 5.4. *Let $\mathcal{O}$ be either CStO_D or CPhsO_D. Then, for any adversary A interacting with $\mathcal{O}$, if $\mathcal{O}$ is measured after A makes q queries, the probability that the measurement outcome $f \leftarrow \mathcal{O}$ contains a collision, that is, $f(x) = f(x')$ for some distinct $x, x' \in \mathrm{dom}(f)$, is at most $32q^3/2^k$, where k is the min-entropy of D.*

Proof. Again, we need only to show this for CPhsO_D. Consider the joint state of the adversary and the oracle right before the jth query:

$$|\psi\rangle = \sum_{x,y,z,f} \alpha_{xyzf} |xyz\rangle \otimes |f\rangle .$$

We see that any f which occurs in the above must satisfy $|f| \le j-1$, because the oracle state is initialized as $\perp$, and each query will increase the rank of partial functions occurring in the oracle state at most by 1.

Let us define four projections P, Q, R, S as follows.

- P is the projection onto the span of $|xyzf\rangle$ where a collision exists in f.
- Q is the projection onto the span of $|xyzf\rangle$ where no collisions exist in f, $y \ne 0^n$, and $f(x) = \perp$.
- R is the projection onto the span of $|xyzf\rangle$ where no collisions exist in f, $y \ne 0^n$, and $f(x) \ne \perp$.
- S is the projection onto the span of $|xyzf\rangle$ where no collisions exist in f, and $y = 0^n$.

Clearly, $P + Q + R + S = I$.

Let us show the following.

Suppose that $|xyzf\rangle$ is in the support of Q. In that case, $f(x) = \perp$, and

$$\begin{aligned}
&P\,\mathsf{CPhsO}_D\,|xyzf\rangle \\
&= P\mathsf{swap} \circ \mathsf{query}' \circ \mathsf{swap}\,|xyzf\rangle \\
&= P\mathsf{swap} \circ \mathsf{query}'\,|xyz\rangle \otimes \sum_{y'} \sqrt{D(y')}\,|f[x \to y']\rangle \\
&= P\mathsf{swap}\,|xyz\rangle \otimes \sum_{y'} (-1)^{y \cdot y'} \sqrt{D(y')}\,|f[x \to y']\rangle \\
&= P\,|xyz\rangle \otimes \sum_{y'} (-1)^{y \cdot y'} \sqrt{D(y')} \Bigg(|f[x \to y']\rangle \\
&\qquad + \sqrt{D(y')}\,|f\rangle - \sqrt{D(y')} \sum_{y''} \sqrt{D(y'')}\,|f[x \to y'']\rangle \Bigg)
\end{aligned}$$

Since f does not contain any collision, when the projection P is applied, $|f\rangle$ will vanish, and only terms of form $|f[x \to w]\rangle$ with $w \in \mathrm{rng}(f)$ will survive. So, the above equals

$$
\begin{aligned}
&= |xyz\rangle \otimes \sum_{y' \in \mathrm{rng}(f)} (-1)^{y \cdot y'} \sqrt{D(y')}\, |f[x \to y']\rangle \\
&- |xyz\rangle \otimes \left(\sum_{y'} (-1)^{y \cdot y'} D(y') \right) \sum_{y'' \in \mathrm{rng}(f)} \sqrt{D(y'')}\, |f[x \to y'']\rangle \\
&= \sum_{y' \in \mathrm{rng}(f)} \sqrt{D(y')} \left((-1)^{y \cdot y'} - \sum_{y''} (-1)^{y \cdot y''} D(y'') \right) |xyz\rangle\, |f[x \to y']\rangle\,.
\end{aligned}
$$

So, if we write $Q\,|\psi\rangle = \sum_{xyzf} \alpha_{xyzf}\, |xyzf\rangle$, then $\|Q\,|\psi\rangle\,\|^2 = \sum_{xyzf} \|\alpha_{xyzf}\|^2$, and then

$$
\begin{aligned}
&\|P\,\mathsf{CPhsO}_D\,Q\,|\psi\rangle\,\|^2 \\
&= \sum_{xyzf} \sum_{y' \in \mathrm{rng}(f)} |\alpha_{xyzf}|^2 D(y') \left| (-1)^{y \cdot y'} - \sum_{y''} (-1)^{y \cdot y''} D(y'') \right|^2 \\
&\leq \sum_{xyzf} \sum_{y' \in \mathrm{rng}(f)} |\alpha_{xyzf}|^2 \frac{1}{2^k} \left(1 + \sum_{y''} D(y'') \right)^2 \\
&= \sum_{xyzf} |\alpha_{xyzf}|^2 \left(\sum_{y' \in \mathrm{rng}(f)} \frac{4}{2^k} \right) \leq \frac{4(j-1)}{2^k} \sum_{xyzf} |\alpha_{xyzf}|^2 \\
&= \frac{4(j-1)}{2^k} \|Q\,|\psi\rangle\,\|^2.
\end{aligned}
$$

In the above, we use the property of min-entropy in the first inequality, $\sum_{y''} D(y'') = 1$ in the equality after that. The condition $|f| \leq j-1$ is used in the last inequality.

Therefore, we have

$$
\|P\,\mathsf{CPhsO}_D\,Q\,|\psi\rangle\,\| \leq 2\sqrt{\frac{j-1}{2^k}}\|Q\,|\psi\rangle\,\|.
$$

Now, suppose that $|xyzf\rangle$ is in the support of R. In that case, $f(x) \neq \perp$, and if $w = f(x)$, then we may write f as $f = f'[x \to w]$, where $f'(x) = \perp$. We see that no collisions exist in f', and moreover $w \notin \mathrm{rng}(f')$ so that $f = f'[x \to w]$

does not have collisions. Similar computation as before gives us

$$
\begin{aligned}
&P\,\mathsf{CPhsO}_D\,|xyzf\rangle \\
&= \sqrt{D(w)} \sum_{y' \in \mathrm{rng}(f')} \Bigg(1 - (-1)^{y\cdot w} - (-1)^{y\cdot y'} \\
&\qquad + \sum_{y''} (-1)^{y\cdot y''} D(y'') \Bigg) \sqrt{D(y')}\,|xyz\rangle \otimes |f'[x \to y']\rangle\,.
\end{aligned}
$$

So, if we write $R\,|\psi\rangle = \sum_{xyzf'w} \alpha_{xyzf'w}\,|xyz\rangle\,|f'[x \to w]\rangle$, then $\|R\,|\psi\rangle\,\|^2 = \sum_{xyzf'w} |\alpha_{xyzf'w}|^2$, and then

$$
\begin{aligned}
&\|P\,\mathsf{CPhsO}_D\,R\,|\psi\rangle\,\|^2 \\
&= \sum_{xyzf'} \sum_{y' \in \mathrm{rng}(f')} D(y') \Bigg| \sum_w \alpha_{xyzf'w} \sqrt{D(w)} \\
&\qquad \Bigg(1 - (-1)^{y\cdot w} - (-1)^{y\cdot y'} + \sum_{y''} (-1)^{y\cdot y''} D(y'') \Bigg) \Bigg|^2 \\
&\le \sum_{xyzf'} \sum_{y' \in \mathrm{rng}(f')} D(y') \Bigg(\sum_w |\sqrt{D(w)}|^2 \Bigg) \\
&\qquad \sum_w \Bigg| \alpha_{xyzf'w} \Bigg(1 - (-1)^{y\cdot w} - (-1)^{y\cdot y'} + \sum_{y''} (-1)^{y\cdot y''} D(y'') \Bigg) \Bigg|^2 \\
&= \sum_{xyzf'} \sum_{y' \in \mathrm{rng}(f')} D(y') \sum_w |\alpha_{xyzf'w}|^2 \Bigg| 1 - (-1)^{y\cdot w} - (-1)^{y\cdot y'} + \sum_{y''} (-1)^{y\cdot y''} D(y'') \Bigg|^2 \\
&\le \sum_{xyzf'} \sum_{y' \in \mathrm{rng}(f')} \frac{1}{2^k} \sum_w |\alpha_{xyzf'w}|^2 \Bigg(1 + 1 + 1 + \sum_{y''} D(y'') \Bigg)^2 \\
&= \sum_{xyzf'w} |\alpha_{xyzf'w}|^2 \Bigg(\sum_{y' \in \mathrm{rng}(f')} \frac{16}{2^k} \Bigg) \\
&\le \|R\,|\psi\rangle\,\|^2\, \frac{16(j-1)}{2^k}.
\end{aligned}
$$

In the above, we have used the Cauchy-Schwarz inequality, the definition of min-entropy, and the fact that $|f'| \le |f| \le j-1$.

Therefore, we have

$$
\|P\,\mathsf{CPhsO}_D\,R\,|\psi\rangle\,\| \le 4\sqrt{\frac{j-1}{2^k}}\,\|R\,|\psi\rangle\,\|.
$$

Finally, suppose $|xyzf\rangle$ is in the support of S. So $y = 0^n$.

Then, for any f, $\mathsf{query}' |xyzf\rangle = (-1)^{y \cdot f(x)} |xyzf\rangle$. So query' acts as an identity, when restricted to the support of S. Then, $\mathsf{CPhsO}_D = \mathsf{swap} \circ \mathsf{query}' \circ \mathsf{swap} = \mathsf{swap} \circ \mathsf{swap}$, which is identity because swap is an involution. Then,

$$P\,\mathsf{CPhsO}_D\,S\,|\psi\rangle = PS\,|\psi\rangle = 0.$$

Also,

$$\|P\,\mathsf{CPhsO}_D\,P\,|\psi\rangle\,\| \leq \|\,\mathsf{CPhsO}_D\,P\,|\psi\rangle\,\| = \|P\,|\psi\rangle\,\|.$$

Now, for any $|\psi\rangle$,

$$\begin{aligned}
&\|P\,\mathsf{CPhsO}_B\,|\psi\rangle\,\| \\
&\leq \|P\,\mathsf{CPhsO}_B\,P\,|\psi\rangle\,\| + \|P\,\mathsf{CPhsO}_B\,Q\,|\psi\rangle\,\| \\
&\qquad + \|P\,\mathsf{CPhsO}_B\,R\,|\psi\rangle\,\| + \|P\,\mathsf{CPhsO}_B\,S\,|\psi\rangle\,\| \\
&\leq \|P\,|\psi\rangle\,\| + 2\sqrt{\frac{j-1}{2^k}}\|Q\,|\psi\rangle\,\| + 4\sqrt{\frac{j-1}{2^k}}\|R\,|\psi\rangle\,\| \\
&\leq \|P\,|\psi\rangle\,\| + 4\sqrt{\frac{j-1}{2^k}}(\|Q\,|\psi\rangle\,\| + \|R\,|\psi\rangle\,\|) \\
&\leq \|P\,|\psi\rangle\,\| + 4\sqrt{\frac{2(j-1)}{2^k}}.
\end{aligned}$$

This shows that if $|\psi\rangle$ denotes the joint state right after qth query, then

$$\|P\,|\psi\rangle\,\| \leq \sum_{j=1}^{q} 4\sqrt{\frac{2(j-1)}{2^k}} \leq 4q\sqrt{\frac{2q}{2^k}}$$

Then, the probability we want to bound is $\|P\,|\psi\rangle\,\|^2$, which is bounded by $32q^3/2^k$. ☐

Corollary 5.5. *Let $\mathcal{X} = \{0,1\}^m$, $\mathcal{Y} = \{0,1\}^n$, and let D be a distribution over $\mathcal{Y}$. Consider any quantum adversary A. When A makes q queries to the non-uniform quantum random oracle $h \leftarrow D^{\mathcal{X}}$ and outputs $(x, x') \in \mathcal{X}^2$, the probability that $x \neq x'$ and $h(x) = h(x')$ is at most $O(q^3/2^k)$, where k is the min-entropy of D.*

Proof. Let A' be another adversary which runs A internally until A outputs (x, x'), then making its own queries to get function values y, y' for x, x', respectively, and output the partial function $f = \{(x, y), (x', y')\}$. Then, A' makes $q + 2$ queries in total. Let R be a relation over partial functions such that $R(f)$ iff $f = \{(x, y), (x', y)\}$ for some $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that $x \neq x'$.

Let us define probabilities p, p', p'' as follows.

$$\begin{aligned}
p &:= \mathbf{Pr}[f \leftarrow A'^{\mathsf{StQRO}_D}(); h \leftarrow \mathsf{StQRO}_D : h \supseteq f \wedge R(f)], \\
p' &:= \mathbf{Pr}[f \leftarrow A'^{\mathsf{StO}_D}(); h \leftarrow \mathsf{StO}_D : h \supseteq f \wedge R(f)],
\end{aligned}$$

$$p'' := \mathbf{Pr}[f \leftarrow A'^{\mathsf{CStO}_D}(); h \leftarrow \mathsf{CStO}_D : h \supseteq f \wedge R(f)].$$

We see that p is the success probability of A which we want to bound (with two extra queries). Also, due to Corollary 3.20 and Lemma 3.23, we have $p = p'$.

Then, by the recordability, we have

$$\sqrt{p'} \leq \sqrt{p''} + \sqrt{\frac{2}{2^k}},$$

as R is trivially $1/2^k$-bounded, and $r_R = 2$. Also, according to Theorem 5.4, p'' is bounded above by $32(q+2)^3/2^k$. Combining, we have

$$p = p' \leq \left(\sqrt{\frac{32(q+2)^3}{2^k}} + \sqrt{\frac{2}{2^k}}\right)^2 = O\left(\frac{q^3}{2^k}\right). \qquad \square$$

6 Conclusion

In this paper, we have extended Zhandry's compressed oracle technique to non-uniform random oracles, and used it to prove optimality of Grover search and collision resistance of non-uniform random oracles.

It would be an interesting question how far we can generalize the compressed oracle technique to other quantum oracles. The original motivation of this work was to try to explain the compressed standard oracle as the tensor product of smaller, 'compressed point oracles', and then to prove that the compressed standard oracle records the standard oracle by showing that the tensor product preserves the (strong) recording property. For example, this might be a way to extend the compressed oracle technique to quantum ideal ciphers, whose purification would be a tensor product of purified quantum random permutations. At this point, we do not know how to implement compressed quantum permutation oracles, nor how to handle a tensor product of them. But such generalizations could be useful in many applications.

Acknowledgements Minki Hhan was supported in part by the KIAS Individual Grant QP089801, and also in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1A2C1010690). Aaram Yun was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1A2C1010690).

References

1. Aaronson, S., Shi, Y.: Quantum lower bounds for the collision and the element distinctness problems. J. ACM 51(4), 595–605 (2004)
2. Ambainis, A.: Quantum lower bounds by quantum arguments. J. Comput. Syst. Sci. 64(4), 750–767 (2002)

3. Ambainis, A.: Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. Theory Comput. 1(1), 37–46 (2005)
4. Balogh, M., Eaton, E., Song, F.: Quantum collision-finding in non-uniform random functions. In: Lange, T., Steinwandt, R. (eds.) Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Lecture Notes in Computer Science, vol. 10786, pp. 467–486. Springer (2018)
5. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM 48(4), 778–797 (2001)
6. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993. pp. 62–73. ACM (1993)
7. Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: Strengths and weaknesses of quantum computing. SIAM J. Comput. 26(5), 1510–1523 (1997)
8. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. Lecture Notes in Computer Science, vol. 7073, pp. 41–69. Springer (2011)
9. Chung, K., Fehr, S., Huang, Y., Liao, T.: On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12697, pp. 598–629. Springer (2021)
10. Chung, K., Guo, S., Liu, Q., Qian, L.: Tight quantum time-space tradeoffs for function inversion. In: Irani, S. (ed.) 61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020. pp. 673–684. IEEE (2020)
11. Cojocaru, A., Garay, J., Kiayias, A., Song, F., Wallden, P.: Quantum Multi-Solution Bernoulli Search with Applications to Bitcoin's Post-Quantum Security. Quantum 7, 944 (Mar 2023)
12. Czajkowski, J., Majenz, C., Schaffner, C., Zur, S.: Quantum lazy sampling and game-playing proofs for quantum indifferentiability. Cryptology ePrint Archive, Report 2019/428 (2019), `https://eprint.iacr.org/2019/428`
13. Ebrahimi, E., Unruh, D.: Quantum collision-resistance of non-uniformly distributed functions: upper and lower bounds. Quantum Inf. Comput. 18(15&16), 1332–1349 (2018)
14. Ebrahimi, E., Unruh, D.: Quantum collision-resistance of non-uniformly distributed functions: upper and lower bounds. Quantum Inf. Comput. 18(15&16), 1332–1349 (2018)
15. Hamoudi, Y., Magniez, F.: Quantum time-space tradeoff for finding multiple collision pairs. ACM Trans. Comput. Theory 15(1-2), 1–22 (2023)
16. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. Cryptology ePrint Archive, Paper 2015/1256 (2015), `https://eprint.iacr.org/2015/1256`

17. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C., Chung, K., Persiano, G., Yang, B. (eds.) Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9614, pp. 387–416. Springer (2016)
18. Liu, Q., Zhandry, M.: On finding quantum multi-collisions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III. Lecture Notes in Computer Science, vol. 11478, pp. 189–218. Springer (2019)
19. Targhi, E.E., Tabia, G.N., Unruh, D.: Quantum collision-resistance of non-uniformly distributed functions. In: Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. pp. 79–85 (2016)
20. Targhi, E.E., Tabia, G.N., Unruh, D.: Quantum collision-resistance of non-uniformly distributed functions. In: Takagi, T. (ed.) Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9606, pp. 79–85. Springer (2016)
21. Unruh, D.: Compressed permutation oracles (and the collision-resistance of sponge/SHA3). Cryptology ePrint Archive, Report 2021/062 (2021), `https://eprint.iacr.org/2021/062`
22. Unruh, D.: Towards compressed permutation oracles. Cryptology ePrint Archive, Paper 2023/770 (2023), `https://eprint.iacr.org/2023/770`
23. Yuen, H.: A quantum lower bound for distinguishing random functions from random permutations. Quantum Inf. Comput. 14(13-14), 1089–1097 (2014)
24. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. pp. 758–775 (2012)
25. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Information & Computation 15(7&8), 557–567 (2015)
26. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 239–268. Springer (2019)