# Note on quantum counting classes[*]

Yaoyun Shi [†] Shengyu Zhang[‡]

**Abstract**

We define counting classes #**BPP** and #**BQP** as natural extensions of the classical well-studied one #**P** to the randomized and quantum cases. It is then shown that $\mathbf{P}^{\#\mathbf{P}} = \mathbf{P}^{\#\mathbf{BQP}}$.

## 1 Introduction

One important type of computational tasks are counting problems, and a particularly interesting class of such problems are for counting the number of the *certificates*. These counting problems naturally arise in a plethora of fields ranging from enumerative combinatorics, to statistical physics and economics; see [AB09] (Chapter 17) for a number of specific examples. Counting certificates is in general harder than the corresponding **NP** problems, which merely requires to decide for an input instance whether at least one certificate exists.

In [Val79b] Valiant initialized the study of counting problems from a complexity perspective by defining a counting class called #**P**. Precisely, the class contains the functions $f : \{0,1\}^* \to \mathbb{N}$ which have a polynomial-time nondeterministic Turing machine $M$ with the number of accepting paths on an input $x$ equal to $f(x)$. In another paper [Val79a] of Valiant, it was showed that computing Perm, the permanent of {0,1}-matrices, is #**P**-complete. That is to say, Perm is in #**P** and any other function in #**P** can be computed in polynomial time given Perm as an oracle. This implies the computational hardness of computing Perm, in a strong contrast to the existence of efficient algorithms for computing the determinant, a quantity closely related to permanent, of a matrix. More properties of the class #**P** were later discovered, including Toda's discovery that the polynomial hierarchy **PH** is in $\mathbf{P}^{\#\mathbf{P}}$.

In this paper, we consider counting classes in the randomized and quantum computational modes. When the probability is involved, one issue needs to be handled properly. For a predicate $P(x, y)$ decided by a probabilistic or quantum Turing machine (PTM or QTM), a (candidate) certificate $y$ is usually not perfectly good or perfectly bad as in the deterministic Turing machine case, but has an accepting probability, and the probabilities for different $y$'s can be quite densely distributed in $[0, 1]$. As in bounded-error classes, we assume a gap between the good and bad certificates by requiring that each certificate has acceptance probability at least $2/3$ or at most $1/3$. Then $f(x)$ is equal

[*] This work is supported by Hong Kong grants RGC-419309 and RGC-418710. Yaoyun: 1. Please add your grant information. 2. I'm not sure this is the most suitable title; please feel free to suggest something else.

[†] Yaoyun: Please add your mailing address.

[‡] Department of Computer Science and Engineering, The Chinese University of Hong Kong. Email: syzhang@cse.cuhk.edu.hk

to the number of the certificates with large acceptance probability; see the next section for precise definition of #**BPP**.

When it comes to the quantum counting, more issues arise. Since the certificate space is a continuous Hilbert space, there are infinitely many good certificates in general, and thus counting may not be meaningful. The continuity also makes the gap between acceptance probabilities impossible: If certificates states $|y_1\rangle$ and $|y_2\rangle$ have acceptance probabilities, say, $\epsilon$ and $1-\epsilon$, respectively, then the acceptance probability for a superposition of $|y_1\rangle$ and $|y_2\rangle$ can be any real number between $\epsilon$ and $1-\epsilon$. A natural measure to use is the dimension of subspace of good certificates. However, how can we guarantee that the set of good certificates form a subspace?

All these issues shall be settled by a spectral result in [MW05]. Basically, what was shown there is a useful fact that if the verifier is a uniform family of quantum circuit, then there is a natural spectral decomposition of the witness space $V = \uplus_p V_p$, such that in each eigenspace $V_p$, the corresponding eigenvalue $p$ is the acceptance probability of a witness $|\psi_p\rangle \in V_p$. In addition, a general witness $|\psi\rangle = \sum_p \alpha_p |\psi_p\rangle$, where $|\psi_p\rangle \in V_p$, has acceptance probability $\sum_p |\alpha_p|^2 p$. Based on this, we define the counting class #**BQP** as those functions $f$ with a uniform family of quantum circuit of polynomial size such that all these eigenvalues are either at least 2/3 or at most 1/3, and $f(x)$ is equal to the number of eigenvalues at least 2/3.

One important question in quantum computing is to understand the ultimate power of quantum computers in various computational modes. Since counting problems form an important class of computational tasks, it is desirable to understand the power of quantum counting classes. In this paper, we shall show the following relation of #**BQP** and #**P**.

**Theorem 1.1** $\mathbf{P}^{\#\mathbf{BQP}} = \mathbf{P}^{\#\mathbf{P}}$.

Another way to look at the result is from a central question of where **BQP** sits in classical complexity classes. While it has been known for more than a decade that $\mathbf{BQP} \subseteq \mathbf{PP} \subseteq \mathbf{P}^{\#\mathbf{P}}$, pursuing a better upper bound turns out to be much harder. One way to improve the containment is to see how much we can boost the power of **BQP** so that it is still upper bounded by a classical complexity class such as **PP**. Observing that the proof that $\mathbf{BQP} \subseteq \mathbf{PP}$ does not use the bounded-error assumption of **BQP**, Watrous [Wat09] improved the relation to $\mathbf{PQP} = \mathbf{PP}$, where **PQP** is the same as **BQP** but only requiring the acceptance probability to be strictly larger than 1/2 for Yes instances and at most 1/2 for No instances. The result of this note can be viewed in the same spirit as an improvement of $\mathbf{BQP} \subseteq \mathbf{P}^{\#\mathbf{P}}$ by pushing up the **BQP** to $\mathbf{P}^{\#\mathbf{BQP}}$.

## Related work

One classical result about the number of witness and its implication on hardness is the UniqueNP problem studied by Valiant and Vazirani [VV86], who showed that an **NP** problem with the promise of at most one certificate exists is no easier than the problem without the promise. Recently the result was extended to the randomized [ABOBS08] and quantum [JKK$^+$10] cases, where a gap is also assumed between the "good" and "bad" certificates.

## 2 Preliminaries and notation

In the model for #**BQP**, there is a uniform family of quantum circuits of polynomial size. We can equivalently think of the circuits as depending on input, so the verifier for input $x$ is $V_x$. Suppose that $V_x$ has an input space $W \otimes S$, where $W$ is the space for an $m$-qubit potential witness $|\psi\rangle \in W$, and $S$ is a $k$-qubit working space, initialized as $|0^k\rangle$. On a particular witness $|\psi\rangle$, the circuit operates on $|\psi\rangle \otimes |0^k\rangle$ and, at the end of the output, measures the first qubit in the $\{|0\rangle, |1\rangle\}$ basis and output the result. Overloading the notation, we also use $V_x$ to denote the unitary operation that the circuit applies. Define two projections

1. $\Pi_{acc} = V_x^\dagger \Pi_{acc} V_x$: projection onto the subspace corresponding to the first qubit being 1 if the computation $V_x$ if performed.
2. $\Pi_{init} = I_m \otimes |0^k\rangle_S \langle 0^k|_S$: projection onto the subspace of $S$ containing $|0^k\rangle$.

A simple but important property for analysis of **QMA** feasible is to consider the eigensystem of $\Pi_{init}\Pi_{acc}\Pi_{init}$. Since it is a positive operator, it enjoys a spectral decomposition. There are $2^m$ eigenvectors $|\phi_i\rangle$ of $\Pi_{init}\Pi_{acc}\Pi_{init}$, all in the form of $|\psi_i\rangle \otimes |0^k\rangle$. The eigenvalue for $|\phi_i\rangle$ turns out to be the accept probability $p_i$ of the witness $|\psi_i\rangle$:

$$\lambda_i(\Pi_{init}\Pi_{acc}\Pi_{init}) = \langle \psi_i 0^k | \Pi_{init}\Pi_{acc}\Pi_{init} | \psi_i 0^k\rangle = \|\Pi_{acc}\Pi_{init}|\psi_i 0^k\rangle\|^2 = \|\Pi_{acc}|\psi_i 0^k\rangle\|^2 \tag{1}$$

Now the acceptance probability for a general witness state $\sum_i \alpha_i |\phi_i\rangle$ can also be computed easily:

$$\|\Pi_{acc} \sum_i \alpha_i |\phi_i\rangle\|^2 = \langle \sum_i \alpha_i \phi_i | \Pi_{acc} | \sum_i \alpha_i \phi_i \rangle = \sum_{ij} \alpha_i^* \alpha_j \langle \phi_i | \Pi_{acc} | \phi_j \rangle = \sum_i |\alpha_i|^2 p_i \tag{2}$$

where the last equality uses the fact that the eigenvectors are orthogonal. With all these setup, we can define the quantum counting class. First recall that #**P** is defined as follows.

**Definition 2.1**

$$f \in \#\mathbf{P} \textit{ if } \exists \textit{ a polynomial-time Turing machine } V \textit{ s.t. } f(x) = |\{w : V(x,w) = 1\}|. \tag{3}$$

The counting classes #**BPP** and #**BQP** are defined as follows.

**Definition 2.2** *$f \in$ #**BPP** if $\exists$ a polynomial-time probabilistic Turing machine $V$ s.t.*

1. *$\forall w, V(x,w) = 1$ with probability either at least 2/3 or at most 1/3,*
2. *$f(x) = |\{w : V(x,w) = 1$ with probability at least $2/3\}|$.*

**Definition 2.3** *$f \in$ #**BQP** if $\exists$ a uniform family of quantum circuits $\{V_x\}$ of size polynomial in $|x|$ s.t.*

1. *The eigenvalues of $\Pi_{init}\Pi_{acc}\Pi_{init}$ are all either at least 2/3 or at most 1/3,*
2. *$f(x) =$ the number of eigenvalues of $\Pi_{init}\Pi_{acc}\Pi_{init}$ that are at least 2/3.*

# 3 On the limitation of the quantum counting class

In this section we shall show that #**BQP** and #**P**, when working as oracles for **P**, give the same class. The idea is to first amplify the correct probability, and then use the double-counting on trace. The same idea was used in [MW05] to prove that **QMA** $\subseteq$ **PP**. Let us first recall the following amplification result for **QMA**.

**Lemma 3.1 (Strong Amplification of QMA, [MW05])** *For any problem in* **PromiseQMA**, *and any polynomials $m(n)$ and $r(n)$, there is a universal family of polynomial-size verifiers $\{V_x : |x| = n\}$ with $m(n)$-qubit witness space and $O(r(n))$-qubit working space s.t. the eigenvalues of $\Pi_{init}\Pi_{acc}\Pi_{init}$ are either more than $1 - 2^{-r(n)}$ or less than $2^{-r(n)}$.*

**Proof** (of Theorem 1.1) We shall simulate each query to a #**BQP** oracle by a #**P** oracle with some further polynomial-time post-processing. For a query to a function $f \in$ #**BQP**, there exists a quantum verifier $V_x$ with $m$-qubit witness space. The strong amplification in Lemma 3.1 gives both the soundness error and completeness error smaller than $2^{-r}$. Actually, denote by $\Pi'_{init}$ and $\Pi'_{acc}$ the corresponding projections for the new verifier, then the eigenvectors of $Q' = \Pi'_{init}\Pi'_{acc}\Pi'_{init}$ are the same as those of $Q = \Pi_{init}\Pi_{acc}\Pi_{init}$, but the corresponding eigenvalues change to either more than $1 - 2^{-r}$ or less than $2^{-r}$.

By the definition of #**BQP**, $f(x)$ is equal to the number of eigenvalues of $Q$ that are at least $2/3$, which is in turn equal to the the number of eigenvalues of $Q'$ that are at least $1 - 2^{-r}$. Now consider the trace of $Q'$. On the one hand, we have

$$\mathtt{tr}(Q') = \sum_i \lambda_i(Q') \geq f(x)(1 - 2^{-r}). \tag{4}$$

On the other hand, since all the "small" eigenvalues are less than $2^{-r(n)}$, we have

$$\mathtt{tr}(Q') = \sum_i \lambda_i(Q') \leq (2^m - f(x)) \cdot 2^{-r} + f(x) \cdot 1 = f(x)(1 - 2^{-r}) + 2^{m-r}. \tag{5}$$

Note that one desirable property of strong amplification is the flexibility of choice of $r$ to be any polynomial of $n$, independent of $m$. Let $r = m + 2$, then

$$f(x) - 1/4 \leq f(x)(1 - 2^{-(m+2)}) \leq \mathtt{tr}(Q') \leq f(x)(1 - 2^{-(m+2)}) + 1/4 \leq f(x) + 1/4. \tag{6}$$

where the first inequality is because $f(x) \leq 2^m$ due to the assumption that the verifier for $f$ has $m$-qubit witness space.

Without loss of generality, we can assume that the quantum circuit is made of Toffoli, Hadamard and $i$-shift gates. Each entry $(i, j)$ of the whole matrix $Q'$ equals to $h(i, j)/2^g$ where $h$ is an #**P** function and $g = poly(n)$ is the number of Hadamard gates in the circuit. Since the trace also equals to the summation of the diagonal entries, and #**P** is closed under exponential sum, we get

$$\mathtt{tr}(Q') = h/2^g \tag{7}$$

for some **GapP** function $h$. Suppose $h = h_1 - h_2$ for some #**P** functions $h_1$ and $h_2$. Now we use our #**P** oracle to get $h_1$ and $h_2$, and then compute $[(h_1 - h_2)/2^g]$ in deterministic polynomial time, where the bracket is to round the number to the closest integer. By Eq. (6), this is equal to $f(x)$. This completes the simulation of the query to the #**BQP** oracle. □

# References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, Cambridge, UK, 2009.

[ABOBS08] Dorit Aharonov, Michael Ben-Or, Fernando Brandao, and Or Sattath. The pursuit for uniqueness: Extending valiant-vazirani theorem to the probabilistic and quantum settings. *arXiv:0906.4425*, 2008.

[JKK$^+$10] Rahul Jain, Iordanis Kerenidis, Greg Kuperberg, Miklos Santha, Or Sattath, and Shengyu Zhang. On the power of a unique quantum witness. In *Proceedings of the First Symposium on Innovations in Computer Science*, pages 470–481, 2010.

[MW05] Chris Marriott and John Watrous. Quantum arthur-merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[Val79a] Leslie Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189201, 1979.

[Val79b] Leslie Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

[VV86] Leslie Valiant and Vijay Vazirani. **NP** is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.

[Wat09] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and System Science*, 2009.