Quantum computing for power systems: tutorial, review, challenges, and prospects

Hualong Liu*, Wenyuan Tang
Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695, USA

Abstract

As a large number of renewable energy resources are connected to power systems, the operation, planning, and optimization of power systems have been becoming more and more complex. Power flow calculation, unit commitment, economic dispatch, energy pricing, and power system planning are essentially computation problems. A lot of computing resources are required for these problems, which are non-trivial, especially for large-scale power systems with the high penetration of renewable energy. Traditionally, the calculation and optimization of power systems are completed by classical computers based on the classical computing theory and the von Neumann architecture. However, with Moore's law getting closer and closer to the limit, the importance of quantum computing has become increasingly prominent. Quantum computing has been applied to some fields to a certain extent, yet the utilization of quantum computing in power systems is rare. As the power industry is the foundation of the national economy, introducing quantum computing into the power system has far-reaching and crucial significance, such as improving the penetration of renewable energy, enhancing the computing efficiency, and helping in achieving the goal of net zero and climate neutrality by 2050. This paper first introduces the core concepts, essential ideas and theories of quantum computing, and then reviews the existing literature on the applications of quantum computing in power systems, and puts forward our critical thinking about the application of quantum computing in power systems. In brief, this paper is dedicated to a tutorial on quantum computing targeting power system professionals and a review of its applications in power systems. The main contributions of this paper are: (1) introduce quantum computing into the field of power engineering in a thoroughly detailed way and delineate the analysis methodologies of quantum circuits systematically without losing mathematical rigor; (2) based on Dirac's notation, the related formulae are derived meticulously with sophisticated schematic diagrams; (3) elaborate and derive some critical quantum algorithms in depth, which will play an important role in power systems; (4) critically summarize and comment on the existing literature on applications of quantum computing in power systems; (5) the future applications and challenges of quantum computing in power systems are prospected and remarked.

Index Terms

quantum computing, optimization, power systems, renewable energy, climate neutrality.

I. Introduction

A. Why the Interest in Quantum Computing?

BECAUSE quantum computing has shown exponential acceleration compared with classical computing under certain conditions, Moore's law is getting closer and closer to the limit, the only correct descriptions which work on the extremely small scale are quantum, and real quantum computers are becoming more and more accessible to the public, quantum computing has been attracting the researcher. All the reasons above have led to the rapid development of quantum computing both in theory and in practice in recent years. Quantum computing has been applied in such some fields of science and engineer as finance, chemistry, and biology. However, there are rare applications of quantum computing in power systems.

There are many problems in the field of power systems, such as optimization and power flow calculation, which require a lot of calculation and a certain computation speed. Therefore, it is essential to introduce quantum computing into the field of power systems.

B. Why do We Write This Paper? (Motivation for This Contribution)

There are many references [1]–[5] on quantum computing, but they are lengthy for power system engineers and researchers to get started with quantum computing. For this reason, this paper introduces quantum computing in a concise and illustrated way without needing profound and obscure physical knowledge. In other words, the introduction of quantum computing in this paper is specially tailored for power system professionals.

C. Organization of the Paper

Firstly, this paper will systematically detail the relevant background knowledge of quantum computing and the analysis methodologies of quantum circuits and some significant quantum algorithms in an illustrated way. Secondly, we review the existing literature on the applications of quantum computing in power systems, put forward our critical thinking about the literature, and give the challenges and prospects for the future work about the applications of quantum computing in power systems. This paper will equip you with the basics that you will need for studying the applications of quantum computing in power systems.

The rest of the paper is arranged as follows. The basic concepts of linear vector spaces and Dirac's notation are elaborated in section II. Section III introduces the fundamental framework of quantum mechanics. Section IV expounds fundamental quantum gates and the analysis methodologies of quantum circuits minutely. In Section V, relevant, important quantum algorithms are described and derived in detail, which will play an important role in power systems. Section VI reviews and comments on the existing literature on the applications of quantum computing in power systems with critical and creative thinking. Section VII presents challenges and prospects for the future work. Conclusions follow in Section VIII. The logical architecture of the entire paper is given in Fig. 1.

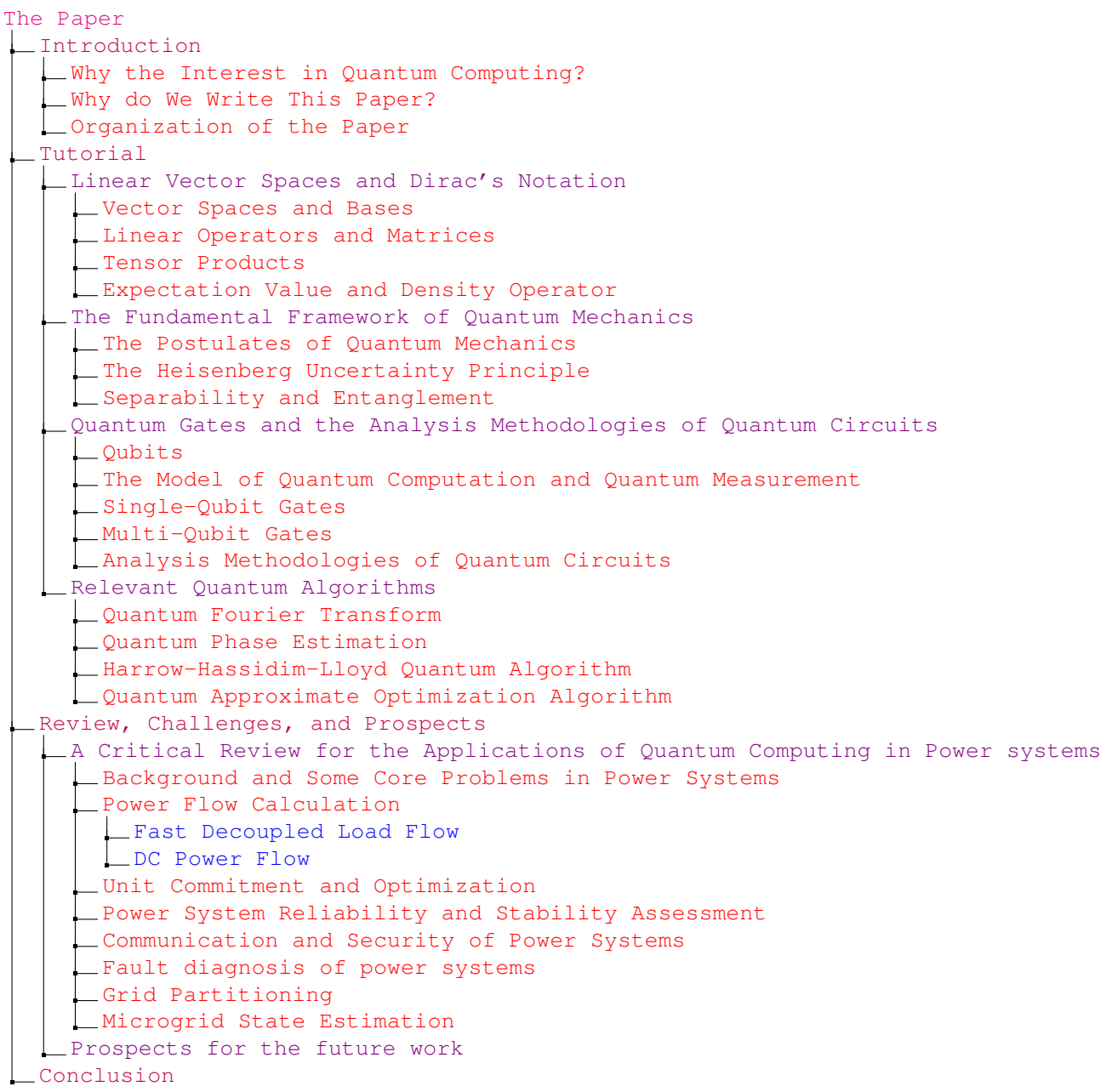

Fig. 1. The logical architecture of the entire paper.

II. Linear Vector Spaces and Dirac's Notation

A. Vector Spaces and Bases

In quantum computating, we need finite dimensional vector spaces mainly, which belong to Hilbert spaces.

Definition 1. *In a Hilbert space $\mathcal{H}$, a vector is specified by n complex numbers $[\alpha_1, \alpha_2, \cdots, \alpha_n]^T$, where n is the dimension of the vector space.*

Definition 2. *The vector* $|\alpha\rangle = [\alpha_1, \alpha_2, \cdots, \alpha_n]^T$ *is called a* ket.

Definition 3. *If* $|\alpha\rangle = [\alpha_1, \alpha_2, \cdots, \alpha_n]^T$*, then* $\langle\alpha| = [\alpha_1^*, \alpha_2^*, \cdots, \alpha_n^*]$*, namely conjugate transpose.* $\langle\alpha|$ *is called a* bra*, which can form the* bra-ket $\langle\alpha|\beta\rangle$ *connecting with* $|\beta\rangle$*.*

Definition 4. *If* $|\alpha\rangle = [\alpha_1, \alpha_2, \cdots, \alpha_n]^T$ *and* $|\beta\rangle = [\beta_1, \beta_2, \cdots, \beta_n]^T \in \mathbb{C}^n$*, then their inner product can be defined as follows:*

$$\langle\alpha|\beta\rangle = \langle\alpha| \times |\beta\rangle = [\alpha_1^*, \alpha_2^*, \cdots, \alpha_n^*] \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \sum_{i=1}^{n} \alpha_i^* \beta_i, \tag{1}$$

such that the following properties are satisfied:

$$\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^* \ \textit{(complex conjugate)}, \tag{2}$$

$$\langle a\alpha + b\beta|\gamma\rangle = a\langle\alpha|\gamma\rangle + b\langle\beta|\gamma\rangle \ \textit{(linearity)}, \tag{3}$$

$$\langle\alpha|\alpha\rangle \geq 0 \ \textit{(positive definite)}, \tag{4}$$

where, a *and* b *are complex numbers.* a^* *stands for complex conjugate, i.e., if* $a = c + id\,(a, b \in \mathbb{R})$*, then* $a^* = c - id$*.*

According to the properties above, we can check that $\langle c\alpha|\beta\rangle = c^*\langle\alpha|\beta\rangle$. The inner product is the matrix multiplication of a $1 \times n$ and an $n \times 1$ matrix.

Definition 5. *If* $|\alpha\rangle = [\alpha_1, \alpha_2, \cdots, \alpha_n]^T \in \mathbb{C}^n$ *and* $|\beta\rangle = [\beta_1, \beta_2, \cdots, \beta_m]^T \in \mathbb{C}^m$*, then their outer product, denoted by* $|\alpha\rangle\langle\beta|$*, is defined as*

$$|\alpha\rangle\langle\beta| = |\alpha\rangle \times \langle\beta| = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} [\beta_1^*, \beta_2^*, \cdots, \beta_m^*] = \begin{bmatrix} \alpha_1\beta_1^* & \alpha_1\beta_2^* & \cdots & \alpha_1\beta_n^* \\ \alpha_2\beta_1^* & \alpha_2\beta_2^* & \cdots & \alpha_2\beta_n^* \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n\beta_1^* & \alpha_n\beta_2^* & \cdots & \alpha_n\beta_m^* \end{bmatrix}, \tag{5}$$

$|\alpha\rangle\langle\beta|$ *is an* $n \times m$ *matrix.*

Unlike the inner product, the outer product no longer requires the same dimension of the two vectors.

Definition 6. *The norm of a vector is defined as* [1]*:*

$$\||\alpha\rangle\| = \sqrt{\langle\alpha|\alpha\rangle} = \left[\sum_{i=1}^{n} \alpha_i^* \alpha_i\right]^{0.5} = \sqrt{\sum_{i=1}^{n} |\alpha_i|^2}. \tag{6}$$

B. Linear Operators and Matrices

In quantum computing, state transformations are delineated by linear operators.

Definition 7. $\forall\, |\alpha\rangle \in \mathbb{V}$*, an operator* A *maps* $|\alpha\rangle$ *into another vector* $|\beta\rangle \in \mathbb{V}$*, namely*

$$|\beta\rangle = A\,|\alpha\rangle\,. \tag{7}$$

Definition 8. *There exists a unique linear operator* $A^\dagger$ *in* $\mathcal{H}$ *associated with any linear operator* A*, called the adjoint or Hermitian conjugate of operator* A*, which satisfies:*

$$\langle\alpha|A\beta\rangle = \langle A^\dagger\alpha|\beta\rangle\,. \tag{8}$$

According to Eq. (8), we are readily to derive $\langle A\alpha|\beta\rangle = \langle\beta|A\alpha\rangle^* = \langle A^\dagger\beta|\alpha\rangle^* = \langle\alpha|A^\dagger\beta\rangle$*.*

Remark 1. *In terms of matrices, the matrix elements of operator* $A^\dagger$ *are the complex conjugates of the matrix elements of the transpose matrix* A^T *of matrix* A*, namely*

$$A^\dagger = (A^*)^T = \left(A^T\right)^*, \tag{9}$$

where T *and* $*$ *denote transpose and complex conjugate, respectively.*

Proposition 9. *For operators* A *and* B*, the following identities hold:*

$$(A + B)^\dagger = A^\dagger + B^\dagger, \tag{10}$$

[1]The norm in this paper refers to the ℓ_2-norm, also known as the Euclidean norm. Here, $\|\cdot\|_2$ is abbreviated as $\|\cdot\|$.

$$(AB)^\dagger = B^\dagger A^\dagger, \tag{11}$$

$$\left(A^\dagger\right)^\dagger = A. \tag{12}$$

Definition 10. *A is said to be Hermitian or self-adjoint if*

$$A = A^\dagger. \tag{13}$$

Obviously, eigenvalues of a Hermitian matrix A are real, and eigenvectors of distinct eigenvalues are orthogonal.

Definition 11. *A is said to be normal if*

$$AA^\dagger = A^\dagger A. \tag{14}$$

Definition 12. *For a linear operator A, if there exists an operator B such that:*

$$AB = BA = I, \tag{15}$$

B is called the inverse of A and written as $B = A^{-1}$.

Definition 13. *An operator U is said to be unitary if*

$$UU^\dagger = U^\dagger U = I. \tag{16}$$

Because unitary operators are normal, they are diagonalizable. Unitary operators play a particularly crucial roles in quantum computing.

Proposition 14. *Unitary operators have the following properties:*

1) *unitary operators are normal and therefore diagonalizable;*
2) *all the eigenvalues of a unitary operator have modulus 1;*
3) *the eigenvectors of a unitary operator corresponding to distinct eigenvalues are orthogonal;*
4) *unitary operators are norm-preserving, namely*

$$\langle U\alpha|U\beta\rangle = \langle\alpha| U^\dagger U |\beta\rangle = \langle\alpha|\beta\rangle ; \tag{17}$$

5) *$U^\dagger$ and U^{-1} are unitary, $U^{-1} = U^\dagger$;*
6) *$\forall U$, it can be expressed as $U = e^{iH}$, where H is a Hermitian matrix, namely, $H = H^\dagger$;*
7) *the magnitude of the determinant of the unitary operator U equals 1, i.e., $|\det(U)| = 1$;*
8) *the rows or columns of the unitary operator U constitute an orthonormal set of vectors.*

C. Tensor Products

Definition 15. *Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ with complete orthonormal bases $\{|e_i\rangle\}_{i=1}^m$ and $\{|f_j\rangle\}_{j=1}^n$, respectively, the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is an mn-dimensional vector space. In the vector space, we can associate with each pair of vectors $|\alpha\rangle \in \mathcal{H}_1$ and $|\beta\rangle \in \mathcal{H}_2$ a vector in $\mathcal{H}$. We call this vector the tensor product of $|\alpha\rangle$ and $|\beta\rangle$, denoted by $|\alpha\rangle \otimes |\beta\rangle$. The vectors in $\mathcal{H}$ are linear superpositions of the vectors $|\alpha\rangle \otimes |\beta\rangle$. The vectors in $\mathcal{H}$ behave bilinearly, i.e., they satisfy the following properties:*

1) *$\forall |\alpha\rangle \in \mathcal{H}_1$, $\forall |\beta\rangle \in \mathcal{H}_2$, and $a \in \mathbb{C}$*

$$a\left(|\alpha\rangle \otimes |\beta\rangle\right) = \left(a|\alpha\rangle\right) \otimes |\beta\rangle = |\alpha\rangle \otimes \left(a|\beta\rangle\right); \tag{18}$$

2) *$\forall |\alpha_1\rangle$, $|\alpha_2\rangle \in \mathcal{H}_1$, and $|\beta\rangle \in \mathcal{H}_2$,*

$$\left(|\alpha_1\rangle + |\alpha_2\rangle\right) \otimes |\beta\rangle = |\alpha_1\rangle \otimes |\beta\rangle + |\alpha_2\rangle \otimes |\beta\rangle ; \tag{19}$$

3) *$\forall |\alpha\rangle \in \mathcal{H}_1$ and $|\beta_1\rangle$, $|\beta_2\rangle \in \mathcal{H}_2$,*

$$|\alpha\rangle \otimes \left(|\beta_1\rangle + |\beta_2\rangle\right) = |\alpha\rangle \otimes |\beta_1\rangle + |\alpha\rangle \otimes |\beta_2\rangle . \tag{20}$$

The basis of the vector space $\mathcal{H}_1$ and $\mathcal{H}_2$ is $\{|e_i\rangle \otimes |f_j\rangle\}_{i,j=(1,1)}^{(m,n)}$.

Remark 2. *If $|\gamma\rangle$ and $|\delta\rangle$ are orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, then $|\gamma\rangle \otimes |\delta\rangle$ is an orthonormal basis for $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Please be noted that we often use the shorthand notations $|\alpha\rangle|\beta\rangle$, $|\alpha, \beta\rangle$, $|\alpha\beta\rangle$ instead of $|\alpha\rangle \otimes |\beta\rangle$. For example, if $\mathcal{H}_1$ and $\mathcal{H}_2$ are two-dimensional Hilbert spaces with the same basis $\{|0\rangle, |1\rangle\}$, then the basis of $\mathcal{H}$ is $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.*

Definition 16. *Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ with complete orthonormal bases $\{|e_i\rangle\}_{i=1}^m$ and $\{|f_j\rangle\}_{j=1}^n$, respectively, the tensor product $A \otimes B$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ of linear operators A and B is defined as*

$$(A \otimes B)\left(|e_i\rangle \otimes |f_j\rangle\right) = A|e_i\rangle \otimes B|f_j\rangle , \quad \forall |e_i\rangle, |f_j\rangle . \tag{21}$$

Proposition 17. *The tensor product of operators has the following properties:*

1) $\forall$ *operators* A, B, C, *and* D,
$$(A \otimes B)(C \otimes D) = AC \otimes BD; \tag{22}$$
2) $\forall$ *operators* A *and* B
$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger; \tag{23}$$
3) *The trace of* $A \otimes B$ *meets the following equation:*
$$\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\,\mathrm{Tr}(B). \tag{24}$$

Remark 3. *In matrix terms, the tensor product* $A \otimes B$ *is given by*

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}, \tag{25}$$

where A *and* B *denote matrix representations of operators* A *and* B (A *and* B *are* $m \times n$ *and* $p \times q$ *matrices, respectively),* $A_{ij}B$ *is a sub-matrix of* $p \times q$. $A \otimes B$ *is an* $mp \times nq$ *matrix. Eq. (25) not only applies to the tensor product of operators but also to that of vectors. Generally,* $A \otimes B \neq B \otimes A$ *and* $|\alpha\rangle \otimes |\beta\rangle \neq |\beta\rangle \otimes |\alpha\rangle$, *which mean the tensor product is not commutative. However,* $A \otimes (B \otimes C) = (A \otimes B) \otimes C$ *and* $|\alpha\rangle \otimes (|\beta\rangle \otimes |\gamma\rangle) = (|\alpha\rangle \otimes |\beta\rangle) \otimes |\gamma\rangle = |\alpha\beta\gamma\rangle$. *That is, the tensor product is associative.*

Given a vector space $\mathbb{W}$, the notation $\mathbb{W}^{\otimes n}$ indicates that the tensor product of $\mathbb{W}$ with itself n times, and the same notation will be used for a operator or matrix A and the complex space $\mathbb{C}^2$:

$$\mathbb{W}^{\otimes n} = \underbrace{\mathbb{W} \otimes \mathbb{W} \otimes \cdots \otimes \mathbb{W}}_{n \text{ times}}, \tag{26}$$
$$A^{\otimes n} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{n \text{ times}}, \tag{27}$$
$$(\mathbb{C}^2)^{\otimes n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}. \tag{28}$$

D. Expectation Value and Density Operator

Definition 18. *The expectation value* $\langle A \rangle$ *of an operator* A *is the mean or average value of that operator with respect to a given quantum state* $|\psi\rangle$.

Remark 4. *If a quantum state* $|\psi\rangle$ *is prepared many times and the operator* A *is measured each time, the expectation value of the measurement results is given by the following equation*

$$\langle A \rangle = \langle \psi | A | \psi \rangle. \tag{29}$$

Generally, in quantum computing it is common to compute the expectation value of higher moments of an operator A, such as $\langle A^2 \rangle = \langle \psi | A^2 | \psi \rangle$.

Definition 19. *The standard deviation or uncertainty* ΔA *for an operator* A *is defined as:*

$$\Delta A = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}. \tag{30}$$

Definition 20. *If a quantum system can be denoted by a ket* $|\psi\rangle$ ($\langle \psi | \psi \rangle = 1$) *in a Hilbert space* $\mathcal{H}$, *then we say this system is in a pure state (a single quantum system).*

Definition 21. *The density operator* ρ *for the pure state* $|\psi\rangle$ *is given by*

$$\rho \coloneqq |\psi\rangle \langle \psi|. \tag{31}$$

Theorem 22. *The density operator* ρ *for the pure state* $|\psi\rangle$ *has the following properties:*

1) $\rho^2 = \rho$,
2) *the density operator is Hermitian, namely* $\rho = \rho^\dagger$,
3) $\mathrm{Tr}(\rho) = 1$,
4) ρ *is a positive operator, namely* $\forall |\alpha\rangle$, $\langle \alpha | \rho | \alpha \rangle \geq 0$.

Remark 5. *In terms of the density operator* ρ, *the expectation value* $\langle A \rangle$ *of an operator* A *can be written as* $\langle A \rangle = Tr(\rho A)$.

Sometimes we need to study a large collection of systems called an ensemble rather than a single quantum system.

Definition 23. *Suppose that there are n possible states in a mixed state, and the probability that a member of the ensemble has been prepared in the state $|\psi_i\rangle$ as p_i. Then the density operator ρ of the mixed state is defined as*

$$\rho \coloneqq \sum_{i=1}^{n} p_i \rho_i = \sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| . \tag{32}$$

For mixed states, properties 2)-4) of Theorem 22 are still valid, yet property 1) does no longer hold. For mixed states, $\rho^2 \neq \rho$, and $\mathrm{Tr}\left(\rho^2\right) < 1$

Obviously, the density matrix for the pure state is a special case of density matrix for the mixed state with $p_1 = 1$.

III. The Fundamental Framework of Quantum Mechanics

A. The Postulates of Quantum Mechanics

It should be noted that quantum mechanics is a framework of physical theories, which is not itself a physical theory. However, quantum electrodynamics, for example, is an actual physical theory, which is built on the foundation of quantum mechanics. It is quantum mechanics that states four postulates that a quantum physical theory must satisfy. Quantum systems are completely different from their classical counterparts, which is mainly reflected in superposition, interference, and entanglement. Quantum mechanics is based on a completely different mathematical framework from classical mechanics.

Postulate 1 (State space)**.** *Associated to any isolated physical system is a Hilbert space $\mathcal{H}$ known as the state space of the system that is completely described by a unit vector $|\psi(t)\rangle$, which is called the (*wave function*) or state vector.*

Postulate 1 solves the state description problem of the microscopic system.

Postulate 2 (Evolution or dynamics)**.** *The time evolution of the state vector $|\psi(t)\rangle$ of the closed quantum system is governed by the following Schrödinger equation:*

$$i\hbar \frac{d\left|\psi(t)\right\rangle}{dt} = H\left|\psi(t)\right\rangle , \tag{33}$$

where $\hbar = h/2\pi$, h is the Planck's constant, $h \approx 6.626 \times 10^{-34}\mathrm{J}\cdot\mathrm{s}$, H is a fixed self-adjoint or Hermitian operator known as the Hamiltonian of the system.

Postulate 2 resolves the problem of solving states in quantum mechanics.

Postulate 2 can be simplified in the way: the evolution of a closed system in a fixed time interval (from t_1 to t_2) is described by the unitary transformation $|\psi(t_2)\rangle = U|\psi(t_1)\rangle$. This expression is more commonly used in quantum computing, because here we are more interested in discrete time evolution than continuous time evolution.

Postulate 3 (Measurement)**.** *Quantum measurements are described by a collection $\{M_m\}$ of measurement operators acting on the state space of the quantum system being measured and satisfying the completeness equation*

$$\sum_m M_m^\dagger M_m = I \tag{34}$$

The index m refers to all measurement outcomes that may occur in the measurement. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the outcome m occurs is governed by

$$p(m) = \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle , \tag{35}$$

and the state of the system immediately after the measurement is given by

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle}}. \tag{36}$$

The completeness equation $\sum_m M_m^\dagger M_m = I$ guarantees that the sum of the probabilities of all outcomes is one, because

$$\begin{aligned} \sum_m p(m) &= \sum_m \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle \\ &= \left\langle\psi\right| \left(\sum_m M_m^\dagger M_m\right) \left|\psi\right\rangle \\ &= \left\langle\psi\right| I \left|\psi\right\rangle \\ &= \left\langle\psi|\psi\right\rangle \\ &= 1. \end{aligned} \tag{37}$$

Postulate 3 solves the problem of describing and measuring mechanical quantities.

Generally, of particular interest is the measurement in the computational basis. Therefore, we take $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$ as measurement operators for a single qubit.

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be a qubit, the probability $p(0)$ of the state $|\psi\rangle$ collapsing to the state $|0\rangle$ when observed is given by

$$\begin{aligned} p(M_0) &= \langle\psi|\left(|0\rangle\langle 0|\right)^\dagger\left(|0\rangle\langle 0|\right)|\psi\rangle \\ &= \langle\psi|\left(|0\rangle\langle 0|\right)\left(|0\rangle\langle 0|\right)|\psi\rangle \\ &= \langle\psi|0\rangle\left(\langle 0|0\rangle\right)\langle 0|\psi\rangle \\ &= \langle\psi|0\rangle\langle 0|\psi\rangle \\ &= \langle 0|\psi\rangle^*\langle 0|\psi\rangle \\ &= \langle 0|\psi\rangle^2 = |\alpha|^2; \end{aligned} \tag{38}$$

similarly, we can derive $p(M_1) = \langle\psi|\left(|1\rangle\langle 1|\right)^\dagger\left(|1\rangle\langle 1|\right)|\psi\rangle = \langle\psi|1\rangle\langle 1|\psi\rangle = \langle 1|\psi\rangle^2 = |\beta|^2$, which are called the Born's Law.

Example 1. *There is a four-dimensional Hilbert space spanned by the orthonormal bases $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$; consider the following state:*

$$\begin{aligned} |\psi\rangle &= -\frac{i}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle - \frac{i}{\sqrt{3}}|2\rangle \\ &= -\frac{i}{\sqrt{3}}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \frac{1}{\sqrt{3}}\begin{bmatrix}0\\1\\0\\0\end{bmatrix} - \frac{i}{\sqrt{3}}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \begin{bmatrix}-\frac{i}{\sqrt{3}}\\ \frac{1}{\sqrt{3}}\\ -\frac{i}{\sqrt{3}}\\ 0\end{bmatrix}. \end{aligned} \tag{39}$$

The measurement operator over the state $|0\rangle$ is given by

$$\begin{aligned} M_0^\dagger M_0 &= \left(|0\rangle\langle 0|\right)^\dagger\left(|0\rangle\langle 0|\right) = |0\rangle\langle 0| \\ &= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}. \end{aligned} \tag{40}$$

If we use matrix notation, the probability of getting the state $|0\rangle$ when measured is governed by

$$\begin{aligned} p(M_0) = \langle\psi|M_0^\dagger M_0|\psi\rangle &= \begin{bmatrix}\frac{i}{\sqrt{3}}\\ \frac{1}{\sqrt{3}}\\ \frac{i}{\sqrt{3}}\\ 0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}\begin{bmatrix}-\frac{i}{\sqrt{3}}\\ \frac{1}{\sqrt{3}}\\ -\frac{i}{\sqrt{3}}\\ 0\end{bmatrix} \\ &= \begin{bmatrix}\frac{i}{\sqrt{3}}\\ \frac{1}{\sqrt{3}}\\ \frac{i}{\sqrt{3}}\\ 0\end{bmatrix}\begin{bmatrix}-\frac{i}{\sqrt{3}}\\ 0\\ 0\\ 0\end{bmatrix} = \frac{1}{3}. \end{aligned} \tag{41}$$

Example 2. *Suppose $|\varphi\rangle = -\frac{i}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$, the probability of getting $|-\rangle$ when measured is given by*

$$\begin{aligned} &p(M_-) = \langle\varphi|M_-^\dagger M_-|\varphi\rangle \\ &= \langle\varphi|\left(|-\rangle\langle -|\right)^\dagger\left(|-\rangle\langle -|\right)|\varphi\rangle = |\langle -|\varphi\rangle|^2 \\ &= \left|\left(\frac{1}{\sqrt{2}}\langle 0| - \frac{1}{\sqrt{2}}\langle 1|\right)\left(-\frac{i}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle\right)\right|^2 \\ &= \left|\frac{-i}{\sqrt{10}}\langle 0|0\rangle + \frac{2}{\sqrt{10}}\langle 0|1\rangle + \frac{i}{\sqrt{10}}\langle 1|0\rangle + \frac{-2}{\sqrt{10}}\langle 1|1\rangle\right|^2 \\ &= \frac{1}{2}. \end{aligned} \tag{42}$$

Postulate 4 (Composition)**.** *The state space of a composite physical system is the tensor product of the state spaces of the individual component physical systems.*

Postulate 4 solves the composition problem of quantum mechanical physical systems. These five postulates can also be

regarded as axioms.

B. The Heisenberg Uncertainty Principle

Theorem 24 (The Heisenberg Uncertainty Principle)**.** *Suppose that there are Hermitian operators A and B associated with observables and $|\psi\rangle$ is a given quantum state. Then the following inequality equation can be satisfied:*

$$\Delta A \Delta B \geq \frac{1}{2} \left| \langle \psi | [A, B] | \psi \rangle \right|. \tag{43}$$

Remark 6. *The Heisenberg Uncertainty Principle demonstrates that it is impossible to simultaneously assign a well-determined position and velocity to a given particle. This is a intrinsic quantum limitation for quantum systems. It can also be expressed as follows:*

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}, \quad \Delta y \Delta p_y \geq \frac{\hbar}{2}, \quad \Delta z \Delta p_z \geq \frac{\hbar}{2}. \tag{44}$$

where Δx, Δy, Δz and Δp_x, Δp_y, Δp_z are the uncertainties in the position and the momentum of the given particle, respectively. $\hbar \equiv h/2\pi$, where h is Planck's constant, and $h \approx 6.626 \times 10^{-34} \boldsymbol{J} \cdot s$.

C. Separability and Entanglement

Definition 25. *A quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is separable if it can be expressed as a tensor product $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ of n 1-qubit states. Otherwise, it is said to be entangled or non-separable.*

Remark 7. *In a bipartite quantum system, a state in the Herbert space $\mathcal{H}$ is separable if it can be expressed as the tensor product of states of the components which belong to $\mathcal{H}_1$ and $\mathcal{H}_2$, namely*

$$|\psi\rangle = |\alpha\rangle_1 \otimes |\beta\rangle_2. \tag{45}$$

Example 3. *Consider the following state $|\psi_1\rangle$. It is separable because it can be written as*

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right). \end{aligned} \tag{46}$$

Remark 8. *In contrast, in a bipartite quantum system, a state is said to be entangled or non-separable if it cannot be expressed as the tensor product of states of the components which belong to $\mathcal{H}_1$ and $\mathcal{H}_2$.*

Example 4. *The following are four famous entangled states which are also called Bell states or Einstein, Podolsky and Rosen (EPR) pairs or the Bell basis:*

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right), \tag{47}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle \right), \tag{48}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle \right), \tag{49}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle \right). \tag{50}$$

Now we prove that $|\phi^+\rangle$ is entangled, and the other three states can be proved similarly.

Proof. Assume that $|\phi^+\rangle$ is a separate state such that there exists states $\alpha |0\rangle + \beta |1\rangle$ and $\gamma |0\rangle + \delta |1\rangle$ which make the following equation hold

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right) = \left(\alpha |0\rangle + \beta |1\rangle \right) \otimes \left(\gamma |0\rangle + \delta |1\rangle \right). \tag{51}$$

Expanding $\left(\alpha |0\rangle + \beta |1\rangle \right) \left(\gamma |0\rangle + \delta |1\rangle \right)$ and $\frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$, the equation above becomes

$$\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle. \tag{52}$$

According the equation above, we have

$$\alpha\gamma = \frac{1}{\sqrt{2}}, \quad \alpha\delta = 0, \quad \beta\gamma = 0, \quad \beta\delta = \frac{1}{\sqrt{2}}. \tag{53}$$

The four equations above cannot be satisfied at the same time, so $|\phi^+\rangle$ is an entangled state. □

Remark 9. *Quantum entanglement plays a crucial role in quantum communication and constitutes the theoretical basis of quantum communication.*

Example 5. *For $|\phi^+\rangle$, we assign the second qubit to Alice and the other to Bob. If Bob measures his qubit, he will get $|0\rangle$ and $|1\rangle$ with the probabilities of 50% and 50%, respectively. But it should be noted that if Bob obtain $|1\rangle$ when he measures his qubit, then the second qubit collapses into $|1\rangle$, which means that Alice must get $|1\rangle$ when she measures her qubit, even if they are geographically far apart, like Alice on Earth and Bob on Mars. Quantum entanglement is one of the most amazing and most counter-intuitive aspects of quantum mechanics, which is completely different from classical mechanics. However, for the state $|\psi_2\rangle = -\frac{i}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$, Bob will measure state $|0\rangle$ with the probability of 100%, and Alice will still get $|0\rangle$ or $|1\rangle$ with 50% probability each, because it is separable based on the following derivation:*

$$\begin{aligned} |\psi_2\rangle &= -\frac{i}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle \\ &= |0\rangle \otimes \left(-\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right). \end{aligned} \tag{54}$$

Example 6. *Here are some other famous entanglement states, such as the Greenberger–Horne–Zeilinger (GHZ) state and Wolfgang Dür (W) state:*

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right); \tag{55}$$

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right); \tag{56}$$

IV. Quantum Gates and the analysis methodologies of quantum circuits

A. Qubits

The fundamental unit of information processing in a classical computational device is a bit, which can assume one of two states 0 and 1. In theory, any system with a finite set of discrete and stable states with controlled transitions between them can be used to construct a computational device. In contrast, in quantum computing the basic unit of information processing is a qubit, which is short for a quantum bit. A qubit is a two-level quantum system, which is described by a two-dimensional complex Hilbert space $\mathcal{H}$. Generally, we choose a pair of orthonormal quantum states for $|0\rangle$ and $|1\rangle$, namely

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{57}$$

$|0\rangle$ and $|1\rangle$ correspond to classical bits 0 and 1, respectively, which form a computational basis in this two-dimensional complex Hilbert space $\mathcal{H}$. Quantum mechanics denotes that any system can exist in a superposition of states, so any state $|\psi\rangle$ of a qubit can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{58}$$

where α and β are complex numbers, satisfying the normalization condition:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{59}$$

Remark 10. *A arbitrary qubit can be written as $|\psi\rangle = e^{i\theta}\left(\gamma|0\rangle + \delta e^{i\phi}|1\rangle\right) = e^{i\theta}|\Psi\rangle\,(\gamma, \delta \in \mathbb{R})$, θ and ϕ are called the global phase and the relative phase, respectively. For any unitary operator U, we have $U|\psi\rangle = e^{i\theta}U|\Psi\rangle$. Moreover, for any measurement operator $M_m, p(m) = \langle\Psi| M_m^\dagger M_m |\Psi\rangle = \langle\Psi| e^{-i\theta} M_m^\dagger M_m |\Psi\rangle = \langle\Psi| M_m^\dagger M_m |\Psi\rangle$. Therefore, the global phase $e^{i\theta}$ is unobservable and indistinguishable, which means that it does not have physical meaning. However, relative phases have physical meaning and are observable. $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, for example, are two different states, which will evolve differently when quantum operations are applied; all of them have a 50% chance of being in either $|0\rangle$ or $|1\rangle$ if measured. However, if they are measured in the basis $|\pm\rangle$, then $|+\rangle$ has a 100% chance of being in $|+\rangle$ and $|-\rangle$ has a 100% chance of being in $|-\rangle$, respectively. Appreciating this point is pivotal to grasp the essence of quantum computing.*

Since there is a global phase of no physical significance in the definition of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, one can get rid of the global phase. Thus, the generic state of a qubit, which can be represented on the Bloch sphere as shown in Fig. 2, may be written as the following equation:

$$\begin{aligned} |\Psi\rangle &= \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \\ &= \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix}, \quad 0 \le \theta \le \pi, \quad 0 \le \phi < 2\pi. \end{aligned} \tag{60}$$

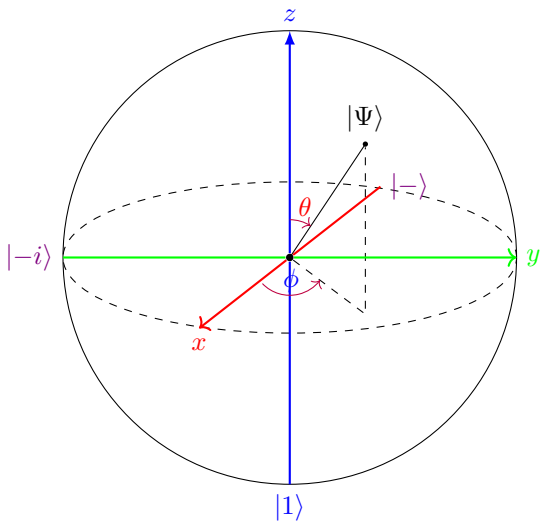

Fig. 2. Bloch sphere representation of a qubit state.

If this sphere is embedded in a three-dimensional space of Cartesian coordinates, then a state on the Bloch sphere can be expressed as $x = \cos\phi\cos\theta$, $y = \sin\phi\sin\theta$, and $z = \cos\theta$.

In $\mathbb{C}^2$, there are three crucial bases, namely,

$$X \text{ basis} = \left\{ |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right\}, \tag{61}$$

$$Y \text{ basis} = \left\{ |+i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle, |-i\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle \right\}, \tag{62}$$

$$Z \text{ basis} = \{|0\rangle, |1\rangle\}. \tag{63}$$

B. The Model of Quantum Computing and Quantum Measurement

It is well known that a classical computer can be represented as a finite register of n bits. Elementary operations, such as AND, OR, and NOT, can be performed on bits and these operations can be combined to produce complex logic functions. The circuit model in classical computing can be introduced into quantum computing such that the quantum computing based on gates can be formed. Like a classical computer, a quantum computer can be thought of as a quantum register of n qubits. An n-bit state in a classical computer can be expressed as a binary number $i \in [0, 2^n - 1]$, namely

$$i = i_{n-1}2^{n-1} + \cdots + i_1 2 + i_0, \tag{64}$$

where $i_0, i_1, \cdots, i_{n-1} \in \{0, 1\}$. Similarly, the state $|\psi\rangle$ of an n-qubit quantum computer is described by Eq. (65)

$$\begin{aligned}
|\psi\rangle &= \sum_{k=0}^{2^n-1} a_k |k\rangle \\
&= \sum_{k_{n-1}=0}^{1} \sum_{k_{n-2}=0}^{1} \cdots \sum_{k_1=0}^{1} \sum_{k_0=0}^{1} a_{k_{n-1},k_{n-2},\cdots,k_1,k_0} \cdot |k_{n-1}\rangle \otimes |k_{n-2}\rangle \otimes \cdots \otimes |k_1\rangle \otimes |k_0\rangle \\
&= \sum_{k_{n-1},k_{n-2},\cdots,k_1,k_0=0}^{1} a_{k_{n-1},k_{n-2},\cdots,k_1,k_0} \cdot |k_{n-1}k_{n-2}\cdots k_1 k_0\rangle \\
&= a_0 |00\cdots00\rangle + a_1 |00\cdots01\rangle + \cdots + a_{2^n-2} |11\cdots10\rangle + a_{2^n-1} |11\cdots11\rangle \\
&= a_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + a_{2^{n-1}} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^{n-1}}. \end{bmatrix}.
\end{aligned} \tag{65}$$

where the values of the weights $\{a_0, a_1, \cdots, a_{2^{n-1}}\}$ are controlled by the normalization condition, that is

$$|a_0|^2 + |a_1|^2 + \cdots + |a_{2^{n-1}}|^2 = \sum_{k=0}^{2^{n-1}} |a_k|^2 = 1. \tag{66}$$

Why is quantum computing exponentially faster than classical computing? This is due in large part to the parallelism of quantum computing, which is another meat-and-potatoes and vital phenomenon in quantum computing apart from quantum entanglement. The quantum register of n qubits can store not only the states corresponding to the basis vectors, but also the states superimposed by these basic states, all of which are up to 2^n. The quantum state grows exponentially as the number of qubits increases. In contrast, n classical bits can only store an integer. In theory, for a classical computer, different inputs require different operations; with a quantum computer, however, it can perform exponentially more operations relative to the input in a single run. Quantum parallelism is the key to the power of quantum computing.

There exist many possible superpositions constrained by the complex numbers $\{a_0, a_1, \cdots, a_{2^{n-1}}\}$ for the quantum state $|\psi\rangle$. The values of the weights $\{a_0, a_1, \cdots, a_{2^{n-1}}\}$ are strictly united with what happens with a particle when measured. According to the properties of the tensor product, it should be noted that a state of an n-qubit quantum computer is a quantum state or a wave function in a 2^n-dimensional Hilbert space $\left(\mathcal{H}^2\right)^{\otimes n}$, also written as $\mathcal{H}^{2^n}$, which is constituted by the tensor product of n 2-dimensional Hilbert spaces $\mathcal{H}^2$, where each qubit corresponds to a 2-dimensional Hilbert space. Eq. (65) shows the superposition principle of quantum states.

Generally, quantum computing is a composite of the following three elements [3]:

1) a set of registers;
2) unitary operators which are used to execute a given quantum algorithm;
3) measurements to extract the needed information.

Specifically, in order to perform quantum computing, one should do the following:

1) prepare the quantum computer in an initial state $|\psi_{in}\rangle$;
2) carry out the given unitary transformation U; that is, $|\psi_{out}\rangle = U|\psi_{in}\rangle$
3) perform a measurement in the computational basis.

C. Single-Qubit Gates

Generally, in classical computing there are only two 1-bit reversible logic gates, identity and NOT gates. However, in quantum computing the time evolution of states is described by the Schrödinger equation when measurements are not made; the operations on a qubit must preserve the normalization condition and states can be placed into superposition. Therefore, the operations on a qubit can be described by 2×2 unitary matrices, i.e., $UU^\dagger = U^\dagger U = I$. Based on the the unitarity of gates, we know that the computational process, except for measurement, is reversible.

Definition 26. *The identity gate I is defined as follows:*

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{67}$$

The quantum circuit representation of the identity gate I is shown as follows.

$$|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle \text{ —} \boxed{I} \text{— } |\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$$

Fig. 3. The quantum circuit representation of the identity gate I.

Proposition 27. *The identity gate I has the following properties:*

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{68}$$

$$I|0\rangle = |0\rangle, \tag{69}$$

$$I|1\rangle = |1\rangle. \tag{70}$$

Definition 28. *The X gate, also called as Pauli-X gate or bit flip gate, is defined as follows:*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{71}$$

The quantum circuit representation of the X gate is shown as follows.

$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\text{—}\boxed{X}\text{—}\; |\psi_{out}\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$$

Fig. 4. The quantum circuit representation of the X gate.

Proposition 29. *The X gate has the following properties:*

$$X = |1\rangle\langle 0| + |0\rangle\langle 1|\,, \tag{72}$$
$$X\,|0\rangle = |1\rangle\,, \tag{73}$$
$$X\,|1\rangle = |0\rangle\,. \tag{74}$$

Definition 30. *The Y gate, also called as Pauli-Y gate, is defined as follows:*

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{75}$$

The quantum circuit representation of the Y gate is shown as follows.

$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\text{—}\boxed{Y}\text{—}\; |\psi_{out}\rangle = -i\beta\,|0\rangle + i\alpha\,|1\rangle$$

Fig. 5. The quantum circuit representation of the Y gate.

Proposition 31. *The Y gate has the following properties:*

$$Y = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1|\,, \tag{76}$$
$$Y\,|0\rangle = +i\,|1\rangle\,, \tag{77}$$
$$Y\,|1\rangle = -i\,|0\rangle\,. \tag{78}$$

Definition 32. *The Z gate, also called as Pauli-Z gate or phase flip gate, is defined as follows:*

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{79}$$

The quantum circuit representation of the Z gate is shown as follows.

$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\text{—}\boxed{Z}\text{—}\; |\psi_{out}\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$$

Fig. 6. The quantum circuit representation of the Z gate.

Proposition 33. *The Z gate has the following properties:*

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|\,, \tag{80}$$
$$Z\,|0\rangle = +\,|0\rangle\,, \tag{81}$$
$$Z\,|1\rangle = -\,|1\rangle\,. \tag{82}$$

Remark 11. *For ease of your reference, we write the relationships of the three matrices here. $X^2 = Y^2 = Z^2 = I$, where I is the identity matrix. $XY = iZ, \quad YZ = iX, \quad ZX = iY$.*

Definition 34. *The Hadamard gate H, a gate frequently used gate in quantum computing, is defined as follows:*

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{83}$$

The quantum circuit representation of the H gate is shown as follows.

$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\text{—}\boxed{H}\text{—}\; |\psi_{out}\rangle = \alpha\,|+\rangle + \beta\,|-\rangle$$

Fig. 7. The quantum circuit representation of the H gate.

Remark 12. *Applying the Hadamard gate H on the state $|0\rangle$ yields:*

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \equiv |+\rangle, \end{aligned} \tag{84}$$

and on the state $|1\rangle$:

$$\begin{aligned} H|1\rangle &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \equiv |-\rangle. \end{aligned} \tag{85}$$

From Eqs. (84) and (85), it can be seen that the gate H turns the computational basis $\{|0\rangle, |1\rangle\}$ into the new basis $\{|+\rangle, |-\rangle\}$. Obviously, $H^2 = I$. As shown in Fig. 8, if $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ after applying the first Hadamard gate, we can derive:

$$\begin{aligned} |\psi_1\rangle &= H|\psi_0\rangle = H(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha H|0\rangle + \beta H|1\rangle = \alpha|+\rangle + \beta|-\rangle \\ &= \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle. \end{aligned} \tag{86}$$

Continue applying the second Hadamard gate, we have:

$$\begin{aligned} |\psi_2\rangle =& H|\psi_1\rangle \\ =& H\left[\left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle\right] \\ =& \left(\frac{\alpha+\beta}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ =& \alpha|0\rangle + \beta|1\rangle = |\psi_0\rangle. \end{aligned} \tag{87}$$

After $|\psi_0\rangle$ passes through two Hadamard gates, the state returns to the original state, namely $|\psi_0\rangle$.

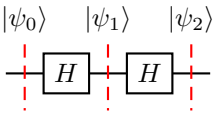

Fig. 8. A circuit showing $H^2 = I$.

Now, we discuss the case in which the Hadamard gates are applied in parallel to all n qubits. As shown in Fig. 9, when $n = 3$, $|\psi_0\rangle = |x\rangle = |x_2x_1x_0\rangle = |000\rangle$, we have

$$\begin{aligned} |\psi_1\rangle =& (H\otimes H\otimes H)|000\rangle = \left(H^{\otimes 3}\right)|000\rangle \\ =& (H|0\rangle)\otimes(H|0\rangle)\otimes(H|0\rangle) \\ =& \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ =& \left(\frac{1}{\sqrt{2}}\sum_{y_i=1}^{1}(-1)^{0\times y_i}|y_i\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}\sum_{y_i=1}^{1}(-1)^{0\times y_i}|y_i\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}\sum_{y_i=1}^{1}(-1)^{0\times y_i}|y_i\rangle\right) \\ =& \prod_{i=0}^{2}\left(\frac{1}{\sqrt{2}}\sum_{y_i=1}^{1}(-1)^{x_i\times y_i}|y_i\rangle\right) \quad \text{IN BINARY} \\ =& \frac{1}{2^{\frac{3}{2}}}(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+|101\rangle+|110\rangle+|111\rangle) \quad \text{IN BINARY} \\ =& \frac{1}{2^{\frac{3}{2}}}(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle) \quad \text{IN DECIMAL} \\ =& \frac{1}{2^{\frac{3}{2}}}\sum_{y=0}^{2^3-1}(-1)^{x\cdot y}|y\rangle \quad \text{IN DECIMAL.} \end{aligned} \tag{88}$$

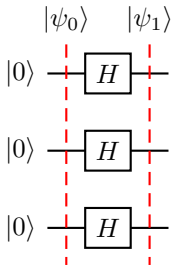

Fig. 9. Two Hadamard gates used in parallel to 3 qubits.

Similarly, when $n = 3$, $|\psi_0\rangle = |x\rangle = |x_2x_1x_0\rangle = |111\rangle$, we have

$$\begin{aligned}\left(H^{\otimes 3}\right)|111\rangle =& \prod_{i=0}^{2}\left(\frac{1}{\sqrt{2}}\sum_{y_i=1}^{1}(-1)^{x_i\times y_i}|y_i\rangle\right) \quad \text{IN BINARY}\\ =& \frac{1}{2^{\frac{3}{2}}}\left(|000\rangle-|001\rangle-|010\rangle+|011\rangle-|100\rangle+|101\rangle+|110\rangle-|111\rangle\right) \quad \text{IN BINARY}\\ =& \frac{1}{2^{\frac{3}{2}}}\left(|0\rangle-|1\rangle-|2\rangle+|3\rangle-|4\rangle+|5\rangle+|6\rangle-|7\rangle\right) \quad \text{IN DECIMAL}\\ =& \frac{1}{2^{\frac{3}{2}}}\sum_{y=0}^{2^3-1}(-1)^{x\cdot y}|y\rangle \quad \text{IN DECIMAL.}\end{aligned} \tag{89}$$

Likewise, one can readily obtain the results of $\left(H^{\otimes 3}\right)|001\rangle$, $\left(H^{\otimes 3}\right)|010\rangle$, $\left(H^{\otimes 3}\right)|011\rangle$, $\left(H^{\otimes 3}\right)|100\rangle$, $\left(H^{\otimes 3}\right)|101\rangle$, and $\left(H^{\otimes 3}\right)|110\rangle$.

As shown in Fig. 10, based on a similar derivation, it is easy to verify that the operation of $H^{\otimes n}$ on a state $|x\rangle = |x_{n-1}x_{n-2}\cdots x_0\rangle$ yields:

$$\begin{aligned}\left(H^{\otimes n}\right)|x\rangle =& \prod_{i=0}^{n-1}\left(\frac{1}{\sqrt{2}}\sum_{y_i=0}^{1}(-1)^{x_iy_i}|y_i\rangle\right) \quad \text{IN BINARY}\\ =& \frac{1}{2^{\frac{n}{2}}}\sum_{y_i=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle \quad \text{IN DECIMAL,}\end{aligned} \tag{90}$$

where $x\cdot y$ represents a sort of dot product for binary numbers which treats their digits with independent components and then does the modulo 2 operation, namely

$$x\cdot y = (x_{n-1}y_{n-1}+x_{n-2}y_{n-2}+\cdots+x_0y_0)\bmod 2. \tag{91}$$

For example, $001\cdot 3_{10} = 001\cdot 111 = (0\times 1+0\times 1+1\times 1)\bmod 2 = 1\bmod 2 = 1$.

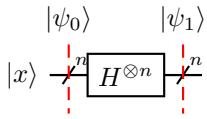

Fig. 10. n Hadamard gates used in parallel to n qubits.

Lemma 35. *Given an operator A such that $A^2 = I$, according to Taylor's theorem, one obtains the following equations:*

$$\begin{aligned}exp\left(i\delta A\right) &= I+i\delta A-\frac{\delta^2}{2!}I-i\frac{\delta^3}{3!}A+\frac{\delta^4}{4!}I+i\frac{\delta^5}{5!}A+\cdots\\ &= \left(I-\frac{\delta^2}{2!}-\frac{\delta^4}{4!}I-\cdots\right)I+i\left(\delta-i\frac{\delta^3}{3!}+i\frac{\delta^5}{5!}+\cdots\right)A\\ &= \cos\delta I+i\sin\delta A\end{aligned} \tag{92}$$

Eq. (92) is a generalization of Euler's formula $e^{i\delta} = \cos\delta + i\sin\delta$.

Definition 36. *The rotation gate $R_X(\delta)$ is defined as follows:*

$$\begin{aligned} R_X(\delta) &= e^{-i\frac{\delta}{2}X} \\ &= \cos\frac{\delta}{2}I - i\sin\frac{\delta}{2}X \\ &= \begin{bmatrix} \cos\frac{\delta}{2} & -i\sin\frac{\delta}{2} \\ -i\sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{bmatrix}, \quad 0 \le \delta < 2\pi. \end{aligned} \tag{93}$$

The quantum circuit representation of the $R_X(\delta)$ gate is shown as follows. $R_X(\delta)$ corresponds to a counterclockwise

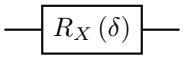

Fig. 11. The quantum circuit representation of the $R_X(\delta)$ gate.

rotation of an angle δ about the X-axis in the Bloch sphere.

Definition 37. *The rotation gate $R_Y(\delta)$ is defined as follows:*

$$\begin{aligned} R_Y(\delta) &= e^{-i\frac{\delta}{2}Y} \\ &= \cos\frac{\delta}{2}I - i\sin\frac{\delta}{2}Y \\ &= \begin{bmatrix} \cos\frac{\delta}{2} & -\sin\frac{\delta}{2} \\ \sin\frac{\delta}{2} & \cos\frac{\delta}{2} \end{bmatrix}, \quad 0 \le \delta < 2\pi. \end{aligned} \tag{94}$$

The quantum circuit representation of the $R_Y(\delta)$ gate is shown as follows. $R_Y(\delta)$ corresponds to a counterclockwise rotation

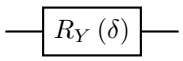

Fig. 12. The quantum circuit representation of the $R_Y(\delta)$ gate.

of an angle δ about the Y-axis in the Bloch sphere.

Definition 38. *The rotation gate $R_Z(\delta)$ is defined as follows:*

$$\begin{aligned} R_Z(\delta) &= e^{-i\frac{\delta}{2}Z} \\ &= \cos\frac{\delta}{2}I - i\sin\frac{\delta}{2}Z \\ &= \begin{bmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix}, \quad 0 \le \delta < 2\pi. \end{aligned} \tag{95}$$

The quantum circuit representation of the $R_Z(\delta)$ gate is shown as follows. $R_Z(\delta)$ corresponds to a counterclockwise rotation

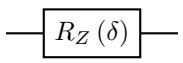

Fig. 13. The quantum circuit representation of the $R_Z(\delta)$ gate.

of an angle δ about the Z-axis in the Bloch sphere.

Definition 39. *The discrete phase gate R_k, which can be applied in the development of quantum Fourier transform, is defined as follows:*

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{bmatrix}. \tag{96}$$

The quantum circuit representation of the R_k gate is shown as follows.

Fig. 14. The quantum circuit representation of the R_k gate.

The R_k gate has the following properties:

$$R_k |0\rangle = |0\rangle , \tag{97}$$

$$R_k |1\rangle = \exp\left(\frac{2\pi i}{2^k}\right) |1\rangle \tag{98}$$

According to Eq. (96), the R_2 and R_3 gates are shown as follows, which are also called the S and T gates, respectively,

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \sqrt{Z} = S, \tag{99}$$

$$R_3 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = \sqrt{S} = T, \tag{100}$$

by the way, $R_1 = Z$.

D. Multi-Qubit Gates

Definition 40. *The standard controlled-NOT gate, called CNOT for short, is defined as follows:*

$$\mathit{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{101}$$

The quantum circuit representation of the CNOT gate is shown in Fig. 15.

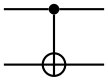

Fig. 15. The quantum circuit representation of the CNOT gate.

The CNOT gate flips the second qubit (target qubit) if the first qubit (control qubit) is the state $|1\rangle$ and leaves it unchanged if it is $|0\rangle$.

The CNOT gate has the following properties:

$$\begin{aligned} \text{CNOT} &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\ &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X. \end{aligned} \tag{102}$$

Similarly, we can obtain the gate C^k-U straightforwardly, which applies a unitary transformation U to the target qubit if and only if all the k control qubits are in $|1\rangle$. These C^k-U gates can be decomposed and implemented by single-qubit gates and CNOT gates. For example, C^2-NOT, also called Toffoli gate or CCNOT, is given by Eq. (103) and shown in Fig. 16, which applies a NOT operation to the target qubit if and only if the two control qubits are in $|1\rangle$. We can achieve the matrix representation of C^k-U effortlessly. We just need to replace the second order matrix in the lower right hand corner with the corresponding the matrix U.

$$\text{CCNOT} = \left[\begin{array}{cccccc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right]. \tag{103}$$

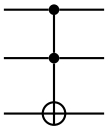

Fig. 16. The quantum circuit representation of the CCNOT gate. Generally, a full circle is drawn on the control qubit if the unitary operator U is applied to the target when the control qubit is $|1\rangle$, an empty circle instead if the unitary operator U is applied to the target when the control qubit is $|0\rangle$.

Definition 41. *The SWAP gate is defined as follows:*

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{104}$$

The quantum circuit representation of the SWAP gate is shown as follows.

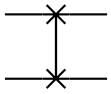

Fig. 17. The quantum circuit representation of the SWAP gate.

Proposition 42. *Generally, the SWAP consists of CNOT gates. One of the ways in which the SWAP is composed of CNOT gates is shown in Fig. 18.*

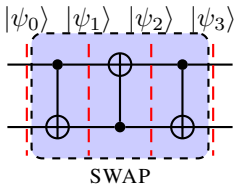

Fig. 18. The SWAP gate consists of CNOT gates.

Proof. If $|\psi_0\rangle = |01\rangle$, then $|\psi_1\rangle = |01\rangle$. Furthermore, $|\psi_2\rangle = |11\rangle$. Finally, $|\psi_3\rangle = |10\rangle$. Similarly, if $|\psi_0\rangle = |00\rangle$, $|10\rangle$, $|11\rangle$, respectively, we can get $|\psi_3\rangle = |00\rangle$, $|10\rangle$, $|11\rangle$, respectively. The SWAP circuit shown in Fig. 18 maps

$$\begin{aligned} &\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \rightarrow \\ &\alpha\,|00\rangle + \beta\,|10\rangle + \gamma\,|01\rangle + \delta\,|11\rangle\,. \end{aligned} \tag{105}$$

Hence, Fig. 18 realizes the function of the SWAP gate. □

In the current quantum computing hardware, 2-qubit quantum gates can only be used for specific quantum pairs. But with the SWAP gate, in theory, we can use SWAP to realize any quantum pairs meeting specific conditions. Moreover, many quantum algorithms also need to apply the SWAP gate. These are the reasons why SWAP is of particular significance. For instance, in the present prevalent superconducting quantum hardware technology, 2-qubit quantum gates can be used only in two physically adjacent qubits on a quantum chip, but if all the qubits are connected, even though two qubits are non-adjacent, then we can put them into being physically adjacent using SWAP gates a certain number of times. This is the power of the SWAP. If you are interested in the adjacency and connectivity of qubits, or want to further your knowledge of quantum hardware, please refer to References [6]–[8].

Theorem 43. *Any unitary matrix in the Hilbert space $\mathcal{H}$ of n qubits can be decomposed into 1-qubit gates and 2-qubit CNOT gates. That is, 1-qubit and 2-qubit CNOT gates are sufficient to assemble any unitary operator with arbitrary precision, which is called the universality in quantum computing.*

Proof. Please see [9]. □

If you are further interested in universality in quantum computing, please refer to Reference [10].

Theorem 44. *(The No-Cloning Theorem) Given that $|\psi\rangle$ is an arbitrary n-qubit quantum state, there does not exist a unitary matrix or a machine which maps $|\psi\rangle_n \otimes |\varphi\rangle_n \rightarrow |\psi\rangle_n \otimes |\psi\rangle_n$.*

Proof. Suppose that there exists such a unitary matrix U, shown in Fig. 19. Then we can derive: when $|\psi_0\rangle = |\psi\rangle_n \otimes |\varphi\rangle_n$, then $|\psi_1\rangle = U\,|\psi_0\rangle = |\psi\rangle_n \otimes |\psi\rangle_n$; when $|\psi_0\rangle = |\phi\rangle_n \otimes |\varphi\rangle_n$, then $|\psi_1\rangle = U\,|\psi_0\rangle = |\phi\rangle_n \otimes |\phi\rangle_n$. Adopting these equalities

and based the norm preserving property of the inner product, we have

$$\begin{aligned}\langle\psi|\phi\rangle &= \langle\psi|\phi\rangle \otimes \langle\varphi|\varphi\rangle \\ &= \left(\langle\psi|_n \otimes \langle\varphi|_n\right)\left(|\phi\rangle_n \otimes |\varphi\rangle_n\right) \\ &= \left(\langle\psi|_n \otimes \langle\varphi|_n\right) U^\dagger U \left(|\phi\rangle_n \otimes |\varphi\rangle_n\right) \\ &= \left(\langle\psi|_n \otimes \langle\varphi|_n U^\dagger\right)\left(U|\phi\rangle_n \otimes |\varphi\rangle_n\right) \\ &= \left(\langle\psi|_n \otimes \langle\psi|_n\right)\left(|\phi\rangle_n \otimes |\phi\rangle_n\right) \\ &= \langle\psi|_n \otimes \left(\langle\psi|\phi\rangle\right) \otimes |\phi\rangle_n = \langle\psi|\phi\rangle^2 .\end{aligned} \tag{106}$$

From Eq. (106), suffice it to say that $\langle\psi|\phi\rangle$ can only be equal to 0 or 1, which contradicts the fact that $|\psi\rangle$, $|\phi\rangle$ are arbitrary quantum states. Therefore, there does not exist a unitary matrix or a machine which maps $|\psi\rangle_n \otimes |\varphi\rangle_n \to |\psi\rangle_n \otimes |\psi\rangle_n$

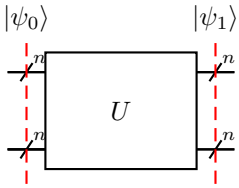

Fig. 19. The diagram used for proving the No-Cloning Theorem.

□

E. Analysis methodologies of quantum circuits

The following is based on Figs. 20 and 21 to discuss some basic derivation methods of quantum circuits and the concept of equivalent circuits. For Fig. 20, we can achieve the following derivation:

$$\begin{aligned}|\psi_1\rangle &= (I \otimes U_1)|\psi_0\rangle = (I \otimes U_1)|000\rangle \\ &= (I \otimes U_1)|0\rangle^{\otimes 3},\end{aligned} \tag{107}$$

$$\begin{aligned}|\psi_2\rangle &= (U_2 \otimes I \otimes I)|\psi_1\rangle = \left(U_2 \otimes I^{\otimes 2}\right)|\psi_1\rangle \\ &= \left(U_2 \otimes I^{\otimes 2}\right)(I \otimes U_1)|0\rangle^{\otimes 3},\end{aligned} \tag{108}$$

$$\begin{aligned}|\psi_3\rangle &= (I \otimes U_3 \otimes U_4)|\psi_2\rangle \\ &= (I \otimes U_3 \otimes U_4)\left(U_2 \otimes I^{\otimes 2}\right)(I \otimes U_1)|0\rangle^{\otimes 3}.\end{aligned} \tag{109}$$

The total unitary matrix representation for Fig. 20 is therefore $(I \otimes U_3 \otimes U_4)\left(U_2 \otimes I^{\otimes 2}\right)(I \otimes U_1)$. For Fig. (21), it can be encoded as $|\psi_1\rangle = U|\psi_0\rangle$; if $U = (I \otimes U_3 \otimes U_4)\left(U_2 \otimes I^{\otimes 2}\right)(I \otimes U_1)$, then Fig. (20) and Fig. (21) are equivalent circuits.

It is desirable to design quantum circuits that contain as few gates (short-depth) as possible when implemented on actual quantum computers, owing to each additional gate adding a small amount of noise to computing.

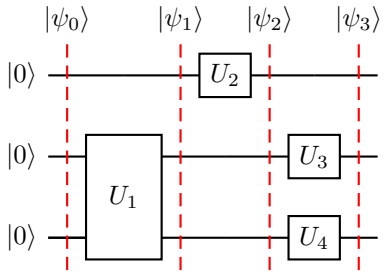

Fig. 20. A example circuit of a three-qubit.

Shown in Fig. 22, the initial state is $|\psi_0\rangle = |01\rangle$; now we derive $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$ based on matrix notation and Dirac's notation, respectively.

The following derivation is based on matrix notation.

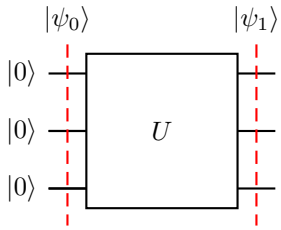

Fig. 21. Another example circuit of a three-qubit.

After applying Hadamard gate, we have:

$$\begin{aligned} |\psi_1\rangle &= (H \otimes I)\,|\psi_0\rangle = (H \otimes I)\,|01\rangle \\ &= \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\left(\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}\right) \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\0\\1\end{bmatrix}. \end{aligned} \tag{110}$$

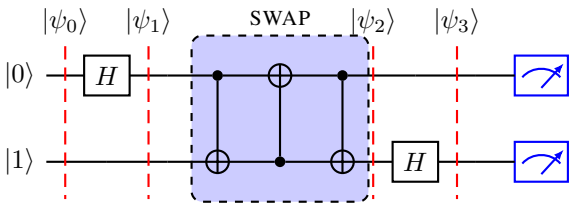

Fig. 22. The quantum circuit which lets $|\psi_0\rangle \to |\psi_3\rangle$.

After applying SWAP gate, it yields:

$$|\psi_2\rangle = \text{SWAP}\,|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}0\\1\\0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\1\end{bmatrix}. \tag{111}$$

After using Hadamard gate, we can get the following derivation:

$$\begin{aligned} |\psi_3\rangle &= (I \otimes H)\,|\psi_2\rangle = (I \otimes H)\,\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\1\end{bmatrix} \\ &= \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{bmatrix}\right)\left(\frac{1}{\sqrt{2}}\begin{bmatrix}0\\0\\1\\1\end{bmatrix}\right) \\ &= \frac{1}{2}\begin{bmatrix}0\\0\\2\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = |10\rangle. \end{aligned} \tag{112}$$

The following deduction is based on the Dirac notation.
After applying Hadamard gate, we get:

$$\begin{aligned} |\psi_1\rangle &= (H\,|0\rangle) \otimes |1\rangle = |+\rangle \otimes |1\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |1\rangle \\ &= \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right). \end{aligned} \tag{113}$$

After applying SWAP gate, we obtain:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|10\rangle + |11\rangle\right). \tag{114}$$

After using Hadamard gate, we can get the following derivation:

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2}}\left(|1+\rangle + |1-\rangle\right) \\ &= \frac{1}{2}\left[|1\rangle \otimes (|0\rangle + |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)\right] \\ &= \frac{1}{2}\left(|10\rangle + |11\rangle + |10\rangle - |11\rangle\right) \\ &= |10\rangle. \end{aligned} \tag{115}$$

From Eqs. (112) and (115), we can see that the result of the derivations based on matrix notation is the same as that based on Dirac's notation, but the use of Dirac's notation avoids complex and tedious matrix operations and thus makes derivations perspicuous and concise. Therefore, this paper will mainly use Dirac's notation for derivations and calculations.

Proposition 45. *The circuit in Fig. 23 can generate the Bell states.*

Proof. Shown in Fig. 23, the initial state is $|\psi_0\rangle$; now we derive $|\psi_1\rangle$, and $|\psi_2\rangle$.

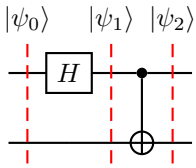

Fig. 23. A circuit generating the Bell states.

If $|\psi_0\rangle = |00\rangle$, then

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right), \tag{116}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{117}$$

Apparently, $|\psi_2\rangle$ is a Bell state, which is entangled. Based on Fig. 23, if $|\psi_0\rangle$ equals $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, respectively, then $|\psi_2\rangle$ equals $|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$, $|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$, and $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$, which are all Bell states. □

As shown in Fig. 24, if $|\psi_0\rangle = |00\rangle$, then we let $|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ pass through the gate $H \otimes H$, then we have

$$\begin{aligned} |\psi_3\rangle =& (H \otimes H)\,|\psi_2\rangle = (H \otimes H)\,\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ =& (H \otimes H)\left(\frac{1}{\sqrt{2}}|00\rangle\right) + (H \otimes H)\left(\frac{1}{\sqrt{2}}|11\rangle\right) \\ =& \frac{1}{\sqrt{2}}\left(H|0\rangle\right) \otimes \left(H|0\rangle\right) + \frac{1}{\sqrt{2}}\left(H|1\rangle\right) \otimes \left(H|1\rangle\right) \\ =& \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ =& \frac{1}{2\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle + \frac{1}{2\sqrt{2}}|00\rangle - \frac{1}{2\sqrt{2}}|01\rangle - \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle \\ =& \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ =& |\psi_2\rangle. \end{aligned} \tag{118}$$

$|\psi_3\rangle$ is the same as $|\psi_2\rangle$, our original EPR pair!

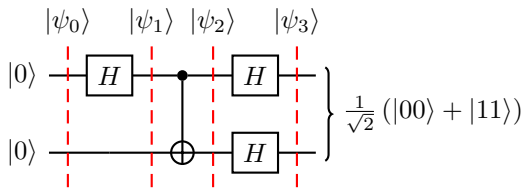

Fig. 24. A circuit showing the magic of entanglement.

V. Relevant Quantum Algorithms

A. Quantum Fourier Transform

Definition 46. *The inverse discrete Fourier transform (IDFT) converts a sequence of complex numbers* $\{x_0, x_1, \cdots, x_{2^n-1}\}$ *into another sequence of complex numbers* $\{y_0, y_1, \cdots, y_{2^n-1}\}$. y_k *is given by*

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j e^{2\pi i jk/2^n}. \tag{119}$$

Eq. (119) is often written as the following:

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j \omega^{jk}, \tag{120}$$

where $\omega = e^{2\pi i/2^n}$.

The quantum Fourier transform (QFT) implements the analog of the classical IDFT. It converts a state space of size 2^n into the frequency domain from the amplitude.

Definition 47. *Same to the DFT, the QFT, which is a unitary operation on* $\mathbb{C}^{2^n}$*, is defined as*

$$\mathcal{F}(|j\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle. \tag{121}$$

Eq. (121) is often expressed as

$$|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle. \tag{122}$$

Therefore, the QFT of an arbitrary quantum state $\sum_{j=0}^{2^n-1} x_j |j\rangle$ is governed by:

$$\mathcal{F}\left(\sum_{j=0}^{2^n-1} x_j |j\rangle\right) = \sum_{k=0}^{2^n-1} y_k |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} x_j e^{2\pi i \frac{jk}{2^n}} |k\rangle. \tag{123}$$

To facilitate the derivations, some notations are introduced. For a binary number $j (j \leq 2^n)$, it can be decomposed into the following form:

$$j_2 = (j_{n-1} j_{n-2} \cdots j_0)_2 = \left(j_{n-1} 2^{n-1} + j_{n-2} 2^{n-2} + \cdots + j_0 2^0\right)_{10} = \left(\sum_{i=1}^{n} j_{n-i} 2^{n-i}\right)_{10}. \tag{124}$$

For a binary fraction $(0.j_l j_{l+1} \cdots j_m)_2$, it can be decomposed into the following form:

$$(0.j_l j_{l+1} \cdots j_m)_2 = \left(\frac{1}{2} j_l + \frac{1}{2^2} j_{l+1} + \cdots + \frac{1}{2^{m-l+1}} j_m\right)_{10}. \tag{125}$$

Based on newly introduced notation above, Eq. (121) can be rewritten as Eq. (126). From Eq. (126), we can see that the output state from a computational basis state of the QFT is a tensor product of single qubit states and is, therefore, not entangled! Based on Eq. (126), the controlled-R_k gate, the Hadamard gate H in Fig. (7), and the SWAP gate in Fig. (17), we can easily construct a quantum circuit shown in Fig. 25 which computes the QFT efficiently. If the input of Fig. 25 is $|\psi_i\rangle = |j_{n-1} j_{n-2} \cdots j_1 j_0\rangle$, then the output is given by

$$|\psi_o\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.j_0} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_1 j_0} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_{n-2} \cdots j_0} |1\rangle\right). \tag{127}$$

Namely, Fig. 25 perfectly implements the QFT shown in Eq. (126). The pseudo-code of the QFT is given in Algorithm 1.

$$
\begin{aligned}
\mathcal{F}\left(|j\rangle\right) &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |k\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} \exp\left(2\pi i j \sum_{\ell=1}^{n} \frac{k_{n-\ell}}{2^\ell}\right) |k_{n-1}\cdots k_0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} \otimes_{\ell=1}^{n} \exp\left(2\pi i j \frac{k_{n-\ell}}{2^\ell}\right) |k_{n-\ell}\rangle \\
&= \frac{1}{\sqrt{2^n}} \otimes_{\ell=1}^{n} \left[\sum_{k_{n-\ell}=0}^{1} \exp\left(2\pi i j \frac{k_{n-\ell}}{2^\ell}\right) |k_{n-\ell}\rangle\right] \\
&= \frac{1}{\sqrt{2^n}} \otimes_{\ell=1}^{n} \left[|0\rangle + \exp\left(2\pi i j \frac{1}{2^\ell}\right) |1\rangle\right] \\
&= \frac{1}{\sqrt{2^n}} \left[|0\rangle + \exp\left(2\pi i \frac{j}{2^1}\right) |1\rangle\right] \otimes \left[|0\rangle + \exp\left(2\pi i \frac{j}{2^2}\right) |1\rangle\right] \cdots \left[|0\rangle + \exp\left(2\pi i \frac{j}{2^n}\right) |1\rangle\right] \\
&= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.j_0} |1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.j_1 j_0} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_{n-2} \cdots j_0} |1\rangle\right).
\end{aligned}
\tag{126}
$$

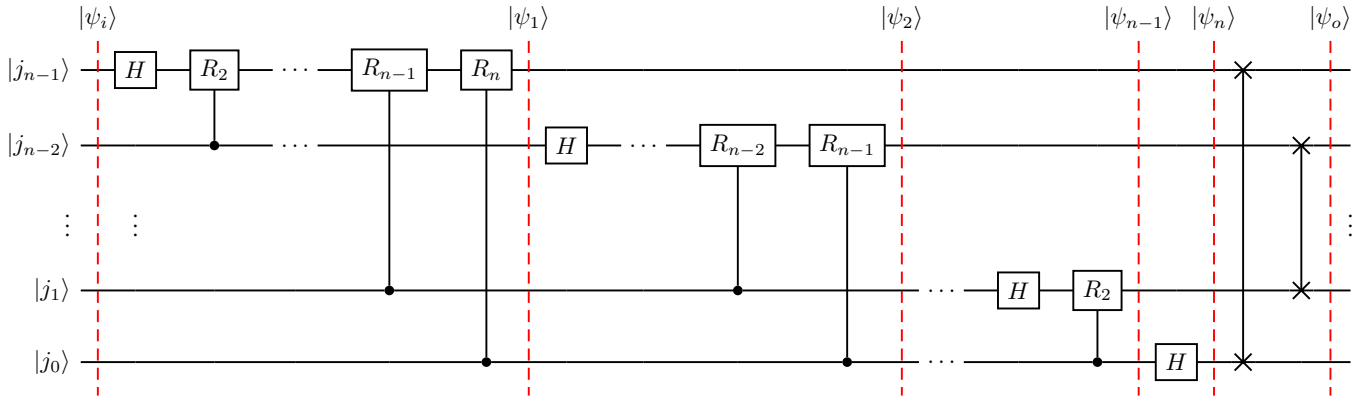

Fig. 25. A circuit implementing the QFT, whose output is Eq. (126).

Algorithm 1 QFT

Input:

- $|\psi_i\rangle = |j_{n-1}j_{n-2}\cdots j_1 j_0\rangle$.

Output:

- $\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.j_0} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_1 j_0} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_{n-2} \cdots j_0} |1\rangle\right)$.

Procedure:

for $0 \leq k \leq n-1$ **do**

Step 1a. As shown in Fig. 25, apply the Hadamard gate H.

Step 1b. As shown in Fig. 25, apply the controlled-R_2 gate to the controlled-R_{k+1} gate.

end for

Step 2. As shown in Fig. 25, apply $O(n)$ SWAP gates.

Remark 13. *From Fig. 25, it can be concluded that the computation of the QFT requires* $1+2+\cdots+n = \frac{n(n+1)}{2}$ *Hadamard and controlled-*R_k *gates, and* $O(n)$ *SWAP gates; thus, the total gates needed for the QFT are* $\frac{n(n+1)}{2} + O(n) = O(n^2)$. *Therefore, the time complexity of the QFT is* $O(n^2)$. *However, the most efficient classical algorithm, the fast Fourier transform (FFT), its time complexity is* $Q(n2^n)$. *The quantum parallelism of the QFT stems from the application of quantum gates acting on the superposition of an input quantum state. Furthermore, just like what we have stated before, a quantum input state can encode* 2^n *bits of classical data using only* n *qubits.*

Definition 48. *The inverse quantum Fourier transform (IQFT or QFT†) is defined as:*

$$\mathcal{F}^{-1}\left(|j\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{-2\pi i \frac{jk}{2^n}} |k\rangle \,. \tag{128}$$

Because $\mathcal{F}\mathcal{F}^{-1} = I$, we can realize the IQFT in Eq. (128) if we run the circuit in Fig. 25 from right to left.

B. Quantum Phase Estimation

Definition 49. *The problem the quantum phase estimation (QPE) algorithm solve is to find the eigenvalue λ corresponding to the eigenvector $|u\rangle$ satisfying $U|u\rangle = \lambda|u\rangle$ given U and the eigenvector $|u\rangle$ of U.*

Remark 14. *This problem can be rephrased into finding a ϕ ($\phi \in \mathbb{R}$) satisfying $U|u\rangle = e^{i\phi}|u\rangle$, where U is a unitary quantum gate. Considering that U is unitary, we know that its eigenvalue can be expressed as $\lambda = e^{i\phi} = e^{2\pi i\theta}$, where $\phi = 2\pi\theta$, $0 \le \phi < 2\pi$, and $0 \le \theta < 1$. Therefore, the QPE can be boiled down to calculating or approximating θ to some desired precision.*

The quantum circuit of the QPE is shown in Fig. 26. Now we derive the QPE step-by-step based on Fig. 26.

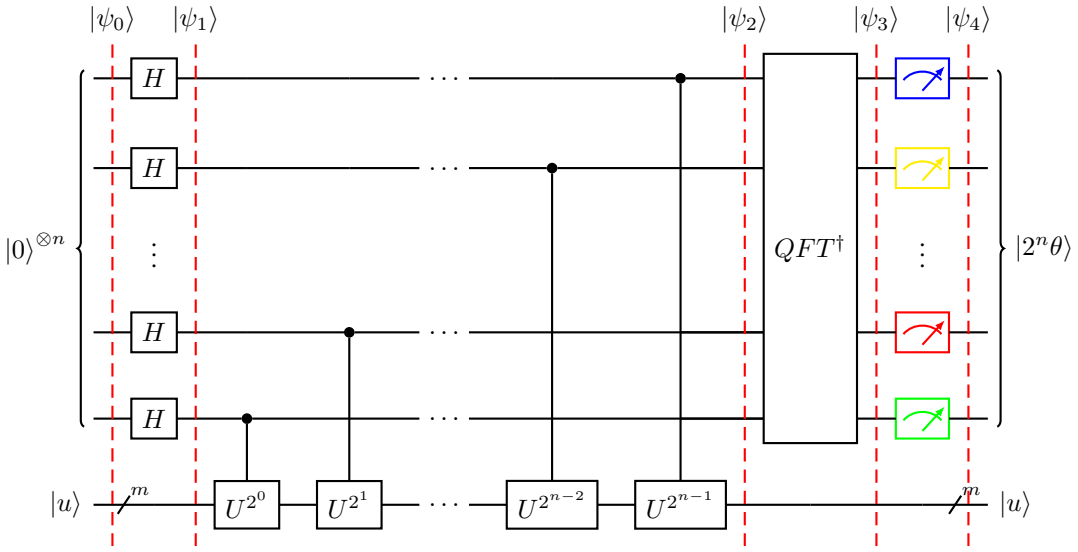

Fig. 26. Quantum phase estimation circuit.

(1) **Initialization**
From Fig. 26, we can have $|\psi\rangle = |00\cdots00\rangle\,|u\rangle = |0\rangle^{\otimes n}\,|u\rangle$.
(2) **Superposition**
Performing an n-bit Hadamard gate operation $H^{\otimes n}$ on the register results in the state

$$\begin{aligned} |\psi_1\rangle &= \left(H^{\otimes n} \otimes I^{\otimes m}\right)|\psi_0\rangle \\ &= \left(H^{\otimes n} \otimes I^{\otimes m}\right)|0\rangle^{\otimes n}\,|u\rangle \\ &= \left(H^{\otimes n} \otimes |0\rangle^{\otimes n}\right) \otimes \left(I^{\otimes m} \otimes |u\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}\,|u\rangle\,. \end{aligned} \tag{129}$$

(3) **Controlled Unitary Gates**
A controlled unitary gate $C\text{-}U^{2^j}$ applies gate U^{2^j} on $|u\rangle$ if and only if the control qubit is in the state $|1\rangle$. The operation

of the gate $C\text{-}U^{2^j}$ on the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle$ is given by:

$$\begin{aligned} C\text{-}U^{2^j}|\psi\rangle &= C\text{-}U^{2^j}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle U^{2^j}|u\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle e^{i2^j\phi}|u\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle e^{2\pi i 2^j\theta}|u\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^j\theta}|1\rangle)|u\rangle \end{aligned} \tag{130}$$

Based on the discussions above, now we can derive the following equation:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^n}}\underbrace{\left(|0\rangle + e^{2\pi i 2^{n-1}\theta}|1\rangle\right)}_{\text{qubit } n}\otimes\cdots\otimes\underbrace{\left(|0\rangle + e^{2\pi i 2^1\theta}|1\rangle\right)}_{\text{qubit 2}}\otimes\underbrace{\left(|0\rangle + e^{2\pi i 2^0\theta}|1\rangle\right)}_{\text{qubit 1}}\otimes|u\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i k\theta}|k\rangle|u\rangle, \end{aligned} \tag{131}$$

where k ($k \in \mathbb{N}$) denotes the integer representations of n-bit binary numbers.

(4) **Inverse Quantum Fourier Transform**

Noticing that Eq. (131) is exactly the result of applying the QFT. The following state is yielded after applying the QFT†:

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{2\pi i k\theta}e^{-2\pi i\frac{jk}{2^n}}|j\rangle|u\rangle \\ &= \frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{(2^n\theta-j)k}{2^n}}|j\rangle|u\rangle. \end{aligned} \tag{132}$$

(5) **Measurement**

The state $|j\rangle$ can encode only discrete set of variables; however, θ is a continuous variable. So there will be errors in some cases. For convenience, we write $\theta = \frac{a}{2^n} + \delta$, namely $2^n\theta = a + 2^n\delta$ where a is the nearest integer to $2^n\theta$ and $0 \le |2^n\delta| \le \frac{1}{2}$. Therefore, Eq. (132) can be rewritten as

$$|\psi_3\rangle = \frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{(a-j)k}{2^n}+2\pi i\delta k}|j\rangle|u\rangle. \tag{133}$$

For the above formula, we discusses two cases.

Case 1: $\delta = 0$, i.e., there is no error ($2^n\theta \in \mathbb{N}, \quad 2^n\theta = a$).

The probability of obtaining state $2^n\theta$ when measuring n control qubits simultaneously is generalized as

$$\begin{aligned} P(|2^n\theta\rangle) &= \left|\frac{1}{2^n}\langle 2^n\theta|\sum_{j=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{(a-j)k}{2^n}}|j\rangle\right|^2 \\ &= \left|\frac{1}{2^n}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{(a-a)k}{2^n}}\langle 2^n\theta|2^n\theta\rangle\right|^2 \\ &= \left|\frac{1}{2^n}\sum_{k=0}^{2^n-1} e^0\right|^2 \\ &= 1. \end{aligned} \tag{134}$$

In this case, we can get the state $|\psi_4\rangle = |2^n\theta\rangle|u\rangle$ with the probability of 100% when measuring the control qubits. Based on θ, we can readily calculate the eigenvalue corresponding to the eigenvector $|u\rangle$.

The case above is the best we can hope for, whereas things are sometimes not perfect. We have to consider the imperfect.

Case 2: $\delta \neq 0$, i.e., there are errors ($2^n\theta \notin \mathbb{N}, \quad 2^n\theta = a + 2^n\delta$).

In this case the state $|a\rangle$ will be yielded with the probability $P(|a\rangle)$ shown in Eq. (135) when the control qubits are measured. The derivation uses $\left|1 - e^{2i\delta}\right| = 2|\sin\delta|$ and for $0 \le |\delta| \le \frac{1}{2^{n+1}}$, $|2\cdot 2^n\delta| \le |\sin(\pi 2^n\delta)| \le |\pi\delta|$. The lower bound of the

$$
\begin{aligned}
P(|a\rangle) &= \left| \frac{1}{2^n} \langle a| \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{(a-j)k}{2^n} + 2\pi i \delta k} |j\rangle \right|^2 \\
&= \left| \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{2\pi i \delta k} \right|^2 \\
&= \frac{1}{2^{2n}} \left| \frac{1 - e^{2\pi i \delta 2^n}}{1 - e^{2\pi i \delta}} \right|^2 \\
&= \frac{1}{2^{2n}} \left| \frac{\sin\left(\pi 2^{2n} \delta\right)}{\sin\left(\pi \delta\right)} \right|^2 \\
&\geq \frac{1}{2^{2n}} \left| \frac{2 \cdot 2^n \delta}{\pi \delta} \right|^2 \\
&= \frac{4}{\pi^2} \approx 0.405.
\end{aligned}
\tag{135}
$$

result of Eq. (135) is $\frac{4}{\pi^2}$. Obviously, $P(|a\rangle)$, converging to 1, raises as n increases. So we need to increase the number of the control qubits in order to increase the probability.

Suppose that we approximate θ with $\theta \approx \tilde{\theta} = 0.\theta_1\theta_2\cdots\theta_t$, where $\theta_1\theta_2\cdots\theta_t \in \{0,1\}$. As shown in [1], to successfully achieve θ to an accuracy to n bits with the success probability of at least $1-\epsilon$, we choose:

$$
t = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil. \tag{136}
$$

The pseudo-code of the QPE is given in Algorithm 2.

Algorithm 2 QPE

Input:
- Controlled unitary gates *C*-U^{2^j} $(0 \leq j \leq n-1)$.
- Eigenvector $|u\rangle$.

Output:
- $|\tilde{\lambda}\rangle |u\rangle$, where $\tilde{\lambda}$ is an estimate for λ.

Procedure:

Step 1. Initialize n ancillary qubits to $|0\rangle^{\otimes n}$.
Step 2. Perform $H^{\otimes n}$ on $|0\rangle^{\otimes n}$ to obtain $\frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}$, namely $|0\rangle^{\otimes n} \rightarrow \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}$.
for $0 \leq j \leq n-1$ **do**
    Step 3. Apply controlled unitary gates *C*-U^{2^j}.
end for
Step 4. Apply QFT†.
Step 4. Measure the ancillary qubits.

C. Harrow-Hassidim-Lloyd Quantum Algorithm

Solving linear equations is an old mathematical problem. Considering that linear systems of equations are ubiquitous, it is no exaggeration to say that solving linear systems of equations is an important fundamental problem throughout science, engineering, and economics. Furthermore, algorithms for linear systems of equations are the core of many other algorithms and pave the way for other algorithms. Therefore, it is of great theoretical and practical significance to study the solution to linear systems of equations.

The HHL quantum algorithm for linear systems of equations, which is one of the most important subroutines in many quantum machine learning algorithms [11], is proposed by Aram Harrow, Avinatan Hassidim and Seth Lloyd [12].

Definition 50. *The HHL algorithm solves a linear system of equations, which is defined as given a matrix $A \in \mathbb{C}^{N\times N}$ and a vector $\mathbf{b} \in \mathbb{C}^N$ finding a vector $\mathbf{x} \in \mathbb{C}^N$ such that $A\mathbf{x} = \mathbf{b}$, or a flag indicating the system has no solution. Without loss of generality, here it is assumed that A is Hermitian, i.e., $A^\dagger = A$.*

Remark 15. *In the definition above, we assume that A is Hermitian. However, if A is not Hermitian, we can easily obtain a Hermitian matrix by the following transformation:*

$$\tilde{A} := \begin{bmatrix} \mathbf{0} & A \\ A^\dagger & \mathbf{0} \end{bmatrix}, \tag{137}$$

with

$$\tilde{\mathbf{x}} = \begin{bmatrix} \mathbf{0} \\ \mathbf{x} \end{bmatrix}, \tilde{\mathbf{b}} = \begin{bmatrix} \mathbf{b} \\ \mathbf{0} \end{bmatrix}. \tag{138}$$

$\tilde{A}$ is Hermitian, and $\tilde{A}\left|\tilde{\mathbf{x}}\right\rangle = \left|\tilde{\mathbf{b}}\right\rangle$. Moreover, $\left|\tilde{\mathbf{x}}\right\rangle$ can be computed given $\left|\tilde{\mathbf{b}}\right\rangle$. Hence, we focus on A being Hermitian in this paper.

Proposition 51. *Because the matrix A, which is Hermitian, satisfies the normality condition, i.e., $AA^\dagger = A^\dagger A$, A is normal. Therefore, there exists a spectral decomposition of A; that is, A is diagonalizable with an orthonormal basis of eigenvectors:*

$$A = \sum_{j=1}^{N} \lambda_j \left|u_j\right\rangle \left\langle u_j\right| \tag{139}$$

where λ_j are eigenvalues of A and $\left|u_j\right\rangle$ the corresponding orthonormal eigenvectors.

Proof. Please see [1]. □

Based on Eq. (139), we can readily obtain the inverse of A by simply inverting the eigenvalues:

$$A^{-1} = \sum_{j=1}^{N} \lambda_j^{-1} \left|u_j\right\rangle \left\langle u_j\right| \tag{140}$$

The vector $\left|b\right\rangle$ can be also expressed in the basis of A, namely:

$$\left|b\right\rangle = \sum_{j=1}^{N} \left\langle u_j|b\right\rangle \left|u_j\right\rangle = \sum_{j=1}^{N} \beta_j \left|u_j\right\rangle, \quad \beta_j \in \mathbb{C}. \tag{141}$$

Therefore, we can get the result $\left|\mathrm{x}\right\rangle$ of $A\mathbf{x} = \mathbf{b}$:

$$\begin{aligned} \left|\mathrm{x}\right\rangle &= A^{-1}\left|b\right\rangle \\ &= \left(\sum_{j=1}^{N} \lambda_j^{-1} \left|u_j\right\rangle \left\langle u_j\right|\right) \left(\sum_{j=1}^{N} \beta_j \left|u_j\right\rangle\right) \\ &= \sum_{j=1}^{N} \lambda_j^{-1} \beta_j \left|u_j\right\rangle. \end{aligned} \tag{142}$$

Although we can easily derive the expression of $\left|\mathrm{x}\right\rangle$ shown in Eq. (142), it is intractable and non-trivial to invert a matrix using classical computing, especially for large matrices.

Theorem 52. *A is Hermitian; thus the unitary operator e^{iAt} has the eigenvalues $e^{i\lambda_j t}$ and corresponding eigenvectors $\left|u_j\right\rangle$.*

Proof. According to Taylor's theorem and considering that A can do a spectral decomposition, one obtains the following

equations:

$$
\begin{aligned}
e^{iAt} &= \sum_{k=0}^{\infty} \frac{(iAt)^k}{k!} \\
&= I + iAt + \frac{(iAt)^2}{2!} + \frac{(iAt)^3}{3!} + \cdots \\
&= I + iAt - \frac{A^2t^2}{2!} - \frac{iA^3t^3}{3!} + \cdots \\
&= I + it\left(\lambda_1 |u_1\rangle\langle u_1| + \lambda_2 |u_2\rangle\langle u_2| + \cdots\right) - t^2 \frac{\left(\lambda_1^2 |u_1\rangle\langle u_1| + \lambda_2^2 |u_2\rangle\langle u_2|\right)}{2!} - \cdots \\
&= \sum_{k=0}^{\infty} \frac{(i\lambda_1 t)^k}{k!} |u_1\rangle\langle u_1| + \sum_{k=0}^{\infty} \frac{(i\lambda_2 t)^k}{k!} |u_2\rangle\langle u_2| + \cdots + \sum_{k=0}^{\infty} \frac{(i\lambda_n t)^k}{k!} |u_n\rangle\langle u_n| \\
&= e^{i\lambda_1 t} |u_1\rangle\langle u_1| + e^{i\lambda_2 t} |u_2\rangle\langle u_2| + \cdots + e^{i\lambda_n t} |u_n\rangle\langle u_n| \\
&= \sum_j e^{i\lambda_j t} |u_j\rangle\langle u_j| .
\end{aligned}
\tag{143}
$$

Apparently, $e^{iAt}\left(e^{iAt}\right)^\dagger = \left(e^{iAt}\right)^\dagger e^{iAt} = I$, so e^{iAt} is a unitary operator. □

From Eq. (143), we can see that the eigenvalues of A can be obtained by the unitary operator e^{iAt}.

As is illustrated in Fig. 27, broadly, the HHL is mainly composed of QPE, eigenvalue inversion, i.e., $R(\tilde{\lambda}^{-1})$ rotation, and inverse quantum phase estimation (IQFT or QFT†). In the following part, the HHL algorithm will be analyzed minutely.

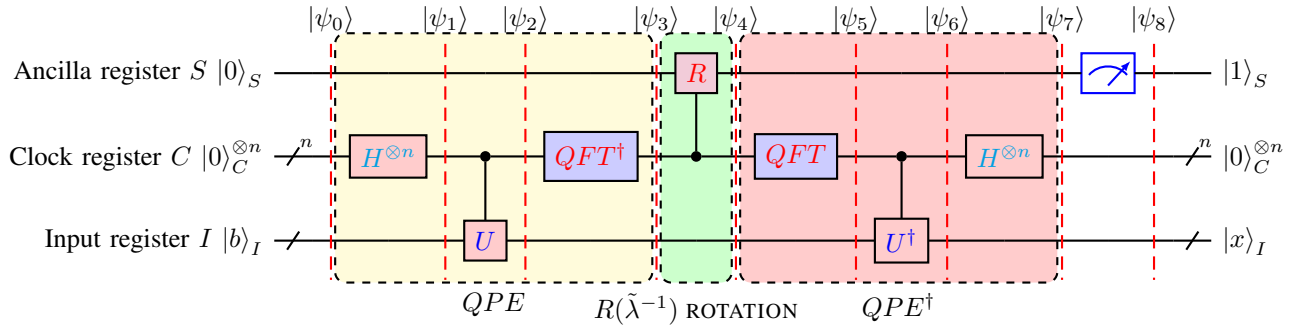

Fig. 27. HHL algorithm circuit.

(1) **QPE**

There are three quantum registers, namely ancilla register S, clock register C, and input register I. Generally, the qubits in the input register are produced by a subroutine called state preparation. For example, we can get $|1\rangle^{\otimes n}$ by applying n parallel X gates to $|0\rangle^{\otimes n}$.

$$
|\psi_0\rangle = |0\rangle_S |0\rangle_C^{\otimes n} |b\rangle_I . \tag{144}
$$

After leveraging $H^{\otimes n}$, $|\psi_1\rangle$ is encoded as

$$
|\psi_1\rangle = H^{\otimes n} |\psi_0\rangle = |0\rangle_S \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} |b\rangle_I . \tag{145}
$$

After applying controlled-U gates, the system evolves to

$$
|\psi_2\rangle = |0\rangle_S \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k\theta} |k\rangle |b\rangle_I . \tag{146}
$$

Here, we set $N = 2^n$. After applying the QFT†, this lead the system to

$$\begin{aligned}
|\psi_3\rangle &= |0\rangle_S \, \text{QFT}^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k\theta} |k\rangle \right) |b\rangle_I \\
&= |0\rangle_S \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k\theta} \text{QFT}^\dagger \left(|k\rangle \right) |b\rangle_I \\
&= |0\rangle_S \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k\theta} \left(\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{-2\pi i \frac{kz}{2^n}} |z\rangle \right) |b\rangle_I \\
&= \frac{1}{2^n} |0\rangle_S \sum_{k=0}^{2^n-1} \sum_{z=0}^{2^n-1} e^{2\pi i k(\theta - \frac{z}{2^n})} |z\rangle |b\rangle_I .
\end{aligned} \tag{147}$$

Now, let $\theta - \frac{z}{2^n} = 0$, namely $\theta - z/N = 0$ or $z = N\theta$; then Eq. (147) can be reformulated as

$$|\psi_3\rangle = |0\rangle_S |N\theta\rangle |b\rangle_I . \tag{148}$$

According to the QPE and Eq. (143), we have

$$U |u_j\rangle = e^{i2\pi\theta_j} |u_j\rangle , \quad e^{iAt} |u_j\rangle = e^{i\lambda_j t} |u_j\rangle . \tag{149}$$

A is only a Hermitian matrix; however, U must be a unitary matrix. Consequently, e^{iAt}, which is a unitary operator, is used to prepare U, i.e., $U = e^{iAt}$. From the two equations above, we have $2\pi\theta_j = \lambda_j t$. So, $\theta_j = \lambda_j t/2\pi$. Let $|\tilde{\lambda_j}\rangle = |N\lambda_j t/2\pi\rangle$. Considering $|b\rangle_I = \sum_{j=1}^{N} \beta_j |u_j\rangle$, we can rewrite Eq. (148) as follows:

$$\begin{aligned}
|\psi_3\rangle &= \sum_{j=1}^{N} |0\rangle_S \beta_j |N\lambda_j t/2\pi\rangle \beta_j |u_j\rangle \\
&= \sum_{j=1}^{N} \beta_j |0\rangle_S |\tilde{\lambda}_j\rangle |u_j\rangle .
\end{aligned} \tag{150}$$

The QPE is leveraged to estimate the eigenvalues of A.

(2) **Eigenvalue Inversion**

In this part, the rotation on the ancilla qubit controlled by the clock register C yields a normalized form:

$$|\psi_4\rangle = \sum_{j=1}^{N} \beta_j \left(\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S \right) |\tilde{\lambda}_j\rangle |u_j\rangle , \tag{151}$$

where C is a normalization constant. Specifically, we can realize the controlled R rotations to perform the controlled Y-rotations through the application of the operator R

$$R = \exp(-i\theta Y) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} . \tag{152}$$

(3) **Uncomputation (QPE†)**

The following derivation will showcase the efficacy of uncomputation. We can have $|\psi_5\rangle$, i.e., Eq. (153), through the application of the QPE†.

$$\begin{aligned}
|\psi_5\rangle =& \sum_{j=1}^{N} \beta_j \left(\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S \right) \text{QFT} \left(|\tilde{\lambda}_j\rangle \right) |u_j\rangle \\
=& \sum_{j=0}^{2^n-1} \beta_j \left(\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S \right) \left(\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i \frac{\tilde{\lambda}_j z}{2^n}} |z\rangle \right) |u_j\rangle \\
=& \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \beta_j \left(\sqrt{1 - \frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S \right) \left(\sum_{z=0}^{2^n-1} e^{2\pi i \frac{\tilde{\lambda}_j z}{2^n}} |z\rangle \right) |u_j\rangle .
\end{aligned} \tag{153}$$

Then inverse controlled-rotations C-$U^\dagger$ on the input register I are applied through $U^\dagger = e^{-iAt}$. From Fig. 27, it is concluded that if the control clock qubit is $|0\rangle$, $|u_j\rangle$ will remain the same and not be affected; however, if the clock qubit is $|1\rangle$, $U^\dagger$ will

be applied to $|u_j\rangle$. From $U|u_j\rangle = e^{i\lambda_j t}|u_j\rangle$, we can get $U^\dagger|u_j\rangle = e^{-i\lambda_j t}|u_j\rangle$. Based on these analyses, we have $|\psi_6\rangle$, i.e., Eq. (154).

$$\begin{aligned}
|\psi_6\rangle =& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)\left(e^{-i\lambda_j t z}\sum_{z=0}^{2^n-1}e^{2\pi i\frac{\tilde{\lambda}_j z}{2^n}}|z\rangle\right)|u_j\rangle \\
=& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)\left(e^{-i\lambda_j t z}\sum_{z=0}^{2^n-1}e^{2\pi i\frac{\tilde{\lambda}_j z}{2^n}}|z\rangle\right)|u_j\rangle \\
=& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)\left(e^{2\pi i\frac{\tilde{\lambda}_j z}{2^n}}\sum_{z=0}^{2^n-1}e^{2\pi i\frac{\tilde{\lambda}_j z}{2^n}}|z\rangle\right)|u_j\rangle \\
=& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)\left(\sum_{z=0}^{2^n-1}|z\rangle\right)|u_j\rangle .
\end{aligned} \tag{154}$$

According to Eq. (90), after passing $H^{\otimes n}$, $|\psi_7\rangle$ is encoded as Eq. (155).

$$\begin{aligned}
|\psi_7\rangle =& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)H^{\otimes n}\left(\sum_{z=0}^{2^n-1}|z\rangle\right)|u_j\rangle \\
=& \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)\left(2^{\frac{n}{2}}|0\rangle^{\otimes n}\right)|u_j\rangle \\
=& \sum_{j=0}^{2^n-1}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)|0\rangle^{\otimes n}|u_j\rangle \\
=& \sum_{j=1}^{N}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)|0\rangle^{\otimes n}|u_j\rangle .
\end{aligned} \tag{155}$$

From Eq. (155), we can see that the clock register qubits and the register I are now unentangled. This is what uncomputation QPE† does.

The QPE† subroutine sets the clock register C to $|0\rangle_C^{\otimes n}$ and leaves the state as $\sum_{j=1}^{N}\beta_j\left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}}|0\rangle_S + \frac{C}{\tilde{\lambda}_j}|1\rangle_S\right)|0\rangle_C^{\otimes n}|u_j\rangle$.

(4) **Measurement**

Measuring the ancilla register S and post-selecting on the outcome of $|1\rangle_S$ result in the state:

$$\begin{aligned}
|\psi_8\rangle =& \frac{1}{\sqrt{\sum_{j=1}^{N}\left|\frac{\beta_j C}{\tilde{\lambda}_j}\right|^2}}\sum_{j=1}^{N}\frac{\beta_j C}{\tilde{\lambda}_j}|1\rangle_S|0\rangle^{\otimes n}|u_j\rangle \\
=& \frac{C}{\sqrt{\sum_{j=1}^{N}\left|\frac{\beta_j C}{\tilde{\lambda}_j}\right|^2}}|1\rangle_S|0\rangle^{\otimes n}\left(\sum_{j=1}^{N}\frac{\beta_j}{\tilde{\lambda}_j}|u_j\rangle\right) \\
=& \frac{C}{\sqrt{\sum_{j=1}^{N}\left|\frac{\beta_j C}{\tilde{\lambda}_j}\right|^2}}|1\rangle_S|0\rangle_C^{\otimes n}|x\rangle_I .
\end{aligned} \tag{156}$$

$C\left(\sum_{j=1}^{N}\frac{\beta_j}{\tilde{\lambda}_j}|u_j\rangle\right)\Big/\sqrt{\sum_{j=1}^{N}\left|\frac{\beta_j C}{\tilde{\lambda}_j}\right|^2}$ is proportional to $|\mathrm{x}\rangle = \sum_{j=1}^{N}\lambda_j^{-1}\beta_j|u_j\rangle$. So, as shown in $|\psi_8\rangle$, we have derived the solution $|\mathrm{x}\rangle$ to the equation $A|\mathrm{x}\rangle = |b\rangle$.

The pseudo-code of the HHL is given in Algorithm 3.

Remark 16. *In the field of classical computation, Gaussian elimination and the conjugate gradient algorithm are commonly used to solve linear equations. The time complexity of generic Gaussian elimination is generally considered as $O\left(N^3\right)$. The time complexity of the classical conjugate gradient algorithm for general purpose, which is distinguished as the optimal algorithm to solve SLE, is $O\left(Ns\kappa\log(1/\epsilon)\right)$ [13], however, that of the HHL algorithm is $O\left(\log(N)s^2\kappa^2/\epsilon\right)$ [14], where N is the dimension of the system, s is the sparsity of the matrix A, κ is the condition number of A which is defined as the ratio*

Algorithm 3 HHL

Input:

• State $|b\rangle = \sum_{j=1}^{N} \beta_j |u_j\rangle, \quad \beta_j \in \mathbb{C}$.

Output:

• $|\mathrm{x}\rangle$.

Procedure:

Step 1. Perform the QFT on $|0\rangle_S |0\rangle_C^{\otimes n} |b\rangle_I$ to obtain $\sum_{j=1}^{N} \beta_j |0\rangle_S |\tilde{\lambda}_j\rangle |u_j\rangle$.

Step 2. Apply the controlled R rotations to $|0\rangle_S$ to get $\sum_{j=1}^{N} \beta_j \left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S\right) |\tilde{\lambda}_j\rangle |u_j\rangle$.

Step 3. Perform QPE†. Then, the system evolves to $\sum_{j=1}^{N} \beta_j \left(\sqrt{1-\frac{C^2}{\tilde{\lambda}_j^2}} |0\rangle_S + \frac{C}{\tilde{\lambda}_j} |1\rangle_S\right) |0\rangle^{\otimes n} |u_j\rangle$.

Step 4. Measuring the ancilla register S and post-selecting on the outcome of $|1\rangle_S$ result in the state $\frac{C}{\sqrt{\sum_{j=1}^{N} \left|\frac{\beta_j C}{\tilde{\lambda}_j}\right|^2}} |1\rangle_S |0\rangle_C^{\otimes n} |x\rangle_I$.

of its largest to smallest eigenvalue, i.e. $\kappa = \lambda_{max}/\lambda_{min}$, and ϵ is the desired precision. The sparsity s of an $N \times N$ matrix is defined as having at most s entries per row. Hence, the HHL algorithm provides an exponential speed-up over its classical counterpart time under specific conditions.

Remark 17. *Uncomputation is an important technique and trick in the design of quantum algorithms, which can liberate qubits in the states of entanglement. Subroutine QPE† of the HHL algorithm is an uncomputation operation.*

HHL can be used to calculate the power flow of power systems and other problems, which are discussed in more detail in the remainder of the paper.

D. Quantum Approximate Optimization Algorithm

Quantum approximate optimization algorithm (QAOA) proposed by Farhi *et al.* [15] is a quantum algorithm for solving combinatorial problems. The QAOA is a hybrid quantum-classical heuristic algorithm [16], and possesses (i) a simple and monotonous structure and (ii) relatively good performance [17].

Definition 53. *Quadratic unconstrained binary optimization (QUBO), which is an NP-hard problem and a kind of combinatorial optimization problem, is defined as follows:*

$$\min f(\mathbf{x}) = \min_{\mathbf{x} \in \mathbb{B}^n} \mathbf{x}^{\mathsf{T}} Q \mathbf{x} = \min_{\mathbf{x} \in \mathbb{B}^n} \sum_{i=1}^{n} \sum_{j=1}^{n} Q_{ij} x_i x_j, \tag{157}$$

where $\mathbb{B}^n = \{0,1\}^n$, $x_i \in \{0,1\}$, and we assume that Q is a symmetric matrix $Q \in \mathbb{R}^{n \times n}$ without loss of generality.

See References [18], [19] for how to formulate QUBO models and approximate an objective function using the QUBO.

Definition 54. *The classical cost function $C(\mathbf{z})$ is the number of satisfied clauses,*

$$C(\mathbf{z}) = \sum_{\alpha=1}^{m} C_\alpha(\mathbf{z}) \tag{158}$$

where $\mathbf{z} = (z_1, z_2, \cdots, z_n) \in \{+1, -1\}^n$ is the n-bit string and $C_\alpha(\mathbf{z}) = 1$ if $\mathbf{z}$ satisfies clause α and 0 otherwise. The QAOA attempts to find a string $\mathbf{z}$ such that $C(\mathbf{z})$ is close to its exact minimum.

A unitary operator which depends on C and an angle parameter γ is introduced

$$U(C, \gamma) = e^{-i\gamma C} = \prod_{\alpha=1}^{m} e^{-i\gamma C_\alpha}, \tag{159}$$

where $0 \leq \gamma \leq 2\pi$.

The mixing operator $U(B, \beta)$ is defined as follows

$$U(B, \beta) = e^{-i\beta B} = \prod_{j=1}^{n} e^{-i\beta X_j}, \tag{160}$$

where $0 \leq \beta \leq \pi$ is a parameter and $B = \sum_{j=1}^{n} X_j$ in which X_j is the Pauli X operator acting on qubit j.

As shown in Fig. 28, initialized state $|s\rangle$ is as follows

$$|s\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}} |\mathbf{z}\rangle \,. \tag{161}$$

Referring to Fig. 28, after alternately applying p layers of $U(C,\gamma)$ and $U(B,\beta)$ we have

$$|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle = \underbrace{U(B,\beta_p)U(C,\gamma_p)\cdots U(B,\beta_1)U(C,\gamma_1)}_{p \text{ times}} |s\rangle \,, \tag{162}$$

where $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_p)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_p)$.

After $|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle$ passing through the measurement gates, we can obtain the expectation value of C

$$\langle C\rangle = \langle \boldsymbol{\gamma},\boldsymbol{\beta}|C|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle \,. \tag{163}$$

Then we can get a new set of $(\boldsymbol{\gamma_{new}}, \boldsymbol{\beta_{new}})$ using a classical computer. And then we assign the new parameters $(\boldsymbol{\gamma_{new}}, \boldsymbol{\beta_{new}})$ to the current parameters $(\boldsymbol{\gamma},\boldsymbol{\beta})$, and we repeat this process until the convergence condition is met.

The pseudo-code of the QAOA is given in Algorithm 4. The UC problem of power systems can be solved by the QAOA, which will be discussed in detail in the remainder of this paper.

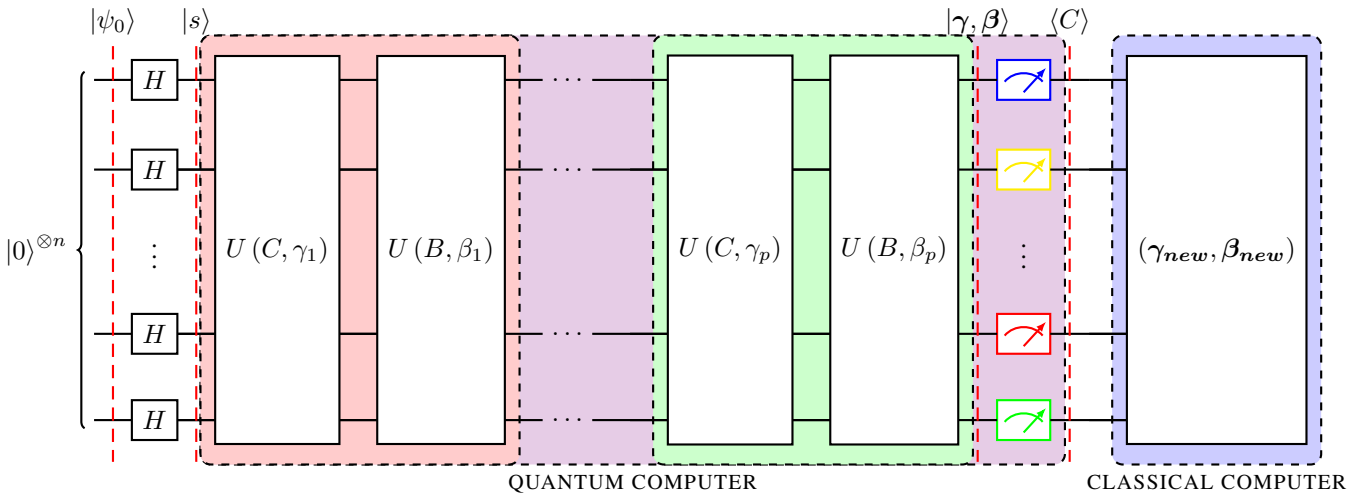

Fig. 28. QAOA circuit.

Algorithm 4 QAOA

Input:

- Number of the optimization levels p.
- Parameters, γ and β.
- Hamiltonians $C\,(\mathbf{z})$ corresponding to the original optimization problem.

Output:

- An approximate solution to the problem in Eq. (158).

Procedure:

Step 1. Construct the initialized state $|s\rangle$ and initialize $|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle$.

for The convergence criteria is not satisfied **do**

Step 2a. Alternately apply $U(C,\gamma)$ and $U(B,\beta)$ p times to obtain the state $|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle$.

Step 2b. Measure the state the state $|\boldsymbol{\gamma},\boldsymbol{\beta}\rangle$ in the standard basis and compute $\langle C\rangle$.

Step 2c. Find a new set of $(\boldsymbol{\gamma_{new}}, \boldsymbol{\beta_{new}})$ using a classical computer (a classical optimization algorithm).

Step 2d. Set the current parameters. $(\boldsymbol{\gamma},\boldsymbol{\beta})$ to be the new parameters $(\boldsymbol{\gamma_{new}}, \boldsymbol{\beta_{new}})$.

end for

VI. A CRITICAL REVIEW FOR THE APPLICATIONS OF QUANTUM COMPUTING IN POWER SYSTEMS

A. Background and some core problems in power systems

Quantum algorithms and quantum computers have come a long way in the past several decades [20]. Quantum computing shows great potential in energy fields, such as power systems [21]–[26]. In recent years, quantum computing has gained wide attention in the field of power systems and produced some research achievements [27]–[54].

As a large number of renewable energy resources are connected to power systems, the operation, planning, and optimization of power systems have been becoming more and more intricate. Power flow calculation, unit commitment, economic dispatch, power system planning, optimal portfolio and sizing and placement of distributed energy resources (DERs) in multi-energy microgrids are essentially computational problems, which consume a lot of computing resources. Conventionally, the calculation and optimization problems of power systems are settled by classical computers based on classical computing theory and von Neumann architecture. Nevertheless, with Moore's law getting closer to the limit, the exponential acceleration of quantum computing compared with classical computing under certain conditions, the development of quantum computing software and hardware, and the availability to quantum computers for the public, the importance of quantum computing has become increasingly crucial, and has been applied to some fields to a certain extent. Because the power industry underpins the national economy, introducing quantum computing into the power system has far-reaching and pivotal significance, such as enhancing the penetration of renewable energy, heightening the computing efficiency of computation and optimization problems of power systems, diminishing greenhouse gas emissions, and achieving the goal of climate neutrality by 2050 established by the United Nations Framework Convention on Climate Change.

There is not to much published literature on the applications of quantum computing in power systems, so it is one of the purposes of this review to serve as a spur to induce more engineers and researchers to come forward with their valuable contributions to this realm, which enriches the area and promote development of the community. Quantum computing can make contributions to the further progress of the power system.

B. Power Flow Calculation

The power flow calculation and analysis are the fundamentals of operation, control, planning, optimization, and security analysis of power systems. However, solving this problem efficiently and effectively is very challenging and non-trivial. Besides, the novel power system with the high penetration of renewable energy and energy storage systems makes the power flow calculation knottier. So it is necessary to resort to quantum computers. The fast decoupled load flow (FDLF) and the DC power flow [55] are often employed to calculte the quantum power flow. The FDLF is one of the most widely used variants of the Newton-Raphson power flow because of its excellent computational efficiency and convergence performance [29]. The DC power flow are in widespread and even increasing use, especially in congestion-constrained electricity markets [55].

1) Fast decoupled load flow: In an N-bus power system, which has one slack bus, N_{pv} PV buses, and N_{pq} PQ buses, the FDLF [56] is given by

$$B'\Delta\theta = {V'}^{-1}\Delta P, \tag{164}$$

$$B''\Delta V = {V''}^{-1}\Delta Q, \tag{165}$$

where $B' \in \mathbb{R}^{(N-1)\times(N-1)}$ and $B'' \in \mathbb{R}^{N_{pq}\times N_{pq}}$ denote coefficient matrices derived from the admittance matrix $Y \in \mathbb{C}^{N\times N}$; $\Delta\theta \in \mathbb{R}^{(N-1)\times 1}$ and $\Delta V \in \mathbb{R}^{N_{pq}\times 1}$ are the differences of voltage angles and voltage magnitudes, respectively; $V' \in \mathbb{R}^{(N-1)\times(N-1)}$ and $V'' \in \mathbb{R}^{N_{pq}\times N_{pq}}$ are diagonal matrices consisting of the voltage amplitudes of the corresponding buses $\Delta P \in \mathbb{R}^{(N-1)\times 1}$ and $\Delta Q \in \mathbb{R}^{N_{pq}\times 1}$ represent the active and reactive power mismatches, respectively.

2) DC power flow: Given an N-bus power system with one slack bus, the DC power flow can be formulated as

$$P' - D' = B'''\theta', \tag{166}$$

where $P' \in \mathbb{R}^{(N-1)\times 1}$ and $Q' \in \mathbb{R}^{(N-1)\times 1}$ are injected active power and loads of non-slack buses, respectively, $B''' \in \mathbb{R}^{(N-1)\times(N-1)}$ denotes the coefficient matrices derived from the admittance matrix $Y \in \mathbb{C}^{N\times N}$; $\theta' \in \mathbb{R}^{(N-1)\times 1}$ is voltage angles of non-slack buses.

Equations (164)–(166) are linear systems of equations, which can be solved by the HHL. In References [27], [28], the HHL algorithm was applied to the calculation of the DC power flow, but the scale of the case study is small, and the exponential acceleration effect of quantum computing has not been proved in practice. In addition, the solutions of some points in the analysis are not very accurate. References [29], [30] also applied the HHL to the calculation of the power flow in the power system. Reference [29] combined the traditional computer with the quantum computer, while reference [30] used different quantum computers for calculation. However, the scale of calculation examples are also small, and the superiority of quantum computing has not been proved in practice.

Reference [57] applied annealing-based quantum computing to the combinatorial optimal power flow. In this reference, an optimal power flow problem incorporating linear multiphase network modelling, discrete sources of energy flexibility, renewable generation placement/sizing and network upgrade decisions is integrated into a QUBO problem, and quantum annealing is used to solve the problem. Case studies were implemented using D-Wave Systems' 5,760 qubit Advantage quantum processing unit and hybrid quantum-classical solver. This reference is based on quantum annealing [58]; we can try to solve this problem on a quantum computer based on gate circuits.

The variational quantum linear solver (VQLS) [59] was applied to the power flow computation. For more information about the VQLS, refer to [60].

C. Unit commitment and optimization

The unit commitment (UC) problem is of crucial importance in the field of power system operation and optimization. By optimizing system resources and coping with the operation risks brought by various uncertain factors, such as renewable energy, the safe, economic, and stable operation of power systems can be guaranteed. The solution of the UC determines the combination of the on or off status of each unit within a specific time frame. With the high penetration of large-scale renewable energy, such as wind power and photovoltaic, the uncertainty of the power system is increasing to the point where it threatens the safe operation of the system. The UC can improve the safety of the system operation and enhance the system's ability to deal with wind power, photovoltaic and other renewable energy. Therefore, it is vital in theory and reality to study the UC, especially the UC of the power system with the high penetration of renewable energy.

However, from a mathematics and computer science point of view, the UC is a fundamentally large-scale mixed-integer nonlinear, NP-complete/NP-hard, non-convex optimization problem, which is particularly computationally expensive. An NP-complete/NP-hard problem means that we cannot develop a classical algorithm which solve it in polynomial time. In view of the exponential acceleration of quantum computing under certain conditions, it is pivotal to explore the applications of quantum computing in the power system optimization problem, such as UC.

Mathematically, a generic UC formation can be summarized as:

$$\min H\left(y_i, p_i\right) = \sum_{i=1}^{N} \left(A_i y_i + B_i p_i + C_i p_i^2\right) \tag{167}$$

s.t.

$$\begin{cases} \sum_{i=1}^{N} p_i = L, \\ P_i^{\min} y_i \le p_i \le P_i^{\max} y_i, \quad \forall i, \\ y_i \in \{0,1\}, \quad p_i \in \mathbb{R}, \quad \forall i, \end{cases} \tag{168}$$

where A_i, B_i, $C_i \in \mathbb{R}$ are constants of unit i; $H\left(y_i, p_i\right)$ specifies the cost of turning on unit i; y_i is a binary variable, we can assume "1" means unit i is on and "0" off. The first constraint ensures power balance and the second guarantees that unit i does not cross the limit.

In [31], a hybrid quantum-classical method, which employs quantum approximation optimization algorithm (QAOA) to turn a quadratic unconstrained binary optimization (QUBO) instance into a continuous optimization problem over variational parameters β and γ, was introduced to the UC. However, this paper only runs numerical examples on the emulator, not on the real quantum computer, and the scale of numerical examples is small, so it is difficult to show the exponential acceleration of quantum computing.

Reference [32] proposed a hybrid quantum-classical algorithm to solve the UC, which is decomposed into three subproblems, i.e., quadratic, a quadratic unconstrained binary optimization (QUBO), and an unconstrained quadratic. The first and third subproblems are solved by a classical optimization solver, and QAOA settles the QUBO subproblem. Nonetheless, the scale of the case study in this reference is relatively small, which does not really demonstrate the superiority of quantum computing.

In [33], it presented the quantum version of the decomposition and coordination alternate direction method of multipliers, which are realized by devising quantum algorithms and exploiting the superposition and entanglement of qubits for solving subproblems, which are then coordinated to obtain feasible solutions. The proposed methodology is employed to solve the microgrid UC problems that contain DERs. However, the exponential acceleration of quantum computing has not been proved in practice.

Reference [34] developed a hybrid quantum-classical (HQC) solution approach to solve the UC in order to leverage the current generation of quantum devices. The article employs a multi-cut Benders decomposition approach that exploits multiple feasible solutions of the master problem to generate multiple valid cuts, which is used as a HQC solver for general mixed-integer linear programming (MILP) problems. In simple terms, the CPU handles MILP problems, while the QPU settles the cut selection problems. The HQC optimization algorithm is applied to the UC problem by using the D-Wave Advantage 4.1 quantum annealer. The process of this algorithm is complicated and has some shortcomings. Firstly, the dependence of the size of matrix M on the number of complicating variables imposes a limit on the size of the problem. Furthermore, minor embedding has to be repeated in every iteration. Third, finding suitable hyperparameters and weights is non-trivial for the quadratic penalty functions to ensure that the lowest-energy solution and reduce logical chain breakage. We can devise more efficient minor-embedding heuristics to exploit previously generated minor embeddings to overcome some shortcoming. The efficiency of minor-embedding techniques should be surmounted and current hardware limitations must be improved before effectively applying the method to large-scale problem instances. We can also implement this algorithm on IBM real quantum computers.

In [35], a synergistic combination of quantum computing and surrogate Lagrangian relaxation (SLR) was developed to solve the UC. It proposed a Quantum-SLR (QSLR) algorithm incorporating quantum approximate optimization algorithm (QAOA)

into the SLR method. A distributed QSLR framework (DQSLR) is capable of coordinating local quantum/classical computing resources.

The authors of [36] proposed a UC formulation modeling minimal variable and starting costs, demand satisfaction as well as minimum running and idle times as a QUBO problem. The formulation reduces the number of and the connectivity between qubits. However, this formulation was only tested on the IBM Qiskit 0.37.1 QASM simulator and the D-Wave Quantum Annealer (Version Advantage system 5.2 with over 5000 qubits), not on a real gate-based quantum computer. The author of [37] advanced the method presented in [36] to solve a relaxed version of the UC. However, as in Reference [36], the this approach has not been tested on gate-based real quantum computers.

Considering that some generic mixed-integer nonlinear programming (MINLP) solvers, such as Artelys Knitro, spend a lot of time solving linear systems, these solvers have the potential to benefit from the HHL. Since the UC is essentially an MINLP, it has the potential to enjoy the benefit from HHL even without the use of the QAOA.

D. Power system reliability and stability assessment

Reference [38] proposed a quantum computing based framework for the reliability assessment of complex systems and the "Quantum Twin" concept. The framework can be applied to accelerate the reliability assessment of large-scale complex systems, such as power systems, which take a lot of computation time for classical computers to obtain accurate results. Because of the quantum decoherence and state fidelity, "Quantum Twin" usually needs error correction. For large-scale power systems, a large number of qubits are needed. With the increase of qubits, the error rate also further increases, which may influence the reliability assessment results. Therefore, we should find ways to reduce the error rate and adopt efficient methods for quantum error correction.

In [39], [40], a quantum transient stability assessment method was devised to enable efficient data-driven transient stability prediction for bulk power systems. It claims that the intractable transient stability assessment can be straightforward and effortless in the Hilbert space.

Reference [41] developed a quantum electromagnetic transients program (QEMTP), which solves electromagnetic transients through quantum computing. The HHL is employed in the program. However, currently the practicality of the QEMTP is limited by some factors such as quantum resources, depth of quantum circuit and noise of quantum computers.

Considering today's noisy intermediate-scale quantum (NISQ) computers, reference [42] proposed a NISQ-QEMTP methodology based on real quantum computers. The method employs shallow-depth quantum circuits and properly handles the state preparation and measurement obstacles, and it is executed on real quantum computers.

E. Communication and security of power systems

The security of power information systems is essential and pivotal, because power systems are important infrastructures for national economic and once the relevant power grid production and enterprise management information are leaked or tampered with, it will cause great losses to customers' privacy, power consumption security and even national information security. Quantum secure communication, based on the basic principles of quantum mechanics, has unconditional security in theory and can provide an absolutely secure information channel for the safe transmission of the power grid production and operation data. The existing security methods of power information system are mainly based on Rivest-Shamir-Adleman (RSA) and other encryption algorithms, which is facing the threat of quantum computing/quantum computers. Therefore, the application of quantum communication technology to the power system will play a crucial role in ensuring the safe, stable and efficient operation of the power grid. The security protection scheme of power communication networks based on quantum secure communication is not easy to be affected by natural environments, has low losses and good throughput performances, and has higher security and feasibility.

As quantum hardware and software advances, developing microgrids containing DERs based on quantum communication has been increasingly rising in significance [43], [44].

In [45], it presented a programmable quantum networked microgrids (PQNMs) architecture, which integrates both quantum key distribution (QKD) and software-defined networking (SDN) techniques capable of enabling scalable, programmable, quantum-engineered, and ultra-resilient networked microgrids.

References [46] proposed a QKD based microgrid distributed control framework for cybersecurity enhancement. To defend the sidechannel attacks and make the framework practical enough for industrial applications, measurement-device-independent QKD is introduced.

Reference [47] demonstrated the feasibility of using QKD to improve the security of critical infrastructure, including future DERs, such as energy storage, and proposed the quantum key-based authentication of smart grid communications across an energy delivery infrastructure environment.

In [48], it conceptually explained the feasibility and superiority of quantum computing in the field of power system security, but there is no actual case study example to prove them.

Reference [49] devised a scheme for resilient electric grids by using a quantum direct communication (QDC) network. But it has some limitations, such as decoherence of qubits and long-distance entanglement distribution issues.

References [50], [51] exploited QKD to resolve the quantum-era microgrid challenges imposed by quantum computers.

Reference [52] proposed a quantum network-based power grid (QNetGrid) framework and develops a real-time, reliable, flexible, programmable, and cost-effective QNetGrid software testbed. But there are still some challenges in implementing hardware-based quantum networks in practice, such as photon loss and the limited quantum memory performance. Reference [53] introduced potential quantum attack defense strategies including QKD and post-quantum cryptography, they can be used to DER networks and gauges defense strategies.

F. Fault diagnosis of power systems

Reference [54] proposed a quantum computing-based deep learning framework for the power system fault diagnosis. This hybrid framework conquers challenges faced by complex deep learning models. The case studies showcase the fault diagnosis method is superior and provides reliable fault diagnosis performance with faster response time.

G. Grid partitioning

Reference [57] employed integer slack (IS) and binary expansion methods to transform grid partitioning into a QUBO problem, and then leveraged quantum annealing to solve it. However, the problem is solved under the framework of quantum annealing; we can try to solve the problem on the gate based quantum computer.

H. Microgrid state estimation

Reference [61] applied the HHL to microgrid state estimation. Case studies verify the correctness of quantum microgrid state estimation.

VII. Prospects for the future work

For your convenience of reference, we summarize and classify the public literature on the applications of quantum computing in power systems, as shown in Table I. As can be seen from Table I, there are limited references on the applications of quantum computing in power systems, and they mainly focus on the UC and the power system security and so on, so it is indispensable to further explore the applications of quantum computing in the current application directions and the applications in other directions.

TABLE I
Literature summary

Application area	Main quantum algorithms	References
Power flow calculation	HHL/Quantum annealing/VQLS	[27]–[30]/ [57]/ [59]
UC	QAOA/HHL	[31]–[37]
Power system reliability and stability assessment	HHL	[38]–[42]
Communication and security of power systems	QKD	[43]–[53]
Fault diagnosis of power systems	Quantum generative training	[54]
Grid partitioning	Quantum annealing	[57]
Microgrid state estimation	HHL	[61]

Quantum computing is an interdisciplinary realm spanning physics, computer and other disciplines. Quantum computing at the current stage is referred to as the NISQ era, which is characterized by quantum processors which are sensitive to noise and are not advanced enough for fault-tolerance and achieving quantum supremacy [62], [63]. The current quantum computer is an imperfect noisy quantum computer under the NISQ framework. The running result on this type of quantum computer may not be accurate. To some extent, the accuracy of results is restricted by factors such as availability of quantum resources, noise, and executable depth of quantum circuits [64], but quantum computing, as one of the hottest technologies in the world today, offers us a new computing paradigm, which is extremely promising. But based on the current NISQ era, we can develop fault-tolerant computing and NISQ algorithms [65]. Considering the current quantum computing hardware, we can design some quantum algorithms, such as HHL-NISQ, suitable for NISQ hardware, and combine classical computers with quantum computers, and integrate classical algorithms with quantum algorithms to propose a hybrid scheme based on classical and quantum computing. In this way, the advantages of classical and quantum computing can be fully exploited, which is an appealing trick for current applications.

Specifically, there are many important directions to explore regarding the potential applications of quantum computing in power systems.

First, further work is needed to investigate the applications of quantum computing in other power system optimization problems, such as planning, economic scheduling, optimal power flow, renewable energy prediction, and energy pricing.

Second, we design hybrid algorithms based on quantum computing and classical computing, which is an important direction in the current NISQ era. This is an important step toward implementing full quantum algorithms on more powerful quantum computers in the future.

Third, further work is needed to attempt to apply some quantum machine learning algorithms, especially quantum deep learning and quantum reinforcement learning, to power systems. For example, explore the load forecasting and solar/wind forecasting based on quantum machine learning. Quantum machine learning is the fusion of quantum theory and machine learning [65]. For more information on quantum machine learning, please refer to [66]–[69].

Fourth, for quantum power communication and quantum power security, we can further demonstrate the practical feasibility and reliability of quantum network. Evaluate their performance in different operating environments.

Fifth, further work is needed to investigate the applications of quantum annealing (a heuristic, stochastic quantum algorithm, for more information about quantum annealing, please see [70], [71]) in power systems. It may be applied to the UC and the economic dispatch.

VIII. CONCLUSION

In this work, we provides an illustrated tutorial without agonizing pains, which targets power system professionals, and a systemic, in-depth, and critical survey which reviews the state-of-the-art applications of quantum computing in power systems. At the same time, we also identify the future research directions of quantum computing in power systems in order to reap the advantages of quantum computing. Advances in quantum algorithms together with better quantum hardware in the future will bring the extensive practical applications of quantum computing in bulk power systems, such as power system analysis, operation, optimization, and control. We are not studying quantum computing to replace common classical computing, let alone high performance computing, but to make quantum computing and classical computing do what they do best.

Although the applications of quantum computing in power systems are still in infancy, the present research is of great significance and lays a foundation for the large-scale applications of quantum computing in the future and can promote the frontier of solving the power system problems in a quantum architecture.

In today's NISQ era, a major challenge for quantum computing in the field of power systems is to design quantum algorithms that conform to current quantum hardware while ensuring the acceleration of quantum computing. At near-term quantum computing, combining the quantum computer with the classical computer to design the quantum algorithm is an important research direction.

The superiority of quantum computing has spawned the research on its applications. In view of the fact that quantum computing can solve certain problems considerably faster than the best known classical algorithms, it is expected to have substantial impact on the power industry. Current quantum computers are very susceptible to the influence of the ambient noise, and the running results on the real quantum computer are not very satisfactory. However, it is possible that we will have more powerful quantum computers containing more qubits in the foreseeable future, paving the way for truly large-scale applications of quantum computing. Quantum computing provides a door for the analysis and computation of power systems, and we expect quantum computing to be widely applied in much more aspects of power systems and other realms of science and engineering.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," 2010.

[2] E. G. Rieffel and W. H. Polak, *Quantum computing: A gentle introduction*. MIT Press, 2011.

[3] G. Benenti, G. Casati, and G. Strini, *Principles of quantum computation and information-volume I: Basic concepts*. World scientific, 2004.

[4] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information-Volume II: Basic Tools and Special Topics*. World Scientific Publishing Company, 2007.

[5] N. D. Mermin, *Quantum computer science: an introduction*. Cambridge University Press, 2007.

[6] A. Cowtan, S. Dilkes, R. Duncan, A. Krajenbrink, W. Simmons, and S. Sivarajah, "On the qubit routing problem," in *14th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2019.

[7] M. H. Devoret and R. J. Schoelkopf, "Superconducting circuits for quantum information: an outlook," *Science*, vol. 339, no. 6124, pp. 1169–1174, 2013.

[8] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, "A quantum engineer's guide to superconducting qubits," *Applied physics reviews*, vol. 6, no. 2, p. 021318, 2019.

[9] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical review A*, vol. 52, no. 5, p. 3457, 1995.

[10] D. E. Deutsch, A. Barenco, and A. Ekert, "Universality in quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 449, no. 1937, pp. 669–677, 1995.

[11] C. Shao, "Reconsider hhl algorithm and its related quantum machine learning algorithms," *arXiv preprint arXiv:1803.01486*, 2018.

[12] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical review letters*, vol. 103, no. 15, p. 150502, 2009.

[13] J. R. Shewchuk *et al.*, "An introduction to the conjugate gradient method without the agonizing pain," 1994.

[14] D. Dervovic, M. Herbster, P. Mountney, S. Severini, N. Usher, and L. Wossnig, "Quantum linear systems algorithms: a primer," *arXiv preprint arXiv:1802.08227*, 2018.

[15] E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," *arXiv preprint arXiv:1411.4028*, 2014.

[16] A. Adedoyin, J. Ambrosiano, P. Anisimov, A. Bärtschi, W. Casper, G. Chennupati, C. Coffrin, H. Djidjev, D. Gunter, S. Karra, *et al.*, "Quantum algorithm implementations for beginners," *arXiv preprint arXiv:1804.03719*, 2018.

[17] J. Choi and J. Kim, "A tutorial on quantum approximate optimization algorithm (qaoa): Fundamentals and applications," in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 138–142, IEEE, 2019.

[18] T. Gabor, M. L. Rosenfeld, C. Linnhoff-Popien, and S. Feld, "How to approximate any objective function via quadratic unconstrained binary optimization," in *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 1249–1257, IEEE, 2022.

[19] F. Glover, G. Kochenberger, and Y. Du, "Quantum bridge analytics i: a tutorial on formulating and using qubo models," *4OR*, vol. 17, pp. 335–371, 2019.

[20] E. National Academies of Sciences, Medicine, *et al.*, "Quantum computing: progress and prospects," 2019.

[21] D. J. Tylavsky and G. T. Heydt, "Quantum computing in power system simulation," in *2003 IEEE Power Engineering Society General Meeting (IEEE Cat. No. 03CH37491)*, vol. 2, pp. 950–956, IEEE, 2003.

[22] A. Ajagekar and F. You, "Quantum computing and quantum artificial intelligence for renewable and sustainable energy: A emerging prospect towards climate neutrality," *Renewable and Sustainable Energy Reviews*, vol. 165, p. 112493, 2022.

[23] R. Eskandarpour, K. J. B. Ghosh, A. Khodaei, A. Paaso, and L. Zhang, "Quantum-enhanced grid of the future: A primer," *IEEE Access*, vol. 8, pp. 188993–189002, 2020.

[24] A. Giani and Z. Eldredge, "Quantum computing opportunities in renewable energy," *SN Computer Science*, vol. 2, no. 5, p. 393, 2021.

[25] A. Ajagekar and F. You, "Quantum computing for energy systems optimization: Challenges and opportunities," *Energy*, vol. 179, pp. 76–89, 2019.

[26] Y. Zhou, Z. Tang, N. Nikmehr, P. Babahajiani, F. Feng, T.-C. Wei, H. Zheng, and P. Zhang, "Quantum computing in power systems," *iEnergy*, 2022.

[27] R. Eskandarpour, K. Ghosh, A. Khodaei, L. Zhang, A. Paaso, and S. Bahramirad, "Quantum computing solution of dc power flow," *arXiv preprint arXiv:2010.02442*, 2020.

[28] R. Eskandarpour, K. Ghosh, A. Khodaei, and A. Paaso, "Experimental quantum computing to solve network dc power flow problem," *arXiv preprint arXiv:2106.12032*, 2021.

[29] F. Feng, Y. Zhou, and P. Zhang, "Quantum power flow," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3810–3812, 2021.

[30] B. Sævarsson, S. Chatzivasileiadis, H. Jóhannsson, and J. Østergaard, "Quantum computing for power flow algorithms: Testing on real quantum computers," *arXiv preprint arXiv:2204.14028*, 2022.

[31] S. Koretsky, P. Gokhale, J. M. Baker, J. Viszlai, H. Zheng, N. Gurung, R. Burg, E. A. Paaso, A. Khodaei, R. Eskandarpour, *et al.*, "Adapting quantum approximation optimization algorithm (qaoa) for unit commitment," in *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pp. 181–187, IEEE, 2021.

[32] R. Mahroo and A. Kargarian, "Hybrid quantum-classical unit commitment," in *2022 IEEE Texas Power and Energy Conference (TPEC)*, pp. 1–5, IEEE, 2022.

[33] N. Nikmehr, P. Zhang, and M. A. Bragin, "Quantum distributed unit commitment: An application in microgrids," *IEEE transactions on power systems*, vol. 37, no. 5, pp. 3592–3603, 2022.

[34] N. G. Paterakis, "Hybrid quantum-classical multi-cut benders approach with a power system application," *arXiv preprint arXiv:2112.05643*, 2021.

[35] F. Feng, P. Zhang, M. A. Bragin, and Y. Zhou, "Novel resolution of unit commitment problems through quantum surrogate lagrangian relaxation," *IEEE Transactions on Power Systems*, 2022.

[36] P. Halffmann, P. Holzer, K. Plociennik, and M. Trebing, "A quantum computing approach for the unit commitment problem," *arXiv preprint arXiv:2212.06480*, 2022.

[37] M. Braun, T. Decker, N. Hegemann, S. Kerstan, and F. Lorenz, "Towards optimization under uncertainty for fundamental models in energy markets using quantum computers," *arXiv preprint arXiv:2301.01108*, 2023.

[38] S. You, "A quantum computing framework for complex system reliability assessment," *arXiv preprint arXiv:2012.03919*, 2020.

[39] Y. Zhou and P. Zhang, "Noise-resilient quantum machine learning for stability assessment of power systems," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 475–487, 2022.

[40] Y. Zhou and P. Zhang, "Quantum machine learning for power system stability assessment.," *arXiv preprint arXiv:2104.04855*, 2021.

[41] Y. Zhou, F. Feng, and P. Zhang, "Quantum electromagnetic transients program," *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3813–3816, 2021.

[42] Y. Zhou, P. Zhang, and F. Feng, "Noisy-intermediate-scale quantum electromagnetic transients program," *IEEE Transactions on Power Systems*, 2022.

[43] Z. Tang, P. Zhang, and W. O. Krawec, "A quantum leap in microgrids security: The prospects of quantum-secure microgrids," *IEEE Electrification Magazine*, vol. 9, no. 1, pp. 66–73, 2021.

[44] J. Ahn, J. Chung, T. Kim, B. Ahn, and J. Choi, "An overview of quantum security for distributed energy resources," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, pp. 1–7, IEEE, 2021.

[45] Z. Tang, P. Zhang, W. O. Krawec, and Z. Jiang, "Programmable quantum networked microgrids," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–13, 2020.

[46] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-key-distribution-based microgrid control for cybersecurity enhancement," *IEEE Transactions on Industry Applications*, vol. 58, no. 3, pp. 3076–3086, 2022.

[47] M. Alshowkan, P. Evans, M. Starke, D. Earl, and N. Peters, "Quantum key distribution-bootstrapped authentication for secure communication of distributed energy resources," *arXiv e-prints*, pp. arXiv–2110, 2021.

[48] R. Eskandarpour, P. Gokhale, A. Khodaei, F. T. Chong, A. Passo, and S. Bahramirad, "Quantum computing for enhancing grid security," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4135–4137, 2020.

[49] Z. Jiang, Z. Tang, Y. Qin, C. Kang, and P. Zhang, "Quantum internet for resilient electric grids," *International Transactions on Electrical Energy Systems*, vol. 31, no. 6, p. e12911, 2021.

[50] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1250–1263, 2020.

[51] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure networked microgrids," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, pp. 1–5, IEEE, 2020.

[52] Z. Tang, P. Zhang, W. Krawec, and L. Wang, "Quantum networks for resilient power grids: Theory and simulated evaluation," *IEEE Transactions on Power Systems*, 2022.

[53] J. Ahn, H.-Y. Kwon, B. Ahn, K. Park, T. Kim, M.-K. Lee, J. Kim, and J. Chung, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (pqc) and quantum key distribution (qkd)," *Energies*, vol. 15, no. 3, p. 714, 2022.

[54] A. Ajagekar and F. You, "Quantum computing based hybrid deep learning for fault diagnosis in electrical power systems," *Applied Energy*, vol. 303, p. 117628, 2021.

[55] B. Stott, J. Jardim, and O. Alsaç, "Dc power flow revisited," *IEEE Transactions on Power Systems*, vol. 24, no. 3, pp. 1290–1300, 2009.

[56] B. Stott and O. Alsac, "Fast decoupled load flow," *IEEE transactions on power apparatus and systems*, no. 3, pp. 859–869, 1974.

[57] T. Morstyn, "Annealing-based quantum computing for combinatorial optimal power flow," *IEEE Transactions on Smart Grid*, 2022.

[58] S. Heng, D. Kim, T. Kim, and Y. Han, "How to solve combinatorial optimization problems using real quantum machines: A recent survey," *IEEE Access*, vol. 10, pp. 120106–120121, 2022.

[59] F. Feng, Y. Zhou, and P. Zhang, "Noise-resilient quantum power flow," *arXiv preprint arXiv:2211.10555*, 2022.

[60] C. Bravo-Prieto, R. LaRose, M. Cerezo, Y. Subasi, L. Cincio, and P. Coles, "Variational quantum linear solver: A hybrid algorithm for linear systems," *Bulletin of the American Physical Society*, vol. 65, 2020.

[61] F. Feng, P. Zhang, Y. Zhou, and Z. Tang, "Quantum microgrid state estimation," *Electric Power Systems Research*, vol. 212, p. 108386, 2022.

[62] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[63] M. Brooks, "Beyond quantum supremacy: the hunt for useful quantum computers," *Nature*, vol. 574, no. 7776, pp. 19–22, 2019.

[64] S. Aaronson, "Read the fine print," *Nature Physics*, vol. 11, no. 4, pp. 291–293, 2015.
[65] K. Bharti, A. Cervera-Lierta, T. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. Kottmann, T. Menke, *et al.*, "Noisy intermediate-scale quantum (nisq) algorithms (2021)," *arXiv preprint arXiv:2101.08448*, 2021.
[66] P. Wittek, *Quantum machine learning: what quantum computing means to data mining*. Academic Press, 2014.
[67] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning," *Contemporary Physics*, vol. 56, no. 2, pp. 172–185, 2015.
[68] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.
[69] S. Arunachalam and R. de Wolf, "A survey of quantum learning theory," *arXiv preprint arXiv:1701.06806*, 2017.
[70] D. de Falco and D. Tamascelli, "An introduction to quantum annealing," *RAIRO-Theoretical Informatics and Applications*, vol. 45, no. 1, pp. 99–116, 2011.
[71] S. Yarkoni, E. Raponi, T. Bäck, and S. Schmitt, "Quantum annealing for industry applications: Introduction and review," *Reports on Progress in Physics*, 2022.