Quantum Science and Quantum Technology

Article *in* Statistical Science · February 2020

DOI: 10.1214/19-STS745

CITATIONS
9

READS
722

2 authors, including:

Xinyu Song
Shanghai University of Finance and Economics
11 PUBLICATIONS **47** CITATIONS

SEE PROFILE

Submitted to Statistical Science

Quantum Science and Quantum Technology

Yazhen Wang and Xinyu Song

University of Wisconsin-Madison
Shanghai University of Finance and Economics

Abstract. Quantum science and quantum technology are of great current interest in multiple frontiers of many scientific fields ranging from computer science to physics and chemistry, and from engineering to mathematics and statistics. Their developments will likely lead to a new wave of scientific revolutions and technological innovations in a wide range of scientific studies and applications. This paper provides a brief review on quantum communication, quantum information, quantum computation, quantum simulation, and quantum metrology. We present essential quantum properties, illustrate relevant concepts of quantum science and quantum technology, and discuss their scientific developments. We point out the need for statistical analysis in their developments, as well as their potential applications to and impacts on statistics and data science.

MSC 2010 subject classifications: Primary 81P45, 81P68, secondary 68Q12, 81P15, 81P40, 81P94.

Key words and phrases: Quantum communication, quantum information, quantum computation, quantum simulation, quantum annealing, quantum sensing and quantum metrology, quantum bit (qubit).

1. INTRODUCTION

Quantum science and quantum technology arise from a synthesis of quantum mechanics, information theory, and computing. They investigate the preparation and control of the quantum states of physical systems to generate new knowledge and technologies for information processing and transmission, computation, measurement, and fundamental understanding in ways that classical approaches can only do much less efficiently, or not at all. The fields comprise quantum communication, quantum information, quantum computation, quantum simulation, and quantum metrology (also known as quantum sensing), where quantum communication utilizes quantum means to transmit data in a provably secure way; quantum information describes the information of the state of a quantum system and the process of the information by quantum devices; quantum computation

Yazhen Wang is Professor, Department of Statistics, University of Wisconsin-Madison, Madison, WI 53706, USA (e-mail: yzwang@stat.wisc.edu). Xinyu Song is Assistant Professor, School of Statistics and Management, Shanghai University of Finance and Economics, Shanghai 200433, China (e-mail: song.xinyu@mail.shufe.edu.cn).

uses quantum effects to speed up certain calculations dramatically; quantum simulation reproduces the behavior of hard accessible quantum systems by manipulating well-controlled quantum systems; quantum metrology exploits the high sensitivity of coherent quantum systems to external perturbations for enhancing the performance of measurements of physical quantities. Quantum science and quantum technology differ from existing applications of quantum mechanics and information theory, such as lasers, transistors, MRI, and currently used classical computers and classical communication tools, in ways that we utilize distinct quantum phenomena like quantum superposition, entanglement, and tunneling, which do not have classical counterparts. In the past two decades, we have made tremendous progress in the study of quantum science and quantum technology for harnessing quantum phenomena to advance information processing and transmission, computation, and measurement.

Quantum science not only establishes a foundation for gaining a deeper understanding of nature, but also makes it possible to invent new quantum technology for accomplishing tasks that are impossible to achieve by classical techniques. Here quantum technology refers to technologies that explicitly deal with individual quantum states and specifically exploit special quantum properties that do not have classical analogue. They enable us to build quantum devices for achieving faster computation, more secure communication, and better physical measurements than classical techniques. This article intends to present an overview of such quantum aspects of science and technology, particularly in quantum information, quantum communication, and quantum computation.

The rest of the paper proceeds as follows. Section 2 briefly introduces quantum physics. Section 3 reviews basic quantum concepts used in quantum science and quantum technology. Sections 4 and 5 discuss quantum communication and quantum information, respectively. Section 6 illustrates quantum computation. It covers universal quantum computing based on the gate (or circuit) model, adiabatic quantum computing based on quantum annealing, and current development on building quantum computers. This section also includes quantum algorithms, quantum simulation, quantum machine learning, and quantum computational supremacy. Section 7 provides a short description of quantum metrology. Section 8 features concluding remarks and points out potential applications of quantum science and quantum technology to statistics and data science as well as the need of statistics in the development of quantum science and quantum technology. Additional materials are collected in Appendix as an Online Supplement.

2. QUANTUM PHYSICS AND ITS COMPUTATIONAL POTENTIAL

2.1 Mathematical concepts and notations

Unlike the typical literature on quantum mechanics that adopts technically more complicated concepts and notations such as operators with a continuous spectrum on an infinite-dimensional Hilbert space, for simplicity we choose to use relatively easy finite-dimensional linear algebra for the purpose of discussing quantum science and quantum technology. Since operators correspond to matrices in the finite dimensional case, we need to deal with only matrices and their operations such as eigen-analysis. Denote by $\mathbb{R}$ and $\mathbb{C}$, respectively, the sets of all real numbers and all complex numbers. A simple vector space is $\mathbb{C}^d$ comprising all d-tuples of complex numbers $(z_1, \cdots, z_d)$. We use Dirac notations $|\cdot\rangle$ (which

is called ket) and $\langle\cdot|$ (which is called bra) to show that the objects are column vectors or row vectors in the vector space, respectively. Denote by superscripts $*$, $'$ and $\dagger$ the conjugate of a complex number, the transpose of a vector or matrix, and conjugate transpose operation, respectively. For $|u\rangle$ and $|v\rangle$ in the vector space, we denote their inner product by $\langle u|v\rangle$, which induces a norm $\|u\| = \sqrt{\langle u|u\rangle}$, and a distance $\|u-v\|$ between $|u\rangle$ and $|v\rangle$. For example, $\mathbb{C}^d$ has a natural inner product

$$\langle u|v\rangle = \sum_{j=1}^{d} u_j^* v_j = (u_1^*, \cdots, u_d^*)(v_1, \cdots, v_d)',$$

where $\langle u| = (u_1, \cdots, u_d)$ and $|v\rangle = (v_1, \cdots, v_d)'$. Given a matrix $\mathbf{A} = (a_{ij})$, we say it is Hermitian if $\mathbf{A} = \mathbf{A}^\dagger$, and denote its trace by $tr(\mathbf{A}) = \sum_{j=1}^{k} a_{jj}$. A matrix $\mathbf{U}$ is said to be unitary if $\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$. For two matrices $\mathbf{A}_1$ and $\mathbf{A}_2$, define their commutator $[\mathbf{A}_1, \mathbf{A}_2] = \mathbf{A}_1\mathbf{A}_2 - \mathbf{A}_2\mathbf{A}_1$. Denote by $\otimes$ the tensor product operation of vectors or matrices. To analyze computer algorithms, we adopt a notation $O(h(m))$ to denote that the asymptotic scaling of an algorithm is upper-bounded by a function $h(m)$ of the input size m, with the notation $\tilde{O}(h(m))$ ignoring logarithmic factors.

2.2 Quantum physics

Quantum mechanics describes microscopic phenomena such as the positions and momentums of individual particles like atoms or electrons, the spins of electrons, the emissions and absorptions of light by atoms, and the detections of light photons. Unlike classical mechanics that can precisely measure physical entities like position and momentum, quantum physics is intrinsically stochastic in the sense that only a probabilistic prediction can be made about the results of the measurements performed.

We may describe a quantum system by its state and the dynamic evolution of the state. A quantum state is often characterized by a unit complex vector with dynamic unitary evolution, where the unitary evolution means that quantum states are connected by unitary matrices, and the dynamic evolution is governed by a differential equation called the Schrödinger equation. Specifically, let $|\psi(t)\rangle$ be the state of the quantum system at time t (also a wave function at time t). The states $|\psi(t)\rangle$ and $|\psi(t+s)\rangle$ at times t and $t+s$, respectively, are connected through $|\psi(t+s)\rangle = \mathbf{U}(s)\,|\psi(t)\rangle$, where $\mathbf{U}(s) = \exp(-\sqrt{-1}\mathbf{H}s)$ is a unitary matrix, and $\mathbf{H}$ is a Hermitian matrix on $\mathbb{C}^d$, which is known as the Hamiltonian of the quantum system. Differentiating both sides of $|\psi(t+s)\rangle = \exp(-\sqrt{-1}\mathbf{H}s)|\psi(t)\rangle$ with respect to s and letting s go to 0, we obtain the following Schrödinger equation for governing the continuous time evolution of $|\psi(t)\rangle$,

$$\sqrt{-1}\,\frac{\partial|\psi(t)\rangle}{\partial t} = \mathbf{H}|\psi(t)\rangle. \tag{2.1}$$

Note that although the Schrödinger equation is regarded as somewhat mysterious when it is first encountered, for a Markov chain in continuous time with a finite state space, transition probability matrix P_t and Q-matrix Q, we use exactly the same argument: from $P_{s+t} = P_s P_t$, by differentiation we obtain the Kolmogorov equation $\frac{\partial P_t}{\partial t} = QP_t$, which has the solution $P_t = \exp(Qt)P_0$.

As an alternative, we can describe a quantum system by a so-called density matrix. For a d-dimensional quantum system, its quantum state can be characterized by a density matrix $\boldsymbol{\rho}$ on the d-dimensional complex space $\mathbb{C}^d$, where $\boldsymbol{\rho}$ satisfies (1) Hermitian; (2) positive semi-definite; (3) unit trace. We often classify a quantum state as a pure state or an ensemble of pure states. A pure state corresponds to a density matrix $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is a unit vector in $\mathbb{C}^d$. An ensemble of pure states has a density matrix

$$\boldsymbol{\rho} = \sum_{j=1}^{J} p_j \, |\psi_j\rangle\langle\psi_j|, \tag{2.2}$$

which corresponds to the scenario that the quantum system is in one of states $|\psi_j\rangle$, $j = 1, \ldots, J$, with probability p_j being in the state $|\psi_j\rangle$. The quantum evolution in the density matrix representation can be described as follows. Let $\boldsymbol{\rho}_t$ be the density matrix of the state of the quantum system at time t. With the unitary matrix $\mathbf{U}(\cdot)$ and Hamiltonian $\mathbf{H}$ introduced above, the density matrix evolution is given by $\boldsymbol{\rho}_{t+s} = \mathbf{U}(t)\boldsymbol{\rho}_s\mathbf{U}^\dagger(t)$, with the Schrödinger equation in the form of

$$\boldsymbol{\rho}_t = e^{-\sqrt{-1}\mathbf{H}t}\boldsymbol{\rho}_0 e^{\sqrt{-1}\mathbf{H}t} \text{ or equivalently } \sqrt{-1}\frac{\partial \boldsymbol{\rho}_t}{\partial t} = [\mathbf{H}, \boldsymbol{\rho}_t]. \tag{2.3}$$

See Sakurai and Napolitano (2017) and Shankar (2012) for details.

As we will see in Section 3.1, the number of complex numbers and the dimensionality of vectors and matrices required to describe a quantum state and its evolution usually increase exponentially in the system size, rather than linearly in a classical system. As a result, a quantum system can store and manage an exponential number of complex numbers and perform data manipulations and calculations during the evolution of the system, while classical computers find it difficult to cope with the quantum system as it requires an exponential number of bits of memory to store the quantum state. Unlike the classical case where we often need to consider some extra structural assumptions or approximations when handling high-dimensional objects, quantum systems have potential to deal with exponentially high-dimensional problems without imposing additional constraints. Special quantum phenomena are utilized to accomplish quantum communication and computational tasks, and subsequent sections will illustrate that the quantum phenomena are often strange, and counter-intuitive. For example, light can be particles and waves (wave-particle duality); a cat can be alive and dead at the same time (quantum superposition); information can transmit instantaneously over a long distance without going through the intervening space (quantum teleportation); without sufficient energy, quantum particles can pass a barrier that is classically impossible (quantum tunneling).

3. QUANTUM BITS AND QUANTUM PROPERTIES

3.1 Quantum bit and superposition

In classical information and computation, the most fundamental entity is the bit, and the information encoded in a bit has two state values, 0 and 1. Classical bits can be materialized in multiple means, for example, they may be realized mechanically as switches or magnetically as hard drives. An important fact of the

classical bit is that its two state values are mutually exclusive, namely, its state can only be either 0 or 1. This fact leads to one thing in common for all of the realization means, that is, all classical physical devices prevent the simultaneous occurrence of the states, with an example of the switch being either on or off.

In quantum science and quantum technology, the counterpart of the classical bit is the quantum bit, which we call qubit for short. Similar to a classical bit with two state values 0 and 1, a qubit has states $|0\rangle$ and $|1\rangle$, where we use the customary Dirac notation $|\cdot\rangle$ to denote the qubit state. However, one key difference exists between a classical bit and a qubit. Specifically, the theory of quantum physics allows the description of a quantum physical system through probabilistic combinations of its states, which is referred to as the superposition property. The superposition of states can accommodate all predictions for the outcomes of physical measurements, moreover, it bears drastic consequences for the nature of the physical states ascribed to a system. In this regard, besides the states $|0\rangle$ and $|1\rangle$, a qubit can be in superposition states with the following form,

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle, \tag{3.1}$$

where complex numbers α_0 and α_1 are called amplitudes and satisfy $|\alpha_0|^2+|\alpha_1|^2 = 1$. As a result, the states of a qubit are unit vectors in a two-dimensional complex vector space $\mathbb{C}^2$. The states $|0\rangle$ and $|1\rangle$ form an orthonormal basis for the space and are often referred to as computational basis states. Unlike classical bits that have mutually exclusive states, qubits can be one and zero simultaneously, which is known as the most fundamental aspects of qubits. In other words, a superposition state is a state of matter that can be viewed as simultaneous occurrence of zero and one at the same time.

Qubits can be realized in various physical systems. Examples of qubits include the two states of an electron orbiting a single atom, the two different polarizations of a photon, the alignment of a nuclear spin in a uniform magnetic field, or the two directions of current flows in superconducting circuits. Specifically, in the atom model, $|0\rangle$ and $|1\rangle$ can be treated respectively as the so-called 'ground' and 'excited' states of the electron; if the atom is shined by light with appropriate energy and for a suitable amount of time, we may transfer the electron from the $|0\rangle$ state to the $|1\rangle$ state and vice versa. Furthermore, by adjusting the time length for shining the light on the atom, the electron can be moved from the initial state $|0\rangle$ into 'halfway' between $|0\rangle$ and $|1\rangle$, for example, into state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, or state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, where $|+\rangle$ and $|-\rangle$ form a qubit basis that is equivalent to the computational qubit basis $|0\rangle$ and $|1\rangle$. Note that the quantum state transformations are solutions of the Schrödinger equation (2.1) for particular choices of Hamiltonian $\mathbf{H}$ and time interval, and it is an interesting exercise for readers to find the appropriate Hamiltonians.

It is easy to examine a classical bit to determine its state, being 0 or 1, however, it is impossible to examine a qubit $|\psi\rangle$ to determine its state or find the values of its amplitudes α_0 and α_1 defined in (3.1). Because of the stochastic nature of quantum theory, performing measurements on the qubit $|\psi\rangle$ will result in measurement outcome 0 with probability $|\alpha_0|^2$, or measurement outcome 1 with probability $|\alpha_1|^2$. Moreover, performing measurements on the qubit will change its state.

Like classic bits, we may define multiple qubits. The states of one b-qubit are

unit vectors in a 2^b-dimensional complex vector space. The quantum exponential complexity is then shown in the exponential growth of dimensionality 2^b and the number of 2^b amplitudes required to specify superposition states. For the 2-qubit case, its superposition states are unit vectors in a 4-dimensional complex vector space, with the following form,

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle, \tag{3.2}$$

where $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ are four computational basis states, amplitudes α_x are complex numbers satisfying $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. As in the single qubit case, when measuring the 2-qubit, we obtain measurement outcome x as one of $00, 01, 10, 11$, with a corresponding probability $|\alpha_x|^2$. Furthermore, we may perform a measurement just on the first qubit of the 2-qubit system and obtain either the measurement outcome 0, with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, or the outcome 1, with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$. As quantum measuring changes the quantum state, depending on the measurement outcome obtained for the first qubit, being either 0 or 1, the 2-qubit system will be in the state

$$\frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \quad \text{or} \quad \frac{\alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}, \tag{3.3}$$

respectively. See Nielsen and Chuang (2000) and Wang (2012) for details.

3.2 Quantum entanglement

As one of the most mind-bending creatures known to science, quantum entanglement is often cited as the phenomenon that two particles that are connected by an invisible wave can share each other's properties regardless of the distance between them, just like a twin. It leads to the fact that none of the particles involved in a quantum system can be described by quantum states of individual subsystems. In other words, all information content of an entangled quantum system is fully entailed in the correlations between the individual subsystems while none of the subsystems on their own convey essential information of the entangled quantum system. For a multi-qubit system, its entangled states are superposition states that are described by joint properties of the individual qubits in the multi-qubit system. Consider an entangled 2-qubit system, we obtain a completely random outcome when performing measurements on only one of its entangled qubits. The measurement outcome is absolutely random, and it is impossible to gain information about the entangled system from the obtained random measurement outcome. As the entangled state involves two qubits, their correlation must contain two bits of classical information, and the classical information can only be gathered by comparatively examining the outcomes of the individual measurements on the separate subsystems. We as well point out an intriguing feature of entangled states: measuring one of the entangled qubits instantaneously casts the other one into the corresponding perfectly correlated state, which immediately destroys the entanglement as qubit measuring changes their quantum state. We take a Bell state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.4}$$

as an example to demonstrate entanglement, where $\alpha_{00} = \alpha_{11} = 0$, $\alpha_{01} = 1/\sqrt{2}$, and $\alpha_{10} = -1/\sqrt{2}$ in the expression of (3.2). As described in Section 3.1, measuring the first qubit of the Bell state $|\psi\rangle$, we obtain measurement outcome 0 or 1 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2 = 1/2$ and $|\alpha_{10}|^2 + |\alpha_{11}|^2 = 1/2$ respectively, which is completely random. According to (3.3), if the measurement outcome is 0 (or 1), then the state will be $|01\rangle$ (or $|10\rangle$, respectively). This result means that if the first measurement outcome is 0 (or 1), then the second qubit's state must be $|1\rangle$ (or $|0\rangle$, respectively) with measurement always being 1 (or 0, respectively), which indicates perfect correlation. Quantum states like the Bell state in (3.4) that can not be expressed as products of some single qubits are called entangled states, while product states refer to quantum states that can be written in the product form of single qubits. Over the past decades many physical experiments have been designed and conducted to test quantum entanglement through the so-called Bell inequality.

For the case of a 2-qubit system realized by the spins of two particles, imagine that the two-particle system is first prepared in an entangled state, then the two particles are drifted far away from each other. We now have Alice and Bob measure the first and second particles, respectively and sequentially. The perfect correlation suggests that after Alice obtains her spin measurement result (i.e., $+1$ or -1) on the first particle, the system has its state immediately plunged into the untangled state. As a result, the second particle now has a definite spin state, and Bob's spin measurement on the second particle always provides a definite opposite result (i.e., -1 or $+1$, respectively). This phenomenon of perfect correlation is referred to as anti-correlation in entanglement experiments. We will show that quantum properties such as superposition and entanglement play key roles in quantum science and quantum technology. See Horodecki et al. (2009), Nielsen and Chuang (2000) and Wang (2012) for more details.

4. QUANTUM INFORMATION

As its classical analog, quantum information targets at determining the laws governing any information process based on quantum theory. The core of classical information theory is Shannon's two coding theorems on noiseless and noisy channels. The coding theorems quantify classical bits by Shannon entropy for transmission over a noiseless channel and character the amount of information transmitted over a noisy channel with some error-correction scheme. On the other hand, the quantum-based theory has been established to apprehend quantum resources such as superposition, entanglement, non-locality, no-cloning, and quantum randomness. The quantum counterparts of Shannon entropy and Shannon noiseless coding theorem are von Neumann entropy and Schumacher's noiseless channel coding theorem, respectively. Schumacher's noiseless channel coding theorem describes quantum information needed to compress quantum states by von Neumann entropy (Schumacher, 1995). The quantum analog of Shannon's noisy channel coding theorem is Holevo-Schumacher-Westmoreland theorem employed to calculate the product quantum state capacity for some noisy channels (Holevo, 1998; Schumacher and Westmoreland, 1997).

Despite the resemblance, there exist inherent distinctions between classical information and quantum information. For example, while classical information such as digital images can be distinguished and copied, quantum superposi-

tion and no-cloning theorem imply that unknown quantum states cannot be completely distinguished or exactly copied. Consider another example, besides the computational basis $|0\rangle$ and $|1\rangle$ for the qubit space, we have another basis $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ given in Section 3.1, and quantum information can be encoded under each of these bases. Different ways of encoding quantum information are employed in quantum error-correction for reliable quantum computation and quantum information processing. Moreover, the information encoded under one basis cannot be extracted by performing measurement under another basis, which plays an important role in quantum cryptography. For example, consider encoding one bit of information in different bases by the polarization of light. Suppose that the computational basis formed by $|0\rangle$ and $|1\rangle$ represents the horizontal and vertical basis (corresponding to horizontally and vertically polarized photons). As diagonally and anti-diagonally polarized photons can be expressed in the horizontal and vertical basis as coherent superpositions of horizontal and vertical parts, the basis formed by $|+\rangle$ and $|-\rangle$ corresponds to the diagonal and anti-diagonal basis. We may encode a bit of information in the $|0\rangle$ and $|1\rangle$ basis by treating 0 to be horizontal polarization and 1 to be vertical polarization. For a photon encoded in either horizontal or vertical polarization, if we measure it in the diagonal and anti-diagonal basis, its information cannot be extracted. Indeed, as described in Section 3.1, we have

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle, \qquad |1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle,$$

and thus, when measuring $|0\rangle$ or $|1\rangle$ in the basis $|+\rangle$ and $|-\rangle$, we observe $+$ and $-$ with equal probability, that is, we observe a diagonally polarized photon in 50% of the cases and an anti-diagonally polarized photon in the other 50% of the cases.

Quantum physics provides new types of resources for information processing and transmission such as quantum teleportation, superdense coding, quantum key distribution, and quantum error-correction. Also, quantum information ideas have effectively been employed in other scientific studies such as many-body physics, quantum gravity, high-energy physics, quantum chemistry, quantum biology, and even for solving conjectures in the fields of classical information and computation. See Hayashi (2006), Krenn et al. (2017), Nielsen and Chuang (2000) and Wang (2012) for more details.

5. QUANTUM COMMUNICATION

5.1 Quantum teleportation

Quantum teleportation is a process through which we transfer the state of a quantum system (or qubit) to another distant quantum system (or qubit) without ever existing in the intervening space in between. The phenomenon can be illustrated by a three-step protocol of quantum teleportation as follows. First, Alice (the sender) and Bob (the receiver) together generated a special pair of entangled qubits, and each took one qubit of the two shared qubits when they split. Second, Alice was given a third qubit whose state was undisclosed to her, and she would like to teleport the unknown state. Third, Alice interacted the third qubit with her qubit and performed a special measurement on her original qubit

so that, while the measurement destroyed the entanglement and ruined any information about the state of her qubit, it would make Bob's qubit instantaneously project onto a new state that Bob could use to recover the original state of Alice's qubit. After the three steps, the state of Alice's qubit was transported to that of Bob's qubit. A key feature in the quantum teleportation protocol is the special entanglement and measurement, and the teleportation protocol only works when Bob was informed by Alice about her measurement outcome so that Bob could work accordingly to recover Alice's state. That is, a successful teleportation event requires classical communication between Alice and Bob, which necessarily restricts the speed of information transfer in the teleportation protocol to the speed of the classical communication channel. See Nielsen and Chuang (2000) and Wang (2012) for details.

It is important to note from the entire three-step protocol of quantum teleportation that contrary to what is usually mistakenly cited, quantum teleportation in principle does not allow faster-than-light communication or any transfer of matter or energy. Quantum teleportation transfers only the state of Alice's qubit to Bob's qubit but does not physically move Alice's qubit (particle) to Bob. Because it is required to send information via the classical channel, quantum teleportation is not capable of transmitting information faster than the speed of light. Otherwise, if Bob can obtain a copy of Alice's qubit (in the sense to physically obtain her 'qubit'), then Bob can make a direct measurement on the copied qubit to obtain the information that was sent over via the classical communication between Alice and Bob. In this way, faster-than-light communication becomes possible, however, the famous no-cloning theorem prevents the teleportation from copying any qubit.

The no-cloning theorem is referred to the fact that quantum mechanics prohibits the creation of identical copies of a general quantum state. Specifically, cloning a quantum state $|\psi\rangle$ means a procedure with the product state $|\psi\rangle|\psi\rangle$ as an output. We begin by introducing an ancilla quantum system whose state $|\varphi\rangle$ is not related to the state $|\psi\rangle$ being cloned. The no-cloning theorem means that there exists no unitary matrix $\mathbf{U}$ such that it evolves the initial state $|\psi\rangle|\varphi\rangle$ to the desired output state $|\psi\rangle|\psi\rangle$, that is,

$$\mathbf{U}(|\psi\rangle|\varphi\rangle) = e^{\sqrt{-1}\theta(\psi,\varphi)}|\psi\rangle|\psi\rangle, \tag{5.1}$$

where $e^{\sqrt{-1}\theta(\psi,\varphi)}$ stands for a phase factor, with phase $\theta(\psi,\varphi)$ being some real number. Indeed, if such $\mathbf{U}$ exists, it has a similar effect on any arbitrarily selected state $|\phi\rangle$ since cloning should work for any state. For the pair of states $|\psi\rangle$ and $|\phi\rangle$ in $\mathbb{C}^d$, we consider their inner product together with the ancilla state $|\varphi\rangle$, and use (5.1) to obtain

$$\begin{aligned}
\langle\psi|\phi\rangle = \langle\psi|\phi\rangle\langle\varphi|\varphi\rangle &= \langle\psi|\langle\varphi||\phi\rangle|\varphi\rangle \\
&= \langle\psi|\langle\varphi|\mathbf{U}^\dagger\mathbf{U}|\phi\rangle|\varphi\rangle \\
&= e^{-\sqrt{-1}\{\theta(\psi,\varphi)-\theta(\phi,\varphi)\}}\langle\psi|\langle\psi||\phi\rangle|\phi\rangle \\
&= e^{-\sqrt{-1}\{\theta(\psi,\varphi)-\theta(\phi,\varphi)\}}[\langle\psi|\phi\rangle]^2,
\end{aligned}$$

which indicates that $|\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2$, namely, $|\langle\psi|\phi\rangle|$ equals to 0 or 1. By the Cauchy-Schwartz inequality, we conclude that $|\psi\rangle$ is either equal to $|\phi\rangle$ (with a

phase factor) or orthogonal to $|\phi\rangle$, which is not possible for an arbitrary pair of states $|\psi\rangle$ and $|\phi\rangle$. This shows the non-existence of such $\mathbf{U}$ and thus proves the no-cloning theorem. Moreover, we may provide a simple illustration to show that no-cloning is a natural consequence of quantum theory as follows. Consider qubits $|0\rangle$, $|1\rangle$, and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, along with an ancilla qubit $|a\rangle$. Cloning implies there exists a unitary matrix $\mathbf{U}$ such that

$$\mathbf{U}(|0\rangle|a\rangle) = |0\rangle|0\rangle, \quad \mathbf{U}(|1\rangle|a\rangle) = |1\rangle|1\rangle, \quad \mathbf{U}(|+\rangle|a\rangle) = |+\rangle|+\rangle. \tag{5.2}$$

Using the first two equalities in (5.2) and linearity of $\mathbf{U}$ we immediately obtain

$$\begin{aligned} \mathbf{U}(|+\rangle|a\rangle) &= \mathbf{U}\left(\frac{1}{\sqrt{2}}|0\rangle|a\rangle + \frac{1}{\sqrt{2}}|1\rangle|a\rangle\right) \\ &= \frac{1}{\sqrt{2}}\mathbf{U}(|0\rangle|a\rangle) + \frac{1}{\sqrt{2}}\mathbf{U}(|1\rangle|a\rangle) \\ &= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle, \end{aligned}$$

which is an entangled state. It is easy to see that the entangled state cannot be written as product state

$$\begin{aligned} |+\rangle|+\rangle &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle). \end{aligned}$$

Therefore, an inconsistency occurs in (5.2), and it is impossible to have all three equalities in (5.2). See Krenn et al. (2017) and Nielsen and Chuang (2000) for more details.

5.2 Communication components

The classical communication required in quantum teleportation does not carry complete information about the qubit being teleported. Even if the information communicated in the classical channel is intercepted by an eavesdropper who may have complete knowledge about what Bob is required to do to recover the desired state, the information is futile if the eavesdropper cannot interact with the entangled qubit held in Bob's hands. Quantum physics opens the door to various distinct quantum secret sharing protocols such as quantum cryptography.

In quantum computation and quantum communication, we need to link qubits in quantum networks and transfer their states. As the no-cloning theorem forbids us to perfectly clone a quantum state, we can not use classical methods like amplifiers to carry out any transfer of qubits' states. The solution to this problem is a so-called quantum repeater, which allows the end-to-end generation of quantum entanglement in a way that every two connective particles of independent entangled pairs is combined so that the entanglement is relayed onto the remaining two particles. Thus, we are able to achieve the end-to-end state transmission of qubits via quantum teleportation. A quantum repeater is an important building block to interconnect different nodes in a quantum network, and quantum teleportation is one crucial requirement for the quantum repeater. This process is referred to as entanglement swapping and enables us to achieve long-distance quantum communication. See Krenn et al. (2017), Nielsen and Chuang (2000) and Sangouard et al. (2011) for more discussions.

5.3 Quantum cryptography

Cryptography allows two parties, the sender Alice and the receiver Bob, to exchange secret messages in their private communications, while at the same time, keeps it very hard for the third parties to 'eavesdrop' on the content of their communications. Applications of cryptography include online bank transactions, electronic commerces, and military communications. We discuss two cryptographic methods adopted in such communications. The first method is a private key cryptosystem, which calls for the two parties to share a secret key. Specifically, Alice employs the key to encrypt a message and obtain the cipher while the cipher can only be understood if the key is known. Alice sends the cipher to Bob who utilizes the key to decrypt the received cipher and read her message. The challenge for the private key cryptosystem lies in guarding the secret key against eavesdropping.

The alternative method is a public key cryptosystem invented in the 1970s that does not require the sharing of a secret key. This method is based on the complexity of hard computational problems such as finding the prime factors of very large numbers. Specifically, Bob first generates a pair of keys, a public one and a private one. He then announces his 'public key' to the general public, everyone including Alice can use the public key to encrypt messages and send him the encrypted messages. The real trick is that the encryption transformation generated by Bob's keys is specially designed such that with only the public key, it is extraordinarily hard, though not impossible, to reverse the encryption transformation. When announcing the public key, Bob retains a corresponding secret key for simple inversion of the encryption transformation and decryption of the received messages. A case in point is the RSA cryptosystem (Rivest et al., 1978), one of the most widely used cryptographic protocols. RSA is built on the extreme difficulty of finding prime factors for large composite numbers. Note the mathematical asymmetry of factoring: it is easy to compute a composite number from its prime factors by multiplying the primes, no matter how large they are; however, the reverse process can be very hard, in fact, it is extremely difficult to find the prime factors of some very large composite numbers. RSA encryption retains the large primes as a secret key and makes use of their product to design a 'public key'. Since the best known classical factoring algorithms have exponential complexity, and massive computational attempts to break the RSA system so far have led to no success, it is widely believed that the RSA system is secure against any classical computer-based attacks.

On the other hand, Peter Shor in 1994 discovered the so-called Shor's quantum factoring algorithm that can solve the factoring problem exponentially faster than the best known classical algorithms, thus quantum computers may be able to break the RSA system easily (Shor, 1994). That is, as quantum computers can factor prime numbers significantly faster than classical computers, an eavesdropper equipped with a quantum computer can decipher the encrypted text and read the secret message, with only the public information distributed by RSA. An approach to circumventing this difficulty is a quantum procedure known as quantum cryptography or quantum key distribution so that communication security cannot be undermined. The security of the quantum key distribution is based on the quantum principle that observing or measuring an unknown quantum system will disturb the system that is being monitored. When an eavesdropper listens to the transmission of the quantum key between Alice and Bob, the quantum

communication channel employed to set up the key will be disturbed by the eavesdropping, and the disturbance will make eavesdropping noticeable. As a result, Alice and Bob are able to discard the compromised key and retain only the secured key for their communication.

Specifically, quantum key distribution enables two authorized parties to create a secret key at a distance in two stages. In the first stage, the two communicating parties, Alice and Bob, obtain a preliminary key by exchanging quantum signals over the quantum channel and performing measurements. The obtained key is preliminary in the sense that it has two strongly correlated, but non-identical, and only partly secret strings. In the second stage, Alice and Bob utilize the classical channel to carry out an interactive post-processing protocol. The protocol permits them to refine the preliminary key and extract two identical and absolutely secret (known only to themselves) strings as two identical copies of the created secret key. During the two-stage process, the quantum channel is open to any possible maneuver from a third person. However, the classical channel communication needs the following authentication: while Alice and Bob recognize themselves, a third person may listen to their exchange, but cannot engage in it. In particular, the mission of Alice and Bob is to guarantee security against an adversarial eavesdropper, whom we call Eve, engaging in the conversation over the classical channel and tapping on the quantum channel. Here we use 'security' to convey precisely that the authorized parties never use a non-secret key, namely, either they can actually generate a secret key, or the protocol is aborted. Hence after transmitting the quantum signals, Alice and Bob need to evaluate the possible amount of information about the preliminary keys may have leaked out to Eve. This is the crucial advantage of quantum communication where information leakage in a quantum channel is quantitatively linked to a degradation of the communication. Such degradation and evaluation are not possible in classical communication. For example, when classical communication channels are tapped, such as phone conversations are bugged, the communication proceeds without any change, as nothing happens.

Besides taking advantage of quantum property that observing a quantum channel disturbs the quantum communication, we may employ quantum entanglement to further enhance the security of quantum key distribution by creating an entanglement-based quantum key distribution. The quantum entanglement property offers secure advantages for designing and implementing the protocol of the entanglement-based quantum key distribution. Let us consider the case where Alice and Bob share an entangled state of a qubit (or particle) pair. When they perform measurements on the qubits, the obtained random measurements will always be opposite due to the perfect correlation between entangled qubits. Alice and Bob then need to communicate over a classical channel regarding how the measurements are performed and obtained in order to sift through the results and obtain a secret key.

The security foundation of quantum key distribution can be established by the core principles of quantum physics such as superposition and no-cloning. When Eve is tapping on a quantum communication channel to extract some information, her act is some kind of measurement performing on the state of the quantum communication system, and the measurement will generally alter the state of the system. On the other hand, if Eve wants a correct copy of the state that Alice

conveys to Bob, she will not be successful as the no-cloning theorem shows that an unknown quantum state cannot be duplicated without being altered.

To be specific, the essential idea behind quantum key distribution is that Eve cannot obtain any information from the qubits, whose state is transmitted from Alice to Bob, without disturbing their state. Our proof arguments are as follows. First the no-cloning theorem described in Section 5.1 prevents Eve from copying Alice's qubit. Second, information gain implies disturbance in the sense that for any try to differentiate between two non-orthogonal quantum states, gaining information is only possible at the cost of brining in disturbance to the signal. Indeed, suppose that $|\psi\rangle$ and $|\phi\rangle$ are two non-orthogonal quantum states. Eve attempts to gain information about $|\psi\rangle$ and $|\phi\rangle$ by unitarily interacting the states $|\psi\rangle$ or $|\phi\rangle$ with an ancilla quantum system prepared in a state $|u\rangle$. If Eve's attempt does not disturb the states, we obtain two unitary matrices $\mathbf{U}_1$ and $\mathbf{U}_2$ such that

$$\mathbf{U}_1(|\psi\rangle|u\rangle) = |\psi\rangle|v_1\rangle, \qquad \mathbf{U}_2(|\phi\rangle|u\rangle) = |\phi\rangle|v_2\rangle,$$

where $|v_1\rangle$ and $|v_2\rangle$ are different states so that Eve can gain information about the identity of the states $|\psi\rangle$ and $|\phi\rangle$. However, since unitary transformations preserve inner products, it must be that

$$\langle v_1|\langle\psi||\phi\rangle|v_2\rangle = \langle u|\langle\psi|\mathbf{U}_1^\dagger\mathbf{U}_2|\phi\rangle|u\rangle = \langle u|\langle\psi||\phi\rangle|u\rangle,$$

that is, $\langle v_1|v_2\rangle\langle\psi|\phi\rangle = \langle u|u\rangle\langle\psi|\phi\rangle$. As $|\psi\rangle$ and $|\phi\rangle$ are non-orthogonal, $\langle\psi|\phi\rangle \neq 0$, and thus we obtain

$$\langle v_1|v_2\rangle = \langle u|u\rangle = 1,$$

which indicates that $|v_1\rangle$ and $|v_2\rangle$ have to be equal. This leads to a contradiction, as $|v_1\rangle \neq |v_2\rangle$. Therefore, distinguishing between $|\psi\rangle$ and $|\phi\rangle$ must disturb at least one of the states, and we can make secure quantum communication by transmitting non-orthogonal qubit states between Alice and Bob and checking for disturbance in their transmitted states.

Furthermore, the quantum key generation relies on the same quantum physical principles that quantum computation is based on. Unlike classical cryptography, the quantum key distribution does not merely depend on the computational difficulty of solving mathematical problems such as the factoring problem. Hence it can not be broken even by quantum computers. In a nutshell, the fundamental quantum physical principles allow for the unconditional security of quantum key distribution, namely, the possibility of guaranteeing security without setting any power limitation on the eavesdropper. See Bennett and Brassard (2014), Bernstein and Lange (2017), Buhrman et al. (2010), Krenn et al. (2017), and Nielsen and Chuang (2000) for more details.

Quantum physics was established to describe nature at the microscopic domain, but many ongoing research endeavors seek answers to what extent the quantum physical laws are relevant to the macroscopic realm. In particular, research efforts in quantum science and quantum technology aim to increase the distance between entangled quantum particles, and search for any possible fundamental restrictions to quantum entanglement, as well as to investigate if it is viable to create a global-scale quantum communication network in the future. Physical experiments on quantum key distribution have been successfully conducted in a long distance with current records of over a hundred kilometers on earth (Krenn et al., 2017) and over a thousand kilometers in space (Yin et al., 2017).

6. QUANTUM COMPUTATION

In contrast to classical computation where transistors are used to crunch the ones and zeroes individually, the new quantum resources such as quantum superposition and entanglement can allow quantum computation to manage both one and zero at the same time and do the trick of performing simultaneous calculations. Thus, quantum computers may outperform classical computers for solving certain computational problems. See Browne (2014), Campbell et al. (2017), Chong et al. (2017), Deutsch (1985), Mohseni et al. (2017), Nielsen and Chuang (2000) and Wang (2012).

6.1 Quantum computers

Classical computers are constructed from electrical circuits containing wires for carrying information around the circuits and logic gates for executing simple computational tasks. Similarly, quantum computers are built from quantum circuits with quantum gates to carry out quantum computation and process quantum information. In spite of the similarity, quantum computers are built on the unitary evolution of b logical qubits operating on a computational state space of 2^b dimensions, and the new quantum resources make it possible for quantum computers to outperform classical computers for certain tough tasks. Quantum information and quantum computation investigate how to harness the enormous information hidden in the quantum systems and how to make use of the immense potential computational power of quantum particles to perform computation and to process information. Intensive efforts are underway around the world to explore a number of physical systems and fabrication technologies for constructing quantum computers, where viable constructions must meet a set of requirements known as the DiVincenzo criteria (DiVincenzo, 1995). Major systems and technologies include superconducting circuits, ion traps, quantum dots, and other electronic semiconductor circuits, impurity spins, and linear optics (Nielsen and Chuang, 2000). Quantum computers of small scale have been built to demonstrate numerous simple examples of quantum algorithms and protocols. Over the years there are steadily increasing efforts by academics, government labs, large companies, and startups to reach the challenging goal of large scale quantum computation (DiCarlo et al., 2009; Johnson et al., 2011; Mariantoni et al., 2011; Sayrin et al., 2011).

As mentioned above, the physical equipment for the quantum computer fabrication must meet the DiVincenzo criteria including requirements that a quantum system realized qubits has to be well isolated to maintain its quantum properties and at the same time, the quantum system needs to be accessible so that the qubits can be operated to carry out computations and perform output measurements. In reality, there always exists some coupling of a quantum system to its environment, and the coupling leads to quantum decoherence, where decoherence refers to the loss of coherence between the components of the quantum system or quantum superposition from the interaction of the quantum system with its external entities. Therefore, the coupling strength dictates the two opposing requirements stated above. It is very challenging but critical to manage a quantum system of qubits for controlling the coupling strength and rectifying the effects of decoherence in quantum technology. Given the significant difficulties to build large-scale quantum computers with present technology, it is very important to

have scalable architectures for building quantum computers with about 100 well-behaved logical qubits in the near future. Such architectures may enable us to demonstrate the so-called quantum (computational) supremacy that is actively pursued by academic labs and companies like Google and IBM, where quantum supremacy refers to any major milestone achievement in the quest for outperforming classical computers on some tough computational tasks (Aaronson and Chen, 2016; Boixo et al., 2018; Harrow and Montanaro, 2017).

The quantum computing approach discussed so far is logic-gate based that has its purpose in developing a quantum version of classic logic gate operations and constructing a universal (or general purpose) quantum computers. Since significant technological difficulties present in the implementation of the gate (or circuit) model for building universal quantum computers, alternative quantum computing architectures, such as adiabatic quantum computing, are actively being explored to build special-purpose quantum computers for solving specific computational problems, though subjected to different challenges (Aharonov and Ta-Shma, 2003; Aharonov et al., 2008; Albash and Lidar, 2016). Examples of special-purpose quantum computers include quantum annealers and quantum simulators for solving tough simulation and optimization problems. Next two Sections 6.2 and 6.3 will present detailed discussions on quantum annealers and quantum simulators, respectively. Quantum annealers mean physical hardware implementations of quantum annealing. Quantum simulators refer to quantum devices utilized for simulating one quantum system by using another more controllable one, with the aim to solve special simulation problems that are computationally too demanding on classical computers.

6.2 Quantum annealers

Quantum annealing may be considered as adiabatic quantum computing that is based on the quantum adiabatic theorem for building special-purpose quantum computers, called quantum annealers, to solve combinatorial optimization problems. Quantum annealing is the quantum analog of classical annealing, with thermodynamics replaced by quantum dynamics. Quantum annealers are physical hardware devices to implement quantum annealing. See Albash and Lidar (2016), McGeoch (2014), and Wang et al. (2016). More detailed descriptions of quantum annealing are in the online appendix of Section A.1.

6.3 Quantum simulators

Quantum simulation is to intentionally and artificially mimic interacting quantum systems, which are hard to access and analyze, by employing other precisely controllable quantum systems that are easy to manipulate and investigate. Since the dimensionality of the space describing a quantum system scales exponentially with the system size, the classical simulation of quantum systems demands exponentially increasing resources. Likewise, it takes exponentially large resources to solve certain classical optimization problems particularly the NP-hard problems, such as finding the ground-state energy of a classical spin glass and solving the traveling salesman's problem. Quantum simulation may provide scientific means to simulate complex biological, chemical or physical systems in order to study and understand certain scientific phenomena and solve the related hard computational problems. Experimental platforms for quantum simulation consist of ultra-cold atomic and molecular quantum gases, ultra-cold trapped ions, polariton

condensates in semiconductor nanostructures, circuit-based cavity quantum electrodynamics, arrays of quantum dots, photonic quantum technology, and superconducting qubits with commercial applications in quantum annealers (Aspuru-Guzik and Walther, 2012; Blatt and Roos, 2012; Bloch et al., 2012; Boghosian and Taylor IV, 1998; Houck et al., 2012; Jané et al., 2002; Johnson et al., 2011; Nielsen and Chuang, 2000; Wang et al., 2016).

The essential of quantum simulation is to understand the dynamic evolution of a quantum system governed by the Schrödinger equation (2.1). That is, quantum simulation needs to describe and solve the Schrödinger equation (2.1) by either digital quantum computers or analog quantum machines. The solution of (2.1) has expression

$$|\psi(t)\rangle = e^{-i\mathbf{H}t}|\psi(0)\rangle, \qquad i = \sqrt{-1}, \tag{6.1}$$

and we need to evaluate $e^{-i\mathbf{H}t}$ numerically. It is extremely difficult to exponentiate the Hamiltonian $\mathbf{H}$ because its size increases exponentially in the system size. Common numerical approach often uses the first-order linear expansion $1 - i\mathbf{H}\delta$ to approximate $e^{-i\mathbf{H}(t+\delta)} - e^{-i\mathbf{H}t}$, which often yields unsatisfactory numerical solutions. Mathematically, quantum simulation is to explore whether higher order approximations are available to provide efficient methods for the evaluation of $e^{-i\mathbf{H}t}$. For example, consider a system with α particles in a d-dimensional space that has the following Hamiltonian

$$\mathbf{H} = \sum_{\ell=1}^{L} \mathbf{H}_\ell,$$

where L is a polynomial in $\alpha + d$, and each $\mathbf{H}_\ell$ acts on a small subsystem of finite size free from α and d. Note that it is easy to evaluate $e^{-i\mathbf{H}_\ell\delta}$ numerically, but very difficult to compute $e^{-i\mathbf{H}\delta}$. Because $\mathbf{H}_\ell$ and $\mathbf{H}_k$ are noncommutable, $e^{-i\mathbf{H}\delta} = e^{-\sum_{\ell=1}^{L} i\mathbf{H}_\ell\delta} \neq e^{-i\mathbf{H}_1\delta}\cdots e^{-i\mathbf{H}_L\delta}$. By the Trotter formula (Trotter (1959) and Proposition 3.1 in Wang (2011)), we obtain

$$e^{-i\mathbf{H}\delta} = \left\{e^{-i\mathbf{H}_1\delta/2}\cdots e^{-i\mathbf{H}_L\delta/2}\right\}\left\{e^{-i\mathbf{H}_L\delta/2}\cdots e^{-i\mathbf{H}_1\delta/2}\right\} + \mathcal{O}(\delta^2). \tag{6.2}$$

Thus, we obtain a second order approximation of $e^{-i\mathbf{H}\delta}$ by the first term on the right hand-side of (6.2), which only needs us to evaluate each $e^{-i\mathbf{H}_\ell\delta}$, $\ell = 1, \ldots, L$.

Introduced by Feynman (1982), quantum simulation itself has been developed into a core field within quantum computation. A quantum simulator can be any physical quantum system precisely prepared or manipulated in a way targeting at studying interesting features of an interacting complex quantum system, which is computationally intractable or difficult to simulate on classical computers. A quantum simulator can be a digital quantum simulator so that the controllable quantum system is implemented on a universal quantum computer, or an analog quantum simulator so that the controllable quantum system is a quantum physical device to reconstruct the time evolution of an interacting quantum system under precisely controlled conditions. Like universal quantum computers, digital quantum simulators face significant challenges in scaling architectures. However, analog quantum simulators can be addressed and experimented in a relatively large scale with currently available technology, and thus may provide

new tools for us to investigate interacting many-particle quantum systems and attack optimization problems beyond the reach of classical computers. See Childs et al. (2018), Jiang et al. (2017), Kassal et al. (2008, 2011), Lanyon et al. (2010), Nielsen and Chuang (2000), and Wang (2011, 2012).

It is likely that the first practical application of quantum computation is quantum simulation since even moderate quantum simulation devices have the potential to carry out simulations infeasible by classical computers. For example, in quantum chemistry, molecular energies can be computed by digital quantum simulation devices of size 100 to 150 logical qubits with excellent precision and accuracy that considerably exceed the limitations of classical computers. In particular, in the near to medium term, analog quantum simulators may offer us a novel tool to study complicated quantum systems and hard optimization problems that are unreachable by classical computers. Again a computational advantage of quantum simulators over classical ones may clearly demonstrate quantum supremacy (given in Section 6.1) in realistic applications. In the long run, the importance of quantum simulation may lie in the applications of large-scale quantum simulations to solve fundamental problems in physics, materials science and quantum chemistry (Abrams and Lloyd, 1997; Aspuru-Guzik et al., 2005; Boghosian and Taylor IV, 1998; Cirac and Zoller, 2012; Kassal et al., 2011; Lloyd, 1996).

6.4 Quantum algorithms

Quantum algorithms are algorithms that run on quantum computation models, such as the most commonly used quantum gate or circuit model, by taking input qubits and producing output measurements for the solutions of specific computational tasks. While a classical algorithm takes a step-by-step procedure to solve a given problem on a classical computer, a quantum algorithm is a step-by-step problem-solving procedure, with each step performed on a quantum computer. We note that all classical algorithms can be in principle executed on a quantum computer, all problems solvable on a quantum computer are solvable on a classical computer, and problems undecidable by classical computers remain undecidable on quantum computers. However, quantum algorithms are essentially different from their classical counterparts in the sense of being genuine quantum, that is, quantum gate operations are reversible unitary transformations, and quantum algorithms utilize fundamental quantum properties such as quantum superposition and quantum entanglement. We refer to quantum algorithms as the algorithms that are inherently quantum for achieving faster speed than classical algorithms in solving some tough problems. It should be pointed out that while quantum algorithms can not be worse than classical algorithms, we should not expect quantum algorithms to yield advantage for every single problem; in fact, they usually do not. As a matter of fact, quantum computers augment, but do not replace classical computers. A continual challenge in quantum science is to invent new quantum algorithms to speed up the best classical algorithms. For example, quantum superposition indicates that we can potentially carry out exponentially many computations in parallel, but it is tricky to extract the solution from such an exponential superposition to achieve some quantum speedup, as observing the qubit system destroys its state. This is where we need clever designs of quantum software. Common techniques employed to create quantum algorithms include quantum Fourier transform, phase estimation, amplitude amplification,

quantum walk, quantum annealing and quantum simulation. The widely known quantum algorithms include Shor's factoring algorithm and Grover's search algorithm, which are, respectively, exponentially faster and quadratically faster than the best known and best classical algorithms for the same tasks. Many other algorithms were created for a wide range of problems and applications such as searching, sorting, counting, sampling, simulation, and optimization. See Montanaro (2016), Nielsen and Chuang (2000) and Wang (2012) for more discussions.

As a case in point, we consider quantum computation for the Grover and parity problems. Let $f(x)$ be a function defined on the integers from 1 to N and taking the values ± 1. Define the parity of $f(x)$ by

$$\mathrm{Par}(f) = \prod_{x=1}^{N} f(x).$$

The parity of $f(x)$ can be either $+1$ or -1, and always depends on the values of $f(x)$ at all N points. It has been proved that with no further information about $f(x)$, both classical and quantum algorithms have $O(N)$ time-complexity to determine its parity, and thus quantum computers cannot outperform classical computers for the parity problem. For the Grover problem, there is a further information that $f(x)$ is either identically equal to 1 or it is 1 for $N-1$ of the x's and equal to -1 at one unknown value of x. For such $f(x)$, its parity indicates its type, and the computational task for the Grover problem is to determine the type of $f(x)$ and search for the unknown value of x (if it exists). With the additional information about $f(x)$, the best classical and quantum algorithms for the Grover problem have complexity $O(N)$ and $O(\sqrt{N})$, respectively, and thus there is an optimal $\sqrt{N}$ quantum speedup. It is interesting to note that, although there is a quadratic quantum speedup for the Grover problem, the parity problem has no quantum speedup (see Farhi et al. (1998) and Grover (1997)). This example indicates that neither classical nor quantum computers are expected to be best for all computational tasks.

6.5 Quantum machine learning

Quantum machine learning extends classical machine learning to the quantum realm. Classical machine learning and statistical learning often refer to an array of statistical approaches to analyzing data, with the goal of inferring the future behavior of target variables (such as the function relationships of variables and their dynamic processes) from training data. The learning procedure involves inference, which addresses how statistically efficient we can learn the functions or processes from given data, and computation, which handles how much computational resources are required to perform a learning task and how fast algorithms can be designed to carry out the learning task. The learning objective is to search for a model that fits well to training data but more importantly enjoys good generalization capability, which refers to the property of the learned model with good prediction performance on new observations. Common learning approaches rely on regularization-based methods leverage on optimization techniques to solve learning problems. Quantum learning theory investigates how quantum resources can affect the learning efficiency. The theory indicates that it is possible for quantum learners to achieve higher efficiency such as better generalization errors in learning difficult functions for some particular learning

models. However, the major advantages that quantum mechanics can provide is largely in terms of computation. In other words, quantum machine learning can offer advantages over its classical counterpart in terms of computational complexity. Therefore, it is reasonable to expect quantum computers to be faster than classical computers for solving some machine learning problems, but it is important and challenging to explore quantum softwares that enable quantum machine learning to realize such quantum speedups. Recent development indeed shows a class of quantum machine learning algorithms exhibit some quantum speedups. For example, from a computational perspective, solving linear equation systems is almost ubiquitous in machine learning, and finding a learning solution usually comprises a sequence of standard linear algebra operations such as matrix multiplication and inversion. Quantum linear algebra algorithms offer quantum speedups over their classical analogs. As a case in point, quantum basic linear algebra subroutines (BLAS), which include finding eigenvectors and eigenvalues and solving linear equations, exhibit exponential quantum speedups over their best known classical counterparts. The quantum BLAS renders quantum speedups for an array of data analysis and machine learning algorithms including linear algebra operation, gradient descent, Newton's method, linear programming, semidefinite and quadratic programming, topological analysis, least-squares, nearest-neighbor, support vector machines, clustering, and principal component analysis (PCA). Also special-purpose quantum computers, such as quantum annealers and programmable quantum optical arrays, bear architectures well suited to quantum optimization and deep learning particularly quantum deep learning with Boltzmann machines. More discussions can be found in Adachi and Henderson (2015), Amin et al. (2018), Arodz and Saeedi (2019), Arunachalam and de Wolf (2018), Benedetti et al. (2016), Biamonte et al. (2017), Brandão et al. (2018), Ciliberto et al. (2018), Dunjko et al. (2016), Dunjko and Briegel (2018), Jordan (2005), Lloyd et al. (2014), O'Gorman et al. (2015), Rebentrost et al. (2014), Salakhutdinov and Hinton (2009), Shenvi et al. (2003), Svore et al. (2014), Wiebe et al. (2014b), Wiebe et al. (2015), Wiebe and Granade (2016), and Wittek (2014). The online appendix of Section A.2 provides detailed illustrations of quantum principal component analysis, quantum support vector machines, quantum deep learning with Boltzmann machines, quantum phase estimation, quantum machine learning for quantum data, quantum sampling, and quantum machine learning with noise.

6.6 Quantum computational supremacy

Determining a quantum speedup depends on how we define the quantum speedup notation. One approach is to take a formal computational complexity perspective based on rigorous mathematical proofs. Another realistic perspective is based on what can be achieved with feasible finite size devices and requires sound statistical evidence to confirm a scaling advantage over certain finite range of problem sizes. For example, it has already been rigorously proved in terms of computational complexity that quantum algorithms like Grover's search algorithm and Shor's factoring algorithm offer speedups over known classical algorithms. Unfortunately, such rigorous poofs are often not available for most cases, and even available, many existing quantum algorithms fail to provide reference for any specific implementation such as the exact number of qubits needed to

implement them; in fact, they often cannot be implemented on about 100 qubit platforms available in the near to medium term. We need to resort to the second perspective, and detecting a scaling advantage of quantum computing over classical computing would hinge on the so-called benchmarking problem, namely, the existence of a quantum computer performed on well designed computational tasks with sound statistical analysis of computing experiments and resulting data. Such advantages may include improved computational speed, accuracy, and sampling for classically inaccessible systems. Quantum algorithms and computational problems are created for these platforms with a limited number of qubits where classical computation is impossible. The mission involving both hardware and software along with statistical analysis aims at demonstrating the quantum computational supremacy given in Section 6.1. Quantum scientists in Google and IBM are building quantum computers of 50 to 100 qubits to demonstrate quantum supremacy. For example, the Google quantum AI group is working on a quantum processor of 72 superconducting qubits to demonstrate quantum supremacy for sampling from the output distributions of random quantum circuits, where it is hard for current supercomputers to handle the sampling problem beyond around 50 qubits. See Aaronson and Chen (2016), Boixo et al. (2018), Bouland et al. (2018), Bravyi et al. (2018), Harrow and Montanaro (2017), Lund et al. (2017), Markov et al. (2018), Neill et al. (2018) and Rønnow et al. (2014). Below we briefly describe boson sampling and random quantum circuits.

6.6.1 **Boson sampling** is a quantum computation model where n identical bosons pass through a network of passive optical elements (beamsplitters and phase-shifters) and then the locations of the bosons are detected. Quantum supremacy can be demonstrated by implementing boson sampling with a medium size network. A network system with 50 photons (qubits) and 2500 paths is currently intractable for classical computers. To implement boson sampling all required physical devices are single-photon sources, beamsplitters, phase-shifters and photon-detectors. The physical implementation of the scheme encounters a myriad of technicalities such as synchronization of pulses, mode-matching, quickly controllable delay lines, tunable beamsplitters and phase-shifters, single-photon sources, and accurate, fast, single photon detectors.

To define the boson sampling model, we adopt a statistical approach based on the permanents of the submatrices of a unitary matrix, which requires minimal quantum physics and quantum computation terminology. For a $n \times n$ matrix $A = (a_{ij})$, we define its permanent by

$$\mathrm{Perm}(A) = \sum_{\pi} \prod_{i=1}^{n} a_{i\pi(i)},$$

where the sum is over all permutations π of $1, 2, \cdots, n$. Consider the quantum system involving n identical photons and m modes, where we may loosely interpret 'mode' as the location of a photon, and we are only interested in the case of $m \geq n$. The quantum system has computational basis states of the form $|\mathbf{s}\rangle = |s_1, s_2, \cdots, s_m\rangle$, where s_i indicates the number of photons in the i-th mode. Denote the set corresponding to all the computational basis states by

$$\Omega_{m,n} = \{\mathbf{s} = (s_1, s_2, \cdots, s_m) : s_1 + s_2 + \cdots + s_m = n\}.$$

It is easy to see that the total number of elements in $\Omega_{m,n}$ is equal to $M = \binom{m+n-1}{n}$. For a given $m \times m$ unitary matrix $\mathbf{U}$ and each $\mathbf{s} \in \Omega_{m,n}$, we obtain matrix $\mathbf{U_s}$ from $\mathbf{U}$ by keeping its first n columns and repeating s_j times its j-th row. Define a discrete probability distribution on $\Omega_{m,n}$ as follows,

$$\Pr(\mathbf{s}) = \frac{|\mathrm{Perm}(\mathbf{U_s})|^2}{s_1!...s_m!}.$$

It can be shown that $\Pr(\mathbf{s})$ is a well-defined probability distribution on $\Omega_{m,n}$ and corresponds to the quantum system with n photons, m modes and an optical network whose action is determined by the unitary matrix $\mathbf{U}$. Boson sampling refers to sampling from distribution $\Pr(\mathbf{s})$. As classical computers can not handle the sampling problem even with moderate size, we may demonstrate the quantum supremacy by successfully implementing boson sampling of reasonable size on quantum computing devices. More details can be found in Harrow and Montanaro (2017) and Lund et al. (2017).

6.6.2 **Random quantum circuits** are created in a specific way so that when they are generated with enough 'complexity', even the most powerful classical supercomputer can not directly simulate the generated quantum circuits. However, quantum computers can sample from the output distributions corresponding to the obtained quantum circuits. Here a quantum circuit is a sequence of d clock cycles of one- and two-qubit gates with gates applied to different qubits in the same cycle. The number d of cycles is called the depth of the circuit. We say a random quantum circuit has enough 'complexity', if both its qubits and depth are large enough. If the gates to be applied are chosen from a universal quantum gate set, the unitary matrix $\mathbf{U}$ of the circuit is a random matrix whose distribution converges to the Haar measure on the collection of unitary matrices when the depth of the circuit goes to infinity. Specifically when a quantum circuit contains n qubits, with 2^n computational basis states $|\mathbf{x}\rangle = |x_1 x_2 \cdots x_n\rangle$, $x_i \in \{0, 1\}$, a quantum state $|\psi_d\rangle$ produced by the random quantum circuit is a linear combination of the computational basis and thus has 2^n amplitudes, each with real and imaginary parts. Therefore there are 2^{n+1} parameters in each quantum state. As the unitary matrix $\mathbf{U}$ of the random quantum circuit converges in distribution to the Haar measure, the random vector of the amplitude parameters asymptotically follows a uniform distribution on the unit sphere. Define the output distribution of the random quantum circuit to be measurement probability $p(\mathbf{x}) = |\langle \mathbf{x}|\psi_d\rangle|^2$. As the depth d of the random quantum circuit goes to infinity, $p(\mathbf{x})$ approaches the Porter-Thomas distribution. The Google research group is working on finding ways to generate random quantum circuits so that their output distributions quickly converge to the Porter-Thomas distribution. Based on the asymptotic distribution, we may develop a statistical approach to determine if a sample is generated from the theoretical output distribution of a desired random quantum circuit. Since it is difficult for classical supercomputers to deal with the sampling problem beyond around 50 qubits at the present time, the Google quantum scientists are working on the implementation of quantum random circuits in a two dimensional lattice to achieve quantum supremacy. See Boixo et al. (2018), and Neill et al. (2018) for more details.

7. QUANTUM METROLOGY

Measurement is at the heart of science, technology, industry, and commerce. We need measurements and metrological standards to quantitatively assess scientific phenomena and technological progress, and gauge the exchange of goods and service including information. Measurement devices are physical apparatuses whose functions and accuracy are governed by the laws of physics, and transformative improvements in measurement technologies often follow the utilization of a new physical law. Quantum metrology (or quantum sensing) is to exploit the strange laws of quantum physics to build new and better sensors and measuring devices. Fueling with quantum laws, quantum metrology may lead to a game-changing shift in scientific studies, technological progress, as well as commerce and industry developments.

The basic concept of quantum metrology is that a probe device interacts with an appropriate system to learn the properties of the system, where the interaction alters the state of the probe, and measurements of the probe uncover the characteristic parameters of the system. For quantum sensing, the probe is usually prepared in one certain quantum state, its encounter with the system normally changes its state with both beneficial and adversarial effects in the sense that it not only responds to the parameters of interest but also decoheres the probe (which means there is loss of information from the probe into the system due to quantum decoherence, illustrated in Section 6.1). Then appropriately devised measurements can ascertain in what way and to what extent such encounter has changed the state of the probe, which enables quantum sensing to evaluate the system parameters. Quantum sensing promises to develop high-resolution and highly sensitive measurement techniques that will provide better precision than the same measurement performed under a classical framework. They include quantum sensors, quantum clocks, and quantum imaging. The applications range from the sub-nano to the galactic scale, while some are in fact close to commercial use. The potential impact of quantum metrology is far-reaching. An array of distinct platforms allow quantum-enhanced measurement of time, space, rotation, as well as gravitational, electrical and magnetic fields. The technologies are promising to make fundamental changes in a wide range of fields such as physics, chemistry, biology, medicine or data storage and processing.

There is a strong link between quantum metrology and quantum information. For example, both quantum information and quantum sensing rely on the same quantum properties such as entanglement, in particular, high level of multipartite entanglement, to achieve better performance than their classical counterparts. See Degen et al. (2017), Kruse et al. (2016), and Pezzè et al. (2016) for more details.

Quantum tomography plays an important role in quantum sensing. Quantum state tomography refers to reconstruction of a quantum state based on measurements performed on the quantum state. Statistically it is a density matrix estimation problem based on quantum measurements. Common quantum measurements are on observable $\mathbf{M}$, which is defined as a Hermitian matrix on $\mathbb{C}^d$. For example, the Pauli matrices as observables are widely employed to perform quantum measurements in quantum science and quantum technology, and we may represent many density matrices through Pauli matrices. Suppose that the observable $\mathbf{M}$ has the following spectral decomposition, $\mathbf{M} = \sum_{a=1}^{r} \lambda_a \mathbf{Q}_a$, where λ_a are r different real eigenvalues of $\mathbf{M}$, and $\mathbf{Q}_a$ are projections onto the eigen-

spaces corresponding to λ_a. Given a quantum system prepared in state $\boldsymbol{\rho}$, we use a probability space $(\Omega, \mathcal{F}, P)$ to define measurement outcomes when performing measurements on the observable $\mathbf{M}$. Let R be the measurement outcome of $\mathbf{M}$. The theory of quantum physics indicates that R is a random variable on $(\Omega, \mathcal{F}, P)$ which takes values in $\{\lambda_1, \lambda_2, \ldots, \lambda_r\}$, and has probability distribution

$$P(R = \lambda_a) = tr(\mathbf{Q}_a \boldsymbol{\rho}),\ a = 1, 2, \ldots, r, \quad E(R) = tr(\mathbf{M}\boldsymbol{\rho}).$$

Quantum state tomography is to reconstruct $\boldsymbol{\rho}$ from independent and identically distributed measurement outcomes $R_1, \ldots, R_n$. See Artiles et al. (2005), Cai et al. (2016), Malley and Hornstein (1993) and Wang and Xu (2015).

Designing and controlling quantum systems are complex and challenging in the development of quantum science and quantum technology. Statistical methods provide powerful tools for the study of quantum design and quantum control. Examples of successful applications include quantum gate constructions with high fidelity precision in quantum computation and quantum information, extraction of theoretical insights about quantum states in condensed matter, and quantum control procedures in optimizing adaptive quantum metrology. Like quantum phase estimation and quantum tomography, many quantum problems are in essence statistical problems, and it is our firm belief that statistics and data science have great potential to make significant improvement in quantum metrology.

8. CONCLUDING REMARKS

Quantum science and quantum technology gain enormous attention in multiple frontiers of many scientific fields. Quantum computation can give rise to an exponential speedup over classical couterpart for tackling certain computational tasks, quantum information can bring about exponential savings in information transmission for handling computational and communication jobs, and quantum communication can offer more secure cryptosystems than classical analogue for solving communication problems. Some of the quantum protocols are already in practical implementation, such as quantum-fingerprinting, quantum key distribution, quantum annealing, and quantum simulation. This paper reviews quantum science and quantum technology from a statistical perspective. We introduce concepts like key quantum properties and qubits. We present quantum communication and quantum information, illustrate quantum computation and quantum metrology, and discuss major quantum technologies associated with them. We show the advantages of quantum techniques over the available classical counterparts.

As statistics and machine learning nowadays heavily involve computation, it is natural to expect quantum computation to play a major role in data science. Indeed, quantum computation and quantum simulation may have tremendous potential to revolutionize computational statistics and data science. On the other hand, there is great demand in studying statistical issues for theoretical research and experimental work in quantum science and quantum technology. As quantum phenomena are intrinsically stochastic, and data collected in quantum experiments become more and more complex, we need to develop sophisticated statistical methods for enhancing data analysis and improving understanding of quantum events (Paesani et al., 2017; Wang, 2011, 2012, 2013; Wang et al., 2016; Wiebe et al., 2014a,b). A great deal of current work is taken place on creating new

protocols and developing novel approaches to certifying quantum devices such as testing and assessing their quantum performances. Clearly, such certification requires efficient and scalable statistical methods for calibrating and validating quantum properties. Moreover, certification needs to take into account commercial considerations for compliance with industry standards by working together with industry, academics, national labs, and government organizations (Acín and Masanes, 2016; Wang et al., 2016; Wiebe et al., 2014a).

As indicated in Section 6.1, the bottleneck of quantum computing at the present time is primarily on quantum hardware, and current quantum computing largely depends on what kinds of quantum computers experimentalists can build. On the other hand, as we have demonstrated in Section 6.6 for the quantum computational supremacy endeavor, besides hardware quantum computing also requires sophisticated mathematical models, sound statistical analysis, and better computational tools. As a matter of fact, in general we call for some combination of new experimental techniques, better mathematical and statistical understanding, and improved computational tools in order to significantly advance the development of quantum science and quantum technology.

ACKNOWLEDGEMENTS

The research of Yazhen Wang was supported in part by NSF grants DMS-1528375, DMS-1707605, and DMS-1913149. The research of Xinyu Song was supported by the Fundamental Research Funds for the Central Universities (2018110128), China Scholarship Council (201806485017) and National Natural Science Foundation of China (Grant No. 11871323). The authors thank David Siegmund for helpful comments and suggestions which led to improvements of the paper.

REFERENCES

Aaronson, S. and Chen, L. (2016). Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*.

Abrams, D. S. and Lloyd, S. (1997). Simulation of many-body fermi systems on a universal quantum computer. *Physical Review Letters*, 79(13):2586.

Acín, A. and Masanes, L. (2016). Certified randomness in quantum physics. *Nature*, 540(7632):213.

Adachi, S. H. and Henderson, M. P. (2015). Application of quantum annealing to training of deep neural networks. *arXiv preprint arXiv:1510.06356*.

Aharonov, D. and Ta-Shma, A. (2003). Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 20–29. ACM.

Aharonov, D., Van Dam, W., Kempe, J., Landau, Z., Lloyd, S., and Regev, O. (2008). Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM review*, 50(4):755–787.

Albash, T. and Lidar, D. A. (2016). Adiabatic quantum computing. *arXiv preprint arXiv:1611.04471*.

Amin, M. H., Andriyash, E., Rolfe, J., Kulchytskyy, B., and Melko, R. (2018). Quantum boltzmann machine. *Physical Review X*, 8(2):021050.

Arodz, T. and Saeedi, S. (2019). Quantum sparse support vector machines. *arXiv:1902.01879v2*.

Artiles, L., Gill, R., and Gut ă, M. (2005). An invitation to quantum tomography. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 67(1):109–134.

Arunachalam, S. and de Wolf, R. (2018). Optimal quantum sample complexity of learning algorithms. *The Journal of Machine Learning Research*, 19(1):2879–2878.

Aspuru-Guzik, A., Dutoi, A. D., Love, P. J., and Head-Gordon, M. (2005). Simulated quantum computation of molecular energies. *Science*, 309(5741):1704–1707.

Aspuru-Guzik, A. and Walther, P. (2012). Photonic quantum simulators. *Nature physics*, 8(4):285.

Benedetti, M., Realpe-Gómez, J., Biswas, R., and Perdomo-Ortiz, A. (2016). Estimation of effective temperatures in quantum annealers for sampling applications: A case study with possible applications in deep learning. *Physical Review A*, 94(2):022308.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(P1):7–11.

Bernstein, D. J. and Lange, T. (2017). Post-quantum cryptography-dealing with the fallout of physics success. *IACR Cryptology ePrint Archive*, 2017:314.

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., and Lloyd, S. (2017). Quantum machine learning. *Nature*, 549(7671):195.

Blatt, R. and Roos, C. F. (2012). Quantum simulations with trapped ions. *Nature Physics*, 8(4):277.

Bloch, I., Dalibard, J., and Nascimbene, S. (2012). Quantum simulations with ultracold quantum gases. *Nature Physics*, 8(4):267.

Boghosian, B. M. and Taylor IV, W. (1998). Simulating quantum mechanics on a quantum computer. *Physica D: Nonlinear Phenomena*, 120(1-2):30–42.

Boixo, S., Isakov, S. V., Smelyanskiy, V. N., Babbush, R., Ding, N., Jiang, Z., Bremner, M. J., Martinis, J. M., and Neven, H. (2018). Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595.

Bouland, A., Fefferman, B., Nirkhe, C., and Vazirani, U. (2018). Quantum supremacy and the complexity of random circuit sampling. *arXiv preprint arXiv:1803.04402*.

Brandão, F., Kalev, A., Li, T., Lin, C. Y.-Y., Svore, K. M., and Wu, X. (2018). Quantum sdp solvers: Large speed-ups, optimality, and applications to quantum learning. *arXiv preprint arXiv:1710.02581*, v2.

Bravyi, S., Gosset, D., and König, R. (2018). Quantum advantage with shallow circuits. *Science*, 362(6412):308–311.

Browne, D. (2014). Quantum computation: Model versus machine. *Nature Physics*, 10(3):179.

Buhrman, H., Cleve, R., Massar, S., and De Wolf, R. (2010). Nonlocality and communication complexity. *Reviews of modern physics*, 82(1):665.

Cai, T., Kim, D., Wang, Y., Yuan, M., and Zhou, H. H. (2016). Optimal large-scale quantum state tomography with pauli measurements. *The Annals of Statistics*, 44(2):682–712.

Campbell, E. T., Terhal, B. M., and Vuillot, C. (2017). Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172.

Childs, A. M., Maslov, D., Nam, Y., Ross, N. J., and Su, Y. (2018). Toward the first quantum simulation with quantum speedup. *Proceedings of the National Academy of Sciences*, 115(38):9456–9461.

Chong, F. T., Franklin, D., and Martonosi, M. (2017). Programming languages and compiler design for realistic quantum hardware. *Nature*, 549(7671):180.

Ciliberto, C., Herbster, M., Ialongo, A. D., Pontil, M., Rocchetto, A., Severini, S., and Wossnig, L. (2018). Quantum machine learning: a classical perspective. *Proceedings Of The Royal Society A: Mathematical, Physical and Engineering Sciences*, 474(2209):20170551.

Cirac, J. I. and Zoller, P. (2012). Goals and opportunities in quantum simulation. *Nature Physics*, 8(4):264.

Degen, C. L., Reinhard, F., and Cappellaro, P. (2017). Quantum sensing. *Reviews of modern physics*, 89(3):035002.

Deutsch, D. (1985). Quantum theory, the church–turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400(1818):97–117.

DiCarlo, L., Chow, J., Gambetta, J., Bishop, L. S., Johnson, B., Schuster, D., Majer, J., Blais, A., Frunzio, L., and Girvin, S. (2009). Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature*, 460(7252):240.

DiVincenzo, D. P. (1995). Quantum computation. *Science*, 270(5234):255–261.

Dunjko, V. and Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, 81(7):074001.

Dunjko, V., Taylor, J. M., and Briegel, H. J. (2016). Quantum-enhanced machine learning. *Phys. Rev. Lett.*, 117:130501.

Farhi, E., Goldstone, J., Gutmann, S., and Sipser, M. (1998). Limit on the speed of quantum computation in determining parity. *Phys. Rev. Lett.*, 81:5442–5444.

Feynman, R. P. (1982). Simulating physics with computers. *International journal of theoretical*

physics, 21(6-7):467–488.

Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325.

Harrow, A. W. and Montanaro, A. (2017). Quantum computational supremacy. *Nature*, 549(7671):203.

Hayashi, M. (2006). *Quantum information*. Springer.

Holevo, A. S. (1998). The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273.

Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K. (2009). Quantum entanglement. *Reviews of modern physics*, 81(2):865.

Houck, A. A., Türeci, H. E., and Koch, J. (2012). On-chip quantum simulation with superconducting circuits. *Nature Physics*, 8(4):292.

Jané, E., Vidal, G., Dür, W., Zoller, P., and Cirac, J. I. (2002). Simulation of quantum dynamics with quantum optical systems. *arXiv preprint quant-ph/0207011*.

Jiang, Z., Smelyanskiy, V. N., Isakov, S. V., Boixo, S., Mazzola, G., Troyer, M., and Neven, H. (2017). Scaling analysis and instantons for thermally assisted tunneling and quantum Monte Carlo simulations. *Physical Review A*, 95(1):012322.

Johnson, M. W., Amin, M. H., Gildert, S., Lanting, T., Hamze, F., Dickson, N., Harris, R., Berkley, A. J., Johansson, J., and Bunyk, P. (2011). Quantum annealing with manufactured spins. *Nature*, 473(7346):194.

Jordan, S. P. (2005). Fast quantum algorithm for numerical gradient estimation. *Physical review letters*, 95(5):050501.

Kassal, I., Jordan, S. P., Love, P. J., Mohseni, M., and Aspuru-Guzik, A. (2008). Polynomial-time quantum algorithm for the simulation of chemical dynamics. *Proceedings of the National Academy of Sciences*, pages pnas–0808245105.

Kassal, I., Whitfield, J. D., Perdomo-Ortiz, A., Yung, M.-H., and Aspuru-Guzik, A. (2011). Simulating chemistry using quantum computers. *Annual review of physical chemistry*, 62:185–207.

Krenn, M., Malik, M., Scheidl, T., Ursin, R., and Zeilinger, A. (2017). Quantum communication with photons. *arXiv preprint arXiv:1701.00989*.

Kruse, I., Lange, K., Peise, J., Lücke, B., Pezze, L., Arlt, J., Ertmer, W., Lisdat, C., Santos, L., and Smerzi, A. (2016). Improvement of an atomic clock using squeezed vacuum. *Physical review letters*, 117(14):143004.

Lanyon, B. P., Whitfield, J. D., Gillett, G. G., Goggin, M. E., Almeida, M. P., Kassal, I., Biamonte, J. D., Mohseni, M., Powell, B. J., and Barbieri, M. (2010). Towards quantum chemistry on a quantum computer. *Nature chemistry*, 2(2):106.

Lloyd, S. (1996). Universal quantum simulators. *Science*, pages 1073–1078.

Lloyd, S., Mohseni, M., and Rebentrost, P. (2014). Quantum principal component analysis. *Nature Physics*, 10(9):631.

Lund, A., Bremner, M. J., and Ralph, T. (2017). Quantum sampling problems, bosonsampling and quantum supremacy. *npj Quantum Information*, 3(1):15.

Malley, J. D. and Hornstein, J. (1993). Quantum statistical inference. *Statist. Sci.*, 8(4):433–457.

Mariantoni, M., Wang, H., Yamamoto, T., Neeley, M., Bialczak, R. C., Chen, Y., Lenander, M., Lucero, E., O'Connell, A. D., and Sank, D. (2011). Implementing the quantum von neumann architecture with superconducting circuits. *Science*, page 1208517.

Markov, I. L., Fatima, A., Isakov, S. V., and Boixo, S. (2018). Quantum supremacy is both closer and farther than it appears. *arXiv preprint arXiv:1807.10749*.

McGeoch, C. C. (2014). Adiabatic quantum computation and quantum annealing: Theory and practice. *Synthesis Lectures on Quantum Computing*, 5(2):1–93.

Mohseni, M., Read, P., Neven, H., Boixo, S., Denchev, V., Babbush, R., Fowler, A., Smelyanskiy, V., and Martinis, J. (2017). Commercialize quantum technologies in five years. *Nature News*, 543(7644):171.

Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, 2:15023.

Neill, C., Roushan, P., Kechedzhi, K., Boixo, S., Isakov, S. V., Smelyanskiy, V., Megrant, A., Chiaro, B., Dunsworth, A., and Arya, K. (2018). A blueprint for demonstrating quantum supremacy with superconducting qubits. *Science*, 360(6385):195–199.

Nielsen, M. A. and Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge Univ. Press.

O'Gorman, B., Babbush, R., Perdomo-Ortiz, A., Aspuru-Guzik, A., and Smelyanskiy, V. (2015).

Bayesian network structure learning using quantum annealing. *The European Physical Journal Special Topics*, 224(1):163–188.

Paesani, S., Gentile, A. A., Santagati, R., Wang, J., Wiebe, N., Tew, D. P., O'Brien, J. L., and Thompson, M. G. (2017). Experimental bayesian quantum phase estimation on a silicon photonic chip. *Physical review letters*, 118(10):100503.

Pezzè, L., Smerzi, A., Oberthaler, M. K., Schmied, R., and Treutlein, P. (2016). Non-classical states of atomic ensembles: fundamentals and applications in quantum metrology. *arXiv preprint arXiv:1609.01609*, v1.

Rebentrost, P., Mohseni, M., and Lloyd, S. (2014). Quantum support vector machine for big data classification. *Phys. Rev. Lett.*, 113:130503.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Rønnow, T. F., Wang, Z., Job, J., Boixo, S., Isakov, S. V., Wecker, D., Martinis, J. M., Lidar, D. A., and Troyer, M. (2014). Defining and detecting quantum speedup. *Science*, 345(6195):420–424.

Sakurai, J. and Napolitano, J. (2017). Modern quantum mechanics. *Modern Quantum Mechanics, by JJ Sakurai, Jim Napolitano, Cambridge, UK: Cambridge University Press, 2017*.

Salakhutdinov, R. and Hinton, G. (2009). Deep boltzmann machines. In *Artificial intelligence and statistics*, pages 448–455.

Sangouard, N., Simon, C., De Riedmatten, H., and Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33.

Sayrin, C., Dotsenko, I., Zhou, X., Peaudecerf, B., Rybarczyk, T., Gleyzes, S., Rouchon, P., Mirrahimi, M., Amini, H., and Brune, M. (2011). Real-time quantum feedback prepares and stabilizes photon number states. *Nature*, 477(7362):73.

Schumacher, B. (1995). Quantum coding. *Physical Review A*, 51(4):2738.

Schumacher, B. and Westmoreland, M. D. (1997). Sending classical information via noisy quantum channels. *Physical Review A*, 56(1):131.

Shankar, R. (2012). *Principles of quantum mechanics*. Springer Science & Business Media.

Shenvi, N., Kempe, J., and Whaley, K. B. (2003). Quantum random-walk search algorithm. *Physical Review A*, 67(5):052307.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE.

Svore, K. M., Hastings, M. B., and Freedman, M. (2014). Faster phase estimation. *Quantum Information & Computation*, 14:306–328.

Trotter, H. F. (1959). On the product of semi-groups of operators. *Proceedings of the American Mathematical Society*, 10(4):545–551.

Wang, Y. (2011). Quantum Monte Carlo simulation. *The Annals of Applied Statistics*, 5(2A):669–683.

Wang, Y. (2012). Quantum computation and quantum information. *Statistical Science*, 27(3):373–394.

Wang, Y. (2013). Asymptotic equivalence of quantum state tomography and noisy matrix completion. *The Annals of Statistics*, 41(5):2462–2504.

Wang, Y., Wu, S., and Zou, J. (2016). Quantum annealing with Markov chain Monte Carlo simulations and D-Wave quantum computers. *Statistical Science*, 31(3):362–398.

Wang, Y. and Xu, C. (2015). Density matrix estimation in quantum homodyne tomography. *Statistica Sinica*, pages 953–973.

Wiebe, N. and Granade, C. (2016). Efficient bayesian phase estimation. *Phys. Rev. Lett.*, 117:010503.

Wiebe, N., Granade, C., Ferrie, C., and Cory, D. G. (2014a). Hamiltonian learning and certification using quantum resources. *Physical review letters*, 112(19):190501.

Wiebe, N., Kapoor, A., and Svore, K. M. (2014b). Quantum deep learning. *arXiv:1412.3489*.

Wiebe, N., Kapoor, A., and Svore, K. M. (2015). Quantum nearest-neighbor algorithms for machine learning. *Quantum Information and Computation*, 15(3-4):318–358.

Wittek, P. (2014). *Quantum machine learning: what quantum computing means to data mining*. Academic Press.

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., and Dai, H. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144.