Hindawi
Advances in Mathematical Physics
Volume 2020, Article ID 2530609, 7 pages
https://doi.org/10.1155/2020/2530609

Research Article

Solovay–Kitaev Approximations of Special Orthogonal Matrices

Anuradha Mahasinghe,[1] **Sachiththa Bandaranayake**,[1] **and Kaushika De Silva**[2]

[1]*Department of Mathematics, University of Colombo, Colombo 03, Sri Lanka*
[2]*Department of Mathematics, University of Sri Jayewardenepura, Nugegoda, Sri Lanka*

Correspondence should be addressed to Anuradha Mahasinghe; anuradhamahasinghe@gmail.com

Received 28 March 2020; Revised 21 May 2020; Accepted 2 June 2020; Published 24 June 2020

Academic Editor: John D. Clayton

The circuit-gate framework of quantum computing relies on the fact that an arbitrary quantum gate in the form of a unitary matrix of unit determinant can be approximated to a desired accuracy by a fairly short sequence of basic gates, of which the exact bounds are provided by the Solovay–Kitaev theorem. In this work, we show that a version of this theorem is applicable to orthogonal matrices with unit determinant as well, indicating the possibility of using orthogonal matrices for efficient computation. We further develop a version of the Solovay–Kitaev algorithm and discuss the computational experience.

1. Introduction

A computer program in the context of classical computing is an ordered list of instructions, expressible in terms of elementary operations, readily convertible to the machine language of a classical computer. A quantum program in quantum computing could be described analogously. According to the circuit-gate framework of quantum computing, a quantum algorithm consists of quantum gates acting on quantum states (qubits) where measuring devices are applied at appropriate instances to collapse the wavefunction. Based on the Heisenberg–Born interpretation of quantum mechanics, this circuit-gate framework has achieved significant progress up to date, as the pioneering model of quantum computing. Also, it is proven to be polynomially equivalent to other quantum computational frameworks. Accordingly, a quantum program can be regarded as the application of several unitary matrices, together with measurements at certain instances.

In order to implement unitary operations, basic quantum gates such as *Pauli gates*, *Hadamard gate*, and *phase gate* are available in the circuit-gate framework, in analogy with basic gates in classical computing. It is quite natural to ask how many basic gates are needed to implement an arbitrary unitary operation in a quantum circuit. The remarkable contributions in this regard made independently by Solovay [1] and Kitaev [2] answered this question, resulting in what is known today as the *Solovay–Kitaev theorem*. This theorem states that it is possible to approximate any 2×2 unitary with unit determinant by a product of $O(\log^4(1/\varepsilon))$ physically realizable 2×2 unitaries (which appear as *basic gates*) to an arbitrary accuracy ε [3, 4]. Recall the other quantum computational frameworks such as *quantum walks*, *quantum Turing machines*, and *adiabatic computing* were proven to be polynomially equivalent to the circuit-gate framework [5–7], the Solovay–Kitaev theorem is widely regarded the theoretical proof for the supremacy of quantum computers. In addition, the number of elementary gates needed to implement an arbitrary unitary provides an indicator of the capacity and limitations of quantum computers.

This reveals an interesting aspect of unconventional models of computing. That is, any computational model with similar speed and limitations would be computationally equivalent to quantum computing. If physically realizable, such a model would have the same advantages and limitations as quantum computing. Though little attention has been paid to this subject in the past, several interesting works have investigated the possibility of having such models. A pioneering work was done by Aerts and Czachor in 2007, proposing geometric algebras instead of unitary matrices [8]. The authors named this model *cartoon computing* and proved its equivalence to quantum computing, demonstrating a simulation of the Deutsch-Jozsa algorithm. A later work

investigated entities in cartoon computing equivalent to elementary gates in quantum computing [9]. In 2008, Fernandez and Schneeberger proposed *quaternionic computing*, in which the possibility of adopting quaternions instead of unitary matrices was proven [10]. In order to show the equivalence to quantum computing, the authors have used the Bernstein–Vazirani theorem in quantum Turing machine framework. In [11], Graydon explored quaternionic quantum processes with respect to standard quantum information theory. Thus, it is an interesting question to ask what other algebraic structures would show similar behaviour, if employed as a computational model.

On the other hand, the progress achieved in three-level quantum systems is noteworthy [12–14]. Instead of qubits with states $|0\rangle$ and $|1\rangle$ in standard circuit-gate framework, *qutrits* having three basis states $|0\rangle$, $|1\rangle$, and $|2\rangle$ are used in these systems. Analogous to the single-qubit quantum gates in the form of 2×2 matrices in the special (unit determinant) unitary group $SU(2)$, the single-qutrit gates are 3×3 special unitaries or the elements in the group SU(3) [15–17]. Though the realization of $SU(3)$ gates has been the topic of interest for several previous works [18–20], computational capacity or theoretical bounds on computing of a three-level quantum system have not been paid the deserved attention. Neither Solovay–Kitaev type approximations were investigated for three-level systems. Nevertheless, a recent work emphasized the significance of the subgroup $SO(3)$ of $SU(3)$ for qutrit-based quantum computation, showing that any state of a qutrit could be obtained from a one-parameter family of states through the action of $SO(3)$ [21]. In this regard, one should not ignore the remarkable relationship between the groups $SO(3)$ and $SU(2)$. This motivates us to check whether the Solovay–Kitaev theorem is extendable to $SO(3)$ and possible to achieve the quantum speedup in three-level quantum systems, when equipped with orthogonal operators. In addition to that, once this question is resolved, one may know exactly whether the 3×3 orthogonal matrices also provide an algebraic structure suitable for efficient computation, such as geometric algebras or quaternions.

In this paper, we show that the question is answered positively. That is, the orthogonal matrices play a role in three-level quantum systems, equivalent to what the unitaries play in standard quantum circuit framework. More precisely, we show that a version of the Solovay–Kitaev theorem is applicable to 3×3 orthogonal matrices with unit determinant. Thus, we indicate the possibility of theoretically replacing the 2×2 unitaries in quantum computing by 3×3 orthogonals and qubits by qutrits. Using Cornwell's two-to-one homomorphic map from the special unitary group $SU(2)$ to special orthogonal group $SO(3)$ [22], we prove the possibility of approximating any 3×3 orthogonal with unit determinant by a product of $O(\log^4(1/\varepsilon))$ elementary 3×3 orthogonals of unit determinants to an arbitrary accuracy ε. We further discuss how to find the sequence of appropriate elementary orthogonals, providing a version of Solovay–Kitaev algorithm in $SO(3)$.

The remainder of the paper is organized as follows. In Section 2, our version of the Solovay–Kitaev theorem for $SO(3)$ is proven. An approximation scheme for unit-determinant orthogonal matrices in accordance with this theorem and the standard Solovay–Kitaev algorithm is presented in Section 3. Computational experience is discussed in Section 4, and we discuss the implications of our work in Section 5 with several remarks on potential future works.

2. Solovay–Kitaev Theorem in $SO(3)$

2.1. Solovay–Kitaev Theorem. Recall the computational power in the circuit-gate framework is guaranteed by the Solovay–Kitaev theorem; its main focus is on approximating a $2^d \times 2^d$ unitary matrix by basic quantum gates. A set of possible basic gates is referred to as an *instruction set* in the context of this theorem. Considering single qubit unitary gates, an instruction set $\mathcal{G}$ is a finite subset of $SU(2)$ such that $\mathcal{G}$ contains its own inverse and $\langle \mathcal{G} \rangle$ is dense in $SU(2)$. For example, the set of gates $\{H, H^\dagger, T, T^\dagger\}$ makes an instruction set for $SU(2)$, where H and T denote, respectively, Hadamard and phase gates in the circuit-gate framework. The set of all strings that can be made from $\mathcal{G}$ without using more than l elements is denoted by $\mathcal{G}_l$. Now, the Solovay–Kitaev theorem for a d-qubit system can be stated as follows.

Theorem 1 (Solovay–Kitaev). *Let $\mathcal{G}$ be an instruction set in $SU(2^d)$. Then, for any $\varepsilon > 0$, $\mathcal{G}_l$ provides an ε–net for $SU(2^d)$ where $l = O_d(\log^4(1/\varepsilon))$.*

The proof of this theorem is highly constructive, and the algorithmic steps of finding the elements in the instruction set that approximate a given element in $SU(2)$ can be found from its proof. A comprehensive version of proof can be found in [4]. An algorithmic version of the theorem with a procedure for finding those elements can be found in [23]. We now explore how a version of this theorem can be adapted to $SO(3)$. Primary motivation for this is the distance relations of the two groups, preserved by a homomorphism from $SU(2)$ onto $SO(3)$.

2.2. Distance Relations. The two-to-one homomorphic mapping ρ from $SU(2)$ onto $SO(3)$ known today as *Cornwell's mapping* is expressible in several ways [22], from which we adopt the following in [24]. An element U in $SU(2)$ is expressible as

$$U = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \tag{1}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$ and its image is given by

$$\rho(U) = \begin{pmatrix} \mathrm{Re}\,(\alpha^2 - \beta^2) & \mathrm{Im}\,(\alpha^2 - \beta^2) & -2\,\mathrm{Re}\,(\alpha\beta) \\ \mathrm{Im}\,(\alpha^2 - \beta^2) & \mathrm{Re}\,(\alpha^2 + \beta^2) & 2\,\mathrm{Im}\,(\alpha\beta) \\ 2\,\mathrm{Re}\,(\alpha\bar{\beta}) & 2\,\mathrm{Im}\,(\alpha\bar{\beta}) & |\alpha|^2 - |\beta|^2 \end{pmatrix}. \tag{2}$$

In order to measure the distances, as in the proof of the standard Solovay–Kitaev theorem, we too use the metric induced by the trace norm for consistency. It is customary to use the operator norm in quantum computation according to the matrix formulation of quantum mechanics. However, the standard proof of the Solovay–Kitaev theorem uses trace norm, as it helps to make the proof more comprehensive by incorporating a special property of the trace norm at some point. Since our intention is finding an analogous version in $SO(3)$, it is more appropriate to consider the trace norm for matrices in $SO(3)$ as well.

Lemma 2 illustrates how the mapping ρ preserves distances to an order $O(\varepsilon)$ in $SO(3)$ with respect to trace norm.

Lemma 2. *For any two $U, V \in SU(2)$, if $\|U - V\| < \varepsilon$, then $\|\rho(U) - \rho(V)\| < O(\varepsilon)$.*

Proof. Due to unitary invariance of the trace norm, it suffices to show that $I - \rho(U) < O(\varepsilon)$ whenever $I - U < \varepsilon$. We use the fact that any element U in $SU(2)$ can be expressed as in equation (1) and the mapping ρ given by equation (2). Then,

$$\rho(I) - \rho(U) = \begin{pmatrix} \operatorname{Re}\left(1-\alpha^2+\beta^2\right) & \operatorname{Im}\left(1-\alpha^2-\beta^2\right) & 2\operatorname{Re}(\alpha\beta) \\ -\operatorname{Im}\left(1-\alpha^2+\beta^2\right) & \operatorname{Re}\left(1-\alpha^2-\beta^2\right) & -2\operatorname{Im}(\alpha\beta) \\ -2\operatorname{Re}\left(\alpha\bar{\beta}\right) & 2\operatorname{Im}\left(\alpha\bar{\beta}\right) & 1-|\alpha|^2-|\beta|^2 \end{pmatrix}, \tag{3}$$

from which we derive

$$\|\rho(I) - \rho(U)\|^2 = \left|1-\alpha^2+\beta^2\right|^2 + \left|1-\alpha^2-\beta^2\right|^2 + 4|\alpha\beta|^2 + 4\left|\alpha\bar{\beta}\right|^2 + \left(1-|\alpha|^2+|\beta|^2\right)^2. \tag{4}$$

Supposing $\|I - U\| < \varepsilon$, it is not difficult to see that the left side of equation (4) is bounded by $O(\varepsilon^2)$ as follows.

$\|I - U\|^2 = 2((1-\alpha)^2 + \beta^2) < \varepsilon^2$. Accordingly, $|1-\alpha| < (\varepsilon/\sqrt{2})$ and $|\beta| < (\varepsilon/\sqrt{2})$. Also, $|\alpha| < (\varepsilon/\sqrt{2}) + 1$. Therefore, $|1-|\alpha|^2| \le |1-\alpha^2| = |1-\alpha||1+\alpha| < (\varepsilon/2)(\varepsilon + 2\sqrt{2})$. Similarly, $|1-\alpha^2+\beta^2| \le |1-\alpha^2| + |\beta^2| < \varepsilon(\varepsilon+\sqrt{2})$. Substituting these in equation (4), $\|\rho(I) - \rho(U)\|^2 < 3(\varepsilon(\varepsilon+\sqrt{2}))^2 + 2(\varepsilon(\varepsilon+2\sqrt{2}))^2$. Therefore, $\|\rho(I) - \rho(U)\| < O(\varepsilon)$.

2.3. Instruction Sets in $SO(3)$. In the context of single qubit unitary gates, an instruction set $\mathcal{G}$ is a finite subset of $SU(2)$ such that $\mathcal{G}$ contains its own inverse and $\langle\mathcal{G}\rangle$ is dense in $SU(2)$. It is possible to adopt the same definition for instruction sets in $SO(3)$. Interestingly, the image of an instruction set in $SU(2)$ under the homomorphism ρ becomes an instruction set in $SO(3)$. Lemmata 3 and 4 prove this claim.

Lemma 3. *Let X and Y be metric spaces, and let A be a dense subset of X. If $f : X \longrightarrow Y$ is continuous and surjective, then $f(A)$ is dense in Y.*

Proof. Let $K = f^{-1}(f(\bar{A}))$. Then, $A \subseteq K$ and since f is continuous, K is closed. This implies $\bar{A} \subseteq K$. On the other hand, since A is dense in X, $\bar{A} = X$. Thus, $K = X$, and therefore, $\overline{f(A)} = f(K) = f(X) = Y$.

Lemma 4. *If $\mathcal{G}$ is an instruction set in $SU(2)$, then $\langle\rho(\mathcal{G})\rangle$ is an instruction set in $SO(3)$.*

Proof. Let $\mathcal{G}$ be an instruction set in $SU(2)$. Then, $\rho(\mathcal{G})$ must contain its own inverse and is finite as ρ is a homomorphism. Since ρ is continuous and $\langle\mathcal{G}\rangle$ is dense in $SU(2)$, by Lemma 3 $\rho(\langle\mathcal{G}\rangle)$ is dense in $SO(3)$. Clearly, since ρ is a homomorphism, we have $\langle\rho(\mathcal{G})\rangle = \rho(\langle\mathcal{G}\rangle)$. Therefore, $\langle\rho(\mathcal{G})\rangle$ is an instruction set in $SO(3)$.

2.4. Solovay–Kitaev Theorem in $SO(3)$. With the results we derived above, it is now possible to establish a version of the Solovay–Kitaev theorem for $SO(3)$.

Theorem 5. *Let $\mathcal{G}$ be an instruction set in $SU(2)$. Then, $\rho(\mathcal{G})$ is an instruction set for $SO(3)$ such that for any $\varepsilon > 0$, $\rho(\mathcal{G})_l$ provides an ε–net for $SO(3)$ where $l = O(\log^4(1/\varepsilon))$.*

Proof. From Lemma 4, $\rho(\mathcal{G})$ is an instruction set. Let $V \in SO(3)$. Then, there exists some $U \in SU(2)$ such that $V = \rho(U)$. The Solovay–Kitaev theorem guarantees the existence of $U_1, U_2, \cdots, U_l \in \mathcal{G}$ such that $\|U - U_1U_2\cdots U_l\| < \varepsilon$ such that $l = O(\log^4(1/\varepsilon))$. By Lemma 2, $\|\rho(U) - \rho(U_1U_2\cdots U_l)\| < O(\varepsilon)$. Since ρ is a homomorphism, $\rho(U_1U_2\cdots U_l) = \rho(U_1)\rho(U_2)\cdots\rho(U_l)$. That is, $\|V - \rho(U_1)\rho(U_2)\cdots\rho(U_l)\| < O(\varepsilon)$, where $l = O(\log^4(1/\varepsilon))$.

3. Approximations in $SO(3)$

Now we describe how an arbitrary unit-determinant orthogonal matrix can be approximated by $\rho(\mathcal{G})$, where $\mathcal{G}$ is an instruction set in $SU(2)$. Recall the proof of the Solovay–Kitaev theorem is highly constructive; it provides essential ingredients for finding the sequence of elements from the instruction set approximating the given unitary to a given accuracy ε. As implied by Theorem 5, our algorithmic version for $SO(3)$ too is based on the steps in finding those elements as in the proof of the original theorem.

For completion, we first describe the algorithm for finding the approximations in $SU(2)$. We follow the procedure given by Dawson and Nielsen [23] in this regard.

3.1. Solovay–Kitaev Algorithm. As described in [23], the Solovay–Kitaev algorithm is explainable using the following lemma.

Lemma 6 [23]. *Suppose $V, W, \tilde{V}$, and $\tilde{W}$ are unitaries such that $\|V - \tilde{V}\|, \|W - \tilde{W}\| < \Delta$, and also $\|I - V\|, \|I - W\| < \delta$. Then,*

$$\left\| VWV^\dagger W^\dagger - \tilde{V}\tilde{W}\tilde{V}^\dagger\tilde{W}^\dagger \right\| < 8\Delta\delta + 4\Delta\delta^2 + 8\Delta^2 + 4\Delta^3 + \Delta^4. \tag{5}$$

The algorithm in $SU(2)$ can be expressed in pseudocode as follows.

The algorithm is a function which takes two inputs: U is an arbitrary element in $SU(2)$ which we desire to approximate by $\mathcal{G}$, and n a nonnegative integer which controls the accuracy of the approximation. This function returns sequence elements from an instruction set $\mathcal{G}$ in $SU(2)$ which approximates U to an accuracy of ε_n, a strictly decreasing function of n. The Solovay–Kitaev algorithm is recursive and the recursion terminates when $n = 0$.

$$\text{if } (n = = 0) \text{Return Basic Approximation } U. \tag{6}$$

In this step, we find an ε_0 approximation to U. To find such an approximation, we have to assure that we have constructed an ε_0-net: a set containing elements from $\langle \mathcal{G} \rangle$ such that for any unitary matrix we can find an ε_0 approximation from it. Since ε_0 is a constant and $\langle \mathcal{G} \rangle$ is dense in $SU(2)$, we can build a gate net by enumerating and sorting a large number of elements from $\mathcal{G}_{l_0}$ for sufficiently large but fixed positive integer l_0 and creating a search algorithm to find the closed approximation. If $n \neq 0$, then we find an ε_{n-1} approximation to U:

$$\text{Set } U_{n-1} = \text{Solovay} - \text{Kitaev}(U, n-1). \tag{7}$$

If $\tilde{\Delta}$ is an ε_n approximation to $\Delta = UU_{n-1}^{\dagger}$, then by the unitary invariance of the norm,

$$\left\| U - \tilde{\Delta} U_{n-1} \right\| = \left\| UU_{n-1}^{\dagger} - \tilde{\Delta} \right\| = \left\| \Delta - \tilde{\Delta} \right\| < \varepsilon_n. \tag{8}$$

Thus, finding an ε_n approximation to Δ with $\varepsilon_n < \varepsilon_{n-1}$ allows us to find an improved approximation (i.e., $\varepsilon_n < \varepsilon_{n-1}$) to U. To find such an approximation, first we decompose $\Delta = UVW^{\dagger}V^{\dagger}$, where U, V are unitaries with $\|I - V\|, \|I - U\| < k_1\sqrt{\varepsilon_{n-1}}$, where k_1 is positive constant:

$$\text{Set } V, W = \text{GC} - \text{Decompose}\left(UU_{n-1}^{\dagger}\right). \tag{9}$$

This decomposition is known as the balance group commutator. To find such a decomposition, we use the fact that any arbitrary unitary can be represented as a rotation in the Bloch sphere. If Δ is a rotation by an angle θ about some axis $\mathbf{n}$ on the Bloch sphere, consider α satisfying

$$\begin{aligned} \sin\frac{\theta}{2} &= 2\sin^2\frac{\alpha}{2}\sqrt{1 - \sin^4\frac{\alpha}{2}}, \\ \alpha &= \sin^{-1}\left(\frac{\sqrt[4]{1 - \cos(\theta/2)}}{\sqrt[4]{2}}\right). \end{aligned} \tag{10}$$

Then, if $\tilde{V}$ is a rotation by α about the x axis and $\tilde{W}$ is a rotation by α about the y axis, on the bloch sphere, then $N = \tilde{V}\tilde{W}\tilde{V}^{\dagger}\tilde{W}^{\dagger}$ is conjugate to Δ (i.e., $\Delta = SNS^{\dagger}$) for some unitary S. Since N and Δ are unitary matrices, they are diagonalizable; moreover, they have the same eigenvalues. Thus,

```
function Solovay–Kitaev(Gate U, depth n)
  if (n == 0)
    Return Basic Approximation U
else
    Set U_{n-1} = Solovay–Kitaev(U, n − 1)
    Set V, W = GC-Decompose(UU†_{n-1})
    Set V_{n-1} = Solovay–Kitaev(V,n − 1)
    Set W_{n-1} = Solovay–Kitaev(W,n − 1)
    Return U_n = V_{n-1} W_{n-1} V†_{n-1} W†_{n-1}
```

Pseudocode 1

by diagonalizing N and Δ, we find a diagonal matrix D and two unitary matrices S_{Δ} and S_N such that

$$\begin{aligned} M &= S_{\Delta} D S_{\Delta}^{\dagger}, \\ N &= S_N D S_N^{\dagger}. \end{aligned} \tag{11}$$

Now, letting $S = S_{\Delta}S_N^{\dagger}$, we have $V = S\tilde{V}S^{\dagger}$ and $W = S\tilde{W}S^{\dagger}$ satisfying

$$\Delta = UVW^{\dagger}V^{\dagger}. \tag{12}$$

Also, for sufficiently small ε_{n-1}, V and W satisfy

$$\|I - V\|, \|I - W\| < k_1\sqrt{\varepsilon_{n-1}} \tag{13}$$

for some positive constant k_1.

Now, we find ε_{n-1} approximations to both V and W:

$$\begin{aligned} &\text{Set } V_{n-1} = \text{Solovay} - \text{Kitaev}(V, n-1), \\ &\text{Set } V_{n-1} = \text{Solovay} - \text{Kitaev}(V, n-1). \end{aligned} \tag{14}$$

By replacing Δ by ε_{n-1} and δ by $k_1\sqrt{\varepsilon_{n-1}}$ in Lemma 6, the group commutator of V_{n-1} and W_{n-1} turns out to be a $k_2\varepsilon_{n-1}^{3/2}$ approximation to Δ for some positive constant k_2. Now, if $(1/k_2^2) < \varepsilon_{n-1}$, then $k_2\varepsilon_{n-1}^{3/2} < \varepsilon_{n-1}$. Hence, $\varepsilon_n = k_2\varepsilon_{n-1}^{3/2}$ provides an improved approximation for U. Accordingly, the value of ε_0 is determined by this constant k_2; i.e., for this construction to guarantee that $\varepsilon_0 > \varepsilon_1 > \cdots$, the value of ε_0 must be strictly less than $1/k_2^2$ (i.e., $\varepsilon_0 < (1/k_2^2)$). This algorithm concludes by returning the sequences of elements in $\mathcal{G}$ that approximate the group commutator as well as U_{n-1}.

3.2. Solovay–Kitaev Algorithm in $SO(3)$. In light of the algorithmic steps described, now it is possible to provide the algorithmic version for $SO(3)$ as follows.

This algorithm is a function which takes two inputs: S: an arbitrary element in $SO(3)$ which we intend to approximate and n: a nonnegative integer which controls the accuracy of the approximation. This function returns a sequence of elements from an instruction set $\rho(\mathcal{G}) \subset SO(3)$, where $\mathcal{G}$ is an instruction set in $SU(2)$, which approximates S

```
function Solovay–Kitaev(S,depth n)
    Set U = SO3ToSU2(S)
    Set Ũ = SK(U, n)
    Set S̃ = SU2ToSO3(S̃)
Return S̃
```

Pseudocode 2

to an accuracy of ε_n, where ε_n is a decreasing function of n, i.e, $\varepsilon_n \longrightarrow 0$ as $n \longrightarrow \infty$.

$$\text{Set } U = \text{SO3ToSU2}(S). \tag{15}$$

In this step, we find $U \in SU(2)$ such that $\rho(U) = S$, where ρ is the homomorphic mapping from $SU(2)$ to $SO(3)$, so that we can find a Solovay–Kitaev approximation for U in $SU(2)$ (SK(.,.) is the Solovay–Kitaev function in $SU(2)$):

$$\text{Set } \tilde{U} = \text{SK}(U, n). \tag{16}$$

Supposing that for a given depth m the SK function approximates any unitary matrix $V \in SU(2)$ to accuracy k_m, we find a k_n approximation $\tilde{U}$ to U. Next, we find $\rho(\tilde{U})$:

$$\text{Set } \tilde{S} = \text{SUToSO3}(S). \tag{17}$$

By Lemma 2, $\tilde{S}$ turns out to be an $\varepsilon_n = ck_n$ approximation for S, for some positive constant c. Since $\tilde{U}$ is a sequence of elements from $\mathcal{G}$, there are $U_1, U_2, \cdots U_n \in \mathcal{G}$ such that $\tilde{U} = U_1 U_2 \cdots U_n$. Then, $\tilde{S} = \rho(\tilde{U}) = \rho(U_1 U_2 \cdots U_n) = \rho(U_1)\rho(U_2) \cdots \rho(U_n)$, because ρ is a homomorphism. Thus, $\tilde{S}$ is a sequence of elements from $\rho(\mathcal{G})$ which approximates S to an accuracy ε_n. For a given depth m, k_m is approximation error associated with the Solovay–Kitaev approximations in $SU(2)$. Therefore, we can ensure that $k_0 > k_1 > \cdots$, which implies $\varepsilon_0 > \varepsilon_2 > \cdots$. Finally, this function returns a sequence of instructions from $\rho(\mathcal{G})$ which approximates S to an accuracy of k_n.

4. Computational Experience

One challenge encountered in the computation is that ρ^{-1} fails to exist as the map is not one to one. This however was overcome using the fact that for given $A \in SO(3)$ it is possible to find $U \in SU(2)$ such that $\rho(U) = A$, for which the following construction was used. Any element in $SO(3)$ can be represented by a real number θ, the angle of rotation, and a rotation axis $\mathbf{a} = (a_x, a_y, a_z)$, which is a 3-dimensional unit vector, denoted by $R_{\mathbf{a}}(\theta)$. The corresponding matrix $R_{\mathbf{a}}(\theta)$ can be expressed explicitly by

$$R_{\mathbf{a}}(\theta) = I + \sin\theta N_{\mathbf{a}} + (1 - \cos\theta){N_{\mathbf{a}}}^2, \tag{18}$$

where

$$N_{\mathbf{a}} = \begin{pmatrix} 0 & -a_z & a_y \\ a_z & 0 & -a_x \\ -a_y & a_x & 0 \end{pmatrix}. \tag{19}$$

For a given rotational matrix $R_{\mathbf{a}}(\theta)$, define

$$U = \begin{pmatrix} \cos\frac{\theta}{2} - i\left(a_z \sin\frac{\theta}{2}\right) & -a_y \sin\frac{\theta}{2} - i\left(a_x \sin\frac{\theta}{2}\right) \\ a_y \sin\frac{\theta}{2} - ia_x \sin\frac{\theta}{2} & \cos\frac{\theta}{2} + i\left(a_z \sin\frac{\theta}{2}\right) \end{pmatrix}. \tag{20}$$

One can verify that $U \in SU(2)$ and $\rho(U) = R_{\mathbf{a}}(\theta)$. Therefore, for an element $A \in SO(3)$, in order to find an element $U \in SU(2)$ such that $\rho(U) = A$, under this construction, we need to find a unit vector $\mathbf{a} \in \mathbb{R}^3$ and a real number θ such that $R_{\mathbf{a}}(\theta) = A$.

Let $A \in SO(3)$, and suppose A is the corresponding rotational matrix of $R_{\mathbf{a}}(\theta)$ (i.e., $A = R_{\mathbf{a}}(\theta)$). If $\mathbf{v}$ is any vector parallel to $\mathbf{a}$, then it must satisfy $A\mathbf{v} = \mathbf{v}$, because the rotation of $\mathbf{v}$ around the axis of rotation must result in $\mathbf{a}$. Since $A \in SO(3)$, we can always find an eigenvalue A which is equal to 1, from which it immediately follows that $\mathbf{a}$ is an eigenvector which corresponds to the eigenvalue 1. So by diagonalizing A, we find the unit vector $\mathbf{a}'$ which is parallel to each other $\mathbf{a}$. Now, since both $\mathbf{a}$ and $\mathbf{a}'$ are unit vectors, we must have $\mathbf{a} = \mathbf{a}'$ or $\mathbf{a}' = \mathbf{a}$. By equation (18), the trace of the matrix A reduces to $\text{Tr}(A) = 1 + 2\cos\theta$, which immediately results in $\theta = \cos^{-1}((\text{Tr}(A) - 1)/2)$. Now, by defining $\alpha \in \mathbb{R}$ such that $|\alpha| = |\theta|$ and choosing the right sign for α to match the rotational axis $\mathbf{a}'$ (i.e., $\mathbf{a}\theta = \mathbf{a}'\alpha$), we get ${R_{\mathbf{a}}}'(\theta) = R_{\mathbf{a}}(\alpha) = A$.

Accordingly, we implemented our algorithm in $SO(3)$ to find the Solovay–Kitaev approximates to several special unitary matrices. The computational experiment was conducted in accordance with the algorithmic steps mentioned and the bound was obeyed as in Theorem 5. We implemented with different instruction sets and the implementation with the instruction set $\{S_1, S_2, S_3, {S_1}^\dagger, {S_2}^\dagger, {S_3}^\dagger\}$ in $SU(2)$ where

$$S_1 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 + 2i & 1 \\ 1 & 1 - 2i \end{pmatrix},$$

$$S_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}, \tag{21}$$

$$S_3 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

resulted in much shorter length for a given ε than the others. It would be an interesting future work to identify any classes or subgroups of matrices that can be approximated best by each instruction set, perhaps with a comparison of different instruction sets.

5. Discussion

Unconventional computing with different algebraic structures had been the topic of interest for a few previous works for which the primary motivation was quantum computing. Based on the fact that the circuit-gate framework of quantum computing relies on the Solovay–Kitaev theorem, we investigated the possibility of deriving a version of this theorem for $SO(3)$ on a three-level quantum system, indicating the potential of using orthogonal matrices for efficient computation.

Three-level quantum systems and relevant operators had already been a topic of interest. In analogy with standard circuit-gate framework, it was customary to use the elements in the unitary group $SU(3)$ as the operators in these systems. Despite the recent experimental achievements, theoretical bounds, capacity, and other related questions on three-level quantum systems were seldom explored. With our version of the Solovay–Kitaev theorem, it is now known that efficient computation is possible with the orthogonal subgroup $SO(3)$ of $SU(3)$. This is a noticeable distinction when compared with the subgroup $SO(2)$ of $SU(2)$. Being an Abelian group, it is impossible to perform Solovay–Kitaev type approximations on $SO(2)$. Thus, an instruction set in standard quantum computation enforces the inclusion of T (the phase gate), T^2, or $T^{\dagger 2}$, the nonorthogonal gates. However, the fault-tolerant implementation of the phase gate T is much more complicated than the orthogonal gates [25]. Therefore, quantum speedup only using orthogonals is beyond feasibility in standard circuit-gate framework, though desired. In contrast to this, as our results indicate, quantum speedup with orthogonals is theoretically feasible in a three-level quantum system.

It is worthwhile to consider our version of the Solovay–Kitaev theorem in the context quantum compilation [26, 27] in which the conversion of a nonfault-tolerant circuit into a fault tolerant one is investigated. A recent paper introduced several efficient methods for quantum compilation using physical machine descriptions, which included one method based on the Solovay–Kitaev approximations [28]. Although compilation and optimization of three-level quantum circuits have been the subject of a few other works [19, 20, 29], none is based on the Solovay–Kitaev theorem. It would be an interesting future task to investigate whether efficient compilations are possible for a three-level system with orthogonals. This would be possible by constructing a Solovay–Kitaev-based compilation method analogous to the one in [28], for which our algorithm in Section 3.1 would be helpful.

Our aim was particularly on exploring the approximation power of special orthogonal matrices. Therefore, we confined our study to a particular form of instruction sets in $SO(3)$; that is, the images of instruction sets in $SU(2)$. A closer inspection reveals that an *arbitrary* instruction set in $SO(3)$ behaves similarly, resulting in the same length for a given accuracy. Therefore, it is an immediate consequence of Theorem 5 that slightly different versions of the Solovay–Kitaev theorem and algorithm for $SO(3)$ can be established. However, the applicability of the Solovay–Kitaev theorem to other Lie groups than $SO(3)$ still remains a nontrivial and theoretically interesting topic, which has not been investigated in literature. It would be a potential future task to see if the theorem is extendable to those groups.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

AM would like to thank Jingbo Wang, Lyle Noakes, André Nies, and Willem Fouché for insightful discussions.

References

[1] R. Solovay, *Proof of Solovay Kitaev Theorem*, 1995.

[2] A. Yur'evich Kitaev, "Quantum computations: algorithms and error correction," *Uspekhi Matematicheskikh Nauk*, vol. 52, no. 6, pp. 53–112, 1997.

[3] L. F. Willem, "An algorithmic construction of quantum circuits of high descriptive complexity," *Electronic Notes in Theoretical Computer Science*, vol. 221, pp. 61–69, 2008.

[4] A. N. Michael and I. Chuang, *Quantum Computation and Quantum Information*, 2000.

[5] D. Aharonov, W. Van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, "Adiabatic quantum computation is equivalent to standard quantum computation," *SIAM Review*, vol. 50, no. 4, pp. 755–787, 2008.

[6] A. M. Childs, D. Gosset, and Z. Webb, "Universal computation by multiparticle quantum walk," *Science*, vol. 339, no. 6121, pp. 791–794, 2013.

[7] A. C.-C. Yao, "Quantum circuit complexity," *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, , pp. 352–361, IEEE, 1993.

[8] D. Aerts and M. Czachor, "Cartoon computation: quantum-like computing without quantum mechanics," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 13, pp. F259–F266, 2007.

[9] M. Czachor, "Elementary gates for cartoon computation," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 31, pp. F753–F759, 2007.

[10] J. M. Fernandez and W. A. Schneeberger, "Quaternionic computing," 2003, http://arxiv.org/abs/quant-ph/0307017.

[11] M. A. Graydon, "Quaternionic quantum dynamics on complex hilbert spaces," *Foundations of Physics*, vol. 43, no. 5, pp. 656–664, 2013.

[12] P. L. Ben, T. J. Weinhold, N. K. Langford et al., "Manipulating biphotonic qutrits," *Physical review letters*, vol. 100, no. 6, article 060504, 2008.

[13] P. Gokhale, J. M. Baker, C. Duckering, F. T. Chong, N. C. Brown, and K. R. Brown, "Extending the Frontier of Quantum

Computers With Qutrits," *IEEE Micro*, vol. 40, no. 3, pp. 64–72, 2020.

[14] Y.-H. Luo, H.-S. Zhong, M. Erhard et al., "Quantum teleportation in high dimensions," *Physical review letters*, vol. 123, no. 7, p. 070505, 2019.

[15] B. Li, Z.-H. Yu, and S.-M. Fei, "Geometry of quantum computation with qutrits," *Scientific reports*, vol. 3, no. 1, p. 2594, 2013.

[16] D. Mc Hugh and J. Twamley, "Trapped-ion qutrit spin molecule quantum computer," *New journal of physics*, vol. 7, no. 1, p. 174, 2005.

[17] G. Khanna, S. Mukhopadhyay, R. Simon, and N. Mukunda, "Geometric phases for $SU(3)$ representations and three level quantum systems," *Annals of Physics*, vol. 253, no. 1, pp. 55–82, 1997.

[18] A. B. Klimov, R. Guzman, J. C. Retamal, and C. Saavedra, "Qutrit quantum computer with trapped ions," *Physical Review A*, vol. 67, no. 6, article 062313, 2003.

[19] R. Nader-Ali, A. Jafari-Dolama, and M. Amniat-Talab, "Implementation of single-qutrit quantum gates via tripod adiabatic passage," *International Journal of Optics and Photonics*, vol. 4, no. 1, pp. 39–48, 2010.

[20] V. E. Zobov and V. P. Shauro, "On time-optimal nmr control of states of qutrits represented by quadrupole nuclei with the spin i=1," *Journal of Experimental and Theoretical Physics*, vol. 113, no. 2, pp. 181–191, 2011.

[21] S. Dogra, K. Dorai, and Arvind, "Majorana representation, qutrit hilbert space and nmr implementation of qutrit gates," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 51, no. 4, p. 045505, 2018.

[22] J. F. Cornwell, *Group Theory in Physics: An Introduction*, Academic press, San Diego, California, United States., 1997.

[23] C. M. Dawson and M. A. Nielsen, "The Solovay Kitaev algorithm," 2005, http://arxiv.org/abs/quant-ph/0505030.

[24] E. Wigner, *Group Theory and Its Application to the Quantum Mechanics of Atomic Spectra*, 2012.

[25] P. Aliferis, D. Gottesman, and J. Preskill, "Quantum accuracy threshold for concatenated distance-3 codes," *Quantum information & computation*, vol. 6, pp. 97–165, 2005.

[26] L. Biswal, D. Bhattacharjee, A. Chattopadhyay, and H. Rahaman, "Techniques for fault-tolerant decomposition of a multicontrolled Toffoli gate," *Physical Review A*, vol. 100, no. 6, 2019.

[27] A. Paler, I. Polian, K. Nemoto, and S. J. Devitt, "Fault-tolerant, high-level quantum circuits: form, compilation and description," *Quantum Science and Technology*, vol. 2, no. 2, p. 025003, 2017.

[28] C.-C. Lin, A. Chakrabarti, and N. K. Jha, "Ftqls: fault-tolerant quantum logic synthesis," *IEEE Transactions on very large scale integration (VLSI) systems*, vol. 22, no. 6, pp. 1350–1363, 2013.

[29] T. Bækkegaard, L. B. Kristensen, N. J. S. Loft, C. K. Andersen, D. Petrosyan, and N. T. Zinner, "Realization of efficient quantum gates with a superconducting qubit-qutrit circuit," *Scientific Reports*, vol. 9, no. 1, p. 13389, 2019.