Invited Paper

Quantum Computation with Supplementary Information

Harumichi Nishimura†

The notion of advised computation was introduced by Karp and Lipton to represent non-uniform complexity in terms of Turing machines. Since then, advised computation has been one of the basic concepts of computational complexity. Recently, the research of advised computation has been originated also in the field of quantum computing. This paper reviews the study of advised quantum computation.

1. Introduction

Turing machines and Boolean circuits are used mostly as computing models to study the uniform and non-uniform complexity, respectively. We can take two approaches to compare between these two computing models. One approach is to restrict how to construct Boolean circuits, which means that the families of Boolean circuits should satisfy a uniform condition. The other is to supplement Turing machines with non-uniform information, called *advice*. As the latter approach, Karp and Lipton [17)] initiated the notion of complexity classes with advice in 1980. Since then, the study of advised computation has been elaborated to understand the power and the limit of non-uniform computation, and the notion of advice complexity classes has appeared in many phrases of computational complexity.

After Shor's excellent quantum algorithm for the factoring problem, a number of complexity notions were imported from classical complexity theory to quantum computing; nondeterministic computation, finite automata, interactive proof systems, and so on. The notion of advice is not an exception for this trend. The research of advised quantum computation was started just a few years ago. In quantum computation, we have two choices as the supplementary information that is given to quantum Turing machines; classical advice (binary strings) and quantum advice (quantum states). While classical advice is suitable to characterize polynomial-size quantum circuits, quantum advice is considered to be a natural quantum analogue of the non-uniform measure of computation. The results obtained so far on advised quantum computation are not yet so many, but the author believes that hereafter the theory of advised quantum computation should be furthermore developed from the importance of non-uniform computation in complexity theory. In this belief, this article surveys the research of quantum computation with advice.

This article is organized as follows. In Section 2, we give uniform complexity classes that appear in this article. In Section 3 we introduce quantum advice complexity classes and compare them and their basic results with classical advice classes. In Section 4, we discuss the amplitudes of quantum Turing machines from the viewpoint of non-uniform quantum complexity classes. Some relation of advised computation to one-way communication complexity is seen in Section 5. In Section 6 we consider a separation between the two quantum complexity classes with polynomial classical advice and with polynomial quantum advice. In Section 7 we review quantum complexity classes with short advice. Comparisons among uniform complexity classes and quantum advice classes are reviewed in Section 8. Finally, we look at the future work with several open problems.

2. Uniform Complexity Classes

To classify the power of uniform machines, a multiplicity of complexity classes for recognizing sets (that is, computing Boolean functions) have been introduced in complexity theory. They are often called *uniform complexity classes* compared to complexity classes with advice, called *non-uniform complexity classes*. In what follows, let $\Sigma = \{0,1\}$. Also, we assume the familiarity with basics of structural complexity [13)] and quantum computing [14),22)].

First, let us recall several classical uniform complexity classes. Let P (NP, resp.) denote the class of sets recognized by polynomial-time

† ERATO Quantum Computation and Information Project, Japan Science and Technology Agency

deterministic (nondeterministic, resp.) Turing machines. Let BPP be the class of sets recognized with bounded error (say, with probability $\geq 2/3$) by polynomial-time probabilistic Turing machines. Let PP be the class of sets recognized with unbounded error (that is, with probability $> 1/2$) by polynomial-time probabilistic Turing machines. Let PSPACE (ESPACE, resp.) be the class of sets recognized by deterministic Turing machines in polynomial space (in space $2^{O(n)}$, resp.).

The quantum Turing machine, an analogue of the probabilistic Turing machine, is a mathematical model of the quantum computer. Each transition of a quantum Turing machine M is determined by a complex-valued finite transition function δ as follows: if the inner state of M is p and the tape head of M scans σ, then the inner state becomes q, and the tape head changes σ to τ and moves to direction d with (probability) amplitude $\delta(p,\sigma,q,\tau,d)$. Let BQP[7)] denote the class of sets recognized with bounded error by polynomial-time quantum Turing machines. (In fact, the transition amplitudes taken by quantum Turing machines are restricted to a subset of complex numbers, as discussed in Section 4). Since quantum Turing machines can simulate probabilistic Turing machines, BPP is included in BQP[7)]. Moreover, the relationships among the above uniform complexity classes are given as follows.

Fact 2.1 *The following relations hold*[3),7),13)].

1) P $\subseteq$ BPP $\subseteq$ BQP $\subseteq$ PP $\subseteq$ PSPACE $\subseteq$ ESPACE.

2) P $\subseteq$ NP $\subseteq$ PP.

3. Quantum Advice Complexity Classes

Now we introduce advice complexity classes. First, we recall a general advice complexity class by Karp and Lipton[17)], which is defined based on the uniform complexity class.

Definition 3.1 Let $\mathcal{C}$ be a class of sets, and let f be a function from $\mathbb{N}$ to $\mathbb{N}$. A set A is in the Karp-Lipton advice class $\mathcal{C}/f$ if there exist a set $B \in \mathcal{C}$ 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 $n \in \mathbb{N}$. Let $\mathcal{C}/\mathcal{F} = \bigcup_{f\in\mathcal{F}} \mathcal{C}/f$ for any set of functions $\mathcal{F}$ from $\mathbb{N}$ to $\mathbb{N}$.

For the class P and the set poly of polynomially bounded functions, we obtain the most representative advice class P/poly. (A function f from $\mathbb{N}$ to $\mathbb{N}$ is called polynomially bounded if there exists a polynomial p such that $f(n) \leq p(n)$ for any $n \in \mathbb{N}$). It is well-known that P/poly exactly characterizes the class of sets recognized by polynomial-size Boolean circuits[17)]. According to Definition 3.1, we can also consider a quantum advice class BQP/poly. However, it is not known whether BQP/poly characterizes the class of sets recognized by polynomial-size quantum circuits. In fact, it can be easily seen that all sets in BQP/poly are recognized by polynomial-size quantum circuits similar to the classical case while the converse fails to show by the following method of the classical case:

To simulate a polynomial-size circuit by a deterministic Turing machine, the code of the circuit is given as advice, and then the set recognized by the circuit can be also recognized by the deterministic Turing machine in polynomial time.

The reason why this method fails for BQP/poly is that polynomial-size quantum circuits do not always satisfy the bounded-error condition. In addition, Definition 3.1 is not meant for extending advice strings $h(n)$ to quantum states without considering the complexity class of quantum states. Thus, at present, the definition of the quantum complexity class with advice is given based on the bounded-error quantum computer[1),24)].

Definition 3.2 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 $\mathbb{N}$.

1. A set A is in BQP/$^*f$ if there exist a polynomial-time quantum Turing machine M and a function h from $\mathbb{N}$ to Σ^* such that M on input $(x, h(|x|))$ produces $A(x)$ with probability at least 2/3 for every $x \in \Sigma^*$, where $|h(n)| = f(n)$. Let BQP/$^*\mathcal{F} = \bigcup_{f\in\mathcal{F}}$ BQP/$^*f$.
2. A set A is in BQP/*Qf if there exist a polynomial-time quantum Turing machine M and a function h from $\mathbb{N}$ to the set of (pure) quantum states such that M on input $(x, h(|x|))$ produces $A(x)$ with probability at least 2/3 for every $x \in \Sigma^*$, where $h(n)$ is an $f(n)$-qubit state. Let BQP/*Q$\mathcal{F} = \bigcup_{f\in\mathcal{F}}$ BQP/*Qf.

Under Definition 3.2, we can exactly characterize polynomial-size quantum circuits in terms of the quantum advice complexity class BQP/*poly[☆].

Proposition 3.3 *A set A is in* BQP/*poly *if*

[☆] In Ref. 1), BQP/*poly and BQP/*Qpoly are respectively denoted by BQP/poly and BQP/qpoly.

and only if A can be recognized with probability at least $2/3$ by a polynomial-size quantum circuit family.

The class P/poly has another characterization to clarify the relationship between obtaining non-uniform information from polynomially long advices and obtaining it from oracles. Let TALLY be the collection of subsets of $\{0^n \mid n \in \mathbb{N}\}$. Then, $\mathrm{P/poly} = \mathrm{P}^{\mathrm{TALLY}}$. Similarly, we can see that BQP/*poly coincides with $\mathrm{BQP}^{\mathrm{TALLY}}$.

Remark 3.4 One might consider that the possibility of a gap between two definitions such as Definitions 3.1 and 3.2 will occur also for the bounded-error class BPP. However, we can see that BPP/*poly coincides with BPP/poly using the proof technique to show BPP $\subseteq$ P/poly (say, see the textbook by Du and Ko [13]). By contrast, it is open whether BQP is included in P/poly (and that inclusion seems not to hold).

Remark 3.5 In Definition 3.1, we take *pure* quantum states as quantum advice, not *mixed* quantum states, the fully general notion of quantum states since we follow the style of the classical advice; fixed strings, not randomly selected strings, are taken as classical advice. By the broadening of the spirit of advice, we could take randomly selected advice or mixed states as advice, which will be shortly mentioned in the last section.

4. Non-uniformity of Amplitudes

What is the complexity class BQP, which is considered to be the most appropriate class for representing the computational power of quantum computers? Roughly speaking, this class is the collection of sets that can be recognized by polynomial-time bounded-error quantum Turing machines. However, Adleman, et al. [3] showed that, if the transition amplitudes of quantum Turing machines are *any complex numbers*, quantum Turing machines can recognize undecidable sets with bounded-error in polynomial time. Thus, rigorously, the definition of BQP [7] is given using quantum Turing machines with amplitudes from the set of polynomial-time computable complex numbers (that is, complex numbers whose real and imaginary parts are approximated within 2^{-n} in time polynomial in n). By contrast, the class of sets recognized by polynomial-time bounded-error quantum Turing machines whose amplitudes are *any complex numbers* is often called $\mathrm{BQP}_{\mathbb{C}}$. According to this line, the uniform condition of quantum circuit families is defined as follows [23]: (i) all circuits are constructed using elementary gates whose matrix representations have polynomial-time computable components; and (ii) the construction of each circuit is computed in time polynomial in the length of the input. Using Yao's simulation of quantum Turing machines by quantum circuits [33], it is shown that BQP equals the class of sets recognized with bounded error by uniform quantum circuit families [23]. On the contrary, to represent the class $\mathrm{BQP}_{\mathbb{C}}$ in terms of quantum circuits, we must consider quantum circuit families that do not satisfy uniform condition (i). Thus, $\mathrm{BQP}_{\mathbb{C}}$ can be regarded as a kind of non-uniform quantum complexity classes. We now bound the amount of non-uniform information obtained by the sets in $\mathrm{BQP}_{\mathbb{C}}$. Here, log denotes the set of functions f satisfying $|f(n)| = O(\log n)$.

Proposition 4.1 $\mathrm{BQP}_{\mathbb{C}} \subsetneq \mathrm{BQP}/^{*}\log$.

Remark 4.2 In Ref. 24) a bit worse upper bound was shown. However, almost the same proof leads to Proposition 4.1 by using the approximation scheme of Harrow et al. [15] for a quantum state given as advice, instead of Solovay-Kitaev theorem [18],[22] used in Ref. 24).

Proposition 4.1 implies that $\mathrm{BQP}_{\mathbb{C}}/^{*}\mathrm{poly} = \mathrm{BQP}/^{*}\mathrm{poly}$ and $\mathrm{BQP}_{\mathbb{C}}/^{*}\mathrm{Qpoly}{=}\mathrm{BQP}/^{*}\mathrm{Qpoly}$. That is, the complexity classes BQP/*poly and BQP/*Qpoly are stable for the change of transition amplitudes taken by underlying quantum Turing machines, like a quantum analogue of NP, the class NQP [30].

By contrast, we can give a lower bound of non-uniformity of $\mathrm{BQP}_{\mathbb{C}}$. Ko [19] introduced another notion of logarithmic advice class Full-P/log[☆] where an advice string $h(n)$ can be used to recognize a subset $L \cap \left(\bigcup_{m \le n} \Sigma^m\right)$ of a set L while it is only available to recognize $L \cap \Sigma^n$ in case of P/log. The class Full-P/log has a nice structure that is closed under polynomial-time Turing reduction, different from P/log. Also, Full-P/log is characterized as $\text{Full-P/}\log = \mathrm{P}^{\mathrm{TALLY2}}$ by a relativized class [5] like $\mathrm{P/poly} = \mathrm{P}^{\mathrm{TALLY}}$. Here, TALLY2 denotes the collection of all subsets of $\{0^{2^n} \mid n \in \mathbb{N}\}$. Similarly, we can define another logarithmic quantum advice class Full-BQP/* log and see that it equals $\mathrm{BQP}^{\mathrm{TALLY2}}$. Then, the proof that $\mathrm{BQP}_{\mathbb{C}}$ includes undecid-

[☆] Ko [19] originally called it Strong-P/poly.

able sets is available for embedding the information on any set in TALLY2 into the amplitudes of quantum Turing machines. Combining Proposition 4.1 with this fact, we obtain the following conclusion that figures out the power of $\mathrm{BQP}_{\mathbb{C}}$.

Theorem 4.3 *The following relations hold.*

1) Full-BQP/* log $\subseteq \mathrm{BQP}_{\mathbb{C}} \subsetneq$ BQP/* log.

2) $\mathrm{BQP}^{\mathrm{TALLY2}} \subseteq \mathrm{BQP}_{\mathbb{C}} \subsetneq \mathrm{BQP}^{\mathrm{TALLY}}$.

5. Relation to One-way Communication Complexity

Since Yao introduced the notion of communication complexity in classical[32] as well as quantum setting[33], it has been intensively studied and applied to various topics in computer science[21]. As one of such applications, we look at the connection between one-way communication complexity and advised computation.

Consider the following cooperative work between the two parties, Alice and Bob. Alice has a string x and Bob has another string y. The aim for Alice is to let Bob compute the value $f(x, y)$ for a function f by sending a message that depends on x only once. We assume that Bob as well as Alice knows the function f and the time in which Bob computes $f(x, y)$ is unlimited. Hence, if Bob knows x then he can compute $f(x, y)$ correctly. Alice wants to shorten her message as much as she can (since, for instance, it is expensive for her to send a long message). In this setting, the minimal length of Alice's message to complete the cooperative work is called the *one-way communication complexity* of f. We can also consider the quantum one-way communication complexity if Alice sends a quantum message to Bob.

Now assume that Bob is a polynomial-time Turing machine M, and wants to recognize a set L. If L is a difficult set, then it is tough that Bob computes $L(x)$ for any given string x of length n. In the worst case, Bob cannot compute $L(x)$ for almost all x. Suppose that Alice completely knows L and n, but she does not know which string in Σ^n is Bob's input. We can regard this situation as the following cooperative work: Alice's aim is to let Bob compute the value $INDEX(L_n, x)$, where L_n is the 2^n-bit characteristic string of $L \cap \Sigma^n$ and $INDEX$ is the Boolean function from $\Sigma^{2^n} \times \Sigma^n$ that maps (L_n, x) to the $\mathrm{Bin}(x)$-th bit of L_n. (Here, $\mathrm{Bin}(x)$ is the lexicographic order of x in Σ^n). Considering Alice's message as advice, we can regard advised computation as a variant of the one-way communication complexity model. This view is often available to show the limit of the advised computation that will appear in the later sections.

6. BQP/*Qpoly $\neq$ BQP/*poly?

Is quantum advice more powerful than classical advice? For many ones that have interest in advised quantum computation, the most natural separation corresponding to this question would be the separation of BQP/*poly from BQP/*Qpoly. To try to solve this problem, Aaronson succeeded to bound from above BQP/*Qpoly by the class PP with polynomial classical advice using a clever algorithm.

Theorem 6.1 BQP/*Qpoly $\subseteq$ PP/poly[1].

In fact, he gave the following result using a simulation of quantum messages by classical messages in the setting of one-way communication complexity:

Assume that to let Bob compute a Boolean function f from $\Sigma^n \times \Sigma^m$ Alice is enough to send Bob a quantum message of length l_n. Then, Alice can let Bob compute f sending a classical message of length $O(ml_n \log l_n)$.

In this simulation method, Bob is required to judge whether the original protocol on a quantum message produces 1 with probability $> 1/2$, which can be implemented by an unbounded-error probabilistic Turing machine. Therefore, the simulation method is also used to the proof of Theorem 6.1 by the connection between advice complexity and one-way communication complexity as follows. Assume $L \in$ BQP/*Q*poly*, and let $L_n = L \cap \Sigma^n$. Then, L_n is computed by a bounded-error quantum Turing machine with quantum advice of length $p(n)$ where p is a polynomial. By incorporating the proof technique of BQP $\subseteq$ PP[3] into the above simulation method, L_n is computed by a polynomial-time probabilistic Turing machine with classical advice of length $O(np(n) \log p(n))$ with probability $> 1/2$.

Unfortunately, Theorem 6.1 means that the separation between BQP/*Qpoly and BQP/*poly is more difficult than a famous open problem that separates P from the class PSPACE. In fact, by Theorem 6.1, BQP/*poly $\neq$ BQP/*Qpoly implies P/poly $\neq$ PP/poly. It leads to P $\neq$ PSPACE since otherwise P = PP by Fact 2.1 and hence P/poly = PP/poly. Thus, it cannot be expected to separate between BQP/*Qpoly and BQP/*poly (and even P/poly). It is pointed out[1] that the group membership problem by Watrous[28] is considered to be a good candidate that separates between BQP/*Qpoly and BQP/*poly in a relativized world. Nevertheless, a relativized separation between these classes still remains open.

7. Unrelativized Separation between Classical Advice and Quantum Advice

In the previous section, we have seen that BQP/*poly and BQP/*Qpoly are extremely difficult to separate. However, we can show some unrelativized separation between quantum complexity classes with short classical advice and quantum advice. For instance, we may ask whether BQP/* log is different from BQP/*Q log. This answer is much easily obtained compared to the separation between polynomial quantum advice and polynomial classical advice.

Theorem 7.1 *Let f be a polynomially bounded function. Then,* $\mathrm{BQP}/^*\mathrm{Q}(O(f(n)\log n)) \nsubseteq \mathrm{BQP}/^*f(n)n$[24]*.*

The above theorem is obtained using a quantum fingerprint[9] (in fact, a quantum fingerprint by de Wolf[29]). Consider a "sparse" set L_n that cannot be recognized by polynomial-time quantum Turing machines with any classical advice of length $f(n)n$, which is guaranteed to exist by a simple counting argument. By contrast, a quantum fingerprint $|\phi(L_n)\rangle$ of length $O(f(n)\log n)$ enables us to "encode" all the elements of L_n in the following sense: given $|\phi(L_n)\rangle$ as supplementary information, we can decide if any given input belongs to L_n in quantum polynomial time. Theorem 7.1 clearly separates between BQP/* log and BQP/*Q log as well as between BQP/*polylog and BQP/*Qpolylog, where polylog is the class of functions f such that $f(n) \leq p(\log n)$ for some polynomial p.

On the contrary, we can also show that any quantum complexity class with quantum advice of length l cannot include a quantum complexity class with classical advice whose length is within a constant factor of l.

Theorem 7.2 *For any function f satisfying $f(n) \leq 2^n$,* $\mathrm{P}/f(n) \nsubseteq \mathrm{BQP}/^*\mathrm{Q}(0.08f(n))$[24]*.*

Theorem 7.2 implies that BQP/*Q log is a proper subset of BQP/*poly since BQP/*Q log $\subseteq$ BQP/*poly can be easily seen by keeping the code of a quantum circuit that generates a quantum state of logarithmic length as polynomial classical advice.

The proof of Theorem 7.2 is obtained again from the connection between advised computation and one-way communication complexity. That is, suppose that a polynomial-time quantum Turing machine M recognizes any subset L_n of Σ^n with the help of quantum advice $|\phi(L_n)\rangle$ of length m, where $L_n(x) = 0$ if the lexicographical order of x in Σ^n is larger than $f(n)$. This is interpreted as follows in the one-way communication setting:

Alice sends the m-qubit state $|\phi(L_n)\rangle$ to Bob, who can compute any given bit of L_n (in fact, of the first $f(n)$ bits in L_n) with probability $\geq 2/3$.

The minimal length of such an m to complete this cooperative work is known as quantum random access coding[4].

Theorem 7.3 *(quantum random access coding[4]) An (n, m, p)-quantum random access coding is a function F mapping n-bit strings to m-qubit states satisfying that: for every $i \in \{1, \ldots, n\}$ there is a measurement O_i with outcome 0 or 1 such that the outcome of O_i on input $F(x)$ is the ith bit of x with at least p for all n-bit strings x. Then, $m \geq (1 - H(p))n$, where $H(p) = -p\log p - (1-p)\log(1-p)$.*

In our case, Alice's coding is an $(f(n),m,2/3)$-quantum random access coding. Hence, there is a set L_n such that M cannot recognize with the help of quantum advice of length at most $0.08f(n)$ (which is $\leq (1-H(2/3))f(n)$). On the contrary, advice of length $f(n)$ clearly allows a deterministic Turing machine to recognize L_n. This argument almost completes the proof of Theorem 7.2.

Now we summarize relationships among logarithmic and polynomial advice classes of quantum Turing machines.

Corollary 7.4 $\mathrm{BQP}/^*\log \subsetneq \mathrm{BQP}/^*\mathrm{Q}\log \subsetneq \mathrm{BQP}/^*\mathrm{poly} \subseteq \mathrm{BQP}/^*\mathrm{Qpoly}$.

8. Separating Uniform Complexity Classes from Non-uniform Complexity Classes

In classical complexity theory, which uniform complexity classes are included in P/poly has been investigated at length to unearth the computational limit of polynomial-size circuits. In this investigation, it is shown that as a relativized result there exists an oracle such that the class NP is not included in P/poly, and as an unrelativized result the class ESPACE[☆] is not included in P/poly. Similarly, we can ask which uniform complexity classes are included in BQP/*poly or BQP/*Qpoly. As a relativized result, the following separation is shown.

Theorem 8.1 *There is a set A relative to which* $\mathrm{NP}^A \nsubseteq \mathrm{BQP}^A/^*\mathrm{Qpoly}$ [1].

By contrast, for the unrelativized case, only a uniform complexity class much higher than NP has been shown to separate from advice complexity class similar to the classical case. Earlier, combining quantum random access coding with a diagonalization argument, a huge uniform complexity class EESPACE (the class of sets recognized by a deterministic Turing machine in space $2^{2^{O(n)}}$) was shown to be outside of BQP/*Qpoly [24]. However, Theorem 6.1, which was proven after the earlier result, implies that a better uniform complexity class ESPACE is not included in BQP/*Qpoly.

Corollary 8.2 ESPACE $\nsubseteq$ BQP/*Qpoly.

Proof. By Theorem 6.1, BQP/*Qpoly $\subseteq$ PP/poly while ESPACE $\nsubseteq$ PP/poly can be shown similar to the proof of ESPACE $\nsubseteq$ P/poly [16]. This completes the proof. □

Finally, we report that the adaptive query to an oracle is more powerful than the nonadaptive query to the oracle with polynomial advice. The nonadaptive query to an oracle A roughly means that a query to A does not depend on any query made at previous steps. In quantum case, the precise definition of the nonadaptive query is not so simple rather than the classical case because of quantum interference among computation paths. (For instance, see Yamakami [31] for the definition of the parallel query, a pattern of the nonadaptive query). Thus, we herewith take a simple definition for the nonadaptive query, called a truth-table query, as follows.

Definition 8.3 We say that a quantum Turing machine M queries to an oracle A in the truth-table manner if (i) M produces a superposition $\sum_{\vec{x}} \alpha_{\vec{x}} |\vec{x}\rangle$ of lists of query words in the first register without querying A, (ii) quantumly receives the answers $A(x_1), \ldots, A(x_m)$ for each list $\vec{x} = (x_1, \ldots, x_m)$ from the oracle in the second register, and (iii) completes the computation without querying A. Let $\mathrm{BQP}^A_{tt}/^*\mathrm{poly}$ be the class of sets recognized by polynomial-time quantum Turing machines with polynomial advice that make queries to the oracle A in the truth-table manner.

Although the nonadaptive query is restrictive, a number of quantum algorithms such as Simon's algorithm [27] indicate that the quantum nonadaptive query is still useful compared to the classical adaptive query. By contrast, Yamakami [31] showed that there exists a relativized world that there is a problem that can be solved in deterministic polynomial time, but cannot be solved by any polynomial-time quantum Turing machine that makes nonadaptive queries. This result was extended to the case that polynomial-time quantum Turing machines have polynomial advice.

Theorem 8.4 *There exists a set A relative to which* $\mathrm{P}^A \nsubseteq \mathrm{BQP}^A_{tt}/^*\mathrm{poly}$ [25].

9. Future Work

In this article, we have reviewed the study of advised quantum computation that is just getting started recently. The quantum complexity class with classical advice exactly characterizes polynomial-size quantum circuits, and enables us to remove non-uniform information in transition amplitudes into classical advice. The quantum complexity class with quantum advice is another candidate representing a broader quantum extension of non-uniform computation, but has the computational limit based on comparisons with the quantum complexity class with classical advice and the uniform complexity class. Moreover, the study of quantum Turing machines with quantum advice is deeply related to quantum one-way communication complexity. Recently, Bar-Yossef, et al. [6] showed some problem (but that is not a function) that quantum one-way communication complexity is exponentially smaller than classical one. As long as the author knows, any connection between this problem and the BQP/*Qpoly $\neq$ BQP/*poly problem has not been shown. It would be interesting to examine which problem of one-way communication complexity has a connection to an oracle that separates BQP/*poly from BQP/*Qpoly. We left a number of open problems other than the BQP/*poly $\neq$ BQP/*Qpoly problem.

(1) Do we give a uniform complexity class lower than the class NP that is outside of BQP/*Qpoly in a relativized

[☆] It is also shown that the exponential-time Merlin-Arthur class $\mathrm{MA}_{\mathrm{EXP}}$ is outside of P/poly [10].

world? (In classical case, Buhrman and Torenvliet[11] constructed an oracle that NP∩co-NP is outside of P/poly).

(2) As the related work to the NP $\not\subseteq$ P/poly problem, the unlikely collapse of complexity classes under the assumption NP $\subseteq$ P/poly has been improved[8],[12],[20] since the Karp-Lipton's result[17] (the polynomial hierarchy collapses the second level if NP is included in P/poly). How is some collapse of complexity classes under the assumption that NP is included in BQP/*Qpoly? Recently, Aaronson[2] showed that the counting hierarchy collapses the first level if PP is included in BQP/*Qpoly.

(3) If classical advice is randomly selected, logarithmic random advice enables us to recognize the set used in the proof that separates BQP/* log from BQP/*Q log. Is a quantum Turing machine with logarithmic quantum advice really powerful than a quantum Turing machine with logarithmic randomly selected advice? On the contrary, we know what happens if quantum advice is randomly selected, that is, a mixed quantum state is allowed as quantum advice. The class BQP/*Q log does not change since a mixed state of m qubits can be easily created from a pure state of only $2m$ qubits by the purification of mixed states[22].

(4) For quantum complexity classes other than BQP, we can define their advice complexity classes similar to BQP/*poly or BQP/*Qpoly. It would be interesting to investigate the power of such advice complexity classes. Recently, Raz[26] showed that the advice complexity class QIP(2)/*Qpoly of the class QIP(2), the class of sets having two-message quantum interactive proof systems, includes *all* languages. Also, it is easily seen that the advice complexity class NQP/*Qpoly of the class NQP includes all languages. How is the power of QMA/*Qpoly, the advice class of quantum Merlin-Arthur class QMA (that is, the class of sets having one-message quantum interactive proof systems)?

References

1) Aaronson, S.: Limitations of quantum advice and one-way communication, *Proc. 19th Annual IEEE Conference on Computational Complexity*, IEEE, New York, pp.320–332 (2004). Its journal version appeared in *Theory of Computing*, Vol.1, pp.1–28 (2005).

2) Aaronson, S.: Oracles are subtle but not malicious. http://arxiv.org/cs.CC/0504048

3) Adleman, L.M., DeMarrais, J. and Huang, M.A.: Quantum computability, *SIAM J. Comput.*, Vol.26, pp.1524–1540 (1997).

4) Ambainis, A., Nayak, A., Ta-shma, A. and Vazirani, U.: Dense quantum coding and quantum finite automata, *J. ACM*, Vol.49, pp.496–511 (2002).

5) Balcázar, J.L. and Hermo. M.: The structure of logarithmic advice complexity classes, *Theoret. Comput. Sci.*, Vol.207, pp.217–244 (1998).

6) Bar-Yossef, Z., Jayram, T.S. and Kerenidis, I.: Exponential separation of quantum and classical one-way communication complexity, *Proc. 36th ACM Symposium on Theory of Computing*, ACM, New York, pp.128–137 (2004).

7) Bernstein, E. and Vazirani, U.: Quantum complexity theory, *SIAM J. Comput.*, Vol.26, pp.1411–1473 (1997).

8) Bshouty, N.H., Cleve, R., Gavaldà, R., Kannan, S. and Tamon, C.: Oracles and queries that are sufficient for exact learning, *J. Comput. Syst. Sci.*, Vol.52, pp.421–433 (1996).

9) Buhrman, H., Cleve, R., Watrous, J. and de Wolf, R.: Quantum fingerprinting, *Phys. Rev. Lett.*, Vol.87, 167902 (Sep. 2001).

10) Buhrman, H., Fortnow, L. and Thierauf, T.: Nonrelativizing separations. *Proc. 13th IEEE Conference on Computational Complexity*, IEEE, New York, pp.8–12 (1998).

11) Buhrman, H. and Torenvliet, L.: Complicated complementations, *Proc. 14th IEEE Conference on Computational Complexity*, IEEE, New York, pp.227–236 (1999).

12) Cai, J-Y.: $S_2^p \subseteq \mathrm{ZPP}^{\mathrm{NP}}$, *Proc. 42nd Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, pp.620–629 (2001).

13) Du, D. and Ko, K.: *Theory of Computational Complexity*, John Wiley & Sons, Inc., New York (2000).

14) Gruska, J.: *Quantum Computing*, McGraw-Hill, London (1999).

15) Harrow, A.W., Recht, B. and Chuang, I.L.: Efficient discrete approximations of quantum gates, *J. Math. Phys.*, Vol.43, pp.4445–4451 (2002).

16) Kannan, R.: Circuit-size lower bounds and non-reducibility to sparse sets, *Inform. Control*, Vol.55, pp.40–56 (1982).

17) Karp, R.M. and Lipton, R.: Some connections between nonuniform and uniform complexity classes, *Proc. 12th ACM Symposium on Theory*

of Computing, ACM, New York, pp.302–309 (1980). An extended version appeared as: Turing machines that take advice, *L'Enseignement Mathematique*, Vol.28, pp.191–209 (1982).

18) Kitaev, A.: Quantum computations: algorithms and error correction, *Russian Math. Surveys*, Vol.52, pp.1191–1249 (1997).

19) Ko, K.: On helping by robust oracle machines, *Theoret. Comput. Sci.*, Vol.52, pp.15–36 (1987).

20) Köbler, J. and Watanabe, O.: New collapse consequences of NP having small circuits, *SIAM J. Comput.*, Vol.28, pp.311–324 (1998).

21) Kushilevitz, E. and Nisan, N.: *Communication Complexity*, Cambridge University Press (1997).

22) Nielsen, M.A. and Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

23) Nishimura, H. and Ozawa, M.: Computational complexity of uniform quantum circuit families and quantum Turing machines, *Theoret. Comput. Sci.*, Vol.276, pp.147–181 (2002).

24) Nishimura, H. and Yamakami, T.: Polynomial time quantum computation with advice, *Inform. Process. Lett.*, Vol.90, pp.195–204 (2004).

25) Nishimura, H. and Yamakami, T.: An algorithmic argument for nonadaptive query complexity lower bounds on advised quantum computation, *Proc. 29th International Symposium on Mathematical Foundations of Computer Science*, Lecture Notes in Computer Science, pp.827–838 (2004).

26) Raz, R.: Quantum information and the PCP theorem, To appear in *Proc. 46th Annual IEEE Symposium on Foundations of Computer Science* (2005).
http://arxiv.org/quant-ph/0504075

27) Simon, D.: On the power of quantum computation, *SIAM J. Comput.*, Vol.26, pp.1474–1483 (1997).

28) Watrous, J.: Succinct quantum proofs for properties of finite groups, *Proc. 41st Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, pp.537–546 (2000).

29) de Wolf, R.: *Quantum Computing and Communication Complexity*, PhD dissertation, University of Amsterdam (2001).

30) Yamakami, T. and Yao, A.C.: $\mathrm{NQP}_{\mathbb{C}}$ =co-$\mathrm{C}_{=}\mathrm{P}$, *Inform. Process. Lett.*, Vol.71, pp.63–69 (1999).

31) Yamakami, T.: Analysis of quantum functions, *International Journal of Foundations of Computer Science*, Vol.14, pp.815–852 (2003).

32) Yao, A.C.: Some questions related to distributed computing, *Proc. 11th ACM Symposium on Theory of Computing*, ACM, New York, pp.209–213 (1979).

33) Yao, A.C.: Quantum circuit complexity, *Proc. 34th Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, pp.352–361 (1993).

(Received January 31, 2005)
(Accepted July 4, 2005)

(Online version of this article can be found in the IPSJ Digital Courier, Vol.1, pp.407–414.)

Harumichi Nishimura is a researcher of ERATO Quantum Computation and Information Project, Japan Science and Technology. He received B.E. degree from Department of Mathematics, Nagoya University in 1993, and M.S. and Ph.D. degrees from Human Informatics, Nagoya University in 1997 and 2001, respectively. His research interests are mainly quantum computing, computational complexity, and cryptography.