Minimum heat dissipation in measurement-based quantum computation

Tomoyuki Morimae*

ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho, Kiryu-shi, Gunma-ken 376-0052, Japan

(Received 3 September 2013; published 28 April 2015)

We show that at least $2kT\ln 2$ of heat dissipation per qubit (in the register of a simulated circuit) occurs in measurement-based quantum computation according to Landauer's principle. This result is derived by using only the fundamental fact that quantum physics respects the no-signaling principle.

DOI: 10.1103/PhysRevA.91.042335 PACS number(s): 03.67.Lx, 03.65.Ta, 05.70.Ln

I. INTRODUCTION

The search for faster, smaller, and more economical computers is the central research subject in today's ever-growing digital society. Heat generation (or, equivalently, energy consumption) during computation is one of the huge obstacles to the above goals, and in fact it has been a long-standing research topic in the interdisciplinary field between information and thermodynamics [1–16]. In 1961, Landauer showed in his seminal paper [1] that an irreversible process, such as an erasure of data in a memory, inevitably causes a minimum amount of heat dissipation. More precisely, the so-called Landauer's principle says that an erasure of a single bit of information in a memory causes at least $k\ln 2$ of entropy generation (hence $kT\ln 2$ of heat dissipation or energy consumption), where k is the Boltzmann constant and T is the temperature of the environment. Landauer's principle has been used not only to exorcise Maxwell's demon in thermodynamics [9], but also to establish fundamental limits of heat generation and energy consumption in irreversible computations.

Although heat dissipation in quantum computers has not yet been fully studied [17], its importance will be arguably more emphasized than that in classical computation given the intrinsic decoherence nature of quantum computers. For the circuit model and the adiabatic model of quantum computation, it is clear that no heat dissipation occurs (in principle), since the energy is conserved (i.e., the unitary process). However, it is not self-evident whether there exist some minimum heat dissipation requirement for measurement-based quantum computation (MBQC) [18], since projective measurements, which are not unitary processes, are necessary in the computation. The purpose of this paper is to study minimum heat dissipation in MBQC. We show that at least $2kT\ln 2$ of heat dissipation per qubit occurs in MBQC according to Landauer's principle (or an inequality due to Sagawa and Ueda [10] and the single-shot version [11]). Interestingly, this result is independent from any specific physical implementation of MBQC, and is in fact derived by using only the fundamental fact that quantum physics respects the no-signaling principle [19]. We will also see that MBQC with the cluster state [18] already achieves this minimum heat dissipation limit, and therefore our result is an achievable lower bound.

*morimae@gunma-u.ac.jp

II. NO-SIGNALING PRINCIPLE

The no-signaling principle is one of the most fundamental principles in physics, and quantum theory also respects it [19]. As is shown in Fig. 1, Alice and Bob share a physical system, which might be classical, quantum, or even superquantum. Alice chooses her measurement parameter x (such as the measurement angle of a spin), and performs a measurement on her part. She obtains the result a. Bob also chooses his measurement parameter y, and performs a measurement on his part. He obtains the result b. The no-signaling principle (from Alice to Bob) is defined by

$$P(b|x,y) = P(b|x',y) \tag{1}$$

for all b, x, x', and y, where $P(\alpha|\beta)$ is the conditional probability distribution of α given β. Equation (1) means that the change in Alice's measurement parameter does not affect the probability distribution of Bob's measurement result. In other words, the shared system cannot transmit any message from Alice to Bob. The no-signaling principle is more fundamental than quantum theory in the sense that there is a theory which is more nonlocal than quantum theory, but respects the no-signaling principle [19].

III. GENERAL MBQC

Measurement-based quantum computation is a new model of quantum computation that was introduced by Raussendorf and Briegel [18]. In this model, universal quantum computation can be done with only the preparation of a highly entangled quantum many-body state, a so-called resource state, and adaptive local measurements on each qubit of the resource state. Here, adaptive means that a measurement basis depends on the previous measurement results. Hence, in addition to the resource state, which is a quantum system, we need a classical computer to process the measurement results (Fig. 2).

The computational power of MBQC is equivalent to the traditional circuit model of quantum computation, but the clear separation between the quantum phase (preparation of the resource state) and the classical phase (local adaptive measurements) has inspired many new results which would not be obtained if we stick to the circuit model. For example, new resource states for MBQC which are closely connected with condensed-matter physics have been proposed [20–30]. Furthermore, relations between MBQC and partition functions of classical spin models were pointed out [31–33]. These discoveries have established a new bridge between quantum information and condensed-matter physics. MBQC has also

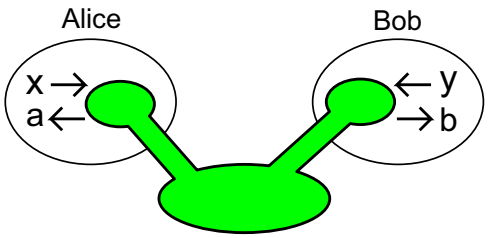

FIG. 1. (Color online) The no-signaling principle.

offered a new framework for fault-tolerant quantum computing which achieves a high threshold [34–39]. The quantum-classical separation in MBQC has enabled us to clarify several relations between the "quantumness" of a resource state and the quantum computational power of MBQC on it [40–45]. New protocols of secure cloud quantum computing, so-called blind quantum computing, were also developed by using MBQC [46–60].

In the most general framework of MBQC, we first prepare the resource state σ of $N = nm$ qubits, as is shown in Fig. 3. Qubits are allocated on sites of the $n \times m$ two-dimensional square lattice, and MBQC simulates a quantum circuit with a register size n and gate depth $m - 1$. (More generally, we can consider a more general graph structure and qudits, but the generalization is straightforward. For simplicity, we here consider a two-dimensional square qubit system.) Be careful that σ is not necessarily the cluster state [18]. We do not assume any specific resource state as σ. Measurements on all qubits in the jth layer of σ implement the n-qubit unitary gate U_j. The initial state of the computation is the n-qubit state $\rho_{\rm in}$, and it is encoded in the first layer of σ. Let C_r be the set of all qubits in the first r layers of σ (Fig. 3). We also define O_r, which is the set of all qubits in the last $m - r$ layers of σ (Fig. 3).

According to the standard theory of quantum measurement [61], a measurement process on C_r is described as follows. First, a correlation between the measurement apparatus and the system σ to be measured is created:

$$\sum_{j=1}^{c} p_r^j |j\rangle\langle j| \otimes \mathcal{E}_r^j(\sigma),$$

where $\mathcal{E}_r^j$ is a completely positive trace-preserving (CPTP) map, and p_r^j is a probability. (Off-diagonal terms are omitted here for simplicity.) Next, the projection measurement $\{|j\rangle\langle j|\}_{j=1}^c$ is performed on the apparatus, which leads to the postmeasurement state $\mathcal{E}_r^j(\sigma)$ with the probability p_r^j.

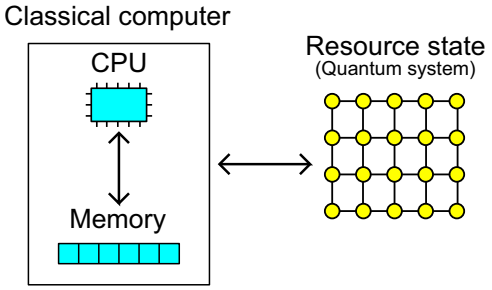

FIG. 2. (Color online) Measurement results on the resource state are processed on a classical computer.

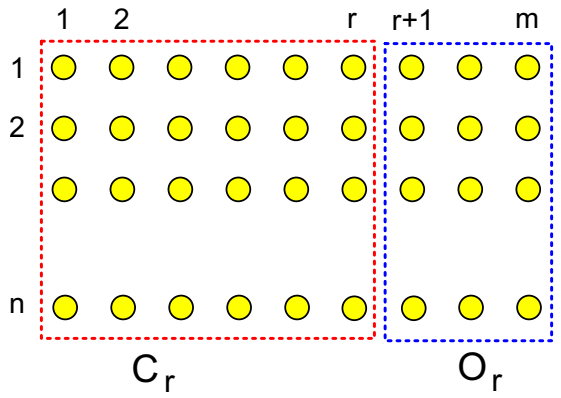

FIG. 3. (Color online) The resource state σ for MBQC.

We require that

$$\rho_{{\rm out},r}^j \equiv {\rm Tr}_{C_r}\left[\mathcal{E}_r^j(\sigma)\right] = B_r^j\left[(U_r \cdots U_1 \rho_{\rm in} U_1^\dagger \cdots U_r^\dagger) \otimes \eta_r^j\right] B_r^{j\dagger}, \quad (2)$$

where ${\rm Tr}_{C_r}$ is the partial trace over C_r, B_r^j is an $(m-r)n$-qubit unitary operator, and η_r^j is a state of $(m-r)n - n$ qubits. The reason why we require the form of $\rho_{{\rm out},r}^j$ in that way can be easily understood if we remember that $\rho_{{\rm out},r}^j$ must contain the complete information about $U_r \cdots U_1 \rho_{\rm in} U_1^\dagger \cdots U_r^\dagger$. (If not, we cannot proceed MBQC with O_r). More precisely, it was shown in Ref. [62] that any invertible CPTP map can be written as an application of a unitary operator on the system plus ancilla. Therefore, the invertible CPTP map,

$$H_n \ni U_r \cdots U_1 \rho_{\rm in} U_1^\dagger \cdots U_r^\dagger \mapsto \rho_{{\rm out},r}^j \in H_{(m-r)n},$$

has to be in the form of Eq. (2), where H_d is the d-qubit Hilbert space. For example, if σ is the cluster state, η_r^j is the $n \times (m - r - 1)$ cluster state, and B_r^j is the operation which applies CZ gates on the border between C_r and O_r, and random Pauli operators on the $(r+1)$th layer.

In particular, after measuring all qubits except for those in the last layer, the state of the last layer becomes

$$\rho_{{\rm out},m-1}^j = B_{m-1}^j U \rho_{\rm in} U B_{m-1}^{j\dagger},$$

with probability p_{m-1}^j, where $U \equiv U_{m-1}U_{m-2}\cdots U_2 U_1$. The operator B_{m-1}^j is an unwanted operator, the so-called by-product operator, but we can correct it if we know j. In such an MBQC, we say that our desired unitary U is implemented on $\rho_{\rm in}$ up to the by-product B_{m-1}^j.

IV. MINIMUM HEAT DISSIPATION IN GENERAL MBQC

Now let us show our main result, that at least $2kT \ln 2$ of heat dissipation per qubit is necessary in the above general MBQC. In order to see it, let us consider MBQC between two parties, Alice and Bob, as is shown in Fig. 4. The resource state σ is shared between Alice and Bob. Alice possesses the subsystem C_r and Bob does O_r. Alice performs MBQC on her part.

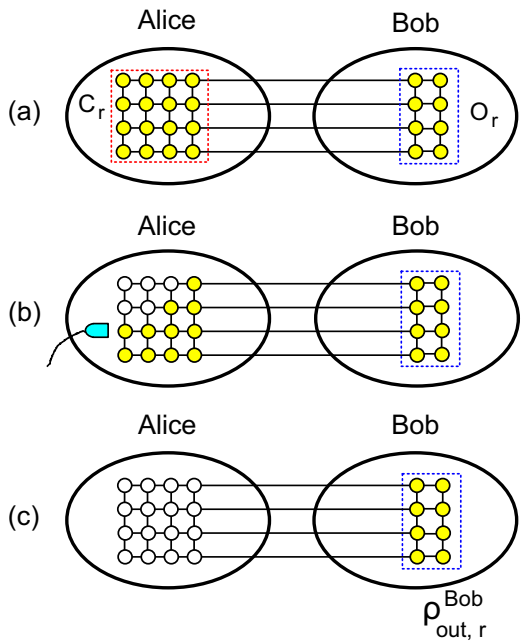

FIG. 4. (Color online) Two-party general MBQC between Alice and Bob.

The state immediately before Alice performing the measurement on her apparatus is

$$\sum_{j=1}^{c} p_r^j |j\rangle\langle j| \otimes \mathcal{E}_r^j(\sigma). \tag{3}$$

If we trace out Alice's system, we obtain Bob's system,

$$\rho_{\mathrm{out},r}^{\mathrm{Bob}} \equiv \sum_{j=1}^{c} p_r^j \rho_{\mathrm{out},r}^j.$$

Now we point out that $\rho_{\mathrm{out},r}^{\mathrm{Bob}}$ must be completely independent from $U_r \cdots U_1 \rho_{\mathrm{in}} U_1^\dagger \cdots U_r^\dagger$, since otherwise Bob can gain some information about $U_r \cdots U_1 \rho_{\mathrm{in}} U_1^\dagger \cdots U_r^\dagger$ by measuring $\rho_{\mathrm{out},r}^{\mathrm{Bob}}$. If Bob gains some information about $U_r \cdots U_1 \rho_{\mathrm{in}} U_1^\dagger \cdots U_r^\dagger$, it contradicts the no-singling principle, because Alice can send some message to Bob by encoding her message into $U_r \cdots U_1 \rho_{\mathrm{in}} U_1^\dagger \cdots U_r^\dagger$. In Refs. [62–64], it was shown that the entropy $H(p_r^1, \ldots, p_r^c)$ of $\{p_r^j\}_{j=1}^c$ must satisfy

$$H\left(p_r^1, \ldots, p_r^c\right) \equiv -\sum_{j=1}^{c} p_r^j \log p_r^j \geqslant 2n \tag{4}$$

if the map

$$H_n \ni \xi \mapsto \sum_{j=1}^{c} p_r^j B_r^j \left(\xi \otimes \eta_r^j\right) B_r^{j\dagger} \in H_{(m-r)n}$$

works as the completely secure quantum one-time pad encryption for any n-qubit state ξ. Here, the completely secure quantum one-time pad encryption means that the state ξ after the map is the completely mixed state from the viewpoint of the person who does not know the key.

Therefore, Alice has to gain at least $2n$ bit (or $2n \ln 2$ nit in the natural base) of information when she measures her apparatus in Eq. (3). The acquisition of information is accompanied by the erasure of it. According to Landauer's principle, this means that at least $2nkT \ln 2$ of heat is dissipated when the data in the memory are erased. Therefore, we conclude that at least $2kT \ln 2$ of heat dissipation per qubit occurs in MBQC.

Landauer's principle is not a mathematical theorem, but an "observation" derived from physically reasonable arguments. In order to obtain a more precise statement, we have to specify the model. For example, if the erasure model is described by the thermalization of the memory interacting with a heat bath, Landauer's principle can be derived [8]. Recently, Sagawa and Ueda [10] introduced an inequality which generalizes Landauer's principle by assuming the following memory model: The state of the memory storing the jth result is given by the canonical state

$$\rho_{j,\mathrm{can}}^M = \exp\left(-H_j^M / kT\right) / Z_j^M,$$

where H_j^M is the Hamiltonian of the memory if it stores the jth result and

$$Z_j^M \equiv \mathrm{Tr}\left[\exp\left(-H_j^M / kT\right)\right].$$

The state of the memory before erasure is given by $\sum_j p_j \rho_{j,\mathrm{can}}^M$. In order to erase data in the memory, we couple the memory with the heat bath,

$$\rho_{\mathrm{can}}^B \equiv \exp[-H^B / kT] / Z^B,$$

where H^B is the Hamiltonian of the bath, and

$$Z^B \equiv \mathrm{Tr}[\exp(-H^B / kT)].$$

The memory plus bath unitary time evolve to the final state ρ^{MB}. Under these assumptions, they derived $W_{\mathrm{eras}} + \Delta F^M \geqslant kT H$, where

$$W_{\mathrm{eras}} \equiv \mathrm{Tr}\left[\rho^{MB}\left(H_0^M + H^B\right)\right] - \sum_j p_j \mathrm{Tr}\left(\rho_{j,\mathrm{can}}^M H_j^M\right) - \mathrm{Tr}\left(\rho_{\mathrm{can}}^B H^B\right)$$

is the work required for the erasure of data in the memory, and

$$\Delta F^M \equiv kT \ln Z_0^M - \sum_j p_j kT \ln Z_j^M$$

is the change of the free energy of the memory due to the erasure. According to Eq. (4), we obtain $W_{\mathrm{eras}} + \Delta F^M \geqslant 2nkT \ln 2$. In particular, if we consider the case when the memory's Hamiltonian does not depend on the stored data, i.e., $H_j^M = H_0^M$ for all j, we conclude that $W_{\mathrm{eras}} \geqslant 2nkT \ln 2$, which means that at least $2kT \ln 2$ of work per qubit is necessary in MBQC.

If we consider the case when the bath is of finite Hilbert space dimension, the improved version of Landauer's principle [14], where the heat generation can be larger than that of the standard Landauer's principle, can also be used.

The operational meaning of the von Neumann entropy assumes the independent and identically distributed (i.i.d.) and the asymptotic limit of the information source [11]. Recently, several results have been obtained to study the single-shot

work extraction in thermodynamics [11–13]. If we consider a single-shot data compression of ρ without those assumptions, the required space to store the information of ρ is quantified by the max entropy $H_{\max}(\rho) \equiv \log[\mathrm{rank}(\rho)]$. In this case the work required for the erasure is given by $W \geqslant kT H_{\max}(\rho)$. Since $H_{\max}(\rho) \geqslant H_{\mathrm{vN}}(\rho)$, where H_{vN} is the von Neumann entropy, we obtain the same result, that $2kT \ln 2$ of work is necessary per qubit in MBQC.

V. DISCUSSION

A. Minimum heat dissipation in the cluster state MBQC

So far, we have given the general arguments. As an example, let us consider the minimum heat dissipation limit in the cluster state MBQC [18]. In the cluster state MBQC, it is well known that measurement results for two previous layers must be kept in order to correct the by-product operators [18]. Therefore, two bits of classical memory per register qubit are always required at any measurement step of the cluster state MBQC. This means that $2kT \ln 2$ of heat dissipation occurs at every step of the cluster state MBQC. In this way, the cluster state MBQC already achieves the minimum heat dissipation limit. Hence we also conclude that our general limit, $2kT \ln 2$, is an achievable limit (i.e., a not too underestimating limit).

For the cluster state MBQC, it is somehow straightforward to derive the $2kT \ln 2$ limit. However, we want to emphasize here that our limit $2kT \ln 2$ for general MBQCs given in the previous section does not make any assumption on the resource state, the measurement method, and the method of classical processing. We have derived a general limit by using only the no-signaling principle. In the future someone might find a very complicated and drastically new MBQC far from the cluster state MBQC. (For example, nonlocal many-body measurements might be allowed.) However, our minimum heat dissipation limit $2kT \ln 2$ still holds for such a new MBQC as long as it satisfies the no-signaling principle.

B. Implication for blind quantum computation

Blind quantum computation is a new secure cloud quantum computing protocol where a client (Alice), who does not have enough quantum technology, can delegate her quantum computation to a server (Bob), who has a full-fledged quantum computer, without leaking any information [46–60]. In blind quantum computing, the no-signaling requirement of the present result is replaced with the security requirement that the server's state must be one-time padded. As pointed out in Ref. [46], the client requires only a classical computer if she interacts with two servers. In this case, we only have to minimize the client's classical technological requirement. Our result suggests that the client cannot be completely free from any technology; she has to possess at least two bits of classical memory per qubit in blind quantum computing.

C. Implication for classical technology requirement in MBQC

The requirement for classical technology in MBQC is a research subject which has not been fully studied. Although classical computation is cheap compared to quantum operations, a detailed understanding of the classical part is important, because, for example, the latency of classical computation could contribute to the entire decoherence time of MBQC. The requirement for the power of the classical CPU was studied in Ref. [65]: A classical XOR gate is sufficient for universal MBQC with cluster states, whereas a classical universal gate set is necessary if we use certain resource states (quantum computational tensor-network states [21]) instead of the cluster state. Our result clarifies the minimum classical memory requirement, namely, two bits per qubit, for MBQC.

D. Heat generation from other degrees of freedom

As was already pointed out by Landauer himself [1], heat generation from Landauer's principle is not a practical limit, but a fundamental one: It is absurd to use Landauer's principle to estimate the overall heat generation in an iPhone, since there are many other factors which contribute to the entire heat generation, and these contributions are many orders of magnitude larger than those from Landauer's principle. This is also the case for our result. For example, the measuring process could cause heat dissipation. If a qubit is encoded in a polarization of a single photon, or a two-level of an atom, a photon detection is necessary for the measurement. Usually, photon detection generates a dissipative electric current, which generates heat that is many magnitudes larger than the Landauer limit. However, these contributions are implementation specific, and therefore beyond the scope of the present paper. (For example, the specific measurement model which uses photons by Brillouin [6] needs some energy for the demon.) The purpose of the present paper is to derive a fundamental limit that is independent from any specific implementation, such as the original motivation of Landauer's paper [1].

E. Maxwell's demon in MBQC

Our result also exorcises Maxwell's demon in MBQC. Since MBQC uses adaptive measurements, it is a kind of a feedback-controlled system with a demon. However, no result was obtained in the study of MBQC from the viewpoint of feedback control. The output of MBQC is a (classical or quantum) element extracted from many possibilities, and therefore MBQC is an entropy decreasing process. However, the entire system (i.e., the resource state of MBQC, the measuring apparatus, the classical computer necessary for the feed-forwarding, and the environment) is a closed system, and therefore the entropy decrease must be compensated by an entropy increase of another degree of freedom so that the second law of thermodynamics is not violated. Such a Maxwell's demon problem in MBQC is solved by our result: An entropy increase necessarily occurs in MBQC (because of the classical memory requirement for the demon, as we have shown in previous sections), and it compensates the entropy decrease caused by the demon's computation.

ACKNOWLEDGMENT

T.M. is supported by Tenure Track System by MEXT Japan and KAKENHI 26730003 by JSPS.

[1] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).
[2] A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, and E. Lutz, Nature (London) **483**, 187 (2012).
[3] L. Szilard, Z. Phys. **53**, 840 (1929).
[4] C. H. Bennett, IBM J. Res. Dev. **17**, 525 (1973).
[5] C. H. Bennett and R. Landauer, Sci. Am. **253**, 48 (1985).
[6] L. Brillouin, J. Appl. Phys. **22**, 334 (1951).
[7] K. Shizume, Phys. Rev. E **52**, 3495 (1995).
[8] K. Maruyama, F. Nori, and V. Vedral, Rev. Mod. Phys. **81**, 1 (2009).
[9] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).
[10] T. Sagawa and M. Ueda, Phys. Rev. Lett. **102**, 250602 (2009).
[11] O. C. O. Dahlsten, R. Renner, E. Rieper, and V. Vedral, New J. Phys. **13**, 053015 (2011).
[12] D. Egloff, O. C. O. Dahlsten, R. Renner, and V. Vedral, arXiv:1207.0434.
[13] P. Faist, F. Dupuis, J. Oppenheim, and R. Renner, arXiv:1211.1037.
[14] D. Reeb and M. M. Wolf, New J. Phys. **16**, 103011 (2014).
[15] M. B. Plenio and V. Vitelli, Contemp. Phys. **42**, 25 (2001).
[16] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **89**, 180402 (2002).
[17] One interesting study about the relation between thermodynamics and MBQC is J. Anders, D. Markham, V. Vedral, and M. Hajdušek, Found. Phys. **38**, 506 (2008).
[18] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[19] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[20] F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).
[21] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
[22] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
[23] J.-M. Cai, W. Dür, M. Van den Nest, A. Miyake, and H. J. Briegel, Phys. Rev. Lett. **103**, 050503 (2009).
[24] A. Miyake, Phys. Rev. Lett. **105**, 040501 (2010).
[25] A. Miyake, Ann. Phys. **326**, 1656 (2011).
[26] T. C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).
[27] J. Cai, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. A **82**, 052309 (2010).
[28] Y. J. Chiu, X. Chen, and I. L. Chuang, Phys. Rev. A **87**, 012305 (2013).
[29] T. Morimae, Phys. Rev. A **83**, 042337 (2011).
[30] T. Morimae, Phys. Rev. A **85**, 062328 (2012).
[31] S. Bravyi and R. Raussendorf, Phys. Rev. A **76**, 022304 (2007).
[32] M. Van den Nest, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **98**, 117207 (2007).
[33] M. Van den Nest, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **100**, 110501 (2008).
[34] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
[35] S. D. Barrett and T. M. Stace, Phys. Rev. Lett. **105**, 200502 (2010).
[36] K. Fujii and Y. Tokunaga, Phys. Rev. Lett. **105**, 250503 (2010).
[37] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).
[38] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Phys. Rev. Lett. **107**, 060501 (2011).
[39] K. Fujii and T. Morimae, Phys. Rev. A **85**, 010304(R) (2012).
[40] K. Fujii and T. Morimae, Phys. Rev. A **85**, 032338 (2012).
[41] D. Gross, S. T. Flammia, and J. Eisert, Phys. Rev. Lett. **102**, 190501 (2009).
[42] M. J. Bremner, C. Mora, and A. Winter, Phys. Rev. Lett. **102**, 190502 (2009).
[43] M. Van den Nest, W. Dür, G. Vidal, and H. J. Briegel, Phys. Rev. A **75**, 012337 (2007).
[44] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).
[45] T. Morimae, Phys. Rev. A **81**, 060307(R) (2010).
[46] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE, New York, 2009), p. 517.
[47] J. Fitzsimons and E. Kashefi, arXiv:1203.5217.
[48] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[49] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[50] T. Morimae, V. Dunjko, and E. Kashefi, Quantum Inf. Comput. **15**, 0200 (2015).
[51] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).
[52] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
[53] T. Morimae, Phys. Rev. A **89**, 060302(R) (2014).
[54] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301(R) (2013).
[55] T. Sueki, T. Koshiba, and T. Morimae, Phys. Rev. A **87**, 060301(R) (2013).
[56] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, arXiv:1301.3662.
[57] T. Morimae and T. Koshiba, arXiv:1306.2113.
[58] T. Morimae and K. Fujii, Phys. Rev. Lett. **111**, 020502 (2013).
[59] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).
[60] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).
[61] J. Von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955).
[62] A. Nayak and P. Sen, Quantum Inf. Comput. **7**, 103 (2007).
[63] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
[64] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proceedings of 41st Annual Symposium on the Foundations of Computer Science* (IEEE, New York, 2000).
[65] J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).