Quantum Algorithms for Wireless Communications

Panagiotis Botsinis, *Member, IEEE,* Dimitrios Alanis, *Member, IEEE,* Zunaira Babar, Hung Nguyen, *Member, IEEE,* Daryus Chandra, Soon Xin Ng, *Senior Member, IEEE,* and Lajos Hanzo, *Fellow Member, IEEE*

***Abstract*—Faster, ultra-reliable, low-power and secure communications has always been high on the wireless evolutionary agenda. However, the appetite for faster, more reliable, greener and more secure communications continues to grow. The state-of-the-art methods conceived for achieving the performance targets of the associated processes may be accompanied by an increase in computational complexity. Alternatively, a degraded performance may have to be accepted due to the lack of jointly optimized system components. In this survey we investigate the employment of quantum computing for solving problems in wireless communication systems. By exploiting the inherent parallelism of quantum computing, quantum algorithms may be invoked for approaching the optimal performance of classical wireless processes, despite their reduced number of cost-function evaluations. In this contribution we discuss the basics of quantum computing using linear algebra, before presenting the operation of the major quantum algorithms, which have been proposed in the literature for improving wireless communications systems. Furthermore, we investigate a number of optimization problems encountered both in the physical and network layer of wireless communications, while comparing their classical and quantum-assisted solutions. Finally, we state a number of open problems in wireless communications that may benefit from quantum computing.**

***Index Terms*—algorithm design and analysis, channel estimation, localization, multiuser detection, non-orthogonal multiple access, optimization, precoding, quantum algorithms, quantum computing, routing, visible light communication, wireless communication**

LIST OF ABBREVIATIONS

ACO	Ant Colony Optimization
AoA	Angle of Arrival
BBHT	Boyer-Brassard-Høyer-Tapp
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CF	Cost Function
CFE	Cost Function Evaluation
CFE	Cost Function Evaluation
CIR	Channel Impulse Response
CoMP	Coordinated Multi-Point
CoMP	Coordinated Multi-Point
DDCE	Decision-Directed Channel Estimation
DEA	Differential Evolution Algorithm
DH	Dürr-Høyer
DN	Destination Node
eMBB	enhanced Mobile BroadBand
EQPO	Evolutionary Quantum Pareto Optimization
FD-CHTF	Frequency Domain - CHannel Transfer Function
FFT	Fast Fourier Transform
GA	Genetic Algorithm
GNFS	General Number Field Sieve
HetNet	Heterogeneous Network
HHL	Harrow-Hassidim-Lloyd
IoT	Internet of Things
IQFT	Inverse Quantum Fourier Transform
LED	Light Emitting Diode
LLR	Log-Likelihood Ratio
LOS	Line Of Sight
LTE	Long-Term Evolution
MAP	Maximum *A posteriori* Probability
MBER	Minimum Bit Error Ratio
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
mMTC	massive Machine Type Communications
MODQO	Multi-Objective Decomposition Quantum Optimization
MPC	Multi-Path Component
MUD	Multi-User Detection
MUT	Multi-User Transmitter
NDQIO	Non-Dominated Quantum Iterative Optimization
NDQO	Non-Dominated Quantum Optmization
NOMA	Non-Orthogonal Multiple Access
NU	Network Utility
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Orthogonal Multiple Access
PDP	Power Delay Profile
PIC	Parallel Interference Cancellation
PLR	Packet Loss Ratio
PSO	Particle Swarm Optimization
QCA	Quantum Counting Algorithm
QGA	Quantum Genetic Algorithm
QHA	Quantum Heuristic Algorithm
QMA	Quantum Mean Algorithm
QoS	Quality of Service
QPEA	Quantum Phase Estimation Algorithm
QPSK	Quadrature Phase Shift Keying
QRWBS	Quantum Weighted Boosting Search
QSA	Quantum Search Algorithm
QSVM	Quantum Support Vector Machine
QWSA	Quantum Weighted Sum Algorithm
RN	Relay Node
RSSI	Received Signal Strength Indicator

The authors are with the School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK (email: {pb1y14, da1d16, zb2g10, hvn08r, dc2n14, sxn, lh}@ecs.soton.ac.uk).

The financial support of the European Research Council under the Advanced Fellow Grant, that of the Royal Society's Wolfson Research Merit Award and that of the Engineering and Physical Sciences Research Council under Grant EP/L018659/1 is gratefully acknowledged. The use of the IRIDIS High Performance Computing Facility at the University of Southampton is also acknowledged.

IEEE Communications Tutorials & Surveys 2018

RWBS	Repeated Weighted Boosting Search
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SIC	Successive Interference Cancellation
SISO	Soft-Input Soft-Output
SN	Source Node
SNR	Signal to Noise Ratio
SVM	Support Vector Machine
TDMA	Time Division Multiple Access
TDoA	Time Difference of Arrival
ToA	Time of Arrival
TPC	Transmit Pre-Coding
URLLC	Ultra-Reliable Low-Latency Communications
UV	Utility Vector
UWB	Ultra WideBand
WSN	Wireless Sensor Network
ZF	Zero Forcing

I. Introduction

The next generation of wireless communications promises Ultra-Reliable Low-Latency Communications (URLLC), massive Machine Type Communications (mMTC), as well as 100x increased throughput in enhanced Mobile BroadBand (eMBB) communications [1], [2]. The plethora of applications, involving the Internet of Things (IoT) and the vision of everything being connected everywhere and anytime has to be achieved [3], [4], while keeping the required resources as low as possible. For example, the transition from Orthogonal Multiple Access (OMA) to Non-Orthogonal Multiple Access (NOMA) [5] is expected to occur in the eMBB use case of 5G for increasing the system throughput. However, the complexity of the signal detection will also be increased, even if a sub-optimal detector based on for example Successive Interference Cancellation (SIC) is adopted [6]. At the same time, agile and accurate channel estimation will be required in URLLC [7], where the target end-to-end delay requirement, which includes both the transmission time as well as processing time, is on the order of a few OFDM symbols. In order to achieve this, a joint channel estimator and data detector may be employed for achieving an improved performance, albeit this tends to impose increased computational complexity. In a mobile mMTC network, the inherent problem of finding the optimal route amongst numerous nodes is again going to require intensive computations [8].

During the last few years the research community has turned its attention to quantum computing [1], [9]–[12] with the objective of amalgamating it with classical communications in order to attain certain performance targets, such as throughput, round trip delay and reliability targets at a low computational complexity. As we will discuss in more detail in this contribution, there are numerous optimization problems in wireless communications systems that may be solved at a reduced number of Cost Function Evaluations (CFEs) by employing quantum algorithms.

A. *Why Quantum Computing?*

The ever-reducing transistor size following Moore's law is approaching the point, where the so-called *quantum effects* [9] become prevalent in the transistors' operation [13]. This specific trend implies that quantum effects become unavoidable, hence rendering the research of quantum computation systems an urgent necessity. In fact, a quantum annealing chipset [14] is already commercially available from *D-Wave*[1] [15], [16]. Apart from the quantum annealing architecture, the so-called *gate-based architecture* [10], which relies on building computational blocks using quantum gates in a similar fashion to classical logic gates, is attracting increasing attention due to the recent advances in *quantum stabilizer codes* [17]–[22], which are capable of mitigating the *decoherence*[2] effects encountered by quantum circuits [9]. In terms of implementation, D-Wave's most recent model, namely *D-Wave 2000Q*[3], has a total of 2000 qubits, while *IBM Q Experience*[4], which relies on the gated-based architecture, has currently only 20 qubits in total. However, IBM has recently announced their plans[5] for delivering a 50 qubit gate-based quantum computer by 2020.

Once quantum computing becomes a commercial reality, it may be used in wireless communications systems in order to speed up specific processes due to its inherent parallelization capabilities. While a classical bit may adopt either the values 0 or 1, a quantum bit, or *qubit*, may have the values $|0\rangle$, $|1\rangle$, or any superposition of the two [9]–[11], where the notation $|\cdot\rangle$ is the ket representation [23] and it is the column vector of a quantum state. If two qubits are used, then the composite quantum state may have the values $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ simultaneously. In general, by employing b bits in a classical register, one out of 2^b combinations is represented at any time. By contrast, in a quantum register associated with b qubits, the composite quantum state may be found in a superposition of all 2^b values *simultaneously*. Therefore, by applying a quantum operation to the quantum register would result in altering all 2^b values at the same time. This represents the parallel processing capability of quantum computing. Multiple quantum algorithms have been proposed [12], which are capable of outperforming their classical counterparts in the same categories of problems, by either requiring fewer computational steps, or by finding a better solution to the specific problem.

In this treatise, we will focus our attention on the employment of quantum algorithms in classical communication systems, which may be termed as *quantum-assisted communications* [1], [9]. More specifically, the employment of quantum algorithms may be capable of improving the already existing processes of classical communications, such as optimal multi-user detection, channel estimation, finding the optimal precoding matrix for the downlink of a multi-user system, or finding the optimal route in a classical wireless network. Quantum-assisted communications should be distinguished from *quantum-based communications* [1], [10], [11]. In the latter, quantum bits are transmitted and received over quantum channels. By contrast, quantum-assisted communications may

[1] https://www.dwavesys.com/d-wave-two-system

[2] As it will be explained in the following, decoherence may be considered as detrimental noise in quantum circuits.

[3] https://www.dwavesys.com/d-wave-two-system

[4] https://quantumexperience.ng.bluemix.net/qx/experience

[5] https://www-03.ibm.com/press/us/en/pressrelease/53374.wss

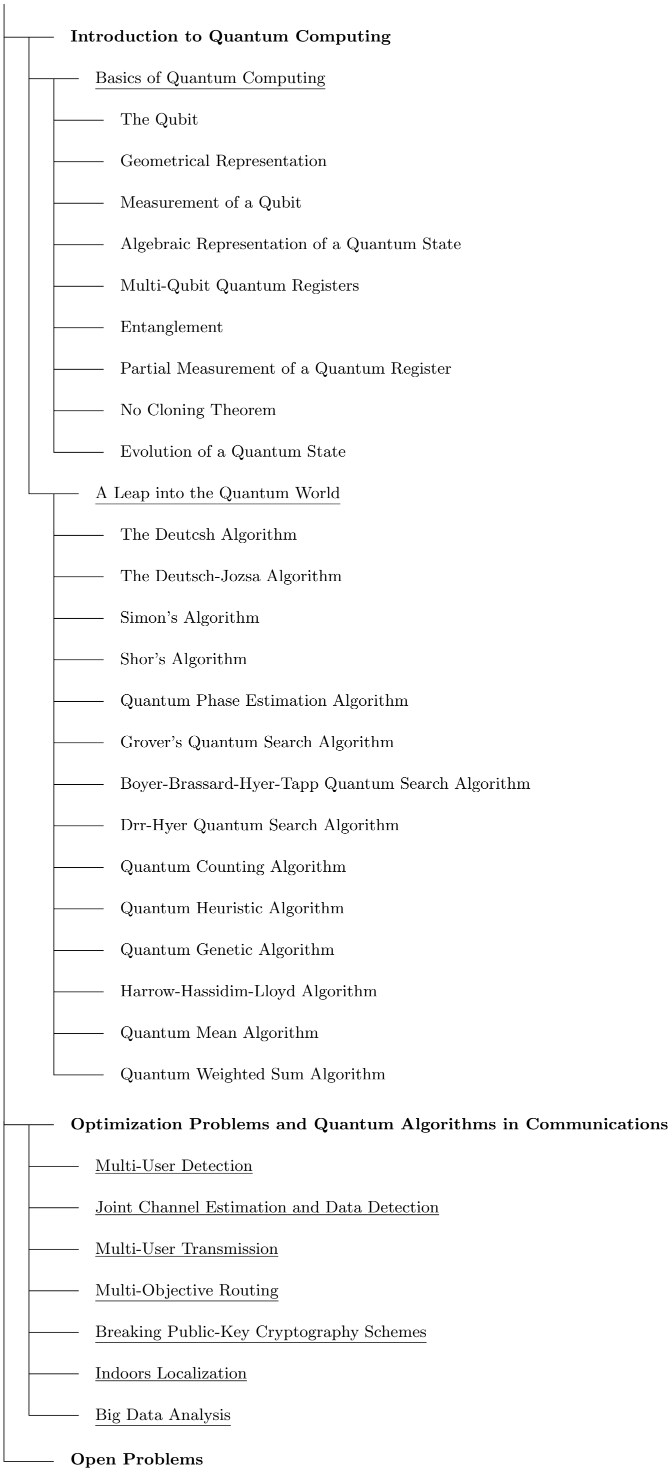

Introduction to Quantum Computing
Basics of Quantum Computing
The Qubit
Geometrical Representation
Measurement of a Qubit
Algebraic Representation of a Quantum State
Multi-Qubit Quantum Registers
Entanglement
Partial Measurement of a Quantum Register
No Cloning Theorem
Evolution of a Quantum State
A Leap into the Quantum World
The Deutcsh Algorithm
The Deutsch-Jozsa Algorithm
Simon's Algorithm
Shor's Algorithm
Quantum Phase Estimation Algorithm
Grover's Quantum Search Algorithm
Boyer-Brassard-Hyer-Tapp Quantum Search Algorithm
Drr-Hyer Quantum Search Algorithm
Quantum Counting Algorithm
Quantum Heuristic Algorithm
Quantum Genetic Algorithm
Harrow-Hassidim-Lloyd Algorithm
Quantum Mean Algorithm
Quantum Weighted Sum Algorithm
Optimization Problems and Quantum Algorithms in Communications
Multi-User Detection
Joint Channel Estimation and Data Detection
Multi-User Transmission
Multi-Objective Routing
Breaking Public-Key Cryptography Schemes
Indoors Localization
Big Data Analysis
Open Problems

Fig. 1: The structure of the paper.

be considered as a classical communication system like the mobile broadband in the Long-Term Evolution (LTE) standard, where hybrid classical and quantum processors are exchanging information at the Base Station (BS).

B. Motivation for this Contribution

There is a number of well-established surveys on quantum algorithms [24]–[27]. In [24], Williams detailed the operation of Grover's Quantum Search Algorithm (QSA) [28], [29] and discussed its applications as a "subroutine" in other quantum algorithms. Quantum walk-based search algorithms were the focus of [25], arguing that they may be used for solving search problems, such as finding out whether a list has unique entries, or determining if a group's elements are commutative with each other. In [26], efficient quantum algorithms substantially outperforming their classical counterparts were reviewed, with a focus on their employment in algebraic problems. In [27], Mosca reviewed a number of quantum algorithms, explaining their operation and their associated computational complexity. The website "Quantum Zoo" [30] has gathered a comprehensive list of quantum algorithms, briefly describing their operation.

Against this background, the main motivation of this paper is to make quantum computing and quantum algorithms accessible to communication engineers, by investigating their operation and employment in communication applications. We provide a list of optimization problems in the area of wireless communications that may be solved using a quantum computer. We review quantum algorithms that have already been used[6] *for solving existing problems in classical wireless communication systems. Furthermore, we discuss both the "why" and the "how" of quantum computation. Quantum computing is still considered by the majority of communication engineers as a term closely intertwined with physics. Therefore, we assume that the reader has no background on quantum computing and we aim for ripping off this mysterious cloak from quantum computing by showing the quantum circuits employed in the quantum algorithms presented. In this study we have focused our attention on the associated algorithmic perspectives, with an emphasis on the potential performance gain as well as on the attainable complexity reduction. Indeed, we concur that also the other important practical requirements have to be taken into consideration, such as the scalability and timing requirements, the required hardware and the potential reuse of existing hardware blocks in a modem chip along with the integration between the classical and quantum parts of the solutions presented, which have not been considered in this paper.*

The rest of the paper is structured as follows. In Section II we state the basic postulates of quantum mechanics and describe how quantum computing systems can be represented and simulated by classical computers. We continue by offering a brief historical perspective of quantum computing and review the operation of the most popular quantum algorithms. In Section III, we describe a number of optimization problems that appear in wireless communication systems, along with their associated classical, as well as quantum algorithms that may be employed for solving them. Finally, we state a number of open problems in Section IV and we conclude in Section V. The paper's structure is given in Fig. 1.

[6] Since a universal quantum computer does not exist at the time of writing, the operation of the quantum algorithms has been demonstrated with simulations on classical super-computers. Please note that the practical creation of the discussed quantum algorithms is out of the scope of this paper. Here we assume that a universal quantum computer exists and that the discussed quantum algorithms are available.

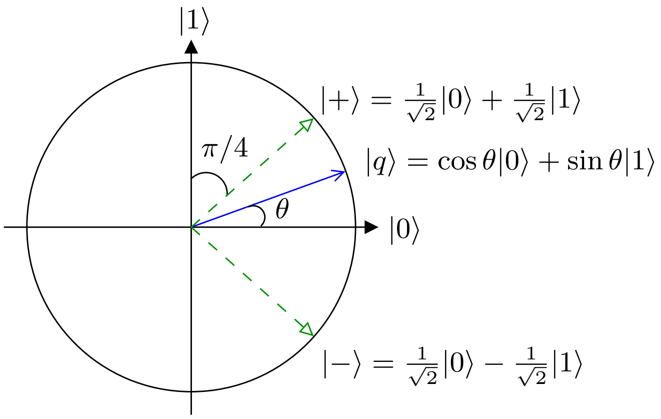

$|1\rangle$
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$\pi/4$
$|q\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$
θ
$|0\rangle$
$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Fig. 2: The 2D representation of a qubit, when the amplitudes of its quantum states are real-valued.

II. Introduction to Quantum Computing

A. Basics of Quantum Computing

1) The Qubit: The quantum state of a qubit may be represented using any chosen orthogonal basis. The most commonly used basis is the computational basis [9], which corresponds to the states $|0\rangle$ and $|1\rangle$. The quantum state $|q\rangle$ of a single-qubit system in the computational basis $\{|0\rangle, |1\rangle\}$ is [9]

$$|q\rangle = a|0\rangle + b|1\rangle, \tag{1}$$

where $a, b \in \mathbb{C}$ are the amplitudes of $|q\rangle$ on the computational basis and we have $|a|^2+|b|^2 = 1$. When $a = 0$, we have $b = 1$ and hence

$$|q\rangle = |1\rangle, \tag{2}$$

which corresponds to the classical bit value 1. Similarly, if $a = 1$, then $b = 0$ and

$$|q\rangle = |0\rangle, \tag{3}$$

which again is a classical bit value. However, if we choose $a = b = 1/\sqrt{2}$, then we have

$$|q\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle. \tag{4}$$

The quantum state in (4) seems to exhibit a symmetry with respect to the orthogonal states $|0\rangle$ and $|1\rangle$, not favoring one over the other. This state is widely used in most of the quantum algorithms that we will investigate.

2) Geometrical Representation: Assuming only real-valued amplitudes for a quantum state $a, b \in \mathbb{R}$, the resultant 2-D geometrical representation of a qubit's state is shown in Fig. 2, since its state may be written as in

$$|q\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle. \tag{5}$$

In the general case, the amplitudes of the quantum states are complex-valued, therefore the state of a qubit is represented by the 3-D Bloch sphere [9]–[11] of Fig. 3, since a qubit's state may always be written as

$$|q\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \tag{6}$$

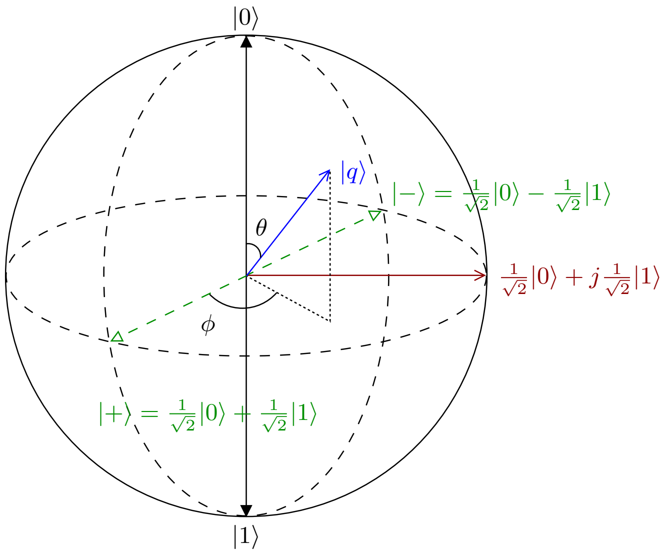

$|0\rangle$
$|q\rangle$
$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
θ
$\frac{1}{\sqrt{2}}|0\rangle + j\frac{1}{\sqrt{2}}|1\rangle$
ϕ
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$|1\rangle$

Fig. 3: The generic 3D representation of a qubit using a Bloch sphere, when the amplitudes of its quantum states are complex-valued.

Many algorithms, such as Grover's QSA [28], the Boyer-Brassard-Høyer-Tapp (BBHT) QSA [31] and the Dürr-Høyer (DH) QSA [32] only consider real-valued amplitudes, therefore the 2-D representation is suitable for their analysis. However, other algorithms, like Shor's algorithm [33] and the quantum counting algorithm [34] exploit the complex-valued nature of the states' amplitudes and the Bloch sphere may be used for geometrically representing their quantum states.

3) Measurement of a Qubit: Before we continue with the investigation of the symmetrical state of (4), let us explicitly mention that even though a qubit may be in a superposition of two orthogonal states, if we desire to *observe,* or *measure* its value, we will only obtain one of the two orthogonal states. The measurement of a quantum state may be considered as a Quantum-to-Classical (Q/C) conversion, since it allows us to gain some insight on the quantum system[7]. The measurement of a qubit's state may also be done in a basis different from that which the qubit was prepared in. For now, let us use the computational basis also for measuring a quantum state. According to the Copenhagen interpretation [35], which is the most widely adopted interpretation of a measurement's operation, a quantum state does not have specific properties before it is measured. However, when it is observed, the probabilities of its superimposed states define not only the outcome of the measurement, but also the new quantum state of the system.

The amplitudes a and b of the quantum state $|q\rangle$ in (1) uniquely define the probabilities of obtaining $|0\rangle$ or $|1\rangle$, when we measure the qubit's state $|q\rangle$ on the orthogonal basis $\{|0\rangle, |1\rangle\}$. More specifically, there is a $|a|^2$ probability that we will obtain the quantum state $|0\rangle$ and a $|b|^2$ probability that $|1\rangle$ will be observed. This is also the reason

[7] Please note that the amount of insight obtained by a measurement heavily depends on the context of the quantum algorithm or protocol which the measurement is a part of

why $|a|^2 + |b|^2 = 1$ is always true. For example, in (2) and (3), since the system's state is already equal to one of the two states of the computational basis, which was used for the measurement, we would always observe $|1\rangle$ and $|0\rangle$, respectively. However, when we measure the quantum state of (4), there is a $|a|^2 = 1/2 = 50\%$ probability of obtaining the quantum state $|0\rangle$ and $|b|^2 = 1/2 = 50\%$ probability of obtaining the quantum state $|1\rangle$. Since the probability of observing either of the two states is the same, the quantum system of (4) is said to be in an *equiprobable superposition* of states, always with respect to the computational orthogonal basis.

After the measurement, the quantum state *collapses* to the observed quantum state. For example, let us assume that the output of the quantum state's measurement in (4) was $|1\rangle$. As mentioned before, this event had a 50% probability of occurrence. Given that it has happened however, the system's quantum state from that point onwards *becomes identical to the observed quantum state*, hence we have $|q'\rangle = |1\rangle$.

This feature is termed as *wave function collapse* in quantum mechanics and it is irreversible. In other words, we are not able to reconstruct the system's quantum state to that before the measurement, unless we have knowledge about the pre-measurement amplitudes a and b of (1).

4) Algebraic Representation of a Quantum State: A quantum state $|q\rangle$ may be fully described by its state vector [9]. The size of the state vector $|q\rangle$ is equal to the number of orthogonal states that the quantum state could be superimposed in. The values of the state vector $|q\rangle$ are the amplitudes of each orthogonal state. For example, when a qubit is in the state $|q\rangle = a|0\rangle + b|1\rangle$ as in (1), the 2-element state vector is

$$|q\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a|0\rangle + b|1\rangle, \tag{7}$$

implying that the first element corresponds to the amplitude of the state $|0\rangle$, while the second element to the amplitude of the state $|1\rangle$. As another example, the state vector of the equiprobable quantum state of (4) is

$$|q\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{8}$$

As expected, when more qubits are used, the system's state vector has more elements in order to accommodate the amplitudes of all legitimate state combinations.

5) Multi-Qubit Quantum Registers: In a two-qubit register, there are four legitimate states that the composite quantum system can be superimposed in. If the first qubit of the register is in the state $|q_1\rangle = a|0\rangle + b|1\rangle$ and the second qubit is in the state $|q_2\rangle = c|0\rangle + d|1\rangle$, the state of the system is

$$\begin{aligned} |q\rangle &= |q_1\rangle \otimes |q_2\rangle = |q_1 q_2\rangle & (9)\\ &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) & (10)\\ &= a \cdot c|00\rangle + a \cdot d|01\rangle + b \cdot c|10\rangle + b \cdot d|11\rangle & (11)\\ &= \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix}, & (12) \end{aligned}$$

where $\otimes$ is the tensor product operator and the system's state vector includes the amplitudes of the four quantum states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.

In general, in an n-qubit register, the state vector will have 2^n entries, each corresponding to the amplitude of the respective orthogonal state. Now let us consider a 2-qubit register with the following quantum state

$$|q\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|10\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix}. \tag{13}$$

After a potential measurement of that quantum register, there is a $\left(\sqrt{3}/2\right)^2 = 0.75$ probability of observing the state $|00\rangle$ and $(1/2)^2 = 0.25$ probability of obtaining the state $|10\rangle$. It is impossible to observe the states $|01\rangle$ or $|11\rangle$. We may also observe that it is possible to rewrite its state as

$$|q\rangle = \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \otimes |0\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |q_1\rangle|q_2\rangle. \tag{14}$$

This means that the first qubit is in a superposition (not equiprobable) of its two possible states, while the second qubit is at the state $|q_2\rangle = |0\rangle$. Since the state of the quantum register may be written as a tensor product of the quantum states of the individual qubits, the two qubits $|q_1\rangle$ and $|q_2\rangle$ are *independent* of each other.

6) Entanglement: When the quantum states of two or more qubits may not be represented separately and independently of each other, the qubits are *entangled* with each other. For example, let us consider the state

$$|q\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}. \tag{15}$$

This 2-qubit register is in an equiprobable superposition of the states $|00\rangle$ and $|01\rangle$. It is impossible to describe the states of the two qubits individually as in (14)[8]. Therefore, the two qubits of the quantum register in (15) are entangled. Actually,

[8] Try it, following the same methodology as in (13) and (14)!

the quantum state in (15) is one of the four *Bell states* [36], [37],

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{16}$$
$$\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \tag{17}$$
$$\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \tag{18}$$
$$\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle, \tag{19}$$

which are widely used, since they are the only four quantum states of a two-qubit register that provide an equiprobable entanglement between two qubits.

7) Partial Measurement of a Quantum Register: In a multi-qubit quantum register, it is possible to only observe a subset of the qubits it consists of. Therefore, when we measure one of the qubits, its quantum state collapses to the observed state, while the quantum state of the rest of the *independent* qubits remains unaltered. However, this is not the case for the rest of the *entangled* qubits, whose state will also be affected by the observation of an entangled qubit.

As an example, let us try to only observe the second qubit of the quantum register in (14). The second qubit has an 100% probability of yielding the observation $|0\rangle$, therefore this is the state we will obtain. At the same time, the state of the first qubit $|q_1\rangle = \sqrt{3}/2|0\rangle + 1/2|1\rangle$ will remain unaltered, because it is in a superposition of its own, independent states.

Let us now try to measure the second qubit of the entangled 2-qubit register of (15). There is a $(1/\sqrt{2})^2 = 0.5 = 50\%$ chance of observing either the state $|0\rangle$ or the state $|1\rangle$. Let us assume that we observed the state $|0\rangle$. Therefore, the quantum state of the second qubit collapses to $|0\rangle$. Based on (15), we should notice that the state of the first qubit also collapses to $|0\rangle$ instantaneously, upon obtaining the measurement output of the second qubit. This happened because the whole quantum register could either be observed in the state $|00\rangle$, or in the state $|11\rangle$. Since we observed the second qubit in the state $|0\rangle$, the first qubit can only be in the state $|0\rangle$ from this point onwards.

Entanglement enables a plethora of applications, since it allows instantaneous information exchange between qubits. As it will be discussed in the following, the quantum algorithms appropriately manipulate the available qubits in order to finally measure a quantum state, which has a desirable property.

8) No Cloning Theorem: The irreversible nature of a quantum measurement is exploited in quantum cryptography [38]–[40], a field which also exploits the no cloning theorem [41]. According to the no cloning theorem, it is impossible to copy the unknown quantum state of a qubit into the quantum state of another qubit, while keeping their states independent of each other at the same time. In other words, it is impossible to make independent copies of qubits, without entangling them with each other in the process.

The rules of entanglement, the no cloning theorem and the irreversible nature of measurements allow quantum-based communications to be very promising for sharing private keys between two parties. By exploiting these features in the available QKD protocols, such as the Bennett-Brassard-1984 (BB84) protocol [42], one or both parties become capable of detecting whether an eavesdropper tempered with their communications or not, due to the imperfections that the eavesdropper would have imposed on the measured and retransmitted states, since the eavesdropper would have been unable to simply copy and forward the intercepted qubits. If the two parties determine that an eavesdropper was present during the transmission of the qubits, the whole process is aborted and restarted.

9) Evolution of a Quantum State: The state of a quantum register may be changed by applying *unitary operators or gates* to its qubits [9]. Let us first investigate a single-qubit system. One of the most widely used single-qubit unitary operators is the *Hadamard operator* H, which creates equiprobable superpositions of the two states, given that the initial state was either $|0\rangle$ or $|1\rangle$, as encapsulated in

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle \tag{20}$$
$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle. \tag{21}$$

The states $|+\rangle$ and $|-\rangle$ form the orthogonal Hadamard basis, as depicted in Fig. 2. The matrix representation of the single-qubit Hadamard operator is

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{22}$$

while that of the two-qubit Hadamard operator is

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{23}$$

An n-qubit Hadamard gate has to be employed for creating an equiprobable superposition of all legitimate states at the beginning of most quantum algorithms, which is achieved by applying it to an n-qubit quantum register in the all-zero state $|0\rangle^{\otimes n}$. The circuit representation of the Hadamard gate is shown in Fig. 4.

The parallel evolution of the state of a quantum register that consists of multiple qubits is termed as *quantum parallelism*. Quantum parallelism is one of the pivotal features of quantum computing, which is exploited in order to create quantum algorithms that solve problems by requiring for example fewer CF evaluations than their classical counterparts.

Another popular set of single-qubit quantum gates is represented by the Pauli gates [9]–[11]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{24}$$

Explicitly, the X operator is the NOT gate, also known from classical logic circuits, since it swaps the amplitudes of the

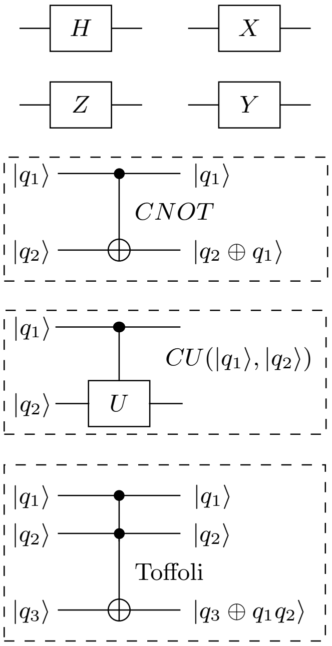


Fig. 4: The circuit representation of the Hadamard gate H, of the three Pauli gates X, Z and Y, as well as of the Controlled-NOT operation, of the general Controlled-U gate and of the Toffoli gate.

quantum states of a qubit as in

$$X(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle.$$

The Z operator is the gate imposing a *phase shift* by π radians, since it flips the sign of the amplitude of just the state $|1\rangle$, as described in

$$Z(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle.$$

The Y operator may be considered as a combination of the X and Z gates, since it results in

$$\begin{aligned} Y(a|0\rangle + b|1\rangle) &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix} \\ &= i\left(-b|0\rangle + a|1\rangle\right). \end{aligned}$$

The circuit representation of the Pauli gates is also depicted in Fig. 4.

Other popular gates require the use of *control qubits*. For example, the Controlled-NOT ($CNOT$) gate applies the NOT operation to the qubit $|q_2\rangle$, only when the qubit $|q_1\rangle$ is in the state $|1\rangle$, as described by

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{25}$$

TABLE I: Operation of a CU Gate

Before: $\|q_1\rangle\|q_2\rangle$	After: $CU\|q_1\rangle\|q_2\rangle$
$\|0\rangle\|0\rangle$	$\|0\rangle\|0\rangle$
$\|0\rangle\|1\rangle$	$\|0\rangle\|1\rangle$
$\|1\rangle\|0\rangle$	$\|1\rangle U\|0\rangle$
$\|1\rangle\|1\rangle$	$\|1\rangle U\|1\rangle$

For example, if the first (control) qubit was in the state $|q_1\rangle = a|0\rangle + b|1\rangle$ and the second (target) qubit was in the state $|q_2\rangle = c|0\rangle + d|1\rangle$, the $CNOT$ gate would result into

$$\begin{aligned} CNOT(|q_1\rangle|q_2\rangle) &= a \cdot c|00\rangle + a \cdot d|01\rangle + b \cdot d|10\rangle + b \cdot c|11\rangle \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix} \\ &= \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot d \\ b \cdot c \end{bmatrix} = a \cdot c|00\rangle + a \cdot d|01\rangle + b \cdot d|10\rangle + b \cdot c|11\rangle. \end{aligned}$$

We may observe that the amplitudes of the quantum states where the first qubit is equal to $|1\rangle$ have been swapped. In general, the *Controlled-U* gate applies a general quantum gate U to a target qubit only when the control qubit is equal to $|1\rangle$, as described by

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}, \tag{26}$$

where the aforementioned general single-qubit unitary operator U is

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}. \tag{27}$$

When the control qubits is equal to $|0\rangle$, the identity gate is applied to the target qubit, as stated in (26). Table I states the operation that the CU gate would carry out based on the four possible quantum states of two qubits, where the first one is the control qubit and the second one is the target qubit.

Finally, the Toffoli gate accepts two control qubits and flips the state of the target qubit, if and only if both control qubits are in the state $|1\rangle$. The matrix representation of the Toffoli

TABLE II: Operation of a Toffoli Gate

Before: $\|q_1\rangle\|q_2\rangle\|q_3\rangle$	After: $CCNOT\|q_1\rangle\|q_2\rangle\|q_3\rangle$
$\|0\rangle\|0\rangle\|0\rangle$	$\|0\rangle\|0\rangle\|0\rangle$
$\|0\rangle\|0\rangle\|1\rangle$	$\|0\rangle\|0\rangle\|1\rangle$
$\|0\rangle\|1\rangle\|0\rangle$	$\|0\rangle\|1\rangle\|0\rangle$
$\|0\rangle\|1\rangle\|1\rangle$	$\|0\rangle\|1\rangle\|1\rangle$
$\|1\rangle\|0\rangle\|0\rangle$	$\|1\rangle\|0\rangle\|0\rangle$
$\|1\rangle\|0\rangle\|1\rangle$	$\|1\rangle\|0\rangle\|1\rangle$
$\|1\rangle\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle\|1\rangle$
$\|1\rangle\|1\rangle\|1\rangle$	$\|1\rangle\|1\rangle\|0\rangle$

gate is [9]:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (28)$$

The circuit representation of the controlled gates is also depicted in Fig. 4. Table II portrays both the initial and resultant states of a three-qubit register, when the Toffoli gate is applied to it, where the first two qubits are the control qubits and the last one is the target qubit.

B. A Leap into the Quantum World

Research on quantum mechanics was initiated by Planck, Bohr, Heisenberg, Einstein and Schrödinger in 1923. Even though arguments and conflicts arose regarding whether the theory of quantum mechanics encapsulates a complete description of Nature, it is currently considered as the most suitable interpretation of both the microscopic and the macroscopic worlds.

The inspiration of quantum computation was provided by Feynman [43], who proposed in 1981 a novel framework for conveying information by the spin of an electron and for simulating the evolution of the quantum states. In the following year, Benioff [44] proposed a technique of simulating quantum systems on Turing machines. Based on these contributions, further quantum algorithms were inspired. In the following sections we describe the general problems and the high-level operation of the major quantum algorithms, before delving into their applicability in wireless communications. A short description of the major quantum algorithms is provided in Fig. 5.

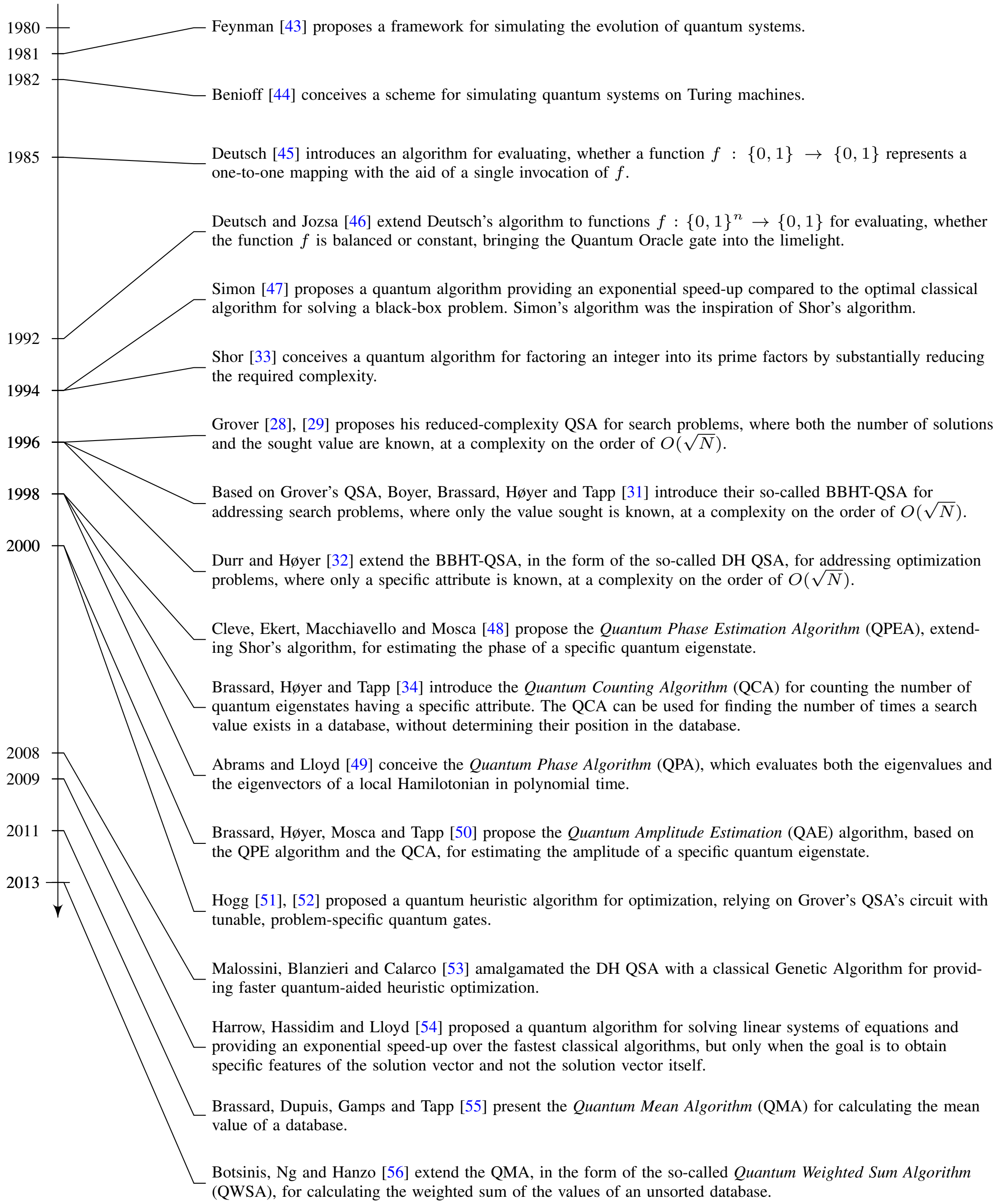
1) The Deutsch Algorithm: A few years later, the benefits of quantum parallelism were exploited by Deutsch [45], who conceived an algorithm, which now has the fond connotation of *Deutsch algorithm*. Let us first define the black box problem that we can solve using Deutsch's algorithm. Generally, a black box problem involves a function f, whose operation is unknown. We have to determine the features of the function by only evaluating it with the aid of different input arguments and then observing its corresponding outputs. Here, we have to determine whether the binary function $f : \{0,1\} \rightarrow \{0,1\}$ does or does not have a one-to-one mapping. When the function f has a one-to-one mapping we would expect $f(0) \oplus f(1) = 1$, otherwise it would be $f(0) \oplus f(1) = 0$, since that would mean $f(0) = f(1)$, where $\oplus$ is the modulo-2 addition. In classical computing, a single evaluation for each of the legitimate inputs would be required, bringing the total number of function evaluations to two. Deutsch algorithm [45] succeeds in determining whether the function f has a one-to-one mapping by only using a single function evaluation.

2) The Deutsch-Jozsa Algorithm: An extension of this algorithm, namely the *Deutsch-Jozsa algorithm* [46], was conceived for determining whether a function $f : \{0,1\}^n \rightarrow \{0,1\}$ is balanced or constant[9]. Let us consider the problem in a real scenario, where the two parties Alice and Bob communicate with each other. Alice sends an n-bit number to Bob, who uses it as the input argument of his function f. Bob then transmits back the output bit. Alice has to determine whether the function that Bob used was balanced or constant. In classical computing, the best-case scenario would only be achieved if the function was balanced, Alice transmitted two different numbers and these two numbers happened to yield the two different outputs. The worst-case scenario is always encountered, when the function is constant, since Alice has to transmit $(2^{n-1}+1)$ different input arguments (one more than half the set of inputs), before she realizes that the function Bob is using is constant. By using the Deutsch-Jozsa algorithm, Alice is able to determine whether the function f used by Bob is balanced or constant, with just a single transmission of n qubits in an equiprobable superposition of all possible inputs. Bob uses an extra auxiliary qubit, Hadamard gates and a quantum gate U_f that performs the same operation as f, but accepts qubits as its inputs. Finally, Bob measures the quantum state of the n qubits at the output of his quantum circuit. If the observed state is the all-zero state $|0\rangle^{\otimes n}$, the function f is constant, otherwise it is balanced.

The Deutsch-Jozsa algorithm solves the generalized black-box problem of the previous section. Indeed, if the function f allows only 0 or 1 as its legitimate inputs, determining whether the function has a one-to-one mapping, or if it is balanced answers exactly the same question. The algorithm was later improved by Cleve, Ekert, Macchiavello and Mosca [48] for achieving a 100% probability of success.

The Deutsch-Jozsa algorithm laid the foundations for the development of the so-called *Quantum Oracle* gates [9],

[9] A function f is constant if it yields the same value at its output regardless of the input argument. On the other hand, a function f is balanced, if it yields one value (e.g. 0) for half the input arguments and another value (e.g. 1) for the other half of the input arguments



Feynman [43] proposes a framework for simulating the evolution of quantum systems.

Benioff [44] conceives a scheme for simulating quantum systems on Turing machines.

Deutsch [45] introduces an algorithm for evaluating, whether a function $f : \{0,1\} \rightarrow \{0,1\}$ represents a one-to-one mapping with the aid of a single invocation of f.

Deutsch and Jozsa [46] extend Deutsch's algorithm to functions $f : \{0,1\}^n \rightarrow \{0,1\}$ for evaluating, whether the function f is balanced or constant, bringing the Quantum Oracle gate into the limelight.

Simon [47] proposes a quantum algorithm providing an exponential speed-up compared to the optimal classical algorithm for solving a black-box problem. Simon's algorithm was the inspiration of Shor's algorithm.

Shor [33] conceives a quantum algorithm for factoring an integer into its prime factors by substantially reducing the required complexity.

Grover [28], [29] proposes his reduced-complexity QSA for search problems, where both the number of solutions and the sought value are known, at a complexity on the order of $O(\sqrt{N})$.

Based on Grover's QSA, Boyer, Brassard, Høyer and Tapp [31] introduce their so-called BBHT-QSA for addressing search problems, where only the value sought is known, at a complexity on the order of $O(\sqrt{N})$.

Durr and Høyer [32] extend the BBHT-QSA, in the form of the so-called DH QSA, for addressing optimization problems, where only a specific attribute is known, at a complexity on the order of $O(\sqrt{N})$.

Cleve, Ekert, Macchiavello and Mosca [48] propose the *Quantum Phase Estimation Algorithm* (QPEA), extending Shor's algorithm, for estimating the phase of a specific quantum eigenstate.

Brassard, Høyer and Tapp [34] introduce the *Quantum Counting Algorithm* (QCA) for counting the number of quantum eigenstates having a specific attribute. The QCA can be used for finding the number of times a search value exists in a database, without determining their position in the database.

Abrams and Lloyd [49] conceive the *Quantum Phase Algorithm* (QPA), which evaluates both the eigenvalues and the eigenvectors of a local Hamiltonian in polynomial time.

Brassard, Høyer, Mosca and Tapp [50] propose the *Quantum Amplitude Estimation* (QAE) algorithm, based on the QPE algorithm and the QCA, for estimating the amplitude of a specific quantum eigenstate.

Hogg [51], [52] proposed a quantum heuristic algorithm for optimization, relying on Grover's QSA's circuit with tunable, problem-specific quantum gates.

Malossini, Blanzieri and Calarco [53] amalgamated the DH QSA with a classical Genetic Algorithm for providing faster quantum-aided heuristic optimization.

Harrow, Hassidim and Lloyd [54] proposed a quantum algorithm for solving linear systems of equations and providing an exponential speed-up over the fastest classical algorithms, but only when the goal is to obtain specific features of the solution vector and not the solution vector itself.

Brassard, Dupuis, Gamps and Tapp [55] present the *Quantum Mean Algorithm* (QMA) for calculating the mean value of a database.

Botsinis, Ng and Hanzo [56] extend the QMA, in the form of the so-called *Quantum Weighted Sum Algorithm* (QWSA), for calculating the weighted sum of the values of an unsorted database.

Fig. 5: Timeline of quantum computing milestones.

which are quantum circuits implementing a generic function $f : \{0,1\}^N \rightarrow \{0,1\}^M$ and they are capable of calculating all the pairs of possible inputs-outputs of f using a single call of f by exploiting quantum parallelism.

3) Simon's Algorithm: In 1994, Simon managed to solve a black-box problem by using on the order of $O(n)$ queries addressed to the black box, while the optimal classical algorithm has to use $\Omega\left(2^{n/2}\right)$ queries for the same task [47]. The black box U_f implements a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ and has the property that $f(x) = f(y)$ if and only if $x = y$ or if $x \oplus y = s$, for some unknown $s \in \{0,1\}^n$, where $x, y \in \{0,1\}^n$. Simon's algorithm succeeds in finding the value s that satisfies the function's above-mentioned property.

4) Shor's Algorithm: In 1994, Shor proposed a quantum algorithm [33], [57] for efficiently solving the problem of factoring a given integer N. The best classical algorithm is the General Number Field Sieve (GNFS) [58]. Shor's algorithm requires an exponentially lower complexity than the GNFS, which is achieved by combining classical and quantum processing. It first reduces the factoring problem to the so-called order-finding problem addressed below using a classical algorithm. Initially, it randomly picks a number $a < N$. Let us assume that the greatest common divisor between a and N is equal to 1[10]. Then a quantum circuit is employed for finding the period r of the function[12]

$$f(x) = a^x \bmod N. \tag{29}$$

If the estimated period r is even and $a^{r/2} = -1 \bmod N$ is false, then $gcd(a^{r/2}+1, N)$ and $gcd(a^{r/2}-1, N)$ are two non-trivial factors of N and the algorithm ends.

The order-finding quantum algorithm initially creates an equiprobable superposition of $C = 2^c$ states, using an appropriate number of c qubits[13], as shown in Fig. 6. It then employs *controlled-U_f* operators[14] , where each of the c qubits controls the operation of a quantum gate that performs the function $f(x)$ of (29) on $n = \log_2 N$ auxiliary qubits. All n auxiliary qubits should initially be in the quantum state $|1\rangle^{\otimes n}$. This part is the bottleneck of Shor's algorithm, since it requires the operation of multiple controlled-U_f gates and $n = \log_2 N$ auxilliary qubits. Therefore, when N is high, more gates are required for a single U_f operation. At the same time, when C is high, the estimation of the period will be more accurate, but more controlled-U_f operations are required, hence increasing the complexity.

After the operation of the controlled-U_f gates in Fig. 6, the c qubits pass through an Inverse Quantum Fourier Transform (IQFT) [10], [59] operator. The IQFT has the same effect as a classical IDFT, where the amplitude of each of the superimposed states is equally spread over the amplitudes of the resultant superimposed state. At the output of the IQFT, if we measure the resultant state of the c-qubit register, we will obtain a value $|q\rangle$, which may then be classically processed to approximate the period r. As mentioned earlier, after finding the period r, classical processing is employed for the rest of Shor's algorithm.

5) Quantum Phase Estimation Algorithm: A few years after Shor's algorithm was introduced, the order-finding quantum algorithm of Fig. 6 used in Shor's algorithm was found in [48] to be just a specific application of a general quantum circuit and algorithm, which is termed as the Quantum Phase Estimation Algorithm (QPEA). The QPEA follows exactly the same procedure as the period-finding quantum algorithm of Section II-B4. More specifically, given a unitary operator U that operates on n qubits and an eigenvector $|\phi\rangle$, such that

$$U|\phi\rangle = 2^{i\pi\theta}|\phi\rangle, \tag{30}$$

the QPEA estimates the period θ, which means that it can find the eigenvalue of a unitary operator. The quantum circuit of the QPEA is given in Fig. 7. The upper c qubits are termed as the *control register*, while the bottom n qubits represent the *function register*.

The QPEA is used as a building block for multiple quantum algorithms. As an example, let us now revisit Shor's algorithm, for the sake of relating it to the operation of the QPEA. In Shor's algorithm, the factoring problem was reduced to finding the period r of the function $f(x)$ of (29). In order to solve this problem, we have $U = f(x)$ and $\theta = r$ in (30). Comparing the quantum circuits of Fig. 6 and Fig. 7, we may observe that in the former, the n qubits of the function register are initialized to the all-one state $|1\rangle^{\otimes n}$, because it is one of the eignevectors of $f(x)$ of (29). Essentially, since we force a controlled function CU to operate on its eigenvectors, instead of altering the quantum states of the function register, we manage to rotate the states of the c-qubit control register. By applying the QFT to that control register, we are able to estimate the phase, eigenvalue, or period of the unitary transform U, upon its measurement.

6) Grover's Quantum Search Algorithm: In 1996, Grover [28], [29] proposed a *Quantum Search Algorithm* (QSA), which solves a search problem. Specifically, the search problem seeks to find a desired value δ in a database of N entries. We aim to find which of the N entries is equal to δ, i.e. we are interested in finding the position of δ in the database. If the database is sorted from lowest to highest values, the classical iterative halving-based search algorithm [60] is indeed optimal. On the other hand, if the database is unsorted, the optimal classical algorithm relies on a full search of the database. The average complexity of the full search would be on the order of $O(N)$ database queries. The worst case scenario occurs when the desired value is found at the entry that is checked last.

By contrast, Grover's QSA succeeds in finding the desired entry with 100% probability of success after querying the database on the order of $O(\sqrt{N})$ times [28]. This provides a quadratic reduction in complexity over the classical full search. Grover's QSA has been shown to be optimal by Zalka [61]. However, Grover's QSA requires some additional knowledge about the database. More explicitly, Grover's QSA employs the Grover operator $\mathcal{G}$ depicted in Fig. 8 L_{opt} number of consecutive times. Apart from knowing N and (obviously) the desired value δ, additionally Grover's QSA requires the knowledge of how many times the entry δ appears in the database, which is termed as the *number of solutions S*. For example, when we have $\delta = 2$ and $N = 16$, if $S = 3$ entries out of $N = 16$ are equal to $\delta = 2$, a different number of iterations L_{opt} is used in Grover's QSA, compared to the scenario, where only $S = 1$ out of $N = 16$ entries is equal to $\delta = 2$. However, in both examples the same procedure is followed at each iteration. Using fewer or more Grover iterations than L_{opt} may reduce the success probability, which might even approach 0%. Grover's QSA relies on the generic *amplitude amplification* process of Brassard *et al.* [50]. Explicitly, the optimal number of Grover operator applications is $L_{opt} = \left\lfloor 0.25\pi\sqrt{N/S} \right\rfloor$.

In Fig. 8, the $n = \log_2 N$ qubits in the register $|x\rangle_1$ are initialized to an equiprobable superposition of N states, each corresponding to the index of an entry in the database. The unitary operator O is termed as the *Oracle*, which marks the

[10] If the greatest common divisor between a and N was not equal to 1, then a would be a non-trivial factor[11] of N and the algorithm ends, since N can be factored in a and N/a. Then we have the problem of factoring a and N/a, if they are not prime numbers, and so on.

[12] The period of a function $f(x)$ is the smallest positive integer r so that $f(x+r) = f(x)$ for all values of x.

[13] Any number of qubits c that results in $C = 2^c$ states such that $N^2 \leq C < 2N^2$ would suffice.

[14] Please note that a controlled-U_f gate performs the U_f gate to the input target qubits only if the control qubits are in the state $|1\rangle$. When the control qubits are in the state $|0\rangle$, the identity operator is applied instead.

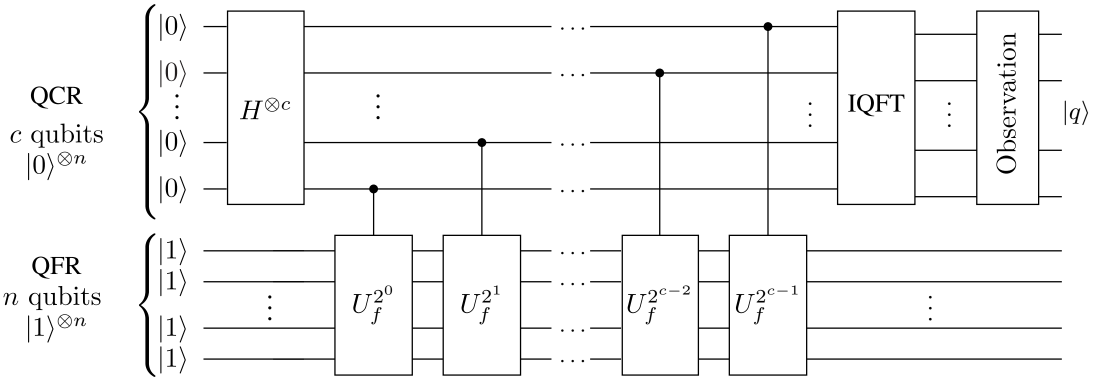


Fig. 6: The quantum circuit employed in Shor's algorithm for finding the period of the function in (29) [33].

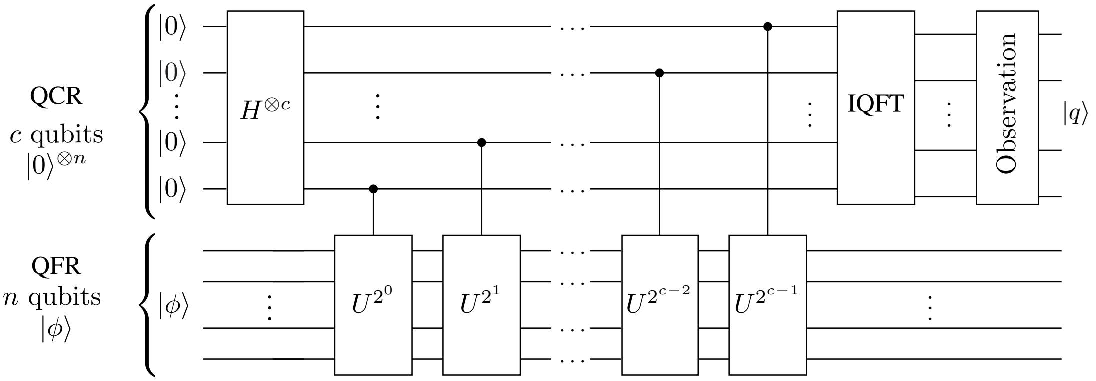


Fig. 7: The quantum circuit of the Quantum Phase Estimation Algorithm, which estimates the eigenvalues of a unitary operator U, which corresponds to its eigenvector $|\phi\rangle$, as described in (30) [48].

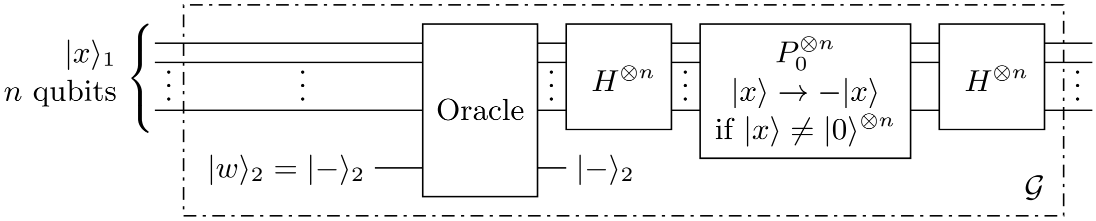

$|x\rangle_1$
n qubits
$|w\rangle_2 = |-\rangle_2$
Oracle
$|-\rangle_2$
$H^{\otimes n}$
$P_0^{\otimes n}$
$|x\rangle \rightarrow -|x\rangle$
if $|x\rangle \neq |0\rangle^{\otimes n}$
$H^{\otimes n}$
$\mathcal{G}$

Fig. 8: Grover operator's quantum circuit including an Oracle, two n-qubit Hadamard gates H and an n-qubit phase shift gate P_0. The HP_0H operator forms the diffusion operator of the Grover operator $\mathcal{G} = HP_0H \cdot O$ [28].

indices of the specific entries in the database that are equal to the sought value δ. Specifically, the Oracle marks an index by changing its sign in the superposition of states. In order to achieve this, an auxiliary qubit $|w\rangle_1$ initialized to the $|-\rangle$ state is used, along with the value δ represented in form of a quantum state. The two Hadamard gates H and a phase rotation gate P_0 that follow the Oracle in Fig. 8 constitute the *diffusion operator* of Grover's circuit, which essentially changes the amplitude of each state by reflecting it with respect to the average amplitude of the current superposition of the states. This has been proven in [28] to result in an amplitude closer to $\sqrt{1/S}$ for each of the specific S states that correspond to the solution entries, while yielding a lower amplitude for the rest of the states that do not correspond to solutions. By repeating this process L_{opt} number of times, the amplitudes of the S quantum states in the superposition that correspond to solution entries gradually become close to $\sqrt{1/S}$, resulting in an $S \cdot (\sqrt{1/S})^2 = 100\%$ probability of observing a state that is indeed the solution state. The resultant amplitude of each solution state prior to measurement is equal to $\sqrt{1/S}$ because all solution states are treated in the same way in Grover's QSA and hence have the same probability $(\sqrt{1/S})^2 = 1/S$ of being observed at the output.

Let us clarify the operation of Grover's QSA with the aid of an example. Let us assume that a database has a size of $N = 32$ entries. Let us also assume that the sought value δ is only only stored in a single entry of the database, but we do not know in which portion exactly. Therefore, we have a single solution $S = 1$, leading us to apply the Grover operator $L_{opt} = \left\lfloor 0.25\pi\sqrt{N/S} \right\rfloor = 4$ times. As shown in Fig. 9a, we commence with an equiprobable superposition of all indices, since we do not have a particular preference as to

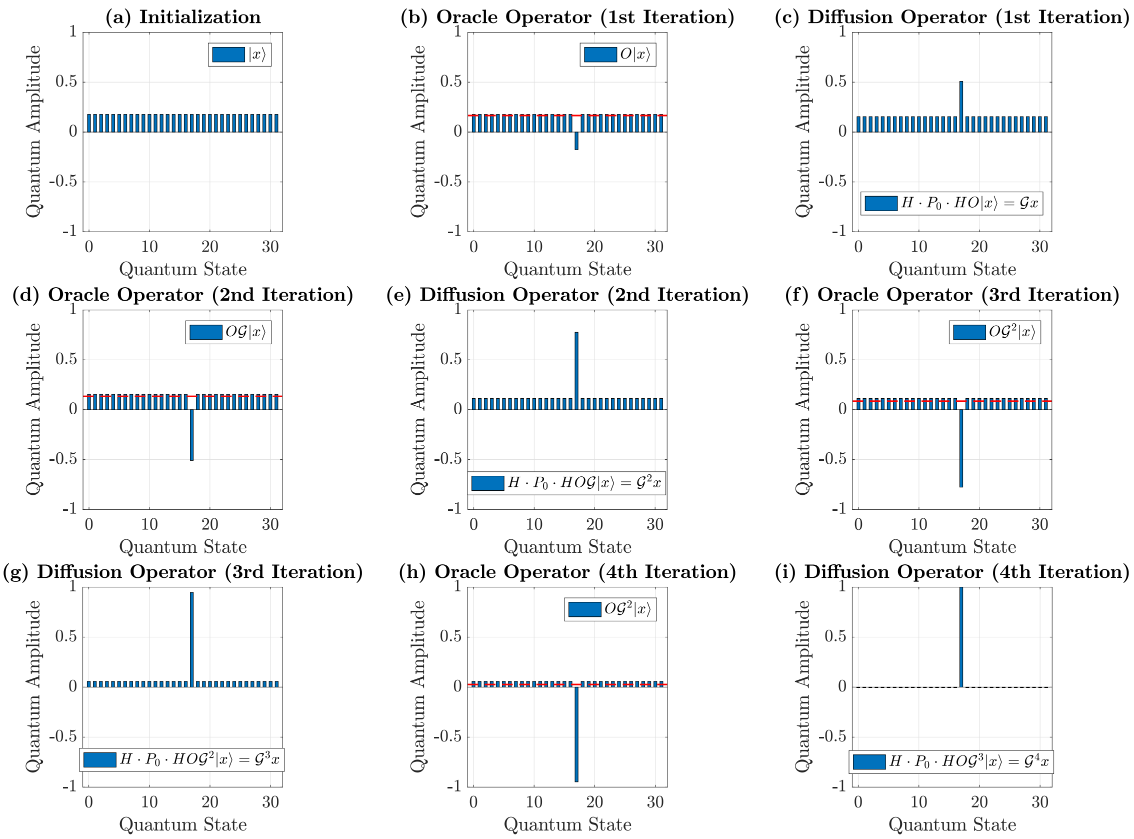


Fig. 9: Example of Grover's QSA in a database with $N = 32$ entries, where the searched value exists only in the entry with index 18. Since there is only a single solution $S = 1$ in a database of size $N = 32$, we have to perform $L_{opt} = 4$ Grover iterations. The red dashed lines indicate the mean value of the amplitudes after each Oracle operation.

which may be associated with the desired entry. After applying the Oracle operator in Fig. 9b, the sign of the amplitude of index 18 is flipped[15]. The red dashed horizontal line in Fig. 9 indicates the mean value of the amplitudes of all superimposed states after the application of the Oracle. In Fig. 9c, the diffusion operator reflects the amplitudes of each state with respect to the aforementioned mean value of the amplitudes. This concludes the first iteration of Grover's QSA. We may conclude that the index 18 has a higher probability of being observed at this stage than the rest of the superimposed states. However, we may increase the probability of observing the solution state 18 even further by applying three more Grover iterations. Following the same approach, Fig. 9d and Fig. 9e characterize the second Grover iteration, Fig. 9f and Fig. 9g the third Grover iteration, while Fig. 9h and Fig. 9i illustrate the fourth and final Grover iteration. In Fig. 9i, the probability of observing the solution state 18 after the fourth Grover iteration is equal to 99.92%. Again, these intermediate steps of Grover's QSA are not readily accessible to us, therefore we have to find another way of determining, when to stop the iterations and observe the resultant state. For that, we have to know both the number of solutions in the database and the size of the database.

Please note that if there are no solutions in a search problem, corresponding to $S = 0$, the Oracle in Fig. 8 will not mark any quantum state and hence the diffusion operator will leave the amplitudes of the quantum states unaltered, since the amplitude of each of the states found in an equiprobable superposition of states is equal to the average amplitude and hence a reflection with respect to the average amplitude will not affect the system. Therefore, regardless of the number of Grover iterations, the initial superposition will not change and a potential measurement at the end will result in any of the N states with equal probability. We can then classically check that the observed index does not correspond to a solution in the database, and hence conclude that there is no solution to the search problem.

7) Boyer-Brassard-Høyer-Tapp Quantum Search Algorithm: Nevertheless, requiring *a priori* knowledge of the number of solutions that exist in the system may not always be viable in practical engineering problems. A beneficial extension of Grover's QSA has been introduced by Boyer *et al.* [31] in the form of the so-called Boyer-Brassard-Høyer-Tap

[15] Please note that in practice we will not be aware of that, since we have not observed the quantum system yet. However, for the sake of clarity, we show the intermediate steps of Grover's QSA.

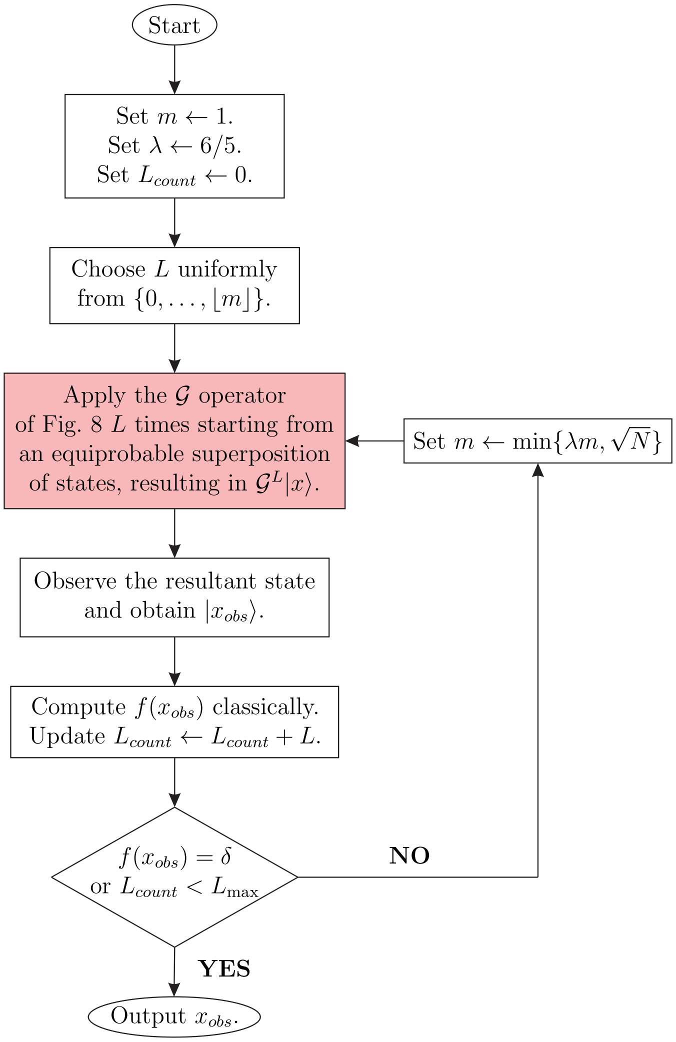

Start
Set $m \leftarrow 1$.
Set $\lambda \leftarrow 6/5$.
Set $L_{count} \leftarrow 0$.
Choose L uniformly from $\{0, \ldots, \lfloor m \rfloor\}$.
Apply the $\mathcal{G}$ operator of Fig. 8 L times starting from an equiprobable superposition of states, resulting in $\mathcal{G}^L|x\rangle$.
Set $m \leftarrow \min\{\lambda m, \sqrt{N}\}$
Observe the resultant state and obtain $|x_{obs}\rangle$.
Compute $f(x_{obs})$ classically.
Update $L_{count} \leftarrow L_{count} + L$.
$f(x_{obs}) = \delta$ or $L_{count} < L_{\max}$
NO
YES
Output x_{obs}.

Fig. 10: Flowchart of the BBHT QSA. The colored box represents the operation of Grover's QSA's quantum circuit of Fig. 8, while the rest of the steps are performed in the classical domain. The value of λ remains constant throughout the operation, while m is always initialized to 1. When the maximum number of allowed iterations $L_{\max}$ is at least $4.5\sqrt{N}$, there is a $\approx 100\%$ probability of success.

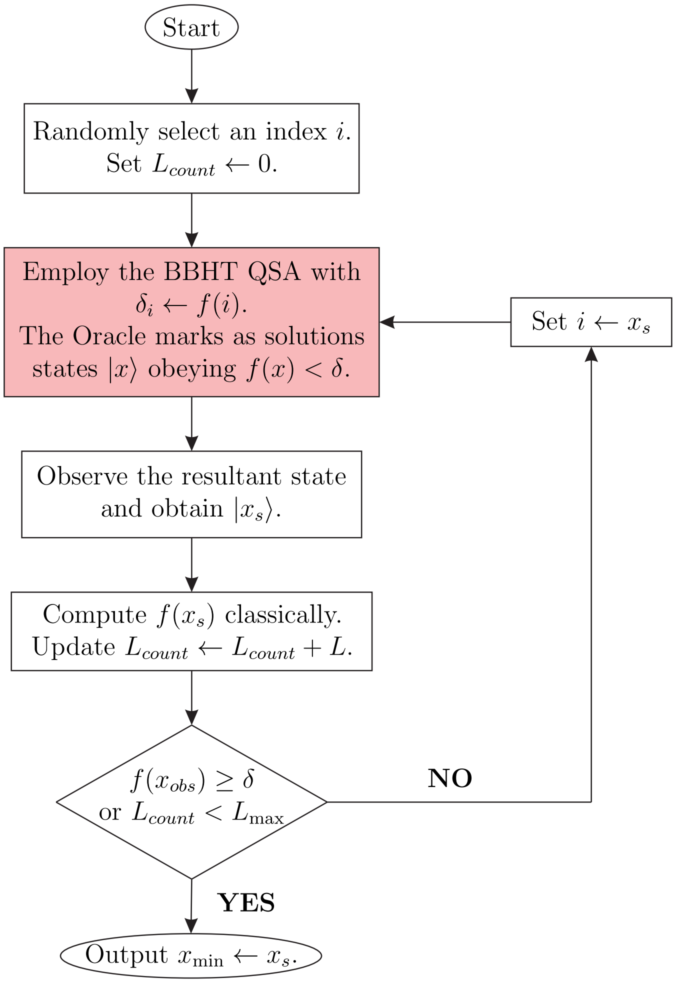

Start
Randomly select an index i.
Set $L_{count} \leftarrow 0$.
Employ the BBHT QSA with $\delta_i \leftarrow f(i)$.
The Oracle marks as solutions states $|x\rangle$ obeying $f(x) < \delta$.
Set $i \leftarrow x_s$
Observe the resultant state and obtain $|x_s\rangle$.
Compute $f(x_s)$ classically.
Update $L_{count} \leftarrow L_{count} + L$.
$f(x_{obs}) \geq \delta$ or $L_{count} < L_{\max}$
NO
YES
Output $x_{\min} \leftarrow x_s$.

Fig. 11: Flowchart of the DH QSA. The colored box represents the operation of Grover's QSA's quantum circuit of Fig. 8, while the rest of the steps are performed in the classical domain. The randomly selected index i at the beginning of the algorithm may be replaced by a deterministically selected index, if there is knowledge that specific indices are favoured to correspond to low-valued entries. The maximum number of applications of Grover's operator is $L_{\max} = 22.5\sqrt{N}$.

(BBHT) QSA, which is applicable in the specific scenario, where the actual number S of valid solutions is unknown, whilst imposing the same order of complexity as Grover's QSA, namely $O(\sqrt{N})$ in a database having N entries. The BBHT QSA solves the same problem as Grover's QSA, while assuming less knowledge about the database. Therefore, it may be employed in a higher number of engineering problems, where no information is available about the entries of the database. Since the number of solutions S is unknown, we are unable to find the optimal number of Grover iterations L_{opt} that we should apply to the initial equiprobable superposition of states in Fig. 8. Hence, it employs classical processing and a "trial-and-error" approach for finding L_{opt}, proven to eventually lead to a 100% probability of success in [31]. The flowchart of the BBHT QSA is depicted in Fig. 10, where $\lambda = 6/5$ is a constant that should be chosen to be in the range $[6/5, 4/3]$ [31]. If the BBHT QSA is not terminated after $4.5\sqrt{N}$ applications of Grover's operator, we may conclude that there is no solution for this search problem.

8) Dürr-Høyer Quantum Search Algorithm: A quantum search algorithm that solves a different search problem was conceived by Dürr and Høyer [32]. More specifically, the Dürr-Høyer (DH) QSA is employed for identifying the extreme values of an unsorted database having N entries, while imposing a low complexity, which is on the order of $O(\sqrt{N})$. In this problem, either the minimum or the maximum entry of a database is sought, without knowing the specific value of that minimum or maximum entry. Therefore, the sought value δ is unknown. Let us describe the problem, when the minimum entry of the database is desired, without any loss of generality, as described in the flowchart of Fig. 11. The DH QSA starts by randomly picking one of the N entries in the database. Let us assume that the randomly selected entry has a value δ_i and an index i. It then invokes the BBHT QSA for finding any entry that has a lower value than the randomly picked one. Since there is no knowledge about the database, it is not possible to know how many entries have a value lower than δ_i, therefore only the BBHT QSA can be used. If we somehow were aware of the number of entries that have a value lower than δ_i, then Grover's QSA could also be used. Once an entry with a lower value than δ_i is found, corresponding to the index x_s and hence $f(x_s) < \delta_i$, we update the value δ_i with the newly found entry's value $\delta_i = f(x_s)$. Then another BBHT QSA iteration is employed for finding an entry that has a lower value than the updated δ_i. This process is repeated until no better value is found.

Since the DH QSA uses the BBHT QSA, its minimum complexity is equal to $4.5\sqrt{N}$ Grover iterations, referring to the case, where the initially selected entry δ_i was indeed the minimum entry in the database. That would result in the BBHT QSA not being able to find an entry with a lower value, causing it to terminate after $4.5\sqrt{N}$ applications of Grover's operator. The maximum number of Grover iterations required for finding the minimum of the database was proven by Dürr and Høyer to be equal to $22.5\sqrt{N}$ Grover iterations [32]. In [62] it was shown that if the initial entry is carefully chosen instead of being randomly chosen, the average complexity of the DH QSA is further reduced. At the same time, if offline statistics are available about the database of the specific engineering problem, a one-to-one relationship between the number of Grover iterations used and the success probability may be found [62].

9) Quantum Counting Algorithm: In 2000, Brassard, Høyer and Tapp proposed the Quantum Counting Algorithm (QCA) [50], by combining Grover's QSA [28] and the QPEA [48]. The problem that is solved by using the QCA is the search for the number of solutions S in a search problem. Given a database having N entries, we are interested in finding how many times a known value δ appears in the database, without aiming to find its position in the database. In order to achieve this, the controlled-U_f gates of Fig. 7 are replaced by controlled-Grover operators. Explicitly, the Grover operators of Fig. 8, are used in the quantum circuit of Fig. 12. Furthermore, the function register consists of $n = \log_2 N$ qubits initialized in an equiprobable superposition of $2^n = N$ states. The eigenvector of Grover's QSA consists of a superposition of the specific states that do correspond to solutions in the database and a superposition of the states that do not correspond to solutions in the database. By creating an equiprobable superposition of all states at the beginning of the circuit, we essentially feed the controlled-Grover operators with their eigenvector. Therefore, an application of Grover's operator to such a superimposed state will result in a rotation of their amplitudes [50]. The rotation angle depends on the ratio between the number of solutions S and the size of the database N. Therefore, by applying the QPEA using Grover's QSA, the QCA obtains the number of solutions S upon observing the control register at the output of the QFT seen in Fig. 12, followed by classical processing.

The QCA's accuracy depends on both the number of qubits in the control register c. Its complexity depends on both the number of qubits in the control register c and in the function register n. In other words, the complexity to be invested depends on the required accuracy in terms of the number of solutions, as well as on the size of the database. Again, the optimal classical algorithm is the full search, since all entries in the unsorted database should be checked in order to count the number of solutions. This results in a complexity on the order of $O(N)$ for the full search. The QCA achieves a quadratic speedup compared to the full search, with the specific complexity required depending on both the estimation error margin and on the size of the database [50].

10) Quantum Heuristic Algorithm: In 2000, Hogg proposed a Quantum Heuristic Algorithm (QHA) [51], [52], which relies on Grover's QSA's circuit. The aim of the QHA is to solve the particular optimization problem of finding either the minimum or the maximum of a database by requiring fewer CFEs than the DH QSA, when the database has some form of correlation. In more detail, Grover's QSA, the BBHT QSA and the DH QSA are optimal, when they perform search in an unsorted database. When the entries of a database are inherently correlated to each other, heuristic algorithms may succeed in solving the optimization problem, while requiring fewer queries to the database. In order to achieve this, Hogg changed both the Oracle and the diffusion operator used in Grover's QSA. Recall that in Grover's QSA, where δ is known, the Oracle marks the quantum states that correspond to solutions by flipping the sign of their amplitudes. This may be interpreted as a rotation by π for the amplitudes of the solution states and no rotation for the rest of the states. Since in the optimization problem the minimum value δ is unknown, Hogg conceived a different Oracle, where the rotation angle of the amplitudes of *each* state depends on the value of the entry it corresponds to. The QHA has been demonstrated to outperform Grover's QSA [51], but it needs fine-tuning for each specific system and scenario, since the exact rotation angles applied by the Oracle and the diffusion operator have to be appropriately chosen. This is reminiscent of the employment of classical heuristic algorithms, like the Genetic Algorithm (GA) [63], [64], where the algorithm's parameters have to be carefully selected in order for a heuristic algorithm to converge to the solution.

11) Quantum Genetic Algorithm: In order to solve the same optimization problem of finding either the minimum or maximum of a database, Malossini *et al.* proposed the Quantum Genetic Algorithm (QGA) [53], which is an amalgam of the classical GA [63], [64] and of the DH QSA. Please note that as with the QHA, the QGA may be employed in particular problems, where there is correlation between the entries of the database.

More specifically, in the classical GA, a population of P *agents* or *chromosomes* is generated, where each agent represents an index of the database. The database is then queried P times, once for each of the agents of the population. After combining the two best so-far found[16] agents, the next generation of the population is created based on them, with

[16] By "best so-far found" we refer to the agents that correspond to the smallest entries in the database in that population.

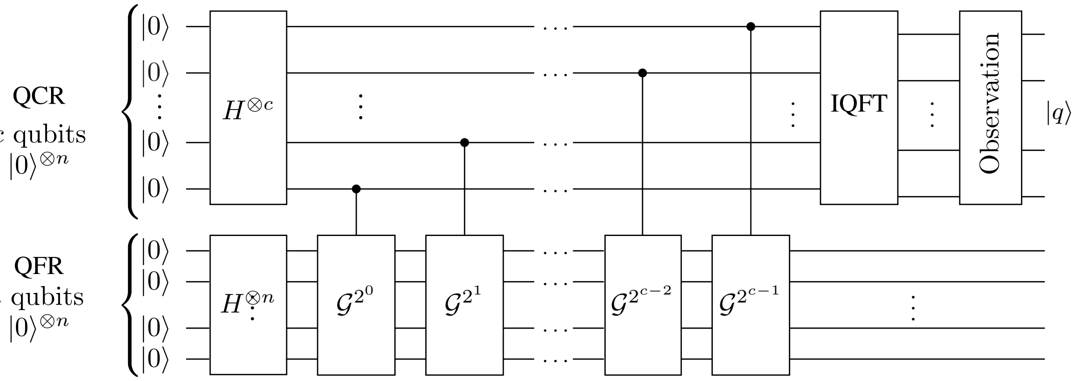


Fig. 12: The quantum circuit of the Quantum Counting Algorithm [34]. It employs the quantum circuit of the QPEA shown in 7, where the U operator is the Grover operator $\mathcal{G}$ and the quantum function register is initialized to an equiprobable superposition of all states, which represents the eigenvector of Grover's operator.

the aim of having agents representing even smaller values. Eventually, after a sufficiently high number of generations, an agent corresponding to the minimum value of the database is found. Since it cannot be mathematically predicted, when the GA will find the minimum of the database, the algorithm is terminated after a predetermined number of generations.

In the QGA, the same procedure is followed as in the GA with one difference. The DH QSA is invoked for searching through the population of each generation for finding the best agents. In other words, the DHA QSA in the QGA is employed for reducing the complexity imposed by the GA while querying the database during each generation. Since only the two best agents have to be found in order to create the subsequent generation's population, the DH QSA may be employed twice. The QGA was demonstrated to outperform the GA for the same complexity, or to require a lower complexity for the same success probability.

12) Harrow-Hassidim-Lloyd Algorithm: The Harrow-Hassidim-Lloyd (HHL) algorithm [54] is a quantum algorithm, which relies on the QPEA and solves linear systems of equations at an exponential reduction of the computational complexity required. The problem of solving a linear system of equations may be formulated as follows. Given an $(N \times N)$-element matrix $\mathbf{A}$ and an $(N \times 1)$-element vector $\mathbf{b}$, find an $(N \times 1)$-element vector $\mathbf{x}$, so that we have $\mathbf{A} \cdot \mathbf{x} = \mathbf{b}$.

In order for the HHL algorithm to be practically applicable, the goal of the problem should be a bit different from the aforementioned one. The linear system of equations has to exhibit a few specific features. Firstly, the output is a superposition of N states $|x\rangle$, where the values of the solution vector are encoded in the amplitudes of that superposition of states. Therefore, it cannot provide all values of the solution vector $\mathbf{x}$ for further classical processing. Alternatively, it may result in specific properties for the solution vector, for example for its moments. Moreover, both the solution vector $\overrightarrow{\mathbf{x}}$ and the vector $\overrightarrow{\mathbf{b}}$ should be unit-vectors. Furthermore, the matrix $\mathbf{A}$ should be sparse.

The HHL algorithm estimates the eigenvalues of the matrix $\mathbf{A}$, using an appropriately modified version of the QPEA of Section II-B5. The QPEA circuit is employed as a subroutine of an amplitude amplification procedure in the HHL algorithm, in order to further reduce its complexity of obtaining the solution quantum state $|x\rangle$. The HHL algorithm's complexity was further reduced by Ambainis in [67], while the precision of the estimated solution was exponentially increased by Childs in [68].

13) Quantum Mean Algorithm: In 2011, Brassard *et al.* proposed the Quantum Mean Algorithm (QMA) [55], which succeeds in finding the mean value $a = \sum_{x=0}^{N} f(x)/N$ of a function f requiring an exponentially reduced number of evaluations of the function than the optimal classical algorithm, since the latter would require access to all legitimate evaluations of the function. In order to achieve this, a modified QPEA is used, where the controlled-U_f operation evaluates the output of the function f to its inputs, as illustrated in Fig. 13. One of the main differences between the QMA and the QPEA is that even though there are N legitimate inputs for the function f, $\log_2(N)+1 = n+1$ qubits are employed in the function register, instead of $n = \log_2(N)$, which would have been the case in the QPEA. The above-mentioned extra qubit is required, because the function register is initialized using a unitary operator A, which relies on the function f and it performs controlled-rotations on the extra qubit [55], [56]. At the output of the unitary operator A, there is a superposition of states $|\Psi\rangle$. Each state of Ψ was used for evaluating U_f in the unitary operator A. Based on the U_f and the controlled-rotations imposed on the auxiliary qubit, the amplitudes of half of the states in $|\Psi\rangle$ are equal to their respective function's output. In fact, this is true for the specific states, for which the auxiliary qubit is equal to $|1\rangle$. The size of the control register determines the precision of the estimated mean value, similarly to the QPEA.

14) Quantum Weighted Sum Algorithm: The Quantum Weighted Sum Algorithm (QWSA) [56], [69] is based on the QMA of Section II-B13 and it finds the weighted sum of the values of a function f with N inputs, again requiring $O(\sqrt{N})$ evaluations of the function f. The difference between the QWSA and the QMA is the initialization of the function register, as seen in Fig. 14. Instead of initializing it in an

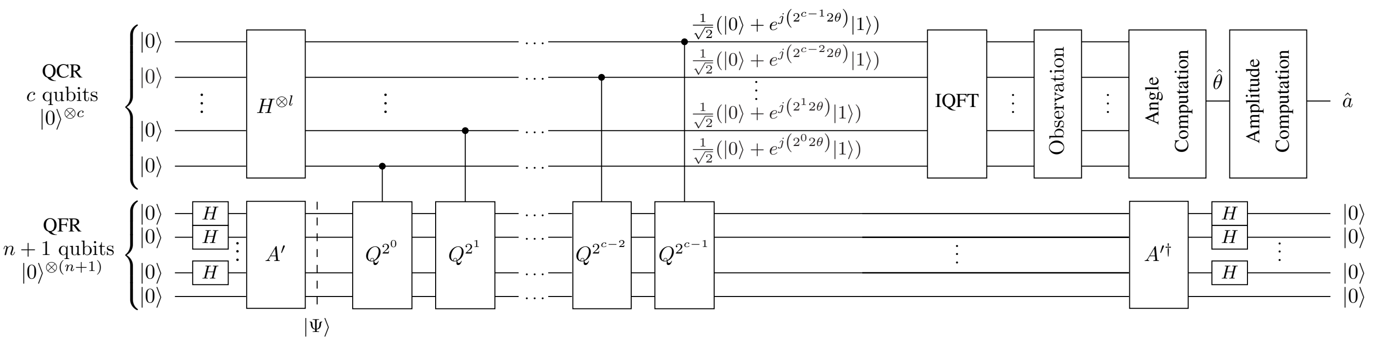

QCR
c qubits
$|0\rangle^{\otimes c}$
$|0\rangle$
$H^{\otimes l}$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{c-1}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{c-2}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{1}2\theta)}|1\rangle)$
$\frac{1}{\sqrt{2}}(|0\rangle + e^{j(2^{0}2\theta)}|1\rangle)$
IQFT
Observation
Angle Computation
$\hat{\theta}$
Amplitude Computation
$\hat{a}$
QFR
$n+1$ qubits
$|0\rangle^{\otimes(n+1)}$
H
A'
Q^{2^0}
Q^{2^1}
$Q^{2^{c-2}}$
$Q^{2^{c-1}}$
$A'^{\dagger}$
$|\Psi\rangle$

Fig. 13: The quantum circuit of the Quantum Mean Algorithm [55]. It employs the quantum circuit of the QPEA shown in 7, where the U operator is the function's operator $U_f = f(x)$. The quantum function register is initialized to the superposition of states $|\Psi\rangle$, using n Hadamard gates and the operator A, which includes two operations of U_f and a controlled rotation of the $(n+1)$th auxiliary qubit. The circuit estimates the mean value of the function's values $a = \sum_{x=0}^{N} f(x)/N$.

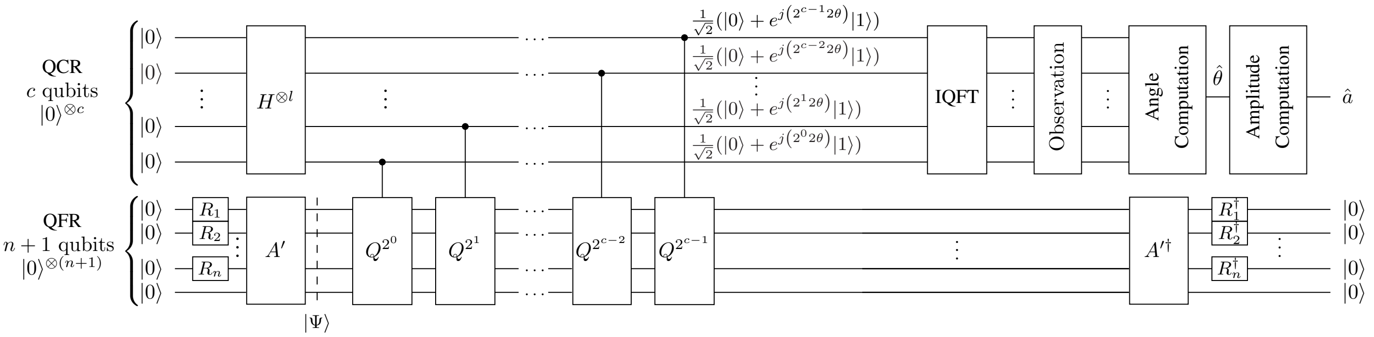


Fig. 14: The quantum circuit of the Quantum Weighted Sum Algorithm [56]. It employs the quantum circuit of the QMA shown in 13, with the difference that the quantum function register is not equiprobably initiliazed. Rather, the initilization is performed based on unitary rotation gates, which rely on the weights of the desired weighted sum.

equiprobable superposition of states, the inputs of the function f are initializated in a superposition of states, where each state's amplitude is the weight of the wanted weighted sum. Therefore, the QWSA may be considered as a generalization of the QMA, since in the latter all weights are the same and equal to $1/N$ in an N-element database, resulting in the use of Hadamard gates instead of general unitary rotation gates, as shown in Fig. 13.

Last but not least, an overview of the quantum algorithms discussed in this survey in terms of their application and complexity is carried out in Tables III and IV. In terms of practical implementation, *IBM Q Experience* has a *drag and drop editor* for the sake of synthesizing quantum circuits out of the fundamental quantum gates of Fig. 4 as well as a *Python toolkit*[17] for designing more complex quantum circuits. Consequently, Grover operator's quantum circuit, presented in Fig. 8, may be readily implemented using IBM's framework at least for a limited number of qubits. Nevertheless, we should state that at the time of writing, there has not yet been any real-life demonstration of employing a quantum-assisted solution in order to solve a practical wireless problem. Therefore, the comparisons between the classical and the quantum solutions employed in the wireless communication problems in the following section are based on the theoretical capabilities of the algorithms.

III. Optimization Problems and Quantum Algorithms in Communications

Let us now shift our attention to discussing potential applications in the field of wireless communications, which would benefit from using a quantum computer. Most of these optimization problems in the current state-of-the-art employ algorithms for finding suboptimal solutions, because of the excessive cost of finding an optimal solution. This is particularly so for joint optimization of several functions, such as joint channel estimation, data detection and synchronization for example, or for multi-component optimization, where the search space is expanded.

A. Multi-User Detection

1) The Problem: In the uplink of an OMA system, like Code Division Multiple Access (CDMA) [70], Orthogonal Frequency Division Multiple Access (OFDMA) [71], Single-Carrier Frequency Division Multiple Access (SC-FDMA) or Time Division Multiple Access (TDMA), the users are either allocated all available resources in a round-robin fashion, or they are allowed to share orthogonal resources simultaneously. For example, in TDMA the whole bandwidth is allocated to a single user for a few time slots. On the other hand, in CDMA

[17] https://developer.ibm.com/code/open/projects/qiskit/

TABLE III: The Quantum Algorithms Reviewed

Algorithm	Application	Description	Complexity
Deutsch Algorithm [45]	Classification	Determines whether a binary function $f : \{0,1\} \to \{0,1\}$ does or does not have a one-to-one mapping.	$O(1)$
Deutsch-Jozsa Algorithm [46]	Classification	Determines whether a function $f : \{0,1\}^n \to \{0,1\}$ is balanced or constant.	$O(1)$
Simon's Algorithm [47]	Evaluates a Function's Property	Operates on functions $f : \{0,1\}^n \to \{0,1\}^n$ that satisfy $f(x) = f(y)$ if and only if $x = y$ or if $x \oplus y = s$, and finds the value s.	$O(n)$
Shor's Algorithm [33]	Factoring	Solves the problem of factoring a given integer N.	$O(\log N)$
Quantum Phase Estimation Algorithm [48]	Order finding, Factoring, Search	Estimates the eigenvalue of a given unitary operator with the aid of c control qubits, which define the estimation precision. The complexity depends on whether that unitary operator is less or more complex than the IFFT operator employed.	$O(2^c)$
Grover's Algorithm [28]	Search	Finds the index of an entry in a database of size N that is equal to δ with $\sim$100% probability of success. The number of times that δ appears in the database has to be known *a priori*.	$O\left(\sqrt{N}\right)$
Boyer-Brassard-Høyer-Tapp (BBHT) Algorithm [31]	Search	Finds the index of an entry in a database of size N that is equal to δ with $\sim$100% probability of success. The number of times that δ appears in the database is not required to be known *a priori*.	$O\left(\sqrt{N}\right)$, but higher than Grover's QSA
Dürr-Høyer Algorithm [32]	Search	Finds the index of the minimum entry in a database of size N with $\sim$100% probability of success. Only the size of the database is required to be known *a priori*.	$O\left(\sqrt{N}\right)$, but higher than BBHT's QSA
Quantum Counting Algorithm [50]	Search	Estimates the number of times a known value δ appears in a database of size N, with the aid of c control qubits. The complexity depends on whether the employed Grover operator is less or more complex than the employed IFFT operator.	$O(2^c)$
Quantum Heuristic Algorithm [51]	Search	Finds the index of an entry in a database of size $N = 2^n$ that is equal to δ using a heuristic approach of Grover's QSA.	$O\left(e^{-\frac{3n}{4}+\frac{\ln n}{4}}\right)$

the whole bandwidth is used by all users supported in the system simultaneously, in order to transmit their narrowband signal after spreading it by a unique user-specific, orthogonal spreading code. In OFDMA, where the spectrum is partitioned in multiple orthogonal subcarriers, each user may be allocated a subset of user-specific subcarriers, which no other user is allowed to activate.

By contrast, in the uplink of a NOMA system [5], [72]–[76] the users are allowed to simultaneously share the same frequency and time resources in order to increase the cell throughput by being able to support more users simultaneously. However, the BS now has the new task of extracting the signal of each user from the received superposition of

TABLE IV: The Quantum Algorithms Reviewed (continued)

Algorithm	Application	Description	Complexity
Quantum Genetic Algorithm [53]	Search	Finds the index of an entry in a database of size $N = 2^n$ that is equal to δ using an amalgam of the DH algorithm and the classical genetic algorithm.	User-defined
Harrow-Hassidim-Lloyd Algorithm [54]	Solving Linear Systems of Equations	Solves llinear systems of equations $Ax = b$, with κ being the ratio of the largest over the lowest eigenvalue of the sparse matrix A and N the dimension of A, with the aid of the phase estimation algorithm. The estimated solution cannot be readily obtained classically, but rather further manipulation may be performed in the quantum domain in order to extract the desired properties of the solution.	$O\left(\kappa^2 \log N\right)$
Quantum Mean Algorithm [55]	Function's Moment Finding	Estimates the mean value a function f over its argument space of size N, with the aid of c control qubits, which determine the estimation's precision.	$O\left(\sqrt{N} c \log c\right)$
Quantum Weighted Sum Algorithm [56]	Function's General Moment Finding	Estimates the weighted sum of the outputs of a function f over its argument space of size N, with the aid of c control qubits, which determine the estimation's precision.	$O\left(\sqrt{N} c \log c\right)$
Non-dominated Quantum Optimization [65]	Search & Solving Non-Linear Systems of Inequalities	Finds the entire set of Pareto-optimal solutions in a database of N entries.	$O\left(N\sqrt{N}\right)$
Non-dominated Quantum Iterative Optimization [66]	Search & Solving Non-Linear Systems of Inequalities	Finds N_{OPF} Pareto-optimal solutions in a database of N entries.	$O\left(N_{\text{OPF}}\sqrt{N}\right)$

signals[18], as illustrated in Fig. 15, given the knowledge of the channel states and the symbol constellation that was used by each user. In more detail, each user transmits its own symbol based on its constellation. Since the system is synchronous, every transmitted signal is added together at each receive antenna. Each transmitted signal is modified based on the channel it utilizes. At the receiver, Additive White Gaussian Noise (AWGN) is added at each receive RF chain. The Multi-User Detector has to estimate the three transmitted symbols based on the received signals, the channel states, the noise power and any prior estimates that may be available. This extraction is also currently required in the uplink of the specific CDMA systems, where non-orthogonal spreading codes have been allocated to the users [70]. This is termed as the problem of Multi-User Detection (MUD).

2) The Classical Algorithms: The optimal Maximum Likelihood (ML) detector finds the most likely U-user symbol vector, relying on the received signal, on the estimates of the channels and on the estimated noise power. More specifically, the ML MUD searches through all legitimate transmitted multi-user symbol combinations that may have resulted in the reception of that specific signal and in the end outputs the most likely U-user symbol vector. As an example, let us assume that $U = 20$ users are supported by the system and that each of them transmits $L = 4$-ary Quadrature Phase Shift Keying (QPSK) symbols. Then, the signal received at the BS has been constructed based on only one out of $L^U = 4^{20}$ possible combinations. In other words, the ML MUD has to search through more than one *trillion* legitimate U-symbol vectors in order to find the most likely one. In general, the computational complexity of the ML MUD is on the order of $O(L^U)$. In an OMA system, where a received signal conveys the information of a single user, the ML MUD may have an affordable complexity, which is on the order of $O(L)$.

Next-generation wireless communication systems may employ iterative receivers in the uplink of a NOMA system. In iterative receivers, information is allowed to be exchanged between the MUD and the channel decoders[19]. In this case, an MUD that outputs soft information and also accepts soft

[18] Please note that the mentioned superposition of signals is their addition in the classical domain, since in a synchronous system the signals arrive simultaneously. It should not be confused with the superposition of quantum states.

[19] Since each of the U users has encoded its own bit information stream independently, the BS has to employ U channel decoders in parallel.

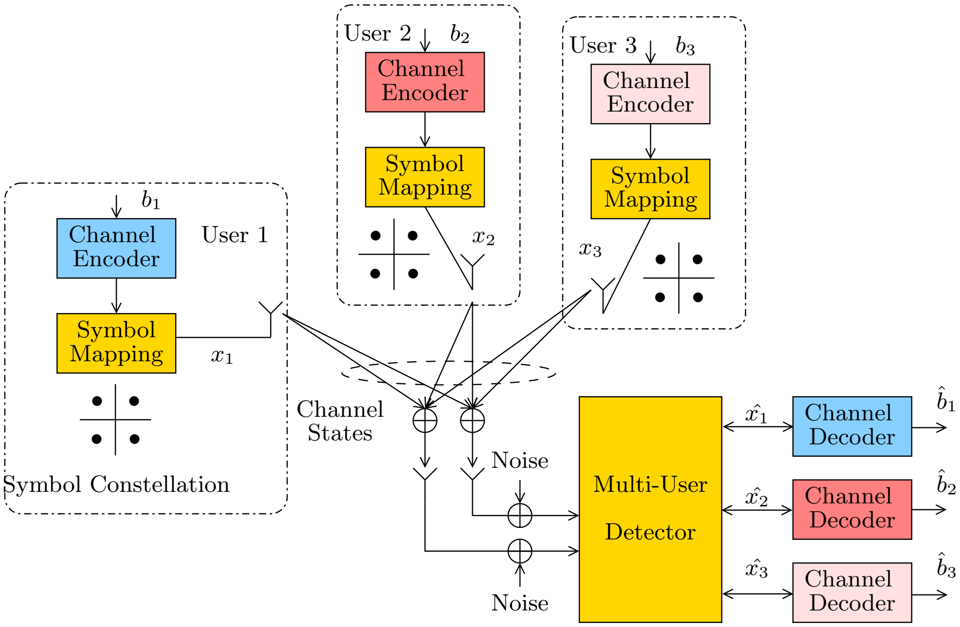


Fig. 15: The problem of Multi-User Detection in the uplink of a synchronous multiple access system.

estimates as input should be used. The optimal Soft-Input Soft-Output (SISO) MUD is the Maximum *A posteriori* Probability (MAP) MUD [6], which outputs bit-based or symbol-based Log-Likelihood Ratios (LLR). The LLR of a bit represents the log-domain probability of that bit to have been 0 or 1, when it was transmitted. Similarly, the symbol LLR describes the log-domain probability of that symbol to have been transmitted as one of the legitimate symbols in the constellation. The MAP MUD creates the LLRs by taking into account all possible multi-level symbol vectors, requiring a computational complexity on the same order as the ML MUD [6].

The excessive complexity required by the ML and MAP MUDs in NOMA systems has driven the research community to low-complexity sub-optimal solutions, such as the Minimum Mean Square Error (MMSE) detector [70], the Zero Forcing (ZF) detectors [70], the Ant Colony Optimization (ACO) based MUD [77], the Particle Swarm Optimization (PSO) based MUD [78] and the SIC [70] MUD.

In the uplink of a multi-user system, the SIC MUD detects the signal of the user experiencing the best channel first, by treating as interference the signals of the rest of the users, which are also present in the superimposed received signal. Having detected the signal of the best user, it reconstructs that user's noiseless transmitted signal and subtracts it from the received signal. Therefore, only the transmitted signals of $(U-1)$ users are left in the composite received signal. The same procedure is repeated until the signals of all users are detected. The SIC MUD requires a low complexity on the order of $O(L\cdot U)$, which scales linearly with the number of users supported. However, it does not perform well in rank-deficient scenarios and when the channel conditions of different users are similar. In the latter case Parallel Interference Cancellation (PIC) is preferred [70]. Therefore, when SIC is employed, appropriate scheduling is required for matching groups of users together in order to share the medium simultaneously.

3) The Quantum Algorithms: In order to reduce the computational complexity of the optimal ML detection, which requires a full search, the DH QSA of Section II-B8 was employed in [56], [62], where it was demonstrated that it approaches the optimal performance. The operation of the DH QSA in the problem of MUD is described in Fig. 16. The DHA employed in the QMUDs makes multiple calls to the BBHT QSA. Grover's QSA is not used, but it is included for completeness, since the BBHT QSA uses the same Oracle O, but may even be capable of finding a solution with a $\sim$100% probability, when the number of solutions is unknown. The QMUD may also be performed on a subcarrier basis in a multi-carrier system. The DHA processes the signals received $\mathbf{y}_q$ at all the receive AEs on the qth subcarrier, along with the channel state estimates $\mathbf{H}_q$, the noise's variance N_0 and the *a priori* LLRs $L_{m,apr}(\hat{\mathbf{b}})$. After it completes its initial procedure, the DHA exchanges information with a classical processing unit, which determines whether the DHA should or should not be called again, while additionally determining its search space. Finally, the QMUD outputs the calculated *a posteriori* LLRs $L_{m,apo}(\hat{\mathbf{b}})$.

In [62], a deterministic initialization of the DH QSA was proposed for exploiting the low-complexity Zero Forcing (ZF) and Minimum Mean Square Error (MMSE) [79] detectors. More specifically, instead of randomly initializing the DH QSA, initially a ZF or MMSE detector is employed and its output is used as the initial guess of the DH QSA. This was shown to further reduce the complexity of the QMUD. Moreover, an early-stopping criterion was proposed in [62], where the DH QSA is terminated after a specific number of Grover iterations, without degrading the Bit Error Rate (BER) performance of the system. The specific number of Grover iterations used for the early-stopping criterion was found via simulations and histograms.

When iterative detection is employed at the base station, a

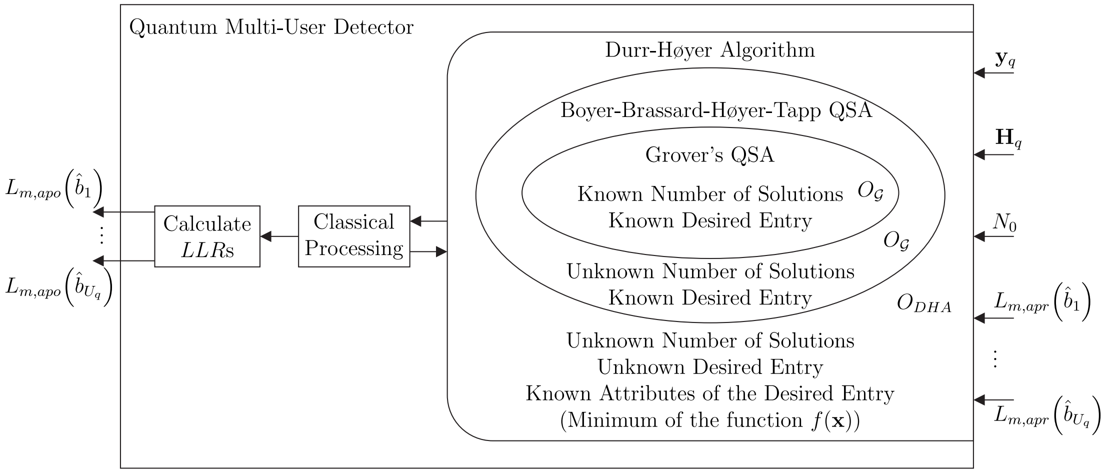

Quantum Multi-User Detector
Durr-Høyer Algorithm
Boyer-Brassard-Høyer-Tapp QSA
Grover's QSA
Known Number of Solutions
Known Desired Entry
$O_{\mathcal{G}}$
$O_{\mathcal{G}}$
Unknown Number of Solutions
Known Desired Entry
O_{DHA}
Unknown Number of Solutions
Unknown Desired Entry
Known Attributes of the Desired Entry
(Minimum of the function $f(\mathbf{x})$)
Classical Processing
Calculate LLRs
$L_{m,apo}\left(\hat{b}_1\right)$
$L_{m,apo}\left(\hat{b}_{U_q}\right)$
$\mathbf{y}_q$
$\mathbf{H}_q$
N_0
$L_{m,apr}\left(\hat{b}_1\right)$
$L_{m,apr}\left(\hat{b}_{U_q}\right)$

Fig. 16: Inside a quantum multi-user detector.

SISO MUD should be used in order to exchange LLRs with the SISO decoders. Therefore, the DH QSA-based hard-output QMUD is not suitable. In [56], [80], a SISO QMUD was proposed based on the QWSA of Section II-B14, exhibiting near-optimal performance, while requiring fewer CFEs[20] (CFE) than the MAP MUD. In order to calculate an LLR, two weighted sums have to be calculated; one for the LLR's numerator and one for its denominator. The MAP MUD evaluates the Cost Function (CF) for all legitimate multi-level symbols. By using the QWSA twice, we may estimate the weighted sums requiring a lower computational complexity. Please note that there is a performance vs. complexity trade-off, when using the QWSA, due to the control register of the QPEA of Section II-B5. In other words, if we employ more qubits at the control register, a higher precision is achieved during the estimation of the weighted sums, hence resulting in a more accurate LLR value. However, a higher complexity is required, since the complexity of the QWSA scales with the size of the control register [56].

In [80], [81] another SISO QMUD was proposed, relying on an amalgamation of classical processing and the DH QSA. The SISO QMUD was demonstrated to achieve near-optimal performance with respect to the MAP MUD, while requiring substantially fewer CFEs. The DH QSA-based SISO QMUD employs the DH QSA multiple times in different databases, in order to create a pool of the "k-best"[21] multi-level symbols of each weighted sum of each LLR. By classically processing the values found, we are able to estimate the weighted sums of the LLRs and hence to attain a near-optimal performance. Please note that even though the precision of the weighted sums, and hence the LLRs, is lower than that achieved by the QWSA QMUD and the MAP MUD, it is sufficiently close to the real values for the channel decoders to successfuly decode each user's bits. Therefore, since a SISO MUD or QMUD is always followed by channel decoders, the DH QSA-based QMUD of [81] achieves a near-optimal performance, while imposing a lower complexity than the MAP MUD.

B. Joint Channel Estimation and Data Detection

1) The Problem: In the uplink of wireless communications system, accurate channel estimation has to be performed at the base station in order to predict and counteract the effect of the channel, when the signal arrives [79], [82], [83]. In a multi-user NOMA system, all channels between the antennas of all users and the antennas of the base station have to be accurately estimated, otherwise the performance of the MUD would be degraded.

In a multi-carrier system like OFDM, the multi-path channel may be estimated either in the time domain or in the frequency domain. For example, let us assume the scenario where the Power Delay Profile (PDP) of a channel exhibits four paths and that we partition the available bandwidth in 512 non-dispersive subchannels. The channel envelope of each of the four paths may be deemed to fade independently. Assuming that the channel envelope at each path is quasi-static[22] during the channel estimation process, we may either estimate the four time-domain (TD) channel gains of the four paths, or the 512 frequency-domain (FD) subcarrier gains, which represent the Fast Fourier Transform (FFT) of the time-domain PDP, having taken the delay spread of the channel and the sampling frequency into consideration. Typically the FD channel is represented by the terminology of FD CHannel Transfer Function factor (FD-CHTF) [71]. Naturally, a lower complexity may be required for estimating the four time-domain channel gains, than for estimating the channel gain of each subcarrier.

However, the FD channel estimation lends itself to joint channel and data estimation, where the FD channel estimation problem may be thought of as a search for the true continuous-valued subcarrier channel gains. This prohibits the employment of the full search approach, which was previously followed in the MUD problem of Section III-A, since

[20] The cost function in the MUD problem is the Euclidean distance of the received, noisy multi-level symbol from a legitimate multi-level symbol from the multi-user constellation.

[21] By "best" here we mean the multi-level symbols of each weighted sum that correspond to the highest CF values.

[22] In an OFDM system, a channel is quasi-static, when its channel gain remains constant during an OFDM symbol period. The channel gain between two OFDM symbols may be different, but still constant within their OFDM symbols.

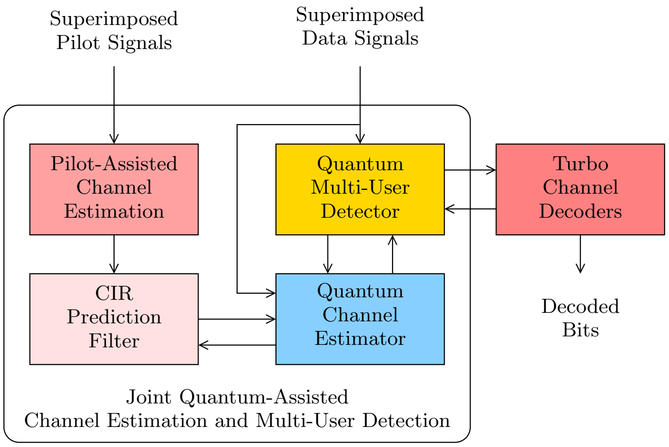

Superimposed Pilot Signals
Superimposed Data Signals
Pilot-Assisted Channel Estimation
Quantum Multi-User Detector
Turbo Channel Decoders
CIR Prediction Filter
Quantum Channel Estimator
Decoded Bits
Joint Quantum-Assisted Channel Estimation and Multi-User Detection

Fig. 17: System model of a joint channel estimation and multi-user detection receiver in the uplink of a multi-carrier NOMA system employing decision-directed channel estimation.

an infinite-sized database should be constructed. The joint channel estimation and data detection problem may however also be considered as two separate problems, the former being dedicated to searching for continuous-valued channel gains, while the latter to searching for discrete-valued multi-user symbols.

2) The Classical Algorithms: In LTE [84], FD pilot signals are transmitted on specific subcarriers of certain OFDM symbols, enabling the user or the base station to estimate the channels for the rest of the subcarriers with the aid of interpolation in the downlink or uplink, respectively. The estimated channel states may be used for the subsequent OFDM information symbols between a pair of OFDM symbols having pilot-subcarriers without any change at the cost of accepting a performance degradation, but not imposing any additional complexity. Alternatively, the estimated subcarrier gain may be used for predicting the subcarrier gains of each subsequent OFDM symbol using linear predictions.

Furthermore, as alluded to above, channel estimation may be combined with data detection for improving both the estimation accuracy of the subcarrier gains and of the detection error probability of the transmitted data, resulting in a joint channel estimator and data detector [85]–[88]. In a multi-user scenario, the MUD replaces the single-usedr symbol detector, hence joint channel estimation and MUD may be used [89]–[93]. In the iterative receiver of a NOMA system, information may be exchanged between the channel estimator, the MUD and the channel decoders for further increasing the channel estimation's accuracy and the channel decoding performance [90]. The Decision-Directed Channel Estimation (DDCE) [94] used in multi-carrier systems initially estimates the FD channel gains based on a pilot OFDM symbol, as depicted in Fig. 17. Initially, the super-imposed pilot signals are used for performing conventional, pilot-assisted channel estimation, associated with the received OFDM symbol period. Based on those channel estimates, the Channel Impulse Response (CIR) prediction filter predicts the channel states that would correspond to the next OFDM symbol, which now carries data. The output of the CIR prediction filter becomes the initial output of the quantum channel estimator. When the next OFDM symbol is received, it invokes the MUD using the predicted channel gains.

It then selects the specific multi-level symbols, which were detected sufficiently reliably[23], and assumes that these were known pilot symbols. Hence it refines the channel estimation process based on those "hypothesized" pilot symbols. In other words, the DDCE combines the separate problems of channel estimation and data detection by employing them sequentially, allowing them to "lend" their output to the other process, in order for it to perform a search in a more accurately constructed database, as exemplified in Fig. 17. The updated FD channel gains may be used for performing a refined MUD process for the same OFDM symbol for improving the estimated LLRs. Similarly, the updated LLRs can be used aftewards for improving the accuracy of the FD channel gains even further. The number of iterations between the channel estimation process and the MUD constitute a design parameter. The DDCE aims for reducing the pilot overhead, and hence increasing the system's effective throughput. Naturally, it imposes a higher complexity than the purely pilot-based channel estimation.

In order to reduce the complexity of the joint channel estimation and data detection, heuristic search algorithms may be used instead of a full search[24]. In [95] a GA-aided joint channel estimator and data detector was proposed, while in [91] the Differential Evolution Algorithm (DEA) was employed for joint channel estimation and data detection. In [93] various heuristic algorithms, such as the GA, the Particle Swarm Optimization (PSO) and the Repeated Weighted Boosting Search (RWBS) algorithm were used instead of a full search for the true continuous-valued channel gains, as well as for the full search of the discrete-valued symbol-space of the MUD. As another design option, a factor-graph based approach was used for joint channel estimation and MUD in MC-IDMA systems in [92]. By exploiting the sparsity of the wireless channels, Prasad *et al.* in [88] proposed a methodology that requires fewer pilot symbols, without degrading the performance.

3) The Quantum Algorithms: In [96] the Quantum Repeated Weighted Boosting Search (QRWBS) algorithm was proposed for reducing the computational complexity of the classical evolutionary algorithms-based joint channel estimation and data detection, without degrading the system's performance. To elaborate a little further, the QRWBS is an amalgam of the DH QSA and the RWBS algorithm. Both the RWBS and the QRWBS algorithms create a population of agents, which are transformed to better agents via multiple generations. Please note that an agent in the context of channel estimation represents a continuous-valued FD channel gain, while in the context of data detection it represents a discrete-valued symbol. Therefore, a continuous-valued QRWBS and a discrete-valued QRWBS are employed in [96] for solving the

[23] Please recall that a symbol's LLR value may be considered an indicator of how reliably it has been detected.

[24] The full search here is meant in the context of finding the channel gain that minimizes a cost function designed based on the maximum likelihood criterion.

two problems. An agent is deemed to have a higher fitness than another agent, if its channel gain or symbol corresponds to a lower cost function value than the other agent's.

The maximum affordable number of generations[25] is Ξ In both the RWBS and the QRWBS. In the classical RWBS a specific number of agents P is created during each generation. During the ξth generation, where $\xi = 1, \ldots, \Xi$, the agents are classically processed in order to create a new agent, which is termed as the best agent or winner of that generation. The lower the cost function values of the P agents during the ξth generation are, the lower the cost function value of the best agent of that generation will be. Therefore, it is beneficial to create populations, which have agents with as low cost function values as possible. The best agent of a generation is subsequently used as the basis for creating new agents for the next generation. Therefore, the population of the $(\xi+1)$st generation is created randomly in the vicinity of the best agent of the ξth generation.

The QRWBS algorithm obeys the same procedure, but differs in the creation of the population of each generation. Instead of creating Z agents in each generation, it creates a much higher number of agents $Z_Q \gg Z$. It then employs the DH QSA in that database of Z_Q agents in order to find the specific agent of the population that corresponds to the minimum cost function value of that generation. As discussed in Section II-B8, in the process of searching for the minimum value, the DH QSA also queries the database for other entries, which are later proven not to be the minimum ones. However, due to the particular nature of the DH QSA, most of the extra observed agents have a cost function value close to the minimum one in the database. All these entries are used in the QRWBS in order to form a population of $Z_\xi \ll Z_Q$ agents. The subscript ξ of Z_ξ reflects the fact that due to the probabilistic nature of the DH QSA, the population size may differ from one generation to the next. Both the continuous-valued and discrete-valued QRWBS employed for channel estimation and MUD, respectively, in the context of a joint channel estimation and MUD receiver was shown to outperform its classical counterpart [96].

C. Multi-User Transmission

1) The Problem: Let us now consider the dual counterpart of MUDs. In a nutshell, given the FD-CHTF of all users, the MUD detects the multi-user symbol vector. By contrast, the Multi-User Transmitter (MUT) relies on the FD-CHTF of all users signalled back to the BS. Explicitly, the multi-user symbol vector is "pre-distorted" by the MUT of the BS invoking the FD-CHTFs of all users for ensuring that after passing through the predicted channel each user receives a symbol-vector having the single non-interfered symbol destined for it. The duality of MUDs and MUTs was discussed for example by [97]. The substantial benefit is that a low-complexity single-user detector may be invoked by the mobile user terminal. This MUT principle is applicable both to OMA and NOMA systems. Hence in the downlink of a NOMA system, the base station may appropriately combine the different information symbols destined for the users supported and transmit a single multi-user signal, in order to increase the system throughput as depicted in Fig. 18 [5], [97]. It is up to each user then to detect and decode their own information upon the reception of the combined multi-user symbol vector. Since the user terminals do not have the same complexity capabilities as the base stations, the complex processing should be performed at the base station's side. Let us assume that the base station desires to transmit a multi-user symbol vector, where each entry of the vector corresponds to a different user. To elaborate a little further, the multi-user transmission problem is that given the symbol vector, as well as the system and channel characteristics, we should find a $(U \times N_t)$-element Transmit Pre-Coding (TPC) matrix $\mathbf{P}$, where U is the number of users and N_t the number of transmit antennas at the base station, in order to multiply with the information symbol vector as in

$$\mathbf{s} = \mathbf{P} \cdot \mathbf{x}, \tag{31}$$

where $\mathbf{x}$ is the $(U \times 1)$-element multi-user vector and $\mathbf{s}$ is the transmitted $(N_t \times 1)$-element vector. Again, by doing so, when each user receives the composite multi-user symbol vector, they can detect and decode their own symbol by employing a low complexity single-user detector. Different criteria may be used for finding the optimal TPC matrix, such as the MMSE [98] or the Minimum Bit Error Ratio (MBER) [99] criteria.

2) The Classical Algorithms: Linear channel inversion algorithms, such as the ZF and the MMSE algorithms [98] perform adequately in underloaded or in full-rank systems, where the number of antennas at the base station is higher than the number of users supported. However, in challenging rank-deficient systems, where the number of users supported is higher than the number of antennas at the base station, more powerful non-linear algorithms should be used for performing the transmit precoding process.

In the 5G NOMA systems, the precoding matrix is expected to be calculated based on the distance between the users and the base stations, as well as on their channels' quality [5], [73], [74]. More specifically, assuming a two-user system, a higher power is allocated to the symbol of the user, who experiences the worse channel and higher losses. This way that user is able to detect and decode its own symbol, treating the other user's symbol as low-power interference. On the other hand, the user experiencing the better channel has received a signal with high multi-user interference, due to the worse user's symbol having been allocated a higher portion of the power. Therefore, the higher-power symbol is detected first, whilst treating the lower-power symbol as interference. Then the detected signal is remodulated and deducted from the composite signal, leaving the weaker signal behind. This is termed as Successive Interference Cancellation (SIC) and it has also been used as an MUD [100] as described in Section III-A.

In [101], the vector perturbation precoding technique was

[25] In an evolutionary algorithm, there are individuals and generations. Each individual takes the form of a legitimate solution to the search problem. Individuals that are created at the same "round" or "iteration" belong to the same generation. The subsequent generations apart from updated individuals, who rely on the previous generations' individuals in order to take the form a better solution. After a number of generations the evolutionary algorithm stops and the best individual is the output of the algorithm.

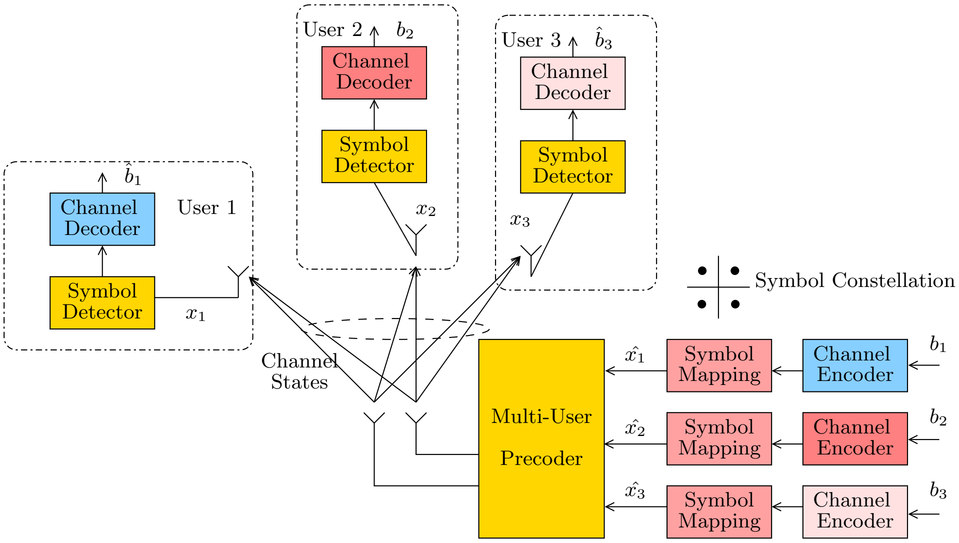


Fig. 18: The problem of Multi-User Transmission in the downlink of a multiple access system.

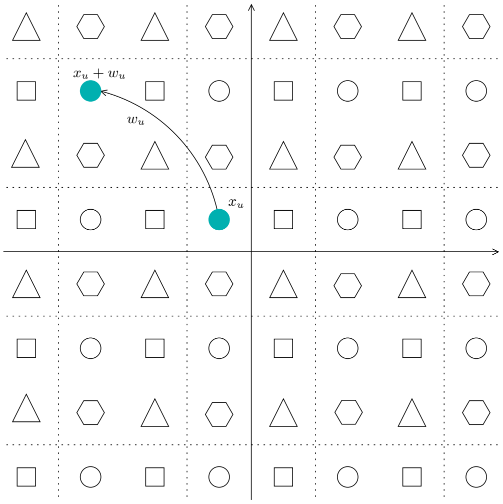


Fig. 19: The resultant legitimate constellation of each user layer, after applying a perturbation vector.

proposed for the downlink of multiple access systems, where a vector $\mathbf{w}$ is added to the multi-user information symbol vector before it is transformed into a multi-antenna vector by multiplying it with the precoding matrix, as encapsulated in

$$\mathbf{s} = \mathbf{P} \cdot (\mathbf{x} + \mathbf{w}). \tag{32}$$

Given an already calculated precoding matrix $\mathbf{P}$, the goal of the perturbation vector is to minimize the required transmission power, while also minimizing the MMSE or the MBER criterion. If the average transmission power at the base station is constant, a scaling factor should be applied to the resultant symbol vector, since its power will depend on the selected perturbation vector. This scaling factor should be signalled to the receivers through a side channel. Since the perturbation vector is discrete-valued, it may be considered as shifting the whole symbol constellation an integer number of times in power as shown in Fig. 19. As an example in Fig. 19, the specific symbol x_u represented by the filled circle of the original QPSK constellation, which is the closest to the origin, would have been transmitted as the uth user's symbol, if no perturbation vector was applied. When that symbol is subjected to the perturbation $w_u = 1 + j$, the top left filled circle $(x_u + w_u)$ will be transmitted instead for the sake of minimizing the transmission power and the interference at the receiver. This operation is performed for each user's symbol, hence the jointly optimal perturbation vector should be found. A simple modulo operation on the perturbed symbol vector may recover the original symbol vector.

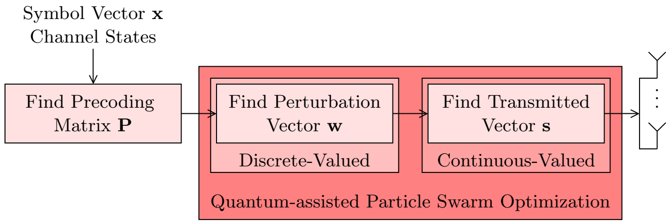

Symbol Vector $\mathbf{x}$
Channel States
Find Precoding Matrix $\mathbf{P}$
Find Perturbation Vector $\mathbf{w}$
Discrete-Valued
Find Transmitted Vector $\mathbf{s}$
Continuous-Valued
Quantum-assisted Particle Swarm Optimization

Fig. 20: The design methodology for the vector perturbation precoding for MUT.

Therefore, using the above-mentioned scaling factor and a low-complexity modulo operation is sufficient at the users in order to map their received signals to the original constellation [101], [102]. The high-complexity part of this problem is to search for the optimal discrete-valued perturbation vector $\mathbf{w}$ of (32). Alternatively, one can immediately search for the optimal continuous-valued transmit vector $\mathbf{s}$ of (32).

A joint block diagonalization and vector perturbation multiple access downlink techinque was proposed in [103]. Furthermore, Yao *et al.* employed a discrete-valued PSO algorithm for finding the perturbation vector that minimizes the MBER criterion in [104], while in [99] a continuous-valued PSO algorithm was proposed for further improving the output of the discrete-valued PSO algorithm. It should be noted that even though the perturbation vector is discrete-valued, the eventually transmitted signal vector is continuous-valued, therefore a continuous-valued fine tuning of the output of the discrete-valued PSO may reduce the system's BER even further. The system model of the vector perturbation precoding technique is shown in Fig. 20. After the precoding matrix is estimated based on the known symbol vector **x**, the channel states and a selected criterion (such as the MMSE criterion), the optimal – with respect to a selected criterion – perturbation vector **w** is found using discrete-valued classical or quantum search. The found perturbation vector determines a transmitted vector **s**. A continuous-valued classical or quantum search may be employed for further fine-tuning the resultant transmitted vector **s**.

Masouros *et al.* [105] proposed a sphere search technique for reducing the complexity of searching for the optimal perturbation vector, with the objective of minimizing the transmission power of the base station. In [102], the authors conceived a vector perturbation algorithm for improving the system's performance, when there is a finite-precision feedback of the scaling factor from the base station to the users, mainly due to the indispensible quantization prior to transmission. The vector perturbation precoding methodology was also employed in the downlink of Coordinated Multi-Point (CoMP) systems [106].

3) The Quantum Algorithms: In [107], the discrete-valued and continuous-valued Quantum-assisted Particle Swarm Optimization (QPSO) algorithms were proposed in the context of finding the optimal perturbation vector and the optimal transmitted vector, respectively, as depicted in Fig. 20. Both the discrete-valued and the continuous-valued QPSO algorithms combine the DH QSA with the classical PSO algorithm. The classical PSO algorithm creates a population of Z particles during each of the Ξ generations. Each particle is associated with a *position* and a *velocity*. The position refers to a legitimate input to the CF, or in other words, an entry in the database. The velocity describes the rate and the direction of the change of its position between two successive generations. During each generation of the classical PSO algorithm, the CF is evaluated for the positions of all particles in the specific generation. Their position and velocity calculated for the subsequent generation are updated based on their current position and velocity, as well as on the current generation's "best" particle's position and velocity[26]. Therefore, a full search of each generation's population has to be performed in order to find the best particle.

The QPSO algorithm employs the DH QSA for finding the best particle during each generation of both the discrete-valued and the continuous-valued QPSO algorithms. This way we are not only able to efficiently search for the best particle, but due to the trial-and-error nature of the DH QSA, only a subset of the original population is available to us. This procedure may be considered as selecting a few of the elite high-fitness particles for creating the population. As shown in [107], both the discrete-valued and continuous-valued QPSO algorithms outperform their classical counterparts for the same number of CF evaluations.

D. Multi-Objective Routing

1) The Problem: So far we have primarily focused our attention on network structures, where the transmission of the messages relies on a single hop, from the mobile users to the BS and vice versa. However, this is not always the case, since occasionally multihop communications are employed to reach remote nodes, which would otherwise be inaccessible [108]. These particular nodes have random locations and limited resources in terms of bandwidth and power and thus they rely on optimal routing for the sake of maximizing their performance. Optimal routing relies on a delicate balance amongst several *Quality of Service* (QoS) criteria apart from the ubiquitous BER performance, which was considered as the primary optimization objective in the majority of the previous applications. On one hand, mobile nodes rely on their batteries having for their communications with the rest of the network, bringing the optimization of their power consumption into the limelight as well [109]. This concept is commonly referred to as *"green" radio* [110]. On the other hand, the widespread use of lip-synchronized audio and video streaming resulted in considering both the delay and the achievable rate [111] as additional QoS criteria. Over the years several other metrics have been proposed such as the routing overhead [112], the control-channel cost [113] or the communication security [114]. Consequently, it becomes clear that routing optimization has to cater for multiple QoS criteria.

Most of the studies in the literature utilize single-component aggregate functions, which combine multiple QoS criteria. In this context, one of the most prominent optimization metrics is the network lifetime [115]. In fact, this specific metric encapsulates several optimization objectives [116], such as the power consumption, the nodes' battery levels and the route's delay. Additionally, the *Network Utility* (NU) also takes into account the routes' achievable rate [117], hence providing a more holistic perspective on the routing problem.

Despite the numerous single-objective approaches advocated in the literature, focusing on a single requirement may unduly degrade all the rest of the metrics. This problem may be mitigated [119] by using a multi-objective approach utilizing the concept of Pareto optimality[27] [120] for evaluating the fitness of multi-objective problems. Likewise, all the requirements considered may be optimized jointly without the need for user-defined parameters in order to aggregate the different design objectives [121]. In this way, we end up with a set of Pareto-optimal solutions, which cannot improve their individual objectives without degrading the rest. *Based on this approach, our ultimate goal is to identify the entire set of Pareto-optimal routes from a database of L routes, given a set of QoS requirements.* To elaborate further, an illustrative example is shown in Fig. 21, where a fully-connected *Heterogeneous Network* (HetNet) [118] is portrayed. In this

[26] Here, by "best" particle we mean the particle in the current population, whose position yields the minimum CF value

[27] In multi-objective routing, each route is now associated with a *Utility Vector* (UV) $\mathbf{f}(x) = [f_1(x), \ldots, f_n(x)]$, where $f_i(x)$ corresponds to the i-th optimization objective out of n objectives in total. For minimization (maximization) problems, a specific route is dominates another if all of its objectives are strictly lower than (greater than) the respective objectives of the second route. Hence, a route is then considered as Pareto-optimal if there exist no other routes dominating it.

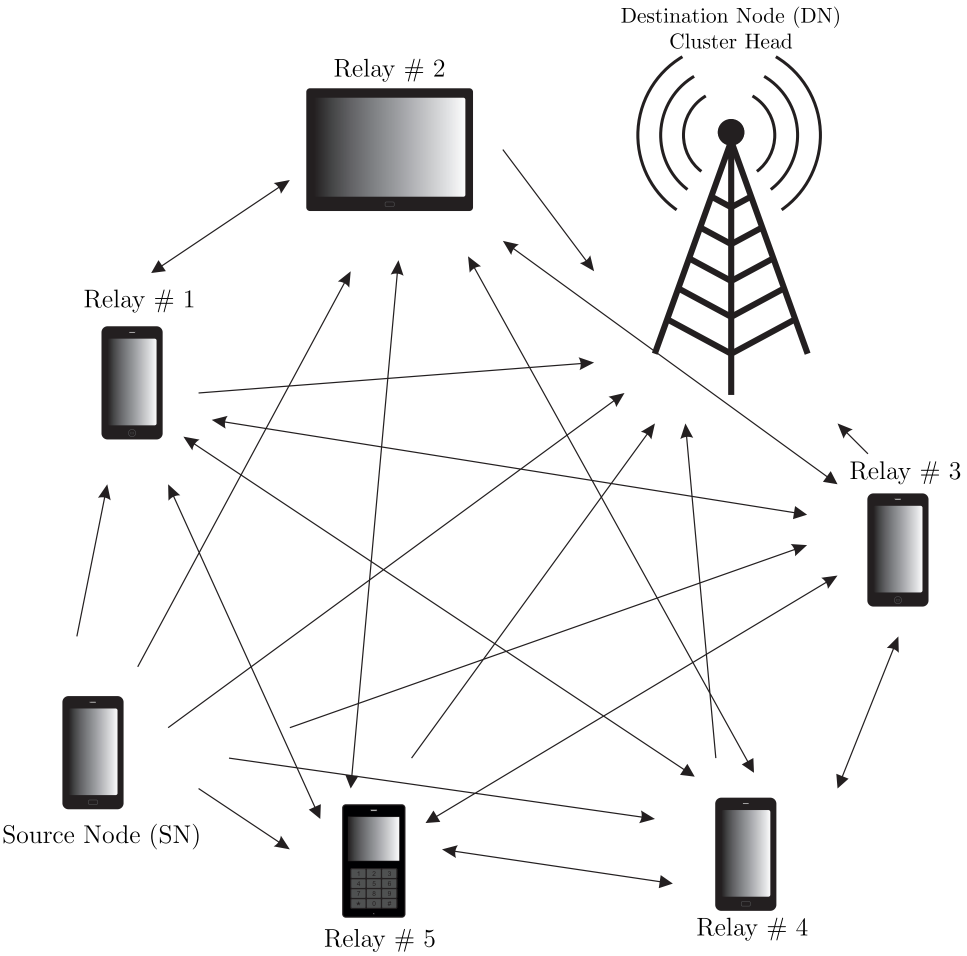


Fig. 21: Exemplified topology for routing optimization in a *Heterogeneous Network* (HetNet) [118].

specific scenario, the *Source Node* (SN) has to transmit its message to the *Destination Node* (DN) through a cloud of heterogeneous mobile *Relay Nodes* (RN). Note that the DN acts as a cluster head and has access to a quantum computer for employing quantum-assisted routing optimization. This specific topology has been studied in [65], [66], [122], [123], where the following *Utility Vector* (UV) $\mathbf{f}(x)$ has been utilized:

$$\mathbf{f}(x) = [P_e(x), D(x), P_L(x)]. \tag{33}$$

Observe in Eq. (33) that the routes' end-to-end BER $P_e(x)$, their end-to-end delay $D(x)$ and their total power dissipation $P_L(x)$ are jointly minimized under the Pareto optimality principle. This process involves a complexity on the order of $O(L^2)$ [65], when using exhaustive search. However, the total number L of routes increases exponentially with the number of nodes [124], as we can observe in Fig. 22, hence rendering the problem NP-hard. Consequently, sophisticated methods are required for addressing the multi-objective routing problem.

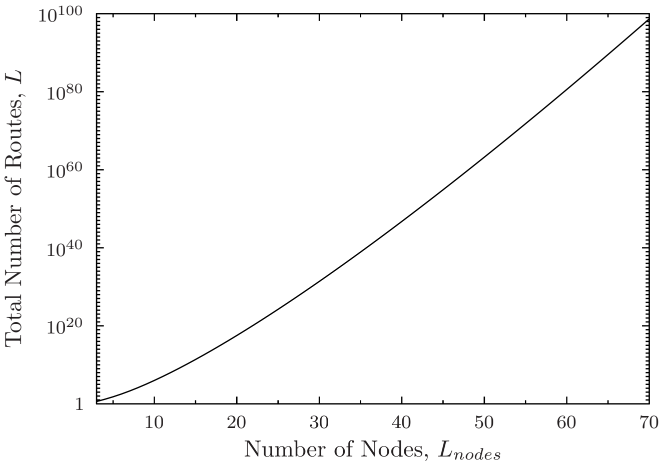


Fig. 22: Total number L of Hamiltonian routes as a function of the number L_{nodes} of nodes of a HetNet.

2) The Classical Algorithms: A plethora of single-objective studies exist in the literature [110], [116], [117], [125]–[131], each addressing different routing aspects. In a nutshell, these specific studies consider the optimization objectives in a single-component aggregate function in an attempt to optimize the latter using either a heuristic or a formal systematic optimization method. To elaborate further, several of these studies [110], [125]–[127] utilize Dijkstra's algorithm [132] for the sake of identifying the optimal routes. Explicitly, this technique is capable of approaching the optimal routes at the cost of imposing a complexity on the order of $O(E^3)$, where

E corresponds to the number of edges in the network's graph. For instance, Zuo *et al.* [126] employed this specific algorithm for optimizing the route's energy efficiency in the context of wireless ad-hoc networks. Hu *et al.* [125] utilized Dijkstra's algorithm for minimizing both the power consumption and the delay, quantified in terms of the number of hops, in socially-aware networks. Additionally, Dehghan *et al.* [127] adapted this specific algorithm to the problem of cooperative routing and attempted to maximize the route's energy efficiency.

The beneficial properties of *convex optimization* [133] have also been exploited in the context of routing optimization. To elaborate further, Dall'Anese and Giannakis [128] transformed the non-convex routing problem of cognitive random access networks into a convex one using successive convex approximations for the sake of minimizing both the routes' *Packet Loss Ratio* (PLR) and the resultant outage probability. Additionally, Yetgin *et al.* [129] maximized the network lifetime in the context of *Wireless Sensor Networks* (WSN) using a similar approach. Based on this specific metric, Abdulla *et al.* [130] have maximized the lifetime of WSNs by introducing a range of Hybrid Multihop Network (HYMN) parameters. The so-called *Network Utility* [131] also constitutes a meritorious single-component optimization.

The employment of Pareto optimality comes at the cost of increased complexity and thus primarily heuristic evolutionary methods have been employed for the sake of making the problem tractable. In fact, there are some comprehensive studies in the literature [124], [135]–[138], each investigating networks from a diverse perspective using the multi-objective approach, while relying on evolutionary algorithms. For instance, both the Non-dominated Sorting Genetic Algorithm II (NSGA-II) and the Multiobjective Differential Evolution Algorithm (MODE) have been invoked in [124] for optimizing their end-to-end delay and power dissipation of transmission routes established in WSNs. Additionally, the NSGA-II has been employed in [135] for satisfying the same QoS requirements in context both of the ubiquitous Voice over Internet Protocol (VoIP) and for file transfer in WSNs. Moreover, Perez *et al.* [136] minimization of the WSN's deployment cost by using a multi-objective model for optimizing both the total energy dissipation and the number of deployed sensor nodes in WSNs. Martins *et al.* [137] employed a hybrid multi-objective evolutionary algorithm for solving the Dynamic Coverage and Connectivity Problem (DCCP) of WSNs subjected to node failures. Additionally, Pinto *et al.* [138] introduced the concept of Pareto Optimality in the ubiquitous single-objective ACO and proposed the so-called *Multiobjective Max-Min Ant System* (MMAS) for solving the multi-objective mutlicast routing problem.

3) The Quantum Algorithms: The application of the aforementioned multi-objective heuristics results in reduced performance due to their tendency to convergence to local optima [65]. Fortunately, quantum computing provides a powerful framework for addressing the multi-objective routing problem by exploiting the complexity reduction offered by the QP, while guaranteeing a near-full-search-based accuracy. In fact, several quantum-assisted treatises have been disseminated in the literature [65], [66], [122], [134] in the context of the multi-objective routing problem.

To the best of our knowledge, the first ever quantum-assisted multi-objective approach to the routing problem is the so-called *Non-dominated Quantum Optimization* (NDQO) algorithm [65]. This specific algorithm extended the DH QSA of Section II-B8 for solving the Pareto optimality problem for the sake of successively approaching the Pareto-optimal routes at a reduced complexity. Assuming a database of L routes in total, the NDQO algorithm succeeds in identifying the entire set of Pareto-optimal routes at a complexity on the order of $O(L\sqrt{L})$, while exhibiting near-optimal routing performance by exploiting the probabilistic nature of the BBHT QSA. In a nutshell, the NDQO algorithm invokes the BBHT QSA to conclude as to whether a reference route is optimal by searching for routes that dominate this specific route.

This process is referred to as a *BBHT-QSA chain* in [65] and its sub-processes are highlighted in Fig. 23. The BBHT-chain's input parameters are shown at the right-hand-side, namely the nodes' geo-locations Z, the initial reference route x_r and the nodes' interference power levels I_0. Initially, the BBHT QSA is invoked for searching for routes that dominate the reference route x_r. The output of this process is the route x_s, which is checked as to whether it dominates x_r. This is denoted by the condition $\mathbf{f}(x_s) \succeq \mathbf{f}(x_r)$, where the operator $\succeq$ corresponds to the Pareto dominance comparison operator. If the referece route x_r is dominated by x_s, x_r is then set equal to x_s and a new BBHT QSA is invoked with the updated reference route value. This process is repeated until the BBHT QSA outputs a route that does not dominate its reference route, thus ensuring that the current reference route is indeed Pareto-optimal in the absence of dominant routes.

Since the BBHT QSA exhibits a $\sim 100\%$ probability of correctly detecting a solution as detailed in Section II-B7, some sub-optimal routes may be erroneously classified as being Pareto-optimal due to BBHT QSA's inability to guarantee 100% probability of correctly detecting a route that dominates the reference route. Therefore, the NDQO algorithm exhibits a modest error floor owing the low-probability inclusion of sub-optimal routes into the set of Pareto-optimal routes. Its error floor has been mitigated by its successor, namely the so-called *Non-dominated Quantum Iterative Optimization* (NDQIO) algorithm [66], where a repair process guaranteeing the identification of only true Pareto-optimal routes has been proposed. The NDQIO algorithm succeeds in further reducing the complexity imposed, which is quantified on the order of $O(L_{\text{OPF}}\sqrt{L})$, with L_{OPF} corresponding to the number of Pareto-optimal routes, while reducing the associated performance error floor to infinitesimally low levels.

An additional source of complexity reduction, namely that of the database correlation exploitation, has been combined with the quantum parallelism for the sake of further complexity reduction. Explicitly, it has been confirmed by Zalka [61] that Grover's QSA and its variants are optimal in terms of the number of database queries in uncorrelated databases. Therefore, database correlation exploitation would significantly increase the efficiency of quantum parallelism. In this context, the so-called *Multi-Objective Decomposition Quantum Optimization* (MODQO) algorithm [134] has been proposed

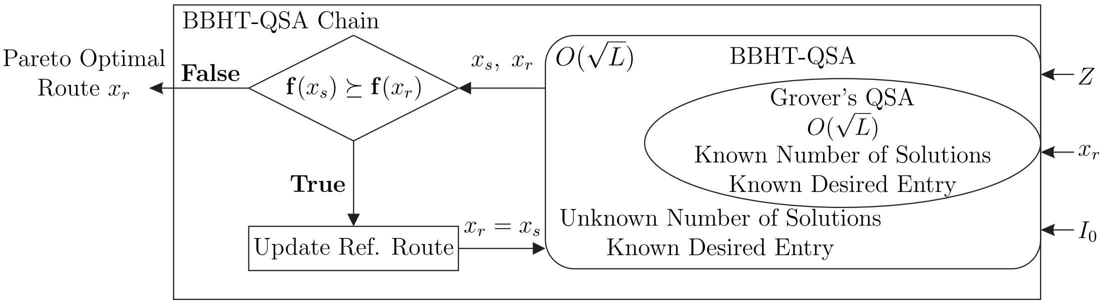


Fig. 23: The *BBHT-QSA chain* process used in [65], [66], [122], [134] for identifying a single Pareto-optimal route.

for multi-objective routing in *socially-aware networks* [125]. Note that the topology considered in [134] is different from that of Fig. 21, since multiple pairs of SNs and DNs are considered. In this scenario, the MODQO algorithm exploited the specific property that the Pareto-optimal route combinations are constituted by individual Pareto-optimal routes. Therefore, by exploiting this observation, the search space has been partitioned into several less correlated databases, where the quantum parallelism framework proposed in [66] can be more efficiently exploited. As for its complexity, the MODQO algorithm succeeds in identifying the entire set of Pareto-optimal route combinations at a complexity, which is on the orders of $O(\sqrt{L})$ and $O(L_{MR}\sqrt{L} + L_{MR}^{2L_{MC}})$ for the best- and worst-case scenarios, respectively, where L_{MR} and L_{MC} correspond to the number mesh routers and clients, respectively. Note that the classical exhaustive search would impose a complexity on the order of $O(L^{L_{MC}})$, where we have $O(L) \gg O(L_{MR})$, hence rendering the problem unsolvable in polynomial time.

Apart from the exploiting the correlations in the formation of Pareto-optimal route combinations, the potential correlations in the formation of Pareto-optimal routes has been investigated in [122] and [123]. To elaborate further, it has been proven in [122] that Pareto-optimal routes exclusively consist of Pareto-optimal sub-routes. Based on this observation, the so-called *Evolutionary Quantum Pareto Optimization* (EQPO) algorithm [122] and an *irregular trellis graph* [139] has been proposed for the sake of guiding the search, hence effectively transforming the search space into a series of weakly correlated databases with the aid of dynamic programming [140], [141]. A quantum-assisted feed-forward process resembling the ubiquitous Viterbi algorithm [142] is then invoked for the sake of identifying the Pareto-optimal routes by processing the trellis-stages. More specifically, the NDQIO algorithm is activated for each trellis-stage to identify the respective Pareto-optimal routes. The EQPO algorithm succeeds in identifying 99.9% of the set Pareto-optimal routes at a complexity order of $O(L_{opt}^{3/2} L_{nodes}^2)$, while exhibiting a performance associated with a low heuristic error floor. Therefore, since the total number L of routes has an exponential relationship with respect to the number L_{nodes} of nodes, as seen in Fig. 22, a substantial complexity reduction is achieved compared to full-search-based NDQO and NDQIO algorithms.

Apart from the aforementioned treatises, which primarily rely on Grover's operator and thus harnessing the power of quantum parallelism, some others exploit the beneficial complexity reduction offered by the *quantum tunneling* effect [143]. Explicitly, the particular quantum algorithms relying on quantum tunneling are referred to as *quantum annealers* [144], [145]. More specifically, a quantum annealer may be treated as a sampler, which approximates the global optimum of a function or of a database with the aid of quantum tunneling. In the context of multi-objective routing, Wang *et al.* [146] proposed a quantum annealing algorithm designed for optimizing the scheduling of the wireless links in interference-limited networks. The proposed quantum annealing algorithm succeeded in jointly optimizing both the network's throughput as well as its interference, whilst imposing a substantially lower complexity than its classical counterpart, namely the simulated annealing algorithm.

E. Breaking Public-Key Cryptography Schemes

1) The Problem: Public-key cryptosystems, such as the RSA [147], named after its creators Rivest, Shamir and Adleman, encrypt data using a public key, which may be eavesdropped by anyone, and they decrypt data using a private key. Node A randomly picks two large prime numbers. Based on these two prime numbers, a public key and a private key are generated. The public key can be used by any other node for encrypting their data and transmitting it back to the node A. However, only node A has the private key, which is the only key that can be used for correctly decrypting the received data. Please note that none of the transmitting nodes should be able to decrypt the data they encrypted themselves. The same applies to any potential eavesdroppers, who have obtained both the public key and the encrypted messages from the transmitting nodes. This means that no processing of the public key should lead to any information concerning the private key. However, due to the process invoked for creating the public and the private keys, if the two prime numbers, which were used for creating the keys are obtained by an eavesdropper, the private key can be replicated and the information messages can be decrypted. This is termed as the RSA problem, which reduces to the following factorization problem. Given a large number N, we have to find its two prime factors.

Even though it would be beneficial if a solution did not exist to the RSA problem, creating algorithms that are able to break a cryptosystem inevitably provides insights for constructing post-quantum cryptosystems.

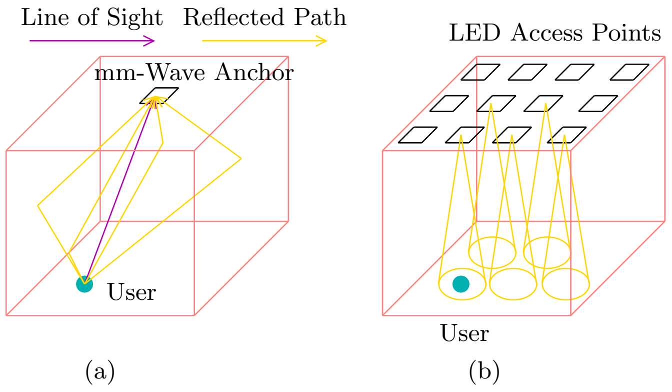


Fig. 24: The indoors localization problem, where an accurate position of the user has to be estimated. (a) Uplink localization, where a mm-Wave anchor processes the received line of sight path, as well as the reflected paths. Based on the RSSI, the ToA and the AoA, the mm-Wave anchor may initially reduce the search space. Then, it may employ the fingerprinting methodology for comparing the received signals to those stored in a pre-calculated database. (b) Downlink localization using a VLC system, where each LED panel is switched on and off sequentially. The RSSI at the user by each LED access point is compared to a pre-calculated database, following the fingerprinting methodology. Quantum search may be employed for searching in the databases in both the downlink and the uplink localization methods.

2) The Classical Algorithms: Integer factorization techniques may be used for finding the prime factors of an integer. The most efficient classical algorithm of solving an integer factorization problem is the *quadratic sieve* [148], when the number to be factored is less than 332 bits long. For higher numbers, the *general number field sieve* [148] outperforms all other classical algorithms, but it imposes a high computational complexity.

3) The Quantum Algorithms: Shor's algorithm [33] can be used for efficiently solving the RSA problem. As discussed in Section II-B4, Shor's algorithm employs a classical subroutine, which resembles the operation of the quadratic sieve, while the QPEA [48] of Section II-B5 is used for finding the necessary period of the function employed. Shor's algorithm achieves an exponential speed-up, over the general number field sieve, as a benefit of the inherent parallelism of quantum computing. In 2012, the number 21 was factored to its prime factors 3 and 7 using Shor's algorithm [149].

F. Indoor Localization

1) The Problem: The problem of indoor localization is to estimate the position of a user in a room, based on the user's transmit or received signals [150]. More precisely, the signals' Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), Angle of Arrival (AoA), or Time Difference of Arrival (TDoA) may be exploited for estimating the user's location [151]. The localization's accuracy is enhanced, when the floor plan of the room is known. The localization problem is illustrated in Fig. 24.

Due to the paradigm shift to mm-Wave communications [152]–[154], *pencil* beams may be formed in order to minimize the multi-user interference and to increase the data rate [155]. In order to use very thin beams, accurate user localization is necessary.

Accurate localization may also be used for tracking the movement of a user in a room. Visible Light Communication (VLC) systems [156]–[158] may exploit accurate localization, since they will be able to form more accurate clusters of access points for serving the users supported by the system. More specifically, since multiple Light Emitting Diodes (LED) will be installed in a room, the accurate localization of users may support efficient spatial MIMO techniques for increasing the data rate of the downlink. Accurate tracking of the user's movement would help the system maintain the throughput attained.

2) The Classical Algorithms: Ultra WideBand (UWB) systems may also be employed for achieving accurate localization [150], [159]–[165] by exploiting the signals' inherently short symbol duration and the ToA of its Line Of Sight (LOS) component. If the floor plan of the room is known, the Multi-Path Components (MPC) of the signal's PDP may also be exploited for increasing the accuracy of the localization [159], [164], [165]. More specifically, the TOA of the LOS path and of the MPCs may be jointly processed in order to extract a small subset of legitimate areas in the room, where the user may be located, as exemplified in Fig. 24.

VLC-based localization has also been employed, by exploiting the limited coverage of the VLC access point [156], [166]. Based on the fingerprinting approach [167], the room may be partitioned into small virtual tiles. The localization algorithm has to determine the center of which specific tile the user is closest to. This is performed by building a database of the potentially received signals' RSSIs, ToAs, AoAs and TDoAs from each legitimate tile. A suitable CF which would compare the actual received signals to the saved ones at the known tile-centre positions would determine, which tile is closest to the supported user. Hence, the localization problem may be reduced to a search problem. The size of the search space depends on the size of each tile. The smaller the dimensions of a tile are, the more accurate the localization will be, but more tiles exist in the database. Therefore, there is a trade-off between the performance attained and the complexity imposed.

The triangulation method [167] combines the signals of three different access points by estimating the distance between them and the user based on their RSSI and then estimating the location of the user to be at the intersection of the three circles. When operating in a system, where the Signal to Noise Ratio (SNR) is low, using the triangulation method based on the RSSI may lead to inaccurate localization. The Global Positioning System (GPS) uses the triangulation method for localization.

3) The Quantum Algorithms: The DH QSA was combined with classical processing for performing indoor localization in the VLC downlink and in the mm-Wave uplink [168]. The fingerprinting approach is used in both systems. In the mm-Wave uplink , multiple antennas may be used at the access point for estimating the AoA. Based on the AoA and the ToA of the LOS and multipath signals, the initial search space may be reduced to a subset of surviving tiles, similarly to [159]. The DH QSA is then employed in the resultant database of CF values, in order to find the particular entry that minimizes the CF. In this problem, the CF takes into account the signal received at all antennas of the access point over the LOS path, as well as over all MPCs, and determines the square distance from the corresponding values associated with the center of each tile.

The fingerprinting approach is also used in the VLC downlink in [168]. Similarly to [156], the signal strength of each access points is measured and stored in a database, which corresponds to a specific tile's center. Therefore, if there are 64 access points and 90 tiles in the room, there are 90 databases with 64 entries each. The entries of each database are then combined and compared to the actual 64 received values at the user's true position and the search problem reduces to that of finding which of the 90 tiles offers the most similar RSSI from all access points to the actually received ones. The DH QSA was employed for offering a quadratic reduction in the associated computational complexity compared to a full search. Similarly, by appropriately reducing the size of each tile in order to increase the search space so that the DH QSA in the larger database requires the same complexity as a full search in a smaller database, a higher localization accuracy may be achieved.

In the uplink and downlink localization problems, the quantum-assisted solutions of [168] achieved an equivalent performance to the optimal classical methods, while requiring a lower computational complexity.

G. Big-Data Analysis

1) The Problem: In big-data systems, multiple-feature data has to be accessed and manipulated. Examples of problems existing in big-data systems involve classification of the high-dimensional data based on their features, search problems and existence problems [169].

In the classification problem [170], the entries of a database have to be classified into multiple classes, based on their features' values. The classification problem may be divided into two parts: a) the *supervised classification* problem, where a set of already classified data exists and can be exploited for aiding the classification of the rest of the data, and b) the *unsupervised classification* problem, where all entries have to be classified.

In a search problem, the index of the entry in a large unsorted database has to be found. Furthermore, the existence problem investigates whether there exists a specific entry in a database or not.

2) The Classical Algorithms: Classical machine learning [170], [171] can be used for solving both unsupervised and supervised classification problems [172]. Support Vector Machines (SVM) [173] may be employed for performing either supervised or the so-called *semi-supervised* classification [174]. They construct a model based on the classified training data for accurately predicting the class that new data should be classified into.

Both the search problem and the existence problem encountered in unstructured high-volume databases can be classically solved by a full search, which however often imposes an excessively high complexity.

3) The Quantum Algorithms: In [175] a Quantum Support Vector Machine (QSVM) was proposed for performing supervised classification in large databases. The QSVM imposes an exponentially lower complexity than its classical counterparts, when the latter are able to classify the same dataset in polynomial time. To elaborate further, the QSVM reformulates the classical SVM originally proposed in [176]. Explicitly, this reformulation transforms the SVM's quadratic formulation into a system of linear equations, which are in turn solved by using the HHL algorithm [54] of Section II-B12.

Grover's QSA [28] of Section II-B6 can be employed for searching through an unstructured database, whilst achieving a quadratic speed-up compared to the classical full search. When the exact position of the desired entry is not required, only the knowledge of whether that entry exists in the database or not is wanted, the Quantum Existence Testing (QET) algorithm of [9], [177] may be used instead. The QET algorithm employs the QCA of Section II-B9, which finds the number of times a desired entry appears in a database. Since in the context of the existence problem we are not interested in finding the specific number of times a value appears in a database, but rather *if* it exists at all or not, the QET algorithm uses fewer qubits in the control register of the QCA of Fig. 12. This way, even though a precise estimate of the number of solutions in a database cannot be obtained the measured control qubits are non-zero, we are informed that there are indeed any solutions in the database. When carrying out this task, the QET algorithm imposes a lower complexity than the QCA, which in indicates a quadratic speed-up over the full search.

IV. Open Problems

A suite of quantum solutions have been proposed for classical wireless problems. Nevertheless, there are numerous open problems in both the physical and network layers of wireless communications systems that may benefit from the power quantum computing. For example, Coordinated Multi-Point [178], also referred to as cooperative network MIMO, is a compelling solution to the problem of degraded user performance at the cell edge. Based on CoMP, a user will be simultaneously connected to multiple base stations, which essentially treat interference as useful information. Quantum search algorithms [28], [31], [32] may be used in the context of CoMP for detecting and processing the excessive amount of information, since the notion of interference will have been eliminated.

Quantum computing may also be used for improving the routing performance of drone communications and networks [181], [182], given their limited battery lifespan and mission-critical nature. For instance, optimal routes may be found in drone networks using quantum algorithms, or when drones are used as emergency base stations, optimal drone placement planning may be performed by solving the associated optimization problem.

The multi-objective quantum computing framework constituted by the algorithms of Sec. III-D could be employed for addressing the problem of *proactive caching* [125], [183]–[185]. Explicitly, in proactive caching the packets are buffered in the nodes by carefully considering their popularity for the sake of reducing both the delay and the power consumption, which is reminiscent of the multi-objective routing problem. Additionally, this specific case study could be undertaken with the aid of *machine learning* [186]. In fact, Kapoor *et al.* [188] have recently proposed a model for quantum perceptrons, which may constitute beneficial building blocks for quantum-aided neural networks. Therefore, it would be worth investigating as to whether quantum-assisted solutions can be adopted in this context.

In addition to the above-mentioned open problems, novel quantum solutions may be explored in the specific wireless communication problems discussed in this contribution. For example, Hogg's heuristic quantum search algorithm [51], [52] may be employed in any database search, where there exists correlation between the database entries, in order to reduce the required search time. In the uplink multi-user detection problem, the constructed database includes the MSE between the actually received signal and a hypothetical noiseless received signal that is based on a legitimate symbol combination. Since there are different symbol combinations that partially consist of the same symbols, there is correlation in the constructed database. Therefore, Hogg's heuristic quantum search algorithm may further decrease the search complexity imposed.

V. Conclusions

In this contribution, we have surveyed the family of quantum algorithms that have been employed for solving realistic problems in wireless communications faster and more accurately than the available classical solutions. In Section II-A we have stated the basic characteristics of quantum computing with the aid of linear algebra and logical gates, reminiscent of classical computing. Familiarity with the basics of quantum computing was then exploited for highlighting the quantum circuits of major quantum algorithms that have been proposed. We have gathered the investigated quantum algorithms in Tables III and IV, where we briefly state their application and description.

Having acquired a feel for the capabilities of quantum computing via the quantum algorithms presented, in Section III, we have shifted the focus of our attention to classical wireless optimization problems. We have opted for discussing each of the optimization problems, as well as their state-of-the-art classical solutions. By comparing the presented quantum-assisted solutions to their classical counterparts, we have argued that for a specific complexity budget, a performance gain is observed when the quantum algorithms are used. Similarly, by employing the quantum algorithms, a specific performance target may be reached at a lower computational complexity.

References

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1853–1888, 2012.

[2] H. Ji, S. Park, J. Yeo, Y. Kim, J. Lee, and B. Shim, "Introduction to Ultra Reliable and Low Latency Communications in 5G," *CoRR*, vol. abs/1704.05565, 2017.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, pp. 22–32, February 2014.

[4] G. Wunder, P. Jung, M. Kasparick, T. Wild, F. Schaich, Y. Chen, S. T. Brink, I. Gaspar, N. Michailow, A. Festag, L. Mendes, N. Cassiau, D. Ktenas, M. Dryjanski, S. Pietrzyk, B. Eged, P. Vago, and F. Wiedmann, "5GNOW: Non-Orthogonal, Asynchronous Waveforms for Future Mobile Applications," *IEEE Communications Magazine*, vol. 52, pp. 97–105, February 2014.

[5] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access," in *IEEE Vehicular Technology Conference (VTC Spring)*, pp. 1–5, June 2013.

[6] L. Hanzo, Y. Akhtman, M. Jiang, and L. Wang, *MIMO-OFDM for LTE, WIFI and WIMAX: Coherent versus Non-Coherent and Cooperative Turbo-Transceivers*. John Wiley & Sons, 2010.

[7] C. She, C. Yang, and T. Q. S. Quek, "Radio Resource Management for Ultra-Reliable and Low-Latency Communications," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 72–78, 2017.

[8] N. Kato, Z. M. Fadlullah, B. Mao, F. Tang, O. Akashi, T. Inoue, and K. Mizutani, "The Deep Learning Vision for Heterogeneous Network Traffic Control: Proposal, Challenges, and Future Perspective," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 146–153, 2017.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. New York, NY, USA: Cambridge University Press, 10th ed., 2011.

[10] S. Imre and F. Balázs, *Quantum Computing and Communications: An Engineering Approach*. John Wiley & Sons, 2005.

[11] S. Imre and L. Gyongyosi, *Advanced Quantum Communications: An Engineering Approach*. John Wiley & Sons, 2013.

[12] R. J. Lipton and K. W. Regan, *Quantum Algorithms via Linear Algebra: A Primer*. MIT Press, 2014.

[13] M. M. Waldrop, "The chips are down for Moore's law," *Nature News*, vol. 530, no. 7589, p. 144, 2016.

[14] S. Boixo, T. Albash, F. M. Spedalieri, N. Chancellor, and D. A. Lidar, "Experimental signature of programmable quantum annealing," *Nature Communications*, vol. 4, 2013.

[15] M. Johnson, M. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. Berkley, J. Johansson, P. Bunyk, *et al.*, "Quantum annealing with manufactured spins," *Nature*, vol. 473, no. 7346, pp. 194–198, 2011.

[16] S. Boixo, T. F. Rønnow, S. V. Isakov, Z. Wang, D. Wecker, D. A. Lidar, J. M. Martinis, and M. Troyer, "Evidence for Quantum Annealing with more than One Hundred Qubits," *Nature Physics*, vol. 10, no. 3, pp. 218–224, 2014.

[17] Z. Babar, S. X. Ng, and L. Hanzo, "Near-Capacity Code Design for Entanglement-Assisted Classical Communication over Quantum Depolarizing Channels," *IEEE Transactions on Communications*, vol. 61, pp. 4801–4807, December 2013.

[18] Z. Babar, S. Ng, and L. Hanzo, "EXIT-Chart Aided Near-Capacity Quantum Turbo Code Design," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 3, pp. 866–875, 2014.

[19] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The Road From Classical to Quantum Codes: A Hashing Bound Approaching Design Procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[20] Z. Babar, P. Botsinis, D. Alanis, S. Ng, and L. Hanzo, "Fifteen Years of Quantum LDPC Coding and Improved Decoding Strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

[21] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, R. G. Maunder, and L. Hanzo, "Fully-Parallel Quantum Turbo Decoder," *IEEE Access*, vol. 4, pp. 6073–6085, 2016.

[22] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. Nguyen, S. X. Ng, and L. Hanzo, "Quantum Error Correction Protects Quantum Search Algorithms Against Decoherence," *Nature Scientfic Reports*, vol. 6, no. 38095, 2016.

[23] P. A. M. Dirac, *The Principles of Quantum Mechanics*. Oxford University Press, USA, 4 ed., February 1982.

[24] C. Williams, "Quantum Search Algorithms in Science and Engineering," *Computing in Science & Engineering*, vol. 3, pp. 44–51, March 2001.

[25] M. Santha, *Quantum Walk Based Search Algorithms*, pp. 31–46. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[26] A. M. Childs and W. van Dam, "Quantum algorithms for algebraic problems," *Rev. Mod. Phys.*, vol. 82, pp. 1–52, Jan 2010.

[27] M. Mosca, *Quantum Algorithms*, pp. 2303–2333. New York, NY: Springer New York, 2012.

[28] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, pp. 212–219, May 1996.

[29] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," *Physical Review Letters*, vol. 79, pp. 325–328, July 1997.

[30] S. Jordan, "Quantum Algorithm Zoo," *http://math.nist.gov/quantum/zoo/*, 2011.

[31] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight Bounds on Quantum Searching," *Fortschritte der Physik*, vol. 46, pp. 493–506, 1998.

[32] C. Durr and P. Høyer, "A Quantum Algorithm for Finding the Minimum," *eprint arXiv:quant-ph/9607014*, July 1996.

[33] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *35th Annual Symposium on Foundations of Computer Science, Proceedings*, pp. 124–134, November 1994.

[34] G. Brassard, P. Høyer, and A. Tapp, "Quantum Counting," *eprint arXiv:quant-ph/9805082*, May 1998.

[35] H. Wimmel, *Quantum Physics & Observed Reality: A Critical Interpretation of Quantum Mechanics*. World Scientific, 1992.

[36] J. S. Bell, "On the Problem of Hidden Variables in Quantum Mechanics," *Reviews of Modern Physics*, vol. 38, pp. 447–452, July 1966.

[37] N. Chandra and R. Ghosh, *Quantum Entanglement in Electron Optics: Generation, Characterization, and Applications*. Springer Berlin Heidelberg, 2013.

[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, Jan. 2002.

[39] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, July 2009.

[40] R. Hughes and J. Nordholt, "Refining Quantum Cryptography," *Science*, vol. 333, no. 6049, pp. 1584–1586, 2011.

[41] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 10 1982.

[42] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, (New York), pp. 175–179, IEEE Press, 1984.

[43] R. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, June 1982.

[44] P. Benioff, "Quantum Mechanical Hamiltonian Models of Turing Machines," *Journal of Statistical Physics*, vol. 29, pp. 515–546, 1982. 10.1007/BF01342185.

[45] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[46] D. Deutsch and R. Jozsa, "Rapid Solution of Problems by Quantum Computation," *Proceedings: Mathematical and Physical Sciences*, vol. 439, pp. 553–558, December 1992.

[47] D. R. Simon, "On the Power of Quantum Computation," *SIAM Journal on Computing*, vol. 26, pp. 116–123, 1994.

[48] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum Algorithms Revisited," *Royal Society of London Proceedings Series A*, vol. 454, pp. 339–357, January 1998.

[49] D. S. Abrams and S. Lloyd, "Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors," *Physical Review Letters*, vol. 83, pp. 5162–5165, Dec 1999.

[50] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum Amplitude Amplification and Estimation," *eprint arXiv:quant-ph/0005055*, May 2000.

[51] T. Hogg, "Quantum Search Heuristics," *Physical Review A*, vol. 61, p. 052311, Apr 2000.

[52] T. Hogg and D. Portnov, "Quantum Optimization," *Information Sciences*, vol. 128, no. 34, pp. 181–197, 2000.

[53] A. Malossini, E. Blanzieri, and T. Calarco, "Quantum Genetic Optimization," *IEEE Transactions on Evolutionary Computation*, vol. 12, pp. 231–241, April 2008.

[54] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum Algorithm for Linear Systems of Equations," *Physical Review Letters*, vol. 103, p. 150502, Oct. 2009.

[55] G. Brassard, F. Dupuis, S. Gambs, and A. Tapp, "An Optimal Quantum Algorithm to Approximate the Mean and its Application for Approximating the Median of a Set of Points Over an Arbitrary Distance," *eprint arXiv:quant-ph/1106.4267v1*, June 2011.

[56] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum Search Algorithms, Quantum Wireless, and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[57] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[58] C. Pomerance, "A Tale of Two Sieves," *Notices Amer. Math. Soc*, vol. 43, pp. 1473–1485, 1996.

[59] J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M. Barrett, R. Blakestad, W. Itano, J. Jost, C. Langer, R. Ozeri, *et al.*, "Implementation of the Semiclassical Quantum Fourier Transform in a Scalable System," *Science*, vol. 308, no. 5724, pp. 997–1000, 2005.

[60] D. E. Knuth, *The Art of Computer Programming, Volume 3: (2Nd Ed.) Sorting and Searching*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1998.

[61] C. Zalka, "Grover's Quantum Searching Algorithm is Optimal," *Physical Review A*, vol. 60, pp. 2746–2751, Oct 1999.

[62] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-Complexity Quantum-Assisted Multi-User Detection for CDMA and SDMA," *IEEE Transactions on Communications*, vol. 62, pp. 990–1000, March 2014.

[63] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1st ed., 1989.

[64] G. Syswerda, "A Study of Reproduction in Generational and Steady State Genetic Algorithms," *Foundations of Genetic Algorithms*, vol. 2, pp. 94–101, 1991.

[65] D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum-assisted routing optimization for self-organizing networks," *IEEE Access*, vol. 2, pp. 614–632, 2014.

[66] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Non-dominated quantum iterative routing optimization for wireless multihop networks," *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[67] A. Ambainis, "Variable Time Amplitude Amplification and a Faster Quantum Algorithm for Solving Systems of Linear Equations," *ArXiv e-prints*, Oct. 2010.

[68] A. M. Childs, R. Kothari, and R. D. Somma, "Quantum Linear Systems Algorithm with Exponentially Improved Dependence on Precision," *ArXiv e-prints*, Nov. 2015.

[69] P. Botsinis, S. X. Ng, and L. Hanzo, "Low-Complexity Iterative Quantum Multi-User Detection in SDMA Systems," in *IEEE International Conference on Communications (ICC)*, pp. 5592–5597, June 2014.

[70] L. Hanzo, L.-L. Yang, E.-L. Kuan, and K. Yen, *Single and Multi-Carrier DS-CDMA: Multi-User Detection, Space-Time Spreading, Synchronisation, Networking, and Standards*. John Wiley & Sons, 2003.

[71] L. Hanzo, M. Münster, B. Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting*. John Wiley & Sons, 2003.

[72] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the Performance of Non-Orthogonal Multiple Access in 5G Systems with Randomly Deployed Users," *IEEE Signal Processing Letters*, vol. 21, pp. 1501–1505, Dec 2014.

[73] L. Dai, B. Wang, Y. Yuan, S. Han, C. l. I, and Z. Wang, "Non-Orthogonal Multiple Access for 5G: Solutions, Challenges, Opportunities, and Future Research Trends," *IEEE Communications Magazine*, vol. 53, pp. 74–81, September 2015.

[74] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the Performance of Non-orthogonal Multiple Access Systems With Partial Channel Information," *IEEE Transactions on Communications*, vol. 64, pp. 654–667, Feb 2016.

[75] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C. L. I, and H. V. Poor, "Application of Non-Orthogonal Multiple Access in LTE and 5G Networks," *IEEE Communications Magazine*, vol. 55, pp. 185–191, February 2017.

[76] Z. Ding, P. Fan, and H. V. Poor, "Random Beamforming in Millimeter-Wave NOMA Networks," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[77] C. Xu, B. Hu, L.-L. Yang, and L. Hanzo, "Ant-Colony-Based Multiuser Detection for Multifunctional-Antenna-Array-Assisted MC DS-CDMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 57, pp. 658–663, January 2008.

[78] K. Soo, Y. Siu, W. Chan, L. Yang, and R. Chen, "Particle-Swarm-Optimization-Based Multiuser Detector for CDMA Communications,"

IEEE Transactions on Vehicular Technology, vol. 56, pp. 3006–3013, September 2007.

[79] L. Hanzo, T. H. Liew, B. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart Aided Near-Capacity Designs for Wireless Channels*. John Wiley & Sons, 2010.

[80] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-Complexity Soft-Output Quantum-Assisted Multiuser Detection for Direct-Sequence Spreading and Slow Subcarrier-Hopping Aided SDMA-OFDM Systems," *IEEE Access*, vol. 2, pp. 451–472, May 2014.

[81] P. Botsinis, D. Alanis, Z. Babar, S. Ng, and L. Hanzo, "Iterative Quantum-Assisted Multi-User Detection for Multi-Carrier Interleave Division Multiple Access Systems," *IEEE Transactions on Communications*, vol. 63, pp. 3713–3727, July 2015.

[82] Y. Li, N. Seshadri, and S. Ariyavisitakul, "Channel Estimation for OFDM Systems with Transmitter Diversity in Mobile Wireless Channels," *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 461–471, Mar 1999.

[83] Y. Li, J. Winters, and N. Sollenberger, "MIMO-OFDM for Wireless Communications: Signal Detection with Enhanced Channel Estimation," *IEEE Transactions on Communications*, vol. 50, no. 9, pp. 1471–1477, 2002.

[84] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley Publishing, 2009.

[85] N. Seshadri, "Joint Data and Channel Estimation using Blind Trellis Search Techniques," *IEEE Transactions on Communications*, vol. 42, pp. 1000–1011, Feb 1994.

[86] S. Chen and Y. Wu, "Maximum Likelihood Joint Channel and Data Estimation Using Genetic Algorithms," *IEEE Transactions on Signal Processing*, vol. 46, pp. 1469–1473, May 1998.

[87] D. So and R. Cheng, "Iterative EM Receiver for Space-Time Coded Systems in MIMO Frequency-Selective Fading Channels with Channel Gain and Order Estimation," *IEEE Transactions on Wireless Communications*, vol. 3, pp. 1928–1935, Nov 2004.

[88] R. Prasad, C. R. Murthy, and B. D. Rao, "Joint Channel Estimation and Data Detection in MIMO-OFDM Systems: A Sparse Bayesian Learning Approach," *IEEE Transactions on Signal Processing*, vol. 63, pp. 5369–5382, Oct 2015.

[89] A. Assra, W. Hamouda, and A. Youssef, "EM-Based Joint Channel Estimation and Data Detection for MIMO-CDMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 1205–1216, March 2010.

[90] L. Zhang, L. Zhang, and H. Peng, "Quantum Clone Genetic Algorithm based Multi-User Detection," in *2nd International Conference on Next Generation Information Technology (ICNIT)*, pp. 115–119, June 2011.

[91] J. Zhang, S. Chen, X. Mu, and L. Hanzo, "Turbo Multi-User Detection for OFDM/SDMA Systems Relying on Differential Evolution Aided Iterative Channel Estimation," *IEEE Transactions on Communications*, vol. 60, pp. 1621–1633, June 2012.

[92] C. Novak, G. Matz, and F. Hlawatsch, "IDMA for the Multiuser MIMO-OFDM Uplink: A Factor Graph Framework for Joint Data Detection and Channel Estimation," *IEEE Transactions on Signal Processing*, vol. 61, pp. 4051–4066, Aug 2013.

[93] J. Zhang, S. Chen, X. Mu, and L. Hanzo, "Evolutionary-Algorithm-Assisted Joint Channel Estimation and Turbo Multiuser Detection/Decoding for OFDM/SDMA," *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 1204–1222, March 2014.

[94] P. Zhang, S. Chen, and L. Hanzo, "Embedded Iterative Semi-Blind Channel Estimation for Three-Stage-Concatenated MIMO-Aided QAM Turbo Transceivers," *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 439–446, January 2014.

[95] M. Jiang, J. Akhtman, and L. Hanzo, "Iterative Joint Channel Estimation and Multi-User Detection for Multiple-Antenna Aided OFDM Systems," *IEEE Transactions on Wireless Communications*, vol. 6, pp. 2904–2914, August 2007.

[96] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Joint Quantum-Assisted Channel Estimation and Data Detection," *IEEE Access*, vol. 4, pp. 7658–7681, 2016.

[97] L.-L. Yang, "Multiuser Transmission Via Multiuser Detection: Altruistic-Optimization and Egocentric-Optimization," in *IEEE 65th Vehicular Technology Conference (VTC)*, pp. 1921–1925, April 2007.

[98] H. Sung, S. R. Lee, and I. Lee, "Generalized Channel Inversion Methods for Multiuser MIMO Systems," *IEEE Transactions on Communications*, vol. 57, pp. 3489–3499, Nov 2009.

[99] W. Yao, S. Chen, S. Tan, and L. Hanzo, "Minimum Bit Error Rate Multiuser Transmission Designs Using Particle Swarm Optimisation," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 5012–5017, October 2009.

[100] S. Verdu, *Multiuser Detection*. New York, NY, USA: Cambridge University Press, 1st ed., 1998.

[101] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A Vector-Perturbation Technique for Near-Capacity Multiantenna Multiuser Communication-Part I: Channel Inversion and Regularization," *IEEE Transactions on Communications*, vol. 53, pp. 195–202, Jan 2005.

[102] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector Perturbation Based on Symbol Scaling for Limited Feedback MISO Downlinks," *IEEE Transactions on Signal Processing*, vol. 62, pp. 562–571, Feb 2014.

[103] C. B. Chae, S. Shim, and R. W. Heath, "Block Diagonalized Vector Perturbation for Multiuser MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 4051–4057, November 2008.

[104] W. Yao, S. Chen, and L. Hanzo, "Improved MMSE Vector Precoding Based on the MBER Criterion," in *IEEE Vehicular Technology Conference*, pp. 1–5, April 2009.

[105] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Computationally Efficient Vector Perturbation Precoding Using Thresholded Optimization," *IEEE Transactions on Communications*, vol. 61, pp. 1880–1890, May 2013.

[106] S. P. Herath, D. H. N. Nguyen, and T. Le-Ngoc, "Vector Perturbation Precoding for Multi-User CoMP Downlink Transmission," *IEEE Access*, vol. 3, pp. 1491–1502, 2015.

[107] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum-Aided Multi-User Transmission in Non-Orthogonal Multiple Access Systems," *IEEE Access*, vol. 4, pp. 7402–7424, 2016.

[108] B. Alawieh, Y. Zhang, C. Assi, and H. Mouftah, "Improving Spatial Reuse in Multihop Wireless Networks - A Survey," *IEEE Communications Surveys Tutorials*, vol. 11, pp. 71–91, rd 2009.

[109] Y. Chen, S. Zhang, S. Xu, and G. Y. Li, "Fundamental trade-offs on green wireless networks," *IEEE Communications Magazine*, vol. 49, pp. 30–37, June 2011.

[110] C. Luo, S. Guo, S. Guo, L. T. Yang, G. Min, and X. Xie, "Green communication in energy renewable wireless mesh networks: Routing, rate control, and power allocation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 3211–3220, Dec 2014.

[111] J. Wen, M. Sheng, X. Wang, J. Li, and H. Sun, "On the capacity of downlink multi-hop heterogeneous cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 4092–4103, Aug 2014.

[112] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for anets," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 2625–2635, July 2012.

[113] H. Huang, S. Guo, W. Liang, K. Li, B. Ye, and W. Zhuang, "Near-optimal routing protection for in-band software-defined heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 2918–2934, Nov 2016.

[114] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Transactions on Communications*, vol. 64, pp. 753–764, Feb 2016.

[115] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, "A survey of network lifetime maximization techniques in wireless sensor networks," *IEEE Communications Surveys Tutorials*, vol. 19, pp. 828–854, Secondquarter 2017.

[116] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "Network-lifetime maximization of wireless sensor networks," *IEEE Access*, vol. 3, pp. 2191–2226, 2015.

[117] Y. Shi, Y. T. Hou, and H. Sherali, "Cross-layer optimization for data rate utility problem in uwb-based ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 764–777, June 2008.

[118] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3GPP heterogeneous networks," *IEEE Wireless Communications*, vol. 18, no. 3, pp. 10–21, 2011.

[119] K. Deb, "Multi-objective optimization," in *Search Methodologies* (E. K. Burke and G. Kendall, eds.), pp. 273–316, Springer US, 2005.

[120] W. Stadler, "A survey of multicriteria optimization or the vector maximum problem, part i: 1776–1960," *Journal of Optimization Theory and Applications*, vol. 29, no. 1, pp. 1–52, 1979.

[121] E. Masazade, R. Rajagopalan, P. Varshney, C. Mohan, G. Sendur, and M. Keskinoz, "A multiobjective optimization approach to obtain decision thresholds for distributed detection in wireless sensor networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 40, no. 2, pp. 444–457, 2010.

[122] D. Alanis, P. Botsinis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "A quantum-search-aided dynamic programming framework for pareto optimal routing in wireless multihop networks," *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1–1, 2018.

[123] D. Alanis, P. Botsinis, Z. Babar, H. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum-aided multi-objective routing optimization using back-tracing-enabled dynamic programming," *IEEE Transactions on Vehicular Technology*, 2017. Under review.

[124] H. Yetgin, K. Cheung, and L. Hanzo, "Multi-objective routing optimization using evolutionary algorithms," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 3030–3034, 2012.

[125] J. Hu, L. L. Yang, and L. Hanzo, "Energy-efficient cross-layer design of wireless mesh networks for content sharing in online social networks," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2017.

[126] J. Zuo, C. Dong, H. V. Nguyen, S. X. Ng, L. L. Yang, and L. Hanzo, "Cross-layer aided energy-efficient opportunistic routing in ad hoc networks," *IEEE Transactions on Communications*, vol. 62, pp. 522–535, February 2014.

[127] M. Dehghan, M. Ghaderi, and D. Goeckel, "Minimum-energy cooperative routing in wireless networks with channel variations," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 3813–3823, November 2011.

[128] E. Dall'Anese and G. B. Giannakis, "Statistical routing for multihop wireless cognitive networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1983–1993, November 2012.

[129] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. Hanzo, "Cross-layer network lifetime maximization in interference-limited wsns," *IEEE Transactions on Vehicular Technology*, vol. 64, pp. 3795–3803, Aug 2015.

[130] A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, "Hymn: A novel hybrid multi-hop routing algorithm to improve the longevity of wsns," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2531–2541, 2012.

[131] L. Tan, Z. Zhu, F. Ge, and N. Xiong, "Utility maximization resource allocation in wireless networks: Methods and algorithms," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, pp. 1018–1034, July 2015.

[132] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numerische mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[133] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[134] D. Alanis, J. Hu, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Quantum-assisted joint multi-objective routing and load balancing for socially-aware networks," *IEEE Access*, vol. 4, pp. 9993–10028, 2016.

[135] M. Camelo, C. Omaa, and H. Castro, "Qos routing algorithm based on multi-objective optimization for wireless mesh networks," in *2010 IEEE Latin-American Conference on Communications (LATINCOM)*, pp. 1–6, 2010.

[136] A. Perez, M. Labrador, and P. Wightman, "A multiobjective approach to the relay placement problem in wsns," in *2011 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 475–480, 2011.

[137] F. Martins, E. Carrano, E. Wanner, R. H. C. Takahashi, and G. Mateus, "A hybrid multiobjective evolutionary approach for improving the performance of wireless sensor networks," *IEEE Sensors Journal*, vol. 11, no. 3, pp. 545–554, 2011.

[138] D. Pinto and B. Barán, "Solving multiobjective multicast routing problem with a new ant colony optimization approach," in *Proceedings of the 3rd international IFIP/ACM Latin American conference on Networking*, pp. 11–19, ACM, 2005.

[139] W. Zhang, M. F. Brejza, T. Wang, R. G. Maunder, and L. Hanzo, "Irregular trellis for the near-capacity unary error correction coding of symbol values from an infinite set," *IEEE Transactions on Communications*, vol. 63, pp. 5073–5088, Dec 2015.

[140] Q. You, Y. Li, M. S. Rahman, and Z. Chen, "A near optimal routing scheme for multi-hop relay networks based on viterbi algorithm," in *2012 IEEE International Conference on Communications (ICC)*, pp. 4531–4536, June 2012.

[141] Y. Wang, M. Z. Bocus, and J. P. Coon, "Dynamic programming for route selection in multihop fixed gain amplify-and-forward relay networks," *IEEE Communications Letters*, vol. 17, pp. 932–935, May 2013.

[142] G. D. Forney, "The viterbi algorithm," *Proceedings of the IEEE*, vol. 61, pp. 268–278, March 1973.

[143] S. Boixo, T. F. Rønnow, S. V. Isakov, Z. Wang, D. Wecker, D. A. Lidar, J. M. Martinis, and M. Troyer, "Evidence for quantum annealing with more than one hundred qubits," *Nature Physics*, vol. 10, no. 3, p. 218, 2014.

[144] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," *arXiv preprint quant-ph/0001106*, 2000.

[145] C. Wang, E. Jonckheere, and T. Brun, "Differential geometric treewidth estimation in adiabatic quantum computation," *Quantum Information Processing*, vol. 15, pp. 3951–3966, Oct 2016.

[146] C. Wang, H. Chen, and E. Jonckheere, "Quantum versus simulated annealing in wireless interference network optimization," *Scientific Reports*, vol. 6, no. 25797, 2016.

[147] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

[148] R. Crandall, C. Pomerance, R. Crandall, and C. Pomerance, *Prime Numbers: A Computational Perspective*. Springer, 2005.

[149] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, "Experimental realization of shor's quantum factoring algorithm using qubit recycling," *Nature Photonics*, vol. 6, pp. 773–776, 11 2012.

[150] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu, "Localization Via Ultra-Wideband Radios: A Look at Positioning Aspects for Future Sensor Networks," *IEEE Signal Processing Magazine*, vol. 22, pp. 70–84, July 2005.

[151] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern WLAN Fingerprinting Indoor Positioning Methods and Deployment Challenges," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, 2017.

[152] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. Wong, J. Schulz, M. Samimi, and F. Gutierrez, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[153] W. Roh, J. Y. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, and F. Aryanfar, "Millimeter-Wave Beamforming as an Enabling Technology for 5G Cellular Communications: Theoretical Feasibility and Prototype Results," *IEEE Communications Magazine*, vol. 52, pp. 106–113, February 2014.

[154] I. A. Hemadeh, M. El-Hajjar, S. Won, and L. Hanzo, "Layered Multi-Group Steered Space-Time Shift-Keying for Millimeter-Wave Communications," *IEEE Access*, vol. 4, pp. 3708–3718, 2016.

[155] V. Degli-Esposti, F. Fuschini, E. M. Vitucci, M. Barbiroli, M. Zoli, L. Tian, X. Yin, D. A. Dupleich, R. Mller, C. Schneider, and R. S. Thom, "Ray-Tracing-Based mm-Wave Beamforming Assessment," *IEEE Access*, vol. 2, pp. 1314–1325, 2014.

[156] S. Feng, X. Li, R. Zhang, M. Jiang, and L. Hanzo, "Hybrid Positioning Aided Amorphous-Cell Assisted User-Centric Visible Light Downlink Techniques," *IEEE Access*, vol. 4, pp. 2705–2713, 2016.

[157] S. Rajagopal, R. D. Roberts, and S. K. Lim, "IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support," *IEEE Communications Magazine*, vol. 50, pp. 72–82, March 2012.

[158] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 2047–2077, Fourthquarter 2015.

[159] K. Witrisal, P. Meissner, E. Leitinger, Y. Shen, C. Gustafson, F. Tufvesson, K. Haneda, D. Dardari, A. F. Molisch, A. Conti, and M. Z. Win, "High-Accuracy Localization for Assisted Living: 5G systems will turn multipath channels from foe to friend," *IEEE Signal Processing Magazine*, vol. 33, pp. 59–70, March 2016.

[160] A. Sahin, Y. S. Erolu, . Gven, N. Pala, and M. Yksel, "Hybrid 3-D Localization for Visible Light Communication Systems," *Journal of Lightwave Technology*, vol. 33, pp. 4589–4599, Nov 2015.

[161] M. Biagi, S. Pergoloni, and A. M. Vegni, "LAST: A Framework to Localize, Access, Schedule, and Transmit in Indoor VLC Systems," *Journal of Lightwave Technology*, vol. 33, pp. 1872–1887, May 2015.

[162] A. Conti, M. Guerra, D. Dardari, N. Decarli, and M. Z. Win, "Network Experimentation for Cooperative Localization," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 467–475, February 2012.

[163] H. Wymeersch, S. Marano, W. M. Gifford, and M. Z. Win, "A Machine Learning Approach to Ranging Error Mitigation for UWB Localization," *IEEE Transactions on Communications*, vol. 60, pp. 1719–1728, June 2012.

[164] P. Meissner and K. Witrisal, "Multipath-assisted single-anchor indoor localization in an office environment," in *International Conference on Systems, Signals and Image Processing (IWSSIP)*, pp. 22–25, April 2012.

[165] E. Leitinger, P. Meissner, C. Rdisser, G. Dumphart, and K. Witrisal, "Evaluation of Position-Related Information in Multipath Components

for Indoor Positioning," *IEEE Journal on Selected Areas in Communications*, vol. 33, pp. 2313–2328, Nov 2015.

[166] K. Qiu, F. Zhang, and M. Liu, "Let the Light Guide Us: VLC-Based Localization," *IEEE Robotics Automation Magazine*, vol. 23, pp. 174–183, Dec 2016.

[167] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," *Trans. Sys. Man Cyber Part C*, vol. 37, pp. 1067–1080, Nov. 2007.

[168] P. Botsinis, D. Alanis, S. Feng, Z. Babar, H. Nguyen, D. Chandra, S. X. Ng, R. Zhang, and L. Hanzo, "Quantum-Assisted Indoor Localization for Uplink mm-Wave and Downlink Visible Light Communication Systems," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[169] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob, "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.

[170] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. The MIT Press, 2012.

[171] C. M. Bishop, *Pattern Recognition and Machine Learning (Information Science and Statistics)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[172] C. J. C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition," *Data Mining and Knowledge Discovery*, vol. 2, pp. 121–167, 1998.

[173] S. T. Li and C. C. Chen, "A Regularized Monotonic Fuzzy Support Vector Machine Model for Data Mining With Prior Knowledge," *IEEE Transactions on Fuzzy Systems*, vol. 23, pp. 1713–1727, Oct 2015.

[174] Z. Qi, Y. Tian, and Y. Shi, "Successive Overrelaxation for Laplacian Support Vector Machine," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, pp. 674–683, April 2015.

[175] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum Support Vector Machine for Big Data Classification," *Physical Review Letters*, vol. 113, p. 130503, Sept. 2014.

[176] J. Suykens and J. Vandewalle, "Least Squares Support Vector Machine Classifiers," *Neural Processing Letters*, vol. 9, pp. 293–300, Jun 1999.

[177] S. Imre, "Quantum Existence Testing and Its Application for Finding Extreme Values in Unsorted Databases," *IEEE Transactions on Computers*, vol. 56, pp. 706–710, May 2007.

[178] S. Yang, X. Xu, D. Alanis, S. X. Ng, and L. Hanzo, "Is the low-complexity mobile relay aided FFR-DAS capable of outperforming the high-complexity CoMP?," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 2154–2169, April 2016.

[179] C. Pan, M. Elkashlan, J. Wang, J. Yuan, and L. Hanzo, "User-centric c-ran architecture for ultra-dense 5g networks: Challenges and methodologies," *IEEE Communications Magazine*, vol. 56, pp. 14–20, June 2018.

[180] H. Ren, N. Liu, C. Pan, M. Elkashlan, A. Nallanathan, X. You, and L. Hanzo, "Low-latency C-RAN: An next-generation wireless approach," *IEEE Vehicular Technology Magazine*, vol. 13, pp. 48–56, June 2018.

[181] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 1123–1152, Secondquarter 2016.

[182] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking Drones to the Next Level: Cooperative Distributed Unmanned-Aerial-Vehicular Networks for Small and Mini Drones," *IEEE Vehicular Technology Magazine*, vol. 12, pp. 73–82, Sept 2017.

[183] M. A. Maddah-Ali and U. Niesen, "Fundamental Limits of Caching," *IEEE Transactions on Information Theory*, vol. 60, pp. 2856–2867, May 2014.

[184] J. Tadrous and A. Eryilmaz, "On Optimal Proactive Caching for Mobile Networks With Demand Uncertainties," *IEEE/ACM Transactions on Networking*, vol. 24, pp. 2715–2727, Oct 2016.

[185] B. Azimdoost, C. Westphal, and H. R. Sadjadpour, "Fundamental Limits on Throughput Capacity in Information-Centric Networks," *IEEE Transactions on Communications*, vol. 64, pp. 5037–5049, Dec 2016.

[186] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications*, vol. PP, pp. 2–9, December 2016.

[187] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, p. 195, 2017.

[188] A. Kapoor, N. Wiebe, and K. Svore, "Quantum Perceptron Models," in *Advances in Neural Information Processing Systems*, pp. 3999–4007, 2016.

[189] N. Wiebe, A. Kapoor, and K. M. Svore, "Quantum deep learning," *arXiv preprint arXiv:1412.3489*, 2014.