Preliminaries: how, in the presence of symmetry, locality restricts realizable unitaries

Runqiu Xu[1]

[1]Department of Math, University of California at San Diego, La Jolla, CA 92093

To understand why we care about how the unitary transformation on a composite system can be generated using local unitaries, we look up a basic result in quantum computing for 2-local unitaries. After understanding using 2-local unitaries can generate universal unitaries of composite systems, it's natural to ask questions if using k-local unitaries can maintain the universality. In particular, we ask if such universality remains valid in the presence of conservation laws and global symmetries. Further question of all symmetric unitaries on a composite system can be generated using local symmetric unitaries on the system as discussed in the main reference [1] using the tool called ancillary qubits.

I. INTRODUCTION

For the first part, we will explain 2-bit gates are universal for quantum computations with a specific 3-bit gates decomposition and algebraic formulation of the problem.

For the second part, We want to understand how the local symmetric conditions affect universal symmetric conditions. Or in other words, whether we can always decompose universal gates into local gates. Our main tool will be $\mathcal{V}_k^G$ the unitaries that can be generated by k-local unitaries. If we can show $\mathcal{V}_k^G = \mathcal{V}_n^G$ where n is the system size, then it means the universal symmetry can be generated locally.

II. SECTION 1

In this section, we will sketch the proof that all necessary three-bits operations can be executed using 2-bits, i.e., the 3-local unitaries can be generated by 2-local unitaries.

A. Background

To classify quantum computation, we need to build the reversible classical network since all unitary quantum operations are necessarily reversible, therefore, reversible computing is a subset of quantum computing. We learned from McGreevy[2] how to build up a reversible XOR gate. To implement AND reversibly, a three-bit gate is required in which a_1 and a_2 are passed through unchange, while the third bit is XOR with the AND of the first two, returning $(a_1 \cdot a_2) \oplus a_3$. Since this three-bit gate comprises both the XOR and the AND functions, it can be considered to be the universal reversible computation gate and it has come to be known as the Toffoli gate T. Given this, Deutsch [3] generalized the posited operation of a three-bit gate, from one which performs transformations (in the reversible case, it's permutations) on the $8 = 2^3$ possible states of three bits, to one which performs unitary transformations within the 2^3-dimentional complex vector space (Hilbert space) spanned by the states of 3 bits, i.e.,

$$|a_1, a_2, a_3\rangle \Longrightarrow |a_1', a_2', a_3'\rangle$$

This leads us to another way of specifying gates. Consider an 8×8 matrix $\mathbf{S_Q}$ with components

$$\mathbf{S_Q}{}^{a_1,a_2,a_3}_{a_1',a_2',a_3'} = \delta^{a_1}_{a_1'}\delta^{a_2}_{a_2'}[(1-a_1\cdot a_2)\delta^{a_3}_{a_3'} + i a_1\cdot a_2 e^{-\frac{1}{2}i\pi\alpha}(\mathbf{S_N^\alpha})^{a_3}_{a_3'}]$$

such that

$$|a_1, a_2, a_3\rangle \Longrightarrow \sum_{a_1',a_2',a_3' \in (0,1]} \mathbf{S_Q}{}^{a_1,a_2,a_3}_{a_1',a_2',a_3'} |a_1', a_2', a_3'\rangle$$

where

$$\mathbf{S_N^\alpha} = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi\alpha} & 1-e^{i\pi\alpha} \\ 1-e^{i\pi\alpha} & 1+e^{i\pi\alpha} \end{pmatrix}$$

is the "αth power of NOT".

B. Proof that Q can be realized by 2-bit gate

Relabel the basis to be "computational basis" labeled 0-7. If n is an integer, we can write out $\mathbf{S_Q^{4n+1}}$ and $\mathbf{S_Q^{4n}}$ such that all gates whose $\mathbf{S}$ are of the form

$$\mathbf{U}_\lambda = \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& 1 && \\ &&&&&& \cos(\lambda) & i\sin(\lambda) \\ &&&&&& i\sin(\lambda) & \cos(\lambda) \end{pmatrix}$$

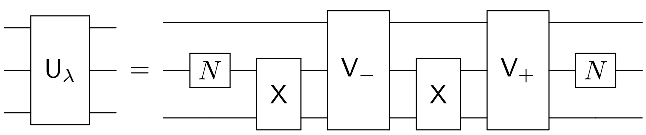
To demonstrate the equivalence of one of Deutsch's 3-bit gates with a sequence of 2-bit gates, for infinitesimal values of the rotation parameter δ, we introduce

$$\mathbf{X}^{(2)} = \begin{pmatrix} e^{i\phi} & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \mathbf{V}^{(2)} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \cos\phi & \sin\phi \\ & & -\sin\phi & \cos\phi \end{pmatrix}$$

The $\mathbf{S}$ matrix of these gates operating in the basis of all three bits is a direct product, i.e., $\mathbf{V}^{(2)} \otimes \mathbb{I}$, and so is a block-diagonal 8×8 matrix. So we get equality:

$$\mathbf{U}_\lambda(\lambda = \delta) \simeq \mathbf{N}_2 \mathbf{V}_{13}(\phi = \sqrt{\delta}) \mathbf{X}_{23}(\phi = -\sqrt{\delta})$$
$$\times \mathbf{V}_{13}(\phi = -\sqrt{\delta}) \mathbf{X}_{23}(\phi = \sqrt{\delta}) \mathbf{N}_2,$$

where $\mathbf{N}$ is simply the classical NOT. The figure below demonstrates how it is decomposed.



C. Complete of the proof

The following result will show the above decomposition may be obtained compactly within the language of Lie algebra.

Lie algebra $\mathbf{H}$ is defined as infinitesimal generators of Lie group by

$$\delta \mathbf{U} = \mathbb{1} + i\epsilon \mathbf{H}$$

A key theorem of Lie-group theory is that, if $\mathbf{H}_1$ and $\mathbf{H}_2$ are generators of the group, then other generators may be obtained by *commutation*, producing the Lie algebra :

$$\mathbf{H}_3 = i[\mathbf{H}_1, \mathbf{H}_2]$$

Moreover, one can write down an explicit expression for how the unitary operation $e^{i\delta \mathbf{H}_3}$ is obtained from $e^{i\delta \mathbf{H}_1}$ and $e^{i\delta \mathbf{H}_2}$, i.e.,

$$e^{i\delta(i[\mathbf{H}_1, \mathbf{H}_2])} \simeq e^{i\sqrt{\delta}\mathbf{H}_2} e^{-i\sqrt{\delta}\mathbf{H}_2} e^{-i\sqrt{\delta}\mathbf{H}_1} e^{i\sqrt{\delta}\mathbf{H}_1}$$

which is valid for small parameter δ. Thus we see that the sequence of gates in illustrated in the figure above is nothing more than the execution of a commutator of the Lie algebra. Further computational details are discussed in DiVincenzo[4].

III. SECTION 2

In this section, we explain the interplay between the symmetric Hermitian operator H(t) and symmetric unitary evolution V(t) in Iman Marvian [1].

A. Setup

An operator is called k-*local* if it acts non-trivially on the Hilbert spaces of, at most, k sites. An operator is called G-*invariant*, or *symmetric*, if satifies $U(g)AU^\dagger = A$, for any group element $g \in G$. Each element $g \in G$ is represented by the unitary $U(g) = u(g)^{\otimes n}$. The set of unitaries that are symmetric under this G representation itself forms a group, denoted by

$$\mathcal{V} \equiv V : VV^\dagger = I, [V, U(g)] = 0, \forall g \in G, \quad (3.1)$$

We define $\mathcal{V}_k^G$ to be the set of all unitary transformations that can be implemented with k-local unitaries. More formally, $\mathcal{V}_k^G = \prod_{i=1}^{m_i} V_i$, generated by composing symmetric k-local unitaries V_i: $i = 1, ..., m$ for a finite m.

A generic *local* Hamiltonian H(t) has a decomposition as $H(t) = \sum_j h_j(t)$, where each term $h_j(t)$ is k-local for a fixed k. The unitary evolution generated by this Hamiltonian is determined by the Shrödinger equation

$$\frac{dV(t)}{dt} = -iH(t)V(t) = -i\,[\sum_j h_j(t)]\,V(t) \quad (3.2)$$

with the initial condition $V(0) = I$

B. Converse statement

We want to prove for all $t \geq 0$, any unitary in $\mathcal{V}_k^G$ can be generated using a G-invariant Hamiltonian H(t) that can be written as the sum of k-local terms.

The group generated by k-local symmetric unitaries is given by

$$\mathcal{V}_k^G \equiv \langle\, V : VV^\dagger = I, [V, U(g)] = 0, \forall g \in G \,\rangle,$$

The real Lie algebra generated by the k-local, skew-Hermitian, G-invariant operators is given by

$$\mathfrak{h} \equiv \mathfrak{alg}_{\mathbb{R}}\{A : k\!-\!local, A + A^\dagger = 0, [A, U(g)] = 0 : \forall g \in G\},$$

Note that for any k-local symmetric Hamiltonian h, the family of unitaries generated by h i.e., $\{e^{-iht} : t \in \mathbb{R}\}$ are all k-local and symmetric, i.e.

$$iH \in \mathfrak{h}_k \implies \forall t : e^{-iH(t)} \in \mathcal{V}_k^G$$

Conversely, any k-local symmetric unitary V can be obtained by applying a k-local symmetric Hamiltonian on the system for a finite time i.e.

$$\forall t : e^{-iH(t)} \in \mathcal{V}_k^G \implies iH \in \mathfrak{h}_k$$

Further, we are given the fact that $\mathcal{V}_k^G$ is a compact connected Lie group and the exponential map from the Lie algebra to the Lie group is subjective i.e.

$$\mathcal{V}_k^G = e^{\mathfrak{h}_k}$$

Therefore, we confirm that by characterizing the lie algebra $\mathfrak{h}_k$ we also find a full and direct characterization of $\mathcal{V}_k^G$

Given the fact $\mathfrak{h}$ is in the real algebra generated by skew-Hermitian operators $\{A_j\}_j$ such that it is in the form

$$iH = \sum_j \alpha_j A_j + \sum_{j_1,j_2} \beta_{j_1,j_2}[A_{j_1}, A_{j2}] + ...,$$

Combining the above parts, we can prove $\mathcal{V}_k^G = e^{\mathfrak{h}_k} = e^{-iH(t)}$ where H(t) is G-invariant that can be written as the sum of k-local terms.

C. Proposition 3

Now we want to prove for all time $t \geq 0$, the unitary evolution V(t) generated by Hamiltonian H(t) according to the Shrödinger equation belongs to the Lie group $\mathcal{V}_k^G$, i.e., can be implemented by a quantum circuit with a finite number of k-local G-invariant gates.

Proof. Supposed $H(t) = \sum_j h_j(t)$ is G-invariant, this doesn't imply that the k-local terms $\{h_j(t)\}$ are also G-invarinat. However, we can easily show that H(t) can be written as sum of k-local G-invariant terms, i.e., $H(t) = \sum_j \tilde{h}_j$, where each $\tilde{h}_j$ is both k-local and G-invariant. Thus, we can make use of the uniforma Haar distribution over group compact Lie group G,we define

$$\tilde{h_j} \equiv \int dgU(g)h_j(t)U(g)^\dagger$$

It can be seen that $\tilde{h_j}$ becomes G-invariant. Note that the operator $U(g)h_j(t)U(g)^\dagger$ acts trivially on all systems except on the k-systems, where $h_j(t)$ acts non-trivially. It follows that $\tilde{h}_j(t)$ is also k-local. Finally, the assumption that $H(t) = \sum_j h_j(t)$ is G-invariant implies $H(t) = \sum_j \tilde{h}_j(t)$. Since all operators $\{\tilde{h}_j(t) : t \geq 0\}_j$ are k-local and G-invariant, the Lie algebra generated by operators $\{\tilde{h}_j(t) : t \geq 0\}_j$ is a sub-algebra of $\mathfrak{h}_k$, the Lie algebra associated to Lie group $\mathcal{V}_k^G$. Together with a standard result of quantum control theory [5], this implies that the family of unitaries $V(t = 0) = I$ belongs to $\mathcal{V}_k^G$ for all $t \geq 0$.

IV. CONCLUSION

This result means that to characterize the group $\mathcal{V}_k^G$ generated by k-local symmetric unitaries, it suffices to characterize the Lie algebra generated by k-local symmetric Hermitian operators. In particular the dimension of this Lie algebra, as a vector space over $\mathbb{R}$, is equal to $\dim(\mathcal{V}_k^G)$, the dimension of the manifold associated to $\mathcal{V}_k^G$, which is also equal to the number of real parameters needed to specify a general element of $\mathcal{V}_k^G$. Using this relation, the main result in the paper is to establish an upper bound on $\dim(\mathcal{V}_k^G)$.

[1] I. Marvian, "Locality and Conservation Laws: How, in the presence of symmetry, locality restricts realizable unitaries," *arXiv preprint arXiv:2003.05524* (2020). 1, 2

[2] J. Mcgreevy, "Quantum Information Theory,". 1

[3] D. E. Deutsch, "Quantum computational networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* **425** (1989), no. 1868 73–90. 1

[4] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," *Physical Review A* **51** (1995), no. 2 1015. 2

[5] D. d'Alessandro, *Introduction to quantum control and dynamics.* CRC press, 2021. 3