Finding resource states of measurement-based quantum computing is harder than quantum computing

Tomoyuki Morimae

Finding resource states of measurement-based quantum computing is harder than quantum computing

Tomoyuki Morimae*

Department of Computer Science, Gunma University,
1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan

Measurement-based quantum computing enables universal quantum computing with only adaptive single-qubit measurements on certain many-qubit states, such as the graph state, the Affleck-Kennedy-Lieb-Tasaki (AKLT) state, and several tensor-network states. Finding new resource states of measurement-based quantum computing is a hard task, since for a given state there are exponentially many possible measurement patterns on the state. In this paper, we consider the problem of deciding, for a given state and a set of unitary operators, whether there exists a way of measurement-based quantum computing on the state that can realize all unitaries in the set, or not. We show that the decision problem is QCMA-hard, which means that finding new resource states of measurement-based quantum computing is harder than quantum computing itself (unless BQP is equal to QCMA). We also derive an upperbound of the decision problem: the problem is in a quantum version of the second level of the polynomial hierarchy.

I. INTRODUCTION

Measurement-based quantum computing [1] is another model of quantum computing than the traditional circuit model where universal quantum computing can be done with only adaptive single-qubit measurements on certain many-qubit states which are called resource states. Although it is mathematically equivalent to the circuit model, the clear separation between the resource preparation phase and the resource consumption phase has enabled plenty of new results in, for example, fault-tolerant quantum computing [2], condensed matter physics [3–8], studying roles of quantumness in quantum computing [9, 10], secure quantum computing (blind quantum computing) [11, 12], and quantum complexity theory [13–15].

The first and the most standard example of universal resource states is the graphs state [1], which is obtained by applying CZ operators on all connected $|+\rangle$ states placed on every vertex of a graph. Researchers have tried to find more condensed-matter physically motivated resource states. For example, the Affleck-Kennedy-Lieb-Tasaki (AKLT) state [16] was found to be a universal resource state [3–6]. Several tensor-network states were also shown to be universal resource states by considering virtual quantum computing in the correlation space [17]. Furthermore, low-temperature thermal equilibrium states of some physically motivated Hamiltonians were shown to be universal resource states for topological measurement-based quantum computing [18, 19]. In spite of much efforts, however, we have only a very short list of universal resource states. One of the main reasons of the difficulty of finding new resource states is the exponential increase of possible measurement patterns on a given state. Therefore we have a natural question: how

hard is it to find a new resource state? Is it, say, NP-hard?

In this paper, we study the computational complexity of finding new resource states of measurement-based quantum computing. We consider the problem of deciding, for a given state and a set of unitary operators, whether there exists a way of measurement-based quantum computing on the state that can realize all unitaries in the set, or not. We show that the decision problem is QCMA-hard. The class QCMA [20, 21] is a quantum version of NP and defined in the following way:

A language L is in QCMA if and only if there exists a uniformly-generated family $\{V_x\}_x$ of polynomial-size quantum circuits such that

- If $x \in L$, then there exists a w-bit string $y \in \{0,1\}^w$ such that the probability of obtaining 1 when the first qubit of $V_x(|y\rangle \otimes |0^n\rangle)$ is measured in the computational basis is $\geq \frac{2}{3}$. Here, $n = poly(|x|)$ and $w = poly(|x|)$.

- If $x \notin L$, then for any w-bit string $y \in \{0,1\}^w$, the probability is $\leq \frac{1}{3}$.

It is known that the error bound $(\frac{2}{3}, \frac{1}{3})$ can be amplified to $(1 - 2^{-r}, 2^{-r})$ for any polynomial r by using the standard argument of the error reduction used in other probabilistic classes such as BPP [26], MA [27], and BQP [28]. Obviously QCMA contains BQP. (We have only to ignore the witness.) Moreover, QCMA seems to be strictly larger than BQP, since it seems to be difficult to find a correct y in a quantum polynomial time. In fact, there are several results that support QCMA $\neq$ BQP. (For example, it is obvious that QCMA contains NP. However, BQP is not believed to contain NP [22].) Therefore, if we assume QCMA $\neq$ BQP, we can put our result concisely as follows: "finding new resource states is harder than quantum computing itself".

We also study upperbounds of the problem. We show that the problem is in a quantum version of the second

level of the polynomial hierarchy. The polynomial hierarchy is one of the most important concepts in complexity theory, and its quantum versions were considered in Refs. [23, 24].

There are many studies about relations between measurement-based quantum computing and complexity. In particular, the result [25] studied how quantum resource states enhance the computational power of classical computing. Our result is in some sense a complementary to these studies: they study complexity below BQP (BPP or classically-non-universal), while we study complexity above BQP, such as QCMA.

II. MEASUREMENT-BASED QUANTUM COMPUTING

Before giving the precise definition of the problem that we show to be QCMA-hard, let us here explain an abstract form of measurement-based quantum computing. Assume that as a resource state, we are given an N-qubit state $|\Psi\rangle$. Let $\mathcal{U} \equiv \{U_y\}_{y \in \{0,1\}^w}$ be a set of unitary operators acting on n qubits $(n \leq N)$. We say that the resource state $|\Psi\rangle$ is $\mathcal{U}$-universal with precision ϵ $(0 \leq \epsilon \leq 1)$ if there exists a polynomial-time classical algorithm Λ such that for any $y \in \{0,1\}^w$,

1. We input $(1, y)$ to Λ. Λ outputs a classical description of a single-qubit unitary operator u_1. We measure the first qubit of the resource state in the basis $\{u_1|0\rangle, u_1|1\rangle\}$. We obtain the measurement result $m_1 \in \{0, 1\}$.

2. We input $(2, y, m_1)$ to Λ. Λ outputs a classical description of a single-qubit unitary operator u_2. We measure the second qubit of the resource state in the basis $\{u_2|0\rangle, u_2|1\rangle\}$. We obtain the measurement result $m_2 \in \{0, 1\}$.

3. We input $(3, y, m_1, m_2)$ to Λ. Λ outputs a classical description of a single-qubit unitary operator u_3. We measure the third qubit of the resource state in the basis $\{u_3|0\rangle, u_3|1\rangle\}$. We obtain the measurement result $m_3 \in \{0, 1\}$.

4. In this way, we repeat this adaptive single-qubit measurements until all but the last n qubits of the resource state are measured. In other words, when we measure jth qubit of the resource state, we input $(j, y, m_1, ..., m_{j-1})$ to Λ, and get a classical description of a single-qubit unitary operator u_j from Λ. We then measure jth qubit of the resource state in the basis $\{u_j|0\rangle, u_j|1\rangle\}$, and obtain the measurement result m_j. We repeat it until $j = N - n$. Let $|\psi'_m\rangle$, where $m \equiv (m_1, ..., m_{N-n})$, be the (normalized) post-measurement state of n qubits of the resource state that are not measured. We also denote the probability of obtaining m by p_m. (For example, if $|\Psi\rangle$ is the graph state, $p_m = 2^{-(N-n)}$

for all m, and $|\psi'_m\rangle$ is equal to $U_y|0^n\rangle$ up to some Pauli byproduct operators.)

5. We input $(N - n + 1, y, m)$ to Λ. Λ outputs classical descriptions of single-qubit unitary operators $\{v_j\}_{j=1}^n$. We apply v_j on jth qubit of $|\psi'_m\rangle$ to obtain

$$|\psi_m\rangle \equiv \Big(\bigotimes_{j=1}^n v_j \Big) |\psi'_m\rangle.$$

(This process is the "final byproduct correction". For example, if $|\Psi\rangle$ is the graph state, each v_j is a Pauli byproduct operator, and $|\psi_m\rangle = U_y|0^n\rangle$ for all m.)

6. The state $\sum_m p_m |\psi_m\rangle\langle\psi_m|$ is close to the ideal state $U_y|0^n\rangle$ in the sense of

$$\frac{1}{2}\Big\| \sum_m p_m |\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \leq \epsilon.$$

Here, $\|X\|_1 \equiv \text{Tr}\sqrt{X^\dagger X}$ is the trace norm.

Note that this definition of the universality is the universality of the state generation: we require that any state is generated with high precision. It is the strongest definition. If one is interested in only the output probability distribution of quantum computing, a weaker definition of universality, namely, any output probability distribution of quantum computing is samplable, is enough. It is an interesting open problem to consider computational complexity for the weaker definition.

III. THE PROBLEM

Now we define the decision problem that we study, which is a promise version of deciding whether a given state is non-$\mathcal{U}$-universal or not. We call the problem NONUNIVERSALITY$_\epsilon$ for a parameter ϵ $(0 \leq \epsilon \leq 1)$:

- Input: $\mathcal{U}$ and $|\Psi\rangle$.

- YES: $|\Psi\rangle$ is not $\mathcal{U}$-universal. In other words, for any Λ there exists y such that,

$$\frac{1}{2}\Big\| \sum_m p_m |\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \geq 1 - \epsilon.$$

- NO: $|\Psi\rangle$ is $\mathcal{U}$-universal. In other words, there exists Λ such that for all y

$$\frac{1}{2}\Big\| \sum_m p_m |\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \leq \epsilon.$$

The main result of the present paper is that the problem is QCMA-hard for $\epsilon = 2^{-t}$, where t is any polynomial.

IV. PROOF

Here we give a proof. Let us assume that a language L is in QCMA, and let V_x be the corresponding verification circuit for an instance x. Due to the standard argument of the error reduction, we can assume without loss of generality that the acceptance probability p satisfies $p \geq 1 - 2^{-r}$ if $x \in L$ and $p \leq 2^{-r}$ if $x \notin L$, where r is any polynomial. Fix one x. From V_x, we construct the unitary operator U that acts on $n + w + 2r + 1$ qubits as follows (see Fig. 1):

1. Apply V_x on $|y0^n\rangle$ to generate $V_x|y0^n\rangle$.

2. Add an ancilla qubit initialized in $|0\rangle_1$ to generate $V_x|y0^n\rangle \otimes |0\rangle_1$.

3. Flip the ancilla qubit if and only if the first qubit of $V_x|y0^n\rangle$ is $|1\rangle$. We therefore obtain

$$(|0\rangle\langle 0| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|0\rangle_1$$
$$+ \ (|1\rangle\langle 1| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|1\rangle_1.$$

Here $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator.

4. Add $2r$ ancilla qubits initialized in $|0^{2r}\rangle_2$. We obtain

$$(|0\rangle\langle 0| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|0\rangle_1|0^{2r}\rangle_2$$
$$+ \ (|1\rangle\langle 1| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|1\rangle_1|0^{2r}\rangle_2.$$

5. Apply a $2r$-qubit unitary operator ME on the $2r$ ancilla qubits $|0^{2r}\rangle_2$ that changes the state $|0^{2r}\rangle$ to the maximally-entangled state

$$|ME\rangle \equiv \frac{1}{\sqrt{2^r}} \sum_{j=1}^{2^r} |j\rangle|j\rangle$$

if and only the first qubit of $V_x|y0^n\rangle$ is $|1\rangle$. We therefore obtain

$$(|0\rangle\langle 0| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|0\rangle_1|0^{2r}\rangle_2$$
$$+ \ (|1\rangle\langle 1| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|1\rangle_1|ME\rangle_2.$$

6. Apply $V_x^\dagger$ on the main register. We thus obtain the final state

$$U|y0^n\rangle|0\rangle_1|0^{2r}\rangle_2$$
$$= \ V_x^\dagger(|0\rangle\langle 0| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|0\rangle_1|0^{2r}\rangle_2$$
$$+ \ V_x^\dagger(|1\rangle\langle 1| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|1\rangle_1|ME\rangle_2.$$

Let us define

$$U_y \equiv U\left[\left(\bigotimes_{j=1}^{w} X_j^{y_j}\right) \otimes I^{\otimes n+2r+1}\right],$$

where y_j is the jth bit of y, and $X_j \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$ is the bit-flip operator acting on jth qubit. (Remember that V_x

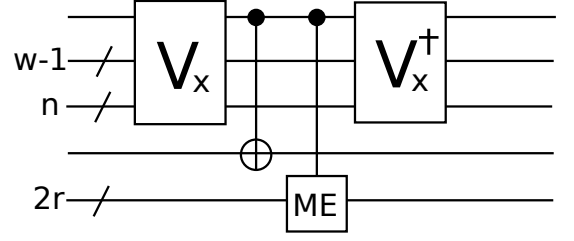
FIG. 1: The unitary operator U. ME means the unitary operator that changes $|0^{2r}\rangle$ to the maximally entangled state $|ME\rangle$.

is universal by the definition of QCMA, and therefore U_y covers a broad region of the circuit space.) We also define

$$|\Psi\rangle \equiv |0^{n+w+2r+2}\rangle.$$

First, we consider the case of $x \in L$. In this case, by the assumption of $L \in$ QCMA, $p \geq 1 - 2^{-r}$ for a certain y. Note that whatever Λ we choose, what we can do in the measurement-based quantum computation is just measuring a single qubit of $|\Psi\rangle$ and then rotating each of the $n + w + 2r + 1$ unmeasured qubits. Therefore, for any Λ, $|\psi_m\rangle$ is an $(n + w + 2r + 1)$-qubit product state for all m. Therefore, from Uhlmann's theorem,

$$|\langle\psi_m|U_y|0^{n+w+2r+1}\rangle|^2$$
$$= \ |\langle\psi_m|U|y0^{n+2r+1}\rangle|^2$$
$$\leq \ F(\rho, \sigma)^2$$
$$= \ (1-p)|\langle\xi_1\xi_2|0^{2r}\rangle|^2 + p|\langle\xi_1\xi_2|ME\rangle|^2$$
$$\leq \ (1-p) \times 1 + p|\langle\xi_1\xi_2|ME\rangle|^2$$
$$\leq \ (1-p) + pF\left(|\xi_1\rangle\langle\xi_1|, \frac{I^{\otimes r}}{2^r}\right)^2$$
$$= \ 1 - p + \frac{p}{2^r}$$
$$\leq \ 2^{-r} + 2^{-r}$$
$$= \ 2^{-r+1},$$

where $F(\rho, \sigma) \equiv \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$ is the fidelity,

$$\rho \equiv \mathrm{Tr}_2(|\psi_m\rangle\langle\psi_m|)$$
$$\equiv |\xi_1\rangle\langle\xi_1| \otimes |\xi_2\rangle\langle\xi_2|,$$
$$\sigma \equiv \mathrm{Tr}_2(U|y0^{n+2r+1}\rangle\langle y0^{n+2r+1}|U^\dagger)$$
$$= \ (1-p)|0^{2r}\rangle\langle 0^{2r}| + p|ME\rangle\langle ME|,$$

Tr_2 is the partial trace except for the send ancilla register, and $|\xi_j\rangle$ $(j = 1, 2)$ is a certain (actually product) r-qubit state. Therefore

$$F\left(\sum_m p_m|\psi_m\rangle\langle\psi_m|, U_y|0^{n+w+2r+1}\rangle\langle 0^{n+w+2r+1}|U_y^\dagger\right)$$
$$= \ \sqrt{\sum_m p_m|\langle\psi_m|U_y|0^{n+w+2r+1}\rangle|^2}$$
$$\leq \ 2^{\frac{-r+1}{2}}.$$

Hence we have shown that for any Λ, there exists y such that

$$\frac{1}{2}\Big\| \sum_m p_m|\psi_m\rangle\langle\psi_m| - U_y|0^{n+w+2r+1}\rangle\langle 0^{n+w+2r+1}|U_y^\dagger \Big\|_1$$
$$\geq 1 - 2^{\frac{-r+1}{2}}$$
$$\geq 1 - 2^{-t},$$

where we have taken $r \geq 2t+1$. It corresponds to the YES instance of the NONUNIVERSALITY.

Next, we consider the case of $x \notin L$. In this case, by the assumption of $L \in \text{QCMA}$, $p \leq 2^{-r}$ for any y. We define Λ in such a way that

$$|\psi_m\rangle = |y0^{n+2r+1}\rangle$$

for any m. This is trivially possible as follows:

1. Measure the first qubit of $|\Psi\rangle = |0^{n+w+2r+2}\rangle$ in the computational basis. Then we obtain $|\tilde{\psi}_{m=0}\rangle = |0^{n+w+2r+1}\rangle$ with probability 1.

2. Apply $X_j^{y_j}$ on the jth qubit of $|\tilde{\psi}_{m=0}\rangle$ for $j = 1,...,w$ to obtain $|\psi_{m=0}\rangle = |y0^{n+2r+1}\rangle$.

Then, for any y,

$$\sum_m p_m|\langle\psi_m|U_y|0^{n+w+2r+1}\rangle|^2$$
$$= |\langle\psi_{m=0}|U_y|0^{n+w+2r+1}\rangle|^2$$
$$= |\langle y0^{n+2r+1}|U|y0^{n+2r+1}\rangle|^2$$
$$= |\langle y0^n|V_x^\dagger(|0\rangle\langle 0| \otimes I^{\otimes n+w-1})V_x|y0^n\rangle|^2$$
$$= (1-p)^2$$
$$\geq (1-2^{-r})^2$$
$$= 1 - 2^{-r+1} + 2^{-2r}$$
$$\geq 1 - 2^{-r+1}.$$

Therefore

$$F\Big(\sum_m p_m|\psi_m\rangle\langle\psi_m|, U_y|0^{n+w+2r+1}\rangle\langle 0^{n+w+2r+1}|U_y^\dagger\Big)$$
$$= \sqrt{\sum_m p_m|\langle\psi_m|U_y|0^{n+w+2r+1}\rangle|^2}$$
$$\geq \sqrt{1 - 2^{-r+1}}.$$

Hence we have shown that there exists Λ such that for any y

$$\frac{1}{2}\Big\| \sum_m p_m|\psi_m\rangle\langle\psi_m| - U_y|0^{n+w+2r+1}\rangle\langle 0^{n+w+2r+1}|U_y^\dagger \Big\|_1$$
$$\leq 2^{\frac{-r+1}{2}}$$
$$\leq 2^{-t}.$$

It corresponds to the NO instance of the NONUNIVERSALITY. In summary, we have shown that the promise problem is QCMA-hard.

V. UPPERBOUND

In the previous section, we have shown that the problem NONUNIVERSALITY is QCMA-hard. In other words, we have derived an lower bound of the problem. It is an important open problem to find any better lower bound and better upper bound of the problem, or to show that the problem is complete for a complexity class. Here we point out that a quantum version of Π_2, which we call $Q\Pi_2$, is an upper bound of the problem. We define the class $Q\Pi_2$ as follows:

A language L is in $Q\Pi_2(a,b)$ if and only if there exists a uniformly generated family $\{V_x\}_x$ of polynomial-size quantum circuits such that

- If $x \in L$ then for any λ-bit string Λ there exists a w-bit string y such that the probability of obtaining 1 when the first qubit of $V_x(|\Lambda\rangle|y\rangle|0^n\rangle)$ is measured in the computational basis is $\geq a$. Here, $\lambda, w, n = poly(|x|)$.

- If $x \notin L$ then there exists a λ-bit string Λ such that for any w-bit string y the probability is $\leq b$.

It is obvious that $Q\Pi_2$ is in PSPACE. (We have only to try all possible Λ and y.) Other types of quantum generalizations of the polynomial hierarchy were studied in Refs. [23, 24].

We can show that the problem NONUNIVERSALITY is in $Q\Pi_2(1-2\epsilon, 2\epsilon)$. In fact, since measurement-based quantum computing can be simulated by a circuit model, there exists a polynomial-size quantum circuit V and polynomials t and n such that the reduced density operator of some n qubits of $V(|\Lambda\rangle|y\rangle|0^t\rangle)$ is

$$\rho \equiv U_y^\dagger\Big(\sum_m p_m|\psi_m\rangle\langle\psi_m|\Big)U_y.$$

We then measure all qubits of ρ in the computational basis, and reject if and only if all qubits are 0. The acceptance probability p is therefore

$$p = 1 - \langle 0^n|U_y^\dagger\Big(\sum_m p_m|\psi_m\rangle\langle\psi_m|\Big)U_y|0^n\rangle,$$

which means

$$1 - \sqrt{1-p} \leq \frac{1}{2}\Big\| \sum_m p_m|\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \quad (1)$$

and

$$\frac{1}{2}\Big\| \sum_m p_m|\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \leq \sqrt{p}. \quad (2)$$

For the the yes case, for any Λ, there exists y such that

$$\frac{1}{2}\Big\| \sum_m p_m|\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \geq 1 - \epsilon.$$

From Eq. (2), it means $1 - \epsilon \leq \sqrt{p}$. Therefore

$$
\begin{aligned}
p &\geq 1 - 2\epsilon + \epsilon^2 \\
&\geq 1 - 2\epsilon.
\end{aligned}
$$

For the no case, there exists Λ such that for any y,

$$
\frac{1}{2}\Big\| \sum_m p_m |\psi_m\rangle\langle\psi_m| - U_y|0^n\rangle\langle 0^n|U_y^\dagger \Big\|_1 \leq \epsilon.
$$

From Eq. (1), it means $1 - \sqrt{1-p} \leq \epsilon$. Therefore

$$
\begin{aligned}
p &\leq 2\epsilon - \epsilon^2 \\
&\leq 2\epsilon.
\end{aligned}
$$

Hence we have shown that the problem is in $Q\Pi_2(1 - 2\epsilon, 2\epsilon)$.

Acknowledgments

[1] R. Raussendorf and H. J. Briegel, A one-way quantum computer. Phys. Rev. Lett. **86**, 5188 (2001).

[2] R. Raussendorf, J. Harrington, and K. Goyal, Topological fault-tolerance in cluster state quantum computation. New J. Phys. **9**, 199 (2007).

[3] G. K. Brennen and A. Miyake, Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian. Phys. Rev. Lett. **101**, 010502 (2008).

[4] A. Miyake, Quantum computational capability of a 2D valence bond solid phase. Ann. Phys. **326**, 1656 (2011).

[5] A. Miyake, Quantum computation on the edge of a symmetry-protected topological order. Phys. Rev. Lett. **105**, 040501 (2010).

[6] T. C. Wei, I. Affleck, and R. Raussendorf, Affleck-Kennedy-Lieb-Tasaki state on a honeycomb lattice is a universal quantum computational resource. Phys. Rev. Lett. **106**, 070501 (2011).

[7] D. V. Else, I. Schwarz, S. D. Bartlett, and A. C. Doherty, Symmetry-protected phases for measurement-based quantum computation. Phys. Rev. Lett. **108**, 240505 (2012).

[8] J. Miller and A. Miyake, Resource quality of a symmetry-protected topologically ordered phase for quantum computation. Phys. Rev. Lett. **114**, 120506 (2015).

[9] D. Gross, S. T. Flammia, and J. Eisert, Most quantum states are too entangled to be useful as computational resources. Phys. Rev. Lett. **102**, 190501 (2009).

[10] M. J. Bremner, C. Mora, and A. Winter, Are random pure states useful for quantum computation? Phys. Rev. Lett. **102**, 190502 (2009).

[11] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation. In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE Computer Society, Los Alamitos, USA, 2009), p.517.

[12] M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. **115**, 220502 (2015).

[13] M. McKague, Interactive proofs for BQP via self-tested graph states. Theor. of Comput. **12**, 1 (2016).

[14] T. Morimae, D. Nagaj, and N. Schuch, Quantum proofs can be verified using only single qubit measurements. Phys. Rev. A **93**, 022326 (2016).

[15] K. Fujii and T. Morimae, Quantum commuting circuits and complexity of Ising partition functions. arXiv:1311.2128

[16] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Valence bond ground states in isotropic quantum antiferromagnets. Comm. Math. Phys. **115**, 477 (1988).

[17] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, Measurement-based quantum computation beyond the one-way model. Phys. Rev. A **76**, 052315 (2007).

[18] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Thermal states as universal resources for quantum computation with always-on interactions. Phys. Rev. Lett. **107**, 060501 (2011).

[19] K. Fujii and T. Morimae, Topologically protected measurement-based quantum computation on the thermal state of a nearest-neighbor two-body Hamiltonian with spin-3/2 particles. Phys. Rev. A **85**, 010304(R) (2012).

[20] S. Aaronson and G. Kuperberg, Quantum versus classical proofs and advice. Theor. of Comput. **3**, 129 (2007).

[21] D. Aharonov and T. Naveh, Quantum NP - a survey. arXiv:0210077

[22] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strength and weakness of quantum computing. SIAM J. of Computing **26**, 1510 (1997).

[23] S. Gharibian and J. Kampe, Hardness of approximation for quantum problems. Quant. Inf. Comput. **14**, 517 (2014).

[24] T. Yamakami, Quantum NP and a quantum hierarchy. In Proc. of the 2nd IFIP International Conference on Theoretical Computer Science, pp.323-336. Kluwer Academic Publishers (2002).

[25] J. Anders and D. E. Browne, Computational power of correlations. Phys. Rev. Lett. **102**, 050502 (2009).

[26] BPP is the class of decision problems that can be solved with polynomial-time classical probabilistic computing.

[27] MA is a generalization of NP where the verifier is BPP.

[28] BQP is the class of decision problems that can be solved with polynomial-time quantum computing.