IEEE Access
practical innovations : open solutions

Received March 17, 2013, accepted April 15, 2013, published May 10, 2013.

Digital Object Identifier 10.1109/ACCESS.2013.2259536

Quantum Search Algorithms, Quantum Wireless, and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design

PANAGIOTIS BOTSINIS (Student Member, IEEE), SOON XIN NG (Senior Member, IEEE), AND LAJOS HANZO (Fellow, IEEE)

School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, U.K.

Corresponding author: P. Botsinis (pb8g10@ecs.soton.ac.uk)

This work was supported in part by the RC-UK, India-UK Advanced Technology Centre (IU-ATC), EU, under the Concerto Project, and the European Research Council Advanced Fellow Grant.

ABSTRACT The high complexity of numerous optimal classic communication schemes, such as the maximum likelihood (ML) multiuser detector (MUD), often prevents their practical implementation. In this paper, we present an extensive review and tutorial on quantum search algorithms (QSA) and their potential applications, and we employ a QSA that finds the minimum of a function in order to perform optimal hard MUD with a quadratic reduction in the computational complexity when compared to that of the ML MUD. Furthermore, we follow a quantum approach to achieve the same performance as the optimal soft-input soft-output classic detectors by replacing them with a quantum algorithm, which estimates the weighted sum of a function's evaluations. We propose a soft-input soft-output quantum-assisted MUD (QMUD) scheme, which is the quantum-domain equivalent of the ML MUD. We then demonstrate its application using the design example of a direct-sequence code division multiple access system employing bit-interleaved coded modulation relying on iterative decoding, and compare it with the optimal ML MUD in terms of its performance and complexity. Both our extrinsic information transfer charts and bit error ratio curves show that the performance of the proposed QMUD and that of the optimal classic MUD are equivalent, but the QMUD's computational complexity is significantly lower.

INDEX TERMS Bit-interleaved coded modulation, computational complexity, EXIT chart, Grover's quantum search algorithm, BBHT quantum search algorithm, Dürr–Høyer algorithm, iterative decoding, multi-user detection, quantum amplitude amplification, quantum amplitude estimation, quantum computation, quantum entanglement, quantum mean algorithm.

NOMENCLATURE

ACO	Ant Colony Optimization
APP	*A Posteriori* Probability
AWGN	Additive White Gaussian-distributed Noise
BBHT	Boyer-Brassard-Høyer-Tapp
BER	Bit Error Ratio
BICM	Bit-Interleaved Coded Modulation
BS	Base Station
CF	Cost Function
CIR	Channel Impulse Response
COMP	Cooperative Multi-cell Processing
DHA	Dürr–Høyer Algorithm
DS-CDMA	Direct-Sequence Code Division Multiple Access
EPR	Einstein-Podolsky-Rosen
EXIT	Extrinsic Information Transfer
GA	Genetic Algorithm
ID	Iterative Decoding
IQFT	Inverse Quantum Fourier Transform
LLR	Log-Likelihood Ratio
MBER	Minimum Bit Error Ratio
MC	Multi-Carrier
MF	Matched Filter
MFAA	Multi-Functional Antenna Array
MIMO	Multiple-Input Multiple Output
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
MSE	Mean Square Error
MUA	Multi-input-approximation
MUD	Multi-User Detection
MUI	Multi-User Interference
NSCC	Non-Systematic Convolutional Code

OFDM	Orthogonal Frequency-Division Multiplexing
PSO	Particle Swarm Optimization
QAA	Quantum Amplitude Amplification
QAE	Quantum Amplitude Estimation
QAM	Quadrature Amplitude Modulation
QCA	Quantum Counting Algorithm
QCR	Quantum Control Register
QD	Quantum Domain
QET	Quantum Existence Testing
QFR	Quantum Function Register
QFT	Quantum Fourier Transform
QGOA	Quantum Genetic Optimization Algorithm
QIR	Quantum Index Register
QMA	Quantum Mean Algorithm
QMUD	Quantum Multi-User Detection
QoS	Quality of Service
QR	Quantum Register
QSA	Quantum Search Algorithm
QWSA	Quantum Weighted Sum Algorithm
SDMA	Spatial Division Multiple Access
SF	Spreading Factor
SISO	Soft-Input Soft-Output
SM	Spatial Multiplexing
SNR	Signal to Noise Ratio
TCCC	Turbo Coding relying on Convolutional Codes
UWB	Ultra-Wide Band

I. MOTIVATION

The history of wireless communications, the evolution of standards and a host of popular enabling techniques was detailed in [1]. These solutions paved the way for inching closer to the Shannonian channel capacity limits. However, these ultimate limits may only be approached for a single user link subjected to pure Additive White Gaussian-distributed Noise (AWGN) under Shannon's idealized simplifying assumptions of using random Gaussian transmit signals. However, in practical state-of-the-art systems we employ digital, rather than Gaussian transmit signals. Furthermore, no quantitative statements were made by Shannon as regards to the system's delay and complexity, whilst in practice only the family of powerful and hence high-complexity, high-delay channel coded systems might be capable of approaching these limits and even then only under perfectly synchronized conditions. Regretfully however, perfect synchronization at near-capacity Signal-to-Noise Ratios (SNR) is again, a real challenge. Hence *the myth of operating in the vicinity of Shannon's capacity limit in practical systems was dispelled in [2], where it was quantitatively demonstrated with the aid of painstakingly meticulous measurements that only a fraction of the theoretically attainable capacity is actually achieved by the standardized systems.*

Another limitation imposed on the operational standard systems is that a single link's Shannonian capacity is limited by the logarithmic Bit/Hz normalized capacity formula of $C/B = \log_2(1 + SNR)$, which only allows the capacity to be increased logarithmically with the SNR, i.e. with the transmit power, where B is the available bandwidth. Nonetheless, we hasten to add that when B tends to infinity, like in Ultra-Wide Band (UWB) systems for example, this capacity formula also tends to a linearly increasing function of the SNR. By contrast, provided that we can construct a sufficiently high number of parallel streams and additionally, we are capable of conceiving low-complexity full-search-based detection techniques, the throughput of wireless systems may be increased linearly, rather than logarithmically with the transmit power, leading to the concept of power-efficient "green" communications systems, which was the motto of the book [3].

Given this motivation, let us briefly elaborate on the potential techniques of creating parallel streams in wireless systems and then embark on conceiving high-efficiency quantum-processing techniques for creating powerful detectors for them!

A. LARGE-DIMENSIONAL HOLISTIC OPTIMIZATION IN WIRELESS SYSTEMS

1) The family of multi-stream wireless systems, such as for example the single-carrier Direct-Sequence Code Division Multiple Access (DS-CDMA) [4], [5] scheme of the operational third-generation wideband-CDMA systems are capable of increasing the throughput linearly with the transmit power - provided that we assign multiple superimposed spreading codes to each of the K users supported.
2) Similarly, the pan-American Multi-Carrier (MC) DS-CDMA [5]–[7] cdma2000 system supports a multiplicity of users by allocating unique, user-specific spreading codes to them, which are also often referred to as user signatures. The throughput of MC-CDMA may also be increased linearly with the transmit power, since we can create superimposed parallel streams in both the time-domain and frequency-domain. Hence it may be anticipated that MC-CDMA systems will play a prominent role in future generations of wireless systems.
3) As a further dimension for creating superimposed parallel streams, the spatial domain of parallel transmit and receive antennas was proposed in the context of Multi-Functional Antenna Arrays (MFAA) [1]:
   - To elaborate a little further, firstly, MFAAs are capable of achieving a multiplexing gain by transmitting independent parallel streams, which may be separated at the receiver, provided that we can estimate the unique, antenna-specific Channel Impulse Responses (CIR) sufficiently accurately at the receiver. This scheme is termed as Spatial Multiplexing (SM).
   - Secondly, the MFAAs are also capable of supporting the uplink transmissions of multiple users instead of transmitting multiple streams for a single user, which is referred to as Spatial Division Multiple Access (SDMA) [8]–[10]. Similarly to separating multiple streams in spatial multiplexing,

in SDMA the separation of users is achieved with the aid of the accurately estimated unique, user-specific CIRs.

- The third key function of MFAAs is the provision of diversity gain for the sake of mitigating the deleterious effects of the wireless channel's fading imposed by the sometimes constructively, sometimes destructively superimposed multiple propagation paths. Naturally, the multiplicity of propagation paths contribute further towards the gradually escalating number of parallel streams, which may be coherently combined with the aid of maximum ratio combining for the sake of mitigating the effects of fading. It is important to note however that in order to achieve the maximum attainable diversity gain, the MFAA elements have to be sufficiently far apart for experiencing independent fading.
- The MFAAs are also capable of attaining angular selectivity, hence potentially mitigating the effects of interference amongst the users, which is termed as co-channel or Multi-User Interference (MUI) - provided that the interfering signals arrive from angles outside the beamformer's main transmit/receive beam. These beamformers typically employ MFAA elements, which are half-the-wavelength apart, because in contrast to the independently fading signal components of the transmit diversity schemes, they aim for transmitting/receiving appropriately phase-combined signal components for creating maxima in the desired user's direction and minima towards the interferers.
- Finally, all the above-mentioned design objectives of MFAAs may be combined in the interest of benefiting from all of these desirable performance improvements—again, provided that low-complexity multi-stream detectors may be conceived.

Similarly to MC-CDMA, all the above-mentioned concepts are also applicable to the fourth-generation Multiple-Input Multiple Output (MIMO) aided Orthogonal Frequency-Division Multiplexing (OFDM) systems [11]–[13], where the users convey their information to and from the Base Station (BS) over multiple subcarriers.

4) However, so far we have only alluded to the multiple streams generated by multiple users and the MFAAs within a single cell. In reality one of the most severe performance limitation of wireless systems is constituted by the MUI imposed by the adjacent cells, because this can only be mitigated with the aid of Cooperative Multi-cell Processing (COMP). More explicitly, the basic philosophy of COMP is that the base-stations are linked with the aid of either optical fibre or by a point-to-point microwave link and this way they exchange all their information, including all the uplink and downlink data of all the users, as well as their CIRs.
5) Albeit the COMP concept imposes a huge amount of data exchange amongst the BSs, as a benefit, *no MUI is experienced, because all the energy received by all receivers is useful signal energy and hence directly contributes towards achieving the best possible holistic system performance. As a result, the theoretically best possible multi-user, multi-cell performance constituted by an idealized system, where the only performance impairment is the AWGN may be asymptotically approached - again, provided that low-complexity parallel processing aided receivers may be constructed.* Expanding the multi-cell, multi-user optimization concept [14], [15] yet another step further, accurate near-instantaneous power control is required at the COMP-aided BSs in order to minimize the transmit power, while maintaining the required Quality of Service (QoS) constraints for each of the K users [16], [17]. In the operational standardized systems this is achieved by carefully optimizing both the step-size and the instants of power-updates as a function of the vehicular speed, but these step-by-step sequential power-adjustments do not necessarily approach the optimum, especially not for high velocities. *Hence a near-instantaneous "direct-dial-style" parallel power-adjustment of all transmitters would be desirable across the entire system.*
Additional large-dimensional optimization algorithms processing numerous parallel streams in wireless communication systems involve message-routing across large cooperative and multi-hop networks [18]–[22], where the specific multi-hop routing path having the minimum overall length, or the minimum number of hops or alternatively, the maximum received power between two predetermined nodes has to be found. These techniques may be readily combined with sophisticated message-scheduling and resource allocation [23], [24], as well as with cognitive radio techniques relying on efficient channel- and power-allocation designed for the primary user [25], [26]. Moreover, soft information exchange between the signal detector and the channel-decoding stages is required in the green communication systems of the future, where holistic optimization is pursued [27] as well as in massive MIMO systems [2], [11], [28], [29] where the computational complexity of the optimal full-search-based algorithms is potentially excessive. *As a remedy, in the next section we propose quantum-domain parallel processing techniques for implementing the above-mentioned massive parallel processing tasks.*

B. MULTI-STREAM DETECTION IN LARGE-DIMENSIONAL WIRELESS SYSTEMS

As argued above, the employment of algorithms imposing a low computational complexity is essential, since

low-complexity algorithms impose a low power-dissipation, which hence requires desirably low-weight, potentially solar-charged or kinetically-charged batteries for the shirt-pocket-sized wireless handsets.

A plethora of both Multi-User Detection (MUD) and multi-stream detections techniques has been proposed in the literature, as detailed for example in [4], [5]. In simple physically tangible terms we may argue that provided all the K users' signals in the above-mentioned holistically optimized system arrive at the base-station synchronously and they transmit M-ary signals, then the optimum full-search-based receiver has to tentatively check all the M^K symbol combinations, in order to reliably detect each of the K user's symbols. More specifically, this is achieved by identifying the most likely transmitted M-ary symbol of all the K users of the entire multi-user, multi-cell system by evaluating a carefully chosen Cost Function (CF), which may be the Mean Squared Error (MSE) or the Bit Error Ratio (BER), etc. *Suffice to say, however that when using 64-level Quadrature Amplitude Modulation (QAM) for example at an airport, where say 10 000 users would like to use their phones/tablet computers, it is entirely unrealistic to evaluate the CF* $64^{10\,000}$ *times...*

This is where Quantum Computing may be employed in the above-mentioned systems for reducing the complexity of the above-mentioned processes by exploiting its inherent parallelism as illustrated in Fig. 1. Assuming that only one of the eight keys unlocks the box in Fig. 1, serial computing would have to perform consecutive trials until the correct key is found, requiring a long time for solving this problem. By contrast, parallel computing would recreate the box eight times and try all the keys in parallel, which is more efficient as far as the required time is concerned, but it requires more hardware resources. Quantum computing on the other hand is capable to try all the keys at the same time in the context of a single box.

Following the above low-paced tutorial exposure, in the rest of this treatise we will expedite the speed of developing our ideas. We continue by reviewing the family of quantum search algorithms that may be used in the above-mentioned large-dimensional wireless systems and then conclude by providing a radically new quantum-MUD DS-CDMA design example.

II. INTRODUCTION

The employment of MUD facilitates achieving a near-single-user performance with the aid of joint iterative detection and decoding, exchanging extrinsic information in the form of Log-Likelihood Ratios (LLR) between the receiver components. The complexity of the optimal Maximum Likelihood (ML) MUD [30] exhibits an exponential increase with the number of users, which prohibits its employment when many simultaneous users are supported by the system. Hence reduced-complexity solutions have been developed, such as the decorrelating and the Minimum Mean-Square Error (MMSE) MUDs [31], the iterative linear MMSE MUD [32], as well as the successive interference cancellation aided detector [33] and the family of iterative interference cancellers [34]. Following an approach, where the aim is to directly minimize the system's BER, the Minimum BER (MBER) detector was conceived [35], [36]. MUDs that can be integrated into an iterative receiver, providing soft decisions for the decoder, while accepting soft estimates from the decoder, have also been proposed [6], [37], [38].

Bio-inspired heuristic algorithms have also been conceived for shrinking the search space by performing a random-guided search, which are capable of near-optimal MUD. For example, Genetic Algorithm (GA)-based MUDs have been proposed in [39]–[41]. Furthermore, an Ant Colony Optimization (ACO) algorithm-based MUD was proposed for the uplink of a synchronous MFAA-assisted MC DS-CDMA system in [7], while its soft-output version, termed as the multi-input-approximation (MUA)-assisted soft output-ACO MUD, was presented in [42]. By exploiting the sheer power of Particle Swarm Optimization (PSO) algorithms,

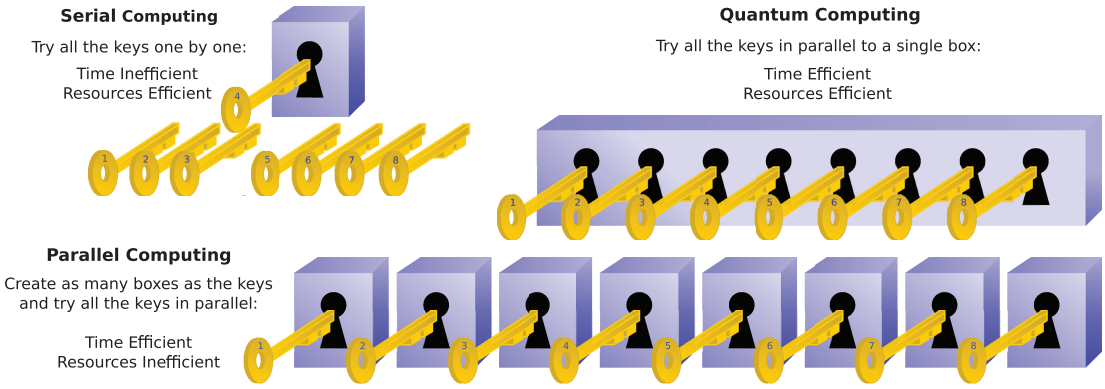

FIGURE 1. Comparison between classic serial, parallel and quantum computing. Assuming that only one of the eight keys unlocks the box, by employing serial computing we have to try each of the keys sequentially until one succeeds to unlock it. Classic parallel computing creates as many boxes as the available keys and tries all of them at once, requiring a large amount of resources. With quantum computing we are able to try all the keys in parallel on a single box. The box corresponds to a function, while the keys represent the legitimate inputs of the function. The key that unlocks the box is the input of the function which will lead to a desired output. By employing quantum computing, the function may be evaluated for the inputs in parallel, as in parallel computing, with the computational cost of a single evaluation, as in serial computing.

PSO-based MUDs were proposed in [43], [44], while further low-complexity suboptimal MUDs were presented in [45], [46].

With the size of a single transistor constantly shrinking according to Moore's law, it is expected to reach the atomic scale in a few years, where the postulates of quantum mechanics replace the laws of classic physics. The transition to quantum computing will unlock capabilities that a conventional classic computer is inherently incapable of [47]–[50]. For instance, quantum computing allows parallel evaluations of a function at a complexity equivalent to that of a single classic evaluation. An astonishing example of the power of quantum computing is the Quantum Amplitude Amplification (QAA) algorithm analysed in [51] employed in Grover's Quantum Search Algorithm (QSA) [52], [53], which performs search in an unsorted database having N elements and finds a single *solution*[1] at a complexity order of $O(\sqrt{N})$, in contrast to its classic optimal counterpart imposing $O(N)$ operations. Boyer *et al.* [54] proposed the so-called Boyer-Brassard-Høyer-Tapp (BBHT) QSA, which is also based on quantum amplitude amplification and manages to perform search in an unsorted database even when the number of solutions is higher than one and even if the exact number is not known *a priori*. The Dürr–Høyer algorithm (DHA) presented in [55] manages to find the index of the minimum entry in a database by activating the BBHT QSA multiple times.

In addition to the breakthroughs in quantum error correction [56], [57] and quantum cryptography [58], [59], a substantial amount of research has been devoted to the quantum search-based MUD field by creating quantum-assisted MUDs (QMUD) [48], [60], where classic algorithms are combined with quantum-processes. It should be noted that the communications systems we investigate operate in the classic domain and only the QMUD processes are performed in the Quantum Domain (QD). The inputs and outputs of the QMUD are in the classic domain, as presented in Fig. 2. A representative example of a quantum-assisted MUD was proposed in [60], [61], where the Quantum Counting Algorithm (QCA) of [62] is employed. Quantum-inspired MUDs have also been proposed, adopting quantum-domain attributes in the classic domain. Representative examples of quantum-inspired MUDs are the combinations of the heuristic algorithms combined with quantum principles, such as the quantum PSO-based MUDs of [63]–[65], the quantum GA-optimized neural network employed for signal detection in [66], and the quantum GA-based MUDs of [67]–[69].

Our novel contributions are:

1) We have proposed a Maximum Likelihood Quantum-assisted Multi-User Detector (ML QMUD), where all the legitimate combinations of the users' transmitted symbols are taken into consideration at the receiver. The ML QMUD matches the performance of the classic ML MUD, while achieving a quadratic reduction in computational complexity.
2) We have designed the first Soft-Input Soft-Output Quantum-assisted MUD (SISO QMUD) for forwarding the bit LLRs to the decoding stage in the classic domain and for processing the decoder's soft outputs as a priori information also in the classic domain, making it eminently eligible for integration into an iterative receiver.
3) We have provided EXtrinsic Information Transfer (EXIT) charts [4], [70] for the proposed QMUDs, comparing them with those of the ML MUD.

[1]A solution is an index of the database the entry of which satisfies the search problem.

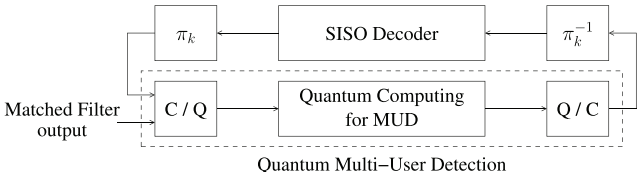

FIGURE 2. Block diagram of soft-input soft-output quantum-assisted multi-user detection, where the input/output signals are converted from/to the classic domain (C) to/from the quantum domain (Q), while the inner operations are performed in the quantum domain.

Based on the QD algorithm of estimating the mean of a function [71], also termed as the Quantum Mean Algorithm (QMA), we conceived an algorithm for estimating the weighted sum of a function. Explicitly, we propose an algorithm termed as the Quantum Weighted Sum Algorithm (QWSA) for estimating the LLRs. This is achieved by computing the numerators and denominators of the LLRs, which involve the summations of conditional probabilities. These operations represent the CF evaluations, while the corresponding a priori probabilities act as the weights of the conditional probabilities, as detailed in Section VII.

The rest of the paper is structured as follows. We will apply the proposed QMUD scheme in a communications system presented in Section III. A review of QSAs and their applications is offered in Section IV. The relevant theoretical background on quantum computing is provided in Section V, while Section VI introduces Grover's QSA, the BBHT algorithm and finally the DHA, which will also be exploited in our proposed QMUD. Section VII introduces the QMA and proposes the measures required for the transfiguration of the QMA into the QWSA. Section VIII states the CF normalization issues and the resultant computational complexity of the QWSA-based MUD, while the performance of our system employing both Bit-Interleaved Coded Modulation (BICM) relying on Iterative Decoding (ID) and on turbo codes is presented in Section IX. Finally, our conclusions are offered in Section X.

III. SYSTEM OVERVIEW

BICM-ID will be used in our uplink communications system presented in Fig. 3. The information bit stream $\{b_k\}$ of each user is encoded into the stream $\{c_k\}$ by a convolutional encoder, which is passed through pseudo-random bit-based interleavers. Then, the interleaved bits $\{u_k\}$ are spread by the user-specific DS-CDMA sequences of the codebook $\mathbf{C}$ and

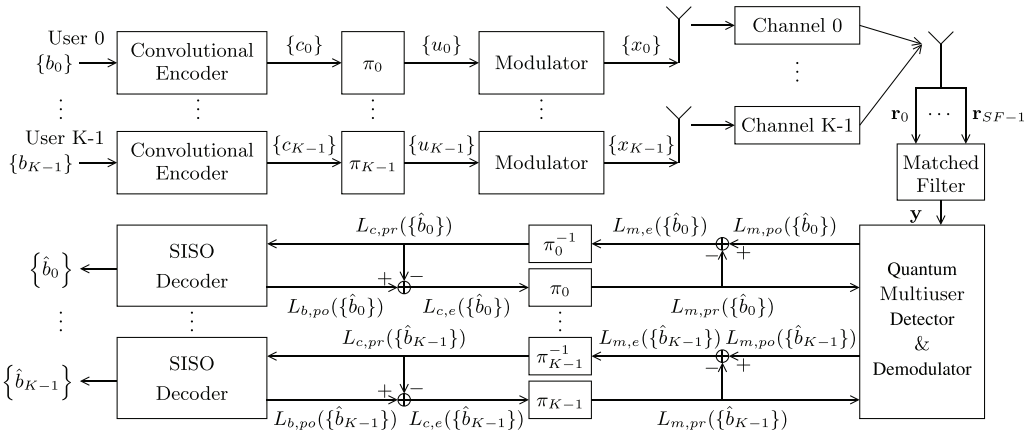

FIGURE 3. BICM-ID system's block diagram with K users and quantum-assisted multi-user detection with soft-input and soft-output.

are modulated onto the symbols $\{x_k\}$, which are transmitted over uncorrelated Rayleigh channels over T time slots. The channel matrix $\mathbf{H}$ is assumed to be perfectly estimated at the BS. Moreover, the DS-CDMA codebook $\mathbf{C} = [\mathbf{c}_0, \ldots, \mathbf{c}_{K-1}]$ storing $\mathbf{c}_k = [c_{k,0} \ldots c_{k,SF-1}]^T$ employed by the individual users having a specific Spreading Factor (SF) is known at the BS. On the other hand, the thermal noise imposed at the receiver, along with the time delay introduced during the propagation is unknown. However, since we assume non-dispersive Rayleigh fading, only the noise levels are unknown.

The classic optimal MUD that accepts soft inputs and provides soft outputs is the one that computes the bit LLRs of every bit of every symbol of each user. Let us consider a multi-user system supporting K users and employing an M-ary modulation scheme. Omitting the time superscript, the Matched Filter's (MF) outputs during a single time slot are described by

$$\begin{aligned}\mathbf{y} &= \mathbf{C}^H\mathbf{C}\mathbf{H}\mathbf{x} + \mathbf{C}^H\mathbf{n} \\ &= \mathbf{R}\mathbf{x} + \tilde{\mathbf{n}}\end{aligned} \tag{1}$$

where $\mathbf{y} = [y_0, \ldots, y_{K-1}]^T$ includes each user's MF output during the same time slot, $\mathbf{x} = [x_0, \ldots, x_{K-1}]^T$ is the multi-level symbol, $\mathbf{n} = [n_0, \ldots, n_{SF-1}]^T$ contains the complex-valued thermal noise at the BS, where we have $\mathbf{R} = \mathbf{C}^H\mathbf{C}\mathbf{H}$ and $\tilde{\mathbf{n}} = \mathbf{C}^H\mathbf{n} = [\tilde{n}_0, \ldots, \tilde{n}_{K-1}]^T$.

The bit-based metric computed at the MUD is the *a posteriori* information of the encoded, interleaved bits, presented in terms of the LLRs as [4]

$$\begin{aligned}L_{m,po}\left(b_k^{(m)}\right) &= \ln \frac{P\left(b_k^{(m)} = 0|\mathbf{y}\right)}{P\left(b_k^{(m)} = 1|\mathbf{y}\right)} \\ &= \log \frac{\left[\sum_{\mathbf{x}\in\chi(k,m,0)} P\left(\mathbf{y}|\mathbf{x}\right) P(\mathbf{x})\right] / P(\mathbf{y})}{\left[\sum_{\mathbf{x}\in\chi(k,m,1)} P\left(\mathbf{y}|\mathbf{x}\right) P(\mathbf{x})\right] / P(\mathbf{y})}\end{aligned} \tag{2}$$

where the subscript k is the index of the specific user $k \in \{0, \ldots, K-1\}$ the bit belongs to, the superscript $m \in \{0, \ldots, \log_2(M)-1\}$ denotes the index of the particular bit the LLR is computed for in the symbol of the kth user, M is the size of the modulation constellation, $\chi(k, m, v)$ is the set of multi-level symbols for which the $\left(k\log_2(M)+m\right)$th bit is equal to v, $P(x)$ is the *a priori* probability of the symbol x, $P(\mathbf{y})$ is the model's likelihood, which reflects the probability of receiving $\mathbf{y}$ as [4]

$$P(\mathbf{y}) = \sum_{\mathbf{x}} P\left(\mathbf{y}|\mathbf{x}\right) P(\mathbf{x}) \tag{3}$$

$P(\mathbf{y}|\mathbf{x})$ is the CF, which represents the probability of having received $\mathbf{y}$, given that the multi-level symbol $\mathbf{x}$ was transmitted [4]

$$f(\mathbf{x}) = P(\mathbf{y}|\mathbf{x}) = \exp\left(-\|\mathbf{y} - Rx\|^2 / 2\sigma^2\right) \tag{4}$$

where σ^2 is the noise variance. Assuming the independence of the bits in a symbol, the *a priori* symbol probability is equal to the product of the *a priori* bit probabilities that the symbol was created from, i.e. we have

$$P(\mathbf{x}) = P(b_0^{(0)}) \cdot \ldots P\left(b_0^{(\log_2(M)-1)}\right) \cdot \ldots P\left(b_{K-1}^{(\log_2(M)-1)}\right). \tag{5}$$

It should be noted that $M^K/2$ CF evaluations are required in the summation in each of the numerator and denominator of (2).

The extrinsic LLRs are passed to the K Max-Log *A Posteriori* Probability (APP) decoders [4], which in turn feed the QMUD with symbol probabilities, given the received encoded soft sequence. These iterations are continued for a specific number of iterations. During the first iteration, or if the MUD is not part of an iterative procedure, as in non-iterative BICM, all the symbols have equal *a priori* probabilities, since no extrinsic information is available.

IV. ORIGINS OF QUANTUM COMPUTING

Research on Quantum Mechanics initiated in 1923 by the renown physicists Planck, Bohr, Heisenberg, Einstein and

Schrödinger. Even though arguments have been arisen against quantum mechanics being a compact and complete theory of describing nature, quantum mechanics is considered to be the superset of physical theories describing both the microscopic and macroscopic worlds, while abiding by the laws of the Newtonian theory.

By using the principles of quantum mechanics in order to improve intelligent computational systems, the field of Quantum Computing emerged. In 1981, Feynman introduced the concept of a quantum computer, which would be able to accurately simulate the evolution of a quantum system [72]. It was only a year later when Benioff presented a complete theoretical framework of the quantum computer concept [73]. The structural element of a quantum computer is a quantum bit, or *qubit*, that, in comparison to the classic bit, has values that are not limited to 0 and 1. Quite the contrary, it can have any of these two values like a spinning coin in a box, which will only assume the value of ''Heads'' or ''Tails'' upon observing it when it stopped. This phenomenon is also often referred to as being in a superposition of the two orthogonal states, 0 and 1 [47]. The reason for this superposition of states being seemingly absent in the macroscopic world is related to the observation of the qubit. When a qubit is observed or ''measured'', any superposition of states that it might have assumed ''collapses'' to the classic states of 0 or 1, as stated by the so-called Copenhagen interpretation [74], introduced by Bohr and Heisenberg in 1924. As a further terminology, Everett in 1957 proposed the ''Many-World'' or ''Parallel-Universes'' interpretation [75], where an observation of a quantum state creates parallel universes that carry on with a different observation outcome taking place in each.

Quantum computing exploits a range of astonishing, non-intuitive characteristics of quantum mechanics, such as quantum parallelism, a term coined by Deutsch in 1985 [76], and entanglement [80] to accomplish computational tasks of stunningly high complexity, which would be deemed excessive in the classic computing world. Entanglement is a mysterious connection that can be established between qubits, where the observation of one of the entangled qubits allows instantaneous knowledge to be obtained for the other qubit. Einstein, Podolsky and Rosen challenged the validity of using quantum mechanics for describing nature by presenting a thought experiment which leads to a paradox (EPR paradox) [81]. Their thought experiment is based on the entanglement between particles. Assume that there are two particles, A and B, which interact with each other and then they are moved to different locations. Quantum theory and Heisenberg's uncertainty principle state that it is impossible to have knowledge of both the position and the momentum of a particle. According to the EPR thought experiment, if a measurement of A's position is made, then the position of B can be calculated. Therefore, the same statement can be made for B's momentum, and hence A's momentum can be calculated. Therefore, both the position and the momentum of particle B become known, resulting in a paradox. Hence Einstein's belief was that quantum mechanics was not a complete theory of nature. As a further advance, in 1966 Bell showed that at least one of the initial assumptions of Einstein, Podolsky and Rosen, namely locality and reality, was flawed, which was encapsulated in Bell's inequalities in [80].

Quantum parallelism is the ability to evolve the qubits of a quantum system in parallel, saving a large amount of computational complexity, when compared to classic computing. Quantum parallelism was first exploited by Deutsch in 1985, who proposed a quantum algorithm [76] based on the principles of quantum parallelism and quantum interference, which is also part of quantum mechanics. By applying Deutsch's algorithm to a function $f : \{0, 1\} \rightarrow \{0, 1\}$, a global property can be determined by relying on a single evaluation of f. This property is the determination of whether the function f is an one-to-one mapping function, hence whether $f(0) \oplus f(1) = 1$, or not, resulting in $f(0) \oplus f(1) = 0$. In the context of a classic apparatus two evaluations of f would be required, one for each legitimate input.

In 1992, Deutsch and Jozsa [77] generalized Deutsch's algorithm of [76]. This algorithm was used to solve the so-called generalized Deutsch problem [77]. Converted into a real life scenario for better intuition, two persons are considered, Alice and Bob, with Alice classically transmitting a number x to Bob with $x \in \{0, 2^n - 1\}$ and $n \in \mathbb{N}$. When Bob receives this number, he evaluates a function $f(x)$ and sends the resultant value back to Alice, which may be either 0 or 1. The function that was used by Bob is either a constant function, in which case the output is fixed to a single value, namely to 0 or 1, regardless of the input, or balanced, which means that for half the possible inputs the outcome is 0 and for the other half it is 1. Alice's goal is to determine whether the function that was used by Bob is a constant or balanced, which she intends to find out by iterating the above procedure. More explicitly, by applying the Deutsch-Jozsa algorithm [77], Alice could achieve her goal in a single correspondence, while in classic computing $2^{n-1} + 1$ enquiries would be required in the worst case scenario, which includes f being a constant and hence reaching this conclusion after evaluating just over half of the legitimate inputs. The best case scenario in classic computing may occur when f is balanced and its first two evaluations output different values. The Deutsch-Josza algorithm was further improved by Cleve, Ekert, Macchiavello and Mosca in [79], where the phase estimation quantum algorithm was introduced.

In 1994 Shor proposed a number of algorithms for quantum computation [78], such as for example a quantum algorithm conceived for integer factorization. Furthermore, Shor introduced the concept of the Quantum Fourier Transform (QFT) [78]. A range of techniques for constructing unitary transformations in the form of matrices, which are used for describing the time-domain evolution of any quantum system, i.e. its consecutive states as a function of time were also presented. During the same year, Simon managed to solve a black-box problem by using on the order of $O(n)$ queries to the black box, compared to the optimal classic algorithm, which uses $\Omega(2^{n/2})$ queries for the same task [82]. The black

box U_f implements a function $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$, which constitutes the input to the problem and has the property that $f(x) = f(y)$ if and only if $x = y$ or $x \oplus y = s$, for some $s \in \{0, 1\}^n$, where $x, y \in \{0, 1\}^n$. Simon's algorithm succeeds in finding this s that satisfies the function's above-mentioned property.

In the mid 1990's the field of quantum-domain search and quantum-assisted optimization of intelligent computational systems started gaining substantial momentum based on the Deutsch-Jozsa algorithm [77] and Shor factoring algorithm [78]. The quantum algorithms touched upon are summarized in Table 1. The rest of this section continues by introducing the quantum search algorithms along with their applications in the field of wireless communications. Nevertheless, this does not limit the applications of the quantum algorithms, since at the time of writing substantial research efforts are devoted into quantum-based communications, where quantum information is conveyed over quantum channels [95]–[97], with particularly attractive applications in the field of optical communications [98], [99].

A. ORIGINS AND APPLICATIONS OF QUANTUM SEARCH ALGORITHMS

In 1996 Grover proposed a quantum mechanical algorithm for performing quantum search in an unsorted classic database [52], [53]. Grover's QSA finds the index of the desired entry in the classic database, assuming that the desired value appears only once in the classic database, or, in other words, when there is only one solution in the classic database. During the same year, Boyer, Brassard, Høyer and Tapp (BBHT) in [54] generalized Grover's QSA to the case, where the desired value appears in more than one entry in the classic database. In the same paper, they proposed the BBHT algorithm, which yields the index of an entry having the desired value, provided that the number of identical desired entries is unknown *a priori*. Furthermore, they derived a closed-form mathematical expression for quantifying the success probability of Grover's QSA in identifying the desired entry. Grover's QSA is essentially an amplitude amplification process that allows the retrieval of the desired search outcome after a specific number L of tentative evaluations in the classic database [51]. The computational complexity of searching an unsorted classic database of size N by employing classic computing is $O(N)$, whereas by using Grover's QSA is $O(\sqrt{N})$.

In July of 1996 Dürr and Høyer proposed the DHA for finding the minimum entry in a classic database with $\sim 100\%$ probability, based on the BBHT QSA [55]. Furthermore, Bennett *et al.* in [83] proved that Grover's QSA is asymptotically optimal, by formally showing that there exists no quantum algorithm that can satisfy the search problem in fewer than $O(\sqrt{N})$ computational steps. In 1997, Zalka provided the mathematical proof that Grover's QSA is optimal in terms of maximizing the success probability of obtaining the index pointing to an entry having the desired value [84].

In 1998, Brassard, Høyer and Tapp proposed the Quantum Counting Algorithm (QCA) based on Grover's QSA and Shor's quantum algorithms in [62]. The concept of QCA was conceived by the same authors in [54]. The QCA is capable of providing the number of entries in a classic database that are equal to the desired value, or, in other words, the number of solutions in the database. The QCA may be viewed as an amplitude estimation process, which is capable of estimating the number of desired entries in the classic database [51]. In 1999, Ahuja and Kappor also presented a similar QSA to the DHA that was capable of finding the maximum entry in a database [87]. During the same year, Long *et al.* introduced the generalized version of Grover's QSA by using arbitrary unitary operators and phase rotations in Grover's quantum circuit [86], replacing Grover's proposed operators [52].

When considering applications, where the entries of the database are related to each other, Hogg presented a heuristic QSA [88], which manages to find the specific index that corresponds to the minimum entry. Since this quantum algorithm is heuristic and application-based, no theoretical limits were provided. Then, Brassard *et al.* proposed a modification in the last part of Grover's QSA in order to successfully conclude the search with 100% probability [51]. In 2002, Imre and Balázs proposed an MUD scheme for a DS-CDMA system employing the QCA [60], [61]. The main process relies on creating symbol-specific quantum databases containing all the potential faded and noise—as well as interference—contaminated received signals corresponding to each user's hypothesized transmitted symbol and then aims for finding the transmitted symbol of each user relying on the QCA. If the faded and noise—as well as interference—

TABLE 1. Origins of Quantum Computing.

Year	Author(s)	Contribution
1981	Feynman [72]	Proposed the basic model of a quantum computer, which was capable of simulating the sequence of quantum states in a quantum system.
1982	Benioff [73]	Proposed a theoretical framework for a quantum computer.
1985	Deutsch [76]	Deutch's Algorithm: A global property of a function $f : \{0, 1\} \rightarrow \{0, 1\}$ can be determined by using only a single evaluation of f.
1992	Deutsch and Jozsa [77]	Deutsch-Jozsa Algorithm: Succeeds to determine whether a function $f : \{0, 2^n - 1\} \rightarrow \{0, 1\}$ is balanced or constant in one correspondence.
1994	Shor [78]	Shor's Algorithm: Proposed a quantum algorithm for integer factorization and introduced the concept of the Quantum Fourier Transform (QFT).
	Cleve *et al.* [79]	Proposed improvements to the Deutsch-Josza algorithm and introduced the phase estimation algorithm.

contaminated received signal appeared in one of the symbol-specific databases, then the specific information symbol this database was constructed on is the most likely symbol to have been transmitted by the corresponding user.

In 2003, Shenvi *et al.* proposed a quantum random-walk search algorithm applied on graphs [89]. In 2004, Imre and Balázs generalized Grover's QSA, where arbitrary unitary operators are employed and only a single iteration of the Grover operator is applied [90]. Furthermore, Imre proposed the Quantum Existence Testing (QET) algorithm [48], [92] for replacing the QCA in the above-mentioned QMUD algorithm. The difference between the QCA and the QET algorithm is that the QET shows whether the faded and noise—as well as interference—contaminated received signal associated with a specific legitimate transmitted symbol does or does not exist in the quantum database. However, this is achieved without providing any information about the number of occurrences. By contrast, the QCA provides an estimate of the number of solutions in the database. Since in the QMUD proposed in [60] the knowledge required is the existence or non-existence of a solution in the databases, the QET is sufficient and less computationally complex. Moreover, Imre proposed a quantum algorithm for finding an extrinsic value in an unsorted database in [92], provided that the desired value was an integer number and that its approximate range was known *a priori*. In [91], Zhao *et al.* proposed the concept of a QMUD based on Grover's QSA [53] and Imre's previously proposed QMUD [60]. The main concept was to create a single quantum database for all users, containing the CF evaluations of all the legitimate multi-level symbols that might have been transmitted, and then to perform quantum search for finding the minimum entry in it.

Malossini *et al.* employed the DHA for creating a Quantum-assisted Genetic Optimization Algorithm (QGOA) [93] that has a performance similar to that of the classic GA, but this is achieved at a lower computational complexity. Briefly, the GAs typically carry out a random-guided search across a large search-space with the goal of finding the desired entry associated with a CF maximum/minimum, while visiting only a fraction of the legitimate entries. In 2011, Li *et al.* proposed a quantum detection scheme for MIMO-OFDM systems by employing Grover's QSA [94]. Similarly to the QMUD algorithm proposed in [91], a quantum database is created by including evaluations of the CF used for classic detection in MIMO systems for all the possible legitimate inputs. A quantum algorithm based on Grover's QSA is then employed for finding the minimum of the CF in the resultant quantum database. Brassard *et al.* proposed in [71] the QMA, which finds the mean of a function with a predefined precision. In the same paper the authors presented an application of the QMA for approximating the median of a function. The major contributions in the field of quantum search along with their applications are summarized gathered in Table 2.

V. FUNDAMENTALS OF QUANTUM COMPUTING

In classic communications the smallest unit of information is the *bit*, which assumes binary values from the set $\{0, 1\}$. Its quantum-domain counterpart is the quantum bit or *qubit*,

TABLE 2. Major contributions to Quantum Search Algorithms (QSA) with their applications.

Year	Author(s)	Contribution
1996	Grover [52], [53]	Grover's Quantum Search Algorithm (QSA): A quantum mechanical algortihm performing quantum search in an unsorted classic database.
	Boyer *et al.* [54]	Showed a closed form for calculating the success probability of Grover's QSA and proposed an algorithm based on Grover's QSA where the wanted searched number appears more than once and also an unknown number of times in the database.
	Dürr and Høyer [55]	Dürr–Høyer Algorithm (DHA): Proposed a quantum algorithm for finding the minimum entry in an unsorted database.
	Bennett *et al.* [83]	Showed that Grover's QSA is asymptotically optimal.
1997	Zalka [84]	Proved that Grover's QSA is exactly optimal, in terms of providing the maximum possible probability of obtaining the solution.
1998	Ventura and Martinez [85]	Presented the concept of Quantum Associative Memory based on Grover's QSA.
	Brassard *et al.* [62]	Proposed the Quantum Counting Algorithm (QCA) based on Grover's QSA and Shor's factoring algorithm.
1999	Long *et al.* [86]	Proposed a generalized Grover's QSA by replacing the quantum circuit's unitary operators with arbitrary ones.
	Ahuja and Kapoor [87]	Presented a QSA similar to the DHA of [55] for finding the maximum entry in a database.
2000	Hogg [88]	Presented a heuristic quantum algorithm that finds the minimum by exploiting the correlation of the database entries.
	Brassard *et al.* [51]	Introduced the Quantum Amplitude Amplification (QAA) and Quantum Amplitude Estimation (QAE) concepts, along with a modified Grover's QSA that finds the solution with 100% probability.
2002	Imre and Balázs [60], [61]	Proposed a Quantum Multi-User Detector (QMUD) employing the QCA of [62].
2003	Shenvi *et al.* [89]	Proposed a quantum random walk search algorithm on graphs, having a similar approach as Grover's QSA [53].
2004	Imre and Balázs [90]	Presented a generalized Grover's QSA with a single application of the generalized Grover's operator.
2006	Zhao *et al.* [91]	Suggested improvements to the Grover's QSA-based MUD of [60].
2007	Imre [92]	Introduced Quantum Existence Testing (QET) based on QCA of [62] and proposed an algorithm searching for extreme values in an unsorted database based on QET.
2008	Malossini *et al.* [93]	Presented a Quantum Genetic Optimization Algorithm (QGOA) where the parent selection is based on the DHA of [55].
2011	Li [94]	Proposed a detection scheme for MIMO-OFDM systems based on the QCA of [62].
	Brassard *et al.* [71]	Proposed a quantum algorithm that finds the mean of a function inspired by the QCA of [62] and presented an application of it which finds the median of a function.

which is denoted as $|q\rangle$, where $|\cdot\rangle$ is termed as a *ket* [100]. A unique and rather unusual feature of the qubit is that apart from assuming the classic {0, 1} states, it also may assume the superposition of them, as encapsulated in:

$$|q\rangle = a|0\rangle + b|1\rangle \tag{6}$$

where we have $|a|^2 + |b|^2 = 1$, with $a, b \in \mathbb{C}$. If either $a = 0$ or $b = 0$, then we have $|q\rangle = |1\rangle$ or $|q\rangle = |0\rangle$, respectively. If neither a nor b is equal to 0, then the qubit is in a superposition of states, implying that it is in both states at the same time, until this somewhat strange state is perturbed by external interference, such as an attempt to ''measure'' or observe it. The probability of finding a qubit being in the state $|0\rangle$ after observing it is $|a|^2$ and in state $|1\rangle$ is $|b|^2$. The physical interpretation of a qubit was elegantly illustrated by Brassard in [101] by presenting a scenario where an atom with an electron orbiting on the ground state receives half the needed energy to excite it to a higher energy level orbit. The atom with the two allowed energy levels that the electron can occupy is presented in Fig. 4. Quantum mechanics do not allow the electron to be observed in an intermediate state, even though it is simultaneously in both the excited and ground state.

The non-intuitive phenomenon of quantum mechanics may be better appreciated by imagining a coin spinning within a black box. Until it settles down and someone opens the box to observe it, it is considered as being 50% ''Heads'' and 50% ''Tails'', simultaneously. Hence the state of a spinning coin may indeed be deemed to be a superposition of states and its state may be described by

$$|q\rangle = a|0\rangle + b|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{7}$$

where $|0\rangle =$ ''Heads'' and $|1\rangle =$ ''Tails'', while $|a|^2 + |b|^2 = 0.5 + 0.5 = 1$.

When the spinning coin settles down and an observer approaches it, there is an $|a|^2 = 0.5$ probability of observing the ''Heads'' side of it and $|b|^2 = 0.5$ probability of observing its ''Tails'' side. When an ''observation'' reminiscent of observing the spinning coin takes place in a quantum system, the observed qubits ''collapse'' to a classic state according to the so-called Copenhagen interpretation [74], where this classic state is the observed one. In our example, if the coin is observed to be in the $|0\rangle$ state, naturally it will remain in this state, until an operation is applied to it. In a quantum communication system, a qubit's state is *decided* to be in a specific classic state upon its observation. According to the No-Cloning Theorem [47], a qubit being in an unknown, unobserved state cannot be copied, which is in contrast to the case of classic bits, which represent known, observed states.

A qubit $|x\rangle = a_x|0\rangle + b_x|1\rangle$ may also be interpreted as a vector on a unit sphere, termed as the Bloch sphere [47], where the positive z-axis represents the state $|0\rangle$ and the state $|1\rangle$ is mapped to the negative z-axis, as depicted in Fig. 5. The relationship between the angles ϑ_x, φ_x and the quantum state's amplitudes a_x and b_x is

$$a_x = \cos\left(\frac{\vartheta_x}{2}\right), \quad b_x = e^{i\varphi_x}\sin\left(\frac{\vartheta_x}{2}\right) \tag{8}$$

where $0 \leq \vartheta_x \leq \pi$ and $0 \leq \varphi_x < 2\pi$. From (8), we may conclude that $a_x \in \mathbb{R}_0^+$ and $b_x \in \mathbb{C}$. The quantum amplitude a_x of $|0\rangle$ may always be made real by applying a global phase rotation to the qubit, without essentially changing its quantum state [47]. A qubit in the quantum state $|q\rangle = a|0\rangle + b|1\rangle$ with $a, b \in \mathbb{R}$ has $\varphi_q = 0$ and $\vartheta_q = 2\cos^{-1}(a) = 2\sin^{-1}(b)$, as illustrated in Fig. 5.

A. COMPOSITE QUANTUM SYSTEMS

Naturally, a quantum system may involve several qubits. For instance, a two-qubit state in a superposition of equiprobable

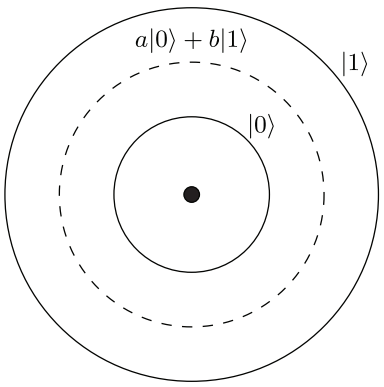

FIGURE 4. An atom with one electron orbiting around the nucleus having two legitimate energy levels (solid orbits). Quantum mechanics allow the electron to be in an arbitrary superposition of these two energy levels (dashed orbit), but when it is observed it may only be found in one of the two legitimate orbits.

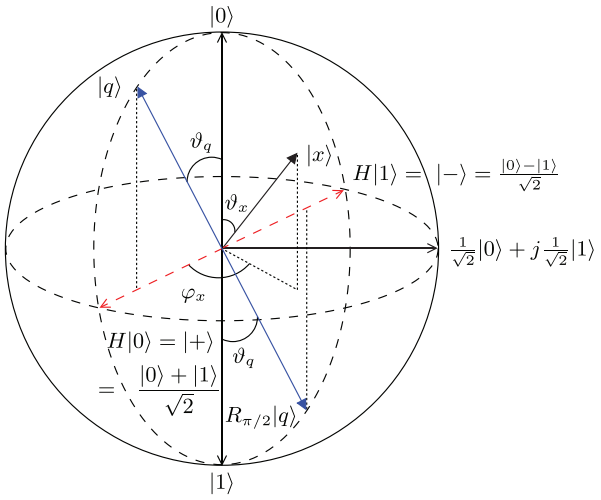

FIGURE 5. Geometrical representation of a qubit $|x\rangle = a_x|0\rangle + b_x|1\rangle = \cos(\vartheta_x/2)|0\rangle + e^{j\varphi_x}\sin(\vartheta_x/2)|1\rangle$ with $a_x \in \mathbb{R}$, $b_x \in \mathbb{C}$, $0 \leq \vartheta \leq \pi$ and $0 \leq \varphi < 2\pi$ on the Bloch sphere, along with the computational basis $\{|0\rangle, |1\rangle\}$, the sign basis $\{|+\rangle, |-\rangle\}$ and the Hadamard H operator. The rotation $R_{\pi/2}$ operator is applied on a qubit $|q\rangle = a|0\rangle + b|1\rangle = \cos(\vartheta_q/2)|0\rangle + e^{j\varphi_q}\sin(\vartheta_q/2)|1\rangle$ with $\varphi_q = 0$ and hence $a, b \in \mathbb{R}$.

states is described by

$$|q\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle, \quad \sum_{i=0}^{3} |a_i|^2 = 1 \quad (9)$$

where again, the square of the coefficients represents the probability of finding the two-qubit register in the corresponding state upon its observation.

A 3-qubit quantum system in a superposition of states may be described as

$$|q\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|100\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|101\rangle \quad (10)$$

where we have $a_2 = a_3 = a_6 = a_7 = 0$ and $\sum_{i=0}^{2^3-1} |a_i|^2 = 1$. In practice, a specific scenario where this system may be found in this particular superposition of states is when unitary operators have been applied to the three qubits, which alter their state.

In this example, the second qubit is in the state $|0\rangle$, since the probability of finding it in $|1\rangle$ is zero. The third qubit can be considered to be in the superposition of equiprobable states, i.e. $|q_3\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, since the probability of observing it in either of the states is the same according to (10). Finally, the first qubit may be considered to be in the state of $|q_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$, indicating a probability of 75% to retrieve $|0\rangle$ and 25% to observe $|1\rangle$. Hence, (10) is derived by

$$\begin{aligned} |q\rangle &= |q_1\rangle|q_2\rangle|q_3\rangle \\ &= \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)|0\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + 0|010\rangle + 0|011\rangle \\ &\quad + \frac{\sqrt{3}}{2\sqrt{2}}|100\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|101\rangle + 0|110\rangle + 0|111\rangle. \end{aligned} \quad (11)$$

This system's state can be equivalently represented in a vectorial form as

$$|q\rangle = \left[\frac{1}{2\sqrt{2}}, \frac{1}{2\sqrt{2}}, 0, 0, \frac{\sqrt{3}}{2\sqrt{2}}, \frac{\sqrt{3}}{2\sqrt{2}}, 0, 0\right]^T. \quad (12)$$

For an arbitrary n-qubit register, its state may be denoted as

$$|q\rangle = [a_0, a_1, a_2, \ldots, a_{2^n-2}, a_{2^n-1}]^T, \quad \sum_{i=0}^{2^n-1} a_i^2 = 1 \quad (13)$$

where $|a_2|^2$ is the probability of observing the system in the state $|2\rangle = |010\rangle$ and $|a_j|^2$ is the probability of observing the system in the state $|j\rangle$, with $j = 0, 1, \ldots, 2^n - 1$. The formulation in (13) will be used in algebraic manipulations in the following discussions. The states $|0\rangle$ and $|1\rangle$, that an 1-qubit system can be found in, may be represented in vectorial form as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (14)$$

The Hermitian counterpart of (13) is referred to as a *bra* [100] and it is denoted as

$$\langle q| = |q\rangle^\dagger = [a_0^* \; a_1^* \; a_2^* \; \ldots \; a_{2^n-2}^* \; a_{2^n-1}^*], \quad \sum_{i=0}^{2^n-1} |a_i^*|^2 = 1 \quad (15)$$

where the superscript $\dagger$ denotes the conjugate transpose of $|q\rangle$. It may be readily verified that the inner product obeys $\langle q||q\rangle = \langle q|q\rangle = 1$ and the outer product becomes

$$|q\rangle\langle q| = \begin{bmatrix} |a_0|^2 & a_0 a_1^* & \cdots & a_0 a_{2^n-1}^* \\ a_1 a_0^* & |a_1|^2 & \cdots & a_1 a_{2^n-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ a_{2^n-1} a_0^* & a_{2^n-1} a_1^* & \cdots & |a_{2^n-1}|^2 \end{bmatrix}. \quad (16)$$

B. EVOLUTION OF QUANTUM SYSTEMS

Unitary operators are employed to evolve a quantum system, altering the amplitude of its superposition of states a_i, but keeping the sum of the probabilities for the system to be observed to one of the superimposed states, to unity. An operator U is a unitary operator if it obeys $U^{-1} = U^\dagger$, where the superscript $\dagger$ denotes the conjugate transpose or the Hermitian adjoint matrix of U. Since a quantum system may be described by its quantum state $|q\rangle$, the application of a unitary operator will transform it into the quantum state $|q'\rangle$ as in

$$|q'\rangle = U|q\rangle. \quad (17)$$

Two unitary operators that will be employed in our QMUD are the Hadamard operator H and the Rotation operator R_θ [47], with their one-qubit matrix representations being [47]:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \; R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \quad (18)$$

Their effect may be interpreted as in Fig. 6, where R_θ rotates $|q\rangle$ by θ anti-clockwise on the unit circle, while H creates an equiprobable superposition of the computational basis states, as encapsulated in

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (19)$$

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (20)$$

The representation of a quantum state portrayed in Fig. 6 is only applicable when $b \in \mathbb{R}$. Comparing it to the portrayal of the quantum state as a vector on the Bloch sphere, we may conclude that the plane consisting of the computational basis $\{|0\rangle, |1\rangle\}$ and the sign basis $\{|+\rangle, |-\rangle\}$ on the Bloch sphere is mapped to the right half circle of Fig. 6. In the case where a rotation operator R_θ results in the quantum state's vector lying on the left-hand plane in Fig. 6, the resultant quantum state may be equivalently represented by applying a rotation gate associated with $\theta = \pi$. The application of a rotation gate with $\theta = \pi$ does not affect a quantum state, since it may be considered as applying a global phase to it, which

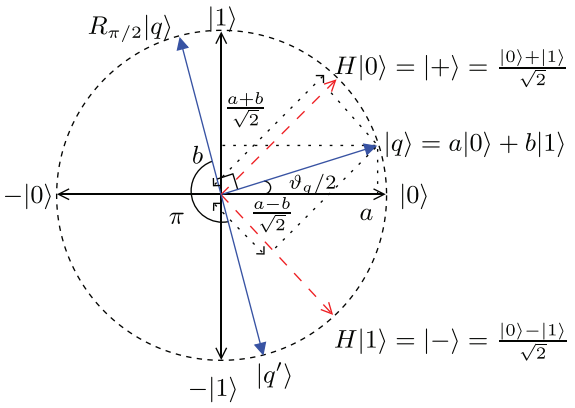

FIGURE 6. Geometrical interpretation of a qubit $|q\rangle = a|0\rangle + b|1\rangle$ with $a, b \in \mathbb{R}$, on the computational basis $\{|0\rangle, |1\rangle\}$ and the sign basis $\{|+\rangle, |-\rangle\}$, along with the Hadamard H and rotation $R_{\pi/2}$ operators.

is unobservable [47]. For example, the unitary rotation gate $R_{\pi/2}$ applied to $|q\rangle = a|0\rangle + b|1\rangle$ in Figs. 5 and 6 results in the state $R_{\pi/2} = -b|0\rangle + a|1\rangle$, which is equivalent to the state $|q'\rangle = -(b|0\rangle - a|1\rangle) = e^{j\pi}(b|0\rangle - a|1\rangle)$. The quantum states $R_{\pi/2}|q\rangle$ and $|q'\rangle$ on the Bloch sphere of Fig. 5 are represented by the same vector, since the amplitude of $|0\rangle$ has to be real and non-negative.

In contrast to H and R_θ, the Controlled-*NOT* (*CNOT*) operator [47] acts on two qubits jointly forming a Quantum Register (QR)[2], with the first qubit $|c\rangle$ being the control qubit and the second qubit $|t\rangle$ the target one. More specifically, if $|c\rangle = |1\rangle$, then the state of $|t\rangle$ is flipped, otherwise it remains intact, as encapsulated in

$$|c\rangle|t\rangle \xrightarrow{CNOT} |c\rangle|c \oplus t\rangle. \tag{21}$$

The QD unitary operator U_f does not have a classic counterpart and it is capable of evaluating the function f with the input qubits simultaneously representing multiple arguments of the function, which is achieved by taking advantage of the superposition of states. More explicitly, it accepts two QRs as inputs, with the first QR $|x\rangle$ containing the argument, while the second QR is formed by the specific number of bits Z that we desire the function's evaluation to be approximated in. This second QR is initialized to the all-zero state $|0\rangle^{\otimes Z}$[3], as depicted in Fig. 7, where the numeric kets subscripts distinguish the QRs employed. Assuming n qubits in the QR $|x\rangle_1 = H|0\rangle_1^{\otimes n}$ and having initialized it in an equiprobable superposition of states by applying a Hadamard gate, the system's quantum state before the application of U_f would be

[2]A QR is formed by any number of qubits and it exists only to underline the purpose of a set of qubits. The state of a two-qubit QR may be equivalently represented as $|q_1\rangle \otimes |q_2\rangle \equiv |q_1\rangle|q_2\rangle \equiv |q_1 q_2\rangle$.

[3]The Z-element tensor product is defined as: $|0\rangle^{\otimes Z} = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{Z} = \underbrace{|0\rangle|0\rangle \ldots |0\rangle}_{Z} = \underbrace{|00\ldots0\rangle}_{Z}$

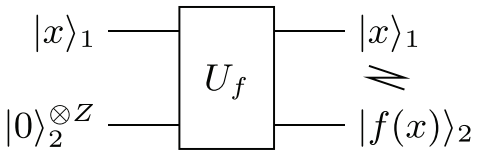

FIGURE 7. Unitary operator U_f entangling the f evaluations with the corresponding input argument. The subscripts of the kets are used to distinguish the QRs throughout a circuit analysis.

$$\begin{aligned}|\psi_1\rangle &= |x\rangle_1|0\rangle_2^{\otimes Z} = H|0\rangle_1^{\otimes n}|0\rangle_2^{\otimes Z} \\ &= \left(\sum_{q=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|q\rangle_1\right)|0\rangle_2^{\otimes Z} \\ &= \sum_{q=0}^{2^n-1}\left(\frac{1}{\sqrt{2^n}}|q\rangle_1|0\rangle_2^{\otimes Z}\right)\end{aligned} \tag{22}$$

where the integer values in q correspond to their respective binary values as for example in $|q\rangle = |5\rangle = |101\rangle$. The unitary operator U_f will evolve the system into

$$\begin{aligned}|\psi_2\rangle &= U_f \sum_{q=0}^{2^n-1}\left(\frac{1}{\sqrt{2^n}}|q\rangle_1|0\rangle_2^{\otimes Z}\right) \\ &= \sum_{q=0}^{2^n-1}\left(\frac{1}{\sqrt{2^n}}|q\rangle_1|f(q)\rangle_2\right).\end{aligned} \tag{23}$$

The U_f operator creates a strange connection between the two QRs. If only the first QR shown in Fig. 7 is observed in the QD and $|x\rangle_1 = |0\rangle_1$ is obtained, then the second QR seen in Fig. 7 will be in the $|f(0)\rangle_2$ state with 100% probability. Similarly, if we have $|f(x)\rangle_2 = |f(1)\rangle_2$ after an act of QD observation, then we have $|x\rangle_1 = |1\rangle_1$ with 100% probability. This peculiar connection is referred to as entanglement, as detailed in [47].

Any classic circuit may be converted to an equivalent circuit in the QD by using the unitary operators H, R_θ and *CNOT* [47]. Additionally, any classic circuit may become reversible in the QD in the sense defined in [47] with the aid of the Toffoli gate, or equivalently by using the Controlled-Controlled-NOT (*CCNOT*) gate, and auxiliary qubits [47]. Hence, the implementation of U_f will be based on the QD equivalent of the classic circuit that computes $f : \{0, 1\}^{\otimes n} \rightarrow \{0, 1\}^{\otimes Z}$. The time required for a single application of U_f compared to that for a single classic evaluation of f will depend on the technology used for creating U_f. In our analysis we will assume that these times are equal.

C. MEASUREMENT OF QUANTUM STATES

When stating the terms "measurement" or "observation", so far we have been referring to measurements with respect to the computational or standard basis $\{|0\rangle, |1\rangle\}$. If an 1-qubit quantum system is observed, its state after the measurement would be either $|0\rangle$ or $|1\rangle$, depending on the observation's result. However, measurements may be performed in a diverse base. In fact, the number of different bases that a qubit may

be observed in is infinite [47]. A commonly used alternative basis the qubit may be measured in is the Hadamard or sign basis $\{|+\rangle, |-\rangle\}$ portrayed in Figs. 5 and 6, where we have:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (24)$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \quad (25)$$

The specific reason for using a particular basis depends on the application. For example, if the intention of the observation is to determine which specific part of the Cartesian plane the qubit $|q\rangle = a|0\rangle + b|1\rangle$ lies on, then a measurement on the Hadamard basis would resolve whether we have $a \cdot b > 0$ or $a \cdot b < 0$, hence again determining the particular part of the plane the qubit exists on. By contrast, if an observation was made on the computational basis for the same purpose, then the resultant state would be mapped to one of the coordinate axes seen in Figs. 5 and 6, hence providing us with no particular clue as to its quadrant.

The representation of a qubit $|q\rangle$ on the computational basis is $|q\rangle = a|0\rangle + b|1\rangle$. In order to convert its representation to the sign basis, we exploit the fact that

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad (26)$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}. \quad (27)$$

Hence, the same qubit may be represented in the sign basis as

$$|q\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle \quad (28)$$

and the probability of getting the state $|+\rangle$ or $|-\rangle$ after a potential observation on the Hadamard basis is $\frac{|a+b|^2}{2}$ and $\frac{|a-b|^2}{2}$, respectively. If the observation's outcome is $|+\rangle$, then the state of the system after the observation will be $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Similarly, if the observation's outcome is $|-\rangle$, then the resultant system's state will be $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

1) PARTIAL MEASUREMENT OF QUANTUM STATES

As far as a multiple-qubit system is concerned, the measurement procedure is similar to the one analysed for a single-qubit system. For example, when considering a 2-qubit system, its general quantum state is presented in (9). As in any quantum system, a potential measurement will only be able to reveal as many bits of information as the number of qubits in the system. In the 2-qubit system considered a measurement of the two qubits would yield the result $|00\rangle$ with probability $|a_{00}|^2$, or the state $|01\rangle$ with probability $|a_{01}|^2$ or in general the bit string $s \in \{0, 1\}^2$ with probability $|a_s|^2$. The state of the quantum system after the measurement would be $|s\rangle$.

However, it is possible to measure only a subset of the qubits that a quantum system consists of by performing a *partial measurement*. Let us assume that in our example of a 2-qubit system we intend to observe only the second qubit. The probabilities of obtaining the second qubit in the state of $|0\rangle$ or $|1\rangle$ are

$$P_q(\text{x0}) = P_q(00) + P_q(10) = |a_{00}|^2 + |a_{10}|^2 \quad (29)$$

$$P_q(\text{x1}) = P_q(01) + P_q(11) = |a_{01}|^2 + |a_{11}|^2. \quad (30)$$

In other words, the probability of obtaining the second qubit in the state of $|0\rangle$ upon its measurement is equal to the probability of observing the full system in the states that have the second qubit equal to $|0\rangle$.

The main difference of the partial measurement compared to the full measurement of a quantum system lies in the gravity of the perturbation imposed on the system's original state and the resultant state. Following the same example, let us assume that the result of the second qubit's observation was $|0\rangle$. The new state of the system after the partial measurement will include all the states that are consistent with the measurement's specific outcome. Hence we have

$$|q_{\text{new}}\rangle = a_{00,\text{new}}|00\rangle + a_{10,\text{new}}|10\rangle \quad (31)$$

where $a_{00,\text{new}}$ and $a_{10,\text{new}}$ are the new amplitudes of the legitimate remaining states. The new amplitudes will be the normalized versions of the corresponding amplitudes of the original states before the measurement, resulting in

$$|q_{\text{new}}\rangle = \frac{a_{00}|00\rangle + a_{10}|10\rangle}{\sqrt{|a_{00}|^2 + |a_{10}|^2}}. \quad (32)$$

Any following measurement of the second qubit in the new quantum state $|q_{\text{new}}\rangle$ will result in the state $|0\rangle$ with 100% probability.

D. ENTANGLEMENT

The new state after the partial measurement may be written as

$$\begin{aligned}|q_{\text{new}}\rangle &= \left(\frac{a_{00}}{\sqrt{|a_{00}|^2 + |a_{10}|^2}}|0\rangle + \frac{a_{10}}{\sqrt{|a_{00}|^2 + |a_{10}|^2}}|1\rangle\right)|0\rangle \\ &= \left(a_{00,\text{new}}|0\rangle + a_{10,\text{new}}|1\rangle\right) \otimes |0\rangle. \end{aligned} \quad (33)$$

As seen in (33), the resultant quantum system consisting of two qubits may be decomposed in a way, where the composite quantum states are represented by the tensor products of the qubits. Another example is the 3-qubit quantum state presented in (10) which may be decomposed as seen in (11). The information that can be gained by the decomposition of (11) is that the first qubit of the system is in the state $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$, regardless of the states the rest of the qubits are in. Similar knowledge may be obtained for the second and third qubit. The quantum system is referred to as being "unentangled", if it is able to be decomposed i.e. it is decomposable.

However, this decomposition is not possible for every quantum state. Let us consider for example the quantum state of a 2-qubit system, which is initially in the state $|\psi_0\rangle = |00\rangle$, as seen in Fig. 8. Once the first qubit passes through the Hadamard gate, the system's state becomes

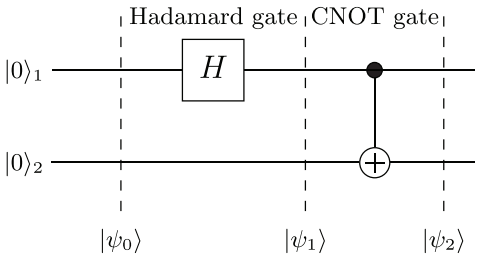

FIGURE 8. Quantum circuit for generating the entnagled Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

$$\begin{aligned}|\psi_1\rangle &= (H|0\rangle_1)|0\rangle_2 \\ &= \left(\frac{1}{\sqrt{2}}|0\rangle_1 + \frac{1}{\sqrt{2}}|1\rangle_1\right)|0\rangle_2 \\ &= \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right). \end{aligned} \tag{34}$$

When the two qubits pass through the *CNOT* gate, the first qubit $|\psi_1\rangle_1 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ acts as the control qubit to the second qubit $|\psi_1\rangle_2 = |0\rangle$, which is the target qubit. The transfer matrix of the *CNOT* gate relying on the first qubit acting as the control qubit and the second qubit as the target qubit may be formulated as

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{35}$$

The final state of the system after passing it through the *CNOT* gate becomes

$$\begin{aligned}|\psi_2\rangle &= CNOT \cdot |\psi_1\rangle \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}^T \\ &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \end{aligned} \tag{36}$$

The resultant state $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be decomposed into a state representing the first qubit and a state corresponding to the second qubit. This may be readily shown by attempting to decompose $|\psi_2\rangle$ into separate states. Let us assume that the state of the first qubit is $|\psi_2\rangle_1 = a_{10}|0\rangle + a_{11}|1\rangle$ and the state of the second qubit is $|\psi_2\rangle_2 = a_{20}|0\rangle + a_{21}|1\rangle$. The resultant composite system of these two qubits would become

$$\begin{aligned}|\psi_2\rangle_1 \otimes |\psi_2\rangle_2 &= (a_{10}|0\rangle + a_{11}|1\rangle)(a_{20}|0\rangle + a_{21}|1\rangle) \\ &= a_{10}a_{20}|00\rangle + a_{10}a_{21}|01\rangle \\ &\quad + a_{11}a_{20}|10\rangle + a_{11}a_{21}|11\rangle. \end{aligned} \tag{37}$$

In order for the state in (37) to be equal to $|\psi_2\rangle$, the amplitudes of $|00\rangle$ and $|11\rangle$ should be non-zero. This leads to $a_{10}, a_{11}, a_{20}, a_{21} \neq 0$. At the same time, the amplitudes of $|01\rangle$ and $|10\rangle$ should be equal to 0, leading to either $a_{10} = 0$ or $a_{21} = 0$ and at the same time $a_{11} = 0$ or $a_{20} = 0$. The latter constraints contradict the former one, making it impossible for the quantum state $|\psi_2\rangle$ to be decomposed.

A system that is not possible to decompose to separate states corresponding to its constituent qubits is termed as "entangled". When one of the two qubits of the state $|\psi_2\rangle$ is observed, the outcome might be $|0\rangle$ with a probability of 1/2 or $|1\rangle$ with a probability of 1/2. If the outcome is 0, then a potential measurement of the second qubit will yield 0 with a probability of 1. Symmetrically, if the outcome of the first qubit's observation is 1, then a measurement of the second qubit will surely result in 1. It seems that a connection exists between these two qubits, relating them to each other, regardless of their spatial distance. This non-intuitive relationship between two entangled qubits was referred to by Einstein as a "spooky action in a distance" [102].

In fact, the state $|\psi_2\rangle$ is one of the four Bell basis states, named after John S. Bell [47], which are constituted by the following four entangled states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{38}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{39}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{40}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{41}$$

As for any other orthonormal basis defined over $\mathbb{C}^4$, a 2-qubit system may be measured on the Bell basis. None of the states of the Bell basis can be decomposed to the separate states constituted by each qubit.

VI. QUANTUM SEARCH ALGORITHMS

For the case of providing further in-depth intuition we will proceed by investigating Grover's QSA [53], the BBHT QSA [54] and the DHA [55] in the context of a simple DS-CDMA scenario supporting $K = 2$ users employing the BPSK modulation scheme associated with $M = 2$ states. The channel coefficients are assumed to be perfectly estimated and Gold spreading codes [5] are used which have a spreading factor of $SF = 31$ chips. The CF evaluations in (4) would be $f : \{0, 1, 2, 3\} \rightarrow [0, 1]$ and the size of the search space is $N = M^K = 4$, since we have four possible two-bit combinations at the BS's receiver. Let us assume that the CF outputs are

$$[f(0),\ f(1),\ f(2),\ f(3)] = [0.24,\ 0.16,\ 0.38,\ 0.27] \tag{42}$$

which represent the probability $P(\mathbf{y}|\mathbf{x})$ of receiving the signal $\mathbf{y}$ in (1), given that the 4-level two-user signal $\mathbf{x}$ was transmitted. Due to the nature of the CF in (4), the smaller the Euclidean distance of a legitimate noise-free 4-level symbol

from the actually received faded and noise-contaminated signal $\mathbf{y}$ is, the higher its CF value. Hence, in our scenario we may conclude that the 4-level symbol $\mathbf{x} = [1, 0]^T$ is the most probable to have been transmitted. Naturally, in real applications we can only draw this conclusion, once we have computed all the possible CF values, hence facilitating an ML decision.

During our analysis of the QSAs, we will refer to the QR which will contain the indices of our search problems as the Quantum Index Register (QIR). In our scenario the QIR will consist of $n = \log_2 N = 2$ qubits forming the four states $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$, corresponding to the legitimate 4-level symbols $\mathbf{x} \in \{[0, 0]^T, [0, 1]^T, [1, 0]^T, [1, 1]^T\} \equiv x \in \{0, 1, 2, 3\}$, respectively. The probabilities of observing each of these states will be evolving and changing as the QSAs proceed, as it will be detailed in Sections VI-A, VI-B and VI-C.

A. GROVER'S QUANTUM SEARCH ALGORITHM

The goal of Grover's QSA is exactly the same as that of any classic search algorithm's, namely that of finding the index of the desired entries, provided of course that the desired entry is indeed part of the database. It was shown in [53] that it succeeds in finding the solution after $O(\sqrt{N})$ CF evaluations, in contrast to the optimal classic full-search algorithms which succeed after $O(N)$ calculations. Let us commence with an unrealistic version of our scenario, namely where we assume that we *know* that $\delta = 0.38$ appears in the database as one of the CF evaluations and also that it is unique. In practice this is unrealistic, because the CF value depends on the contaminating effects of random fading, noise and interference. Employing Grover's QSA we will determine the index x_s that corresponds to $f(x_s) = \delta$. Hence, we have $S = 1$ solution and $N = 4$ database indices. In classic search algorithms, once the desired entry associated with the lowest Euclidean distance was found, its index is readily observed and retrieved. In Grover's QSA on the other hand, the process aims for maximizing the probability of observing the index in the QIR x_s. Each of the N indices is treated as a legitimate solution to the search problem. The QIR should be initialized in a superposition of N equiprobable states, which is formulated as:

$$|x\rangle = \sum_{q=0}^{N-1} a_q |q\rangle = \sum_{q=0}^{N-1} \frac{1}{\sqrt{N}} |q\rangle = \sum_{q=0}^{3} \frac{1}{2} |q\rangle \tag{43}$$

since there is no *a priori* "preference" for any of the legitimate solutions. The initialization is performed with the aid of a two-qubit Hadamard gate $H^{\otimes 2}$ and two qubits in the $|00\rangle$ state which may be described based on (20) as

$$\begin{aligned} |x\rangle &= H^{\otimes 2}|00\rangle = H|0\rangle H|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \\ &= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle. \end{aligned} \tag{44}$$

The initial quantum amplitudes of the QIR $|x\rangle$ are depicted in Fig. 9a which shows the evolution of the quantum states in our scenario.

Finding the highest-probability solution in the QIR is accomplished by the iterations of Grover's QSA as detailed below. A single iteration of Grover's QSA is carried out by applying a unitary operator $\mathcal{G}$, referred to as the *Grover operator* to the QIR $|x\rangle$. The operator's circuit-based representation is shown in Fig. 10, which consists of a unitary operator termed as the *Oracle*, two Hadamard gates H exemplified in (20), and a controlled phase shift gate P_0. The Hadamard gate creates a superposition of equiprobable states, when applied to a state of the computational basis, $|0\rangle$ or $|1\rangle$. The controlled phase shift gate P_0 inverts the sign of all the input states except for the $|0\rangle^{\otimes n}$ one. The Hadamard gate, $H^{\otimes n} = H^{\otimes 2}$, and the controlled phase shifter gate $P_0^{\otimes 2}$ of Fig. 10 obey the following format

$$H^{\otimes n} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes(n-1)} & H^{\otimes(n-1)} \\ H^{\otimes(n-1)} & -H^{\otimes(n-1)} \end{bmatrix}, \quad H^{\otimes 0} = 1 \tag{45}$$

$$P_0^{\otimes n} = \left.\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{bmatrix}\right\} (2^n \times 2^n). \tag{46}$$

In our scenario we have $n = 2$, hence the matrix representations of the Hadamard gate $H^{\otimes 2}$ and the controlled phase shift gate $P_0^{\otimes 2}$ are

$$H^{\otimes 2} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{47}$$

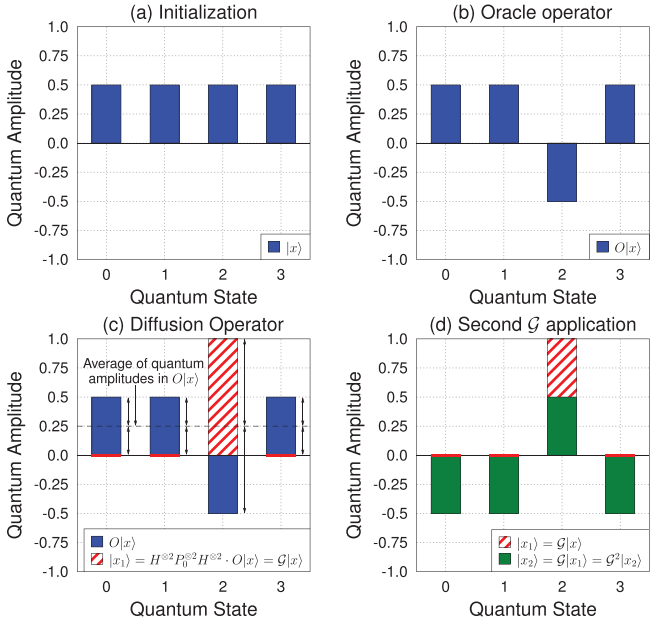

FIGURE 9. Graphical representation of Grover operator's $\mathcal{G}$ applications in our $K = 2$, $M = 2$ scenario with a unique solution $S = 1$ and $N = M^K = 4$ entries. The colours correspond to the rotations in Fig. 12.

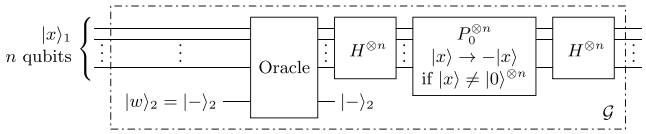

FIGURE 10. Grover operator's quantum circuit including an Oracle, two n-qubit Hadamard gates H and a controlled n-qubit phase shift gate P_0.

$$P_0^{\otimes 2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \tag{48}$$

respectively.

The Oracle is capable of recognizing the legitimate solutions in the QIR by evaluating the CF at this input. More explicitly, the Oracle's task in Grover's QSA is that of finding and marking the specific index sought. The Oracle may be described algebraically by an $(N \times N)$-element matrix with all the non-zero elements lying on its diagonal. Each of the N elements on the diagonal of the Oracle-matrix represents a specific cell of the QIR. The diagonal elements may assume the values of -1 or $+1$, depending on whether their corresponding CF evaluation is deemed to be a legitimate solution or not, respectively. Hence the format of the Oracle-matrix obeys

$$O = \begin{bmatrix} \pm 1 & 0 & \cdots & 0 \\ 0 & \pm 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \pm 1 \end{bmatrix}. \tag{49}$$

In our scenario, since the third index of the QIR, namely $x = 2$ is a solution to the search problem, the Oracle will recognize this by comparing the corresponding entry $f(2) = 0.38$ to the desired value $\delta = 0.38$ and the third element of the Oracle-matrix diagonal will be set to -1. On the other hand, since the first state $|0\rangle$ is not deemed to be a solution, because $f(0) = 0.24 \neq \delta = 0.38$, the first element of the Oracle's diagonal is set to $+1$. The second index $x = 1$ as well as the fourth index $x = 3$ are also not deemed to be solutions since $f(1) = 0.16 \neq \delta = 0.38$ and $f(3) = 0.27 \neq \delta = 0.38$, respectively, resulting to their corresponding positions on the diagonal of the Oracle-matrix to be set to $+1$ as encapsulated in

$$O = \begin{bmatrix} +1 & 0 & 0 & 0 \\ 0 & +1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & +1 \end{bmatrix}. \tag{50}$$

Moving deeper into the Oracle's operation, the Oracle's workspace is described by a single qubit, $|w\rangle$, initialized to the superposition of equiprobable states $|w\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. This superposition of states is acquired by applying the Hadamard gate H to the state $|1\rangle$ as described in

$$\begin{aligned} |w\rangle = H|1\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle. \end{aligned} \tag{51}$$

The Oracle will then map the N input states of the QIR $|x\rangle$ to

$$|x\rangle|w\rangle \xrightarrow{O} |x\rangle|w \oplus g(x)\rangle \tag{52}$$

where we have

$$g(x) = \begin{cases} 1 \text{ if } f(x) = \delta \\ 0 \text{ otherwise.} \end{cases} \tag{53}$$

Since we have $|w\rangle = |-\rangle$, the operations encapsulated in (52) may be expanded as

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{g(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{54}$$

The function $g(x)$ of (53) in our scenario is

$$g(x) = \begin{cases} 0 \; x = 0, \text{ since } f(0) = 0.24 \neq \delta = 0.38 \\ 0 \; x = 1, \text{ since } f(1) = 0.16 \neq \delta = 0.38 \\ 1 \; x = 2, \text{ since } f(2) = 0.38 = \delta = 0.38 \\ 0 \; x = 3, \text{ since } f(3) = 0.27 \neq \delta = 0.38 \end{cases} \tag{55}$$

and according to (52) and (54) the Oracle operation in our scenario is

$$\begin{aligned} |x\rangle|-\rangle &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) |-\rangle \\ &= \frac{1}{2} (|0\rangle + |1\rangle + |2\rangle + |3\rangle) |-\rangle \\ &= \frac{1}{2}|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\quad + \frac{1}{2}|2\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{2}|3\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\xrightarrow{O} \frac{1}{2}|0\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus g(0)\right) \\ &\quad + \frac{1}{2}|1\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus g(1)\right) \\ &\quad + \frac{1}{2}|2\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus g(2)\right) \\ &\quad + \frac{1}{2}|3\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus g(3)\right) \\ &= \frac{1}{2}|0\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle \oplus g(0) - |1\rangle \oplus g(0))\right) \\ &\quad + \frac{1}{2}|1\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle \oplus g(1) - |1\rangle \oplus g(1))\right) \\ &\quad + \frac{1}{2}|2\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle \oplus g(2) - |1\rangle \oplus g(2))\right) \\ &\quad + \frac{1}{2}|3\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle \oplus g(3) - |1\rangle \oplus g(3))\right) \\ &= \frac{1}{2}|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\quad + \frac{1}{2}|2\rangle\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) + \frac{1}{2}|3\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

$$= \frac{1}{2}|0\rangle|-\rangle + \frac{1}{2}|1\rangle|-\rangle + \frac{1}{2}|2\rangle\left(-|-\rangle\right) + \frac{1}{2}|3\rangle|-\rangle$$
$$= \frac{1}{2}\left(|0\rangle + |1\rangle - |2\rangle + |3\rangle\right)|-\rangle$$
$$= \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle + |11\rangle\right)|-\rangle. \quad (56)$$

The Oracle generates the function g by evaluating f in parallel, thus a single Oracle operation will be considered to have the computational complexity of one CF evaluation. By combining (45), (46) and (49), the algebraic description of the Grover operator may be constructed with the aid of Fig. 10 as

$$\mathcal{G} = H^{\otimes n} P_0^{\otimes n} H^{\otimes n} \cdot O. \quad (57)$$

Since in our scenario we have $n = \log_2 N = 2$, by substituting $H^{\otimes 2}$ from (47), $P_0^{\otimes 2}$ from (48) and the Oracle from (50), the Grover operator in our scenario becomes equal to

$$\mathcal{G} = H^{\otimes 2} P_0^{\otimes 2} H^{\otimes 2} \cdot O = \frac{1}{2}\begin{bmatrix} -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}. \quad (58)$$

The effect of the operation $\mathcal{G}$ on $|x\rangle$ may be seen in Fig. 11, where the y-axis represents the superposition of states that are solutions—which are given by $|s\rangle = \sqrt{\frac{1}{S}}|2\rangle = |2\rangle$ in our scenario—while the x-axis represents the set of states that are not solutions, which are given by $|ns\rangle = \sqrt{\frac{1}{N-S}}\left(|0\rangle + |1\rangle + |3\rangle\right) = \sqrt{\frac{1}{3}}\left(|0\rangle + |1\rangle + |3\rangle\right)$. It should be noted that this is a geometrical representation, which explains the operation of $\mathcal{G}$ and that the states $|s\rangle$ and $|ns\rangle$ are not physically created. The initial state $|x\rangle$ may be represented as

$$|x\rangle = \sqrt{\frac{S}{N}}|s\rangle + \sqrt{\frac{N-S}{N}}|ns\rangle$$
$$= \sqrt{\frac{1}{4}}|s\rangle + \sqrt{\frac{3}{4}}|ns\rangle$$
$$= \frac{1}{2}|2\rangle + \frac{\sqrt{3}}{2}\left(\frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |3\rangle\right)\right)$$
$$= \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right). \quad (59)$$

The Oracle reflects $|x\rangle$ with respect to $|s\rangle$, since it marks the solution in $|x\rangle$ by transforming $|s\rangle$ to $-|s\rangle$ and leaving $|ns\rangle$ unaltered as in (56). The HP_0H operator of Fig. 11 reflects $O|x\rangle$ with respect to the input state $|x\rangle$, as it may be seen in Fig. 11. More explicitly, the resultant state $|x_1\rangle = HP_0H \cdot O|x\rangle$ may be considered as a anti-clockwise rotation by 2φ with respect to $|x\rangle$, while the quantum state $O|x\rangle$ before HP_0H was applied may be considered as a clockwise rotation by 2φ with respect to the initial state $|x\rangle$, as illustrated in Fig. 11. The HP_0H operator is considered to perform inversion about the average, as depicted in Fig. 9c. Hence, $\mathcal{G}$ results in a total anti-clockwise rotation of the input state by 2φ, where we have [54]

$$\varphi = \arcsin\sqrt{S/N}. \quad (60)$$

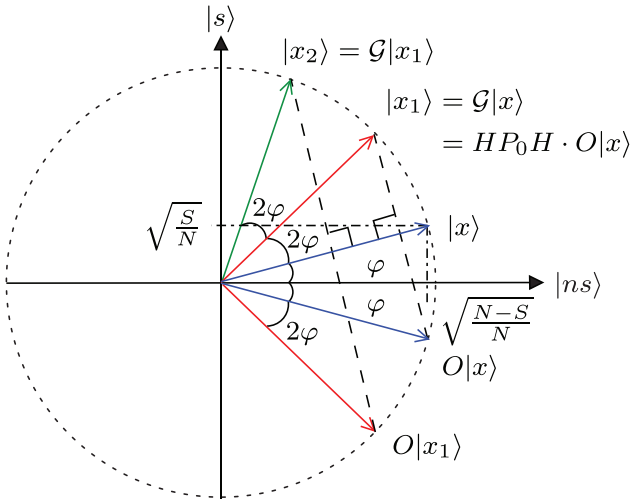

FIGURE 11. Geometrical interpretation of Grover's quantum search algorithm.

It should be noted that φ is the angle that the initial state $|x\rangle$ had with respect to the x-axis, which corresponds to $|ns\rangle$, and its value depends on the number of solutions S in the database, in addition to the size of the database N. If there was no solution in our problem $S = 0$, then $|ns\rangle = \sqrt{\frac{1}{N}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$ and $\varphi = 0$ from (60), resulting in $|x\rangle = |ns\rangle$. In other words, the initial quantum state in Fig. 11 would be on the x-axis and any application of $\mathcal{G}$ would have no effect on it, since it would rotate it by $2\varphi = 0$.

The same process is repeated, if subsequent Grover operators are applied, with the initial state of the next iteration being the final state of the previous iteration. The target is for $\mathcal{G}^L|x\rangle$ to approach $|s\rangle$ as closely as possible so that when we observe the QIR, we will have the maximum possible probability of obtaining a state of the solutions set $|s\rangle$. This occurs the earliest after [54]

$$L_{opt} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{S}} \right\rfloor \quad (61)$$

consecutive applications of the $\mathcal{G}$ operator of Fig. 10. This process is the QAA [51]. If we observe the resultant state in the QD, the probability of obtaining the correct answer is $\sin^2\left[(2L_{opt}+1)\varphi\right]$.

In our scenario, we have $\varphi = 30$ŭ and $L_{opt} = 1$ according to (60) and (61), respectively. The geometric representation of the evolution of our scenario's QIR with respect to the applications of Grover operators may be seen in Fig. 12. The application of the Oracle to the initial QIR state $|x\rangle$ in (43) would result into

$$O|x\rangle = \begin{bmatrix} +1 & 0 & 0 & 0 \\ 0 & +1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & +1 \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} \quad (62)$$

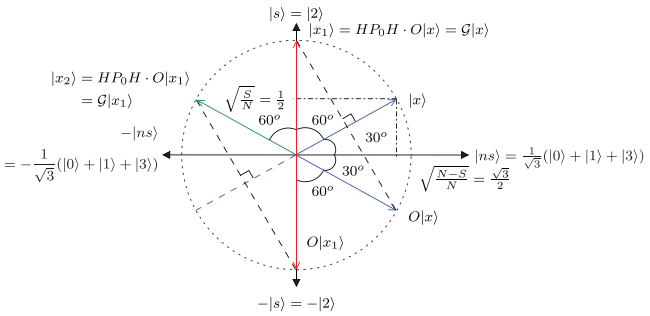

FIGURE 12. Geometrical interpretation of Grover's quantum search algorithm applied in our $K = 2$, $M = 2$ scenario, where we have a unique solution $S = 1$ and $N = 4$ legitimate entries.

and its graphical and geometrical representation may be seen in Figs. 9b and 12, respectively. If we applied the operators $H^{\otimes 2}P_0^{\otimes 2}H^{\otimes 2}$ on $O|x\rangle$ we would obtain

$$\begin{aligned}|x_1\rangle &= H^{\otimes 2}P_0^{\otimes 2}H^{\otimes 2} \cdot O|x\rangle = \mathcal{G}|x\rangle \\ &= \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix} \cdot \\ &\quad \cdot \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix}1\\ 1\\ -1\\ 1\end{bmatrix} \\ &= \frac{1}{2}\begin{bmatrix}-1 & 1 & 1 & 1\\ 1 & -1 & 1 & 1\\ 1 & 1 & -1 & 1\\ 1 & 1 & 1 & -1\end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix}1\\ 1\\ -1\\ 1\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 1\\ 0\end{bmatrix}. \end{aligned} \quad (63)$$

The sequence of the operators HP_0H is termed as the *diffusion operator*, since it reflects the amplitudes of the quantum states in $O|x\rangle$ with respect to the average of their amplitudes, as illustrated in Fig. 9c, where the average of the amplitudes in our scenario's $O|x\rangle$ is $(3 \cdot 0.5 - 0.5)/4 = 0.25$ as it may be verified from (62). At the same time, when considering the QIR as the superposition of the states $|s\rangle$ and $|ns\rangle$, the reflection with respect to the initial state $|x\rangle$ may be seen in Fig. 12. Hence, a single application of $\mathcal{G}$ to the initial QIR state $|x\rangle$ verifies that it succeeds in maximizing the probability of obtaining the solution upon a potential observation of the QIR, since we have $|x_1\rangle = 0\cdot|0\rangle + 0\cdot|1\rangle + 1\cdot|2\rangle + 0\cdot|3\rangle$ in (63). It should be noted that in different systems, the probability of finding the solution might not become equal to 100%, but it may be close to it. In fact, the probability of obtaining a solution is equal to 100% only when the number of solutions S is 25% of all the entries N, or, equivalently, when we have the ratio $S/N = 1/4$ [54]. If we apply $\mathcal{G}$ one more time, we arrive at

$$|x_2\rangle = \mathcal{G}|x_1\rangle = \mathcal{G}^2|x\rangle = \frac{1}{2}\begin{bmatrix}-1\\ -1\\ 1\\ -1\end{bmatrix} \quad (64)$$

which is translated to another equiprobable superposition of all states, as presented in Fig. 9d, verifying the rotation that $\mathcal{G}$ imposes on $|x\rangle$ with respect to the states $|s\rangle$ and $|ns\rangle$, as depicted in Fig. 12. The periodicity imposed on the quantum amplitudes of the states in the QIR due to the consecutive applications of $\mathcal{G}$ is illustrated in Fig. 13. The probability of success in finding the unique solution by applying the same number of $\mathcal{G}$ operators in systems having a different search space size N will vary. There is a non-negligible probability that applying the same number of $\mathcal{G}$ operators to a search space having a size of $N = 2^n$ would provide an almost 100% probability of finding the unique solution, while applying the same number of $\mathcal{G}$ operators to a search space having a size of $N = 2^{n+1}$ would result in a probability of obtaining the unique solution which is close to zero. This phenomenon is depicted in Fig. 14 in quantitative terms.

B. BBHT QUANTUM SEARCH ALGORITHM

In many practical applications the number of solutions is higher than one and the exact number of solutions is not known beforehand. Grover's QSA would most probably fail, or, more precisely, we would have a successful detection probability of $\sin^2\left[(2L_{opt}+1)\varphi\right] \approx 0$, if the same number of L_{opt} was used in diverse systems having different number of solutions, since φ of (60) would have changed. The BBHT QSA of [54] circumvents this problem by applying $\mathcal{G}$ of Fig. 10 a pseudo-random consecutive number of times to the initial system, observing the resultant state in the QD and then repeating it until a solution is obtained after the observation. Assuming $0 \leq S \leq 3N/4$, as it is the case in our scenario, the steps of the BBHT algorithm are summarized as in Algorithm 1 [54]:

Algorithm 1: BBHT Quantum Search Algorithm

1: Set $m \leftarrow 1$, $\lambda \leftarrow 6/5$ and $L_{BBHT} \leftarrow 0$.
2: Choose L uniformly from the set $\{0, \ldots, \lfloor m \rfloor\}$.
3: Apply the $\mathcal{G}$ operator L times starting from the initial state $|x\rangle$ in (43), resulting in the final state $|x_f\rangle = \mathcal{G}^L|x\rangle$.
4: Observe $|x_f\rangle$ in the QD and obtain $|j\rangle$.
5: Update $L_{BBHT} \leftarrow L_{BBHT} + L$.
6: **if** $f(j) = \delta$ or $L_{BBHT} \geq L_{BBHT}^{\max}$ **then**
7: Set $x_s \leftarrow j$, output x_s and exit.
8: **else**
9: Set $m \leftarrow \min\left\{\lambda m, \sqrt{N}\right\}$ and go to Step 2.
10: **end if**

The BBHT QSA [54] manages to find a solution after $L_{BBHT}^{\max} = 4.5\sqrt{N/S}$ $\mathcal{G}$ operations, or, equivalently, Oracle calls in the worst case as formally proved in [54]. It should be noted at this point that the number of CF evaluations during a BBHT iteration is equal to the number of Oracle calls, plus an additional one required for determining whether the obtained value j is a solution or not. If no solution is found after $L_{BBHT}^{\max}$ iterations, it may be concluded that we have $S = 0$. The parameter λ may be chosen in the set $(1, 4/3)$ and the evaluation of $f(j)$ at Step 6 is performed in the classic domain. If there is no solution for the search problem, i.e. we have $S = 0$, the BBHT QSA will realize this fact after $4.5\sqrt{N}$

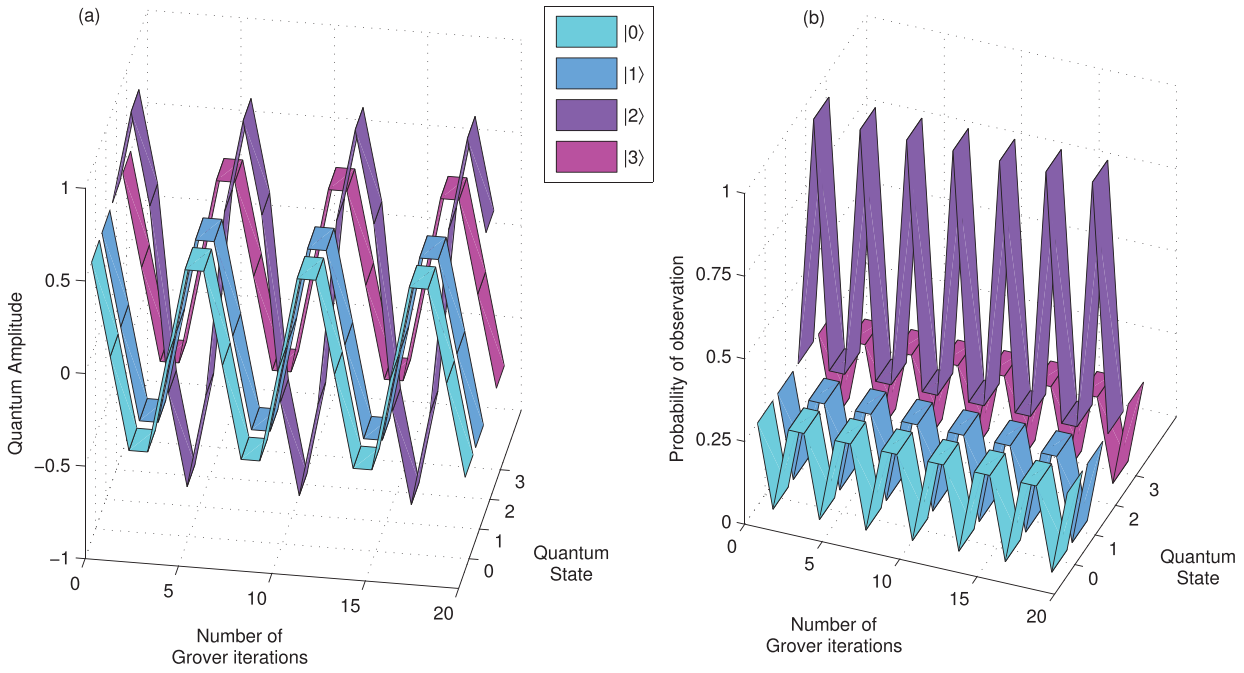

FIGURE 13. (a) Quantum amplitudes of the QIR $|x\rangle$ with respect to the number of Grover operators $\mathcal{G}$ applied to it. (b) Probability of obtaining a quantum state after applying the corresponding number of Grover operators $\mathcal{G}$. The minimum optimal number of Grover operations is one, which in our scenario is also the global optimal number of Grover operations, since the marked state reaches 100% probability to be observed.

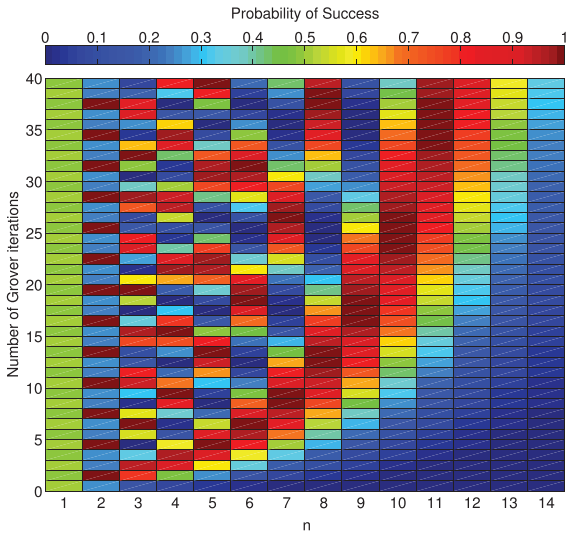

FIGURE 14. Probability of obtaining the solution when observing a QIR with $N = 2^n$ quantum states after having applied a specific number of Grover operators $\mathcal{G}$. The periodical nature of Grover's QSA is evident.

TABLE 3. BBHT QSA Scenario's Instance.

Step	Process
1	Set $m \leftarrow 1$, $\lambda \leftarrow 6/5$ and $L_{BBHT} \leftarrow 0$
2	Since $m = 1$, we have $L \in \{0, 1\}$ and we randomly choose $L \leftarrow 0$
3	After $L = 0$ $\mathcal{G}$ operations: $\|x_f\rangle = \mathcal{G}^L\|x\rangle = \mathcal{G}^0\|x\rangle = \|x\rangle$
4	We observe $\|x_f\rangle$ and obtain $\|1\rangle$ (25% probability)
5	$L_{BBHT} \leftarrow L_{BBHT} + L = 0$
6	We compute $f(1) = 0.16$ in the classic domain and check that $f(1) \neq \delta$
8–9	$L_{BBHT} < L_{BBHT}^{\max} = 9$, thus $m \leftarrow \min\{\lambda m, \sqrt{N}\} = \lambda m = 6/5 = 1.2$
2	Since $m = 1.2$, we have $L \in \{0, 1\}$ and we randomly choose $L = 1$
3	After $L = 1$ $\mathcal{G}$ operations: $\|x_f\rangle = \mathcal{G}^L\|x\rangle = \mathcal{G}^1\|x\rangle = \|x_1\rangle$, where $\|x_1\rangle$ is in (63)
4	We observe $\|x_f\rangle$ and obtain $\|2\rangle$ (100% probability)
5	$L_{BBHT} \leftarrow L_{BBHT} + L = 1$
6–7	We compute $f(2) = 0.38 = \delta$, thus $x_s \leftarrow 2$. Output x_s and exit.

Oracle operations by delivering a final output of x_f for which we have $f(x_f) \neq \delta$.

Let us proceed by applying the BBHT QSA in our scenario for finding the index x_s such that $f(x_s) = 0.38 = \delta$, assuming that we do not know that $\delta = f(2) = 0.38$ appears only once as a result of the CF evaluations. Assuming uniqueness of our solution, which is the worst case scenario, the BBHT QSA has to find it after a maximum of $L_{BBHT}^{\max} = 4.5\sqrt{N} = 9$ $\mathcal{G}$/Oracle calls and we choose $\lambda = 6/5$. Since the BBHT QSA includes randomly generated parameters, we offer one of the possible outcomes in Table 3, where the steps visited by the BBHT QSA are also given. The probabilities included in the parentheses denote the probability of observing the obtained state before the measurement, but naturally, these probabilities are not available in real applications.

C. DÜRR–HØYER ALGORITHM

The DHA [55] finds the solution $x_{\min} = \arg\min_{\forall x}\{f(x)\}$ that minimizes $f(x)$ by employing the BBHT QSA. The only modification in the BBHT QSA is that the Oracle in

$\mathcal{G}$ of Fig. 10 will mark as solutions the particular states x that satisfy $f(x) < \delta$. The steps of the DHA are stated in Algorithm 2 [55]:

Algorithm 2: Dürr–Høyer Algorithm

1: Choose i uniformly from the set $\{0, \ldots, N-1\}$ and set $L_{total} \leftarrow 0$.
2: The BBHT QSA is employed with $\delta \leftarrow f(i)$ and an Oracle that marks as solutions the states $|x\rangle$ that obey $f(x) < \delta$. Obtain x_s and L_{BBHT} from the BBHT QSA.
3: $L_{total} \leftarrow L_{total} + L_{BBHT}$.
4: **if** $f(x_s) \geq f(i)$ or $L_{total} \geq L_{DHA}^{\max}$ **then**
5: Set $x_{\min} \leftarrow i$, output $x_{\min}$ and exit.
6: **else**
7: Set $i \leftarrow x_s$ and go to Step 2.
8: **end if**

It was formally shown in [55] that $x_{\min}$ is found with 100% probability after $L_{DHA}^{\max} = 22.5\sqrt{N}$ applications of the $\mathcal{G}$ operator of Fig. 10 in the worst-case scenario and from Section VI-B we may conclude that the best case scenario includes as few as $4.5\sqrt{N}$ Grover iterations, if the initial i is chosen to be equal to $x_{\min}$ and thus $S = 0$. Hence, the DHA may be carried out in $22.5\sqrt{N}$ and $4.5\sqrt{N}$ Oracle operations in the worst-case and best-case scenario, respectively. Once again, the CF evaluations in Step 4 of Alg. 2 are realized in the classic domain. It should be noted that in contrast to Grover's QSA [53] and the BBHT QSA [54], the DHA [55] does not assume any *a priori* knowledge of the values of the CF evaluations, making it applicable in a broad range of applications, where low-cost optimization is desired.

The DHA relies on a range of randomly generated variables, as exemplified in Algorithms 2 and 1, hence resulting into different sequences of steps, even if we employ it in the same scenario. In our DS-CDMA scenario, the most likely 4-level symbol to have been transmitted is the one that maximizes the CF in (4). Hence, we employ the DHA to find the minimum of the function $-f(x)$. An instance where the DHA is employed to find $x_{\min}$ such that $-f(x_{\min}) \leq -f(x)$, where $x = 0, 1, 2, 3$ in our DS-CDMA MUD scenario of (42) is presented in Table 4, where we have $\lambda = 6/5$, $L_{BBHT}^{\max} = 4.5\sqrt{N} = 9$ and $L_{DHA}^{\max} = 22.5\sqrt{N} = 45$ Grover iterations. The acronym BBHT refers to the numbered step in the BBHT QSA. Even though the total number of CF evaluations in this scenario turns out to be higher than $N/2$, which is the average in the optimal classic algorithm, its computational power is revealed systems associated with a large N.

Let us proceed by stating some insightful comments on the instance of the DHA's application in our scenario. For deeper intuition of the processes, let us assume that we knew *a priori* the CF evaluations of (42). The first time when we visit Step 2 in Table 4, it may be concluded that we found a solution in the BBHT QSA without applying Grover operators of Fig. 10 at all. This is very likely since all the CF evaluations of $-f(x)$ for $x = 0, 2, 3$ are smaller than $\delta = -f(1)$ and hence there are $S = 3$ solutions amongst the $N = 4$ entries, resulting in 75% probability of obtaining a solution by simply observing the equiprobable initialized superposition of states, with 25% probability of obtaining each of the four states. When the BBHT QSA of Alg. 1 is employed for the second time, we have $S = 1$ solution and that solution is $|x_s\rangle = |2\rangle$. Since there are $N = 4$ entries, if $L = 1$ was chosen in the BBHT QSA we would obtain $|x_f\rangle = |2\rangle$ with 100% probability, as it was the case in our instance. Finally, when the BBHT QSA was employed for the last time, there were $S = 0$ solutions, since $x_{\min}$ had already been found. Naturally, this knowledge is unavailable to the BBHT QSA, which hence performed the maximum number of $\mathcal{G}$ operations, namely $L_{BBHT}^{\max} = 9$, finally yielding $x_{new} = 0$ and allowing us to conclude that we have $x_{\min} = 2$, since $-f(2) < -f(0)$.

TABLE 4. DHA in the DS-CDMA MUD Scenario.

Step	Process
1	We randomly choose $i \leftarrow 1$ from the set $\{0, 1, 2, 3\}$ and set $L_{total} \leftarrow 0$
2	Set $\delta \leftarrow -f(1) = -0.16$ and employ the BBHT QSA
BBHT 1	Set $m \leftarrow 1$, $\lambda \leftarrow 6/5$ and $L_{BBHT} \leftarrow 0$
BBHT 2	Since $m = 1, L \in \{0, 1\}$ and we randomly choose $L \leftarrow 0$
BBHT 3	After $L = 0$ $\mathcal{G}$ operations: $\|x_f\rangle = \mathcal{G}^L\|x\rangle = \mathcal{G}^0\|x\rangle = \|x\rangle$
BBHT 4–5	We observe $\|x_f\rangle$ and obtain $\|3\rangle$ (25% probability). Set $L_{BBHT} \leftarrow 0$
BBHT 6–7	We compute $-f(3) = -0.27$ in the classic domain and check that $-f(3) < \delta$. Hence, set $x_s \leftarrow 3$ and exit
3	Set $L_{total} \leftarrow L_{total} + L_{BBHT} = 0$
4	$-f(3) < -f(1)$ and $L_{total} < L_{DHA}^{\max} = 45$
6-7	Set $i \leftarrow x_s = 3$
2	Set $\delta \leftarrow -f(3) = -0.27$ and employ the BBHT QSA
BBHT 1	Set $m \leftarrow 1$, $\lambda \leftarrow 6/5$ and $L_{BBHT} \leftarrow 0$
BBHT 2	Since $m = 1, L \in \{0, 1\}$ and we randomly choose $L \leftarrow 1$
BBHT 3	After $L = 1$ $\mathcal{G}$ operations: $\|x_f\rangle = \mathcal{G}^L\|x\rangle = \mathcal{G}^1\|x\rangle = \|x_1\rangle$, where $\|x_1\rangle$ is in (63)
BBHT 4–5	We observe $\|x_f\rangle$ and obtain $\|2\rangle$ (100% probability). Set $L_{BBHT} \leftarrow 1$
BBHT 6–7	We compute $-f(2) = -0.38$ in the classic domain and check that $-f(2) < \delta$. Hence, set $x_s \leftarrow 2$ and exit
3	Set $L_{total} \leftarrow L_{total} + L_{BBHT} = 1$
4	$-f(2) < -f(3)$ and $L_{total} < L_{DHA}^{\max} = 45$
6–7	Set $i \leftarrow x_s = 2$
2 & BBHT	Set $\delta \leftarrow -f(2) = -0.38$ and the BBHT QSA outputs $x_s = 0$ with $L_{BBHT} = 9$
3	$L_{total} \leftarrow L_{total} + L_{BBHT} = 1 + 9 = 10$
4–5	Since $-f(0) > -f(2)$, set $x_{\min} \leftarrow 2$, output $x_{\min}$ and exit

VII. QUANTUM WEIGHTED SUM ALGORITHM

The QWSA is capable of estimating the weighted sum of the CF in both the numerator and denominator of the LLR expressed in (2) by using a fixed number of CF evaluations, regardless of the number of users K or of the modulation order M. It can be applied to any function $f : \{0, 1, \ldots, N-1\} \rightarrow [0, 1]$, including the CF of (4) in conjunction with $N = M^K/2$. Where necessary, we will present application examples for a system supporting $K = 2$ users and QPSK modulation relying on $M = 4$. Furthermore, $N = 8$ CF evaluations contribute to each summation and the numerator ($b = 0$) of the first user's ($k = 0$) first bit ($m = 0$)

LLR is estimated. The same process is also applied for the denominator of the same bit, as well as for the numerators and denominators of the rest of the bits of the multi-level M^K-ary symbol.

The QWSA invoked for a user's bit value estimates the weighted sum of the evaluations of the function $f(x)$ in (4) for all the x values that contribute to that bit value. The process of the QWSA invoked for determining each user's bit value may be summarized in two steps:

1) Construct a QR associated with $(K \log_2 M)$ qubits in the state

$$|\Psi\rangle = \sum_{x\in\chi(0,0,0)} \left(\sqrt{P(x)(1-f(x))}|x\rangle\right)|0\rangle + \sum_{x\in\chi(0,0,0)} \left(\sqrt{P(x)f(x)}|x\rangle\right)|1\rangle. \quad (65)$$

The number of qubits is one less than the number of bits in our M^K-ary symbols, $(K \cdot \log_2(M) - 1) = 3$, plus 1. The last qubit distinguishes between the states which have the probability of $P(x)(1-f(x))$ and those with a probability of $P(x)f(x)$, when the last qubit is $|0\rangle$ and $|1\rangle$, respectively. It should be noted that the probability of a state associated with the last qubit being $|1\rangle$ is one of the additive terms in our desired summation in the numerator of (2).

2) Employ l qubits and the Quantum Amplitude Estimation (QAE) algorithm [51] to estimate the probability of obtaining a state with the last qubit equal to $|1\rangle$, when observing $|\Psi\rangle$ in the QD. This probability is given by the sum of the square of the amplitudes of all the states for which the last qubit is $|1\rangle$, hence $\sum_{x\in\chi(0,0,0)}[P(x)f(x)]$ from (65), which is the numerator of the first user's first bit as in (2).

A. PREPARATION OF THE QR $|\Psi\rangle$

Let us commence our analysis by introducing the unitary operator A, relying on the quantum circuit of Fig. 15. We employ $n = \log_2 N$ qubits for representing all the input arguments of the CF evaluations included in the summation, Z qubits to store the CF evaluations and an additional auxiliary qubit, $|0\rangle_3$, all initialized to the $|0\rangle$ state. The first n qubits are rotated by a qubit-specific rotation operator R_i. The rotation angle of each qubit depends on the *a priori* probability of the specific classic bit being equal to 0, which the qubit corresponds to. If for example $P(b_k^{(m)} = 0)$ is the *a priori* probability of the kth user's mth bit being 0, and the currently estimated LLR does not belong to it, then the $i = ((k-1)\log_2 M + m)$th qubit's unitary rotation operator R_i would be equal to

$$R_i = \begin{bmatrix} \sqrt{P(b_k^{(m)}=0)} & -\sqrt{P(b_k^{(m)}=1)} \\ \sqrt{P(b_k^{(m)}=1)} & \sqrt{P(b_k^{(m)}=0)} \end{bmatrix}. \quad (66)$$

This is the only difference with respect to the QMA, which uses H operators instead of R_i, for creating an equiprobable

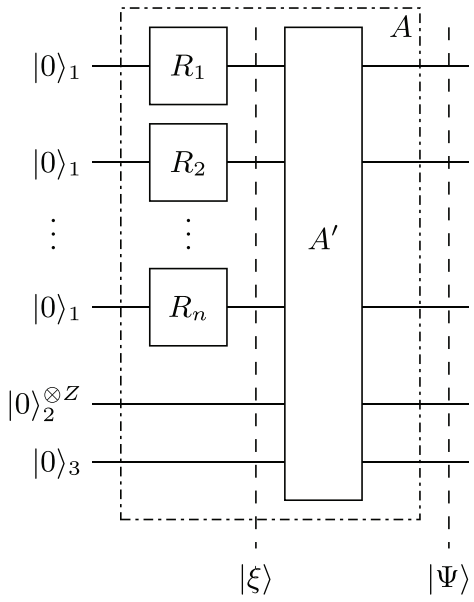

FIGURE 15. Quantum circuit of the unitary operator A. In the first QR, the $i = ((k-1)\log_2 M + m)$th rotation gate R_i, $i = 0, 1, \ldots, n$ maps the ith qubit to the state $\sqrt{P\left(b_k^{(m)}=0\right)}|0\rangle + \sqrt{P\left(b_k^{(m)}=1\right)}|1\rangle$, where the resultant amplitudes are the *a priori* bit probabilities included in (5). The A' operator illustrated in Fig. 16 is then applied to the three QRs.

superposition of all the input arguments at this point. It should be noted that if all the *a priori* bit probabilities are equal to 0.5, the QWSA transforms into the QMA, since the weights will be equal to each other and we have $R_i = H$. This part of the QWSA describes the C/Q section of the QMUD of Fig. 2, since classic information is encoded into the probabilities of quantum states. Therefore, the quantum state $|\xi\rangle$ at the input of the block A' in Fig. 15 is equal to

$$|\xi\rangle = \sum_{x=0}^{N-1} \sqrt{P(x)}|x\rangle_1|0\rangle_2^{\otimes Z}|0\rangle_3 \quad (67)$$

where $P(x)$ is the product of all the probabilities of the bits' values, which contribute to the evaluation of $f(x)$ presented in (4), except for the specific bit for which the LLR is estimated.

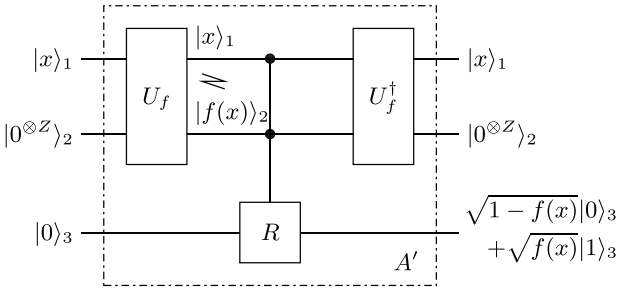

FIGURE 16. Quantum circuit of the unitary operator A'. The unitary operator U_f accepts as inputs a quantum state $|x\rangle$ and Z qubits in the zero state, where Z is the number of bits $f(x)$ is desired to be calculated in. After the controlled R operation, the inverse quantum circuit of U_f is applied in order to return the second QR to the all-zero state.

In our scenario, for $x = 1$, we have $P(1) = P(0001) = P(b_0^{(1)} = 0)P(b_1^{(0)} = 0)P(b_1^{(1)} = 1)$.

The unitary operator A' is then applied to the state $|\xi\rangle$. The quantum circuit is presented in Fig. 16 and its operation may be summarized as

$$|x\rangle|0^{\otimes Z}\rangle|0\rangle \xrightarrow{A'} |x\rangle|0^{\otimes Z}\rangle \left(\sqrt{1-f(x)}|0\rangle + \sqrt{f(x)}|1\rangle\right) \quad (68)$$

where the controlled rotation gate R may be described as

$$R = \begin{bmatrix} \sqrt{1-f(x)} & -\sqrt{f(x)} \\ \sqrt{f(x)} & \sqrt{1-f(x)} \end{bmatrix}. \quad (69)$$

Equation (68) may be further simplified by removing $|0^{\otimes Z}\rangle$, since it is independent of $|x\rangle$ and the operation of the block A' in Fig. 16 becomes

$$|x\rangle|0\rangle \xrightarrow{A'} |x\rangle \left(\sqrt{1-f(x)}|0\rangle + \sqrt{f(x)}|1\rangle\right). \quad (70)$$

The operator A shown in Fig. 15 uses 2 CF evaluations and its output state $|\Psi\rangle$ is

$$|\Psi\rangle = \underbrace{\sum_{x=0}^{N-1} \sqrt{P(x)(1-f(x))}|x\rangle|0\rangle}_{\sqrt{1-a}|\Psi_0\rangle} + \underbrace{\sum_{x=0}^{N-1} \sqrt{P(x)f(x)}|x\rangle|1\rangle}_{\sqrt{a}|\Psi_1\rangle}. \quad (71)$$

where a is the probability of arriving at the states belonging to the set $|\Psi_1\rangle$ when $|\Psi\rangle$ is observed, which is equal to the desired weighted sum

$$a = \sum_{x=0}^{N-1} P(x)f(x). \quad (72)$$

The states in $|\Psi_1\rangle$ are the wanted states, which differ from the unwanted states of $|\Psi_0\rangle$ only in terms of the last qubit being $|1\rangle$ and $|0\rangle$, respectively.

B. QUANTUM AMPLITUDE ESTIMATION

The QAE process of [51] is employed for estimating the amplitude $\sqrt{a}$ of $|\Psi_1\rangle$ in (71). The quantum circuit of the QWSA integrating A and the QAE is illustrated in Fig. 17. The superscript of the Q operator indicates the number of Q operator activations. Every time the unitary operator Q is applied, it rotates the Quantum Function Register (QFR) by 2θ, where we have

$$\theta = \arcsin\sqrt{a} \Rightarrow a = \sin^2\theta. \quad (73)$$

Therefore, an estimate of θ would also provide an estimate of a. More specifically, the quantum circuit of Q is shown in Fig. 18 and its operation is formulated as

$$Q = AP_0A^\dagger B \quad (74)$$

where B is a unitary operator that "marks" the desired states by changing their sign and P_0 changes a state's sign if and only if that state is not the all-zero state as encapsulated in (46). Operator B may be implemented with the aid of a *CNOT* gate as in (21) controlled by the particular qubit that determines if a state is a wanted one or not, and by an auxiliary target qubit in the $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ state. The unitary operator Q may be considered as a generalized Grover operator, since it is constructed in a similar way as the generalized Grover operators in [86], [90], by replacing the Hadamard operators H with the unitary operators A, as well as the Oracle O by B and leaving the controlled phase shift operator P_0 unaltered. Geometrically, when B is applied to $|\Psi\rangle$, the input state $|\Psi\rangle$ is reflected with respect to the unwanted states $|\Psi_0\rangle$ and $U_\Psi = AP_0A^\dagger$ reflects the resultant state $B|\Psi\rangle$ with respect to the input state $|\Psi\rangle$, resulting in an anti-clockwise rotation by 2θ, as presented in Fig. 19. Since Q is unitary, its eigenvectors of $|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(\pm j|\Psi_0\rangle + |\Psi_1\rangle)$, which are associated with the corresponding eigenvalues of $\lambda_\pm = e^{\pm j2\theta}$ form an orthonormal basis. A repeated application of the Q operator i times would yield

$$\begin{aligned} Q^i|\Psi\rangle &= \cos((2i+1)\theta)|\Psi_0\rangle + \sin((2i+1)\theta)|\Psi_1\rangle \\ &= -\frac{j}{\sqrt{2}}\left(e^{j(2i+1)\theta}|\Psi_+\rangle - e^{-j(2i+1)\theta}|\Psi_-\rangle\right). \end{aligned} \quad (75)$$

The amplitudes of $|\Psi_0\rangle$ and $|\Psi_1\rangle$, with respect to the number of applications of the Q operator, are sinusoidal functions with a period of θ/π. The resemblance that the Q operator in (74) has with the Grover operator $\mathcal{G}$ in (57) may be seen by comparing their circuits in Figs. 18 and 10, respectively as well

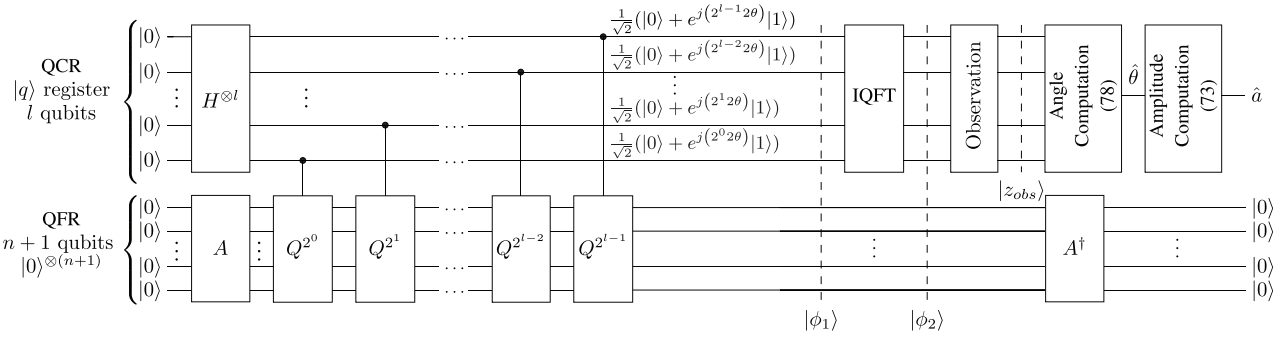

FIGURE 17. Quantum circuit of the QWSA, where the operators A and Q are depicted in Figs. 15 and 18, respectively. The superscripts of the Q operators signify the number of times the Q operator will be consecutively applied. The number of qubits in the QFR is $(n+1) = (K\log_2 M - 1 + 1) = K\log_2 M$.

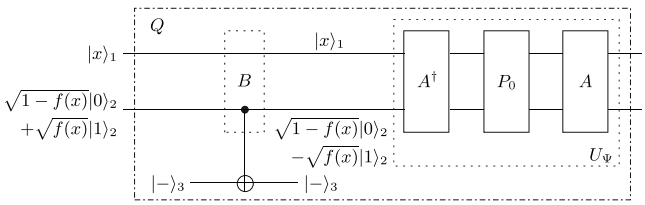

FIGURE 18. Quantum circuit of the unitary operator Q, where B consists of a CNOT gate, the quantum circuit of A is illustrated in Fig. 15 and the controlled phase shift gate P_0 is stated in (46).

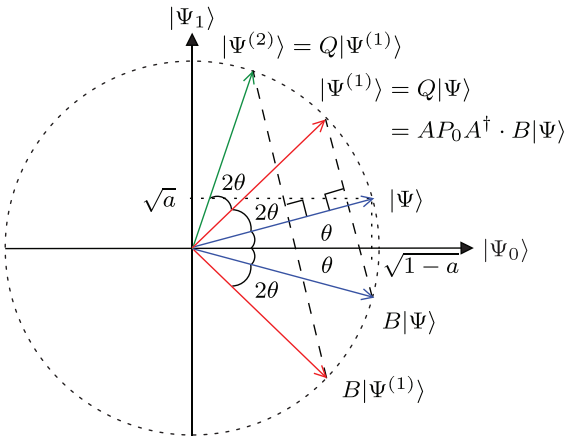

FIGURE 19. Geometrical interpretation of the operations of Q on $|\Psi\rangle$. The unitary operator B reflects the initial state $|\Psi\rangle$ with respect to $|\Psi_0\rangle$, while the unitary operator $AP_0A^\dagger$ reflects the state $B \cdot |\Psi\rangle$ with respect to $|\Psi\rangle$, resulting in the state $|\Psi^{(1)}\rangle = Q|\Psi\rangle$ and an overall counter-clockwise rotation of 2θ. The same process is repeated in subsequent applications of Q.

as their operations illustrated in Figs. 19 and 11, respectively. A Quantum Control Register (QCR) $|t\rangle$ containing l qubits will be initialized in an equiprobable superposition of states and will encode the angle of θ/π into its phases by using controlled Q operators, as seen in Fig. 17. Elaborating further, each of the QCR's qubits will apply a specific number of Q operators to the QFR, but only when its state is $|1\rangle$. The state $|\phi_1\rangle$ shown in Fig. 17 may be formulated after the controlled Q operators as

$$|\phi_1\rangle = \frac{e^{j\theta}}{\sqrt{2^{(l+1)}}} \sum_{q=0}^{2^l-1} e^{jq2\theta}|q\rangle|\Psi_+\rangle - \frac{e^{-j\theta}}{\sqrt{2^{(l+1)}}} \sum_{q=0}^{2^l-1} e^{-jq2\theta}|q\rangle|\Psi_-\rangle \quad (76)$$

which may be interpreted as an encoding of θ into the phases of 2^l quantum states.

The Inverse Quantum Fourier Transform (IQFT) [47] is applied to $|\phi_1\rangle$, resulting in

$$|\phi_2\rangle = \frac{e^{j\theta}}{\sqrt{2}} \left(\frac{1}{2^l} \sum_{z=0}^{2^l-1} \sum_{q=0}^{2^l-1} \left(e^{j2\pi\left(\frac{\theta}{\pi}-\frac{z}{2^l}\right)} \right)^q |z\rangle \right) |\Psi_+\rangle - \frac{e^{-j\theta}}{\sqrt{2}} \left(\frac{1}{2^l} \sum_{z=0}^{2^l-1} \sum_{q=0}^{2^l-1} \left(e^{j2\pi\left(-\frac{\theta}{\pi}-\frac{z}{2^l}\right)} \right)^q |z\rangle \right) |\Psi_-\rangle. \quad (77)$$

A QCR's state $|z\rangle$ in $|\phi_2\rangle$ has the same probability to be observed in the QD as the state $|2^l - z\rangle$, with the maximum probability belonging to the states that minimize $z \pm 2^l\theta/\pi$. Once the QCR is observed and $|z_{obs}\rangle$ is obtained, θ is estimated as

$$\hat{\theta} = \pi \frac{z_{obs}}{2^l}. \quad (78)$$

The QD observation performed at this step of the QWSA is the Q/C conversion stage of the QMUD seen in Fig. 2, since the quantum state of the system converts to a classic one. Finally, the weighted sum a is estimated from (73) and the operator $A^\dagger$ returns the QFR of Fig. 17 to the all-zero state.

VIII. NORMALIZATION AND COMPUTATIONAL COMPLEXITY

The operators A and $A^\dagger$ perform $C = 2$ CF evaluations each. The QWSA repeatedly uses the Q operator $(2^l - 1)$ times, which in turn performs $C = 4$ CF evaluations each, resulting in a complexity of $C = 4 \cdot 2^l = 2^{l+2}$ CF evaluations. It should be noted that the number of qubits employed in the QCR unambiguously determines the complexity of the algorithm, which is independent of the number of the additive terms [71], or, in other words, independent of both the number of users and of the modulation scheme employed. For example, a QWSA MUD employing $l = 12$ qubits results in a complexity of 2^{14} CF evaluations for each user's each bit. According to our simulation results presented in Section IX, a choice of $l = 11$ qubits is sufficient in terms of balancing the performance versus complexity relationship. In the QWSA-based MUD, the QWSA of Fig. 17 is employed twice for each bit of every user, namely once for that bit's value being 0 and once for 1, during each MUD-decoder outer iteration.

The minimum non-zero detectable sum in (72) is equal to $S_{\min} = \sin^2(\pi/2^l)$. The QWSA MUD may deliver a zero output if the actual sum is smaller than $S_{\min}/2$. When many users are supported in the system, $f(\mathbf{x})$ in (4) becomes extremely small even for the $\mathbf{x}_{\max}$ that provides the maximum CF value, $f(\mathbf{x}_{\max}) < S_{\min}/2$. Hence, the QWSA will fail to estimate the summation of both the numerator and denominator of (2), mapping them to 0. In order to circumvent this problem, we normalize $f(x) = P(\mathbf{y}|\mathbf{x})$ with respect to the maximum value $f(\mathbf{x}_{\max})$ of the CF. This will result in the normalized $f(\mathbf{x})$ being equal to 1 at $\mathbf{x}_{\max}$ and will be lower for the remaining arguments. In order to determine the maximum value of $f(\mathbf{x})$ during each timeslot, various techniques may be employed, such as a quantum-inspired GA MUD, the classic ACO algorithm of [7], or the DHA that finds the minimum of a function [55], with the function in our case being $-f(\mathbf{x})$.

The classic ACO algorithm employs ζ ants in each of the Ξ generations and outputs the argument $\mathbf{x}_{\max}$ that maximizes the CF in the majority of the cases, while imposing a complexity

of $(\zeta \times \Xi)$ CF evaluations. Each of the parameters ζ and Ξ may be chosen to be $\log_2(M^K)$, resulting in a total complexity of $\log_2^2(M^K)$ CF evaluations [7].

As analysed in Section VI-C, the DHA employs the BBHT QSA. The DHA is provided with a random initial argument $\mathbf{x}_{init}$ and finds $\mathbf{x}_{\max}$ with $\sim 100\%$ probability after $22.5\sqrt{M^K}$ CF evaluations in the worst case [55]. Since in our scenarios we have access to the output of the MF, we choose $\mathbf{x}_{init} = \mathbf{x}_{MF}$ for avoiding this worst case scenario. Furthermore, in some of the cases we have $\mathbf{x}_{\max} = \mathbf{x}_{MF} = \mathbf{x}_{init}$, resulting in the lowest bound of $4.5\sqrt{M^K}$ CF evaluations per time slot [54] for finding $f(\mathbf{x}_{\max}) = P(\mathbf{y}|\mathbf{x}_{\max})$. The individual employment of the DHA provides a quantum-assisted optimal hard-output MUD, since it finds the argument $\mathbf{x}_{\max}$ that maximizes the CF at a complexity of $O(\sqrt{M^K})$.

Hence, a QWSA MUD relying on l qubits, M-ary modulation, K users and J MUD-decoder iterations will have an overall complexity order of

$$O(C) = 2^{l+3} \cdot J \cdot \log_2(M^K) + \begin{cases} 22.5\sqrt{M^K} & \text{upper bound} \\ 4.5\sqrt{M^K} & \text{lower bound} \end{cases} \quad (79)$$

CF evaluations when DHA is employed for normalization, compared to M^K for the classic ML MUD. The factor $O(\sqrt{M^K})$ becomes dominant in large-dimensional systems. If the ACO algorithm is used in order to find the maximum of $f(x)$, the complexity imposed will be smaller, as illustrated in

$$O(C) = 2^{l+3} \cdot J \cdot \log_2(M^K) + \log_2^2(M^K) \quad (80)$$

but the attainable performance would also be degraded, if an erroneous $\mathbf{x}_{\max}$ was chosen. If $l = 11$ is chosen and there are $J = 4$ iterations between the MUD and the decoder, the upper bound of the DHA-QWSA MUD's complexity becomes $2^{16} \cdot K \log_2 M + 22.5\sqrt{M^K}$ CF evaluations, which is less complex than the ML MUD for $K > 6$ users transmitting 8-PSK symbols or for $K > 10$ users employing QPSK modulation, as quantified in Fig. 20. If the affordable complexity of our receiver processor is a maximum of $\left(4 \cdot 10^6\right)$ CF evaluations, a BPSK system will be able to support $K = 33$ users using the QWSA MUD in contrast to $K = 22$ users, when the ML MUD is employed. Similarly, in a 64-QAM system supporting $K = 5$ users, the complexity of the QWSA MUD is 0.25% of that of the ML MUD in the worst-case scenario. On the other hand, if the ACO-QWSA MUD is used, the complexity is always lower than that of the DHA-QWSA MUD complexity's upper bound and also smaller than its lower bound in large-dimensional systems. In greater detail, for $K = 30$ users and QPSK symbols, the complexity of the ACO-QWSA is a fraction of 10^{-12} in comparison to that of the ML MUD. It should be stated that the ACO-QWSA MUD's performance is extremely dependent on the accuracy of the ACO algorithm involved for finding the maximum value of the CF. Comparing the proposed QWSA MUD to the hard-output QMUD introduced in [60] that has a complexity of $O[2^{l+1} \log_2(M^K)]$ CF evaluations [60], for $l \geq \log_2\left(M^K\right)$

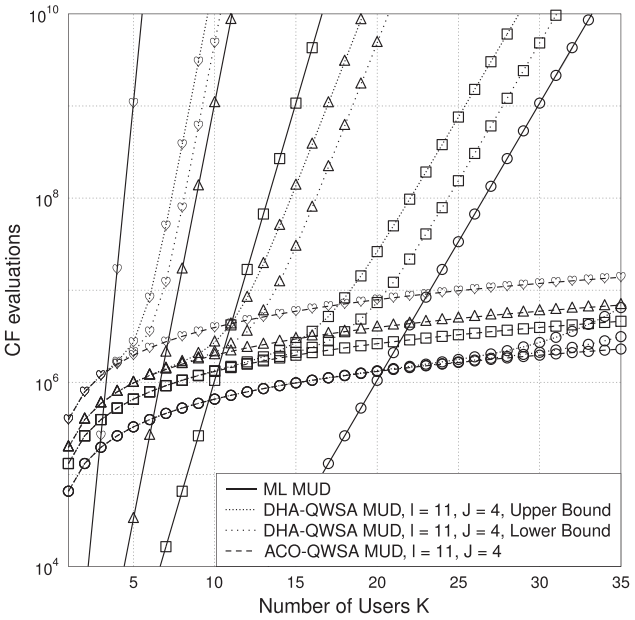

FIGURE 20. Complexity in terms of number of CF evaluations for the proposed QWSA MUD with $I = 11$ qubits, $I_{model} = 15$ qubits and the classic, optimal ML MUD, without MUD-decoder iterations ($J = 1$).

operating in a noiseless scenario [60], we may conclude that its complexity is lower, regardless of whether the DHA or ACO is used.

The simulation results of Section IX have been recorded for a DHA-QWSA MUD, where the DHA offers $\sim 100\%$ probability of success in finding the minimum of $-f(\mathbf{x})$. The reason behind our choice was to demonstrate the capabilities of the QWSA, providing it with perfect and error-free normalization of the CF, hence reaching the upper bound of the QWSA-based MUD's performance. It should be noted that the DHA-QWSA MUD is a quantum-based MUD implementable in classic systems, whereas the ACO-QWSA MUD is a hybrid of the classic- and the quantum-domain. After finding $f(\mathbf{x}_{\max})$ with the aid of the DHA, the CF is transformed into

$$f'(\mathbf{x}) = \frac{f(\mathbf{x})}{f(\mathbf{x}_{\max})} = \frac{P(\mathbf{y}|\mathbf{x})}{P(\mathbf{y}|\mathbf{x}_{\max})}. \quad (81)$$

The accuracy of the weighted sum's estimate according to [51], [71] is upper-bounded by

$$|\hat{a} - a| \leq 2\pi w \frac{\sqrt{a(1-a)}}{2^l} + w^2 \frac{\pi^2}{2^{2l}}, \quad w = 1, 2, \ldots \quad (82)$$

with a probability $8/\pi^2$ for $w = 1$ and at least $1 - 1/(2(w-1))$ for $w \geq 2$. The choice of the number of qubits l in the QCR depends on both the maximum tolerable probability of erroneously deciding θ and on the accuracy, expressed in terms of the number of bits that θ is represented by.

If during the calculation of the LLRs only one of the two bit's values turn out to be 0 according to the QWSA MUD, then we assume maximum confidence and we map that bit's LLR to 20 or -20, where $\sum_{\mathbf{x} \in \chi(k,m,1)} P(\mathbf{y}|\mathbf{x}) P(\mathbf{x}) = 0$ or $\sum_{\mathbf{x} \in \chi(k,m,0)} P(\mathbf{y}|\mathbf{x}) P(\mathbf{x}) = 0$, respectively. If according to the QWSA MUD the numerator and the denominator of a bit LLR

turns out to be equal to each other, but not equal to 0 or $S_{\min}$, at low E_b/N_0, there is no significant error, since the actual LLR will also be close to 0. In this scenario, the dominant source of error may occur due to having an inadequate precision in terms of the number of qubits l.

IX. SIMULATION RESULTS AND DISCUSSIONS

In this section we will characterize the design of the proposed QMUD both with the aid of EXIT charts [4], as well as by its BER performance. In Fig. 21 we commence by first presenting the BER performance of BICM-ID systems supporting $K = 4, 6$ and 8 users employing QPSK modulation associated with $M = 4$. Turbo Coding relying on Convolutional Codes (TCCC) is used at a rate of $R = 1/2$, relying on 8 trellis states and $I_{inner} = 4$ iterations between the convolutional codes. The performance of the DHA-based hard-input hard-output MUD is compared to that of the ML MUD and to that of the MF detection. We may conclude that the performance of the DHA is optimal, since it matches that of the hard ML MUD. The number of CF evaluations performed by the ML MUD of the systems supporting $K = 4, 6$ and 8 users employing QPSK is $M^K = 256$, 4096 and 65 536, respectively, while the average number of CF evaluations in the same systems when the DHA was used is 78, 342 and 1456, respectively. Hence, by using the DHA for hard MUD we may achieve optimal performance at a substantially reduced computational complexity.

Let us now proceed to the soft-input soft-output QMUD by introducing a CDMA system supporting $K = 2$ coexisting users, employing Gold codes having a spreading factor of

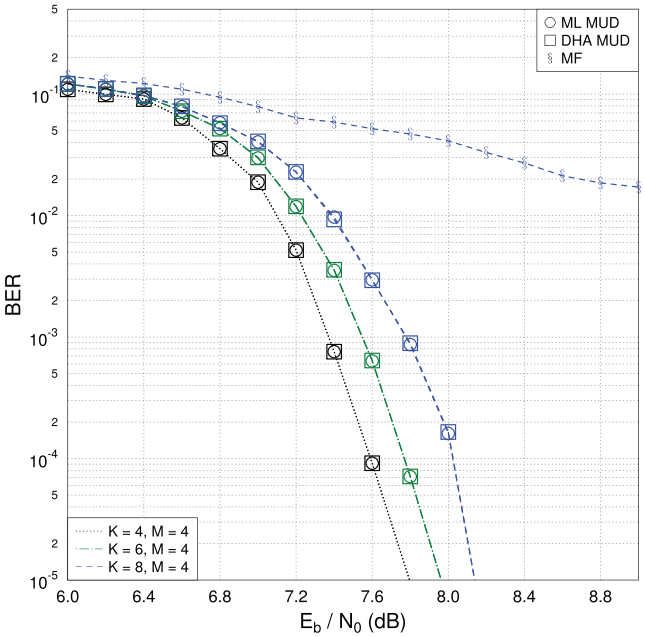

FIGURE 21. BER performance of BICM-ID DS-CDMA systems supporting $K = 4, 6, 8$ users transmitting QPSK $M = 4$ symbols. The DHA MUD is compared to the ML MUD and the MF detection, verifying its optimality in finding the minimum of a function. The interleaver length is equal to 20 000 bits.

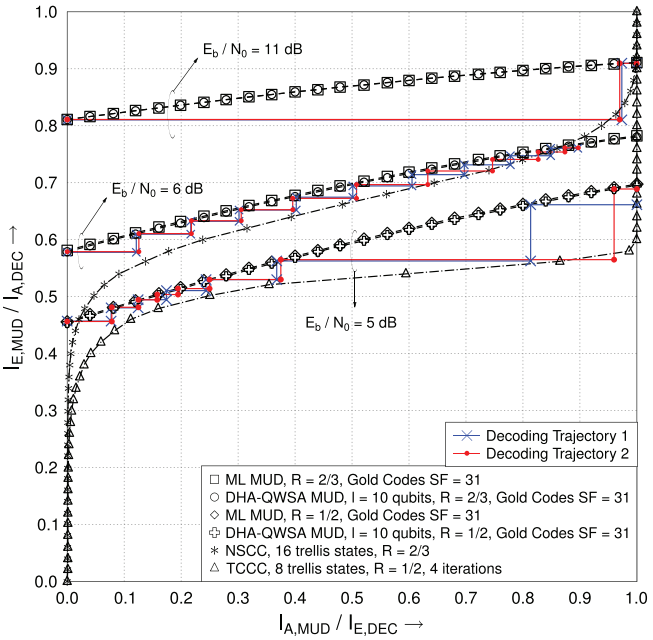

FIGURE 22. EXIT charts of a CDMA system with $K = 2$ users, $SF = 31$ chips, BICM-ID with Non-Systematic Convolutional Codes, $R = 2/3$, 16 trellis states and Turbo Code relying on Convolutional Codes, $R = 1/2$, 8 trellis states and $I_{inner} = 4$ inner iterations. DHA-QWSA-based MUD is used with $l = 10$ qubits in the QCR of Fig. 17.

$SF = 31$. Each of them uses BICM-ID constructed by a Non-Systematic Convolutional Code (NSCC) having a rate of $R = 2/3$ and 16 trellis states, 3 parallel bit interleavers and 8-PSK modulators. The system model may be found in Fig. 3. The EXIT curves[4] of both the inner MUD and of the outer decoder are presented in Fig. 22 for $E_b/N_0 = 6$ dB and 11 dB. It may be clearly observed that the EXIT curves of the QWSA MUD match those of the ML MUD, confirming that the two systems have the same performance. In Fig. 22 we have also presented the EXIT curves of a system for $K = 2$ users and $M = 8$, but replacing the $R = 2/3$-rate NSCC by a TCCC having a rate of $R = 1/2$, relying on 8 trellis states and 4 iterations between the convolutional codes. It may be readily verified that the EXIT curve of the inner QWSA MUD is identical to that of the ML MUD. The Monte-Carlo simulation based decoding trajectories of Fig. 22 further justify that the proposed QWSA MUD may be integrated into an iterative receiver. At $E_b/N_0 = 6$ dB and employing a $R = 2/3$ NSCC there is no open EXIT-tunnel leading to the $I_{E,DEC} = 1$ point, which is in contrast to the $E_b/N_0 = 11$ dB and $R = 2/3$ scenario, where we have $I_{E,DEC} \approx 1$ after $J = 2$ outer iterations between the MUD and the decoder. We may conclude that the extrinsic information at the NSCC decoder's output recorded at 6 dB and the rate $R = 2/3$ scheme will not exceed $I_{E,DEC} = 0.9$, even if an infinite number of MUD-decoder outer iterations are performed, while at 11 dB the maximum $I_{E,DEC} = 1$ is reached even with as few as $J = 2$ outer iterations. Furthermore, the system using TCCC needs $J \approx 7$ outer iterations at

[4]For a tutorial on EXIT charts please refer to [4].

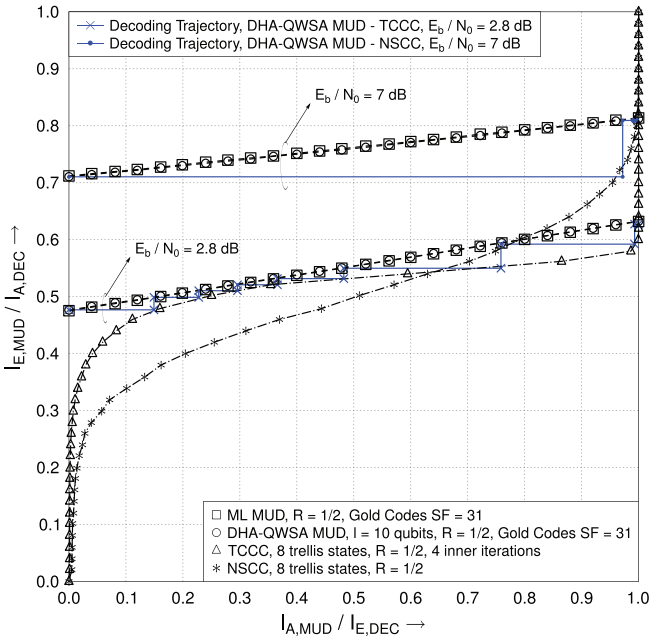

FIGURE 23. EXIT charts of two CDMA systems with $K = 2$ users, $SF = 31$ chips, BICM-ID with $R = 1/2$, Turbo Code relying on Convolutional Codes and Non-Systematic Convolutional Code, along with ML-based and DHA-QWSA-based MUD with $I = 10$ qubits in the QCR of Fig. 17.

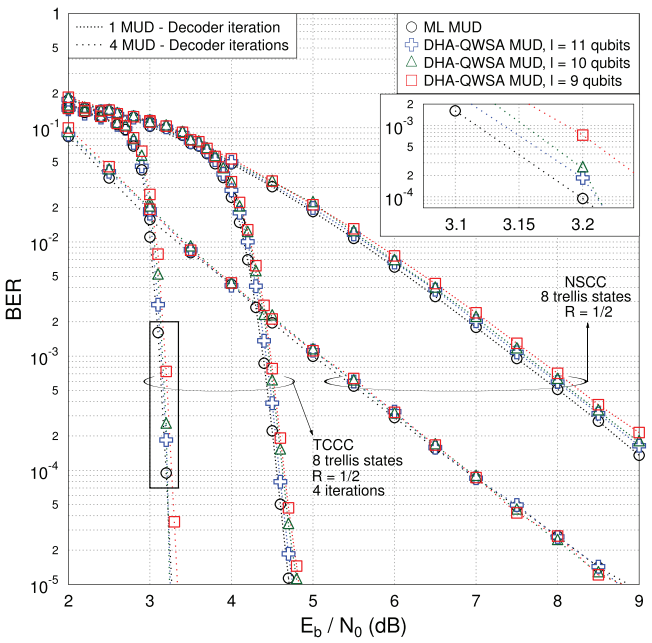

FIGURE 24. BER performance of two CDMA systems with $K = 2$ users, $SF = 31$ chips, BICM-ID with $R = 1/2$, Turbo Code relying on Convolutional Codes and Non-Systematic Convolutional Code, along with ML-based and QWSA-based MUD with $I = 9$, 10 and 11 qubits in the QCR of Fig. 17. The interleaver length is equal to 20 000 bits and 4 MUD-decoder iterations have been applied.

$E_b/N_0 = 5$ dB in order to reach $I_{E,DEC} = 1$. The size of the interleaver in the NSCC systems is 20 000 bits, while that in the TCCC system is 21 000 bits. The reason why the decoding trajectories undershoot the NSCC curve for $I_{A,MUD} < 0.5$ is because the outputs of the ML and QWSA MUDs cannot be modelled as a Gaussian distribution, whereas the outer EXIT curve was created assuming that the LLRs obey the Gaussian distribution.

Even though the complexity of the DHA-QWSA MUD in this two-user scenario is higher than that of the ML MUD, which are associated with 393 446 CF evaluations in the worst case and 64 CF evaluations per time slot, respectively, our objective was to demonstrate the match between the classic and quantum MUDs EXIT curves. The application area of our QWSA MUD is in systems designed for numerous users and larger modem constellations, since its complexity is proportional to $O(\sqrt{M^K})$ when the DHA [55] is used and $O[2^{I+3}\log(M^K)]$ when the ACO is employed, while that of the classic ML-MUD is proportional to $O(M^K)$, as seen in Fig. 20.

In a BICM-ID system using $R = 1/2$ TCCC and supporting $K = 2$ users employing Gold codes associated with $SF = 31$ chips each, the performance of the QWSA MUD again matches the ML MUD's, as it may be concluded from the EXIT chart of Fig. 23. Two encoders are compared, namely a TCCC and an NSCC. The choice of $E_b/N_0 = 2.8$ dB for the TCCC system was made with a value in mind, where the "turbo cliff" emerges, whereas in the NSCC system $I_{E,DEC}$ has exceeded 0.9 at $E_b/N_0 = 7$ dB. The similarity in the BER performance between the quantum and classic ML-MUD is seen in Fig. 24. The size of the interleaver is 20 000 for each user, the number of inner iterations in the TCCC is $I_{inner} = 4$, while the number of MUD-decoder outer iterations is also fixed to $J = 4$. The large size of the interleaver allows the BER floor of the TCCC system to be

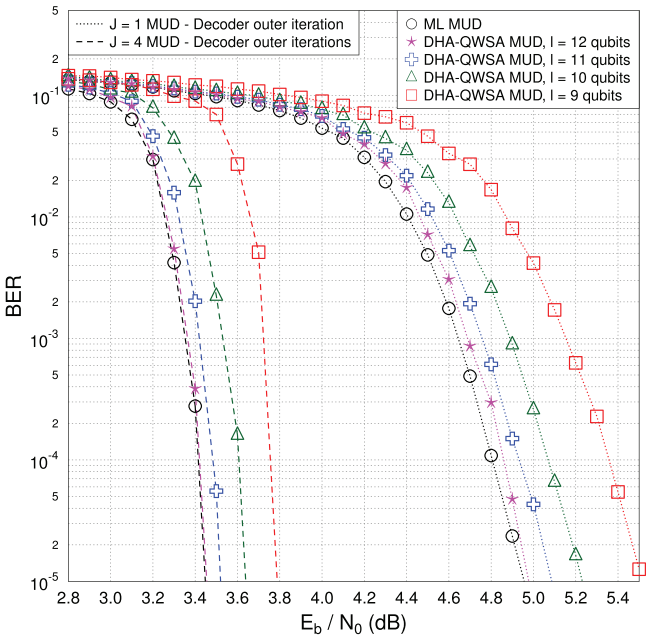

FIGURE 25. BER performance of a CDMA system with $K = 4$ users, $SF = 7$ chips, BICM-ID employing QPSK and a Turbo Code relying on Convolutional Codes with $R = 1/2$, 8 trellis states and $I_{inner} = 5$ iterations, along with ML-based and QWSA-based MUD for various number of qubits I in the QCR of Fig 17. The interleaver length is equal to 20 000 bits and the number of MUD-decoder outer iterations is $J = 1$ and $J = 4$.

lower than 10^{-5}. If more qubits are used in the QCR, the system's performance approaches that of the ML MUD more closely. Furthermore, if more MUD-decoder outer iterations are performed, the overall QMUD system's BER becomes closer to that of the ML MUD.

In order to further investigate the effect that the l QCR qubits have on the attainable performance, Fig. 25 characterizes a BICM-ID system supporting $K = 4$ users with the aid of $SF = 7$ chips, TCCC with $R = 1/2$, 8 trellis states and $I_{inner} = 4$. The DHA-QWSA MUD is used in conjunction with l ranging from 9 to 12 qubits in the QCR and the number of MUD-decoder outer iterations considered are $J = 1$ and $J = 4$. The system characterized in Fig. 25 has a higher complexity than that used in Fig. 24. As the number of qubits l increases, the precision in the QWSA becomes better and $S_{\min}$ becomes smaller. Hence, the performance is improved and it approaches that of the ML MUD, as it is clearly seen in Fig. 25. In more detail, for $J = 1$ the E_b/N_0 loss that is experienced when we have $l = 12$, $l = 11$, $l = 10$ and $l = 9$ compared to the optimal ML MUD is approximately 0.05 dB, 0.1 dB, 0.2 dB and 0.5 dB, respectively. In all cases, the DHA-QWSA MUD performance has more closely approached that of the ML MUD for $J = 4$, because the classic decoder helps mitigate both the probabilistic nature of quantum computation and the errors due to the limited precision of the QWSA. If $l > 12$ qubits were used, the performance would be expected to be even closer to that of the ML MUD. Once again, the trade-off between the performance attained and the complexity imposed becomes explicit.

X. CONCLUSIONS

We have conceived an improved QMA resulting in the QWSA, which is employed for designing a quantum-assisted MUD relying on soft inputs and providing soft outputs. The proposed QWSA-based MUD may be considered as the quantum-domain equivalent of the ML MUD. The process within the QWSA MUD takes place in the QD, while its inputs and outputs remain in the classic domain, enabling the quantum-assisted MUD to be integrated in a state-of-the-art iterative receiver of a classic communications system. The DHA is used prior to QWSA in order to detect the specific multi-level symbol that maximizes the CF and for normalizing its outputs. The EXIT charts and BER curves presented verify that the QWSA MUD has the same performance as the classic optimal ML MUD, which is achieved at a substantially reduced computational complexity, when compared to the ML MUD supporting numerous users and high-order modulation schemes.

REFERENCES

[1] L. Hanzo, M. El-Hajjar, and O. Alamri, "Near-capacity wireless transceivers and cooperative communications in the MIMO era: Evolution of standards, waveform design, and future perspectives," *Proc. IEEE*, vol. 99, no. 8, pp. 1343–1385, Aug. 2011.

[2] 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," *Proc. IEEE*, vol. 100, no. 13, pp. 1853–1888, May 2012.

[3] L. Hanzo, O. Alamri, M. El-Hajjar, and N. Wu, *Near-Capacity Multi-Functional MIMO Systems: Sphere-Packing, Iterative Detection and Cooperation*. New York, NY, USA: Wiley, May 2009.

[4] 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*. New York, NY, USA: Wiley, 2010.

[5] 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*. New York, NY, USA: Wiley, 2003.

[6] T. Zemen, C. Mecklenbrauker, J. Wehinger, and R. Muller, "Iterative joint time-variant channel estimation and multi-user detection for MC-CDMA," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1469–1478, Jun. 2006.

[7] 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 Trans. Veh. Technol.*, vol. 57, no. 1, pp. 658–663, Jan. 2008.

[8] S. Chen, L. Hanzo, and A. Livingstone, "MBER space-time decision feedback equalization assisted multiuser detection for multiple antenna aided SDMA systems," *IEEE Trans. Signal Process.*, vol. 54, no. 8, pp. 3090–3098, Aug. 2006.

[9] C. Wei, J. Akhtman, S. Ng, and L. Hanzo, "Iterative near-maximum-likelihood detection in rank-deficient downlink SDMA systems," *IEEE Trans. Veh. Technol.*, vol. 57, no. 1, pp. 653–657, Jan. 2008.

[10] C.-Y. Wei, L. Wang, and L. Hanzo, "Iterative irregular sphere detection in high-rate downlink SDMA systems," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3855–3861, Sep. 2009.

[11] L. Hanzo, Y. Akhtman, M. Jiang, and L. Wang, *MIMO-OFDM for LTE, WIFI and WIMAX: Coherent Versus Non-Coherent and Cooperative Turbo-Transceivers*. New York, NY, USA: Wiley, 2010.

[12] Y. Li, J. Winters, and N. Sollenberger, "MIMO-OFDM for wireless communications: Signal detection with enhanced channel estimation," *IEEE Trans. Commun.*, vol. 50, no. 9, pp. 1471–1477, Sep. 2002.

[13] M. Jiang and L. Hanzo, "Multiuser MIMO-OFDM for next-generation wireless systems," *Proc. IEEE*, vol. 95, no. 7, pp. 1430–1469, Jul. 2007.

[14] C. Botella, G. Pinero, A. Gonzalez, and M. De Diego, "Coordination in a multi-cell multi-antenna multi-user W-CDMA system: A beamforming approach," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4479–4485, Nov. 2008.

[15] M. Pischella and J. C. Belfiore, "Distributed resource allocation for rate-constrained users in multi-cell OFDMA networks," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 250–252, Apr. 2008.

[16] C. Liu, C. Liu, Y. Hou, and H. Zhou, "Power allocation of multi-users based on optimal power allocation algorithm in uplink base stations cooperative system," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–5.

[17] J. G. Kim and W. S. Choi, "Joint ZF and partial ML detection for uplink cellular base station cooperation," in *Proc. Int. Conf. ICT Converg.*, Sep. 2011, pp. 321–326.

[18] Y. Yuan, Z. He, and M. Chen, "Virtual MIMO-based cross-layer design for wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 3, pp. 856–864, May 2006.

[19] H. Wang, Y. Yang, M. Ma, J. He, and X. Wang, "Network lifetime maximization with cross-layer design in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3759–3768, Oct. 2008.

[20] H. Wang, N. Agoulmine, M. Ma, and Y. Jin, "Network lifetime optimization in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 7, pp. 1127–1137, Sep. 2010.

[21] G. Shirazi and L. Lampe, "Lifetime maximization in UWB sensor networks for event detection," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4411–4423, Sep. 2011.

[22] Y. Lin, J. Zhang, H.-H. Chung, W. H. Ip, Y. Li, and Y. Hui Shi, "An ant colony optimization approach for maximizing the lifetime of heterogeneous wireless sensor networks," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 3, pp. 408–420, May 2012.

[23] Z. Shen, J. Andrews, and B. Evans, "Adaptive resource allocation in multiuser OFDM systems with proportional rate constraints," *IEEE Trans. Wireless Commun.*, vol. 4, no. 6, pp. 2726–2737, Nov. 2005.

[24] J. Huang, V. Subramanian, R. Agrawal, and R. Berry, "Joint scheduling and resource allocation in uplink OFDM systems for broadband wireless access networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 2, pp. 226–234, Feb. 2009.

[25] L. Zhang, Y.-C. Liang, and Y. Xin, "Joint beamforming and power allocation for multiple access channels in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 38–51, Jan. 2008.

[26] D. Ngo, C. Tellambura, and H. Nguyen, "Resource allocation for OFDMA-based cognitive radio multicast networks with primary user activity consideration," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1668–1679, May 2010.

[27] P. Zhang, S. Chen, and L. Hanzo, "Differential space-time shift keying aided successive relaying assisted cooperative multi-user CDMA," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, p. 1, Jan. 2013.

[28] S. Sugiura, S. Chen, and L. Hanzo, "MIMO-aided near-capacity turbo transceivers: Taxonomy and performance versus complexity," *IEEE Commun. Surv. Tuts.*, vol. 14, no. 2, pp. 421–442, May 2012.

[29] J. Hoydis, S. ten Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?" *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, Feb. 2013.

[30] S. Verdu, *Multiuser Detection*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[31] S. Moshavi, "Multi-user detection for DS-CDMA communications," *IEEE Communn. Mag.*, vol. 34, no. 10, pp. 124–136, Oct. 1996.

[32] B. Shim, J. W. Choi, and I. Kang, "Towards the performance of ML and the complexity of MMSE: A hybrid approach for multiuser detection," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2508–2519, Jul. 2012.

[33] K. Li and X. Wang, "EXIT chart analysis of turbo multiuser detection," *IEEE Trans. Wireless Commun.*, vol. 4, no. 1, pp. 300–311, Jan. 2005.

[34] X. Wang and H. Poor, "Space-time multiuser detection in multipath CDMA channels," *IEEE Trans. Signal Process.*, vol. 47, no. 9, pp. 2356–2374, Sep. 1999.

[35] S. Chen, A. Samingan, B. Mulgrew, and L. Hanzo, "Adaptive minimum-BER linear multiuser detection for DS-CDMA signals in multipath channels," *IEEE Trans. Signal Process.*, vol. 49, no. 6, pp. 1240–1247, Jun. 2001.

[36] S. Chen, A. Livingstone, and L. Hanzo, "Minimum bit-error rate design for space-time equalization-based multiuser detection," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 824–832, May 2006.

[37] S. Tan, S. Chen, and L. Hanzo, "On multi-user EXIT chart analysis aided turbo-detected MBER beamformer designs," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 314–323, Jan. 2008.

[38] M. Jiang, J. Akhtman, and L. Hanzo, "Iterative joint channel estimation and multi-user detection for multiple-antenna aided OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2904–2914, Aug. 2007.

[39] C. Ergun and K. Hacioglu, "Multiuser detection using a genetic algorithm in CDMA communications systems," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1374–1383, Aug. 2000.

[40] M. Alias, S. Chen, and L. Hanzo, "Multiple-antenna-aided OFDM employing genetic-algorithm-assisted minimum bit error rate multiuser detection," *IEEE Trans. Veh. Technol.*, vol. 54, no. 5, pp. 1713–1721, Sep. 2005.

[41] K. Yen and L. Hanzo, "Antenna-diversity-assisted genetic-algorithm-based multiuser detection schemes for synchronous CDMA systems," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 366–370, Mar. 2003.

[42] C. Xu, R. Maunder, L.-L. Yang, and L. Hanzo, "Near-optimum multiuser detectors using soft-output ant-colony-optimization for the DS-CDMA uplink," *IEEE Signal Process. Lett.*, vol. 16, no. 2, pp. 137–140, Feb. 2009.

[43] K. Soo, Y. Siu, W. Chan, L. Yang, and R. Chen, "Particle-swarm-optimization-based multiuser detector for CDMA communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 9, pp. 3006–3013, Sep. 2007.

[44] H. Liu and J. Li, "A particle swarm optimization-based multiuser detection for receive-diversity-aided STBC systems," *IEEE Signal Process. Lett.*, vol. 15, no. 1, pp. 29–32, Jan. 2008.

[45] K. Vishnu Vardhan, S. Mohammed, A. Chockalingam, and B. Sundar Rajan, "A low-complexity detector for large MIMO systems and multicarrier CDMA systems," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 3, pp. 473–485, Apr. 2008.

[46] H. S. Lim and B. Venkatesh, "An efficient local search heuristics for asynchronous multiuser detection," *IEEE Commun. Lett.*, vol. 7, no. 7, pp. 299–301, Jul. 2003.

[47] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[48] S. Imre and F. Balázs, *Quantum Computing and Communications: An Engineering Approach*. New York, NY, USA: Wiley, 2005.

[49] D. C. Marinescu, *Classical and Quantum Information*, 1st ed. San Francisco, CA, USA: Academic, 2011.

[50] S. Imre and L. Gyongyosi, *Advanced Quantum Communications: An Engineering Approach*. New York, NY, USA: Wiley, 2013.

[51] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, *Quantum Amplitude Amplification and Estimation*. Cambridge, U.K.: Cambridge Univ. Press, May 2000.

[52] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, May 1996, pp. 212–219.

[53] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325–328, Jul. 1997.

[54] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte Der Phys.*, vol. 46, nos. 4–5, pp. 493–506, 1998.

[55] C. Durr and P. Hoeyer, *A Quantum Algorithm for Finding the Minimum*. Cambridge, U.K.: Cambridge Univ. Press, Jul. 1996.

[56] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. 2493–2496, Oct. 1995.

[57] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[58] R. Hughes and J. Nordholt, "Refining quantum cryptography," *Science*, vol. 333, no. 6049, pp. 1584–1586, Sep. 2011.

[59] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, Oct. 2012.

[60] S. Imre and F. Balazs, "Non-coherent multi-user detection based on quantum search," in *Proc. IEEE Int. Conf. Commun.*, vol. 1. May 2002, pp. 283–287.

[61] S. Imre and F. Balazs, "Performance evaluation of quantum based multiuser detector," in *Proc. IEEE 7th Int. Symp. Spread Spectr. Tech. Appl.*, vol. 3. Sep. 2002, pp. 722–725.

[62] G. Brassard, P. Høyer, and A. Tapp, *Quantum Counting*. Cambridge, U.K.: Cambridge Univ. Press, May 1998.

[63] L. de Oliveira, F. Ciriaco, T. Abrao, and P. Jeszensky, "Particle swarm and quantum particle swarm optimization applied to DS/CDMA multiuser detection in flat rayleigh channels," in *Proc. IEEE 9th Int. Symp. Spread Spectr. Tech. Appl.*, Aug. 2006, pp. 133–137.

[64] H. Gao and M. Diao, "Quantum particle swarm optimization for MC-CDMA multiuser detection," in *Proc. Int. Conf. Artif. Intell. Comput. Intell.*, vol. 2. Nov. 2009, pp. 132–136.

[65] H. Liu and G. Song, "A multiuser detection based on quantum PSO with pareto optimality for STBC-MC-CDMA system," in *Proc. IEEE Int. Conf. Commun. Technol. Appl.*, Oct 2009, pp. 652–655.

[66] F. Li, M. Zhou, and H. Li, "A novel neural network optimized by quantum genetic algorithm for signal detection in MIMO-OFDM systems," in *Proc. IEEE Symp. Comput. Intell. Control Autom.*, Apr. 2011, pp. 170–177.

[67] A. Narayanan and M. Moore, "Quantum-inspired genetic algorithms," in *Proc. IEEE Int. Conf. Evol. Comput.*, May 1996, pp. 61–66.

[68] S. Yang, M. Wang, and L. Jiao, "A novel quantum evolutionary algorithm and its application," in *Proc. Congr. Evol. Comput.*, vol. 1. Jun. 2004, pp. 820–826.

[69] F. Li, L. Hong, and B. Zheng, "Quantum genetic algorithm and its application to multi-user detection," in *Proc. 9th Int. Conf. Signal Process.*, Oct. 2008, pp. 1951–1954.

[70] S. Ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[71] 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*. Cambridge, U.K.: Cambridge Univ. Press, Jun. 2011.

[72] R. Feynman, "Simulating physics with computers," *Int. J. Theoretical Phys.*, vol. 21, nos. 6–7, pp. 467–488, Jun. 1982.

[73] P. Benioff, "Quantum mechanical hamiltonian models of turing machines," *J. Stat. Phys.*, vol. 29, no. 3, pp. 515–546, Nov. 1982.

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

[75] H. Everett, "Relative state formulation of quantum mechanics," *Rev. Modern Phys.*, vol. 29, pp. 454–462, Jul. 1957.

[76] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. Royal Soc. London Ser. A, Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, Jul. 1985.

[77] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc., Math. Phys. Sci.*, vol. 439, no. 1907, pp. 553–558, Dec. 1992.

[78] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.

[79] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proc. Royal Soc. London Ser. A*, vol. 454, no. 1, pp. 339–357, Jan. 1998.

[80] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Rev. Modern Phys.*, vol. 38, no. 3, pp. 447–452, Jul. 1966.

[81] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935.

[82] D. R. Simon, "On the power of quantum computation," *SIAM J. Comput.*, vol. 26, pp. 116–123, Apr. 1994.

[83] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM J. Sci. Stat. Comput.*, vol. 54, no. 5, pp. 3824–3851, 1996.

[84] C. Zalka, "Grover's quantum searching algorithm is optimal," *Phys. Rev. A*, vol. 60, pp. 2746–2751, Oct. 1999.

[85] D. Ventura and T. Martinez, *Quantum Associative Memory*. Cambridge, U.K.: Cambridge Univ. Press, Jul. 1998.

[86] G. L. Long, Y. S. Li, W. L. Zhang, and L. Niu, "Phase matching in quantum searching," *Phys. Lett. A*, vol. 262, pp. 27–34, Oct. 1999.

[87] A. Ahuja and S. Kapoor, *A Quantum Algorithm for finding the Maximum*. Cambridge, U.K.: Cambridge Univ. Press, Nov. 1999.

[88] T. Hogg, "Quantum search heuristics," *Phys. Rev. A*, vol. 61, no. 5, pp. 052311-1–052311-7, Apr. 2000.

[89] N. Shenvi, J. Kempe, and K. B. Whaley, "Quantum random-walk search algorithm," *Phys. Rev. A*, vol. 67, no. 5, pp. 052307-1–052307-11, May 2003.

[90] S. Imre and F. Balázs, "The generalized quantum database search algorithm," *Computing*, vol. 73, no. 3, pp. 245–269, Oct. 2004.

[91] S. M. Zhao, J. Yao, and B. Y. Zheng, "Multiuser detection based on Grover's algorithm," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2006, pp. 4735–4738.

[92] S. Imre, "Quantum existence testing and its application for finding extreme values in unsorted databases," *IEEE Trans. Comput.*, vol. 56, no. 5, pp. 706–710, May 2007.

[93] A. Malossini, E. Blanzieri, and T. Calarco, "Quantum genetic optimization," *IEEE Trans. Evol. Comput.*, vol. 12, no. 4, pp. 231–241, Apr. 2008.

[94] F. Li, L. Zhou, L. Liu, and H. Li, "A quantum search based signal detection for MIMO-OFDM systems," in *Proc. 18th Int. Conf. Telecommun.*, May 2011, pp. 276–281.

[95] A. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan. 1998.

[96] J. Concha and H. Poor, "Multiaccess quantum channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 725–747, May 2004.

[97] M.-H. Hsieh and M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4682–4704, Sep. 2010.

[98] X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K.-I. Kitayama, "Asynchronous multiuser coherent OCDMA system with code-shift-keying and balanced detection," *IEEE J. Sel. Topics Quantum Electron.*, vol. 13, no. 5, pp. 1463–1470, Sep.–Oct. 2007.

[99] L. Gyongyosi and S. Imre, "Information geometrical analysis of additivity of optical quantum channels," *IEEE/OSA J. Optical Commun. Netw.*, vol. 3, no. 1, pp. 48–55, Jan. 2011.

[100] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4 ed. New York, NY, USA: Oxford Univ. Press, Feb. 1982.

[101] G. Brassard, "Searching a quantum phone book," *Science*, vol. 275, no. 5300, pp. 627–628, Jan. 1997.

[102] A. Einstein, M. Born, and H. Born, *The Born-Einstein Letters*, 1st ed. New York, NY, USA: Macmillan, 1971, pp. 1916–1955.

PANAGIOTIS BOTSINIS (S'12) received the M.Eng. degree from the School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece, in 2010, and the M.Sc. degree in wireless communications with distinction from the University of Southampton, Southampton, U.K., in 2011. He is currently pursuing the Ph.D. degree in the Communications, Signal Processing and Control Group, School of Electronics and Computer Science of the University of Southampton. He has been a member of the Technical Chamber of Greece since October 2010. His current research interests include quantum-assisted communications, iterative detection, MIMO, coded modulation, channel coding, cooperative communications, and as well as combinatorial optimization.

SOON XIN NG (S'99–M'03–SM'08) received the B.Eng. degree (First class) in electronics engineering and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow working on collaborative European research projects known as SCOUT, NEWCOM, and PHOENIX. Since August 2006, he has been an Academic Staff Member with the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently a Senior Lecturer with the University of Southampton.

His current research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes and joint wireless-and-optical-fiber communications. He has published over 150 papers and co-authored two John Wiley/IEEE Press books. He is a Chartered Engineer and a fellow of the Higher Education Academy in the U.K.

LAJOS HANZO (M'91–SM'92–F'08) received the F.R.Eng., FIEEE, FIET, fellow of EURASIP, and D.Sc. degrees in electronics in 1976, and the Doctorate in 1983. In 2009, he was awarded the Honorary Doctorate "Doctor Honoris Causa" by the Technical University of Budapest. During his 35-year career in telecommunications he has held various research and academic posts in Hungary, Germany, and U.K. Since 1986, he has been with the School of Electronics and Computer Science, University of Southampton, Southampton, U.K., where he holds the chair in telecommunications. He has successfully supervised 80 Ph.D. students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totaling in excess of 10 000 pages, published 1300+ research entries, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently, he is directing a 100-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council, U.K., the European IST Programme and the Mobile Virtual Centre of Excellence, U.K. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses. He is also a Governor of the IEEE VTS. From 2008 to 2012, he was the Editor-in-Chief of the *IEEE Press and a Chaired Professor* also at Tsinghua University, Beijing, China. His research is funded by the European Research Council's Senior Research Fellow Grant. He has over 16000 citations.