ISSN 2186-6570

A Simple Demonstration of a Fallacy in Implementability Arguments on Quantum Computation

Mitsuru Hamada

Quantum Information Science Research Center
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.4, No.1, 31-32, 2014

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.4 No.1 : 31–32 (2014)

A Simple Demonstration of a Fallacy in Implementability Arguments on Quantum Computation

Mitsuru Hamada
Quantum Information Science Research Center
Quantum ICT Research Institute
Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

***Abstract*—A misleading erroneous claim often found in the literature on quantum computation is disproved in a simple manner. The incorrect claim states that for any non-parallel vectors $\hat{m}$ and $\hat{n}$, any 2×2 unitary matrix can be written as a scalar multiple of the product of some three rotations about either $\hat{m}$ or $\hat{n}$. Here, a rotation means a 2×2 unitary matrix of determinant 1 that corresponds to a 3×3 rotation matrix (real orthogonal matrix with determinant 1). This error has already been pointed out by the present author [M. Hamada, "Overlooked restrictions on Euler angles in quantum computation," *APS 2013 March Meeting*, Baltimore, USA, 2012, http://meetings.aps.org/link/BAPS.2013.MAR.H1.318 (abstract)], but a streamlined proof is presented in order to help one recognize the error quickly. While this demonstration is a negative result, in a recent constructive result, the author has clarified what is the best we can do instead of the wrongly claimed impossible thing quantitatively, formulating a problem of constructing an arbitrary rotation mathematically. A brief history on this recent result is described.**

I. Introduction

The aim of this report is to present a simple demonstration of a widespread fallacy regarding universal gates often found in textbooks on quantum computation. This has been pointed out by the present author [1], [2] by means of a lemma found by him. The core of the fallacy is the following erroneous claim. Writing the 'rotation' about a real unit vector $\hat{v}$ by an angle θ as $R_{\hat{v}}(\theta)$, they have claimed, without a proof, that any 2×2 unitary matrix can be written as $e^{i\phi}R_{\hat{m}}(\psi)R_{\hat{n}}(\theta)R_{\hat{m}}(\psi')$ for appropriate choices of real numbers ϕ, ψ, θ, and ψ' if $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Specific sources of this statement will not be repeated here but can be found in [2].

In essence, the demonstration below may be viewed as a streamlined version of the one obtained in [1], [2]. The author's view that there ought to be needs for reading such one is based on the following thought. While this demonstration is negative, the author has already obtained an affirmative result on construction of an arbitrary rotation [3]. Namely, while constructing an arbitrary rotation with three successive rotations is impossible, in general, he has clarified what is the best we can do instead of the wrongly claimed impossible thing quantitatively, formulating a problem of constructing an arbitrary rotation mathematically. Naturally, the obtained result contradicts the above erroneous claim. Then, in view of the fact that the error has appeared in, at least, three textbooks on quantum computation, many people misguided by the error would be confused with this contradiction. This streamlined version of demonstration would help such people recognize the error quickly.

II. Definitions

The following Pauli matrices are used:

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

The 2×2 identity matrix is denoted by I. We put $\hat{y} = (0,1,0)^{\mathrm{T}}$ and $\hat{z} = (0,0,1)^{\mathrm{T}}$. As usual, $\mathbb{R}$ and $\mathbb{C}$ denote the set of real numbers and that of complex numbers, respectively. We put

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

for $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ with $\|\hat{v}\| = \sqrt{v_x^2 + v_y^2 + v_z^2} = 1$ and $\theta \in \mathbb{R}$. For example,

$$R_{\hat{z}}(\psi) = \begin{pmatrix} e^{-i\frac{\psi}{2}} & 0 \\ 0 & e^{i\frac{\psi}{2}} \end{pmatrix}, \quad \psi \in \mathbb{R}. \quad (2)$$

III. Demonstration of the fallacy

We focus on disproving the above claim in the case where the two vectors $\hat{m}$ and $\hat{n}$ are $\hat{z} = (0,0,1)^{\mathrm{T}}$ and $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}}$ with $0 < |v_z| < 1$ and $\|\hat{v}\| = 1$. Namely, we will show that whenever $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ is a unit vector with $0 < |v_z| < 1$, there exists some 2×2 unitary matrix that cannot be written in the form $e^{i\phi}R_{\hat{z}}(\psi)R_{\hat{v}}(\theta)R_{\hat{z}}(\psi')$ for any real numbers ϕ, ψ, θ, and ψ' (while $\hat{z}$ and $\hat{v}$ are non-parallel unit vectors by the assumption $|v_z| < 1$). (The counterexamples below

generalize to the case of generic non-parallel vectors $\hat{m}$ and $\hat{n}$ straightforwardly.)

Proposition 1: Let arbitrary numbers $a, b, c, d \in \mathbb{C}$ and an arbitrary unit vector $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ be given. If $|a| < |v_z|$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq e^{i\phi} R_{\hat{z}}(\psi) R_{\hat{v}}(\theta) R_{\hat{z}}(\psi') \tag{3}$$

for any $\phi, \psi, \theta, \psi' \in \mathbb{R}$.

Proof. The absolute value of the $(1,1)$-entry of $e^{i\phi} R_{\hat{z}}(\psi) R_{\hat{v}}(\theta) R_{\hat{z}}(\psi')$ [or of $R_{\hat{v}}(\theta)$, see (2)] is

$$\sqrt{\cos^2 \tfrac{\theta}{2} + v_z^2 \sin^2 \tfrac{\theta}{2}} = A(\theta).$$

Note $\min_{\theta \in \mathbb{R}} A(\theta) = |v_z|$. Hence, comparing the $(1,1)$-entries of both sides of (3), we obtain the proposition. □

This proposition demonstrates the fallacy mentioned above. Specifically, for any number $a \in \mathbb{C}$ with $|a| < |v_z|$, any unitary matrix whose $(1,1)$-entry equals a, such as

$$\begin{pmatrix} a & -\sqrt{1-|a|^2} \\ \sqrt{1-|a|^2} & a^* \end{pmatrix}, \tag{4}$$

cannot be written in the form $e^{i\phi} R_{\hat{m}}(\psi) R_{\hat{n}}(\theta) R_{\hat{m}}(\psi')$ for any $\phi, \psi, \theta, \psi' \in \mathbb{R}$ by the proposition. This is a counterexample to the claim in question in the case where $\hat{m} = \hat{z}$, $\hat{n} = \hat{v}$, and $0 < |v_z| < 1$. (There exist infinitely many numbers $a \in \mathbb{C}$ with $|a| < |v_z|$ since $0 < |v_z|$.)

IV. Concluding Remarks

As already mentioned, the demonstration in this article may be viewed as a streamlined version of the original one based on the following lemma.

Lemma 1: [1], [2]. Let arbitrary numbers $\alpha, \gamma, \theta \in \mathbb{R}$ and a unit vector $\hat{v} = (v_x, v_y, v_z)^{\mathrm{T}} \in \mathbb{R}^3$ be given; then, there exist some $\beta, \delta \in \mathbb{R}$ satisfying $R_{\hat{v}}(\theta) = e^{i\alpha} R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma) R_{\hat{z}}(\delta)$ if and only if $e^{i\alpha} \in \{1, -1\}$ and $\sqrt{1-v_z^2}\,|\sin(\theta/2)| = |\sin(\gamma/2)|$.

In particular, the above counterexamples were found through this lemma. Then, the following question may be asked. Now that the demonstration of the fallacy is streamlined, is Lemma 1 obsolete? The answer is 'no.' This is because while the 'only if' part of this lemma has been used in the above negative result, the lemma also asserts its converse, i.e., the 'if' part. The 'if' part says primarily that the condition $\sqrt{1-v_z^2}\,|\sin(\theta/2)| = |\sin(\gamma/2)|$ is *sufficient* for $R_{\hat{v}}(\theta) = R_{\hat{z}}(\beta) R_{\hat{y}}(\gamma) R_{\hat{z}}(\delta)$ to hold for some $\beta, \delta \in \mathbb{R}$. Using this part, the author has obtained an affirmative result on construction, i.e., a method for constructing an arbitrary rotation with a finite number of successive rotations about two non-parallel axes.

Specifically, Lemma 1 soon led to the following constructive result (unpublished). The least value, $L(\hat{m}, \hat{n})$, of a positive integer k such that any rotation in $\mathrm{SU}(2)$ can be decomposed into a product of k rotations about either $\hat{m}$ or $\hat{n}$ is upper-bounded by $2\lceil \pi/(2 \arccos |\hat{m}^{\mathrm{T}} \hat{n}|) \rceil + 1$ for any pair of unit vectors $\hat{m}, \hat{n} \in \mathbb{R}^3$ with $|\hat{m}^{\mathrm{T}} \hat{n}| < 1$. In other words, $2\lceil \pi/(2 \arccos |\hat{m}^{\mathrm{T}} \hat{n}|) \rceil + 1$ is an upper bound on $L(\hat{m}, \hat{n}) = \max_U \texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$, where $\texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$ denotes the minimum number of factors needed in decomposing a rotation U, and U runs through $\mathrm{SU}(2)$ in the maximization.

After the author noticed this, he investigated whether this bound was tight or not and since he found it improvable, struggled to find the tightest bound. Finally, the present author determined $\texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$ for an arbitrary rotation U, and also presented decompositions achieving $\texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$ explicitly; he also gave $L(\hat{m}, \hat{n})$ in terms of a simple function of $\arccos |\hat{m}^{\mathrm{T}} \hat{n}|$ as a consequence of determining $\texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$. After obtaining these results, he learned that in the mathematics literature, the same result on $L(\hat{m}, \hat{n})$, in a less concise expression, had already existed. But this result on $L(\hat{m}, \hat{n})$ is weaker than the present author's other results relevant to $L(\hat{m}, \hat{n})$. For the details of these results, the reader is referred to [3].

In particular, the most distinctive feature of [3] would be its presenting (an algorithm for obtaining) an optimal decomposition of an arbitrary rotation U explicitly, where the optimality refers to achieving $\texttt{MinimumNumber}(\hat{m}, \hat{n}, U)$. This would be significant for quantum computation, and probably, also in other fields.

Acknowledgments

This work was supported by SCOPE, and by JSPS KAKENHI Grant numbers 22540150 and 26247016.

References

[1] M. Hamada, "Overlooked restrictions on Euler angles in quantum computation," *APS 2013 March Meeting* (abstract), 2012, http://meetings.aps.org/link/BAPS.2013.MAR.H1.318.

[2] M. Hamada, "A lemma on Euler angles," *Tamagawa University Quantum ICT Research Institute Bulletin*, vol. 3, pp. 25–27, Dec. 2013.

[3] M. Hamada, "The minimum number of rotations about two axes for constructing an arbitrarily fixed rotation," *Royal Society Open Science*, 1:140145, Nov. 2014 (http://dx.doi.org/10.1098/rsos.140145).