Quantum Algorithm for Higher-Order Unconstrained Binary Optimization and MIMO Maximum Likelihood Detection

Masaya Norimoto, *Graduate Student Member, IEEE*, Ryuhei Mori, *Non Member, IEEE*, and
Naoki Ishikawa, *Senior Member, IEEE*.

arXiv:2205.15478v2 [eess.SP] 16 Feb 2023

Abstract—In this paper, we propose a quantum algorithm that supports a real-valued higher-order unconstrained binary optimization (HUBO) problem. This algorithm is based on the Grover adaptive search that originally supported HUBO with integer coefficients. Next, as an application example, we formulate multiple-input multiple-output maximum likelihood detection as a HUBO problem with real-valued coefficients, where we use the Gray-coded bit-to-symbol mapping specified in the 5G standard. The proposed approach allows us to construct an efficient quantum circuit for the detection problem and to analyze specific numbers of required qubits and quantum gates, whereas other conventional studies have assumed that such a circuit is feasible as a quantum oracle. To further accelerate the quantum algorithm, we also derive a probability distribution of the objective function value and determine a unique threshold to sample better states. Assuming a future fault-tolerant quantum computing, our proposed algorithm has the potential for significantly reducing query complexity in the classical domain and providing a quadratic speedup in the quantum domain.

Index Terms—Grover adaptive search (GAS), quadratic unconstrained binary optimization (QUBO), higher-order unconstrained binary optimization (HUBO), multiple-input multiple-output (MIMO), maximum-likelihood detection (MLD).

I. INTRODUCTION

MARCONI invented a practical long-range wireless system in 1895. Since then, driven by its intense demand, wireless communication has continued to become more sophisticated as if there were no limits. The limit of communication throughput is known as the Shannon capacity, which is constrained by the bandwidth, the signal-to-noise ratio (SNR), and the numbers of transmit and receive antennas for multiple-input multiple-output (MIMO) scenarios. Clearly, there are physical limits on bandwidth, SNR, and the number of antennas. The forward error correction techniques such as the low-density parity-check code (LDPC) and polar code can achieve near-capacity performance efficiently, but under a certain energy constraint, their performance is constrained by semiconductor miniaturization limits. Marconi mentioned that *it is dangerous to put limits on wireless*. However, wireless communication will reach its physical limits in the near future.

After the eventual end of Moore's law, from a long-term perspective, we must rely on a different computing paradigm, and quantum computing in particular is considered to be promising. Since it is impossible to simulate a quantum computer in an efficient manner on a classical computer, quantum computers offer an essential speed advantage over classical computers [1]. Specifically, Shor's algorithm [2] factors an n-bit integer with the complexity $O(n^2 \log n \log \log n)$, while the best classical algorithm requires $\exp(\Theta(n^{1/3} \log^{2/3} n))$ operations [1],[1] which is an *exponential speedup*. Grover's algorithm [4] finds a specific element from a database of unsorted N elements with the query complexity $O(\sqrt{N})$, while the classic exhaustive search requires $O(N)$ evaluations, which is a *quadratic speedup*. Note that both long-term algorithms assume the realization of fault-tolerant quantum computing (FTQC), which is not yet realized with current technology.

Grover's algorithm has been extended to support binary optimization problems. The pioneering algorithm, *Grover adaptive search* (GAS) [5], requires a complex quantum circuit to evaluate an objective function. For example, an m-qubit register requires $2m - 1$ Toffoli gates to perform quantum addition [6], which is still expensive. To solve this issue, Gilliam *et al.* used a concept of quantum dictionary and allowed for the efficient representation of an arbitrary polynomial function, including quadratic and higher-order terms [7, 8]. This efficient representation improved the feasibility of GAS, and in [8], a quadratic unconstrained binary optimization (QUBO) problem with integer coefficients was solved on a real-world quantum computer with 32 qubits. Unlike the quantum annealing (QA) [9], the GAS proposed by Gilliam *et al.* is innovative in that it supports a higher-order unconstrained binary optimization (HUBO) problem with integer coefficients, which cannot be solved efficiently with state-of-the-art mathematical programming solvers on a classical computer such as CPLEX[2].

In designing wireless systems, the trade-off between performance and complexity is, in general, a source of concern for engineers and researchers. For example, low-complexity MIMO detectors and polar decoders inevitably involve the penalty of lower performance, and complexity is sacrificed to achieve optimal performance. In this situation, the potential for quantum speedup has inspired those who dream of striking the

M. Norimoto and N. Ishikawa are with the Faculty of Engineering, Yokohama National University, Kanagawa 240-8501, Japan (e-mail: ishikawa-naoki-fr@ynu.ac.jp). R. Mori is with the Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology, Tokyo 152-8500, Japan (e-mail: mori@c.titech.ac.jp). This research was partially supported by the Japan Society for the Promotion of Science (JSPS) KAKENHI (Grant Number 22H01484).

[1] $O(\cdot)$ denotes the big-O notation, while $\Theta(\cdot)$ denotes the big-Θ notation [3].

[2] https://www.ibm.com/analytics/cplex-optimizer

fundamental trade-off and achieving the optimal performance with reduced complexity. A pioneering attempt in wireless communications was provided in [10] by Botsinis *et al.* who demonstrated the potential of quantum algorithms to reduce the complexity involved in maximum likelihood detection (MLD). Specifically, they used the Grover-type algorithms, such as Boyer–Brassard–Høyer–Tapp (BBHT) [11] and Dürr–Høyer (DH) search algorithms [12], for performing MLD of data symbols on a quantum computer [13]. Subsequently, a number of important studies have shown promising results [13–20]. However, in those studies, it was assumed that an ideal quantum circuit to evaluate the objective function is feasible as a quantum oracle, which will be detailed in Section II. For more information on quantum-assisted wireless communications, a comprehensive survey can be found in [21, 22].

Against this background, we propose a quantum algorithm that supports a HUBO problem with real-valued coefficients. Then, as a first step toward breaking the trade-off between performance and complexity, we formulate the MIMO MLD as a real-valued HUBO problem and verify the potential of quadratic speedup. The major contributions of this paper are organized as follows.

1) While the conventional GAS [8] supports HUBO with integer coefficients, we modify the quantum algorithm to handle real-valued coefficients. This allows us to solve a HUBO problem even if the objective function contains real-valued coefficients, which is achieved at the cost of one more query in the classical domain (CD).[3]

2) As an application example, we formulate the objective function of MIMO MLD as a real-valued HUBO problem. This formulation is not a straightforward task because the objective function contains complex-valued random variables and a Frobenius norm calculation. This new formulation allows us to analyze specific numbers of qubits and quantum gates required in the constructed quantum circuits, which has been overlooked in conventional studies.

3) We clarify the probability distribution of the objective function value and determine the threshold used inside GAS more efficiently. Then, we demonstrate that the proposed threshold further accelerates the convergence of GAS to the optimal solution.

It is important to note that quantum circuits are sensitive to noise [23], and industrial applications require decades of effort and challenge. The noise induces quantum errors, and quantum error-correcting codes must be used to perform reliable arithmetic on a quantum computer. For example, if we use the surface code with code distance 27, which is one of the quantum error-correcting codes, a logical qubit requires 1568 physical qubits to correct errors [24]. This indicates that even a simple quantum circuit with fewer qubits, e.g., as in Fig. 1, may require many more physical qubits. Since this limitation is beyond the scope of our contributions, we assume the realization of future FTQC as in the conventional

---

[3] The definition of query complexity in CD is detailed in Section III-D, which is the same as the conventional study [13].

TABLE I
LIST OF IMPORTANT MATHEMATICAL SYMBOLS

$\mathbb{B}$		Binary numbers
$\mathbb{R}$		Real numbers
$\mathbb{C}$		Complex numbers
$\mathbb{Z}$		Integers
N_{t}	$\in \mathbb{Z}$	Number of transmit antennas
N_{r}	$\in \mathbb{Z}$	Number of receive antennas
L_{c}	$\in \mathbb{Z}$	Modulation order (constellation size)
σ^2	$\in \mathbb{R}$	Noise variance
γ	$\in \mathbb{R}$	Signal-to-noise ratio
$E(\cdot)$	$\in \mathbb{Z}$	Objective function
n	$\in \mathbb{Z}$	Number of binary variables = transmission rate
m	$\in \mathbb{Z}$	Number of qubits required to encode $E(\cdot)$
i	$\in \mathbb{Z}$	Index of GAS iterations
y, y_i	$\in \mathbb{Z}$	Threshold that is adaptively updated by GAS
L, L_i	$\in \mathbb{Z}$	Number of Grover operators
P	$\in \mathbb{R}$	Probability that controls the proposed threshold
$\mathbf{b}, \mathbf{b}_i$	$\in \mathbb{B}^n$	Binary variables, or data bits
$\mathbf{s}$	$\in \mathbb{C}^{N_{\mathrm{t}} \times 1}$	Data symbols, each symbol is denoted by s_t
$\mathbf{r}$	$\in \mathbb{C}^{N_{\mathrm{r}} \times 1}$	Received symbols, each symbol is denoted by r_u
$\mathbf{H}_{\mathrm{c}}$	$\in \mathbb{C}^{N_{\mathrm{r}} \times N_{\mathrm{t}}}$	Channel coefficients, h_{ut}
$\mathbf{v}$	$\in \mathbb{C}^{N_{\mathrm{r}} \times 1}$	Additive white Gaussian noise, v_u

studies [2, 4, 5, 7, 8, 10–22, 25]. In fact, IBM's roadmap for quantum computers is to achieve 4000 qubits by 2025 [26]. In the subsequent years, they expect 10000 to 100000 qubits, enabling quantum error corrections. Additionally, it was proved in [27] that quantum advantages are unlikely for optimization on a noisy intermediate-scale quantum device. Therefore, we focus on long-term algorithms assuming FTQC in this paper.

The remainder of this paper is organized as follows. Section II is a review of important related works, while in Section III, we introduce the conventional GAS and its modification to support real-valued coefficients. In Section IV, a method to solve MIMO MLD on a quantum computer is proposed, and algebraic and numerical evaluations are given in Section V. Finally, in Section VI, we conclude this paper. Italicized symbols represent scalar values, and bold symbols represent vectors and matrices. Table I summarizes a list of important mathematical symbols used in this paper.

II. RELATED WORKS

Quantum computation has the potential to break through the fundamental trade-off between performance and complexity. Hence, it has been applied to multi-user detection [10, 13–15, 17, 28, 29], multiple symbol differential detection [16], channel coding [30, 31], wireless routing [18, 19], indoor localization [20], intelligent reflecting surfaces [32], and code-word optimization problem [25]. In this section, we introduce important related works targeting detection problems in wireless communications.

A. Multi-User Detection Using DH Algorithm [13]

Botsinis *et al.* proposed a novel method of applying the DH algorithm to multi-user detection [13], which is a detection problem for multi-user scenarios. The original DH algorithm [12] is terminated if the sum of the number of Grover iterations becomes greater than or equal to $22.5\sqrt{N}$, where N denotes the search space size. By contrast, Botsinis *et al.* modified the

algorithm to terminate early for an arbitrary number of queries smaller than $22.5\sqrt{N}$. Additionally, the modified algorithm calculates the output of a low-complexity detector, such as the zero-forcing (ZF) or minimum mean square error (MMSE) detector, and exploits the output as an initial value to sample better states. Both contributions are innovative in that they accelerate the quantum algorithm more for a specific problem in wireless communications.

The objective function presented in [13] involves a Frobenius norm of complex-valued variables. However, the quantum circuit that evaluates the norm is idealized as an oracle, and no specific construction method is considered. Unlike in [13], we consider specific quantum circuits and analyze their hardware and query complexities, which is the missing piece in the literature.

B. MIMO MLD Using QA [28]

Kim *et al.* formulated MIMO MLD as a QUBO problem and solved it using QA, the D-Wave 2000Q quantum annealer [28]. Specifically, binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK) symbols are represented as first-order functions with respect to information bits, while gray-coded 16 quadrature amplitude modulation (QAM) symbols are represented as second-order functions. Since the objective function of MLD contains the squared norm, it may result in a higher-order function such as fourth, eighth, or higher, which is not supported by QA. To solve this problem, Kim *et al.* used first-order functions that represent higher-order modulation, such as 16-QAM or 64-QAM, without the Gray coding. Then, the objective function contains first- and second-order terms only. To achieve performance equivalent to that of the Gray-coded case, the projection between before and after Gray coding is used on a classical computer. That is, encoding at the transmitter and decoding at the receiver require additional steps.

Unlike in the above study [28] targeting QA, we directly handle the Gray-coded data symbols specified in the 5G standard owing to the proposed real-valued GAS that supports higher-order terms. Our approach is capable of supporting any signal modulation, such as star-QAM and constellation shaping schemes, as long as data symbols can be represented as a function of information bits.

C. MIMO MLD Using DH Algorithm [29]

Mondal *et al.* proposed a method to solve MIMO MLD using the DH algorithm [29]. Specifically, to improve the success probability of the algorithm, the uniform selection of the number of Grover operators, L, was modified to a random value from the Gamma distribution, leading to a better selection of L. Here, the Gamma distribution depends on a scale parameter, and the scale parameter depends on the exact number of solutions to be marked. Since the exact number of solutions varies dynamically depending on the threshold, the quantum counting algorithm [33] is crucial, as stated in [29]. Additionally, the concept of reducing the search space was verified.

As in [13], a specific construction method for a quantum circuit is not considered in [29]. Herein, we determine a threshold in accordance with the distribution of objective function values, which is known in advance.

III. GROVER ADAPTIVE SEARCH (GAS)

GAS [8] supports binary optimization problems with integer coefficients, including QUBO and HUBO problems. It requires n qubits for n binary variables $\mathbf{b} \in \mathbb{B}^n$ and m qubits for encoding the objective function value $E(\mathbf{b}) \in \mathbb{Z}$, resulting in a circuit equipped with $n + m$ qubits. Here, $E(\mathbf{b})$ is an arbitrary polynomial function, such as $E(\mathbf{b}) = 1 + b_0 - 2b_1 b_2$. The classic exhaustive search requires $O(2^n)$ queries, while GAS requires $O(\sqrt{2^n})$ queries, which potentially provides a quadratic speedup. GAS obtains a global minimum solution by amplifying the states in which the objective function value $E(\mathbf{b})$ is smaller than the current threshold $y_i \in \mathbb{Z}$. Here, y_i is a temporal minimum and i is an iteration count in CD. We measure the quantum states and update the threshold, which is repeated until a termination condition is satisfied.

Before executing GAS, it is not a straightforward task to determine an appropriate number of qubits m. The objective function value is expressed by the two's complement representation. This is because positive or negative can be identified simply by focusing on the beginning of m qubits, and this representation simplifies the quantum circuit to the identification of the states of interest that should be amplified. Let the objective function value or its coefficient be an integer k. Then, m must satisfy [8]

$$-2^{m-1} \le k < 2^{m-1}. \tag{1}$$

As the threshold y_i is updated in each iteration of GAS, the calculated value may become $E(\mathbf{b}) - y_i$, which results in a smaller minimum value or a larger maximum value. Thus, it is necessary to set a sufficient m that might handle $E_{\max}$, $E_{\min}$, and $E_{\max} - E_{\min}$ without overflow, where $E_{\max}$ and $E_{\min}$ are the maximum and minimum of $E(\mathbf{b})$, respectively. For example, when we have $E_{\max} = 8$ and $E_{\min} = -6$, the maximum of $E(\mathbf{b}) - y_i$ may become $E_{\max} - E_{\min} = 8 - (-6) = 14$, and $m = 5$ is sufficient to represent the values of $E(\mathbf{b}) - y_i$.

A. Conventional GAS for Integer QUBO [8]

We review a specific construction method for the quantum circuit used in GAS. First, a state preparation operator $\mathbf{A}_{y_i}$ is constructed, in which an n-qubit input register is transformed into the equal superposition of all states and an m-qubit input register is used to represent the corresponding value $E(\mathbf{b}) - y_i$. Taking the binary variable $\mathbf{b}$ as a binary number and converting it to a decimal number b, the state should be [8]

$$\mathbf{A}_{y_i} |0\rangle_n |0\rangle_m = \frac{1}{\sqrt{2^n}} \sum_{b=0}^{2^n-1} |b\rangle_n |E(b) - y_i\rangle_m. \tag{2}$$

This operator $\mathbf{A}_{y_i}$ can be composed of the Hadamard gates $\mathbf{H}$, controlled unitary operators $\mathbf{U}_G(\theta)$, and the inverse quantum

Fig. 1. Quantum circuit corresponding to $E(\mathbf{b}) = 1 + b_0 - 2b_1b_2$.

(a) $L = 0$.   (b) $L = 1$.   (c) $L = 2$.

Fig. 2. Output probabilities of the circuit shown in Fig. 1

Fourier transform (IQFT). Let k be a constant term in the objective function. The noncontrolled unitary operator $\mathbf{U}_G(\theta)$ is defined such that [8]

$$\mathbf{U}_G(\theta)\mathbf{H}^{\otimes m}\ket{0}_m = \frac{1}{\sqrt{2^m}}\sum_{l=0}^{2^m-1} e^{jl\theta}\ket{l}_m, \qquad (3)$$

where we have $\theta = 2\pi k/2^m$. That is, it is constructed by

$$\mathbf{U}_G(\theta) = \mathbf{R}(2^{m-1}\theta) \otimes \mathbf{R}(2^{m-2}\theta) \otimes \cdots \otimes \mathbf{R}(2^0\theta) \qquad (4)$$

and the phase gate

$$\mathbf{R}(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\theta} \end{bmatrix}. \qquad (5)$$

Here, phase advance represents integer addition and phase delay represents subtraction. Following (3), IQFT yields only one state that represents the original integer value of k.

The interaction between a binary variable and a coefficient can be represented by a controlled qubit. Similarly, the interaction between binary variables can be represented by controlled qubits on a register $\ket{b}_n$. As exemplified in Fig. 1, the constant term $+1$ corresponds to $\mathbf{U}_G(\pi/4)$, the term $+1b_0$ corresponds to controlled $\mathbf{U}_G(\pi/4)$, and the term $-2b_1b_2$ corresponds to controlled $\mathbf{U}_G(-2\pi/4)$. Likewise, higher-order terms, such as third or fourth order, can be represented by increasing the number of controlled qubits.

In the classic Grover search [4], an oracle operator $\mathbf{O}$ identifies the states of interest and inverts the phases of these states. Only the inverted states are amplified by the Grover operator. The operator $\mathbf{A}_{y_i}$ above calculates the values

Algorithm 1 Conventional GAS designed for integer coefficients [8].

Input: $E: \mathbb{B}^n \rightarrow \mathbb{Z}, \lambda = 8/7$
Output: b
1: Uniformly sample $\mathbf{b}_0 \in \mathbb{B}^n$ and set $y_0 = E(\mathbf{b}_0)$.
2: Set $k = 1$ and $i = 0$.
3: **repeat**
4:    Randomly select the rotation count L_i from the set $\{0, 1, ..., \lceil k-1 \rceil\}$.
5:    Evaluate $\mathbf{G}^{L_i}\mathbf{A}_{y_i}\ket{0}_{n+m}$, and obtain $\mathbf{b}$ and y. {Grover search}
6:    **if** $y < y_i$ **then**
7:       $\mathbf{b}_{i+1} = \mathbf{b}, y_{i+1} = y$, and $k = 1$. {Improvement found}
8:    **else**
9:       $\mathbf{b}_{i+1} = \mathbf{b}_i, y_{i+1} = y_i$, and $k = \min\{\lambda k, \sqrt{2^n}\}$. {No Improvement}
10:   **end if**
11:   $i = i + 1$.
12: **until** a termination condition is met.

$E(\mathbf{b}) - y_i$ for all 2^n states in parallel. Here, states that are better than the current threshold y_i, i.e., states that satisfy $E(\mathbf{b}) - y_i < 0$, should be marked to find the minimum solution. Since the calculated values are represented by the two's complement, we can identify the negative states by focusing only on the beginning of the m qubits, and $\mathbf{O}$ can be constructed by applying the Z-gate only to that qubit.

Let the Grover diffusion operator be $\mathbf{D}$ of [4]

$$D_{i,j} = \begin{cases} 0 & (i \neq j) \\ 1 & (i = j = 0) \\ -1 & (i = j \neq 0) \end{cases}. \qquad (6)$$

The Grover operator is finally constructed by $\mathbf{G} = \mathbf{A}_{y_i}\mathbf{D}\mathbf{A}_{y_i}^{\mathrm{H}}\mathbf{O}$, and we evaluate $\mathbf{G}^L\mathbf{A}_{y_i}\ket{0}_{n+m}$, which will maximize the amplitudes of the states of interest. The ideal L that successfully maximizes the amplitude is given by [34]

$$L_{\mathrm{opt}} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{N_s}} \right\rfloor, \qquad (7)$$

where N denotes the search space size, 2^n, and N_s denotes the number of solutions. Let $\mathbf{b}$ be the bit sequence and y be the objective function value obtained by the evaluation.

From (7), the query complexity of GAS can be derived as $O(\sqrt{2^n})$ [8] in the quantum domain (QD), which is the total number of Grover operators. Since N_s, the number of states better than the current threshold, is unknown in advance, L is typically drawn from a uniform distribution ranging from 0 to a specific value that increases by a factor of $\lambda = 8/7$ at each iteration. GAS is terminated if the sum of the Grover operators is greater than $22.5\sqrt{2^n}$, which is the same as the conventional DH algorithm. In the Qiskit implementation, the number of times no improvement is observed is also considered as one of the termination conditions. Overall, GAS is summarized in Algorithm 1.

As a specific example, Fig. 1 shows a quantum circuit of GAS that tries to minimize the objective function $E(\mathbf{b}) = 1 + b_0 - 2b_1b_2$, where the threshold of $y_i = 0$ and $\mathbf{A}_{y_i=0}$ are considered for simplicity. The upper $n = 3$ qubits correspond to variables $|b_0\rangle$, $|b_1\rangle$, and $|b_2\rangle$, and the lower $m = 3$ qubits $|z\rangle_3$ encode the calculated value. The Hadamard gate at the beginning of $\mathbf{A}_{y_i=0}$ initializes the qubits and creates an equal superposition of all the possible states, 000000 to 111111. The black circle in Fig. 1 indicates a control qubit. The unitary operator $\mathbf{U}_G(\theta)$ is applied if all the associated control qubits are 1. Here, the control qubit is in a superposition state, and it creates a quantum entanglement state, which plays a key role in GAS. IQFT is applied at the last part of $\mathbf{A}_{y_i=0}$. After that, the Grover operator $\mathbf{G}$ is applied L times, and we measure the quantum state. Fig. 2 shows the probability that each state is measured, where the number of Grover operators was varied from $L = 0$ to 2. The comma-separated text in this figure shows n and m qubits, and the latter is converted to a decimal number. As shown in Fig. 2, when $L = 0$, $2^3 = 8$ different states were observed with equal probability, and the corresponding values of the objective function were correctly calculated, demonstrating the potential of quantum computation. When $L = 1$ and 2, only the state of interest $\mathbf{b} = [0 \ 1 \ 1]$, which yields $E(\mathbf{b}) = -1 < 0$, was successfully amplified by the Grover operator. In this manner, GAS amplifies the states that are better than the current threshold and finds a binary solution that minimizes the objective function.

B. Handling of Real-Valued Coefficients [8]

A polynomial may contain real-valued coefficients. To deal with real-valued coefficients, Gilliam *et al.* proposed the following two methods [8].

1) Integer Approximation: Multiplying the objective function by a positive constant does not affect the minimization process. A real-valued coefficient can be approximated by multiplying a large number and rounding down to an integer. Specifically, real coefficients are approximated as fractions with a common denominator, the denominator is multiplied to the objective function, and the numerators become approximated integer coefficients. As can be inferred from (1), the drawback is that the number of required qubits m increases as the value range of the objective function expands. If m is kept small, this approximation becomes less accurate.

2) Direct Encoding: In this method, an integer k in $\theta = 2\pi k/2^m$ of (3) is replaced with a real-valued coefficient $a \in \mathbb{R}$. Then, the output probability indicates multiple integers, which is known as the Fejér distribution. Specifically, the state $\mathbf{U}_{\text{Fejér}}(\theta)|0\rangle_m$ after applying IQFT to $\mathbf{U}_G(\theta)\mathbf{H}^{\otimes m}|0\rangle_m$ is given by [8][4]

$$\mathbf{U}_{\text{Fejér}}(\theta)|0\rangle_m = \sum_{l=0}^{2^m-1} \langle \mathbf{g}(\theta), \mathbf{g}(2\pi l/2^m)\rangle |l\rangle, \quad (8)$$

[4]This definition differs from [8], but is essentially identical.

Algorithm 2 Proposed GAS designed for real-valued coefficients.

Input: $E : \mathbb{B}^n \to \mathbb{R}, \lambda = 8/7$
Output: $\mathbf{b}$
1: Uniformly sample $\mathbf{b}_0 \in \mathbb{B}^n$ and set $y_0 = E(\mathbf{b}_0)$. {This step will be improved in Section IV-C}
2: Set $k = 1$ and $i = 0$.
3: **repeat**
4:      Randomly select the rotation count L_i from the set $\{0, 1, ..., \lceil k-1 \rceil\}$.
5:      Evaluate $\mathbf{G}^{L_i}\mathbf{A}_{y_i}|0\rangle_{n+m}$, and obtain $\mathbf{b}$.
6:      Evaluate $y = E(\mathbf{b})$ in CD. {This is the additional step}
7:      **if** $y < y_i$ **then**
8:          $\mathbf{b}_{i+1} = \mathbf{b}, y_{i+1} = y$, and $k = 1$.
9:      **else**
10:         $\mathbf{b}_{i+1} = \mathbf{b}_i, y_{i+1} = y_i$, and $k = \min\{\lambda k, \sqrt{2^n}\}$.
11:      **end if**
12:      $i = i + 1$.
13: **until** a termination condition is met.

---

where we have $\theta = 2\pi a/2^m$ and $\mathbf{g}(\theta) = [1, e^{j\theta}, \cdots, e^{j(2^m-1)\theta}]/\sqrt{2^m}$. The number of qubits m must satisfy [8]

$$-2^{m-1} \le a < 2^{m-1}. \quad (9)$$

In this distribution, the probabilities of two integers close to a given real number a are greater than the other probabilities. For example, if $m = 3$ qubits and $a = -2.5$, from (8), -2 and -3 are observed with equal probability. If $a = -2.3$, -2 is observed more frequently than -3.

C. Proposed GAS for Real-Valued HUBO

As previously reviewed in Section III-B, in their innovative study [8], Gilliam *et al.* proposed two methods for handling real-valued coefficients, but did not specifically investigate how GAS behaves in the case of direct encoding. In such a case, in our evaluation, GAS samples a wrong value of the objective function, which obeys the Fejér distribution. For example, if the objective function value is -2.5, we may observe an integer value less than or equal to -3. A value lower than the actual value is updated as the minimum and set as a new threshold y_i. Then, no states satisfy $E(\mathbf{b}) - y_i < 0$, and one of all states is randomly sampled. As a result, GAS will not be able to obtain an optimal solution.

A possible solution here is that we ignore y evaluated in QD. Instead, we use $\mathbf{b}$ returned by GAS and calculate a correct objective function value $y = E(\mathbf{b})$ in CD. Since the quantum circuit using the direct encoding amplifies the states of interest with high probability, with this simple modification, GAS obtains an optimal solution correctly. Overall, the above procedure is summarized in Algorithm 2.

We have two major drawbacks. First, Algorithm 2 increases query complexity in CD, although the asymptotic order remains the same. Second, the probability amplification may not be sufficient, which is illustrated in Fig. 4.

Fig. 3. Quantum circuit corresponding to $E(\mathbf{b}) = 1 + b_0 - 1.8b_1b_2b_3$.

(a) $L = 0$.   (b) $L = 1$.   (c) $L = 2$.   (d) $L = 3$.

Fig. 4. Output probabilities of the circuit shown in Fig. 3, where only the top 16 states are shown.

As a specific example, Fig. 3 shows a quantum circuit corresponding to the objective function $E(\mathbf{b}) = 1 + b_0 - 1.8b_1b_2b_3$, where we set $n = 4$ and $m = 3$. Since we used the direct encoding method, $-1.8b_1b_2b_3$ was represented as $\mathbf{U}_G(-1.8\pi/4)$, and it was associated with three qubits $|b_1\rangle$, $|b_2\rangle$, and $|b_3\rangle$. Additionally, Fig. 4 shows the output probabilities of Fig. 3, where only the top 16 states are shown for the sake of readability. As given in (8), the direct encoding method may not result in a unique integer. For example, the states $(0111, -1)$ and $(0111, -2)$ had positive probabilities in Fig. 3. The state of interest here is $\mathbf{b} = [0\ 1\ 1\ 1]$ and $E(\mathbf{b}) = 1 - 1.8 = -0.8 < 0$. That is, before amplitude amplification, at $L = 0$, integers close to the real value are observed, and after amplification, at $L > 0$, the negative states are observed with high probabilities. As shown in Fig. 4(d), the states $(0111, -1)$ and $(0111, -2)$ were amplified as the number of Grover operators L increased, while the wrong state $(0111, -2)$ was observed with a lower probability than $(0111, -1)$. Another wrong state $(1111, -1)$ was also observed with a low probability. This is the reason why the correction of the objective function value is required for real-valued GAS, as summarized in Algorithm 2.

D. Evaluation Metrics

In the literature, a quantum circuit has been evaluated by the numbers of qubits and gates and its depth, while a quantum algorithm has been evaluated by query complexity.

Fig. 5. System model for MIMO with $N_{\rm t}$ transmit and $N_{\rm r}$ receiver antennas.

1) Numbers of Qubits and Gates and Depth: The size of the quantum circuit determines its feasibility. As the numbers of qubits and gates in a quantum circuit increase, more advanced quantum computation becomes possible. At the same time, however, it becomes more susceptible to noise and more difficult to implement in hardware. In our evaluations, the number of required qubits is represented as $n + m$, and the number of quantum gates is derived as a function with respect to n and m.

2) Query Complexity [13]: To investigate query complexity, we count how many times the objective function is queried. Specifically, the query complexity in the classical domain (CD) is the number of times the objective function is evaluated, i.e., i in Algorithm 1. By contrast, the query complexity in the quantum domain (QD) is the number of times the Grover operator $\mathbf{G}$ is applied, i.e., $L_0 + L_1 + \cdots + L_i$ in Algorithm 1. The definitions of query complexities in CD and QD are the same as those used in [13].

IV. QUANTUM SPEEDUP FOR MIMO MLD

Conventional studies on quantum-assisted wireless communications have not considered a specific construction method of the quantum circuit. In many cases, the circuit to calculate an objective function has been idealized as a black-box quantum oracle. In this section, we formulate the MIMO MLD as a new real-valued HUBO problem, which can be represented by a quantum circuit, as described in Section III. We also analyze the probability distribution of the objective value for enabling further speedup.

A. System Model

We consider a MIMO communication scenario with $N_{\rm t}$ transmit antennas and $N_{\rm r}$ receive antennas, as illustrated in Fig. 5. The input n-bit sequence $\mathbf{b} = [b_0\ b_1\ \cdots\ b_{n-1}] \in \mathbb{B}^n$ is mapped to a symbol vector $\mathbf{s} = [s_0\ s_1\ \cdots\ s_{N_{\rm t}-1}] \in \mathbb{C}^{N_{\rm t}\times 1}$, where s_t for $0 \leq t \leq N_{\rm t} - 1$ denotes a Gray-coded data symbol specified in 5G NR [35]. We represent this bit-to-symbol mapper as $\mathbf{s} = M(\mathbf{b}) = M(b_0, \cdots, b_{n-1})$, which will be defined in detail in Section IV-B. The baseband received symbols $\mathbf{r} \in \mathbb{C}^{N_{\rm r}\times 1}$ is given by

$$\mathbf{r} = \frac{1}{\sqrt{N_{\rm t}}}\mathbf{H}_{\rm c}\mathbf{s} + \sigma\mathbf{v}, \qquad (10)$$

where $\mathbf{H}_\text{c} \in \mathbb{C}^{N_\text{r} \times N_\text{t}}$ denotes the channel matrix, and $\mathbf{v} \in \mathbb{C}^{N_\text{r} \times 1}$ denotes the additive white Gaussian noise. Here, we assume the narrowband Rayleigh flat fading. That is, each element of $\mathbf{H}_\text{c}$, h_{ut}, and each element of $\mathbf{v}$, v_u, follow the standard complex Gaussian distribution $\mathcal{CN}(0,1)$ for $0 \leq u \leq N_\text{r} - 1$ and $0 \leq t \leq N_\text{t} - 1$. The SNR is defined as $\gamma = 1/\sigma^2$ because the symbol vector has the power constraint $\mathrm{E}\left[\|\mathbf{s}/\sqrt{N_\text{t}}\|_\text{F}^2\right] = \mathrm{E}\left[\sum_{t=0}^{N_\text{t}-1} |s_t|^2/N_\text{t}\right] = 1$. The constellation size, or modulation order, is denoted by L_c, and the transmission rate is calculated by

$$n = N_\text{t} \log_2(L_\text{c}) \quad \text{[bit/symbol]}. \tag{11}$$

Corresponding to (10), the ideal MLD is performed as

$$\hat{b}_0, \cdots, \hat{b}_{n-1} = \arg \min_{b_0, \cdots, b_{n-1}} E(b_0, \cdots, b_{n-1}), \tag{12}$$

where we have the objective function

$$E(b_0, \cdots, b_{n-1}) = \left\| \mathbf{r} - \frac{1}{\sqrt{N_\text{t}}} \mathbf{H}_\text{c} M(b_0, \cdots, b_{n-1}) \right\|_\text{F}^2. \tag{13}$$

From (12), the exhaustive search using a classical computer requires the computational time complexity of $O(2^n)$, which is equivalent to the query complexity in CD. Both complexities increase exponentially with the transmission rate n.

To mitigate the exponential complexity, a number of low-complexity detectors have been proposed in the literature. The classic ZF detector uses the pseudo-inverse matrix of

$$\mathbf{W}_\text{ZF} = \begin{cases} (\mathbf{H}_\text{c}^\text{H}\mathbf{H}_\text{c})^{-1}\mathbf{H}_\text{c}^\text{H} & (N_\text{t} \leq N_\text{r}) \\ \mathbf{H}_\text{c}^\text{H}(\mathbf{H}_\text{c}\mathbf{H}_\text{c}^\text{H})^{-1} & (N_\text{t} > N_\text{r}) \end{cases} \tag{14}$$

and enables independent detection of data symbols as

$$\hat{b}_0, \cdots, \hat{b}_{n-1} = M^{-1}(\mathbf{W}_\text{ZF}\mathbf{r}), \tag{15}$$

where $M^{-1}(\cdot)$ denotes the hard-decision symbol-to-bit demapper. Similarly, the MMSE detector uses

$$\mathbf{W}_\text{MMSE} = \begin{cases} (\mathbf{H}_\text{c}^\text{H}\mathbf{H}_\text{c} + \sigma^2\mathbf{I})^{-1}\mathbf{H}_\text{c}^\text{H} & (N_\text{t} \leq N_\text{r}) \\ \mathbf{H}_\text{c}^\text{H}(\mathbf{H}_\text{c}\mathbf{H}_\text{c}^\text{H} + \sigma^2\mathbf{I})^{-1} & (N_\text{t} > N_\text{r}) \end{cases} \tag{16}$$

and obtains

$$\hat{b}_0, \cdots, \hat{b}_{n-1} = M^{-1}(\mathbf{W}_\text{MMSE}\mathbf{r}). \tag{17}$$

An MMSE-based interference cancelation method has been adopted in typical wireless standards such as 5G NR. The performance of a ZF or MMSE detector is worse than that of MLD. In general, low-complexity detectors improve complexity at the sacrifice of performance.

The above system model and detectors are typical and common in the field of wireless communications. Since we consider a general MIMO system, the simulation results given in this paper are the same as those for a multicarrier scenario without inter-subcarrier interference or an uplink multi-user scenario in which N_t single-antenna user terminals transmit their symbols and these symbols are received simultaneously at a base station equipped with N_r antennas.

Fig. 6. Constellation for Gray-coded data symbols specified in the 5G NR standard [35]

B. Proposed Method to Transform MLD into HUBO

As described in Section III, the proposed GAS is capable of solving a real-valued HUBO problem. We transform the objective function of MIMO MLD (13) into a HUBO problem. Specifically, we use the relationship between transmission bits and data symbols, which is specified in the 5G NR standard [35]. The input n-bit sequence is denoted by $\mathbf{b} = [b_0 \; b_1 \; \cdots \; b_{n-1}] \in \mathbb{B}^n$ and the symbol vector is denoted by $\mathbf{s} = [s_0 \; s_1 \; \cdots \; s_{N_\text{t}-1}] \in \mathbb{C}^{N_\text{t}}$. Then, BPSK symbols $\mathbf{s} = M_2(\mathbf{b})$ are generated by [35]

$$s_t = \frac{1}{\sqrt{2}}[(1 - 2b_t) + j(1 - 2b_t)] \tag{18}$$

and QPSK symbols $\mathbf{s} = M_4(\mathbf{b})$ are generated by [35]

$$s_t = \frac{1}{\sqrt{2}}[(1 - 2b_{2t}) + j(1 - 2b_{2t+1})]. \tag{19}$$

Furthermore, 16-QAM symbols $\mathbf{s} = M_{16}(\mathbf{b})$ are generated by [35]

$$s_t = \frac{1}{\sqrt{10}}(1 - 2b_{4t+0})[2 - (1 - 2b_{4t+2})]$$
$$+ \frac{j}{\sqrt{10}}(1 - 2b_{4t+1})[2 - (1 - 2b_{4t+3})] \tag{20}$$

and 64-QAM symbols $\mathbf{s} = M_{64}(\mathbf{b})$ are generated by [35]

$$s_t = \frac{1}{\sqrt{42}}(1 - 2b_{6t+0})[4 - (1 - 2b_{6t+2})[2 - (1 - 2b_{6t+4})]]$$
$$+ \frac{j}{\sqrt{42}}(1 - 2b_{6t+1})[4 - (1 - 2b_{6t+3})[2 - (1 - 2b_{6t+5})]]. \tag{21}$$

A similar relationship for 256-QAM is defined in [35] and its extension for higher modulation orders can be defined easily. Overall, Fig. 6 shows the Gray-coded data symbols defined by (18), (19), and (20).

Our proposed objective function is obtained by substituting $M(\cdot)$ in (13) with (18), (19), (20), or (21), which contains n number of binary variables $b_0, \cdots, b_{n-1}$. In the cases of BPSK and QPSK, our objective function results in a quadratic form since both symbols are represented by a linear relationship and the MLD (12) contains the square of the Frobenius norm. In the case of 16-QAM, the objective function results in a quartic form since the symbols are represented by a quadratic relationship. Similarly, the objective function results in a sextic form in the 64-QAM case.

The use of data symbols specified in 5G NR is not straight-forward since the objective function inevitably contains higher-order terms if the modulation order is 16 or higher. Thus, in this form, the conventional QA requires a transformation from HUBO to QUBO, and this transformation involves an increase in binary variables, making the problem more difficult. Our proposed approach is only possible with the aid of the real-valued support of GAS. Because of GAS, the query complexity is expected to be reduced from $O(2^n)$ to $O(\sqrt{2^n})$.

The structure of the proposed objective function depends only on the number of transmit antennas, N_t, the number of receive antennas, N_r, and the modulation order, L_c. The coefficients in the objective function change depending on the channel matrix $\mathbf{H}_c$. The calculation cost of coefficients determines the complexity of classical processing required before executing GAS, which relates to the latency of the algorithm. If we approximate the computational complexity as the number of real-valued multiplications, the largest burden is the product of channel coefficients, such as $h_{00}h_{01}^*$. The total number of multiplications is calculated as $4N_r N_t(N_t-1)/2 = O(N_r N_t^2)$, which is sufficiently small with respect to the detection complexity.

Example (QPSK): As a specific example, we consider the QPSK case (19) with $N_t = N_r = 2$. The objective function of (13) can be transformed into

$$
\begin{aligned}
&E(b_0, b_1, b_2, b_3) \\
=&2\sum_{u=0}^{1}\sum_{t=0}^{1}(\mathrm{Re}(h_{ut}r_u^*)b_{2t} - \mathrm{Im}(h_{ut}r_u^*)b_{2t+1}) \\
&+2a_1(b_0b_2 + b_1b_3) + 2a_2(b_0b_3 - b_1b_2) \\
&-(a_1+a_2)(b_0+b_3) - (a_1-a_2)(b_1+b_2),
\end{aligned}
\tag{22}
$$

where we have $a_1 = \mathrm{Re}(h_{00}h_{01}^*) + \mathrm{Re}(h_{10}h_{11}^*)$ and $a_2 = \mathrm{Im}(h_{00}h_{01}^*) + \mathrm{Im}(h_{10}h_{11}^*)$. This function (22) is in a quadratic form.

Example (16-QAM): Additionally, Fig. 7 exemplifies a specific quantum circuit for the 16-QAM case with $N_t = N_r = 2$, where we have $n = 8$ qubits for binary variables, $m = 5$ qubits for real-valued encoding, random channel coefficients

$$
\begin{aligned}
\mathbf{H}_c = [&[0.748510757437062 - 0.014877263039446401j, \\
&1.3215983896521515 + 0.06298233870206783j], \\
&[0.6371630706424066 - 0.14262155021296025j, \\
&-0.3888005272494009 - 0.15170387681055802j]],
\end{aligned}
\tag{23}
$$

and the original information bits of 00110101. As shown in Fig. 7, the objective function results in a quartic form: $E(\mathbf{b}) = 1.22b_0b_2b_4b_6 + 0.61b_0b_2b_4 + \cdots$ using (13) and (20). As an example, the coefficient of $b_0b_2b_4b_6$ is calculated as $\frac{1}{2} \cdot \frac{4}{\sqrt{10}} \cdot \frac{4}{\sqrt{10}}(h_{00}h_{01}^* + h_{00}^*h_{01} + h_{10}h_{11}^* + h_{10}^*h_{11}) = 1.22$, which is rounded down to the second decimal place for simple illustration.

C. Proposed Threshold for Further Speedup

GAS obtains a global minimum solution by updating the threshold value y_i and amplifying the probability amplitudes

corresponding to values smaller than the threshold. The query complexity can be reduced by setting the initial threshold in a manner different from that in classic random sampling, although the asymptotic performance may not change. In this section, we derive the probability distribution of the objective function value and use it to determine a strict threshold, which enables further speedup.

If the information bits in (13) are estimated correctly, the minimum value of (13) is the Frobenius norm of additive noise $\mathbf{v} \in \mathbb{C}^{N_r \times 1}$ as follows:

$$
E_{\min} = \underbrace{\sigma^2}_{\text{known}} \underbrace{\sum_{u=0}^{N_r-1} |v_u|^2}_{\text{unknown}}.
\tag{24}
$$

That is, $E_{\min}$ depends on the noise variance σ^2, which is typically known at the receiver, and instantaneous noise v_u, which is unknown in any case. Since the noise is assumed to follow the complex Gaussian distribution, the magnitude of the norm follows the Rayleigh distribution, and its square follows the exponential distribution. As a result, $E_{\min}$ in (24) follows the Erlang distribution, whose probability density function is

$$
f(y) = \frac{\gamma^{N_r} y^{N_r-1} e^{-\gamma y}}{(N_r-1)!},
\tag{25}
$$

where we have SNR $\gamma = 1/\sigma^2$. The corresponding cumulative distribution function (CDF) is given by

$$
F(y) = \Pr[Y \le y] = 1 - e^{-\gamma y} \sum_{u=0}^{N_r-1} \frac{(\gamma y)^u}{u!}.
\tag{26}
$$

As an example, if we consider the case with $N_r = 2$, the CDF is calculated as

$$
F(y) = \Pr[Y \le y] = 1 - e^{-\gamma y}(1 + \gamma y)
\tag{27}
$$

from (26). Fig. 8 exemplifies CDF (27) when SNR is varied as $\gamma = 5$ to 20 dB. Additionally, the CDF of the simulated objective function values with $N_t = 2$ and QPSK is also plotted. As shown in Fig. 8, if the SNR is sufficient, such as above 10 dB, the theoretical and simulated values are identical. Thus, it is possible to know in advance that the minimum value to be calculated is below a certain threshold, which can be determined with a very high degree of certainty. Given an SNR γ, theoretical values of (26) can be used to determine a strict threshold.

From (26), the probability that the threshold y is below the minimum value is

$$
\Pr[Y > y] = e^{-\gamma y}(1 + \gamma y).
\tag{28}
$$

Let $\tilde{y}$ be the threshold to be determined and P be a small constant probability, such as $P = 10^{-3}$ and 10^{-4}. Replacing y and $\Pr[Y > y]$ in (28) with $\tilde{y}$ and P yields

$$
P = e^{-\gamma \tilde{y}}(1 + \gamma \tilde{y}).
\tag{29}
$$

Dividing both sides by $-e$ gives

$$
-\frac{P}{e} = -(1 + \gamma \tilde{y})e^{-(1+\gamma \tilde{y})}.
\tag{30}
$$

Fig. 7. Quantum circuit corresponding to objective function of 16-QAM detection.

Fig. 8. Cumulative distribution of the minimum of objective function values (27).

Then, using the Lambert W function, we obtain

$$W_{-1}\left(-\frac{P}{e}\right) = -(1 + \gamma\tilde{y}) = -\left(1 + \frac{\tilde{y}}{\sigma^2}\right), \quad (31)$$

where $W_{-1}(\cdot)$ denotes the lower branch of the Lambert W function, i.e., $W_{-1}(\cdot) \le -1$ and $W_{-1}(-1/e) = -1$. Finally, the threshold to be determined is

$$\tilde{y} = \underbrace{\sigma^2}_{\text{known}} \underbrace{\nu}_{\text{known}}, \quad (32)$$

which is similar to (24), and

$$\nu = -1 - W_{-1}\left(-\frac{P}{e}\right). \quad (33)$$

Here, ν is a positive constant and is calculated once before running our proposed algorithm. For example, we have $\nu = 9.23$ if $P = 10^{-3}$ and $\nu = 11.8$ if $P = 10^{-4}$.

For further speedup, we opt to use the output of the MMSE detector (16). In [13], Botsinis *et al.* proposed the MMSE-based threshold of

$$\bar{y} = E(\bar{\mathbf{b}}_0), \quad (34)$$

where we have a rough estimate $\bar{\mathbf{b}}_0 = M^{-1}(\mathbf{W}_{\text{MMSE}}\mathbf{r})$. Our proposed threshold $\tilde{y}$, which is simpler than $\bar{y}$, can be used together with $\bar{y}$. Specifically, we calculate both $\tilde{y}$ and $\bar{y}$ at the beginning of Algorithm 2, set the initial threshold as the

smaller of the two, and initialize the first solution with $\bar{\mathbf{b}}_0$. Let $\mathbf{b}_0$ be a random n-bit sequence. The initial threshold used for the proposed Algorithm 2 can be summarized as follows:

$$y_0 = \begin{cases} E(\mathbf{b}_0) & \text{(Original GAS [8])} \\ \bar{y} & \text{(MMSE-based threshold [13])} \\ \tilde{y} & \text{(Proposed threshold)} \\ \min(\bar{y}, \tilde{y}) & \text{(Proposed combination)} \end{cases}. \quad (35)$$

One problem with the proposed threshold $\tilde{y}$ and the combination $\min(\bar{y}, \tilde{y})$ is that they may become smaller than the actual minimum. In this case, since there are no states of interest, GAS will be in a state where the solution $\mathbf{b}_i$ in Algorithm 2 is not updated. The probability of this undesirable event occurring is P, i.e.,

$$\Pr[\tilde{y} < E_{\min}] = \Pr[\min(\bar{y}, \tilde{y}) < E_{\min}] = P, \quad (36)$$

because we have the relationship $\Pr[\bar{y} < E_{\min}] = 0$. Then, it can be expected that the proposed threshold $\tilde{y}$ may degrade the bit error ratio (BER) significantly if P is inappropriate. Specifically, the BER of the proposed threshold $\tilde{y}$ is approximated by

$$P \cdot 0.5 + (1 - P) \cdot \text{BER}_{\text{MLD}}, \quad (37)$$

where BER_{MLD} is the BER of MLD. In the proposed combination method, we initialize the first solution with the MMSE output $\bar{\mathbf{b}}_0$. Since the initial threshold $\min(\bar{y}, \tilde{y})$ becomes smaller than the actual minimum with probability P, the BER of the proposed combination method is approximated by

$$P \cdot \text{BER}_{\text{MMSE}} + (1 - P) \cdot \text{BER}_{\text{MLD}}, \quad (38)$$

where BER_{MMSE} is the BER of the MMSE detector. Both (37) and (38) indicate that the design of P exerts no significant effect as long as it is smaller than BER_{MLD}, which can be calculated exactly in a closed form in advance. For our performance analysis, the effect of P is shown in Fig. 13.

V. PERFORMANCE ANALYSIS

In this section, we analyze the number of quantum gates required by GAS, which is represented as a function of the numbers of qubits n and m. Then, we investigate the performance of the proposed formulation in terms of BER and evaluate the proposed algorithm in terms of the rate

of convergence. Here, both integer approximation and direct encoding are considered. Finally, we evaluate the effects of the proposed threshold.

A. Algebraic Analysis of the Number of Quantum Gates

A quantum circuit for GAS is composed of $\mathbf{H}$, $\mathbf{X}$, $\mathbf{Z}$, phase, controlled-phase gates, and the IQFT. In particular, the state preparation operator $\mathbf{A}_{y_i}$ is the most complex part corresponding to the objective function and is dynamically configured in accordance with the threshold y_i. In the quantum circuit $\mathbf{A}_{y_i}$, the number of controlled-phase gates depends on the number of terms in the objective function. We therefore derive the number of terms in the objective function that correspond to each order in an algebraic manner. Ignoring the power scaling factor, the objective function of MIMO MLD (13) is transformed into

$$\sum_{u=0}^{N_{\mathrm{r}}-1} |r_u - h_{u0}s_0 - h_{u1}s_1 - \cdots - h_{u(N_{\mathrm{t}}-1)}s_{N_{\mathrm{t}}-1}|^2$$
$$= \sum_{u=0}^{N_{\mathrm{r}}-1} (r_u - h_{u0}s_0 - h_{u1}s_1 - \cdots - h_{u(N_{\mathrm{t}}-1)}s_{N_{\mathrm{t}}-1})$$
$$\cdot (r_u - h_{u0}s_0 - h_{u1}s_1 - \cdots - h_{u(N_{\mathrm{t}}-1)}s_{N_{\mathrm{t}}-1})^*. \quad (39)$$

Here, we focus on three types of terms: first-order terms such as $-r_0^* h_{00} s_0$ and $-r_0 h_{00}^* s_0^*$, squares of the same symbol such as $|h_{00}|^2|s_0|^2$ and $|h_{01}|^2|s_1|^2$, and products of two symbols such as $h_{00}h_{10}^* s_0 s_1^*$ and $h_{00}^* h_{10} s_0^* s_1$.

For example, in the relatively simple QPSK case, squares of the same symbol result in constant terms because of (19). First-order terms directly result in first-order terms with respect to binary variables. Products between two symbols result in products of binary variables. If $N_{\mathrm{t}} = 2$ and $N_{\mathrm{r}} = 2$, four second-order terms appear: $b_0 b_2$, $b_1 b_3$, $b_0 b_3$, and $b_1 b_2$. The number of corresponding terms is equal to the combination of two choices from N_{t} antennas, e.g.,

$$\binom{N_{\mathrm{t}}}{2} = \frac{N_{\mathrm{t}}(N_{\mathrm{t}} - 1)}{2} = \frac{n(n-2)}{8}, \quad (40)$$

where we have the relationship $n = N_{\mathrm{t}} \cdot \log_2(L_{\mathrm{c}}) = 2N_{\mathrm{t}}$. In total, the number of second-order terms is calculated as $4 \cdot n(n-2)/8 = n(n-2)/2$.

Extending the QPSK case, we counted the number of terms in the objective function for each modulation order and derived the number of quantum gates required by GAS. Table II summarizes the derived results, where the quantum gates were categorized by type. As given in Table II, the number of controlled-phase gates mainly depends on the number of binary variables n. Here, 1-CR represents the controlled-phase gate, and 2-CR, 3-CR, $\cdots$ represent multi-controlled-phase gates. Since we have the relationship $n = N_{\mathrm{t}} \cdot \log_2(L_{\mathrm{c}})$, the quantum circuit becomes increasingly complex depending on the square of the number of antennas N_{t} and the modulation order L_{c}.

We analyze the number of quantum gates in the entire circuit $\mathbf{G}^{L_i} \mathbf{A}_{y_i} |0\rangle_{n+m}$, where we have $\mathbf{G} = \mathbf{A}_{y_i} \mathbf{D} \mathbf{A}_{y_i}^{\mathrm{H}} \mathbf{O}$. In each iteration, the Grover operator is applied L_i times, where L_i is a uniform random number. $\mathbf{O}$ is composed of a single $\mathbf{Z}$

Fig. 9. BER for the QPSK case with $N_{\mathrm{t}} = N_{\mathrm{r}} = 2$.

gate and $\mathbf{D}$ is the Grover diffusion operator, each of which is repeated L_i times. The other part contains $(2L_i + 1)(n + m)$ $\mathbf{H}$ gates, $(2L_i + 1)m$ phase gates, $(2L_i + 1)c$ controlled-phase gates, and $(2L_i + 1)$ IQFT, where c is the number of controlled-phase gates given in Table II. In summary, N_{t} and L_{c} affect the number of gates by the power of two, while m and L_i affect it in direct proportion.

Real quantum computers rely on decomposed elementary gates: single unitary gates and controlled NOT gates [36]. Specifically, a phase gate with c control qubits is decomposed into $O(c)$ elementary gates. Thus, according to Table II, the number of elementary gates required for controlled-phase gates is $O(cn^2 m)$ in total. Additionally, IQFT requires $O(m^2)$ elementary gates [1]. Here, the only parameters that can be designed are n and m. With the aid of our efficient HUBO formulation, the number of qubits n cannot be further reduced, since the search space size of MIMO ML detection is 2^n. Later, we investigate whether our real-valued GAS can reduce m.

B. Effects of Integer Approximation

First, Fig. 9 shows BER of the classic MLD and the proposed formulations that consider the integer approximation with different accuracies. Specifically, the real values were multiplied by 1, 3, 10 or 20, and approximated by rounding them to the nearest integers. As references, the BER curves of ZF, MMSE, and the real-valued formulation were also plotted. To analyze the effects of approximation accuracy, BER values were calculated using the state-of-the-art optimization solver, IBM CPLEX, instead of quantum simulations. As shown in Fig. 9, BER performance varied significantly depending on the accuracy of the conventional integer approximation. High approximation accuracy leads to large integers, resulting in an increase in the number of qubits m. In contrast, the proposed real-valued formulation achieved the same performance as the classic MLD. This observation indicates that the proposed real-valued GAS algorithm must be invoked to solve the MIMO MLD problem on a quantum computer.

Next, Fig. 10 shows the average objective function values when increasing the number of iterations, where iterations in

TABLE II
NUMBER OF QUANTUM GATES REQUIRED FOR $\mathbf{A}_{y_i}$ (n-BIT TRANSMISSION WITH m-BIT ACCURACY)

Gate	BPSK		QPSK		16-QAM		64-QAM	
H	$n+m$	$= O(n+m)$	$n+m$	$= O(n+m)$	$n+m$	$= O(n+m)$	$n+m$	$= O(n+m)$
R	m	$= O(m)$	m	$= O(m)$	m	$= O(m)$	m	$= O(m)$
1-CR	nm	$= O(nm)$	nm	$= O(nm)$	nm	$= O(nm)$	nm	$= O(nm)$
2-CR	$n(n-1)m/2$	$= O(n^2m)$	$n(n-2)m/2$	$= O(n^2m)$	$n(n-3)m/2$	$= O(n^2m)$	$n(n-4)m/2$	$= O(n^2m)$
3-CR	0		0		$n(n-4)m/2$	$= O(n^2m)$	$n(n-6)m+nm/3$	$= O(n^2m)$
4-CR	0		0		$n(n-4)m/8$	$= O(n^2m)$	$5n(n-6)m/6$	$= O(n^2m)$
5-CR	0		0		0		$n(n-6)m/3$	$= O(n^2m)$
6-CR	0		0		0		$n(n-6)m/18$	$= O(n^2m)$
IQFT	1		1		1		1	

(a) QPSK (3x approximation, $n = 4$, $m = 6$ qubits).

(b) 16-QAM (14x approximation, $n = 8$, $m = 8$ qubits).

Fig. 10. Average objective function values with the integer approximation and $N_\mathrm{t} = N_\mathrm{r} = 2$.

both CD and QD were considered. We assumed a sufficiently high SNR and the fixed 2×2 channel matrix given in (23).[5] We used the original GAS with a random initial threshold and terminated the simulation if the objective function value remained the same more than 20 times in CD. In Fig. 10(a), real values were multiplied by 3 and rounded down to integers, and in Fig. 10(b), real values were multiplied by 14 and were approximated. The number of qubits m required for encoding the value $E(\mathbf{b}) - y_i$ was set to an integer sufficient not to overflow, i.e., $m = 6$ in Fig. 10(a) and $m = 8$ in

[5]Note that we observed the same trend for different channel coefficients and SNRs.

Fig. 10(b). Note again that the integer approximation requires more qubits to encode the value. Because quantum simulations with $n+m = 16$ qubits are time-consuming, we fixed the input bits to 00110101 in Fig. 10(b), while the bits were generated randomly in Fig. 10(a). For a clear illustration, we added a constant value to the objective function so that $E_{\min} = 0$. It was observed in Fig. 10(a) that the query complexities of GAS in CD and QD were almost the same as in the exhaustive search of MLD. By contrast, in Fig. 10(b), GAS exhibited better query complexities in both CD and QD than did MLD. That is, the quantum advantage improved as the problem size increased.

C. Effects of Direct Encoding

Similar to Fig. 10, Fig. 11 shows the average objective function values when increasing the number of iterations in CD and QD, where we used direct encoding. The simulation parameters were the same as those used in Fig. 10 except for the real-valued expression and the number of required qubits m. Specifically, the number of qubits $m = 6$ in Fig. 10(a) was reduced to $m = 5$ in Fig. 11(a). Similarly, the number of qubits was reduced from $m = 8$ to $m = 5$ in Fig. 11(b). As shown in Fig. 11, the same trend as in Fig. 10 was observed. The important aspect here is that almost the same query complexities were achieved despite the reduction in the number of required qubits m. Hence, our proposed real-valued GAS is capable of reducing the size of quantum circuits while maintaining a good performance.

Depending on the channel coefficients and noise, the integer approximation requires a different number of qubits. Since both follow the standard Gaussian distribution, the probability of 0 is the highest, and to deal with smaller values, a larger factor must be multiplied to the objective function, resulting in a larger m. By contrast, direct encoding is capable of keeping m constant. The only disadvantage is that the probability amplification of $\mathbf{G}^L$ may become insufficient, which was also demonstrated in Fig. 4.

To investigate the disadvantage of the proposed real-valued GAS and insufficient amplification, in Fig. 12, we generated random channel coefficients and investigated the probability density distribution of the number of queries required to reach the optimal solution, where the parameters were the same as those used in Fig. 10(a) except that m was minimized depending on the random channel coefficients. It was observed in Fig. 12 that query complexities in CD and QD increased compared with the ideal case. Here, the same trend was observed for different SNRs. Albeit at this expense, the proposed

(a) QPSK ($n = 4$, $m = 5$ qubits).

(b) 16-QAM ($n = 8$, $m = 5$ qubits).

Fig. 11. Average objective function values with direct encoding and $N_t = N_r = 2$.

(a) CD.

(b) QD.

Fig. 13. BER transition with respect to the number of iterations, where we used random channel coefficients, QPSK, $N_t = 2$, $N_r = 2$, and SNR = 20 dB.

Fig. 12. Number of queries required to reach the optimal solution.

algorithm could reach the optimal solution in any case. Note that the integer approximation with the same m as in direct encoding could not be plotted in Fig. 12 because it was unable to reach the solution in most cases.

D. Effects of Initial Threshold for Further Speedup

Finally, in Fig. 13, we show the results of evaluating the proposed initial threshold for GAS described in Section IV-C. Here, we averaged BER with random channel coefficients and noise, considered SNR of 20 dB, and assumed idealized quantum circuits to examine the impact of the initial threshold only. Other parameters were the same as those used in Fig. 11(a). Fig. 13(a) shows the number of queries in CD, while Fig. 13(b) shows these in QD. Note that the vertical axis is BER rather than the objective function value. Specifically, at the left end of Fig. 13, BER of 0.5 corresponds to the bit errors between the input bits $\mathbf{b}$ and the random bits $\mathbf{b}_0$, and BER of 6.8×10^{-3} corresponds to the errors between $\mathbf{b}$ and the MMSE output $\bar{\mathbf{b}}_0$. As shown in Fig. 13, in both CD and QD, the proposed threshold, $\tilde{y}$, converged to the optimal solution much faster than the classic random threshold. The slopes in the random and proposed thresholds differed significantly. This is because the random threshold ranged from the best to the worst cases, resulting in slow convergence in some cases. To be more specific, in Fig. 13, the variance of the random threshold $E(\mathbf{b}_0)$ was 14.30 at the first iteration. By contrast, the proposed threshold $\tilde{y}$ is determined by constant factors, P

and SNR, and its variance is always zero. Thus, it significantly improved convergence on average.

It was also found in Fig. 13 that the proposed threshold achieved the best performance for $P = 10^{-4}$ and exhibited lower performance for $P = 10^{-3}$. As described in Section IV-C, P equals the probability that GAS is in a state where the solution is not updated. That is, an event of $\mathrm{BER} = 0.5$ occurred with probability $P = 10^{-3}$, and it resulted in the error floor of BER around 10^{-3}. This result indicates that the parameter P has no significant impact if it is smaller than BER. Since the exact BER at a given SNR can be calculated in a closed form in advance, an appropriate P can also be determined in advance accordingly.

Additionally, in Fig. 13, the proposed threshold combined with the MMSE output achieved a faster convergence compared with the conventional MMSE only case. This improvement was greater for CD than for QD. That is, the proposed threshold is particularly useful for improving the query complexity in CD. This is because it aims to set a strict threshold even in the case of erroneous MMSE output. Errors in MMSE estimation lead to higher objective function values and may increase the number of solutions, which can be avoided by adopting the proposed combination. To be more specific, at the first iteration, the variance of the MMSE-based threshold $\bar{y}$ was $1.58 \cdot 10^{-2}$, while that of the proposed combination $\min(\bar{y}, \tilde{y})$ was much smaller, $3.76 \cdot 10^{-5}$, resulting in the faster convergence. The performance advantage increased upon increasing SNR, which can be verified from the results shown in Fig. 8. As confirmed in Fig. 8, the gap between simulated and theoretical values decreased upon increasing SNR.

In Fig. 13, the conventional GAS using the random threshold exhibited slower convergence than the classic MLD. It can be inferred that this slower convergence was caused by the smaller search space. Since the quadratic speedup is an improvement from $O(2^n)$ to $O(\sqrt{2^n})$, the larger search space leads to the larger reduction. In Fig. 14, we considered the case of 16-QAM, where other parameters were same as those used in Fig. 13. The classic MLD required $16^2 = 256$ iterations to reach the optimal solution in the worst case. As shown in Fig. 14, the conventional MMSE-based threshold exhibited an increase in BER after the first few iterations. This issue is caused because improvements in objective function values may not correspond to improvements in BER in some cases. By contrast, the proposed combination successfully avoided the issue and reached the optimal solution with reduced query complexity. This advantage is expected to increase as the search space size grows, and the proposed approach is especially beneficial for a large-scale MIMO system.

VI. CONCLUSIONS AND FUTURE WORKS

In this paper, we proposed a GAS-based quantum algorithm that supports real-valued HUBO. Then, as an application example, we formulated the MIMO MLD as a HUBO problem. The complexity of MLD exponentially increases with the transmission rate, and low-complexity detectors sacrifice the achievable performance. Unlike in conventional studies, we

(a) CD.

(b) QD.

Fig. 14. BER transition with respect to the number of iterations, where we used random channel coefficients, 16-QAM, $N_\mathrm{t} = 2, N_\mathrm{r} = 2$, SNR = 20 dB, and $P = 10^{-3}$.

constructed specific quantum circuits instead of assuming an idealized quantum oracle. This enabled us to analyze the number of qubits and quantum gates in an algebraic manner. To further accelerate the algorithm, we derived the probability distribution of the objective function value and conceived a unique threshold to sample better states. Assuming FTQC, simulations demonstrated the potential for reducing query complexity in CD and providing a quadratic speedup in QD.

Since this paper focused on a specific construction method for quantum circuits and their algebraic analysis, we considered only the hard-decision MLD, instead of error-correcting codes and soft-decision decoding for classical bits, which are common in wireless standards. The error correction capability improves with increasing code distance and length. For example, the maximum code length of 5G NR is 1024 for polar code and 8448 for LDPC. However, with the current computing resources, it is a challenging task to represent such a large-scale system as a specific quantum circuit. The proposed real-valued GAS can be applied to soft-decision decoding, which will be addressed in our future work.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. Cambridge ; New York: Cambridge University Press, 2010.

[2] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134.

[3] D. E. Knuth, "Big Omicron and big Omega and big Theta," *ACM SIGACT News*, vol. 8, no. 2, pp. 18–24, 1976.

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. Philadelphia, Pennsylvania, United States: ACM Press, 1996, pp. 212–219.

[5] D. Bulger, W. Baritompa, and G. Wood, "Implementing pure adaptive search with Grover's quantum algorithm," *Journal of Optimization Theory and Applications*, vol. 116, pp. 517–529, Mar. 2003.

[6] C. Gidney, "Halving the cost of quantum addition," *Quantum*, vol. 2, p. 74, 2018.

[7] A. Gilliam, M. Pistoia, and C. Gonciulea, "Optimizing quantum search using a generalized version of Grover's algorithm," *arXiv:2005.06468 [quant-ph]*, May 2020.

[8] A. Gilliam, S. Woerner, and C. Gonciulea, "Grover adaptive search for constrained polynomial binary optimization," *Quantum*, vol. 5, p. 428, Apr. 2021.

[9] T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model," *Phys. Rev. E*, vol. 58, pp. 5355–5363, Nov 1998.

[10] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[11] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, 1998.

[12] C. Durr and P. Hoyer, "A quantum algorithm for finding the minimum," *arXiv:quant-ph/9607014*, Jan. 1999.

[13] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 990–1000, Mar. 2014.

[14] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems," *IEEE Access*, vol. 2, pp. 451–472, 2014.

[15] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Transactions on Communications*, vol. 63, no. 10, pp. 3713–3727, Oct. 2015.

[16] ——, "Noncoherent quantum multiple symbol differential detection for wireless systems," *IEEE Access*, vol. 3, pp. 569–598, 2015.

[17] W. Ye, W. Chen, X. Guo, C. Sun, and L. Hanzo, "Quantum search-aided multi-user detection for sparse code multiple access," *IEEE Access*, vol. 7, pp. 52 804–52 817, 2019.

[18] D. Alanis, P. Botsinis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "A quantum-search-aided dynamic programming framework for pareto optimal routing in wireless multihop networks," *IEEE Transactions on Communications*, vol. 66, no. 8, pp. 3485–3500, Aug. 2018.

[19] ——, "Quantum-aided multi-objective routing optimization using back-tracing-aided dynamic programming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7856–7860, Aug. 2018.

[20] P. Botsinis, D. Alanis, S. Feng, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, R. Zhang, and L. Hanzo, "Quantum-assisted indoor localization for uplink mm-wave and downlink visible light communication systems," *IEEE Access*, vol. 5, pp. 23 327–23 351, 2017.

[21] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Coherent versus non-coherent quantum-assisted solutions in wireless systems," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 144–153, Dec. 2017.

[22] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless commu-

nications," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.

[23] K. Fujii, "Noise threshold of quantum supremacy," *arXiv:1610.03632 [quant-ph]*, Oct. 2016.

[24] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021.

[25] N. Ishikawa, "Quantum speedup for index modulation," *IEEE Access*, vol. 9, pp. 111 114–111 124, 2021.

[26] G. Jay, "IBM Quantum roadmap to build quantum-centric supercomputers," https://research.ibm.com/blog/ibm-quantum-roadmap-2025, May 2022.

[27] D. Stilck Franca and R. Garcia-Patron, "Limitations of optimization algorithms on noisy quantum devices," *Nature Physics*, vol. 17, no. 11, pp. 1221–1227, 2021.

[28] M. Kim, D. Venturelli, and K. Jamieson, "Leveraging quantum annealing for large MIMO processing in centralized radio access networks," *Proceedings of the ACM Special Interest Group on Data Communication*, pp. 241–255, Aug. 2019.

[29] 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 Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1688–1698, Feb. 2021.

[30] Z. Babar, Z. B. Kaykac Egilmez, L. Xiang, D. Chandra, R. G. Maunder, S. X. Ng, and L. Hanzo, "Polar codes and their quantum-domain counterparts," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 123–155, 2020.

[31] T. Matsumine, T. Koike-Akino, and Y. Wang, "Channel decoding with quantum approximate optimization algorithm," in *IEEE International Symposium on Information Theory*, Jul. 2019, pp. 2574–2578.

[32] T. Ohyama, Y. Kawamoto, and N. Kato, "Intelligent reflecting surface (IRS) allocation scheduling method using combinatorial optimization by quantum computing," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 3, 2022.

[33] G. Brassard, P. Hoyer, and A. Tapp, "Quantum counting," *arXiv:quant-ph/9805082*, vol. 1443, pp. 820–831, 1998.

[34] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *arXiv:quant-ph/0005055*, vol. 305, pp. 53–74, 2002.

[35] 3GPP, "TS 138 211 - V15.2.0 - 5G; NR; Physical channels and modulation (3GPP TS 38.211 version 15.2.0 Release 15)," 2018.

[36] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995.

Masaya Norimoto (S'22) received the B.E. degree from Yokohama National University, Kanagawa, Japan, in 2022. He is currently pursuing the M.E. degree with the Graduate School of Engineering Science, Yokohama National University, Kanagawa, Japan. His research interests include quantum algorithms and wireless communications.

Ryuhei Mori received the B.E. degree from Tokyo Institute of Technology, Tokyo, Japan in 2008, and the M.Inf. and D.Inf. degrees from Kyoto University, Kyoto, Japan in 2010 and 2013, respectively. From 2013 to 2014, he was a Postdoctoral Fellow at Tokyo Institute of Technology, Tokyo, Japan. He is currently an Assistant Professor of the Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology, Tokyo, Japan. His research interests include quantum information, information theory, computer science and statistical physics.

Naoki Ishikawa (S'13–M'17–SM'22) is an Associate Professor with the Faculty of Engineering, Yokohama National University, Kanagawa, Japan. He received the B.E., M.E., and Ph.D. degrees from the Tokyo University of Agriculture and Technology, Tokyo, Japan, in 2014, 2015, and 2017, respectively. In 2015, he was an academic visitor with the School of Electronics and Computer Science, University of Southampton, UK. From 2016 to 2017, he was a research fellow of the Japan Society for the Promotion of Science. From 2017 to 2020, he was an assistant professor in the Graduate School of Information Sciences, Hiroshima City University, Japan. He was certified as an Exemplary Reviewer of IEEE TRANSACTIONS ON COMMUNICATIONS in 2017 and 2021. His research interests include massive MIMO, physical layer security, and quantum speedup for wireless communications.