A-010

A Result on Complexity of Quantum Computation

Mitsuru Hamada

I. Introduction

One fundamental issue often discussed in the literature on quantum computation is that on realization of an arbitrary unitary operator with universal gates. It is known that, in principle, there exist universal sets of gates, which are building blocks of quantum circuits [1]. Known arguments on the universality reduce the issue of constructing any unitary operation on multiple primitive systems to that of constructing any unitary operation on a single primitive system [2]. The primitive system is represented by a two-dimensional Hilbert space, and is sometimes called a quantum-bit system. This work is concerned with the issue of constructing an arbitrary unitary operator on the two-dimensional Hilbert space.

Such unitary operators are often represented as 2×2 unitary matrices, and any 2×2 unitary matrix is a scalar multiple of an element of $\mathrm{SU}(2)$. Recall that the group under multiplication $\mathrm{SU}(2)$ consists of 2×2 unitary matrices with determinant 1, and $\mathrm{SO}(3)$ consists of 3×3 orthogonal matrices with determinant 1. There is a homomorphism from $\mathrm{SU}(2)$ onto $\mathrm{SO}(3)$. Thus, we often speak of rotations to mean elements of $\mathrm{SU}(2)$.

II. Definitions

Let X, Y, and Z denote the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Throughout, I denotes the 2×2 identity matrix.

We will work with a matrix

$$R_{\hat{v}}(\theta) = (\cos\tfrac{\theta}{2})I - i(\sin\tfrac{\theta}{2})(v_x X + v_y Y + v_z Z) \quad (1)$$

where $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ with $\|\hat{v}\| = \sqrt{v_x^2 + v_y^2 + v_z^2} = 1$ and $\theta \in \mathbb{R}$, with $\mathbb{R}$ denoting the set of real numbers. Note in traditional quantum physics [3], special attentions are paid to $R_{\hat{v}}(\theta)$ with $\hat{v} = (0,1,0)^{\mathrm{T}}$ and $R_{\hat{v}}(\theta)$ with $\hat{v} = (0,0,1)^{\mathrm{T}}$, which we denote by $R_y(\theta)$ and $R_z(\theta)$, respectively.

We put $S^2 = \{\hat{v} \in \mathbb{R}^3 \mid \|v\| = 1\}$; $\mathbb{N}$ denotes the set of strictly positive integers; $\lceil x \rceil$ denotes the smallest integer not less than $x \in \mathbb{R}$. As usual, $\arccos x \in [0, \pi]$ for $x \in [-1, 1]$.

The author is with Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan.

III. Method for Decomposing Arbitrary Rotations

Theorem 1: Let vectors $\hat{m}, \hat{n} \in S^2$ such that $0 < \hat{m}^{\mathrm{T}}\hat{n} < 1$ be given. Put $\hat{l} = \|\hat{n} \times \hat{m}\|^{-1}\hat{n} \times \hat{m}$. Then, for any $\alpha, \gamma \in \mathbb{R}$, and $\beta \in (0, \pi]$,

$$R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma) = R_{\hat{m}}(\alpha - \alpha_1)R_{\hat{n}}(\theta_1)R_{\hat{m}}(-\gamma_1)[R_{\hat{m}}(-\pi)R_{\hat{n}}(\pi)]^{k-1}R_{\hat{m}}(\gamma)$$

where

$$k = \left\lceil \frac{\beta}{2\arccos \hat{m}^{\mathrm{T}}\hat{n}} \right\rceil, \quad (2)$$

$$\alpha_1 = \eta_1 - \zeta_1 \quad \text{and} \quad \gamma_1 = \eta_1 + \zeta_1, \quad (3)$$

and with

$$\beta_1 = \beta - 2(k-1)\arccos \hat{m}^{\mathrm{T}}\hat{n},$$

$\theta_1, \eta_1, \zeta_1$ are specified by

$$|\sin\tfrac{\theta_1}{2}| = \frac{\sin\frac{\beta_1}{2}}{\sqrt{1 - \hat{m}^{\mathrm{T}}\hat{n}}},$$

$$\cos\eta_1 = \frac{\cos\frac{\theta_1}{2}}{\cos\frac{\beta_1}{2}} \quad \text{and} \quad \sin\eta_1 = \frac{\hat{m}^{\mathrm{T}}\hat{n}\sin\frac{\theta_1}{2}}{\cos\frac{\beta_1}{2}}, \quad (4)$$

and

$$\sin\zeta_1 = \frac{(\hat{l} \times \hat{m})^{\mathrm{T}}\hat{n}\sin\frac{\theta_1}{2}}{\sin\frac{\beta_1}{2}} \quad \text{and} \quad \cos\zeta_1 = \frac{\hat{l}^{\mathrm{T}}\hat{n}\sin\frac{\theta_1}{2}}{\sin\frac{\beta_1}{2}}. \quad (5)$$

This suggests how to decompose an arbitrary element $U \in \mathrm{SU}(2)$. The decomposition can be represented as a function $\Omega(\hat{m}, \hat{n}, U)$ to be described below.

We can show that if $\hat{l}$ and $\hat{m} \in S^2$ are orthogonal, any element $U \in \mathrm{SU}(2)$ can be written as $R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma)$ with $(\alpha, \beta, \gamma) \in \mathcal{A}$, where $\mathcal{A} \subset \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is some region such that $\{\beta \mid (\alpha, \beta, \gamma) \in \mathcal{A}\} = [0, \pi]$ and for any $U \in \mathrm{SU}(2)$, a triple $(\alpha, \beta, \gamma) \in \mathcal{A}$ satisfying $U = R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma)$ is unique (see Appendices, in particular, (35)).

Let $\mathcal{W} = \{(\hat{m}, \hat{n}, U) \in S^2 \times S^2 \times \mathrm{SU}(2) \mid 0 < \hat{m}^{\mathrm{T}}\hat{n} < 1\}$. We define a function $\Omega : \mathcal{W} \to \mathcal{L}$, where $\mathcal{L}$ consists of all j-tuple that can be written as $(V_1, \ldots, V_j) \in \mathrm{SU}(2)^j$ with some $j \in \mathbb{N}$.

Given an arbitrary element $U \in \mathrm{SU}(2)$, write $U = R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma)$ with some $(\alpha, \beta, \gamma) \in \mathcal{A}$, where $\hat{l} = \|\hat{n} \times \hat{m}\|^{-1}\hat{n} \times \hat{m}$.

First, assume $\beta > 0$. For this (α, β, γ), put

$$\begin{aligned} V_1 &= R_{\hat{m}}(\alpha - \alpha_1), \\ V_2 &= R_{\hat{n}}(\theta_1), \\ V_3 &= R_{\hat{m}}(-\gamma_1 - \pi), \\ V_4 &= R_{\hat{n}}(\pi), \\ V_5 &= R_{\hat{m}}(-\pi), \\ &\cdots, \\ V_{2k} &= R_{\hat{n}}(\pi), \\ V_{2k+1} &= R_{\hat{m}}(\gamma) \end{aligned}$$

where $k, \alpha_1, \gamma_1, \theta_1$ are as in Theorem 1. Remove all identity matrices Is in $(V_1, \ldots, V_{2k+1})$ to obtain L as the result. Then, set $\Omega(\hat{m}, \hat{n}, U) = L$. Here, the meaning of removing Is in $(V_1, \ldots, V_{2k+1})$ should be clear. For example, removing Is in $L_{\mathrm{o}} = (X, I, Y, I, I, Z)$ means obtaining $L = (X, Y, Z)$ from L_{o}. If $\beta = 0$, set $\Omega(\hat{m}, \hat{n}, U) = U$.

A natural measure of goodness of a method for decomposing unitary matrices in $\mathrm{SU}(2)$ is the length of the output, i.e., the number of constituent unitary matrices. In this sense, $\Omega(\hat{m}, \hat{n}, U)$ is good, and in some mathematical problem formulation, the author has proved that Ω achieves the optimal performance for some region. Namely, the output length of Ω cannot be improved for a wide range of targets. For other regions, the following decomposition is useful: $\Omega'(\hat{m}, \hat{n}, U, V) = \mathrm{cat}[V, \Omega(\hat{m}, \hat{n}, V^\dagger U)]$, where $\mathrm{cat}[L, L']$ means the concatenation of the lists L and L' in this order. In $\Omega'(\hat{m}, \hat{n}, U, V)$, the target to be decomposed is U. How to tune $V \in \mathrm{SU}(2)$ would not be obvious. It would be presented elsewhere together with a proof of the optimality of $\Omega'(\hat{m}, \hat{n}, U, V)$ (note Ω' includes Ω as a special case).

In the rest of this article, a proof of Theorem 1 is presented in such a way that how it has been found is described. The proof is based on unpublished results of this author [4], and a large portion is devoted to presenting these results.

IV. Fundamental lemma on Euler angles

The above theorem was found using the following lemma (or its generalization below) of the author (unpublished manuscript (2012), an abstract of which is [4]).

Lemma 1: For any $\phi, \beta, \theta \in \mathbb{R}$ and $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ with $v_x^2 + v_y^2 + v_z^2 = 1$, the following two conditions are equivalent.

I. There exist some $\alpha, \gamma \in \mathbb{R}$ such that

$$R_{\hat{v}}(\theta) = e^{i\phi} R_z(\alpha) R_y(\beta) R_z(\gamma). \tag{6}$$

II. Both of the following hold:

$$e^{i\phi} \in \{1, -1\}, \tag{7}$$

$$\sqrt{1 - v_z^2} |\sin\tfrac{\theta}{2}| = |\sin\tfrac{\beta}{2}|. \tag{8}$$

Proof of Lemma 1.

0) We will first give a more concrete form of (6). A direct calculation shows

$$\begin{aligned} &R_z(\alpha) R_y(\beta) R_z(\gamma) \\ &\quad = \cos\frac{\beta}{2} \cos\frac{\gamma+\alpha}{2} I - i \sin\frac{\beta}{2} \sin\frac{\gamma-\alpha}{2} X \\ &\qquad - i \sin\frac{\beta}{2} \cos\frac{\gamma-\alpha}{2} Y - i \cos\frac{\beta}{2} \sin\frac{\gamma+\alpha}{2} Z. \end{aligned} \tag{9}$$

Hence, (6) is equivalent to

$$\begin{cases} \cos\frac{\theta}{2} = e^{i\phi} \cos\frac{\beta}{2} \cos\frac{\gamma+\alpha}{2}, & (10) \\ v_x \sin\frac{\theta}{2} = e^{i\phi} \sin\frac{\beta}{2} \sin\frac{\gamma-\alpha}{2}, & (11) \\ v_y \sin\frac{\theta}{2} = e^{i\phi} \sin\frac{\beta}{2} \cos\frac{\gamma-\alpha}{2}, & (12) \\ v_z \sin\frac{\theta}{2} = e^{i\phi} \cos\frac{\beta}{2} \sin\frac{\gamma+\alpha}{2}. & (13) \end{cases}$$

1) We will prove I $\Rightarrow$ II.

From (10), we have $e^{i\phi} \in \mathbb{R}$, i.e., (7). On each side of (11) and (12), taking the absolute values, squaring, summing the resultant pair, we have (8). [Eqs. (10) and (13) also imply (8) similarly.]

2) Next, we will prove II $\Rightarrow$ I.

Transforming (α, β) into (η, ζ), where the two pairs are related by

$$\eta = \frac{\gamma+\alpha}{2} \quad \text{and} \quad \zeta = \frac{\gamma-\alpha}{2}, \tag{14}$$

we see that I is equivalent to the following condition: There exist some $\eta, \zeta \in \mathbb{R}$ such that

$$\begin{cases} \cos\frac{\theta}{2} = e^{i\phi} \cos\frac{\beta}{2} \cos\eta, & (15) \\ v_x \sin\frac{\theta}{2} = e^{i\phi} \sin\frac{\beta}{2} \sin\zeta, & (16) \\ v_y \sin\frac{\theta}{2} = e^{i\phi} \sin\frac{\beta}{2} \cos\zeta, & (17) \\ v_z \sin\frac{\theta}{2} = e^{i\phi} \cos\frac{\beta}{2} \sin\eta. & (18) \end{cases}$$

Hence, we will prove that (15)–(18) are implied by II.

Now suppose $\cos\frac{\beta}{2} \neq 0$. Then, if we show

$$\frac{\cos^2\frac{\theta}{2}}{\cos^2\frac{\beta}{2}} + \frac{v_z^2 \sin^2\frac{\theta}{2}}{\cos^2\frac{\beta}{2}} = 1, \tag{19}$$

it will imply the existence of η satisfying (15) and (18). Namely, η will be specified by

$$\cos\eta = \frac{\cos\frac{\theta}{2}}{e^{i\phi}\cos\frac{\beta}{2}} \quad \text{and} \quad \sin\eta = \frac{v_z \sin\frac{\theta}{2}}{e^{i\phi}\cos\frac{\beta}{2}}, \tag{20}$$

where we should note $e^{i\phi} \in \{1, -1\}$ by assumption II. From (8) of II, however, we have $(1 - v_z^2)\sin^2\frac{\theta}{2} = \sin^2\frac{\beta}{2}$, i.e., $1 - (1 - v_z^2)\sin^2\frac{\theta}{2} = \cos^2\frac{\beta}{2}$, which is equivalent to (19) by the assumption $\cos\frac{\beta}{2} \neq 0$.

If $\cos\frac{\beta}{2} = 0$, then $|\sin\frac{\beta}{2}| = 1$. This and II imply $1 - v_z^2 = |\sin\frac{\theta}{2}| = 1$, and hence, $v_z = \cos\frac{\theta}{2} = 0$. Then, both (15) and (18) hold for any choice of η.

In a similar way, if $\sin\frac{\beta}{2} \neq 0$,

$$\frac{v_x^2 \sin^2\frac{\theta}{2}}{\sin^2\frac{\beta}{2}} + \frac{v_y^2 \sin^2\frac{\theta}{2}}{\sin^2\frac{\beta}{2}} = 1 \tag{21}$$

will imply the existence of ζ satisfying (16) and (17). Namely, ζ will be specified by

$$\sin\zeta = \frac{v_x \sin\frac{\theta}{2}}{e^{i\phi}\sin\frac{\beta}{2}} \quad \text{and} \quad \cos\zeta = \frac{v_y \sin\frac{\theta}{2}}{e^{i\phi}\sin\frac{\beta}{2}}. \tag{22}$$

But (21) follows again from (8) since $1 - v_z^2 = v_x^2 + v_y^2$. If $\sin\frac{\beta}{2} = 0$, both (16) and (17) hold for any choice of ζ similarly. □

We remark that we have done more than showing the existence of parameters α, γ in the above proof. Specifically, suppose we are given an arbitrary rotation $R_{\hat{v}}(\theta)$, and want to choose some $\alpha, \beta, \gamma \in \mathbb{R}$ such that $R_{\hat{v}}(\theta) = R_y(\alpha)R_z(\beta)R_y(\gamma)$. Since $R_{\hat{v}}(\theta)$ lies in $\mathrm{SU}(2)$, as can be seen from Appendix B, it is obvious that such real numbers α, β, and γ exist from Appendix A. Lemma 1 and its proof give more information. Namely, Lemma 1 implies that we should set $\sin\frac{\beta}{2} = \pm\sqrt{1-v_z^2}\sin\frac{\theta}{2}$. A way to choose η and ζ, which determine α and γ by (14) as $\alpha = \eta - \zeta$ and $\gamma = \eta + \zeta$, is described with (20) and (22) in the proof of Lemma 1.

V. Implications of Lemma 1

We present two corollaries to Lemma 1, which were originally obtained to demonstrate a fallacy (Appendix E).

Corollary 1: For any $\phi, \beta \in \mathbb{R}$, and $\hat{v} \in \mathbb{R}^3$ with $\|\hat{v}\| = 1$, the following two conditions are equivalent.

I′. There exist some $\alpha, \gamma, \theta \in \mathbb{R}$ such that

$$R_{\hat{v}}(\theta) = e^{i\phi}R_z(\alpha)R_y(\beta)R_z(\gamma).$$

II′. Both of the following hold:

$$e^{i\phi} \in \{1, -1\},$$
$$|\cos\tfrac{\beta}{2}| \geq |v_z|. \tag{23}$$

Corollary 2: For any $\beta \in \mathbb{R}$ and $\hat{v} \in \mathbb{R}^3$ with $\|\hat{v}\| = 1$, the following statement I″ implies $|\cos\frac{\beta}{2}| \geq |v_z|$.

I″. There exist some $\phi', \alpha', \gamma', \theta \in \mathbb{R}$ such that

$$e^{i\phi'}R_z(\alpha')R_{\hat{v}}(\theta)R_z(\gamma') = R_y(\beta). \tag{24}$$

VI. Generalization of Lemma 1

A. Generalization of Lemma 1

Lemma 1 can be generalized as follows.

Lemma 2: For any $\phi, \beta, \theta \in \mathbb{R}$ and for any $\hat{n}, \hat{l}, \hat{m} \in \mathbb{R}^3$ such that $\|\hat{n}\| = \|\hat{l}\| = \|\hat{m}\| = 1$ and $\hat{l}^{\mathrm{T}}\hat{m} = 0$, the following two conditions are equivalent.

III. There exist some $\alpha, \gamma \in \mathbb{R}$ such that

$$R_{\hat{n}}(\theta) = e^{i\phi}R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma). \tag{25}$$

IV. Both of the following hold:

$$e^{i\phi} \in \{1, -1\},$$
$$\sqrt{1-(\hat{n}^{\mathrm{T}}\hat{m})^2}|\sin\tfrac{\theta}{2}| = |\sin\tfrac{\beta}{2}|. \tag{26}$$

This has been shown using the homomorphism described in Appendix C or D. The proof is omitted.

B. Implications

Obviously, the implications described in Sec. V extend to this general case. In particular, the next corollary to Lemma 2 follows in the same way as Corollary 1 follows from Lemma 1.

Corollary 3: For any $\phi, \beta \in \mathbb{R}$ and for any $\hat{n}, \hat{l}, \hat{m} \in \mathbb{R}^3$ such that $\|\hat{n}\| = \|\hat{l}\| = \|\hat{m}\| = 1$ and $\hat{l}^{\mathrm{T}}\hat{m} = 0$, there exist some $\alpha, \gamma, \theta \in \mathbb{R}$ such that

$$R_{\hat{n}}(\theta) = e^{i\phi}R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma)$$

if and only if $e^{i\phi} \in \{1, -1\}$ and

$$|\cos\tfrac{\beta}{2}| \geq |\hat{n}^{\mathrm{T}}\hat{m}|. \tag{27}$$

This leads to the following affirmative result on construction of an arbitrary rotation with successive rotations about two non-parallel axes.

Corollary 4: If $\hat{m}$ and $\hat{n}$ are unit vectors in $\mathbb{R}^3$ such that $|\hat{n}^{\mathrm{T}}\hat{m}| < 1$, any element in $\mathrm{SU}(2)$ can be written as

$$R_{\hat{m}}(\tau_1)R_{\hat{n}}(\theta_1)R_{\hat{m}}(\tau_2)\cdots R_{\hat{m}}(\tau_k)R_{\hat{n}}(\theta_k)R_{\hat{m}}(\tau_{k+1}) \tag{28}$$

for some integer $k > 0$ and $\tau_1, \ldots, \tau_{k+1}, \theta_1, \ldots, \theta_k \in \mathbb{R}$.

Proof: Choose some $\hat{l} \in \mathbb{R}^3$ such that $\|\hat{l}\| = 1$ and $\hat{l}^{\mathrm{T}}\hat{m} = 0$. Then, Lemma 2, together with Appendix A, ensures that any element in $\mathrm{SU}(2)$ can be written as $U = R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta')R_{\hat{m}}(\gamma)$ for some $\alpha, \beta', \gamma \in \mathbb{R}$. For some positive integer k and real numbers $\beta_1, \ldots, \beta_k$ with $|\cos\frac{\beta_j}{2}| \geq |\hat{n}^{\mathrm{T}}\hat{m}|$ for $j = 1, \ldots, k$, we can write $\beta' = \beta_1 + \cdots + \beta_k$. Then, $R_{\hat{l}}(\beta') = R_{\hat{l}}(\beta_1)\cdots R_{\hat{l}}(\beta_k)$. Note that for $j = 1, \ldots, k$, there exist some $\alpha_j, \gamma_j, \theta_j \in \mathbb{R}$ such that $R_{\hat{l}}(\beta_j) = R_{\hat{m}}(-\alpha_j)R_{\hat{n}}(\theta_j)R_{\hat{m}}(-\gamma_j)$ by Corollary 3. Hence, we have Corollary 4. □

VII. Proof of Theorem 1

Theorem 1 is implied directly by the following proposition, which may be viewed as a detailed form of Corollary 4. (Instead of proving Theorem 1 through the proposition, Theorem 1 can be directly proved modifying the proof of the proposition below.)

Proposition 1: Let arbitrary vectors $\hat{l}, \hat{m}, \hat{n} \in S^2$ such that $0 < \hat{m}^{\mathrm{T}}\hat{n} < 1$ and $\hat{l}^{\mathrm{T}}\hat{m} = 0$, numbers $\alpha, \gamma \in \mathbb{R}$, and $\beta \in (0, \pi]$ be given. If numbers $\beta_1, \ldots, \beta_k \in (0, 2\arccos\hat{m}^{\mathrm{T}}\hat{n}]$ satisfy

$$\beta = \beta_1 + \cdots + \beta_k, \tag{29}$$

then,

$$\begin{aligned} &R_{\hat{m}}(\alpha)R_{\hat{l}}(\beta)R_{\hat{m}}(\gamma) = \\ &R_{\hat{m}}(\alpha - \alpha_1)R_{\hat{n}}(\theta_1) \\ &R_{\hat{m}}(-\gamma_1 - \alpha_2)R_{\hat{n}}(\theta_2) \\ &R_{\hat{m}}(-\gamma_2 - \alpha_3)R_{\hat{n}}(\theta_3) \\ &\cdots \\ &R_{\hat{m}}(-\gamma_{k-1} - \alpha_k)R_{\hat{n}}(\theta_k)R_{\hat{m}}(-\gamma_k + \gamma) \end{aligned}$$

where

$$\alpha_j = \eta_j - \zeta_j \quad \text{and} \quad \gamma_j = \eta_j + \zeta_j, \tag{30}$$

and $\theta_j, \eta_j, \zeta_j$ are specified by

$$|\sin\tfrac{\theta_j}{2}| = \frac{\sin\frac{\beta_j}{2}}{\sqrt{1-\hat{m}^{\mathrm{T}}\hat{n}}}$$

$$\cos\eta_j = \frac{\cos\frac{\theta_j}{2}}{\cos\frac{\beta_j}{2}} \quad \text{and} \quad \sin\eta_j = \frac{\hat{m}^{\mathrm{T}}\hat{n}\sin\frac{\theta_j}{2}}{\cos\frac{\beta_j}{2}}, \tag{31}$$

and

$$\sin\zeta_j = \frac{(\hat{l}\times\hat{m})^{\mathrm{T}}\hat{n}\sin\frac{\theta_j}{2}}{\sin\frac{\beta_j}{2}} \quad \text{and} \quad \cos\zeta_j = \frac{\hat{l}^{\mathrm{T}}\hat{n}\sin\frac{\theta_j}{2}}{\sin\frac{\beta_j}{2}}. \tag{32}$$

Proof (sketch). First, consider the case where $\hat{l} = (0,1,0)^{\mathrm{T}}$ and $\hat{m} = (0,0,1)^{\mathrm{T}}$. See the proof of Corollary 4, and observe that the parameters α_j, γ_j and θ_j are specified as in the proposition recalling the remark at the end of Section IV.

In the general case where $\hat{l}$ and $\hat{m}$ are an arbitrary pair of orthogonal vectors, use the unitary matrix U in Appendix C or D and modify the proof for the special case. □

VIII. Concluding Remarks

This work has presented a method for decomposing an arbitrary unitary matrices in $\mathrm{SU}(2)$. The method is obtained using a fundamental lemma that clarifies when the two parametric expressions of matrices in $\mathrm{SU}(2)$ equal each other. The lemma was originally obtained to pointed out a misleading erroneous claim in the literature.

Acknowledgments

This work was supported by SCOPE, and by JSPS KAKENHI Grant numbers 22540150 and 21244007.

Appendix A
Parameterizations of the Elements in SU(2)

It can be shown easily that any matrix in $\mathrm{SU}(2)$ can be written as [5]

$$\begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \tag{33}$$

with some complex numbers a and b such that $|a|^2+|b|^2 = 1$. Hence, any matrix in $\mathrm{SU}(2)$ can be written as

$$\begin{pmatrix} w+iz & y+ix \\ -y+ix & w-iz \end{pmatrix} = wI + i(xX+yY+zZ) \tag{34}$$

with some real numbers x, y, z, and w such that $w^2+x^2+y^2+z^2 = 1$. Take a real number θ such that $\cos(\theta/2) = w$ and $\sin(\theta/2) = \sqrt{1-w^2} = \sqrt{x^2+y^2+z^2}$; write x, y, and z as $x = -v_x\sin(\theta/2), y = -v_y\sin(\theta/2)$, and $z = -v_z\sin(\theta/2)$, where $v_x, v_y, v_z \in \mathbb{R}$ and $v_x^2+v_y^2+v_z^2 = 1$. Thus, using real numbers $\theta, v_x, v_y, v_z \in \mathbb{R}$ with $v_x^2+v_y^2+v_z^2 = 1$, any matrix in $\mathrm{SU}(2)$ can be written as

$$(\cos\tfrac{\theta}{2})I - i(\sin\tfrac{\theta}{2})(v_xX+v_yY+v_zZ),$$

which is nothing but $R_{\hat{v}}(\theta)$ in (1).

Another well-known parameterization is

$$\begin{pmatrix} e^{-i\frac{\gamma+\alpha}{2}}\cos\frac{\beta}{2} & -e^{i\frac{\gamma-\alpha}{2}}\sin\frac{\beta}{2} \\ e^{-i\frac{\gamma-\alpha}{2}}\sin\frac{\beta}{2} & e^{i\frac{\gamma+\alpha}{2}}\cos\frac{\beta}{2} \end{pmatrix} = R_z(\alpha)R_y(\beta)R_z(\gamma) \tag{35}$$

where α, β, and γ are real numbers, which are called Euler angles.

Appendix B
Rotation about an Arbitrary Axis

The two matrices $R_z(\theta)$ and $R_y(\theta)$ represent rotations in the following sense. Let $M(x,y,z)$ be defined by

$$M(x,y,z) = xX+yY+zZ = \begin{pmatrix} z & x-iy \\ x+iy & -z \end{pmatrix}$$

for $(x,y,z)^{\mathrm{T}} \in \mathbb{R}^3$. Then, for $\theta \in \mathbb{R}$, we have

$$R_z(\theta)M(x,y,z)R_z(\theta)^{\dagger} = M(x',y',z')$$

where the coordinates obey

$$(x',y',z')^{\mathrm{T}} = \hat{R}_z(\theta)(x,y,z)^{\mathrm{T}} \tag{36}$$

with

$$\hat{R}_z(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{37}$$

We also have

$$R_y(\theta)M(x,y,z)R_y(\theta)^{\dagger} = M(x',y',z')$$

where

$$(x',y',z')^{\mathrm{T}} = \hat{R}_y(\theta)(x,y,z)^{\mathrm{T}} \tag{38}$$

with

$$\hat{R}_y(\theta) := \begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}. \tag{39}$$

Thus, $R_z(\theta)$ and $R_y(\theta)$ act as the rotation about the z-axis by the angle θ and the rotation about the y-axis by the angle θ, respectively, in $\mathbb{R}^3$. Using these facts, we will derive a unitary matrix that corresponds to a rotation about an arbitrary vector in $\mathbb{R}^3$.

Now note that any unit vector $\hat{v} \in \mathbb{R}^3$ can be obtained by rotating $(0,0,1)^{\mathrm{T}}$ about the y-axis and then rotating the obtained vector about the z-axis:

$$\hat{v} = \hat{R}_z(\varphi)\hat{R}_y(\psi)(0,0,1)^{\mathrm{T}}.$$

As a result, $\hat{v}$ can be written as

$$\hat{v} = (\sin\psi\cos\varphi, \sin\psi\sin\varphi, \cos\psi)^{\mathrm{T}}, \tag{40}$$

cf. spherical coordinates. Then,

$$\hat{R}_{\hat{v}}(\theta) := \hat{R}_z(\varphi)\hat{R}_y(\psi)\hat{R}_z(\theta)[\hat{R}_z(\varphi)\hat{R}_y(\psi)]^{-1} \tag{41}$$

is the matrix that represents the rotation about $\hat{v}$ by the angle θ in $\mathbb{R}^3$. This is obvious since $[\hat{R}_z(\varphi)\hat{R}_y(\psi)]^{-1}$ moves $\hat{v}$ to $(0,0,1)^{\mathrm{T}}$.

Then,

$$\begin{aligned} U &= R_z(\varphi)R_y(\psi)R_z(\theta)[R_z(\varphi)R_y(\psi)]^\dagger \\ &= R_z(\varphi)R_y(\psi)R_z(\theta)R_y(-\psi)R_z(-\varphi) \quad (42) \end{aligned}$$

acts as $UM(x,y,z)U^\dagger = M(x',y',z')$, where $(x',y',z')^{\mathrm{T}} = \hat{R}_{\hat{v}}(\theta)(x,y,z)^{\mathrm{T}}$. Performing the multiplication in (42), we have

$$\begin{aligned} U &= (\cos\tfrac{\theta}{2})I - i(\sin\tfrac{\theta}{2})[(\sin\psi\cos\varphi)X \\ &\quad + (\sin\psi\sin\varphi)Y + (\cos\psi)Z], \quad (43) \end{aligned}$$

which is the same as $R_{\hat{v}}(\theta)$ in (1) since we have set $(v_x,v_y,v_z) = (\sin\psi\cos\varphi, \sin\psi\sin\varphi, \cos\psi)$. Note $R_y(\psi), R_z(\varphi), R_z(\theta) \in \mathrm{SU}(2)$, so that $R_{\hat{v}}(\theta) \in \mathrm{SU}(2)$.

Appendix C
A relation of SU(2) to SO(3)

We define a map $F : \mathrm{SU}(2) \to \mathrm{SO}(3)$ as follows. With any matrix $U \in \mathrm{SU}(2)$, we associate a 3×3 real matrix $R = F(U)$ that satisfies

$$UM(x,y,z)U^\dagger = M(x',y',z')$$

and

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = R \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

for any $(x,y,z)^{\mathrm{T}} \in \mathbb{R}^3$ as in Appendix B. We claim that the map $F : \mathrm{SU}(2) \to \mathrm{SO}(3)$ is surjective (onto), i.e., that for any $R \in \mathrm{SO}(3)$, we have some $U \in \mathrm{SU}(2)$ with $R = F(U)$. This fact will be proved in Appendix D, where one should note that $\mathrm{SO}(3)$ can be expressed as

$$\{(\hat{l} \times \hat{m} \;\; \hat{l} \;\; \hat{m}) \mid \hat{l}, \hat{m} \in \mathbb{R}^3, \|\hat{l}\| = \|\hat{m}\| = 1, \hat{l}^{\mathrm{T}}\hat{m} = 0\}. \quad (44)$$

Appendix D
Proof that the map from SO(2) to SO(3) is surjective and a remark

Proof that the map F in Appendix C is onto $\mathrm{SO}(3)$. In view of the expression of $\mathrm{SO}(3)$ in (44), our goal is to prove that for any pair of vectors $\hat{l}, \hat{m} \in \mathbb{R}^3$ with $\|\hat{l}\| = \|\hat{m}\| = 1$ and $\hat{l}^{\mathrm{T}}\hat{m} = 0$, there exists some element in $\mathrm{SU}(2)$ such that $\hat{l} = F(U)(0,1,0)^{\mathrm{T}}$, $\hat{m} = F(U)(0,0,1)^{\mathrm{T}}$, and $\hat{l} \times \hat{m} = F(U)(1,0,0)^{\mathrm{T}}$. Expressing U as

$$U = U_{\alpha,\beta,\gamma} := R_z(\alpha)R_y(\beta)R_z(\gamma),$$

we can calculate $F(U)$ directly as

$$\begin{aligned} F(U) &= F(U_{\alpha,\beta,\gamma}) = \hat{R}_z(\alpha)\hat{R}_y(\beta)\hat{R}_z(\gamma) \\ &= \begin{pmatrix} a & -\cos\alpha\cos\beta\sin\gamma - \sin\alpha\cos\gamma & \cos\alpha\sin\beta \\ b & -\sin\alpha\cos\beta\sin\gamma + \cos\alpha\cos\gamma & \sin\alpha\sin\beta \\ c & \sin\beta\sin\gamma & \cos\beta \end{pmatrix} \end{aligned} \quad (45)$$

where $(a,b,c)^{\mathrm{T}}$ is the vector product of the second and third columns of $F(U)$. Moreover, the condition $\hat{l} = F(U)(0,1,0)^{\mathrm{T}}$ is equivalent to

$$\hat{R}_y(-\beta)\hat{R}_z(-\alpha)\hat{l} = \hat{R}_z(\gamma)(0,1,0)^{\mathrm{T}},$$

i.e.,

$$\begin{pmatrix} \cos\beta\cos\alpha & \cos\beta\sin\alpha & -\sin\beta \\ -\sin\alpha & \cos\alpha & 0 \\ \cos\alpha\sin\beta & \sin\alpha\sin\beta & \cos\beta \end{pmatrix} \hat{l} = \begin{pmatrix} -\sin\gamma \\ \cos\gamma \\ 0 \end{pmatrix}. \quad (46)$$

From (45) and (46), we conclude that for any pair of orthogonal unit vectors $\hat{l}$ and $\hat{m}$, there exists some $\alpha, \beta, \gamma \in \mathbb{R}$, and hence, an element $U = U_{\phi,\beta,\gamma}$ in $\mathrm{SU}(2)$ such that $\hat{l} = F(U)(0,1,0)^{\mathrm{T}}$, $\hat{m} = F(U)(0,0,1)^{\mathrm{T}}$, and $\hat{l} \times \hat{m} = F(U)(1,0,0)^{\mathrm{T}}$, as desired. (This conclusion, together with a remark, will be derived again in a more detailed manner in the last paragraph below of this appendix.) □

We remark that for any $R \in \mathrm{SO}(3)$, there are exactly two elements U such that $F(U) = R$. The easiest way to see this would be noting that F is a homomorphism and checking $\{U \in \mathrm{SU}(2) \mid F(U) = I_3\} = \{I, -I\}$, where I_3 is the 3×3 identity matrix. This shows that the map from $\mathrm{SU}(2)/\{I,-I\}$ onto $\mathrm{SO}(3)$ that is naturally induced by F is one-to-one (by the homomorphism theorem). Thus, $F(U) = F(-U)$ for any $U \in \mathrm{SU}(2)$.

Alternatively, that there are two elements U such that $F(U) = R$, and that we have $F(U) = F(-U)$ can be seen directly by examining the proof. In fact, given a rotation matrix $R \in \mathrm{SO}(3)$, the elements $U \in \mathrm{SU}(2)$ such that $R = F(U)$ are directly specified by (45) and (46). Namely, the relation $\hat{m} = (\cos\alpha\sin\beta, \sin\alpha\sin\beta, \cos\beta)^{\mathrm{T}}$, which is from (45), specifies α and β, cf. spherical coordinates, and (46) specifies γ. Recall $R_z(\alpha) = (\cos\frac{\alpha}{2})I - i(\sin\frac{\alpha}{2})Z$, where half the angle α appears. Then, one would notice that for any $R \in \mathrm{SO}(3)$, there are two elements U such that $R = F(U)$. (In this alternative verification, an inspection would be needed to see that there are no more than two such elements U.)

Appendix E
Fallacy

The contents of this article include most parts of a previous closely related piece of work of this author (unpublished except the abstract [4]). A motivation of that piece of work is having found a widespread fallacy in textbooks on quantum computation. This seems to have survived for more than ten years [6]. The fallacy is based on the following erroneous claim. Writing the 'rotation' about a unit vector $\hat{n}$ by an angle θ as $R_{\hat{n}}(\theta)$, they have claimed that any 2×2 unitary matrix can be written as $e^{i\phi}R_{\hat{m}}(\alpha)R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)$ for appropriate choices of real numbers ϕ, α, β, and γ if $\hat{n}$ and $\hat{m}$ are non-parallel real unit vectors in three dimensions [6, p. 176, Exercise 4.11], [7, p. 34], [8, p. 66, Theorem 4.2.2].

We will describe the original application of Lemma 1 to this issue. We have presented corollaries to Lemma 1 in Section V.

To see the incorrectness of the claim that any 2×2 unitary U can be written in the form $e^{i\phi}R_z(\alpha)R_{\hat{v}}(\beta)R_z(\gamma)$ if real unit vectors $\hat{v} = (v_x,v_y,v_z)^{\mathrm{T}}$ and $(0,0,1)^{\mathrm{T}}$ are not parallel, assume $|\cos(\beta/2)| < |v_z| < 1$. According to this

claim, $R_y(\beta)$ could be written as $e^{i\phi}R_z(\alpha)R_{\hat{v}}(\theta)R_z(\gamma)$ for some $\phi, \alpha, \gamma, \theta \in \mathbb{R}$. This is incorrect by Corollary 2.

In this counterexample, the two non-parallel unit vectors are set equal to $\hat{v}$ and $(0, 0, 1)^{\mathrm{T}}$. We remark that essentially the same counterexamples can be obtained for a generic pair of non-parallel non-orthogonal unit vectors. This can be done immediately using Lemma 2, which generalizes Lemma 1.

REFERENCES

[1] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On universal and fault-tolerant quantum computing," e-Print arXiv:quant-ph/9906054, 1999.

[2] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Phys. Rev. Lett.*, vol. 73, no. 1, pp. 58–61, Jul. 1994.

[3] J. J. Sakurai, *Modern Quantum Mechanics*. Menlo Park: Benjamin/Cummings Publishing, 1985.

[4] M. Hamada, "Overlooked restrictions on Euler angles in quantum computation," *APS March Meeting*, 2013, http://meetings.aps.org/link/BAPS.2013.MAR.H1.318.

[5] E. P. Wigner, *Group Theory and Its Application to the Quantum Mechanics of Atomic Spectra*. New York: Academic Press, 1959.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. Cambridge, UK: Cambridge University Press, 2010.

[7] K. R. Parthasarathy, *Lectures on Quantum Computation, Quantum Error Correcting Codes and Information Theory*. New Delhi, India: Narosa Publishing House, 2006.

[8] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*. New York: Oxford University Press, 2007.