Chinese Journal of Physics 72 (2021) 248–269

Contents lists available at ScienceDirect

Chinese Journal of Physics

journal homepage: www.sciencedirect.com/journal/chinese-journal-of-physics

Quantum computation: Algorithms and Applications

Chien-Hung Cho [a,*], Chih-Yu Chen [a], Kuo-Chin Chen [b], Tsung-Wei Huang [c], Ming-Chien Hsu [b,d], Ning-Ping Cao [e,f], Bei Zeng [g], Seng-Ghee Tan [h], Ching-Ray Chang [i]

[a] Department of Physics, National Taiwan University, Taipei, Taiwan
[b] Quantum Computing Research Center, Hon Hai Research Institute, Taipei, Taiwan
[c] Department of Information and Computer Engineering, Chung Yuan Christian University, Chungli, Taiwan
[d] Department of Physics, National Sun Yat-sen University, Kaohsiung, Taiwan
[e] Department of Mathematics & Statistics, University of Guelph, Guelph N1G 2W1, ON, Canada
[f] Institute for Quantum Computing, University of Waterloo, Waterloo N2L 3G1, ON, Canada
[g] Department of Physics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China
[h] Department of Optoelectric Physics, Chinese Culture University, 55 Hwa-Kang Road, Yang-Ming-Shan, Taipei, Taiwan
[i] Graduate Institute of Applied Physics and NTU-IBM Quantum Hub, National Taiwan University, Taipei, Taiwan

ARTICLE INFO

Keywords:
Quantum algorithm
Quantum computation
Applications

ABSTRACT

As the prospect of commercial quantum computers turns ever more real in recent times, research in quantum algorithms becomes the center of attention. Due to the strong parallelism of quantum computing in Hilbert space, ordinarily intractable calculation problems could now be solved very efficiently with non-classical means. To exploit parallelism, creative quantum algorithms are required so that efficient quantum oracles can be tailor-designed to specific computation needs. Therefore, in the quest for quantum supremacy, quantum algorithms and their related applications are as important as the quantum computer hardware. This article covers the basic concepts of quantum computation and reviews some important quantum algorithms and their applications.

1. INTRODUCTION

1.1. Overview of quantum computation

The concept of quantum computers was first proposed by Richard Feynman in 1982 [1] to simulate the complex physical systems. Although the rapid development of classical computers enables theoretical physicists to numerically study and calculate the basic properties of various states of matter [2], calculating the real physical system with a great number of electrons is still an intractable problem even to the most advanced classical computers. For example, it is easy to simulate a two-level quantum state spanned by the basis states of $|0\rangle$ and $|1\rangle$; but in the case of n quantum states, the Hilbert dimension of the state rises to 2^n , and the exponential growth makes the simulation even harder. In the late 1970s, Feynman published a paper titled "Simulating Physics with Computers" [1], advancing the point that a quantum computer must be built in order to simulate the complex quantum system. However, the concept of quantum computers was for years limited to mostly theoretical work because of the lack of means to perform the function of a quantum bit, ubiquitously known as the qubit today. Recently, the technology of quantum computing hardware achieved rapid breakthroughs.

* Corresponding author.
E-mail address: f06222035@ntu.edu.tw (C.-H. Cho).

https://doi.org/10.1016/j.cjph.2021.05.001
Received 21 November 2020; Received in revised form 30 April 2021; Accepted 1 May 2021
Available online 8 May 2021

In 2016, IBM placed the first 5-qubit quantum computer on the cloud [3] and launched an open-source framework aka the Qiskit [4], so that everyone could access it using his/her own computers. The IBM initiative promotes the rapid development of quantum algorithms and practical applications, and increases the number of users on the IBMQ Experience. Meanwhile, different kinds of hardware for quantum computation are under development as well [5-7] and related technologies have achieved great progress as well, for example, quantum state transfer(QST) [8], qubit controlled [9], etc.

Since we are in the era of Noisy-Intermediate-Scale-Quantum (NISQ) [10], demonstrating the superiority of quantum computers over classical computers, and finding near-term quantum computing applications are the main issues. Recently, Google used a 53-qubit quantum processor, named Sycamore, to showcase quantum supremacy – it takes just 200 s for the Sycamore to complete a task that would take the current state-of-the-art classical supercomputer around 10,000 years [11]. While IBM argues the same task can be completed in 2.5 days on classical computers with great fidelity [12] and a team from the Chinese Academy of Sciences claims to achieve fidelity higher than those in Google's experiments [13], the work done by Google is still a landmark in the development of quantum computing. On the other hand, finding useful near-term applications of quantum computing relies on the new design of quantum algorithm: for example, hybrid quantum-classical algorithms are designed to run on the NISQ devices which have limited circuit width and depth [14], or incorporate the machine-learning techniques [15, 16]. In the meantime, error mitigation methods are proposed to suppress errors in these applications on NISQ devices. To date, there are 420 related papers being cited on the "Quantum algorithm Zoo" website, and many excellent articles introduce quantum algorithms with great details [17, 18]. In this paper, we will not cover all of them but review several common algorithms.

This review article is constructed as follows: we first outline the history of quantum computation and provide the concept of basic physics and mathematics for quantum computation in Section 1. The introduction of several quantum algorithms and quantum error mitigation is given in Section 2. In the last part (Section3), we conclude the article with some perspectives and future directions.

Table 1

1.2. History of quantum computations

In 1982, Richard Feynman first proposed to build a quantum machine that follows quantum laws to simulate the real quantum system problems. A few years later, in 1985, David Deutsch proposed the idea of Quantum Turing machine and stated the Church-Turing-Deutsch principle [19]: Every physics process can be simulated by universal quantum computing devices, but to efficiently solve problems in the real world, quantum computers need well-designed quantum algorithms. Deutsch algorithm is the first quantum algorithm proposed by David Deutsch in 1985 and its generalized algorithm, Deutsch-Jozsa algorithm, is developed by David Deutsch and Richard Jozsa in 1992 [20]. Deutsch-Jozsa algorithm needs just one evaluation of the function to distinguish whether the function is constant or balanced, where a constant function means that the outputs of the function are either all 0 or all 1, and a balanced function means there is an equal number of 1 s and 0 s on the outputs. Deutsch-Jozsa algorithm is one of the examples that show exponentially faster computation than the classical algorithm in the constant-balanced problem [21]. In 1992, Ethan Bernstein and Umesh Vazirani proposed the Bernstein–Vazirani algorithm [22]. This algorithm is able to find the secret string of bits which gives the dot product of the secrete string. The same problem needs to use m bits to find out each bit in the secret string. Simon's algorithm was created by Daniel Simon in 1994, and the algorithm shows exponentially faster computation than the classical algorithm in finding s, for the function $f(x) = f(x \oplus s)$ [21]. Both Deutsch's and Simon's algorithms show the advantages of quantum computing over classical. However, these algorithms are limited to solving only very specific problems, thus having very little practical value.

The real breakthrough comes with the appearance of the Shor's algorithm in 1994 [23]. Shor's algorithm is exponentially faster than classical algorithms in terms of factoring integers, which can be used to break the asymmetry encryption system, RSA (Rivest–Shamir–Adleman). We will introduce the details for Shor's algorithm in the next section. Another breakthrough in the late 20th century was Grover's algorithm in 1996 [24]. Grover's algorithm is more effective and faster for searching an unstructured database than the classical algorithm, performing just $O(\sqrt{N})$ evaluations of the function, where N is the size of the database. In 2008, Aram Harrow, Avinatan Hassidim, and Seth Lloyd developed the quantum algorithm, called the HHL algorithm, which utilizes the Quantum-Fourier transform as its subroutine to solve linear equation systems [25]. HHL algorithm aims to solve linear equations which can be beneficial to many science and engineering fields, for instance, machine learning.

The appearance of NISQ device means we have actual quantum devices but with noise. In order to find near-term applications,

Table 1
Major quantum algorithms and their possible applications.

Core computing algorithm	The name of algorithms	Applications	Potential application field
Quantum Fourier Transform (QFT)	Shor's algorithm	RSA decryption	Cryptography
	HHL	Inverse transform of a matrix	Machine learning
Grover's operator	Grover's algorithm	Search problem	Search in unsorted databases
Quantum-classical hybrid methods	Variational Quantum Eigensolver (VQE)	Eigensolver	New material finding Medicine industry
	Quantum Approximate optimization algorithm (QAOA)	Optimization	Financial industry Satisfiability problems
Quantum adiabatic algorithm	Quantum Annealing algorithm	Optimization	Computing science Machine learning Financial industry

apart from those described above, hybrid quantum algorithms are also one of the main directions in the NISQ era. The hybrid algorithms include the VQE (Variation Quantum Eigensolver) [26], and the QAOA (Quantum Approximate Optimization Algorithm) [27]. The VQE algorithm is designed to solve problems in chemistry simulation, where the variational principle is applied, and optimization is performed by the classical computers to find the ground state for a given Hamiltonian [26]. The QAOA is on the hand applied to solve the Max-Cut problems or some combinatorial problems [27]. Another important quantum algorithm is the QAA (Quantum Annealing Algorithm) which can be realized on the special quantum annealing device, for example the quantum annealer made by D-wave [28].

1.3. Basic concepts of quantum computations

Quantum computer as well as the principle of quantum computing are based on the physics of a two-level quantum system. Here, we will not review all the required concepts of quantum mechanics, but only the essential quantum principles and the basic mathematics required to illustrate the working of quantum computation.

Quantum logical gates or quantum operators are similar in concepts to the logical gates of a classical computer. However, the realization of quantum gates follows the Schrödinger equation, $H(t)\psi(t) = i\hbar\frac{\partial}{\partial t}\psi(t)$, where $H(t)$ is the Hamiltonian of the systems with control parameters and $\psi(t) = e^{-iHt/\hbar}\psi(0)$ is the energy state in the system. In the quantum computer, by manipulating the control parameters and operating time, special operators can be constructed, for example, the Hadamard, Pauli, and CNOT gates. It should be mentioned that there is an infinite number of ways to obtain operator sequences for a quantum computing process, but in "noisy" quantum computers, it is necessary to make the operation time as short as possible to avoid the destruction of quantum states due to the environments. The quantum state, ψ, lies in the span of eigenstates. For example, in a two-energy level quantum system, ψ can be represented as the linear combination of $|0\rangle$ and$|1\rangle$. The states that lie in the vector space spanned by $|0\rangle$ and $|1\rangle$ are called qubits, which is totally different from the classical bits of 0 and 1.

The mathematical models for describing the quantum system is introduced in this section. The mathematic model for quantum computation is based on the linear algebra, which is a branch of mathematics related to the linear transformation of the state vectors. A notable linear vector space describing quantum mechanics is known as the Hilbert space, which is a complete inner product space. We will describe two important concepts in the design of quantum algorithm: qubits and quantum gates. The primary differences between qubits and the classical bits lie mainly in the physics of superposition and entanglement in the qubits. Because a single qubit has just two energy levels, the superposition state can be expressed as a linear combination of its energy eigenstates as follows:$|\psi = a|0\rangle + b|1\rangle$, where a and b are complex number with the condition $|a|^2 + |b|^2 = 1$. This unique property cannot appear in the classical bits. A multi-qubit system can be described as the tensor product of the many single qubits as follows: $|\psi\rangle = |\psi_1\rangle \oplus |\psi_2\rangle \cdots \oplus |\psi_n\rangle$, where n is the number of qubits and $|\psi_i\rangle$=$a_i|0\rangle + b_1|1\rangle$ describe the superposition state of the i-th single qubit. The tensor product of the single qubits forms a Hilbert space and each vector in the standard basis can be described as $|c_1c_2\ldots c_n\rangle$ where $c_i = 0$ or 1 is the state of the i-th single qubit. The dimension of the Hilbert space is $N = 2^n$, thus each vector in the standard basis can also be expressed as $|x_i\rangle$ for $i = 0, 1, \ldots, N-1$ with coefficients α_i. The multi-qubit system is expressed as follows:

$$|\psi\rangle = |\psi_1\rangle \oplus |\psi_2\rangle \cdots \oplus |\psi_n\rangle = (a_1|0\rangle + b_1|1\rangle) \oplus (a_2|0\rangle + b_2|1\rangle) \oplus \cdots \oplus (a_n|0\rangle + b_n|1\rangle) = \alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-1}|11\cdots1\rangle = \sum_{i=0}^{N-1}\alpha_i|x_i = [\alpha_0, \alpha_1, \ldots, \alpha_{N-1}]$$

The multi-qubit system above is defined as separable because its quantum state could be expressed as a tensor product of the individual sub-states. When a system state could not be expressed as a tensor product of the individual sub-states, we call the state entangled. It is indeed another notable property of the quantum computer.

To be more specific, $|\psi\rangle$ lies in $\mathbb{C}^N$, that is a Hilbert space with $\forall\ |\psi_a\rangle = \sum_{i=0}^{N-1}\alpha_i|x_i\rangle, |\psi_b\rangle = \sum_{i=0}^{N-1}\beta_i|x_i\rangle$ defined by the inner product function $\langle\psi_a|\psi_b\rangle = \sum_{i=0}^{N-1}\alpha_i{}^*\beta_i$, vector sum operator $|\psi_a\rangle + |\psi_b\rangle = \sum_{i=0}^{N-1}(\alpha_i + \beta_i)|x_i\rangle$, and scalar multiplication $a^*|\psi_a\rangle = \sum_{i=0}^{N-1}a^*\alpha_i|x_i\rangle$.

The quantum gate is an operator in $\mathbb{C}^N$ and could be described by a unitary matrix U ($UU^\dagger = I$ where $U^\dagger$ is the complex conjugate of U). It transforms a vector $|\psi_a\rangle$ that lies in $\mathbb{C}^n$ to another vector $|\psi_b\rangle$ by a mathematical operation of $U|\psi_a\rangle = |\psi_b\rangle$. There are some notable properties of the unitary matrices:

1 The unitary matrix preserves their inner product

$$\langle U\psi_a|U\psi_b\rangle = \langle\psi_a|\psi_b\rangle,\ \forall|\psi_a\rangle\ ,|\psi_b\rangle \in \mathbb{C}^{nN}$$

2 2. U is diagonalizable according to the spectral theorem.
3 Determinant of U=*1*
4 U can be expresses as matrix exponential of a Hermitian matrix H. ($U = e^{iH}$)
5 The eigenspaces of U are orthogonal.
6 U is normal ($UU^\dagger = U^\dagger U$).

2. QUANTUM ALGORITHMS AND THEIR APPLICATIONS

2.1. Quantum fourier transformation

Quantum Fourier transformation has many applications, such as breaking the cryptosystems and solving problems of linear systems. Breaking the cryptosystems is a NP complete problem (one that could not be solved in polynomial time) in classical computers. Keys to breaking the cryptosystems are solving hidden subgroup problems that includes problems such as factoring, discrete logarithm, graph isomorphism, and the shortest vector Peter Shor [23] has claimed in 1997 that factoring and discrete logarithm can be solved in polynomial time with the help of quantum Fourier transform. A famous branch of the theory, Shor's algorithm, can break an RSA cryptosystem by factorizing a natural number. Shor's algorithm is equivalent to the hidden subgroup problem for finite Abelian groups $\mathbb{Z}$ and the procedure will be presented later.

Another important application is solving problems of linear systems. Harrow, Hassidim and Lloyd (HHL) in 2009 [25] provided a way of solving the linear systems in a given quantum state. Nevertheless, solving the linear systems is not a NP complete problem in classical algorithm. The HHL algorithm still provides better complexity in $O(log(N))$ in comparison with the complexity $O(N^3)$ of classical algorithm (Gaussian elimination).

The quantum Fourier transform is a linear transformation on the state of qubits. The state of a quantum system can be expressed as $\sum_{j=0}^{2^n-1} x_j|j\rangle$, where $|j\rangle$ is the state of a n-qubit system. The quantum Fourier transform acting on the orthonormal basis states $|j\rangle \in \{|0\rangle \cdots |2^n-1\rangle\}$ is given by

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{2^n-1} |k\rangle exp\left[\frac{2\pi i}{N} k \cdot j\right] \tag{1}$$

The quantum state $|j\rangle$ lies in a complex vector space of dimension $N = 2^n$, and j could be expressed as binary form $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^{n-n}$. It is convenient to denote j as series of number $j_1 j_2 \cdots j_n$. The quantum Fourier transform acting on the quantum state $|j\rangle = |\sum_{a=1}^{n} j_a 2^{n-a}\rangle = |j_1 j_2 \cdots j_n\rangle$ is expressed as the following:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle exp\left[\frac{2\pi i}{N} k \cdot j\right] = \frac{1}{\sqrt{N}} \left[|0\rangle + exp\left[2\pi i \cdot j_n \cdot 2^{-1}\right]|1\rangle\right] \otimes \left[|0\rangle + exp\left[2\pi i \cdot \left(j_{n-1} \cdot 2^{-1} + j_n \cdot 2^{-2}\right)\right]|1\rangle\right] \otimes$$

$$\cdots \otimes \left[|0\rangle + exp\left[2\pi i \cdot \left(\frac{j_1}{2} + \frac{j_2}{4} + \cdots + \frac{j_n}{2^n}\right)\right]|1\rangle\right] \tag{2}$$

It is convenient to define the expression $\frac{j_1}{2} + \frac{j_2}{4} + \cdots + \frac{j_n}{2^n}$ as $0.j_1 j_2 \cdots j_n$. Then we have a clean form of quantum Fourier transform

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} [|0\rangle + exp[2\pi i \cdot 0.j_n]|1\rangle] \otimes [|0\rangle + exp[2\pi i \cdot 0.j_{n-1} j_n]|1\rangle] \otimes \cdots$$

$$\otimes [|0\rangle + exp[2\pi i \cdot 0.j_1 j_2 \cdots j_n]|1\rangle] \tag{3}$$

The quantum Fourier transform can be constructed by the Hadamard gate $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $R_k = \begin{bmatrix} 1 & 0 \\ 0 & exp[2\pi i/2^k] \end{bmatrix}$ as follows circuit: Fig. 1

The quantum Fourier transform is a key procedure in the performance of phase estimation. We could think of the phase estimation as a subroutine to perform some algorithms such as amplitude estimation [29] and quantum counting algorithm [30] etc. Suppose we have a unitary operator U and its eigenstate $|u\rangle$ such that $U|u\rangle = e^{2\pi i \cdot \phi}|u\rangle$. The purpose of phase estimation is to determine the binary expression of $\phi \approx 0.\phi_1 \phi_2 \cdots \phi_t$ (note that $\frac{\phi_1}{2} + \frac{\phi_2}{4} + \cdots + \frac{\phi_t}{2^t} + O(2^{-t}) = 0.\phi_1 \phi_2 \cdots \phi_t + O(2^{-t})$ with accuracy 2^{-t}. The selection of the unitary operator U is determined by the problems, for example, quantum counting algorithm adopt the Grover operator as the unitary operator U to determine the number of selected states in the Grover search problem [30].

Here we address the standard procedure in the performance of phase estimation. Suppose we could design an oracle to encode the

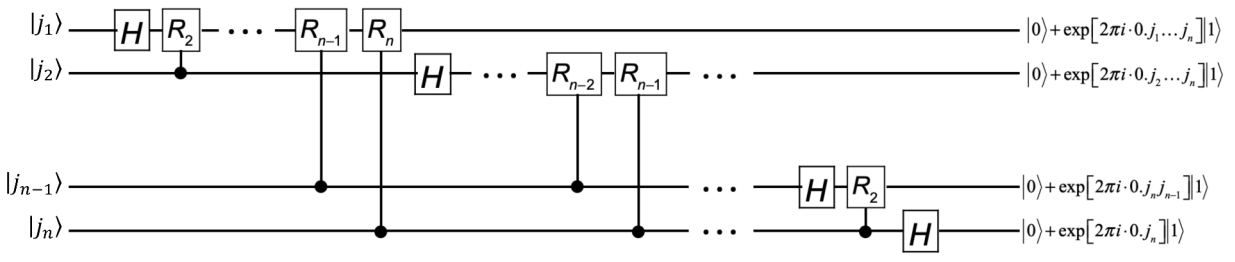

Fig. 1. Quantum circuit of Quantum Fourier transform.

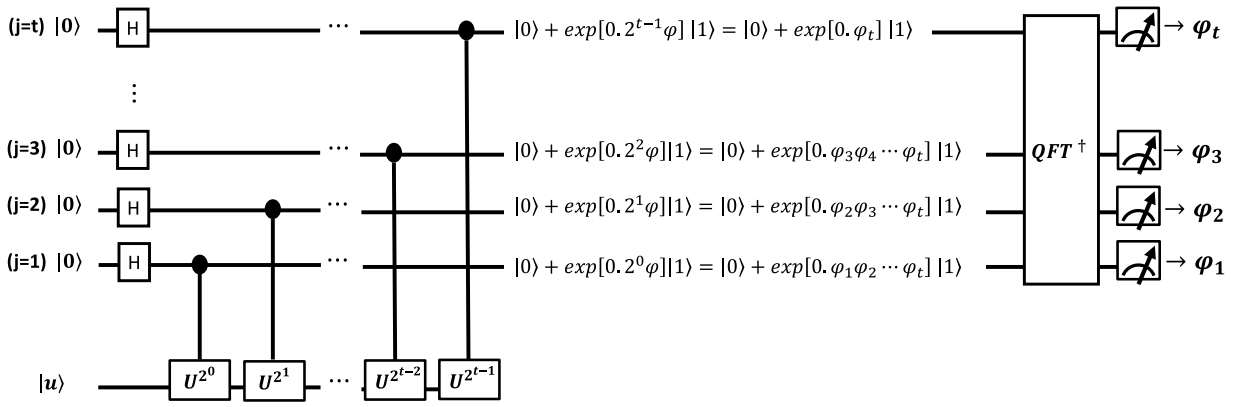

Fig. 2. Quantum circuit of Quantum phase estimation.

eigenstate $|u\rangle$and perform the controlled-$U^{2^{j-1}}$, we can then apply the quantum circuit described in Fig 2. to perform phase estimation. The quantum circuit contains two registers. The first register uses t qubits initially in the state $|0$. The quantity of qubits t is related to the accuracy we desired and the successful probability of performing phase estimation [31]. The Hadamard gates then transform each qubit in the first register. Each qubit with superposition state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ is then fed into a controlled-$U^{2^{j-1}}$ gate, where j is the label of the qubit in the first register, and the second register is initially in the eigenstate $|u\rangle$ of unitary operator U. Finally, we apply the inverse quantum Fourier transform on the first register and measure the entangled quantum state. We could obtain t bit strings $(\phi_1, \phi_2, \cdots, \phi_t)$ and ϕ could be approximated to be $\phi \approx 0.\phi_1\phi_2\cdots\phi_t$ with the accuracy 2^{-t} .

2.1.1. Shor's algorithm

Prime factorization is actually an NP problem that classical computer cannot necessarily solve more efficiently [32]. Peter Shor provided an algorithm that could solve the problem in polynomial time by using quantum computers [23]. The realization of a scalable Shor's algorithm exhibits the factorization of the number 15 using an ion-trap quantum computer [33] and the number 21 by Bulk optics [34]. In comparison with classical computer, a number with 768 bits could be factorized by using hundreds of classical computers with a runtime of 2 years [35]. The basic constrain of a quantum computer is the lack of qubits as well as the effects of quantum noise.

Factoring a composite integer number N into two coprime numbers is the main purpose of the Shor's algorithm. Shor's algorithm contains two parts. The first part is picking a random number a that is between 1 and N, and then checking for the greatest common divider $\gcd(N, a)$ of N and a. If $\gcd(N, a) \neq 1$, then this number is a nontrivial factor of N, which means that one has solved the problem. If $\gcd(N,a) = 1$, then one needs to find a positive natural even number r such that $a^r \equiv 1 \ (mod\ N)$. If $a^r \equiv 1 \ (mod\ N)$, then one could conclude that $(a^{r/2}-1)(a^{r/2}+1) = Nd$ for any pick of a natural number d. Therefore, $(a^{r/2}-1)$ and $(a^{r/2}+1)$ could contain nontrivial factors of N, and one would have solved the problem.

The hardest part of this algorithm is finding a positive natural number r such that $a^r \equiv 1 \ (mod\ N)$ and r is even. This part is an NP complete problem on classical computers, and a quantum computer could solve this within polynomial time. Next, we will address the procedure of this algorithm. A classical computer could solve the remainder part of this algorithm easily.

The quantum circuit for finding a positive natural number r consists of two registers: the first register determines the precision of the output with $2n$ qubits ($n = \log_2 N$), and the second register performs modular arithmetic with n qubits. The first step is applying Hadamard gates on the first register (i.e., set it to $|0\rangle$ initially) to produce a superposition over all states and leave the second register (i.e., set it to be $|00\cdots1\rangle$ initially) unchanged. The initial state of both registers is thus $|\psi_0\rangle = \frac{1}{2^n}\sum_{x=0}^{2^{2n}-1}|x\rangle \otimes |1\rangle$. The second step is applying control unitary gate on both register with the relation $U(|x\rangle \otimes |1\rangle) = |x\rangle \otimes |a^x \ (mod\ N)\rangle$. The superposition state can be expressed as $|\psi_1\rangle = \frac{1}{2^n}\sum_{x=0}^{2^{2n}-1}|x\rangle \otimes |a^x \ (mod\ N)\rangle$. The last step is applying inverse quantum Fourier transform to the first register, then state can be expressed as

$$|\psi_2\rangle = \frac{1}{2^n}\sum_{x=0}^{2^{2n}-1}\sum_{y=0}^{2^{2n}-1} exp\left[\frac{-2\pi i}{2^{2n}}x\cdot y\right]|y\rangle \otimes |a^x \ (mod\ N)\rangle. \tag{4}$$

After performing a measurement, we have "$|y\rangle$" and "$|a^{x_m} \ (mod\ N)\rangle$", so the probability of a certain measuring state $|y\rangle \otimes |a^{x_m} \ (mod\ N)\rangle$ could be represented by:

$$\left|\frac{1}{2^n}\sum_{\{\forall x \ s.t. \ \ a^x = a^{x_m} \ (mod\ N)\}} exp\left[\frac{-2\pi i}{2^{2n}}x\cdot y\right]\right|^2 \tag{5}$$

Due to the periodic property of $|a^x \ (mod\ N)\rangle$, we denote the period r such that $a^x = a^{x+r} \ (mod\ N) \ \forall\ x \in [0, 1, \cdots, 2^{2n}]$. Then the probability of the state which we measured is

$$\left|\frac{1}{2^{2n}}\sum_{b=0}^{k-1} exp\left[\frac{-2\pi i}{2^{2n}}(x_0 + b\cdot r)\cdot y\right]\right|^2 = \frac{1}{2^{4n}}\left|\sin\left(k\frac{\pi r y}{2^{2n}}\right)\Big/\sin\left(\frac{\pi r y}{2^{2n}}\right)\right|^2 \tag{6}$$

, where $x_0 = min\{\forall x\ s.t.\ \ a^x = a^{x_m}\ (mod\ N)\}$ and b is a positive integer number for a certain k. The probability of the state could be represented as a function of y. The probability is as high as $\frac{r\cdot y}{2^{2n}} = c \in \mathbb{N}$. Then y could be solved by the continued fraction expansion algorithm with classical computers easily.

2.1.2. HHL algorithm

HHL algorithm was proposed by Aram Harrow, Avinatan Hassidim and Seth Lloyd in 2009. This algorithm uses quantum phase estimation which is an application of quantum Fourier transform to solve some linear systems problem with exponential speedup [25].

The algorithm aims to solve the inverse linear transformation

$$A|x\rangle = |b\rangle \rightarrow |x\rangle = A^{-1}|b\rangle \tag{7}$$

, where A is a Hermitian $N \times N$ matrix, $|b\rangle$ is a given unit vector, and $|x\rangle$ is to be determined.

For a given matrix A, theoretically, we can express it in diagonal form,

$$A = \sum_j a_j |u_j\rangle\langle u_j| \tag{8}$$

The given vector $|b\rangle$ can also be written as the linear combinations of eigenvectors of A,

$$|b\rangle = \sum_j b_j |u_j\rangle \tag{9}$$

Then $|x\rangle$ can be written as

$$|x\rangle = A^{\dagger}|b\rangle = \sum_j \frac{b_j}{a_j}|u_j\rangle \tag{10}$$

In the original paper, they consider the case that there is no need to know the details of $|x\rangle$, and then we can approximately obtain the expectation value of operators $\langle x|M|x\rangle$ [25]. Detailed procedures of the HHL algorithm is provided in the following part.

The total qubits are prepared for three parts: input registers for encoding the vector $\overrightarrow{b}$ onto the state $|b\rangle$, clock register for encoding the eigenvalues of A, and the rest for ancilla registers.

I Encode the vector $|b\rangle$ onto input register, and we can denote it as the linear combination of eigenvectors of A which we denoted them as $|u_j\rangle_{input}$,

$$|b\rangle = \sum_j b_j |u_j\rangle_{input} \tag{11}$$

II Use quantum gates to construct the operator $U = e^{iAt}$. Operate Quantum Phase estimation on clock registers and input registers with the operator $U = e^{iAt}$, and then we can have eigenvalues of A encoded onto clock registers.

$$\sum_{j=1}^{N-1} b_j |a_{j\,clock}|u_{j\,input} \tag{12}$$

III Implement a rotation condition on ancilla registers which is conditioned on clock register $|a_j\rangle$. C is a normalized constant.

$$\sum_{j=1}^{N-1} b_j |a_{j\,clock}|u_{j\,input}\left(\sqrt{1-\frac{C^2}{a_j^2}}\ |0 + \frac{C}{a_j}\ |1\right) \tag{13}$$

IV Un-compute the clock and input register by using the inverse Quantum phase estimation

$$\sum_{j=1}^{N-1} b_j |0\rangle_{clock}|u_j\rangle_{input}\left(\sqrt{1-\frac{C^2}{a_j^2}}\ |0 + \frac{C}{a_j}\ |1\right)_{ancilla} \tag{14}$$

V Measure the ancilla register if the outcome is "1", then the registers are in the state which contains the information of $|x\rangle$

$$\sum_{j=1}^{N-1} C\left(\frac{b_j}{a_j}\ |1\rangle_{ancilla}\right)|0\rangle_{clock}|u_j\rangle_{input} \tag{15}$$

VI Put the quantum gate of M on input register to calculate the expectation value $\langle x|M|x\rangle$

Fig. 3

HHL algorithm can solve linear algebra problems; therefore, there are many areas in which it can be applied, for instance, machine learning [15], solving linear differential equations [36], finite element methods [37], etc. However, there is still room for efficiency improvement, for example, encoding vector $\overrightarrow{b}$ onto the register, and constructing operator e^{iAt}. To input vector $\overrightarrow{b}$, it takes exponential steps to transfer the classical vector into a quantum system, and hence, the advantage of HHL algorithm is destroyed by encoding classical data onto quantum computers. In addition, the operator e^{iAt} needs to be efficiently constructed as well, and only several kinds of matrices are known to have this property, for example, local Hamiltonians [38], and s sparse Hamiltonian [39]. If someday, one can find an effective method for these problems, he quantum advantage of inverse linear transformation will become much more evident.

2.2. Grover's algorithm

Grover's algorithm can have quadratic speed-up over classical algorithms on unstructured data-searching task [24]. Supposed that there is a large unsorted database with N elements, and there are M solutions in it. If we want to find out the matched answer, in the classical algorithm the worst case requires $O(N/M)$ call to get it. However, the power of Grover's algorithm is able to improve the answer with $O(\sqrt{N/M})$ number of calls, which is a quadratic speed-up over the classical algorithm. In addition, it has been shown that no other quantum algorithms can calculate task fewer than $\Omega(\sqrt{N/M})$, which means that the Grover's search algorithm is optimal $\Theta(\sqrt{N/M})$ in the searching case [31].

2.2.1. Formalism

In a geometry way, we can view the process of Grover's algorithm as the rotation in the Hilbert space spanned by the answer, $|w\rangle$, and the other elements in the database $|s'\rangle$,

$$|s\rangle = \sqrt{\frac{N-M}{N}}|s'\rangle + \sqrt{\frac{M}{N}}|w\rangle \tag{16}$$

Fig. 4

Grover's algorithm uses two reflection operators to enhance the amplitude of $|w\rangle$, one is $U_{ora} = I - 2|w\rangle\langle w|$, and the other one is $U_s = 2|s\rangle\langle s| - I$, where U_{ora} comes from the oracle and U_G is the Grover diffusion operator. After one iteration, $|s\rangle$ state effectively rotates an angle 2θ, Figuer 5

Then after several iterations, it is possible to reach the maximum amplitude of answers, and the bound of number of iterations is given by [31],

$$R \leq \frac{\pi}{4}\sqrt{\frac{N}{M}} \tag{17}$$

The procedure of Grover's algorithm is provided in following parts.

2.2.2. Steps of grover's algorithm

Consider an unsorted N elements database with $M = 1$ match,

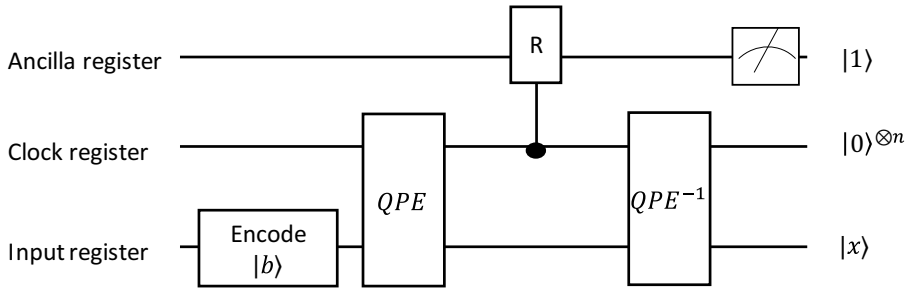

Fig. 3. The quantum circuit of HHL algorithm.

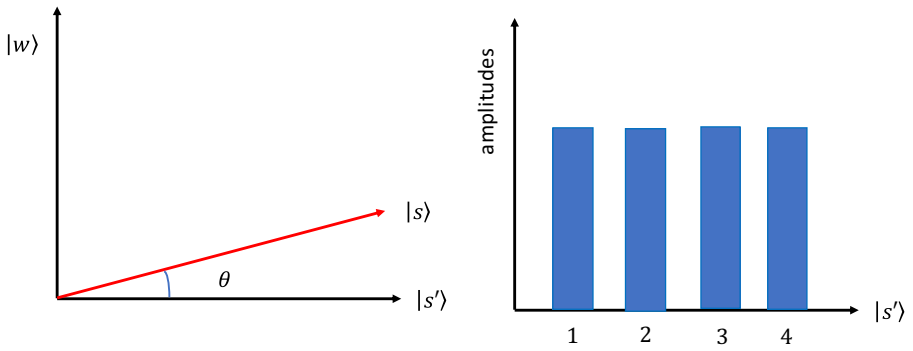

Fig. 4. Initial states are in the Hilbert space spanned by $|w\rangle$ and $|s'\rangle$.

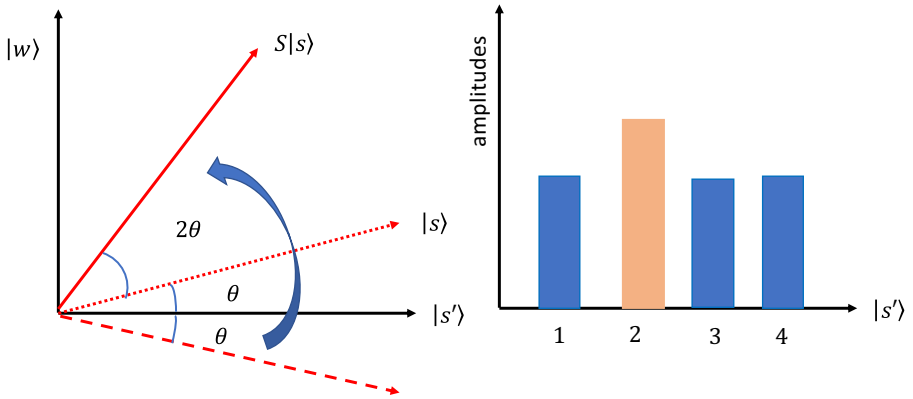

Fig. 5. The effect of oracle operators and Grover's diffusion operators.

i We need $n = \log_2 N$ qubits to construct the Hilbert space of the database, and several qubits for oracle workspace

ii The initial states are prepared in $|0\rangle^{\otimes n}$, and we apply Hadamard gate on each of the n qubits in parallel to construct a uniform superposition state: $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ where we encode the element of database on it with equal probabilities. Fig. 6

iii Apply the oracle, where the oracle can flip the matches by adding extra minus sign. Fig. 7

iv Next, we operate Grover diffusion operators on the circuit, and this can increase the amplitude of the matches. Fig. 8

v Iteratively operate the oracle and Grover diffusion operator $O(\sqrt{N})$ times, then we can get the matches with high possibilities when we measure the state. Fig. 9, Fig. 10

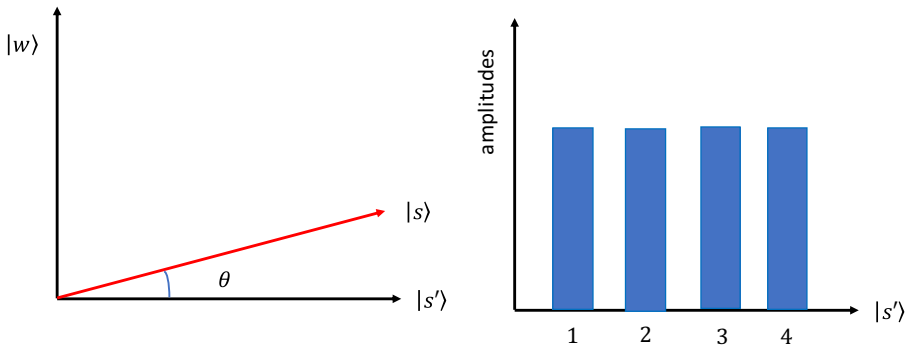

Fig. 6. The initial states are in equal amplitude.

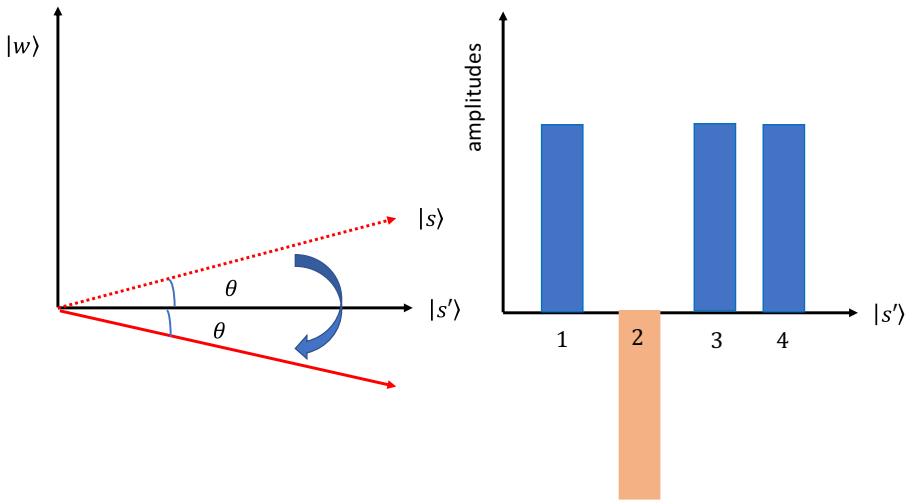

Fig. 7. The state after applying the oracle operator.

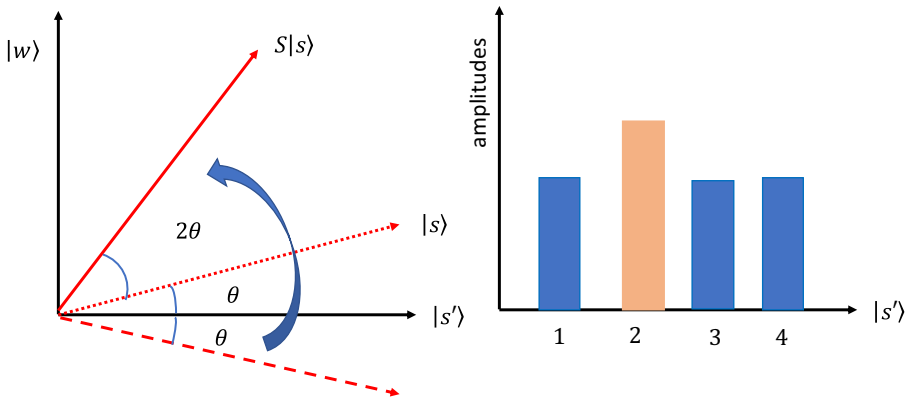

Fig. 8. The states after applying the Grover's operators.

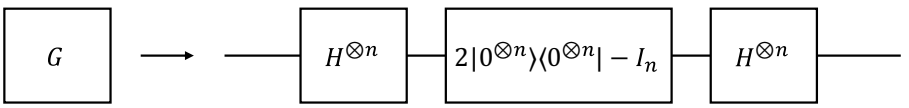

Fig. 9. Grover diffusion operator consists of three parts: 1. Apply Hadamard gate on each n qubits., 2. Apply the reflection operator $U_s = 2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I_n$, 3. Apply Hadamard gate on each n qubits again.

In some cases, we may not know the number of solutions, M, beforehand, and therefore there is a method, quantum counting, can help us quickly estimate the number of answers.

From the geometry point of view, single iteration of Grover's process effectively rotates states at an angle 2θ, which is determined by the number of matches in the database. Here we define the effective operator of one iteration of Grover's as S,

$$S = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \ \sin\theta = \sqrt{\frac{M}{N}}$$

$$S|s = \cos 3\theta|s' + \sin 3\theta|w \tag{18}$$

Fig. 11

Once we can use the phase estimation procedure to calculate eigenvalues of S, $e^{i\theta}$ and $e^{i(2\pi-\theta)}$, then we can approximately estimate the number of matches from Eq. (20) [30].

Grover's algorithm can be applied to solve the optimized solution of satisfiability problems [40, 41]. Many daily life problems can

$$O(\sqrt{N})$$

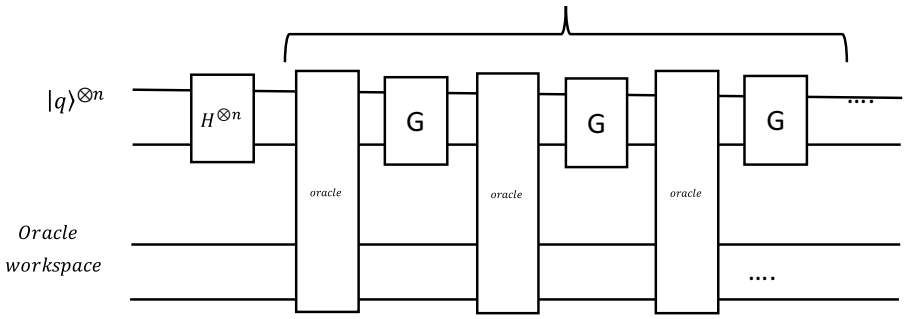

Fig. 10. The quantum circuit of Grover's algorithm.

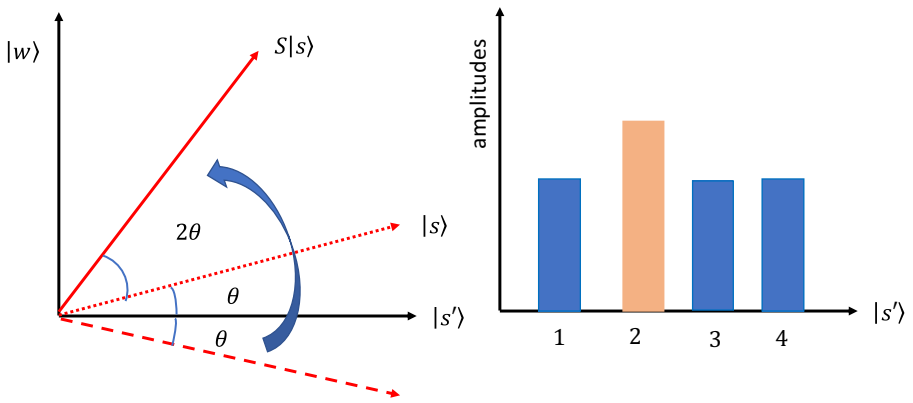

Fig. 11. Schematic figure of one Grover's iteration.

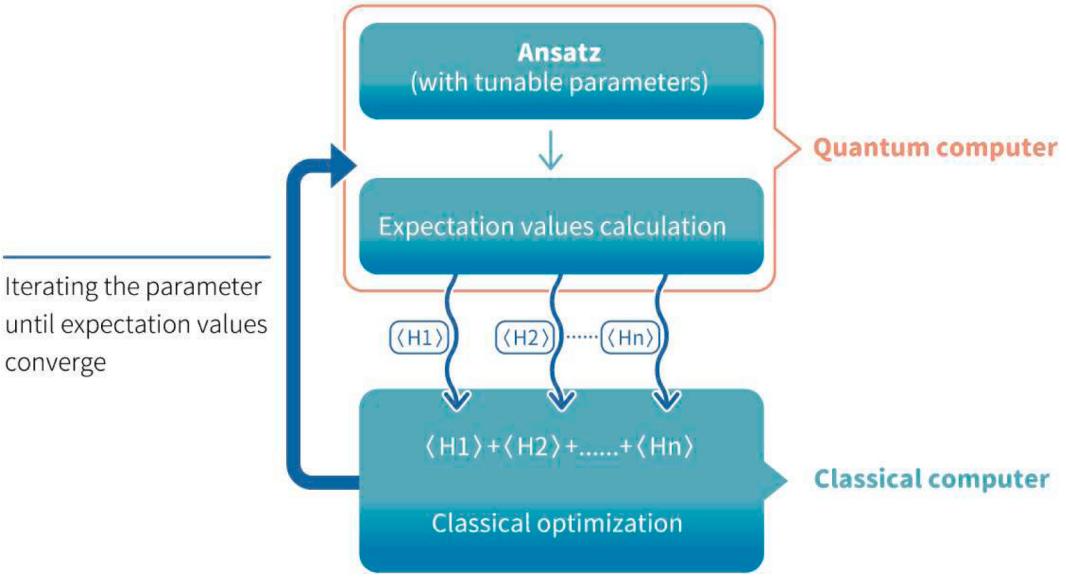

Fig. 12. The standard procedure of VQE.

be cast into the forms of satisfiability problems, for example, traveling salesman problems, knapsack problems. In a satisfiability problem, if there are n elements in it, then the search space is of size 2^n, which cannot be solved in polynomial time [42]. By using Grover's algorithm, we can have the quadratic speed up in some problems, which is faster than classical algorithms. For example, in 3SAT problems, with the assistance of a combination of Grover's algorithm with the best classical algorithm, we can solve problems in time $O(1.153\ldots^n \mathrm{poly}(n))$ which performs better than relying solely on classical algorithm in time $O(1.329\ldots^n)$ [43].

2.3. Hybrid quantum-classical algorithm

In the Noisy Intermediate-Scale Quantum (NISQ) era, the number of gates which can be implemented on current quantum computers is limited, and we are still far from building fault-tolerance quantum computers which is on the scale of millions of qubits. Therefore, in order to find near-term applications for the quantum computer, hybrid quantum classical algorithms which combine the quantum computer and the classical computer are inevitable. Here we list two kinds of hybrid algorithm, VQE and QAOA as an example.

2.3.1. Variational quantum eigensolver (VQE)

Variational Quantum Eigensolver (VQE), is a hybrid quantum-classical algorithm which is robust against noise, and that makes it suitable for NISQ devices. The spirit of VQE is to use variational principle to find the ground state energy of a given Hamiltonian H.

$$\langle\psi(\theta)|H|\psi(\theta)\rangle \geq E_0 \tag{19}$$

By changing the parameter in the well-prepared ansatz state and then minimizing the energy expectation value, theoretically, we can find the ground state energy of the Hamiltonian.

Fig. 12

First, we prepare an ansatz state with some parameters and use quantum computers to sample its expectation values. From these values, classical computers start to minimize the expectation value of the Hamiltonian, output a new set of parameters, and these new parameters are fed back to the ansatz to start another iteration until the expectation values of the Hamiltonian converges.

The growth of the dimension of Hilbert space requires calculation resources to increase exponentially for classical computers. Therefore, calculation of such superposition state is hard to achieve with classical computers. When we are dealing with strong correlated system, for instance, molecule excited states, calculation will be intractable for classical computer if high accuracy results are intended. VQE algorithm has some advantages in this aspect [38, 44], because of the built-in superposition and entanglement nature of quantum computers. Hence, it has been applied to calculate some simple molecule properties [45]. In order to get the results with higher accuracy or using lesser quantum resources, the know-how to improve each of the subroutine of the VQE are still under development, and those topics will be introduced in the following sections.

2.3.1.1. Hamiltonian preparation

2.3.1.1.1. Chemical basis. In chemical calculations, choosing an efficient orbital basis can approximate the chemical system with high accuracy. In traditional molecule or lattice calculations, several basis sets have already been used, for example, STO-nG basis, 6–31 G basis, or plane wave basis.

STO-nG basis is a minimal orbital basis sets, where each orbital is composed of the linear combinations of Gaussian type orbital basis. Split-valence basis sets (e.g. 6–31 G) is also a minimal basis, where an inner core orbital is single-zeta representation of STO basis but outer orbitals are double-zeta representation, and this gives more flexibility to simulate molecule orbitals [46]. Apart from those traditional chemical basis sets, the plane wave basis set is also commonly used in lattice system computation, and it can be applied on the 2D electron gas simulations [47].

2.3.1.1.2. Mapping method. This part is to encode the second quantized fermionic Fock state onto qubits, and there are two common encoding methods listed in the following.

Jordan-Wigner

In this method, the number of electrons on each orbital is encoded onto single qubit as $|0\rangle$ and $|1\rangle$ which represent unoccupied and occupied state, respectively. We can write down the total electron system in the form of,

$$|q_i,\ q_{i-1}, \ldots, q_0\rangle_{JW},\ q_p \in \{0, 1\}$$

One can show that the mapping of the creation and annihilation operator can recover the property of fermionic operator on i^{th} qubit,

$$a_i = L_i \otimes Z_{i-1} \otimes \ldots \otimes Z_0$$

$$a_i^\dagger = L_i^\dagger \otimes Z_{i-1} \otimes \ldots \otimes Z_0 \tag{20}$$

where $L = \frac{1}{2}(X + iY),\ \ L^\dagger = \frac{1}{2}(X - iY),$ and X, Y, Z are Pauli matrices.

Parity

One important feature of this method is that occupied number is not locally stored onto single qubits. We can directly get the parity form by transforming the encoding form of Jordan-Wigner.

$$|q_i,\ q_{i-1},\ldots,q_0\rangle_{JW},\ q_p\in\{0,1\}$$

$$|q_i,\ q_{i-1},\ldots,q_0\rangle_{JW}\rightarrow|P_i,\ P_{i-1},\ldots,P_1\rangle_{parity},\ P_p=[\Sigma_i^p q_i](mod\ 2)$$

The creation and annihilation can be constructed as,

$$a_i=X_{M-1}\otimes\ldots\otimes X_{i+1}\otimes\ \left(L_i\otimes|0\rangle\langle 0|_{i-1}-L_i^\dagger\otimes|1\rangle\langle 1|_{i-1}\right)$$

$$a_i^\dagger=X_{M-1}\otimes\ldots\otimes X_{i+1}\otimes\left(L_i^\dagger\otimes|0\rangle\langle 0|_{i-1}-L_i\otimes|1\rangle\langle 1|_{i-1}\right)\tag{21}$$

2.3.1.2. Ansatz state. VQE is a heuristic algorithm, which means that we can get high accuracy results with ansatz states prepared to suit the physical system. Currently, there are several ways to construct the ansatz state for a given Hamiltonian.

2.3.1.2.1. Hardware efficient ansatz. The hardware efficient ansatz has been first proposed to calculate the small molecule [45]. This ansatz is composed of the single rotation and the operation by the entanged two-qubit gate, which can be efficiently implemented on current noisy quantum devices,

$$|\psi(\vec{\theta})\rangle=U_R^d\ (\vec{\theta})U_{ent}U_R^{d-1}\ (\vec{\theta})U_{ent}\ldots U_R^1\ (\vec{\theta})|\psi_0\rangle|\tag{22}$$

Fig. 13

2.3.1.2.2. Unitary coupled cluster (UCC) ansatz. The idea of UCC comes from the coupled cluster (CC) theory and scientists modifies it into unitary form [48], where we usually take the Hartree-Fock state $|\psi_0\rangle$ as our reference state.

$$|\Psi_{UCC}\rangle=e^{\widehat{T}-\widehat{T}^\dagger}|\psi_0\rangle\tag{23}$$

In the couple-cluster theory, the couple-cluster operator $\widehat{T}$ is defined as follows,

$$\widehat{T}=\widehat{T_1}+\widehat{T_2}+\ldots$$

$$\widehat{T_1}=\sum_{\alpha,\ i}t_{\alpha i}a_\alpha^\dagger a_i$$

$$\widehat{T_2}=\sum_{\alpha,\beta,i,j}t_{\alpha\beta ij}a_\alpha^\dagger a_\beta^\dagger a_i a_j\tag{24}$$

($\alpha,\ \beta\in$ unoccupied orbitals, $i,j\in$ occupied orbitals)

$\widehat{T_1},\ \widehat{T_2}$ represent the single, double excitation operators respectively.

2.3.1.2.3. Trotterized adiabatic state preparation ansatz. David Wecker et al. [49] proposed a way to construct the Hamiltonian dependent ansatz by variationally tuning the parameter in Hamiltonian with several adiabatic steps s. If there is a Hamiltonian $H_s=tH_h+tH_V+suH_U,\ s\in[0,1]$, where H_U is interacting term and H_h and H_V are noninteracting term. They decompose the variational task into many steps, for each step the variational ansatz having the form,

$$|\Psi_T\rangle=\Pi_{b=1}^m\left[U_U\left(\frac{\theta_U^b}{2}\right)U_h(\theta_h^b)U_V(\theta_V^b)U_U\left(\frac{\theta_U^b}{2}\right)\right]|\psi_I\rangle,$$

$$U_U(\theta_U^b)=e^{i\theta_U^b H_U},\ U_h(\theta_h^b)=e^{i\theta_h^b H_h},U_V(\theta_V^b)=e^{i\theta_V^b H_V}.$$

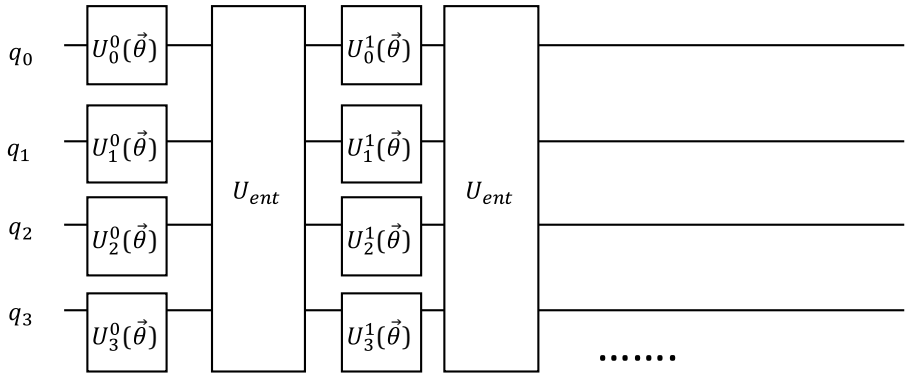

Fig. 13. One U_{ent} and U_R^n compose one-layer ansatz.

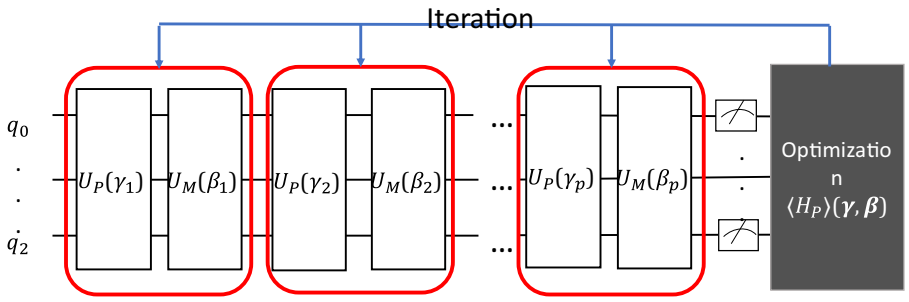

Fig. 14. p-level Quantum Approximate Optimization Algorithm (QAOA-p) [56].

When $s = 1$, it corresponds to the target Hamiltonian. Then we start from the eigenstate of the noninteracting term, $|\psi_I\rangle$, which is easy to prepare, and we target $H_{1/m}$. After the calculations, we can get a set of parameters, θ_i^1. For second step calculations, we take $|\Psi_T\rangle$ in the previous calculation as our second step $|\psi_I\rangle$ and target to $H_{2/m}$, and, likewise, we can get another set of function, θ_i^2. We can keep increasing the parameter s in evolution operator with an amount of $1/m$ until $s = 1$ and obtain the ground state of H_1.

2.3.1.2.4. Adiabatic preparation. One can prepare the Hamiltonian in this way,

$$H_T(s) = A(s)H_0 + (1-s)H_1, \ s \in [0,1] \tag{25}$$

, where H_0 is with the ground state easy to prepare, and H_1 is the target Hamiltonian. From quantum adiabatic theorem, if the parameter s changes slow enough, one can get the ground state of the target Hamiltonian H_1.

A. Garcia-Saez et al. [50] study the case that the adiabatic evolution path is sliced into many pieces (i.e. change the parameter s gradually from 0 to 1), where each sliced point correspond to a single VQE calculation task, and from the adiabatic theorem, the ultimate state could highly overlap with the true ground state.

Shunji Matsuura et al. [51] propose including an extra navigator intermediate Hamiltonian term into the adiabatic ground state preparation. They consider the chemistry case and choose the Hermitian cluster operator with single and double excitations to be navigator Hamiltonian and this modification can help the state to reach the ground state as close as possible with a shorter annealing time.

$$H_{\eta,\theta}(t) = A(t)H_{ini}(\eta) + C(t)H_{nav}(\theta) + B(t)H_{fin}$$

$$where\ A(1) = C(0) = C(1) = 0\ and\ A(0) = B(1) = 1$$

$$H_{nav}(\theta) = \Sigma_{i\in occ,\ \alpha\in vir}\theta_{i\alpha}a_i^\dagger a_\alpha + \Sigma_{ij\in occ,\quad \alpha\beta\in vir}\ \theta_{ij\alpha\beta}a_i^\dagger a_j^\dagger a_\alpha a_\beta \tag{26}$$

2.3.1.2.5. Adaptive ansatz. Harper R. Grimsley et al. [52] proposed an adaptive way to construct ansatzs. There is an operator pool containing several operators, and it can be a set of generalized single or double excitation operator in the case of chemical calculation. The formation of ansatz is adapted by measuring gradients with respect to each operator in the pool,add the operator with largest gradient into ansatz, and then do the VQE procedure to find the current ground energy. Next, the algorithm iterates the same procedure as above to extend the ansatz, and the final result can have high accuracy by using this adaptive ansatz.

2.3.1.3. Measurements. Extracting calculation results from quantum computer during VQE calculations needs a huge number of measurements depending on the required precision. Approximately $O(1/\epsilon^2)$ measurements are required for results with precision ϵ [53]. The total number of measurements also relates to the size of the system, and developing an efficient measurement subroutine is pivotal reducing the total calculation time. Daochen Wang et al. [54] proposed a way to corporate the quantum phase estimation with the VQE to reduce the number of measurements under the constrain of limited coherent time, and this procedure can also be included as an improvement of the measurement subroutine in other applications.

As for the application part, VQE algorithm can calculate the ground state energy of given Hamiltonian, and several simple molecules (i.e. H_2, LiH) [45], and some electron model (i.e. Hubbard model) cases has been studied recently [49, 55]. Understanding these molecules and electron model properties can benefit to drug design and discover new materials [47].

2.3.2. Quantum approximate optimization algorithm (QAOA)

2.3.2.1. Formalism. Among the algorithms of optimization, QAOA (Quantum Approximate Optimization Algorithm) is a widely used one. It's first proposed in the paper of E. Farhi *et al.* [27]. It is a hybrid quantum-classical algorithm. Using quantum mechanical tool, Hamiltonian, and operating on quantum states to attack the problem of optimization of an objective function via classical iteration process.

The basic idea of QAOA can be easily found in literature and website resources, for example [27, 56-58]. In addition, it is worthwhile to mention that IBM just launched new optimization module in Qiskit, which use QAOA and other methods aiming to

model and solve the optimization problems. In the beginning, QAOA is created to solve so-called MAX-CUT problem [59]-a math branch dealing with maximum division of a given graph. Similar ideas can be extended to many aspects such as compress graph signals, via minimization problem, optimization problems, etc.

The basic elements of QAOA are: objective function, phase operators, mixing operators, and initial state. A typical QAOA runs as following process.

Consider a sequence of l variables $\boldsymbol{x} = x_1 x_2 \ldots x_l$, defined on l-bit binary strings. The general form of a combinational optimization problem is given by

$$\min C(x). \tag{27}$$

The $C(\boldsymbol{x})$ is also called an objective function. Some people use $f(z)$ corresponds to $C(\boldsymbol{x})$ as instead. Mapping of objective function to the phase Hamiltonian H_P where

$$H_P|x\rangle = C(x)|x\rangle. \tag{28}$$

The optimal problem (31) now becomes a case of finding extremal eigenvalue of H_P. Now we define the phase operator as

$$U_P(\gamma) = e^{-i\gamma H_P}, \tag{29}$$

where γ is the parameter. Different problem corresponds to different Hamiltonian H_P. For example, the H_P of the MAX-CUT problem is $\sum_{ij}\frac{1}{2}(I - Z_i Z_j)$, where Z_i is the Pauli Z-matrix. This H_P is nothing but Ising model in condensed matter physics [60]. In the quantum mechanical point of view, the phase operator is equivalent to the role of rotation operator in 2^l dimensional Hilbert space.

We then define the mixing Hamiltonian as

$$H_M|x\rangle = \sum_{i=1}^{l} X_i, \tag{30}$$

, where X_i is the Pauli-X matrix operating on i^{th} site. In quantum computing, the Pauli-X represents the NOT gate, with function $X|0\rangle \rightarrow |1\rangle$ and $X\langle 1| \rightarrow |0\rangle$. The initial state can be defined as $|+\rangle^{\otimes l} = \frac{1}{\sqrt{2^l}}\sum_x |x\rangle$. For p-level QAOA, i.e. there are p quantum rotations of initial state, we now generate a variational function

$$|\psi_P(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle = e^{-i\beta_p H_M} e^{-i\gamma_p H_P} \cdots e^{-i\beta_1 H_M} e^{-i\gamma_1 H_P} |+\rangle^{\otimes l}. \tag{31}$$

Therefore, there are $2p$ parameters γ_i and β_i $(i = 1 \ldots l)$ for us to adjust. We then determine the expectation value H_P in the variational state

$$C_P(\boldsymbol{\gamma},\boldsymbol{\beta}) = \langle \psi_P(\boldsymbol{\gamma},\boldsymbol{\beta})|H_P|\psi_P(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle, \tag{32}$$

which is done by repeated measurements of the quantum system in the computational basis. Similar to the classical optimization method, we do the iteration to find the optimal combination of $\boldsymbol{\gamma}$ and $\boldsymbol{\beta}$. The image of p-level QAOA is shown in Fig.14.

Suppose we have a set of optimized parameters $(\boldsymbol{\gamma}^*, \boldsymbol{\beta}^*)$, we define a parameter r as

$$r = \frac{\langle C^* \rangle}{C_{max}} = \frac{\langle \boldsymbol{\gamma}^*, \boldsymbol{\beta}^* | H_P | \boldsymbol{\gamma}^*, \boldsymbol{\beta}^* \rangle}{C_{max}}. \tag{33}$$

It is not hard to conclude the $0 \leq r < 1$ for a givem finite iteration level. For different problems, there are different best records of the r value [61, 62]. Ideally and theoretically, QAOA is somewhat a "stupid poof" algorithm. The performance can only improve with increasing p, that is, QAOA monotonically improve with depth and succeed in the $p \rightarrow \infty$ limit [27].

However, even at the lowest circuit depth ($p = 1$), QAOA has non-trivial provable performance guarantees [27, 63]. On the other hand, QAQA cannot be efficiently simulated even when $p = 1$ by classical computers. Comparing with the predecessor algorithm – Quantum Annealing (QA), QAOA demonstrates the advantage to shorter running time. QA shows the running time of adiabatic quantum computation is proportional to $T \sim O(1/g_{min}^2)$, where g_{min} is the energy gap between ground state and first excited state. Thus, adiabatic quantum computation is inefficient as g_{min} small [28]. Due to the above characters and advantage, QAOA is an efficient algorithm which gives a meaningful result in finite p levels.

2.3.2.2. Applications. One of the most common issue to apply optimization algorithms is finance. Finance is a topic dealing with pricing, cost control, portfolio, etc. [64]. There is no doubt that maximize the profits is a prior policy of a company.

In contrast to maximization, some problems need to find the minimal values. For example, the arrangement of logistic paths requested by shortest-distance path or the shortest-time path actually depends on minimal cost.

2.3.3. Adiabatic optimization

2.3.3.1. Quantum adiabatic theorem. The main idea of QAA comes from quantum adiabatic theorem.

The evolution of a state follows the Schrödinger equation with respect to parameter t,

$$i\hbar\frac{d|\psi(t)\rangle}{dt} = H(t)|\psi(t)\rangle \tag{34}$$

One can write the Hamiltonian into a function of $s = \frac{t}{T}$ where T controls the rate change of $H(t)$. The quantum adiabatic theorem state that if we start from a ground state of a Hamiltonian $H_0 = H(0)$, $|E_{0,\ s=0}\rangle$, which is easy to prepared, and change slow enough with respect to s, we can always get to the instantaneous ground state of $H(s)$, $|E_{0,s=s'}\rangle$; ultimately, the ground state of the target Hamiltonian, $H_1 = H(1)$, can be reached.

$$H_T(s) = A(s)H_0 + (1-A(s))H_1,\ s \in [0,1]$$

$$H(s)\left|E_{0,\ s=s'}\right\rangle = E_0(s)\left|E_{0,\ s=s'}\right\rangle$$

$$\lim_{T\to\infty}\left\langle E_{0,\ s=1}|\psi(T)\right\rangle = 1 \tag{35}$$

The criteria of T are

$$T \gg \frac{\max\limits_{0\le s\le 1}\left|E_{1,s}\left|\frac{dH}{ds}\right|E_{0,s}\right|}{\min\limits_{0\le s\le 1}\left(E_{1,s}-E_{0,s}\right)^2} \tag{36}$$

which means that an appropriate T depends on the rate change and the energy gap between $E_{0,s}$ and $E_{1,s}$ [65].

Satisfiability is one of problems that QAA algorithm could solve. For example, an n-bit satisfiability problem with a K clauses can be formulated as,

$$C_1 \wedge C_2 \wedge C_3 \ldots \wedge C_K \tag{37}$$

, where C_K is the function of Boolean function $x_K \in \{0,1\}$, and it has True or False values with respect to a n-bit string. The target is to find n-bit strings which satisfies all K clauses.

In quantum computation, the n-qubit quantum state can represent the n-bit string

One can then construct a Hamiltonian, H_{C_K}, which relates to the clause, C_K, and the total Hamiltonian describing the problem has the form,

$$H(t) = H_{C_1}(t) + H_{C_2}(t) + H_{C_3}(t) + \ldots + H_{C_K}(t). \tag{38}$$

In QAA algorithm, problem Hamiltonian, H_P, and initial Hamiltonian, H_i, have to be prepared beforehand, and they can be all written into the sum of Hamiltonian of each clause,

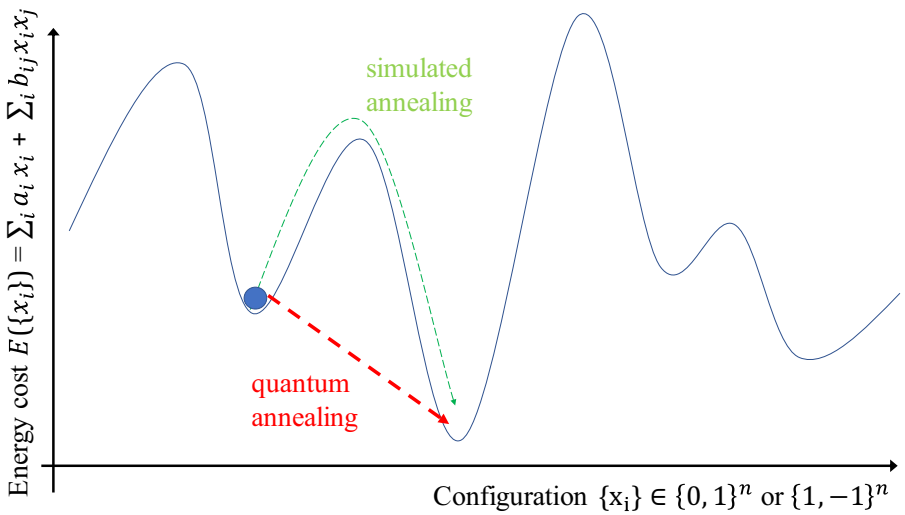

Fig. 15. The optimization problem is to find the minimum in the cost function or energy surface. Simulated annealing (SA) utilize the thermal fluctuation to overcome the energy barrier. In contrast, quantum annealing (QA) tunnel through the barrier in a quantum fashion so that it can find the other minima.

$$H_P = \sum_C H_{C,P}$$

$$H_i = \sum_C H_{C,i} \tag{39}$$

We can relate these two Hamiltonians with a parameter $s = \frac{t}{T}$,

$$H(s) = (1 - A(s))H_i + A(s)H_P \tag{40}$$

If T value is large enough, and the energy gap ($g_{min} = E_1 - E_0$) is not zero, according to the adiabatic theorem, we can reach the final ground state of H_P with the starting point at the ground state of H_i.

The idea of QAA can be also applied to design as a subroutine of others quantum algorithm, for instance, to avoid the local minimum, the Dave Wecker et.al. [49] use the "annealed variation" strategy to calculate the eigenenergy of electron systems. A. Garcia-Saez et al. [50] break the annealing path into several VQE tasks to calculate the classical exact cover problem.

2.3.3.2. Quantum annealing. Quantum annealing (QA) [66, 67] is a special type of quantum machine designed for combinatorial optimization. In other words, it doesn't quite belong to any of the universal quantum computers. Most optimization problem, if not all, can be converted to finding the global minimum solution of a cost function or an energy surface (Fig. 15). The basic approaches like gradient-based algorithm [68] and greedy algorithm [69] can only guarantee search for the local minimum. To overcome an energy barrier which may occur along the energy surface, a heuristic algorithm, simulated annealing (SA) [68, 70] was proposed to introduce the temperature concept so that search under higher temperature can have access to higher energy in order to overcome the barrier (Fig. 15). SA operates by taking advantage of thermal fluctuation, and the approach is still classical. In contrast, the quantum annealing algorithm (QAA) utilizes the superposition property of the quantum principle to escape from the local minimum. The possible superposition of two minimum states with certain probability allows the state in one minimum to tunnel by virtue of quantum physics to the other minimum separated by an energy barrier. The tunneling probability is of course related to the barrier height and width. Therefore, QA is particularly suitable for problems with thin but extremely high barriers, which cannot be easily handled by the SA approach.

The combinatorial optimum problem that QA deals with can be formulated as finding the minimum solution of the energy function

$$E(\{x_i\}) = \sum_i a_i x_i + \sum_{j>i} b_{ij} x_i x_j, \tag{41}$$

where x_i take binary values. The binary type problem can be classified as the Ising model with $x_i \in \{-1, 1\}$ or the quadratic unconstrained binary optimization (QUBO) model with $x_i \in \{0, 1\}$. The two models can be converted to each other through some transformation, which can be done manually or using automated tools provided by the D-Wave. Each variable x_i is represented by a qubit q_i (or chained qubits) in QAA in a way that the $\{x_i\}$ solution is found from the $\{q_i\}$ values for the ground state. The a_i and b_{ij} are real numbers whose allowed range is limited by the hardware implementation. If the weight a_i and b_{ij} vary outside the range, the rescaling

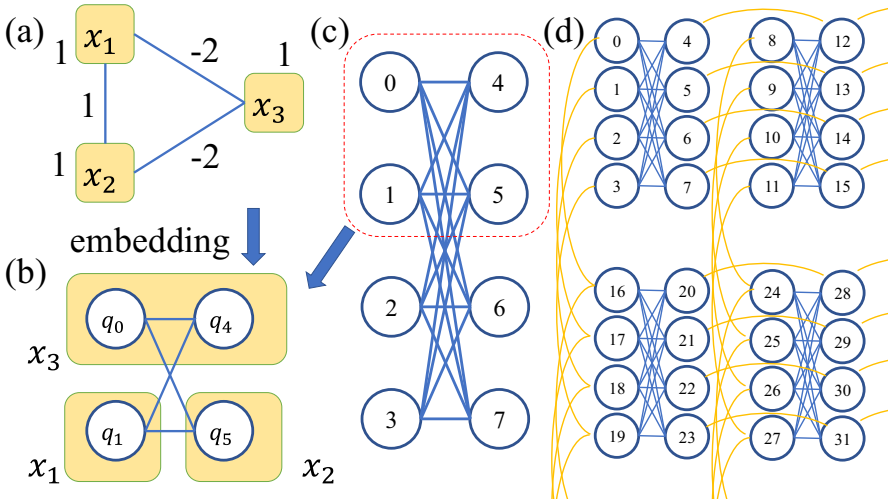

Fig. 16. The graph network represents the Boolean OR gate by Eq. (43). (b) The embedding of the graph above is shown. Qubits q_0 and q_4 are chained together to equivalently represent the OR gate output x_3, while qubits q_1 and q_5 represent the input x_1 and x_2, respectively. (c) The unit cell of the Chimera structure adopted by the D-Wave with number in the circle representing the qubit labeling as shown. (d) The sets of connected unit cell that constitute the Chimera architecture is shown. Lines with blue color represent coupling within the unit cell, while the yellow ones represent coupling between nearby unit cells.

must be applied to the entire set of coefficients to ensure the fitness of value ranges. The rescaling mainly causes two drawbacks: increase of computation time and the subjection of noise. The noise is inherent in the system due to the thermal fluctuation and possible hardware imperfections.

The way the QA finds the ground-state in the energy surface described by Eq. (41) is by using the adiabatic theorem [71], as described in the previous section. Starting from a predetermined simple Hamiltonian H_0, the QA prepares the system in the ground state of H_0 initially. The QA then evolves the system Hamiltonian from H_0 to the target Hamiltonian H_1 which is user-defined. The spirit of the adiabatic theorem is that the system can maintain in the lowest-energy state as long as the transition is adiabatically slow. In comparison, the classical SA climbs the energy landscape to find its minimum without changing the system Hamiltonian, while the QA evolves the system from a predetermined Hamiltonian to the target Hamiltonian by always sitting at the ground state.

The transition time to complete the annealing can be controlled by the user, and the typical minimum annealing time is about 10 μs. The minimum time for an annealing is determined by the energy level difference at any transition time between the ground state and the first excited state, since overly fast transition may cause the system to tunnel to the excited state. Therefore, besides operating over a long enough duration for each annealing, the usual strategy is to choose the best solution from a large amount of anneals sampling or simply performing the average. Under optimal operating condition, the distribution obeys a Boltzmann distribution that can be estimated [72, 73], while the output deviates from a Boltzmann distribution for non-optimal operation. Fair sampling can be achieved by some methods and can have important applications [74].

To successfully simulate the system having more than one qubit, it is important to maintain the coherent connection of the qubits as far as possible. For a system with n_q qubits described by Eq. (42), it can be thought of as a graphical network connecting the n_q qubits. Each qubit represents a node with assigned weight a_i in the graph, and edges between them have weights b_{ij} to describe the interaction strength. Since the real physical implementation adopted by the D-Wave is the Chimera structure (Fig 16c & d), the embedding that describes the mapping from the graphical network of Eq. (42) to the physical hardware is necessary for real simulations. In Chimera structure, each qubit is connected to at most six other qubits to maintain coherence. Due to the sparsely connected structure of the Chimera graph, multiple qubits may be grouped together and treated as if they were a single qubit, depending on the purpose of the problem, i.e. the Hamiltonian. Once the embedding is done, the readout of the physical hardware can be unembedded to the output of the target Hamiltonian.

One example to show the embedding is in the following. For a Boolean OR gate ($x_3 = x_1 \vee x_2$), it can be reformulated as a penalty model

$$E(a_i,\ b_{ij}; x_i) = x_1x_2 + (x_1 + x_2)(1 - 2x_3) + x_3. \tag{42}$$

The correct answers $(x_3 = x_1 \vee x_2)$ give the lower values of $E(\{x_i\}) = E(x_1,x_2,x_3)$ for $E(0,0,0) = E(0,1,1) = E(1,0,1) = E(1,1,1) = 0$, while the false answers $E(0,0,1) = E(0,1,0) = E(1,0,0) = 1 \text{and} E(1,1,0) = 3$ always give higher penalty. The graphical model with corresponding weights and coefficients is shown in Fig. 16(a) which must be embedded into the physical Chimera structure (Fig. 16 (b)). Fig. 16(c) represents the unit cell of the Chimera structure, while Fig. 16(d) represents the sets of connected unit cells. The number in the circle is the qubit labeling $(q_i = q_0, q_1, q_2, \ldots)$. Due to the structure, the embedding of x_3 is represented by the chained qubits $q_0 =$

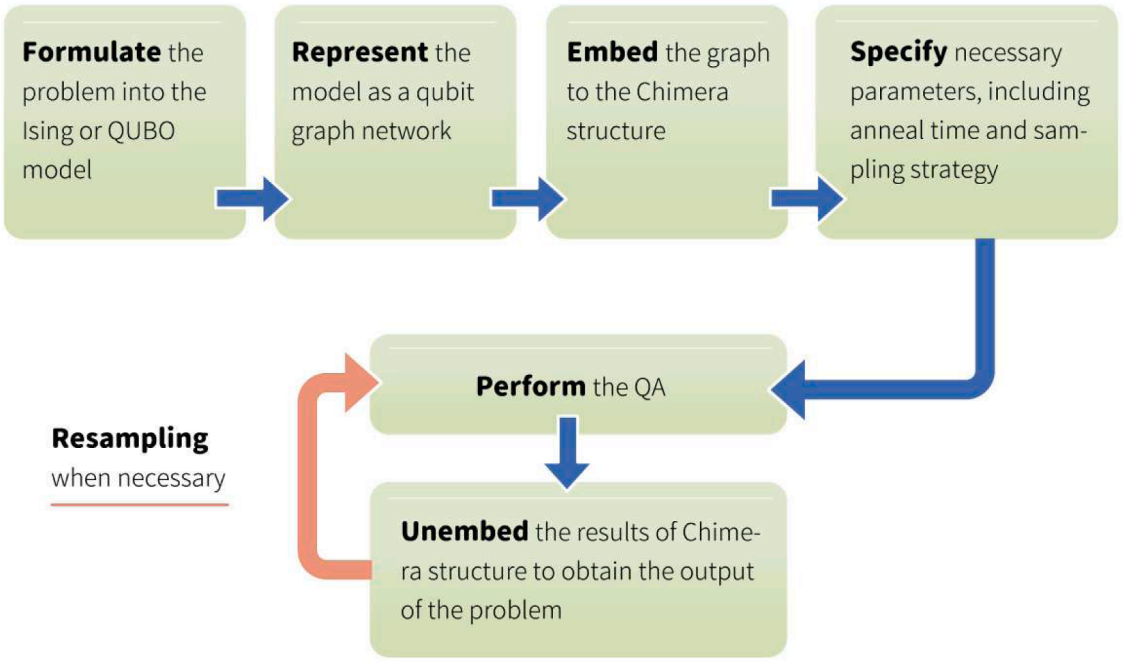

Fig. 17. The procedure of Quantum Annealing .

q_4, while x_1 and x_2 are represented by q_1 and q_5 respectively, as shown in Fig. 16(b).

For practical applications, several problems can be formulated into the QUBO problems (Eq. (42)) so they can be solved by the QAA. One example is the Max-cut problem which seeks to partition the vertex V into two sets with edges as large as possible between them for a given undirected graph G(V, E), where V = $\{x_i\}$ is the vertex set and E is the edge set [75]. The x_i is chosen to be 0 or 1 representing two different sets, so an edge (i,j) in the cut means $(x_i, x_j) = (0,1)$ or $(1,0)$, otherwise edges are not in the cut. Therefore, the quantity $x_i + x_j - 2x_i\, x_j$ can be used to identify if the edge (i,j) is in the cut, since the quantity is equal to 1 if (i,j) is in the cut, and equal to 0 otherwise. The problem can then be formulated to maximize

$$y = \sum_{(i,\ j)\in E} \left(x_i + x_j - 2x_i x_j\right), \tag{43}$$

which is in the form of QUBO Eq. (42). Other QUBO problems include quadratic assignment problems, multiple Knapsack problems, clique partitioning problems, graph coloring problems, budgeting problems, etc. [75]. As shown in the previous Boolean gate example, the applications include circuit fault diagnosis problem or the Boolean Satisfiability (SAT) problem [76]. Computer vision problems like the stereo matching can also be formulated as a QUBO problem [77]. Recently, integer factorization problem was demonstrated in the QUBO format so that the solution is available by the D-Wave [78, 79]. The relation between the spin-glass ground state and the QUBO was also analyzed [80].

Fig. 15, Fig. 16

Finally, steps to perform the QA is summarized in Fig. 17. The necessary steps for users are step 1 and probably step 4, while some steps like embedding, unembedding and analysis can be automatically handled by the QA machine, the D-Wave.

2.4. Digital annealing

Recently, Fujitsu developed the digital annealer unit (DAU) chip, which is a form of physical-inspired simulated annealing that deals with optimization problems. This quantum-inspired annealer utilizes the parallel-trial Monte Carlo update, which can have a speedup advantage over single trial Monte Carlo in low temperature cases [81]. Compared with current commercial annealer, DAU is much more robust against the thermal noise, and thus it can work at room temperature. Currently, DAU is in its second generation — the max scale of DAU can go up to 8192 bits with 62 bit precision [82].

2.5. Quantum error mitigation

Ideally, we would expect every operation to be perfect in Quantum Computation. However, due to various reasons, the cruel reality is that errors may occur everywhere — at quantum state preparation, gates implementation, state transmission, or even during measurements. Protecting computational results from errors is crucial for all kind of quantum tasks. Quantum Error Correction (QEC) fights against noise by encoding logic qubits to more physical qubits, it is the way we defend quantum information in the long run [83-85]. With QEC, realizing quantum tasks are operating the encoded quantum states to execute gates. The study that concerns error propagation and accumulation in these processes is known as fault tolerance [86-88]. To perform Shor's factorizing algorithm [89] of a L-bit number in a fault-tolerant manner, one requires 2 L logical qubits and a huge circuit depth ($32L^3$to the leading order) [90].

The size of current quantum devices clearly cannot afford the overhead of a fault-tolerant quantum computation. A class of approaches is invented to mitigate errors aimed at noisy, shallow circuit depth, near-term devices (a.k.a. NISQ devices). These approaches refer to the Error Mitigation (EM) methods. Since EM methods usually do not require encoding processes, they normally do not need additional physical qubits. In this section, we introduce the main ideas of several EM methods and report EM related experiments on actual physical systems.

2.5.1. Error extrapolation and quasiprobability decomposition

The causes and locations of noise in quantum computing are various: the state preparation and measurement (SPAM) errors, the imperfect control of the quantum system while implementing circuits, the flawed isolation from the environment (the system interacts with the environment that causes decoherence), etc. SPAM errors are relatively stable for a given quantum system, they could be treated separately from circuit noise.

Two main approaches have been developed for controlling circuit noise – Error Extrapolation (EE) [91, 92] and Quasiprobability Decomposition (QD) [91]. Assume that the goal of running a quantum circuit is to obtain an expectation value $E(A)$ for the operator A with respect to the circuit outcome state ρ. Error Extrapolation (or zero-noise extrapolation) is based on Richardson's deferred approach [93]. The intensity of noise is represented by a parameter λ (where $\lambda \to 0$ is the noiseless situation). Error extrapolation method analyzes the influences of noise on expectation values to different orders (linear or higher order), delivers estimations about main losses due to noise, and adds the estimations back to compensate the noisy experimental data [91]. More specifically, the noisy expectation value $E_{noise}(A)$ is expanded around E^*, which is the desired ideal expectation value of A:

$$E_{\text{noise}}(A) = E^* + \sum_k a_k \lambda_k + \mathcal{O}\left(\lambda^{n+1}\right)$$

where a_k's are parameters which depend on the chosen error model [94]. The goal of EE is to get E^* from a series of $E_{noise}(A)$. New protocols along this line are designed to improve performance and reduce resources [94-96].

Quasi-probability decomposition was first proposed in [91]. The main idea is to rewrite noiseless quantum circuits in terms of a mixture of the noisy ones [97], apply the Monte Carlo method afterwards to achieve the estimation of the expectation values $E(A)$. QD can also be interpreted more intuitively – inverse the noise channel $\mathcal{N}(\rho)$ [26]. The inverse map $\mathcal{N}^{-1}$ may not be physical. Assuming that the noise model is known, the QD process is to determine the parameters in the noise model for the system of interest. A set of noise operators that fully characterize the system noise is prescribed by this method. This requires detailed knowledge of the noise of the system, but often it is not the case in laboratories. An improved protocol in [94] allows experimentalists to calibrate noise with the algorithm and give an estimation about the ideal (noiseless) expectation value $E(A)$. This protocol also suppresses the SPAM error by using the gate set tomographic techniques [94].

2.5.2. *Other methods*

There are various other EM approaches striving to ameliorate error by using different techniques or from disparate points of view, such as machine learning based methods [98-100], protocols designed for VQE [101] and methods aimed for SPAM errors [102].

Traditional and novel numerical techniques could naturally come into play since mitigating errors is, in general, data processing. Clifford data regression [98] applies linear regression methods to model the difference between classically simulated ideal data and noisy data. After learning from the numerical model, ideal expectation values can be extracted from the noisy data. A learning based general protocol is introduced in [100]. The lost function is the square of the L_2 norm associated with the difference between the ideal expectation values and the error-mitigated ones. The protocol finds the optimal mitigation model by minimizing the lost function. One similar device-specific methods with convolutional neural networks are proposed in [99].

As mentioned in the previous section, VQE is one of the most promising applications for NISQ devices. Although it is well-known that VQE is robust against coherent errors [53], its accuracy can still be boosted with EM [26]. The method of quantum subspace expansion is specifically designed for VQE, it can mitigate errors as well as generate excited states [101]. This method measures the coefficients of system Hamiltonian H under a certain kind of expansion. From the reconstructed Hamiltonian representation (HLR), the error mitigated eigenstates as well as other information can be generated.

SPAM error mitigation can improve the results of quantum computing and may also compensate for the fault-tolerant error correcting schemes [103]. Measurement errors in multi-qubit experiments are considered in [102]. Authors of this paper propose two different schemes for unbiased error mitigation based on (1) the tensor product and (2) continued Time Markovian noise model. These two schemes provide information for non-correlated noise and correlated two-qubit Markovian noise. It shows that the tensor product model is a good approximation to the full error matrix. However, errors in the measurements are still correlated (the correlated Markovian noise model behaves slightly better). Ref. [103] mitigates SPAM error in a similar fashion, that is approximating the full error matrix with a simpler assumption to reduce the calibration cost.

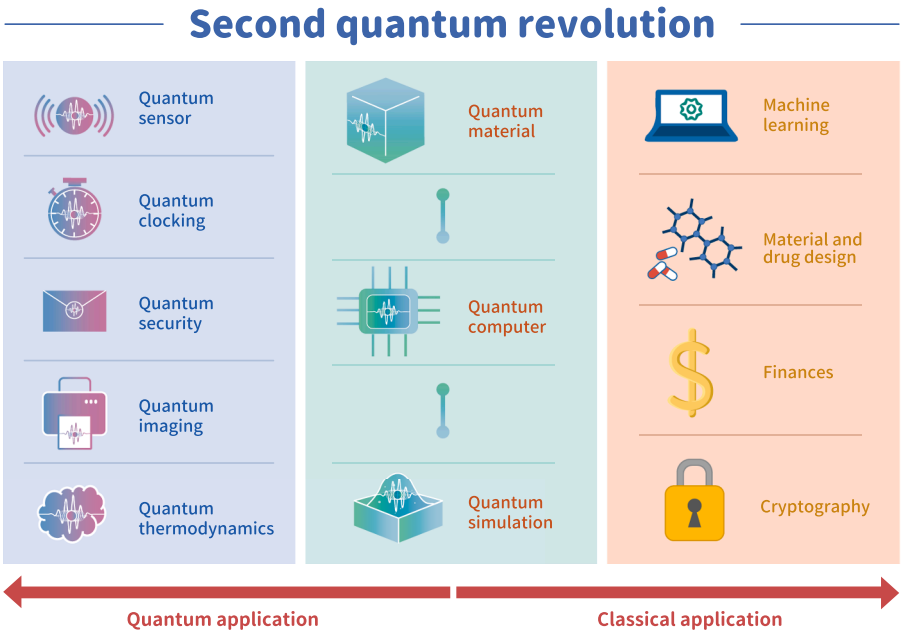

Fig. 18. Top: Classical applications: Machine learning, finances, materials and drug design, RSA problems etc. Middle: A fault-tolerant quantum computer needs appropriate quantum materials with a long coherence time. Effective quantum algorithms operating on a fault-tolerant quantum computer can solve all kinds of quantum and classical problems and quantum advantage will be in the entire spectrum of applications. Bottom: Quantum applications: Including a new sensor, new methods to define time, new security systems, and new methods to transfer information and to solve the statistical problem in quantum regimes.

2.5.3. Related experiments

Experiments are conducted in actual quantum systems to demonstrate the effects of the EM methods. Most of the systems are superconducting systems.

Quasi-probability decomposition and gate set tomography are used in [104] to mitigate errors in a 4-qubit superconducting system. Both one-qubit and two-qubit gate errors are suppressed. As a consequence, the ground state preparation accuracy is significantly increased. QD is also implemented in a trapped-ion system [105] - it leads to a two and a one order-of-magnitude error reduction for the single and the two-qubit gates, respectively. In [106], quantum subspace expansion is used to improve the accuracy of VQE implementation on the H_2 molecule. Incoherent errors are suppressed, near-chemical accuracy of ground states and excited states are all realized from the process. Symmetric verification method mitigates error for a 2-qubit superconducting system while applying VQE [107], the error is reduced by an order-of-magnitude.

It is also worth noting that increasingly more and more EM experiments are being carried out on the IBMQ platform. Error extrapolation helps to boost the accuracy of a 5-qubit system [108]. The measurement error mitigation method in [102] is also conducted on a 20-qubit system. The other protocol for measurement errors [103] mentioned above is tested out in a 16-qubit system. The Clifford data regression method in [98] is tested on a 16-qubit system, and it significantly reduces errors in the ground state energy problem. Three 20-qubit- systems are used to test a software mitigation method for crosstalk errors [109].

Fig. 18

3. CONCLUSIONS AND PROSPECTS

With great efforts from inter-disciplinary experts, the world is now seeing the functioning of prototype quantum computers with about fifty to one hundred qubits, and the number of qubits is still increasing. This rapid improvement leads to the prediction by "Neven's law": the number of quantum computer qubits will be increasing at a double exponential rate. So long as Neven's law holds true, (see Fig. 19), quantum computers will run on millions of qubits by around 2026 – which is to say quantum advantage is around the corner. In order to achieve quantum advantage, the importance of developing quantum algorithm cannot be neglected as well, since well-designed quantum algorithms can solve problems with less computational resources. Before we could reach the era of fault-tolerant quantum computing, it is crucial in the near terms to actively develop lots of quantum algorithms and quantum error mitigation approaches. As for near-term algorithms, it could be in the form of hybrid quantum-classical which incorporates both classical and quantum computation in the subroutine so as to decrease the sensitivity to noise. On the other hand, developing more speed-up algorithms for fault-tolerant quantum computers remains a vital problem in the long run [17].

The emergence of functional quantum computers implies that research in this field is past the stage of pure academic effort. Quantum computers have demonstrated great potentials for solving problems in different fields, for instance, finance [41], transportation [110], medicine [111] and chemistry [26]. In addition, exploring for new applications in new fields continue to be very important. This would be a collaborative effort that relies not only on physicists and computer scientists but also experts from different backgrounds. Governments (e.g. the United States, Europe, Japan, China) and major companies (e.g. Google, IBM) have formulated a series of research and development plans for quantum computers [112]. Still we believe it will take scientists many years and lots of inter-disciplinary cooperation to overcome the technical issues discussed above before humanity could formally enter the era of fault-tolerant quantum computing. Last, we hope this review article would provide a clear overview of recent developments in quantum computation, and inspire those who are interested in this promising area of research.

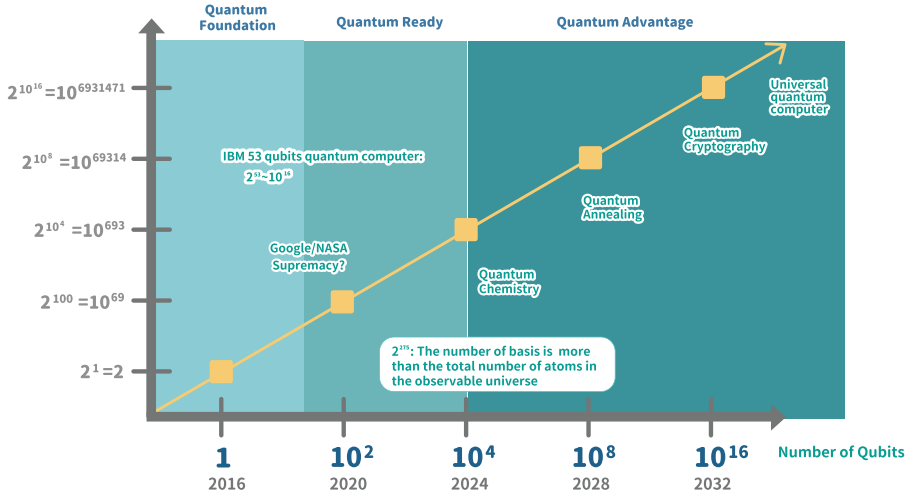

Fig. 19. The roadmap for quantum computer. Horizontal axis is the hardware technology of qubits which follows Neven's law and the vertical axis is the dimensionality of Hilbert space with 2^n qubits. Integration with existing and forthcoming semiconductor technologies will expedite the system's integration pace.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENTS

CRC thanks the support of the NTU-IBM Q Hub at National Taiwan University from the Ministry of Science and Technology, Taiwan, under grant No. MOST 107–2627-E-002–001-MY3 and 108–2627-E-002–002. N.C. thanks NSERC of Canada.

REFERENCES

[1] R.P. Feynman, Simulating physics with computers, Int. J. of Theor. Phy. 21 (1982) 467–488.
[2] J. Thijssen, Computational Physics, Cambridge university press, 2007.
[3] D. Castelvecchi, IBM's quantum cloud computer goes commercial, Nat. News 543 (2017) 159.
[4] G. Aleksandrowicz, et al. Qiskit: an open-source framework for quantum computing. Accessed on: Mar. 16 (2019).
[5] H. Häffner, C.F. Roos, R. Blatt, Quantum computing with trapped ions, Phys. Rep. 469 (2008) 155–203.
[6] M.G. Dutt, et al., Quantum register based on individual electronic and nuclear spin qubits in diamond, Sci. 316 (2007) 1312–1316.
[7] K. Takeda, et al., A fault-tolerant addressable spin qubit in a natural silicon quantum dot, Sci. Adv. 2 (2016), e1600694.
[8] Q. Liao, Y. Fu, J. Hu, High-fidelity quantum state transfer and strong coupling in a hybrid NV center coupled to CPW cavity system, Chinese J. Phys. 66 (2020) 9–14.
[9] L. Petit, et al., Universal quantum logic in hot silicon qubits, Nat. 580 (2020) 355–359.
[10] J. Preskill, Quantum computing in the NISQ era and beyond, Quant. 2 (2018) 79.
[11] F. Arute, et al., Quantum supremacy using a programmable superconducting processor, Nat. 574 (2019) 505–510.
[12] E. Pednault, et al. Leveraging secondary storage to simulate deep 54-qubit sycamore circuits. arXiv preprint arXiv:1910.09534. (2019).
[13] F. Pan and P. Zhang. Simulating the Sycamore quantum supremacy circuits. arXiv preprint arXiv:2103.03074. (2021).
[14] K. Bharti, et al. Noisy intermediate-scale quantum (NISQ) algorithms. arXiv preprint arXiv:2101.08448. (2021).
[15] J. Biamonte, et al., Quantum machine learning, Nat. 549 (2017) 195–202.
[16] G. Torlai, R.G. Melko, Machine-learning quantum states in the NISQ era, Ann. Rev. of Conden. Matt. Phy. 11 (2020) 325–344.
[17] A. Montanaro, Quantum algorithms: an overview, NPJ. Quant. Info. 2 (2016) 1–8.
[18] D. Bacon, W. Van Dam, Recent progress in quantum algorithms, Commun. ACM. 53 (2010) 84–93.
[19] D. Deutsch, Quantum theory, the church–turing principle and the universal quantum computer, Proceed. Of The Roy. Soci. of Lond. A. Mathemat. and Physi. Sci. 400 (1985) 97–117.
[20] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proceed. of the Roy. Soci. of Lond.. Series A: Mathemat. and Physi. Sci.. 439 (1992) 553–558.
[21] D.R. Simon, On the power of quantum computation, SIAM. J. On Comput. 26 (1997) 1474–1483.
[22] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM. J. On Comput. 26 (1997) 1411–1473.
[23] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM. Rev. 41 (1999) 303–332.
[24] L.K. Grover. A fast quantum mechanical algorithm for database search. in Proceedings of the Twenty-Eighth Annual ACM Symposium On Theory of Computing. (1996).
[25] A.W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for linear systems of equations, Phys. Rev. Lett. 103 (2009), 150502.
[26] S. Mcardle, et al., Quantum computational chemistry, Rev. Mod. Phys. 92 (2020), 015003.
[27] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm. arXiv preprint arXiv:1411.4028. (2014).
[28] T. Albash, D.A. Lidar, Adiabatic quantum computation, Rev. Mod. Phys. 90 (2018), 015002.
[29] V.I. Voloshin, S.J. Lomonaco, and H.E. Brandt, Quantum computation and information: AMS special session quantum computation and information, january 19-21, 2000, Washington. Vol. 305. American Mathematical Soc. (2002).
[30] G. Brassard, P. Høyer, A. Tapp, Quantum counting. in International Colloquium On Automata, Languages, and Programming, Springer, 1998.
[31] M.A. Nielsen, I. Chuang, Quantum Computation and Quantum Information, American Association of Physics Teachers, 2002.
[32] J.P. Buhler, H.W. Lenstra, C. Pomerance, Factoring integers with the number field sieve. The Development of the Number Field Sieve, Springer, 1993, pp. 50–94.
[33] T. Monz, et al., Realization of a scalable Shor algorithm, Sci. 351 (2016) 1068–1070.
[34] E. Martin-Lopez, et al., Experimental realization of Shor's quantum factoring algorithm using qubit recycling, Nat. Photon. 6 (2012) 773–776.
[35] T. Kleinjung, et al., Factorization of a 768-bit RSA modulus. Annual Cryptology Conference, Springer, 2010.
[36] D.W. Berry, High-order quantum algorithm for solving linear differential equations, J. Of Phy. A: Mathemat. and Theoret. 47 (2014), 105301.
[37] A. Montanaro, S. Pallister, Quantum algorithms and the finite element method, Physi. Revi. A 93 (2016), 032324.
[38] S. Lloyd, Universal quantum simulators, Sci. (1996) 1073–1078.
[39] D. Aharonov and A. Ta-Shma. Adiabatic quantum state generation and statistical zero knowledge. in Proceedings of the Thirty-Fifth Annual ACM Symposium On Theory of Computing. (2003).
[40] W.P. Baritompa, D.W. Bulger, G.R. Wood, Grover's quantum algorithm applied to global optimization, SIAM. J. On Optimiz. 15 (2005) 1170–1184.
[41] A. Gilliam, S. Woerner, and C. Gonciulea. Grover adaptive search for constrained polynomial binary optimization. arXiv preprint arXiv:1912.04088. (2019).
[42] A. Ambainis, Quantum search algorithms, ACM. SIGACT. News 35 (2004) 22–35.
[43] D. Rolf. 3-SAT in RTIME (1.32971ˆn). (2003).
[44] A. Aspuru-Guzik, et al., Simulated quantum computation of molecular energies, Sci. 309 (2005) 1704–1707.
[45] A. Kandala, et al., Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, Nat. 549 (2017) 242–246.
[46] K. Ramachandran, G. Deepa, K. Namboori, Computational Chemistry and Molecular modeling: Principles and Applications, Springer Science & Business Media, 2008.
[47] R. Babbush, et al., Low-depth quantum simulation of materials, Physi. Revi. X 8 (2018), 011044.
[48] J. Romero, et al., Strategies for quantum computing molecular energies using the unitary coupled cluster ansatz, Quant. Sci. and Technol. 4 (2018), 014008.
[49] D. Wecker, M.B. Hastings, M. Troyer, Progress towards practical quantum variational algorithms, Physi. Revi. A 92 (2015), 042303.
[50] A. Garcia-Saez and J. Latorre. Addressing hard classical problems with adiabatically assisted variational quantum eigensolvers. arXiv preprint arXiv: 1806.02287. (2018).
[51] S. Matsuura, et al., VanQver: the variational and adiabatically navigated quantum eigensolver, New J. Phys. 22 (2020), 053023.
[52] H.R. Grimsley, et al., An adaptive variational algorithm for exact molecular simulations on a quantum computer, Nat. Commun. 10 (2019) 1–9.
[53] J.R. Mcclean, et al., The theory of variational hybrid quantum-classical algorithms, New. J. Phys. 18 (2016), 023023.
[54] D. Wang, O. Higgott, S. Brierley, Accelerated variational quantum eigensolver, Phys. Rev. Lett. 122 (2019), 140504.

[55] J.-.M. Reiner, et al., Finding the ground state of the Hubbard model by variational methods on a quantum computer with gate errors, Quant. Sci. and Technol. 4 (2019), 035005.
[56] J. Choi, J. Kim, A tutorial on quantum approximate optimization algorithm (QAOA): fundamentals and applications. 2019 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2019.
[57] L. Zhou, et al. Quantum approximate optimization algorithm: performance, mechanism, and implementation on near-term devices. arXiv preprint arXiv: 1812.01041. (2018).
[58] Ibmq. Solving combinatorial optimization problems using QAOA tutorial.).
[59] H.Q. Nguyen, M.N. Do, Downsampling of signals on graphs via maximum spanning trees, IEEE Trans. On Signal Process. 63 (2014) 182–191.
[60] K. Huang. Statistical mechanics. stme. (1987) 512.
[61] J. Håstad, Some optimal inapproximability results, J. Of The ACM. (JACM) 48 (2001) 798–859.
[62] M.X. Goemans, D.P. Williamson, Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming, J. Of The ACM. (JACM) 42 (1995) 1115–1145.
[63] A. Peruzzo, et al., A variational eigenvalue solver on a photonic quantum processor, Nat. Commun. 5 (2014) 4213.
[64] M. Hodson, et al. Portfolio rebalancing experiments using the quantum alternating operator ansatz. arXiv preprint arXiv:1911.05296. (2019).
[65] E. Farhi, et al. Quantum computation by adiabatic evolution. arXiv preprint quant-ph/0001106. (2000).
[66] T. Kadowaki, H. Nishimori, Quantum annealing in the transverse Ising model, Phys. Rev. E 58 (1998) 5355.
[67] A.B. Finnila, et al., Quantum annealing: a new method for minimizing multidimensional functions, Chem. Phys. Lett. 219 (1994) 343–348.
[68] X.-.S. Yang, Optimization and metaheuristic algorithms in engineering, Metaheuristics In Water, Geotech. And Trans. Engineer. (2013) 1–23.
[69] P.E. Black, Greedy algorithm, Dictionary Of Algo. and Data Struct. 2 (2005) 62.
[70] S. Kirkpatrick, C.D. Gelatt, M.P. Vecchi, Optimization by simulated annealing, Sci. 220 (1983) 671–680.
[71] E. Farhi, et al., A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem, Sci. 292 (2001) 472–475.
[72] Z. Bian, et al., The Ising model: teaching an old problem new tricks, D-Wave Syst. 2 (2010).
[73] J. Raymond, S. Yarkoni, E. Andriyash, Global warming: temperature estimation in annealers, Front. In ICT. 3 (2016) 23.
[74] M. Yamamoto, M. Ohzeki, K. Tanaka, Fair sampling by simulated annealing on quantum annealer, J. Of The Physi. Soc. Of Jap. 89 (2020), 025002.
[75] F. Glover, G. Kochenberger, Y. Du, Quantum bridge analytics I: a tutorial on formulating and using QUBO models, 4OR. 17 (2019) 335–371.
[76] J. Su, T. Tu, L. He, A quantum annealing approach for boolean satisfiability problem. 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE, 2016.
[77] W. Cruz-Santos, S.E. Venegas-Andraca, M. Lanzagorta, A QUBO formulation of the stereo matching problem for D-wave quantum annealers, Entro. 20 (2018) 786.
[78] S. Jiang, et al., Quantum annealing for prime factorization, Sci. Rep. 8 (2018) 1–9.
[79] W. Peng, et al., Factoring larger integers with fewer qubits via quantum annealing with optimized parameters, SCI. CHINA Phy, Mech. & Astro. 62 (2019) 60311.
[80] S. Boettcher, Analysis of the relation between quadratic unconstrained binary optimization and the spin-glass ground-state problem, Physi. Revi. Res. 1 (2019), 033142.
[81] M. Aramon, et al., Physics-Inspired optimization for quadratic unconstrained problems using a digital annealer, Front. Phys. 7 (2019).
[82] M. Ladue. Delivering quantum-inspired optimization solutions with fujitsu's digital annealer. (2019).
[83] C.H. Bennett, et al., Mixed-state entanglement and quantum error correction, Physi. Revi. A 54 (1996) 3824.
[84] D. Gottesman. Stabilizer codes and quantum error correction. arXiv preprint quant-ph/9705052. (1997).
[85] E. Knill, R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A 55 (1997) 900.
[86] A.Y. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. (N Y) 303 (2003) 2–30.
[87] P.W. Shor, Fault-tolerant quantum computation. Proceedings of 37th Conference on Foundations of Computer Science, IEEE, 1996.
[88] D. Gottesman, Theory of fault-tolerant quantum computation, Phys. Rev. A 57 (1998) 127.
[89] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium On Foundations of Computer Science, Ieee, 1994.
[90] S.J. Devitt, et al., Requirements for fault-tolerant factoring on an atom-optics quantum computer, Nat. Commun. 4 (2013) 1–8.
[91] K. Temme, S. Bravyi, J.M. Gambetta, Error mitigation for short-depth quantum circuits, Phys. Rev. Lett. 119 (2017), 180509.
[92] Y. Li, S.C. Benjamin, Efficient variational quantum simulator incorporating active error minimization, Physi. Revi. X 7 (2017), 021050.
[93] L.F. Richardson, J.A. Gaunt VIII, The deferred approach to the limit, Philosoph. Trans.Of The Roy. Soc. of Lond. Series A, Containing Papers Of A Mathemat. Or Physi. Char. 226 (1927) 299–361.
[94] S. Endo, S.C. Benjamin, Y. Li, Practical quantum error mitigation for near-future applications, Physi. Revi. X 8 (2018), 031027.
[95] T. Giurgica-Tiron, et al. Digital zero noise extrapolation for quantum error mitigation. arXiv preprint arXiv:2005.10921. (2020).
[96] A. He, et al. Resource efficient zero noise extrapolation with identity insertions. arXiv preprint arXiv:2003.04941. (2020).
[97] H. Pashayan, J.J. Wallman, S.D. Bartlett, Estimating outcome probabilities of quantum circuits using quasiprobabilities, Phys. Rev. Lett. 115 (2015), 070501.
[98] P. Czarnik, et al. Error mitigation with Clifford quantum-circuit data. arXiv preprint arXiv:2005.10189. (2020).
[99] A. Zlokapa and A. Gheorghiu. A deep learning model for noise prediction on near-term quantum devices. arXiv preprint arXiv:2005.10811. (2020).
[100] A. Strikis, et al. Learning-based quantum error mitigation. arXiv preprint arXiv:2005.07601. (2020).
[101] J.R. Mcclean, et al., Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states, Physi. Revi. A 95 (2017), 042308.
[102] S. Bravyi, et al. Mitigating measurement errors in multi-qubit experiments. arXiv preprint arXiv:2006.14044. (2020).
[103] M.R. Geller and M. Sun. Efficient correction of multiqubit measurement errors. arXiv preprint arXiv:2001.09980. (2020).
[104] C. Song, et al., Quantum computation with universal error mitigation on a superconducting quantum processor, Sci. Adv. 5 (2019) eaaw5686.
[105] X.-.M. Zhang, et al. Detection-based error mitigation using quantum autoencoders. arXiv preprint arXiv:2005.04341. (2020).
[106] J.I. Colless, et al., Computation of molecular spectra on a quantum processor with an error-resilient algorithm, Physi. Revi. X 8 (2018), 011021.
[107] R. Sagastizabal, et al., Experimental error mitigation via symmetry verification in a variational quantum eigensolver, Physi. Revi. A 100 (2019), 010302.
[108] A. Kandala, et al., Error mitigation extends the computational reach of a noisy quantum processor, Nat. 567 (2019) 491–495.
[109] P. Murali, et al. Software mitigation of crosstalk on noisy intermediate-scale quantum computers. in Proceedings of the Twenty-Fifth International Conference on Architectural Support For Programming Languages and Operating Systems. (2020).
[110] F. Neukart, et al., Traffic flow optimization using a quantum annealer, Front. In ICT. 4 (2017) 29.
[111] D. Solenov, J. Brieler, J.F. Scherrer, The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine, Mo. Med. 115 (2018) 463.
[112] E. National Academies of Sciences and Medicine, Quantum computing: Progress and Prospects, National Academies Press, 2019.