HDSR
HARVARD DATA SCIENCE REVIEW

Volume 4 Issue 1
DOI: /10.1162/99608f92.ef5d8928
ISSN: 2644-2353

When Quantum Computation Meets Data Science: Making Data Science Quantum

Yazhen Wang*
University of Wisconsin-Madison

Abstract. Quantum computation and quantum information have attracted considerable attention on multiple frontiers of scientific fields ranging from physics to chemistry and engineering, as well as from computer science to mathematics and statistics. Data science combines statistical methods, computational algorithms, and domain science information to extract knowledge and insights from big data, and to solve complex real-world problems. While it is well-known that quantum computation has the potential to revolutionize data science, much less has been said about the potential of data science to advance quantum computation. Yet because the stochasticity of quantum physics renders quantum computation random, data science can play an important role in the development of quantum computation and quantum information. This article gives an overview of quantum computation and promotes interplay between quantum science and data science. Overall, it advocates for the development of quantum data science for advancing quantum computation and quantum information.

Keywords: quantum computation, quantum information, data science, statistics, quantum speedup, quantum supremacy

1. Introduction

The interface of statistics and computation is a signature issue in data science, which characteristically uses statistics, computation, and domain science knowledge to extract information and insights from data for the solving of big data problems. The discovery of solutions of complicated real problems with big data requires the development of statistical methods to analyze the data and computational algorithms to implement data analysis procedures. The statistical analysis is often computationally challenging. For example, statistical approaches that are mathematically optimal may not be computationally tractable, and data analysis methods that are computationally efficient may not be statistically optimal. Thus, sound statistics and tractable computation constitute fundamental but often competing pillars of data science, and a tradeoff is needed to balance statistical efficiency and computation efficiency.

As data continuously grow in scale and complexity, and models used, particularly in deep learning, become more elaborate, computational techniques from chips to software to systems involved

*yzwang@stat.wisc.edu

in data science become increasingly hard to develop. At the very same time, Moore's Law—the decades-old rule of thumb in semiconductor technology stating that chips double in power every twelve to eighteen months—has lost ground. Indeed, the current computing demand in machine learning pushes the limits of computer technology; as such, the interplay between data science (machine learning) and computation (computer hardware) becomes more important than ever. For example, more powerful hardware can help in developing data science methods to scale to the enormous size of big data, and data science may affect computer chip fabrication technology for designing sophisticated chips for carrying out machine learning tasks.

Conventional high-performance computer systems have struggled to meet the demand posed by machine learning and AI research, and companies like Google, Amazon, and Facebook have joined Intel and Nvidia to develop machine learning chips. Machine learning itself can be a boon for the design of these chips, as it utilizes the features of parallelization and the repetitive nature of algebraic computation to boost their performance and efficiency, rendering them superior to conventional chips for accomplishing machine learning tasks. Hardware capabilities and software tools both motivate and limit computational and inferential missions. Thus, data scientists are currently poised to launch new explorations at the interface of computing and data-driven science. One paramount example of such an endeavor entails quantum computation, which harnesses quantum physics for the purpose of computation in such a way as to hold significant promise for the development of data science. And, in turn, data science, especially in the form of machine learning, can play an important role in the development of quantum computation and quantum information.

This article provides an overview of quantum computation and its potential interplay with data science. The selected topics are geared toward data scientists, with the aim of advocating for the development of quantum data science. The rest of the article proceeds as follows. Section 2 introduces basic quantum computation concepts, such as quantum bits and quantum gates, along with their quantum properties, such as quantum superposition and quantum computational spaces of exponential size. Section 3 presents quantum entanglement and its applications in quantum computation and quantum information. Section 4 describes quantum factoring algorithms and their impact on cryptography. Section 5 illustrates computational advantages of quantum computers over classical computers. Section 6 features a recent breakthrough in quantum complexity theory and its consequences within and beyond quantum computation. Section 7 explores the interface of quantum science and data science and advocates quantum data science for advancing both quantum computation and data science developments. Quantum computing scientists who would like to understand the role of statistics and data science in quantum computation may jump from Section 1 to Section 5.2.2 and Section 7. Readers who would like to quickly learn something about quantum computational complexity and its impact on physics and pure mathematics may directly go from Sections 2 and 3 to Sections 5.1 and 6.

2. Quantum Computer Concepts

2.1. **Classical Bits and Quantum Bits.** In computation, bits must be materialized by some physical systems, and the information encoded in the bits is stored in the system states. For example, ancient counting frames use beads and their positions to represent numbers, such as the Chinese abacus displayed in the top panel of Figure 1. Old-fashioned mechanical computers utilize gears and their positions to symbolize numbers. Modern computers employ electric systems to materialize bits, and the two values, 0 and 1, in a bit can be realized by an electric switch with

Figure 1. An illustration of a Chinese abacus (top), a Mac laptop computer (middle), and a quantum computer cartoon (bottom). The Chinese abacus generally has two decks divided by a beam, with five beads on each rod in the bottom deck and two beads each in the top deck. The beads are counted by moving them toward the beam, with each top bead for 5 and each bottom bead for 1.

current 'on' and 'off' representing 0 and 1, respectively. Based on these computing devices, it is easy to see that the physical systems must have obviously identifiable states to encode information, such as the binary states for modern computers to represent the bit 0 in a state and the bit 1 in another state.

Various quantum systems exist that possess the required physical states to realize bits and encode information. For example, the two states in the atom model are the so-called 'ground' and 'excited'

states of its electron that can be used to encode the bit values 0 and 1, respectively. Insofar as both classical and quantum systems are discussed here, it may be useful to introduce notations for distinguishing their physical states and associated bits. Thus, if a quantum system is used to represent the bit value 0 through one of its quantum states, I refer to the bit in the quantum state as a quantum bit, or a qubit for short, and denote it by $|0\rangle$; similarly I write $|1\rangle$ for a quantum state representing the bit value 1. As Figure 1 displays a Chinese abacus, a classical computer (Mac laptop), and a quantum computer (cartoon), the word 'computer' is used in both classical and quantum computing machines. Yet, perhaps surprisingly, a classical computer differs from a quantum computer to a great extent than does an abacus from a Mac laptop.

2.2. **Quantum Superposition.** An intrinsic difference exists between bit representations by classical and quantum systems. All classical physical systems prevent the simultaneous occurrence of their states. For example, one classical state representing the bit 0 must mutually exclude the simultaneous presence of the other state representing the bit 1. A quantum system, however, allows for the simultaneous occurrence of different states. For example, consider the atom model where two quantum states, the 'ground' and 'excited' states of the electron, represent $|0\rangle$ and $|1\rangle$, respectively. Giving the shining of light upon the atom with suitable energy and for a proper amount of time, one can transfer the electron between the $|0\rangle$ and $|1\rangle$ states and even move it from one of $|0\rangle$ and $|1\rangle$ states into a state 'halfway' between $|0\rangle$ and $|1\rangle$ states. The 'halfway' state is a so-called superposition of the $|0\rangle$ and $|1\rangle$ that allows for a blend of the two states simultaneously. The superposition phenomenon, a characteristic of quantum physics, does not exist in classical physics. Unlike classical bits with mutually exclusive states, qubits in superposition states can be viewed as simultaneous occurrence of zero and one at the same time.

To be specific, while a classical bit can be either 0 or 1 but not both, a qubit can be a superposition of both $|0\rangle$ and $|1\rangle$ in a form of

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|0\rangle, \tag{2.1}$$

where α_0 and α_1 are complex numbers that meet the constraint $|\alpha_0|^2 + |\alpha_1|^2 = 1$. α_0 and α_1 are called amplitudes of $|\psi\rangle$.

It is easy to find the state of a classical bit, which is either 0 or 1. But a qubit can not be examined to determine its state. The theory of quantum physics allows for the probabilistic description of random behaviors in quantum physical systems. The qubit $|\psi\rangle$ can be measured to obtain measurement results. Each measurement outcome is random and takes a value being either 0 or 1; the probability of obtaining the outcome 0 is equal to $|\alpha_0|^2$, with probability $|\alpha_1|^2$ for the outcome 1. Thus, $|\alpha_0|^2$ and $|\alpha_1|^2$ can be accurately estimated by statistical results based on enough measurement outcomes of quantum systems identically prepared in the state $|\psi\rangle$. Notably, performing a measurement on the qubit alters its state.

The described probabilistic aspect of the quantum theory indicates that for any qubit, the multiplication of a global phase factor bears no observable effect, where a global factor refers to e^{ia} for some real number a and the imaginary unit $i = \sqrt{-1}$. Thus, I may ignore global phase factors in qubit expressions. For qubit $|\psi\rangle$ given by (2.1), due to the unit norm constraint on α_0 and α_1 and ignoring global phase factors, I can facilitate the representation of the qubit $|\psi\rangle$ by the so-called Bloch sphere shown in Figure 2, where each qubit state corresponds to a point on the sphere specified by two angles $\theta \in [0, \pi]$ and $\vartheta \in [0, 2\pi)$, with the north and south poles corresponding to $|0\rangle$ and $|1\rangle$, respectively. In stark contrast to a classical bit (with its two states, 0 and 1, corresponding

to two points on the Bloch sphere: the north and south poles), a qubit possesses states that occupy the whole Bloch sphere.

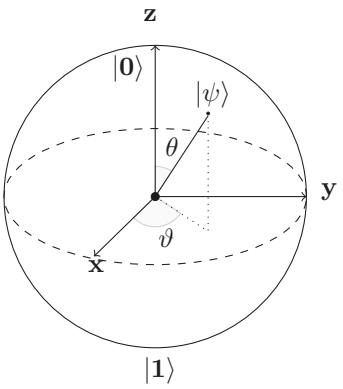

Figure 2. Qubit representation by the Bloch sphere.

To give an animated illustration of a quantum superposition in everyday objects, a thought experiment known as Schrödinger's cat presents a hypothetical cat that may be simultaneously both alive and dead. The scenario often refers to the phrase 'cat state' in quantum computation, and its corresponding qubit $|\psi_{cat}\rangle$ may be vividly exhibited as follows:

$$|\psi_{cat}\rangle = \frac{1}{\sqrt{2}}\Big|\text{  }\Big\rangle + \frac{1}{\sqrt{2}}\Big|\text{  }\Big\rangle. \tag{2.2}$$

It is easy to see from the representation equations (2.1) and (2.2) that the states $|0\rangle$ and $|1\rangle$ correspond to the alive and dead states, respectively. Although the cat state $|\psi_{cat}\rangle$ can be both alive and dead, what can be observed is a measurement outcome—either a living cat or a dead cat, resulting from measuring $|\psi_{cat}\rangle$.

2.3. **Multiple Qubits and Computational Spaces of Exponential Size.** The qubit expression (2.1) and its Bloch sphere representation in Figure 2 indicate that the states of a qubit are unit vectors in a two-dimensional complex vector space, and that the states $|0\rangle$ and $|1\rangle$ constitute an orthonormal basis for the complex vector space; they are thus called computational basis states. A single qubit is the simplest quantum system. I describe multiple qubits as follows. For a system of b qubits, its states are unit vectors in a 2^b-dimensional complex vector space. The computational basis states take the form of $|x_1x_2\cdots x_b\rangle$, $x_j = 0$ or 1, $j = 1,\ldots,b$, and any superposition state is a linear combination of the 2^b computational basis states whose complex coefficients are called amplitudes and satisfy the constraint of unit norm. Specifically, a b-qubit state $|\psi\rangle$ may take a superposition state with the following form:

$$|\psi\rangle = \sum_{x_1,x_2,\ldots,x_b=0,1} \alpha_{x_1x_2\cdots x_b}|x_1x_2\cdots x_b\rangle, \quad \sum_{x_1,x_2,\ldots,x_b=0,1} |\alpha_{x_1x_2\cdots x_b}|^2 = 1. \tag{2.3}$$

For example, a two-qubit system is described by a four-dimensional complex vector space with four computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, and its superposition state $|\psi\rangle$ is specified by the corresponding four amplitudes $\alpha_{00}, \alpha_{01}, \alpha_{10}$, and α_{11} as follows:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{2.4}$$

where the amplitudes $\alpha_{00}, \alpha_{01}, \alpha_{10}$, and α_{11} satisfy the constraint

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1. \tag{2.5}$$

As in the single-qubit case, measuring the two-qubit system in the state $|\psi\rangle$ given by (2.4) yields measurement outcome $\mathbf{x}$ as one of 00, 01, 10, and 11, with the corresponding probability $|\alpha_{\mathbf{x}}|^2$. As the lively Schrödinger's cat described in the single-qubit case, I may display the two-qubit 'cat state' as follows:

$$|\psi_{\text{2-cats}}\rangle = \frac{1}{2}\{|\,\rangle + |\,\rangle + |\,\rangle + |\,\rangle\}.$$

When performing a measurement on the two-qubit system in the cat state $|\psi_{\text{2-cats}}\rangle$, I can observe only one of the four possible outcomes—that is, two living cats, two dead cats, the first living cat and the second dead cat, or the first dead cat and the second living cat. Moreover, I may perform a measurement just on the first cat of the two-qubit system in the state $|\psi_{\text{2-cats}}\rangle$ and obtain either the measurement outcome, 'the first living cat,' with probability $(1/2)^2 + (1/2)^2 = 1/2$ or the measurement outcome, 'the first dead cat,' with probability $(1/2)^2 + (1/2)^2 = 1/2$. Since quantum measuring changes quantum states, after the quantum measurement performed on the two-qubit system in the cat state $|\psi_{\text{2-cats}}\rangle$, its state will be changed. Depending on the measurement outcome obtained for the first cat, being either alive or dead, the two-qubit cat state after the measurement will be, respectively, in either state

$$\frac{1}{\sqrt{2}}\{|\,\rangle + |\,\rangle\}$$

or state

$$\frac{1}{\sqrt{2}}\{|\,\rangle + |\,\rangle\}.$$

A b-qubit quantum system is described by its computational space—namely, a 2^b-dimensional complex vector space—and each superposition state is a unit vector in the computational space and specified by 2^b amplitudes. For example, it would require 16 petabytes of memory for a classical computer with double-precision values to store the state of 50 qubits. Since 2^b increases exponentially in b, the quantum exponential complexity is obviously demonstrated by the exponential growth of the dimensionality of the computational space and the number of amplitudes required to describe the qubit system and specify superposition states. Quantum superposition and exponential complexity are among special properties of quantum physics that can be utilized in quantum computation and quantum information.

2.4. **Quantum Gates and Quantum Circuits.** Classical logic gates transform classical bits from one form to another. Quantum gates are the quantum analog of classical logic gates that operate on qubits. According to quantum physics, quantum gates are unitary transformations and represented by unitary matrices. Quantum circuits contain quantum gates with associated connections to perform quantum computation and to manipulate quantum information. As in the classical case, considered as a model of computation, a quantum circuit is specified by the contained gates and the produced results.

As the classical NOT gate maps 1 to 0 and 0 to 1, the quantum NOT gate changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. It transforms $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ into $\alpha_1|0\rangle + \alpha_0|1\rangle$. I may use vectors and matrices to represent qubits and quantum gates. Denote by $\mathbb{C}^2$ the vector space consisting of all pairs of complex numbers. I identify $|0\rangle$ and $|1\rangle$ with vectors $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}1\\0\end{bmatrix}$ in $\mathbb{C}^2$, respectively. Then $|\psi\rangle$ is represented by vector $\begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix}$ in $\mathbb{C}^2$, and a quantum gate acting on $|\psi\rangle$ corresponds to a unitary matrix on $\mathbb{C}^2$. For example, the quantum NOT gate can be represented by a matrix $\boldsymbol{\sigma}_x$ that satisfies

$$\boldsymbol{\sigma}_x \begin{bmatrix}\alpha_0\\\alpha_1\end{bmatrix} = \begin{bmatrix}\alpha_1\\\alpha_0\end{bmatrix},$$

where

$$\boldsymbol{\sigma}_x = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \quad \boldsymbol{\sigma}_y = \begin{bmatrix}0 & -\sqrt{-1}\\\sqrt{-1} & 0\end{bmatrix}, \quad \boldsymbol{\sigma}_z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \tag{2.6}$$

$\boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y$ and $\boldsymbol{\sigma}_z$ are called Pauli-x, y and z matrices, respectively, and their associated quantum gates are called Pauli-x, y and z gates. Note that the quantum NOT gate is the same as the Pauli-x gate.

All classical gates can be realized by quantum gates, but the converse is not true. Consider the 'Square-Root-of-NOT' gate, which is defined to be the gate, denoted by $\sqrt{NOT}$, such that two $\sqrt{NOT}$ gates, connected back to back, perform the NOT operation. This is impossible classically, yet there is a quantum $\sqrt{NOT}$ gate, because the square root of the Pauli-x matrix exists in the complex domain but not in the real domain. In fact, the square root of $\boldsymbol{\sigma}_x$ in the complex domain is given by

$$\sqrt{\boldsymbol{\sigma}_x} = \begin{bmatrix}\frac{1}{2} + \frac{\sqrt{-1}}{2} & \frac{1}{2} - \frac{\sqrt{-1}}{2}\\\frac{1}{2} - \frac{\sqrt{-1}}{2} & \frac{1}{2} + \frac{\sqrt{-1}}{2}\end{bmatrix}.$$

See Nielsen and Chuang, 2010, Wang, 2012, Wang and Song, 2020, Wilde, 2017 and Williams, 2011 for more details.

3. Quantum Entanglement and Its Applications

3.1. **Entanglement.** Quantum entanglement refers to a mind-bending phenomenon that two separated particles A and B behave like twins that are connected by an invisible wave that allows each to share each other's properties. It plays a crucial role in quantum computation and quantum information. Consider an entangled two-qubit system in a state

$$|\phi_{AB}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{3.1}$$

All information content of the two entangled qubits is fully entailed in the correlation between the two individual qubits, while each qubit on its own does not convey essential information of the entangled qubits. For example, measuring each of the two qubits yields an outcome being

either 0 or 1 with probability 50% and 50%, respectively. The completely random outcome allows anyone to gain no essential information about the entangled qubit system. Recall that performing measurements changes quantum states. As a consequence, an intriguing feature of the entangled qubits shows that measuring one qubit immediately destroys the entanglement and instantaneously casts the other qubit into a perfectly correlated state. For example, as described in Section 2.3, if one measures the first qubit to obtain a completely random measurement outcome, being 0 or 1, then the state of the two entangled qubits changes to $|00\rangle$ or $|11\rangle$, respectively. Hence, for the first measurement outcome 0 or 1, the second qubit must be in the state $|0\rangle$ or $|1\rangle$, which produces the same measurement outcome being 0 or 1, respectively. This indicates a perfect correlation between the measurements of the two qubits, which refers to the perfect correlation phenomenon in entanglement experiments.

3.2. **Quantum Teleportation.** Quantum teleportation refers to a process in which the state of a qubit is transferred to another distant qubit without going through the intervening space between them. The phenomenon is described by a three-step protocol. First, a special pair of entangled qubits (denoted by AB) were prepared in the state given by (3.1); Alice (the sender) took the first qubit (called qubit A) of the two shared qubits, and Bob (the receiver) took the second qubit (called qubit B) when they moved apart. Second, Alice was provided with a third qubit with unknown state $|\psi\rangle$, and her job was to teleport the unknown state to Bob. Third, Alice performed a measurement on her original qubit and the third qubit to obtain a measurement result a_1a_2 being 00, 01, 10, or 11; she informed Bob by a classical communication of her measurement outcome a_1a_2 so that Bob applied the transformation $\boldsymbol{\sigma}_z^{a_1}\boldsymbol{\sigma}_x^{a_2}$ to recover the state $|\psi\rangle$, where $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$ are the Pauli matrices defined in (2.6). Vital ingredients in the quantum teleportation protocol are the special entanglement, the quantum measurement, and its corresponding transformation. The teleportation protocol functions only if Alice informed Bob of her measurement outcome by classical communication so that Bob could apply the corresponding transformation to recover the unknown state. Because the particle pair was in the entangled state $|\psi_{AB}\rangle$, Alice's measurement destroyed the entanglement and changed the state of her qubit, and at the same time it cast Bob's qubit into a new state. The new state was related to the unknown state $|\psi\rangle$ where it could be used by Bob to recover $|\psi\rangle$ by utilizing Alice's measurement outcome a_1a_2 to apply the transformation $\boldsymbol{\sigma}_z^{a_1}\boldsymbol{\sigma}_x^{a_2}$, $a_1, a_2 = 0, 1$—that is, for the unknown state recovery, Bob applied nothing, $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_z$, or $\boldsymbol{\sigma}_x$ and then $\boldsymbol{\sigma}_z$ depending on a_1a_2 being 00, 01, 10, or 11, respectively. After the three steps, the unknown state $|\psi\rangle$ was transported from Alice to Bob. Note that the information transferred from Alice to Bob by quantum teleportation is the unknown state of the qubit $|\psi\rangle$, and that quantum teleportation does not move any underlying physical particles that realize the qubits. Moreover, the requirement on classical communication between Alice and Bob limits the speed of quantum teleportation to the speed of the classical communication channel and thus, quantum teleportation does not entail any faster-than-light communication.

3.3. **Game Show: The Magic-Square Game.** As a Bayesian game, the magic-square game features a referee called Verifier and two players, Alice and Bob. The game requires the players to fill a 3×3 table as follows: Verifier randomly selects a row and a column of the table, and Alice and Bob are asked to fill the selected row and column with plus and minus ones, respectively. The players are subject to the following row and column parity requirements: Alice must fill in her row such that the row product is equal to $+1$ (an even number of minus ones in that row); and Bob must fill in his column such that the column product is equal to -1 (an odd number of minus ones

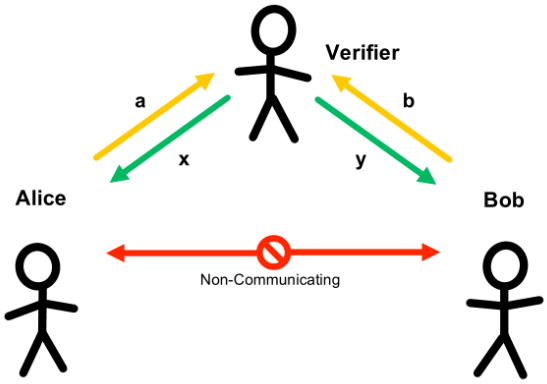

Figure 3. An illustration of the classical magic-square game.

Table 1. Classical variables to fill the nine cells of the 3×3 table.

X_1	X_2	X_3
X_4	X_5	X_6
X_7	X_8	X_9

in that column). Alice and Bob win the game if they place the same number in the cell shared by their row and column, and lose the game otherwise.

Alice and Bob are separated at the beginning of the game, and subsequently not allowed to communicate. Because of the random row and column selection by the referee, before the game starts, Alice does not know which row of the table she will be required to fill in; likewise Bob does not know which column he will be required to fill in. More importantly, during the game, Alice does not know which column Bob has been asked to fill in, and Bob does not know which row Alice has been asked to fill in. Without any communication, the players do not know the numbers placed by each other before the game is finished.

3.3.1. *Classical Strategies.* Denote by x and y the row and column that Verifier has selected for Alice and Bob to fill, respectively, with a and b the numbers that Alice and Bob have placed in the cell shared by their row and column, as shown in Figure 3. Alice and Bob win the game if $a = b$.

It can be shown that this classical formulation of the magic-square game allows the players to win the game with the maximum probability 8/9, regardless of strategy. That is, there is no strategy that Alice and Bob can find, such as meeting and exchanging information before the game begins, that would allow them for winning the game with a probability greater than 8/9. Indeed, denote by X_j, $j = 1, \ldots, 9$, the nine variables taking values ± 1 to fill the table as shown in Table 1. Then

Table 2. A classical optimal winning strategy to fill the 3×3 table.

$+1$	$+1$	$+1$
$+1$	-1	-1
-1	$+1$	?

they must satisfy the parity constraints

$$X_1X_2X_3 = +1, \quad X_4X_5X_6 = +1, \quad X_7X_8X_9 = +1, \tag{3.2}$$

$$X_1X_4X_7 = -1, \quad X_2X_5X_8 = -1, \quad X_3X_6X_9 = -1. \tag{3.3}$$

Equations (3.2) and (3.3) immediately render that the positiveness and negativeness on the respective row and column products are self-contradictory, because the product of all nine variables must be equal to $+1$ or -1 in order to satisfy the three equations in (3.2) or (3.3), respectively. Thus, there exists no perfectly consistent table. The game can be won only with a probability at most 8/9. In fact, a winning strategy is described in Table 2 as follows: Alice and Bob always take $X_1 = X_2 = X_3 = X_4 = X_8 = +1$ and $X_5 = X_6 = X_7 = -1$, and for the last cell with X_9, Alice selects -1, and Bob chooses $+1$. With the row and column are selected at random, Alice and Bob use the prescribed values accordingly to fill in the selected row and column and thus win the game 8/9 of the time—that is, they win all the time except in the event that they are asked to fill the third row and column.

3.3.2. *Quantum Strategies.* Quantum strategies exist that would allow Alice and Bob to win the magic-square game 100% of the time without any communication once the game has begun. In the quantum formulation displayed in Figure 4, Alice and Bob possess two pairs of particles, with one particle of each pair held by Alice and the other by Bob. Before the start of the game the particles are prepared by Charlie in entangled states $|\phi_{AB}\rangle|\phi_{AB}\rangle$, where $|\phi_{AB}\rangle$ is the state defined in (3.1).

While classically it is impossible to construct a perfectly consistent table for meeting all row and column parity constraints, as shown in Table 2, quantumly it is possible to do so with Hermitian matrices. As shown in Section 2, vectors and matrices are used to describe quantum physics and quantum computation. Here a quantum measurement is characterized through a Hermitian matrix (which is called an observable) with its eigenvalues for the possible measurement outcome. Observables as tensor products of the Pauli matrices and the 2-by-2 identity matrix are placed in Table 3 to satisfy the row and column parity requirements for the game. Because of the special properties of the Pauli matrices, it is straightforward to check that each row contains a mutually commuting set of three observables with eigenvalues $+1$ and -1 and its row product being the identity matrix $\mathbf{I}$, and each column consists of a mutually commuting set of three observables with eigenvalues $+1$ and -1 and its column product equal to $-\mathbf{I}$.

Alice and Bob proceed to play the game as follows. Once a row and a column are selected for Alice and Bob to fill, they use the observables in the selected row and column of Table 3 to perform

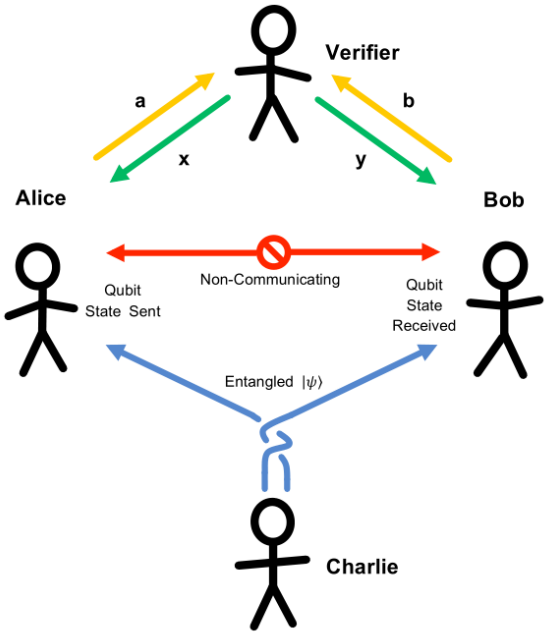

Figure 4. An illustration of the quantum magic-square game.

measurements on their particles, and place the resulted measurement outcomes in the corresponding cells of the selected row and column.

The quantum setup guarantees that the strategy works. Indeed, (i) all three observables in a given row or column of Table 3 commute and thus can be measured simultaneously to obtain random measurement outcomes. (ii) Their eigenvalues ± 1 and their row and column products $\pm\mathbf{I}$ indicate that the three measurement results of each player are ± 1 and always multiply to $+1$ for Alice and -1 for Bob. (iii) The entangled states of their particles ensure that, for the cell shared by Alice and Bob, their measurement results will always be the same due to the fact of quantum entanglement. This means that once one player performs a measurement on his/her particles with the common observable in the corresponding shared cell, the particle state of the other player will be immediately cast into a definite state to produce the same measurement outcome. (iv) Alice and Bob are separated at the start of the game and, after that point, no communication between them takes place.

Strikingly, whereas in the classical case Alice and Bob can win the magic-square game with a probability of at most 8/9, in the quantum case they can win the game with a probability of 1.

3.4. **Tests and Nonlocal Games.** Like the magic square game, another famous game called the CHSH game has a classical winning probability of at most 0.75 and a quantum winning probability of $\cos^2(\pi/8) \approx 0.854$. The CHSH game arising in physics was originally formulated not as a game involving Alice and Bob, but rather as an experiment involving two spatially separated devices. These experiments, which are named after John Bell and hence, known as Bell tests, are used to test classical physics against quantum physics. The tests are developed through Bell's and Tsirelson's inequalities to check classical correlations versus quantum correlations, where a version of the Bell inequality may be described as follows: For four random variables X_1, X_2, X_3, and X_4

Table 3. A quantum optimal winning strategy to fill the 3×3 table. $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_y$ and $\boldsymbol{\sigma}_z$ are Pauli matrices defined in (2.6), and $\mathbf{I}$ is the identity matrix of size 2.

$+\mathbf{I} \otimes \boldsymbol{\sigma}_z$	$+\boldsymbol{\sigma}_z \otimes \mathbf{I}$	$+\boldsymbol{\sigma}_z \otimes \boldsymbol{\sigma}_z$
$+\boldsymbol{\sigma}_x \otimes \mathbf{I}$	$+\mathbf{I} \otimes \boldsymbol{\sigma}_x$	$+\boldsymbol{\sigma}_x \otimes \boldsymbol{\sigma}_x$
$-\boldsymbol{\sigma}_x \otimes \boldsymbol{\sigma}_z$	$-\boldsymbol{\sigma}_z \otimes \boldsymbol{\sigma}_x$	$+\boldsymbol{\sigma}_y \otimes \boldsymbol{\sigma}_y$

taking values ± 1, one has

$$E(X_1X_3) + E(X_2X_3) + E(X_2X_4) - E(X_1X_4) \leq 2,$$

while as its quantum counterpart, Tsirelson's inequality has upper bound $2\sqrt{2}$ instead of 2. The classical correlations may be described by local hidden variables, while the quantum correlations from entanglement may be stronger than the classical correlations and cannot be explained by any local hidden variables. Over the years, the Bell tests have provided overwhelming evidence to support the presence of quantum correlations (or nonlocal correlations) between separated systems, leading to the conclusion that nature behaves in line with quantum physics but not classical physics. Games like the magic square game and the CHSH game, which involve nonlocal correlations due to quantum entanglement, are called nonlocal games.

Quantum protocols based on nonlocal games have been developed, which are known as the so-called self-tests, to certify quantum systems, such as quantum computation machines and quantum communication devices, in a black-box scenario so that the focus is on what the machines and devices do without sophisticated models on how the work is accomplished. For example, it is important to certify that a product for cryptography is actually working properly without having

to comprehend exactly how it works. See Aravind, 2004, Gill, 2014, Gill, 2018, Nielsen and Chuang, 2010, Šupić and Bowles, 2019, Wang, 2012, and Wilde, 2017 for more details.

4. Quantum Factoring Algorithms and Cryptography

The factoring problem refers to the challenge of finding all prime factors of a given positive composite number. It is known to be very hard for classical computers, since the current best known classical algorithm needs computational operations of order $\exp(n^{1/3}log^{2/3}n)$ for factoring an n-bit composite number (Crandall and Pomerance, 2006). Kitaev, 1995, Shor, 1994, Shor, 1995, and Shor, 1999 developed quantum algorithms, including Shor's algorithm, that can accomplish the task of factoring an n-bit integer with operations of order $n^2 \log n \log\log n$. The quantum factoring algorithms offer theoretical evidence for the belief that quantum computers can be intrinsically more powerful than classical computers and present a credible challenge to the strong Church-Turing thesis, which asserts that any algorithmic process can be simulated efficiently by a probabilisitic Turing machine.

Cryptography enables private communications between two parties, the sender Alice and the receiver Bob, to share secret messages, while simultaneously making it extremely difficult for the third parties to 'eavesdrop' on the content of their communications. Its applications include online security systems, business transactions, and military communications. Public key cryptosystems rely on the complexity of hard computational problems; they work as follows. Bob produces a pair of keys, a public one and a private one, and makes his 'public key' available to everyone, including Alice, for encrypting messages and sending him the encrypted messages. The actual trick is that Bob possesses a specially devised encryption transformation to produce the key pair so that it is extremely difficult, albeit not impossible, to reverse the encryption transformation with only the available public key. When making the public key available to the general public, Bob keeps a matched secret key that allows for the simple inversion of the encryption transformation and decryption of the received messages.

The factoring problem plays an important role in cryptography. The complexity of the best classical factoring algorithm grows exponentially in correspondence with the size of the number being factored, and the quantum factoring algorithms are exponentially faster than the most efficient known classical factoring algorithm. Because of the exponential complexity, the factoring problem is usually considered to be an intractable problem for classical computers. Consider a public key cryptosystem called RSA, which is named after its creators Rivest, Shamir, and Adleman (Katz et al., 1996 and Rivest et al., 1978). The extremely difficult computational problem in the RSA case entails the factoring of large composite numbers, and the trick is the mathematical asymmetry of factoring, which means that while it is simple to find a composite number from its prime factors by simply multiplying the primes, the factoring problem as its reverse process is extremely difficult. RSA encryption selects large primes to design a secret key and uses their product, a very large composite number, to create a public key. Because the best known classical factoring algorithm has exponential complexity, and efforts to break the RSA system so far have resulted in failure, it is widely believed that the RSA system is secure against any classical computer-based attacks.

Due to the exponential speedup of the quantum algorithms over the classical algorithms in solving the factor problem, quantum computers can factor large composite numbers at a speed that is remarkably faster than that of classical computers. Consequently, an eavesdropper equipped with a quantum computer can easily break the RSA system. Moreover, there is a quantum approach

known as quantum cryptography or quantum key distribution that is secure against any quantum computer-based attacks. Its security is guaranteed by the quantum principle that observing or measuring an unknown quantum system will disturb the system. As long as an eavesdropper taps into a quantum communication channel, the eavesdropping disturbs the quantum communication channel, and the disturbance makes eavesdropping noticeable so that a secure communication can be ensured. See Nielsen and Chuang, 2010, Wang, 2012, Wang and Song, 2020 and Wilde, 2017 for more details.

5. Quantum Speedup and Quantum Supremacy

5.1. **Grover's algorithm.** It has been rigorously proved that quantum algorithms may provide for substantial speedups over classical algorithms. As described in Section 4, the quantum factoring algorithms offer an exponential speedup over the best known classical factoring algorithm. Consider another problem—that of searching a database. For example, the task is to search for the name matching with a given phone number in a telephone directory or the shortest route passing through the locations in a city that one would like to visit. Suppose that the database has N entries, such as N names in the telephone directory and N possible routes to pass through all the locations. Classical search algorithms generally need to run computational operations of order N on classical computers. A simple classical algorithm is to search exhaustively all names to get a name corresponding to the given phone number or to inspect all possible routes to obtain the shortest route among all routes. Grover's algorithm is a quantum search algorithm that requires computational operations of order $\sqrt{N}$ to find a solution to the search problem. Moreover, the computational complexity results of orders N and $\sqrt{N}$ are optimal in the sense that any quantum algorithm to solve the search problem must require operations of at least order $\sqrt{N}$, while classical algorithms can not solve the search problem with a less than N order of operations. Thus, Grover's algorithm is asymptotically optimal, and offers a quadratic speedup over the best classical search algorithm. The quadratic speedup may not be as impressive as other quantum algorithms, such as Shor's factoring algorithm, which provide exponential speedup over its classical counterpart, yet it can be very significant for large N. Furthermore, Grover's search algorithm can be considered as a special case of a large class of quantum algorithms based on quantum walk and quantum Markov chain that allow for quantum speedups over their classical counterparts. See Childs et al., 2003, Childs, 2010, Grover, 1996, Grover, 1997, Tulsi, 2008 and Szegedy, 2004 for more details.

5.2. **Quantum Computational Supremacy.** Various physical systems are currently being investigated to build quantum computers, but many technological hurdles exist that must be surmounted to allow for the construction of large-scale quantum computers. In fact, there are a wide spectrum of views, ranging from those suggestive of hype to those informed by skepticism, regarding quantum computation. Quantum skeptics believe that it is not physically possible to build scalable quantum computers to realize the theoretical advantage of quantum computation over classical computation. A very large number of high-quality qubits are required for a quantum computer to run faster quantum algorithms, such as Grover's search algorithm and Shor's factoring algorithm, for demonstrating the quantum advantage. While large-scale quantum computers are still many years away, it is important to design scalable architectures for building quantum computers with about 100 well-behaved qubits in the near-term future. The architectures can be used to demonstrate the so-called quantum (computational) supremacy, where quantum supremacy refers to any major

milestone achievement in the quest for outperforming classical computers on some tough computational tasks. Quantum supremacy has attracted considerable interest in quantum computation and is being actively explored by academic institutes, government labs, and private companies (Aaronson and Arkhipov, 2011, Aaronson and Chen, 2017, Arute et al., 2019, Boixo et al., 2018, Hamilton et al., 2017, Harrow and Montanaro, 2017, Lund et al., 2017, Quesada et al., 2018 and Zhong et al., 2020).

5.2.1. *Two Quantum Supremacy Projects.* This section illustrates two well-known quantum supremacy studies for solving hard statistical sampling problems. First, I present the quantum supremacy project reported in Arute et al., 2019 by the Google AI research group. Google's quantum computer (processor), called Sycamore, is built on superconducting technology to perform the computational task of sampling the output distributions of random quantum circuits. The project investigators constructed random quantum circuits, studied sampling from the output distributions of the random quantum circuits, and checked the Sycamore processor against state-of-the-art classical supercomputers in terms of runtime for accomplishing the sampling task. As described in Section 2.4, a quantum circuit is composed of quantum gates, and a small-scale quantum computer can be essentially equivalent to a quantum circuit. Here a random quantum circuit consists of a sequence of clock cycles of one-qubit and two-qubit gates with gates applied to different qubits in the same cycle. Sampling from the output distribution of the quantum circuit means measuring the circuit qubits in the computational basis to produce bitstrings like $\{1000101, 0010100, \dots\}$. Because of the quantum exponential complexity, sampling a random quantum circuit by classical computers renders computational complexity which grows exponentially in size, where the size of the random quantum circuit is determined by the number of qubits created in the quantum circuit as well as the number of cycles used by the quantum circuit. Thus, the classical sampling of the output distribution suffers from an exponential scaling of runtime with circuit size. Quantum supremacy is demonstrated by accomplishing a sampling task by random quantum circuits of sufficient size that, due to the exponential cost, rule out the execution of the task by classical computers. The study in Arute et al., 2019 shows that the Google quantum computer can successfully carry out sampling output distributions of random quantum circuits with 53 qubits and 20 cycles, while the sampling task is practically beyond the reach of the fastest classical supercomputers available at the time. In fact, the computing experiments and statistical analysis have shown that it took 200 seconds for the Sycamore processor to sample a million bitstrings from random quantum circuits with 53 qubits and 20 cycles, while classical sampling by the best supercomputers at the time would take $10,000$ years. Also, it was reported in Wu et al., 2021 that a programmable superconducting quantum processor called Zuchongzhi was built with 66 qubits to perform random quantum circuits sampling and further demonstrate quantum computational advantage.

Another more recent quantum supremacy project is reported in Zhong et al., 2020 that has built a photonic quantum computer (processor) called Jiuzhang to perform Gaussian Boson sampling. Boson sampling was first introduced in Aaronson and Arkhipov, 2011 to employ photonic platforms for demonstrating quantum computational advantage. Boson sampling and its variants refer to a quantum computation model where nonclassical light (source) passes through a network of optical elements (such as beamsplitters and phase-shifters) and then photons (bosons) are detected. Due to quantum exponential complexity, current classical compute cannot handle an optical network of medium size, such as a network system with about 50 photons and 2500 paths. A successful quantum computing experiment on an optical network of sufficient size will render quantum supremacy

(Aaronson and Arkhipov, 2011, Aaronson and Chen, 2017, Hamilton et al., 2017, Harrow and Montanaro, 2017, Lund et al., 2017 and Quesada et al., 2018). A statistical definition of Boson sampling in Aaronson and Arkhipov, 2011 is given as follows. Suppose that the optical network involves n identical photons and m modes, where 'mode' may be loosely interpreted as the location of a photon, and $m \geq n$. The quantum network 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. Define the set of elements corresponding to all the computational basis states in the following manner:

$$\Omega_{m,n} = \{\mathbf{s} = (s_1, s_2, \ldots, s_m) : \ s_i \in \mathbb{N} \text{ and } s_1 + s_2 + \cdots + s_m = n\},$$

where $\mathbb{N}$ denotes the set of all nonnegative integers. Let $\mathbf{U} = (u_{ij})$ be the $m \times m$ unitary matrix to determine the action of the optical network. For each $\mathbf{s} \in \Omega_{m,n}$, a matrix $\mathbf{U_s}$ is obtained from $\mathbf{U}$ by keeping its first n columns and repeating s_j times its j-th row, and then its permanent is calculated, where for a $d \times d$ matrix $\mathbf{A} = (a_{ij})$, its permanent is defined by

$$\text{Permanent}(\mathbf{A}) = \sum_{\pi} \prod_{i=1}^{d} a_{i\pi(i)},$$

and the sum is taken over all permutations π of $1, 2, \ldots, d$. A discrete probability distribution is defined on $\Omega_{m,n}$ as follows:

$$\Pr(\mathbf{s}) = \frac{|\text{Permanent}(\mathbf{U_s})|^2}{s_1! \ldots s_m!}, \ \ \mathbf{s} = (s_1, \ldots, s_m) \in \Omega_{m,n}. \tag{5.1}$$

The probability distribution $\Pr(\mathbf{s})$ corresponds to the optical network system whose action is determined by the unitary matrix $\mathbf{U}$, and Boson sampling in Aaronson and Arkhipov, 2011 refers to statistical sampling from the distribution $\Pr(\mathbf{s})$. Gaussian Boson sampling has been proposed to make use of Gaussian states as probability sources of photons (Hamilton et al., 2017 and Quesada et al., 2018), instead of deterministic sources of photons (used in Boson sampling by Aaronson and Arkhipov, 2011). The resulting probability distribution for a Gaussian state case is similar to (5.1) with permanent replaced by a matrix function, which is either Hafnian or Torontonian, and $\mathbf{U}$ by a sampling matrix characterizing the state. The Torontonian can be interpreted as a sum of Hafnians, and the Hafnian of a $2d \times 2d$ matrix $\mathbf{B} = (b_{ij})$ is defined to be

$$\text{Hafnian}(\mathbf{B}) = \sum_{\varpi \in \mathcal{D}} \prod_{(k,\ell) \in \varpi} b_{k\ell},$$

where $\mathcal{D}$ is the set of all possible ways to partition the set $\{1, \cdots, 2d\}$ into d subsets of size 2. Theoretical and empirical work indicates that Permanent, Hafnian, and Torontonian are in the #P-complete complexity class. Gaussian Boson sampling refers to statistical sampling from the distribution of an optical network with a Gaussian state as a nonclassical source. It has been shown in Zhong et al., 2020 that the photonic quantum computer Jiuzhang can enable up to 76 qubits to successfully accomplish Gaussian Boson sampling tasks that are effectively above the capacity of the best classical supercomputers at the time. Indeed, the computing experiments and data analysis have shown that a 200-second job of Gaussian Boson sampling on Jiuzhang would require 0.6 billon years for the fastest supercomputer available at the time to finish. It was reported in Zhong et al., 2021 that the second generation of Jiuzhang was built with up to 113 qubits and enhanced performance.

5.2.2. *The role of Statistics in Quantum Supremacy.* The two quantum supremacy projects presented in Section 5.2.1 aim to solve statistical sampling problems, and their studies involve extensive statistical analysis. Due to the random nature of quantum computation and circumstantial evidence used in quantum supremacy investigation, quantum supremacy claims should heavily rely on sound statistical analysis and justification including quantum and classical computing experiment design, data collection and analysis, assumption validation, and model assessment. Quantum supremacy involves the development of hardware (building quantum computing devices) and software (developing computational problems and algorithms) as well as the use of statistics (designing computing experiments, collecting data, and carrying out statistical analysis). Thus, confirming (or refuting) a quantum supremacy claim hinges on building a quantum computer, finding a suitable computational problem that is very hard for classical supercomputers but relatively easy for the quantum computer, and the proper evaluation of computational results, outcome data, and circumstantial evidence that is obtained from running the quantum computer and classical supercomputers to solve the computational problem. As the core of quantum computation entails the creation of quantum computers and the development of quantum algorithms that are significantly faster than classical computers, plenty of quantum computation research has devoted to these tasks. Yet much more effort is currently needed to deal with the statistical aspects of evaluating quantum supremacy claims.

Quantum computing devices are unique and expensive, and it is difficult to repeat experiments and carry out independent tests. This is also true to some extent for classical supercomputers. However, statistical analysis can be done thoroughly and independently. Furthermore, statistics can be used to alleviate the challenge of evaluation that follows from the lack of the repeated experiments and independent tests. For example, statistical ideas and concepts from blind experiments in clinical trials and the randomized response technique used in a sampling survey with sensitive questions can be borrowed to design a scheme that would allow an independent third party to outsource a computational job to a quantum computer. This scheme would potentially make it possible for repeated experiments and independent tests to be performed on the quantum computer to some extent. The statistical task for quantum supremacy evaluation is similar to usual statistical applications used for solving complex scientific problems such as research questions in biology and engineering. The challenges are that each problem is different, and statistical analysis needs to take into account the specifics of the problem including the nature of the problem and background knowledge in the domain science. The statistical evaluation of establishing a quantum supremacy claim depends on many factors, which may include both quantum and classical computing devices, computational problems, computing experiments, experimental designs to collect data, methods to analyze the data, and techniques to check assumptions and validate models. For example, as described in Section 5.2.1, the two quantum supremacy projects utilize different quantum technologies, distinct computing platforms, and separate sampling problems; their computing experiments, models, data, and analyses are all different. I wish to point out that, despite extensive data analysis carried out in the two quantum supremacy projects, there are serious statistical issues that need to be carefully examined. As a case in point, I found that the proposed noisy quantum circuit model in the Google study does not fit to the bitstrings data generated from the experiments (also see Rinott et al., 2021 and Wang and Liu, 2022).

6. A Study on Quantum Computational Complexity

Despite the existence of a large volume of literature on classical and quantum computational complexity theory, many fundamental problems remain unsettled, such as questions on how powerful are quantum computers, what are the relationships between classical complexity classes and their quantum counterparts, and whether quantum computation challenges the Church-Turing theses. Here I present a recent landmark work on computational complexity and quantum entanglement.

Quantum resources are utilized for computation and information. In particular, quantum entanglement plays a key role in quantum computation and quantum information. While the study of entanglement was started in 1935 by Albert Einstein, Boris Podolsky, and Nathan Rosen, a year later Alan Turing introduced so-called Turing machines to formulate the general theory of computing and subsequently proved that the halting problem is undecidable over Turing machines. The halting problem refers to the problem of determining, given a computer program and an input to the program, whether the program will continue to run forever or eventually halt, and Turing's result indicates that there exists no all-purpose algorithm to decide whether a computer program will keep running all the time or finish running at a certain time. Turing machines are used in computational complexity to classify computational problems by their relative levels of difficulty and to verify that a given answer to a problem is correct.

Quantum entanglement and the halting problem seem to be unrelated, but they are merged with interactive proofs to solve open problems in computer science, physics, and mathematics. Interactive proofs are based on the logical analog to police interrogation where asking the right questions may lead to confidence in or skepticism regarding an elaborate story provided by a suspect. An interactive proof system in computational complexity theory involves two parties called a prover and a verifier that interact by exchanging messages in order to ascertain whether a specified string belongs to a language or not. Their interactive communication continues until the verifier, having obtained an answer to the problem, becomes convinced that it is correct. While the honest verifier possesses bounded computation power, the powerful prover has boundless computational resources but cannot be trusted. The untrusted prover can convince the honest verifier of any true statement but cannot persuade the verifier that a false statement is true, except for a small probability. Moreover, an interactive proof system may have multi-provers to enable the verifier with more leverage for cross-checking their answers.

As nonlocal games and Bell tests are introduced in Sections 3.3 and 3.4, in the context of computational complexity they can be considered as multi-prover interactive proofs. A Bell test is viewed as an interactive proof with the two provers to convince the verifier of quantum entanglement. A nonlocal game like the magic-square game is treated as an interactive proof system to find the optimal winning probability and to determine if the optimal quantum strategy can do better than the best possible classical strategy.

Given that entanglement can help to win a nonlocal game, two provers may share entangled particles, and interrogating such entangled provers changes the range of problems that can be verified. In fact, it is natural to believe that entanglement provides means to coordinate answers and to tell consistent lies; thus, it may work against verification. However, entanglement may permit one to verify a much larger class of problems than would be possible without entanglement. For example, one might recall the magic-square game, in which Alice and Bob hope to place an identical number in the same cell albeit without any knowledge on the part of either as to which row or column the other has been asked about. Entanglement enables provers to come up with correlated

questions on their own that the verifier wants. Interacting with entangled provers actually allows one to expand the class of nonlocal games to play and enlarge the variety of problems to verify.

A recent landmark result establishes that 'MIP*=RE' (Ji et al., 2020), where MIP* denotes the class of problems that can be verified through interactions with entangled quantum provers, and RE stands for the class of problems that are not harder than the halting problem. The class MIP* can be characterized through the computational complexity of approximating the optimal winning probability for a nonlocal game. The halting problem has an interactive proof with entangled provers called Alice and Bob, and there is a nonlocal game associated with the given Turing machine so that the verifier plays the nonlocal game to conclude that the Turing machine eventually terminates or gets stuck in an infinite loop, depending on whether the provers win or lose the game. That is, the verifier has offloaded the computational task to all-powerful Alice and Bob for determining if the Turing machine halts or not, and thus, the two classes are exactly the same. This quantum computational complexity work has had a cascade of consequences in computer science, physics, and mathematics including the solving of a long standing conjecture called Tsirelson's problem on two different entanglement models in quantum physics and an over-40-year-old operator algebra problem called the Connes' Embedding Conjecture in pure mathematics. See Connes, 1976, Fritz, 2012, Ji et al., 2020, Junge et al., 2011, Nielsen and Chuang, 2010, Šupić and Bowles, 2019 and Tsirelson, 1993 for more details.

7. A Concluding Proposal to Develop Quantum Data Science

As described here, the advantages of quantum computation over classical computation hold great potential for data science, in particular, machine learning and statistical learning. Already, quantum learning theory is being developed to synthesize classical learning and quantum computation and to investigate how quantum resources can affect learning efficiency and computational complexity for handling data science problems. For example, quantum approaches can achieve higher efficiency in learning difficult functions or policies for some machine learning tasks, while quantum machine learning may have great computational advantages over its classical counterpart for solving certain machine learning problems. Specific cases include linear algebra operations, linear and quadratic programming, gradient descent, support vector machines, principal component analysis, annealing, Boson sampling, and Boltzmann machines. See 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, Cai et al., 2016, Ciliberto et al., 2018, Dunjko et al., 2016, Dunjko and Briegel, 2018, Granade et al., 2012, Hu and Wang, 2021, Jordan, 2005, Kieferova and Wiebe, 2016, Lloyd et al., 2014, O'Gorman et al., 2015, Paesani et al., 2017, Rebentrost et al., 2014, Salakhutdinov and Hinton, 2009, Shenvi et al., 2003, Svore et al., 2014, Wang, 2013, Wang and Wu, 2020, Wang et al., 2016, Wiebe, Granade, Ferrie, et al., 2014, Wiebe, Kapoor, et al., 2014, Wiebe, Granade, and Cory, 2015, Wiebe, Kapoor, et al., 2015, Wiebe and Granade, 2016, Wittek, 2014 and Zhong et al., 2020 for more details.

It is natural to expect quantum computation to play a major role in data science; I further anticipate that quantum computation has tremendous potential to revolutionize computational statistics and data science. As might be expected, there is huge demand in data science for theoretical research and experimental work in quantum computation and quantum information. Because of the stochastic nature underlying quantum physics and complex data involved in quantum experiments,

there is a great need to develop better data science approaches for quantum computation and quantum information. As a case in point I list some specific topics below to illustrate or speculate as to potential points of interplay between quantum science and data science, and to advocate for the development of quantum data science.

Quantum certification has been developed to create protocol approaches to certifying quantum devices, such as testing and assessing their quantum performances, and the certification certainly needs data science for calibrating and validating quantum properties. Quantum supremacy heavily involves inferential methods and data analysis techniques. Such developments suggest that data science may provide useful ideas and offer valuable insights for quantum computation and quantum information (Alpaydin, 2020, Artiles et al., 2005, Barndorff-Nielsen et al., 2003, Goodfellow et al., 2016, Hastie et al., 2009 and Sutton and Barto, 2018). For example, nonlocal games with quantum entanglement allow more correlations than what is possible classically. There is a class of quantum algorithms, including Grover's algorithm, that is based on quantum walk. It is known that the quantum walk has larger variance than the corresponding classical random walk. The quantum algorithms are random and their associated computational tasks may be considered as statistical problems. Thus, from the viewpoint of the tradeoff between statistical efficiency and computational efficiency, these quantum algorithms gain more computational efficiency (with faster computational speed) at the expense of less statistical efficiency (with larger variance) in comparison with their classical counterparts. Shor's factoring algorithm is based on quantum phase estimation, and Bayesian quantum phase estimation has been proposed; thus, it is feasible to adopt the probability interpretation of prime numbers in number theory as a prior for developing Bayesian quantum factoring and investigating its computational speedup and statistical efficiency. Last but not least, it is interesting to explore data augmentation, thermal-based classical annealing, and tunneling-based quantum annealing (Wang et al., 2016).

While quantum speedup may be due to the use of quantum physics, the acceleration phenomena in recursive algorithms may be attributed to some mathematical means since accelerated algorithms often involve differential equations of higher order (Mou et al., 2020, Wang and Wu, 2020 and Wibisono et al., 2016). The data science approach may lead to the study of general resources for the computational speedup phenomenon, whether the resources used are expressed in terms of physical materials, digital contents, or mathematical elements. In fact, there should be more synergy between quantum computation and data science than between the classical computation and machine learning described in Section 1. Overall, I advocate for the development of quantum data science for the interplay between quantum science and data science, where quantum information science serves as its domain science. The aim is to develop a combination of quantum experimental techniques, mathematical models, statistical methods, and computational tools in order to advance the development of quantum computation and quantum information. Quantum data science enables data scientists to work with quantum scientists and engineers on this exciting frontier of scientific endeavor by integrating quantum science and data science. For the purpose of inspiration, I conclude this article with my big data poem, with its Chinese version displayed in Figure 5.

Big Data

Yazhen Wang (5/18/2017)

Figure 5. The Big Data Poem in Chinese.

Long ago,
big data was a thick screen,
I was here,
mainframe computing was there.

And now,
big data is a thin smart-phone,
I am here,
cloud computing is there.

In the future,
big data will be a tiny particle,

I will be here,
quantum computing will be there.

Disclosure Statement. The authors have no conflicts of interest to declare.

Acknowledgments. The research of Yazhen Wang was supported in part by NSF grants DMS-1707605 and DMS-1913149. The author thanks Editor-in-Chief Xiao-Li Meng, Richard Gill, Suzanne Smith, Steven Finch, Hongzhi Liu, an associate editor, and two anonymous referees for comments and suggestions that led to improvements of the paper.

References

Aaronson, S., & Arkhipov, A. (2011). The computational complexity of linear optics. *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, *10*, 333–342. https://doi.org/10.1145/1993636.1993682

Aaronson, S., & Chen, L. (2017). Complexity-theoretic foundations of quantum supremacy experiments. In R. O'Donnell (Ed.), *32nd computational complexity conference (ccc2017)* (22:1–67). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/LIPIcs.CCC.2017.22
Keywords: computational complexity, quantum computing, quantum supremacy

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

Alpaydin, E. (2020). *Introduction to machine learning* (4th). The MIT Press.

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

Aravind, P. K. (2004). Quantum mysteries revisited again. *American Journal of Physics*, *72*(10), 1303–1307.

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

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

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

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., ... Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510.

Barndorff-Nielsen, O. E., Gill, R. D., & Jupp, P. E. (2003). On quantum statistical inference. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, *65*(4), 775–804.

Benedetti, M., Realpe-Gómez, J., Biswas, R., & 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.

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

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

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

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

Childs, A. M. (2010). On the relationship between continuous- and discrete-time quantum walk. *Communications in Mathematical Physics*, *294*(2), 581–603.

Childs, A. M., Cleve, R., Deotto, E., Farhi, E., Gutmann, S., & Spielman, D. A. (2003). Exponential algorithmic speedup by a quantum walk. *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, 59–68.

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

Connes, A. (1976). Classification of injective factors Cases II_1, II_∞, III_λ, $\lambda \neq 1$. *Annals of Mathematics*, *104*(1), 71–115.

Crandall, R., & Pomerance, C. B. (2006). *Prime numbers: A computational perspective* (Vol. 182). Springer Science & Business Media.

Dunjko, V., & 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., & Briegel, H. J. (2016). Quantum-enhanced machine learning. *Physical Review Letters*, *117*, 130501. https://doi.org/10.1103/PhysRevLett.117.130501

Fritz, T. (2012). Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, *24*(05), 1250012. https://doi.org/10.1142/S0129055X12500122

Gill, R. D. (2014). Statistics, causality and Bell's theorem. *Statistical Science*, *29*(4), 512–528.

Gill, R. D. (2018). Teleportation into quantum statistics. *Journal of the Korean Statistical Society*, *100*(10), 1–35.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. The MIT Press.

Granade, C. E., Ferrie, C., Wiebe, N., & Cory, D. G. (2012). Robust online Hamiltonian learning. *New Journal of Physics*, *14*(10), 103013.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219.

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

Hamilton, C. S., Kruse, R., Sansoni, L., Barkhofen, S., Silberhorn, C., & Jex, I. (2017). Gaussian boson sampling. *Physical Review Letters*, *119*, 170501. https://doi.org/10.1103/PhysRevLett.119.170501

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

Hastie, T., Tibshirani, R., & Friedman, J. H. (2009). *The elements of statistical learning: Data mining, inference, and prediction* (Second). Springer.

Hu, J., & Wang, Y. (2021). Quantum annealing via path-integral Monte Carlo with data augmentation. *Journal of Computational and Graphical Statistics*, *30*(2), 284–296.

Ji, Z., Natarajan, A., Vidick, T., Wright, J., & Yuen, H. (2020). MIP*=RE. *arXiv preprint arXiv:2001.04383*.

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

Junge, M., Navascues, M., Palazuelos, C., Perez-Garcia, D., Scholz, V. B., & Werner, R. F. (2011). Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, *52*(1), 012102. https://doi.org/10.1063/1.3514538

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Kieferova, M., & Wiebe, N. (2016). Tomography and generative data modeling via quantum Boltzmann training. *arXiv preprint arXiv:1612.05204*.

Kitaev, A. Y. (1995). Quantum measurements and the abelian stabilizer problem. *arXiv preprint arXiv:quant-ph/9511026*.

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

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

Mou, W., Ma, Y.-A., Wainwright, M. J., Bartlett, P. L., & Jordan, M. I. (2020). High-order Langevin diffusion yields an accelerated MCMC algorithm. *Journal of Machine Learning Research*, *21*.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th Anniversary). Cambridge University Press.

O'Gorman, B., Babbush, R., Perdomo-Ortiz, A., Aspuru-Guzik, A., & 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., & Thompson, M. G. (2017). Experimental Bayesian quantum phase estimation on a silicon photonic chip. *Physical Review Letters*, *118*(10), 100503.

Quesada, N., Arrazola, J. M., & Killoran, N. (2018). Gaussian boson sampling using threshold detectors. *Physical Review A*, *98*, 062322. https://doi.org/10.1103/PhysRevA.98.062322

Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical Review Letters*, *113*, 130503. https://doi.org/10.1103/PhysRevLett.113.130503

Rinott, Y., Shoham, T., & Kalai, G. (2021). Statistical aspects of the quantum supremacy demonstration. *Statistical Science*.

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

Salakhutdinov, R., & Hinton, G. (2009). Deep Boltzmann machines. In D. van Dyk & M. Welling (Eds.), *Proceedings of the twelth international conference on artificial intelligence and statistics* (pp. 448–455). PMLR.

Shenvi, N., Kempe, J., & 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. *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, 124–134.

Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, *52*(4), R2493.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, *41*(2), 303–332.

Šupić, I., & Bowles, J. (2019). Self-testing of quantum systems: A review. *arXiv preprint quant-ph/1904.10042*.

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction* (Second). A Bradford Book.

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

Szegedy, M. (2004). Quantum speed-up of Markov chain based algorithms. *Proceedings of 45th Annual IEEE Symposium on Foundations of Computer Science*, 32–41. https://doi.org/10.1109/FOCS.2004.53

Tsirelson, B. S. (1993). Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, *8*(4), 329–345.

Tulsi, A. (2008). Faster quantum-walk algorithm for the two-dimensional spatial search. *Physical Review A*, *78*(1), 012310.

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., & Liu, H. (2022). Quantum computing in a statistical context. *Annual Review of Statistics and Its Application*, *9*.

Wang, Y., & Song, X. (2020). Quantum science and quantum technology. *Statistical Science*, *35*(1), 51–74. https://doi.org/10.1214/19-STS745

Wang, Y., & Wu, S. (2020). Asymptotic analysis via stochastic differential equations of gradient descent algorithms in statistical and computational paradigms. *Journal of Machine Learning Research*, *21*(199), 1–103.

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

Wibisono, A., Wilson, A. C., & Jordan, M. I. (2016). A variational perspective on accelerated methods in optimization. *Proceedings of the National Academy of Sciences*, *113*(47), E7351–E7358. https://doi.org/10.1073/pnas.1614734113

Wiebe, N., & Granade, C. (2016). Efficient Bayesian phase estimation. *Physical Review Letters*, *117*, 010503. https://doi.org/10.1103/PhysRevLett.117.010503

Wiebe, N., Granade, C., & Cory, D. G. (2015). Quantum bootstrapping via compressed quantum Hamiltonian learning. *New Journal of Physics*, *17*(2), 022005.

Wiebe, N., Granade, C., Ferrie, C., & Cory, D. G. (2014). Hamiltonian learning and certification using quantum resources. *Physical Review Letters*, *112*(19), 190501.

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

Wiebe, N., Kapoor, A., & Svore, K. M. (2015). Quantum nearest-neighbor algorithms for machine learning. *Quantum Information and Computation*, *15*(3-4), 318–358. https://www.microsoft.com/en-us/research/publication/quantum-nearest-neighbor-algorithms-for-machine-learning/

Wilde, M. M. (2017). *Quantum information theory* (Second). Cambridge University Press.

Williams, C. P. (2011). *Explorations in quantum computating* (Second). Springer.

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

Wu, Y., Bao, W.-S., Cao, S., Chen, F., Chen, M.-C., Chen, X., Chung, T.-H., Deng, H., Du, Y., Fan, D., Gong, M., Guo, C., Guo, C., Guo, S., Han, L., Hong, L., Huang, H.-L., Huo, Y.-H., Li, L., ... Pan, J.-W. (2021). Strong quantum computational advantage using a superconducting quantum processor. *Physical Review Letters*, *127*, 180501. https://doi.org/10.1103/PhysRevLett.127.180501

Zhong, H.-S., Deng, Y.-H., Qin, J., Wang, H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Wu, D., Gong, S.-Q., Su, H., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., ... Pan, J.-W. (2021). Phase-programmable gaussian boson sampling using stimulated squeezed light. *Physical Review Letters*, *127*, 180502. https://doi.org/10.1103/PhysRevLett.127.180502

Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Qin, J., Wu, D., Ding, X., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., You, L., ... Pan, J.-W. (2020). Quantum computational advantage using photons. *Science*. https://doi.org/10.1126/science.abe8770