Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 59 (2003)

Polynomial Time Quantum Computation with Advice [*]

Harumichi Nishimura Tomoyuki Yamakami

School of Information Technology and Engineering
University of Ottawa, Ottawa, Ontario, Canada K1N 6N5

Abstract. Advice is supplementary information that enhances the computational power of an underlying computation. This paper focuses on advice that is given in the form of a pure quantum state and examines the influence of such advice on the behaviors of an underlying polynomial-time quantum computation with bounded-error probability.

Key Words: computational complexity, quantum circuit, advice function

1 Prologue

Quantum computation has emerged to shape a future computational paradigm based on quantum physics. To carry out a given task faster and more precisely, it is also practical to supplement such a quantum computation with a small piece of information beside an original input. Ideally, such information should be succinct and given equally to all inputs of fixed size. The notion of such supplemental information, under the name of "advice," was first sought in a classical setting by Karp and Lipton [15] in the early 1980s. Originally, Karp and Lipton introduced the notion of advice to characterize non-uniform models of computations, following the early work of Savage [21] and Adleman [1] on non-uniform Boolean circuits.

In this paper, we consider polynomial-time bounded-error quantum computations that take advice, which is given in the form of a pure quantum state (referred to as *quantum advice*). Of particular interest are the languages recognized by polynomial-time quantum computations with quantum advice under the condition that the quantum computations should not err with probability more than 1/3, provided that the given advice is correct. The major difference from the original definition of Karp and Lipton is that we do not impose any condition on the acceptance probability of an underlying quantum computation whenever advice is supplied incorrectly, since such languages, when advice is limited to classical states (specially called *classical advice*), establish a direct correspondence to non-uniform quantum circuits as well as tally languages. For simplicity, we use the notation $\mathrm{BQP}/^*\mathcal{F}$ for the collection of aforementioned languages with classical advice whose size is particularly described by functions in $\mathcal{F}$ (in contrast with the Karp-Lipton advice class $\mathrm{BQP}/\mathcal{F}$) and we write $\mathrm{BQP}/^*\mathrm{Q}\mathcal{F}$ for the quantum advice case, where prefix "Q" represents "quantum."

A central question on an advised computation is how to hide meaningful information into advice and how to recover this information from the advice with high accuracy. The key issue in this paper is an efficient use of quantum advice, from which the strengths and limitations of advised quantum computations follow. Using quantum fingerprinting [9], we demonstrate that subpolynomial-size quantum advice is more useful than classical advice of the same size. In contrast, quantum information theory sometimes draws a clear limitation on how efficiently we can hide information into quantum advice. Using quantum random access coding (QRAC) [3], we show that quantum advice cannot be made shorter than the 8 per cent of the size of classical advice for specific languages. Moreover, by combining the QRAC with our quantum-circuit characterization, we construct a set in EESPACE that does not belong to $\mathrm{BQP}/^*\mathrm{Qpoly}$. This result can be compared with Kannan's earlier result $\mathrm{ESPACE} \nsubseteq \mathrm{P/poly}$ [14].

The use of quantum amplitudes is another way to enhance computational power. We can hide information within amplitudes and use a quantum computation to access such information. Adleman, DeMarrais, and Huang [2] showed that quantum computation can benefit more from complex amplitudes than from rational amplitudes by proving $\mathrm{BQP}_{\mathbb{Q}} \neq \mathrm{BQP}_{\mathbb{C}}$. This clearly contrasts the recent result $\mathrm{NQP}_{\mathbb{Q}} = \mathrm{NQP}_{\mathbb{C}}$ [24]. To some extent, we can view such complex amplitudes as advice given to an underlying quantum computation with rational amplitudes. We show that a finite set of complex amplitudes are roughly equivalent to polylogarithmic advice.

[*] This work was in part supported by the Natural Sciences and Engineering Research Council of Canada.

ISSN 1433-8092

We assume the reader's familiarity with the fundamental concepts in the theory of computational complexity (e.g., [12]) and quantum computation (e.g., [18]). In this paper, all *logarithms* have base 2 and a *polynomial* means a multi-variate polynomial with integer coefficients. We fix our alphabet Σ to be $\{0,1\}$ unless otherwise stated. A *pairing function* $\langle\cdot,\cdot\rangle$ is a map from $\Sigma^*\times\Sigma^*$ to Σ^*, assumed to be one-to-one and polynomial-time computable with the polynomial-time computable inverse. We also use the same notation $\langle\cdot,\cdot\rangle$ for a standard bijection from $\mathbb{N}\times\mathbb{N}$ to $\mathbb{N}$, where $\mathbb{N}=\{0,1,2,\cdots\}$. A *quantum string* (*qustring*, for short) *of length* n is a pure quantum state of n qubits. For any qustring $|\phi\rangle$, $\ell(|\phi\rangle)$ denotes the length of $|\phi\rangle$. Let Φ_n be the collection of all qustrings of length n and define $\Phi_{\leq m}=\bigcup_{1\leq i\leq m}\Phi_i$. The union $\bigcup_{n\in\mathbb{N}}\Phi_n$ is denoted Φ_∞ [23]. For convenience, let $\mathbb{N}^+=\mathbb{N}-\{0\}$.

2 Advice for Quantum Computation

We focus on a polynomial-time quantum computation with bounded-error probability as an underlying computation that takes advice. We model a quantum computation by a *multi-tape quantum Turing machine* (*QTM*, for short) whose heads are allowed to stay still [8, 10, 20, 23]. Hereafter, the term "QTM" refers to a QTM M whose time-evolution is precisely described by a certain unitary operator over the space spanned by all configurations of M. For convenience, our QTMs as well as classical TMs are equipped with multiple input tapes. Whenever we write $M(x,y)$, we assume that x is given in M's *first* input tape and y is in the *second* input tape. Similarly, we use the notation $M(x,y,z)$ for three input tapes. Let $\mathrm{Prob}_M[M(|\phi_1\rangle,|\phi_2\rangle)=s]$ denote the probability that a binary string s is observed on the designated output tape of a QTM M after M halts on qustring inputs $|\phi_1\rangle$ and $|\phi_2\rangle$. When M's amplitudes are concerned, we say that M has *K-amplitudes* if all amplitudes of M are chosen from a subset K of $\mathbb{C}$.

Now, we want to define our central notion, a quantum advice complexity class. To cope with the quantum nature of underlying computations, we give the following special definition to our advice class. The justification of our definition will be given in Section 3. For simplicity, we identify a set A with its characteristic function (i.e., $A(x)=1$ if $x\in A$ and 0 otherwise).

Definition 2.1 Let f be any function from $\mathbb{N}$ to $\mathbb{N}$ and let $\mathcal{F}$ be any set of functions mapping from $\mathbb{N}$ to $\mathbb{N}$. Let K be any nonempty subset of $\mathbb{C}$.

1. A set A is in $\mathrm{BQP}_K/^*f$ (or $\mathrm{BQP}_K/^*f(n)$) if there exist a polynomial-time QTM M with K-amplitudes and a function h from $\mathbb{N}$ to Σ^* such that $\mathrm{Prob}_M[M(x,h(|x|))=A(x)]\geq 2/3$ for every $x\in\Sigma^*$, where $|h(n)|=f(n)$. This function h is called a *classical advice function* and f is the *length function* of h. Let $\mathrm{BQP}_K/^*\mathcal{F}=\bigcup_{f\in\mathcal{F}}\mathrm{BQP}_K/^*f$.

2. A set A is in $\mathrm{BQP}_K/^*\mathrm{Q}f$ (or $\mathrm{BQP}_K/^*\mathrm{Q}(f(n))$) if there exist a polynomial-time QTM M with K-amplitudes and a function h from $\mathbb{N}$ to Φ_∞ such that $\ell(h(|x|))=f(|x|)$ and $\mathrm{Prob}_M[M(x,h(|x|))=A(x)]\geq 2/3$ for every $x\in\Sigma^*$, where h is called a *quantum advice function*. Let $\mathrm{BQP}_K/^*\mathrm{Q}\mathcal{F}=\bigcup_{f\in\mathcal{F}}\mathrm{BQP}_K/^*\mathrm{Q}f$.

The prefix "BQP_K" in $\mathrm{BQP}_K/^*\mathcal{F}$ and $\mathrm{BQP}_K/^*\mathrm{Q}\mathcal{F}$ is an abbreviation of "bounded-error quantum polynomial-time with K-amplitudes." Similar notions can be introduced to probabilistic computations ($\mathrm{BPP}/^*\mathcal{F}$) and other types of quantum computations ($\mathrm{EQP}_K/^*\mathcal{F}$ and $\mathrm{QMA}_K/^*\mathcal{F}$). For readability, we suppress the subscript "K" if K is the set of all *polynomial-time approximable complex numbers* (that is, their real and imaginary parts are both deterministically approximated to within 2^{-k} in time polynomial in k). We are particularly interested in polynomial-length and logarithmic-length functions. Conventionally, write poly for the collection of all functions f from $\mathbb{N}$ to $\mathbb{N}$ satisfying that $f(n)\leq p(n)$ for all $n\in\mathbb{N}$, where p is a certain polynomial. Similarly, write log for the collection of all f's satisfying that $f(n)\leq c\log n+c$ for a certain fixed nonnegative integer c.

Earlier, Karp and Lipton [15] defined a general advice complexity class[†] $\mathcal{C}/\mathcal{F}$ for any class $\mathcal{C}$ of languages and any set $\mathcal{F}$ of length functions. This Karp-Lipton style definition naturally introduces another advice class $\mathrm{BQP}/\mathcal{F}$ for the *language class* BQP of Bernstein and Vazirani [8]. Clearly, $\mathrm{BQP}/\mathcal{F}$ is included in $\mathrm{BQP}/^*\mathcal{F}$ for any set $\mathcal{F}$ of length functions. The major difference between $\mathrm{BQP}/^*\mathcal{F}$ and $\mathrm{BQP}/\mathcal{F}$ is that the definition of $\mathrm{BQP}/^*\mathcal{F}$ lacks the promise-free property of underlying QTMs, where a QTM M is called *promise-free* if, for every pair (x,s), either $\mathrm{Prob}_M[M(x,s)=0]\geq 2/3$ or $\mathrm{Prob}_M[M(x,s)=1]\geq 2/3$. Such a difference seems, nonetheless, insignificant in the classical setting since the corresponding two definitions $\mathrm{BPP}/^*\mathrm{poly}$

[†] The Karp-Lipton advice class $\mathcal{C}/\mathcal{F}$ is the collection of all sets A for which there exist a set $B\in\mathcal{C}$, a function $f\in\mathcal{F}$, and a function h from $\mathbb{N}$ to Σ^* such that $A=\{x\mid\langle x,h(|x|)\rangle\in B\}$ provided that $|h(n)|=f(n)$ for all $n\in\mathbb{N}$.

and BPP/poly coincide[‡]. We note that there is no known proof for the collapse between BQP/*poly and BQP/poly. Their separation on the contrary seems difficult to prove since Promise-P = Promise-BQP implies P/$\mathcal{F}$ = BQP/$\mathcal{F}$ = BQP/$^*\mathcal{F}$, where Promise-$\mathcal{C}$ is the promise version of complexity class $\mathcal{C}$ [13].

The following fundamental properties hold for advice classes BQP/$^*\mathcal{F}$ and BQP/*Q$\mathcal{F}$. The *power set* of Σ^* is denoted 2^{Σ^*} in the lemma below.

Lemma 2.2 *Let f and g be any functions from $\mathbb{N}$ to $\mathbb{N}$ and let $\mathcal{F}$ and $\mathcal{G}$ be any sets of functions from $\mathbb{N}$ to $\mathbb{N}$.*
(1) BQP/*0 = BQP/*Q(0) = BQP.
(2) BQP/$^*2^n$ = BQP/*Q(2^n) = 2^{Σ^*}.
(3) BQP/$^*\mathcal{F}$ $\subseteq$ BQP/*Q$\mathcal{F}$.
(4) If $\mathcal{F} \subseteq \mathcal{G}$ then BQP/$^*\mathcal{F}$ $\subseteq$ BQP/$^*\mathcal{G}$ *and* BQP/*Q$\mathcal{F}$ $\subseteq$ BQP/*Q$\mathcal{G}$.
(5) If $g(n) < f(n) \leq 2^n$ for infinitely many n, then P/$^*f \nsubseteq$ BQP/$^*g$.

The complexity class BQP is known to enjoy a strong form of the so-called *amplification property*, for which we can amplify the success probability of any underlying QTM from 2/3 to $1-2^{-p(n)}$ for an arbitrary polynomial p. This form of the amplification property can be easily extended into any classical advice class BQP/$^*\mathcal{F}$. The quantum advice class BQP/*Q$\mathcal{F}$, however, demands a more delicate attention since quantum advice in general cannot be copied due to the *no-cloning theorem.* For the following lemma, we say that a set $\mathcal{F}$ of length functions is *closed under integer multiplication* if, for every $f \in \mathcal{F}$ and every integer $k \in \mathbb{Z}$, there exists a function $g \in \mathcal{F}$ such that $f(n) \cdot k \leq g(n)$ for all $n \in \mathbb{N}$.

Lemma 2.3 (Amplification Lemma) *Let $\mathcal{F}$ be any set of length functions. (1) A set A is in* BQP/$^*\mathcal{F}$ *if and only if, for every polynomial q, there exist a polynomial-time QTM M and a classical advice function h whose length function is in $\mathcal{F}$ such that* $\mathrm{Prob}_M[M(x,h(|x|)) = A(x)] \geq 1 - 2^{-q(|x|)}$ *for every x. (2) Assume that $\mathcal{F}$ is closed under integer multiplication. A set A is in* BQP/*Q$\mathcal{F}$ *if and only if, for every constant $\epsilon \geq 0$, there exist a polynomial-time QTM M and a quantum advice function h whose length function is in $\mathcal{F}$ such that* $\mathrm{Prob}_M[M(x,h(|x|)) = A(x)] \geq 1 - \epsilon$ *for every x.*

3 Non-Uniform Quantum Circuits and Tally Sets

Our definition BQP/$^*\mathcal{F}$ is preferable to the Karp-Lipton style definition BQP/$\mathcal{F}$ because, as shown in Lemma 3.1, our definition can precisely characterize non-uniform polynomial-size quantum circuits, where a *quantum circuit* [11, 25] is assumed to be built from a finite universal set of quantum gates and the *size* of a quantum circuit is the number of quantum gates in use.

Throughout this paper, we fix a *universal* set $\mathcal{U}$ of quantum gates, consisting of a Controlled-NOT gate and a finite number of single-qubit gates that generates a dense subset in $SU(2)$ with their inverses. Without loss of generality, we may assume that all entries of these quantum gates are polynomial-time approximable complex numbers. We say that a set A has *non-uniform polynomial-size quantum circuits with error probability* ϵ if there exist a polynomial p and a non-uniform family $\{C_n\}_{n\in\mathbb{N}}$ of quantum circuits such that, for every string x, (i) $C_{|x|}$ on input $|x\rangle|0^m\rangle$ outputs $A(x)$ with probability at least $1-\epsilon$, where $|0^m\rangle$ is an auxiliary input and (ii) $C_{|x|}$ uses at most $p(|x|)$ quantum gates chosen from $\mathcal{U}$. The notation $\mathrm{Prob}_C[C(x,y) = b]$ expresses the probability that C, taking x and y as a pair of inputs with an auxiliary input 0^m, outputs b to the first qubit of C.

Lemma 3.1 *(1) A set A is in* BQP/*poly *if and only if A has non-uniform polynomial-size quantum circuits with error probability at most* 1/3.
(2) A set A in BQP/*Qpoly *if and only if there exist a positive polynomial p, a non-uniform family $\{C_n\}_{n\in\mathbb{N}}$ of polynomial-size quantum circuits, and a series $\{U_n\}_{n\in\mathbb{N}}$ of unitary operators acting on $p(n)$ qubits such that, for every $n \in \mathbb{N}$ and every string x of length n,* $\mathrm{Prob}_{C_n}[C_n(x, U_n|0^{p(n)}\rangle) = A(x)] \geq 2/3$.

Obviously, Lemma 3.1(1) is a special case of (2). The “only if” part of Lemma 3.1(2) follows from the explicit simulation of QTMs by quantum circuits [19, 25]. For any set A in BQP/*Qpoly via a polynomial quantum advice function h, we can build a family $\{C_n\}_{n\in\mathbb{N}}$ of polynomial-size quantum circuits such that

[‡] Let $A \in$ BPP/*poly. By a standard majority vote technique, there exist a polynomial p, a polynomial-time deterministic TM M, and a polynomial advice function h such that $\mathrm{Prob}_{r\in\Sigma^{p(|x|)}}[M(x,h(|x|),r) = A(x)] \geq 1 - 2^{-2n}$ for all x. For each n, choose an $r_n \in \Sigma^{p(n)}$ that satisfies $M(x,h(n),r_n) = A(x)$ for all $x \in \Sigma^n$. By setting the new advice $k(n) = 0^{p(n)}1h(n)r_n$, we obtain $A \in$ P/poly $\subseteq$ BPP/poly.

$\mathrm{Prob}_{C_n}[C_n(x,h(n)) = A(x)] \geq 2/3$ for every x of length n. The "if" part needs an effective binary encoding of a quantum circuit, provided that the length of such an encoding is not less than the size of the circuit. We use the notation $Code(C)$ to describe this encoding of a quantum circuit C. If a quantum circuit C_n satisfies $\mathrm{Prob}_{C_n}[C_n(x, U_n|0^{p(n)}\rangle) = A(x)] \geq 2/3$ for every x of length n, the desired advice function $h(n)$ is defined to be the encoding $Code(C_n)$ tensored with the qustring $U_n|0^{p(n)}\rangle$. This puts A into BQP/*Qpoly via h. The above characterizations in Lemma 3.1 represent the clear difference between BQP/*Qpoly and BQP/*poly because $U_n|0^{p(n)}\rangle$ may be exponentially difficult to construct. However, it does not address the separation between BQP/*poly and BQP/*Qpoly.

The following lemma allows us to replace the unitary operator U_n in Lemma 3.1(2) by any exponential-size quantum circuit with no ancillary qubit. This lemma can be obtained directly from the Solovay-Kitaev theorem [16, 18] following the standard decomposition of unitary matrices [6]. For any complex square matrix A, let $\|A\| = \sup_{|\phi\rangle\neq 0} \|A|\phi\rangle\|/\||\phi\rangle\|$.

Lemma 3.2 *(1) For every sufficiently large $k \in \mathbb{N}$, every $|\phi\rangle \in \Phi_k$, and every $\epsilon > 0$, there exists a quantum circuit C acting on k qubits such that C has size at most $2^{2k}\log^3(1/\epsilon)$ and $\|C|0^k\rangle - |\phi\rangle\| < \epsilon$.*

(2) For every sufficiently large $k \in \mathbb{N}$, every k-qubit unitary operator U_k, and every $\epsilon > 0$, there exists a quantum circuit C acting on k qubits such that C has size at most $2^{3k}\log^3(1/\epsilon)$ and $\|U(C) - U_k\| < \epsilon$, where $U(C)$ is the unitary operator representing C.

The quantum-circuit characterization of BQP/*poly yields the following containment.

Proposition 3.3 BQP/*Qlog ⊆ BQP/*poly.

Proof. Assume that $A \in$ BQP/*Qlog. By Lemma 2.3(2), there exist a polynomial-time QTM M and a series $\{|\psi_n\rangle\}_{n\in\mathbb{N}}$ of qustrings of length logarithmic in n such that $\mathrm{Prob}_M[M(|x\rangle, |\psi_{|x|}\rangle) \neq A(x)] \leq 1/6$ for every string x. There exists a family $\{C_n\}_{n\in\mathbb{N}}$ of polynomial-size quantum circuits that simulate M. By Lemma 3.2(1), each $|\psi_n\rangle$ can be approximated to within $1/6$ by a certain quantum circuit D_n of size polynomial in n. Combining C_n with D_n produces a new quantum circuit of polynomial size that recognizes $A \cap \Sigma^n$. This implies that A has polynomial-size quantum circuits with error probability at most $1/6 + 1/6 = 1/3$. By Lemma 3.1(1), A is in BQP/*poly. □

Non-uniform quantum circuits also characterize polylogarithmic advice classes. For each positive integer k, let $\log^k$ be the collection of all functions f from $\mathbb{N}$ to $\mathbb{N}$ such that $f(n) \leq c(\log n)^k + c$ for any $n \in \mathbb{N}$, where c is a certain fixed nonnegative integer. In early 1990s, Balcázar, Hermo, and Mayordomo [5] showed that $\mathrm{P}/\log^k$ can be expressed in terms of Boolean circuits whose encodings belong to the resource-bounded Kolmogorov complexity class $K[\log^k, \mathrm{poly}]$, which is the collection of all languages A such that any string x in A can be produced deterministically in time polynomial in $|x|$ from a certain string w (called a *program*) of length at most $f(|x|)$ for a certain function $f \in \log^k$. The following lemma naturally expands their result into $\mathrm{BQP}/^*\log^k$.

Lemma 3.4 *Let $k \in \mathbb{N}^+$. A set A is in $\mathrm{BQP}/^*\log^k$ if and only if there is a non-uniform family $\{C_n\}_{n\in\mathbb{N}}$ of polynomial-size quantum circuits that recognize A with probability $\geq 2/3$ and satisfy $\{Code(C_n) \mid n \in \mathbb{N}\} \in K[\log^k, \mathrm{poly}]$.*

Notice that a polynomial-size quantum circuit can be encoded into a set of strings of polynomial length over a single-letter alphabet. Hence, there is a strong connection between polynomial-size quantum circuits and tally sets, where a *tally* set is a subset of $\{0\}^*$ or $\{1\}^*$. In particular, the collection of all tally sets is represented as TALLY. Using Lemma 3.1(1), we can establish the following tally characterization of BQP/*poly, which expands the classical result $\mathrm{P/poly} = \mathrm{P}^{\mathrm{TALLY}}$ [7]. This lemma also supports the legitimacy of our definition $\mathrm{BQP}/^*\mathcal{F}$.

Lemma 3.5 $\mathrm{BQP}/^*\mathrm{poly} = \mathrm{BQP}^{\mathrm{TALLY}}$.

The tally characterization of a logarithmic advice class draws special attention. Unlike BQP/*poly, BQP/* log is not closed even under polynomial-time Turing reductions (P-T-reductions, for short) since $\mathrm{P}^{\mathrm{BQP}/^*\log} = \mathrm{BQP}/^*\mathrm{poly}$ but BQP/*poly ≠ BQP/* log. Because of a similar problem on P/ log, Ko [17] gave an alternative definition to a logarithmic advice class, which is now known as Full-P/ log [4, 5]. (Ko [17] originally called this class Strong-P/ log.) Similarly, we introduce the new advice class Full-BQP/* log.

Definition 3.6 Let f be any length function. A set A is in Full-BQP/$^*f$ if there exist a polynomial-time QTM M and a function h from $\mathbb{N}$ to Σ^* such that, for all n, $|h(n)| = f(n)$ and $\mathrm{Prob}_M[M(x,h(n)) = A(x)] \geq 2/3$ for any string x of length at most n. For a class $\mathcal{F}$ of length functions, let Full-BQP/$^*\mathcal{F}$ denote the union $\bigcup_{f\in\mathcal{F}}$ Full-BQP/$^*f$.

It is clear from Definition 3.6 that Full-BQP/$^*\mathcal{F} \subseteq$ BQP/$^*\mathcal{F}$ for any set $\mathcal{F}$ of length functions. Note that Full-BQP/*poly $=$ BQP/*poly. Let TALLY2 denote the collection of all subsets of $\{0^{2^k} \mid k \in \mathbb{N}\}$ [4].

Lemma 3.7 Full-BQP/* log $= \mathrm{BQP}^{\mathrm{TALLY2}}$.

The proof of Lemma 3.7 is a straightforward modification of the proof for Full-P/ log $= \mathrm{P}^{\mathrm{TALLY2}}$ [4, 5]. It immediately follows from the lemma that Full-BQP/* log is closed under P-T-reductions.

4 Power of Quantum Advice

To make efficient use of quantum advice, we want to embed classical information schematically into shorter quantum advice and retrieve the information using quantum computation with small errors. The following theorem implies that subpolynomial quantum advice is more useful than classical advice of the same size. For the theorem, we introduce the following terminology: a function f from $\mathbb{N}$ to $\mathbb{N}$ is called *infinitely-often polynomially bounded* if there is a positive polynomial p such that $f(n) \leq p(n)$ for infinitely-many numbers n in $\mathbb{N}$.

Theorem 4.1 *Let f be any positive length function. If f is infinitely-often polynomially bounded, then* BQP_K/*Q$(O(f(n)\log n)) \nsubseteq$ BQP/$^*f(n)\cdot n$, *where* $K = \{0,1\}$.

By choosing an appropriate f in Theorem 4.1, we obtain the following consequence. The union of $\log^k$ for all $k \in \mathbb{N}^+$ is denoted *polylog*.

Corollary 4.2 *(1)* BQP/* log $\neq$ BQP/*Qlog.
(2) BQP/$^*n^k \neq$ BQP/*Q(n^k) *for each fixed* $k \in \mathbb{N}^+$.
(3) BQP/*Qlog $\nsubseteq$ BQP/*polylog *and hence,* BQP/*polylog $\neq$ BQP/*Qpolylog.

To prove Theorem 4.1, we use the notion of quantum fingerprinting introduced by Buhrman, Cleve, Watrous, and de Wolf [9]. The following simple quantum fingerprint given in [22] suffices for our proof. Fix n and $\epsilon > 0$. Let $\mathbb{F}_{n,\epsilon}$ be any field of size $pw(n/\epsilon)$, where $pw(m)$ is the least prime power larger than m. Note that $pw(n/\epsilon) \leq 2n/\epsilon$. For any string $x = x_1\cdots x_n$ of length n, the *quantum fingerprint* $|\phi_n(x)\rangle$ of x is the qustring of length $2\lceil\log(pw(n/\epsilon))\rceil$ defined by $|\phi_n(x)\rangle = (1/\sqrt{|\mathbb{F}_{n,\epsilon}|})\sum_{z\in\mathbb{F}_{n,\epsilon}}|z\rangle|p_x(z)\rangle$, where $p_x(z)$ denotes the polynomial $p_x(z) = \sum_{i=1}^{n} x_i \cdot z^{i-1}$ over $\mathbb{F}_{n,\epsilon}$.

Proof of Theorem 4.1. Fix an arbitrary positive polynomial p satisfying $f(n) \leq p(n)$ for infinitely-many n in $\mathbb{N}$. Assume an effective enumeration of polynomial-time QTMs, say $\{M_i\}_{i\in\mathbb{N}^+}$. We construct by stages the set L that separates BQP_K/*Q$(O(f(n)\log n))$ from BQP/$^*f(n)n$. At stage 0, let $n_0 = 0$. At stage $i \geq 1$, choose the minimal integer n_i such that $n_i > n_{i-1}$, $f(n_i) \leq p(n_i)$, and $n_i > 2(1+\log p(n_i))$. Consider the collection C_{n_i} of all sets $A \subseteq \Sigma^{n_i}$ that satisfy the following criterion: there exists a string $s \in \Sigma^{f(n_i)n_i}$ satisfying $\mathrm{Prob}_{M_i}[M_i(x,s) = A(x)] \geq 2/3$ for all $x \in \Sigma^{n_i}$. Note that there are at most $2^{f(n_i)n_i}$ such sets. By contrast, there are exactly $\sum_{j=0}^{2f(n_i)}\binom{2^{n_i}}{j}$ subsets of Σ^{n_i} of cardinality at most $2f(n_i)$. Since $\sum_{j=0}^{2f(n_i)}\binom{2^{n_i}}{j} > (2^{n_i}/2f(n_i))^{2f(n_i)} > 2^{f(n_i)n_i} \geq |C_{n_i}|$, we can find a set $L_{n_i} \subseteq \Sigma^{n_i}$ of cardinality $\leq 2f(n_i)$ that does not belong to C_{n_i}. Take such a set L_{n_i} for each $i \in \mathbb{N}^+$ and define $L = \bigcup_{i\geq 1} L_{n_i}$. Since $L_{n_i} \notin C_{n_i}$ for all $i \in \mathbb{N}^+$, L is located outside BQP/$^*f(n)n$.

To complete the proof, we show that L is in BQP/*Q$(f(n)\log n)$. Write $k(n)$ for $2f(n)n$. Fix i and write n for n_i for readability. Take a field $\mathbb{F}_{k(n),1/4}$ and define $g(n) = |0^m1\rangle|\phi_{k(n)}(y_1)\rangle|\phi_{k(n)}(y_2)\rangle\cdots|\phi_{k(n)}(y_m)\rangle$ when $L_n = \{y_1, y_2, \ldots, y_m\}$ for a certain number $m \leq 2f(n)$. Recall that $|\mathbb{F}_{k(n),1/4}| \geq 8nf(n)$. Consider the following algorithm $\mathcal{A}$: given input $(x, g(|x|))$, if, for some $i \in \{1,2,\ldots,m\}$, the first half part of $|\phi_{k(n)}(y_i)\rangle$ is z and $p_x(z)$ equals the second half part of $|\phi_{k(n)}(y_i)\rangle$, then accept the input. If there is no such i, then reject the input.

Now, take any string x of length n. Clearly, if $x \in L_n$, then $\mathcal{A}$ always accepts the input in time polynomial in $n + g(n)$. If $x \notin L_n$, then $p_x \neq p_{y_j}$ for any $j \in \{1,\ldots,m\}$. Since p_x and p_{y_j} have degree at most

$n-1$, they agree on at most $n-1$ elements in $\mathbb{F}_{k(n),1/4}$. Thus, the probability that $\mathcal{A}$ erroneously accepts the input is at most $m\cdot(n-1)/|\mathbb{F}_{k(n),1/4}| < 1/4$. Overall, we can recognize L with error probability at most $1/4$ in polynomial time. Since $f(n)\leq p(n)$, the length of quantum advice $g(n)$ is at most $f(n)+1+2\lceil f(n)\log(pw(4f(n)n))\rceil \leq cf(n)\log n + c$, where c is an appropriate constant independent of n. Hence, we have $L\in \mathrm{BQP}_K/^*\mathrm{Q}(O(f(n)\log n))$. □

A careful examination of the above proof suggests that a deterministic Turing machine with "randomly selected" classical advice of size $f(n)n$ can replace a QTM with quantum advice of the same size. The difference between randomly selected advice and quantum advice is open while the former can be simulated by the latter.

5 Limitation of Quantum Advice

Quantum fingerprinting demonstrates in Section 4 an efficient way to compress a large volume of classical information into relatively-short quantum advice. There is, however, a quantum information theoretical limitation on such quantum compression. In the following theorem, we claim that quantum advice cannot be made shorter than classical advice with the multiplicative factor of at least 0.08 on the QTMs.

Theorem 5.1 *For any positive length function f such that $f(n)\leq 2^n$, $\mathrm{P}/f \nsubseteq \mathrm{BQP}/^*\mathrm{Q}(0.08f(n))$.*

Theorem 5.1 contrasts with the result $\mathrm{P}/f\nsubseteq \mathrm{BQP}/^*(f(n)-1)$ obtained from Lemma 2.2(5). As a consequence of Theorem 5.1, we can show the following corollary.

Corollary 5.2 *(1)* $\mathrm{P}/\log^2 \nsubseteq \mathrm{BQP}/^*\mathrm{Qlog}$.
(2) $\mathrm{P}/\mathrm{poly}\nsubseteq \mathrm{BQP}/^*\mathrm{Q}(n^k)$ *for each fixed $k\in\mathbb{N}^+$ and hence* $\mathrm{BQP}/^*\mathrm{Qlog}\neq \mathrm{BQP}/^*\mathrm{poly}$.
(3) $\mathrm{BQP}/^*\mathrm{Qlog}\subsetneq \mathrm{BQP}/^*\mathrm{Q}(n^k)\subsetneq \mathrm{BQP}/^*\mathrm{Qpoly}$ *for each fixed $k\in\mathbb{N}^+$.*

The proof of Theorem 5.1 requires a lower bound of quantum random access encodings introduced by Ambainis, Nayak, Ta-shma, and Vazirani [3]. An (n,m,p)-*quantum random access coding* (QRAC) is a function f that maps n-bit strings to (pure or mixed) quantum states over m qubits satisfying the following: for every $i\in\{1,\ldots,n\}$, there is a measurement O_i with outcome 0 or 1 such that $\mathrm{Prob}[O_i(f(x))=x_i]\geq p$ for all $x\in\Sigma^n$. It is known in [3] that any (n,m,p)-QRAC should satisfy the inequality $m\geq(1-H(p))n$, where $H(p)=-p\log p-(1-p)\log(1-p)$. We now prove Theorem 5.1.

Proof of Theorem 5.1. Let $\{M_i\}_{i\in\mathbb{N}^+}$ be any effective enumeration of polynomial-time QTMs. We build by stages the set $L=\bigcup_{n\in\mathbb{N}}L_n$ that separates $\mathrm{P}/\mathcal{F}$ from $\mathrm{BQP}/^*\mathrm{Q}(0.08f(n))$. At stage n, consider the set $\mathcal{A}_n$ of all subsets of $\{x\in\Sigma^n \mid x \text{ is lexicographically at most } s_{f(n)}\}$, where s_i is lexicographically the ith string in Σ^n. Note that $\mathcal{A}_n$ can be viewed as the set of all strings of length $f(n)$. For each $s\in\Sigma^{f(n)}$, let B_s be the set in $\mathcal{A}_n$ such that $s=B_s(s_1)B_s(s_2)\cdots B_s(s_{f(n)})$. Consider any number $m\geq 1$ satisfying the following: for every $s\in\Sigma^{f(n)}$, there exists a qustring $|\phi_s\rangle\in\Phi_m$ such that $\mathrm{Prob}_{M_n}[M_n(x,|\phi_s\rangle)=B_s(x)]\geq 2/3$ for all $x\in\Sigma^n$. Since the function g defined as $g(s)=|\phi_s\rangle$ for every $s\in\Sigma^{f(n)}$ is an $(f(n),m,2/3)$-QRAC, we obtain $m\geq(1-H(1/3))f(n)>0.08f(n)$ for all n. Therefore, there exists a string $s\in\Sigma^{f(n)}$ such that no qustring $|\phi\rangle$ in Φ_m, where $m\leq 0.08f(n)$, satisfies $\mathrm{Prob}_{M_n}[M_n(x,|\phi\rangle)=B_s(x)]\geq 2/3$ for all $x\in\Sigma^n$. Choose such an s and define $L_n=B_s$. The above construction guarantees that $L\notin \mathrm{BQP}/^*\mathrm{Q}(0.08f(n))$. Since $|L_n|\leq f(n)$ for all n, we have $L\in\mathrm{P}/f$. □

Another application of QRACs yields the existence of a set in EESPACE that does not belong to BQP/*Qpoly, where EESPACE is the class of all sets computed by deterministic Turing machines using $2^{2^{O(n)}}$ space. Similarly, ESPACE is defined using $2^{O(n)}$ space.

Theorem 5.3 *(1)* $\mathrm{ESPACE}\nsubseteq \mathrm{BQP}/^*\mathrm{poly}$.
(2) $\mathrm{EESPACE}\nsubseteq \mathrm{BQP}/^*\mathrm{Qpoly}$.

Theorem 5.3(1) expands Kannan's result ESPACE $\nsubseteq$ P/poly [14]. The proof of Theorem 5.3(2) combines a diagonalization argument with the lower bound of QRACs.

Proof of Theorem 5.3. We show only 2) since 1) can be obtained by an argument similar to the proof of ESPACE $\nsubseteq$ P/poly [14]. Let $\{M_i\}_{i\in\mathbb{N}^+}$ be any effective enumeration of all polynomial-time QTMs and let $\{p_i\}_{i\in\mathbb{N}^+}$ be that of all polynomials with nonnegative coefficients. Note from Lemma 3.2(1) that any qustring of length m can be approximated to within $1/6$ by a certain quantum circuit with input $|0^m\rangle$ of size at most 2^{2m+6}. Consider the following algorithm $\mathcal{A}$ that starts with the empty input and proceeds by stages.

> At stage 0, set $Q = \emptyset$. At stage $n \geq 1$, first enumerate all numbers in $\{1, 2, \ldots, n\} \setminus Q$ in the increasing order. For each of such numbers m, we carry out the following procedure. At round $m = \langle i, j\rangle$, for each quantum circuit D of size at most $2^{2p_i(n)+6}$ acting on $p_i(n)$ qubits, compute $z_D^{(m)} = z_1 \cdots z_{2^n}$ as follows. For each k $(1 \leq k \leq 2^n)$, let z_k be the outcome (either 0 or 1) of M_j on input $(s_k, D|0^{p_i(n)}\rangle)$ with probability $\geq 5/6$, where s_k is lexicographically the kth string in Σ^n. If some z_k does not exist, then let $z_D^{(m)}$ be undefined and go to next D. After all D's are examined, consider the set Z of all $z_D^{(m)}$'s (which are defined). If both $Z = \Sigma^{2^n}$ and $m < n$, then go to next round $m + 1$. Assume otherwise. If $m = n$ then output $\perp$, or else output the minimal z not in Z and let $Q = Q \cup \{m\}$. Go to next stage $n + 1$.

Now, we show that Q eventually equals $\mathbb{N}$. Assume otherwise. Let $m = \langle i, j\rangle$ be the minimal number not in Q. Take any sufficiently large number n_0 and assume that, at any stage $n \geq n_0$, $\mathcal{A}$ always checks M_j at its first round. This happens when Σ^{2^n} equals the set of all $z_D^{(m)}$'s for all $n \geq n_0$. Hence, for every length $n \geq n_0$ and every set $A \subseteq \Sigma^n$, there exists a qustring $|\phi_{n,A}\rangle$ of length $p_i(n)$ such that $\mathrm{Prob}_{M_i}[M_i(x, |\phi_{n,A}\rangle) = A(x)] \geq 2/3$ for all $x \in \Sigma^n$. Letting $A[n] = A(0^n)A(0^{n-1}1)\cdots A(1^n)$ for each n, we define $f(A[n]) = |\phi_{n,A}\rangle$. Since f is a $(2^n, p_i(n), 2/3)$-QRAC, it follows that $p_i(n) \geq (1 - H(1/3))2^n > 0.08 \cdot 2^n$ for all $n \geq n_0$, a contradiction. Therefore, $Q = \mathbb{N}$.

The desired language L is defined as follows: $x \in L$ if and only if $\mathcal{A}$ outputs a binary string whose kth bit is 1 at stage $|x|$, assuming that x is the kth string in $\Sigma^{|x|}$. Then, L is not in BQP/*Qpoly since, otherwise, L is recognized by a certain QTM M_j with quantum advice of length $p_i(n)$ with high probability, and thus $\langle i, j\rangle \notin Q$, which contradicts $Q = \mathbb{N}$. On the other hand, $L \in$ EESPACE since $L(x)$ is computed by running $\mathcal{A}$ up to stage $|x|$ using space $2^{O(2^{|x|})}$. □

6 Roles of Amplitudes as Advice

Amplitudes can be viewed as a resource given to quantum computations. We can hide meaningful information within amplitudes and recover it using a certain type of quantum computation. Adleman, DeMarrais, and Huang [2] first demonstrated how to hide such information and proved that $\mathrm{BQP}_{\mathbb{C}}$ properly includes BQP, which equals $\mathrm{BQP}_{\mathbb{Q}}$. We further claim that amplitudes may play a role of logarithmic advice.

Theorem 6.1 Full-BQP/$^*\log \subseteq \mathrm{BQP}_{\mathbb{C}} \subseteq$ BQP/$^*\log^3$.

Proof. The first inclusion is shown in the following fashion. It is sufficient to prove that TALLY2 $\subseteq \mathrm{BQP}_{\mathbb{C}}$ since Full-BQP/$^*\log = \mathrm{BQP}^{\mathrm{TALLY2}} \subseteq \mathrm{BQP}^{\mathrm{BQP}_{\mathbb{C}}} = \mathrm{BQP}_{\mathbb{C}}$ by Lemma 3.7. Assume that L is any set in TALLY2. We encode L into the real number $\theta_L = 2\pi(\sum_{n=1}^{\infty} \frac{h(n)}{8^n})$, where $h(n) = (-1)^{1-L(0^{2^n})}$. Consider the QTM M that carries out the following algorithm: given input x, reject x if $x \neq 0^{2^k}$ for any $k \in \mathbb{N}$. If $x = 0^{2^k}$ for $k = \log|x|$, then prepare the state $|0\rangle$, conduct the transformation $|0\rangle \mapsto \cos(8^{k-1}\theta_L + \pi/4)|0\rangle + \sin(8^{k-1}\theta_L + \pi/4)|1\rangle$, and measure it on the $\{|0\rangle, |1\rangle\}$-basis. If the result of the measurement is 1, then accept x, or else reject x. An argument similar to the proof of Theorem 5.1 in [2] shows that, on any input x, M outputs $L(x)$ in polynomial time with probability at least $2/3$. This concludes that L is indeed in $\mathrm{BQP}_{\mathbb{C}}$. The second inclusion is shown as follows. Let L be any set in $\mathrm{BQP}_{\mathbb{C}}$ recognized by a polynomial-time QTM M with error probability $\leq 2^{-n}$ together with its amplitudes chosen from $\mathbb{C}$. Let p be any polynomial that bounds the running time of M. Since the transition function of M is a finite function, it induces the corresponding unitary operator acting over a finite-dimensional Hilbert space. Let $U(M)$ denote this unitary operator. By choosing $k = \dim(U(M))$ and $\epsilon = 1/n^c$ for a sufficiently large $c > 0$ in Lemma 3.2(2), we obtain a family of quantum circuits $\{C_n \mid n \in \mathbb{N}\}$ of size $O(\log^3 n)$ such that each C_n implements a unitary matrix $U(C_n)$ satisfying $||U(C_n) - U(M)|| \leq 1/3p(n)$. Note that all single-qubit gates in C_n have polynomial-time approximable numbers as their components. With the help of the encoding $Code(C_n)$ as an advice string, we can simulate M with error probability at most $p(n) \cdot (1/3p(n)) \leq 1/3$ in polynomial time. This implies that L is in $\mathrm{BQP}/^* \log^3$. □

Theorem 6.1 leads to the following direct consequence.

Corollary 6.2 *(1)* $\mathrm{BQP}_{\mathbb{C}} \subsetneq \mathrm{BQP}/^*\mathrm{polylog}$.
(2) $\mathrm{BQP}_{\mathbb{Q}}/^*\mathcal{F} = \mathrm{BQP}_{\mathbb{C}}/^*\mathcal{F}$ *and* $\mathrm{BQP}_{\mathbb{Q}}/^*\mathrm{Q}\mathcal{F} = \mathrm{BQP}_{\mathbb{C}}/^*\mathrm{Q}\mathcal{F}$ *for any* $\mathcal{F} \in \{\mathrm{polylog}, \mathrm{poly}\}$.

The proof of Corollary 6.2(2) needs the fact that $\mathrm{BQP}_{\mathbb{Q}}/^*\mathcal{F} = \mathrm{BQP}/^*\mathcal{F}$ and $\mathrm{BQP}_{\mathbb{Q}}/^*\mathrm{Q}\mathcal{F} = \mathrm{BQP}/^*\mathrm{Q}\mathcal{F}$ for any set $\mathcal{F}$. In Theorem 6.1, however, we cannot replace Full-BQP/* log by BQP/* log or even BQP/*1.

Proposition 6.3 $\mathrm{BQP}/^*1 \nsubseteq \mathrm{BQP}_{\mathbb{C}}$ *and thus,* $\mathrm{BQP}/^* \log \nsubseteq \mathrm{BQP}_{\mathbb{C}}$.

Proof. Assume that $\mathrm{BQP}/^*1 \subseteq \mathrm{BQP}_{\mathbb{C}}$. Recall from Lemma 3.5 that $\mathrm{BQP}/^*\mathrm{poly} = \mathrm{BQP}^{\mathrm{TALLY}}$. Since $\mathrm{TALLY} \subseteq \mathrm{BQP}/^*1$, it follows that $\mathrm{BQP}/^*\mathrm{poly} = \mathrm{BQP}^{\mathrm{TALLY}} \subseteq \mathrm{BQP}^{\mathrm{BQP}/^*1} \subseteq \mathrm{BQP}^{\mathrm{BQP}_{\mathbb{C}}} = \mathrm{BQP}_{\mathbb{C}}$. Hence, we obtain $\mathrm{BQP}_{\mathbb{C}} = \mathrm{BQP}/^*\mathrm{poly}$, which contradicts Corollary 6.2(1). □

7 Epilogue

We have initiated a study of advised quantum computations and addressed several relations among complexity classes with classical or quantum advice and some known complexity classes. The important questions we left open include: (1) $\mathrm{BQP}/^*\mathrm{poly} =?\, \mathrm{BQP}/^*\mathrm{Qpoly}$, (2) $\mathrm{BQP} \subseteq?\, \mathrm{EQP}/^*\mathrm{Qpoly}$, and (3) $\mathrm{ESPACE} \nsubseteq?\, \mathrm{BQP}/^*\mathrm{Qpoly}$.

References

[1] L. Adleman. Two theorems on random polynomial time. In *Proc. 19th Symposium on Foundations of Computer Science*, pp.75–83, 1978.

[2] L. M. Adleman, J. DeMarrais and M. A. Huang. Quantum computability. *SIAM J. Comput.* **26** (1997) 1524–1540.

[3] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. of the ACM* **49** (2002) 496–511.

[4] J. L. Balcázar and M. Hermo. The structure of logarithmic advice complexity classes *Theoret. Comput. Sci.* **207** (1998) 217–244.

[5] J. L. Balcázar, M. Hermo, and E. Mayordomo. Characterizations of logarithmic advice complexity classes. In *Proc. 12th IFIP World Computer Congress* Vol.1, North-Holland, pp.315–321, 1992.

[6] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A.* **52** (1995) 3457–3467

[7] L. Berman and J. Hartmanis. On isomorphisms and density of NP and other complexity classes. *SIAM J. Comput.* **6** (1977) 305–322.

[8] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.* **26** (1997) 1411–1473.

[9] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.* **87(16)** 167902 September 26 (2001)

[10] D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum computer. *Proc. R. Soc. London* Ser. A **400** (1985) 97–117.

[11] D. Deutsch. Quantum computational networks. *Proc. R. Soc. London* Ser. A **425** (1989) 73–90.

[12] D. Du and K. Ko. *Theory of Computational Complexity* (2000), John Wiley & Sons, Inc.

[13] S. Even and Y. Yacobi. Cryptocomplexity and NP-completeness. In *Proc. 7th Colloquium on Automata, Languages, and Programming*, Lecture Notes in Comput. Sci., Vol.85, pp.195–207, 1980.

[14] R. Kannan. Circuit-size lower bounds and non-reducibility to sparse sets. *Inform. Control* **55** (1982) 40–56.

[15] R. M. Karp and R. Lipton. Turing machines that take advice. *L'Enseignement Mathematique* **28** (1982) 191–209.

[16] A. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys* **52** (1997) 1191–1249.

[17] K. Ko. On helping by robust oracle machines. *Theoret. Comput. Sci.* **52** (1987) 15–36.

[18] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information* (2000), Cambridge University Press.

[19] H. Nishimura and M. Ozawa. Computational complexity of uniform quantum circuit families and quantum Turing machines. *Theoret. Comput. Sci.* **276** (2002) 147–187.

[20] M. Ozawa and H. Nishimura. Local transition functions of quantum Turing machines. *RAIRO Theor. Inform. Appl.* **34** (2000) 379–402.

[21] S. E. Savage. Computational work and time on finite machines. *J. of the ACM* **19** (1972) 660–674.

[22] R. de Wolf. *Quantum Computing and Communication Complexity.* PhD dissertation. University of Amsterdam, 2001.

[23] T. Yamakami. A foundation of programming a multi-tape quantum Turing machine. In *Proc. 24th International Symposium on Mathematical Foundations of Computer Science*, Lecture Notes in Comput. Sci., Vol.1672, pp.430–441, 1999.

[24] T. Yamakami and A. C. Yao. $\mathrm{NQP}_{\mathbb{C}} = \mathrm{co}\text{-}\mathrm{C}_{=}\mathrm{P}$. *Inform. Process. Lett.* **71** (1999) 63–69.

[25] A. C. Yao. Quantum circuit complexity. In *Proc. 34th Annual IEEE Symposium on Foundations of Computer Science*, pp.352–361, 1993.