Recording quantum queries – explained

Dominique Unruh

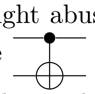
This draft was intended to give a formal treatment of Zhandry's results from [2], with all definitions and proofs worked out.

It is unfinished and there are currently no plans to finish it. See our paper "Compressed Permutation Oracles" [1] for an alternative.

However, since the manuscript has been cited in some places, we provide this incomplete draft as-is for reference.

Contents

1 Some notation

We assume that $\bot$ is a fixed symbol different from any bitstring in $\{0,1\}^*$. Let $\{0,1\}^n_\bot := \{0,1\}^n \cup \{\bot\}$. In slight abuse of notation, we define $CNOT^{\otimes n}$ to be the unitary $CNOT^{\otimes n}|x,y\rangle := |x, y\oplus x\rangle$, and we write  for it (it will always be clear from the context that $CNOT^{\otimes n}$ is meant since $CNOT$ can only be applied to single qubit wires).

Given a unitary transformation U that operates on $\mathbb{C}^{\{0,1\}^n}$, we naturally extend it to $\mathbb{C}^{\{0,1\}^n_\bot}$ by setting $U|\bot\rangle := |\bot\rangle$. For example, when applied to a quantum register with space $\mathbb{C}^{\{0,1\}^n_\bot}$, $H^{\otimes n}$ is the following matrix: $H^{\otimes n}|x\rangle := \sum_y 2^{-n/2}(-1)^{x\cdot y}|y\rangle$, $H^{\otimes n}|\bot\rangle := |\bot\rangle$.

This generalizes directly to unitaries that operate on more than one quantum register. For example, $CNOT^{\otimes n}$ operates on $\mathbb{C}^{\{0,1\}^n_\perp} \otimes \mathbb{C}^{\{0,1\}^n}$ as $CNOT^{\otimes n}|x,y\rangle := |x, y \oplus x\rangle$, $CNOT^{\otimes n}|\perp, y\rangle := |\perp, y\rangle$ and on $\mathbb{C}^{\{0,1\}^n} \otimes \mathbb{C}^{\{0,1\}^n_\perp}$ as $CNOT^{\otimes n}|x,y\rangle := |x, y \oplus x\rangle$, $CNOT^{\otimes n}|x, \perp\rangle := |x, \perp\rangle$. That is, when one wire contains $|\perp\rangle$, the unitary operates as the identity on all other wires.

2 Oracles

In our setting, an *oracle* O consists of the following:

- A state register S_O (described by the underlying Hilbert space).
- One or more query registers $X_1, \dots, X_n$ (described by the underlying Hilbert spaces).
- An initial state $|\Psi_O\rangle$ for the state register, or a probability distribution D_O^Ψ of initial states.
- A unitary operating U_O operating on $S_O, X_1, \dots, X_n$.

An *oracle algorithm* A is an algorithm that can make queries to an oracle O. More specifically, an execution of A^O uses four registers, the state register S_A of A, the state register S_O of O, as well as the query registers $X_1, \dots, X_n$ of O. S_O is initialized with the initial state $|\Psi_O\rangle$ (or with a state sampled according to D_O^Ψ). Then A can perform arbitrary operations on $S_A, X_1, \dots, X_n$ but not on S_O. In addition, A can query O which means that the unitary U_O is applied to $S_O, X_1, \dots, X_n$.

Definition 1: Perfectly indistinguishable

Two oracles O_1, O_2 are *perfectly indistinguishable* iff for any oracle algorithm A that outputs a classical bit b, $\Pr[b = 1 : b \leftarrow A^{O_1}] = \Pr[b = 1 : b \leftarrow A^{O_2}]$.

We say O_1, O_2 are *perfectly indistinguishable within q queries* if the above holds for every q-query oracle algorithm A.

2.1 Growing oracles

Definition 2: Growing core oracles

Let $O_{\mathfrak{core}}$ be an oracle with state register $S_{O_{\mathfrak{core}}}$ with Hilbert space $\mathcal{H}_{\mathfrak{core}}$ and query register Y with Hilbert space $\mathcal{H}_Y$, and with initial state $|\Psi_{O_{\mathfrak{core}}}\rangle$ (not a distribution).

Fix some length n.

Then $\mathbf{Grow}(O_{\mathfrak{core}})$ is the following oracle:

- Its state register $S_{\mathbf{Grow}(O_{\mathfrak{core}})}$ consists of registers $(S_x)_{x\in\{0,1\}^n}$, each with Hilbert space $\mathcal{H}_{\mathfrak{core}}$.
- It has query registers X with Hilbert space $\mathbb{C}^{\{0,1\}^n}$ and Y with Hilbert space $\mathcal{H}_Y$.
- It has initial state $|\Psi_{\mathbf{Grow}(O_{\mathfrak{core}})}\rangle := \bigotimes_{x\in\{0,1\}^n} |\Psi_{O_{\mathfrak{core}}}\rangle$.
- Its unitary is $U_{\mathbf{Grow}(O_{\mathfrak{core}})} := \sum_{x\in\{0,1\}^n} U_x \otimes |x\rangle\langle x|$ where U_x stands for $U_{O_{\mathfrak{core}}}$ applied to S_x, Y.

Definition 3: Efficiently growing core oracles

Let $O_{\mathfrak{core}}$, n be as in Definition 2. Let q be an integer (query number). Then $\mathbf{FastGrow}_q(O_{\mathfrak{core}})$ is defined as .

Lemma 4

$\mathbf{Grow}(O_{\mathfrak{core}})$ and $\mathbf{FastGrow}_q(O_{\mathfrak{core}})$ are perfectly indistinguishable within q queries.

2.2 Random oracle

For this and the following subsections, fix two integers n, m (denoting the input / output size of the random oracle).

Definition 5: Random oracle

The *random oracle* RO has state register S_{RO} with Hilbert space $\mathbb{C}^{Fun}$ where Fun is the set of all functions $\{0,1\}^n \to \{0,1\}^m$. It has query registers X and Y with Hilbert spaces $\mathbb{C}^{\{0,1\}^n}$ and $\mathbb{C}^{\{0,1\}^m}$, respectively. Its unitary is $U_{\mathsf{RO}} : |H\rangle|x\rangle|y\rangle \mapsto |H\rangle|x\rangle|y \oplus H(x)\rangle$. The initial state distribution D^{Ψ}_{RO} returns $|H\rangle$ for uniformly random $H \in \mathit{Fun}$.

2.3 Standard oracle

Definition 6: Standard oracle

The standard oracle StdO has state register S with Hilbert space $\bigotimes_{x\in\{0,1\}^n} \mathbb{C}^{\{0,1\}^m_\perp}$, query registers X and Y with Hilbert spaces $\mathbb{C}^{\{0,1\}^n}, \mathbb{C}^{\{0,1\}^m}$, respectively. The initial state is $\bigotimes_{x\in\{0,1\}^n}|0^m\rangle$ (i.e., $|0^{2^n m}\rangle$). The unitary operation is:

$$U_{\mathsf{StdO}} : |D\rangle|x\rangle|y\rangle := \begin{cases} |D\rangle|x\rangle|y \oplus D_x\rangle & (\text{if } D_x \neq \perp) \\ |D\rangle|x\rangle|y\rangle & (\text{if } D_x = \perp) \end{cases}$$

for $D \in \prod_{x\in\{0,1\}^n}\{0,1\}^m_\perp$.

Note: we could have easily defined the standard oracle to use state space $\bigotimes_{x\in\{0,1\}^n} \mathbb{C}^{\{0,1\}^m}$ (no $\perp$). This would be more natural. However, defining it this way makes it easier to derive the "compressed" oracles below.

Lemma 7

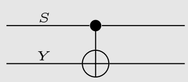
StdO and RO are perfectly indistinguishable.

We show how the standard oracle can be alternatively defined by just specifying its core:

Definition 8: Standard oracle core

The standard oracle core $\mathsf{StdO}_{\mathfrak{core}}$ has state register $S_{\mathsf{StdO}_{\mathfrak{core}}} =: S$ with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\Psi_{\mathsf{StdO}_{\mathfrak{core}}}\rangle := |+\rangle^{\otimes m}$. The unitary operation is $U_{\mathsf{StdO}_{\mathfrak{core}}} := \mathit{CNOT}^{\otimes m}$, i.e.,

$U_{\mathsf{StdO}_{\mathfrak{core}}} \equiv$



Lemma 9

$\mathsf{StdO} = \mathbf{Grow}(\mathsf{StdO}_{\mathfrak{core}})$.

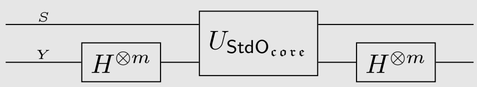
Since this definition is considerably more compact, we will define the following oracles simply by specifying their cores.

2.4 Phase oracle

Definition 10: Phase oracle core

The phase oracle core $\mathsf{PhO}_{\mathfrak{core}}$ has state register $S_{\mathsf{PhO}_{\mathfrak{core}}} =:$ with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\Psi_{\mathsf{PhO}_{\mathfrak{core}}}\rangle := |+\rangle^{\otimes m}$. The unitary operation $U_{\mathsf{PhO}_{\mathfrak{core}}}$ is given by the following quantum circuit:

$U_{\mathsf{PhO}_{\mathfrak{core}}} \equiv$

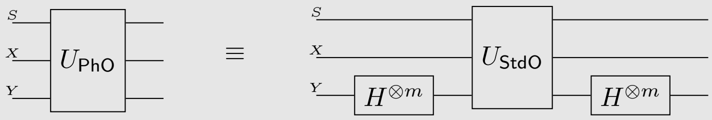


Lemma 11

$\mathsf{PhO} := \mathbf{Grow}(\mathsf{PhO}_{\mathfrak{core}})$.

Lemma 12

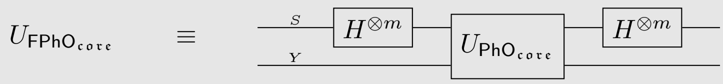
$|\Psi_{\mathsf{PhO}}\rangle = |\Psi_{\mathsf{StdO}}\rangle$ and



2.5 Fourier phase oracle

Definition 13: Fourier phase oracle core

The Fourier phase oracle core $\mathsf{FPhO}_{\mathfrak{core}}$ has state register $S_{\mathsf{FPhO}_{\mathfrak{core}}} =: S$ with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\Psi_{\mathsf{FPhO}_{\mathfrak{core}}}\rangle := |0^m\rangle$. The unitary operation is given by the following quantum circuit:



Definition 14

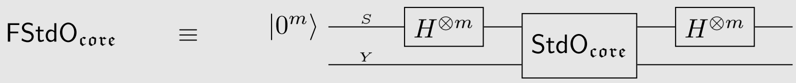
$\mathsf{FPhO} := \mathbf{Grow}(\mathsf{FPhO}_{\mathfrak{core}})$.

Lemma 15

2.6 Fourier standard oracle

Definition 16: Fourier standard oracle core

The Fourier standard oracle core $\mathsf{FStdO}_{\mathfrak{core}}$ has state register S with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|0^m\rangle$. The unitary operation is given by the following quantum circuit:



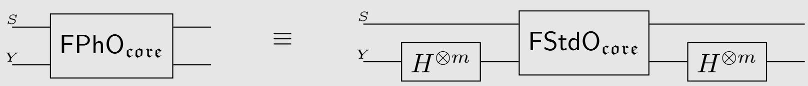
Definition 17

$\mathsf{FStdO} := \mathbf{Grow}(\mathsf{FStdO}_{\mathfrak{core}})$.

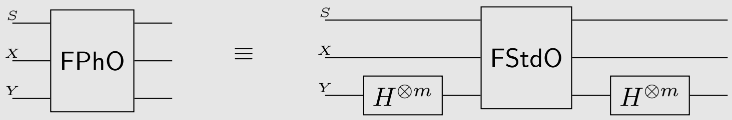
Lemma 18

$\mathsf{FStdO}_{\mathfrak{core}}$ is perfectly indistinguishable from $\mathsf{StdO}_{\mathfrak{core}}$. FStdO is perfectly indistinguishable from StdO.

Lemma 19



and



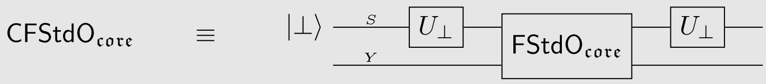
3 Compressed oracles

Let $U_\perp$ be the unitary on $\mathbb{C}^{\{0,1\}^m_\perp}$ defined by: $U_\perp|0^m\rangle := \perp$, $U_\perp|\perp\rangle := |0^m\rangle$, $U_\perp|x\rangle := |x\rangle$ for $x \in \{0,1\}^m$, $x \neq 0^m$.

3.1 Compressed Fourier standard oracle

Definition 20: Compressed Fourier standard oracle core

The compressed Fourier standard oracle core $\mathsf{CFStdO}_{\mathfrak{core}}$ has state register S with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\perp\rangle$. The unitary operation is given by the following quantum circuit:



Definition 21: Compressed Fourier standard oracle

$\mathsf{CFStdO} := \mathbf{Grow}(\mathsf{CFStdO}_{\mathfrak{core}})$.

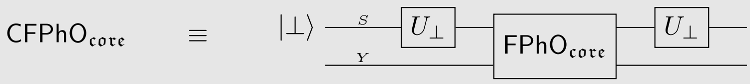
Lemma 22

$\mathsf{CFStdO}_{\mathfrak{core}}$, $\mathsf{FStdO}_{\mathfrak{core}}$, and $\mathsf{StdO}_{\mathfrak{core}}$ are perfectly indistinguishable. CFStdO, FStdO, and StdO are perfectly indistinguishable.

3.2 Compressed Fourier phase oracle

Definition 23: Compressed Fourier phase oracle core

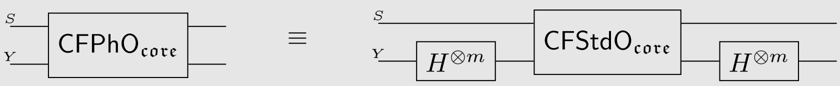
The compressed Fourier phase oracle core $\mathsf{CFPhO}_{\mathfrak{core}}$ has state register S with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\perp\rangle$. The unitary operation is given by the following quantum circuit:



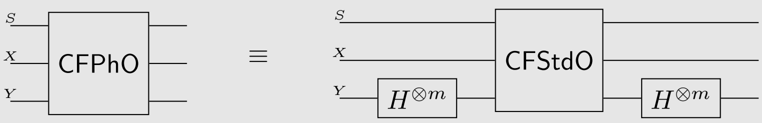
Definition 24: Compressed Fourier phase oracle

$\mathsf{CFPhO} := \mathbf{Grow}(\mathsf{CFPhO}_{\mathfrak{core}})$.

Lemma 25



and



Lemma 26

$\mathsf{CFPhO}_{\mathfrak{core}}$, $\mathsf{FPhO}_{\mathfrak{core}}$, and $\mathsf{PhO}_{\mathfrak{core}}$ are perfectly indistinguishable. CFPhO, FPhO, and PhO are perfectly indistinguishable.

Lemma 27

For all $d \in \{0,1\}^m_\perp$, $y \in \{0,1\}^m$:

$$\begin{array}{llll} \mathsf{CFPhO}_{\mathfrak{core}}: & |\perp\rangle|y\rangle & \mapsto |y\rangle|y\rangle & (y \neq 0^m) \\ & |\perp\rangle|0^m\rangle & \mapsto |\perp\rangle|0^m\rangle & \\ & |d\rangle|y\rangle & \mapsto |d \oplus y\rangle|y\rangle & (d \neq 0^m, \perp,\ y \neq d) \\ & |y\rangle|y\rangle & \mapsto |\perp\rangle|y\rangle & (y \neq 0^m) \\ & |0\rangle|y\rangle & \mapsto |0\rangle|y\rangle & \end{array}$$

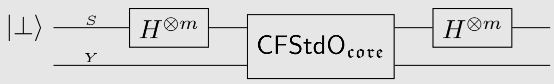
Note: this differs from Zhandry's description in the "impossible" case $d = 0^m$, $y \neq d$.

3.3 Compressed standard oracle

Definition 28: Compressed standard oracle core

The compressed standard oracle core $\mathsf{CStdO}_{\mathfrak{core}}$ has state register S with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\perp\rangle$. The unitary operation is given by the following quantum circuit:

$\mathsf{CStdO}_{\mathfrak{core}}$ $\equiv$



Definition 29

$\mathsf{CStdO} := \mathbf{Grow}(\mathsf{CStdO}_{\mathfrak{core}})$.

Lemma 30

$\mathsf{CStdO}_{\mathfrak{core}}$, $\mathsf{CFStdO}_{\mathfrak{core}}$, $\mathsf{FStdO}_{\mathfrak{core}}$, and $\mathsf{StdO}_{\mathfrak{core}}$ are perfectly indistinguishable. CStdO, CFStdO, FStdO, and StdO are perfectly indistinguishable.

Lemma 31: Some useful equations for working with CStdO

For clarity, the "error terms" are in gray.

$$H^{\otimes m} U_\perp H^{\otimes m}|d\rangle = |d\rangle - 2^{-m/2}|+^m\rangle + 2^{-m/2}|\perp\rangle \qquad (d \neq \perp)$$

$$H^{\otimes m} U_\perp H^{\otimes m}|\perp\rangle = |+^m\rangle$$

$$\mathsf{CStdO}_{\mathfrak{core}}|d\rangle|y\rangle = |d\rangle|y \oplus d\rangle + 2^{-m/2}|\perp\rangle|y \oplus d\rangle - \sum_{e \in \{0,1\}^m} 2^{-m}|e\rangle|y \oplus e\rangle + 2^{-m}|+^m\rangle|+^m\rangle - 2^{-m}|\perp\rangle|+^m\rangle \qquad (d \neq \perp)$$

$$\mathsf{CStdO}_{\mathfrak{core}}|\perp\rangle|y\rangle = \sum_{e \in \{0,1\}^m} 2^{-m/2}|e\rangle|y \oplus e\rangle - 2^{-m/2}|+^m\rangle|+^m\rangle + 2^{-m/2}|\perp\rangle|+^m\rangle$$

Lemma 32

Let ψ be a vector in $\mathbb{C}^{\{0,1\}^m} \otimes \mathbb{C}^{\{0,1\}^m} \otimes \mathcal{H}$. Let $P := \sum_{d \in M}|d\rangle\langle d| \otimes I \otimes I$ for some $M \subseteq \{0,1\}^m$. Then

$$\|P\,(\mathsf{CStdO}_{\mathfrak{core}} \otimes I)\psi\| \ \leq\ 2^{-m/2+1}\sqrt{|M|}\,\|(1-P)\psi\| \ +\ \|P\psi\|$$

Lemma 33

Let ψ be a vector in . Fix a family $M_x \subseteq \{0,1\}^m$ with $x \in \{0,1\}^n$. Assume $|M_x| \leq B$ for all x. Let $P := 1 - \bigotimes_x (\sum_{d \notin M_x} |d\rangle\langle d|)$. Then

$$\|P\,(\mathsf{CStdO} \otimes I)\psi\| \;\leq\; 2^{-m/2+1}\sqrt{B}\,\|(1-P)\psi\| \;+\; \|P\psi\|$$

Can we generalize this? This only allows us to talk about properties like "for each x, $D(x) \notin M_x$." But not about properties like "D has no collision".

Lemma 34

Let ψ be a vector in . Fix $M, N \subseteq (\{0,1\}^n \to \{0,1\}^m_\perp)$. Assume $N \subseteq M$. Assume that for all $x \in \{0,1\}^n$ and all $D \notin M$, we have that

$$\left|\left\{d : d \in \{0,1\}^m_\perp, D(x := d) \in N\right\}\right| \leq B.$$

Let $P_M := \sum_{D \in M} |D\rangle\langle D| \otimes I \otimes I$ and P_N analogous.

Then

$$\|P_N\,(\mathsf{CStdO}_{\mathfrak{core}} \otimes I)\psi\| \;\leq\; 2^{-m/2+1}\sqrt{B}\,\|(1-P_M)\psi\| \;+\; \|P_M\psi\|$$

Example: For collision resistance, in the i-th query, M is the set of all D that have a collision or more than $i-1$ non-$\perp$, and N is the set of all D that have a collision or more than i non-$\perp$. Then $B = i-1$. Total success probability: $\left(2^{-m/2+1}\sum_{i=0}^{q-1}\sqrt{i-1}\right)^2 \leq 2^{-m+2}(q\sqrt{q})^2 = 4q^3/2^m$.

Lemma 35

Let A be an algorithm with oracle access to CStdO that outputs a list L of input/output pairs (i.e., a list $L = \{(x_1,y_1),\dots,(x_n,y_n)\}$). Assume that if $(x,y) \in L$, then A has made a classical query with input x to CStdO and measured the output and gotten the result y.

Then, conditioned on output $L = \{(x_1,y_1),\dots,(x_n,y_n)\}$, the final state of CStdO in register is of the form $\sum_D \alpha_D |D\rangle\langle D|$ ranging only over values D with $D(x_i) = y_i \forall i$.

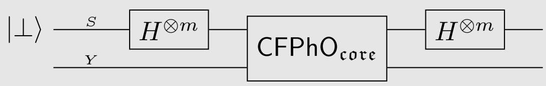
For example, for analyzing Grover, we transform a search algorithm B into A which queries the final output of B and outputs the result. If B is successful, then A will have a zero-value in the D-register, and thus happens with small probability by analysis via Lemma 34. For collision-finder B, we let A query the collision and output the result. This reduces it to the probability that D contains a collision.

3.4 Compressed phase oracle

Definition 36: Compressed phase oracle core

The compressed phase oracle core $\mathsf{CPhO}_{\mathfrak{core}}$ has state register S with Hilbert space $\mathbb{C}^{\{0,1\}^m_\perp}$, and query register Y with Hilbert space $\mathbb{C}^{\{0,1\}^m}$. The initial state is $|\perp\rangle$. The unitary operation is given by the following quantum circuit:

$\mathsf{CPhO}_{\mathfrak{core}} \quad \equiv$



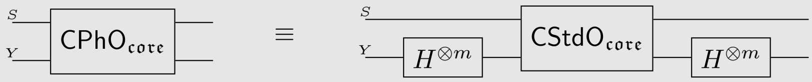
Definition 37

$\mathsf{CPhO} := \mathbf{Grow}(\mathsf{CPhO}_{\mathfrak{core}})$.

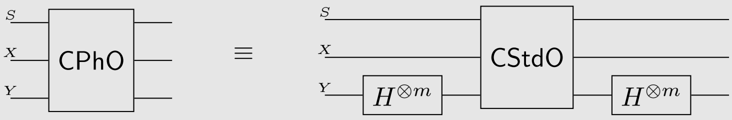
Lemma 38

$\mathsf{CPhO}_{\mathfrak{core}}$, $\mathsf{CFPhO}_{\mathfrak{core}}$, $\mathsf{FPhO}_{\mathfrak{core}}$, and $\mathsf{PhO}_{\mathfrak{core}}$ are perfectly indistinguishable. CPhO, CFPhO, FPhO, and PhO are perfectly indistinguishable.

Lemma 39



and



4 Efficient compressed oracles

5 Example: Hardness of finding collisions

Let A be an oracle quantum algorithm making at most q queries to a random oracle $H : \{0,1\}^n \to \{0,1\}^m$. Let $\varepsilon := \Pr[x \neq x' \land H(x) = H(x') : (x, x') \leftarrow A^H]$.

Let B^H do: Run $(x, x') \leftarrow A^H$, query $y \leftarrow H(x)$, $y' \leftarrow H(x')$. Return $(x, y), (x', y')$. We call the output of B *good* iff $x \neq x'$ and $y = y'$. Then $\Pr[\mathit{out} \text{ good} : \mathit{out} \leftarrow B^H] = \varepsilon$.

By , $\Pr[\mathit{out} \text{ good} : \mathit{out} \leftarrow B^{\mathsf{CStdO}}] = \varepsilon$.

By Lemma 35, this implies that measuring the oracle's state register using P_M where M is the set of all D that contains a collision will succeed with probability $\geq \varepsilon$. (P_M is as in Lemma 34.)

Let ψ_i be the quantum state before the i-th query, and ψ_i' after the i-th query. Let M_i be the set of all D such that D contains a collision or contains $\geq i$ entries.

Note that for all $i \leq q + 2$ and $D \notin M_{i-1}$, we have

$$\left|\left\{d : d \in \{0,1\}^m_\perp, D(x := d) \in M_i\right\}\right| \leq q.$$

Since ψ_1 contains $D = \perp$, we have $\|P_{M_0}\psi_1\| = 0$.

By Lemma 34, $\|P_{M_i}\psi_i'\| \leq 2^{-m/2+1}\sqrt{q} + \|P_{M_{i-1}}\psi_i\|$. Furthermore, since P_{M_i} operates only on the state register, $\|P_{M_i}\psi_i'\| = \|P_{M_i}\psi_{i+1}\|$. By induction, $\|P_{M_{q+2}}\psi_{q+2}'\| \leq (q+2)2^{-m/2+1}\sqrt{q}$.

Then

$$\varepsilon = \|P_M\psi_{q+2}'\|^2 \leq \|P_{M_{q+2}}\psi_{q+2}'\|^2 \leq (q+2)^2 2^{-m+2} q.$$

Symbol index

U_O	Unitary of oracle O	
$\|n\rangle$	Basis vector n	
$\mathbb{C}$	Complex numbers	
H	Hadamard matrix	
$\langle n\|$	Adjoing of basis vector n	
RO	Random oracle	
$CNOT$	CNOT matrix	1
$\mathsf{StdO}_{\mathfrak{core}}$	Standard oracle core	3
StdO	Standard oracle	3
$\mathsf{PhO}_{\mathfrak{core}}$	Phase oracle core	3
PhO	Phase oracle	3
$\mathsf{CFPhO}_{\mathfrak{core}}$	Compressed Fourier phase oracle core	5
CFPhO	Compressed Fourier phase oracle	5
$\mathsf{CFStdO}_{\mathfrak{core}}$	Compressed Fourier standard oracle core	5
CFStdO	Compressed Fourier standard oracle	5
$\\|\psi\\|$	(Hilbert space-)norm of vector ψ	
$\mathbf{Grow}(q)U_{\mathfrak{core}}$	"Growing" an oracle efficiently for q queries	
$\|x\|$	Absolute value / cardinality	

Index

References

[1] Dominique Unruh. *Compressed Permutation Oracles (and the Collision-Resistance of Sponge/SHA3)*. IACR ePrint 2021/062. 2021.

[2] Mark Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Eprint is IACR ePrint 2018/276. Cham: Springer International Publishing, 2019, pp. 239–268. ISBN: 978-3-030-26951-7.