18a-F4-6

A simple demonstration of a fallacy on universal gates for quantum computation

Mitsuru Hamada
Quantum ICT Research Institute, Tamagawa University
1-1 Tamagawa-Gakuen 6-chome, Machida-shi, Tokyo 194-8610 E-mail: mitsuru@ieee.org

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 overlooked for more than ten years [1] and propagated widely [2, 3]. 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 [1, p. 176, Exercise 4.11], [2, p. 34], [3, p. 66, Theorem 4.2.2].

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 $\hat{z} = (0,0,1)^{\mathrm{T}}$. $\mathbb{R}$ and $\mathbb{C}$ denote the set of real numbers and that of complex numbers, respectively.

We put

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

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,

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

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 $\hat{v}$ and $\hat{z}$ 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*

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

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

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

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 $0 < |v_z|$.)

The theorem in [4], with which the counterexamples were first obtained, soon led to the following constructive result (unpublished). The least value of a positive integer k such that any rotation in 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 $|\hat{m}^{\mathrm{T}}\hat{n}| < 1$.

The reader is referred to [5] for stronger results. The results in [5] also demonstrate the fallacy in a different way, in terms of a geodesic metric, though a trifle therein.

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

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. (Cambridge University Press, Cambridge, UK, 2010).
[2] K. R. Parthasarathy, *Lectures on Quantum Computation, Quantum Error Correcting Codes and Information Theory* (Narosa Publishing House, New Delhi, India, 2006).
[3] P. Kaye, et al., *An Introduction to Quantum Computing* (Oxford University Press, New York, 2007).
[4] M. Hamada, APS 2013 March Meeting, abstract (2012) http://meetings.aps.org/link/BAPS.2013.MAR.H1.318.
[5] M. Hamada, manuscript (2013), arXiv:1401.0153 [math.ph].