IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 24, 2022, accepted March 18, 2022, date of publication April 5, 2022, date of current version April 8, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3164071

Applications of a Quantum Linear System Algorithm to Linear MIMO Detections

JEONGHOON PARK[1], YOUNGJIN SEO[2], AND JUN HEO[2], (Member, IEEE)
[1]Research Institute for Information and Communication Technology, Korea University, Seoul 02841, South Korea
[2]School of Electrical Engineering, Korea University, Seoul 02841, South Korea

Corresponding author: Jun Heo (junheo@korea.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2019R1A2C2010061, and in part by the Samsung Research in Samsung Electronics.

ABSTRACT A linear system can be solved more efficiently by quantum computing. However, previously known quantum algorithms provide only a quantum state as the solution; consequently, we cannot obtain the value of each component of the solution. We propose a method to extract the component values of the solution, and we present an application to linear multiple-input multiple-output (MIMO) detections. In the proposed algorithm, we demonstrate a concrete method that applies a quantum linear system algorithm (QLSA) when the components of a solution have binary variables, quaternary variables, or roots of a complex number. Whereas the conventional method requires an additional process to read out the values of the components, the proposed algorithm does not need any post-procedure. Instead, our method uses a QLSA iteratively, and the number of uses is logarithmic in the size of the linear system. Thus, our method maintains the runtime with the quantum advantage, but the conventional approach increases the runtime significantly. Furthermore, the application of the proposed method shows that quantum computing can collaborate with communication systems for large-scale MIMO systems.

INDEX TERMS Linear MIMO detection, quantum computing, quantum linear system algorithm.

I. INTRODUCTION

Quantum computation has developed into a rising field of research for the last twenty years. Along with physical realizations of quantum computing, quantum algorithms, which run on realistic quantum devices, have been studied deeply. Many quantum algorithms have been proposed that achieve computational speed-ups compared to classical algorithms [1]. For example, Grover's algorithm provides a quadratic speed-up for unstructured search [2], and Shor's algorithm can solve the factoring problem exponentially faster than the best classical algorithm [3]. Such quantum speed-ups indicate that we can utilize quantum computing to solve existing problems efficiently.

Systems of linear equations are used in various fields. Even though a linear system can be solved in polynomial time, we need more efficient algorithms to find a solution for practical use. A quantum linear system algorithm (QLSA) was first proposed by Harrow, Hassidim and Lloyd [4]. The Harrow–Hassidim–Lloyd (HHL) algorithm can compute the solution of a linear system in time $O(\log(N)\kappa^2/\epsilon)$ for $N \times N$ sparse matrices with condition number κ, where ϵ is the desired error parameter. The HHL algorithm has an exponential speed-up over the fastest known classical algorithm, which can obtain the solution in time $O(N\kappa \log(1/\epsilon))$ for sparse matrices [5]. The dependence on κ and ϵ was subsequently improved [6], [7]. Recently, several QLSAs for dense matrices have been proposed [8]–[11]. In particular, the block-encoding framework is applied in [9], and the quantum column iteration method is used in [11].

Although a QLSA can solve a linear system much faster than classical algorithms, it has an intrinsic problem. We obtain the solution $|\mathbf{x}\rangle$ as a quantum state after applying the algorithm. This means that we cannot obtain any knowledge of the solution, unless the state is measured. It does not matter when we want to have the solution as a quantum state. For example, we can consider a QLSA as a subroutine of a larger algorithm so that we use the state as an input of the next procedure. However, when we need classical information in the solution state, in particular, the component values x_j of the solution $\mathbf{x}$, we may need to measure the solution state from which we extract some information.

The associate editor coordinating the review of this manuscript and approving it for publication was Li Zhang.

It is possible to apply the quantum amplitude estimation (QAE) algorithm [12] as a post-procedure when the information we want to obtain is the amplitudes in $|\mathbf{x}\rangle$. More generally, A method was proposed to obtain the overlap between $|\mathbf{x}\rangle$ and $|\phi\rangle$ for an arbitrary state $|\phi\rangle$ [13]. This method also uses the QAE algorithm after solving the linear system. Unfortunately, the extra process increases the runtime complexity significantly, and the QAE algorithm of the above methods consists of mainly controlled-U gates, where U is the unitary gate implementing the whole QLSA. This makes the construction of the algorithm extremely complicated in a practical sense. We remark that several algorithms based on the QAE have been introduced that can be used to approximate the norm $\|\mathbf{x}\|$ [14], the absolute value $|x_j|$ of a component x_j [15], and the real-valued x_j [16].

Many quantum-assisted solutions have been presented to solve optimization problems in wireless communications [17], [18]. Especially, the authors in [18] have proposed two quantum-assisted methods for MIMO-OFDM systems with maximum likelihood detection. Most of those works have shown the potential performance gain and attainable complexity reduction using quantum search algorithms based on Grover's algorithm [2]. Moreover, the proposed algorithm in [16] can be used as a linear MIMO detector, but it can estimate only real components x_j, and its QAE process substantially increases the computational complexity.

A. CONTRIBUTIONS

In this paper, we take into account a multiple-input multiple-output (MIMO) system with M-ary phase-shift keying (MPSK) signals in communication systems, and we present an application of a QLSA to the MIMO detection problem. More generally, we propose a QLSA capable of extracting the values x_j from the solution state when the solution has binary variables, quaternary variables, or roots of a complex number. The proposed algorithm does not need any additional procedure to extract classical information except the final measurement step. Instead, we modify the original equations, and then apply a QLSA. In particular, the modified equations do not increase the runtime complexity. Then, while exploiting the quantum advantage of a QLSA, we can obtain the values x_j of the solution.

Moreover, the proposed method can be used to read out a given quantum state under the same condition. This implies that for any MIMO detector that can be executed by a quantum algorithm, the proposed technique can be applied to extract the values of the obtained quantum state. Indeed, the application to MIMO systems shows that we can efficiently solve the detection problem in large-scale MIMO systems using quantum computing techniques.

B. PAPER STRUCTURE

The remainder of this paper is organized as follows. In Section II, we briefly introduce a QLSA and the QAE algorithm, as well as quantum computing. In Section III, we present our proposed QLSA to extract classical information. In Section IV, we show how to reduce the condition number and the runtime complexity. In addition, we compare the proposed algorithm with the method using the QAE algorithm. Then, we give an application to the MIMO detection problem and the performance results of our method in Section V. Finally, we conclude our results in Section VI.

C. NOTATIONS

The notations used in this paper are as follows:

$\mathbf{A}$	A matrix
$\mathbf{A}^*$	The complex conjugate of a matrix $\mathbf{A}$.
$\mathbf{A}^T$	The transpose of a matrix $\mathbf{A}$.
$\mathbf{A}^\dagger$	The Hermitian conjugate of a matrix $\mathbf{A}$.
$\mathbf{I}_N$	The $N \times N$ identity matrix.
$\mathbf{a}$	A (column) vector.
a_j	The jth component of a vector $\mathbf{a}$.
$\|\psi\rangle$	A quantum state, equivalently, a unit (column) vector.
$\langle\psi\|$	The Hermitian conjugate of $\|\psi\rangle$.
$\|i\rangle$	The unit (column) vector having 1 only in the $(i+1)$th entry.
$\|\mathbf{a}\rangle$	The normalized vector of a vector $\mathbf{a}$.
$\|\mathbf{a}\|$	The Euclidean norm of a vector $\mathbf{a}$.
$O(\cdot)$	Big O notation.
$\Omega(\cdot)$	Big Omega notation.
$\lceil a \rceil$	The ceiling function of a real value a.

II. PRELIMINARIES

A. QUANTUM COMPUTING

A quantum state $|\phi\rangle$ is represented by a unit vector in a Hilbert space. Let

$$|\phi\rangle = \sum_i a_i |i\rangle, \tag{1}$$

where $a_i \in \mathbb{C}$ with $\sum_i |a_i|^2 = 1$, and $|i\rangle$ are orthonormal states. Then the state $|\phi\rangle$ is in a superposition of states $|i\rangle$. We note that $|\cdot\rangle$ is the bra-ket notation to denote quantum states in quantum physics. The dynamics of a quantum state is governed by a unitary operator. This means that the inner products of quantum states are preserved, and quantum computation is a reversible process. Unlike classical objects, a quantum state can be observed only through a measurement process, and the measured state can differ from the previous state. For example, let

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

Measuring $|\psi\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$, we obtain $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. We can say that the superposition in (2) collapses due to the measurement.

In particular, a two-level quantum state is called a qubit. A qubit is the quantum analog of a classical bit and a basic unit in quantum computing. A quantum circuit consists of quantum gates. There are quantum gates similar to classical gates, including the Pauli gates X, Y, and Z; the Hadamard gate H; the controlled-NOT gate CNOT; the swap gate

SWAP; and the Toffoli gate T. A measurement procedure is crucial to quantum computing because we can obtain classical information only by measuring the state in the final step. Conversely, we must prepare a quantum state as the initial state of a quantum algorithm. In other words, we need a translation step from a quantum state to a classical state, and vice versa.

B. QLSA

Since the HHL algorithm was introduced in [4], there have been proposed several variants that employ slightly different techniques. We here review the HHL algorithm.

The HHL algorithm is utilized to solve a system of linear equations

$$\mathbf{A}\mathbf{x} = \mathbf{y}, \tag{3}$$

where $\mathbf{A}$ is an $N \times N$ Hermitian matrix, and $\mathbf{y}$ is an N-dimensional unit vector. The solution is given as a quantum state proportional to $\mathbf{A}^{-1}\mathbf{y}$.

Let

$$\mathbf{A} = \sum_{j=1}^{N} \lambda_j |u_j\rangle\langle u_j| \tag{4}$$

in the spectral decomposition form, where λ_j and $|u_j\rangle$ are the eigenvalues and eigenstates of $\mathbf{A}$, respectively. Then $|\mathbf{y}\rangle$ can be written in the form

$$|\mathbf{y}\rangle = \sum_{j=1}^{N} \alpha_j |u_j\rangle, \tag{5}$$

where $\sum_{j=1}^{N} |\alpha_j|^2 = 1$. The initial state of the HHL algorithm is

$$|0\rangle|\mathbf{y}\rangle = \sum_{j=1}^{N} \alpha_j |0\rangle|u_j\rangle, \tag{6}$$

where $|0\rangle$ is in an n-qubit register, and $|\mathbf{y}\rangle$ is a quantum state representing $\mathbf{y}$. We first apply the quantum phase estimation (QPE) for a unitary operator $e^{2\pi i\mathbf{A}}$ without measurement. Then the state in (6) becomes

$$\sum_{j=1}^{N} \sum_{x=0}^{2^n-1} \alpha_j \beta_{x|j} |\lambda_x\rangle|u_j\rangle, \tag{7}$$

where $\beta_{x|j} = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{2\pi i k(\lambda_j - x/2^n)}$ and $\lambda_x = x/2^n$. Next, we add an ancillary qubit $|0\rangle$ to which we apply the controlled σ_y-rotation conditioned on the state $|\lambda_x\rangle$. We then obtain

$$\sum_{j=1}^{N} \sum_{x=0}^{2^n-1} \alpha_j \beta_{x|j} \left(\sqrt{1 - \frac{c^2}{\lambda_x^2}} |0\rangle + \frac{c}{\lambda_x} |1\rangle \right) |\lambda_x\rangle|u_j\rangle. \tag{8}$$

Here, c is chosen to be $O(1/\kappa)$, where κ is the condition number of $\mathbf{A}$. Finally, we perform the inverse QPE to uncompute the state $|\lambda_x\rangle$, and then measure the ancillary qubit.

When the QPE is done perfectly, $\beta_{x|j} = \delta_{x,2^n\lambda_j}$, and so the state in (8) becomes

$$\sum_{j=1}^{N} \alpha_j \left(\sqrt{1 - \frac{c^2}{\lambda_j^2}} |0\rangle + \frac{c}{\lambda_j} |1\rangle \right) |0\rangle|u_j\rangle. \tag{9}$$

If the measurement outcome of the ancillary qubit is 1, we obtain the state

$$|\mathbf{x}\rangle = \frac{1}{\sqrt{\sum_{k=1}^{N} |\alpha_k|^2/\lambda_k^2}} \sum_{j=1}^{N} \frac{\alpha_j}{\lambda_j} |u_j\rangle = \frac{\mathbf{A}^{-1}|\mathbf{y}\rangle}{\left\|\mathbf{A}^{-1}|\mathbf{y}\rangle\right\|}, \tag{10}$$

which represents the solution of the linear system $\mathbf{A}\mathbf{x} = \mathbf{y}$. The running time complexity of finding the solution $|\mathbf{x}\rangle$ is $O(\log(N)\kappa^2/\epsilon)$ for a sparse matrix $\mathbf{A}$, where κ is the condition number of $\mathbf{A}$, and ϵ is the desired error. A detailed explanation is presented in [4].

We note that the assumptions for $\mathbf{A}$ and $\mathbf{y}$ can be relaxed. When $\mathbf{y}$ is not a unit vector, we rescale the linear system $\mathbf{A}\mathbf{x} = \mathbf{y}$ so that $\mathbf{y}$ becomes a unit vector. Indeed, let

$$\mathbf{A}' = \frac{\mathbf{A}}{\|\mathbf{y}\|} \text{ and } \mathbf{y}' = \frac{\mathbf{y}}{\|\mathbf{y}\|}. \tag{11}$$

We then solve $\mathbf{A}'\mathbf{x} = \mathbf{y}'$, giving the same solution. When $\mathbf{A}$ is non-Hermitian, let

$$\mathbf{A}' = \begin{pmatrix} \mathbf{O} & \mathbf{A} \\ \mathbf{A}^\dagger & \mathbf{O} \end{pmatrix} \text{ and } \mathbf{y}' = \begin{pmatrix} \mathbf{y} \\ \mathbf{0} \end{pmatrix}. \tag{12}$$

Then the solution of $\mathbf{A}'\mathbf{x}' = \mathbf{y}'$ is

$$\mathbf{x}' = \begin{pmatrix} \mathbf{0} \\ \mathbf{x} \end{pmatrix}, \tag{13}$$

and the HHL algorithm outputs the state

$$|\mathbf{x}'\rangle = |1\rangle|\mathbf{x}\rangle. \tag{14}$$

Thus, we can deal with any $\mathbf{A}$ and $\mathbf{y}$. In the rest of this paper, we implicitly assume that a linear system $\mathbf{A}\mathbf{x} = \mathbf{y}$ is modified in the above manner if necessary.

C. QAE ALGORITHM

Although a QLSA is exponentially faster than the best classical algorithm, we cannot know each value of the solution x since the obtained solution $|\mathbf{x}\rangle$ is a quantum state. We may need an additional procedure, for example, measuring the state $|\mathbf{x}\rangle$ in a specific basis. In the method proposed by [13], the QAE is used to extract each value of the solution. We here introduce the QAE algorithm briefly.

Given a unitary transformation $\mathcal{U}$ on a Hilbert space $\mathcal{H}$ and a subspace $\mathcal{H}_1$ of $\mathcal{H}$, let $|0\rangle$ be the initial zero state. Then $\mathcal{U}|0\rangle$ can be decomposed as

$$\mathcal{U}|0\rangle = a|\psi\rangle + b|\phi\rangle, \tag{15}$$

where $|\psi\rangle \in \mathcal{H}_1$, $|\phi\rangle \in \mathcal{H}_1^\perp$, and $|a|^2 + |b|^2 = 1$. The QAE algorithm estimates the value $\alpha \equiv |a|^2$.

The initial state is prepared in

$$|0\rangle \otimes \mathcal{U}|0\rangle, \tag{16}$$

where the first register is in an M-dimensional quantum state $|0\rangle$. We first apply the quantum Fourier transform F_M on an M-dimensional quantum system to the first register, and then perform the controlled-unitary operation $\Lambda_M(Q)$ defined by

$$\Lambda_M(Q) : |i\rangle|x\rangle \to |i\rangle Q^i|x\rangle \qquad (0 \le i < M), \tag{17}$$

where

$$Q = -\mathcal{U}S_0\mathcal{U}^{-1}S_{\mathcal{H}_1}, \tag{18}$$

the operator S_0 flips the phase of the state $|0\rangle$, and the operator $S_{\mathcal{H}_1}$ flips the phase of states in $\mathcal{H}_1$. We next apply F_M^{-1} to the first register. Finally, measuring the first register, we obtain the outcome $|w\rangle$, from which we can find the estimated value $\tilde{\alpha} = \sin^2(\pi w/M)$.

For any $k \in \mathbb{N}$, we obtain the estimated value $\tilde{\alpha}$ such that

$$|\tilde{\alpha} - \alpha| \le 2\sqrt{\alpha(1-\alpha)}\frac{k\pi}{M} + \left(\frac{k\pi}{M}\right)^2 \tag{19}$$

with probability at least $\frac{8}{\pi^2}$ for $k = 1$ and with probability greater than $1 - \frac{1}{2(k-1)}$ for $k \ge 2$. In particular, when $\alpha = 0$, $\tilde{\alpha} = 0$ with certainty, and when $\alpha = 1$ and M is even, $\tilde{\alpha} = 1$ with certainty. We can observe that the value k determines the probability of obtaining the estimated value, and the value M determines the error bound of the estimated value for a fixed k. For the right-hand side of (19), let ϵ be a multiplicative error such that

$$2\sqrt{\alpha(1-\alpha)}\frac{k\pi}{M} + \left(\frac{k\pi}{M}\right)^2 \le \epsilon\alpha. \tag{20}$$

Then we can find a lower bound of M:

$$M \ge \frac{k\pi}{\epsilon\sqrt{\alpha}}\left(\sqrt{1-\alpha} + \sqrt{1-\alpha+\epsilon}\right) \tag{21}$$

for $\alpha > 0$ [19]. Since the QAE uses the given unitary $\mathcal{U}$ repetitively to obtain the amplitude α, from (17), (18), and (21), the number R of applications of $\mathcal{U}$ is

$$R = 2M - 2 \tag{22}$$
$$\ge \frac{2k\pi}{\epsilon\sqrt{\alpha}}\left(\sqrt{1-\alpha} + \sqrt{1-\alpha+\epsilon}\right) - 2 \tag{23}$$
$$\ge \frac{2k\pi}{\sqrt{\epsilon}} - 2. \tag{24}$$

Thus, we can conclude that the computational complexity of the QAE algorithm is $\Omega\left(k/\sqrt{\epsilon}\right)$ times the complexity of the unitary $\mathcal{U}$.

III. PROPOSED METHOD TO EXTRACT CLASSICAL INFORMATION

Let us consider a system of linear equations

$$\mathbf{A}\mathbf{x} = \mathbf{y}, \tag{25}$$

where $\mathbf{A} \in \mathbb{C}^{N\times N}$, $\mathbf{x} = (x_1, \ldots, x_N)^T$, and $\mathbf{y} = (y_1, \ldots, y_N)^T$. We assume that the unknowns x_j are binary variables, quaternary variables, or roots of a complex number. Such a situation can occur in various fields, including computer science, statistics, binary integer programming, and MIMO channel detection in communication systems [20].

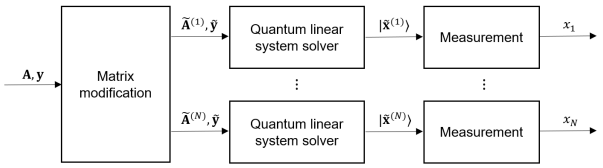

FIGURE 1. Block diagram of the proposed algorithm for binary variables.

The proposed algorithm consists of three steps: matrix modification, quantum linear system solver (QLSS), and measurement as shown in Figs. 1 and 2. We modify a given linear system for x_j, in order that the solution obtained by a QLSS contains classical information associated with x_j. Then, by measuring the solution state, we can obtain the value of x_j. Especially, we execute the process in parallel to obtain the values of all x_j simultaneously. We state our result as follows:

Theorem 1: Let $\mathbf{A}\mathbf{x} = \mathbf{y}$ *be a system of linear equations. Suppose that the unknowns* x_j *are (i) binary variables, (ii) quaternary variables of the form* $s + it$*, where* s *and* t *are binary variables in* $\mathbb{R}$*, or (iii)* M*th roots of a complex number. Then the proposed quantum algorithm determines the values of* x_j *almost certainly by applying a QLSS* $O(\log N)$ *times in parallel.*

A. CASE OF BINARY VARIABLES

We now present the proposed method for the case of binary variables in detail. Assume that the unknowns x_j have two distinct values a and b in $\mathbb{C}$, where $|a| \le |b|$. In the first step, we modify a given linear system by adding the following equations:

$$\begin{aligned} x_j + \alpha^{-1}(b-a)x_{N+1} &= b, \\ x_j + \alpha^{-1}(a-b)x_{N+2} &= a, \end{aligned} \tag{26}$$

where x_{N+1} and x_{N+2} are new variables, and $\alpha \in \mathbb{C}$ is chosen later. Then we obtain the modified linear system

$$\tilde{\mathbf{A}}^{(j)}\tilde{\mathbf{x}}^{(j)} = \tilde{\mathbf{y}}, \tag{27}$$

where

$$\tilde{\mathbf{x}}^{(j)} = (x_1, \ldots, x_N, x_{N+1}, x_{N+2})^T, \tag{28}$$
$$\tilde{\mathbf{y}} = (y_1, \ldots, y_N, \alpha b, \alpha a)^T. \tag{29}$$

From (26), the solution $\tilde{\mathbf{x}}^{(j)}$ is

$$\tilde{\mathbf{x}}^{(j)} = \left(x_1, \ldots, x_N, \alpha\frac{b-x_j}{b-a}, \alpha\frac{x_j-a}{b-a}\right)^T, \tag{30}$$

where the first N components are the solution of the original linear system $\mathbf{A}\mathbf{x} = \mathbf{y}$.

In the second step, we apply a QLSS to the modified linear system in (27). Then we obtain the solution in (30) as a quantum state:

$$|\tilde{\mathbf{x}}^{(j)}\rangle = \frac{\|\mathbf{x}\|}{\sqrt{\|\mathbf{x}\|^2 + |\alpha|^2}}|\mathbf{x}\rangle + \frac{\alpha}{\sqrt{\|\mathbf{x}\|^2 + |\alpha|^2}}|x_j\rangle, \tag{31}$$

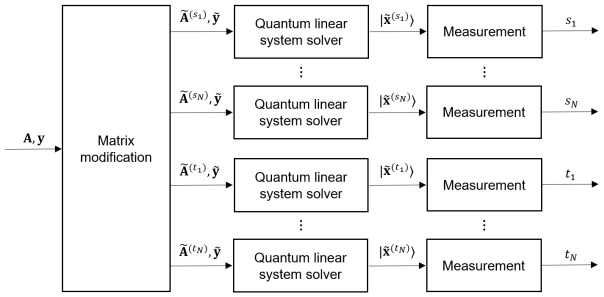

FIGURE 2. Block diagram of the proposed algorithm for quaternary variables.

where

$$|\mathbf{x}\rangle = \frac{1}{\|\mathbf{x}\|}\sum_{i=0}^{N-1} x_{i+1}|i\rangle, \tag{32}$$

$$|x_j\rangle = \frac{b-x_j}{b-a}|N\rangle + \frac{x_j-a}{b-a}|N+1\rangle. \tag{33}$$

In the third step, we measure the state $|\tilde{\mathbf{x}}^{(j)}\rangle$ in the computational basis. Note that $|x_j\rangle = |N\rangle$ if $x_j = a$, and that $|x_j\rangle = |N+1\rangle$ if $x_j = b$. Thus, we can decide the value of x_j when we obtain $|x_j\rangle$ after the measurement.

The probability of obtaining $|x_j\rangle$ is

$$\frac{|\alpha|^2}{\|\mathbf{x}\|^2 + |\alpha|^2}. \tag{34}$$

Because we apply a QLSS in parallel to extract the values of x_j, the probability P of obtaining $|x_1\rangle\otimes\cdots\otimes|x_N\rangle$ from $|\tilde{\mathbf{x}}^{(1)}\rangle\otimes\cdots\otimes|\tilde{\mathbf{x}}^{(N)}\rangle$ is

$$P = \left(\frac{|\alpha|^2}{\|\mathbf{x}\|^2 + |\alpha|^2}\right)^N. \tag{35}$$

We now choose $\alpha = m|b|N$ for $m > 0$. Since $\|\mathbf{x}\|^2 \leq |b|^2 N$, the probability P becomes

$$P = \left(\frac{m^2|b|^2N^2}{\|\mathbf{x}\|^2 + m^2|b|^2N^2}\right)^N \tag{36}$$

$$\geq \left(\frac{m^2N}{1+m^2N}\right)^N \equiv l_m(N). \tag{37}$$

We note that $l_m(N)$ is decreasing for N, and that it converges to e^{-1/m^2} as N grows large. Thus, the probability P of obtaining all $|x_j\rangle$ is at least e^{-1/m^2}.

B. CASE OF QUATERNARY VARIABLES

For the case of quaternary variables, we assume that the unknowns x_j are of the form

$$x_j = s_j + it_j, \tag{38}$$

where s_j has two distinct values a and b in $\mathbb{R}$, t_j has two distinct values c and d in $\mathbb{R}$, and $i = \sqrt{-1}$. Moreover, we let $|a| \leq |b|$ and $|c| \leq |d|$.

As shown in Fig. 2, we extract the real part s_j and the imaginary part t_j of x_j separately. First, we describe the procedure to obtain the value of s_j. In the first step, we modify a given linear system by adding the following equations:

$$\begin{aligned}
&\mathbf{A}^*\,(x_{N+1},\ldots,x_{2N})^T = \mathbf{y}^*,\\
&x_j + x_{N+j} - 2(a-b)\alpha^{-1}x_{2N+1} = 2b,\\
&x_j + x_{N+j} + 2(a-b)\alpha^{-1}x_{2N+2} = 2a,
\end{aligned} \tag{39}$$

where $\alpha \in \mathbb{C}$ is chosen later. Then we obtain the modified linear system

$$\tilde{\mathbf{A}}^{(s_j)}\tilde{\mathbf{x}}^{(s_j)} = \tilde{\mathbf{y}}, \tag{40}$$

where

$$\tilde{\mathbf{x}^{(s_j)}} = (x_1,\ldots,x_{2N+2})^T, \tag{41}$$

$$\tilde{\mathbf{y}} = \left(y_1,\ldots,y_N,y_1^*,\ldots,y_N^*,2b,2a\right)^T. \tag{42}$$

From (39), the solution is

$$\tilde{\mathbf{x}}^{(s_j)} = \left(x_1,\ldots,x_N,x_1^*,\ldots,x_N^*,\alpha\frac{s_j-b}{a-b},\alpha\frac{a-s_j}{a-b}\right)^T. \tag{43}$$

In the second step, by applying a QLSS to the modified linear system in (40), we obtain the quantum state of the solution in (43):

$$|\tilde{\mathbf{x}}^{(s_j)}\rangle = \frac{\sqrt{2}\,\|\mathbf{x}\|}{\sqrt{2\,\|\mathbf{x}\|^2 + |\alpha|^2}}|\phi\rangle + \frac{\alpha}{\sqrt{2\,\|\mathbf{x}\|^2 + |\alpha|^2}}|s_j\rangle, \tag{44}$$

where

$$|\phi\rangle = \frac{1}{\sqrt{2}\,\|\mathbf{x}\|}\sum_{i=0}^{N-1}(x_{i+1}|i\rangle + x_{i+1}^*|N+i\rangle), \tag{45}$$

$$|s_j\rangle = \frac{s_j-b}{a-b}|2N\rangle + \frac{a-s_j}{a-b}|2N+1\rangle. \tag{46}$$

In the third step, we measure the state $|\tilde{\mathbf{x}}^{(s_j)}\rangle$ in the computational basis. We then extract the value of s_j by noting that $|s_j\rangle = |2N\rangle$ if $s_j = a$, and that $|s_j\rangle = |2N+1\rangle$ if $s_j = b$. The probability of obtaining $|s_j\rangle$ from $|\tilde{x}^{(s_j)}\rangle$ is

$$\frac{|\alpha|^2}{2\,\|\mathbf{x}\|^2 + |\alpha|^2}. \tag{47}$$

Similarly for the value of t_j, we first modified a given linear system by adding the following equations:

$$\begin{aligned}
&\mathbf{A}^*\,(x_{N+1},\ldots,x_{2N})^T = \mathbf{y}^*,\\
&x_j - x_{N+j} - 2i(c-d)\alpha^{-1}x_{2N+1} = 2id,\\
&x_j - x_{N+j} + 2i(c-d)\alpha^{-1}x_{2N+2} = 2ic.
\end{aligned} \tag{48}$$

Then the modified linear system

$$\tilde{\mathbf{A}}^{(t_j)}\tilde{\mathbf{x}}^{(t_j)} = \tilde{\mathbf{y}}, \tag{49}$$

where

$$\tilde{\mathbf{x}}^{(t_j)} = (x_1,\ldots,x_{2N+2})^T, \tag{50}$$

$$\tilde{\mathbf{y}} = \left(y_1,\ldots,y_N,y_1^*,\ldots,y_N^*,2id,2ic\right)^T, \tag{51}$$

has the solution

$$\tilde{\mathbf{x}}^{(t_j)} = \left(x_1, \ldots, x_N, x_1^*, \ldots, x_N^*, \alpha\frac{t_j - d}{c - d}, \alpha\frac{c - t_j}{c - d}\right)^T. \quad (52)$$

Next, a QLSS solves the modified linear system, giving the following state:

$$|\tilde{\mathbf{x}}^{(t_j)}\rangle \equiv \frac{\sqrt{2}\,\|\mathbf{x}\|}{\sqrt{2\,\|\mathbf{x}\|^2 + |\alpha|^2}}|\phi\rangle + \frac{\alpha}{\sqrt{2\,\|\mathbf{x}\|^2 + |\alpha|^2}}|t_j\rangle, \quad (53)$$

where

$$|\phi\rangle = \frac{1}{\sqrt{2}\,\|\mathbf{x}\|}\sum_{i=0}^{N-1}(x_{i+1}|i\rangle + x_{i+1}^*|N+i\rangle), \quad (54)$$

$$|t_j\rangle = \frac{t_j - d}{c - d}|2N\rangle + \frac{c - t_j}{c - d}|2N+1\rangle. \quad (55)$$

Finally, we measure the state $|\tilde{\mathbf{x}}^{(t_j)}\rangle$ in the computational basis. The probability of obtaining $|t_j\rangle$ from $|\tilde{\mathbf{x}}^{(t_j)}\rangle$ is

$$\frac{|\alpha|^2}{2\,\|\mathbf{x}\|^2 + |\alpha|^2}. \quad (56)$$

From (47) and (56), the probability P of obtaining all $|s_j\rangle$ and $|t_j\rangle$ is

$$P = \left(\frac{|\alpha|^2}{2\,\|\mathbf{x}\|^2 + |\alpha|^2}\right)^{2N}. \quad (57)$$

Let us choose $\alpha = 2m\sqrt{(|b|^2 + |d|^2)}N$ for $m \in \mathbb{C}$. Since $\|\mathbf{x}\|^2 \le (|b|^2 + |d|^2)N$,

$$P = \left(\frac{4m^2(|b|^2 + |d|^2)N^2}{2\,\|\mathbf{x}\|^2 + 4m^2(|b|^2 + |d|^2)N^2}\right)^{2N} \quad (58)$$

$$\ge \left(\frac{2m^2N}{1 + 2m^2N}\right)^{2N} \equiv l_m(N). \quad (59)$$

We observe that $l_m(N)$ is decreasing for N, and that it converges to e^{-1/m^2} as N grows large. Thus, we can conclude that the probability of obtaining all the values of x_j is at least e^{-1/m^2}.

C. CASE OF ROOTS OF A COMPLEX NUMBER

We consider the case when the unknowns x_j are the Mth roots of a complex number. An Mth root z of a complex number z_0, where M is a positive integer, is a complex number satisfying

$$z^M = z_0. \quad (60)$$

Let us assume that the unknowns x_j are of the form

$$x_j = \sqrt{r}e^{i\theta_j}, \quad (61)$$

where $r > 0$,

$$\theta_j = \varphi + \frac{2\pi}{M}k, \quad (62)$$

$\varphi \in [0, 2\pi/M)$, $M = 2^m$, m is a positive integer, and $k = 0, 1, \ldots, M-1$. Then x_j are the Mth roots of $r^{M/2}e^{iM\varphi}$.

Given $\mathbf{Ax} = \mathbf{y}$, for $s = 0, \ldots, m-1$, we let $\tilde{\mathbf{A}}_s^{(j)} \in \mathbb{C}^{2^{s+1}N \times 2^{s+1}N}$ and $\tilde{\mathbf{y}}_s \in \mathbb{C}^{2^{s+1}N}$ as follows:

$$\text{for } m \ge 2,\ \tilde{\mathbf{A}}_s^{(j)} = |0\rangle\langle 0| \otimes \Omega + \sum_{t=1}^{2^{s+1}-1}|t\rangle\langle t| \otimes \mathbf{AR}\Omega + \sum_{t=1}^{2^{s+1}-2}|t+1\rangle\langle t| \otimes \mathbf{Y}\Omega, \quad (63)$$

$$\text{for } m = 1,\ \tilde{\mathbf{A}}_s^{(j)} = |0\rangle\langle 0| \otimes \Omega + \sum_{t=1}^{2^{s+1}-1}|t\rangle\langle t| \otimes \mathbf{AR}\Omega, \quad (64)$$

$$\tilde{\mathbf{y}}_s = |0\rangle \otimes \sum_{i=0}^{N-1}|i\rangle + |1\rangle \otimes \mathbf{y}, \quad (65)$$

where

$$\Omega = \mathbf{I}_N + (\alpha^{-1} - 1)|j-1\rangle\langle j-1|, \quad (66)$$

$$\mathbf{R} = \mathbf{I}_N + (\sqrt{r} - 1)|j-1\rangle\langle j-1|, \quad (67)$$

$$\mathbf{Y} = -\mathbf{y}\,\langle j-1|\,, \quad (68)$$

and the value of $\alpha \in \mathbb{C}$ is chosen later. The solution of $\tilde{\mathbf{A}}_s^{(j)}\tilde{\mathbf{x}}_s^{(j)} = \tilde{\mathbf{y}}_s$ is

$$\tilde{\mathbf{x}}_s^{(j)} = \alpha\left(\sum_{k=0}^{2^{s+1}-1}(e^{i\theta_j})^k|k\rangle\right)|j-1\rangle + \sum_{t\ne j-1}\left(|0\rangle + x_{t+1}\sum_{k=1}^{2^{s+1}-1}(e^{i\theta_j})^{k-1}|k\rangle\right)|t\rangle, \quad (69)$$

and a QLSS gives the state $|\tilde{\mathbf{x}}_s^{(j)}\rangle$ of the following form:

$$|\tilde{\mathbf{x}}_s^{(j)}\rangle = \sum_{t=1}^{N} c_t|\psi_t^{(s)}\rangle|t-1\rangle \in \mathbb{C}^{2^{s+1}} \otimes \mathbb{C}^N, \quad (70)$$

where

$$c_j = \frac{\sqrt{2^{s+1}}\alpha}{\sqrt{2^{s+1}|\alpha|^2 + \left(r(2^{s+1}-1)+1\right)(N-1)}}, \quad (71)$$

$$|\psi_j^{(s)}\rangle = \frac{1}{\sqrt{2^{s+1}}}\sum_{k=0}^{2^{s+1}-1}e^{ik\theta_j}|k\rangle. \quad (72)$$

We next measure the second register of the state $|\tilde{\mathbf{x}}_s^{(j)}\rangle$ in the computational basis. Then, with probability

$$P_s \equiv \frac{2^{s+1}|\alpha|^2}{2^{s+1}|\alpha|^2 + (r(2^{s+1}-1)+1)(N-1)}, \quad (73)$$

we obtain $|j-1\rangle$, and the state in the first register becomes $|\psi_j^{(s)}\rangle$, which can be written as

$$|\psi_j^{(s)}\rangle = |x_j^{(s)}\rangle|x_j^{(s-1)}\rangle \cdots |x_j^{(0)}\rangle \in \mathbb{C}^{2(s+1)}, \quad (74)$$

where

$$|x_j^{(k)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2^k\theta_j}|1\rangle\right), \quad k = 0, \ldots, s. \quad (75)$$

We now define the modified matrices in the first step. Let

$$\tilde{\mathbf{A}}^{(j)} \equiv \bigotimes_{s=0}^{m-2} \left(\tilde{\mathbf{A}}_s^{(j)}\right)^{\otimes 2^{m-2-s}} \otimes \tilde{\mathbf{A}}_{m-1}^{(j)}, \tag{76}$$

$$\tilde{\mathbf{y}} \equiv \bigotimes_{s=0}^{m-2} \tilde{\mathbf{y}}_s^{\otimes 2^{m-2-s}} \otimes \tilde{\mathbf{y}}_{m-1}. \tag{77}$$

Then we measure the (quantum) solution $|\tilde{\mathbf{x}}^{(j)}\rangle$ of $\tilde{\mathbf{A}}^{(j)}\tilde{\mathbf{x}}^{(j)} = \tilde{\mathbf{y}}$, and obtain $|x_j\rangle$ with a certain probability:

$$|x_j\rangle = \bigotimes_{s=0}^{m-2} |\psi_j^{(s)}\rangle^{\otimes 2^{m-2-s}} \otimes |\psi_j^{(m-1)}\rangle, \tag{78}$$

which can be rewritten as

$$|x_j\rangle = \bigotimes_{s=0}^{m-1} |x_j^{(s)}\rangle^{\otimes 2^{m-1-s}}. \tag{79}$$

We observe that letting $k = k_{m-1}k_{m-2}\cdots k_0$ in binary notation,

$$2^s\theta_j = 2^s\left(\varphi + \frac{2\pi}{M}\sum_{t=0}^{m-1} 2^t k_t\right) \tag{80}$$

$$\equiv 2^s\varphi + \pi \sum_{t=0}^{m-1-s} 2^{t-(m-1-s)}k_t \ (\mathrm{mod}\ 2\pi). \tag{81}$$

Then

$$|x_j^{(s)}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i(2^s\varphi+\phi_s)}|1\rangle\right), \tag{82}$$

where

$$\phi_s = \pi \sum_{t=0}^{m-1-s} 2^{t-(m-1-s)}k_t. \tag{83}$$

We note that the state $|x_j^{(s)}\rangle$ is one of the 2^{m-s} possible states, which are 2^{m-1-s} pairs of two orthogonal states.

In the third step, we measure each state $|x_j^{(s)}\rangle$ in certain bases using its 2^{m-1-s} copies. We then decide the value of x_j from the measurement outcomes. For $s = m-1$, the state $|x_j^{(m-1)}\rangle$ has two possible states, which are orthogonal. By measuring $|x_j^{(m-1)}\rangle$ in the basis

$$\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2^{m-1}\varphi}|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i2^{m-1}\varphi}|1\rangle\right)\right\}, \tag{84}$$

we can decide the value of k_0. Then, for $s = m-2$, the state $|x_j^{(m-2)}\rangle$ has four possible states, which are two pairs of two orthogonal states. We measure two copies of the state in the bases

$$\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i2^{m-2}\varphi}|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i2^{m-2}\varphi}|1\rangle\right)\right\}, \tag{85}$$

$$\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + ie^{i2^{m-2}\varphi}|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - ie^{i2^{m-2}\varphi}|1\rangle\right)\right\}. \tag{86}$$

The outcome from the former basis is the value of k_1 when the value of k_0 is 0, and the outcome from the latter basis is the value of k_1 when the value of k_0 is 1. We then determine the value of k_1 from the previously obtained value of k_0. By continuing this measurement procedure, we determine all values of $k_0, k_1, \ldots, k_{m-1}$, i.e., the value of θ_j. The procedure presented above is depicted as a flowchart in Fig. 3.

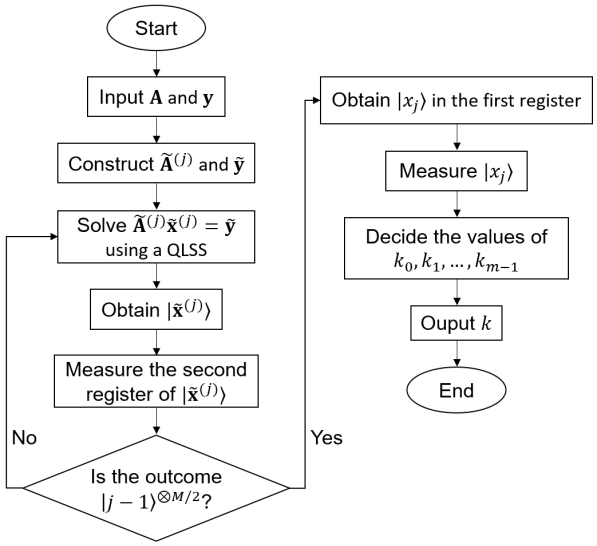

FIGURE 3. Flowchart of the proposed method for roots of a complex number.

The probability P of obtaining all $|x_j\rangle$ can be close to 1. Suppose that we choose $\alpha = u\sqrt{(1+r)M/2N}$ for $u \in \mathbb{N}$. Then

$$P_s > \frac{u^2MN}{u^2MN+2} \tag{87}$$

and

$$P = \left(P_{m-1}\prod_{s=0}^{m-2} P_s^{2^{m-2-s}}\right)^N \tag{88}$$

$$> \left(1 + \frac{2}{u^2MN}\right)^{-MN/2} = l_u(N). \tag{89}$$

Thus, the probability P of obtaining all $|x_j\rangle$ is at least e^{-1/u^2} as noted in (59).

IV. EFFICIENCY OF THE PROPOSED METHOD

A. CONDITION NUMBER AND RUNTIME COMPLEXITY

The condition number of a given matrix is an important parameter in a QLSA, and it affects the runtime of a QLSS. Because we modify a given linear system in the proposed method, it may increase the condition number significantly. For a matrix norm $\|\cdot\|$, the condition number $\kappa(\mathbf{M})$ of a matrix $\mathbf{M}$ is defined by $\kappa(\mathbf{M}) \equiv \|\mathbf{M}\|\left\|\mathbf{M}^{-1}\right\|$. Typically, the spectral norm is used in a QLSA. Let us consider $\tilde{\mathbf{A}}^{(j)}$ in (27). It is straightforward to show that $\kappa(\tilde{\mathbf{A}}^{(j)}) \geq N\kappa(\mathbf{A})$ with respect to the max norm and Frobenius norm in the worst case. Then the additional factor N eliminates the exponential speed-up of a QLSS.

We here present how to reduce the condition number. First, let us consider the case of binary variables. Given $\mathbf{Ax} = \mathbf{y}$, we add the following equations:

$$\begin{aligned} x_j + (b-a)x_{N+1} &= b, \\ x_j + (a-b)x_{N+2} &= a. \end{aligned} \tag{90}$$

Then we obtain the modified linear system

$$\mathbf{B}\mathbf{x}^{(0)} = \tilde{\mathbf{y}}, \tag{91}$$

where

$$\mathbf{x}^{(0)} = (x_1, \ldots, x_N, x_{N+1}, x_{N+2})^T, \tag{92}$$

$$\tilde{\mathbf{y}} = (y_1, \ldots, y_N, b, a)^T. \tag{93}$$

The matrix $\tilde{\mathbf{A}}^{(j)}$ in (27) can be decomposed into matrices having small condition numbers:

$$\tilde{\mathbf{A}}^{(j)} = \mathbf{B}\mathbf{P}^n, \tag{94}$$

where

$$\mathbf{P} = \mathbf{I}_N \oplus \frac{1}{2}\mathbf{I}_2 \tag{95}$$

and $n = \lceil \log |\alpha| \rceil$.

We solve $\mathbf{B}\mathbf{P}^n\tilde{\mathbf{x}}^{(j)} = \tilde{\mathbf{y}}$ by applying a QLSS to each matrix in the decomposed form of $\tilde{\mathbf{A}}^{(j)}$. After applying a QLSS $(n+1)$ times, we get the same solution as in (31). It is not hard to show that $\kappa(\mathbf{B}) = O(\kappa(\mathbf{A}))$ and $\kappa(\mathbf{P}) = 2$, and so the each runtime of a QLSS does not increase. Since we choose $\alpha = m|b|N$ for $m > 0$ in our proposed method, the number of QLSSs used is

$$\lceil \log (m|b|N) \rceil + 1. \tag{96}$$

Therefore, the runtime increases by a factor of $O(\log(N))$, and hence the proposed method maintains the quantum speed-up of a QLSS.

Similarly, we can reduce the condition number for the case of quaternary variables. By adding to $\mathbf{Ax} = \mathbf{y}$ the following equations:

$$\begin{aligned} \mathbf{A}^* (x_{N+1}, \ldots, x_{2N})^T &= \mathbf{y}^*, \\ x_j + x_{N+j} - 2(a-b)x_{2N+1} &= 2b, \\ x_j + x_{N+j} + 2(a-b)x_{2N+2} &= 2a, \end{aligned} \tag{97}$$

we obtain a linear system

$$\mathbf{S}\mathbf{x}^{(0)} = \tilde{\mathbf{y}}, \tag{98}$$

where

$$\mathbf{x}^{(0)} = (x_1, \ldots, x_N, x_{N+1}, x_{N+2})^T, \tag{99}$$

$$\tilde{\mathbf{y}} = \left(y_1, \ldots, y_N, y_1^*, \ldots, y_N^*, 2b, 2a\right)^T. \tag{100}$$

Then the matrix $\tilde{\mathbf{A}}^{(s_j)}$ in (40) can be decomposed as follows:

$$\tilde{\mathbf{A}}^{(s_j)} = \mathbf{S}\mathbf{P}^n, \tag{101}$$

where

$$\mathbf{P} = \mathbf{I}_N \oplus \frac{1}{2}\mathbf{I}_2 \tag{102}$$

and $n = \lceil \log |\alpha| \rceil$. Moreover, $\kappa(\mathbf{S}) = \Theta(\kappa(\mathbf{A}))$. We can also decompose the matrix $\tilde{\mathbf{A}}^{(t_j)}$ in (49) similarly.

Finally, $\tilde{\mathbf{A}}^{(j)}$ in (76) consists of $\tilde{\mathbf{A}}_s^{(j)}$'s, and so it is sufficient to consider only $\tilde{\mathbf{A}}_{m-1}^{(j)}$. This can be decomposed as

$$\tilde{\mathbf{A}}_{m-1}^{(j)} = \mathbf{D}_1 \left(\prod_{i=2}^{M-1} \mathbf{Q}_i \mathbf{D}_i \right) \mathbf{J}^n, \tag{103}$$

where

$$\mathbf{D}_i = \mathbf{I}_M \otimes \mathbf{I}_N + |i\rangle\langle i| \otimes (\mathbf{AR} - \mathbf{I}_N), \tag{104}$$

$$\mathbf{Q}_i = \mathbf{I}_M \otimes \mathbf{I}_N + |i\rangle\langle i-1| \otimes \mathbf{Y}, \tag{105}$$

$$\mathbf{J} = \mathbf{I}_M \otimes \left(\mathbf{I}_N - \frac{1}{2}|j-1\rangle\langle j-1| \right), \tag{106}$$

$$n = \lceil \log \alpha \rceil. \tag{107}$$

We can easily show that $\kappa(\mathbf{D}_i) = O(\kappa(\mathbf{A}))$, $\kappa(\mathbf{Q}_i)$ is $\frac{3+\sqrt{5}}{2}$, and $\kappa(\mathbf{J}) = 2$. Thus, $\tilde{\mathbf{A}}_{m-1}^{(j)}$ is decomposed into $2M + \lceil \log \alpha \rceil - 3$ matrices whose condition numbers are at most $O(\kappa(\mathbf{A}))$. When we choose $\alpha = u\sqrt{1+rN}$ for some u, we can obtain the values of x_j with probability at least e^{-1/u^2} by applying a QLSS $O(\log(N))$ times. Therefore, the runtime of the proposed method increases at most by a factor of $\log(N)$ for all the cases considered.

B. COMPARISON WITH THE METHOD USING THE QAE

We compare our proposed algorithm with the method using the QAE for the case of binary variables. Let us recall the QAE algorithm introduced in Section II-C. For a unitary operator $\mathcal{U}$, let

$$\mathcal{U}|0\rangle = a|\psi\rangle + b|\phi\rangle, \tag{108}$$

where $|\psi\rangle$ and $|\phi\rangle$ are orthogonal states. Then the QAE algorithm estimates the value $\alpha \equiv |a|^2$, and the estimated value $\tilde{\alpha}$ is such that

$$|\tilde{\alpha} - \alpha| \leq 2\sqrt{\alpha(1-\alpha)}\frac{k\pi}{M} + \left(\frac{k\pi}{M}\right)^2 \tag{109}$$

with probability at least $\frac{8}{\pi^2}$ for $k = 1$ and with probability greater than $1 - \frac{1}{2(k-1)}$ for $k \geq 2$. In particular, when $\alpha = 0$, $\tilde{\alpha} = 0$ with certainty, and when $\alpha = 1$ and M is even, $\tilde{\alpha} = 1$ with certainty. Moreover, the operator $\mathcal{U}$ is used $2(M-1)$ times as a controlled operation.

Let ϵ be such that

$$|\tilde{\alpha} - \alpha| \leq 2\sqrt{\alpha(1-\alpha)}\frac{k\pi}{M} + \left(\frac{k\pi}{M}\right)^2 \leq \epsilon\alpha. \tag{110}$$

Thus, ϵ is a multiplicative error of the estimated value $\tilde{\alpha}$. We can then find a lower bound of M:

$$M \geq \frac{k\pi}{\epsilon\sqrt{\alpha}} \left(\sqrt{1-\alpha} + \sqrt{1-\alpha+\epsilon} \right) \tag{111}$$

for $\alpha > 0$ [19].

Let $\mathbf{Ax} = \mathbf{y}$ be a linear system of equations with binary variables x_j, where $\mathbf{A} \in \mathbb{C}^{N \times N}$, $\mathbf{x} = (x_1, \ldots, x_N)^T$, and $\mathbf{y} = (y_1, \ldots, y_N)^T$. For simplicity, we let the binary variables x_j

have the values 0 and 1, not all zero. Then a QLSS gives the solution $|\mathbf{x}\rangle$

$$|\mathbf{x}\rangle = \frac{1}{\|\mathbf{x}\|}(x_1, \ldots, x_N)^T \tag{112}$$

$$= \frac{x_j}{\|\mathbf{x}\|}|j\rangle + \frac{\sqrt{\|\mathbf{x}\|^2 - |x_j|^2}}{\|\mathbf{x}\|}|\phi\rangle, \tag{113}$$

where $|\phi\rangle$ is orthogonal to $|j\rangle$. The probability of obtaining $|j\rangle$ from $|x\rangle$ is 0 if $x_j = 0$, and $\frac{1}{\|\mathbf{x}\|^2}$ if $x_j = 1$. Let $\mathcal{U}$ be a QLSA for the above linear system. We note that a QLSA does not include a measurement step, and hence it can be considered as a unitary operator. Then $\mathcal{U}|0\rangle = |\mathbf{x}\rangle$, the state to estimate is $|\psi\rangle = |j\rangle$, and the estimated value α is 0 or $\frac{1}{\|\mathbf{x}\|^2}$.

Since we can achieve a perfect estimation with certainty if $\alpha = 0$, let us consider when $\alpha = \frac{1}{\|\mathbf{x}\|^2}$. From (21),

$$M \geq \frac{k\pi}{\epsilon}\|\mathbf{x}\|\left(\frac{\sqrt{\|\mathbf{x}\|^2 - 1}}{\|\mathbf{x}\|} + \frac{\sqrt{(1+\epsilon)\|\mathbf{x}\|^2 - 1}}{\|\mathbf{x}\|}\right) \tag{114}$$

$$\geq \frac{2k\pi}{\epsilon}\sqrt{\|\mathbf{x}\|^2 - 1}. \tag{115}$$

Since $\|\mathbf{x}\|^2$ has the range from 0 to N, M must satisfy the following inequality:

$$M \geq \frac{2k\pi}{\epsilon}\sqrt{N-1}. \tag{116}$$

In the method using the QAE, a QLSA $\mathcal{U}$ is applied $2(M-1)$ times for estimating the value $\alpha = \frac{1}{\|\mathbf{x}\|^2}$. By (116), the number of $\mathcal{U}$ used is at least

$$\frac{4k\pi}{\epsilon}\sqrt{N-1} - 2. \tag{117}$$

We note that neither k nor ϵ depends on N. Indeed, $\epsilon = 1/2$ is enough to distinguish two possible values 0 and $\frac{1}{\|\mathbf{x}\|^2}$ of α. Thus, the number of $\mathcal{U}$ used is in $O(\sqrt{N})$, and so the method using the QAE has the runtime complexity of

$$\Omega(\sqrt{N}\log N). \tag{118}$$

However, our proposed method has the same runtime complexity as a QLSA, that is, $O(\log N)$.

V. APPLICATION AND PERFORMANCE

A. APPLICATION TO THE MIMO DETECTION PROBLEM

We now introduce an application of the proposed algorithm. In communication systems, MIMO is a technique that employs multiple antennas to increase the channel capacity and improve the communication performance. For example, a user can transmit signals via multiple antennas, then the base station receives the signals from multiple antennas.

A MIMO system can be described as a system of linear equations. Let a MIMO system have N input antennas and M output antennas, and let $\mathbf{H} \in \mathbb{C}^{M\times N}$ be the associated matrix of the MIMO channel. Then an input signal vector $\mathbf{x} \in \chi^N$ with alphabet set χ changes to the output signal vector $\mathbf{y} \in \mathbb{C}^M$ as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{119}$$

where $\mathbf{n} \in \mathbb{C}^M$ is the noise vector. The MIMO detection problem is to recover the transmitted signal $\mathbf{x}$ reliably.

We consider two MIMO detectors: the zero-forcing (ZF) detector and the linear minimum mean square error (MMSE) detector [20]. These detectors provide the estimated vector $\mathbf{x}'$ of the input signal vector $\mathbf{x}$. Specifically, the ZF detector gives

$$\mathbf{x}' = \mathbf{H}^+ y, \tag{120}$$

where $\mathbf{H}^+$ is the Moore–Penrose pseudoinverse of $\mathbf{H}$, and the linear MMSE detector gives

$$\mathbf{x}' = (\mathbf{H}^\dagger\mathbf{H} + \mu\mathbf{I}_N)^{-1}\mathbf{H}^\dagger\mathbf{y} \tag{121}$$

for some value μ. Thus, obtaining the estimated input signal is equivalent to solving the linear system

$$\mathbf{A}\mathbf{x}' = \mathbf{y}', \tag{122}$$

where $\mathbf{A} = \mathbf{H}$ and $\mathbf{y}' = \mathbf{y}$ for the ZF detector, and $\mathbf{A} = \mathbf{H}^\dagger\mathbf{H} + \mu\mathbf{I}_N$ and $\mathbf{y}' = \mathbf{H}^\dagger\mathbf{y}$ for the linear MMSE detector. In other words, the ZF and MMSE detectors can be performed using a QLSA, and so we can call the proposed algorithm a quantum ZF/MMSE detector. From now on, we assume that the proposed method is quantum versions of the ZF and MMSE detectors when we compare with the (classical) ZF and MMSE detectors, respectively.

In particular, the proposed method can be effectively exploited in large-scale MIMO systems [20], [21] because of the quantum speed-up of a QLSA. Furthermore, we remark that the proposed method can extract the values of a given quantum state $|\psi\rangle$, which has roots of a complex number when we let $\mathbf{A} = \mathbf{I}$ and $\mathbf{y} = |\psi\rangle$. Therefore, the proposed technique can be appropriate for any other MIMO detectors if the MIMO detection is performed by quantum computing with a quantum speed-up.

The proposed method can be directly applied to the MIMO detection problem with binary phase-shift keying (BPSK) or quadrature phase-shift keying (QPSK) modulation. Indeed, for the case of BPSK with $\chi = \{1, -1\}$, we let $a = -1$ and $b = 1$ in (26). Furthermore, we can apply this to MPSK modulation. For the case of 8PSK with $\chi = \{e^{i\frac{\pi}{4}k} : k = 0, 1, \ldots, 7\}$, we let $r = 1, \varphi = 0$, and $M = 8$ in (61). We note that the proposed technique can be applied to $M \times N$ channel matrices $\mathbf{H}$ by considering the modified one as shown in (12).

The noise of a channel induces a detection error. For the ZF detector, the recovered vector $\mathbf{x}'$ is

$$\mathbf{x}' = \mathbf{A}^+\mathbf{y} \tag{123}$$

$$= \mathbf{x} + \boldsymbol{\epsilon}, \tag{124}$$

where $\boldsymbol{\epsilon} \equiv \mathbf{A}^+\mathbf{y} - \mathbf{x}$, and $\mathbf{A} = \mathbf{H}$ is a MIMO channel matrix. Similarly, the recovered vector $\mathbf{x}'$ of the MMSE detector is

$$\mathbf{x}' = (\mathbf{A}^\dagger\mathbf{A} + \boldsymbol{\mu}\mathbf{I})^{-1}\mathbf{A}^\dagger\mathbf{y} \tag{125}$$

$$= \mathbf{x} + \boldsymbol{\epsilon}, \tag{126}$$

where $\boldsymbol{\epsilon} \equiv (\mathbf{A}^\dagger\mathbf{A} + \boldsymbol{\mu}\mathbf{I})^{-1}\mathbf{A}^\dagger\mathbf{y} - \mathbf{x}$. Thus, the noise affects the precision of the final state when we solve the problem using a QLSA. We can present the solution state of a QLSA in terms of the error term ϵ. Let us first consider the case of BPSK modulation. With the error term ϵ, the final state in (33) becomes

$$|x_j'\rangle = \frac{(1 - x_j - \epsilon_j)|N\rangle + (1 + x_j + \epsilon_j)|N+1\rangle}{\sqrt{|1 - x_j - \epsilon_j|^2 + |1 + x_j + \epsilon_j|^2}}, \quad (127)$$

where we set $a = -1$ and $b = 1$. Thus, a measurement error when deciding the transmitted bit inevitably occurs. Then the probability P_{bpsk} of error is

$$P_{bpsk} = \frac{|\epsilon_j|^2}{|2x_j + \epsilon_j|^2 + |\epsilon_j|^2}. \quad (128)$$

Similarly, for the case of QPSK modulation, we can see that the final states in (46) and (55) become

$$|s_j'\rangle = \frac{(b - s_j - p_j)|2N\rangle + (s_j + p_j - a)|2N+1\rangle}{\sqrt{|b - s_j - p_j|^2 + |s_j + p_j - a|^2}}, \quad (129)$$

$$|t_j'\rangle = \frac{(d - t_j - q_j)|2N\rangle + (t_j + q_j - c)|2N+1\rangle}{\sqrt{|d - t_j - q_j|^2 + |t_j + q_j - c|^2}}, \quad (130)$$

where $x_j = s_j + it_j$ and $\epsilon_j = p_j + iq_j$. Then the probabilities P_1 and P_2 of error for s_j and t_j are

$$P_1 = \frac{|p_j|^2}{|2s_j + p_j|^2 + |p_j|^2}, \quad (131)$$

$$P_2 = \frac{|q_j|^2}{|2t_j + q_j|^2 + |q_j|^2}, \quad (132)$$

respectively. Moreover, the state for the case of MPSK modulation in (82) becomes

$$|x_j^{\prime(s)}\rangle = \frac{1}{\sqrt{1 + |x_j + \epsilon_j|^{2^{s+1}}}}\left(|0\rangle + (x_j + \epsilon_j)^{2^s}|1\rangle\right), \quad (133)$$

where we choose $r = 1$ and $s = 0, \ldots, m-1$.

We can obtain some information of a quantum state only by quantum measurement, and we cannot distinguish nonorthogonal states without error. In other words, when we measure a state in a certain basis to obtain a particular value, even a small amount of noise can induce a nonzero probability of error. To overcome this, we can measure sufficiently many copies of a state, then we decide the binary value depending on the majority of measurement outcomes. Specifically, we measure $2l + 1$ copies of the final state, and we select the outcome that appears more than l times. From now on, we call this l-measurement, and we call the number l the order of measurement repetition. For a probability P and $l = 0, 1, 2, \ldots,$ we define

$$P^{(l)} \equiv \sum_{t=0}^{l} \binom{2l+1}{t} P^{2l+1-t}(1-P)^t, \quad (134)$$

$$P^{(\infty)} \equiv \begin{cases} 0 & \text{if } P < 1/2 \\ 1/2 & \text{if } P = 1/2 \\ 1 & \text{if } P > 1/2 \end{cases}. \quad (135)$$

Then, after applying l-measurement to the state in (127), the probability of (one bit) error is $P_{bpsk}^{(l)}$, and the limit of $P_{bpsk}^{(l)}$ as l grows is $P_{bpsk}^{(\infty)}$. For the QPSK modulation, the bit error ratio $P_{qpsk}^{(l)}$ with respect to l-measurement is

$$P_{qpsk}^{(l)} = \frac{1}{2}\left(P_1^{(l)} + P_2^{(l)}\right), \quad (136)$$

and the limit is

$$P_{qpsk}^{(\infty)} = \frac{1}{2}\left(P_1^{(\infty)} + P_2^{(\infty)}\right). \quad (137)$$

We finally consider the 8PSK. Let $k = k_2k_1k_0$ be the phase label of x_j. It is not hard to show that the bit error ratio $P_{8psk}^{(l)}$ with respect to l-measurement is

$$P_{8psk}^{(l)} = \frac{1}{3}\sum_{k_2',k_1',k_0'=0}^{1} \mathrm{P}_{k'}^{(l)}\mathrm{Q}_{k'}^{(l)}\mathrm{R}_{k'}^{(l)}D(k'), \quad (138)$$

where

$$\mathrm{P}_{k'} = \frac{1}{2}\frac{|(x_j + \epsilon_j) + e^{i\frac{\pi}{4}(4k_2' + 2k_1' + k_0')}|^2}{1 + |x_j + \epsilon_j|^2}, \quad (139)$$

$$\mathrm{Q}_{k'} = \frac{1}{2}\frac{|(x_j + \epsilon_j)^2 + e^{i\frac{\pi}{2}(2k_1' + k_0')}|^2}{1 + |x_j + \epsilon_j|^4}, \quad (140)$$

$$\mathrm{R}_{k'} = \frac{1}{2}\frac{|(x_j + \epsilon_j)^4 + e^{i\pi(k_0')}|^2}{1 + |x_j + \epsilon_j|^8}, \quad (141)$$

$$D(k') = (k_2' \oplus g_2) + (k_2' \oplus k_1' \oplus g_1) + (k_1' \oplus k_0' \oplus g_0), \quad (142)$$

and $g = g_2g_1g_0$ is the Gray code of x_j. Then the limit is

$$P_{8psk}^{(\infty)} = \frac{1}{3}\sum_{k_2',k_1',k_0'=0}^{1} \mathrm{P}_{k'}^{(\infty)}\mathrm{Q}_{k'}^{(\infty)}\mathrm{R}_{k'}^{(\infty)}D(k'). \quad (143)$$

B. PERFORMANCE COMPARISON

We first present the system model, and then the performance results of the proposed method. We consider a MIMO system with N transmit and N receive antennas. The channel is assumed to be block Gaussian fading, and the transmitted vector $\mathbf{x}$ is drawn from the BPSK/QPSK/8PSK constellation. Then the received vector is given by

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \quad (144)$$

where $\mathbf{H} \in \mathbb{C}^{N\times N}$ is the channel matrix whose entries are independent and identically distributed (i.i.d.) $\mathcal{CN}(0, 1)$, the noise vector $\mathbf{n}$ is additive white Gaussian noise whose

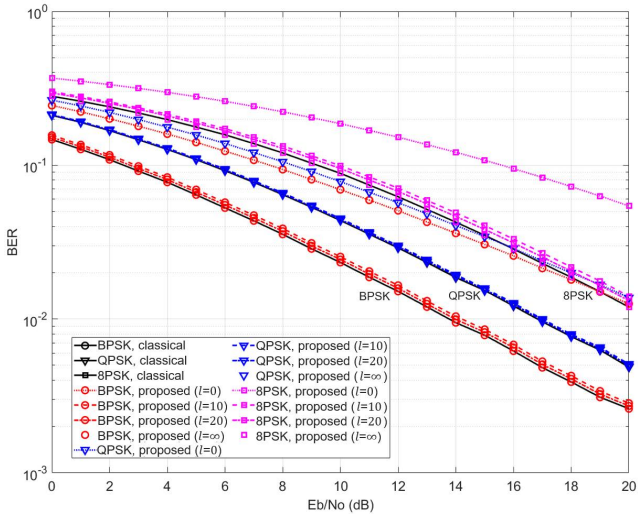

FIGURE 4. BER performance comparison for 2 × 2 MIMO with ZF.

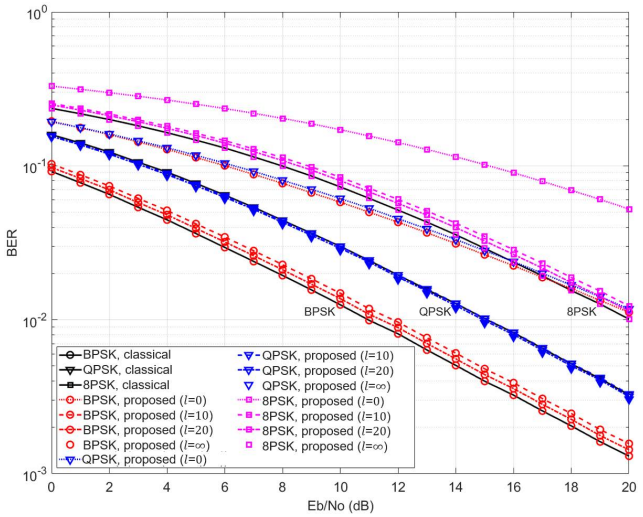

FIGURE 5. BER performance comparison for 2 × 2 MIMO with MMSE.

entries are i.i.d. $\mathcal{CN}(0, N_0)$, and N_0 is the power of noise. We use the ZF and MMSE detectors, and we compare the bit error rate (BER) performance of the proposed method with the classical one for each signal-to-noise ratio (SNR) from 0 dB to 20 dB in steps of 1 dB. We execute the detection algorithms one million times, and then evaluate the average value of the BERs. Although the proposed method can be executed in a quantum computing device, its computing ability has been insufficient to achieve good performance so far. Thus, we start with the results obtained theoretically by a QLSA.

We first present the BER performances of the classical ZF detector and the proposed method associated with ZF for 2 × 2 MIMO channels as shown in Fig. 4. We can see that the BER performance of the proposed method gets close to that of the classical one as the order l grows large. Indeed, the limit value (when $l = \infty$) of the BER performance with l-measurement

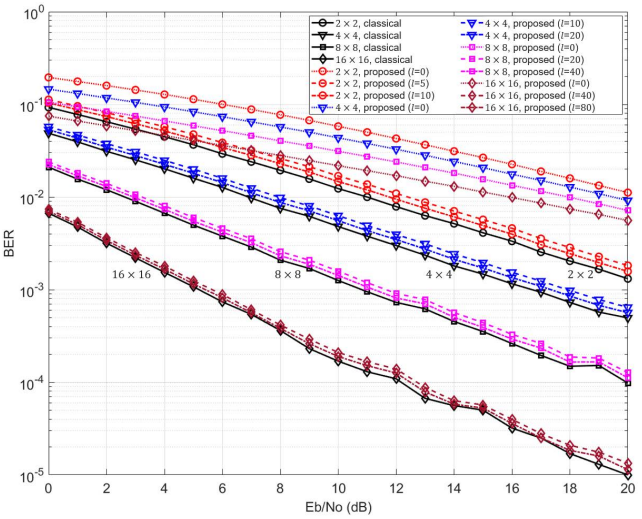

FIGURE 6. BER performance comparison for MMSE in various sizes of MIMO with BPSK.

almost coincides with that of the classical method. Fig. 5 shows the BER performances of the classical MMSE detector and the proposed method associated with MMSE for 2 × 2 MIMO channels, and the results are the same as in the case of the ZF. Remarkably, the performance of the proposed method for QPSK is better than the others for both cases, and hence it seems counter-intuitive. In fact, the proposed methods for QPSK and MPSK can be viewed as generalizations of the method for BPSK. Whereas we decide the phase of x_j close to the point of x_j in the constellation diagram for MPSK, the method for QPSK provides us the real and imaginary parts of x_j separately. For example, we perform measurements in three axes for 4PSK to decide the phase label similar to a binary decision, but we perform two measurements for QPSK to obtain the real and imaginary values. We speculate that the difference in the measurement process could make the improved performance.

Fig. 6 shows the BER performances of the classical MMSE detector and the proposed method associated with MMSE for various sizes of MIMO with BPSK. We choose different l-measurements depending on the sizes of MIMO channel matrices. We can observe that for the proposed method, the larger the size of MIMO channel, the higher the value of l required to obtain the same performance.

As shown in Figs. 4, 5, and 6, The results of the proposed algorithm without repeated measurements are worse than those of the classical method. However, the performance approaches that of the classical method as the order l grows large, and the quantum limit is almost the same as that of the classical performance. We now present the rate of convergence of the performance. For the proposed method with a certain modulation, let $P^{(l)}$ be the bit error ratio with respect to l-measurement, and let $P^{(\infty)}$ be defined as before. Then the rate of convergence for $P^{(l)}$ is defined as the limit value

$$\lim_{l\to\infty} R_l, \tag{145}$$

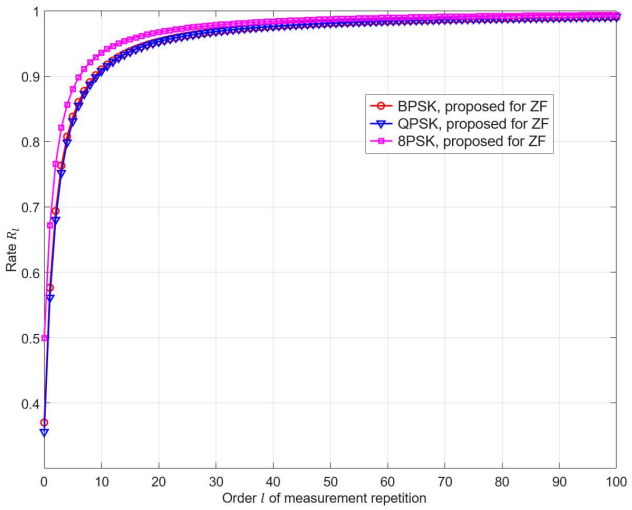

FIGURE 7. Numerical results for the convergence rate of the proposed method in 2 × 2 MIMO with ZF, where the SNR is 10 dB.

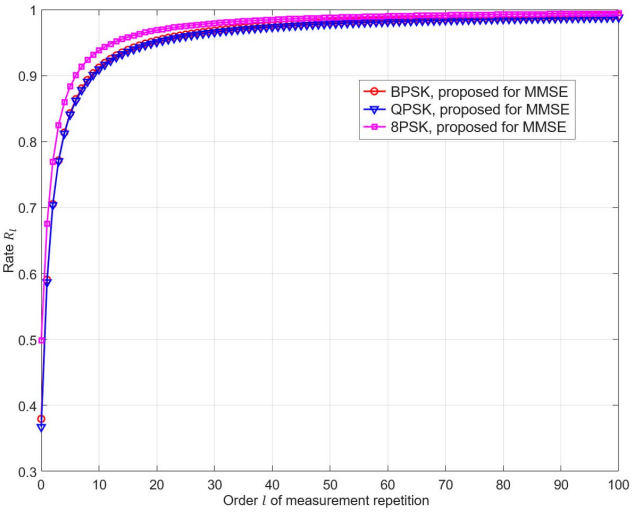

FIGURE 8. Numerical results for the convergence rate of the proposed method in 2 × 2 MIMO with MMSE, where the SNR is 10 dB.

where $R_l = \frac{|P^{(l+1)} - P^{(\infty)}|}{|P^{(l)} - P^{(\infty)}|}$. Figs. 7 and 8 show that the rate of convergence could be 1 for both cases. This means that the sequence $P^{(l)}$ converges sublinearly to $P^{(\infty)}$. In other words, the sequence $P^{(l)}$ increases rapidly for low values of l, and goes to the limit value $P^{(\infty)}$ slowly for high values of l. Thus, we can obtain a good performance using l-measurement with a low value of l.

VI. CONCLUSION

In this paper, we have presented a proposed QLSA that can be used to obtain classical information from the solution. We explicitly construct the modified linear systems when the solutions have binary variables, quaternary variables, or roots of a complex number. In particular, our method does not require any extra process to obtain classical information, and so the proposed algorithm has a lower complexity than the previous method using the QAE. Moreover, we show that the proposed algorithm can be applied to solve the MIMO detection problem, and we present and discuss the simulation results of our method compared to those of classical linear MIMO detectors.

REFERENCES

[1] A. Montanaro, "Quantum algorithms: An overview," *NPJ Quantum Inf.*, vol. 2, no. 1, p. 15023, Jan. 2016.
[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. STOC*, New York, NY, USA, 1996, pp. 212–219.
[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.
[4] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Phys. Rev. Lett.*, vol. 103, no. 15, Oct. 2009, Art. no. 150502.
[5] J. R. Shewchuk, "An introduction to the conjugate gradient method without the agonizing pain," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-CS-94-125, Mar. 1994.
[6] A. Ambainis, "Variable time amplitude amplification and quantum algorithms for linear algebra problems," in *Proc. STACS*, Paris, France, 2012, pp. 636–647.
[7] A. M. Childs, R. Kothari, and R. D. Somma, "Quantum algorithm for systems of linear equations with exponentially improved dependence on precision," *SIAM J. Comput.*, vol. 46, no. 6, pp. 1920–1950, Jan. 2017.
[8] L. Wossnig, Z. Zhao, and A. Prakash, "Quantum linear system algorithm for dense matrices," *Phys. Rev. Lett.*, vol. 120, Jan. 2018, Art. no. 050502.
[9] S. Chakraborty, A. Gilyén, and S. Jeffery, "The power of block-encoded matrix powers: Improved regression techniques via faster Hamiltonian simulation," in *Proc. ICALP*, Patras, Greece, 2019, pp. 33:1–33:14.
[10] I. Kerenidis and A. Prakash, "Quantum gradient descent for linear systems and least squares," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 2, Feb. 2020, Art. no. 022316.
[11] C. Shao and H. Xiang, "Row and column iteration methods to solve linear systems on a quantum computer," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 2, Feb. 2020, Art. no. 022322.
[12] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *AMS Contemp. Math.*, vol. 305, pp. 53–74, Oct. 2002.
[13] B. D. Clader, B. C. Jacobs, and C. R. Sprouse, "Preconditioned quantum linear system algorithm," *Phys. Rev. Lett.*, vol. 110, no. 25, Jun. 2013, Art. no. 250504.
[14] P. A. M. Casares and M. A. Martin-Delgado, "A quantum active learning algorithm for sampling against adversarial attacks," *New J. Phys.*, vol. 22, no. 7, Jul. 2020, Art. no. 073026.
[15] G. Wang, "Efficient quantum algorithms for analyzing large sparse electrical networks," *Quantum Info. Comput.*, vol. 17, nos. 11–12, pp. 987–1026, Sep. 2017.
[16] I. Kerenidis and A. Prakash, "A quantum interior point method for LPs and SDPs," *ACM Trans. Quantum Comput.*, vol. 1, no. 1, pp. 1–32, Dec. 2020.
[17] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2019.
[18] S. Mondal, M. R. Laskar, and A. K. Dutta, "ML criterion based signal detection of a MIMO-OFDM system using quantum and semi-quantum assisted modified DHA/BBHT search algorithm," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1688–1698, Feb. 2021.
[19] A. Scherer, B. Valiron, S.-C. Mau, S. Alexander, E. van den Berg, and T. E. Chapuran, "Concrete resource analysis of the quantum linear-system algorithm used to compute the electromagnetic scattering cross section of a 2D target," *Quantum Inf. Process.*, vol. 16, no. 3, p. 60, Jan. 2017.
[20] S. Yang and L. Hanzo, "Fifty Years of MIMO detection: The road to large-scale MIMOs," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 1941–1985, Sep. 2015.

[21] K. Zheng, L. Zhao, J. Mei, B. Shao, W. Xiang, and L. Hanzo, "Survey of large-scale MIMO systems," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1738–1760, 3rd Quart., 2015.

JEONGHOON PARK received the B.S. degree in physics and mathematics and the Ph.D. degree in mathematics from Kyung Hee University, Seoul, South Korea, in 2008 and 2016, respectively.

He was a Postdoctoral Researcher and a Research Professor for a period of four years with the Smart Quantum Communication Research Center, Korea University, where he is currently a Research Professor with the Research Institute for Information and Communication Technology. His research interests include quantum channel capacity, zero-error information theory, and quantum algorithm.

YOUNGJIN SEO received the B.S. degree in electrical engineering from Korea University, Seoul, South Korea, in 2018, where he is currently pursuing the Ph.D. degree with the School of Electrical Engineering.

His research interests include quantum algorithm and quantum random number generation.

JUN HEO (Member, IEEE) received the B.S. and M.S. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1989 and 1991, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 2002.

From 1991 to 1997, he was a Senior Research Engineer with LG Electronics Company Inc. He is currently a Professor with the School of Electrical Engineering, Korea University, Seoul. His research interests include channel coding theory and quantum communication.