Universality of a gate-type quantum computer comprising Controlled-Z and three rotation gates, and its quantum advantage over classical computers

Kiyotaka Hammura[1] and Katsuhiko Yamaguchi[2]

Faculty of Symbiotic Systems Science, Fukushima University,

1 Kanayagawa, Fukushima 960-1296, Japan

Kazuo Sakai[3]

School of Law, Meiji University, 1-9-1 Eifuku, Suginami, Tokyo 168-8555, Japan

(Dated: September 9, 2019)

Abstract

This article deals with algorithmic investigation of a gate-type quantum computer that comprises the following quantum gates: Controlled-Z, $R_x(\phi)$, $R_y(\phi)$ and $R_z(\phi)$ for $\phi = \pm\pi/4, \pm\pi/2, \pi$ (hereinafter *our potential computer*). We investigate two topics. The first topic is to check whether our potential computer is a universal quantum computer or not by reviewing and following the procedures in Nielsen and Chuang[1]. We can confirm that our gate set is equivalent to the ultimate universal set of gates in quantum computing. The availability of the ultimate set makes it possible to construct an arbitrary unitary matrix, the key to implement a universal quantum computer; thus, our potential computer proves to be universal. The second topic is to review to what extent our potential quantum computer could be useful from a viewpoint of its availability to solve a real problem, in comparison to a classical one. We can also confirm that our potential computer can implement *the Deutsch-Jozsa algorithm*[2] (or *DJA* for short). DJA makes it possible to solve a certain problem in much less steps than classical computing; thus, our potential computer is confirmed to possess *quantum advantage*.

CONTENTS

I. INTRODUCTION 57
A. Problems 57
B. Questions/Aims 58
C. Questions/Objectives 58

II. RESULTS 59
A. Universality of our potential computer 59
1. Definition of the gate-type quantum information processing 59
2. A universal set of gates for quantum computation 60
3. Towards the ultimate universal set of gates 60
4. Examination of our potential computer's universality in quantum computing 81
B. Quantum advantage of our potential computer 83
1. Definition of the problem to solve 84
2. How the Deutsch-Jozsa algorithm enables us to solve it in less steps 85
3. Examination of the availability of DJA on our potential computer 88

III. SUMMARY and FUTURE ISSUES 88

A. Derivation of Eq.(77) 89

B. Derivation of Eq.(78) 89

C. Derivation of Eq.(82) 90

References 91

I. INTRODUCTION

A. Problems

The general concern of KH, the primary author of this article, is that if we plan to implement a gate-type quantum computer that is supposed to embody a certain set of operation

gates, it is important studying the computer from a viewpoint of quantum information processing (or *QIP* for short) algorithm at the same time as producing *tangible* things. Here, let us suppose the computer to embody the following quantum gates: Controlled-Z, $R_x(\phi)$, $R_y(\phi)$ and $R_z(\phi)$ for $\phi = \pm\pi/4, \pm\pi/2, \pi$. The definitions of these gates are detailed later, and hereinafter we call such computer *our potential computer*. In particular, the assessment of our potential computer's availability to solve a problem is, among other things, vital and should be done prior to any processing activities. This article focuses on the assessment. Other algorithmic investigations, e.g., the development of an efficient QIP code and the development of an error correction code, taking into account the physical characteristics of the computer, may follow the assessment study.

B. Questions/Aims

We have two aims for the assessment of our gate-type computer's potential availability to solve a problem.

The first aim is to confirm its universality. A gate-type quantum computer is said to possess universality if it is verified to be able to perform arbitrary unitary transformations on internal data. An arbitrary unitary transformation is made possible if a quantum computer embodies an arbitrary single-qubit gate and a CNOT gate as well[1]. In case that our quantum computer could not embody a full set of these gates, there still might be a possibility of it being able to solve some limited types of problems, though.

The second aim is to understand its practicality. Assuming that our potential computer will prove to be universal in the first half of this article, to what extent our potential quantum computer could be useful in a practical point of view, i.e., how good it is in comparison to a classical computer in terms of solving a real problem.

C. Questions/Objectives

We set two objectives corresponding to the two aims, respectively.

The first objective is concerning universality, and we examine whether our potential computer embodies "the $\pi/8$ gate", phase gate, Hadamard gate, and CNOT gate or not (to be mentioned in Section II A).

Organisation of II A is as follows: giving a simple definition of the gate-type quantum information processing in a bit conceptual manner, followed by introducing the concept of a universal set of operations or gates, then reviewing in detail how to obtain the ultimate universal set comprising "the $\pi/8$ gate", phase gate, Hadamard gate, and CNOT gate. Now, having had these fundamental concepts, we examine our potential computer's universality, to confirm it.

The second objective is concerning practicality, and we plan to verify that our potential computer can exhibit *quantum advantage*. To this end, we demonstrate that ours can implement the Deutsch-Jozsa algorithm[2] (or *DJA* for short). DJA is an algorithm that is introduced to solve a certain problem (to be mentioned in Section II B), and the algorithm can only be implemented using the theoretical framework of quantum information processing, i.e., a classical computer cannot implement it. Quantum advantage is the potential ability of a quantum computer to solve problems faster than a classical computer do[4] while quantum supremacy is the potential ability to solve those that cannot be done practically by a classical computer[5].

Organisation of II B is as follows: defining a problem to be tackled, followed by introducing DJA and reviewing how DJA makes it possible solve the problem in much less number of steps, then confirming that DJA can be implemented with our potential computer.

The successful implementation of DJA is understood as a successful demonstration of *a quantum advantage.* This advantage is among those characteristics that help to affirm that a quantum computer is superior to a classical counterpart. The implementation of DJA requires the Hadamard gate, which is also a centerpiece of the whole quantum information processing.

Throughout this article, terms *operation* and *gating*, and *operator* and *gate* are used interchangeably, respectively.

II. RESULTS

A. Universality of our potential computer

1. Definition of the gate-type quantum information processing

A gate-type quantum computer (of n-qubit) is defined as follows[1, 3]:

a. It has a register that holds $2n$ complex numbers, where each qubit has two complex numbers.

b. It changes the contents of the register (= n-qubit state) by carrying out unitary operations repeatedly on the original register using $2n \times 2n$ complex unitary matrices until the intended register is obtained.

c. It *measures* the contents of the intended register, to produce a real number and the intended register is projected onto one computational basis associated with the real number. This is represented by measurement of *a measurement operator* $M_m (\equiv |m\rangle\langle m|$, where $|m\rangle$ is one computational basis) with respect to the intended n-qubit state: We obtain the probability of the state being found in the specific state $|m\rangle$.

The proceeding chapters deal with the issues regarding (II A 1 b) above. The author follows the mathematical notations, e.g., tensor representation, in particular, found in the notable references [1, 6–9].

2. A universal set of gates for quantum computation

As mentioned above, QIP is basically a repetition of $2n \times 2n$ unitary operations on the original n-qubit state. A quantum computer might be appreciated well if it is specially built to solve some specific problem and embody all the necessary $2n \times 2n$ unitary operators or gates to solve it. We, however, tend to like to have the type of quantum computer that is available to solve any problems given. Otherwise, we will build different quantum computers for different problems one by one. Here the concept of a universal set of gates or a universal quantum computer came in. Details of the universal sets are described below.

3. Towards the ultimate universal set of gates

If a set of gates (referring to quantum gates in this writing) can be equivalent to an arbitrary gate, i.e., the set is capable to replace the arbitrary gate, the set is said to be universal for quantum computation. A quantum computer equipped with a universal set of gates is then called a universal quantum computer. In the following, three universal sets α, β and γ are explained. The three sets relate to others in that the set-α is decomposed to the set-β and the set-β is further decomposed to the set-γ. What should be noted is that

the set-γ is not exactly equivalent to the set-β. The set-β is approximated to the set-γ to *arbitrary accuracy*, instead. The set-γ is called the ultimate universal set of gates.

a. set-α : two-level unitary operations

The target is to verify that an arbitrary unitary matrix with an arbitrary size is decomposed to *two-level unitary matrices*.

Start with an arbitrary 3×3 unitary matrix $U^{(3)}$:

$$U^{(3)} \equiv \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}. \tag{1}$$

Our strategy is to find three unitary matrices $U_1^{(3)}, U_2^{(3)}, U_3^{(3)}$ such that

$$U_3^{(3)} U_2^{(3)} U_1^{(3)} U^{(3)} = \tilde{I}. \tag{2}$$

For if Eq.(2) holds, $U^{(3)}$ is then decomposed as

$$U^{(3)} = {U_1^{(3)}}^{-1} {U_2^{(3)}}^{-1} {U_2^{(3)}}^{-1} = {U_1^{(3)}}^{\dagger} {U_2^{(3)}}^{\dagger} {U_2^{(3)}}^{\dagger}. \tag{3}$$

Now we can explain that *the two-level unitary matrices* do this job. A two-level unitary matrix is one that acts non-trivially on two-or-fewer vector components. First, take a first two-level unitary matrix $U_1^{(3)}$ as

$$U_1^{(3)} = \begin{cases} \begin{pmatrix} \frac{a^*}{A_3} & \frac{b^*}{A_3} & 0 \\ \frac{b}{A_3} & \frac{-a}{A_3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ A_3 = \sqrt{|a|^2 + |b|^2} & (\text{for b} \neq 0) \\ \tilde{I}^{(3)} & (\text{for b} = 0). \end{cases} \tag{4}$$

Thus,

$$U_1^{(3)} U^{(3)} = \begin{pmatrix} A_3 & \frac{a^* d + b^* e}{A_3} & \frac{a^* g + b^* h}{A_3} \\ 0 & \frac{bd - ea}{A_3} & \frac{bg - ah}{A_3} \\ c & f & j \end{pmatrix} \tag{5}$$

$$\equiv \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}. \tag{6}$$

While the deviations of Eq.(5) and Eq.(6) are done for $b \neq 0$, Eq(6) holds for $b = 0$, either. Next, take a second two-level unitary matrix $U_2^{(3)}$ as

$$U_2^{(3)} = \begin{cases} \begin{pmatrix} \frac{a'^*}{A'_3} & 0 & \frac{c'^*}{A'_3} \\ 0 & 1 & 0 \\ \frac{c'}{A'_3} & 0 & \frac{-a'}{A_3} \end{pmatrix}, \ A'_3 = \sqrt{|a'|^2 + |c'|^2} \ \ (\text{for c}' \neq 0) \\ \tilde{I}^{(3)} \qquad\qquad\qquad\qquad\qquad\qquad (\text{for c}' = 0). \end{cases} \tag{7}$$

Thus,

$$U_2^{(3)} \left(U_1^{(3)} U^{(3)} \right) = \begin{pmatrix} \frac{a'^*}{A'_3} & 0 & \frac{c'^*}{A'_3} \\ 0 & 1 & 0 \\ \frac{c'}{A'_3} & 0 & \frac{-a'}{A_3} \end{pmatrix} \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix} = \begin{pmatrix} A'_3 & \frac{a'^* d' + c'^* f'}{A'_3} & \frac{a'^* g' + c'^* j'}{A'_3} \\ 0 & e' & h' \\ 0 & \frac{c' d' - a' f'}{A'_3} & \frac{c' g' - a' j'}{A'_3} \end{pmatrix}. \tag{8}$$

Here, by recalling the unitarity of $U_2^{(3)} \left(U_1^{(3)} U^{(3)} \right)$, the most RHS of Eq.(8) further reduces to

$$\Longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & e' & h' \\ 0 & \frac{c' d' - a' f'}{A'_3} & \frac{c' g' - a' j'}{A'_3} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & g'' \end{pmatrix}. \tag{9}$$

Finally, if we take $U_3^{(3)}$ as

$$U_3^{(3)} \equiv \left(U_2^{(3)} \left(U_1^{(3)} U^{(3)} \right) \right)^\dagger = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & g''^* \end{pmatrix}, \tag{10}$$

clearly we have

$$U_3^{(3)} \left(U_2^{(3)} \left(U_1^{(3)} U^{(3)} \right) \right) = \tilde{I}. \tag{11}$$

$U_3^{(3)}$ is another two-level unitary matrix. We have just verified Eq.(3): An arbitrary 3×3 unitary matrix $U^{(3)}$ is decomposed to multiplications of three 3×3 two-level unitary matrices.

The next is regarding an arbitrary 4×4 unitary matrix $U^{(4)}$:

$$U^{(4)} \equiv \begin{pmatrix} a & d & g & \varepsilon \\ b & e & h & \eta \\ c & f & j & \theta \\ \alpha & \beta & \gamma & \delta \end{pmatrix}. \tag{12}$$

We take the procedures similar to the case of $U^{(3)}$. First, take a first two-level unitary matrix $U_1^{(4)}$ as

$$U_1^{(4)} = \begin{cases} \begin{pmatrix} \frac{a^*}{A_4} & \frac{b^*}{A_4} & 0 & 0 \\ \frac{b}{A_4} & \frac{-a}{A_4} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ A_4 = \sqrt{|a|^2 + |b|^2} \ \ (\text{for b} \neq 0) \\ \tilde{I}^{(4)} \qquad\qquad\qquad\qquad\qquad\qquad (\text{for b} = 0). \end{cases} \tag{13}$$

Thus,

$$U_1^{(4)} U^{(4)} = \begin{pmatrix} A_4 & \frac{a^*d+b^*e}{A_4} & \frac{a^*g+b^*h}{A_4} & \frac{a^*\varepsilon+b^*\eta}{A_4} \\ 0 & \frac{bd-ea}{A_4} & \frac{bg-ah}{A_4} & \frac{b\varepsilon-a\eta}{A_4} \\ c & f & j & \theta \\ \alpha & \beta & \gamma & \delta \end{pmatrix} \tag{14}$$

$$\equiv \begin{pmatrix} a' & d' & g' & \varepsilon' \\ 0 & e' & h' & \eta' \\ c' & f' & j' & \theta' \\ \alpha' & \beta' & \gamma' & \delta' \end{pmatrix}. \tag{15}$$

A quick reminder: as in Eq.(5) and Eq.(6) regarding $U^{(3)}$, while the deviations of Eq.(14) and Eq.(15) are done for $b \neq 0$, Eq(15) holds for $b = 0$, either.

Next, take a second two-level unitary matrix $U_2^{(4)}$ as

$$U_2^{(4)} = \begin{cases} \begin{pmatrix} \frac{a'^*}{A'_4} & 0 & \frac{c'^*}{A_4} & 0 \\ 0 & 1 & 0 & 0 \\ \frac{c'}{A'_4} & 0 & \frac{-a'}{A'_4} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ A'_4 = \sqrt{|a'|^2 + |c'|^2} \ \ (\text{for c}' \neq 0) \\ \tilde{I}^{(4)} \qquad\qquad\qquad\qquad\qquad\qquad (\text{for c}' = 0) \end{cases} \tag{16}$$

, to have

$$U_2^{(4)}\left(U_1^{(4)}U^{(4)}\right) = \begin{pmatrix} A'_4 & \frac{a'^* d' + c'^* f'}{A'_4} & \frac{a'^* g' + c'^* j'}{A'_4} & \frac{a'^* \varepsilon' + c'^* \theta'}{A'_4} \\ 0 & e' & h' & \eta' \\ c & \frac{c' d' - a' f'}{A'_4} & \frac{c' g' - a' j'}{A'_4} & \frac{c' \varepsilon' - a' \theta'}{A'_4} \\ \alpha' & \beta' & \gamma' & \delta' \end{pmatrix} \tag{17}$$

$$\equiv \begin{pmatrix} a'' & d'' & g'' & \varepsilon'' \\ 0 & e'' & h'' & \eta'' \\ 0 & f'' & j'' & \theta'' \\ \alpha'' & \beta'' & \gamma'' & \delta'' \end{pmatrix}. \tag{18}$$

Further, take a third two-level unitary matrix $U_3^{(4)}$ as

$$U_3^{(4)} = \begin{cases} \begin{pmatrix} \frac{a''^*}{A''_4} & 0 & 0 & \frac{\alpha''^*}{A''_4} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{\alpha''}{A''_4} & 0 & 0 & \frac{-a''}{A''_4} \end{pmatrix}, \ A''_4 = \sqrt{|a''|^2 + |\alpha''|^2} \ \ (\text{for } \alpha'' \neq 0) \\ \tilde{I}^{(4)} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{for } \alpha'' = 0) \end{cases} \tag{19}$$

, to have

$$U_3^{(4)}\left(U_2^{(4)}\left(U_1^{(4)}U^{(4)}\right)\right) = \begin{pmatrix} A_4'' & \frac{a''^*d''+\alpha''^*\beta''}{A_4''} & \frac{a''^*g''+\alpha''^*\gamma''}{A_4''} & \frac{a''^*\varepsilon''+\alpha''^*\delta''}{A_4''} \\ 0 & e'' & h'' & \eta'' \\ 0 & f'' & j''' & \theta'' \\ 0 & \frac{\alpha''d''-a''\beta''}{A_4''} & \frac{\alpha''g''-a''\gamma''}{A_4''} & \frac{\alpha''\varepsilon''-a''\delta''}{A_4''} \end{pmatrix} \tag{20}$$

$$= \begin{pmatrix} A_4'' & 0 & 0 & 0 \\ 0 & e'' & h'' & \eta'' \\ 0 & f'' & j''' & \theta'' \\ 0 & \frac{\alpha''d''-a''\beta''}{A_4''} & \frac{\alpha''g''-a''\gamma''}{A_4''} & \frac{\alpha''\varepsilon''-a''\delta''}{A_4''} \end{pmatrix} \tag{21}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e'' & h'' & \eta'' \\ 0 & f'' & j''' & \theta'' \\ 0 & \frac{\alpha''d''-a''\beta''}{A_4''} & \frac{\alpha''g''-a''\gamma''}{A_4''} & \frac{\alpha''\varepsilon''-a''\delta''}{A_4''} \end{pmatrix} \tag{22}$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e''' & h''' & \eta''' \\ 0 & f''' & j''' & \theta''' \\ 0 & \beta''' & \gamma''' & \delta''' \end{pmatrix}. \tag{23}$$

The last matrix form Eq.(23) implies that, by using three 4×4 two-level unitary matrices, an arbitrary 4×4 unitary matrix $U^{(4)}$ is deformed to one effectively of an arbitrary 3×3 unitary matrix, which has just been verified to be decomposed to multiples of three 3×3 two-level unitary matrices.

By repeating the procedures above, an arbitrary unitary matrix with an arbitrary size can be decomposed to multiplications of two-level unitary matrices.

We have verified that two-level unitary matrices form a universal set in quantum computing.

b. set-β : CNOT operation and single-qubit unitary operation

We will verify below that an arbitrary $2n \times 2n$ two-level unitary operator is decomposed to multiplications of CNOT operation(s) and single-qubit unitary operations.

Start with a case of $n = 1$, where an arbitrary 2×2 unitary matrix is supposed to operate on a single-qubit system or *a two-component spinor*, which is represented by a 1×2 column

matrix or vector. The corresponding two-level unitary operator to such vector is nothing but a single-qubit unitary operation. Now, the case is verified.

Next, for a case of n=2, where an 4×4 arbitrary unitary matrix operates on a two-qubit system represented by a 1×4 column matrix or vector. What should be noted first is that there exist such 6 types of two-level unitary matrices only as follows, with each matrix being accompanied by the two computational basis that the matrix acts non-trivially on:

$$\bar{U}_1^{(4)} \equiv \begin{pmatrix} a & c & 0 & 0 \\ b & d & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad : \{|00\rangle, |01\rangle\}, \tag{24}$$

$$\bar{U}_2^{(4)} \equiv \begin{pmatrix} a & 0 & c & 0 \\ 0 & 1 & 0 & 0 \\ b & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad : \{|00\rangle, |10\rangle\}, \tag{25}$$

$$\bar{U}_3^{(4)} \equiv \begin{pmatrix} a & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ b & 0 & 0 & d \end{pmatrix} \quad : \{|00\rangle, |11\rangle\}, \tag{26}$$

$$\bar{U}_4^{(4)} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & c & 0 \\ 0 & b & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad : \{|01\rangle, |10\rangle\}, \tag{27}$$

$$\bar{U}_5^{(4)} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & c \\ 0 & 0 & 1 & 0 \\ 0 & b & 0 & c \end{pmatrix} \quad : \{|01\rangle, |10\rangle\}, \tag{28}$$

$$\bar{U}_6^{(4)} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix} \quad : \{|10\rangle, |11\rangle\}. \tag{29}$$

N.B.: $|vw\rangle$, $|v\rangle|w\rangle$ or $|v, w\rangle$ are the abbreviated notations for tenso product $|v\rangle \otimes |w\rangle$, where

$|v\rangle$ and $|w\rangle$ are vectors of inner product spaces V and W, respectively. We define U as

$$U \equiv \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \tag{30}$$

To decompose the two-level unitary matrices, we use the following five procedures:

1. Translate the two computational bases that the matrix acts non-trivially on, which are written next to the matrix above (Eq.(24) for instance), into two *Gray code* sequences. Hereinafter, such two computational bases may be called *the original* computational bases occasionally. Then, interpolate the two sequences with other Gray code sequences to make a series of the sequences, in a manner that the adjacent sequences differ in exactly one bit.

2. Translate back the resultant sequences into the computational bases or the two-qubit state. Now you might have new bases also that are originally not recognized as those that the matrix acts non-trivially on. Then, read the series to determine which of the two qubits to flip one by one to transform the basis from *the initial computational basis* to one step before *the final computational basis*. The initial and the final computational bases refer to the ones listed as the first and second terms of the original computational bases, respectively. For example, $|00\rangle$ and $|11\rangle$ are the initial and the final computation bases in case of $\bar{U}_3^{(4)}$ (Eq.(26)).

3. To execute transforming the computational basis from the initial one, carry out the controlled flipping operation (= Controlled-X) on the qubit that is to be flipped (= *target qubit*), conditional on the other qubit being in the state $|0\rangle$ (or $|1\rangle$) if this qubit (= *control qubit*) should remain in $|0\rangle$ (or $|1\rangle$) before and after the operation. Repeat this Controlled-X operation until the basis is transformed to one step before the final computational basis (as mentioned in 2).

4. We need to do one more flipping (of either qubit) to reach the final computational basis. To this end, carry out the controlled unitary (*Controlled-U* for short) operation, which executes U operation on the target qubit, conditional on the state of the control qubit.

5. To complete the deformation, we must carry out the same flipping operations again as have been done to reach the computational basis that will be executed with the Controlled-U operation.

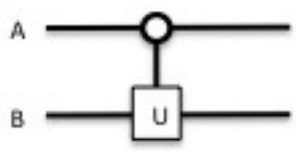

FIG. 1. A diagram equivalent to $\bar{U}_1^{(4)}$. A and B represent the first and the second qubit, respectively. Each line indicates a time-line on which time advances from left to right. At some point in time, B is acted on with U operations, conditional on A being in the state $|0\rangle$.

Now, look at $\bar{U}_1^{(4)}$. We follow the procedures above to interpret as a decomposition of the Controlled-X and the Controlled-U operations. The Gray code sequences corresponding to the original two bases are (00) and (01), and as the two sequences differ in one bit only they have already constituted the complete Gray code series, i.e., there is no need of flipping to do prior to the Controlled-U operation. Thus, $\bar{U}_1^{(4)}$ can be interpreted in terms of flipping and the Controlled-U as: Simply operate the Controlled-U operation on the two-qubit state $|00\rangle$, where do U operation on the second qubit, conditional on the first qubit being in the state $|0\rangle$, and reach $|01\rangle$, which is the final computational basis. Now, by following the procedures, we reach a diagram FIG. 1, which should be *equivalent* to $\bar{U}_1^{(4)}$. In the diagram, A and B represent the first and the second qubit, respectively, and each line indicates *a time-line*, on which time advances from left to right. The diagram indicates how the two qubits A and B correlate with each other in the course of time. FIG. 1 shows that at some point in time, U operation is acted on the qubit B, conditional on the qubit A being in $|0\rangle$. The whole circle on the time-line of the qubit A indicates that the condition imposed on the qubit A, which is linked with U, is $|0\rangle$. If the condition on the qubit A were $|1\rangle$, the circle would be painted in solid black. We can verify that the diagram FIG. 1 indeed represents

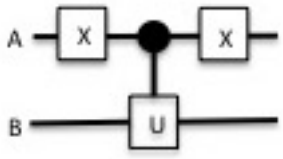

FIG. 2. A diagram equivalent to FIG. 1. The white circle in FIG. 1, representing that U will be done conditional on the qubit A being in $|0\rangle$, is replaced to a black circle that is sandwiched by two X operations. A black circle means that the condition on the qubit A in the Controlled-U is now the qubit A being in $|1\rangle$.

$\bar{U}_1^{(4)}$ by reading the diagram with mathematical formulas as follows:

$$(|0\rangle\langle 0|)_A \otimes U_B + (|1\rangle\langle 1|)_B \otimes \tilde{I}_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_A \begin{pmatrix} 1 & 0 \end{pmatrix}_A \otimes U_B + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_A \begin{pmatrix} 0 & 1 \end{pmatrix}_A \otimes \tilde{I}_B \quad (31)$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}_A \otimes U_B + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}_A \otimes \tilde{I}_B \quad (32)$$

$$= \begin{pmatrix} U_B & 0 \\ 0 & \tilde{I}_B \end{pmatrix} = \begin{pmatrix} U & 0 \\ 0 & \tilde{I} \end{pmatrix} = \begin{pmatrix} a & c & 0 & 0 \\ b & d & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (33)$$

$$\equiv \bar{U}_1^{(4)}. \quad (34)$$

The next task is to try to decompose the two-qubit operation shown in the diagram into multiplications of CNOT and single-qubit operations. The diagram FIG. 1 indeed prompts us to re-draw it to the diagram in FIG. 2. The conditional part on the qubit A is replaced to one with $|1\rangle$, i.e., the conventional controlled operation, by flipping the qubit A using X operation just before the Controlled-U operation. The flipping is compensated by another X operation just after the Controlled-U operation. We can verify that the diagram in FIG. 2 also represents $\bar{U}_1^{(4)}$, i.e., equivalence between FIG. 1 and 2, as follows:

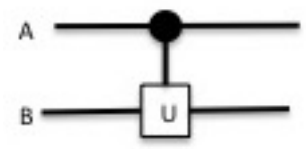

FIG. 3. A diagram for the Controlled-U, by which U will act on B, conditional on the qubit A being in $|1\rangle$.

$$\left(X_A \otimes \tilde{I}_B\right)\left(\left(|0\rangle\langle 0|\right)_A \otimes \tilde{I}_B + \left(|1\rangle\langle 1|\right)_A \otimes U_B\right)\left(X_A \otimes \tilde{I}_B\right) \tag{35}$$

$$= \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_A \otimes \tilde{I}_B\right)\begin{pmatrix} \tilde{I}_B & 0 \\ 0 & U_B \end{pmatrix}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_A \otimes \tilde{I}_B\right) \tag{36}$$

$$= \begin{pmatrix} 0 & \tilde{I}_B \\ \tilde{I}_B & 0 \end{pmatrix}\begin{pmatrix} \tilde{I}_B & 0 \\ 0 & U_B \end{pmatrix}\begin{pmatrix} 0 & \tilde{I}_B \\ \tilde{I}_B & 0 \end{pmatrix} = \begin{pmatrix} U_B & 0 \\ 0 & \tilde{I}_B \end{pmatrix} = \begin{pmatrix} U & 0 \\ 0 & \tilde{I} \end{pmatrix} \equiv \bar{U}_1^{(4)}. \tag{37}$$

Now our final task here is to decompose the controlled-U operation shown in FIG. 3 (not FIG. 1) into single qubit operations and CNOT operation. A mathematical formula for the controlled-U (FIG. 3) is

$$\left(|0\rangle\langle 0|\right)_A \otimes \tilde{I}_B + \left(|1\rangle\langle 1|\right)_A \otimes U_B = \begin{pmatrix} \tilde{I} & 0 \\ 0 & U \end{pmatrix}. \tag{38}$$

Here, the Controlled-NOT or CNOT is regarded as a special case of the Controlled-U. It is defined as one that has X for U in the Controlled-U. The diagram of CNOT is shown in FIG. 4 and its mathematical formula is

$$\left(|0\rangle\langle 0|\right)_A \otimes \tilde{I}_B + \left(|1\rangle\langle 1|\right)_A \otimes X_B = \begin{pmatrix} \tilde{I} & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{39}$$

The Controlled-U (FIG. 3) is widely know to be re-drawn as in FIG. 5 by using the fact that an arbitrary 2×2 unitary matrix U is decomposed as $U = e^{i\alpha}AXBXC$ with three single qubit operations A, B, and C such that $ABC = \tilde{I}$ and a physically insignificant global phase $e^{i\alpha}$. We can confirm that the RHS diagram in FIG. 5 represents the Controlled-U in

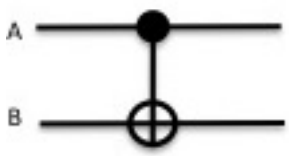

FIG. 4. A diagram for the Controlled-NOT or CNOT operation. It is defined as a special case of the Controlled-U in that U is specified as X.

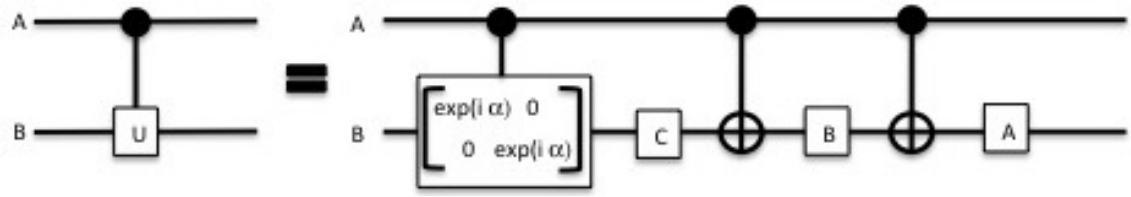

FIG. 5. Controlled-U (FIG. 3) can be decomposed as RHS.

FIG. 3 as follows:

$$\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \tilde{I}_B & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} \tilde{I}_B & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} \tilde{I}_B & 0 \\ 0 & e^{i\alpha}\tilde{I}_B \end{pmatrix} \tag{40}$$

$$= \begin{pmatrix} ABC & 0 \\ 0 & e^{i\alpha}AXBXC \end{pmatrix} \tag{41}$$

$$= \begin{pmatrix} \tilde{I} & 0 \\ 0 & U \end{pmatrix}. \tag{42}$$

In Eq.(40), we pay attention to the order of the matrices so that it reflects the correct order in time (as designated in FIG. 5). For example, $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ is put in the left-most position in Eq.(40) because the operation comes at last in the course of time. Eq.(42) uses $U = e^{i\alpha}AXBXC$ and $ABC = \tilde{I}$[1]. FIG. 6 is an alternative diagram to represent the Controlled-U in FIG. 3. In FIG. 6 the phase operation is done on the qubit A at last in the course of time, while it is on the qubit B at first in FIG. 5. With the diagram in FIG. 6 taken, for example, and recalling the two X operations in FIG. 2, we finally conclude that $\bar{U}_1^{(4)}$ is decomposed to multiplications of single qubit operations and CNOT operation (FIG. 7).

Next, look at $\bar{U}_2^{(4)}$. The Gray code sequences corresponding to the original two computational bases $|00\rangle$ and $|10\rangle$ are (00) and (10); therefore, as is the case with $\bar{U}_1^{(4)}$, there is no need to inset other Gray code sequences between (00) and (10). Thus, the diagram that

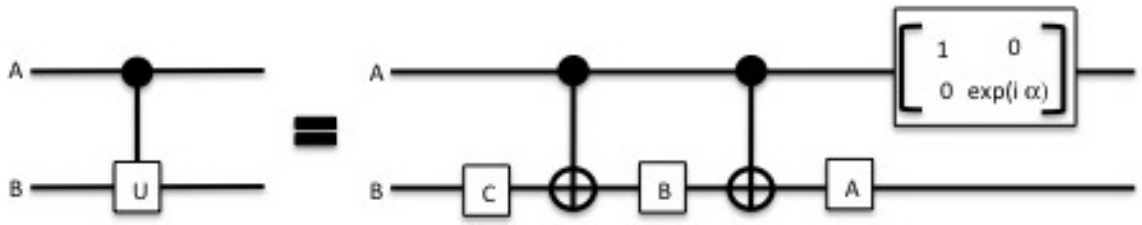

FIG. 6. An alternative diagram for the Controlled-U in FIG. 3. A position of the phase operation differs from FIG. 5.

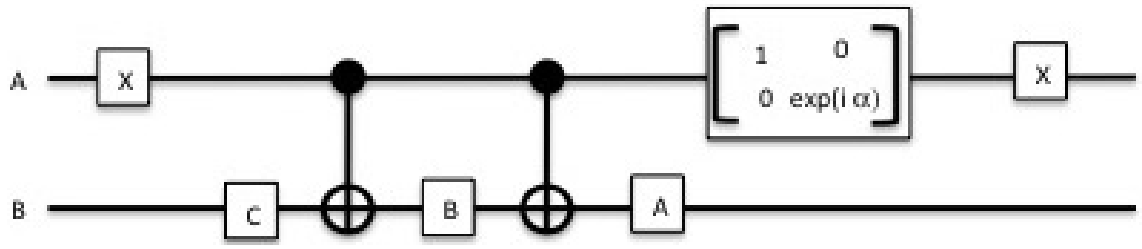

FIG. 7. The eventual diagram to represent $\bar{U}_1^{(4)}$. The two-qubit operation shown in FIG. 6 is sandwiched by two X operations to complete $\bar{U}_1^{(4)}$ and $ABC = \tilde{I}$.

corresponds to $\bar{U}_2^{(4)}$ is shown in FIG. 8, where Controlled-U operation is acted on the qubit A, conditional on the qubit B being in the state $|0\rangle$. The validity of the diagram is verified

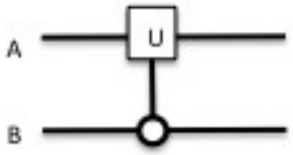

FIG. 8. A diagram to represent $\bar{U}_2^{(4)}$. Controlled-U operation is acted on the qubit A, conditional on the qubit B being in the state $|0\rangle$.

by

$$U_A \otimes (|0\rangle\langle 0|)_B + \tilde{I}_A \otimes (|1\rangle\langle 1|)_B \tag{43}$$

$$= \begin{pmatrix} a & c \\ b & d \end{pmatrix}_A \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}_B + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_A \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}_B \tag{44}$$

$$= \begin{pmatrix} a & 0 & c & 0 \\ 0 & 0 & 0 & 0 \\ b & 0 & d & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & 1 & 0 & 0 \\ b & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \bar{U}_2^{(4)}. \tag{45}$$

The basic strategy to further decompose the two-qubit operation in FIG. 8 is to deform it to have the Controlled-U operation such that it operates U on the qubit B, conditional on the qubit A being in $|1\rangle$. Once we extract such Controlled-U in FIG. 3, the section will be decomposed to the composite two-qubit operation in FIG. 5 or FIG. 6. Following the strategy, we deform the diagram in FIG. 8 to ones shown in FIG. 9. In the left-most diagram, a white circle has been replaced with a black one, to change the condition on the qubit B from $|0\rangle$ to $|1\rangle$, to become the *inverted* Controlled-U. In the middle diagram, the *inverted* Controlled-U has been inverted (= upside down) between the two qubits by using two swapping operations, to become the conventional controlled-U in FIG. 3. In the right-most diagram, each swapping operation is replaced with a composite of two CNOT gates and an *inverted* CNOT operation. The double oblique lines in the right-most diagram means that a mirrored structure excluding the Controlled-U should come beyond the lines. The decomposition of the swap gate is verified as

$$\begin{pmatrix} \tilde{I} & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \tilde{I} & 0 \\ 0 & X \end{pmatrix} \tag{46}$$

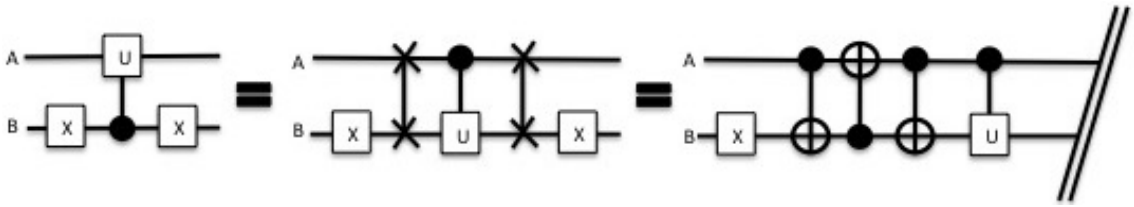

FIG. 9. $\bar{U}_2^{(4)}$ in FIG. 8 is deformed further step by step. The original $\bar{U}_2^{(4)}$ has been deformed in the left-most diagram using two X gates to replace a white circle to a black one. Then, the *inverted* Controlled-U has been deformed in the middle diagram using two swap gates to have the conventional Controlled-U. In the right-most diagram, each swap gate is replaced with a composite of two CNOT and one *inverted* CNOT. The double oblique lines means that a mirrored structure excluding the Controlled-U should come beyond the lines.

, where the middle matrix, the *inverted* CNOT, is obtained as

$$\tilde{I}_A \otimes (|0\rangle\langle 0|)_B + X_A \otimes (|1\rangle\langle 1|)_B \tag{47}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_A \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}_B + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_A \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}_B \tag{48}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{49}$$

The *inverted* CNOT is replaced to a composite of four Hadamard gates and one CNOT (FIG. 10), and the validity is verified as

$$\left(\tilde{I}_A \otimes \tilde{H}_B\right)\left(\tilde{H}_A \otimes \tilde{I}_B\right)\begin{pmatrix} \tilde{I} & 0 \\ 0 & X \end{pmatrix}\left(\tilde{H}_A \otimes \tilde{I}_B\right)\left(\tilde{I}_A \otimes \tilde{H}_B\right) \tag{50}$$

$$= \begin{pmatrix} \tilde{H}_B & 0 \\ 0 & \tilde{H}_B \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \tilde{I}_B & \tilde{I}_B \\ \tilde{I}_B & -\tilde{I}_B \end{pmatrix} \begin{pmatrix} \tilde{I} & 0 \\ 0 & X \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \tilde{I}_B & \tilde{I}_B \\ \tilde{I}_B & -\tilde{I}_B \end{pmatrix} \begin{pmatrix} \tilde{H}_B & 0 \\ 0 & \tilde{H}_B \end{pmatrix} \tag{51}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{52}$$

Thus, with the results in FIG. 9 and FIG. 10 and the decomposition of the Controlled-U

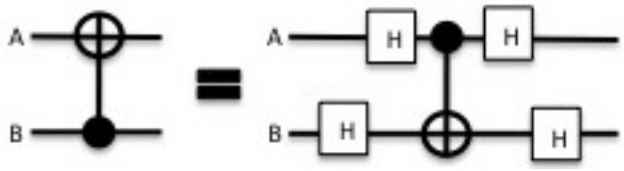

FIG. 10. The *inverted* CNOT gate is replaced to a composite of four Hadamard gates and one CNOT gate.

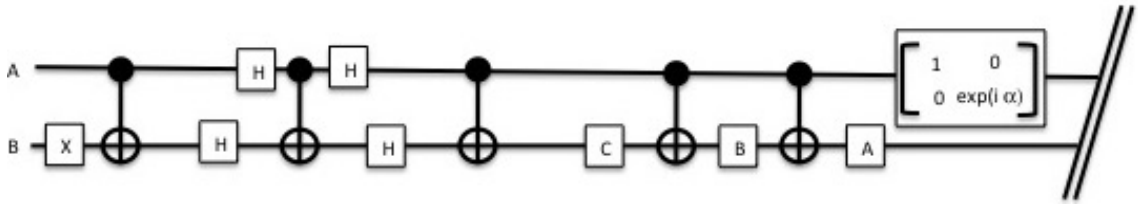

FIG. 11. $\bar{U}_2^{(4)}$ is decomposed to multiplications of single qubit gates –$X, \tilde{H}, A, B, C$, phase – and CNOT gates, where $ABC = \tilde{I}$.

(FIG. 6), we verify that $\bar{U}_2^{(4)}$ is decomposed to multiplications of single qubit operations – $X, \tilde{H}, A, B, C$, phase – and CNOT operations (FIG. 11). The double oblique lines in FIG. 11 means that a mirrored structure excluding a composite for the Controlled-U should come beyond the lines.

Next, look at $\bar{U}_3^{(4)}$. With (00) and (11) being the two Gray code sequences that correspond to the initial and final computational basis of the original bases, we must interpolate another Gray code sequence (01) between them. Using these three Gray code sequences, we can draw in FIG. 12 the diagram for $\bar{U}_3^{(4)}$. The left-most operation is the *white-circle* CNOT, defined in Eq. (53), by which the computational basis $|00\rangle$ is transformed to $|01\rangle$. The middle operation in FIG. 12 is the *inverted* Controlled-U, by which the qubit A is acted on with U, conditional on the qubit B being in the state $|1\rangle$. Finally, another *white-circle* CNOT is done on the two-qubit state to compensate the flipping that has been done at first.

$$(|0\rangle\langle 0|)_A \otimes X_B + (|1\rangle\langle 1|)_A \otimes \tilde{I}_B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{53}$$

By using the various replacements mentioned above, the diagram for $\bar{U}_3^{(4)}$ is further deformed

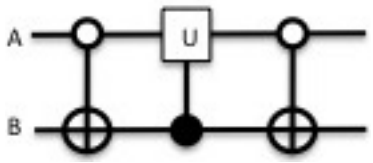

FIG. 12. A diagram to represent $\bar{U}_3^{(4)}$, according to the three Gray code sequences (00), (01), and (11). The last operation, the *white-circle* CNOT, following the *inverted* Controlled-U, is to compensate the flipping operation that has been done at first.

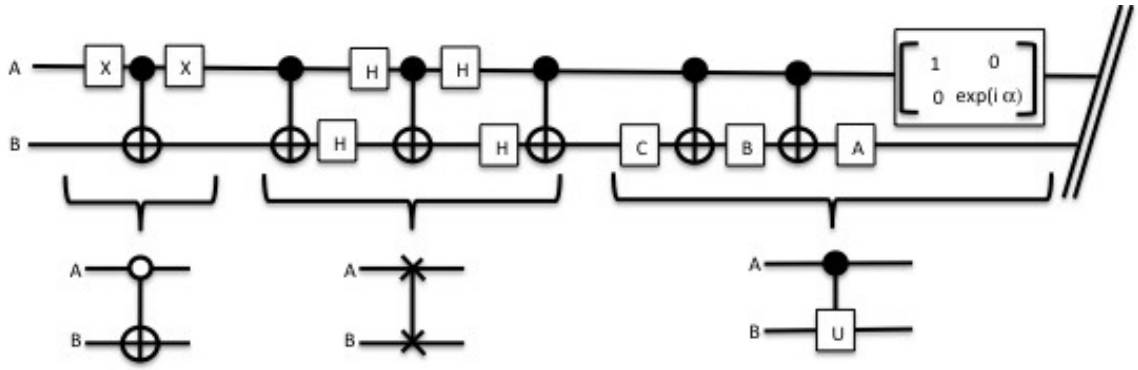

FIG. 13. The eventual diagram to represent $\bar{U}_3^{(4)}$. By using various equivalent deformations, it becomes made up of single qubit operations – $X, \tilde{H}, A, B, C$, and phase – and CNOT operations, where $ABC = \tilde{I}$.

so that it contains only single qubit operations and CNOT operations (FIG. 13). In FIG. 13, the *white-circle* CNOT has been deformed using two flipping operations on the qubit A, so that this section comprises the conventional CNOT. Then, a swapping between the qubit A and the qubit B is carried out, so that the *inverted* Controlled-U is converted to the conventional Controlled-U. And the swapping is decomposed following FIG. 10. The Controlled-U is decomposed following FIG. 6. The double oblique lines in FIG. 13 means that a mirrored structure excluding a composite for the Controlled-U should come beyond the lines.

For the rest of 2×2 two-level unitary matrices and all other two-level unitary matrices with larger size, we can verify that they are all decomposed to multiplications of single-qubit operations and CNOT operations by following exactly the similar procedures to those explained above.

Recalling that an arbitrary unitary matrix with arbitrary size is decomposed to two-

level unitary matrices, we have just shown that CNOT operator and single-qubit operator constitute a universal set of gates in quantum computing.

c. set-γ : CNOT operation, Hadamard operation, and "the $\pi/8$ operation"

It has just been verified that an arbitrary unitary operator with arbitrary size is decomposed to multiplications of CNOT operation and single-qubit operation. That is, these operators constitute a universal set of gates in quantum computing. Now that, what to do next is to try to further decompose the universal operators and reach the ultimate universal set by limiting the variety of the single-qubit operations. We will see that the single-qubit operations are actually limited to those that are called the "$\pi/8$ gate" (or *T gate* for short) regarding z-axis and the Hadamard gate $\tilde{H}$. More precisely, an arbitrary single-qubit operation is approximated using $\tilde{H}$ and the "$\pi/8$ gate" to arbitrary accuracy. Here, it should be noted that the "$\pi/8$ gate" is not coming from $\pi/8$ but $\pi/4$ rotation around z-axis.

It is useful to recall a notion of a quantum mechanical rotation following the notations in [1, 6]. An operator that rotates a 2-component spinor around a unit vector $\hat{l} = (l_x, l_y, l_z)$ by ϕ is written as:

$$R_{\hat{l}}(\phi) = exp\left(-i\frac{\vec{\sigma}\cdot\hat{l}}{2}\phi\right) = \tilde{I}\cos\frac{\phi}{2} - i\left(\vec{\sigma}\cdot\hat{l}\right)\sin\frac{\phi}{2} \tag{54}$$

$$= \begin{pmatrix} \cos\frac{\phi}{2} - i_z\sin\frac{\phi}{2} & (-il_x - l_y)\sin\frac{\phi}{2} \\ (-il_x + l_y)\sin\frac{\phi}{2} & \cos\frac{\phi}{2} + i_z\sin\frac{\phi}{2} \end{pmatrix}, \tag{55}$$

where $\vec{\sigma} \equiv (\sigma_x, \sigma_y, \sigma_z)$. These three components $\sigma_x, \sigma_y, \sigma_z$ are called the Pauli matrices whose specific forms are

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{56}$$

The σ_x, σ_y, and σ_z are designated as X, Y, and Z occasionally in this writing. The rotation operators around $x-, y-$, and $z-$axes become

$$R_x(\phi) = exp\left(-i\frac{\sigma_x}{2}\phi\right) = \begin{pmatrix} \cos\frac{\phi}{2} & -i\sin\frac{\phi}{2} \\ -i\sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}, \tag{57}$$

$$R_y(\phi) = exp\left(-i\frac{\sigma_y}{2}\phi\right) = \begin{pmatrix} \cos\frac{\phi}{2} & -\sin\frac{\phi}{2} \\ \sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}, \tag{58}$$

$$R_z(\phi) = exp\left(-i\frac{\sigma_z}{2}\phi\right) = \begin{pmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{+i\frac{\phi}{2}} \end{pmatrix}. \tag{59}$$

Take U as the operator that you want to implement and V as the one that is actually implemented instead of U. That you want to approximate U to V to arbitrary accuracy means that the *error*, $E(U,V)$, that is defined in Eq.(60) becomes negligibly small [1, 10]:

$$E(U,V) \equiv \max_{\psi} || \left(U - V\right) |\psi\rangle || = \max_{\psi} \left(2 - \langle\psi| \left(V^{\dagger}U + U^{\dagger}V\right) |\psi\rangle\right), \tag{60}$$

where $\max_{\psi}$ means that we will use $|\psi\rangle$ such that the argument of $\max_{\psi}$ becomes maximum and $|| \, |\Psi\rangle ||$ is the norm of a vector $|\Psi\rangle$, i.e., $|| \, |\Psi\rangle || \equiv \sqrt{\langle\Psi|\Psi\rangle}$.

We derive two relations with respect to "$\pi/8$ operator" (or T operator for short), which are

$$e^{-i\frac{\pi}{8}} T \equiv e^{-i\frac{\pi}{8}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = e^{-i\frac{Z}{2}\frac{\pi}{4}} = R_z\left(\frac{\pi}{4}\right), \tag{61}$$

$$e^{-i\frac{\pi}{8}} \tilde{H} T \tilde{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = e^{-i\frac{X}{2}\frac{\pi}{4}} = R_x\left(\frac{\pi}{4}\right). \tag{62}$$

Multiply both formulae, to have

$$e^{-i\frac{\pi}{8}} T e^{-i\frac{\pi}{8}} \tilde{H} T \tilde{H} = R_z\left(\frac{\pi}{4}\right) R_x\left(\frac{\pi}{4}\right) = e^{-i\frac{Z}{2}\frac{\pi}{4}} e^{-i\frac{X}{2}\frac{\pi}{4}} \tag{63}$$

$$= \left(\tilde{I}\cos\frac{\pi}{8} - iZ\sin\frac{\pi}{8}\right)\left(\tilde{I}\cos\frac{\pi}{8} - iX\sin\frac{\pi}{8}\right) \tag{64}$$

$$= \tilde{I}\cos^2\frac{\pi}{8} + \sin\frac{\pi}{8}\left(-iZ\cos\frac{\pi}{8} - iX\cos\frac{\pi}{8} - ZX\sin\frac{\pi}{8}\right) \tag{65}$$

$$= \tilde{I}\cos^2\frac{\pi}{8} - i\left(\frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}X + \frac{\sin\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}Y + \frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}Z\right)\sqrt{1-\cos^4\frac{\pi}{8}} \tag{66}$$

$$\equiv R_{\hat{n}}\left(\theta\right). \tag{67}$$

By comparing the expression Eq.(66) and Eq.(54), we understand that $e^{-i\frac{\pi}{8}} T e^{-i\frac{\pi}{8}} \tilde{H} T \tilde{H}$ is equivalent to a rotation (defined as $R_{\hat{n}}\left(\theta\right)$) around a certain unit vector $\hat{n}$ defined as

$$\hat{n} = \left(\frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}, \frac{\sin\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}, \frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}\right), \tag{68}$$

and by a certain angle of θ such that

$$\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}. \tag{69}$$

Next, we detail how repeated iteration of $R_{\hat{n}}\left(\theta\right)$ can be used to approximate to arbitrary accuracy a rotation operator $R_{\hat{n}}\left(\alpha\right)$ that rotates a two-component spinor around the same

vector $\hat{n}$ as in $R_{\hat{n}}(\theta)$ by an arbitrary angle of α. Let $\delta > 0$ be the desired accuracy, and let N be an integer such that $N > 2\pi/\delta$. Define θ_k $(k = 1, 2, \ldots, N)$ so that $\theta_k \in [0, 2\pi\}$ and $\theta_k \equiv k\theta \mod 2\pi$. Then we can say that there are distinct j and k $(1, 2, \ldots, N)$ such that $|\theta_k - \theta_j| \leq 2\pi/N < \delta$. This derivation is due to *the pigeonhole principle* or *Dirichlet's box principle* [11, 12]. Imagine a circle of a radius of 1 and divide its circumference by N, so that we have now N *pigeonholes*, each of which has an arc of $2\pi/N$. Here, the principle states that *if n items are put into m containers, with $n > m$, then at least one container must contain more than one item*[12]. Under the principle, we can deduce that each arc $2\pi/N$ "contains" an angle θ_k one by one, or at least one arc must contain more than one angle. This proves that $|\theta_k - \theta_j| \leq 2\pi/N$ for distinct k and j. Without loss of generality, we can assume that $k > j$, and we can choose k and j such that $|\theta_{k-j}| \equiv |\theta_k - \theta_j| \mod 2\pi < \delta$. Since $k \neq j$, and θ is an irrational mulitiple of 2π ($\because \cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$), $\theta_{k-j} \neq 0$. It follows that the interaval $[0, 2\pi\}$ is filled up by $\theta_{l(k-j)}$ as l is varied. All the adjacent members of $\theta_{l(k-j)}$ are no more than δ apart.

A quick reminder: $R_{\hat{n}}(\alpha)$ is the target operator that rotates a two-component spinor in 3D space around a certain unit vector $\hat{n}$ by an arbitrary angle of α while $R_{\hat{n}}(\theta_{0\alpha})$ is the operator that we actually implement, aiming to approximate $R_{\hat{n}}(\alpha)$. $R_{\hat{n}}(\theta_{0\alpha})$ rotates a state around the same vector $\hat{n}$ but its rotation angle is a multiple of a certain angle of θ such that $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. The angle $\theta_{0\alpha}$ is one that is carefully chosen with ε $(< \delta)$ as

$$\theta_{0\alpha} \equiv \theta_{l_{0\alpha}(k-j)} \equiv l_{0\alpha}(k-j)\theta \mod 2\pi \tag{70}$$

$$|\theta_{0\alpha} - \alpha| = \varepsilon < \delta. \tag{71}$$

Thus, the error $E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta_{0\alpha})\right)$ is evaluated as

$$\max_\psi \left(2 - \langle\psi| R^\dagger_{\hat{n}}\left(\theta_{0\alpha}\right) R_{\hat{n}}\left(\alpha\right) + R^\dagger_{\hat{n}}\left(\alpha\right) R_{\hat{n}}\left(\theta_{0\alpha}\right) |\psi\rangle\right) \tag{72}$$

$$= \max_\psi \left(2 - \langle\psi|[e^{i\frac{\vec{\sigma}}{2}\cdot\hat{n}(l_{0\alpha}(k-j)\theta)} e^{-i\frac{\vec{\sigma}}{2}\cdot\hat{n}\alpha} + e^{i\frac{\vec{\sigma}}{2}\cdot\hat{n}\alpha} e^{-i\frac{\vec{\sigma}}{2}\cdot\hat{n}(l_{0\alpha}(k-j)\theta)}]|\psi\rangle\right) \tag{73}$$

$$= \max_\psi \left(2 - \langle\psi|[e^{i\frac{\vec{\sigma}}{2}\cdot\hat{n}(l_{0\alpha}(k-j)\theta-\alpha)} + e^{-i\frac{\vec{\sigma}}{2}\cdot\hat{n}(l_{0\alpha}(k-j)\theta-\alpha)}]|\psi\rangle\right) \tag{74}$$

$$= \max_\psi \left(2 - \langle\psi|2\cos[\frac{\vec{\sigma}\cdot\hat{n}}{2}\left(l_{0\alpha}(k-j)\theta - \alpha\right)]|\psi\rangle\right) \tag{75}$$

$$= \max_\psi \left(2 - 2\langle\psi|\cos\frac{\vec{\sigma}\cdot\hat{n}}{2}\varepsilon|\psi\rangle\right) \tag{76}$$

$$= \max_\psi \left(2 - 2\langle\psi|\cos\frac{\varepsilon}{2}|\psi\rangle\right) \tag{77}$$

$$= 2(1 - \cos\frac{\varepsilon}{2}) \leq \varepsilon. \tag{78}$$

See appendices A and B for the derivations of Eq.(77) and Eq.(78). We have managed to approximate $R_{\hat{n}}\left(\alpha\right)$ to the operator having the common rotation vector $\hat{n}$ but a different rotation angle, to arbitrary accuracy. Next, in turn we will see that $R_{\hat{n}}\left(\alpha\right)$ is replaced, using Hadamard gate $\tilde{H}$, with another rotation operator $R_{\hat{m}}\left(\alpha\right)$ that has the common rotation angle α but a different rotation vector $\hat{m}$. With $\sqrt{1+\cos^2\frac{\pi}{8}} \equiv P$, $\sqrt{1-\cos^4\frac{\pi}{8}} \equiv Q$,

$$\tilde{H} R_{\hat{n}}\left(\alpha\right) \tilde{H} \tag{79}$$

$$= \frac{1}{\sqrt{2}}(X+Z)\left(\tilde{I}\cos^2\frac{\pi}{8} - i\left(\frac{\cos\frac{\pi}{8}}{P}\left(X+Z\right) + \frac{\sin\frac{\pi}{8}}{P}Y\right)Q\right)\frac{1}{\sqrt{2}}(X+Z) \tag{80}$$

$$= \frac{1}{2}\left(2\hat{I}\cos^2\frac{\pi}{8} - i\left(\frac{\cos\frac{\pi}{8}}{P}2\hat{I}(X+Z) + \frac{\sin\frac{\pi}{8}}{P}(X+Z)Y(X+Z)\right)Q\right) \tag{81}$$

$$= \hat{I}\cos^2\frac{\pi}{8} - i\left(\frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}(X+Z) - \frac{\sin\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}Y\right)\sqrt{1-\cos^4\frac{\pi}{8}} \tag{82}$$

$$\equiv R_{\hat{m}}\left(\alpha\right) \tag{83}$$

The following identity equation for Pauli matrices is used to derive Eq.(82)(See appendix C):

$$(X+Z)Y(X+Z) = -2Y \tag{84}$$

Eq.(82) shows that $\tilde{H} R_{\hat{n}}\left(\alpha\right) \tilde{H}$ can be interpreted as a rotation operator $R_{\hat{m}}\left(\alpha\right)$ such that a two-component spinor is rotated by α around $\hat{m}$ defined as

$$\hat{m} = \left(\frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}, -\frac{\sin\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}, \frac{\cos\frac{\pi}{8}}{\sqrt{1+\cos^2\frac{\pi}{8}}}\right). \tag{85}$$

Since $\hat{n}$ and $\hat{m}$ are linearly independent, we can decompose an arbitrary single-qubit unitary operator U using $R_{\hat{n}}$ and $R_{\hat{m}}$ [1] as:

$$U = e^{i\tau} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\eta), \tag{86}$$

using certain three angles β, γ, and η, and $e^{i\tau}$ is a physically insignificant global phase.

Finally, we can verify that U is approximated to arbitrary accuracy using "$\pi/8$ gate" (or *T gate* for short) and Hadamard gate $\tilde{H}$. U is the target operator which we want to implement and is specified with three angles β, γ, and η, and certain two unit vectors $\hat{n}$ and $\hat{m}$. On the other hand, we can actually implement $R_{\hat{n}}(\theta_{0\beta}), R_{\hat{n}}(\theta_{0\gamma}), R_{\hat{n}}(\theta_{0\eta})$, and $\tilde{H}$, and we construct a composite operator V as

$$V \equiv R_{\hat{n}}(\theta_{0\beta}) \tilde{H} R_{\hat{n}}(\theta_{0\gamma}) \tilde{H} R_{\hat{n}}(\theta_{0\eta}). \tag{87}$$

Now let us evaluate the error $E(U, V)$ with $e^{i\tau}$ in U being dropped:

$$E\left(R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\eta), R_{\hat{n}}(\theta_{0\beta}) \tilde{H} R_{\hat{n}}(\theta_{0\gamma}) H R_{\hat{n}}(\theta_{0\eta})\right) \tag{88}$$

$$= E\left(R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\eta), R_{\hat{n}}(\theta_{0\beta}) R_{\hat{m}}(\theta_{0\gamma}) R_{\hat{n}}(\theta_{0\eta})\right) \tag{89}$$

$$\leq E\left(R_{\hat{n}}(\beta), R_{\hat{n}}(\theta_{0\beta})\right) + E\left(R_{\hat{n}}(\gamma), R_{\hat{n}}(\theta_{0\gamma})\right) + E\left(R_{\hat{n}}(\eta), R_{\hat{n}}(\theta_{0\eta})\right) \tag{90}$$

$$\leq 3\varepsilon, \tag{91}$$

where a widely-known mathematical theorem [1] is used for the derivation from Eq.(89) to Eq.(90). Recalling that $R_{\hat{n}}(\theta_{0\beta}), R_{\hat{n}}(\theta_{0\gamma})$, and $R_{\hat{n}}(\theta_{0\eta})$ are all made up of "$\pi/8$ gate" and $\tilde{H}$, V is decomposed to multiplications of "$\pi/8$ gate" and $\tilde{H}$. Thus, an arbitrary single-qubit unitary operator U is approximated to arbitrary accuracy to decompositions of "$\pi/8$ gate" and $\tilde{H}$. Therefore, by combining the fact that an arbitrary unitary operator with arbitrary size is decomposed to multiplication of CNOT and single-qubit unitary operator (mentioned in II A 3 b), we verify that CNOT, $\tilde{H}$ and "$\pi/8$ gate around z-axis" constitute a universal set of gates in quantum computing. Also, through the discussions in II A 3 a, II A 3 b, and II A 3 c, it is fair to say that the universal set of gates comprising CNOT, $\tilde{H}$ and "$\pi/8$ gate around z-axis" is the ultimate universal set of gates in quantum computing.

4. Examination of our potential computer's universality in quantum computing

We examine to what extent our potential computer under construction could be "universal." To this end, we compare the ultimate universal set of gates and our gates under

construction. The ultimate set is taken here among other universal ones because it is constituted by most simplified, i.e., most universal, gates.

Our gates under construction are $R_x(\phi), R_y(\phi), R_z(\phi)$ [1, 6], and Controlled-Z (*CPHASE* or U_{CZ} for short) [13, 14] defined as:

$$R_x(\phi) = \begin{pmatrix} \cos\frac{\phi}{2} & -i\sin\frac{\phi}{2} \\ -i\sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}, \tag{92}$$

$$R_y(\phi) = \begin{pmatrix} \cos\frac{\phi}{2} & -\sin\frac{\phi}{2} \\ \sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}, \tag{93}$$

$$R_z(\phi) = \begin{pmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{+i\frac{\phi}{2}} \end{pmatrix}, \tag{94}$$

$$U_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{95}$$

Our gate set above will be equivalent to the ultimate set of gates if $R_x(\phi), R_y(\phi)$, and $R_z(\phi)$ are available with $\phi = \pm\frac{\pi}{2}, \frac{\pi}{4}, \pi$. And in fact these rotation operators are available under precise experimental conditions. Thus, the author observes that ours constitute the universal set of gates in quantum computing. The details of how to replace (=construct) each member of the ultimate set of gates with ours are described as follows:

- For the Hadamard gate $\tilde{H}$

  $\tilde{H}$ is decomposed into various forms using rotation operators: $R_x(\phi), R_y(\phi)$, and $R_z(\phi)$.

$$\tilde{H} = R_x(\pi)e^{i\frac{3\pi}{4}}R_y(\frac{\pi}{2}) = e^{i\frac{\pi}{4}}R_y(-\frac{\pi}{2})R_x(\pi) = R_z(\pi)e^{i\frac{\pi}{4}}R_y(-\frac{\pi}{2}) \tag{96}$$

$$= e^{i\frac{3\pi}{4}}R_y(\frac{\pi}{2})R_z(\pi) = e^{-i\frac{\pi}{2}}R_x(-\frac{\pi}{2})R_z(-\frac{\pi}{2})R_x(-\frac{\pi}{2}) \tag{97}$$

$$= e^{i\frac{3\pi}{2}}R_y(\frac{\pi}{4})R_x(\pi)R_y(-\frac{\pi}{4})R_z(-\frac{\pi}{2})R_x(\pi)R_z(\frac{\pi}{2}) \tag{98}$$

- For "the $\pi/8$ gate" (or T gate for short)

  T can be prepared directly from $R_z\left(\frac{\pi}{4}\right)$.

$$e^{i\frac{\pi}{8}}R_z\left(\frac{\pi}{4}\right) \equiv T. \tag{99}$$

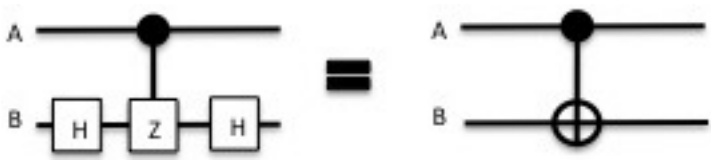

FIG. 14. The left diagram $\tilde{H}_B U_{CZ} \tilde{H}_B$ is equivalent to CNOT on the right. The proof is given in the text.

- For the CNOT gate (or U_{CN} for short)
  Using $\tilde{H}$ above, U_{CN} is decomposed to $\tilde{H}$ and U_{CZ} as follows:

$$\tilde{H}_B U_{CZ} \tilde{H}_B = \left(\tilde{I}_A \otimes \tilde{H}_B\right) U_{CZ} \left(\tilde{I}_A \otimes \tilde{H}_B\right) \tag{100}$$

$$= \begin{pmatrix} \tilde{H}_B & 0 \\ 0 & \tilde{H}_B \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} \tilde{H}_B & 0 \\ 0 & \tilde{H}_B \end{pmatrix} \tag{101}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \tag{102}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \equiv U_{CN} \tag{103}$$

  This replacement may be drawn in FIG. 14.

B. Quantum advantage of our potential computer

The author attempts to assess to what extent our potential computer under construction could be useful from a viewpoint of its availability to solve a real problem. The problem given here is known as one that can be solved in much less steps than usual if the computer implements so-called *the Deutsch-Jozsa algorithm*[2]. To implement DJA, the multi-qubit, say n, Hadamard gate $\tilde{H}^{\otimes n}$ is required, where $\tilde{H}$ cannot be implemented unless it is a

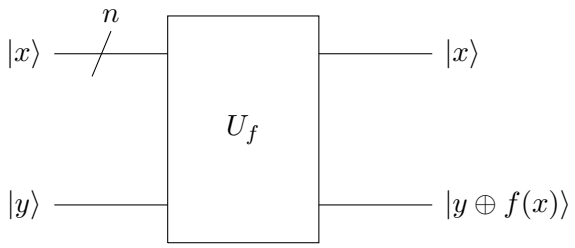

FIG. 15. A schematic diagram to represent the problem to solve. Through a black box (or *oracle*) U_f, the two inputs, $|x\rangle$ and $|y\rangle$, are processed to provide two outputs, $|x\rangle$ and $|y \oplus f(x)\rangle$, where $x \in \{0,1\}^n, y \in \{0,1\}$.

quantum computer. Thus, it is fair to claim that a quantum computer that $H^{(n)}$ can be implemented on is useful in that it is ready to exhibit so-called *quantum advantage* over classical computers. In the preceding, the author defines the problem to solve and explain how DJA works to help to accelerate problem-solving by following the procedures in [3, 15], and examines the availability of DJA on our potential computer.

1. Definition of the problem to solve

Let x be some n-bit sequence and let y be either 0 or 1, i.e., $x \in \{0,1\}^n, y \in \{0,1\}$. Now imagine a black box (or "an oracle" in a computer glossary) U_f such that

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle, \tag{104}$$

where $f(x)$ takes one of the following two characteristics:

1. $f(x)$ is a *constant* function: the value of $f(x)$ is either 0 or 1 for all arguments x's (=n-bit sequences).

2. $f(x)$ is a *balanced* function: the value of $f(x)$ is 0 for 50% of all the possible arguments x's or 1 for the rest (= 50%) of the possible arguments.

When U_f is given, decide which of the two characteristics has been given to $f(x)$. Here "When U_f is given" means that we are allowed to know of as many sets of $\{|x, y\rangle, |x, y \oplus f(x)\rangle\}$ as we want upon our request. The problem may be drawn in the diagram in FIG. 15.

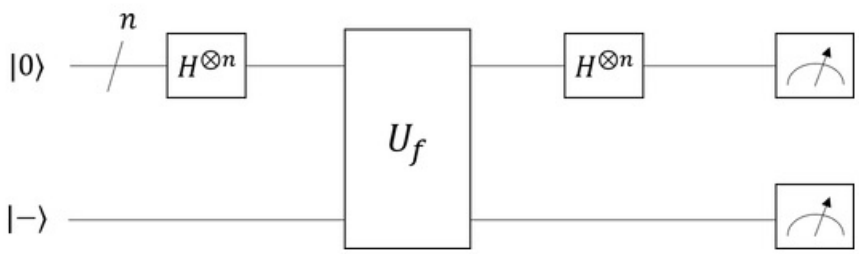

FIG. 16. A diagram to represent a solution to the problem using the Deutsch-Joza algorithm. We set an input state $|x\rangle$ as $|000\cdots0\rangle$, set another input state $|y\rangle$ as $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and measure the first n-qubit of the output state. This diagram is taken from [3].

2. How the Deutsch-Jozsa algorithm enables us to solve it in less steps

a. Classical approach to the problem Before introducing the Deutsch-Jozsa algorithm, let us take a look at how to solve it in a classical manner. How many trials are needed to decide the characteristics of $f(x)$? In other words, how many times do we need to carry out U_f operation? Consider it depending on the answer. In case that $f(x)$ has been set "balanced", the minimum number of necessary trial is 2 if we are lucky. For if the first output is different from the second one, this means that $f(x)$ is not "constant" and this implies that $f(x)$ is "balanced." On the other hand, the maximum number of necessary trial is $\frac{2^2}{2} + 1$. The total number of different sequences is 2^n, and we cannot be sure that $f(x)$ is "balanced" until we try half of the input arguments plus one extra trial. In case that $f(x)$ has been set "constant", the necessary number of trial of U_f is always $\frac{2^2}{2} + 1$. As is the case of "balanced", we cannot be sure that $f(x)$ is "constant" until we try half of the input arguments plus one extra trail.

Remind that even if the *ket* representation like $|x, y\rangle$ is used, this does not necessarily mean that the problem is being treated in quantum mechanically. In fact, we have just treated it completely classically.

b. The Deutsch-Jozsa algorithm The author will see how to handle the problem by exploiting the concepts in quantum mechanics. First, the quantum mechanical solution to it is represented in a form of diagram in FIG. 16, following which the solution is explained below.

For a n-qubit state $|a\rangle$;

$$|a\rangle \equiv |a_0\rangle \otimes |a_1\rangle \otimes |a_2\rangle \otimes |a_1\rangle \otimes \cdots \otimes |a_{n-1}\rangle, \tag{105}$$

we apply the n-qubit Hadamard gate $\tilde{H}^{\otimes n}$, i.e.,

$$\tilde{H}^{\otimes n} = \tilde{H}_0|a_0\rangle \otimes \tilde{H}_1|a_1\rangle \otimes \tilde{H}_2|a_2\rangle \otimes \cdots \otimes \tilde{H}_{n-1}|a_{n-1}\rangle, \tag{106}$$

where

$$\tilde{H}_s|a_s\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(|0\rangle_s + |1\rangle_s\right) \ (\text{for } a_s = 0) \\ \frac{1}{\sqrt{2}}\left(|0\rangle_s - |1\rangle_s\right) \ (\text{for } a_s = 1) \end{cases}. \tag{107}$$

A target is to deform RHS of Eq.(106) for a n-qubit state. In preparation for it, let us examine a case of a state comprising a smaller number of qubits, 4, for example, and $|a\rangle \equiv |1\rangle_0 \otimes |0\rangle_1 \otimes |1\rangle_2 \otimes |1\rangle_3$. For this $|a\rangle$, $\tilde{H}^{\otimes 4}|a\rangle$ leads to,

$$\frac{1}{\sqrt{2}}\left(|0\rangle_0 - |1\rangle_0\right) \otimes \frac{1}{\sqrt{2}}\left(|1\rangle_1 + |1\rangle_1\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_2 - |1\rangle_2\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_3 - |1\rangle_3\right) \tag{108}$$

$$= \frac{1}{\sqrt{2^4}}(|0\rangle_0|0\rangle_1|0\rangle_2|0\rangle_3 - |0\rangle_0|0\rangle_1|0\rangle_2|1\rangle_3 + |0\rangle_0|0\rangle_1|1\rangle_2|1\rangle_3 \cdots - |1\rangle_0|1\rangle_1|1\rangle_2|1\rangle_3), \tag{109}$$

where $|x\rangle_0 \otimes |x\rangle_1 \otimes |x\rangle_2 \otimes |x\rangle_3 \equiv |x\rangle_0|x\rangle_1|x\rangle_2|x\rangle_3 \equiv |x_0x_1x_2x_3\rangle$. Here, the sign of each term is determined as follows: $|x\rangle_0 = |0\rangle_0$ comes from either $|a_0\rangle = |0\rangle_0$ or $|1\rangle_0$. Recalling Eq.(107), whichever between $|0\rangle_0$ and $|1\rangle_0$ produces $|x\rangle_0$, $|x\rangle_0$ does not come with (-1). On the other hand, despite $|x\rangle_0 = |1\rangle_0$ comes from either $|a_0\rangle = |0\rangle_0$ or $|1\rangle_0$, $|x\rangle_0 = |1\rangle_0$ does actually come with (-1) when being produced from $|a_0\rangle = |1\rangle_1$. That is, $|x_k\rangle$ comes with (-1) if and only if $(a_k = 1)\&(x_k = 1)$. Therefore, for a term $|x_0x_1x_2x_3\rangle$, (-1) is put on top of it if and only if $\sum_{k=0}^{3} x_k a_k$ is odd. Using the observation above, the n-qubit Hadamard operation on $|a\rangle$ leads to

$$\tilde{H}^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x' \in \{0,1\}^n} (-1)^{\sum_{i=0}^{n} x_i a_i} |x'\rangle \tag{110}$$

In our case, following the FIG. 16, we take the input $|x\rangle$ such that

$$|a\rangle \equiv |000\cdots0\rangle \tag{111}$$

, to have

$$\tilde{H}^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x' \in \{0,1\}^n} |x'\rangle. \tag{112}$$

Also, take $|y\rangle$ as

$$|y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{113}$$

Thus, we have $U_f|x,y\rangle$ as

$$U_f|x,y\rangle = |x, y\oplus f(x)\rangle = \frac{1}{\sqrt{2^n}}|\sum_{x'\in\{0,1\}^n}|x'\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\oplus f(x')\rangle \tag{114}$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_{x'\in\{0,1\}^n}(|x'\rangle\,(|0\oplus f(x')\rangle - |1\oplus f(x')\rangle)) \tag{115}$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_{x'\in\{0,1\}^n}\left((-1)^{f(x')}|x'\rangle\,(|0\rangle - |1\rangle)\right). \tag{116}$$

Here, the following relation was used:

$$|0\oplus f(x')\rangle - |1\oplus f(x')\rangle = \begin{cases} (|0\rangle - |1\rangle \ \ (\text{for } f(x')=0) \\ (|1\rangle - |0\rangle \ \ (\text{for } f(x')=1) \end{cases}. \tag{117}$$

Eq.116 surprises us that the information of $f(x)$, which is originally expected to affect y, appears as $(-1)^{f(x')}$. Thus, with Eq.116, we drop the $(n+1)th$ term and take the first n terms only, to obtain

$$\frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')}|x'\rangle. \tag{118}$$

We remind that this state in Eq.118 is the one that comes out from the black box U_f.

Then, let us apply $\tilde{H}^{\otimes n}$ again on the state in Eq.118 and we will obtain

$$\tilde{H}^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')}|x'\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')}\tilde{H}^{\otimes n}|x'\rangle \tag{119}$$

$$= \frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}\left((-1)^{f(x')}\left(\frac{1}{\sqrt{2^n}}\sum_{Z\in\{0,1\}^n}(-1)^{\sum_{i=0}^n x'_i Z_i}|Z\rangle\right)\right) \tag{120}$$

$$= \frac{1}{2^n}\sum_{x'\in\{0,1\}^n}\sum_{Z\in\{0,1\}^n}(-1)^{f(x')+\sum_{i=0}^n x'_i Z_i}|Z\rangle \tag{121}$$

$$= \frac{1}{2^n}\sum_{x'\in\{0,1\}^n}\sum_{Z\in\{0,1\}^n}(-1)^{f(x')\oplus Z\cdot x'}|Z\rangle. \tag{122}$$

The last form Eq.122 implies that the probability amplitude for some $|Z\rangle$ is

$$\frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')\oplus Z\cdot x'}. \tag{123}$$

Now, let us calculate the probability amplitude for $|Z\rangle = |000\cdots0\rangle$. The square of the absolute value of the amplitude correspond to the probability of $|000\cdots0\rangle$ being measured when we measure the output state. The probability amplitude is found out to be

$$\frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')\oplus Z\cdot x'} = \frac{1}{\sqrt{2^n}}\sum_{x'\in\{0,1\}^n}(-1)^{f(x')}. \tag{124}$$

This form means that the probability amplitude for $|Z\rangle = |000\cdots0\rangle$ is simply classified depending on the characteristics of $f(x)$ into,

$$\begin{cases} 1 & (\text{if } f(x) = 0) \\ -1 & (\text{if } f(x) = 1)\,. \\ 0 & (\text{otherwise}) \end{cases} \tag{125}$$

That is, if $f(x)$ is "constant", all time we measure the output, $|000\cdots0\rangle$ is measured, while if $f(x)$ is "balanced", we will never measure $|000\cdots0\rangle$. In brief, with DJA, we can solve the problem instantly by following the procedures in the diagram in FIG. 16, where we set an input state $|x\rangle$ as $|000\cdots0\rangle$, set another input state $|y\rangle$ as $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and measure the first n-qubit of the output state.

3. Examination of the availability of DJA on our potential computer

We examine the availability of DJA on our potential computer under construction. As seen above, the point is whether it implements the n-qubit Hadamard gate $\tilde{H}^{\otimes n}$ or not. As discussed in II A 4 above, the Hadamard gate $\tilde{H}$ is available on our potential computer under the circumstances where we can prepare $R_x(\phi), R_y(\phi)$, and $R_z(\phi)$ with $\phi = \pm\frac{\pi}{2}, \pm\frac{\pi}{4}$, and π. Thus, our potential computer can implement the Deutsch-Jozsa algorithm that can be implemented on a universal quantum computer only. This implies that ours is ready to exhibit the quantum advantage that quantum computer has, in that DJA enables it to solve some certain problem in much less steps than classical computing. What should also be pointed out is the preparation of the multiple qubit version of $\tilde{H}$ is critical for the implementation of DJA.

III. SUMMARY AND FUTURE ISSUES

We can confirm that our gate set is equivalent to the ultimate universal set of gates in quantum computing in that each members of the ultimate set proves to be constructed using appropriate multiplications of the members of ours. The availability of the ultimate set makes it possible to construct an arbitrary unitary matrix, the key to implement a universal quantum computer; thus, our potential computer proves to be universal. The Hadamard gate $\tilde{H}$, the vital gate in quantum information processing, can be constructed using our

three single-qubit rotation operators $R_x(\phi), R_y(\phi)$, and $R_z(\phi)$ with the rotation angles of $\phi = \pm\frac{\pi}{2}, \pm\frac{\pi}{4}$, and π. We can also confirm that our potential computer can implement the Deutsch-Jozsa algorithm using our computer's universality. DJA makes it possible to solve a certain problem in much less steps than classical computing; thus, our potential computer is confirmed to possess quantum advantage.

We must tackle plenty of outstanding issues in the frame work of mathematical physics, following the basic work in this article. From an aspect of a QIP algorithm, important and urgent issues include a discovery of a new problem that is soluble on a quantum computer, the development of an efficient QIP code for either a well-known problem or a new problem, and the development of an error correction code [16–18], with keeping the compatibility with the physical characteristics of the computer. From an aspect of materials physics, helping to design QIP physical implementation from a quantum dynamical approach is among the issues required. It might be a good idea to start it from analysing some specific structures that are aimed to work as single-qubit gates, i.e.,$R_x(\phi), R_y(\phi)$, and $R_z(\phi)$, and the two-qubit gate, i.e., the CPHASE gate, by numerically calculating the time evolution of the quantum states (See [19] for calculating a time evolution of quantum wave packet). How the states deform as times goes by will provide information about various limiting performances, including the maximum time limit for the structures to function appropriately as quantum gates. Apart from above, we might have to examine the predictions that distinct two-level quantum state can no longer be available in some extreme conditions[20–23].

Appendix A: Derivation of Eq.(77)

Pauli matrices $\vec{\sigma} \equiv (\sigma_x, \sigma_y, \sigma_z)$ satisfy the following identity equation for an odd number m for an arbitrary unit vector $\hat{p}$ [6],

$$(\vec{\sigma} \cdot \hat{p})^m \equiv 1. \tag{A1}$$

Appendix B: Derivation of Eq.(78)

We derive $\sin^2 x \leq x$ using a concrete example. We compare two areas inside a circle of radius 1 with common angle x $(0 < x < \frac{\pi}{2})$ (FIG. 17). One is a sector S_1 of radius 1: $S_1 = \pi \cdot 1^2 \times \frac{x}{2\pi} = \frac{x}{2}$. The other is a triangle S_2 that has base 1 and height $\sin x$:

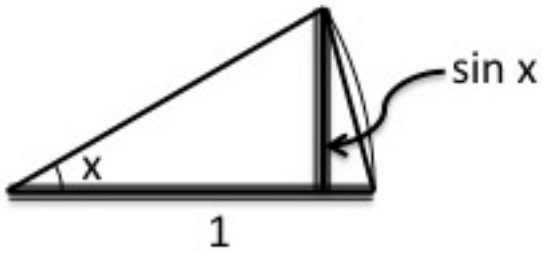

FIG. 17. A sector of a circle of radius 1 and angle x.

$S_2 = 1 \cdot \sin(x) \times \frac{1}{2} = \frac{\sin x}{2}$. By construction, $S_2 \leq S_1$, i.e.,

$$\frac{\sin x}{2} \leq \frac{x}{2}, \tag{B1}$$

thus

$$\sin x \leq x. \tag{B2}$$

Combining Eq.(B2) with

$$\sin x \leq 1, \tag{B3}$$

we have

$$2\sin^2 x \leq 2x. \tag{B4}$$

On the other hand, with $\varepsilon/2 \equiv 2x$,

$$1 - \cos\frac{\varepsilon}{2} = 1 - \cos 2x = 2\sin^2 x. \tag{B5}$$

Using Eq.(B4) and Eq.(B5), we reach

$$2\left(1 - \cos\frac{\varepsilon}{2}\right) \leq \varepsilon. \tag{B6}$$

Appendix C: Derivation of Eq.(82)

Using the commutation and anti-commutation relations among Pauli matrices $\sigma_x(\equiv X), \sigma_y(\equiv Y), \sigma_z(\equiv Z)$:

$$[X, Y] = 2iZ, \tag{C1}$$

$$\{X, Y\} = 0, \tag{C2}$$

we have

$$(X+Z)Y(X+Z) = XYX + ZYX + XYZ + ZYZ \tag{C3}$$
$$= (iZ)X + Z(-iZ) + (iZ)Z + Z(iX) \tag{C4}$$
$$= -ZX - iZ^2 + iZ^2 + iZX \tag{C5}$$
$$= 2iZX = 2i(iY) = -2Y. \tag{C6}$$

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, United Kingdom, 2000).

[2] D. Deutsch and R. Jozsa, Proceedings of the Royal Society of London A **439**, 553 (1992).

[3] @tehishik, "Introduction to Quantum Computing through learning Quantum Katas $|4\rangle$: Deutsch-Jozsa Algorithm," https://qiita.com/tehishik/items/1e68c6e2ee0605b3cd16.

[4] A. Papageorgiou and J. F. Traub, Physical Review A **88**, 022316 (2013).

[5] J. Preskill, "Quantum computing and the entanglement frontier," (2012), arXiv:1203.5813 [quant-ph].

[6] J. J. Sakurai, *Modern Quantum Mechanics (Revised Edition)* (Addison-Wesley, MA, USA, 1994).

[7] K. Riley, M. Hobson, and S. Bence, *Mathematical Methods for Physics and Engineering (Third Edition)* (Cambridge University Press, Cambridge, United Kingdom, 2006).

[8] P. A. M. Dirac, *The Principles of Quantum Mechanics* (Oxford University Press, Oxford, United Kingdom, 1958).

[9] G. B. Arfken and H. J. Weber, *Mathematical Methods for Physicists (Fifth Edition)* (Academic Press, CA, USA, 2001).

[10] @ground0state, "Comments on the universality of a universal quantum computer," https://qiita.com/ground0state/items/aaf924cce37f71fad149.

[11] P. G. L. Dirichlet, "Vorlesungen über zahlentheorie," (1834), (Lectures on Number Theory, prepared for publication by Dedekind, first edition 1863).

[12] I. N. Herstein, *Topics In Algebra* (Blaisdell Publishing Company, MA, USA, 1964).

[13] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Review of Modern Physics **79**, 135 (2007).

[14] D. J. Brod and J. Combesn, Physical Review Letters **117**, 080502 (2016).

[15] Microsoft Corporation, "QuantumKatas," https://github.com/Microsoft/QuantumKatas.

[16] C. D. Hill, E. Peretz, S. J. Hile, M. G. House, M. Fuechsle, S. Rogge, M. Y. Simmons, and L. C. L. Hollenberg, Science Advances **1**, e1500707 (2015).

[17] M. Veldhorst, H. G. J. Eenink, C. H. Yang, and A. S. Dzurak, Nature Communications **8**, 1 (2017).

[18] M. Veldhorst, C. H. Yang, J. C. C. Hwang, W. H. J. P. Dehollain, J. T. Muhonen, S. Simmons, A. Lauxhit, F. E. Hudson, K. M. Itoh, A. Morello, and A. S. Dzurak, Nature **526**, 410 (2015).

[19] T. Iitaka, Physical Review E **49**, 4648 (1994).

[20] B. Georgeot and D. L. Shepelyansky, Physical Review E **62**, 6366 (2000).

[21] B. Georgeot and D. L. Shepelyansky, Physical Review Letters **86**, 2890 (2001).

[22] B. Georgeot and D. L. Shepelyansky, Physical Review E **62**, 3504 (2000).

[23] B. Georgeot and D. L. Shepelyansky, "Quantum Computing of Classical Chaos: Smile of the Arnold-Schrödinger Cat," (2001), arXiv:quant-ph/0101004v1.

About the author

[1] Mr. Kiyotaka HAMMURA

Mr. Kiyotaka HAMMURA, DSc is a researcher at Meiji University in Tokyo, Japan and a researcher at Fukushima University, Japan. He teaches Physics and Mathematics. His research interests include studying novel computational algorithms by combining Machine Learning with Quantum Computing. Email: hammurak@gmail.com

[2] Mr. Katsuhiko YAMAGUCHI

Mr. Katsuhiko YAMAGUCHI, PhD is a professor at Fukushima University, Japan. He teaches Quantum Physics. His research interests include solid-state magnetism.

Email: yama@sss.fukushima-u.ac.jp

[3] Mr. Kazuo SAKAI

Mr. Kazuo SAKAI, DSc is a professor at Meiji University in Tokyo, Japan. He teaches Science. His research interests include innovation and educational effects. Email: sakai@meiji.ac.jp