Quantum Information and Statistical Mechanics: An Introduction to Frontier

Keisuke FUJII[1,2,3,*]

[1]*The Hakubi Center for Advanced Research, Kyoto University, Kyoto 606-8302, Japan*
[2]*Graduate School of Informatics, Kyoto 606-8501, Japan*
[3]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*

This is a short review on an interdisciplinary field of quantum information science and statistical mechanics. We first give a pedagogical introduction to the stabilizer formalism, which is an efficient way to describe an important class of quantum states, the so-called stabilizer states, and quantum operations on them. Furthermore, graph states, which are a class of stabilizer states associated with graphs, and their applications for measurement-based quantum computation are also mentioned. Based on the stabilizer formalism, we review two interdisciplinary topics. One is the relation between quantum error correction codes and spin glass models, which allows us to analyze the performances of quantum error correction codes by using the knowledge about phases in statistical models. The other is the relation between the stabilizer formalism and partition functions of classical spin models, which provides new quantum and classical algorithms to evaluate partition functions of classical spin models.

KEYWORDS: quantum information science, stabilizer formalism, statistical mechanics

1. Introduction

Quantum information science is a rapidly growing field of physics, which explores comprehensive understanding of extremely complex quantum systems. An ultimate goal is building quantum computer or quantum simulator, which outperform conventional high performance (classical) computing. To achieve this goal, there still exist a lot of problems to be overcome. One of the main obstacles is decoherence, i.e., loss of coherence, due to an undesirable interaction between environments. Without a fault-tolerant design, any promising computing scheme is nothing but pie in the sky. Actually it has been shown that NP-complete problems (even PSPACE-complete problems), which are though to be intractable in classical digital computer, can be solved in polynomial time by using analog computer that can perform $x + y$, $x - y$, xy, and $\lfloor x \rfloor$ for any two real numbers x and y [1, 2]. However, such an analog computer has not been realized so far, since unlimited-precision real numbers cannot be physically realizable. Fortunately, in quantum computation, we have a fault-tolerant theory [3–10], which guarantees an arbitrary accuracy of quantum computation as long as noise levels of elementary quantum gates are sufficiently smaller than a constant value, the so-called threshold value. Fault-tolerant quantum computation utilizes quantum error correction [3] to overcome decoherence, where we utilize many physical particles and classical processing to infer the error location. Another important problem for quantum computation is to identify the class of problems that can be solved by using quantum computer. Of course, we already have several quantum algorithms, Shor's factorization [11], Grover's search [12], etc., which outperform existing classical algorithms. However, these instances are not enough to understand the whole class of problems that quantum computer can solve, i.e., BQP problems, since they are, so far, not shown to be BQP-complete. Finding a good BQP-complete problem will lead us to a deeper understanding.

Interestingly, in both fault-tolerant quantum computing and finding new quantum algorithms, the idea of statistical mechanics has been applied, recently. One is a correspondence between quantum error correction and spin glass theory [13], where posterior probabilities in Bayesian inference problems for quantum error correction are mapped onto partition functions of spin glass theory. Thus the knowledge about phases in spin glass theory tells us the performance of quantum error correction codes [14–22]. Another is a relationship between overlaps (inner products) of quantum states and partition functions of statistical mechanical models [23–25]. Since the overlaps (inner products) can be estimated efficiently in quantum computer, this mapping gives us a new quantum algorithm to calculate the partition

functions. Are these correspondences between quantum information and statistical mechanics accidental or inevitable? At least there is one common idea behind them, stabilizer states or stabilizer formalism [26], which might be an important clew to bridge the two fields and find new things.

The stabilizer states are a class of quantum states, which takes quite important roles in quantum information processing. The stabilizer formalism provides an efficient tool to provide a class of quantum operations on stabilizer states. In this review, we give a pedagogical introduction to the stabilizer formalism. Then we review two interesting interdisciplinary topics between quantum information science and statistical mechanics: the correspondence between quantum error correction and spin glass theory and the relation between the stabilizer formalism and partition functions of statistical models.

The rest of the paper is organized as follows: In §2, we introduce quantum-bit and elementary gates (unitary matrices). In §3, we introduce the stabilizer formalism. In §4, we explain how to describe a class of unitary operations and measurements on the stabilizer states in the stabilizer formalism. In §5, we demonstrate utility of the stabilizer formalism on the graph states [27], which are also an important class of quantum states associated with mathematical graphs. Specifically, we explain how Pauli basis measurements transform the graph states. Furthermore, we also introduce a model of quantum computation, measurement-based quantum computation. In §6, we review the relation between quantum error correction codes and spin glass models. In the last part of §6, we also mention a route toward building a fault-tolerant quantum computer. In §7, we review the relation between the stabilizer formalism and partition functions of classical spin models. As an exercise, we also show a duality relation between two distinct spin models by using the stabilizer formalism. Section 8 is devoted to a conclusion.

2. Quantum Bit and Quantum Gates

In classical information science, the minimum unit of information is described by a binary digit or *bit*, which takes a value either 0 or 1. Its quantum counterpart is a quantum bit, so-called *qubit*. Qubit is defined as a superposition of two orthogonal quantum states $|0\rangle$ and $|1\rangle$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are arbitrary complex values satisfying $|\alpha|^2 + |\beta|^2 = 1$. An n-qubit state is described by

$$|\Psi\rangle = \sum_{i_1, i_2, \ldots, i_n} C_{i_1 i_2 \ldots i_n} |i_1 i_2 \ldots i_n\rangle, \tag{2.1}$$

where $|i_1 i_2 \ldots i_n\rangle \equiv |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$. Since time evolutions are given by unitary operators in quantum physics, gate operations for a single qubit can be given by 2×2 unitary matrices. The most fundamental gates are identity and Pauli operators:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The set of tensor products of the Pauli matrices on the n-qubit system $\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$ forms the n-qubit Pauli group $\mathscr{P}_n$. A Pauli operator $A \in \{X, Y, Z\}$ acting on the ith qubit is denoted by $A_i \equiv I_1 \otimes \cdots \otimes I_{i-1} \otimes A_i \otimes I_{i+1} \otimes \cdots \otimes I_n$.

In stead of the computational basis $\{|0\rangle, |1\rangle\}$, we may also choose different orthogonal bases:

$$\{|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, \ |-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}\}, \ \text{or} \ \{|+i\rangle \equiv (|0\rangle + i|1\rangle)/\sqrt{2}, \ |-i\rangle \equiv (|0\rangle - i|1\rangle)/\sqrt{2}\}.$$

The Hadamard and phase gates are defined as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

These gates transform the computational bases, $\{|0\rangle, |1\rangle\} \leftrightarrow \{|+\rangle, |-\rangle\}$ and $\{|+\rangle, |-\rangle\} \leftrightarrow \{|+i\rangle, |-i\rangle\}$, respectively. These X, Y, Z, H, and S gates are normalizers of the Pauli group and generate a group $\mathcal{C}_1$ of single-qubit Clifford gates. (That is, a Clifford gate, say $A \in \mathcal{C}_1$, transforms the single-qubit Pauli group onto itself under the conjugation $A[\cdot]A^\dagger$. For example, $HXH = Z$, $SXS^\dagger = Y$, and so on.) Since the single-qubit Clifford group is a discrete group, one cannot generate arbitrary single-qubit unitary operations. Fortunately, it has been known that the existence of a non-Clifford gate in addition to the Clifford gates is enough for an efficient construction of an arbitrary single-qubit gate with arbitrarily high accuracy according to the Kitaev–Solovay theorem [28]. A non-Clifford gate can be, for example, $\pi/8$ gate $U_{\pi/8} = e^{-i\pi Z/8}$.

Single-qubit gates are not enough for constructing an arbitrary n-qubit unitary matrix, and hence at least one two-qubit gate operation is inevitable. There are two famous two-qubit gates, controlled-NOT (CNOT) and controlled-Z (CZ) gates, which are given, respectively, by

$$\Lambda(X)_{c,t} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t, \quad \Lambda(Z)_{c,t} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes Z_t.$$

Here a controlled-A gate is denoted by $\Lambda(A)_{c,t}$, where the gate A acts on the state labeled by t conditioned on the state labeled by c. Thus these qubits c and t are called control and target qubits, respectively. These two two-qubit gates are

both Clifford gates, that is, $\Lambda(A)$ $(A = X, Z)$ transforms $\mathcal{P}_2$ onto itself under the conjugation $\Lambda(A)[\cdots]\Lambda(A)^\dagger$. For example, $\Lambda(X)_{c,t}X_c \otimes I_t\Lambda(X)_{c,t}^\dagger = X_c \otimes X_t$, $\Lambda(X)_{c,t}I_c \otimes Z_t\Lambda(X)_{c,t}^\dagger = Z_c \otimes Z_t$, $\Lambda(Z)_{c,t}X_c \otimes I_t\Lambda(Z)_{c,t}^\dagger = X_c \otimes Z_t$, and so on. It is known that an arbitrary unitary operation of n qubits can be constructed from these elementary gates $\{H, S, U_{\pi/8}, \Lambda(X)\}$ or $\{H, S, U_{\pi/8}, \Lambda(Z)\}$. Such a set of elementary unitary gates is called a *universal set*, which is an instruction set of quantum computer.

3. Stabilizer States

In general, a description of quantum states is difficult since it requires exponentially many parameters in the number of qubits as shown in Eq. (2.1). To understand such a complex quantum system, efficient tools to describe important classes of complex quantum systems are essential. The matrix-product-states (MPS) [29], projected-entangled-pair-states (PEPS) [30–32], and multiscale-entanglement-renormalization-ansatz (MERA) [33] are such examples. The stabilizer states are another important class of quantum states, which take important roles in quantum information processing.

Now we introduce the definition of stabilizer states and the stabilizer formalism [26]. We define a stabilizer group $\mathcal{S}$ of an n-qubit system as an Abelian subgroup of the n-qubit Pauli group that does not includes $-I$ as its element. In other words, all elements in the stabilizer group are commutable with each other and hermitian. For example, a set

$$\mathcal{S}_{\text{Bell}} = \{II, XX, ZZ, -YY\}$$

is a two-qubit stabilizer group, where $A \otimes B$ is denoted by AB for simplicity.

The stabilizer group $\mathcal{S}$ can be defined in terms of the maximum independent set of the stabilizer group, which we call stabilizer generators. Here independence is defined such that each element in the generator set cannot be expressed as a product of other elements in the generator set. The stabilizer group generated by a stabilizer generators $\{S_i\}$ is denoted by $\langle\langle\{S_i\}\rangle\rangle$. For example, the stabilizer group $\mathcal{S}_{\text{Bell}} = \{II, XX, ZZ, -YY\}$ can be written simply by $\langle XX, ZZ\rangle$. Any stabilizer group of n qubits can be defined if at most n stabilizer generators are given.

The stabilizer state is defined as a simultaneous eigenstate of all stabilizer elements with the eigenvalue $+1$. It is sufficient that the state is an eigenstate of all stabilizer generators:

$$S_i|\psi\rangle = |\psi\rangle \text{ for all stabilizer generators } S_i.$$

The dimension 2^d of the space spanned by the stabilizer states is calculated to be $2^d = 2^{n-k}$ with n and k being the number of qubits and stabilizer generators, respectively. This can be understood that the 2^n-dimensional space is divided into two orthogonal subspaces for each stabilizer generator.

For example, the stabilizer state defined by the stabilizer group $\mathcal{S}_{\text{Bell}} = \langle XX, ZZ\rangle$ is $(|00\rangle + |11\rangle)/\sqrt{2}$, which is a maximally entangled state of two qubits [34]. The maximally entangled state is a useful resource for teleporting an unknown quantum state between two separate sites, that is, quantum teleportation [35].

Another representative example of the stabilizer states is an n-qubit cat state,

$$|\text{cat}\rangle = \frac{1}{\sqrt{n}}(|00\ldots0\rangle + |11\ldots1\rangle),$$

whose stabilizer group is given by

$$\left\langle Z_1Z_2, \ldots, Z_{n-1}Z_n, \prod_{i=1}^{n} X_i \right\rangle,$$

where A_i indicates a Pauli operator $A \in \{X, Y, Z\}$ on the ith qubit. The cat state is a representative example of macroscopically entangled states. If one particle is determined whether it is $|0\rangle$ or $|1\rangle$, the superposition is completely destroyed.

4. Quantum Operations on Stabilizer States

Let us consider the action of a Clifford gate U on the stabilizer state $|\psi\rangle$ defined by a stabilizer group $\mathcal{S} = \langle\langle\{S_i\}\rangle\rangle$:

$$U|\psi\rangle = US_i|\psi\rangle = US_iU^\dagger U|\psi\rangle = S_i'U|\psi\rangle,$$

where $S_i' \equiv US_iU^\dagger$. This indicates that a state $U|\psi\rangle$ is an eigenstate of the operator S_i' with an eigenvalue $+1$ for all S_i'. Furthermore, since the Clifford group of unitary gates are normalizer of the Pauli group (and hence a Pauli product is transformed to another Pauli product under its conjugation), the group $\mathcal{S}' = \langle\langle\{S_i'\}\rangle\rangle$ is also a stabilizer group. That is, $U|\psi\rangle$ is the stabilizer state defined by the stabilizer group $\mathcal{S}'$. In this way, the action of U on the stabilizer state can be regarded by a map between the stabilizer groups. For example, a stabilizer group $\langle X_1I_2, I_1Z_2\rangle$ (the corresponding state is $|+\rangle_1|0\rangle_2$) is transformed to $\langle X_1X_2, Z_1Z_2\rangle$ (the corresponding state is $(|00\rangle + |11\rangle)/\sqrt{2}$) by $\Lambda(X)_{1,2}$.

The projective measurement of a hermitian Pauli product as an observable can also be described by a map between stabilizer groups as follows. Suppose A is an n-qubit hermitian Pauli product and $P_\pm = (I \pm A)/2$ are the corresponding

projection operators. Due to the projective measurement, a state $|\psi\rangle$ is projected to $P_+|\psi\rangle/\sqrt{\|P_+|\psi\rangle\|}$ or $P_-|\psi\rangle/\sqrt{\|P_-|\psi\rangle\|}$ with probabilities $\|P_\pm|\psi\rangle\|$. For simplicity, we consider the case with the measurement outcome $+$. There are three possibilities:

(i) A (or $-A$) is an element of the stabilizer group.

(ii) While A (or $-A$) does not belong to the stabilizer group, A is commutable with all elements of the stabilizer group.

(iii) At least one stabilizer operator does not commute with A.

In the case (i), the state does not change. In the case (ii), the stabilizer group for the post-measurement state is given by $\langle A, \{S_i\}\rangle$. That is, A is added to the generator set. In the case (iii), we can always choose a generator set $\langle S_1, S_2, \ldots, S_k\rangle$ ($k < n$) of the original stabilizer group such that A commutes with all generators $S_2, \ldots, S_k$ except for S_1. Then the stabilizer group of the post-measurement state is given by $\langle A, S_2, \ldots, S_k\rangle$. That is, in addition to adding A, S_1 is removed from the generator set.

5. Graph States

In this section, we exercise to use the stabilizer formalism. As an example of the stabilizer states, we use the most important subclass of stabilizer states, graph states [27]. A graph state is defined associated with a graph $G(V, E)$, where V and E are the sets of the vertices and edges, respectively. A qubit is located on each vertex of the graph. The stabilizer generator of the graph state $|\psi_G\rangle$ associated with a graph $G(V, E)$ is given by

$$K_i = X_i \prod_{j \in N_i} Z_j \text{ for all } i \in V,$$

where the neighbor $N_i := \{j | (i, j) \in E\}$ of vertex i indicates the set of vertices that are connected to vertex i on the graph.

Each stabilizer generator K_i is transformed to $X_i = UK_iU$ by $U = \prod_{(i,j) \in E} \Lambda(Z)_{i,j}$, where we aggressively used the fact that $\Lambda(Z)_{i,j} X_i I_j \Lambda(Z)_{i,j} = X_i Z_j$. This fact indicates that U transforms the stabilizer group from $\langle \{K_i\}_{i \in V}\rangle$ to $\langle \{X_i\}_{i \in V}\rangle$. The stabilizer state defined by the latter is $|+\rangle^{\otimes|V|}$ where $|V|$ is the number of the vertices. This implies that we can obtain the graph state $|\psi_G\rangle$ from the product state $|+\rangle^{\otimes|V|}$ as $|\psi_G\rangle = U|+\rangle^{\otimes|V|}$. Specifically, when the graphs are regular such as one-dimensional, square, hexagonal, and cubic lattices, the corresponding graph states are also referred to as cluster states [36]. It has been known that any stabilizer state is equivalent to a certain graph state up to local Clifford operations [27, 37]. However, the graph associated with a stabilizer state is not uniquely defined, since there exist local Clifford operations that change the associated graph. This property is called local complementarity of the graph states [27, 37].

Next we will see how Pauli basis measurements transform the graph states. Let us consider a one-dimensional graph state as shown in Figs. 1(a)–1(c). At first, we consider the Z basis measurement (projective measurement of the observable Z) on the ith qubit. The stabilizer group for the post-measurement state is given by

$$\langle \ldots, K_{i-1}, Z_i, K_{i+1}, \ldots \rangle,$$

since K_i does not commute with Z_i. After the projection, the ith qubit is $|0\rangle$ and hence decoupled with the other qubits. By rewriting the stabilizer generators, we obtain three decoupled stabilizer groups

$$\langle \ldots, Z_{i-2}X_{i-1}\rangle, \langle Z_i \rangle, \langle X_{i+1}Z_{i+2}, \ldots \rangle,$$

which means the graph is separated by the Z basis measurement as shown in Fig. 1(a).

Similarly, we consider the X-basis measurement. Since X_i does not commute with K_{i-1} and K_{i+1} but commutes with $K_{i-1}K_{i+1} = Z_{i-2}X_{i-1}X_{i+1}Z_{i+2}$, the stabilizer group for the post-measurement state is given by

$$\langle \ldots, Z_{i-2}X_{i-1}X_{i+1}Z_{i+2}, Z_{i-1}Z_{i+1}, \ldots \rangle, \langle X_i \rangle.$$

By performing the Hadamard gate H on the $(i-1)$th qubit, we obtain a new stabilizer group

$$\langle \ldots, Z_{i-2}Z_{i-1}X_{i+1}Z_{i+2}, X_{i-1}Z_{i+1}, \ldots \rangle, \langle X_i \rangle,$$

which indicates that the graph is transformed as shown in Fig. 1(b) up to the Hadamard gate. Instead of the $(i-1)$th qubit, we can obtain a similar result by performing the Hadamard gate on the $(i+1)$th qubit.

The final example is the Y-basis measurement. Since Y_i does not commute with K_{i-1}, K_i, and K_{i+1} but commutes with $K_{i-1}K_i = Z_{i-2}Y_{i-1}Y_iZ_{i+1}$, and $K_iK_{i+1} = Z_{i-1}Y_iY_{i+1}Z_{i+2}$, the stabilizer group for the post-measurement state is given by

$$\langle \ldots, Z_{i-2}Y_{i-1}Z_{i+1}, Z_{i-1}Y_{i+1}Z_{i+2}, \ldots \rangle, \langle Y_i \rangle.$$

By performing the phase gates S on the $(i-1)$th and $(i+1)$th qubits, we obtain a new stabilizer group

$$\langle \ldots, Z_{i-2}X_{i-1}Z_{i+1}, Z_{i-1}X_{i+1}Z_{i+2}, \ldots \rangle, \langle Y_i \rangle.$$
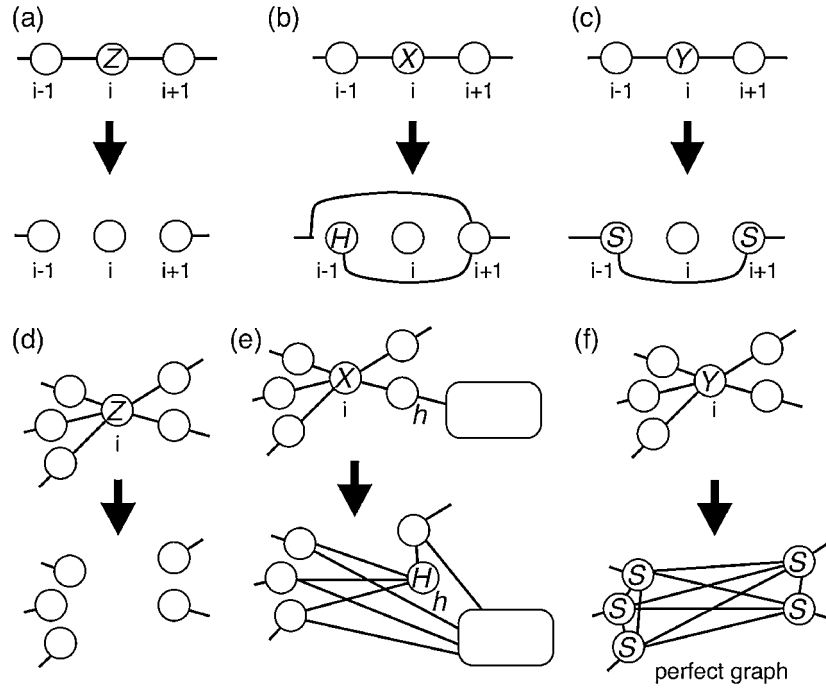
Fig. 1. The transformations of graph states by the Pauli basis measurements. (a) The Z-basis measurement on a one-dimensional graph state. (b) The X-basis measurement on a one-dimensional graph state. H indicates the Hadamard gate. (c) The Y-basis measurement on a one-dimensional graph state. Ss indicates the phase gates. (d) The Z-basis measurement on a general graph state. The edges incident to the ith (measured) qubit is removed. (e) The X-basis measurement on a general graph state. A qubit h is chosen from the set V_i of qubits connected to the ith (measured) qubit. All edges connected to the ith qubit are removed, and the edges between $V_i \setminus h$ and h and between $V_i \setminus h$ and vertices which are connected with h (shown by a blank box) are added. In addition, the H gate is performed on the hth qubit. For arbitrary choices of $h \in V_i$, the associated graph states, which are equivalent up to local Clifford gates with each other, are defined. (f) The Y-basis measurement on a general graph state. All edges connected to the ith qubit are removed. Instead, a complete graph of the vertices V_i adjacent to the ith (measured) qubits is added. In addition, the S gates are performed on the qubits belonging to V_i.

This indicates that the graph is directly connected up to the phase gates as shown in Fig. 1(c).

The actions of the Pauli basis measurements for general graph structures can be also calculated in a similar manner as shown in Figs. 1(d)–1(f), where no loop is included for clarity, but their extensions to arbitrary graphs are straightforward.

The graph states take important roles in quantum information processing [27]. First of all, graph states defined on a certain class of graphs, such as square and hexagonal lattices, can be used for resources for measurement-based quantum computation (MBQC) [38–41]. This can be understand as follows. The circuit in Fig. 2(a) is well-known quantum teleportation [35], where a Bell pair $(|00\rangle + |11\rangle)/\sqrt{2}$ is prepared as a resource, and the unknown input state is teleported into the output up to a Pauli byproduct depending on the measurement outcomes. This circuit is equivalent to that in Fig. 2(b), which reads X-basis measurements on a graph state transfer the input state to the output state. Here we should recall that a graph state is generated by CZ gates from $|+\rangle^{\otimes n}$. The measurement-based identity gate can be decomposed into two Hadamard gates, one of which is shown in Fig. 2(c). By measuring in the X-basis after $Z(\theta) \equiv e^{-i\theta Z/2}$, a unitary transformation $HZ(\theta)$ can be performed in a teleportation-based way as shown in circuit equivalences in Fig. 2(d). The Pauli byproduct made due to the probabilistic nature of measurements has to be always placed at the top of the output state to handle the nondeterminism. However, $Z(\theta)$ does not commute with the Pauli byproduct if it contains the Pauli X operator, i.e., $Z(\theta)X = XZ(-\theta)$. To settle this, the measurement angle θ is adaptively changed to $-\theta$ beforehand according to the previous measurement outcomes, which is called feedforward in MBQC.

By using commutability of CZ gates as shown in Fig. 2(e), the CZ gate performed for the output of teleportation can be moved into the offline graph state preparation. This trick is the so-called quantum gate teleportation [42]. In this way, an arbitrary single qubit rotation and the CZ gate, which are sufficient for universal quantum computation, can be implemented by adaptive measurements on a specific type of graph state Starting from, for example, a two-dimensional (2D) cluster state on a square lattice, we can generate an arbitrary graph state required for universal quantum computation by using Pauli basis measurements mentioned before. Roughly speaking, the universality of measurement-based quantum computation means that by performing measurements in appropriately chosen bases $\{|\alpha_i\rangle\}$, the output of a quantum computation $U|0\rangle^{\otimes n}$ of n qubits can be simulated as
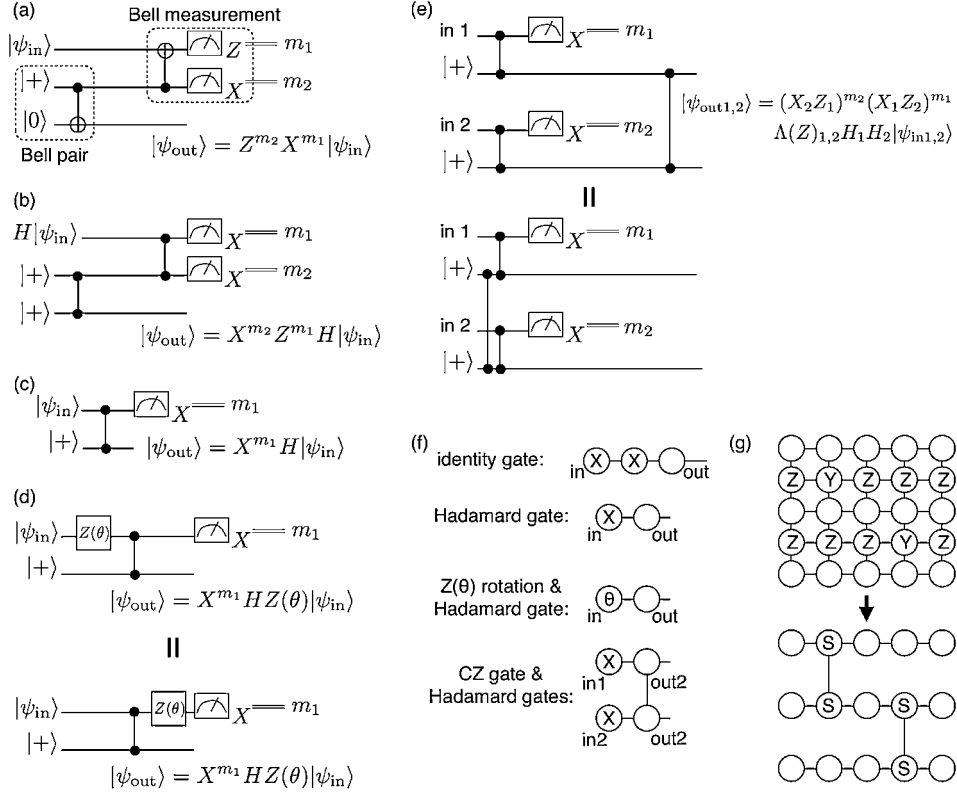
Fig. 2. (a) A circuit for quantum teleportation [35]. The two-qubit gates are the CNOT gates, where the control and target qubits are denoted by black and white circles, respectively. (b) An equivalent circuit of (a), which consists of the CZ gates. The Hadamard gates come from the equivalence $\Lambda(X)_{c,t} = H_t \Lambda(Z)_{c,t} H_t$. (c) A minimum unit of teleportation-based gate, which transforms the input state to the output with the Hadamard operation. (d) The circuit equivalence for the $HZ(\theta)$ operation. The measurement in the X basis after the $Z(\theta)$ rotation teleports the output state with the $HZ(\theta)$ operation up to a Pauli byproduct. (e) The CZ gate for the output states (upper circuit) can be moved into the generation of a graph state (lower circuit), where the commutability of CZ gates is utilized. (f) Graph diagrams of MBQC. From top to bottom, they describe the identity gate (b), the Hadamard gate (c), the $Z(\theta)$ rotation followed by the Hadamard gate (d), and the teleportation-based CZ gate followed by the Hadamard gates (e). (g) A graph state required for quantum computation is generated from the 2D cluster state on a square lattice by using Pauli basis measurements.

$$U|0\rangle^{\otimes n} = 2^{(|V|-n)/2} \left(\bigotimes_{i \in V \setminus \text{output } n \text{ qubits}} \langle \alpha_i| \right) |\psi_G\rangle. \tag{5.1}$$

Such a state, which allows universal quantum computation in a measurement-based way, is called universal resource. Recently, MBQC on more general many-body quantum states has been proposed [43, 44], which utilizes MPS and PEPS as resources. MBQC on ground or thermal states of valence-bond-solid systems have been proposed [45–51], which might be useful to relax experimental difficulties in preparations of universal resources for quantum computation.

6. Quantum Error Correction Codes and Spin Glass Models

In the following two sections, we will review the interdisciplinary topics between quantum information science and statistical mechanics. In this section, we describe the correspondence between quantum error correction codes and spin glass models.

Quantum error correction [3] is one of the most successful schemes to handle errors on quantum states originated from an undesirable interaction with environments. Quantum error correction codes employ multiple physical qubits to encode logical information into a subspace, so-called *code space*. The stabilizer formalism is vital to describe such a complex quantum system. Below we will describe one of the most important quantum error correction codes, the surface code [13, 52], which has a close relation to a spin glass model, the random-bond Ising model (RBIM).

The surface code on the square lattice consists of qubits located on edges $i \in E$ of the square lattice [13, 52] (note that the location of qubits is different from that of the graph states). Specifically, we consider a periodic boundary condition, that is, the surface code on a torus. The face and vertex stabilizer operators of the surface code are defined for each face $f \in F$ and vertex $v \in V$ as
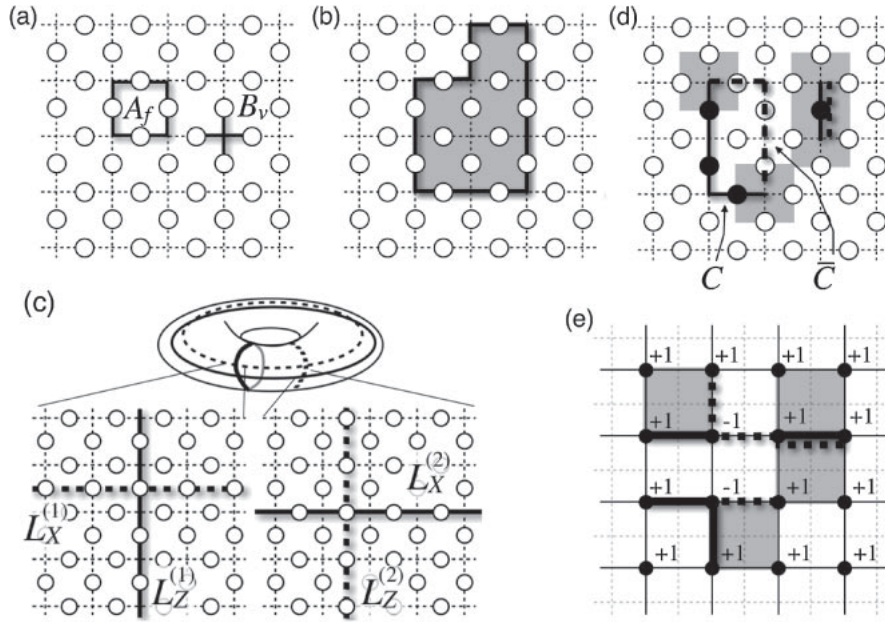
Fig. 3. (a) The vertex and face stabilizer operators. (b) A trivial cycle. The product of the Pauli Z operators on a trivial cycle is equivalent to the product of face stabilizer generators inside the cycle, and hence it belongs to the stabilizer group. (c) Two pairs of the logical operators, $L_X^{(1)}$ (left dotted line), $L_Z^{(1)}$ (left solid line), $L_X^{(2)}$ (right dotted line), and $L_Z^{(2)}$ (right solid line). (d) The black circles and solid lines denote a chain C of Z errors. The vertices with $b_v = -1$ are denoted by gray squares. The estimated chain $\bar{C}$ of errors for a recovery is shown by dotted lines. If $C + \bar{C}$ is a trivial cycle, the error correction succeeds. Otherwise if $C + \bar{C}$ is a nontrivial cycle, it changes the code space nontrivially. (e) RBIM on the dual lattice. The error chain C corresponds to the locations of antiferromagnetic interactions. The recovery chain $\bar{C}$ corresponds to the excited domain wall. The vertices with $b_v = -1$ correspond to Ising vortexes. At zero temperature, a spin configuration is chosen so that the length of excited domain wall is minimum, i.e., MWPM of the Ising vortexes (or frustrations).

$$A_f = \prod_{i \in E_f} Z_i, \text{ and } B_v = \prod_{j \in E_v} X_j,$$

respectively [see Fig. 3(a)]. Here E_f and E_v ($E_{f,v} \subset E$) indicate the sets of four edges that are surrounding the face f and are adjacent to the vertex v, respectively. The code state $|\Psi\rangle$ is defined as the simultaneous eigenstate of all stabilizer operators with the eigenvalue $+1$:

$$|\Psi\rangle = A_f|\Psi\rangle, \ |\Psi\rangle = B_v|\Psi\rangle \text{ for all } f, v.$$

As will be seen below, the eigenvalues of these stabilizer operators are used to diagnose syndromes of errors.

The logical information encoded in the code space is defined by those operators that are commutable with all elements in the stabilizer group but are independent from them. Such operators characterize the degrees of freedom in the degenerated code space and hence called *logical operators*. The products of Zs on any trivial cycle of the lattice are commutable with stabilizer operators. But they are also elements of the stabilizer group, since they are written by the product of all A_fs inside the trivial cycle as shown in Fig. 3(b). This is also the case for the products of Xs on any trivial cycle of the dual lattice. The products of Zs (Xs) on nontrivial cycles wrapping around the torus on the primal (dual) lattice give the logical operators, which we denote by L_Z (L_X). Since the genus of the torus is one, we can find two pairs of logical operators ($L_X^{(1)}, L_Z^{(1)}$) and ($L_X^{(2)}, L_Z^{(2)}$) on the torus as shown in Fig. 3(c). Note that the actions of the logical operators on the code space depend only on the homology class of the logical operators. Since these logical operators are subject to the Pauli commutation relation $L_X^{(i)} L_Z^{(j)} = -\delta_{ij} L_Z^{(j)} L_X^{(i)}$ and $(L_A^{(i)})^2 = I$, they represent two logical qubits encoded in the code space. In general, a surface code defined on a surface of a genus g can encode $2g$ logical qubits.

Let us consider how errors appear on the code state. We, for simplicity, consider the Pauli operators X (bit-flip error) and Z (phase-flip error) act on the code state with an identical and independent distribution. However, possibility of correcting these two types of errors guarantees the validity under a general noise model. While, in the following, we only consider how to correct Z (phase-flip) errors for clarity, it is straightforward to correct X (bit-flip) errors in the same manner. Suppose a chain of Z errors occur on the set C of the qubits [see Fig. 3(d)]. The code state is given by $|\Psi'\rangle = \prod_{i \in E} Z_i^{u_i^C} |\Psi\rangle$, where $u_i^C = 1$ if $i \in C$ and $u_i^C = 0$ if $i \notin C$. Due to the errors, the state $|\Psi'\rangle$ is not in the code space anymore. If $|E_v \cap C|$ is odd,

$$B_v|\Psi'\rangle = -\left(\prod_{i \in E} Z_i^{u_i^C}\right) B_v|\Psi\rangle = -|\Psi'\rangle$$

and hence the eigenvalue of the vertex stabilizer B_v is flipped to -1. The error syndrome of a chain C of Z errors is defined as a set of eigenvalues $\{b_v = \pm 1\}$ of the vertex stabilizers $\{B_v\}$. Similarly the error syndrome of X errors is defined as a set of eigenvalues $\{a_f = \pm 1\}$ of the face stabilizers $\{A_f\}$. The eigenvalues $b_v = -1$ are obtained at the boundaries ∂C [grayed squares in Fig. 3(d)] of the error chain C, since the vertex stabilizers anticommute with the error chain there. In order to recover from the errors, we infer the most likely error operator $\bar{C}_{\mathrm{ML}}$ which has the same error syndromes as C, i.e., $\partial \bar{C}_{\mathrm{ML}} = \partial C$. If $C + \bar{C}_{\mathrm{ML}}$ becomes a trivial cycle the error correction succeeds, since it acts on the code space trivially as a face stabilizer operator. Otherwise, if the chain $C + \bar{C}_{\mathrm{ML}}$ becomes a nontrivial cycle, the operator $\prod_{i \in E} Z_i^{C + \bar{C}_{\mathrm{ML}}}$ is a logical operator. Thus the recovery operation destroys the original logical information, meaning a failure of the error correction.

Suppose errors occur with an independent and identical probability p. (Note that p is a parameter in the posterior probability of the inference problem, and hence can be different from the actual error probability p'.) The error probability of an error chain $\bar{C}$ conditioned on the $\partial \bar{C} = \partial C$ becomes

$$P(\bar{C}|\partial \bar{C} = \partial C) = \mathcal{N} \prod_i \left(\frac{p}{1-p} \right)^{u_i^{\bar{C}}} \Bigg|_{\partial \bar{C} = \partial C} = \mathcal{N}' \exp\left[-\beta J \sum_i (2u_i^{\bar{C}} - 1) \right]\Bigg|_{\partial \bar{C} = \partial C} \tag{6.1}$$

where $\mathcal{N}$ and $\mathcal{N}'$ are the normalization factors, $e^{-\beta J} \equiv \sqrt{p/(1-p)}$. The most likely error operator $\bar{C}_{\mathrm{ML}}$ conditioned on the syndrome ∂C can be obtained by maximizing the posterior probability:

$$\bar{C}_{ML} = \arg \max_{\bar{C}} P(\bar{C}|\partial \bar{C} = \partial C) = \arg \min_{\bar{C}} \sum_i u_i^{\bar{C}}|_{\partial \bar{C} = \partial C}.$$

This indicates that the most likely chain $\bar{C}_{\mathrm{ML}}$ is an error chain that connects pairs of two boundaries with a minimum Manhattan length. Such a problem can be efficiently solved in classical computer by using the Edmonds' minimum-weight-perfect-matching (MWPM) algorithm [53]. The accuracy threshold with the decoding by the MWPM algorithm has been estimated to be 10.3% (MWPM) [14].

The MWPM algorithm is not optimal for the present purpose, since we have to take not only the probability of each error $\bar{C}$ but also the combinatorial number of the error chains $\bar{C}$ such that $\bar{C} + C$ belongs to the same homology class (recall that the action of logical operators on the code state depends only on the homology class of the associated chains). By taking a summation over such a $\bar{C}$ that belongs to the same homology class, we obtain a success probability of the error correction

$$p_{\mathrm{suc}} = \mathcal{N}'' \sum_{\bar{C}+C=\text{trivial cycles}} \exp\left[\beta J \sum_i v_i^{\bar{C}} \right],$$

where $v_i^{\bar{C}} = -2u_i^{\bar{C}} + 1$ is defined. In order to simplify the summation over trivial cycles, we introduce an Ising spin $\sigma_i \in \{+1, -1\}$ on each face center (i.e., vertex of the dual lattice) of the lattice [see Fig. 3(e)]. If $\bar{C} + C$ a trivial cycle, there exists a configuration $\{\sigma_i\}$ such that $v_i^{\bar{C}} = v_l^C \sigma_i \sigma_j$ with l being the bond between the spins σ_i and σ_j. The variable v_l located on the bond in-between the sites i and j is denoted by v_{ij} hereafter. By using this fact, the success probability can be reformulated as

$$p_{\mathrm{suc}} = \mathcal{N}''' \sum_{\{\sigma_i\}} \exp\left[\beta \sum_{\langle ij \rangle} J_{ij} \sigma_i \sigma_j \right],$$

where $\mathcal{N}'''$ is a normalization factor, and $J_{ij} \equiv J v_{ij}^C$.

Now that the relation between quantum error correction and a spin glass model becomes apparent; the success probability of the Z error correction is nothing but the appropriately normalized partition function of the RBIM, whose Hamiltonian is given by $H = -\sum_{\langle ij \rangle} J_{ij} \sigma_i \sigma_j$. The location of Z errors represented by $J_{ij} = -1$ corresponds to the anti-ferromagnetic interaction due to disorder, whose probability distribution is given by $P(J_{ij}) = (1 - p')\delta(J_{ij} - 1) + p'\delta(J_{ij} + 1)$. (Recall that the hypothetical error probability p is given independently of the actual error probability p'.) The error syndrome $b_v = -1$ corresponds to the frustration of Ising interactions [see Fig. 3(e)]. Equivalently it is also the end point (Ising vortex) of the excited domain wall.

In order to storage quantum information reliably, the success probability has to be reduced exponentially by increasing the system size. This is achieved with an error probability p' below a certain value, so-called *accuracy threshold* p^{th}. However, if the error probability is higher than it, the success probability converges to a constant value. This drastic change on the function p_{suc} corresponds to a phase transition of the RBIM. Specifically, in the ferromagnetic phase, quantum error correction succeeds. [Actually the logical error probability is related to the domain-wall free-energy via $-(1/\beta) \ln p_{\mathrm{suc}}$. In the ferromagnetic phase, the domain-wall free-energy scales like $O(N)$ with N being the vertical or horizontal dimension of the system. This supports the exponential suppression of logical errors.] Of course, we should take $p = 1/(e^{2\beta} + 1) = p'$, that is, the actual and hypothetical error probabilities are the same, in order to perform a better error correction. This condition corresponds to the Nishimori line [54] on the (β, p)

phase diagram. The precise value of the optimal threshold has been calculated to be 10.9% [15], which is fairly in good agreement with the numerical estimation [55]. The threshold value 10.3% with the MWPM algorithm corresponds to the critical point at zero temperature, since the solution of the MWPM algorithm is obtained in the $\beta \to \infty$ limit.

Recently the surface codes have been also studied on general lattices including random lattices [15–19]. Furthermore, the performance analyses in the presence of qubit-loss error have been also argued [17, 20–22], which corresponds to bond dilution in the RBIM.

The surface code is one example of topological stabilizer codes, whose stabilizer operators are local (i.e., finite-body Pauli products) and translation invariant. A complete classification of topological stabilizer codes is obtained in Ref. [56]. Another well-studied example of topological stabilizer codes is the color codes [57, 58], which are related to the random three-body Ising models. The performance of the color codes has been also discussed via the spin glass theory [59, 60].

An important issue in quantum error correction, where the knowledge of statistical mechanics seems to be quite useful, is finding a fast classical decoding algorithm. Recently several new efficient algorithms have been proposed [62–64]. They are based on a renormalization group algorithm [62], local search [63], and parallel tempering [64], each of which is well studied in statistical mechanics.

In fault-tolerant quantum computation, we have to take all sources of errors into account, such as imperfections in syndrome measurements. Thus, in fault-tolerant quantum computation the code performances under perfect syndrome measurements are of limited interest. For both surface and color codes, their performances have been investigated under imperfect syndrome measurements [13, 14, 61]. Interestingly, the inference problems of errors in them are mapped into three-dimensional random $\mathbf{Z}_2$ gauge theories. Recently, topologically protected measurement-based quantum on the symmetry breaking thermal state has been proposed [65]. This model is mapped into a correlated random-plaquette $\mathbf{Z}_2$ gauge model, whose critical point on the Nishimori line is shown to be equivalent to that of the three-dimensional Ising model.

More comprehensive studies of fault-tolerant quantum computation has been taken by considering errors in state initializations, measurements, and elementary gate operations used in both quantum error correction itself and universal quantum computation on the code space [66–69]. Based on these analyses, physical implementations and quantum architecture designs have been argued recently [70–78], which clarify the experimental requirements for building fault-tolerant quantum computer. On the other side, extensive experimental resources have been paid to achieve these requirements, and very encouraging results have already obtained in some experiments, for example, in trapped ions [79, 80] and superconducting systems [81, 82]. Finding a high performance quantum error correction code, an efficient classical algorithm for decoding, and a detailed analysis of an architecture under a realistic situation will further help an experimental realization of large scale quantum computer.

7. Statistical Models and Stabilizer Formalism

In this section, we describe a mapping between the stabilizer formalism and classical statistical models [24, 25], which allows us to analyze classical statistical models via quantum information and vice versa. More precisely, we will relate an overlap $\langle \alpha | \Psi_G \rangle$ of a product state $|\alpha\rangle \equiv \prod_i |J_i\rangle$, which will be defined later in detail, and a graph state $|\Psi_G\rangle$ to a partition function $\mathcal{Z}(\beta)$ of a spin model associated with interactions J_i:

$$\mathcal{Z}(\beta) = \frac{1}{2^{|V_1|/2}} \langle \alpha | \Psi_G \rangle,$$

where $|V_1|$ denotes the number of sites in the spin model. Since the right hand side can be efficiently evaluated by using quantum computer, the overlap mapping gives us an algorithm to calculate the partition functions. Below we explain a derivation of the overlap mapping in detail.

We consider a classical statistical model on a lattice L:

$$H = \sum_i J_i s_i + \sum_{\langle i,j \rangle} J_{i,j}(s_i \oplus s_j) + \sum_{\langle i,j,k \rangle} J_{i,j,k}(s_i \oplus s_j \oplus s_k) + \cdots + \sum_{\langle i_1,i_2,\ldots,i_m \rangle} J_{i_1,i_2,\ldots,i_m} \left(\bigoplus_{j=1}^m s_{i_j} \right),$$

where $s_i \in \{0, 1\}$ is the ith Ising spin variable, $J_{i_1,i_2,\ldots,i_m}$ is the coupling constant for the m-body interaction on i_1th, ..., and i_mth spins, and $\bigoplus$ indicates the addition modulo 2. We can choose any lattices and interaction geometries as shown in Fig. 4. Let us denote the number of j-body interactions by n_j. Specifically, n_1 is the number of sites. Next we relate the classical statistical model to another graph. This graph consists of m sets of vertices, V_j ($j = 1, \ldots, m$), each of which has n_j vertices. The total number of vertices on the graph is denoted by $n \equiv \sum_{j=1}^m n_m$. The set V_1 and V_j ($j \neq 1$) represent information about the sites and the j-body interactions, respectively. The graph associated with the classical model on a lattice L, which we call the mediated graph, is defined such that if there is a j-body interaction among the sites i_1, i_2, ..., and i_j, the corresponding vertices in V_1 and V_j are connected as shown in Fig. 4. Then we consider the graph state on the mediated graph. By using the definition given in §5, the mediated graph state $|\psi_G\rangle$ can be written by
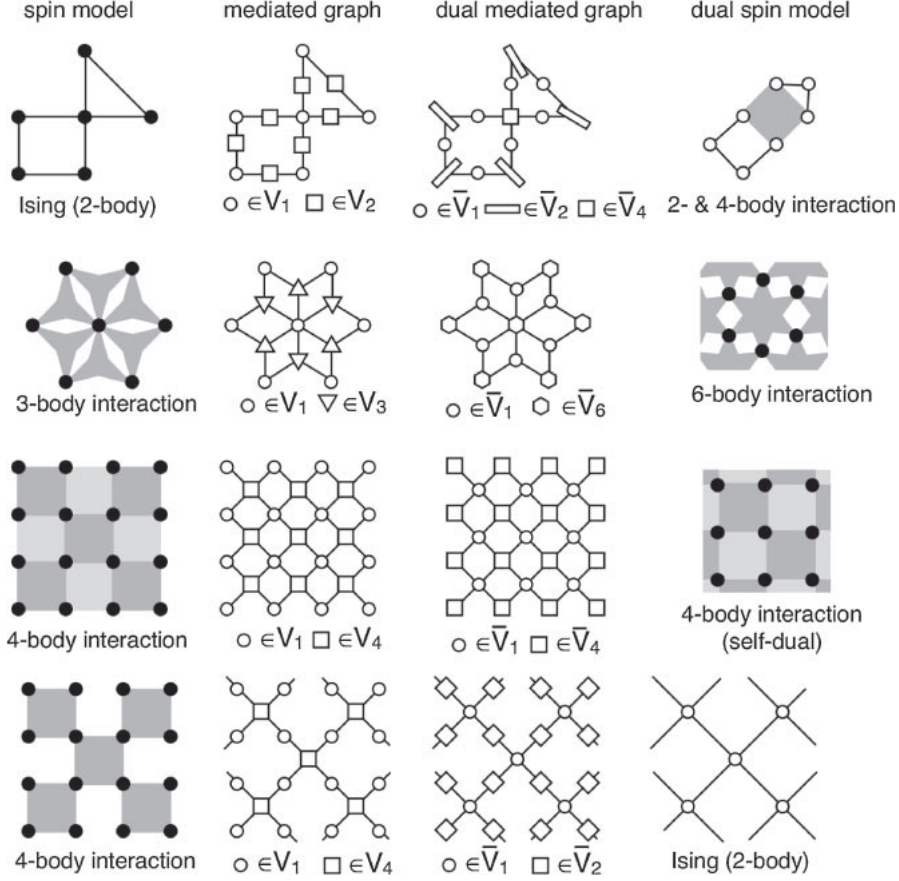
Fig. 4.   From left to right, spin models, corresponding mediated graph states, dual mediated graph states, and dual spin models. In the mediated graph states, circles indicate the qubits representing sites of spin models. The magnetic fields are given by a product state defined on these site qubits. The polygons indicate the qubits, which mediate the many-body interactions. The number of the edges of each polygon is equivalent to the number of spins engaged in the corresponding interaction. The coupling strengths of the many-body interactions are determined by a product state defined on these mediating qubits.

$$|\psi_G\rangle = \prod_{(i,j)\in E} \Lambda(Z)_{i,j}|+\rangle^{\otimes n} \Leftrightarrow \left(\prod_{i\in\bigcup_{j=2}^m V_j} H_i\right)|\psi_G\rangle = \prod_{(i,j)\in E \text{ where } i\in n_1} \Lambda(X)_{i,j}|+\rangle^{\otimes|V_1|}|0\rangle^{\otimes n-n_1}$$

$$= \frac{1}{2^{n_1/2}} \sum_{\{s_i\}} \bigotimes_i |s_i\rangle \bigotimes_{\langle i,j\rangle} |s_i \oplus s_j\rangle \otimes \cdots \bigotimes_{\langle i_1,...,i_m\rangle} \left|\bigoplus_{j=1}^m s_{i_j}\right\rangle$$

where we used that facts that $H_j\Lambda(Z)_{i,j}H_j = \Lambda(X)_{i,j}$ and $|+\rangle = H|0\rangle$. The summation $\sum_{\{s_i\}}$ is taken over all configurations of $\{s_i\}$. The mediated graph state does not have any information about the coupling constants. Thus we define a product state $\bigotimes_i |J_i\rangle \bigotimes_{\langle i,j\rangle} |J_{ij}\rangle \otimes \cdots \otimes \bigotimes_{\langle i_1,...,i_m\rangle} |J_{i_1,...,i_m}\rangle$, where $|J\rangle \equiv |0\rangle + e^{-\beta J}|1\rangle$. Then we take the inner product between the mediated graph state with Hadamard gates and the product state:

$$\bigotimes_{i\in V_1}\langle J_i| \bigotimes_{\langle i,j\rangle\in V_2} \langle J_{ij}| \otimes \cdots \otimes \bigotimes_{\langle i_1,...,i_m\rangle\in V_m} \langle J_{i_1,...,m}| \left(\prod_{i\in\bigcup_{j=2}^m V_j} H_i\right)|\psi_G\rangle = \frac{1}{2^{|V_1|/2}} \sum_{s_i} e^{-\beta H} = \frac{1}{2^{|V_1|/2}} Z(\beta). \qquad (7.1)$$

This is the Van den Nest–Dür–Briegel (VDB) overlap mapping obtained in Refs. [24, 25] (an extension to q-state spin models is straightforward [25]). The VDB overlap mapping has a great potential to understand both quantum information and statistical mechanics. First of all, the overlap between the product and graph states can be regarded as an MBQC as given in Eq. (5.1). Thus VDB overlap mapping helps us to find a new quantum algorithm that calculates partition functions [83–85]. If a spin model with an appropriately chosen lattice geometry and coupling constants allows universal MBQC, evaluation of the corresponding partition function is BQP-complete, that is, as hard as any problem that quantum computer can solve. Furthermore, by using universality of MBQC, we can relate different statistical models [25, 86–88]. For example, the partition functions of all classical spin models are equivalent to those of the 2D Ising models with appropriately chosen complex coupling constants and magnetic fields on polynomially enlarged lattices [25, 89]. On the other hand, if a quantum computation is related to an exactly solvable model, the

corresponding quantum computation is classically simulatable [83]. MBQC on certain types of graphs, such as tree graphs, has been known to be classically simulatable [40, 41, 90]. This also provides a good classical algorithm to evaluate the partition function [83].

Very recently, another overlap mapping has been developed in Ref. [91], which has the following forms:

$$\mathcal{Z}_{3-\text{Ising}} = \frac{1}{2^{|V_1|}} \langle \Psi_{\text{color}} | A | \Psi_{\text{color}} \rangle.$$

The left hand side is a partition function of an Ising model with only three-body interactions. In the right hand side, $|\Psi_{\text{color}}\rangle$ is the color code states [57, 58], and $A \equiv \bigotimes_i (ZS^\dagger H D_i H S)$ with D_i being a 2×2 diagonal matrix. In comparison with the VDB overlap mapping, the mapping Eq. (7.1) improves the scale factor exponentially. Since the overlap $\langle \Psi_{\text{color}} | A | \Psi_{\text{color}} \rangle$ is the mean value of an observable A with respect to $|\Psi_{\text{color}}\rangle$, its evaluation can be easily obtained in quantum computer. Furthermore, the overlap can be rewritten as

$$\langle \Psi_{\text{color}} | A | \Psi_{\text{color}} \rangle = \langle \Psi | \bigotimes_i D_i | \Psi \rangle,$$

where $|\Psi\rangle$ is a stabilizer state. Recently, it has been found that the right hand side can be simulated efficiently in classical computer with a polynomial overhead, which uses classically simulatability of a restricted type of quantum computation, i.e., Clifford circuit [92]. This provides an efficient classical algorithm, taking a detour, to evaluate partition functions of three-body Ising models.

As a final topic, we demonstrate a duality relation between two classical spin models by using the VDB overlap mapping. We define a set of vertices $\bar{V}_j := \{i | i \in V_1 \text{ and connected to } j \text{ vertices on the mediated graph}\}$ and $\bar{V}_1 = V_2 \cup \cdots \cup V_m$. Then, Eq. (7.1) is reformulated as

$$\bigotimes_{\langle i,j \rangle \in \bar{V}_2} f_{i,j} \langle \tilde{J}_{i,j} | \cdots \bigotimes_{\langle i_1, \ldots, i_j \rangle \in \bar{V}_j} f_{i_1, \ldots, i_j} \langle \tilde{J}_{i_1, \ldots, i_j} | \bigotimes_{i \in \bar{V}_1} f_i \langle \tilde{J}_i | \left(\prod_{i \in \bigcup_{j=2}^m \bar{V}_j} H_i \right) | \psi_G \rangle$$

$$= \frac{1}{2^{|\bar{V}_1|/2}} \prod_{i \in \bar{V}_1} f_1 \prod_{\langle i,j \rangle \in \bar{V}_2} f_{i,j} \cdots \prod_{\langle i_1, \ldots, i_m \rangle \in \bar{V}_m} f_{i_1, \ldots, i_m} \tilde{Z}(\beta). \qquad (7.2)$$

Here we defined $f_{i_1, \ldots, i_j} \langle \tilde{J}_{i_1, \ldots, i_j} | = \langle J_{k(i_1, \ldots, i_j)} | H$ with site $k(i_1, \ldots, i_j) \in V_1$ being connected to sites $i_1, \ldots, i_j$, and $f_{\bar{k}(i_1, \ldots, i_j)} \langle \tilde{J}_{\bar{k}(i_1, \ldots, i_j)} | = \langle J_{i_1, \ldots, i_j} | H$ with site $\bar{k}(i_1, \ldots, i_j) \in \bar{V}_1$ being connected to sites $i_1, \ldots, i_j$, where $f_{i_1, \ldots, i_j}$ and $f_{\bar{k}(i_1, \ldots, i_j)}$. These $\tilde{J}_{i_1, \ldots, i_j}$, $f_{i_1, \ldots, i_j}$, $\tilde{J}_{\bar{k}(i_1, \ldots, i_j)}$, and $f_{\bar{k}(i_1, \ldots, i_j)}$ are specifically given by

$$e^{-\beta \tilde{J}_{i_1, \ldots, i_j}} = \tanh(\beta J_{k(i_1, \ldots, i_j)}/2), \quad f_{i_1, \ldots, i_j} = (1 + e^{-\beta J_{k(i_1, \ldots, i_j)}})/\sqrt{2},$$

$$e^{-\beta \tilde{J}_{\bar{k}(i_1, \ldots, i_j)}} = \tanh(\beta J_{i_1, \ldots, i_j}/2), \quad f_{\bar{k}(i_1, \ldots, i_j)} = (1 + e^{-\beta J_{i_1, \ldots, i_j}})/\sqrt{2}.$$

Up to the constant factor, R.H.S. of Eq. (7.2) reads the partition function of the dual model, which corresponds to the mediated graph with the set of vertices $\bar{V}_j$ (see Fig. 4 for examples). For example, the two-body Ising model with magnetic fields on the square lattice is the dual of the four-body Ising model of a checker board type with magnetic fields as shown in Fig. 4 (the forth row). A four-body Ising model on all plaquettes with magnetic fields is self-dual as shown in Fig. 4 (the third row). While we only considered the duality relations between spin models on two dimensions here, it is straightforward to extend them to general cases.

8. Conclusion

In this review, we give a pedagogical introduction for the stabilizer formalism. Then we review two interdisciplinary topics, the relations between the surface code and the RBIM, and the mapping between the stabilizer formalism and the partition function of classical spin models. Both of two are quite important topics in quantum information science; one provides a basis for building fault-tolerant quantum computer, the other provides a new quantum algorithm to evaluate the partition functions of statistical mechanical models.

These topics mentioned here are a small fraction of interdisciplinary fields between quantum information science and statistical mechanics, or more generally, condensed matter physics. The coding theory based on the stabilizer quantum error correction codes provides an important clew to understand topological order [52, 93]. There is a quantum algorithm that calculates the Jones and Tutte polynomials [94–96], which are equivalent to the partition functions of Potts models with complex coupling constants. It has been shown that the class of additive approximations of Jones or Tutte polynomials at certain complex points within specific algorithmic scales is BQP-complete. There is a classically simulatable class of quantum computation, the so-called match gates [97–100], which is based on the exact solvability of free-fermion systems. Here we did not addressed quantum annealing [101] or adiabatic quantum computation [102], where a ground state configuration of a statistical mechanical model is obtained by adiabatically changing parameters of another quantum Hamiltonian. The quantum annealing or adiabatic quantum computation are thought to be easy for

a physical implementation [103], while there are still ongoing debates [104] on whether or not the current experimental quantum annealing [103] utilizes genuine quantumness. The adiabatic model has been shown to be equivalent to the standard model of quantum computation in an ideal situation [105, 106]. However, the equivalence in an ideal situation does not mean that a fault-tolerant theory in one model automatically ensures fault-tolerance in the other model. Thus fault-tolerance of the adiabatic model against all sources of experimental imperfections has to be addressed [107, 108].

The correspondences between quantum information science and other fields including statistical mechanics are continuing to be discovered, and the complete understanding of both fields in the same language is being obtained. The interdisciplinary interactions will further deepen understanding of both fields of physics, and will lead us to an emerging new field.

Acknowledgments

REFERENCES

[1] Aaronson, S., "NP-complete problems and physical reality," *ACM SIGACT News*, **36**: 30–52 (2005).
[2] Schönhage, A., "On the power of random access machines," *Proc. Intl. Colloquium on Automata, Languages, and Programming*, 520–529 (1979).
[3] Shor, P. W., "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, **52**: R2493–R2496 (1995).
[4] DiVincenzo, D. P., and Shor, P. W., "Fault-tolerant error correction with efficient quantum codes," *Phys. Rev. Lett.*, **77**: 3260–3263 (1996).
[5] Kitaev, A. Yu., "Quantum computations: Algorithms and error correction," *Russ. Math. Surv.*, **52**: 1191–1245 (1997).
[6] Preskill, J., "Reliable quantum computers," *Proc. R. Soc. London, Ser. A*, **454**: 385–410 (1998).
[7] Knill, E., Laflamme, R., and Zurek, W. H., "Resilient quantum computation: Error models and thresholds," *Proc. R. Soc. London, Ser. A*, **454**: 365–384 (1998).
[8] Knill, E., Laflamme, R., and Zurek, W. H., "Resilient quantum computation," *Science*, **279**: 342–345 (1998).
[9] Aharonov, D., and Ben-Or, M., "Fault-tolerant quantum computation with constant error rate," *Proc. 29th Annu. ACM Symp. Theor. Comput.*, **176–188**: (1998).
[10] Aharonov, D., and Ben-Or, M., "Fault-tolerant quantum computation with constant error rate," *SIAM J. Comput.*, **38**: 1207–1282 (2008).
[11] Shor, P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 124–134 (1994).
[12] Grover, L. K., "A fast quantum mechanical algorithm for database search," *Proc. ACM STOC*, 212–219 (1996).
[13] Dennis, E., Kitaev, A., Landhal, A., and Preskill, J., "Topological quantum memory," *J. Math. Phys.*, **43**: 4452 (2002).
[14] Wang, C., Harrington, J., and Preskill, J., "Confinement-Higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory," *Ann. Phys.*, **303**: 31–58 (2003).
[15] Ohzeki, M., "Locations of multicritical points for spin glasses on regular lattices," *Phys. Rev. E*, **79**: 021129 (2009).
[16] Röthlisberger, B., Wootton, J. R., Heath, R. M., Pachos, J. K., and Loss, D., "Incoherent dynamics in the toric code subject to disorder," *Phys. Rev. A*, **85**: 022313 (2012).
[17] Fujii, K., and Tokunaga, Y., "Error and loss tolerances of surface codes with general lattice structures," *Phys. Rev. A*, **86**: 020303 (2012).
[18] Ohzeki, M., and Fujii, K., "Duality analysis on random planar lattices," *Phys. Rev. E*, **86**: 051121 (2012).
[19] Al-Shimary, A., Wootton, J. R., and Pachos, J. K., "Lifetime of topological quantum memories in thermal environment," arXiv:12092940 (2012).
[20] Stace, T. M., Barrett, S. D., and Doherty, A. C., "Thresholds for topological codes in the presence of loss," *Phys. Rev. Lett.*, **102**: 200501 (2009).
[21] Stace, T. M., and Barrett, S. D., "Error correction and degeneracy in surface codes suffering loss," *Phys. Rev. A*, **81**: 022317 (2010).
[22] Ohzeki, M., "Error threshold estimates for surface code with loss of qubits," *Phys. Rev. A*, **85**: 060301 (2012).
[23] Bravyi, S., and Raussendorf, R., "Measurement-based quantum computation with the toric code states," *Phys. Rev. A*, **76**: 022304 (2007).
[24] Van den Nest, M., Dür, W., and Briegel, H. J., "Classical spin models and the quantum-stabilizer formalism," *Phys. Rev. Lett.*, **98**: 117207 (2007).
[25] Van den Nest, M., Dür, W., and Briegel, H. J., "Completeness of the classical 2D Ising model and universal quantum computation," *Phys. Rev. Lett.*, **100**: 110501 (2008).
[26] Gottesman, "Stabilizer codes and quantum error correction," Ph.D. thesis, California Institute of Technology (1997).
[27] Hein, M., Dür, W., Eisert, J., Raussendorf, R., Van den Nest, M., and Briegel, H.-J., "Entanglement in graph states and its applications," *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy, July*, 115–218 (2006).
[28] Kitaev, A., "Quantum computations: Algorithms and error correction," *Russ. Math. Surv.*, **52:61**: 1191–1249 (2002).
[29] Fannes, M., Nachtergaele, B., and Werner, R. F., "Finitely correlated states on quantum spin chains," *Commun. Math. Phys.*, **144**: 443–490 (1992).
[30] Verstraete, F., Wolf, M. M., Perez-Garcia, D., and Cirac, J. I., "Criticality, the area law, and the computational power of

projected entangled pair states," *Phys. Rev. Lett.*, **96**: 220601 (2006).

[31] Verstraete, F., Cirac, J. I., and Murg, V., "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems," *Adv. Phys.*, **57**: 143–224 (2008).

[32] Cirac, J. I., and Verstraete, F., "Renormalization and tensor product states in spin chains and lattices," *J. Phys. A: Math. Theor.*, **42**: 504004 (2009).

[33] Vidal, G., "Entanglement renormalization," *Phys. Rev. Lett.*, **99**: 220405 (2007).

[34] Einstein, A., Podolsky, B., and Rosen, N., "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, **47**: 777–780 (1935).

[35] Bennett, C. H., Brassard, G., Crëpeau, C., Jozsa, R., Peres, A., and Wootters, W. K., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, **70**: 1895–1899 (1993).

[36] Briegel, H. J., and Raussendorf, R., "Persistent entanglement in arrays of interacting particles," *Phys. Rev. Lett.*, **86**: 910–913 (2001).

[37] Van den Nest, M., Dehaene, J., and De Moor, B., "Graphical description of the action of local Clifford transformations on graph states," *Phys. Rev. A*, **69**: 022316 (2004).

[38] Raussendorf, R., and Briegel, H. J., "A one-way quantum computer," *Phys. Rev. Lett.*, **86**: 5188–5191 (2001).

[39] Raussendorf, R., Browne, D. E., and Briegel, H. J., "Measurement-based quantum computation on cluster states," *Phys. Rev. A*, **68**: 022312 (2003).

[40] Van den Nest, M., Miyake, A., Dür, W., and Briegel, H. J., "Universal resources for measurement-based quantum computation," *Phys. Rev. Lett.*, **97**: 150504 (2006).

[41] Van den Nest, M., Miyake, A., Dür, W., and Briegel, H. J., "Fundamentals of universality in one-way quantum computation," *New J. Phys.*, **9**: 204 (2007).

[42] Gottesman, D., and Chuang, I. L., "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, **402**: 390–393 (1999).

[43] Gross, D., and Eisert, J., "Novel schemes for measurement-based quantum computation," *Phys. Rev. Lett.*, **98**: 220503 (2007).

[44] Gross, D., and Eisert, J., "Measurement-based quantum computation beyond the one-way model," *Phys. Rev. A*, **76**: 052315 (2007).

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

[46] Cai, J., Miyake, A., Dür, W., and Briegel, H. J., "Universal quantum computer from a quantum magnet," *Phys. Rev. A*, **82**: 052309 (2010).

[47] Bartlett, S. D., Brennen, G. K., Miyake, A., and Renes, J. M., "Quantum computational renormalization in the Haldane phase," *Phys. Rev. Lett.*, **105**: 110502 (2010).

[48] Miyake, A., "Quantum computational capability of a 2D valence bond solid phase," *Ann. Phys.*, **326**: 1656–1671 (2011).

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

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

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

[52] Kitaev, A., "Fault-tolerant quantum computation by anyons," *Ann. Phys.*, **303**: 2–30 (2003).

[53] Edmonds, J., "Paths, trees, and flowers," *Can. J. Math.*, **17**: 449–467 (1965).

[54] Nishimori, H., Statistical Spin Glasses and Information Processing: An Introduction, Oxford University Press (2001).

[55] Merz, F., and Chalker, J. T., "Two-dimensional random-bond Ising model, free fermions, and the network model," *Phys. Rev. B*, **65**: 054425 (2002).

[56] Yoshida, B., "Classification of quantum phases and topology of logical operators in an exactly solved model of quantum codes," *Ann. Phys.*, **326**: 15–95 (2011).

[57] Bombin, H., and Martin-Delgado, M. A., "Topological quantum distillation," *Phys. Rev. Lett.*, **97**: 180501 (2006).

[58] Bombin, H., and Martin-Delgado, M. A., "Topological computation without braiding," *Phys. Rev. Lett.*, **98**: 160502 (2007).

[59] Ohzeki, M., "Accuracy thresholds of topological color codes on the hexagonal and square-octagonal lattices," *Phys. Rev. E*, **80**: 011141 (2009).

[60] Bombin, H., Andrist, R. S., Ohzeki, M., Katzgraber, H. G., and Martin-Delgado, M. A., "Strong resilience of topological codes to depolarization," *Phys. Rev. X*, **2**: 021004 (2012).

[61] Andrist, R. S., Katzgraber, H. G., Bombin, H., and Martin-Delgado, M. A., "Tricolored lattice gauge theory with randomness: Fault tolerance in topological color codes," *New J. Phys.*, **13**: 083006 (2011).

[62] Duclos-Cianci, G., and Poulin, D., "Fast decoders for topological quantum codes," *Phys. Rev. Lett.*, **104**: 050504 (2010).

[63] Fowler, A. G., Whiteside, A. C., and Hollenberg, L. C. L., "Towards practical classical processing for the surface code," *Phys. Rev. Lett.*, **108**: 180501 (2012).

[64] Wootton, J. R., and Loss, D., "High threshold error correction for the surface code," *Phys. Rev. Lett.*, **109**: 160503 (2012).

[65] Fujii, K., Nakata, Y., Ohzeki, M., and Murao, M., "Measurement-based quantum computation on symmetry breaking thermal states," *Phys. Rev. Lett.*, **110**: 120502 (2013).

[66] Raussendorf, R., Harrington, J., and Goyal, K., "A fault-tolerant one-way quantum computer," *Ann. Phys.*, **321**: 2242–2270 (2006).

[67] Raussendorf, R., and Harrington, J., "Fault-tolerant quantum computation with high threshold in two dimensions," *Phys. Rev. Lett.*, **98**: 190504 (2007).

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

[69] Landahl, A. J., Anderson, J. T., and Rice, P. R., "Fault-tolerant quantum computing with color codes," arXiv:1108.5738 (2011).

[70] Van Meter, R., Ladd, T. D., Fowler, A. G., and Yamamoto, Y., "Distributed quantum computation architecture using semiconductor nanophotonics," *Int. J. Quant. Inf.*, **8**: 295–323 (2010).

[71] Li, Y., Barrett, S. D., Stace, T. M., and Benjamin, S. C., "Fault tolerant quantum computation with nondeterministic gates," *Phys. Rev. Lett.*, **105**: 250502 (2010).

[72] Fujii, K., and Tokunaga, Y., "Fault-tolerant topological one-way quantum computation with probabilistic two-qubit gates," *Phys. Rev. Lett.*, **105**: 250503 (2010).

[73] Jones, N. C., *et al.*, "Layered architecture for quantum computing," *Phys. Rev. X*, **2**: 031007 (2012).

[74] Fujii, K., Yamamoto, T., Koashi, M., and Imoto, N., "A distributed architecture for scalable quantum computation with realistically noisy devices," arXiv:1202.6588 (2012).

[75] Li, Y., and Benjamin, S. C., "High threshold distributed quantum computing with three-qubit nodes," *New J. Phys.*, **14**: 0930008 (2012).

[76] Nickerson, N. H., Li, Y., and Benjamin, S. C., "Topological quantum computing with a very noisy network and local error rates approaching one percent," *Nature Comm.*, **4**: 1756 (2013).

[77] Ghosh, J., Fowler, A. G., and Geller, M. R., "Surface code with decoherence: An analysis of three superconducting architectures," *Phys. Rev. A*, **86**: 062318 (2012).

[78] Fowler, A. G., Mariantoni, M., Martinis, J. M., and Cleland, A. N., "Surface codes: Towards practical large-scale quantum computation," *Phys. Rev. A*, **86**: 032324 (2012).

[79] Benhelm, J., Kirchmair, G., Christian, F. R., and Blatt, B., "Towards fault-tolerant quantum computing with trapped ions," *Nature Phys.*, **4**: 463–466 (2008).

[80] Schindler, P., *et al.*, "Experimental repetitive quantum error correction," *Science*, **332**: 1059–1061 (2011).

[81] Chow, J. M., *et al.*, "Universal quantum gate set approaching fault-tolerant thresholds with superconducting qubits," *Phys. Rev. Lett.*, **109**: 060501 (2012).

[82] Reed, M. D., *et al.*, "Realization of three-qubit quantum error correction with superconducting circuits," *Nature*, **482**: 382–385 (2012).

[83] Van den Nest, M., Dür, W., Raussendorf, R., and Briegel, H. J., "Quantum algorithms for spin models and simulable gate sets for quantum computation," *Phys. Rev. A*, **80**: 052334 (2009).

[84] De las Cuevas, G., Dür, W., Van den Nest, M., and Martin-Delgado, M. A., "Quantum algorithms for classical lattice models," *New J. Phys.*, **13**: 093021 (2011).

[85] Iblisdir, S., Cirio, M., Boada, O., and Brennen, G. K., "Low depth quantum circuit for Ising models," arXiv:1208.3918 (2012).

[86] De las Cuevas, G., Dür, W., Briegel, H. J., and Martin-Delgado, M. A., "Unifying all classical spin models in a lattice gauge theory," *Phys. Rev. Lett.*, **102**: 230502 (2009).

[87] De las Cuevas, G., Dür, W., Briegel, H. J., and Martin-Delgado, M. A., "Mapping all classical spin models to a lattice gauge theory," *New J. Phys.*, **12**: 043014 (2010).

[88] Xu, Y., De las Cuevas, G., Dür, W., Briegel, H. J., and Martin-Delgado, M. A., "The U(1) lattice gauge theory universally connects all classical models with continuous variables, including background gravity," *J. Stat. Mech.*, **2011**: P02013 (2011).

[89] Karimipour, V., and Zarei, M. H., "Algorithmic proof for the completeness of the two-dimensional Ising model," *Phys. Rev. A*, **86**: 052303 (2012).

[90] Van den Nest, M., Dür, W., Vidal, G., and Briegel, H. J., "Classical simulation versus universality in measurement-based quantum computation," *Phys. Rev. A*, **75**: 012337 (2007).

[91] Van den Nest, M., and Dür, W., "Ising models and topological codes: Classical algorithms and quantum simulation," arXiv:1304.2879 (2013).

[92] Van den Nest, M., "Simulating quantum computers with probabilistic methods," *Quant. Inf. Comp.*, **11**: 784–812 (2011).

[93] Yoshida, B., "Feasibility of self-correcting quantum memory and thermal stability of topological order," *Ann. Phys.*, **326**: 2566–2633 (2011).

[94] Aharonov, D., Jones, V., and Landau, Z., "A polynomial quantum algorithm for approximating the Jones polynomial," arXiv:quant-ph/0511096 (2005).

[95] Aharonov, D., and Arad, I., "The BQP-hardness of approximating the Jones polynomial," arXiv:quant-ph/0605181 (2006).

[96] Aharonov, D., Arad, I., Eban, E., and Landau, Z., "Polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane," arXiv:quant-ph/0702008 (2007).

[97] Valiant, L., "Quantum circuits that can be simulated classically in polynomial time," *SIAM J. Comput.*, **31**: 1229–1254 (2002).

[98] Terhal, B., and DiVincenzo, D., "Classical simulation of nonintercating-fermion quantum circuits," *Phys. Rev. A*, **65**: 032325 (2002).

[99] Jozsa, R., and Miyake, A., "Matchgates and classical simulation of quantum circuits," *Proc. R. Soc. London, Ser. A*, **464**: 3089–3106 (2008).

[100] Jozsa, R., Kraus, B., Miyake, A., and Watrous, J., "Matchgate and space-bounded quantum computations are equivalent," *Proc. R. Soc. London, Ser. A*, **466**: 809–830 (2010).

[101] Kadowaki, T., and Nishimori, H., "Quantum annealing in the transverse Ising model," *Phys. Rev. E*, **58**: 5355–5363 (1998).

[102] Farhi, E., *et al.*, "A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem,"

Science, **292**: 472–475 (2001).

[103] Boixo, S., *et al.*, "Quantum annealing with more than one hundred qubits," arXiv:1304.4595 (2013).

[104] Smolin, J. A., and Smith, G., "Classical signature of quantum annealing," arXiv:1305.4904 (2013).

[105] Aharonov, D., *et al.*, "Adiabatic quantum computation is equivalent to standard quantum computation," *Proc. 45th Annu. Symp. Found. Comput. Sci.*, 42–51 (2004).

[106] Aharonov, D., *et al.*, "Adiabatic quantum computation is equivalent to standard quantum computation," *SIAM J. Comput.*, **37**: 166–194 (2007).

[107] Childs, A. M., Farhi, E., and Preskill, J., "Robustness of adiabatic quantum computation," *Phys. Rev. A*, **65**: 012322 (2001).

[108] Lidar, D. A., "Towards fault tolerant adiabatic quantum computation," *Phys. Rev. Lett.*, **100**: 160506 (2008).