Formations for the Quantum Random Oracle

Aaram Yun

Department of Cyber Security, Ewha Womans University, Seoul, Korea
aaramyun@ewha.ac.kr

Abstract. In the quantum random oracle model, the adversary may make quantum superposition queries to the random oracle. Since even a single query can potentially probe exponentially many points, classical proof techniques are hard to be applied. For example, recording the oracle queries seemed difficult.
In 2018, Mark Zhandry showed that, despite the apparent difficulties, it is in fact possible to 'record' the quantum queries. He has defined the compressed oracle, which is indistinguishable from the quantum random oracle, and records information the adversary has gained through the oracle queries. It is a technically subtle work, which we believe to be a challenging work to grasp fully.
Our aim is to obtain a mathematically clean, simple reinterpretation of the compressed oracle technique. For each partial function, we define what we call the *formation* and the *completion* of that partial function. The completions describe what happens to the real quantum random oracle, and the formations describe what happens to the compressed oracle. We will show that the formations are 'isomorphic' to the completions, giving an alternative proof that the compressed oracle is indistinguishable from the quantum random oracle.

Keywords: quantum random oracle, compressed oracle, oracle recording, quantum superposition query, formation, completion, partial function

1 Introduction

Classically, often it is easier to prove cryptographic security in the random oracle model 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.

On the other hand, in the quantum random oracle model, the adversary can make quantum superposition queries. Each query may potentially inspect exponentially many points, which makes recording and programming the quantum random oracle difficult, apparently.

But, surprisingly, Zhandry showed that one can in fact record the adversarial quantum random oracle queries [7]. He constructed something called a *compressed oracle*, and showed that this compressed oracle can handle quantum random oracle queries, and indeed records the queries, giving a very useful tool for proving security in the quantum random oracle model.

Zhandry's result is technically quite sophisticated. When the initial version [6] of the paper was first uploaded to ePrint archive in 2018, it was generally received with astonishment due to its powerful ideas, but it contained insufficient technical details, making it difficult to understand, use, and even to verify. Later versions added the necessary details, and the proof is now clear and easy to verify. Also, many tried to understand, reconstruct, and apply Zhandry's results to other settings and applications (e.g. [3,4,1,5,2]). But, despite all these, still we believe that it is a difficult and subtle work to grasp, and the rationale of the construction is not very well understood.

The goal of this paper is to understand Zhandry's compressed oracle technique. We may say that Zhandry's results can be considered as made of two parts.

1. *Indistinguishability*: from the adversarial point of view, the compressed oracle is indistinguishable from the quantum random oracle.
2. *Recordability*: the state of the compressed oracle 'records' information the adversary has gathered by its oracle queries.

In this paper, our main focus is on the indistinguishability. We are going to work with partial functions, and we will define what we call the *completion* and the *formation* of such a partial function. We may say that completions describe what happens to the real quantum random oracle, and formations describe what happens to the compressed oracle. We will show that once we introduce the formation of partial functions and express the compressed oracle in terms of the formation, the whole mechanics of the compressed oracle becomes isomorphic to that of the ordinary quantum random oracle. Due to this, we get an alternative proof of the indistinguishability.

Table 1 summarizes some of the basic properties of the completion and the formation.

Table 1. Comparing basic properties of completions and formations

Properties of completions	Properties of formations
(Theorem 4.4) $\mathsf{StO}\,\lvert xy\rangle \otimes \lvert p\rangle^{\mathsf{c}} = \begin{cases} \lvert x\rangle\,\lvert y \oplus p(x)\rangle \otimes \lvert p\rangle^{\mathsf{c}} & \text{if } p(x) \neq \perp, \\ \frac{1}{\sqrt{N}} \sum_z \lvert x\rangle\,\lvert y \oplus z\rangle \otimes \lvert p \cup (x,z)\rangle^{\mathsf{c}} & \text{if } p(x) = \perp. \end{cases}$	**(Theorem 6.2)** $\mathsf{CStO}\,\lvert xy\rangle \otimes \lvert p\rangle^{\mathsf{f}} = \begin{cases} \lvert x\rangle\,\lvert y \oplus p(x)\rangle \otimes \lvert p\rangle^{\mathsf{f}} & \text{if } p(x) \neq \perp, \\ \frac{1}{\sqrt{N}} \sum_z \lvert x\rangle\,\lvert y \oplus z\rangle \otimes \lvert p \cup (x,z)\rangle^{\mathsf{f}} & \text{if } p(x) = \perp. \end{cases}$
(Lemma 4.3) $\lvert p\rangle^{\mathsf{c}} = \frac{1}{\sqrt{N}} \sum_y \lvert p \cup (x,y)\rangle^{\mathsf{c}}, \qquad \text{if } p(x) = \perp.$	**(Lemma 5.10)** $\lvert p\rangle^{\mathsf{f}} = \frac{1}{\sqrt{N}} \sum_y \lvert p \cup (x,y)\rangle^{\mathsf{f}}, \qquad \text{if } p(x) = \perp.$
(Theorem 4.5) $\langle p_1 \vert p_2\rangle^{\mathsf{c}} = \begin{cases} \sqrt{\frac{1}{N^{\lvert p_1 \triangle p_2\rvert}}} & \text{if } p_1, p_2 \text{ are consistent,} \\ 0 & \text{if } p_1, p_2 \text{ are inconsistent.} \end{cases}$	**(Theorem 5.7)** $\langle p_1 \vert p_2\rangle^{\mathsf{f}} = \begin{cases} \sqrt{\frac{1}{N^{\lvert p_1 \triangle p_2\rvert}}} & \text{if } p_1, p_2 \text{ are consistent,} \\ 0 & \text{if } p_1, p_2 \text{ are inconsistent.} \end{cases}$

2 Preliminaries

2.1 Notations and conventions

For any nonnegative integer n, we define $[n]$ as the set $\{0, 1, \dots, n-1\}$. In this paper, we will consider functions and partial functions from $[M]$ to $[N]$, where M, N are exponentially large numbers. For concreteness, it would be all right to assume that $M = 2^m, N = 2^n$ for some $m, n \geq 0$.

2.2 Partial functions

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

$$\mathrm{pre}(p) := \{x \in \mathrm{dom}(p) \mid p(x) \neq \bot\}.$$

Similarly, the *image* of p is defined as

$$\mathrm{img}(p) := \{y \in \mathrm{cod}(p) \mid y \neq \bot \text{ and } y = p(x) \text{ for some } x \in \mathrm{dom}(p)\}.$$

When $\mathrm{pre}(p) = \mathrm{dom}(p)$, $p : X \rightharpoonup Y$ is called *total*, and such a total p can be written as $p : X \to Y$. When we use variables for functions, perhaps not always but often, we will use p, q, r and s to denote partial functions and f, g and h to denote total functions.

We are going to identify a partial function with its (set-theoretic) graph, which is

$$\{(x, p(x)) \mid p(x) \neq \bot\}.$$

Hence, we can apply set-theoretic operations to partial functions, and we are going to take this viewpoint extensively in this paper. For example, when p is a partial function, then $|p| = |\,\mathrm{pre}(p)|$. We are going to call this quantity $|p|$ as the *rank* of p.

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

Due to this identification of a partial function with its set-theoretic graph, the empty set $\emptyset$ also naturally denotes the empty partial function, where $\emptyset(x) = \bot$ for any x in the domain.

Also, we have $\mathrm{pre}(p) = \{x \mid \exists y, (x, y) \in p\}$, and $\mathrm{img}(p) = \{y \mid \exists x, (x, y) \in p\}$.

We can certainly form new sets $p \cup q$, $p \cap q$ from two partial functions p, q. When $p \cup q$ is again a partial function, then we say that p and q are *consistent*, meaning that $p(x) = q(x)$, whenever $p(x) \neq \bot$ and $q(x) \neq \bot$. When p and q are consistent, we denote that by $p \heartsuit q$. We say that p and q are *inconsistent* if they are not consistent. When p and q are inconsistent, we denote that as $p \not\heartsuit q$. Unlike $p \cup q$, which is a partial function only when $p \heartsuit q$, $p \cap q$ is always a partial function, the 'greatest common restriction' of p and q.

$p \triangle q$ is the *symmetric difference* of p and q, which is $(p \setminus q) \cup (q \setminus p)$. When p and q are partial functions with $p \heartsuit q$, then $p \triangle q$ is a partial function.

Let us denote the rank-1 partial function $\{(x, y)\}$ by $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$. For example, if $p : \{1, 2, 3\} \rightharpoonup \{0, 1\}$ is a partial function with $p(1) = 0, p(3) = 1$, then p can be written as $p = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \cup \left[\begin{smallmatrix} 3 \\ 1 \end{smallmatrix}\right]$. Further, if $\{x_1, \dots, x_l\} \subseteq [N]$ and $y_1, \dots, y_l \in [N]$, then we define

$$\left[\begin{smallmatrix} x_1 & \cdots & x_l \\ y_1 & \cdots & y_l \end{smallmatrix}\right] := \left[\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right] \cup \cdots \cup \left[\begin{smallmatrix} x_l \\ y_l \end{smallmatrix}\right].$$

We are going to work in the Hilbert space spanned by $|p\rangle$ for partial functions p. Let us introduce one more convention: when $p = \left[\begin{smallmatrix} x_1 & \cdots & x_l \\ y_1 & \cdots & y_l \end{smallmatrix}\right]$, the ket vector $|p\rangle$ of the partial function p, which is $\left|\left[\begin{smallmatrix} x_1 & \cdots & x_l \\ y_1 & \cdots & y_l \end{smallmatrix}\right]\right\rangle$, is further simplified notationally as

$$|p\rangle = \left|\begin{smallmatrix} x_1 & \cdots & x_l \\ y_1 & \cdots & y_l \end{smallmatrix}\right\rangle.$$

We make similar convention for the bra vectors of partial functions.

When p, q are partial functions, we will define

$$|p\rangle \ocup |q\rangle := \begin{cases} |p \cup q\rangle & \text{if } p \heartsuit q, \\ 0 & \text{if } p \not\heartsuit q. \end{cases}$$

We will make this $\ocup$ a bilinear operator, by, well, extending the above definition bilinearly. So, for example, if $p \heartsuit q$ and $p \heartsuit r$, then we have $|p\rangle \ocup (|q\rangle + |r\rangle) = |p \cup q\rangle + |p \cup r\rangle$. We call this operator as the *union product*. Note that the union product is commutative: $\phi \ocup \psi = \psi \ocup \phi$ for any vectors ϕ, ψ. This is because $|p\rangle \ocup |q\rangle = |p \cup q\rangle = |q \cup p\rangle = |q\rangle \ocup |p\rangle$, for any partial functions p, q. Similarly, the union product is associative. In other words, the union product gives the Hilbert space spanned by ket vectors of partial functions a commutative ring structure. For example, the unity element of the ring is $|\emptyset\rangle$.

3 Quantum oracles

Here we define the notion of quantum oracles formally.

Definition 3.1. *A* quantum oracle *is a tuple* $\mathcal{O} = (\mathcal{H}^I, \mathcal{H}^O, \mathsf{query}, |\mathsf{init}\rangle)$*, where* $\mathcal{H}^I$ *and* $\mathcal{H}^O$ *are Hilbert spaces called the* interface space *and the* oracle space*, respectively, and*

$$\mathsf{query} : \mathcal{H}^I \otimes \mathcal{H}^O \to \mathcal{H}^I \otimes \mathcal{H}^O$$

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

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

Definition 3.2. *Given two quantum oracles* $\mathcal{O}_1 = (\mathcal{H}_1^I, \mathcal{H}_1^O, \mathsf{query}_1, |\mathsf{init}_1\rangle)$ *and* $\mathcal{O}_2 = (\mathcal{H}_2^I, \mathcal{H}_2^O, \mathsf{query}_2, |\mathsf{init}_2\rangle)$, *a* morphism $f : \mathcal{O}_1 \to \mathcal{O}_2$ *from* $\mathcal{O}_1$ *to* $\mathcal{O}_2$ *is a tuple* $f = (f^I, f^O)$ *satisfying the following.*

1. $f^I : \mathcal{H}_1^I \to \mathcal{H}_2^I$ *and* $f^O : \mathcal{H}_1^O \to \mathcal{H}_2^O$ *are inner-product preserving linear maps. In addition, we require* f^I *to be bijective: so* f^I *is a unitary transformation.*
2. $f^O(|\mathsf{init}_1\rangle) = |\mathsf{init}_2\rangle$.
3. *The following is a commutative diagram.*

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

In other words, we have $(f^I \otimes f^O) \circ \mathsf{query}_1 = \mathsf{query}_2 \circ (f^I \otimes f^O)$.
The mappings f^I *and* f^O *are called the* converter *and the* transformer *of the morphism* f, *respectively.*

Composition of two morphisms $f_1 = (f_1^I, f_1^O) : \mathcal{O}_1 \to \mathcal{O}_2$ and $f_2 = (f_2^I, f_2^O) : \mathcal{O}_2 \to \mathcal{O}_3$ are defined obviously: $f_2 \circ f_1 = (f_2^I \circ f_1^I, f_2^O \circ f_1^O)$.

Definition 3.3. *A morphism* $f = (f^I, f^O) : \mathcal{O}_1 \to \mathcal{O}_2$ *is called an* isomorphism, *if* f^I *and* f^O *are both unitary transformations (bijective inner-product preserving linear maps).*

Remark 3.4. The definition of an isomorphism can be equivalently given by the existence of the inverse morphism.

When two oracles are isomorphic, in a sense this could mean that they are identical, mathematically. But that does not necessarily mean that they are the same in all aspects. For example, one oracle might have an efficient implementation, and the other oracle might not, even though they are isomorphic. Now, let us take a look at some examples of quantum oracles.

Example 3.5. The foremost example of a quantum oracle is the *standard oracle* StO. While the quantum random oracle is a uniform random function $H : [M] \to [N]$, Zhandry in [7] observed that it is possible to initialize the oracle with the 'uniform superposition'

$$|\mathsf{init}\rangle = \frac{1}{\sqrt{N^M}} \sum_f |f\rangle .$$

When this is measured before interacting with the adversary, we obtain the original quantum random oracle model. But due to the principle of deferred measurement, it is all right to leave it unmeasured. This purification of the quantum random oracle is called the standard oracle. More specifically, the oracle state is $\mathcal{H}^{\mathsf{t}}$, which is the Hilbert space spanned by $|f\rangle$ of all total functions $f : [M] \to [N]$, the interface space is $[M] \otimes [N]$, the query operator is defined as

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

with the initial state of the oracle as given above.

(As above example shows, we will often denote the query operator of a quantum oracle by the name of the quantum oracle itself.)

Example 3.6. Another important example is the *phase oracle* PhO. It is identical to StO in all aspects, except the query operator:

$$\mathsf{PhO}\,|x\rangle\,|u\rangle \otimes |f\rangle := (-1)^{u\cdot f(x)}\,|x\rangle\,|u\rangle \otimes |f\rangle\,.$$

Theorem 3.7. *If there exists a morphism $f : \mathcal{O}_1 \to \mathcal{O}_2$, then, for any adversary $\boldsymbol{A}$ outputting 0 or 1, there exists another adversary $\boldsymbol{B}$ such that the following holds.*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = 1] = \mathbf{Pr}[B^{\mathcal{O}_2}() = 1].$$

The proof of this easy but somewhat tedious theorem is given in the Appendix, p. 17.

Remark 3.8. Theorem 3.7 does not necessary mean that $\boldsymbol{B}$ is an efficient adversary, even when A is. But, when the converter f^I can be implemented efficiently, and if A is an efficient adversary, then $\boldsymbol{B}$ also is.

Moreover, the order of the quantification can be reversed: for any $\boldsymbol{B}$, there exists an A so that the same equality as above holds. The proof may proceed similarly.

Remark 3.9. When there is a morphism $f = (f^I, f^O)$ from $\mathcal{O}_1 = (\mathcal{H}_1^I, \mathcal{H}_1^O, \mathsf{query}_1, |\mathsf{init}_1\rangle)$ to $\mathcal{O}_2 = (\mathcal{H}_2^I, \mathcal{H}_2^O, \mathsf{query}_2, |\mathsf{init}_2\rangle)$, while the oracle space of $\mathcal{O}_2$ is $\mathcal{H}_2^O$, actually the state vector of $\mathcal{O}_2$ resides in a subspace $f^O(\mathcal{H}_1^O) \subseteq \mathcal{H}_2^O$, and the rest of the oracle space $\mathcal{H}_2^O$ is unused.

Definition 3.10. *When there exists a morphism $f = (f^I, f^O) : \mathcal{O}_1 \to \mathcal{O}_2$, where the interface spaces of $\mathcal{O}_1$ and $\mathcal{O}_2$ are the same and the converter f^I is the identity operator, 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 f is called an* embedding *of $\mathcal{O}_1$ into $\mathcal{O}_2$.*

Corollary 3.11. *Suppose that $f = (f^I, f^O)$ is an embedding from a suboracle $\mathcal{O}_1$ to its superoracle $\mathcal{O}_2$. Then, the two oracles are completely indistinguishable: for any adversary $\boldsymbol{A}$, we have*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = 1] = \mathbf{Pr}[A^{\mathcal{O}_2}() = 1].$$

Proof. When we examine the proof of Theorem 3.7, we can see that $\boldsymbol{B}$ is the same adversary as $\boldsymbol{A}$, as f^I is the identity operator. □

The following is a well-known result, merely translated in this language.

Theorem 3.12. StO *and* PhO *are isomorphic quantum oracles.*

Proof. The isomorphism $f = (f^I, f^O)$ from StO to PhO is simple: f^O is the identity operator, and $f^I\,|x\rangle\,|y\rangle := |x\rangle\,H^{\otimes n}\,|y\rangle$, where $H^{\otimes n}$ is the Hadamard transformation. It can be easily verified that this f is an isomorphism between StO and PhO. □

Remark 3.13. Since the converter of the isomorphism between StO and PhO is not the identity, obviously they are not indistinguishable oracles.

4 Completion of a partial function

We will consider ourselves with partial functions $[M] \rightharpoonup [N]$.

Definition 4.1. *When $p : [M] \rightharpoonup [N]$ is a partial function, we define its* completion $\lvert p\rangle^{\mathsf{c}}$ *as follows.*

$$\lvert p\rangle^{\mathsf{c}} := \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} \lvert f\rangle$$

where the running variable f is over total functions $f : [M] \to [N]$ whose restriction is p.

We call $\lvert p\rangle^{\mathsf{c}}$ the completion of p, because it is a linear combination of all possible ‘completions’ of p to total functions, scaled to be a unit vector.

We can consider the corresponding ‘bra’ vector $\langle p\rvert^{\mathsf{c}}$, and form the inner product $\langle p\rvert^{\mathsf{c}}\lvert q\rangle^{\mathsf{c}}$. Abbreviating and simplifying this ugly notation, we will write the inner product as $\langle p|q\rangle^{\mathsf{c}}$. Note that this notation will *never* be used for denoting the product of the simple bra vector $\langle p\rvert$ and the completion $\lvert q\rangle^{\mathsf{c}}$. (For many cases, that does not even make sense, because $\lvert q\rangle^{\mathsf{c}}$ is a linear combination of kets of total functions, while $\langle p\rvert$ is a bra vector of a partial function. But, when p is total, we will have to use $(\langle p\rvert)\lvert q\rangle^{\mathsf{c}}$ or $\langle p\rvert\ \lvert q\rangle^{\mathsf{c}}$, unfortunately.)

Intuitively, we may say that the completion $\lvert p\rangle^{\mathsf{c}}$ of a partial function represents the state of the oracle where values corresponding to the partial function p is determined, and the rest is completely undetermined.

Example 4.2. We have

$$\lvert \emptyset\rangle^{\mathsf{c}} = \frac{1}{\sqrt{N^M}} \sum_{f} \lvert f\rangle .$$

So, the completion of the empty partial function is the ‘uniform superposition’ of all total functions, which is the initial state of both StO and PhO.

Here is a very basic fact about the completion.

Lemma 4.3. *For any partial function $p : [M] \rightharpoonup [N]$, if $p(x) = \bot$, we have*

$$\lvert p\rangle^{\mathsf{c}} = \frac{1}{\sqrt{N}} \sum_{y \in [N]} \left\lvert p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \right\rangle^{\mathsf{c}}.$$

Proof. We have

$$\begin{aligned} \lvert p\rangle^{\mathsf{c}} &= \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} \lvert f\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{y \in [N]} \frac{1}{\sqrt{N^{M-|p|-1}}} \sum_{f \supseteq p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]} \lvert f\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{y \in [N]} \left\lvert p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \right\rangle^{\mathsf{c}}. \end{aligned}$$

□

We can express the evolution of the random oracle state by completions of partial functions. The next theorem describes this precisely. The proof can be obtained by straightforward manipulation of the definition, which will be given in the Appendix, p. 18.

Theorem 4.4. *For any partial function $p : [M] \rightharpoonup [N]$, we have*

$$\mathsf{StO}\,|xy\rangle \otimes |p\rangle^{\mathsf{c}} = \begin{cases} |x\rangle\,|y \oplus p(x)\rangle \otimes |p\rangle^{\mathsf{c}} & \text{if } p(x) \neq \bot, \\ \dfrac{1}{\sqrt{N}} \displaystyle\sum_{z \in [N]} |x\rangle\,|y \oplus z\rangle \otimes \left|p \cup \left[\begin{smallmatrix} x \\ z \end{smallmatrix}\right]\right\rangle^{\mathsf{c}} & \text{if } p(x) = \bot. \end{cases}$$

So, we can see that completions can be used to describe the state of the standard oracle. In fact, while in the definition of StO and PhO, the oracle space is given as $\mathcal{H}^{\mathsf{t}}$, the Hilbert space which is the span of all $|f\rangle$ for total functions $f : [M] \to [N]$, the state vector stays in the proper subspace spanned by the completions $|p\rangle^{\mathsf{c}}$.

Therefore, let us define RStO, which is the *restricted standard oracle*, whose oracle space is $\mathcal{H}^{\mathsf{c}}$, which is the span of all completions $|p\rangle^{\mathsf{c}}$ of partial functions $p : [M] \rightharpoonup [N]$, and the query operator is given as in Theorem 4.4. This is a suboracle of StO, with an obvious embedding ι : RStO → StO, whose transformer is the inclusion map $\mathcal{H}^{\mathsf{c}} \hookrightarrow \mathcal{H}^{\mathsf{t}}$. By Corollary 3.11, RStO and StO are completely indistinguishable.

Completions of partial functions are not in general orthogonal to each other. Let us compute their inner products.

Theorem 4.5. *For any partial functions p_1, p_2, we have*

$$\langle p_1 | p_2 \rangle^{\mathsf{c}} = \begin{cases} \sqrt{\dfrac{1}{N^{|p_1 \triangle p_2|}}} & \text{if } p_1 \heartsuit p_2, \\ 0 & \text{if } p_1 \not\heartsuit p_2. \end{cases}$$

Proof. For any two partial functions p_1, p_2, we have

$$\begin{aligned} \langle p_1 | p_2 \rangle^{\mathsf{c}} &= \frac{1}{\sqrt{N^{M-|p_1|}}\sqrt{N^{M-|p_2|}}} \sum_{\substack{f_1 \supseteq p_1 \\ f_2 \supseteq p_2}} \langle f_1 | f_2 \rangle \\ &= \frac{1}{\sqrt{N^{M-|p_1|}}\sqrt{N^{M-|p_2|}}} \sum_{f \supseteq p_1 \cup p_2} \langle f | f \rangle \end{aligned}$$

So, if $p_1 \not\heartsuit p_2$, then $\langle p_1 | p_2 \rangle^{\mathsf{c}} = 0$.

On the other hand, if $p_1 \heartsuit p_2$, then $p_1 \cup p_2$ is a partial function, and

$$\begin{aligned} \langle p_1 | p_2 \rangle^{\mathsf{c}} &= \frac{1}{\sqrt{N^{M-|p_1|}}\sqrt{N^{M-|p_2|}}} \sum_{f \supseteq p_1 \cup p_2} \langle f | f \rangle \\ &= \frac{N^{M-|p_1 \cup p_2|}}{\sqrt{N^{M-|p_1|}}\sqrt{N^{M-|p_2|}}} = \sqrt{\frac{N^{|p_1|+|p_2|}}{N^{2|p_1 \cup p_2|}}} = \sqrt{\frac{N^{|p_1 \cap p_2|}}{N^{|p_1 \cup p_2|}}} \\ &= \sqrt{\frac{1}{N^{|p_1 \triangle p_2|}}}. \end{aligned}$$

□

Since the oracle state of the standard oracle can be represented by completions of the partial functions, we may hope that we can manipulate, or even record the completions by manipulating the partial functions. In a sense, that is true. But there are obvious differences between how partial functions behave and how their completions behave. For one thing, $\langle p_1|p_2\rangle = 0$ whenever $p_1 \neq p_2$, even when p_1 and p_2 are consistent so $\langle p_1|p_2\rangle^{\mathrm{c}} \neq 0$.

Therefore, for each partial function p, we need to construct something which behaves similar to $|p\rangle^{\mathrm{c}}$. We are going to do that in the next section.

5 Formation of a partial function

Definition 5.1. *Suppose* $p : [M] \rightharpoonup [N]$ *is a partial function. We define its* formation*,* $|p\rangle^{\mathrm{f}}$ *as follows.*

$$|p\rangle^{\mathrm{f}} := \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_{\mathrm{pre}(q)\subseteq\mathrm{pre}(p)} (1-N)^{|p\cap q|}\left(-\frac{1}{\sqrt{N}}\right)^{|q|} |q\rangle\,.$$

Here, q runs over all possible partial functions $q : [M] \rightharpoonup [N]$ with $\mathrm{pre}(q) \subseteq \mathrm{pre}(p)$*.*

Similar to completions, we will write the inner product of formations as $\langle p|q\rangle^{\mathrm{f}}$.

We will soon see that the formation $|p\rangle^{\mathrm{f}}$ 'behaves' essentially the same as the completion $|p\rangle^{\mathrm{c}}$. But first, let us have some examples.

Example 5.2. For the empty partial function $\emptyset$, if $\mathrm{pre}(q) \subseteq \mathrm{pre}(\emptyset)$, then $q = \emptyset$. So,

$$|\emptyset\rangle^{\mathrm{f}} = \left(\frac{1}{\sqrt{N}}\right)^{|\emptyset|}(1-N)^{|\emptyset|}\left(-\frac{1}{\sqrt{N}}\right)^{|\emptyset|}|\emptyset\rangle = |\emptyset\rangle\,.$$

Example 5.3. For any rank-1 partial function $\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]$, we have

$$\begin{aligned}
\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle^{\mathrm{f}} = \left(\frac{1}{\sqrt{N}}\right)^{1}\Bigg((1-N)^{1}&\left(-\frac{1}{\sqrt{N}}\right)^{1}\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle \\
&+ (1-N)^{0}\left(-\frac{1}{\sqrt{N}}\right)^{0}|\emptyset\rangle \\
&+ \sum_{z\neq y}(1-N)^{\left|\left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\cap\left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right|}\left(-\frac{1}{\sqrt{N}}\right)^{1}\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle\Bigg) \\
= \frac{1}{\sqrt{N}}\Bigg((1-N)&\left(-\frac{1}{\sqrt{N}}\right)\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle + |\emptyset\rangle + \sum_{z\neq y}\left(-\frac{1}{\sqrt{N}}\right)\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle\Bigg) \\
= \left(1-\frac{1}{N}\right)&\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}}|\emptyset\rangle - \frac{1}{N}\sum_{z\neq y}\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle \\
= \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle &+ \frac{1}{\sqrt{N}}|\emptyset\rangle - \frac{1}{N}\sum_{z}\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle.
\end{aligned}$$

In fact, we can decompose the formation using the union product.

Theorem 5.4. *Suppose $p_1, p_2 : [M] \rightharpoonup [N]$ are arbitrary partial functions with disjoint preimages:* $\mathrm{pre}(p_1) \cap \mathrm{pre}(p_2) = \emptyset$. *Then,*

$$|p_1 \cup p_2\rangle^{\mathsf{f}} = |p_1\rangle^{\mathsf{f}} \circledcup |p_2\rangle^{\mathsf{f}}.$$

Proof. When p_1 and p_2 have disjoint preimages, then any partial function q with $\mathrm{pre}(q) \subseteq \mathrm{pre}(p_1 \cup p_2)$ can be uniquely written as $q = q_1 \cup q_2$, with $\mathrm{pre}(q_1) \subseteq \mathrm{pre}(p_1)$ and $\mathrm{pre}(q_2) \subseteq \mathrm{pre}(p_2)$. So,

$$\begin{aligned}
|p_1 \cup p_2\rangle^{\mathsf{f}} &= \left(\frac{1}{\sqrt{N}}\right)^{|p_1 \cup p_2|} \sum_{q_1,q_2} (1-N)^{|(p_1\cup p_2)\cap(q_1\cup q_2)|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_1 \cup q_2|} |q_1 \cup q_2\rangle \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|+|p_2|} \sum_{q_1,q_2} (1-N)^{|p_1\cap q_1|+|p_2\cap q_2|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_1|+|q_2|} |q_1\rangle \circledcup |q_2\rangle \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|} \left(\sum_{q_1} (1-N)^{|p_1\cap q_1|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_1|} |q_1\rangle\right) \\
&\qquad \circledcup \left(\frac{1}{\sqrt{N}}\right)^{|p_2|} \left(\sum_{q_2} (1-N)^{|p_2\cap q_2|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_2|} |q_2\rangle\right) \\
&= |p_1\rangle^{\mathsf{f}} \circledcup |p_2\rangle^{\mathsf{f}}.
\end{aligned}$$

□

Corollary 5.5. *Suppose $p : [M] \rightharpoonup [N]$ is any partial function and $p(x) = \bot$. Then, for any $y \in [N]$, we have*

$$\left|p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]\right\rangle^{\mathsf{f}} = |p\rangle^{\mathsf{f}} \circledcup \left(\left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}} |\emptyset\rangle - \frac{1}{N} \sum_{z\in[N]} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right).$$

Corollary 5.6. *Suppose $p : [M] \rightharpoonup [N]$ is a partial function. Then, we have*

$$|p\rangle^{\mathsf{f}} = \bigcircledcup_{x\in\mathrm{pre}(p)} \left(\left|\begin{smallmatrix} x \\ p(x) \end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}} |\emptyset\rangle - \frac{1}{N} \sum_{z\in[N]} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right).$$

It turns out that formations of partial functions give us the correct inner product.

Theorem 5.7. *For any partial functions p_1, p_2, we have*

$$\langle p_1|p_2\rangle^{\mathsf{f}} = \begin{cases} \sqrt{\dfrac{1}{N^{|p_1 \triangle p_2|}}} & \text{if } p_1 \heartsuit p_2, \\ 0 & \text{if } p_1 \not\heartsuit p_2. \end{cases}.$$

Especially, we have $\langle p_1|p_2\rangle^{\mathsf{f}} = \langle p_1|p_2\rangle^{\mathsf{c}}$.

The proof of Theorem 5.7 can be obtained by combinatorial arguments and multiple applications of the binomial theorem, which will be given in the Appendix, p. 19.

Now, let us define a few more Hilbert spaces. Let $\mathcal{H}^{\mathrm{p}}$ be the Hilbert space spanned by $|p\rangle$ of partial functions p. And let $\mathcal{H}^{\mathrm{f}}$ be the Hilbert space spanned by the formations $|p\rangle\!\rangle^{\mathrm{f}}$ of partial functions.

Recall that we have already defined $\mathcal{H}^{\mathrm{c}}$ and $\mathcal{H}^{\mathrm{t}}$. $\mathcal{H}^{\mathrm{c}}$ is the Hilbert space spanned by the completions $|p\rangle\!\rangle^{\mathrm{c}}$, and $\mathcal{H}^{\mathrm{t}}$ is the Hilbert space spanned by $|f\rangle$ of total functions f.

We want to relate formations and completions. For this, we need to define the formation and the completion as linear mappings.

Let us define the linear mapping $\mathrm{K} : \mathcal{H}^{\mathrm{f}} \to \mathcal{H}^{\mathrm{c}}$ by first defining $\mathrm{K}\,|p\rangle := |p\rangle\!\rangle^{\mathrm{c}}$ for any partial function p, and then extending K linearly to all linear combinations of partial functions. (And then restricting the resulting mapping $\mathrm{K} : \mathcal{H}^{\mathrm{p}} \to \mathcal{H}^{\mathrm{c}}$ to $\mathcal{H}^{\mathrm{f}}$.) Similarly, let us define $\Phi : \mathcal{H}^{\mathrm{p}} \to \mathcal{H}^{\mathrm{p}}$ by first defining $\Phi\,|p\rangle := |p\rangle\!\rangle^{\mathrm{f}}$ for any partial function p, and extending Φ linearly to all linear combinations of partial functions.

Theorem 5.8. *For any partial function p, we have*

$$\mathrm{K}|p\rangle\!\rangle^{\mathrm{f}} = |p\rangle\!\rangle^{\mathrm{c}}$$

and

$$\Phi|p\rangle\!\rangle^{\mathrm{f}} = |p\rangle\!\rangle^{\mathrm{f}}.$$

The proof of Theorem 5.8 is again based on combinatorial arguments and the binomial theorem, which will be given in the Appendix, p. 21.

Corollary 5.9. *The linear mapping* $\mathrm{K} : \mathcal{H}^{\mathrm{f}} \to \mathcal{H}^{\mathrm{c}}$ *is an isomorphism of the Hilbert spaces: it is a unitary transformation, so it preserves the inner product and is bijective. For any partial function p, the mapping* K *satisfies*

$$\mathrm{K}|p\rangle\!\rangle^{\mathrm{f}} = |p\rangle\!\rangle^{\mathrm{c}},$$

and the inverse mapping K^{-1} *satisfies*

$$\mathrm{K}^{-1}|p\rangle\!\rangle^{\mathrm{c}} = |p\rangle\!\rangle^{\mathrm{f}}.$$

Also, $\Phi : \mathcal{H}^{\mathrm{p}} \to \mathcal{H}^{\mathrm{p}}$ *is a projection onto the subspace* $\mathcal{H}^{\mathrm{f}}$.

Proof. Theorem 5.7 and Theorem 4.5 immediately implies that K preserves inner product. As for the injectivity, suppose $\sum_p \alpha_p |p\rangle\!\rangle^{\mathrm{f}} \in \ker(\mathrm{K})$. Then,

$$\mathrm{K}\left(\sum_p \alpha_p |p\rangle\!\rangle^{\mathrm{f}}\right) = \sum_p \alpha_p |p\rangle\!\rangle^{\mathrm{c}} = 0.$$

Then, for any partial function q, we have

$$\begin{aligned} 0 &= \langle q|^{\mathsf{c}}\left(\sum_p \alpha_p |p\rangle^{\mathsf{c}}\right) \\ &= \sum_p \alpha_p \langle q|p\rangle^{\mathsf{c}} \\ &= \sum_p \alpha_p \langle q|p\rangle^{\mathsf{f}} \\ &= \langle q|^{\mathsf{f}}\left(\sum_p \alpha_p |p\rangle^{\mathsf{f}}\right). \end{aligned}$$

Since this holds for any $\langle q|^{\mathsf{f}}$, we have $\sum_p \alpha_p |p\rangle^{\mathsf{f}} = 0$ in $\mathcal{H}^{\mathsf{f}}$.

Finally, the surjectivity directly comes from the definition of $\mathcal{H}^{\mathsf{f}}$ and $\mathcal{H}^{\mathsf{c}}$. □

The formation also satisfies the same identity as the completion. Compare the following Lemma 5.10 with Lemma 4.3.

Lemma 5.10. *For any partial function $p : [M] \rightharpoonup [N]$, if $p(x) = \bot$, then we have*

$$|p\rangle^{\mathsf{f}} = \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|p \cup \begin{bmatrix} x \\ y \end{bmatrix}\right\rangle^{\mathsf{f}}.$$

Proof. This can in fact be proved by direct computation, but we may use the isomorphism K to 'lift' Lemma 4.3 to $\mathcal{H}^{\mathsf{f}}$ as follows. We have

$$\begin{aligned} &\mathrm{K}\left(|p\rangle^{\mathsf{f}} - \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|p \cup \begin{bmatrix} x \\ y \end{bmatrix}\right\rangle^{\mathsf{f}}\right) \\ &= |p\rangle^{\mathsf{c}} - \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|p \cup \begin{bmatrix} x \\ y \end{bmatrix}\right\rangle^{\mathsf{c}} \\ &= 0 \end{aligned}$$

So, $|p\rangle^{\mathsf{f}} - \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|p \cup \begin{bmatrix} x \\ y \end{bmatrix}\right\rangle^{\mathsf{f}} \in \ker(\mathrm{K})$. Since K is an isomorphism, $\ker(\mathrm{K}) = 0$. Therefore we get

$$|p\rangle^{\mathsf{f}} - \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|p \cup \begin{bmatrix} x \\ y \end{bmatrix}\right\rangle^{\mathsf{f}} = 0.$$ □

We will also provide an alternative proof based on direct computation in the Appendix, p. 25.

Remark 5.11. Due to the isomorphism K, we may observe that Lemma 4.3 can be generalized further: for any linear relation between completions, there is a corresponding linear relation between formations, and vice versa.

6 Formation and the quantum random oracle

Recall that Zhandry defines the compressed standard oracle query operation CStO as

$$\mathsf{CStO} := \mathsf{decomp} \circ \mathsf{CStO}' \circ \mathsf{decomp}.$$

Here, $\mathsf{CStO}' \left|xy\right\rangle \otimes \left|p\right\rangle = \left|x\right\rangle \left|y \oplus p(x)\right\rangle \otimes \left|p\right\rangle$ for any partial function p. Note that when $p(x) = \perp$, by definition $y \oplus p(x) = y \oplus \perp = y$. Also, decomp, 'decompression', is defined as[1]

$$\mathsf{decomp} \left|xy\right\rangle \otimes \left|p\right\rangle = \left|xy\right\rangle \otimes \mathsf{decomp}_x \left|p\right\rangle,$$

and, finally we need only to define decomp_x for each x.

When $p(x) = \perp$, it is defined as

$$\mathsf{decomp}_x \left|p\right\rangle = \frac{1}{\sqrt{N}} \sum_{y \in [N]} \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle.$$

The rest of the cases are given as follows[2]: when $p'(x) = \perp$,

$$\mathsf{decomp}_x \left(\frac{1}{\sqrt{N}} \sum_y (-1)^{z \cdot y} \left|p' \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle \right) := \frac{1}{\sqrt{N}} \sum_y (-1)^{z \cdot y} \left|p' \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle \quad \text{for } z \neq 0.$$

$$\mathsf{decomp}_x \left(\frac{1}{\sqrt{N}} \sum_y \left|p' \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle \right) := \left|p'\right\rangle.$$

For our purposes, there are three things to mention about the decomp_x operator. More details can be found at [7].

1. It is a well-defined unitary operator.
2. It is an involution: $\mathsf{decomp}_x \circ \mathsf{decomp}_x$ is the identity operator.
3. It can be easily checked that, when $p(x) = \perp$,

$$\mathsf{decomp}_x \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle = \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle + \frac{1}{\sqrt{N}} \left|p\right\rangle - \frac{1}{N} \sum_{z \in [N]} \left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle.$$

This form turns out to be more useful to us than the form in the original definition.

Now, we see that the decompression has a very clean form when expressed in terms of the formation.

Lemma 6.1. *For any partial function p, we have*

$$\mathsf{decomp}_x \left|p\right\rangle^{\mathsf{f}} = \begin{cases} \dfrac{1}{\sqrt{N}} \displaystyle\sum_{y \in [N]} \left|p\right\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle, & \textit{if } p(x) = \perp, \\ \left|p \setminus \left[\begin{smallmatrix}x\\p(x)\end{smallmatrix}\right]\right\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix}x\\p(x)\end{smallmatrix}\right\rangle, & \textit{if } p(x) \neq \perp. \end{cases}$$

[1] Zhandry's original notation in [7] was $\mathsf{StdDecomp}$.

[2] Zhandry in [7] considers some implementational details, so defines an additional operator $\mathsf{Increase}$. We work at a slightly more abstract level of partial functions instead of databases, so we will omit that.

Also, when $p(x) = \bot$, then

$$\mathsf{decomp}_x\left(|p\rangle^{\mathsf{f}} \mathbin{\textcircled{$\cup$}} \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle\right) = \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle^{\mathsf{f}}.$$

Proof. When $p(x) = \bot$, we know

$$\mathsf{decomp}_x\left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle = \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle + \frac{1}{\sqrt{N}}\,|p\rangle - \frac{1}{N}\sum_{z\in[N]}\left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle.$$

Note that this identity can be conveniently expressed using the union product.

$$\mathsf{decomp}_x\left(|p\rangle \mathbin{\textcircled{$\cup$}} \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle\right) = |p\rangle \mathbin{\textcircled{$\cup$}} \left(\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}}\,|\emptyset\rangle - \frac{1}{N}\sum_{z\in[N]}\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle\right).$$

Because this applies to any p with $p(x) = \bot$, and because if $p(x) = \bot$ and $\mathrm{pre}(q) \subseteq \mathrm{pre}(p)$ then $q(x) = \bot$, we have

$$\begin{aligned}\mathsf{decomp}_x\left(|p\rangle^{\mathsf{f}} \mathbin{\textcircled{$\cup$}} \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle\right) &= |p\rangle^{\mathsf{f}} \mathbin{\textcircled{$\cup$}} \left(\left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}}\,|\emptyset\rangle - \frac{1}{N}\sum_{z\in[N]}\left|\begin{smallmatrix}x\\z\end{smallmatrix}\right\rangle\right)\\ &= \left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle^{\mathsf{f}}.\end{aligned}$$

This proves the last identity. Now, since decomp_x is an involution, we have

$$\mathsf{decomp}_x\left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle^{\mathsf{f}} = |p\rangle^{\mathsf{f}} \mathbin{\textcircled{$\cup$}} \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle.$$

This proves the second case of the first identity. Finally, the first case can be proved by using Lemma 5.10:

$$\begin{aligned}\mathsf{decomp}_x\,|p\rangle^{\mathsf{f}} &= \mathsf{decomp}_x\,\frac{1}{\sqrt{N}}\sum_{y\in[N]}\left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle^{\mathsf{f}}\\ &= \frac{1}{\sqrt{N}}\sum_{y\in[N]}\mathsf{decomp}_x\left|p \cup \left[\begin{smallmatrix}x\\y\end{smallmatrix}\right]\right\rangle^{\mathsf{f}}\\ &= \frac{1}{\sqrt{N}}\sum_{y\in[N]}|p\rangle^{\mathsf{f}} \mathbin{\textcircled{$\cup$}} \left|\begin{smallmatrix}x\\y\end{smallmatrix}\right\rangle.\end{aligned}$$

□

The following Theorem 6.2 shows that the behavior of $|p\rangle^{\mathsf{f}}$ with respect to CStO is exactly the same as the behavior of $|p\rangle^{\mathsf{c}}$ with respect to StO.

Theorem 6.2. *For any partial function $p : [M] \rightharpoonup [N]$, we have*

$$\mathsf{CStO}\,|xy\rangle \otimes |p\rangle^{\mathsf{f}} = \begin{cases} |x\rangle\,|y \oplus p(x)\rangle \otimes |p\rangle^{\mathsf{f}} & \text{if } p(x) \neq \bot,\\ \dfrac{1}{\sqrt{N}}\displaystyle\sum_{z\in[N]}|x\rangle\,|y \oplus z\rangle \otimes \left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle^{\mathsf{f}} & \text{if } p(x) = \bot.\end{cases}$$

Proof. Let us prove the first case. When $p(x) \neq \bot$, let p' be defined as $p' = p \setminus \left[\begin{smallmatrix} x \\ p(x) \end{smallmatrix}\right]$. Then,

$$\begin{aligned}
\mathsf{CStO}\,|xy\rangle \otimes |p\rangle^{\mathsf{f}} &= \mathsf{decomp}\,\mathsf{CStO}'\,\mathsf{decomp}\,|xy\rangle \otimes |p\rangle^{\mathsf{f}} \\
&= \mathsf{decomp}\,\mathsf{CStO}'\,|xy\rangle \otimes \ |p'\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix} x \\ p(x) \end{smallmatrix}\right\rangle \\
&= \mathsf{decomp}\,|x\rangle\,|y \oplus p(x)\rangle \otimes \ |p'\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix} x \\ p(x) \end{smallmatrix}\right\rangle \\
&= |x\rangle\,|y \oplus p(x)\rangle \otimes \left|p' \cup \left[\begin{smallmatrix} x \\ p(x) \end{smallmatrix}\right]\right\rangle^{\mathsf{f}} \\
&= |x\rangle\,|y \oplus p(x)\rangle \otimes |p\rangle^{\mathsf{f}}.
\end{aligned}$$

Now, as for the second case, when $p(x) = \bot$,

$$\begin{aligned}
\mathsf{CStO}\,|xy\rangle \otimes |p\rangle^{\mathsf{f}} &= \mathsf{decomp}\,\mathsf{CStO}'\,\mathsf{decomp}\,|xy\rangle \otimes |p\rangle^{\mathsf{f}} \\
&= \mathsf{decomp}\,\mathsf{CStO}'\,|xy\rangle \otimes \frac{1}{\sqrt{N}} \sum_z |p\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \\
&= \frac{1}{\sqrt{N}} \sum_z \mathsf{decomp}\,|x\rangle\,|y \oplus z\rangle \otimes \ |p\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{z \in [N]} |x\rangle\,|y \oplus z\rangle \otimes \left|p \cup \left[\begin{smallmatrix} x \\ z \end{smallmatrix}\right]\right\rangle^{\mathsf{f}}. \qquad \square
\end{aligned}$$

Remark 6.3. In Lemma 6.1 and Theorem 6.2, we can see that the operator decomp_x decompresses the formation $|p\rangle^{\mathsf{f}}$ into the form $|p'\rangle^{\mathsf{f}} \circledcup \left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle$ which is amenable for querying, and later compresses it back to the formation $|p\rangle^{\mathsf{f}}$, for correct entanglement and adversarial computation.

Remark 6.4. We may observe an interesting feature of the CStO oracle: while it is necessary to extend the XOR operation to define $y \oplus \bot = y$, in order to define CStO as a unitary operator, the above analysis shows that in fact, despite all quantum superpositions, that degenerate case *never* happens. Hence, the only reason why the definition $y \oplus \bot = y$ is needed is purely for implementation.

At the same time, this is to be expected in the light of the isomorphism, because, due to Theorem 6.2 and Theorem 4.4, we have $\mathsf{CStO} = (I \otimes \mathrm{K}^{-1}) \circ \mathsf{StO} \circ (I \otimes \mathrm{K})$, and the degenerate case $y \oplus \bot = y$ never happens for StO, obviously.

Based on the above, let us define the compressed standard oracle CStO formally as a quantum oracle. It is

$$\Big([M] \otimes [N], \mathcal{H}^{\mathsf{f}}, \mathsf{CStO}, |\emptyset\rangle^{\mathsf{f}}\Big).$$

7 Indistinguishability of the compressed oracle

We may observe the following:

Theorem 7.1. *There exists an isomorphic embedding from the compressed standard oracle* CStO *to the restricted standard oracle* RStO.

Proof. The embedding is simply (I, K). Theorem 4.4 and Theorem 6.2 show that the query operators of both oracles have the identical form. Corollary 5.9 shows that the mapping K is a unitary transformation which maps the formation to the corresponding completion. We can verify that the morphism (I, K) is indeed an isomorphism and an embedding. □

Now, we are ready to prove the indistinguishability of the compressed standard oracle.

Theorem 7.2. *The compressed standard oracle* CStO *is completely indistinguishable from the standard oracle* StO*.*

Proof. This is essentially a corollary: since CStO is a suboracle of RStO, and RStO is a suboracle of StO, it follows that CStO is a suboracle of StO. Then the indistinguishability directly follows from Corollary 3.11. □

Remark 7.3. In the standard oracle of Zhandry, the uniform distribution of the quantum random oracle is purified to the 'uniform superposition' $|\emptyset\rangle^{\mathsf{c}} = N^{-M} \sum_f |f\rangle$, which can be efficiently implemented by the formation $|\emptyset\rangle^{\mathsf{f}} = |\emptyset\rangle$. We can observe that any non-uniform distribution of the oracle which can be purified and then efficiently implemented by a linear combination of formations can be 'compressed', exactly like the case of the uniform distribution.

8 Conclusion

The goal of this paper is to understand Zhandry's compressed oracle technique. While Zhandry's construction and the proof is simple and straightforward, still it is a very subtle and technically demanding work. We believe that our viewpoint in terms of the formation of a partial function is a natural way to understand the compressed oracle, and could be potentially useful in applying the technique and extending it to other settings.

Acknowledgements This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2021R1A2C1010690). The author would like to thank Minki Hhan for many fruitful discussions on the quantum random oracle.

References

1. Chung, K.M., Fehr, S., Huang, Y.H., Liao, T.N.: On the compressed-oracle technique, and post-quantum security of proofs of sequential work. Cryptology ePrint Archive, Report 2020/1305 (2020), `https://eprint.iacr.org/2020/1305`
2. Czajkowski, J.: Quantum indifferentiability of SHA-3. Cryptology ePrint Archive, Report 2021/192 (2021), `https://eprint.iacr.org/2021/192`
3. 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`

4. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I. Lecture Notes in Computer Science, vol. 11921, pp. 145–174. Springer (2019)
5. 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`
6. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. Cryptology ePrint Archive, Report 2018/276 (2018), `https://eprint.iacr.org/2018/276`, the original ePrint Archive version
7. 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)

A Missing proofs

Theorem 3.7. *If there exists a morphism $f : \mathcal{O}_1 \to \mathcal{O}_2$, then, for any adversary A outputting 0 or 1, there exists another adversary B such that the following holds.*

$$\mathbf{Pr}[A^{\mathcal{O}_1}() = 1] = \mathbf{Pr}[B^{\mathcal{O}_2}() = 1].$$

Proof. Suppose $\mathcal{O}_1 = (\mathcal{H}_1^I, \mathcal{H}_1^O, \mathsf{query}_1, |\mathsf{init}_1\rangle)$, $\mathcal{O}_2 = (\mathcal{H}_2^I, \mathcal{H}_2^O, \mathsf{query}_2, |\mathsf{init}_2\rangle)$, and a morphism $f = (f^I, f^O)$ 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 $U_i : \mathcal{H}^P \otimes \mathcal{H}_1^I \to \mathcal{H}^P \otimes \mathcal{H}_1^I$ for $i = 0, \dots, t$, with the initial state $|\mathsf{init}_1^P\rangle \otimes |\mathsf{init}_1^I\rangle \in \mathcal{H}^P \otimes \mathcal{H}_1^I$. Also assume that the final output of A is obtained by a projective measurement with respect to an orthogonal set of projectors $\{P_0, P_1\}$ on $\mathcal{H}^P \otimes \mathcal{H}_1^I$.

Then, let U_i' be the unitary operator defined by $(I \otimes f^I) \circ U_i \circ (I \otimes (f^I)^\dagger)$. Also, we define two projectors $\bar{P}_0, \bar{P}_1$ on $\mathcal{H}^P \otimes \mathcal{H}_2^I$ by $\bar{P}_b := (I \otimes f^I) \circ P_b \circ (I \otimes (f^I)^\dagger)$ for $b = 0, 1$.

Now, let B be the adversary with the sequence $U_0', \dots, U_t'$, and the initial state $|\mathsf{init}_2^P\rangle \otimes |\mathsf{init}_2^I\rangle$, where $|\mathsf{init}_2^P\rangle = |\mathsf{init}_1^P\rangle$, $|\mathsf{init}_2^I\rangle = f^I(|\mathsf{init}_1^I\rangle)$, with the final output obtained by the projective measurement with respect to $\bar{P}_0, \bar{P}_1$.

Let $|\Phi_1\rangle$ be the final state of the joint system of A and $\mathcal{O}_1$, and let $|\Phi_2\rangle$ be the final state of the joint system of B and $\mathcal{O}_2$.

Now, the following is a commutative diagram.

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

So, when we chase this diagram, starting from top left, with the element $|\mathsf{init}_1^P\rangle \otimes |\mathsf{init}_1^I\rangle \otimes |\mathsf{init}_1^O\rangle$, 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

$$|\Phi_2\rangle = I \otimes f^I \otimes f^O \; |\Phi_1\rangle .$$

Then,

$$\begin{aligned}\bar{P}_1 \otimes I\,|\Phi_2\rangle &= (I \otimes f^I \otimes I)(P_1 \otimes I)(I \otimes (f^I)^\dagger \otimes I)(I \otimes f^I \otimes f^O)\,|\Phi_1\rangle \\ &= (I \otimes f^I \otimes I)(P_1 \otimes I)(I \otimes I \otimes f^O)\,|\Phi_1\rangle \\ &= (I \otimes f^I \otimes f^O)(P_1 \otimes I)\,|\Phi_1\rangle\end{aligned}$$

Since f^I, f^O are both inner-product preserving, so is $I \otimes f^I \otimes f^O$. Since $|\Phi_2\rangle = I \otimes f^I \otimes f^O\,|\Phi_1\rangle$ and $\bar{P}_1 \otimes I\,|\Phi_2\rangle = (I \otimes f^I \otimes f^O)(P_1 \otimes I)\,|\Phi_1\rangle$, we have

$$\langle\Phi_2|\,\bar{P}_1 \otimes I\,|\Phi_2\rangle = \langle\Phi_1|\,P_1 \otimes I\,|\Phi_1\rangle .$$

Now, we can compute

$$\begin{aligned}\mathbf{Pr}[B^{\mathcal{O}_2}() = 1] &= \langle\Phi_2|\,\bar{P}_1 \otimes I\,|\Phi_2\rangle \\ &= \langle\Phi_1|\,P_1 \otimes I\,|\Phi_1\rangle \\ &= \mathbf{Pr}[A^{\mathcal{O}_1}() = 1].\end{aligned}$$

□

Theorem 4.4. *For any partial function $p : [M] \rightharpoonup [N]$, we have*

$$\mathsf{StO}\,|xy\rangle \otimes |p\rangle^{\mathsf{c}} = \begin{cases} |x\rangle\,|y \oplus p(x)\rangle \otimes |p\rangle^{\mathsf{c}} & \text{if } p(x) \neq \bot, \\ \dfrac{1}{\sqrt{N}} \displaystyle\sum_{z \in [N]} |x\rangle\,|y \oplus z\rangle \otimes \left|p \cup \left[\begin{smallmatrix} x \\ z \end{smallmatrix}\right]\right\rangle^{\mathsf{c}} & \text{if } p(x) = \bot. \end{cases}$$

Proof. The proof is straightforward. Let us first prove the case $p(x) \neq \bot$.

$$\begin{aligned}\mathsf{StO}\,|xy\rangle \otimes |p\rangle^{\mathsf{c}} &= \mathsf{StO}\,|xy\rangle \otimes \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} |f\rangle \\ &= \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} \mathsf{StO}\,|x\rangle\,|y\rangle \otimes |f\rangle .\end{aligned}$$

Since $p(x) \neq \bot$ and $f \supseteq p$, $f(x) = p(x) \neq \bot$. So,

$$\mathsf{StO}\,|x\rangle\,|y\rangle \otimes |f\rangle = |x\rangle\,|y \oplus p(x)\rangle \otimes |f\rangle .$$

Then,

$$\begin{aligned}\mathsf{StO}\,|xy\rangle \otimes |p\rangle^{\mathsf{c}} &= \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} |x\rangle\,|y \oplus p(x)\rangle \otimes |f\rangle \\ &= |x\rangle\,|y \oplus p(x)\rangle \otimes \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} |f\rangle \\ &= |x\rangle\,|y \oplus p(x)\rangle \otimes |p\rangle^{\mathsf{c}}.\end{aligned}$$

The proof of the second case can be done by combining the first case and Lemma 4.3. When $p(x) = \perp$,

$$\begin{aligned}\mathsf{StO}\,|xy\rangle \otimes |p\rangle^{\mathsf{c}} &= \mathsf{StO}\,|xy\rangle \otimes \frac{1}{\sqrt{N}} \sum_z \left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle^{\mathsf{c}} \\ &= \frac{1}{\sqrt{N}} \sum_z \mathsf{StO}\,|xy\rangle \otimes \left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle^{\mathsf{c}} \\ &= \frac{1}{\sqrt{N}} \sum_z |x\rangle\,|y \oplus z\rangle \otimes \left|p \cup \left[\begin{smallmatrix}x\\z\end{smallmatrix}\right]\right\rangle^{\mathsf{c}}. \qquad \square\end{aligned}$$

Theorem 5.7. *For any partial functions p_1, p_2, we have*

$$\langle p_1|p_2\rangle^{\mathsf{f}} = \begin{cases} \sqrt{\dfrac{1}{N^{|p_1 \triangle p_2|}}} & \text{if } p_1 \heartsuit p_2, \\ 0 & \text{if } p_1 \not\heartsuit p_2. \end{cases}.$$

Especially, we have $\langle p_1|p_2\rangle^{\mathsf{f}} = \langle p_1|p_2\rangle^{\mathsf{c}}$.

Proof. For any partial functions p_1, p_2,

$$\begin{aligned}\langle p_1|p_2\rangle^{\mathsf{f}} &= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|} \left(\frac{1}{\sqrt{N}}\right)^{|p_2|} \sum_{q_1,q_2} (1-N)^{|p_1 \cap q_1|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_1|} \\ &\qquad\qquad \cdot (1-N)^{|p_2 \cap q_2|} \left(-\frac{1}{\sqrt{N}}\right)^{|q_2|} \langle q_1|q_2\rangle \\ &= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|+|p_2|} \sum_q (1-N)^{|p_1 \cap q|+|p_2 \cap q|} \left(\frac{1}{N}\right)^{|q|},\end{aligned}$$

where q runs over all partial permutations with $\mathrm{pre}(q) \subseteq \mathrm{pre}(p_1) \cap \mathrm{pre}(p_2)$.

Let us define two sets $\boldsymbol{E}, \boldsymbol{U}$ as follows.

$$\begin{aligned}\boldsymbol{E} &= \{x \in \mathrm{pre}(p_1) \cap \mathrm{pre}(p_2) \mid p_1(x) = p_2(x)\}, \\ \boldsymbol{U} &= \{x \in \mathrm{pre}(p_1) \cap \mathrm{pre}(p_2) \mid p_1(x) \neq p_2(x)\}.\end{aligned}$$

Let $\boldsymbol{A}, \boldsymbol{B}$ be disjoint subsets of $\boldsymbol{E}$, where $x \in \boldsymbol{A}$ iff $q(x) = p_1(x) = p_2(x)$, and $x \in \boldsymbol{B}$ iff $q(x) \neq p_1(x), p_2(x)$. Also, let $\boldsymbol{C}, \boldsymbol{D}, \boldsymbol{F}$ be disjoint subsets of $\boldsymbol{U}$, where $x \in \boldsymbol{C}$ iff $q(x) = p_1(x)$, $x \in \boldsymbol{D}$ iff $q(x) = p_2(x)$, and $x \in \boldsymbol{F}$ iff $q(x) \neq p_1(x), p_2(x)$. We can see that, selecting q is equivalent to selecting $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{F}$ and $q|_{\boldsymbol{B}}$, $q|_{\boldsymbol{F}}$. Let $a = |\boldsymbol{A}|$, $b = |\boldsymbol{B}|$, $c = |\boldsymbol{C}|$, $d = |\boldsymbol{D}|$, $f = |\boldsymbol{F}|$. Note that $|p_1 \cap q| = a + c$, $|p_2 \cap q| = a + d$, and $|q| = a + b + c + d + e$. Also, for any given a, b, c, d, f, the number of q's with $|\boldsymbol{A}| = a, |\boldsymbol{B}| = b, |\boldsymbol{C}| = c, |\boldsymbol{D}| = d, |\boldsymbol{F}| = f$ is

$$\binom{|\boldsymbol{E}|}{a}\binom{|\boldsymbol{E}| - a}{b}\binom{|\boldsymbol{U}|}{c}\binom{|\boldsymbol{U}| - c}{d}\binom{|\boldsymbol{U}| - c - d}{f}(N-1)^b(N-2)^f.$$

So,

$$\begin{aligned}
\langle p_1|p_2\rangle^{\mathsf{f}} = \left(\frac{1}{\sqrt{N}}\right)^{|p_1|+|p_2|} &\sum_{a+b\le|E|}\sum_{c+d+f\le|U|} \\
&\binom{|E|}{a}\binom{|E|-a}{b}\binom{|U|}{c}\binom{|U|-c}{d}\binom{|U|-c-d}{f}(N-1)^b(N-2)^f \\
&\cdot(1-N)^{(a+c)+(a+d)}\left(\frac{1}{N}\right)^{a+b+c+d+f} \\
= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|+|p_2|} &\sum_{a+b\le|E|}\binom{|E|}{a}\binom{|E|-a}{b}(N-1)^b(1-N)^{2a}\left(\frac{1}{N}\right)^{a+b} \\
&\sum_{c+d+f\le|U|}\binom{|U|}{c}\binom{|U|-c}{d}\binom{|U|-c-d}{f}(N-2)^f(1-N)^{c+d}\left(\frac{1}{N}\right)^{c+d+f} \\
= \left(\frac{1}{\sqrt{N}}\right)^{|p_1|+|p_2|} &\sum_{a+b\le|E|}\binom{|E|}{a}\binom{|E|-a}{b}\left(\frac{(1-N)^2}{N}\right)^a\left(\frac{N-1}{N}\right)^b \\
&\sum_{c+d+f\le|U|}\binom{|U|}{c}\binom{|U|-c}{d}\binom{|U|-c-d}{f}\left(\frac{1-N}{N}\right)^c\left(\frac{1-N}{N}\right)^d\left(\frac{N-2}{N}\right)^f.
\end{aligned}$$

In the above, the first summation can be simplified using the binomial theorem.

$$\begin{aligned}
&\sum_{a+b\le|E|}\binom{|E|}{a}\binom{|E|-a}{b}\left(\frac{(1-N)^2}{N}\right)^a\left(\frac{N-1}{N}\right)^b \\
&= \sum_{a=0}^{|E|}\binom{|E|}{a}\left(\frac{(1-N)^2}{N}\right)^a\sum_{b=0}^{|E|-a}\binom{|E|-a}{b}\left(\frac{N-1}{N}\right)^b 1^{|E|-a-b} \\
&= \sum_{a=0}^{|E|}\binom{|E|}{a}\left(\frac{(1-N)^2}{N}\right)^a\left(\frac{N-1}{N}+1\right)^{|E|-a} \\
&= \left(\frac{(1-N)^2}{N}+\frac{N-1}{N}+1\right)^{|E|} \\
&= N^{|E|}.
\end{aligned}$$

The second summation can be simplified similarly.

$$\begin{aligned}
&\sum_{c+d+f\le|U|}\binom{|U|}{c}\binom{|U|-c}{d}\binom{|U|-c-d}{f}\left(\frac{1-N}{N}\right)^c\left(\frac{1-N}{N}\right)^d\left(\frac{N-2}{N}\right)^f \\
&= \left(\frac{1-N}{N}+\frac{1-N}{N}+\frac{N-2}{N}+1\right)^{|U|} \\
&= 0^{|U|}
\end{aligned}$$

Then,

$$\langle p_1 | p_2 \rangle^{\mathrm{f}} = \left(\frac{1}{\sqrt{N}} \right)^{|p_1|+|p_2|} N^{|E|} 0^{|U|}.$$

The above calculation is based on the binomial theorem, which expands $(X+Y)^n$ as $\sum_i \binom{n}{i} X^i Y^{n-i}$. So, when $n = 0$, $(X+Y)^n = 1$. Therefore, in this case, $0^0 = 1$.

Now, if $U \neq \emptyset$, then $\langle p_1 | p_2 \rangle^{\mathrm{f}} = 0$. This case occurs exactly when p_1 💔 p_2.

On the other hand, if p_1, p_2 are consistent, then $U = \emptyset$, and $N^{|E|} = N^{|p_1 \cap p_2|}$. Then,

$$\begin{aligned}
\langle p_1 | p_2 \rangle^{\mathrm{f}} &= \left(\frac{1}{\sqrt{N}} \right)^{|p_1|+|p_2|} N^{|p_1 \cap p_2|} \\
&= \left(\frac{1}{\sqrt{N}} \right)^{|p_1 \cap p_2|+|p_1 \cup p_2|} N^{|p_1 \cap p_2|} \\
&= \sqrt{\frac{N^{|p_1 \cap p_2|}}{N^{|p_1 \cup p_2|}}} = \sqrt{\frac{1}{N^{|p \triangle q|}}},
\end{aligned}$$

which is exactly $\langle p_1 | p_2 \rangle^{\mathrm{c}}$. □

Theorem 5.8. *For any partial functions p, we have*

$$\mathrm{K} | p \rangle^{\mathrm{f}} = | p \rangle^{\mathrm{c}}$$

and

$$\Phi | p \rangle^{\mathrm{f}} = | p \rangle^{\mathrm{f}}.$$

Proof. Let us prove the first identity. We have

$$\begin{aligned}
\mathrm{K} | p \rangle^{\mathrm{f}} &= \left(\frac{1}{\sqrt{N}} \right)^{|p|} \sum_q (1-N)^{|p \cap q|} \left(-\frac{1}{\sqrt{N}} \right)^{|q|} | q \rangle^{\mathrm{c}} \\
&= \left(\frac{1}{\sqrt{N}} \right)^{|p|} \sum_q (1-N)^{|p \cap q|} \left(-\frac{1}{\sqrt{N}} \right)^{|q|} \frac{1}{\sqrt{N^{M-|q|}}} \sum_{f \supseteq q} | f \rangle \\
&= \left(\frac{1}{\sqrt{N}} \right)^{|p|+M} \sum_f \left(\sum_q (1-N)^{|p \cap q|} (-1)^{|q|} \right) | f \rangle
\end{aligned}$$

Here, we have switched the order of the summations. Now, f runs over all total functions, and q runs over all partial functions with $q \subseteq f$, $\mathrm{pre}(q) \subseteq \mathrm{pre}(p)$.

So, first we need to compute

$$\sum_q (1-N)^{|p \cap q|} (-1)^{|q|}.$$

Since $q \subseteq f$, choosing q is equivalent to choosing $\mathrm{pre}(q)$.

Let E and U be defined as

$$E := \{x \in \mathrm{pre}(p) \mid p(x) = f(x)\}, \quad U := \{x \in \mathrm{pre}(p) \mid p(x) \neq f(x)\}.$$

When choosing $\mathrm{pre}(q)$, let us define $A := \mathrm{pre}(q) \cap E$, $B := \mathrm{pre}(q) \cap U$. So, choosing q is equivalent to choosing $A \subseteq E$, $B \subseteq U$. Let $a = |A|, b = |B|$. Then, $|p \cap q| = a$, $|q| = a + b$. So,

$$\begin{aligned}
&\sum_q (1-N)^{|p\cap q|}(-1)^{|q|} \\
&= \sum_{a=0}^{|E|}\sum_{b=0}^{|U|} \binom{|E|}{a}\binom{|U|}{b}(1-N)^a(-1)^{a+b} \\
&= \sum_{a=0}^{|E|} \binom{|E|}{a}(N-1)^a \cdot \sum_{b=0}^{|U|} \binom{|U|}{b}(-1)^b \\
&= N^{|E|} \cdot 0^{|U|}
\end{aligned}$$

Here, if $U \neq \emptyset$ then $0^{|U|} = 0$, and when $U = \emptyset$, then $p \subseteq f$, and $E = \mathrm{pre}(p)$. In this case, $N^{|E|}0^{|U|} = N^{|p|}$. So,

$$\begin{aligned}
\mathrm{K}|p\rangle^{\mathrm{f}} &= \left(\frac{1}{\sqrt{N}}\right)^{|p|+M} \sum_{f \supseteq p} N^{|p|}\,|f\rangle \\
&= \frac{1}{\sqrt{N^{M-|p|}}} \sum_{f \supseteq p} |f\rangle \\
&= |p\rangle^{\mathrm{c}}.
\end{aligned}$$

Let us prove the second identity. We have

$$\begin{aligned}
\Phi|p\rangle^{\mathrm{f}} &= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_q (1-N)^{|p\cap q|}\left(-\frac{1}{\sqrt{N}}\right)^{|q|} |q\rangle^{\mathrm{f}} \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_q (1-N)^{|p\cap q|}\left(-\frac{1}{\sqrt{N}}\right)^{|q|} \\
&\quad \cdot \left(\frac{1}{\sqrt{N}}\right)^{|q|} \sum_r (1-N)^{|q\cap r|}\left(-\frac{1}{\sqrt{N}}\right)^{|r|} |r\rangle \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_r \left(\sum_q (1-N)^{|p\cap q|+|q\cap r|}\left(-\frac{1}{N}\right)^{|q|}\right)\left(-\frac{1}{\sqrt{N}}\right)^{|r|} |r\rangle\,.
\end{aligned}$$

In the above, we have switched the order of the summations. r runs over all partial functions with $\mathrm{pre}(r) \subseteq \mathrm{pre}(p)$, and q runs over all partial functions with $\mathrm{pre}(r) \subseteq \mathrm{pre}(q) \subseteq \mathrm{pre}(p)$.

Let us first compute the sum involving q:

$$\sum_q (1-N)^{|p\cap q|+|q\cap r|}\left(-\frac{1}{N}\right)^{|q|}.$$

We define sets E and U as

$$E := \{x \in \mathrm{pre}(r) \mid p(x) = r(x)\}, \quad U := \{x \in \mathrm{pre}(r) \mid p(x) \neq r(x)\}.$$

We will choose subsets $A \subseteq E$, $B, C \subseteq U$, $D, F \subseteq \mathrm{pre}(p) \setminus \mathrm{pre}(r)$ so that

$$\begin{aligned}
&q(x) = p(x) = r(x) && \text{if } x \in A\\
&q(x) \neq p(x) = r(x) && \text{if } x \in E \setminus A\\
&q(x) = p(x) \neq r(x) && \text{if } x \in B\\
&q(x) = r(x) \neq p(x) && \text{if } x \in C\\
&q(x) \neq p(x) \neq r(x) && \text{if } x \in U \setminus (B \cup C)\\
&q(x) = p(x) && \text{if } x \in D\\
&q(x) \neq p(x) && \text{if } x \in F.
\end{aligned}$$

Let $a = |A|, b = |B|, c = |C|, d = |D|, f = |F|$. Choosing q is equivalent to choosing A, B, C, D, F, $q|_{E\setminus A}$, $q|_{U\setminus(B\cup C)}$, and $q|_F$. So, for any given a, b, c, d, f, the number of qs satisfying these is

$$\binom{|E|}{a}\binom{|U|}{b}\binom{|U|-b}{c}\binom{|p|-|r|}{d}\binom{|p|-|r|-d}{f}(N-1)^{|E|-a}(N-2)^{|U|-b-c}(N-1)^{f}.$$

Also, in this case, $|p \cap q| = a + b + d$, $|q \cap r| = a + c$, $|q| = |r| + d + f$. Then,

$$\begin{aligned}
&\sum_q (1-N)^{|p\cap q|+|q\cap r|}\left(-\frac{1}{N}\right)^{|q|}\\
&= \sum_{a\le|E|}\ \sum_{b+c\le|U|}\ \sum_{d+f\le|p|-|r|}\binom{|E|}{a}\binom{|U|}{b}\binom{|U|-b}{c}\binom{|p|-|r|}{d}\binom{|p|-|r|-d}{f}\\
&\qquad\qquad \cdot (N-1)^{|E|-a+f}(N-2)^{|U|-b-c}\cdot(1-N)^{(a+b+d)+(a+c)}\left(-\frac{1}{N}\right)^{|r|+d+f}\\
&= \sum_{a\le|E|}\binom{|E|}{a}(N-1)^{|E|-a}(1-N)^{2a}\\
&\quad\cdot \sum_{b+c\le|U|}\binom{|U|}{b}\binom{|U|-b}{c}(N-2)^{|U|-b-c}(1-N)^{b+c}\\
&\quad\cdot \sum_{d+f\le|p|-|r|}\binom{|p|-|r|}{d}\binom{|p|-|r|-d}{f}(N-1)^{f}(1-N)^{d}\left(-\frac{1}{N}\right)^{|r|+d+f}.
\end{aligned}$$

The first sum is

$$\sum_{a=0}^{|E|}\binom{|E|}{a}(N-1)^{|E|-a}(1-N)^{2a} = ((N-1)+(1-N)^2)^{|E|} = (N(N-1))^{|E|}.$$

The second sum can be simplified as

$$\begin{aligned}
&\sum_{b=0}^{|U|}\binom{|U|}{b}(1-N)^b\sum_{c=0}^{|U|-b}\binom{|U|-b}{c}(N-2)^{|U|-b-c}(1-N)^c\\
&=\sum_{b=0}^{|U|}\binom{|U|}{b}(1-N)^b((N-2)+(1-N))^{|U|-b}\\
&=\sum_{b=0}^{|U|}\binom{|U|}{b}(1-N)^b(-1)^{|U|-b}\\
&=(-N)^{|U|}.
\end{aligned}$$

The last sum can be simplified as

$$\begin{aligned}
&\left(-\frac{1}{N}\right)^{|r|}\sum_{d=0}^{|p|-|r|}\binom{|p|-|r|}{d}(1-N)^d\left(-\frac{1}{N}\right)^d\sum_{f=0}^{|p|-|r|-d}\binom{|p|-|r|-d}{f}(N-1)^f\left(-\frac{1}{N}\right)^f\\
&=\left(-\frac{1}{N}\right)^{|r|}\sum_{d=0}^{|p|-|r|}\binom{|p|-|r|}{d}(1-N)^d\left(-\frac{1}{N}\right)^d\left(\frac{1-N}{N}+1\right)^{|p|-|r|-d}\\
&=\left(-\frac{1}{N}\right)^{|r|}\sum_{d=0}^{|p|-|r|}\binom{|p|-|r|}{d}\left(\frac{N-1}{N}\right)^d\left(\frac{1}{N}\right)^{|p|-|r|-d}\\
&=\left(-\frac{1}{N}\right)^{|r|}\left(\frac{N-1}{N}+\frac{1}{N}\right)^{|p|-|r|}\\
&=\left(-\frac{1}{N}\right)^{|r|}.
\end{aligned}$$

Combining these, we see that

$$\begin{aligned}
\sum_q(1-N)^{|p\cap q|+|q\cap r|}\left(-\frac{1}{N}\right)^{|q|}&=(N(N-1))^{|E|}(-N)^{|U|}\left(-\frac{1}{N}\right)^{|r|}\\
&=(1-N)^{|E|}(-N)^{|E|+|U|}\left(-\frac{1}{N}\right)^{|r|}\\
&=(1-N)^{|p\cap r|}(-N)^{|r|}\left(-\frac{1}{N}\right)^{|r|}\\
&=(1-N)^{|p\cap r|}.
\end{aligned}$$

Putting this result back into the sum we were calculating,

$$\begin{aligned}
\Phi|p\rangle^{\mathsf{f}} &= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_{q} (1-N)^{|p\cap q|} \left(-\frac{1}{\sqrt{N}}\right)^{|q|} |q\rangle^{\mathsf{f}} \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_{r} \left(\sum_{q} (1-N)^{|p\cap q|+|q\cap r|} \left(-\frac{1}{N}\right)^{|q|} \right) \left(-\frac{1}{\sqrt{N}}\right)^{|r|} |r\rangle \\
&= \left(\frac{1}{\sqrt{N}}\right)^{|p|} \sum_{r} (1-N)^{|p\cap r|} \left(-\frac{1}{\sqrt{N}}\right)^{|r|} |r\rangle \\
&= |p\rangle^{\mathsf{f}},
\end{aligned}$$

which proves the second identity. □

Lemma 5.10. *For any partial function $p : [M] \rightharpoonup [N]$, if $p(x) = \bot$, then we have*

$$|p\rangle^{\mathsf{f}} = \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left| p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \right\rangle^{\mathsf{f}}.$$

Proof. Here we give an alternative proof of Lemma 5.10 based on direct computation.

$$\begin{aligned}
&\frac{1}{\sqrt{N}} \sum_{y\in[N]} \left| p \cup \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \right\rangle^{\mathsf{f}} \\
&= \frac{1}{\sqrt{N}} \sum_{y\in[N]} |p\rangle^{\mathsf{f}} \circledcup \left(\left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}} |\emptyset\rangle - \frac{1}{N} \sum_{z\in[N]} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right) \\
&= |p\rangle^{\mathsf{f}} \circledcup \frac{1}{\sqrt{N}} \sum_{y\in[N]} \left(\left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle + \frac{1}{\sqrt{N}} |\emptyset\rangle - \frac{1}{N} \sum_{z\in[N]} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right) \\
&= |p\rangle^{\mathsf{f}} \circledcup \left(\frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle + \frac{1}{N} \sum_{y\in[N]} |\emptyset\rangle - \frac{1}{N\sqrt{N}} \sum_{y,z} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right) \\
&= |p\rangle^{\mathsf{f}} \circledcup \left(\frac{1}{\sqrt{N}} \sum_{y\in[N]} \left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right\rangle + |\emptyset\rangle - \frac{1}{\sqrt{N}} \sum_{z\in[N]} \left|\begin{smallmatrix} x \\ z \end{smallmatrix}\right\rangle \right) \\
&= |p\rangle^{\mathsf{f}} \circledcup |\emptyset\rangle = |p\rangle^{\mathsf{f}}.
\end{aligned}$$

□