Quantum Information and Computation, Vol. 16, No. 5&6 (2016) 0498–0514

QUANTUM INTERPRETATIONS OF AWPP AND APP

TOMOYUKI MORIMAE
ASRLD Unit, Gunma University
1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan
morimae@gunma-u.ac.jp

HARUMICHI NISHIMURA
Graduate School of Information Science, Nagoya University
Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
hnishimura@math.cm.is.nagoya-u.ac.jp

Received June 5, 2015
Revised Juanuary 15, 2016

AWPP is a complexity class introduced by Fenner, Fortnow, Kurtz, and Li, which is defined using GapP functions. Although it is an important class as the best upperbound of BQP, its definition seems to be somehow artificial, and therefore it would be better if we have some "physical interpretation" of AWPP. Here we provide a quantum physical interpretation of AWPP: we show that AWPP is equal to the class of problems efficiently solved by a quantum computer with the ability of postselecting an event whose probability is close to an FP function. This result is applied to also obtain a quantum physical interpretation of APP. In addition, we consider a "classical physical analogue" of these results, and show that a restricted version of $\mathrm{BPP_{path}}$ contains $\mathrm{UP} \cap \mathrm{coUP}$ and is contained in WAPP.

Keywords: AWPP, APP, postselection
Communicated by: R Cleve & M Mosca

1 Introduction

AWPP is a complexity class introduced by Fenner, Fortnow, Kurtz, and Li [5] to understand the structure of counting complexity classes (see also Refs. [11, 4]). It is defined as follows:

Definition 1. A language L is in AWPP iff for any polynomial r, there exist $f \in \mathrm{FP}$ and $g \in \mathrm{GapP}$ such that for all w, $f(w) > 0$ and

1. If $w \in L$ then $1 - 2^{-r(|w|)} \leq \frac{g(w)}{f(w)} \leq 1$.
2. If $w \notin L$ then $0 \leq \frac{g(w)}{f(w)} \leq 2^{-r(|w|)}$.

Here, FP is the class of functions from bit strings to integers that are computable in polynomial time by a Turing machine. A GapP function [3] is a function from bit strings to integers that is equal to the number of accepting paths minus that of rejecting paths of a nondeterministic Turing machine which takes the bit strings as input. The FP function f can be replaced with $2^{q(|w|)}$ for a polynomial q [3, 11], and the error bound $(2^{-r(|w|)}, 1 - 2^{-r(|w|)})$ can be replaced with, for example, $(1/3, 2/3)$ [4].

Interestingly, AWPP was shown to contain BQP, by Fortnow and Rogers [7] in 1997, and since then it has been the best upperbound of BQP (in classical complexity classes). Here, BQP is a class of problems efficiently solved by a quantum computer:

Definition 2. A language L is in BQP iff there exists a uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits such that

1. If $w \in L$ then $P_{V_w}(o = 1) \geq \frac{2}{3}$.
2. If $w \notin L$ then $P_{V_w}(o = 1) \leq \frac{1}{3}$.

Here, we say that a family $V = \{V_n\}_n$ of quantum circuits is uniform if there is a classical polynomial-time algorithm that outputs a description of V_n on input 1^n, where n is the input size of V_n. We denote the output bit by $o \in \{0, 1\}$, and $P_{V_w}(o = 1)$ is the probability of obtaining $o = 1$ (i.e., output 1) if we measure the single output qubit of the circuit $V_{|w|}$ on input w. The pair of the thresholds $(\frac{1}{3}, \frac{2}{3})$ is rather arbitrary. For example, we can take $(2^{-r(|w|)}, 1 - 2^{-r(|w|)})$ for any polynomial r.

(We note that, for simplicity, we choose Hadamard and Toffoli gates as a universal gate set of quantum circuits. This choice is crucial to obtain some of our results, while this choice is also taken in Ref. [1], and we believe that this choice is enough to study the essential parts of what we are interested in. It may be possible to extend our results to other gate sets, but it would be a future research subject.)

The name of AWPP is thus known by many researchers including physicists. However, the definition of AWPP seems to be somehow artificial and difficult to understand for ones who are not familiar with GapP functions. The purpose of the present contribution is to provide a quantum physical interpretation of AWPP. For the goal, we consider quantum computing with a postselection. Here, a postselection is a (fictious) ability that we can choose an event with probability 1 even if its probability is exponentially small. Quantum computing with postselection was first considered by Aaronson [1]. He defined the following class postBQP, and showed that it is equal to PP (see also Ref. [10] and Appendix D for another proof of postBQP = PP):

Definition 3. A language L is in postBQP iff there exist a uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits with the ability of a postselection and a polynomial u such that for any input w,

1. $P_{V_w}(p = 1) \geq 2^{-u(|w|)}$.
2. If $w \in L$ then $P_{V_w}(o = 1|p = 1) \geq \frac{2}{3}$.
3. If $w \notin L$ then $P_{V_w}(o = 1|p = 1) \leq \frac{1}{3}$.

Here, $p \in \{0, 1\}$ is the measurement result of the postselected qubit of the circuit $V_{|w|}$, and $P_{V_w}(o = 1|p = 1)$ is the conditional probability that $V_{|w|}$ on input w obtains $o = 1$ under $p = 1$. Like BQP, the pair of the thresholds $(\frac{1}{3}, \frac{2}{3})$ is arbitrary. In particular, it can be $(2^{-r(|w|)}, 1 - 2^{-r(|w|)})$ for any polynomial r. Furthermore, without loss of generality, we can assume that only a single qubit is postselected, since postselections on more than two qubits can be transformed to that on a single qubit by using the generalized Toffoli gate, which can be implemented in a polynomial-size quantum circuit.

We introduce a restricted version of postBQP, which we call $\mathrm{postBQP}_{\mathrm{aFP}}$:

Definition 4. A language L is in $\mathrm{postBQP}_{\mathrm{aFP}}$ iff for any polynomials $r_1 \geq 0$ and $r_2 \geq 0$ there exist a uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits with the ability of a postselection, an FP function f, and a polynomial q such that for any input w, $0 < f(w) \leq 2^{q(|w|)}$ and

1. If $w \in L$ then $1 - 2^{-r_1(|w|)} \leq P_{V_w}(o = 1|p = 1) \leq 1$.
2. If $w \notin L$ then $0 \leq P_{V_w}(o = 1|p = 1) \leq 2^{-r_1(|w|)}$.
3. $\left| P_{V_w}(p = 1) - \frac{f(w)}{2^{q(|w|)}} \right| \leq 2^{-r_2(|w|)} P_{V_w}(p = 1)$.

The third condition intuitively means that the postselection probability $P_{V_w}(p = 1)$ can be approximated to $f(w)/2^{q(|w|)}$ within the multiplicative error $2^{-r_2(|w|)}$. (Hence the subscript "aFP" means "approximately FP".) We show that $\mathrm{postBQP}_{\mathrm{aFP}} = \mathrm{AWPP}$, which provides a quantum physical interpretation of AWPP: AWPP can be considered as an example of postselected quantum complexity classes. We note that while one might consider that $\mathrm{postBQP}_{\mathrm{aFP}}$ is also artificial due to the fiction of postselection, we consider that this class is easier to understand for physicists since it is defined by using the terminology of quantum physics, or at least it gives another interpretation of AWPP, which might be useful for future studies on AWPP.

We also introduce another restricted version of postBQP, which we call $\mathrm{postBQP}_{\mathrm{asize}}$:

Definition 5. The definition of $\mathrm{postBQP}_{\mathrm{asize}}$ is the same as that of $\mathrm{postBQP}_{\mathrm{aFP}}$ except that the FP function $f(w)$ is replaced with $g(1^{|w|})$, where g is a GapP function.

We show that $\mathrm{postBQP}_{\mathrm{asize}}$ is equal to the classical complexity class APP defined by Li [11]. Therefore, not only AWPP but also APP have quantum physical interpretations.

There are some researches on quantum physical interpretations of classical complexity classes. For example, the above mentioned Aaronson's result postBQP = PP [1] is considered as a quantum physical interpretation of PP. Furthermore, Kuperberg [10] showed that $\mathrm{A_0PP}$ is equal to SBQP, which is a quantum version of SBP [2], and Fenner et al. [6] (see also Ref. [12]) showed that $\mathrm{coC_=P}$ is equal to NQP, which is a quantum analogue of NP. Our contributions are in the same line of these researches, while we take a different way for the proofs. We not only use the relations between quantum computation and GapP functions as used in Refs. [4, 6], but combine them with the notion of restricted postselection probability introduced in this paper. Moreover, we also use tactically the property that AWPP and APP are closed under complement in order to satisfy such a restriction of postselection probability.

In addition to $\mathrm{postBQP}_{\mathrm{aFP}}$ and $\mathrm{postBQP}_{\mathrm{asize}}$, we introduce several restricted versions of postBQP, and study relations among them and other complexity classes. For example, we define a simpler version (the exact version) of $\mathrm{postBQP}_{\mathrm{aFP}}$, which we call $\mathrm{postBQP}_{\mathrm{FP}}$:

Definition 6. A language L is in $\mathrm{postBQP}_{\mathrm{FP}}$ iff it is in postBQP and there exist a polynomial q and $f \in \mathrm{FP}$ $(f > 0)$ such that for any input w, $P_{V_w}(p = 1) = \frac{f(w)}{2^{q(|w|)}}$, where V is the uniform family of quantum circuits that assures $L \in \mathrm{postBQP}$.

Since it is simpler than $\mathrm{postBQP}_{\mathrm{aFP}}$, it would be better if we could show the equivalence of it to AWPP. Currently, we do not know whether the equivalence holds. However, we show that $\mathrm{postBQP}_{\mathrm{FP}}$ sits between WPP and AWPP. (The definition of WPP is given in Sec. 2.) It is nearly tight except showing the equivalence since WPP is one of the best lower bounds of AWPP [5] (in fact, AWPP was named as "approximate WPP"). All our results are summarized in Fig. 1. Definitions of new classes in the figure are given in Sec. 2.

A classical analogue of postBQP is postBPP, which is known to be equal to $\mathrm{BPP}_{\mathrm{path}}$ [8]. We also consider a classical version, $\mathrm{postBPP}_{\mathrm{FP}}$, of $\mathrm{postBQP}_{\mathrm{FP}}$, and show that $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{postBPP}_{\mathrm{FP}} \subseteq \mathrm{WAPP}$. (The definitions of $\mathrm{postBPP}_{\mathrm{FP}}$ and WAPP are given in Sec. 2.)

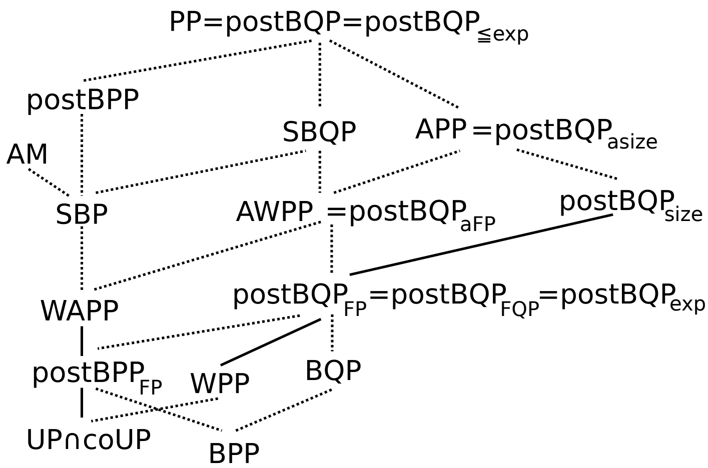

Fig. 1. Relations among complexity classes studied in this paper. Dotted lines are known results or inclusions followed by definitions. Solid lines and all equalities (except for PP = postBQP) are new results of this paper.

2 Preliminaries

In this section, we provide several definitions and facts used in this paper.

Definition 7. [3] A counting machine is a nondeterministic Turing machine running in polynomial time with two halting states, accepting and rejecting, and every computation path must end in one of these states. Without loss of generality, we may assume each node of the computation tree has outdegree at most two. A counting machine is called normal if for any input each computational path has the same number of nodes with outdegree two.

Definition 8. A function $f : \{0,1\}^* \to \mathbb{N} \cup \{0\}$ is a #P function if there exists a counting machine C such that $f(w)$ is the number of accepting paths of $C(w)$, where $C(w)$ denotes the nondeterministic computation of C on input w.

Definition 9. [3] A function $f : \{0,1\}^* \to \mathbb{Z}$ is a GapP function if there exists a counting machine C such that $f(w)$ is the number of accepting paths of $C(w)$ minus the number of rejecting paths of $C(w)$.

Definition 10. [11] A language L is in APP iff for any polynomial r, there exist $f, g \in \mathrm{GapP}$ such that for all w, $f(1^{|w|}) > 0$ and

1. If $w \in L$ then $1 - 2^{-r(|w|)} \leq \frac{g(w)}{f(1^{|w|})} \leq 1$.
2. If $w \notin L$ then $0 \leq \frac{g(w)}{f(1^{|w|})} \leq 2^{-r(|w|)}$.

Definition 11. [2] A language L is in WAPP iff there exist $g \in \#\mathrm{P}$, a polynomial p, and a constant $\epsilon > 0$ such that

1. If $w \in L$ then $\frac{1+\epsilon}{2} < \frac{g(w)}{2^{p(|w|)}} \leq 1$.
2. If $w \notin L$ then $0 \leq \frac{g(w)}{2^{p(|w|)}} < \frac{1-\epsilon}{2}$.

Note that $2^{p(|w|)}$ can be replaced with an FP function $f(w) > 0$.

Definition 12. [3] A language L is in WPP iff there exist a GapP function g and an FP function f with $0 \notin range(f)$ such that

1. If $w \in L$ then $g(w) = f(w)$.
2. If $w \notin L$ then $g(w) = 0$.

There are relations between an output probability distribution of a quantum circuit and a GapP function.

Theorem 1. *(Fortnow and Rogers [7]) For any uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits, there exist $g \in \mathrm{GapP}$ and a polynomial q such that for any w, $P_{V_w}(o = 1) = \frac{g(w)}{2^{q(|w|)}}$, where $P_{V_w}(o = 1)$ is the probability that the output of the circuit $V_{|w|}$ is $o = 1$ on input w. (Note that this theorem depends on the gate set. As we have noted, in this paper, we consider the Hadamard and Toffoli gates as a universal gate set.)*

Theorem 2. *(Fenner, Green, Homer, and Pruim [6]) For any $g \in \mathrm{GapP}$, there exist a polynomial s and a uniform family $\{V_n\}_n$ of polynomial-size quantum circuits such that $P_{V_w}(o = 1) = \frac{g(w)^2}{2^{s(|w|)}}$.*

Now we introduce the restricted postBQP classes other than those introduced in the previous section. (Here, V is the uniform family of polynomial-size quantum circuits that assures $L \in \mathrm{postBQP}$ as in Definition 6.)

Definition 13. A language L is in $\mathrm{postBQP}_{\mathrm{size}}$ iff it is in postBQP and $P_{V_w}(p = 1)$ depends only on $|w|$.

From Theorem 1, it is an exact version of $\mathrm{postBQP}_{\mathrm{asize}}$.

Definition 14. A language L is in $\mathrm{postBQP}_{\leq\exp}$ iff it is in postBQP and there exists a polynomial $q > 0$ such that for any input w, $P_{V_w}(p = 1) \leq 2^{-q(|w|)}$.

Definition 15. A language L is in $\mathrm{postBQP}_{\exp}$ iff it is in postBQP and there exists a polynomial q such that for any input w, $P_{V_w}(p = 1) = \frac{1}{2^{q(|w|)}}$.

Definition 16. A language L is in postBQP$_{\rm FQP}$ iff it is in postBQP and there exist a polynomial q and a function $f:\{0,1\}^*\to\mathbb{N}$, which can be calculated* by a uniform family of polynomial-size quantum circuits, such that for any input w, $P_{V_w}(p=1)=\frac{f(w)}{2^{q(|w|)}}$.

We also consider the classical analogue of postBQP$_{\rm FP}$.

Definition 17. We consider the following polynomial-time probabilistic Turing machine.

1. At every nondeterministic step, it makes a random decision between two possibilities, and each possibility is chosen with probability 1/2.

2. The number of random decisions is the same for all computation paths.

Therefore, if the machine halts after t nondeterministic steps, the probability of obtaining a specific computation path is 2^{-t}.

A language L is in postBPP$_{\rm FP}$ iff there exist a polynomial-time probabilistic Turing machine V that satisfies the above properties and outputs two bits p and o, an FP function $f>0$, a polynomial q, and a constant $\epsilon>0$ such that

1. $P_{V_w}(p=1)=\frac{f(w)}{2^{q(|w|)}}$.

2. If $w\in L$ then $\frac{1+\epsilon}{2}\le P_{V_w}(o=1|p=1)\le 1$.

3. If $w\notin L$ then $0\le P_{V_w}(o=1|p=1)\le\frac{1-\epsilon}{2}$.

Here, $P_{V_w}(p=1)$ and $P_{V_w}(o=1|p=1)$ are defined similarly to the case where V is a uniform family of circuits.

3 Results

The main result of the present contribution is the following quantum interpretation of AWPP:

Theorem 3. AWPP = postBQP$_{\rm aFP}$.

The proof is given in Sec. 4.

By replacing some FP functions in the proof with GapP functions, we can also show the following quantum interpretation of APP:

Theorem 4. APP = postBQP$_{\rm asize}$.

The proof is given in Appendix A.

If we consider not the approximate version, postBQP$_{\rm aFP}$, but the exact version, postBQP$_{\rm FP}$, we do not know whether it is equal to AWPP. Since postBQP$_{\rm FP}\subseteq$ postBQP$_{\rm aFP}$, we know postBQP$_{\rm FP}\subseteq$ AWPP. Furthermore, we can show the following nearly tight lowerbound:

Theorem 5. WPP $\subseteq$ postBQP$_{\rm FP}$.

The proof is given in Appendix B.

We can also show several relations among restricted postBQP classes:

Theorem 6. postBQP = postBQP$_{\le\rm exp}$.

*We assume that f can be calculated without any error.

The proof is given in Appendix C.

Theorem 7. $\mathrm{postBQP}_{\mathrm{FP}} = \mathrm{postBQP}_{\mathrm{FQP}} = \mathrm{postBQP}_{\mathrm{exp}} \subseteq \mathrm{postBQP}_{\mathrm{size}}$.

Its proof is given in Sec. 5.

Finally, we consider the classical analogue, $\mathrm{postBPP}_{\mathrm{FP}}$, of $\mathrm{postBQP}_{\mathrm{FP}}$, and show the following result:

Theorem 8. $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{postBPP}_{\mathrm{FP}} \subseteq \mathrm{WAPP}$.

Its proof is given in Sec. 6. Note that the inclusion $\mathrm{postBPP}_{\mathrm{FP}} \subseteq \mathrm{WAPP}$ is a "classical analogue" of $\mathrm{postBQP}_{\mathrm{FP}} \subseteq \mathrm{AWPP}$, since WAPP is a "#P analogue" of AWPP. Since $\mathrm{WAPP} \subseteq \mathrm{AM}$ [2] and $\mathrm{BQP} \subseteq \mathrm{AM}$ is unlikely, it is also unlikely that $\mathrm{BQP} \subseteq \mathrm{postBPP}_{\mathrm{FP}}$. Furthermore, since it is unlikely that BQP contains $\mathrm{UP} \cap \mathrm{coUP}$, the inclusion $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{postBPP}_{\mathrm{FP}}$ suggests that $\mathrm{postBPP}_{\mathrm{FP}} = \mathrm{BPP}$ and $\mathrm{postBPP}_{\mathrm{FP}} \subseteq \mathrm{BQP}$ are unlikely.

4 Proof of Theorem 3

We first show $\mathrm{AWPP} \cap \mathrm{coAWPP} \subseteq \mathrm{postBQP}_{\mathrm{aFP}}$. Since $\mathrm{AWPP} = \mathrm{coAWPP}$ [11], this means $\mathrm{AWPP} \subseteq \mathrm{postBQP}_{\mathrm{aFP}}$.

Let us assume that a language L is in $\mathrm{AWPP} \cap \mathrm{coAWPP}$. Then, for any polynomial r, there exist $g_1, g_2 \in \mathrm{GapP}$ and $f_1, f_2 \in \mathrm{FP}$ ($f_1 > 0$, $f_2 > 0$) such that

1. If $w \in L$ then

$$1 - 2^{-r(|w|)} \leq \frac{g_1(w)}{f_1(w)} \leq 1, \text{ and } 0 \leq \frac{g_2(w)}{f_2(w)} \leq 2^{-r(|w|)}.$$

2. If $w \notin L$ then

$$0 \leq \frac{g_1(w)}{f_1(w)} \leq 2^{-r(|w|)}, \text{ and } 1 - 2^{-r(|w|)} \leq \frac{g_2(w)}{f_2(w)} \leq 1.$$

In the following, for simplicity, we omit the $|w|$ dependancy of r, and just write $r(|w|)$ as r.

Then, there exist two GapP functions $h_1(w) \equiv g_1(w)f_2(w)$ and $h_2(w) \equiv g_2(w)f_1(w)$, such that

1. If $w \in L$ then

$$1 - 2^{-r} \leq \frac{h_1(w)}{f_1(w)f_2(w)} \leq 1, \text{ and } 0 \leq \frac{h_2(w)}{f_1(w)f_2(w)} \leq 2^{-r}.$$

2. If $w \notin L$ then

$$0 \leq \frac{h_1(w)}{f_1(w)f_2(w)} \leq 2^{-r}, \text{ and } 1 - 2^{-r} \leq \frac{h_2(w)}{f_1(w)f_2(w)} \leq 1.$$

Then there exist two counting machines C^1 and C^2 such that $h_1(w) = C_a^1(w) - C_r^1(w)$ and $h_2(w) = C_a^2(w) - C_r^2(w)$, where $C_a^j(w)$ and $C_r^j(w)$ ($j = 1, 2$) are the numbers of accepting and rejecting paths of C^j on input w, respectively.

There exist two normal counting machines N^1 and N^2 such that $h_1(w) = \frac{1}{2}(N_a^1(w) - N_r^1(w))$ and $h_2(w) = \frac{1}{2}(N_a^2(w) - N_r^2(w))$ [3]. Without loss of generality, we can assume that computation paths of N^1 and N^2 on input w can be represented by strings in $\{0,1\}^{q(|w|)}$, where q is a polynomial. (In the following, for simplicity, we write $q(|w|)$ as q.) Then we consider a uniform family $V = \{V_n\}_n$ of quantum circuits defined by the following procedure on input w. First, the state

$$\frac{|0\rangle^{\otimes 2k}}{\sqrt{2^{q+1}}}\sum_{x\in\{0,1\}^q}|x\rangle\Big((-1)^{N^1(w,x)}|N^1(w,x)\rangle|1\rangle + (-1)^{N^2(w,x)}|N^2(w,x)\rangle|0\rangle\Big)$$

can be generated by a polynomial-size quantum circuit. Here, k is a polynomial chosen later (k precisely means $k(|w|)$), and $N^j(w,x) = 0$ (=1, resp.) if the path x of N^j on input w is an accepting (rejecting, resp.) one. Let us postselect the first, second, and third registers to $|+\rangle^{\otimes 2k+q+1}$. The (unnormalized) state on the last register, which is the output qubit, after the postselection is

$$\frac{1}{2^{q+1+k}}\Big((N_a^1(w) - N_r^1(w))|1\rangle + (N_a^2(w) - N_r^2(w))|0\rangle\Big),$$

and therefore

$$P_{V_w}(p=1) = \frac{(N_a^1(w) - N_r^1(w))^2 + (N_a^2(w) - N_r^2(w))^2}{2^{2q+2+2k}} = \frac{4(h_1^2(w) + h_2^2(w))}{2^{2q+2+2k}}.$$

Therefore, irrespective of $w \in L$ or $w \notin L$, we obtain

$$\frac{f_1^2(w)f_2^2(w)}{2^{2q+2k}}(1-2^{-r})^2 \le P_{V_w}(p=1) \le \frac{f_1^2(w)f_2^2(w)}{2^{2q+2k}}(1+2^{-2r}).$$

Let us define $s(w) = f_1^2(w)f_2^2(w)$. Then the above inequality means

$$\frac{s(w)}{2^{2q+2k}}(1-2^{-r})^2 \le P_{V_w}(p=1) \le \frac{s(w)}{2^{2q+2k}}(1+2^{-2r}).$$

Since $1-2^{-r+1} \le (1-2^{-r})^2$ and $1+2^{-2r} \le 1+2^{-r+1}$, we obtain

$$\frac{s(w)}{2^{2q+2k}}(1-2^{-r+1}) \le P_{V_w}(p=1) \le \frac{s(w)}{2^{2q+2k}}(1+2^{-r+1}),$$

which means, if we take $r \ge 2$,

$$\frac{P_{V_w}(p=1)}{1+2^{-r+1}} \le \frac{s(w)}{2^{2q+2k}} \le \frac{P_{V_w}(p=1)}{1-2^{-r+1}}. \tag{1}$$

Note that

$$\frac{1}{1-2^{-r+1}} \quad \le \quad 1+2^{-r+2}, \tag{2}$$

and

$$\frac{1}{1+2^{-r+1}} - (1-2^{-r+2}) = \frac{1}{1+2^{-r+1}}(2^{-r+1} + 2^{-2r+3}) \ge 0. \tag{3}$$

Therefore, from Eqs. (2) and (3), Eq. (1) becomes

$$(1-2^{-r+2})P_{V_w}(p=1) \leq \frac{s(w)}{2^{2q+2k}} \leq (1+2^{-r+2})P_{V_w}(p=1),$$

which means

$$\left|P_{V_w}(p=1) - \frac{s(w)}{2^{2q+2k}}\right| \leq 2^{-r+2}P_{V_w}(p=1).$$

Remember that $s(w) = f_1^2(w)f_2^2(w) > 0$ and it is in FP. We denote $t \equiv 2q+2k$ and take k such that $s(w) \leq 2^t$. For any polynomial r_2, let us take $r \geq r_2 + 2$. Then,

$$\left|P_{V_w}(p=1) - \frac{s(w)}{2^t}\right| \leq 2^{-r_2}P_{V_w}(p=1).$$

Furthermore, from the state after the postselection, we have

$$P_{V_w}(o=1|p=1) = \frac{(N_a^1(w)-N_r^1(w))^2}{(N_a^1(w)-N_r^1(w))^2 + (N_a^2(w)-N_r^2(w))^2} = \frac{h_1^2(w)}{h_1^2(w)+h_2^2(w)}.$$

For any polynomial r_1, let us take $r \geq r_1 + 2$. Then, if $w \in L$ we obtain

$$P_{V_w}(o=1|p=1) = \frac{h_1^2(w)}{h_1^2(w)+h_2^2(w)} \geq \frac{(1-2^{-r})^2}{1+2^{-2r}} \geq 1-2^{-r_1},$$

and if $w \notin L$ we obtain

$$P_{V_w}(o=1|p=1) = \frac{h_1^2(w)}{h_1^2(w)+h_2^2(w)} \leq \frac{2^{-2r}}{(1-2^{-r})^2} \leq 2^{-r_1}.$$

Therefore, by taking $r \geq \max(r_1+2, r_2+2)$, L is in $\mathrm{postBQP_{aFP}}$.

Next we show $\mathrm{postBQP_{aFP}} \subseteq \mathrm{AWPP}$. Let us assume that a language L is in $\mathrm{postBQP_{aFP}}$. Then for any polynomials r_1 and r_2 there exist a uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits, an FP function f, and a polynomial q satisfying the condition in Definition 4. From Theorem 1, there exist a GapP function g and a polynomial s such that $P_{V_w}(o=1,p=1) = \frac{g(w)}{2^s}$, where $P_{V_w}(o=1,p=1)$ is the joint probability distribution for o and p. Therefore, if we take $r_2 \geq 1$, we obtain

1. If $w \in L$ then $P_{V_w}(p=1)(1-2^{-r_1}) \leq P_{V_w}(o=1,p=1) \leq P_{V_w}(p=1)$, which means

$$\frac{f(w)}{2^q(1+2^{-r_2})}(1-2^{-r_1}) \leq \frac{g(w)}{2^s} \leq \frac{f(w)}{2^q(1-2^{-r_2})},$$

   and therefore

$$\frac{1-2^{-r_2}}{1+2^{-r_2}}(1-2^{-r_1}) \leq \frac{g(w)2^q(1-2^{-r_2})}{2^s f(w)} \leq 1.$$

2. If $w \notin L$ then $0 \leq P_{V_w}(o=1,p=1) \leq 2^{-r_1}P_{V_w}(p=1)$, which means

$$0 \leq \frac{g(w)}{2^s} \leq 2^{-r_1}\frac{f(w)}{2^q(1-2^{-r_2})},$$

   and therefore

$$0 \leq \frac{g(w)2^q(1-2^{-r_2})}{2^s f(w)} \leq 2^{-r_1}.$$

Note that

$$\frac{g(w)2^q(1-2^{-r_2})}{2^s f(w)} = \frac{g(w)2^q(2^{r_2}-1)}{2^{s+r_2} f(w)},$$

and we can see $g(w)2^q(2^{r_2}-1) \in \text{GapP}$, $2^{s+r_2} f(w) > 0$, and $2^{s+r_2} f(w) \in \text{FP}$.

If we take $r_1 = r_2 \geq 3$, $\frac{(1-2^{-r_1})^2}{1+2^{-r_1}} \geq \frac{2}{3}$, and $2^{-r_1} \leq \frac{1}{3}$. Therefore L is in AWPP due to the definition of AWPP in Ref. [4].

5 Proof of Theorem 7

The inclusions $\text{postBQP}_{\text{exp}} \subseteq \text{postBQP}_{\text{size}}$ and $\text{postBQP}_{\text{FQP}} \supseteq \text{postBQP}_{\text{FP}} \supseteq \text{postBQP}_{\text{exp}}$ are obvious. Let us show $\text{postBQP}_{\text{FQP}} \subseteq \text{postBQP}_{\text{exp}}$. Its proof uses the idea of an additive adjustment of the acceptance probability from Ref. [9] with a standard multiplicative adjustment.

Let us assume that a language L is in $\text{postBQP}_{\text{FQP}}$. Then, there exist a uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits, a function $f : \{0,1\}^* \to \mathbb{N}$ whose $f(w)$ can be calculated by another uniform family of polynomial-size quantum circuits for any input w, and a polynomial $h \geq 0$ such that $P_{V_w}(p=1) = \frac{f(w)}{2^h}$ (h precisely means $h(|w|)$) and

1. If $w \in L$, then $\frac{9}{10} \leq P_{V_w}(o=1|p=1) \leq 1$.
2. If $w \notin L$, then $0 \leq P_{V_w}(o=1|p=1) \leq \frac{1}{10}$.

We can take a function $t : \{0,1\}^* \to \mathbb{N} \cup \{0\}$ such that $2^{t(w)} \leq f(w) < 2^{t(w)+1}$ for any input w. Note that $t(w)$ can be calculated by a uniform family of polynomial-size quantum circuits.

From V, we construct the uniform family $W = \{W_n\}_n$ of polynomial-size quantum circuits implemented on input w as follows:

1. $W_{|w|}$ flips a coin. If heads, it simulates $V_{|w|}$.
2. If tails, $W_{|w|}$ outputs $o = 1$ with probability $1/2$, and $p = 1$ with probability $\frac{2^{t(w)+1}-f(w)}{2^h}$ independently.

Since

$$2^h - 2^{t(w)+1} + f(w) \geq f(w) - 2^{t(w)+1} + f(w) = 2(f(w) - 2^{t(w)}) \geq 0,$$

we obtain $\frac{2^{t(w)+1}-f(w)}{2^h} \leq 1$.

Then,

$$P_{W_w}(p=1) = \frac{1}{2}P_{V_w}(p=1) + \frac{1}{2}\frac{2^{t(w)+1}-f(w)}{2^h} = \frac{2^{t(w)}}{2^h},$$

and

$$\begin{aligned} P_{W_w}(o=1|p=1) &= \frac{P_{W_w}(o=1,p=1)}{P_{W_w}(p=1)} \\ &= \frac{\frac{1}{2}P_{V_w}(o=1|p=1)P_{V_w}(p=1) + \frac{1}{2}\frac{2^{t(w)+1}-f(w)}{2^h}\frac{1}{2}}{\frac{2^{t(w)}}{2^h}} \\ &= \frac{f(w)}{2^{t(w)+1}}P_{V_w}(o=1|p=1) + \frac{1}{2}\frac{2^{t(w)+1}-f(w)}{2^{t(w)+1}}. \end{aligned}$$

If $w \in L$,

$$\begin{aligned} P_{W_w}(o=1|p=1) &= \frac{f(w)}{2^{t(w)+1}} P_{V_w}(o=1|p=1) + \frac{1}{2}\frac{2^{t(w)+1}-f(w)}{2^{t(w)+1}} \\ &\geq \frac{1}{2}\frac{9}{10} + \frac{1}{2}\frac{1}{2} = \frac{7}{10}. \end{aligned}$$

If $w \notin L$,

$$\begin{aligned} P_{W_w}(o=1|p=1) &= \frac{f(w)}{2^{t(w)+1}} P_{V_w}(o=1|p=1) + \frac{1}{2}\frac{2^{t(w)+1}-f(w)}{2^{t(w)+1}} \\ &\leq \frac{1}{2}\frac{1}{10} + \frac{1}{2}\frac{1}{2} = \frac{3}{10}. \end{aligned}$$

Here, we have used the fact that $\alpha\frac{9}{10} + (1-\alpha)\frac{1}{2} \geq \frac{1}{2}\frac{9}{10} + \frac{1}{2}\frac{1}{2}$ and $\alpha\frac{1}{10} + (1-\alpha)\frac{1}{2} \leq \frac{1}{2}\frac{1}{10} + \frac{1}{2}\frac{1}{2}$ for $\alpha \geq 1/2$. Note that $f(w)/2^{t(w)+1} \geq 1/2$, since $f(w) \geq 2^{t(w)}$.

From W, we construct the uniform family $R = \{R_n\}_n$ of polynomial-size quantum circuits implemented on input w in the following way:

1. $R_{|w|}$ simulates $W_{|w|}$.
2. $R_{|w|}$ outputs $o = 1$ if and only if $W_{|w|}$ outputs $o = 1$.
3. $R_{|w|}$ generates a random bit b which takes $b = 1$ with probability $2^{-t(w)}$. (Note that $t(w) \leq h$.)
4. $R_{|w|}$ outputs $p = 1$ if and only if $b = 1$ and $W_{|w|}$ outputs $p = 1$.

Then, $P_{R_w}(o = 1|p = 1) = P_{W_w}(o = 1|p = 1)$ and $P_{R_w}(p = 1) = P_{W_w}(p = 1)2^{-t(w)} = 2^{-h}$. Therefore, L is in $\mathrm{postBQP}_{\mathrm{exp}}$.

6 Proof of Theorem 8

Let us first show $\mathrm{postBPP}_{\mathrm{FP}} \subseteq \mathrm{WAPP}$. We assume that a language L is in $\mathrm{postBPP}_{\mathrm{FP}}$. Then, there exist a probabilistic Turing machine V, an FP function $f > 0$, and a polynomial s such that $P_{V_w}(p = 1) = \frac{f(w)}{2^s}$. There exist a #P function g and a polynomial q such that $P_{V_w}(o = 1, p = 1) = \frac{g(w)}{2^q}$. Therefore, by the conditions on $P_{V_w}(o = 1|p = 1)$, we obtain if $w \in L$, $\frac{1+\epsilon}{2} \leq \frac{2^s g(w)}{2^q f(w)} \leq 1$, and if $w \notin L$, $0 \leq \frac{2^s g(w)}{2^q f(w)} \leq \frac{1-\epsilon}{2}$. Since $2^s g(w)$ is a #P function and $2^q f(w)$ is an FP function, L is in WAPP.

Now let us show $\mathrm{UP} \cap \mathrm{coUP} \subseteq \mathrm{postBPP}_{\mathrm{FP}}$. Let us assume that a language L is in $\mathrm{UP} \cap \mathrm{coUP}$. Then, there exist two polynomial-time nondeterministic Turing machines N and M such that

1. If $w \in L$ then N has exactly one accepting path, and all paths of M reject.
2. If $w \notin L$ then all paths of N reject, and M has exactly one accepting path.

Without loss of generality, we can assume that both N and M have 2^q computation paths. Let us consider the following algorithm V:

1. Randomly choose $x \in \{0, 1\}^q$, and simulate the computation paths represented by x of N and M on input w.

2. If both N and M reject, output $p=0$ and $o=0$. If N accepts and M rejects, output $p=1$ and $o=1$. If M accepts and N rejects, output $p=1$ and $o=0$.

3. Postselect on $p=1$.

The probability of postselecting $p=1$ is 2^{-q}. Furthermore, $P_{V_w}(o=1|p=1)=1$ if $w\in L$, and it is 0 if $w\notin L$. Therefore, L is in $\mathrm{postBPP}_{\mathrm{FP}}$.

Acknowledgements

TM is supported by the Tenure Track System by MEXT Japan, the JSPS Grant-in-Aid for Young Scientists (B) No.26730003, and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850. HN is supported by the JSPS Grant-in-Aid for Scientific Research (A) Nos.23246071, 24240001, 26247016, and (C) No.25330012, and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.24106009. We acknowledge an anonymous reviewer for pointing out a possibility of improving the lowerbound of $\mathrm{postBQP}_{\mathrm{FP}}$ in an early draft of this paper.

References

1. S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time. Proc. R. Soc. A **461**, 3473-3482 (2005).
2. E. Böhler, C. Glaßer, and D. Meister, Error-bounded probabilistic computations between MA and AM. J. Comput. Syst. Sci. **72**, 1043-1076 (2006).
3. S. Fenner, L. Fortnow, and S. Kurtz, Gap-definable counting classes. J. Comput. Syst. Sci. **48**, 116-148 (1994).
4. S. A. Fenner, PP-lowness and a simple definition of AWPP. Theory Comput. Syst. **36**, 199-212 (2003); ECCC Report TR02-036.
5. S. Fenner, L. Fortnow, S. Kurtz, and L. Li, An oracle builder's toolkit. Inf. Comput. **182**, 95-136 (2003); Earlier version in Proc. 8th IEEE Conference on Structure in Complexity Theory, pp.120-131 (1993).
6. S. Fenner, F. Green, S. Homer, and R. Pruim, Determining acceptance probability for a quantum computation is hard for PH. Proc. R. Soc. A **455**, 3953-3966 (1999); arXiv:quant-ph/9812056
7. L. Fortnow and J. Rogers, Complexity limitations on quantum computation. J. Comput. Syst. Sci. **59**, 240-252 (1999).
8. Y. Han, L. Hemaspaandra, and T. Thierauf, Threshold computation and cryptographic security. SIAM J. Comput. **26**, 59-78 (1997).
9. S. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura, Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. Quant. Inf. Comput. **12**, 461-471 (2012).
10. G. Kuperberg, How hard is it to approximate the Jones polynomial? arXiv:0908.0512
11. L. Li, On the counting functions. Ph.D. thesis, University of Chicago (1993).
12. T. Yamakami and A. C. Yao, $\mathrm{NQP}_{\mathbb{C}}=\mathrm{coC_{=}P}$. Inf. Process. Lett. **71**, 63-69 (1999).

Appendixes

A Proof of Theorem 4

The proof is the same as that of $\mathrm{postBQP}_{\mathrm{aFP}}=\mathrm{AWPP}$ (Theorem 3) given in Sec. 4.

First, we show $\mathrm{APP}\subseteq\mathrm{postBQP}_{\mathrm{asize}}$. Since $\mathrm{APP}=\mathrm{coAPP}$ [11], we show $\mathrm{APP}\cap\mathrm{coAPP}\subseteq\mathrm{postBQP}_{\mathrm{asize}}$. The rest of the proof is the same as that of $\mathrm{AWPP}\cap\mathrm{coAWPP}\subseteq\mathrm{postBQP}_{\mathrm{aFP}}$

except that two FP functions $f_1(w)$ and $f_2(w)$ are replaced with two GapP functions $f_1(1^{|w|})$ and $f_2(1^{|w|})$.

Furthermore, the proof of $\mathrm{postBQP}_{\mathrm{asize}} \subseteq \mathrm{APP}$ is also the same as that of $\mathrm{postBQP}_{\mathrm{aFP}} \subseteq$ AWPP. We have only to replace the FP function $f(w)$ with a GapP function $f(1^{|w|})$.

B Proof of Theorem 5

Since WPP = coWPP, we show $\mathrm{WPP} \cap \mathrm{coWPP} \subseteq \mathrm{postBQP}_{\mathrm{FP}}$. Let us assume that a language L is in WPP$\cap$coWPP. Then, there exist GapP functions g_1 and g_2, and FP functions f_1 and f_2 with $0 \notin range(f_1)$ and $0 \notin range(f_2)$ such that

1. If $w \in L$

$$\begin{aligned} g_1(w) &= f_1(w), \\ g_2(w) &= 0. \end{aligned}$$

2. If $w \notin L$

$$\begin{aligned} g_1(w) &= 0, \\ g_2(w) &= f_2(w). \end{aligned}$$

Then, there exist GapP functions $g'_1(w) \equiv g_1(w)f_2(w)$ and $g'_2(w) \equiv g_2(w)f_1(w)$ such that

1. If $w \in L$

$$\begin{aligned} g'_1(w) &= g_1(w)f_2(w) = f_1(w)f_2(w), \\ g'_2(w) &= g_2(w)f_1(w) = 0. \end{aligned}$$

2. If $w \notin L$

$$\begin{aligned} g'_1(w) &= g_1(w)f_2(w) = 0, \\ g'_2(w) &= g_2(w)f_1(w) = f_2(w)f_1(w). \end{aligned}$$

In other words, there exist counting machines C^1 and C^2 such that

1. If $w \in L$

$$\begin{aligned} C_a^1(w) - C_r^1(w) &= f_1(w)f_2(w), \\ C_a^2(w) - C_r^2(w) &= 0. \end{aligned}$$

2. If $w \notin L$

$$\begin{aligned} C_a^1(w) - C_r^1(w) &= 0, \\ C_a^2(w) - C_r^2(w) &= f_2(w)f_1(w). \end{aligned}$$

Here, $C_a^j(w)$ and $C_r^j(w)$ are numbers of accepting and rejecting paths of C^j on input w, respectively.

There exist normal counting machines N^1 and N^2 such that [3]

1. If $w \in L$

$$\begin{aligned} N_a^1(w) - N_r^1(w) &= 2f_1(w)f_2(w), \\ N_a^2(w) - N_r^2(w) &= 0. \end{aligned}$$

2. If $w \notin L$

$$\begin{aligned} N_a^1(w) - N_r^1(w) &= 0, \\ N_a^2(w) - N_r^2(w) &= 2f_1(w)f_2(w). \end{aligned}$$

Without loss of generality, we can assume that both N^1 and N^2 have computation trees on input w whose paths are represented by $\{0,1\}^{q(|w|)}$.

For a given input w, $V = \{V_n\}_n$ is defined as the following procedure. First, we generate

$$\frac{1}{\sqrt{2^{q(|w|)+1}}} \sum_{x\in\{0,1\}^{q(|w|)}} \Big((-1)^{N^1(w,x)}|x\rangle \otimes |N^1(w,x)\rangle \otimes |1\rangle + (-1)^{N^2(w,x)}|x\rangle \otimes |N^2(w,x)\rangle \otimes |0\rangle \Big)$$

by a polynomial-size quantum circuit. Let us postselect the first and second registers on $|+\rangle^{\otimes q(|w|)+1}$. Then, the (unnormalized) state after the postselection is

$$\frac{1}{2^{q(|w|)+1}} \Big((N_a^1(w) - N_r^1(w))|1\rangle + (N_a^2(w) - N_r^2(w))|0\rangle \Big).$$

Therefore, the postselection probability is

$$\begin{aligned} P_{V_w}(p=1) &= \frac{(N_a^1(w) - N_r^1(w))^2 + (N_a^2(w) - N_r^2(w))^2}{2^{2q(|w|)+2}} \\ &= \frac{(2f_1(w)f_2(w))^2}{2^{2q(|w|)+2}} \geq \frac{1}{2^{2q(|w|)}}. \end{aligned}$$

Furthermore,

$$P_{V_w}(o=1|p=1) = \begin{cases} 1 & (w \in L), \\ 0 & (w \notin L). \end{cases}$$

Therefore, L is in $\text{postBQP}_{\text{FP}}$.

C Proof of Theorem 6

$\text{postBQP} \supseteq \text{postBQP}_{\leq\exp}$ is obvious. Let us show $\text{postBQP} \subseteq \text{postBQP}_{\leq\exp}$. We assume that a language L is in postBQP. Then, from the uniform family $V = \{V_n\}_n$ of polynomial-size quantum circuits that assures $L \in \text{postBQP}$, we construct the uniform family $W = \{W_n\}_n$ of polynomial-size quantum circuits which run as follows on input w: $W_{|w|}$ generates a random bit b which is $b = 1$ with probability $2^{-q(|w|)}$, where $q > 0$ is any polynomial. Then, $W_{|w|}$ simulates $V_{|w|}$ and outputs $p = 1$ if $b = 1$ and $V_{|w|}$ outputs $p = 1$. $W_{|w|}$ outputs $o = 1$ if $V_{|w|}$ outputs $o = 1$.

Then,

$$P_{W_w}(p=1) = P_{V_w}(p=1)2^{-q(|w|)} \leq 2^{-q(|w|)}$$

and

$$P_{W_w}(o=1|p=1) = P_{V_w}(o=1|p=1).$$

Therefore, L is in $\text{postBQP}_{\leq\text{exp}}$.

D Another proof of postBQP = PP

Here we give another proof of postBQP = PP. Before showing the proof, we will give two definitions of PP.

A standard definition of PP is as follows.

Definition 18. A language L is in PP iff there exists a polynomial-time non-deterministic Turing machine such that

1. If $w \in L$ then at least $1/2$ of computation paths accept.
2. If $w \notin L$ then less than $1/2$ of computation paths accept.

There is another definition of PP that we will use:

Definition 19. (Fortnow [11, Theorem 6.4.16]) A language L is in PP iff for any polynomial r, there exist $f, g \in \text{GapP}$ such that $f > 0$ and

1. If $w \in L$ then $1 - 2^{-r(|w|)} \leq \frac{g(w)}{f(w)} \leq 1$.
2. If $w \notin L$ then $0 \leq \frac{g(w)}{f(w)} \leq 2^{-r(|w|)}$.

Theorem 9. *(Aaronson [1])* PP = postBQP*.*

Proof. First we show postBQP $\subseteq$ PP. We assume that a language L is in postBQP. Then, for any polynomial r, there exists a uniform family $\{V_n\}_n$ of polynomial-size quantum circuits. As in the proof of $\text{postBQP}_{\text{FP}} \subseteq \text{AWPP}$, if $w \in L$,

$$\begin{aligned} & 1 - 2^{-r} \leq P_{V_w}(o=1|p=1) \leq 1 \\ \Leftrightarrow\ & 1 - 2^{-r} \leq \frac{P_{V_w}(o=1,p=1)}{P_{V_w}(p=1)} \leq 1 \\ \Leftrightarrow\ & 1 - 2^{-r} \leq \frac{g(w)2^{q'}}{2^q f(w)} \leq 1 \end{aligned}$$

for $f, g \in \text{GapP}$ and polynomials q and q'. Here, we have used the fact from Theorem 1 that

$$\begin{aligned} P_{V_w}(o=1,p=1) &= \frac{g(w)}{2^q} \\ P_{V_w}(p=1) &= \frac{f(w)}{2^{q'}} \end{aligned}$$

for some $g, f \in$ GapP and polynomials q and q'. Note that for simplicity, we omit the $|w|$ dependancies of some polynomials.

If $w \notin L$

$$\begin{aligned} & 0 \leq P_{V_w}(o=1|p=1) \leq 2^{-r} \\ \Leftrightarrow \quad & 0 \leq \frac{P_{V_w}(o=1,p=1)}{P_{V_w}(p=1)} \leq 2^{-r} \\ \Leftrightarrow \quad & 0 \leq \frac{g(w)2^{q'}}{2^q f(w)} \leq 2^{-r}. \end{aligned}$$

Since $2^{q'}g(w), 2^q f(w) \in$ GapP, L is in PP.

Second, let us show PP $\subseteq$ postBQP. We assume that a language L is in PP. If $w \in L$, for any polynomial r, there exist $g, f \in$ GapP such that

$$(1-2^{-r})^2 \leq \frac{g(w)^2}{f(w)^2}.$$

Then, from Theorem 2, we have

$$\begin{aligned} P_{W'_w}(o=1) &= 2^{-q'} f(w)^2, \\ P_{V'_w}(o=1) &= 2^{-q} g(w)^2, \end{aligned}$$

which means

$$(1-2^{-r})^2 \leq \frac{2^q P_{V'_w}(o=1)}{2^{q'} P_{W'_w}(o=1)}$$

for some polynomials q and q', and uniform families $\{V'_n\}_n$ and $\{W'_n\}_n$ of polynomial-size quantum circuits. Let us define $V_{|w|}$ and $W_{|w|}$ such that

$$\begin{aligned} P_{V_w}(o=1) &= P_{V'_w}(o=1)2^{-q'}, \\ P_{W_w}(o=1) &= P_{W'_w}(o=1)2^{-q}. \end{aligned}$$

The circuit $V_{|w|}$ ($W_{|w|}$) can be constructed by simulating $V'_{|w|}$ ($W'_{|w|}$) and outputting $o=1$ with probability $2^{-q'}$ (2^{-q}) if and only if $V'_{|w|}$ ($W'_{|w|}$) outputs $o=1$. Then, we obtain

$$(1-2^{-r})^2 \leq \frac{P_{V_w}(o=1)}{P_{W_w}(o=1)}.$$

Similarly, if $w \notin L$, we have

$$\begin{aligned} & \frac{g(w)^2}{f(w)^2} \leq 2^{-2r} \\ \Leftrightarrow \quad & \frac{P_{V_w}(o=1)}{P_{W_w}(o=1)} \leq 2^{-2r}. \end{aligned}$$

Let us consider the following quantum circuit R_n: It first flips two unbiased coins. If both are heads, R_n simulates W_n.

1. If W_n outputs $o = 1$, then R_n outputs $o = 0$ and $p = 1$.
2. If W_n outputs $o = 0$, then R_n outputs $o = 0$ and $p = 0$.

Otherwise, R_n simulates V_n.

1. If V_n outputs $o = 1$, then R_n outputs $o = 1$ and $p = 1$.
2. If V_n outputs $o = 0$, then R_n outputs $o = 0$ and $p = 0$.

Then,

$$\begin{aligned} P_{R_w}(p=1) &= \frac{3}{4}P_{V_w}(o=1) + \frac{1}{4}P_{W_w}(o=1) \\ &\geq \frac{f(w)^2}{4 \times 2^{q+q'}} \\ &> \frac{1}{2^{q+q'+2}}, \end{aligned}$$

and

$$\begin{aligned} P_{R_w}(o=1|p=1) &= \frac{P_{R_w}(o=1,p=1)}{P_{R_w}(p=1)} \\ &= \frac{\frac{3}{4}P_{V_w}(o=1)}{\frac{3}{4}P_{V_w}(o=1) + \frac{1}{4}P_{W_w}(o=1)}. \end{aligned}$$

If $w \in L$,

$$\begin{aligned} P_{R_w}(o=1|p=1) &= \frac{3P_{V_w}(o=1)}{3P_{V_w}(o=1) + P_{W_w}(o=1)} \\ &\geq \frac{3P_{V_w}(o=1)}{3P_{V_w}(o=1) + \frac{P_{V_w}(o=1)}{(1-2^{-r})^2}} \\ &= \frac{3 - 6 \times 2^{-r} + 3 \times 2^{-2r}}{4 - 6 \times 2^{-r} + 3 \times 2^{-2r}} \\ &\geq \frac{3 - 6 \times 2^{-r}}{4 + 3 \times \frac{1}{2}} \\ &\geq \frac{1}{2} + \frac{1}{22} - \frac{12}{11} \times 2^{-r}. \end{aligned}$$

If $w \notin L$,

$$\begin{aligned} P_{R_w}(o=1|p=1) &= \frac{3P_{V_w}(o=1)}{3P_{V_w}(o=1) + P_{W_w}(o=1)} \\ &\leq \frac{3P_{V_w}(o=1)}{3P_{V_w}(o=1) + \frac{P_{V_w}(o=1)}{2^{-2r}}} \\ &\leq 3 \times 2^{-2r}. \end{aligned}$$

Therefore, $L \in \text{postBQP}$. □