Commuting quantum circuits and complexity of Ising partition functions

2017 New J. Phys. 19 033003

(http://iopscience.iop.org/1367-2630/19/3/033003)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
21 August 2016

REVISED
6 February 2017

ACCEPTED FOR PUBLICATION
10 February 2017

PUBLISHED
1 March 2017

PAPER

Commuting quantum circuits and complexity of Ising partition functions

Keisuke Fujii[1,2,4] **and Tomoyuki Morimae**[3]

[1] The Hakubi Center for Advanced Research, Kyoto University Yoshida-Ushinomiya-cho, Sakyo-ku, Kyoto 606-8302, Japan
[2] Graduate School of Informatics, Kyoto University Yoshida Honmachi, Sakyo-ku, Kyoto 606-8501, Japan
[3] ASRLD Unit, Gunma University 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052 Japan
[4] Author to whom any correspondence should be addressed

E-mail: fujii@qi.t.u-tokyo.ac.jp

Keywords: instantaneous quantum polynomial time computation, commuting quantum circuit, quantum supremacy, classical simulation, partition function, Ising model, quantum algorithm

Abstract

Instantaneous quantum polynomial-time (IQP) computation is a class of quantum computation consisting only of commuting two-qubit gates and is not universal. Nevertheless, it has been shown that if there is a classical algorithm that can simulate IQP efficiently, the polynomial hierarchy collapses to the third level, which is highly implausible. However, the origin of the classical intractability is still less understood. Here we establish a relationship between IQP and computational complexity of calculating the imaginary-valued partition functions of Ising models. We apply the established relationship in two opposite directions. One direction is to find subclasses of IQP that are classically efficiently simulatable by using exact solvability of certain types of Ising models. Another direction is applying quantum computational complexity of IQP to investigate (im)possibility of efficient classical approximations of Ising partition functions with imaginary coupling constants. Specifically, we show that a multiplicative approximation of Ising partition functions is #P-hard for almost all imaginary coupling constants even on planar lattices of a bounded degree.

1. Introduction

Quantum computation has a great possibility to offer substantial advantages in solving some sorts of mathematical problems and also in simulating physical dynamics of quantum systems. A representative instance is Shor's factoring algorithm [1], which solves integer factoring problems in polynomial time, while no polynomial-time classical algorithm has been known. Recently, quantum algorithms for approximating Jones polynomial [2, 3], Tutte polynomial [4], and Ising partition functions [5–7] have been found, and they are shown to be BQP-complete in certain parameter regions. Furthermore, there are some evidences that quantum computation, more precisely, BQP (bounded-error quantum polynomial-time computation [8]), can solve problems outside the polynomial hierarchy (PH) [9, 10, 11]. These results strike the extended Church–Turing thesis [8, 12, 13], which states that every reasonable physical computing devices can be simulated efficiently (with a polynomial overhead) on a probabilistic Turing machine. One of the most revolutionary and challenging goals of human beings is to realize a universal quantum computer and verify such quantum benefits in experiments. However, experimental verification, which is the most essential part in science, is still extremely hard to achieve, requiring a huge number of qubits and extremely high accuracy in controls.

Is there any possible pathway to verify computational complexity benefits of quantum systems that are realizable in the near future, say, one-hundred-qubit (or particle) systems under reasonable accuracy of controls [14]? If there is such a subclass of quantum computation that consists of experimental procedures much simpler than universal quantum computation but is still hard to simulate efficiently in classical computers, experimental verification of complex quantum systems reaches a new phase.

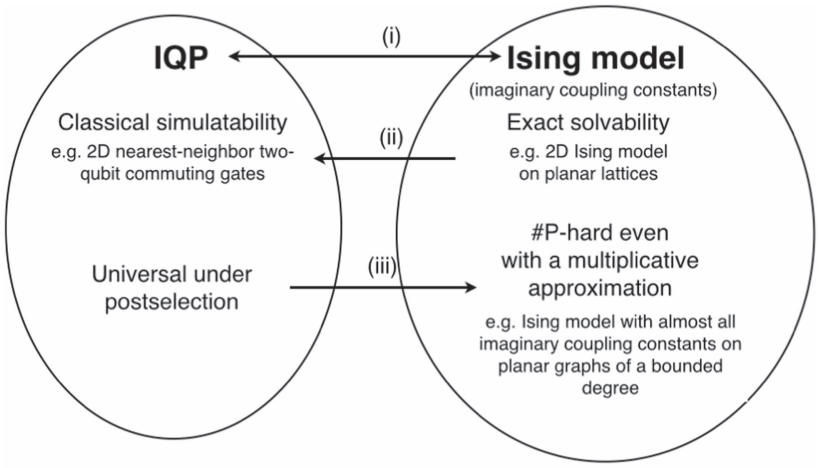

Figure 1. The summary of results obtained in this work.

Aaronson and Arkhipov introduced BOSONSAMPLING [15], a sampling problem according to the probability distribution of n bosons scattered by linear optical unitary operations. The probability distribution is given by the permanent of a complex matrix, which is determined by the linear optical unitary operations. Calculation of the permanent of complex matrices is known to be #P-hard [16, 17]. Since a polynomial-time machine with an oracle for #P can solve all problems in the PH according to Toda's theorem [18], an exact classical simulation (in the strong sense [19, 20] meaning a calculation of the probability distribution of the output) of BOSONSAMPLING is highly intractable in a classical computer. They showed under assumptions of plausible conjectures that if there exists an efficient classical approximation of BOSONSAMPLING (classical simulation in the weak sense [19, 20] meaning a sampling according the probability distribution of the output), the PH collapses to the third level, which is unlikely to occur. (The detailed notions of classical simulation are provided in section 3.) This result brings a novel perspective on linear optical quantum computation and drives many researchers into the recent proof-of-principle experiments [21–28].

Another subclass of quantum computation of this kind is instantaneous quantum polynomial-time computation (IQP) proposed by Shepherd and Bremner [29]. IQP consists only of commuting unitary gates, such as $\exp[i\theta\prod_{k\in S} Z_k]$. Here $\theta \in [0,\ 2\pi)$ is a rotational angle, Z_k indicates the Pauli operator on the kth qubit, and S indicates a set of qubits on which the commuting gate acts. (A detailed definition will be provided in the next section.) The input is given by $|+\rangle^{\otimes n}$ with $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, and the output qubits are measured in the X-basis. Since all unitary operations are commutable with each other, there is no temporal structure in the circuits. (This is the reason why it is called instantaneous quantum polynomial-time computation.) The commutability implies that IQP cannot perform an arbitrary unitary operation for the input qubits and hence seems to be less powerful than standard quantum computation, i.e., BQP. Nevertheless, Bremner, Jozsa, and Shepherd showed that if there exists an efficient classical algorithm that samples the outcomes according to the probability distribution of IQP with a certain multiplicative approximation error, then the PH collapses to the third level. While the collapse of the PH to the third level is not as unlikely as $\mathsf{P} = \mathsf{NP}$, it is also considered to be highly implausible. This result is obtained by introducing postselection and using the fact that post-$\mathsf{BQP} = \mathsf{PP}$ shown by Aaronson [30]. Here postselection means that an additional ability to choose, without any computational cost, arbitrary measurement outcomes of possibly exponentially decreasing probabilities. However, in comparison to BOSONSAMPLING [15, 31], the origin of the classical intractability of IQP is still not well understood.

2. Brief summary of the results

The purpose of this paper is to further explore IQP by relating it with computational complexity of calculating imaginary-valued Ising partition functions, which has been well studied in statistical physics, condensed matter physics, and computer science.

Specifically we obtain the following results (see figure 1):

(i) We reformulate IQP from a viewpoint of computational complexity of calculating Ising partition functions. The probability distribution of the output of IQP including its marginal distributions is mapped into an Ising partition function with imaginary coupling constants (theorems 1 and 2).

(ii) By using the above relation, we specify classically simulatable classes of IQP, which correspond to exactly solvable Ising models (theorems 3 and 4). For example, IQP that consists only of nearest-neighbor two-qubit commuting gates in two-dimensions (2D) is classically simulatable, at least in the weak sense, irrespective of their rotational angles.

(iii) We show that a multiplicative approximation of the Ising partition functions with almost all imaginary coupling constants is #P-hard even on 2D planar lattices with a bounded degree (theorem 5). So there is no polynomial-time approximation scheme unless the PH collapses completely.

The first result bridges IQP and computational complexity of imaginary-valued Ising partition functions. Since an exact calculation of the partition functions takes an exponential time in the worst case, the above connection tells us the origin of hardness of classical simulation of IQP (an exact calculation of Ising partition functions is #P-hard even in the ferromagnetic case [32, 33]). Only restricted models are known to be exactly solvable such as Ising models on the 2D planar lattices without magnetic fields.

One might naively expect that a subclass of IQP, which is mapped into an exactly solvable Ising model, is classically simulatable in the strong sense [19, 20], since the joint probability distribution of the output can be calculated efficiently. However, there are exponentially many instances of the measurement outcome, and hence an efficient calculation of the joint probability distribution of an output does not directly applied to an efficient weak simulation of IQP. For example, in [19], it is pointed out that there exists the case where the joint probability distribution is easily calculated but its marginals are rather hard to calculate. In order to construct an efficient weak simulation of IQP, we need the marginal distributions, which allow a recursive simulation of the sampling problem by using the Bayes theorem. To this end, we map not only the joint probability distribution but also the marginal distributions of IQP into the Ising partition functions on another lattices. In the proof, we virtually utilize measurement-based quantum computation (MBQC) [34] on graph states [35], which are defined associated with the IQP circuits.

The established relationship between IQP and Ising partition functions is useful since computational complexity of Ising models have been well studied. We can apply preexisting knowledge to understand quantum computational complexity of IQP. Specifically, in the second result, we provide classical simulatable classes of IQP by using exact solvability of certain types of Ising models. We provide two examples of classically simulatable classes of IQP. One is based on the sparsity of the commuting gates. Another is a class of IQP that consists only of two-qubit commuting gates acting on nearest-neighbor qubits on the 2D planar graphs, which we call planar-IQP. Planar-IQP is mapped into a two-body Ising model on a 2D planar lattice without magnetic fields, which is known to be solvable by using the Pfaffian method [32, 36, 37]. In the proof, we also utilize properties of graph states in order to renormalize random $i\pi/2$ magnetic fields into two-body interactions, which originated from the random nature of the measurements. Then the marginal distributions can be efficiently calculated irrespective of their rotational angles by using the Pfaffian method [32, 36, 37].

On the other hand, IQP consisting of single- and two-qubit commuting gates acting on a 2D planar graph is sufficient to simulate universal quantum computation under postselection [38]. (Hereafter, such a property that a quantum computational task A can simulate universal quantum computation under postselection is called as *universal-under-postselection*.) This fact and the above classically simulatable class imply that single-qubit rotations play a very important role for IQP to be classically intractable. Actually single-qubit rotations make a drastic change of complexity from almost strongly simulatable to not simulatable even in the weak sense. A similar result is also obtained for Toffoli-Diagonal circuits, where the Hadamard gates at the final round plays very important role [19].

In the final result, we apply the first result in an opposite direction, from quantum complexity to classical one. We consider certain universal-under-postselection instances of IQP to understand classical complexity of calculating the Ising partition functions. Specifically we show that a multiplicative approximation of Ising partition functions (corresponding to a strong simulation of IQP with a multiplicative error) is #P-hard for almost all imaginary coupling constants even on 2D planar lattices with a bounded degree. Hence if there exists a fully polynomial-time classical approximation scheme, it results in a complete collapse of the PH. This can be viewed as a 'quantum proof' of #P-hardness of approximating the imaginary Ising partition functions. Aaronson's post-BQP = PP theorem [30], which is employed to show the above result, is also utilized to provide a 'quantum proof' [39] of #P-hardness of approximating the permanent [17] and the Jones polynomial [40] with a multiplicative error.

The rest of the paper is organized as follows. In section 3, we introduce the definition and useful properties of the graph states in order to fix the notation. Then we review IQP and the postselection argument introduced by Bremner, Jozsa, and Shepherd. We also mention how to utilize post-BQP = PP theorem by Aaronson [30] to obtain classical complexity results. As the final part of the preliminary section, we summarize related works on commuting quantum circuits and quantum and classical computational complexity of calculating the Ising

partition functions. In section 4, we establish a relationship between IQP and Ising partition functions, not only for the joint probability distribution of the output but also for its marginal distributions. In section 5, we demonstrate two classically simulatable classes of IQP. One is based on the sparsity of the IQP circuits. Another is based on exact solvability of the Ising models on the 2D planar lattice without magnetic fields. In section 6, we apply the relationship between IQP and Ising partition functions in an opposite direction to investigate (im) possibility of an efficient classical approximation scheme of the Ising partition functions with imaginary coupling constants. Section 7 is devoted to conclusion and discussion.

3. Preliminary

In this section, we summarize preliminary knowledges to understand our main results. Fundamental properties of the graph states are provided in section 3.1. Complexity theoretical notions are provided in section 3.2. The existing results on IQP are reviewed in section 3.3, where the postselection argument is explained in detail. In section 3.4, we present an interesting application of post-BQP = PP theorem to show hardness of strong simulatability. Related works are summarized in section 3.5.

3.1. Graph states and their properties

In the proofs of the main theorems, we work with a measurement-based version of IQP, namely MBIQP, introduced by Hoban *et al* [41]. The reason is that transformations on the resource state for MBQC [34], so-called graph states [35], are much easier and more intuitive than transformations on the unitary gates themselves. Here we introduce the definition and useful properties of graph states in order to fix the notations.

The Pauli matrix on the ith qubit is denoted by A_i ($A = I, X, Y, Z$). The Hadamard gate is denoted H. The eigenstates of Z with eigenvalues $+1$ and -1 are denoted by $|0\rangle$ and $|1\rangle$, respectively. The eigenstates of X with eigenvalues $+1$ and -1 are denoted by $|+\rangle$ and $|-\rangle$, respectively. We denote the controlled-A gate acting on the ith (control) and jth (target) qubits by $\Lambda_{i,j}(A) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes A$. Specifically, $\Lambda_{i,j}(Z) = \Lambda_{j,i}(Z)$ and $H_j\Lambda_{i,j}(Z)H_j = \Lambda_{i,j}(X)$.

Definition 1 (Graph state). Suppose $G = (V, E)$ is a graph consisting of vertices V and edges E. We define the neighbor $\mathcal{N}_i$ of i as the set of vertices adjacent to vertex i. An operator $K_i = X_i \prod_{j\in\mathcal{N}_i} Z_j$ is defined for each vertex i. The graph state $|G\rangle$ is defined as the simultaneous eigenstate of the operator K_i with eigenvalue $+1$ for all i:

$$K_i|G\rangle = |G\rangle.$$

The above relation reads that the graph state $|G\rangle$ is stabilized by the operator K_i for all i. Such a state is called a stabilizer state. The operator K_i, which stabilizes the stabilizer state, is called a stabilizer operator. A detailed description of the stabilizer formalism could be found in [42, 43].

The graph state $|G\rangle$ is generated from a tensor product state of $|+\rangle$ by performing $\Lambda_{i,j}(Z)$ on the pairs of qubits connected by edges $(i, j) \in E$:

$$|G\rangle = \left(\prod_{(i,j)\in E} \Lambda_{i,j}(Z)\right)|+\rangle^{\otimes|V|}.$$

This can be confirmed as follows. The product state $|+\rangle^{\otimes|V|}$ is the eigenstate of X_i with eigenvalue $+1$ for all $i \in V$, and hence $X_i|+\rangle^{\otimes|V|} = |+\rangle^{\otimes|V|}$. By applying $\prod_{(i,j)\in E}\Lambda_{i,j}(Z)$ for both sides, we obtain

$$\left(\prod_{(i,j)\in E} \Lambda_{i,j}(Z)\right)X_i|+\rangle^{\otimes|V|} = \left(\prod_{(i,j)\in E} \Lambda_{i,j}(Z)\right)|+\rangle^{\otimes|V|}$$

$$\Leftrightarrow K_i\left(\prod_{(i,j)\in E} \Lambda_{i,j}(Z)\right)|+\rangle^{\otimes|V|} = \left(\prod_{(i,j)\in E} \Lambda_{i,j}(Z)\right)|+\rangle^{\otimes|V|},$$

where we used the fact that $\Lambda_{i,j}(Z)X_i = X_iZ_j\Lambda_{i,j}(Z)$. This is the definition of the graph state, and we conclude $|G\rangle = (\prod_{(i,j)\in E}\Lambda_{i,j}(Z))|+\rangle^{\otimes|V|}$.

In the proofs of the main theorems, we repeatedly consider single-qubit projective measurements on the graph state and the resultant post-measurement graph state. In the following we will provide two important facts on the graph states under projective measurements in certain bases.

Fact 1 (**Z-basis measurement**). If the kth qubit of the graph state $|G\rangle$ is measured in the Z-basis, the resultant post-measurement state is the graph state associated with the graph $G' \equiv G\backslash k$, where the byproduct operator $B_k = \prod_{j\in\mathcal{N}_k} Z_j$ is located according to the measurement outcome $m_k \in \{0, 1\}$, i.e., $B_k^{m_k}|G'\rangle$.

See appendix A.1 for the proof. Intuitively, the Z-basis measurement on the kth qubit removes the kth qubit from the graph state, and then the byproduct operator B_k is located according the measurement outcome m_k.

Next we consider a projective measurement on the kth qubit in the $\{|\theta_{k,m_k}\rangle \equiv X^{m_k}(e^{-i\theta_k}|+\rangle + e^{i\theta_k}|-\rangle)/\sqrt{2}\}$ basis, where $m_k \in \{0, 1\}$ is the measurement outcome.

Fact 2 (**Remote Z-rotation**). The projective measurement of the kth qubit on the graph state $|G\rangle$ in the $\{|\theta_{k,m_k}\rangle\}$ basis results in

$$\exp\left[i(\theta_k + m_k\pi/2)\left(\prod_{j\in\mathcal{N}_k} Z_j\right)\right]|G\backslash k\rangle/\sqrt{2}.$$

See appendix A.2 for the proof.

The measurement in the $\{|\theta_{k,m_k}\rangle\}$ basis induces a multi-body Z rotation on the qubits adjacent to the kth qubit. The norms of the post-measurement states are both $1/2$, which indicates that the outcomes $m_k = 0, 1$ appear randomly.

Another class of measurements, which is frequently used in MBQC, is the measurement in a $\{e^{i\theta Z}|\pm\rangle\}$ basis. It is known that adaptive measurements in these bases on a certain graph state is enough to perform universal quantum computation, i.e., BQP [34]. Here the adaptive measurement means to change the following measurement angles according to the previous measurement outcomes in order to handle the random nature of the measurements. This process is often called a feedforward. A wide variety of graph states have been known to be universal resources for MBQC [35].

3.2. Definitions of complexity theoretical notions

Here we provide definitions of complexity theoretical notions, which are relevant to our main arguments.

When we consider classical simulation of quantum tasks, there are two important notions of simulatability.

Definition 2 (**Strong and weak simulations** [19, 20]). Suppose $\mathcal{C}$ is a uniformly generated quantum circuit of a model of quantum computation A (e.g., IQP, one-clean-qubit model [44], and universal quantum computation, etc). The probability distribution of the output x (classical bits) is denoted by $P_A(x|\mathcal{C})$. An efficient weak simulation of A is a classical polynomial-time randomized computation that samples x with the probability $P_A(x|\mathcal{C})$.

On the other hand, an efficient strong simulation of a quantum circuit $\mathcal{C}$ for a given output x is a classical polynomial-time (randomized) computation that calculates the probability $P_A(x|\mathcal{C})$ including its marginal distributions $\sum_{x'} P_A(x|\mathcal{C})$ with respect to an arbitrary subset x' of the output bits x.

In addition to these notions of classical simulation, we can further consider types of approximations. In an approximated simulation with a multiplicative error $1 < c$, we can replace the probability distribution $P_A(x|\mathcal{C})$ with its approximation $P_A^{\rm ap}(x|\mathcal{C})$ that lies inside the following approximation range

$$\frac{1}{c}P_A(x|\mathcal{C}) \leqslant P_A^{\rm ap}(x|\mathcal{C}) \leqslant cP_A(x|\mathcal{C}).$$

Apparently, if we can simulate A in the strong sense, we can sample the output in the weak sense. Thus a strong simulation trivially includes a weak one. In fact, it has been known that a strong simulation is much harder than a weak simulation, i.e., what a model of quantum computation A can actually do. For example, an exact strong simulation of the output of universal quantum computation is #P-hard [19]. We should also note that, in strong simulation, calculation of the marginal distributions is crucial, since there is the case where a strong simulation of the output probability (joint probability) is easy but its marginal distributions are hard to calculate [19].

In the proof of the main theorems, we frequently use the postselection argument; two complexity classes are compared by assuming a fictitious ability to postselect a desired output, whose probability can be exponentially small. To this end, the postselected class, post-A, is defined as a class of decision problems solvable by using a computational model associated with A (e.g. instantaneous polynomial-time quantum computation for IQP, universal quantum computation for BQP, and and polynomial-time classical randomized computation for BPP) with a bounded error under postselection [30].

Definition 3 (Postselected class). A language L is in the class post-A iff there exists a uniform family $\{C_w\}$ of circuits of a computational model associated with A, where a single line output register $\mathcal{O}_w$ (for the L-membership decision problem) and a (generally O(poly(n))-line) postselection register $\mathcal{P}_w$ are specified such that

(i) if $w \in L$ then $\mathrm{Prob}(\mathcal{O}_w = 1 | \mathcal{P}_w = 00 \ldots 0) \geqslant 1/2 + \delta$,

(ii) if $w \notin L$ then $\mathrm{Prob}(\mathcal{O}_w = 1 | \mathcal{P}_w = 00 \ldots 0) \leqslant 1/2 - \delta$,

with a constant $0 < \delta < 1/2$.

In [30], post-BQP is shown to be equal to PP, a class of probabilistic computation whose success probability is greater than $1/2$ (possibly unbounded).

In the postselection argument, we compare two postselected complexity classes via the PH. The PH is a natural way of classifying the complexity of problems (languages) beyond NP (nondeterministic polynomial-time computation) using oracles. A computation A with an oracle for B is denoted by A^{B}. Further, the nondeterministic version of A is denoted by 'N'A. The level-k class Δ_k of the hierarchy is defined recursively by $\Delta_{k+1} = \mathsf{P}^{\mathsf{N}\Delta_k}$. Then the PH is defined as the union $\mathsf{PH} \equiv \cup_k \Delta_k$ of them. NP = P implies a collapse of the HP to the first level, that is, the PH collapses completely. It is known that $\mathsf{P}^{\text{post-BPP}}$ is included in Δ_3 [45], and $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$ [18].

3.3. Instantaneous quantum polynomial-time computation

Here we introduce IQP and its measurement-based version. We first define IQP:

Definition 4 (IQP by Bremner *et al* [29, 38]). Let n be the number of qubits. A commuting gate is defined by

$$D(\theta_j, S_j) \equiv \exp\left[\mathrm{i}\theta_j \prod_{k \in S_j} Z_k \right],$$

where $\theta_j \in [0, 2\pi)$ is a real number meaning the rotational angle, and $\{S_j\}$ is a set of subsets of $\{1, 2, \ldots n\}$, on which the commuting gates act. We refer to a poly(n) number of commuting gates, including the input state $|+\rangle^{\otimes n}$ and the X-basis measurements, as an IQP circuit. IQP is defined as a sampling problem from the IQP circuit, whose probability distribution is given by

$$P_{\mathrm{IQP}}(\{s_i\} | \{\theta_j\}, \{S_j\}) \equiv \left| \bigotimes_{i=1}^{n} \langle +_{s_i} | \prod_j D(\theta_j, S_j) | + \rangle^{\otimes n} \right|^2,$$

where $s_i \in \{0, 1\}$ is the measurement outcome and $|+_{s_i}\rangle = Z^{s_i}| + \rangle$.

For each commuting circuit, we can naturally define a bipartite graph $G = (V_A \cup U_B, E)$, where V_A and U_B are disjoint sets of vertices, and every edge $\in E$ connects a vertex in V_A with another in U_B. Each vertex $v_i \in V_A$ is associated with the ith input qubit of the IQP circuit, and hence $|V_A| = n$. Each vertex $u_j \in U_B$ is associated with the jth commuting gate $D(\theta_j, S_j)$, and hence $|U_B| = \mathrm{poly}(n)$. The set of edge E is defined as $E := \{(u_j, v_i) | u_j \in U_B, i \in S_j\}$, that is, the set S_j specifies the vertices v_i that are connected with the vertex u_j. For a given weighted bipartite graph $G = (V_A \cup U_B, E, \{\theta_j\})$, where a weight θ_j is defined on each vertex $u_j \in U_B$, we can define an IQP circuit.

By using definition 1 and fact 2, IQP can be rewritten as MBQC on a graph state $|G\rangle$ associated with the graph $G = (V_A \cup U_B, E)$. In this case, the set $\mathcal{N}_{u_j}$ of vertices corresponds to S_j. More precisely, for a given bipartite graph state $G = (V_A \cup U_B, E)$ and weights $\{\theta_j\}$, measurement-based IQP (MBIQP) is defined as follows:

Definition 5 (MBIQP by Hoban *et al* [41]). MBIQP is defined as a sampling problem according to the probability distribution

$$P_{\mathrm{MBIQP}}(\{m_{v_i}\}, \{m_{u_j}\} | \{\theta_j\}, G) \equiv \left| \bigotimes_{v_i \in V_A} \langle +_{m_{v_i}} | \bigotimes_{u_j \in U_B} \langle \theta_{j, m_{u_j}} | | G \rangle \right|^2,$$

where $m_{v_i} \in \{0, 1\}$, $m_{u_j} \in \{0, 1\}$ and $|\theta_{j,m_{u_j}}\rangle \equiv X^{m_{u_j}}(\mathrm{e}^{-\mathrm{i}\theta_j}| +_0 \rangle + \mathrm{e}^{\mathrm{i}\theta_j}|+_1\rangle)/\sqrt{2}$.

The bit strings $\{m_{v_i}\}$ and $\{m_{u_j}\}$ correspond to the measurement outcomes on the qubits belonging to V_A and U_B, respectively. We should note that there is no temporal order in the measurements since there is no feedforward of the measurement angles in MBIQP.

Then we can prove MBIQP $=$ IQP.

Lemma 1 (MBIQP $=$ IQP by Hoban *et al* [41]). *MBIQP and IQP are equivalent in the sense that if one sampler exists, another sampler can be simulated.*

Proof. Since a stabilizer operator of the graph state is given by $K_{u_j} = X_{u_j} \prod_{v_i \in \mathcal{N}_{u_j}} Z_{v_i}$, $K_{u_j}|G\rangle = |G\rangle$ for each vertex $u_j \in U_B$. By using this equality, we obtain

$$\begin{aligned} P_{\mathrm{MBIQP}}(\{m_{v_i}\}, \{m_{u_j}\}|\{\theta_j\}, G) &= \left| \bigotimes_{v_i \in V_A} \langle +_{m_{v_i}}| \bigotimes_{u_j \in U_B} \langle \theta_{j,m_{u_j}}| \left(\prod_{u_j \in U_B} K_{u_j}^{m_{u_j}} \right) |G\rangle \right|^2 \\ &= \left| \bigotimes_{v_i \in V_A} \langle +_{m_{v_i}}| \bigotimes_{u_j \in U_B} \langle \theta_{j,0}| \left[\prod_{u_j \in U_B} \left(\prod_{v_i \in \mathcal{N}_{u_j}} Z_{v_i} \right)^{m_{u_j}} \right] |G\rangle \right|^2 \\ &= 2^{-|U_B|} P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\}, \{S_j\}), \end{aligned} \tag{1}$$

where m_{v_i} and s_i are related via

$$s_i \equiv m_{v_i} \oplus \left(\bigoplus_{u_j \in \mathcal{N}_{v_i}} m_{u_j} \right).$$

In the above, we used the facts that each measurement outcome $\{m_{u_j}\}$ is randomly distributed with probability $1/2$, and the projection $\langle \theta_{j,0}|$ results in the commuting gate $D(\theta_j, S_j)$ (see fact 2). The above equality means that, regardless of the measurement outcomes $\{m_{v_i}\}$ and $\{m_{u_j}\}$, we can simulate IQP by using MBIQP.

On the other hand, by using a random bit string $\{m_{u_j}\}$ with an equal probability $1/2$ for each bit and $\{s_i\}$ sampled from the IQP circuit, we obtain $\{m_{v_i} \equiv s_i \oplus_{u_j \in \mathcal{N}_{v_i}} m_{u_j}\}$ and $\{m_{u_j}\}$, which is equivalent to the output of MBIQP. □

As mentioned previously, there is no feedforward for the measurement angles in MBIQP, and hence the measurements can be done simultaneously. This means that MBIQP cannot perform universal quantum computation in MBIQP unless constant depth circuits can simulate universal quantum computation. However, if postselection is allowed, we can choose the measurement outcomes in such a way that no byproduct operator is applied. Thus, with an appropriately chosen graph structure and weights, we can simulate universal quantum computation with the commuting circuits under postselection.

This means that MBIQP with an appropriate graph state and weights (measurement angles) is universal-under-postselection, and hence post-MBIQP $=$ post-BQP. On the other hand, Aaronson showed that post-BQP $=$ PP [30]. Accordingly, post-IQP $=$ post-MBIQP $=$ PP.

In order to simulate post-BQP, it is sufficient to consider post-IQP or post-MBIQP associated with planar bipartite graphs $G = (V_A \cup U_B, E)$ with $|S_j| \leqslant 2$ and $\theta_j = \pi/8$ for all j [38]. (As shown in section 6, we can obtain the same result not only for $\theta_j = \pi/8$ but also for almost all angles θ_j.) In this case, each instance is encoded into a structure of a graph. In another encoding, we can fix the structure of the graph but choose each angle θ_j from $\{\pi/4, \pi/8, 0\}$. Specifically, $\theta_j = 0$ corresponds to a deletion of vertex u_j from the graph (see fact 1). $\theta_j = \pi/4$ and $\pi/8$ correspond to Clifford and non-Clifford gates, respectively. Examples of graphs and weights of MBIQP that are universal-under-postselection are presented in figures 2(a) and (b).

In [38], Bremner, Jozsa, and Shepherd showed that if IQP is weakly simulatable by using a classical randomized algorithm with a multiplicative approximation error $1 < c < \sqrt{2}$:

$$\frac{1}{c} P_{\mathrm{IQP}} \leqslant P_{\mathrm{IQP}}^{\mathrm{ap}} \leqslant c P_{\mathrm{IQP}},$$

then the PH collapses to the third level. The collapse of the PH to the third level is not as unlikely as NP $=$ P but still thought to be highly implausible.

Lemma 2 (Hardness of IQP by Bremner *et al* [38]). *If IQP is weakly simulatable by a classical polynomial time randomized algorithm within multiplicative error $1 \leqslant c \leqslant \sqrt{2}$, PP $=$ post-BPP, resulting in a collapse of the PH to the third level.*

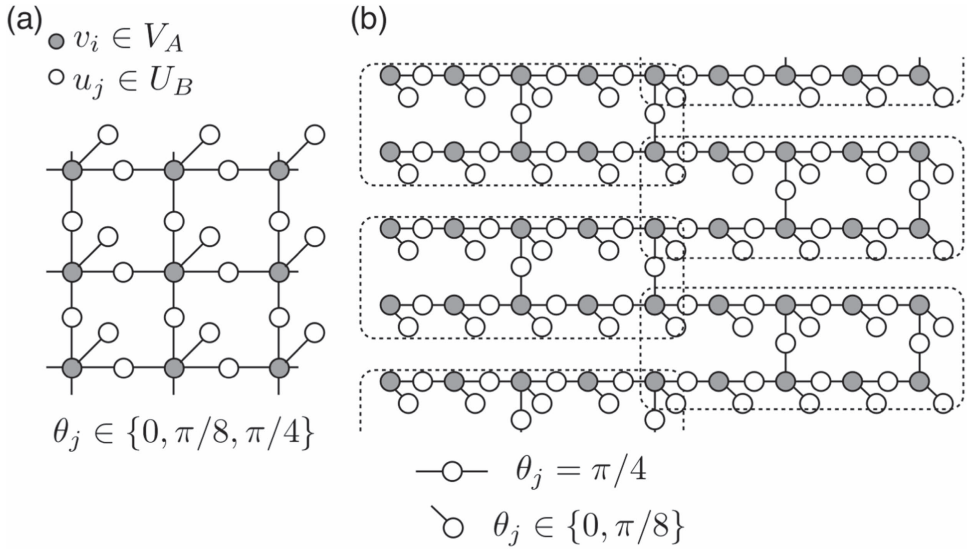

Figure 2. (a) An example of a planar bipartite graph and weights for universal IQP, where $\theta_j \in \{0, \pi/8, \pi/4\}$. (b) Another example of a planar bipartite graph and weights, where $\theta_j = \pi/4$ for all j with $|S_j| = 2$ (corresponding to two-qubit commuting gates) and $\theta_j \in \{0, \pi/8\}$ for all j with $|S_j| = 1$ (corresponding to single-qubit rotations). The associated graph state is a decollated version of the brickwork state utilized in blind quantum computation [46, 47]. Each dotted square indicates a unit cell of the brickwork state. The brickwork state allows us to perform universal quantum computation with measurements only in $\{|\pm\rangle\}$ and $\{e^{i(\pi/8)Z}|\pm\rangle\}$ bases. A similar brickwork state is employed for hardness proof of an IQP with random measurements on a translation invariant lattice [89].

Proof. (See also [38].) Let L be a language decided by post-IQP with a bounded error $0 < \delta < 1/2$, that is,

$$\text{if } w \in L,\ P_{\rm IQP}(\mathcal{O}_w = 1|\mathcal{P}_w = 00\ldots0) \geqslant 1/2 + \delta, \tag{2}$$

$$\text{if } w \notin L,\ P_{\rm IQP}(\mathcal{O}_w = 1|\mathcal{P}_w = 00\ldots0) \leqslant 1/2 - \delta, \tag{3}$$

with a constant $0 < \delta < 1/2$. Suppose we have a classical polynomial-time randomized algorithm that weakly simulates IQP, i.e., a sampling according to the probability distribution $P_{\rm IQP}(\mathcal{O}_w = x, \mathcal{P}_w = y)$ with a multiplicative error $1 < c < \sqrt{2}$. Under postselection, we can simulate post-IQP, a sampling according to the probability distribution

$$P^{\rm ap}_{\rm IQP}(\mathcal{Q}_w = x|\mathcal{P}_w = 00..0) = \frac{P^{\rm ap}_{\rm IQP}(\mathcal{O}_w = x, \mathcal{P}_w = 00\ldots0)}{P^{\rm ap}_{\rm IQP}(\mathcal{P}_w = 00\ldots0)}.$$

The multiplicative error for the conditional probability $P^{\rm ap}_{\rm IQP}(\mathcal{Q}_w = x|\mathcal{P}_w = 00..0)$ is bounded by c^2:

$$\frac{1}{c^2}P_{\rm IQP}(\mathcal{Q}_w = x|\mathcal{P}_w = 00..0) \leqslant P^{\rm ap}_{\rm IQP}(\mathcal{Q}_w = x|\mathcal{P}_w = 00..0) \leqslant c^2 P_{\rm IQP}(\mathcal{Q}_w = x|\mathcal{P}_w = 00..0).$$

Using this and equations (2) and (3), we obtain

$$\text{if } w \in L,\ P^{\rm ap}_{\rm IQP}(\mathcal{Q}_w = 1|\mathcal{P}_w = 00..0) \geqslant \frac{1}{c^2}(1/2 + \delta),$$

$$\text{if } w \notin L,\ P^{\rm ap}_{\rm IQP}(\mathcal{Q}_w = 1|\mathcal{P}_w = 00..0) \leqslant c^2(1/2 - \delta).$$

Thus if both $c^{-2}(1/2 + \delta) > 1/2$ and $c^2(1/2 - \delta) < 1/2$ are satisfied, we can construct a classical randomized algorithm that decides L with bounded error. In other words, post-IQP $\subseteq$ post-BPP. Since post-IQP does not depend on the level of error δ, we can choose any value $0 < \delta < 1/2$. By using the fact that IQP is universal-under-postselection, we conclude that if $c < \sqrt{2}$, PP = post-BQP = post-IQP $\subseteq$ post-BPP. Apparently, post-BQP includes post-BPP, and hence PP = post-BPP.

Due to Toda's theorem [18], P with an oracle for PP includes whole classes in the PH, i.e., PH $\subseteq$ P^{PP}. On the other hand, P with an oracle for post-BPP is in the third level of the PH, i.e, $\mathsf{P}^{\text{post-BPP}} \subseteq \Delta_3$. Thus PP = post-BPP implies a collapse of the PH to the third level, which is highly implausible. In other words, unless the PH collapses to the third level, there exists no efficient weak classical simulation of IQP. □

3.4. Strong simulation and post-BQP = PP theorem

Aaronson's theorem, post-BQP = PP [30], is quite useful to obtain not only quantum complexity results combined with the postselection argument by Bremner *et al* [38], but also to provide 'quantum proofs' of classical complexity results [39]. For example, in [30], Aaronson provided alternative and much simpler proof

that PP is closed under intersection [48]. Moreover, by using post-BQP = PP, we can show that strong simulation of some computational tasks, which are as hard as post-BQP under postselection, is #P-hard even in an approximated case with a multiplicative error:

Lemma 3 (Strong simulation and post-BQP = PP). *Suppose a (classical or quantum) computation A is universal-under-postselection and has enough postselection ports, so that post-A = post-BQP. If the output of A is efficiently strongly simulatable with a multiplicative error* $1 < c < \sqrt{2}$ *(or if there is a fully polynomial-time classical approximation scheme for the output distribution of A), the PH collapses completely.*

Proof. Suppose the probability distribution $P_A(\mathcal{O}_w = x, \mathcal{P}_w = y)$ of the output of A can be strongly simulated with a multiplicative error $1 < c < \sqrt{2}$:

$$\frac{1}{c}P_A(\mathcal{O}_w = x, \mathcal{P}_w = 00\ldots0) \leqslant P_A^{\mathrm{ap}}(\mathcal{O}_w = x, \mathcal{P}_w = 00\ldots0) \leqslant cP_A(\mathcal{O}_w = x, \mathcal{P}_w = 00\ldots0).$$

By using this, we can calculate the postselected probability distribution

$$P_A^{\mathrm{ap}}(\mathcal{O}_w = x|\mathcal{P}_w = 00\ldots0) = \frac{P_A^{\mathrm{ap}}(\mathcal{O}_w = x, \mathcal{P}_w = 00\ldots0)}{\sum_{x'=0,1}P_A^{\mathrm{ap}}(\mathcal{O}_w = x', \mathcal{P}_w = 00\ldots0)}$$

with a multiplicative error $1 < c^2 < 2$. Since post-A = post-BQP = PP, if we can calculate $P_A^{\mathrm{ap}}(\mathcal{O}_w = x|\mathcal{P}_w = 00\ldots0)$ efficiently with a multiplicative error $c^2 < 2$, it is sufficient to decide a complete problem in PP. Since $\mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}}$, the multiplicative approximation is enough to find a solution of $\#P$-complete problem and hence #P-hard. Therefore, the existence of such an efficient strong simulation with the multiplicative error $1 < c < \sqrt{2}$ results in an entire collapse of the PH. □

The above lemma indicates that if a function $f(x)$ of interest is given as a probability distribution of some quantum task that is universal-under-postselection, then computation of $f(x)$ is #P-hard even in the approximated case with a multiplicative error. This argument has been utilized by Kuperberg to show #P-hardness of approximating the Jones polynomial with a multiplicative error [40]. In [17], Aaronson provided an alternative proof of #P-hardness of calculating the permanent [16] based on the above argument and the KLM scheme [49]. We will also utilize it to provide the #P-hardness of a multiplicative approximation of Ising partition functions with an imaginary parameter region, in section 6. Moreover, lemma 3 also implies that there is a good chance for a quantum computer in an approximation a function $f(x)$ with an additive error under an appropriate normalization through the Hadamard test [2–4].

3.5. Related works

As a final part of the preliminary section, we review related works on computational complexity of commuting quantum circuits and Ising partition functions.

In [50], they have investigated rather general commuting quantum circuits of d-level (qudit) systems. Not only the diagonal gates in the computational basis, but also general commuting gates are considered. Specifically they showed that a single qudit output (or at most polylogarithmic number of qudits) of 2-local commuting quantum circuits is strongly simulatable with an exponential accuracy. Moreover, a single qudit output of 3-local commuting quantum circuits cannot be strongly simulated, unless every problem in #P has a polynomial-time classical algorithm. The former result and intractability of IQP with two-local commuting gates imply that a polynomial size of the output is essential for commuting quantum circuits to be hard for a weak classical simulation. Recently, hardness of IQP is improved from sampling with a constant multiplicative error to that with a constant l_1 additive error, where the relation between IQP and Ising partition functions are utilized [51].

In [52], it has been shown that an approximated random state, t-design, can be generated by diagonal (i.e., commuting) quantum circuits [53, 54] (see also a review [52]). Since random states are shown to be useful in various quantum information tasks [55–57], they are one of the most important applications of commuting quantum circuits.

For the ferromagnetic Ising models with a constant magnetic field on arbitrary graphs, there exists a fully polynomial-time randomized approximation scheme (FPRAS) [58], which approximates the partition function Z_{Ising} of the size n with a multiplicative error $c = 1 + \epsilon$ in a poly$(n, 1/\epsilon)$ time. However, under the random magnetic fields, approximation of ferromagnetic Ising partition functions below a certain critical temperature equivalent, under an approximation-preserving reduction, to #BIS, which is a counting problem of the number of independent sets of a bipartite graph [59]. The counting problem #BIS is conjectured to lie in-between FPRAS and #SAT under an approximation-preserving reduction. Here #SAT indicates a counting problem of the number of satisfying configurations, and does not have an efficient (polynomial) multiplicative

approximation unless NP = RP [60]. Moreover, it has been shown that a multiplicative approximation of antiferromagnetic Ising partition functions (below a certain threshold temperature) on d-regular graphs ($d \geqslant 3$) are NP-hard [61]. All these earlier works have done on the Ising models with real coupling strengths and fields. A comprehensive classification of complexity of multiplicative approximation of complex-valued Ising partition functions (including our results) has been provided in [62].

In [63], a quantum algorithm to prepare quantum states encoding the thermal states of Ising models has been proposed for a restricted type of lattice structures. In [64], it has been shown that calculations of partition functions of $\pm J$ random-bond Ising models are equivalent to quadratically signed weight enumerators, with an oracle for which classical probabilistic computation is polynomially equivalent to quantum computation [65]. Based on this mapping, certain quantum circuits corresponding to Ising models on planar lattices without magnetic fields have been shown to be efficiently simulatable by a classical computer in the strong sense [66].

Quantum algorithms to approximate the Ising partition functions in a complex parameter region have been studied so far using a transfer matrix method [5, 67], an overlap mapping [7, 68–70], and a path integral method [6]. Specifically, certain sets of instances are shown to be BQP-complete, which means that such algorithms can actually do a nontrivial task, which would be intractable on a classical computer. In [6], a quantum algorithm for an additive approximation of real Ising partition functions on square lattices has been proposed by using an analytic continuation (see also a Fourier sampling scheme for spin models for estimating free energy [71]). In [7], another quantum algorithm for an additive approximation of square-lattice Ising partition functions with completely general parameters including real physical ones has been constructed based on a linear operator simulation by a unitary circuit with ancilla qubits (see also a linear operator simulation for an additive approximation of Tutte polynomials [4]). Specifically, in this case, the achievable approximation scale was also calculated explicitly. The Ising partition functions on square lattices with magnetic fields are know to be universal in the sense that the partition function of any other classical spin model can be mapped into an Ising partition function by choosing a certain parameter [69]. Furthermore, the 2D Ising models are know to be universal, which means that we can embed an arbitrary classical spin models to its low energy sector [72]. Thus the above quantum algorithm allows approximation of an arbitrary classical spin partition function with a certain approximation scale.

4. Bridging IQP and Ising partition functions

In this section, we establish a bridge between IQP and Ising partition functions. In section 4.1, we will first show that the joint probability distribution of the output of an IQP circuit associated with a graph G is given by normalized squared norm of the partition function of the Ising model defined by the graph G. Since there are exponentially many instances of the measurement outcomes, a straightforward sampling using the joint probability distributions does not work efficiently. To resolve this, we simulate IQP in a recursive way according to the conditional distribution on the previous measurement outcomes by using the Bayes theorem. To this end, we need the marginal distributions with respect to the measured qubits. In section 4.2 we will establish a relationship between the marginal distribution with respect to a set M of the measured qubits and the Ising partition function defined on another graph $\tilde{G}_M$, which is systematically constructed from the graph G and the set M.

4.1. Joint probability distribution

We define an Ising model, which may include multibody interactions, according to the bipartite graph $G = (V_A \cup U_B, E)$ and weights $\{\theta_j\}$. The Ising model consists of the sites associated with the vertices $v_i \in V_A$ and multibody interactions represented by the vertices $u_j \in U_B$. The spins engaged in the jth interaction and its coupling constant are given by $\mathcal{N}_{u_j}$ (or equivalently S_j) and θ_j, respectively.

Definition 6 (Multibody Ising model with random $i\pi/2$ magnetic fields). For a given bipartite graph $G = (V_A \cup U_B, E)$ and weights $\{\theta_j\}$ defined on the vertices in U_B, a Hamiltonian of an Ising model with random $i\pi/2$ magnetic fields is defined by

$$H(\{s_i\}, \{\theta_j\}, G) \equiv -\sum_{v_i \in V_A} i\pi s_i \frac{1-\sigma_{v_i}}{2} - \sum_{u_j \in U_B} i\theta_j \left(\prod_{v_i \in \mathcal{N}_{u_j}} \sigma_{v_i} \right), \tag{4}$$

where $\sigma_{v_i} \in \{+1, -1\}$ is an Ising variable defined on each vertex $v_i \in V_A$. The partition function of the Ising model is defined by

$$\mathcal{Z}(\{s_{v_i}\},\{\theta_j\},G)=\sum_{\{\sigma_{v_i}\}}\mathrm{e}^{-H(\{s_i\},\{\theta_j\},G)},$$

where $\sum_{\{\sigma_{v_i}\}}$ means the summation over all configuration $\{\sigma_{v_i}\}$.

We should note that, in addition to the interactions defined by the graph and weights, random $\mathrm{i}\pi/2$ magnetic fields are also introduced according to the bit string $\{s_{v_i}\}$. This corresponds to the measurement outcome of IQP as seen below. Furthermore, in section 5, these random $\mathrm{i}\pi/2$ magnetic fields will be successfully removed for a certain class of Ising models by renormalizing them into the coupling constants $\{\theta_j\}$.

The probability distribution of IQP associated with $G=(V_A\cup U_B,E)$ and weights $\{\theta_j\}$ is now shown to be equivalent to the normalized squared norm of the partition function of Ising model defined by the graph G and weights $\{\theta_j\}$ as follows:

Theorem 1 (IQP **and Ising partition functions**). *IQP associated with the graph $G=(V_A\cup U_B,E)$ and weights $\{\theta_j\}$ is equivalent to the sampling problem according to the normalized squared norm of an Ising partition function defined by the graph G and weights $\{\theta_j\}$:*

$$\begin{aligned}P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\},\{S_j\})&=2^{|U_B|}P_{\mathrm{MBIQP}}(\{m_{v_i}\},\{m_{u_j}\}|\{\theta_j\},G)\\&=2^{-2|V_A|}\,|\mathcal{Z}(\{s_i\},\{\theta_j\},G)|^2.\end{aligned}$$

Proof. We reformulate the left-hand side of equation (1) using the overlap mapping developed by Van den Nest *et al* [69, 70]:

$$\begin{aligned}&P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\},\{S_j\})\\&=2^{|U_B|}P_{\mathrm{MBIQP}}(\{m_{v_i}\},\{m_{u_j}\}|\{\theta_j\},G)\\&=2^{|U_B|}\left|\left(\bigotimes_{v_i\in V_A}\langle+_{s_i}|\right)\left(\bigotimes_{u_j\in U_B}\langle\theta_{j,0}|H\right)\prod_{u_j\in U_B}H_{u_j}|G\rangle\right|^2\\&=2^{|U_B|}\left|\left(\bigotimes_{v_i\in V_A}\frac{\langle0|+\mathrm{e}^{\mathrm{i}s_i\pi}\langle1|}{\sqrt{2}}\right)\left(\bigotimes_{u_j\in U_B}\frac{\langle0|\mathrm{e}^{\mathrm{i}\theta_j}+\langle1|\mathrm{e}^{-\mathrm{i}\theta_j}}{\sqrt{2}}\right)\left(2^{-|V_A|/2}\sum_{\{\bar\sigma_{v_i}\}}|\{\bar\sigma_{v_i}\}\rangle\bigotimes_{u_j\in U_B}\left|\bigoplus_{v_i\in N_{u_j}}\bar\sigma_{v_i}\right\rangle\right)\right|^2\\&=2^{|U_B|}\left|2^{-|U_B|/2-|V_A|}\sum_{\{\bar\sigma_{v_i}\}}\exp\left[\sum_{v_i\in V_A}\mathrm{i}\pi s_i\bar\sigma_{v_i}\right]\exp\left[\sum_{u_j\in U_B}-\mathrm{i}\left[2\theta_j\left(\bigoplus_{v_i\in N_{u_j}}\bar\sigma_{v_i}\right)-\theta_j\right]\right]\right|^2\\&=2^{-2|V_A|}\left|\sum_{\{\sigma_i\}}\mathrm{e}^{-H(\{s_i\},\{\theta_j\},G)}\right|^2\\&=2^{-2|V_A|}\,|\mathcal{Z}(\{s_i\},\{\theta_j\},G)|^2,\end{aligned}\tag{5}$$

where we define a binary variable $\bar\sigma_{v_i}\equiv(1-\sigma_{v_i})/2$, and $\sum_{\bar\sigma_{v_i}}$ indicates a summation over all binary strings. From the second to the third lines, we used the fact that

$$\begin{aligned}|G\rangle&=\left(\prod_{u_j\in U_B}\prod_{v_i\in\mathcal{N}_{u_j}}\Lambda_{v_i,u_j}(Z)\right)|+\rangle^{\otimes|V_A|}|+\rangle^{\otimes|U_B|}\\&=\left(\prod_{u_j\in U_B}H_{u_j}\right)\left(\prod_{u_j\in U_B}\prod_{v_i\in\mathcal{N}_{u_j}}\Lambda_{v_i,u_j}(X)\right)\sum_{\{\bar\sigma_{v_i}\}}|\{\bar\sigma_{v_i}\}\rangle|0\rangle^{\otimes|U_B|}\\&=\left(\prod_{u_j\in U_B}H_{u_j}\right)\sum_{\{\bar\sigma_{v_i}\}}|\{\bar\sigma_{v_i}\}\rangle\bigotimes_{u_j\in U_B}|\oplus_{v_i\in\mathcal{N}_{u_j}}\bar\sigma_{v_i}\rangle.\end{aligned}$$

□

Equation (5) shows that IQP is equivalent to the sampling problem according to the probabilities proportional to the squared norm of the partition functions of an Ising model with imaginary coupling constants. Note that the measurement outcome $\{s_i\}$ corresponds to the random $\mathrm{i}\pi/2$ magnetic fields.

The present sampling problem is not related directly to what is well studied in the fields of statistical physics, such as the Metropolis sampling according to the Boltzmann distribution. However, as we will see below, the relation between IQP and Ising partition functions leads us to several interesting results about complexity of IQP, since calculation of the Ising partition functions are well studied in both fields of statistical physics and

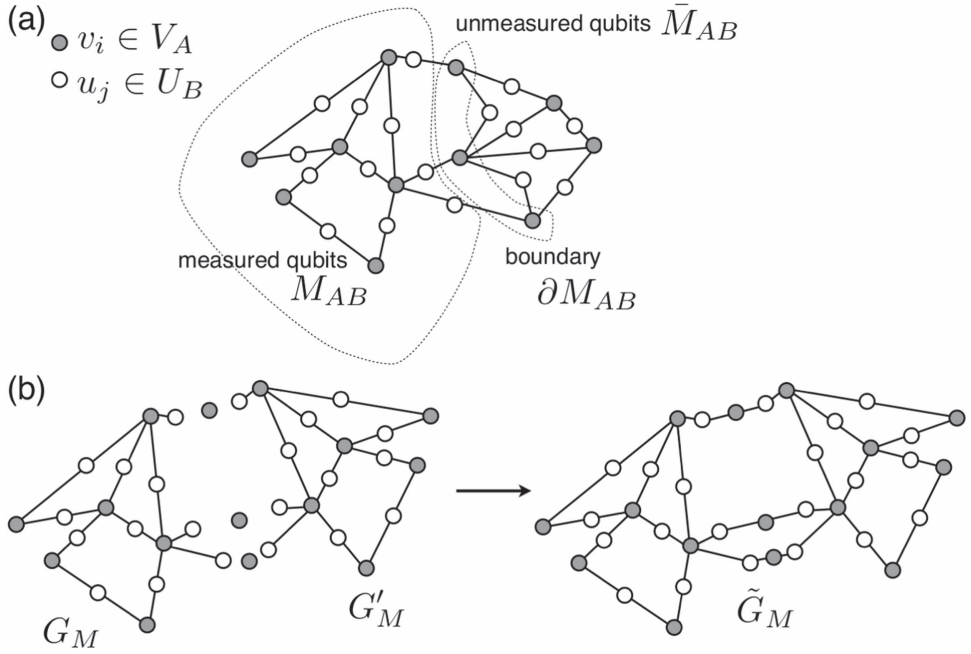

Figure 3. (a) The graph state $|G\rangle$ associated with the graph G. The gray and white circles indicate qubits associated with $v_i \in V_A$ and $u_j \in U_B$, respectively. (b) The subgraph state $|G_M\rangle$ and its copy $|G'_M\rangle$ are merged via the qubits $|+\rangle^{|\partial M_{AB}|}$ located on the boundary. The merged graph is denoted by $\tilde{G}_M$.

computer science. It was shown in [32] that exact calculation of partition functions of the Ising models with real coupling strengths and magnetic fields is NP-hard even on the planar graphs. Furthermore, in general, exact calculation of partition functions of two-body Ising models with magnetic fields is #P-hard [33]. No polynomial-time approximation scheme with multiplicative error exists unless NP = RP. While IQP does not provide the exact values of the partition functions, it is surprising that the sampling according to the partition functions of many-body Ising models $H(\{s_{v_b}\}, \{\theta_{v_a}\}, G)$ with imaginary coupling constants, can be done in IQP, which consists only of commuting gates and seems much weaker than BQP.

Only in the limited cases, the partition function of an Ising model can be calculated efficiently. Such an example is two-body Ising models on the 2D planar lattices without magnetic fields. In the next section, we show that certain classes of IQP are classically simulatable, at least in the weak sense, by using the fact that the associated Ising models are exactly solvable. To this end, we need not only the joint distribution of the output of IQP circuits but also the marginal distributions with respect to measured qubits, in order to simulate the sampling problem recursively.

4.2. Marginal distribution

Even if we can calculate the probability distribution $P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\}, \{S_j\})$ efficiently, it does not directly mean that the corresponding IQP is classically simulatable, since there are exponentially many varieties of the measurement outcomes $\{s_i\}$. An efficient weak classical simulation of IQP requires the marginal distribution with respect to measured qubits, by which we can simulate IQP recursively. In the following we will establish a mapping between the marginal distribution with respect to the set M of measured qubits and the partition function of an Ising model defined on a merged graph $\tilde{G}_M$. The merged graph $\tilde{G}_M$ constructed by merging a subgraph G_M corresponding to the measured part of the graph G and its copy G'_M (see figure 3). (The detailed definition of the subgraph G_M and the merged graph $\tilde{G}_M$ are given in the proof of the following theorem.)

Theorem 2 (Marginal distribution of IQP). *Let $M \subset \{1, 2, \ldots, n\}$ and $\bar{M} \subset \{1, 2, \ldots, n\}$ be sets of the measured and unmeasured qubits, respectively (and hence $M \cup \bar{M} = \{1, 2, \ldots, n\}$ and $M \cap \bar{M} = \varnothing$). A marginal distribution with respect to the set M*

$$P_{\mathrm{IQP}}(\{s_i\}_{i\in M}|\{\theta_j\}, \{S_j\}, M) \equiv \sum_{\{s_i\}_{i\in\bar{M}}} P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\}, \{S_j\})$$

is related to the Ising partition function defined by the merged graph $\tilde{G}_M$ and weights $\{\theta_j\} \cup \{-\theta_j\}$.

Proof. In order to prove this, we consider the corresponding MBIQP. However, it is just for a proof, and hence we do not need to simulate MBIQP in classical simulation as seen later. Thus without loss of generality, we can assume that the measurement outcome is subject to $m_{u_j} = 0$ for all $u_j \in U_B$.

Based on the sets M and $\bar{M}$, the sets of measured and unmeasured qubits in V_A is defined as M_A and $\bar{M}_A$, i.e., $M_A \cup \bar{M}_A = V_A$. We define a subgraph $G_M(M_A \cup M_B, E_M)$, where $M_B \subset U_B$ is a set of vertices that are connected with any vertices in M_A, i.e., $M_B = \{u_j \in U_B | (u_j, v_i) \in E, v_i \in M_A\}$. E_M is a set of edges whose two incident vertices both belong to $M_A \cup M_B$. We denote $M_A \cup M_B$ simply by M_{AB} and $(V_A \cup U_B) \setminus M_{AB}$ by $\bar{M}_{AB}$ (see figure 3(a)).

The marginal distribution can be written as measurements on the reduced density matrix on the qubits M_{AB}:

$$P_{\mathrm{IQP}}(\{s_i\}_{i\in M} | \{\theta_j\}, \{S_j\}, M) = \langle \Theta | \mathrm{Tr}_{\bar{M}_{AB}}[|G\rangle\langle G|] | \Theta \rangle,$$

where $|\Theta\rangle \equiv \bigotimes_{v_i \in M_A} |+_{s_i}\rangle \bigotimes_{u_j \in M_B} |\theta_{j,0}\rangle$, and $\mathrm{Tr}_{\bar{M}_{AB}}$ indicates the partial trace with respect to the unmeasured qubits $\bar{M}_{AB}$.

We define a subset $\partial M_{AB} \subset \bar{M}_{AB}$ as a set of vertices connected with any vertices in M_{AB}, i.e., $\partial M_{AB} = \{v_i \in \bar{M}_A | (v_i, u_j) \in E, u_j \in M_B\}$ (note that $\partial M_{AB} \subset \bar{M}_A$). We refer to the qubits associated with the vertices in ∂M_{AB} as the boundary qubits, since they are the boundary of the measured and unmeasured qubits in the graph state as shown in figure 3(a).

For the graph state $|G\rangle$, the tracing out with respect to the unmeasured qubits $\bar{M}_{AB}$ can be equivalently done by Z basis measurements on the boundary qubits and forgetting about the measurement outcomes. This is because, Z-basis measurements on the boundary qubits separate the measured and unmeasured qubits (see fact 1), and hence the tracing out of the qubits in $\bar{M}_{AB} \setminus \partial M^{AB}$ does not have any effect on the measured qubits M_{AB}. From this observation we obtain

$$\mathrm{Tr}_{\bar{M}_{AB}}[|G\rangle\langle G|] = 2^{-|\partial M_{AB}|} \sum_{\{m_{v_i}\}_{\partial M_{AB}}} \left(\prod_{v_i \in \partial M_{AB}} B(v_i)^{m_{v_i}} \right) |G_M\rangle\langle G_M| \left(\prod_{v_i \in \partial M_{AB}} B(v_i)^{m_{v_i}} \right),$$

where $\{m_{v_i}\}_{\partial M_{AB}}$ is the set of the measurement outcomes on the boundary qubits, and we define a byproduct operator $B(v_i) = \prod_{u_j \in \mathcal{N}_{v_i} \cap M_{AB}} Z_{u_j}$ (see fact 1).

Let us consider a merged graph $\tilde{G}_M$ that is constructed from the graph G_M and its copy G'_M, and the boundary ∂M_{AB}. Two copies of graph states, $|G_M\rangle$ and $|G'_M\rangle$, are merged via $|+\rangle^{\otimes|\partial M_{AB}|}$ as shown in figure 3(b). The vertices in ∂M_{AB} and those in G_M and G'_M are connected iff there is an edge between them in the original graph G and its copy G'. The graph state associated with the merged graph $\tilde{G}_M$ is written as

$$|\tilde{G}_M\rangle = \prod_{v_i \in \partial M_{AB}} \left(\prod_{u_j \in \mathcal{N}_{v_i} \cup M_B} \Lambda_{v_i,u_j}(Z) \prod_{u'_j \in \mathcal{N}'_{v_i} \cup M'_B} \Lambda_{v_i,u'_j}(Z) \right) |G_M\rangle |+\rangle^{\otimes|\partial M_{AB}|} |G'_M\rangle.$$

Let us consider a projection of $|\tilde{G}_M\rangle$ by $|+\rangle^{\otimes|\partial M_{AB}|}$:

$$\langle +|^{\otimes|\partial M_{AB}|} |\tilde{G}_M\rangle = 2^{-|\partial M_{AB}|} \sum_{\{m_{v_i}\}_{\partial M_{AB}}} \left[\prod_{v_i \in \partial M_{AB}} [B(v_i)B'(v_i)]^{m_{v_i}} \right] |G_M\rangle |G'_M\rangle,$$

where $B'(v_i)$ is defined similarly to $B(v_i)$ on the graph state $|G'_M\rangle$. Let us define

$$|\Theta'\rangle \equiv \bigotimes_{v_i \in M_A} |+_{s_i}\rangle \bigotimes_{u_j \in M_B} |-\theta_{j,0}\rangle,$$

where we should note that the sign of the angle $\theta_{j,0}$ is flipped. Next we consider a projection by $|\Theta\rangle|\Theta'\rangle$ as follows:

$$\begin{aligned}
&\langle \Theta | \langle +|^{\otimes|\partial M_{AB}|} \langle \Theta' || \tilde{G}_M \rangle \\
&= 2^{-|\partial M_{AB}|} \sum_{\{m_{v_i}\}_{\partial M_{AB}}} \langle \Theta | \left[\prod_{v_i \in \partial M_{AB}} [B(v_i)]^{m_{v_i}} \right] |G_M\rangle \langle \Theta' | \left[\prod_{v_i \in \partial M_{AB}} [B'(v_i)]^{m_{v_i}} \right] |G'_M\rangle \\
&= \langle \Theta | \mathrm{Tr}_{\bar{M}_{AB}}[|G\rangle\langle G|] | \Theta \rangle \\
&= P_{\mathrm{IQP}}(\{s_i\}_{i\in M} | \{\theta_j\}, \{S_j\}, M).
\end{aligned} \tag{6}$$

This indicates that the summation over exponentially many variables for the marginalization is taken simply in an overlap between the product state and the merged graph state.

On the other hand, the overlap $\langle \Theta | \langle +|^{\otimes|\partial M_{AB}|} \langle \Theta' || \tilde{G}_M \rangle$ is also reformulated as an Ising partition function as done in the proof of theorem 1. Specifically, the interaction patterns are given by the merged graph $\tilde{G}_M$. The coupling strengths are given by two copies of $\{\theta_j\}_{u_j \in M_B}$ and $\{-\theta_j\}_{u'_j \in M'_B}$:

$$\begin{aligned}&\langle\Theta|\langle+|^{\otimes|\partial M_{AB}|}\langle\Theta'||\tilde{G}_M\rangle\\&= 2^{-2|M_A|-|\partial M_{AB}|-|M_B|}\,|\mathcal{Z}(\{s_i\}_M\cup\{0\}_{v_i\in\partial M_{AB}}\cup\{s_i'\}_{M'},\{\theta_j\}_{u_j\in M_B}\cup\{-\theta_j\}_{u_j\in M_B'},\tilde{G}_M)|,\\&\equiv 2^{-2|M_A|-|\partial M_{AB}|-|M_B|}\,|\mathcal{Z}(\{s_i\}^*,\{\theta_j\}^*,\tilde{G}_M)|,\end{aligned}\tag{7}$$

where we defined $\{s_i\}^* \equiv \{s_i\}_M \cup \{0\}_{v_i\in\partial M_{AB}} \cup \{s_i'\}_{M'}$ and $\{\theta_j\}^* \equiv \{\theta_j\}_{u_j\in M_B} \cup \{-\theta_j\}_{u_j\in M_B'}$. We should note that s_i and s_i' take the same value but θ_j's sign is flipped on its copy $u_j' \in M_B'$. From equations (6) and (7),

$$P_{\mathrm{IQP}}(\{s_i\}_{i\in M}|\{\theta_j\},\{S_j\},M) = 2^{-2|M_A|-|\partial M_{AB}|}\,|\mathcal{Z}(\{s_i\}^*,\{\theta_j\}^*,\tilde{G}_M)|$$

That is, the marginal distribution with respect to the set M of the measured qubits is given by the normalized squared norm of the partition function of the Ising model defined by the merged graph $\tilde{G}_M$. □

The above theorem also indicates that the marginal distribution is equivalent to the square root of the joint probability of the IQP circuit associated with the merged graph $\tilde{G}_M$, weights $\{\theta_j\}^*$ and the measurement outcomes $\{s_i\}^*$:

$$P_{\mathrm{IQP}}(\{s_i\}_{i\in M}|\{\theta_j\},\{S_j\},M) = [P_{\mathrm{IQP}}(\{s_i\}^*,\{\theta_j\}^*,\{\mathcal{N}_{u_j}|u_j\in\tilde{G}_M\})]^{1/2}.$$

This indicates that if the joint probability distributions of the IQP circuits associated with a class of graphs can be calculated efficiently, and the class of graphs is closed under merging mentioned above, then the marginal distributions of such a class of IQP circuits can also be calculated efficiently. An example of such a class is planar graphs, where the merged graph $\tilde{G}_{M^{(k)}}$ is also a planar graph with an appropriately chosen measurement order such that $M^{(k)}$ is always connected.

Conditioned on the measurement outcome $\{s_i\}_{i\in M}$ on the set M, the probability of obtaining the next measurement outcome s_k is calculated by using the Bayes rule as

$$p(s_k|\{s_i\}_{i\in M}) = \frac{P_{\mathrm{IQP}}(\{s_i\}_{i\in M\cup k}|\{\theta_j\},\{S_j\},M\backslash k)}{P_{\mathrm{IQP}}(\{s_i\}_{i\in M}|\{\theta_j\},\{S_j\},M)}.$$

By denoting the set of all measured qubits after the kth measurements as $M^{(k)}$ (since there is no order in the measurements in IQP, we can choose an arbitrary order of measurements for our convenience), we can reconstruct the joint probability distribution of IQP as follows:

$$P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\},\{S_j\}) = \prod_{k=1}^{n} p(s_{i_k}|\{s_i\}_{i\in M^{(k)}}),$$

where the i_kth qubit is measured at step k, i.e., $\{i_k\}\cup M^{(k-1)} = M^{(k)}$. If the marginal distribution, that is, the Ising partition functions defined on $\tilde{G}_{M^{(k)}}$ can be calculated efficiently for all $M^{(k)}$ for a measurement order, IQP is classically simulatable at least in the weak sense.

Note that even if we can calculate the marginal distributions for an appropriately chosen measurement order, it is not sufficient to show strong simulatability in a strict sense. In order to shown strong simulatability, we have to show that arbitrary marginal distributions can be calculated efficiently. In the next section, we will see a classically simulatable class based on planarity of the associated Ising models. However, if we choose a wrong measurement order, the merged graph results in a non-planar graph. In such a case, the marginal distribution is mapped into a partition function of an Ising model on a non-planar lattice, which is hard to calculate [32, 73, 74]. To clarify this situation, we say *almost strongly simulatable* if there exists a measurement order, and all marginal distributions with respect it can be calculated efficiently.

5. Classical simulatable classes of IQP

In this section, we will provide two classes of IQP that are classically simulatable efficiently. One in section 5.1 is based on the sparsity of the commuting gates. The other in section 5.2 is based on the exact solvability of Ising models on the 2D planar lattices without magnetic fields [32, 36, 37].

In general, exact calculation of partition functions of Ising models in the presence of magnetic fields is highly intractable in classical computers even on 2D planar lattice [32, 33]. The Ising models, to which we have mapped IQP in section 4, include the random $i\pi/2$ magnetic fields depending on the output $\{s_i\}$. In both cases, we will show that if the geometries of the graphs have some properties, we can safely remove the magnetic fields renormalizing it into the coupling constants $\{\theta_j\}$.

5.1. Classical simulatability: sparse commuting circuits

Let us define a $|V_A|\times|U_B|$ matrix R, associated with the bipartite graph $G = (V_A\cup U_B, E)$, such that $R_{v_i}^{u_j} = 1$ iff a vertex $v_i \in V_A$ is in $\mathcal{N}_{u_j}$, otherwise $R_{v_i}^{u_j} = 0$. We consider a class of bipartite graphs with $|V_A| = |U_B|$, for which the row vectors of R are linearly independent in $\mathbf{Z}_2^{|U_B|}$. We call such a bipartite graph as an independent-bipartite

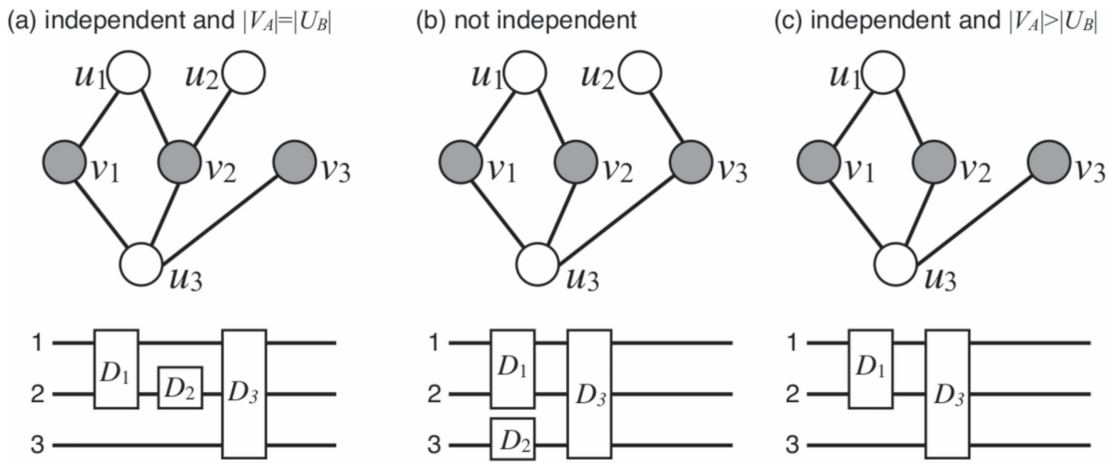

Figure 4. Bipartite graph states (top) and associated commuting circuits (bottom). The white and gray shaded circles indicate qubits in U_B and V_A, respectively. (a) A graph that is independent and $|V_A| = |U_B|$. (b) A graph that is not independent. (c) A graph that is independent but $|V_A| > |U_B|$.

graph (IBG). Examples of the IBGs is depicted in figure 4(a). Later we will weaken the condition $|V_A| = |U_B|$ to $|V_A| \geqslant |U_B|$.

Now we consider the Ising model associated with an IBG. If we consider only computational basis, we can replace the classical spin variable σ with the Pauli Z operator. Therefore, we can rewrite the Ising Hamiltonian equation (4) as

$$\hat{H}(\{s_i\}, \{\theta_j\}, G) \equiv -\sum_i \frac{i\pi}{2} s_i (1 - Z_{v_i}) - \sum_j i\theta_j \left(\bigotimes_{v_i \in N_{u_j}} Z_{v_i} \right).$$

Then the partition function is given by

$$\mathcal{Z}(\{s_i\}, \{\theta_j\}, G) = \mathrm{Tr}\,[e^{-\hat{H}(\{s_i\},\{\theta_j\},G)}].$$

Our main goal here is to calculate $|\mathcal{Z}(\{s_i\}, \{\theta_j\}, G)|^2$ exactly. To this end, let us first consider the case $s_i = 0$ for all v_i. In this case, there is no magnetic field, and hence we can transform the Hamiltonian into an interaction-free Ising model by virtue of the properties of the IBGs.

Lemma 4 (Mapping to interaction-free Ising model). *For any Ising model associated with an IBG, there exists a unitary operator W that transforms $\hat{H}(\{0\}, \{\theta_j\}, G)$ to interaction-free Ising Hamiltonian:*

$$W\hat{H}(\{0\}, \{\theta_j\}, G)W^\dagger = \sum_j i\theta_j Z_{v_j}.$$

Proof. Since the column vectors of R are independent, we can transform the matrix R to the identity matrix by using the Gauss–Jordan elimination method. Since the matrix R defines the graph and the Hamiltonian, the Gauss–Jordan elimination can be viewed as a transformation of the graph and the corresponding Hamiltonian. The graph associated with the identity matrix consists of pairs of vertices (v_i, u_i) connected by edges. Since each vertex in U_B is always connected only one vertex in V_A, the corresponding Ising Hamiltonian is interaction-free.

Each process in the Gauss–Jordan elimination for the matrix R can be implemented on the Hamiltonian by conjugations of controlled-Not (CNOT) and swapping gate operations. The CNOT gate from the ith to the jth qubits is equivalent to adding the jth row vector to the ith one on the matrix R. The swapping gate exchanges the labels $\{v_i\}$ of the vertices. Thus there exists a unitary operator W consisting of swapping and CNOT gates such that $W\hat{H}(\{0\}, \{\theta_j\}, G)W^\dagger = \sum_j i\theta_j Z_{v_j}$. □

For example, in the case of the IBG shown in figure 4(a), the set of operators in the Hamiltonian is given by $\{Z_{v_1}Z_{v_2}, Z_{v_1}Z_{v_2}Z_{v_3}, Z_{v_2}\}$. This can be mapped to $\{Z_{v_1}, Z_{v_2}, Z_{v_3}\}$ by using the unitary operator $W = S^{\mathrm{wap}}_{v_2,v_3}\Lambda(X)_{v_1,v_3}\Lambda(X)_{v_2,v_1}$, where $S^{\mathrm{wap}}_{v_i,v_j}$ is the swapping operation between qubits v_i and v_j.

By using such a W, the partition function can be calculated as

$$\begin{aligned}\mathcal{Z}(\{s_i\},\{\theta_j\},G) &= \mathrm{Tr}[e^{-\hat{H}(\{s_i\},\{\theta_j\})}]\\ &= \mathrm{Tr}[We^{-W^\dagger\hat{H}(\{s_i\},\{\theta_j\})W}W^\dagger]\\ &= 2^{|U_B|}\prod_{u_j}\cos\theta_j.\end{aligned}$$

Thus the probability of obtaining $\{s_i=0\}$ is computed as

$$P_{\mathrm{IQP}}(\{s_i=0\}|\{\theta_j\},\{S_j\}) = \left(\prod_{u_j}\cos\theta_j\right)^2.$$

Since the joint probability is factorized for each θ_j, we can easily calculate its marginal distribution (without using theorem 2 in this case).

Next we extend the above result to the general measurement outcomes $\{s_i\}$. This is done by renormalizing the random $i\pi/2$ magnetic fields into the coupling constants as follows.

Lemma 5 (Renormalization of $i\pi/2$ magnetic fields). *For any* IQP *associated with an IBG, we can find a bit string* $\{c_{u_j}\}$ *such that*

$$P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\}) = P_{\mathrm{IQP}}(\{s_i=0\}|\{\tilde{\theta}_j\}),$$

with $\tilde{\theta}_j \equiv \theta_j + c_{u_j}\pi/2$.

Proof. Let us consider the corresponding MBIQP. From the definition of MBIQP,

$$\begin{aligned}P_{\mathrm{MBIQP}}(\{m_{v_i}\},\{m_{u_j}\}|\{\theta_j\},G) &= \left|\bigotimes_{v_i\in V_A}\langle+_{m_{v_i}}|\bigotimes_{u_j\in U_B}\langle\theta_{j,m_{u_j}}||G\rangle\right|^2\\ &= \left|\langle+_0|^{\otimes|V_A|}F(\{m_{v_i}\})\bigotimes_{u_j\in U_B}\langle\theta_{j,m_{u_j}}||G\rangle\right|^2,\end{aligned}$$

where $F(\{m_{v_i}\}) \equiv \bigotimes_{v_i\in V_A} Z_{v_i}^{m_{v_i}}$. Since the row vectors of R are independent, we can find a vector c_{u_j} in $\mathbf{Z}_2^{|U_B|}$ such that $m_{v_i} = \sum_{u_j} R_{v_i}^{u_j} c_{u_j}$ for any $\{m_{v_i}\}$. By using this vector c_{u_j}, we obtain the following equality,

$$\prod_{u_j\in U_B}(X_{u_j}K_{u_j})^{c_{u_j}} = \prod_{u_j\in U_B}\left(\prod_{v_i\in\mathcal{N}_{u_j}} Z_{v_i}\right)^{c_{u_j}} = F(\{m_{v_i}\}).$$

By using this and the fact that K_{u_j} stabilizes $|G\rangle$, we obtain

$$\begin{aligned}P_{\mathrm{MBIQP}}(\{m_{v_i}\},\{m_{u_j}\}|\{\theta_j\},G) &= \left|\langle+_0|^{\otimes|V_A|}\bigotimes_{u_j\in U_B}\langle\theta_{j,m_{u_j}}|\left(\prod_{u_j\in U_B}X_{u_j}^{m_{v_i}}\right)|G\rangle\right|^2\\ &= \left|\langle+_0|^{\otimes|V_A|}\bigotimes_{u_j\in U_B}\langle\tilde{\theta}_{j,m_{u_j}}||G\rangle\right|^2\\ &= P_{\mathrm{MBIQP}}(\{\tilde{s}_{v_j}=0\},\{m_{u_j}\}|\{\tilde{\theta}_j\},G),\end{aligned}$$

where $\tilde{\theta}_j \equiv \theta_j + c_{u_j}\pi/2$. Specifically, if we consider the case $m_{u_j}=0$, we obtain that

$$\begin{aligned}P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\},\{S_j\}) &= 2^{|U_B|}P_{\mathrm{MBIQP}}(\{s_{v_i}\},\{m_{u_j}=0\}|\{\theta_j\},G)\\ &= 2^{|U_B|}P_{\mathrm{MBIQP}}(\{s_{v_i}=0\},\{m_{u_j}=0\}|\{\tilde{\theta}_j\},G)\\ &= P_{\mathrm{IQP}}(\{s_i=0\}|\{\tilde{\theta}_j\},\{S_j\}).\end{aligned}$$

□

Let us consider the example shown in figure 4(a) again. For instance, if $\{s_{v_i}\}=\{0,0,1\}$, $F(\{0,0,1\}) = Z_{v_3}$, and $\{c_{u_1}=1, c_{u_2}=0, c_{u_3}=1\}$. By multiplying the stabilizer operators of the graph state with respect to the 4th and 6th vertices, we obtain another stabilizer operator $(X_{u_1}Z_{v_1}Z_{v_2})(X_{u_3}Z_{v_1}Z_{v_2}Z_{v_3}) = X_{u_1}X_{u_3}Z_{v_3}$. Thus the action of $F(\{0,0,1\})$ is equivalent to that of X_4X_6, which rotates the angles θ_{u_1} and θ_{u_3} by $\pi/2$.

By combining lemmas 4 and 5, we can show classical simulatability of IQP associated with IBGs.

Theorem 3 (**Classical simulatability: sparse circuits**). IQP *associated with an IBG is classically simulatable.*

Proof. From lemmas 4 and 5, we can calculate $P_{\rm IQP}(\{s_i\}|\{\theta_j\})$ exactly for an IBG including its arbitrary marginal distributions. Thus such a class of IQP is classically simulatable for arbitrary angles $\{\theta_j\}$ in the strong sense. □

Finally, we slightly weaken the condition, $|U_B| = |V_A|$. Even if $|U_B| < |V_A|$ (as shown in figure 4(c)), there exist W such that transforms the many-body Ising Hamiltonian to interaction-free Ising Hamiltonian as long as the column vectors of R are independent. In this case, the existence of c_{u_j} for all $\{m_{u_j}\}$ is not guaranteed, and hence we have to find another way to deal with this situation.

To settle this, we add ancilla vertices $u_{j'} \in U_{B'}$ to the set U_B in such a way that $R^{u_j}_{v_i}$ $(u_j \in U_B \cup U_{B'})$ satisfies $|V_A| = |U_B \cup U_{B'}|$ (The 5th qubit in figure 4(a) can be viewed as the ancilla qubit for the non-full rank graph in figure 4(c)). Due to theorem 3, we can exactly calculate the probability for the slightly enlarged problem, $P_{\rm IQP}(\{s_i\}|\{\theta_j\} \cup \{\theta_{j'}\})$. Then, the probability $P_{\rm IQP}(\{s_i\}|\{\theta_j\})$, with which we want to sample $\{s_i\}$, can be obtained by considering a specific case $\theta_{j'} = 0$ for all $u_{j'} \in U_{B'}$, i.e.,

$$P_{\rm IQP}(\{s_i\}|\{\theta_j\} \bigcup \{\theta_{j'} = 0\}) = P_{\rm IQP}(\{s_i\}|\{\theta_j\}).$$

A representative example of classically simulatable IQP circuits are depicted in figures 4(a) and (c). If we restrict ourselves into two-body Ising models (i.e., $|S_j| = 2$), the meaning of independence becomes clear; independence means that the lattice does not contain any loop, such as Ising models on one-dimensional chain or tree graphs. Thus IQP with two-qubit commuting gates whose interaction geometry does not contain any loop can be efficiently simulated in the strong sense. In order to avoid the present class of classically simulatable IQP, the IQP circuits that consist of at least n $(=|V_A|)$ commuting gates acting on different subsets $\{S_j\}$ of qubits are sufficient.

5.2. Classical simulatability: planar-IQP

Classical simulatability in the previous case is based on the sparsity of the commuting gates, where at most only $n - 1$ commuting gates are included. In such a case we can calculate the partition functions without using theorem 2. Next we will provide another classically simulatable class of IQP, that includes commuting gates much more than n. Specifically, we will show below that IQP with two-qubit commuting gates acting on nearest-neighbor two qubits on the 2D planar graphs, which we call planar-IQP, is classically simulatable almost in the strong sense. That is, the probability distribution of the output and its marginal distribution for an appropriately chosen measurement order can be calculated efficiently. To this end, we first show, by using properties of the graph states, that for two-body Ising models we can always remove the random $i\pi/2$ magnetic fields by appropriately renormalizing their effects into coupling constants $\{\theta_j\}$. This allows us to map planar-IQP to two-body Ising models without magnetic fields. Then we utilize theorem 2 and exact solvability of two-body Ising models on planar lattices to construct an efficient classical simulation of IQP.

Consider a planar bipartite graph G with $|S_j| = 2$, that is, every vertex $u_j \in U_B$ are connected with just two vertices $v_i \in V_A$. The weights $\{\theta_j\}$ are arbitrary. For simplicity, we assume that G is connected. Let us consider properties of the graph state associated with such a planar bipartite graph G.

Lemma 6 (**Property of graph states 1**). *For any connected bipartite graph G with $|S_j| = 2$ for all j, the associated graph state $|G\rangle$ is subject to the following property:*

$$\left(\prod_{v_i \in V_A} \langle +_{m_{v_i}}|\right)|G\rangle = 0$$

for any $\{m_{v_i}\}$ such that $\bigoplus_{v_i \in V_A} m_{v_i} = 1$. Here the addition is taken modulo two.

Proof. The bipartite graph state is stabilized by

$$\prod_{v_i \in V_A} \left(X_{v_i} \prod_{u_j \in \mathcal{N}_{v_i}} Z_{u_j}\right) = \prod_{v_i \in V_A} X_{v_i},$$

and hence $(\prod_{v_i \in V_A} X_{v_i})|G\rangle = |G\rangle$. By using this, we obtain

$$\left(\prod_{v_i \in V_A} \langle +_{m_{v_i}}|\right)|G\rangle = \left(\prod_{v_i \in V_A} \langle +_{m_{v_i}}|\right)\left(\prod_{v_i \in V_A} X_{v_i}\right)|G\rangle = \left(\prod_{v_i \in V_A} \langle +_{m_{v_i}}|\right)(-1)^{\bigoplus_{v_i \in V_A} m_{v_i}}|G\rangle.$$

Thus if $\bigoplus_{v_i \in V_A} m_{v_i} = 1$, then $(\prod_{v_i \in V_A} \langle +_{m_{v_i}}|)|G\rangle = 0$. □

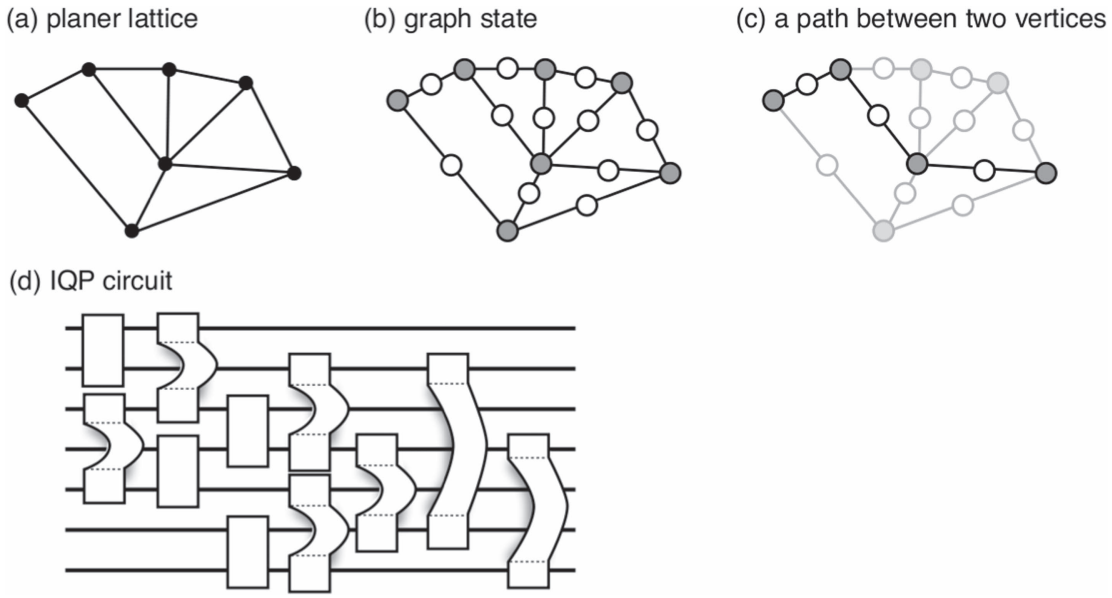

Figure 5. (a) A planar lattice. (b) An associated bipartite graph state, where gray and white circles denote qubits in V_A and U_B, respectively. (c) A path between a pair of qubits in V_A. (d) The corresponding commuting circuit.

Thus we only consider the case $\bigoplus_{v_i\in V_A} m_{v_i} = 0$, that is, the number of vertices with $m_{v_i} = 1$ is even. In such a case, we can show that modifying the coupling constants $\{\theta_j\}$ appropriately as follows can renormalize $i\pi/2$ magnetic fields.

Lemma 7 (**Property of graph states 2**). *For any* IQP *associated with a connected bipartite graph G with* $|S_j| = 2$ *for all* j, *by appropriately choosing* $\{\tilde{\theta}_j\}$,

$$P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\},\ \{S_j\}) = P_{\mathrm{IQP}}(\{s_i = 0\}|\{\tilde{\theta}_j\},\ \{S_j\}),$$

where $\{s_i = 0\}$ *means that* $s_i = 0$ *for all i. Equivalently, for the corresponding Ising models, we have*

$$H(\{s_i\},\ \{\theta_j\},\ G) = H(\{s_i = 0\},\ \{\tilde{\theta}_j\},\ G),$$

that is, the random $i\pi/2$ *magnetic fields can be renormalized into the coupling constants* $\{\tilde{\theta}_j\}$.

Proof. Consider the graph state $|G\rangle$. Due to lemma 6, the number of $\tilde{s}_i = 1$ is always even. The graph is connected. Thus we can always make pairs of vertices $v_i \in V_A$ of $m_{v_i} = 1$. Apparently this can be done in polynomial-time, since arbitrary paring is allowed. Let us denote such a pair as $(v_k \sim v_{k'})$ and a set of vertices on a path (arbitrarily) connecting them as $\mathrm{path}(v_k \sim v_{k'})$. The graph state is stabilized by

$$\prod_{u_j\in \mathrm{path}(v_k\sim v_{k'})\bigcap U_B} K_{u_j} = Z_{v_k}\left(\prod_{u_j\in \mathrm{path}(v_k\sim v_{k'})\bigcup U_B} X_{u_j}\right)Z_{v_{k'}},$$

(see figures 5(b) and (c)). By using this fact, we can obtain

$$\begin{aligned}
&\left(\bigotimes_{v_i\in V_A}\langle +_{m_{v_i}}|\right)\left(\bigotimes_{u_j\in U_B}\langle \theta_{j,m_{u_j}}|\right)|G\rangle \\
&= \left(\bigotimes_{v_i\in V_A}\langle +_{m_{v_i}}|\right)\left(\bigotimes_{u_j\in U_B}\langle \theta_{j,m_{u_j}}|\right)\left[Z_{v_k}\left(\prod_{u_j\in \mathrm{path}(v_k\sim v_{k'})\bigcup U_B} X_{u_j}\right)Z_{v_{k'}}\right]|G\rangle \\
&= \left(\bigotimes_{v_i\in V_A}\langle +_{m_{v_i}\oplus\delta_{v_i,v_k}\oplus\delta_{v_i,v_{k'}}}|\right)\left(\bigotimes_{u_j\in U_B}\langle \theta_{j,m_{u_j}\bigoplus_{u_{j'}\in \mathrm{path}(v_k\sim v_{k'})}\delta_{u_j,u_{j'}}}|\right)|G\rangle.
\end{aligned}$$

By doing this repeatedly for all pairs of $m_{v_i} = 1$, i.e., a perfect matching of $m_{v_i} = 1$ vertices, we can transform all $m_{v_i} = 1$ to $m_{v_i} = 0$. Let us define an arbitrary perfect matching $\mathcal{M}$ of vertices of $m_{v_i} = 1$ and a set $\mathrm{path}(\mathcal{M})$ of paths of the matching $\mathcal{M}$. By denoting the addition modulo two over $u_{j'}$s on all these paths by $\bigoplus_{u_{j'}\in \mathrm{path}(\mathcal{M})}$, the renormalized coupling constant is given by

$$\tilde{\theta}_j = \theta_j + \left(\bigoplus_{u_{j'} \in \mathrm{path}(\mathcal{M})} \delta_{u_j, u_{j'}} \right) \pi/2.$$

Then we obtain

$$\left(\bigotimes_{v_i \in V_A} \langle +_{m_{v_i}}| \right) \left(\bigotimes_{u_j \in U_B} \langle \theta_{j, m_{u_j}}| \right) |G\rangle = \langle +_0|^{\otimes |V_A|} \left(\bigotimes_{u_j \in U_B} \langle \tilde{\theta}_{j, m_{u_j}}| \right) |G\rangle.$$

This leads that

$$\begin{aligned} P_{\mathrm{IQP}}(\{s_i\}|\{\theta_j\}, \{S_j\}) &= 2^{|U_B|} P_{\mathrm{MBIQP}}(\{m_{v_i}\}, \{m_{u_j} = 0\}|\{\theta_j\}, G) \\ &= 2^{|U_B|} P_{\mathrm{MBIQP}}(\{\tilde{s}_{v_i} = 0\}, \{m_{u_j} = 0\}|\{\tilde{\theta}_j\}, G) \\ &= P_{\mathrm{IQP}}(\{s_i = 0\}|\{\tilde{\theta}_j\}, \{S_j\}). \end{aligned}$$

□

Note that in the proofs of the properties of graph states with $|S_j| = 2$, we did not use the planeness of the graph. Thus lemmas 6 and 7 hold even for nonplanar graphs as long as $|S_j| = 2$ for all j. Accordingly, we can always remove the random $i\pi/2$ magnetic fields of arbitrary two-body Ising models by appropriately renormalizing them into the two-body coupling constants.

Interestingly, these properties of the graph states are closely related to the properties of anyonic excitations on surface codes with a smooth boundary [75]. On the graph state with $|S_j| = 2$ for all j, if one project the qubits in V_A by $|+\rangle^{\otimes |V_A|}$, we obtain the surface code state defined on a lattice $\mathcal{L}$, where vertex and edge corresponds to vertices in V_A and U_B of G respectively, and a qubit is assigned on each edge. This can be confirmed as follows. The post-measurement state is stabilized by $\prod_{u_j \in \mathcal{N}_{v_i}} Z_{u_j} \equiv A_{v_i}$ for all v_i. Furthermore, for all faces f of the lattice $\mathcal{L}$, $\prod_{u_j \in \partial f} K_{u_j} = \prod_{u_j \in \partial f} X_{u_j} \equiv B_f$ stabilizes the post-measurement state, where ∂f is the set of the edges that are boundary of the face f. These two types operators are called star and plaquette operators in [75]. The post-measurement state or equivalently the surface code state is the ground state of the Hamiltonian, so-called Kitaev's toric code Hamiltonian,

$$H = -J \sum_i A_i - J \sum_f B_f.$$

A projection by $|-\rangle_{v_i}$ results in the eigenvalue -1 of the star operator at vertex v_i, which corresponds to the anyonic excitation in the Kitaev model. Then lemma 6 indicates that the parity of anyonic excitations is always even. They are created and annihilated in pairs. Lemma 7 corresponds a way to annihilate the pairs of the anyonic excitations. The trajectory of anyonic excitations in the annihilation process corresponds to path($\mathcal{M}$).

Now we are ready to show that classical simulatability of IQP consisting of 2D nearest-neighbor two-qubit commuting gates.

Theorem 4 (Classical simulatability: planar-IQP). *Planer-*IQP *consisting of two-qubit commuting gates acting on nearest-neighbor qubits on the 2D planar graphs is classically simulatable almost in the strong sense.*

Proof. According to theorem 1, the joint probability distribution of planar-IQP can be calculated from a two-body Ising partition function on a planar lattice. Since the graph G is a planar bipartite graph, we can easily find an order of measurements such that $\tilde{G}_{M^{(k)}}$ is also planar at any measurement step k. (Any order of measurements such that the subgraph $G_{M^{(k)}}$ becomes a connected graph for all k can be utilized.) Due to theorem 2, the marginal distributions are also given as Ising partition functions on planar lattices. Furthermore, in the merged graph, the vertices $u_j \in M_B^{(k)} \cup M'^{(k)}_B$ are connected with just two vertices, i.e., $|\mathcal{N}_{u_j}| = 2$. For such Ising models, by using lemmas 6 and 7, the random magnetic $i\pi/2$ fields can be renormalized into the coupling constants $\{\theta\} \to \{\tilde{\theta}_j\}$. Thus all marginal distributions can be calculated from the two-body Ising partition functions on planar lattices without magnetic fields. On the other hand, it is well known that the partition function of two-body Ising models on planar lattices without magnetic fields can be calculated efficiently by expressing them as the Pfaffians [32, 36, 37].

Thus we conclude that IQP of this class can be simulated efficiently almost in the strong sense, which is sufficient for an efficient weak simulation with a recursive method. □

Note that a similar argument is also made in [76] by considering classical simulatability of MBQC on the planar surface codes [75]. Indeed, as mentioned before, if we apply the projection by $|+\rangle^{\otimes |V_A|}$ on the bipartite planar graph state with $|S_j| = 2$, we obtain an unnormalized planar surface code state consisting of the qubits on U_B. The effect of $m_{v_i} = 1$ (i.e., the projection by $|+_1\rangle$) can be renormalized into the coupling constants $\{\theta_j\} \to \{\tilde{\theta}_j\}$, where an arbitrary perfect matching is chosen as shown in lemma 7. Thus we may construct an

alternative proof of theorem 4 without using theorem 2. However, theorem 2, employing the properties of the graph states, is much straightforward and simple for our purpose. Furthermore, theorem 2 is valid not only for the case with $|S_j| = 2$, but also the general cases, which cannot be regarded as MBQC on the planar surface codes.

While we have shown planar-IQP is almost strongly simulatable, it seems not to be strongly simulatable in the strict sense. Suppose that we choose a measurement order $\{M^{(k)}\}$ such that any subgraph $G^{M^{(k)}}$ consists of multiple disjoint subgraphs. In such a case, the merged graph becomes a non-planar graph of a higher genus. The Ising partition functions on lattices of a higher genus are hard to calculate in general [32, 73, 74]. There seems to be an intermediate class of classical simulation, which we named *almost strongly simulatable*, between strongly simulatable (in the strict sense) and weakly simulatable.

The Pfaffian is the square root of the determinant, and hence the probability distribution of planar-IQP is given by the determinant of an appropriately defined complex matrix. This result contrasts with BOSONSAMPLING related with the permanent of a complex matrix. The exact solvability with the determinant (Pfaffian) naturally reminds us free-fermionic models, which have been also studied as matchgates [77–81]. Since a determinant can be mapped into a probability amplitude of a free-fermionic system, the classically simulatable class of IQP can be regarded as FERMIONSAMPLING discussed in [31]. This suggests that the sampling problems in physics can be classified in a unified way as sampling problems of elementary particles.

Important implications of theorem 4 are twofold. One is that planar-IQP can generate highly entangled state but its output is classically simulatable almost in the strong sense. This is also the case for the Clifford circuits and match gates, which generate genuinely entangled states but are classically simulatable [43, 77–80]. Secondary, if single-qubit rotations are added to planer-IQP, it becomes universal-under-postselection, whose weak simulation is intractable unless the PH collapses to the third level. Thus single-qubit rotations take a quite important rule for IQP to be classically intractable. Indeed, single-qubit rotations make a drastic change of computational complexity from almost strongly simulatable to not simulatable even in the weak sense.

We would like to note that a similar result is also obtained in a rather different situation [19]. He showed that Toffoli-Diagonal circuits, which include quantum Fourier transformation for Shor's factorization algorithm, can be efficiently simulated if there is no basis change at the final round before the the computational basis measurements. Thus single-qubit rotations also play a very important role for the Toffoli-Diagonal circuits to be classically intractable.

Another consequence of theorem 4 lies in the context of experimental verification of quantum benefits. When we utilize IQP for the purpose of experimental verification of quantum benefits, we have to avoid planar-IQP, since a malicious quantum device can cheat experimentalists by classically sampling the results instead of implementing the IQP circuit. At the same time, the existence of efficient classical simulation for planar-IQP implies that checking the correctness of experiments of this class is much easier. Thus when experimentalists realize IQP, they should, at least, try to implement planar-IQP, since its correctness can be easily checked. It might be possible to efficiently ensure, under a plausible assumption, that two-qubit commuting gates are implemented appropriately, since experimental devices are usually well known and not so malicious. Hopefully, classical intractability of quantum devices may be verified by an efficient experimental verification of planar-IQP combined with other efficient witness or plausible assumptions [82]. Moreover, planar commuting circuits can generate an interesting class of entangled states, called weighted graph states [35]. The constructed classical simulation would be useful to check an experimental preparation of such states efficiently.

6. Hardness of approximating Ising partition functions

In this section, we utilize the established relationship between IQP and Ising partition functions in an opposite direction; by considering universal-under-postselection instances of IQP, we show that a multiplicative approximation of Ising partition functions with almost all imaginary coupling constants is #P-hard even on planar lattices with a bounded degree. Note that this argument based on universality-under-postselection and post-BQP = PP have been already utilized to show #P-hardness of approximating the permanent [17] and the Jones polynomial [40].

Theorem 5 (Hardness of approximating imaginary Ising partition functions). *A multiplicative approximation of Ising partition functions with almost all imaginary coupling constants is #P-hard even on planar lattices with a bounded degree. Thus if there exists a fully polynomial-time classical approximation scheme, the PH collapses completely.*

Proof. We consider IQP with a homogeneous rotational angle θ. As shown in [38], IQP associated with a bounded-degree planar graph with $|S_j| \leqslant 2$ is universal-under-postselection when the homogeneous rotational

angle is given by $\theta = \pi/8$. Thus a multiplicative approximation of the Ising partition functions with the homogeneous coupling constant $i\theta = i\pi/8$ is #P-hard due to theorem 1 and lemma 3. The same result holds not only $i\theta = i\pi/8$ but also $i\theta = i(2l+1)\pi/(8m)$ for integers l and m.

Suppose the homogeneous coupling is given by an irrational angle i.e., $\theta = 2\nu\pi$ with $\nu \in [0, 1)$ being an irrational number. Let m be an integer. Since $2m\nu\pi \pmod{2\pi}$ is distributed in a uniform fashion, we can find an approximation of $\pi/8$ with an additive error ϵ with some integer $m = \mathcal{O}(1/\epsilon)$ [43]. Accordingly the commuting gates $D(2\nu\pi, S_j)^m = D(2m\nu\pi, S_j)$ is sufficiently close to the rotation $D(\pi/8, S_j)$ in the sense of an appropriately defined distance such as the diamond norm [83]. In the present case, the erroneous rotation $D(\pi/8 + \epsilon, S_j)$ is unitary, and hence the diamond norm is equivalent to the square of the operator norm, which is given by

$$||D(\pi/8, S_j)[I - D(\epsilon, S_j)]||^2 = ||I - D(\epsilon, S_j)||^2 = 2(1 - \cos\epsilon) = O(\epsilon^2).$$

If a set of instances of IQP is universal-under-postselection, post-IQP can simulate universal fault-tolerant quantum computation. If the error ϵ is sufficiently smaller than the threshold value of fault-tolerant quantum computation [84–86], we can reliably simulate universal quantum computation (i.e., BQP) and moreover PP with the help of postselection. (See [82, 87] for an application of the fault-tolerance theory to the postselection argument, where it is shown that if the amount of the error is sufficiently small, we can solve a PP-complete problem under postselection.) Thus IQP with almost all rotational angles is universal-under-postselection. This fact and lemma 3 lead that a multiplicative approximation of the Ising partition functions is #P-hard for almost all imaginary coupling constants even on planar lattices with a bounded degree. □

The above result indicates that almost all imaginary Ising partition functions are substantially hard to calculate even in the approximated case with a multiplicative error. This result contrasts with the existence of a FPRAS in the ferromagnetic cases with magnetic fields shown by Jerrum and Sinclair [33] and antiferromagnetic cases on a sort of lattices shown by Sinclair, Srivastava, and Thurley [88]. In these cases, an exact calculation is #P-hard but its approximation with a multiplicative error is easy. On the other hand, as noted in lemma 3, #P-hardness associated with post-BQP = PP theorem is also holds in the approximated case automatically.

With the random magnetic fields, approximation of ferromagnetic Ising partition functions below a certain critical temperature belongs, under an approximation-preserving reduction, to a class #BIS, which is defined as a counting problem of the number of independent sets of a bipartite graph [59]. Moreover, it has been shown that a multiplicative approximation of antiferromagnetic Ising partition functions on d-regular graphs ($d \geqslant 3$) are NP-hard [61]. Compared with the complexity of these real Ising partition functions, the imaginary Ising partition functions seem to be much more intractable.

This result also contrasts with the recent studies on quantum computational complexity of Ising partition functions with imaginary coupling constants [2–5, 7, 67]. These quantum algorithms calculate the Ising partition functions or, more generally, Jones or Tutte polynomials with additive error ϵ in polynomial time of $1/\epsilon$:

$$|\mathcal{Z} - \mathcal{Z}_{\rm ap}| \leqslant \epsilon\Delta,$$

where $\mathcal{Z}$ and $\mathcal{Z}_{\rm ap}$ are true and approximated values respectively, and Δ is a certain algorithmic scale. Furthermore, it has been shown that such an additive approximation is as powerful as solving BQP-complete problems (i.e., BQP-hard). This implies that these quantum algorithms do a nontrivial task that would be intractable on a classical computer. However, these quantum algorithms seem not to achieve an efficient multiplicative approximation, since it is #P-hard as shown above.

7. Conclusion and discussion

We have investigated IQP by relating it with computational complexity of Ising partition functions with imaginary coupling constants and magnetic fields. We found classes of IQP that are classically simulatable at least in the weak sense (and almost in the strong sense). Specifically, the IQP circuits consisting only of 2D nearest-neighbor two-qubit commuting gates, namely planar-IQP, are classically simulatable. However, if single-qubit rotations are allowed, planar-IQP becomes universal-under-postselection, which are as powerful, with the help of postselection, as PP. Thus single-qubit rotations make a drastic change of the IQP circuits from almost strongly simulatable to not simulatable even in the weak sense, which stems from hardness of the Ising models under magnetic fields.

The classical simulatability of planar-IQP stems from the exact solvability of Ising models on planar lattices without magnetic fields. Both classical computational complexity of Ising models on nonplanar lattices [32, 73] and quantum computation complexity of MBQC on nonplanar surface codes [74] have been studied already.

While we did not addressed here, computational complexity of the IQP circuits consisting of two-qubit commuting gates with a nonplanar geometry is an intriguing future topic.

By considering strong simulation of IQP, we further explored hardness of a multiplicative approximation of the Ising partition functions. We have shown that a multiplicative approximation of Ising partition functions with almost all imaginary coupling constants is #P-hard even on planar lattices with a bounded-degree.

The results are relevant for the Ising models with imaginary parameters, which complements to the existing complexity results on those model with real parameters [32, 33, 62, 72]. The Ising models with real parameters are of prime importance in both computer science and physics. It would be intriguing to extrapolate the present results to the real parameters by using the correspondence between imaginary and real Ising partition functions shown in [7] (corollary 1), which allows us to compare preexisting classical complexity results with quantum one.

Acknowledgments

The authors thank S. Tamate for useful discussions. KF was supported by JSPS Grant-in-Aid for Research Activity Start-up 25887034. TM is supported by Tenure Track System by MEXT, Japan and KAKENHI 26730003 by JSPS.

Appendix A. Proofs of facts on the graph states

A.1. Proof of fact 1

Proof. We observe the effect of the measurement on the stabilizer operator K_i. If $i \neq k$ nor $i \neq \mathcal{N}_k$, the measurement does not make any effect on a stabilizer K_k, and hence the post-measurement state is stabilized by such a K_k. If $i = k$, K_i anticommutes with Z_k and hence does not stabilize the post-measurement state anymore. Instead, $(-1)^{m_k} Z_k$ stabilizes the post-measurement state $|m_k\rangle_k$, where $m_k = 0, 1$ is the measurement outcome. If $i \in \mathcal{N}_k$, we define a new stabilizer operator $K_i' = Z_k K_i$ such that K_k does not contain Z_k. The post-measurement state is stabilized by $(-1)^{m_k} K_i'$. Thus the graph state with the byproduct operator, $B_k^{m_k}|G'\rangle$, is the post-measurement state. (Note that $B_k^{m_k}$ anticommutes with K_i's for all i but commutes with K_is with $i \neq k$ and $i \notin \mathcal{N}$.) □

A.2. Proof of fact 2

Proof. By using the fact that

$$|G\rangle = \left(\prod_{j\in\mathcal{N}_k} \Lambda_{k,j}(Z)\right)|+\rangle_k |G\backslash k\rangle,$$

we can calculate the projection as follows:

$$\begin{aligned}
\langle\theta_{k,m_k}|_k|G\rangle &= \langle\theta_{k,m_k}|_k \left(\prod_{j\in\mathcal{N}_k} \Lambda(Z)_{kj}\right)|+\rangle_k |G\backslash k\rangle \\
&= \langle+|_k e^{i(\theta_k + m_k\pi/2)Z_k} H_k \left(\prod_{j\in\mathcal{N}_k} \Lambda(Z)_{kj}\right)|+\rangle_k |G\backslash k\rangle \\
&= \left[\cos(\theta_k + m_k\pi/2) I + i\sin(\theta_k + m_k\pi/2)\left(\prod_{j\in\mathcal{N}_k} Z_j\right)\right]|G\backslash k\rangle/\sqrt{2} \\
&= \exp\left[i(\theta_k + m_k\pi/2)\left(\prod_{j\in\mathcal{N}_k} Z_j\right)\right]|G\backslash k\rangle/\sqrt{2}.
\end{aligned}$$

□.

References

[1] Shor P W 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Annual Symp. on Foundations of Computer Science, FOCS '94* (Washington, DC: IEEE Computer Society) pp 124–34

[2] Aharonov D, Jones V and Landau Z 2009 A polynomial quantum algorithm for approximating the Jones polynomial *Algorithmica* **55** 395–421
[3] Aharonov D and Arad I 2006 The BQP-hardness of approximating the Jones polynomial arXiv:quant-ph/0605181
[4] Aharonov D, Arad I, Eban E and Landau Z 2007 Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane arXiv:quant-ph/0702008
[5] De las Cuevas G, Dür W, van den Nest M and Martin-Delgado M 2011 Quantum algorithms for classical lattice models *New J. Phys.* **13** 093021
[6] Iblisdir S, Cirio M, Boada O and Brennen G 2014 Low depth quantum circuits for ising models *Ann. Phys., NY* **340** 205–51
[7] Matsuo A, Fujii K and Imoto N 2014 Quantum algorithm for an additive approximation of ising partition functions *Phys. Rev.* A **90** 022304
[8] Bernstein E and Vazirani U 1993 Quantum complexity theory *Proc. 25th Annual ACM Symp. on Theory of Computing* (New York: ACM) pp 11–20
[9] Arora S and Barak B 2009 *Computational Complexity: A Modern Approach* 1st edn (New York: Cambridge University Press)
[10] Papadimitriou C H 1994 *Computational Complexity* (Reading, MA: Addison-Wesley)
[11] Aaronson S 2010 BQP and the polynomial hierarchy *Proc. 42nd ACM Symp. Theory of Computing, STOC '10* (New York: ACM) pp 141–50
[12] Turing A M 1936 On computable numbers, with an application to the Entscheidungsproblem *Proc. London Math. Soc.* **42** 230–65
[13] Church A 1932 A set of postulates for the foundation of logic *Ann. Math.* **33** 346–66
[14] Preskill J 2012 Quantum computing and the entanglement frontier arXiv:1203.5813
[15] Aaronson S and Arkhipov A 2011 The computational complexity of linear optics *Proc. 43rd Annual ACM Symp. Theory of Computing, STOC'11* (New York: ACM) pp 333–42
[16] Valiant L G 1979 The complexity of computing the permanent *Theor. Comput. Sci.* **8** 189–201
[17] Aaronson S 2011 A linear-optical proof that the permanent is# p-hard *Proc. R. Soc.* A **467** 3393–405
[18] Toda S 1991 PP is as hard as the polynomial-time hierarchy *SIAM J. Comput.* **20** 865–77
[19] van den Nest M 2010 Classical simulation of quantum computation, the Gottesman–Knill theorem, and slightly beyond *Quant. Inf. Comp.* **10** 0258–71
[20] Jozsa R and van den Nest M 2013 Classical simulation complexity of extended Clifford circuits arXiv:1305.6190
[21] Broome M A, Fedrizzi A, Rahimi-Keshari S, Dove J, Aaronson S, Ralph T C and White A G 2013 Photonic boson sampling in a tunable circuit *Science* **339** 794–8
[22] Spring J B *et al* 2013 Boson sampling on a photonic chip *Science* **339** 798–801
[23] Tillmann M, Dakić B, Heilmann R, Nolte S, Szameit A and Walther P 2013 Experimental boson sampling *Nat. Photon.* **7** 540–4
[24] Crespi A, Osellame R, Ramponi R, Brod D J, Galvão E F, Spagnolo N, Vitelli C, Maiorino E, Mataloni P and Sciarrino F 2013 Integrated multimode interferometers with arbitrary designs for photonic boson sampling *Nat. Photon.* **7** 545–9
[25] Carolan J *et al* 2014 On the experimental verification of quantum complexity in linear optics *Nat. Photon.* **8** 621–6
[26] Spagnolo N *et al* 2014 Experimental validation of photonic boson sampling *Nat. Photon.* **8** 615–20
[27] Bentivegna M *et al* 2015 Experimental scattershot boson sampling *Sci. Adv.* **1** e1400255
[28] Carolan J *et al* 2015 Universal linear optics *Science* **349** 711–6
[29] Shepherd D and Bremner M J 2009 Temporally unstructured quantum computation *Proc. R. Soc.* A **465** 1413–39
[30] Aaronson S 2005 Quantum computing, postselection, and probabilistic polynomial-time *Proc. R. Soc.* A **461** 3473–82
[31] Aaronson S and Arkhipov A 2013 Bosonsampling is far from uniform arXiv:1309.7460
[32] Barahona F 1982 On the computational complexity of Ising spin glass models *J. Phy. A: Math. Gen.* **15** 3241
[33] Jerrum M and Sinclair A 1993 Polynomial-time approximation algorithms for the ising model *SIAM J. Comput.* **22** 1087–116
[34] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
[35] Hein M, Dür W, Eisert J, Raussendorf R, van den Nest M and Briegel H 2006 Quantum computers, algorithms and chaos *Int. School of Physics Enrico Fermi* vol 162
[36] Kasteleyn P W 1961 The statistics of dimers on a lattice: I. The number of dimer arrangements on a quadratic lattice *Physica* **27** 1209–25
[37] Fisher M E 1966 On the dimer solution of planar ising models *J. Math. Phys.* **7** 1776
[38] Bremner M J, Jozsa R and Shepherd D J 2011 Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy *Proc. R. Soc.* A **467** 459–72
[39] Drucker A and de Wolf R 2011 Quantum proofs for classical theorems *Theory Comput. Libr. Grad. Surv.* **2** 1–54
[40] Kuperberg G 2009 How hard is it to approximate the Jones polynomial arXiv:0908.0512
[41] Hoban M J, Wallman J J, Anwar H, Usher N, Raussendorf R and Browne D E 2014 Measurement-based classical computation *Phys. Rev. Lett.* **112** 140505
[42] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis* California Institute of Technology
[43] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge university press)
[44] Knill E and Laflamme R 1998 Power of one bit of quantum information *Phys. Rev. Lett.* **81** 5672
[45] Han Y, Hemaspaandra L A and Thierauf T 1997 Threshold computation and cryptographic security *SIAM J. Comput.* **26** 59–78
[46] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation *50th Annual IEEE Symp. Foundations of Computer Science, 2009, FOCS'09* (Piscataway, NJ: IEEE) pp 517–26
[47] Morimae T and Fujii K 2013 Blind quantum computation protocol in which Alice only makes measurements *Phys. Rev.* A **87** 050301
[48] Beigel R, Reingold N and Spielman D 1995 Pp is closed under intersection *J. Comput. Syst. Sci.* **50** 191–202
[49] Knill E, Laflamme R and Milburn G J 2001 A scheme for efficient quantum computation with linear optics *Nature* **409** 46–52
[50] Ni X and van den Nest M 2013 Commuting quantum circuits: efficient classical simulations versus hardness results *Quantum Inf. Comput.* **13** 0054–72
[51] Bremner M J, Montanaro A and Shepherd D J 2016 Average-case complexity versus approximate simulation of commuting quantum computations *Phys. Rev. Lett.* **117** 080501
[52] Nakata Y and Murao M 2014 Diagonal quantum circuits: their computational power and applications *Eur. Phys. J. Plus* **129** 152
[53] Nakata Y and Murao M 2013 Diagonal-unitary 2-design and their implementations by quantum circuits *Int. J. Quantum Inf.* **11** 1350062
[54] Nakata Y, Koashi M and Murao M 2014 Generating a state t-design by diagonal quantum circuits *New J. Phys.* **16** 053043
[55] Sen P 2005 Random measurement bases, quantum state distinction and applications to the hidden subgroup problem *21st Annual IEEE Conf. Computational Complexity, 2006, CCC 2006* (Piscataway, NJ: IEEE) p 14

[56] Radhakrishnan J, Rötteler M and Sen P 2009 Random measurement bases, quantum state distinction and applications to the hidden subgroup problem *Algorithmica* **55** 490–516
[57] Dankert C, Cleve R, Emerson J and Livine E 2009 Exact and approximate unitary 2-designs and their application to fidelity estimation *Phys. Rev.* A **80** 012304
[58] Jerrum M and Sinclair A 1993 Polynomial-time approximation algorithms for the ising model *SIAM J. Comput.* **22** 1087–116
[59] Goldberg L A and Jerrum M 2007 The complexity of ferromagnetic ising with local fields *Comb. Probab. Comput.* **16** 43–61
[60] Zuckerman D 1996 On unapproximable versions of np-complete problems *SIAM J. Comput.* **25** 1293–304
[61] Sly A and Sun N 2012 The computational hardness of counting in two-spin models on d-regular graphs *2012 IEEE 53rd Annual Symp. Foundations of Computer Science FOCS* (Piscataway, NJ: IEEE) pp 361–9
[62] Goldberg L A and Guo H 2014 The complexity of approximating complex-valued ising and tutte partition functions arXiv:1409.5627
[63] Lidar D A and Biham O 1997 Simulating ising spin glasses on a quantum computer *Phys. Rev.* E **56** 3661
[64] Lidar D A 2004 On the quantum computational complexity of the ising spin glass partition function and of knot invariants *New J. Phys.* **6** 167
[65] Knill E and Laflamme R 2001 Quantum computing and quadratically signed weight enumerators *Inf. Process. Lett.* **79** 173–9
[66] Geraci J and Lidar D A 2010 Classical ising model test for quantum circuits *New J. Phys.* **12** 075026
[67] van den Nest M, Dür W, Raussendorf R and Briegel H J 2009 Quantum algorithms for spin models and simulable gate sets for quantum computation *Phys. Rev.* A **80** 052334
[68] van den Nest M, Dür W and Briegel H J 2007 Classical spin models and the quantum-stabilizer formalism *Phys. Rev. Lett.* **98** 117207
[69] van den Nest M, Dür W and Briegel H J 2008 Completeness of the classical 2d ising model and universal quantum computation *Phys. Rev. Lett.* **100** 110501
[70] Fujii K 2013 Quantum information and statistical mechanics: an introduction to frontier *Interdiscip. Inf. Sci.* **19** 1–15
[71] Master C P, Yamaguchi F and Yamamoto Y 2003 Efficiency of free-energy calculations of spin lattices by spectral quantum algorithms *Phys. Rev.* A **67** 032311
[72] De las Cuevas G and Cubitt T S 2016 Simple universal models capture all classical spin physics *Science* **351** 1180–3
[73] Istrail S 2000 Statistical mechanics, three-dimensionality and NP-completeness: I. Universality of intracatability for the partition function of the Ising model across non-planar surfaces *Proc. 32nd Annual ACM Symp. Theory of Computing STOC* (New York: ACM) pp 87–96
[74] Goff L and Raussendorf R 2012 Classical simulation of measurement-based quantum computation on higher-genus surface-code states *Phys. Rev.* A **86** 042301
[75] Kitaev A Y 2003 Fault-tolerant quantum computation by anyons *Ann. Phys., NY* **303** 2–30
[76] Bravyi S and Raussendorf R 2007 Measurement-based quantum computation with the toric code states *Phys. Rev.* A **76** 022304
[77] Valiant L G 2002 Quantum circuits that can be simulated classically in polynomial time *SIAM J. Comput.* **31** 1229–54
[78] Terhal B M and DiVincenzo D P 2002 Classical simulation of noninteracting-fermion quantum circuits *Phys. Rev.* A **65** 032325
[79] Knill E 2001 Fermionic linear optics and matchgates arXiv:quant-ph/0108033
[80] Jozsa R and Miyake A 2008 Matchgates and classical simulation of quantum circuits *Proc. R. Soc.* A **464** 3089–106
[81] Jozsa R, Kraus B, Miyake A and Watrous J 2010 Matchgate and space-bounded quantum computations are equivalent *Proc. R. Soc.* A **466** 809–30
[82] Fujii K and Tamate S 2016 Computational quantum-classical boundary of noisy commuting quantum circuits *Sci. Rep.* **6**
[83] Aharonov D, Kitaev A and Nisan N 1998 Quantum circuits with mixed states *Proc. 30th Annual ACM Symp. Theory of Computing STOC* (New York: ACM) pp 20–30
[84] Aharonov D and Ben-Or M 1997 Fault-tolerant quantum computation with constant error *Proc. 29th Annual ACM Symp. Theory of Computing STOC* (New York: ACM) pp 176–88
[85] Raussendorf R 2003 Measurement-based quantum computation with cluster states *PhD Thesis* Ludwig-Maximillians Universität München
[86] Nielsen M A and Dawson C M 2005 Fault-tolerant quantum computation with cluster states *Phys. Rev.* A **71** 042323
[87] Fujii K 2016 Noise threshold of quantum supremacy arXiv:1610.03632
[88] Sinclair A, Srivastava P and Thurley M 2012 Approximation algorithms for two-state anti-ferromagnetic spin systems on bounded degree graphs *Proc. 23rd Annual ACM-SIAM Symp. Discrete Algorithms SODA* (Philadelphia: SIAM) pp 941–53
[89] Gao X, Wang S-T and Duan L M 2017 Quantum Supremacy for Simulating a Translation-Invariant Ising Spin Model *Phys. Rev. Lett.* **118** 040502