An Optimal Oracle Separation of Classical and Quantum Hybrid Schemes

Atsuya Hasegawa ✉
Graduate School of Information Science and Technology, The University of Tokyo, Japan

François Le Gall ✉
Graduate School of Mathematics, Nagoya University, Japan

──── **Abstract** ────

Recently, Chia, Chung and Lai (STOC 2020) and Coudron and Menda (STOC 2020) have shown that there exists an oracle $\mathcal{O}$ such that $\mathsf{BQP}^{\mathcal{O}} \neq (\mathsf{BPP}^{\mathsf{BQNC}})^{\mathcal{O}} \cup (\mathsf{BQNC}^{\mathsf{BPP}})^{\mathcal{O}}$. In fact, Chia et al. proved a stronger statement: for any depth parameter d, there exists an oracle that separates quantum depth d and $2d + 1$, when polynomial-time classical computation is allowed. This implies that relative to an oracle, doubling quantum depth gives classical and quantum hybrid schemes more computational power.

In this paper, we show that for any depth parameter d, there exists an oracle that separates quantum depth d and $d + 1$, when polynomial-time classical computation is allowed. This gives an optimal oracle separation of classical and quantum hybrid schemes. To prove our result, we consider d-Bijective Shuffling Simon's Problem (which is a variant of d-Shuffling Simon's Problem considered by Chia et al.) and an oracle inspired by an "in-place" permutation oracle.

1 Introduction

Background

In recent years, the development of quantum computers has been very active (see, e.g., [1] for information about current quantum computers) and "quantum supremacy" has been claimed [8, 22]. However, it is still difficult to implement large-depth quantum circuits with current quantum technology since such quantum devices are subjective to noise and have short coherent time. One potential way to extract the computational powers of such quantum devices is to consider a hybrid scheme combining them with classical computers. For example, variational quantum algorithms are considered in such a scheme to obtain quantum advantage (see [9] for a survey).

Therefore, understanding the capabilities and limits of this hybrid approach is an essential topic in quantum computation. As one of the most notable results, Cleve and Watrous [14] showed the quantum Fourier transformation can be implemented by combining logarithmic-depth quantum circuits with a classical polynomial-time algorithm. With the

33rd International Symposium on Algorithms and Computation (ISAAC 2022).
Editors: Sang Won Bae and Heejin Park; Article No. 6; pp. 6:1–6:14
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

possibility to implement Shor's algorithm in such a hybrid scheme and the developments of measurement-based quantum computation, Jozsa [18] conjectured that "Any quantum polynomial-time algorithm can be implemented with only $O(\log n)$ quantum depth interspersed with polynomial-time algorithm classical computations". This can be formalized as $\mathsf{BQP} = \mathsf{BQNC}^{\mathsf{BPP}}$. On the other hand, Aaronson [3, 4, 5] conjectured "there exists an oracle separation between BQP and $\mathsf{BPP}^{\mathsf{BQNC}}$". $\mathsf{BPP}^{\mathsf{BQNC}}$ is a complexity class recognized by a polynomial classical scheme which has access to poly-logarithmic depth quantum circuits. $\mathsf{BQNC}^{\mathsf{BPP}}$ and $\mathsf{BPP}^{\mathsf{BQNC}}$ are sets of problems recognized by two natural and seemingly incomparable models of hybrid classical and quantum computation.

Recent works by Chia, Chung and Lai [11] and Coudron and Menda [15] proved Aaronson's conjecture and refuted Jozsa's conjecture in a relativized setting. Interestingly, computational problems and oracles they considered were completely different. Coudron and Menda [15] considered, as an oracle problem, the Welded Tree Problem which exhibits a difference between quantum walks and classical random walks: this problem can be solved efficiently by a quantum algorithm [13] but, in the classical setting, exponential queries are required [13, 17]. To prove a lower bound of classical and quantum hybrid schemes, Coudron and Menda introduced "Information Bottleneck" to simulate classical and quantum hybrid schemes with fewer classical queries. They showed if we assume the hybrid schemes solve the problem, we reach a contradiction with the lower bound of classical queries from [17].

Chia, Chung and Lai [11] considered d-Shuffling Simon's Problem, which is a variant of Simon's Problem [20]. Since Simon's Problem can be solved with a constant-depth quantum circuit with classical post-processing, we cannot prove the hardness for classical and quantum hybrid schemes. To devise a harder problem, they combine Simon's function with sequential random permutations: for a Simon's function f, they consider random one-to-one functions $f_0, ..., f_{d-1}$ and two-to-one function f_d such that $f = f_d \circ \cdots \circ f_0$. They also hide the domains of the functions in larger domains and apply the idea of the Oneway-to-Hiding (O2H) lemma [6, 21] to prove the hardness. In fact, they proved a stronger statement below.

▶ **Theorem 1** ([11]). *For any $d \in \mathbb{N}$, there exists an oracle $\mathcal{O}$ such that*

$$(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}} \cup (\mathsf{BPP}^{\mathsf{BQNC_d}})^{\mathcal{O}} \neq (\mathsf{BQNC}_{2d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC_{2d+1}}})^{\mathcal{O}}.$$

Description of our result

In this paper, we improve Theorem 1 above and show the following result.

▶ **Theorem 2.** *For any $d \in \mathbb{N}$, there exists an oracle $\mathcal{O}$ such that*

$$(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}} \cup (\mathsf{BPP}^{\mathsf{BQNC_d}})^{\mathcal{O}} \neq (\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC_{d+1}}})^{\mathcal{O}}.$$

Our result implies that, relative to an oracle, increasing the quantum depth even by *one* gives the hybrid schemes more computational power and it cannot be traded by combining polynomial-time classical processing.

In Theorem 2, quantum circuits consisting of any 1- and 2-qubit gates are considered. Indeed, we give an algorithm by $d+1$-depth quantum circuits consisting only of $\{H, CNOT\}$ with classical processing for the upper bound (this is also the case for Theorem 1 but not mentioned in [11]). Therefore we also prove that, even if we are allowed to use quantum circuits consisting of a restricted gate set contains $\{H, CNOT\}$ such as Clifford circuits, adding even one quantum depth gives the two hybrid schemes more computational power relative to an oracle.

Outline of our approach

Chia et al. gave the upper bound $(\mathsf{BQNC}_{2d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{2d+1}})^{\mathcal{O}}$ for d-Shuffling Simon's Problem by an algorithm inspired by the Simon's algorithm. Since they considered a standard oracle, $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$, it is required to erase the information of past queries and it takes d-quantum depth. To eliminate the d-quantum depth, we propose an idea to consider an "in-place" permutation oracle [2, 16] acts as $U_f |x\rangle = |f(x)\rangle$. However, when f is a Simon's function, f_d on a restricted domain is also a two-to-one function and there is no unitary operator U_{f_d} such that $U_{f_d} |x\rangle = |f_d(x)\rangle$. Therefore, in this paper, we consider another function η and make the function bijective. We name the problem d-Bijective Shuffling Simon's Problem and show an upper bound $(\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}}$. The other obstacle is, for f_d and the shadows to prove the lower bounds, how to define a unitary operator that includes mappings to $\perp$ (a constant with no information). Note that this is because there exists no unitary operator $U_\perp$ such that $U_\perp |x\rangle = |\perp\rangle$. In this paper, we give a solution by keeping values on domains and considering "flags" on ancilla qubits. Finally we carefully tailor the Oneway-to-Hiding lemma in our quantum oracle setting and show that the similar proofs of the lower bounds also follow as [11].

Related work

Arora, Gheorghiu and Singh [7] proved oracle separations of $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$ and $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$ with respect to each other. As corollaries, they obtained sharper separations than [11] for each scheme. For the quantum-classical scheme, they proved an oracle separation between quantum depth d and $d + 1$ if the Hadamard measurements are allowed in every layer. In our result, we only need to measure qubits in the Hadamard basis in the last layer. For the classical-quantum scheme, they proved a separation between quantum depth d and $d + 5$ relative to what they call a stochastic oracle (which is non-unitary). Our separation is between quantum depth d and $d + 1$ relative to a unitary oracle.

In an independent work [12], Chia and Hung have also shown how to reduce the gap from d versus $2d + 1$ to d versus $d + 1$ by techniques similar to ours (they consider an oracle inspired by an "in-place" permutation oracle and manage to make the final function one-to-one). They also instantiate the oracle separation to construct a protocol such that a classical verifier can check if a prover has a quantum depth of at least $d + 1$.

Organization of the paper

After giving preliminaries in Section 2, in Section 3 we define the oracle problem that we call d-Bijective Shuffling Simon's Problem and give the upper bound $(\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}}$. In Section 4, we prove the Oneway-to-Hiding lemma for our quantum oracle and, in Section 5, we prove the lower bounds for $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$ and $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$.

The main contribution of our work is to define the d-Bijective Shuffling Simon's Problem and give the upper bound with quantum depth $d + 1$ (Section 3). The proof of the lower bound (Section 5) is very similar to [11] except the Oneway-to-Hiding lemma (Section 4), which has to be adapted to the quantum oracle of this paper. We are grateful to Nai-Hui Chia for discussions about this, and in particular for clarifying that all steps in the lower bound from [11] remain true for our new oracle as well, with the exception of this Oneway-to-Hiding lemma.

2 Preliminaries

2.1 State distances

Let us recall some notions about the distances of quantum states [19].

▶ **Definition 3.** *For any two mixed states ρ and σ,*
- *(Fidelity) $F(\rho, \sigma) := \mathrm{tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$.*
- *(Bures distance) $B(\rho, \sigma) := \sqrt{2 - 2F(\rho, \sigma)}$.*

▷ Claim 4. For any two mixed states ρ and σ, any quantum algorithm $\mathcal{A}$ and any classical string s,

$$|\Pr[\mathcal{A}(\rho) = s] - \Pr[\mathcal{A}(\sigma) = s]| \leq B(\rho, \sigma).$$

2.2 Computational models

Let us introduce computational models in this paper, especially two relativized hybrid schemes of quantum and classical computations.

2.2.1 Quantum circuits

First, we define d-depth quantum circuits and promise problems solved by the computational schemes. We refer to [19] for a standard reference of quantum computation and circuits. We define a one-layer (depth) unitary is a set of one- and two-qubit gates act on disjoint sets of qubits. A promise problem denotes a pair $L = (L_{\mathrm{yes}}, L_{\mathrm{no}})$, where $L_{\mathrm{yes}}, L_{\mathrm{no}} \subseteq \Sigma^*$ are sets of strings satisfying $L_{\mathrm{yes}} \cap L_{\mathrm{no}} = \emptyset$.

▶ **Definition 5** (d-depth quantum circuit, QNC_d). *QNC_d is the class of all quantum circuit family $\{C_n : n \in \mathbb{N}\}$ satisfying that C_n acts on n input qubits and $poly(n)$ ancilla qubits, and consists of successive d-layers of arbitrary one- and two-qubit gates, $U_1 U_2 ... U_d$, and measure all qubits in the computational basis.*

▶ **Definition 6** (BQNC_d). *A promise problem L is in BQNC_d if and only if there exists a circuit family $\{C_n : n \in \mathbb{N}\} \in \mathsf{QNC}_d$ satisfying the following properties:*
- *for all $x \in L_{\mathrm{yes}}$, $\Pr[C_{|x|}(x) = 1] \geq \frac{2}{3}$;*
- *for all $x \in L_{\mathrm{no}}$, $\Pr[C_{|x|}(x) = 1] \leq \frac{1}{3}$.*

In the definition above, we consider arbitrary one- and two-qubit gates. In this paper, we also consider a gate set $\{H, CNOT\}$, where $H = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$ is the Hadamard gate and $CNOT = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix} \right)$ is the controlled-not gate. A quantum circuit consisting only of Clifford gates $\{H, S, CNOT\}$, where $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix} \right)$ is the phase gate, is called a Clifford circuit.

For an oracle $\mathcal{O}$, let us define $(\mathsf{QNC}_d)^{\mathcal{O}}$ be a computational scheme similar to QNC_d considering $U_{d+1}\mathcal{O}U_d...\mathcal{O}U_1$ as layers and $(\mathsf{BQNC}_d)^{\mathcal{O}}$ be a set of promise problems solved by $(\mathsf{QNC}_d)^{\mathcal{O}}$ with high probability. Note that for relativized d-depth quantum circuit, we consider to add an extra single layer to process the final oracle access following [11]. We refer to Figure 1 for an illustration.
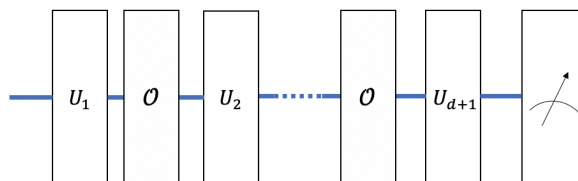
Figure 1 d-depth quantum circuit which can access to an oracle $\mathcal{O}$.

2.2.2 Quantum-classical hybrid schemes

Next, we consider the d-quantum-classical scheme, which is a generalized model for d-depth measurement-based quantum computation. This is the same model as in [11]. The scheme is denoted as d-QC scheme and we represent it as the following sequence:

$$\left(\mathcal{A}_c \xrightarrow{c} (\textstyle\prod_{0/1} \otimes I) \circ U_1\right) \xrightarrow{c,q} \left(\mathcal{A}_c \xrightarrow{c} (\textstyle\prod_{0/1} \otimes I) \circ U_2\right) \xrightarrow{c,q} (\mathcal{A}_c \cdots \circ U_d) \xrightarrow{c} \mathcal{A}_c,$$

where $\mathcal{A}_c$ is a classical probabilistic polynomial-time algorithm, U_i is a one-depth quantum layer and $\prod_{0/1}$ is a measurement in the computational basis or the Hadamard basis[1]. The arrows $\xrightarrow{c}$ and $\xrightarrow{q}$ represent transmissions of polynomial-size classical and quantum bits. Between quantum layers U_i and U_{i+1}, $\mathcal{A}_c$ can use measurement results of an arbitrary part of qubits after U_i applies and send classical polynomial-size information to U_{i+1}. We refer to Figure 2 for an illustration.
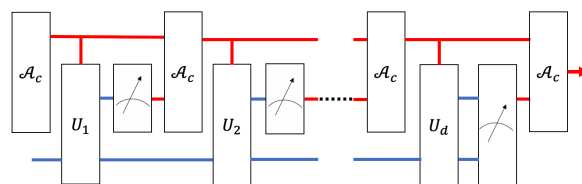
Figure 2 The d-QC scheme. Red lines stand for classical wires and blue ones stand for quantum wires.

Let us consider a relativized version of the scheme. Let $\mathcal{A}^{\mathcal{O}}$ be a d-QC scheme with access to an oracle $\mathcal{O}$. We represent the relativized d-QC scheme $\mathcal{A}^{\mathcal{O}}$ as a sequence of operators:

$$(L_1)^{\mathcal{O}} \xrightarrow{c,q} \cdots \xrightarrow{c,q} (L_d)^{\mathcal{O}} \xrightarrow{c} \mathcal{A}_c^{\mathcal{O}},$$

where $\mathcal{A}_c^{\mathcal{O}}$ is a classical polynomial-time algorithm which can query to the oracle $\mathcal{O}$, and $(L_i)^{\mathcal{O}} := \mathcal{A}_c^{\mathcal{O}} \xrightarrow{c} (\prod_{0/1} \otimes I) \circ \mathcal{O}U_i$. We refer to Figure 3 for an illustration. Then, we define the set of promise problems which can be solved by the relativized d-QC schemes.

▶ **Definition 7** (($\mathsf{BQNC}_d^{\mathsf{BPP}}$)$^{\mathcal{O}}$, Definition 3.8 in [11]). *A promise problem L is in* ($\mathsf{BQNC}_d^{\mathsf{BPP}}$)$^{\mathcal{O}}$ *if and only if there exists a family of relativized d-QC schemes $\{\mathcal{A}_n^{\mathcal{O}} : n \in \mathbb{N}\}$ satisfying the following properties:*
- *for all $x \in L_{\mathrm{yes}}$, $\Pr[\mathcal{A}_{|x|}^{\mathcal{O}}(x) = 1] \geq \frac{2}{3}$;*
- *for all $x \in L_{\mathrm{no}}$, $\Pr[\mathcal{A}_{|x|}^{\mathcal{O}}(x) = 1] \leq \frac{1}{3}$.*

---

[1] Without the Hadamard measurements, our upper bound becomes quantum depth $d+2$ for the quantum-classical hybrid scheme. The upper bound of Theorem 1 for the scheme also becomes quantum depth $2d+2$ without the Hadamard measurements.
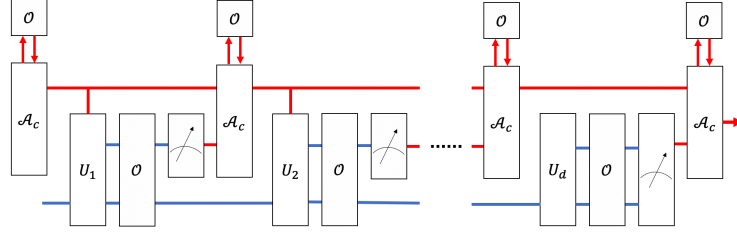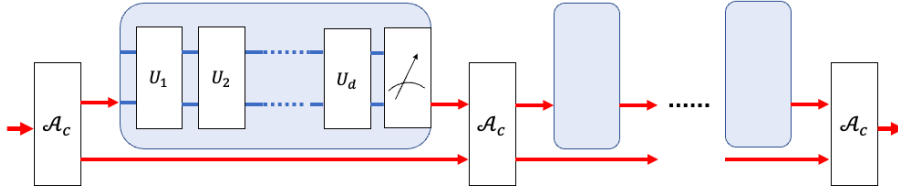
Figure 3 The d-QC scheme with access to an oracle $\mathcal{O}$.

2.2.3   Classical-quantum hybrid schemes

Finally, we define the d-classical-quantum scheme, which is a classical polynomial-time algorithm which has access to a d-depth quantum circuit during the computation (up to polynomial times). This is the same model as in [11]. The scheme is denoted as d-CQ scheme and represented as follows:

$$\mathcal{A}_{c,1} \xrightarrow{c} \prod\nolimits_{0/1} \circ\, U_d \cdots U_1 \xrightarrow{c} \cdots \xrightarrow{c} \mathcal{A}_{c,m-1} \xrightarrow{c} \prod\nolimits_{0/1} \circ\, U_d \cdots U_1 \xrightarrow{c} \mathcal{A}_{c,m},$$

where m is a polynomial in n, $\mathcal{A}_{c,i}$ is an ith classical probabilistic polynomial-time algorithm, U_i is a one-depth quantum layer, and $\prod_{0/1}$ is the computational basis measurement. Each $\mathcal{A}_{c,i+1}$ can depend on the polynomial-size information sent from $\mathcal{A}_{c,i}$ and the measurement results of the d-depth quantum circuit $\mathcal{A}_{c,i}$ calls. We refer to Figure 4 for an illustration.

Figure 4 The d-CQ scheme. Red lines stand for classical wires and blue ones stand for quantum wires.

Let us consider a relativized version of the scheme. Let $\mathcal{A}^{\mathcal{O}}$ be a d-CQ scheme with an access to an oracle $\mathcal{O}$. We represent $\mathcal{A}^{\mathcal{O}}$ as follows:

$$(L_1)^{\mathcal{O}} \xrightarrow{c} (L_2)^{\mathcal{O}} \xrightarrow{c} \cdots \xrightarrow{c} (L_{m-1})^{\mathcal{O}} \xrightarrow{c} (\mathcal{A}_{c,m})^{\mathcal{O}},$$

where $\mathcal{A}_{c,i}$ is an ith classical polynomial-time algorithm which can query to the oracle $\mathcal{O}$, and $(L_i)^{\mathcal{O}} := (\mathcal{A}_{c,i})^{\mathcal{O}} \xrightarrow{c} \prod_{0/1} \circ (U_{d+1}\mathcal{O}U_d \cdots \mathcal{O}U_1)$. We refer to Figure 5 for an illustration. Then, we define the set of promise problems which can be solved by the relativized d-CQ schemes.

▶ **Definition 8** (($\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$, Definition 3.10 in [11]). *A promise problem L is in* $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$ *if and only if there exists a family of relativized d-CQ schemes $\{\mathcal{A}_n^{\mathcal{O}} : n \in \mathbb{N}\}$ satisfying the following properties:*
- *for all $x \in L_{\mathrm{yes}}$, $\Pr[\mathcal{A}_{|x|}^{\mathcal{O}}(x) = 1] \geq \frac{2}{3}$;*
- *for all $x \in L_{\mathrm{no}}$, $\Pr[\mathcal{A}_{|x|}^{\mathcal{O}}(x) = 1] \leq \frac{1}{3}$.*
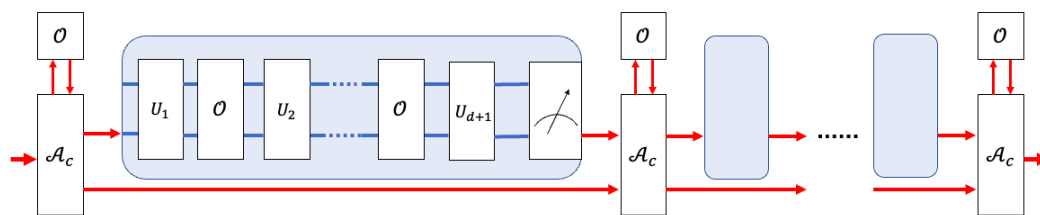
■ **Figure 5** The d-CQ scheme with access to an oracle $\mathcal{O}$.

2.3 Simon's problem

Let us recall the definitions of Simon's function and Simon's problem [20].

▶ **Definition 9** (Simon's function)**.** *A two-to-one function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ for $n \in \mathbb{N}$ is a Simon's function if there exists a period $s \in \mathbb{Z}_2^n$ such that $f(x) = f(x \oplus s)$ for $x \in \mathbb{Z}_2^n$. Let $\mathbf{F}$ be the set of all Simon's functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$.*

▶ **Definition 10** (Simon's problem)**.** *Given f chosen from $\mathbf{F}$ uniformly at random, the problem is to obtain the period s.*

▶ **Definition 11** (Decision Simon's problem)**.** *Given f to be either a random Simon's function from $\mathbf{F}$ or a random one-to-one function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ with equal probability, the promise problem is to distinguish the two cases.*

3 d-Bijective Shuffling Simon's Problem (d-BSSP)

In this section, we introduce the oracle problem, the d-Bijective Shuffling Simon's Problem, which is abbreviated as d-BSSP in the rest of the paper. It is similar to d-Shuffling Simon's Problem (d-SSP) in [11] but there are several modifications of quantum oracles to make the upper bound $(\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}} \cap (\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}}$.

Let us consider shufflings of functions. For any two set X and Y, let $P(X, Y)$ be the set of one-to-one functions from X to Y. In this work, it is enough to consider random shufflings of one-to-one functions and Simon's functions.

▶ **Definition 12** ((d, f)-shuffling, Definition 4.1 in [11])**.** *Let $d \in \mathbb{N}$ and f be a one-to-one function or a Simon's function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$. A (d, f)-shuffling is $\mathcal{F} := (f_0, f_1, ..., f_d)$, where $f_0, ..., f_{d-1}$ are chosen uniformly at random from $P(\mathbb{Z}_2^{(d+2)n}, \mathbb{Z}_2^{(d+2)n})$ and $f_d : \mathbb{Z}_2^{(d+2)n} \to \mathbb{Z}_2^{(d+2)n}$ is a function satisfying the following properties: Let $S_d := \{f_{d-1} \circ \cdots \circ f_0(x') : x' = 0, ..., 2^n - 1\}$.*
- *For $x \in S_d$, $f_d(x) = f \circ f_0^{-1} \circ \cdots \circ f_{d-1}^{-1}(x)$.*
- *For $x \notin S_d$, $f_d(x) = \perp$.*
Let $\mathbf{SHUF}(d, f)$ be a set of all (d, f)-shuffling functions.

Note that the way to choose f_d is unique for each $f_0, ..., f_{d-1}$.

We consider a standard oracle for f_0 and "in-place" permutation oracles for $f_1, ..., f_{d-1}, f_d$. When f is a Simon's function, f_d on S_d is also two-to-one and there exists no quantum oracle to implement f_d "in-place" since a two-to-one function is not a unitary operator. Therefore, we consider a function η to make the mapping bijective. We also consider a function ζ which represents whether x_d is in S_d.

▶ **Definition 13** ((d, f)-bijective shuffling). *For a (d, f)-shuffling $\mathcal{F} = (f_0, f_1, ..., f_d)$, a ($d, f$)-bijective shuffling is $\mathcal{F}_b := (f_0, f_1, ..., f_{d-1}, f_d', \zeta, \eta)$, where $f_d' : \mathbb{Z}_2^{(d+2)n} \to \mathbb{Z}_2^{(d+2)n}$, $\zeta : \mathbb{Z}_2^{(d+2)n} \to \mathbb{Z}_2$ and $\eta : \mathbb{Z}_2^{(d+2)n} \to \mathbb{Z}_2$ satisfying the following properties: Let $S_d := \{f_{d-1} \circ \cdots \circ f_0(x') : x' = 0, ..., 2^n - 1\}$.*

- *For $x \in S_d$, $f_d'(x) = f_d(x)$ and $\zeta(x) = 1$*
- *For $x \notin S_d$, $f_d'(x) = x$ and $\zeta(x) = 0$*
- *If f is a Simon's function,*
  - *For $x \in S_d$, $\eta(x) = \eta(x') \oplus 1$ where x' is the unique element in S_d such that $f_d(x) = f_d(x')$.*
  - *For $x \notin S_d$, $\eta(x) = 1$*
  - *Otherwise,*
  - *For $x \in S_d$, $\eta(x)$ is chosen uniformly at random from $\{0, 1\}$*
  - *For $x \notin S_d$, $\eta(x) = 1$*

Let $\mathbf{BSHUF}(d, f)$ be a set of all (d, f)-bijective shuffling functions.

For fixed $d \in \mathbb{N}$ and a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, we can define a random oracle which is a (d, f)-bijective shuffling chosen uniformly randomly from $\mathbf{BSHUF}(d, f)$.

▶ **Definition 14** (Bijective shuffling oracle $\mathcal{O}_{\text{unif}}^{f,d}$). *Let $d, n \in \mathbb{N}$. Let f be a Simon's function or a one-to-one function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$. The bijective shuffling oracle $\mathcal{O}_{\text{unif}}^{f,d}$ is a (d, f)-bijective shuffling $\mathcal{F}_b$ uniformly chosen from $\mathbf{BSHUF}(d, f)$.*

If we sample a (d, f)-bijective shuffling uniformly randomly from $\mathbf{BSHUF}(d, f)$, the permutations $f_0, ..., f_{d-1}$ are uniformly distributed in $P(\mathbb{Z}_2^{(d+2)n}, \mathbb{Z}_2^{(d+2)n})$ independently of f. This is because for each (d, f)-shuffling, f_d' and ζ are uniquely chosen and the number of ways to choose η and (d, f)-bijective shufflings is the same. From the definition of $\mathbf{BSHUF}(d, f)$, for such a (d, f)-bijective shuffling $\mathcal{F}_b$, only f_d' and η on S_d encodes the information of f.

Next, let us define the quantum oracle access to the bijective shuffling oracle $\mathcal{O}_{\text{unif}}^{f,d}$. In this paper, as in [11], we represent the input quantum state $|\phi\rangle$ to $\mathcal{O}_{\text{unif}}^{f,d}$ as follows:

$$|\phi\rangle := \sum_{\mathbf{X}_0, ..., \mathbf{X}_d} c(\mathbf{X}_0, ..., \mathbf{X}_d) \left(\bigotimes_{i=0}^{d} |i, \mathbf{X}_i\rangle \right)_{\mathbf{R}_Q} \otimes |0\rangle_{\mathbf{R}_N} \otimes |w(\mathbf{X}_0, ..., \mathbf{X}_d)\rangle_{\mathbf{R}_W},$$

where $\mathbf{X}_i$ is a set of elements in the domain of the functions $f_0, ..., f_{d-1}, f_d'$ and $c(\mathbf{X}_0, ..., \mathbf{X}_d)$ is an arbitary coefficient and $|w(\mathbf{X}_0, ..., \mathbf{X}_d)\rangle$ is an arbitrary working state for quantum layers, U_is. By the access to the quantum oracle, the parallel queries in the register $\mathbf{R}_Q$ and the ancilla qubits in the register $\mathbf{R}_N$ are processed, while the remaining qubits in the register $\mathbf{R}_W$ are unchanged.

For $\mathcal{F}_b \in \mathbf{BSHUF}(d, f)$, we define

$$\mathcal{F}_b |\phi\rangle := \sum_{\mathbf{X}_0, ..., \mathbf{X}_d} c(\mathbf{X}_0, ..., \mathbf{X}_d) \bigg(|0, \mathbf{X}_0\rangle |f_0(\mathbf{X}_0)\rangle \otimes \bigotimes_{i=1}^{d-1} |i, f_i(\mathbf{X}_i)\rangle |0\rangle$$
$$\otimes |d, f_d'(\mathbf{X}_d)\rangle |\zeta(\mathbf{X}_d)\rangle |\eta(\mathbf{X}_d)\rangle |0\rangle \bigg)_{\mathbf{R}_Q, \mathbf{R}_N} \otimes |w(\mathbf{X}_0, ..., \mathbf{X}_d)\rangle_{\mathbf{R}_W}.$$

Note that the ancilla qubits $|0\rangle$ are required to define the shadow in Section 4. We also define applying $\mathcal{O}_{\text{unif}}^{f,d}$ on $|\phi\rangle$ as

$$\mathcal{O}_{\text{unif}}^{f,d}(|\phi\rangle \langle\phi|) := \sum_{\mathcal{F}_b \in \mathbf{BSHUF}(d, f)} \frac{1}{|\mathbf{BSHUF}(d, f)|} \mathcal{F}_b |\phi\rangle \langle\phi| \mathcal{F}_b.$$

Now we can define the d-Bijective Shuffling Simon's Problem (d-BSSP).

▶ **Definition 15** (The search d-Bijective Shuffling Simon's Problem). *Let $d \in \mathbb{N}$ and f be a random Simon's function. Given the (d, f)-bijective shuffling oracle $\mathcal{O}^{f,d}_{\mathrm{unif}}$, the problem is to obtain the period s.*

▶ **Definition 16** (The decision d-Bijective Shuffling Simon's Problem). *Let $d \in \mathbb{N}$ and f be either a random Simon's function or a random one-to-one function with equal probability. Given the (d, f)-bijective shuffling oracle $\mathcal{O}^{f,d}_{\mathrm{unif}}$, the promise problem is to distinguish the two cases.*

We show that the d-BSSP can be solved with $d + 1$-depth quantum circuits and classical processing.

▶ **Theorem 17.** *The search d-BSSP can be solved with a $(d + 1)$-depth quantum circuit composed of $\{H, CNOT\}$ with polynomial-time classical processing. Therefore it can be solved with the $(d + 1)$-QC scheme and the $(d + 1)$-CQ scheme, and the decision d-BSSP is in $(\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}} \cap (\mathsf{BQNC}^{\mathsf{BPP}}_{d+1})^{\mathcal{O}}$.*

Proof. The d-BSSP can be solved by the following algorithm which is inspired by the Simon's algorithm and queries to the quantum oracle $d + 1$ times.

$$|0\rangle |0\rangle |0\rangle |0\rangle \xrightarrow{H^{\otimes n}} \sum_{x \in \mathbb{Z}^n_2} |x\rangle |0\rangle |0\rangle |0\rangle \xrightarrow{f_0} \sum_{x \in \mathbb{Z}^n_2} |x\rangle |f_0(x)\rangle |0\rangle |0\rangle$$

$$\xrightarrow{f_1} \sum_{x \in \mathbb{Z}^n_2} |x\rangle |f_1(f_0(x))\rangle |0\rangle |0\rangle \xrightarrow{f_2} \cdots$$

$$\xrightarrow{f_{d-1}} \sum_{x \in \mathbb{Z}^n_2} |x\rangle |f_{d-1}(\cdots f_1(f_0(x)))\rangle |0\rangle |0\rangle$$

$$\xrightarrow{f'_d, \zeta, \eta} \sum_{x \in \mathbb{Z}^n_2} |x\rangle |f(x)\rangle |\zeta(f_{d-1}(\cdots f_1(f_0(x))))\rangle |\eta(f_{d-1}(\cdots f_1(f_0(x))))\rangle$$

$$\xrightarrow{Measure} [|x\rangle |\eta(f_{d-1}(\cdots f_1(f_0(x))))\rangle + |x \oplus s\rangle |\eta(f_{d-1}(\cdots f_1(f_0(x \oplus s))))\rangle] |f(x)\rangle |1\rangle$$

$$\xrightarrow{H^{\otimes n+1}} \sum_{j \in \mathbb{Z}^n_2} \left[(-1)^{x \cdot j}(1 + (-1)^{s \cdot j}) |j\rangle |0\rangle + (-1)^{(x \cdot j) \oplus \eta(f_{d-1}(\cdots f_1(f_0(x))))}(1 - (-1)^{s \cdot j}) |j\rangle |1\rangle \right]$$

When the measurement result of the last qubit is 0, then $s \cdot j = 0$. Otherwise, $s \cdot j = 1$. Therefore, by sampling $O(n)$ times and solving linear equations, we can obtain the period s with high probability. ◀

4 Analyzing the Bijective Shuffling Oracle and Oneway-to-Hiding (O2H) Lemma

In this section, we define several notations of the bijective shuffling problem and prove Oneway-to-Hiding (O2H) Lemma [6] for our quantum oracle defined in the previous section. First, let us introduce notations of hidden sets.

▶ **Definition 18.** *Let $S_0 = \{0, ..., 2^n - 1\}$. For $j = 1, ..., d$, let $S_j = f_{j-1} \circ \cdots f_0(S_0)$.*

▶ **Definition 19** (The hidden sets **S**, Definition 5.2 in [11]). *Let $\mathcal{F}_b$ be a (d, f)-bijective shuffling. The sequence of hidden sets* $\mathbf{S} = (\overline{S}^{(0)}, ..., \overline{S}^{(d)})$ *is defined as follows:*

- *Let $S_j^{(0)} = \mathbb{Z}_2^{(d+2)n}$ for $j = 0, ..., d$. $\overline{S}^{(0)} := (S_0^{(0)}, ..., S_0^{(d)})$.*

- *For $l = 1, ..., d$, for $j = l, ..., d$, we choose $S_j^{(l)} \subseteq S_j^{(l-1)}$ randomly satisfying that $\frac{|S_j^{(l)}|}{|S_j^{(l-1)}|} \leq \frac{1}{2^n}$, $f_{j-1}(S_{j-1}^{(l)}) = S_j^{(l)}$, and $S_j \subseteq S_j^{(l)}$. $\overline{S}^{(l)} := (S_l^{(l)}, ..., S_d^{(l)})$.*

▶ **Definition 20** ($\mathcal{F}^{(l)}$ and $\hat{\mathcal{F}}^{(l)}$). *For $l = 1, ..., d-1$, let $f_j^{(l)}$ be f_j on $S_j^{(l-1)} \setminus S_j^{(l)}$ and $\hat{f}_j^{(l)}$ be f_j on $S_j^{(l)}$. Let $f_d'^{(l)}$ be f_d' on $S_d^{(l-1)} \setminus S_d^{(l)}$ and $\hat{f}_d'^{(l)}$ be f_d' on $S_d^{(l)}$. For $l = 1, ..., d$, let $\zeta^{(l)}$ be ζ on $S_d^{(l-1)} \setminus S_d^{(l)}$ and $\hat{\zeta}^{(l)}$ be ζ on $S_d^{(l)}$. Also for $l = 1, ..., d$, let $\eta^{(l)}$ be η on $S_d^{(l-1)} \setminus S_d^{(l)}$ and $\hat{\eta}^{(l)}$ be η on $S_d^{(l)}$. Then, we define $\mathcal{F}^{(1)} := (f_0, f_1^{(1)}, ..., f_d'^{(1)}, \zeta^{(1)}, \eta^{(1)})$, $\mathcal{F}^{(d+1)} := (\hat{f}_d'^{(d)}, \hat{\zeta}^{(d)}, \hat{\eta}^{(d)})$, and $\mathcal{F}^{(l)} := (\hat{f}_{l-1}^{(l)}, f_l^{(l)}, ..., f_d'^{(l)}, \zeta^{(l)}, \eta^{(l)}))$ for $l = 2, ..., d$. Also, we define $\hat{\mathcal{F}}^{(0)} := (f_0, ..., f_d', \zeta, \eta)$ and $\hat{\mathcal{F}}^{(l)} := (\hat{f}_l^{(l)}, ..., \hat{f}_d'^{(l)}, \hat{\zeta}^{(l)}, \hat{\eta}^{(l)})$ for $l = 1, ..., d$.*

We stress that for $l = 1, ..., d$, conditioned on $\mathcal{F}^{(1)}, ..., \mathcal{F}^{(l)}$, the function $\hat{f}_j^{(l)}$ is still uniformly distributed in $P(S_j^{(l)}, S_{j+1}^{(l)})$ for $j = l, ..., d-1$. This is because the number of the ways to choose $\hat{\eta}^{(l)}$ is the same for any condition $\mathcal{F}^{(1)}, ..., \mathcal{F}^{(l)}$ and $\hat{f}_l^{(l)}, ..., \hat{f}_{d-1}^{(l)}$ in **BSHUF**(d, f). In this paper, similarly to [11], we say that a quantum state ρ or a classical string s is uncorrelated to $\mathcal{F}^{(l)}$ if the process which outputs ρ or s will not change the output distribution even if we replace $\mathcal{F}^{(l)}$ by any other mapping.

Following the concept of the hidden set **S**, let us define the shadow. Definition 21 is similar to Definition 5.3 in [11], but, instead of $\perp$ (a symbol represents a constant with no information), we consider the value of the domain and a function ξ which can be recognized as a boolean flag of the shadow. Note that the reason why we also consider the function ξ is to make the quantum oracle unitary.

▶ **Definition 21** (Shadow function). *Let $\mathcal{F}_b := (f_0, ..., f_{d-1}, f_d', \zeta, \eta)$ be a (d, f)-bijective shuffling. Fix the hidden sets $\mathbf{S} = (\overline{S}^{(0)}, ..., \overline{S}^{(d)})$. Let c be a constant bit independent of $\mathcal{F}_b$ and $\mathbf{S}$. For $j = l, ..., d-1$, let g_j be the function such that if $x \in S_j^{(l)}$, $g_j(x) = x$; otherwise, $g_j(x) = f_j(x)$. Let g_d be the function such that if $x \in S_d^{(l)}$, $g_d(x) = x$; otherwise, $g_d(x) = f_d'(x)$. Let ζ_g be the function such that if $x \in S_d^{(l)}$, $\zeta_g(x) = c$; otherwise, $\zeta_g(x) = \zeta(x)$. Let η_g be the function such that if $x \in S_d^{(l)}$, $\eta_g(x) = c$; otherwise, $\eta_g(x) = \eta(x)$. Finally, for $j = l, ..., d$, let ξ_j be the function such that if $x \in S_j^{(l)}$, $\xi_j = c$; otherwise, $\xi_j(x) = c \oplus 1$. The shadow $\mathcal{G}$ of $\mathcal{F}_b$ in $\overline{S}^{(l)} = (S_l^{(l)}, ..., S_d^{(l)})$ is defined as $\mathcal{G} := (f_0, ..., f_{l-1}, g_l, ..., g_d, \xi_l, ..., \xi_d, \zeta_g, \eta_g)$.*

We stress that the shadow $\mathcal{G}$ does not contain any information of $\mathcal{F}_b$ in $\overline{S}^{(l)}$, which is $\hat{\mathcal{F}}^{(l)}$. Now we define the quantum oracle $\mathcal{G}$ of $\mathcal{F}_b$ in $\overline{S}^{(l)}$ as follows:

$$\mathcal{G}|\phi\rangle \quad := \quad \sum_{\mathbf{X}_0, ..., \mathbf{X}_d} c(\mathbf{X}_0, ..., \mathbf{X}_d) \Bigg(|0, \mathbf{X}_0\rangle |f_0(\mathbf{X}_0)\rangle \otimes \bigotimes_{i=1}^{l-1} |i, f_i(\mathbf{X}_i)\rangle |0\rangle \otimes$$
$$\bigotimes_{i=l}^{d-1} |i, g_i(\mathbf{X}_i)\rangle |\xi_i(\mathbf{X}_i)\rangle \otimes |d, g_d(\mathbf{X}_d)\rangle |\zeta_g(\mathbf{X}_d)\rangle |\eta_g(\mathbf{X}_d)\rangle |\xi_d(\mathbf{X}_d)\rangle \Bigg)_{\mathbf{R}_Q, \mathbf{R}_N}$$
$$\otimes |w(\mathbf{X}_0, ..., \mathbf{X}_d)\rangle_{\mathbf{R}_W}.$$

We will introduce the "semi-classical" oracle [6] in our setting.

▶ **Definition 22** ($U^{\mathcal{F}_b \backslash \overline{S}^{(l)}}$, Definition 5.5 in [11]). *Let $\mathcal{F}_b$ be a (d, f)-bijective shuffling. Let $\mathbf{S} = (\overline{S}^{(0)}, ..., \overline{S}^{(d)})$ be the hidden sets. Let U be a unitary operator acts on qubits of the register $\mathbf{R}$. For $l = 1, ..., d$, let $U^{\mathcal{F}_b \backslash \overline{S}^{(l)}} := \mathcal{F}_b U_{\overline{S}^{(l)}} U$ be a unitary operator acts on qubits of registers $(\mathbf{R}, \mathbf{I})$ where $\mathbf{I}$ is a one-qubit register and $U_{\overline{S}^{(l)}}$ is defined as follows:*

$$U_{\overline{S}^{(l)}} |(l, \mathbf{X}_l), ..., (d, \mathbf{X}_d)\rangle_{\mathbf{R}} |b\rangle_{\mathbf{I}} := \begin{cases} |(l, \mathbf{X}_l), ..., (d, \mathbf{X}_d)\rangle_{\mathbf{R}} |b\rangle_{\mathbf{I}} & \text{if every } \mathbf{X}_i \cap S_i^{(l)} = \emptyset, \\ |(l, \mathbf{X}_l), ..., (d, \mathbf{X}_d)\rangle_{\mathbf{R}} |b \oplus 1\rangle_{\mathbf{I}} & \text{otherwise.} \end{cases}$$

▶ **Definition 23** ($\Pr(find \overline{S}^{(k)} : U^{\mathcal{F}_b \backslash \overline{S}^{(k)}}, \rho)$, Definition 5.6 in [11]). *Let $k, d \in \mathbb{N}$ satisfying $k \leq d$. Let ρ be any input quantum state and U be any unitary operator acts on ρ. We define*

$$\Pr[find \overline{S}^{(k)} : U^{\mathcal{F}_b \backslash \overline{S}^{(k)}}, \rho] := \mathbb{E}\left[\text{tr}\left((I_{\mathbf{R}} \otimes (I - |0\rangle \langle 0|)_{\mathbf{I}}) \circ U^{\mathcal{F}_b \backslash \overline{S}^{(k)}} \circ \rho \otimes |0\rangle \langle 0|_{\mathbf{I}})\right)\right],$$

where $\mathbb{E}$ is the expectation value over the random $\mathcal{F}_b$ and $\overline{S}^{(k)}$.

When ρ is a pure state, say $|\psi\rangle$, we have

$$U^{\mathcal{F}_b \backslash \overline{S}^{(l)}} |\psi\rangle_{\mathbf{R}} |0\rangle_{\mathbf{I}} := |\phi_0\rangle_{\mathbf{R}} |0\rangle_{\mathbf{I}} + |\phi_1\rangle_{\mathbf{R}} |1\rangle_{\mathbf{I}}$$

and $\Pr[find \overline{S}^{(k)} : U^{\mathcal{F}_b \backslash \overline{S}^{(k)}}, |\psi\rangle] = \mathbb{E}[||\,|\phi_1\rangle_{\mathbf{R}}\,||^2]$. Note that, due to the definition of $\mathcal{F}_b$, $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal because $|\phi_0\rangle$ involves no query to $\overline{S}^{(k)}$ but $|\phi_1\rangle$ does. Thus,

$$\mathcal{F}_b U |\psi\rangle = |\phi_0\rangle + |\phi_1\rangle.$$

Similarly, let us consider

$$\mathcal{G} U_{\overline{S}^{(k)}} U |\psi\rangle_{\mathbf{R}} |0\rangle_{\mathbf{I}} := |\phi_0\rangle_{\mathbf{R}} |0\rangle_{\mathbf{I}} + |\phi_1^{\perp}\rangle_{\mathbf{R}} |1\rangle_{\mathbf{I}}.$$

Since $|\phi_0\rangle$ and $|\phi_1^{\perp}\rangle$ are orthogonal from the definition of $\mathcal{G}$,

$$\mathcal{G} U |\psi\rangle = |\phi_0\rangle + |\phi_1^{\perp}\rangle.$$

Note that $|\phi_1\rangle$ and $|\phi_1^{\perp}\rangle$ are orthogonal from the definition of $\mathcal{F}_b$ and $\mathcal{G}$. Then, by the concavity of the mixed state, we can prove the following lemma in a very similar way to Lemma 5.7 in [11].

▶ **Lemma 24** (Oneway-to-hiding(O2H) lemma for the bijective shuffling oracle). *Let $k, d \in \mathbb{N}$ satisfying $k \leq d$. Let $\mathcal{F}_b$ be a (d, f)-bijective shuffling. Let $\mathbf{S} = (\overline{S}^{(0)}, ..., \overline{S}^{(d)})$ be the hidden sets. Let $\mathcal{G}$ be the shadow of $\mathcal{F}_b$ in $\overline{S}^{(k)}$. Then, for any quantum algorithm $\mathcal{A}$, any unitary operator U, any initial quantum state ρ and any classical string t,*

$$\begin{aligned} |\Pr[\mathcal{A}(\mathcal{F}_b U(\rho)) = t] - \Pr[\mathcal{A}(\mathcal{G} U(\rho)) = t]| &\leq B(\mathcal{F}_b U(\rho), \mathcal{G} U(\rho)) \\ &\leq \sqrt{2\Pr[find \overline{S}^{(k)} : U^{\mathcal{F}_b \backslash \overline{S}^{(k)}}, \rho]}. \end{aligned}$$

By the union bound, it is also shown that the finding probability of $\overline{S}^{(k)}$ is bounded. The following lemma and its proof are very similar to Lemma 5.8 in [11] since

$$\left(|0, \mathbf{X}_0\rangle |f_0(\mathbf{X}_0)\rangle \otimes \bigotimes_{i=1}^{d-1} |i, f_i(\mathbf{X}_i)\rangle |0\rangle \otimes |d, f_d'(\mathbf{X}_d)\rangle |\zeta(\mathbf{X}_d)\rangle |\eta(\mathbf{X}_d)\rangle |0\rangle\right)$$

are orthogonal for different sets of queries $\mathbf{X}_0, ..., \mathbf{X}_d$.

▶ **Lemma 25.** *Suppose* $\Pr[x \in S_i^{(k)} | x \in S_i^{(k-1)}] \leq p$ *for* $i = k, ..., d$. *Then for any unitary operator* U *and initial quantum state* ρ, *which are promised to uncorrelated to* $\hat{\mathcal{F}}^{(k-1)}$ *and* $\overline{S}^{(k)}$,

$$\Pr[\text{find } \overline{S}^{(k)} : U^{\mathcal{F}_b \setminus \overline{S}^{(k)}}, \rho] \leq p \cdot q,$$

where q *is the number of parallel queries* $\mathcal{F}_b U$ *performs, which is* $\sum_{i=0}^d |\mathbf{X}_i|$.

5   Proof of Lower Bounds

In this section, we prove the lower bounds of d-BSSP for $(\mathsf{BQNC}_d)^{\mathcal{O}}$, $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$ and $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$. The proofs are almost the same as the proof of Theorem 6.1, 7.1 and 8.1 in [11] respectively except applying Lemma 24 and Lemma 25 instead of Lemma 5.7 and Lemma 5.8 in [11].

5.1   Lower bounds for $(\mathsf{BQNC}_d)^{\mathcal{O}}$

First we establish d-BSSP is intractable for any QNC_d circuit. By applying the Oneway-to-Hiding lemma inductively, it can be shown that $U_{d+1} \mathcal{F}_b U_d \cdots \mathcal{F}_b U_1$ is indistinguishable from $U_{d+1} \mathcal{G} U_d \cdots \mathcal{G} U_1$. The same argument as in [11] gives the following result.

▶ **Theorem 26.** *Let* $n, d \in \mathbb{N}$. *Let* $\mathcal{A}$ *be any* d-*depth quantum circuit and* ρ *be any initial state. Let* f *be a random Simon's function from* $\mathbb{Z}_2^n$ *to* $\mathbb{Z}_2^n$ *with period* s *and* $\mathcal{F}_b$ *be the* (d, f)-*bijective shuffling sampled from* $\mathcal{O}_{\mathrm{unif}}^{f,d}$. *Then*

$$\Pr[\mathcal{A}^{\mathcal{F}_b}(\rho) = s] \leq d \cdot \sqrt{\frac{\mathsf{poly(n)}}{2^n}} + \frac{1}{2^n}.$$

▶ **Corollary 27.** *The search* d-*BSSP can be solved with at most negligible probability by any* $(\mathsf{QNC}_d)^{\mathcal{O}}$ *and the decision* d-*BSSP is not in* $(\mathsf{BQNC}_d)^{\mathcal{O}}$

5.2   Lower bounds for $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$

Next, we establish the search d-BSSP is intractable by any d-QC scheme. Since each classical algorithms interspersed quantum layers can find polynomial-size number of points of each domains, a new procedure to define the hidden sets is needed. The same argument as in [11] gives the following result.

▶ **Theorem 28.** *Let* $n, d \in \mathbb{N}$. *Let* $\mathcal{A}$ *be any* d-*QC scheme and* ρ *be any initial state. Let* f *be a random Simon's function from* $\mathbb{Z}_2^n$ *to* $\mathbb{Z}_2^n$ *with period* s *and* $\mathcal{F}_b$ *be the* (d, f)-*bijective shuffling sampled from* $\mathcal{O}_{\mathrm{unif}}^{f,d}$. *Then*

$$\Pr[\mathcal{A}^{\mathcal{F}_b}(\rho) = s] \leq d \cdot \sqrt{\frac{\mathsf{poly(n)}}{2^n}}.$$

▶ **Corollary 29.** *The search* d-*BSSP can be solved with at most negligible probability by any* d-*QC scheme and the decision* d-*BSSP is not in* $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$.

5.3 Lower bounds for $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$

Finally, we establish the search d-BSSP is hard for any d-CQ scheme. The main difficulty lies in that conditioned on measurement results of quantum circuits, the distribution of the permutations might be not uniform enough to prove the hardness in a similar way. Chia et al. resolved the problem by approximating it by a convex combination of "almost" uniform shufflings. The same argument as in [11] gives the following result. [2]

▶ **Theorem 30.** *Let $n, d \in \mathbb{N}$. Let $\mathcal{A}$ be any d-CQ scheme. Let f be a random Simon's function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ with period s and $\mathcal{F}_b$ be the (d, f)-bijective shuffling sampled from $\mathcal{O}_{\mathrm{unif}}^{f,d}$. Then*

$$\Pr[\mathcal{A}^{\mathcal{F}_b}() = s] \leq d \cdot \sqrt{\frac{\mathsf{poly(n)}}{2^n}}.$$

▶ **Corollary 31.** *The search d-BSSP can be solved with at most negligible probability by any d-CQ scheme and the decision d-BSSP is not in $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$.*

─── **References** ───

1 URL: `https://en.wikipedia.org/wiki/List_of_quantum_processors`.

2 Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC 2002)*, pages 635–642, 2002. `doi: 10.1145/509907.509999`.

3 Scott Aaronson. Ten semi-grand challenges for quantum computing theory, 2005. URL: `https://www.scottaaronson.com/writings/qchallenge.html`.

4 Scott Aaronson. BQP and the polynomial hierarchy. In *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC 2010)*, pages 141–150, 2010. `doi:10.1145/ 1806689.1806711`.

5 Scott Aaronson. Projects aplenty, 2011. URL: `https://scottaaronson.blog/?p=663`.

6 Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In *Advances in Cryptology – CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2019. `doi:10.1007/978-3-030-26951-7_10`.

7 Atul Singh Arora, Alexandru Gheorghiu, and Uttam Singh. Oracle separations of hybrid quantum-classical circuits. *arXiv*, 2022. `doi:10.48550/arXiv.2201.01904`.

8 Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019. `doi:10.1038/s41586-019-1666-5`.

9 Marco Cerezo et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021. `doi:10.1038/s42254-021-00348-9`.

10 Nai-Hui Chia. Personal communication, 2022.

11 Nai-Hui Chia, Kai-Min Chung, and Ching-Yi Lai. On the need for large quantum depth. In *Proceedings of the 52nd ACM Symposium on Theory of Computing (STOC 2020)*, pages 902–915, 2020. `doi:10.1145/3357713.3384291`.

12 Nai-Hui Chia and Shih-Han Hung. Classical verification of quantum depth. *arXiv*, 2022. `doi:10.48550/arXiv.2205.04656`.

13 Andrew M Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC 2003)*, pages 59–68, 2003. `doi: 10.1145/780542.780552`.

---

[2] In fact, there exists a small issue in the current proof of Theorem 8.1 in [11]. However, it has already been fixed and the fixed proof can be applied to the setting of this work [10].

14   Richard Cleve and John Watrous. Fast parallel circuits for the quantum Fourier transform. In *Proceedings of 41st IEEE Annual Symposium on Foundations of Computer Science (FOCS 2000)*, pages 526–536, 2000. `doi:10.1109/SFCS.2000.892140`.

15   Matthew Coudron and Sanketh Menda. Computations with greater quantum depth are strictly more powerful (relative to an oracle). In *Proceedings of the 52nd ACM Symposium on Theory of Computing (STOC 2020)*, pages 889–901, 2020. `doi:10.1145/3357713.3384269`.

16   Bill Fefferman and Shelby Kimmel. Quantum vs. classical proofs and subset verification. In *Proceedings of 43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*, pages 22:1–22:23, 2018. `doi:10.4230/LIPIcs.MFCS.2018.22`.

17   Stephen A Fenner and Yong Zhang. A note on the classical lower bound for a quantum walk algorithm. *arXiv*, 2003. `doi:10.48550/arXiv.quant-ph/0312230`.

18   Richard Jozsa. An introduction to measurement based quantum computation. *arXiv*, 2005. `doi:10.48550/arXiv.quant-ph/0508124`.

19   Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. `doi:10.1017/CBO9780511976667`.

20   Daniel R. Simon. On the power of quantum computation. In *Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 116–123, 1994. `doi:10.1109/SFCS.1994.365701`.

21   Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6):1–76, 2015. `doi:10.1145/2817206`.

22   Han-Sen Zhong et al. Quantum computational advantage using photons. *Science*, 370:1460–1463, 2020. `doi:10.1126/science.abe8770`.