

Locality and Conservation Laws: How, in the presence of symmetry, locality restricts realizable unitaries

Iman Marvian¹

¹*Departments of Physics & Electrical and Computer Engineering,
Duke University, Durham, North Carolina 27708, USA*

According to an elementary result in quantum computing, any unitary transformation on a composite system can be generated using 2-local unitaries, i.e., those which act only on two subsystems. Beside its fundamental importance in quantum computing, this result can also be regarded as a statement about the dynamics of systems with local Hamiltonians: although locality puts various constraints on the short-term dynamics, it does not restrict the possible unitary evolutions that a composite system with a general local Hamiltonian can experience after a sufficiently long time. We ask if such universality remains valid in the presence of conservation laws and global symmetries. In particular, can k -local symmetric unitaries on a composite system generate *all* symmetric unitaries on that system? Interestingly, it turns out that the answer is negative in the case of continuous symmetries, such as $U(1)$ and $SO(3)$: unless there are interactions which act non-trivially on every subsystem in the system, some symmetric unitaries cannot be implemented using symmetric Hamiltonians. In fact, the difference between the dimensions of the Lie algebra of all symmetric Hamiltonians and its subalgebra generated by k -local symmetric Hamiltonians with a fixed k , constantly increases with the system size (i.e., the number of subsystems). On the other hand, in the case of group $U(1)$, we find that this no-go theorem can be circumvented if one is allowed to use a pair of ancillary qubits. In particular, any unitary which is invariant under rotations around z , can be implemented using Hamiltonians $XX + YY$ and local Z on qubits. We discuss some implications of these results in the context of quantum thermodynamics and quantum computing.

Locality of interactions of a quantum many-body system imposes strong constraints on the dynamics of the system. A well-known example is the finite speed of propagation of information, as highlighted by the celebrated Lieb-Robinson bound [1]. Nevertheless, it turns out that after a sufficiently long time, systems with general local interactions can still experience any arbitrary unitary time evolution. In particular, according to a fundamental result in quantum control and quantum computing, any unitary transformation on a composite system can be generated by a sequence of 2-local unitary transformations, i.e. those which act non-trivially on, at most, two sites [2–5].

In this Letter, we study this phenomenon in the presence of conservation laws and global symmetries. Clearly, if all the local unitaries obey a certain symmetry, e.g. $SO(3)$, then the overall unitary evolution also obeys the same symmetry. The question is if *all* symmetric unitaries on a composite system can be generated using *local* symmetric unitaries on the system. Perhaps surprisingly, it turns out that the answer is negative in the case of continuous groups, such as $SO(3)$ and $U(1)$. In fact, we find that unless there are terms in the Hamiltonian which act non-trivially on all the subsystems, there are some symmetric unitaries which cannot be implemented using symmetric Hamiltonians.

More generally, we derive simple constraints on the family of unitaries which can be implemented using k -local symmetric Hamiltonians. These constraints imply that the difference between the dimensions of the Lie algebra of all symmetric Hamiltonians and its subalgebra generated by k -local symmetric Hamiltonians constantly grows with the system size. As an example, we consider a composite system formed from qubits, with the symmetry group $U(1)$, corresponding to rotations around z axis, and show that these constraints uniquely

characterize the class of all diagonal Hamiltonians which can be generated using $U(1)$ -invariant k -local Hamiltonians.

The case of $U(1)$ symmetry is specially relevant in the contexts of quantum computing and quantum thermodynamics. For systems with periodic time evolution, the time translations $\{e^{-iH_0t}\}$ generated by the system intrinsic Hamiltonian H_0 , form a group isomorphic to $U(1)$. Energy-conserving unitaries, i.e., those which commute with H_0 , respect this $U(1)$ symmetry. In the context of quantum computing, such *phase-insensitive* unitaries are of special interest, because they are less sensitive to fluctuations and instability of the master clock which determines the timing of the control pulses. Furthermore, in the resource theory of quantum thermodynamics, energy conserving unitaries play a distinct role: they are assumed to be *free*, i.e., realizable with negligible costs [6–8]. However, the above no-go theorem makes this assumption questionable, because it suggests that it may not be possible to implement all such unitaries with local energy-conserving interactions.

Remarkably, we find that in the case of the group $U(1)$, this no-go theorem can be circumvented using ancillary qubits, i.e., auxiliary systems initially prepared in a fixed state which return to their initial state at the end of process. In particular, we show that using 2-local Hamiltonian $XX + YY$ and local Pauli Z , which are both invariant under rotations around z , it is possible to implement all unitaries which are invariant under this symmetry, provided that one can employ two ancillary qubits.

General Setup– We start by formalizing the problem in the most general case, where the system is not necessarily composite. Consider a system with a finite-dimensional Hilbert space \mathcal{H} and let $\mathcal{L}(\mathcal{H})$ be the linear space of operators on

\mathcal{H} . Consider a symmetry described by a finite or compact Lie group G , and let $U : G \rightarrow \mathcal{L}(\mathcal{H})$ be a unitary representation of this symmetry, where the group element $g \in G$ is represented by the unitary $U(g)$. An operator A is called symmetric, or G -invariant, if it is invariant under the action of group G , such that $[A, U(g)] = 0, \forall g \in G$.

As an example, we consider the case of the group $U(1)$, with representation $\{U(e^{i\theta}) = e^{i\theta Q} : \theta \in [0, 2\pi)\}$, where Q is a Hermitian operator with integer eigenvalues and with eigen-decomposition $Q = \sum_{q \in \text{Spec}(Q)} q \Pi_q$. Here, $\text{Spec}(Q)$ is the set of eigenvalues and Π_q is the projector to the eigensubspace corresponding to the eigenvalue q . Operator Q , for instance, could be a conserved charge, angular momentum in a certain direction, or the intrinsic Hamiltonian of a periodic system (multiplied by its period). Then, $U(1)$ -invariant operators are those which are block-diagonal with respect to projectors $\{\Pi_q\}$. Depending on the interpretation of Q , a $U(1)$ -invariant unitary could be called a charge-conserving or energy-conserving unitary.

Suppose one can implement G -invariant unitary transformations $\{e^{-itH_j} : t \in \mathbb{R}, j = 1, \dots\}$ generated by a set of G -invariant Hamiltonians $\{\pm H_j \in \mathcal{L}(\mathcal{H}) : j = 1, \dots\}$. Later, we focus on the special case of local Hamiltonians; but, for now, they can be arbitrary G -invariant Hermitian operators. Composing these unitaries, one can implement any unitary in the form $e^{-it_L H_{j_L}} \dots e^{-it_2 H_{j_2}} e^{-it_1 H_{j_1}}$ for arbitrary integer L . What is the set of all unitaries which can be generated in this way? Clearly, this set forms a group. Furthermore, since all the unitaries in the sequence respect the symmetry, so does their product. Therefore, the generated group is a subgroup of the group of all G -invariant unitaries, denoted by

$$\mathcal{V}_{G-\text{inv}} \equiv \{V : VV^\dagger = I, \forall g \in G : [V, U(g)] = 0\}. \quad (1)$$

We are interested to determine if unitaries $\{e^{-itH_j} : t \in \mathbb{R}, j = 1, \dots\}$ generate any arbitrary G -invariant unitary, i.e. the entire group $\mathcal{V}_{G-\text{inv}}$. Furthermore, if this is not the case, we are interested to determine which elements of $\mathcal{V}_{G-\text{inv}}$ are missing in the generated subgroup.

From Lie groups to Lie algebras– According to a well-known result in quantum computing and control [2, 3, 9], which follows immediately from the standard properties of Lie groups, the Lie group generated by unitaries $\{e^{-itH_j} : t \in \mathbb{R}, j = 1, \dots\}$ includes the one-parameter family of unitaries $\{e^{-iKt} : t \in \mathbb{R}\}$ generated by Hamiltonian K if, and only if, the anti-Hermitian operator iK is an element of the real Lie algebra $\mathfrak{h} \equiv \text{alg}\{iH_j\}_j$, generated by anti-Hermitian operators $\{iH_j\}_j$. For instance, by combining unitaries generated by H_1 and H_2 , one obtains

$$\lim_{n \rightarrow \infty} (e^{-i\frac{t}{n}H_1} e^{-i\frac{c}{n}H_2})^n = e^{-t(iH_1 + cH_2)}, \quad (2a)$$

$$\lim_{n \rightarrow \infty} (e^{-i\frac{t}{n}H_1} e^{-i\frac{t}{n}H_2} e^{i\frac{t}{n}H_1} e^{i\frac{t}{n}H_2})^{n^2} = e^{-t[iH_1, iH_2]}, \quad (2b)$$

for arbitrary $t, c \in \mathbb{R}$. Moreover, by repeating such combinations, one obtains arbitrary linear combinations of generators $\{iH_j\}_j$ and their nested commutators $\{[iH_{j_1}, iH_{j_2}], [[iH_{j_1}, iH_{j_2}], iH_{j_3}], \dots\}$ with real coefficients, and hence all elements of the real Lie algebra \mathfrak{h} .

Since any G -invariant unitary $V \in \mathcal{V}_{G-\text{inv}}$ is a member of a one-parameter family $\{e^{-iKt} : t \in \mathbb{R}\}$ for a G -invariant Hamiltonian K , we find that

Proposition 1. *The family of G -invariant unitaries $\{e^{-itH_j} : t \in \mathbb{R}, j = 1, \dots\}$ generates the set of all G -invariant unitaries $\mathcal{V}_{G-\text{inv}}$ if, and only if, the Lie algebra $\mathfrak{h} = \text{alg}\{iH_j\}_j$ is equal to the Lie algebra of G -invariant anti-Hermitian operators, i.e.*

$$\mathfrak{a} \equiv \{A \in \mathcal{L}(\mathcal{H}) : A + A^\dagger = 0, \forall g \in G : [A, U(g)] = 0\}. \quad (3)$$

Therefore, to characterize $\mathcal{V}_{G-\text{inv}}$ and its subgroup generated by $\{e^{-itH_j} : t \in \mathbb{R}, j = 1, \dots\}$, in the following we focus on the properties of their corresponding Lie algebras, namely \mathfrak{a} and \mathfrak{h} .

Charge vectors– Consider the decomposition of the unitary representation $\{U(g) : g \in G\}$ into the irreducible representations (irreps) of G . The Hilbert space can be decomposed as $\mathcal{H} \cong \bigoplus_{\mu \in \text{irrep}(U)} \mathcal{H}_\mu$, where the summation is over $\text{irrep}(U)$, the set of inequivalent irreps of G appearing in this representation and \mathcal{H}_μ is the subspace corresponding to irrep μ , also known as the isotypic component of μ . A G -invariant Hamiltonian is block-diagonal with respect to this decomposition and, in general, can have support in any arbitrary subset of these sectors. However, as we show next, for Hamiltonians generated by a fixed set of G -invariant Hamiltonians $\{H_j\}_j$, the supports in different subspaces $\{\mathcal{H}_\mu\}$ satisfy particular constraints, dictated by Hamiltonians $\{H_j\}_j$.

For any operator A , consider the vector

$$|\chi_A\rangle \equiv \sum_{\mu \in \text{irrep}(U)} \text{Tr}(A \Pi_\mu) |\mu\rangle, \quad (4)$$

where Π_μ is the projector to the subspace \mathcal{H}_μ and $\{|\mu\rangle : \mu \in \text{irrep}(U)\}$ is a set of orthonormal vectors in an abstract vector space (not the state space of the system). Vector $|\chi_A\rangle$, which will be called the *charge vector* of operator A , encodes information about the components of this operator in different sectors $\{\mathcal{H}_\mu\}$. A general G -invariant Hamiltonian can have any charge vector with real coefficients. In particular, for any set of real numbers $\{a_\mu \in \mathbb{R}\}$, the Hamiltonian $\sum_{\mu \in \text{irrep}(U)} a_\mu \Pi_\mu / \text{Tr}(\Pi_\mu)$ is G -invariant and has the charge vector $\sum_{\mu \in \text{irrep}(U)} a_\mu |\mu\rangle$. In other words, under the linear map $A \rightarrow |\chi_A\rangle$, the image of the Lie algebra of anti-Hermitian G -invariant operators \mathfrak{a} is $\{i \sum_{\mu} a_\mu |\mu\rangle : a_\mu \in \mathbb{R}\}$, which is a vector space over field \mathbb{R} , with dimension equal to $|\text{irrep}(U)|$, the number of inequivalent irreps of G appearing in representation $\{U(g) : g \in G\}$.

Next, consider the set of charge vectors for Hamiltonians

which can be generated using Hamiltonians $\{H_j\}_j$, i.e.

$$\mathcal{S}_\mathfrak{h} \equiv \left\{ |\chi_K\rangle : iK \in \mathfrak{h} \equiv \mathfrak{alg}\{iH_j\}_j \right\}. \quad (5)$$

Clearly, $\mathcal{S}_\mathfrak{h}$ contains the charge vectors of Hamiltonians $\{H_j\}$, denoted by $\{|\chi_j\rangle = \sum_{\mu \in \text{irrep}(U)} \text{Tr}(H_j \Pi_\mu) |\mu\rangle\}$, as well as their linear combinations with real coefficients. The Lie algebra \mathfrak{h} also contains the commutators, such as $\{[iH_{j_1}, iH_{j_2}], [[iH_{j_1}, iH_{j_2}], iH_{j_3}], \dots\}$. However, due to the symmetry of Hamiltonians $\{H_j\}_j$, these commutators do not contribute in $\mathcal{S}_\mathfrak{h}$: for any operator B , by the cyclic property of trace, we have $\text{Tr}(\Pi_\mu [H_j, B]) = \text{Tr}([H_j, B] \Pi_\mu) = 0$, where we have used the fact that H_j commutes with Π_μ . We conclude that the set of charge vectors for Hamiltonians which can be generated using $\{H_j\}_j$ is

$$\mathcal{S}_\mathfrak{h} = \left\{ \sum_j a_j |\chi_j\rangle : a_j \in \mathbb{R} \right\} \equiv \text{Span}_\mathbb{R}\{|\chi_j\rangle\}. \quad (6)$$

In other words, the image of the Lie algebra \mathfrak{h} under the linear map $A \rightarrow |\chi_A\rangle$ is $\text{Span}_\mathbb{R}\{|\chi_j\rangle\}$. Since \mathfrak{h} is a subspace of \mathfrak{a} , the difference between their dimensions is lower bounded by the difference between the dimensions of their images under this linear map. We conclude that

Lemma 1. *Let \mathfrak{a} be the Lie algebra of anti-Hermitian G -invariant operators and \mathfrak{h} be its sub-algebra generated by $\{iH_j \in \mathfrak{a}\}_j$. The difference between their dimensions is lower bounded by*

$$\dim(\mathfrak{a}) - \dim(\mathfrak{h}) \geq |\text{irrep}(U)| - \dim(\text{Span}_\mathbb{R}\{|\chi_j\rangle\}_j). \quad (7)$$

Furthermore, for any G -invariant Hamiltonian A , if its corresponding charge vector $|\chi_A\rangle$ is not in the subspace $\text{Span}_\mathbb{R}\{|\chi_j\rangle\}_j$, then $iA \notin \mathfrak{h}$ and therefore the family of unitaries $\{e^{-iAt} : t \in \mathbb{R}\}$ cannot be generated using Hamiltonians $\{H_j\}_j$.

For instance, in the case of our $U(1)$ example, where the symmetry is represented by unitaries $\{e^{iQ\theta}\}$, the number of inequivalent irreps is $|\text{irrep}(U)| = |\text{Spec}(Q)|$, i.e., the number of distinct eigenvalues of Q . Then, lemma 1 implies that Hamiltonians $\{H_j\}_j$ generate all $U(1)$ -invariant unitaries, only if

$$\dim(\text{Span}\left\{ \sum_{\lambda \in \text{Spec}(Q)} \text{Tr}(H_j \Pi_\lambda) |\lambda\rangle : j = 1, \dots \right\}) = |\text{Spec}(Q)|. \quad (8)$$

Finally, it is worth noting that the conditions in lemma 1 can be stated without using the notions of charge vectors and irreducible representations. For the set of G -invariant operators, there is an invertible linear map between the charge vector $|\chi_A\rangle$ associated to an operator A on one hand, and the function $\chi_A : G \rightarrow \mathbb{C}$ defined by equation $\chi_A(g) = \text{Tr}(AU(g))$ on the other hand; namely they are related via Fourier transform (See Supplementary Material). It follows that for any

G -invariant operators A and $\{H_j\}_j$,

$$|\chi_A\rangle \in \text{Span}_\mathbb{R}\{|\chi_j\rangle\}_j \iff \chi_A \in \text{Span}_\mathbb{R}\{\chi_j\}_j, \quad (9)$$

where χ_A and χ_j are complex functions over group G defined by $\chi_A(g) = \text{Tr}(AU(g))$, and $\chi_j(g) = \text{Tr}(H_j U(g))$, for all $g \in G$. This also implies that $\dim(\text{Span}_\mathbb{R}\{|\chi_j\rangle\}) = \dim(\text{Span}_\mathbb{R}\{\chi_j\})$.

Composite Systems—Next, we apply this result to the case of composite systems. We start with the special case of identical subsystems and later explain how the result can be generalized. Consider a system formed from n local sites, each with a finite-dimensional Hilbert space $\mathcal{H}_i \cong \mathbb{C}^d : i = 1, \dots, n$. Let $\mathcal{H} \cong \bigotimes_{i=1}^n \mathcal{H}_i$ be the joint Hilbert space. Assume all sites have the same representation of symmetry, namely $\{u(g) \in \mathcal{L}(\mathbb{C}^d) : g \in G\}$, and therefore $\{U(g) = u(g)^{\otimes n} : g \in G\}$ is the representation of symmetry on the total system.

We say an operator $A \in \mathcal{L}(\mathcal{H})$ acting on the total system is k -local if it acts non-trivially on, at most, k sites, and acts as the identity operator on the rest (Note that a k -local operator may not be geometrically local). From proposition 1 we know that for any G -invariant Hamiltonian C , the family of unitaries $\{e^{-iCt} : t \in \mathbb{R}\}$ can be generated using k -local G -invariant Hamiltonians if, and only if, iC is in the Lie algebra generated by k -local anti-Hermitian G -invariant operators, denoted by \mathfrak{h}_k , i.e. $iC \in \mathfrak{h}_k \equiv \mathfrak{alg}\{A \in \mathfrak{a} : A \text{ is } k\text{-local}\}$. Consider the set of charge vectors for Hamiltonians which can be generated using k -local G -invariant Hamiltonians, i.e.

$$\mathcal{S}_k \equiv \{|\chi_C\rangle : iC \in \mathfrak{h}_k\} \quad (10a)$$

$$= \text{Span}_\mathbb{R}\{|\chi_C\rangle : iC \in \mathfrak{a}, C \text{ is } k\text{-local}\}, \quad (10b)$$

where the equality follows from Eq.(6). This equality means that, even though using k -local G -invariant Hamiltonians we can generate Hamiltonians which are not k -local, they can only have charge vectors which are allowed for k -local G -invariant Hamiltonians. To characterize these charge vectors we note that, up to a permutation, any k -local operator C can be written as $C = \tilde{C} \otimes I_d^{\otimes(n-k)}$, where $\tilde{C} \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$ acts on the first k sites, $i = 1, \dots, k$, and I_d is the identity operator on \mathbb{C}^d . Since all sites have identical representation of symmetry, any such permutation leaves the total charge in the system invariant (In other words, projectors $\{\Pi_\mu\}$ are permutationally invariant). It follows that

$$\mathcal{S}_k = \{|\chi_C\rangle : iC \in \mathfrak{a}, C = \tilde{C} \otimes I_d^{\otimes(n-k)}\}. \quad (11)$$

In words, this means that the set of charge vectors of Hamiltonians which can be generated using k -local G -invariant Hamiltonians is equal to the set of charge vectors of G -invariant Hamiltonians which act non-trivially only on the first k sites. This immediately implies that the dimension of this linear space does not grow with n and, in fact, is equal to $N_{\text{irrep}}(k)$, where $N_{\text{irrep}}(l)$ is the number of inequivalent irreps of G appearing in the representation $\{u(g)^{\otimes l} : g \in G\}$ (See

Supplementary Material). Therefore, using lemma 1, we find

Theorem 1. *For n identical sites, the difference between the dimensions of the Lie algebra of anti-Hermitian G -invariant operators and its sub-algebra generated by k -local elements of this algebra, is lower bounded by*

$$\dim(\mathfrak{a}) - \dim(\mathfrak{h}_k) \geq N_{\text{irreps}}(n) - N_{\text{irreps}}(k). \quad (12)$$

In the case of Lie groups such as $\text{SO}(3)$ and $\text{U}(1)$, $N_{\text{irreps}}(l)$ increases linearly with l . Therefore, unless $k = n$, which means the interactions act non-trivially on all sites in the system, it is impossible to implement an arbitrary symmetric unitary using k -local symmetric unitaries. In particular, for any fixed k , the difference between the dimensions of \mathfrak{a} and \mathfrak{h}_k grows, at least, linearly in n .

In the Supplementary Material we explain how this argument can be generalized to the case of non-identical sites.

Diagonal unitaries on qubits—Consider a system formed from n qubits. Let $X_l, Y_l, Z_l \in \mathcal{L}((\mathbb{C}^2)^{\otimes n})$ be Pauli x, y , and z operators on qubit $l \in \{1, \dots, n\}$, tensor product with the identity operators on the rest of qubits. The set of rotations around z -axis, i.e. unitaries $\{e^{i\theta \sum_{l=1}^n Z_l} : \theta \in [0, 2\pi)\}$ is a representation of the group $\text{U}(1)$. In the following, we say a unitary V is $\text{U}(1)$ -invariant if it is invariant under rotations around z , or equivalently, commutes with $\sum_{l=1}^n Z_l$. This family of unitaries is relevant, for instance, in the context of quantum thermodynamics: if each qubit has Hamiltonian $\omega Z/2$, then energy-conserving unitaries on this system are those which satisfy this $\text{U}(1)$ symmetry.

For any bit string $\mathbf{b} = b_1 \dots b_n \in \{0, 1\}^n$, let $|\mathbf{b}\rangle = \bigotimes_{l=1}^n |b_l\rangle$, where $|0\rangle$ and $|1\rangle$ are eigenvectors of Z with eigenvalues $+1$ and -1 , respectively. Clearly, all diagonal unitaries in this basis are $\text{U}(1)$ -invariant. We are interested to determine which diagonal unitaries can be generated using k -local $\text{U}(1)$ -invariant unitaries. Interestingly, it turns out that using the notion of charge vectors and the constraint in lemma 1, we can fully characterize this set.

For any bit string $\mathbf{b} \in \{0, 1\}^n$, let $w(\mathbf{b}) = \sum_{l=1}^n b_l$ be its Hamming weight and $\mathbf{Z}^{\mathbf{b}} \equiv \prod_{l=1}^n Z_l^{b_l}$. We prove that

Theorem 2. *Consider an arbitrary diagonal Hamiltonian*

$$H = \sum_{\mathbf{z} \in \{0,1\}^n} h(\mathbf{z}) |\mathbf{z}\rangle \langle \mathbf{z}| = \sum_{\mathbf{b} \in \{0,1\}^n} \tilde{h}(\mathbf{b}) \mathbf{Z}^{\mathbf{b}}, \quad (13)$$

where $\tilde{h}(\mathbf{b}) = 2^{-n} \sum_{\mathbf{z} \in \{0,1\}^n} (-1)^{\mathbf{b} \cdot \mathbf{z}} h(\mathbf{z})$ is the Fourier transform of $h(\mathbf{z})$. The family of diagonal unitaries $\{e^{-itH} : t \in \mathbb{R}\}$ can be generated using k -local $\text{U}(1)$ -invariant Hamiltonians if, and only if

$$\sum_{\mathbf{b} \in \{0,1\}^n : w(\mathbf{b})=v} \tilde{h}(\mathbf{b}) = 0, \quad \text{for } \forall v : k < v \leq n, \quad (14)$$

where the summation is over all bit strings with Hamming weight v .

As an example, this theorem implies that, under the restriction to $\text{U}(1)$ -invariant interactions, to be able to implement the family of unitaries $\{e^{-itZ^{\otimes m}} : t \in \mathbb{R}\}$, one needs to have access to interactions which act non-trivially on $k \geq m$ qubits (Recall that, without the constraint of symmetry, these unitaries can be implemented using 2-local interactions).

It is interesting to compare the condition in Eq.(14), with the stronger condition $\tilde{h}(\mathbf{b}) = 0$ for all \mathbf{b} with $w(\mathbf{b}) > k$. The latter condition is relevant if rather than $\text{U}(1)$ -invariance, we impose the stronger constraint that the generating set should also be diagonal (as well as k -local). Therefore, in the scenario described in the theorem, due to the presence of the non-diagonal $\text{U}(1)$ -invariant k -local Hamiltonians, this stronger constraint can be relaxed to the constraint in Eq.(14).

As we show in the Supplementary Material, Eq.(14) is simply the statement that the charge vector of H should be in the subspace of charge vectors of k -local $\text{U}(1)$ -invariant Hamiltonians, which by lemma 1, is a necessary condition. In the following, we explain the proof of the sufficiency of this condition.

For any pair of distinct qubits $r, s \in \{1, \dots, n\}$, consider the 2-local $\text{U}(1)$ -invariant Hamiltonians

$$R_{rs} = \frac{X_r X_s + Y_r Y_s}{2}, \quad T_{rs} = \frac{i}{2} [Z_r, R_{rs}]. \quad (15)$$

For any set of distinct qubits $r_1, r_2, \dots, r_{v+1} \in \{1, \dots, n\}$, with $v < n$, we have

$$\begin{aligned} ic_v \times (Z_{r_1} - Z_{r_{v+1}}) Z_{r_2} \dots Z_{r_v} = \\ [\dots [iR_{r_1 r_2}, iR_{r_2 r_3}], iR_{r_3 r_4} \dots, iR_{r_v, r_{v+1}}], iR_{r_{v+1}, r_1} : v \text{ even}, \\ [\dots [iR_{r_1 r_2}, iR_{r_2 r_3}], iR_{r_3 r_4} \dots, iR_{r_v, r_{v+1}}], iT_{r_{v+1}, r_1} : v \text{ odd}, \end{aligned} \quad (16)$$

where $c_v = \pm 1$, depending on v . In the Supplementary Material we show that the real span of operators in Eq.(16) for different values of $v < n$, is equal to the subspace

$$\left\{ i \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}} : a_{\mathbf{b}} \in \mathbb{R}, \sum_{\mathbf{b} : w(\mathbf{b})=v} a_{\mathbf{b}} = 0 \text{ for all } v \leq n \right\}. \quad (17)$$

Since R_{rs} and $T_{rs} = \frac{i}{2} [Z_r, R_{rs}]$ are 2-local and $\text{U}(1)$ -invariant, this subspace is included in \mathfrak{h}_k for $k \geq 2$. By definition, \mathfrak{h}_k also includes operators $\{i\mathbf{Z}^{\mathbf{b}} : w(\mathbf{b}) \leq k\}$. The linear combinations of these operators with the set of operators in Eq.(17), yield all diagonal anti-Hermitian operators $i \sum_{\mathbf{b} \in \{0,1\}^n} \tilde{h}(\mathbf{b}) \mathbf{Z}^{\mathbf{b}}$, which satisfy condition in Eq.(14). This proves the sufficiency of this condition and completes the proof of theorem 2.

Universality with a pair of ancillary qubits—Next, we show that the above constraints on the realizable $\text{U}(1)$ -invariant unitaries can be circumvented if one is allowed to interact with a pair of ancillary qubits. In particular, suppose one is given the ancillary qubits a and \bar{a} , initially prepared in states $|0\rangle$ and $|1\rangle$, respectively. At the end of the process these qubits should be returned in their initial states.

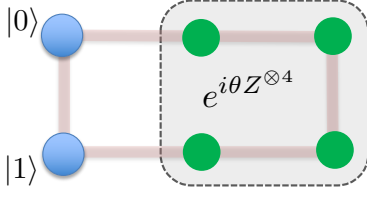


FIG. 1: Without ancillary qubits, the family of unitaries $\{e^{i\theta Z^{\otimes m}} : \theta \in [0, 2\pi)\}$, for $m > 2$, cannot be implemented using 2-local $U(1)$ -invariant interactions (i.e. those which conserve $\sum_r Z_r$). On the other hand, if one is allowed to use a pair of ancillary qubits, then any $U(1)$ -invariant unitary can be implemented using local Z on one ancillary qubit together with interactions $X_r X_s + Y_r Y_s$, which are $U(1)$ -invariant and 2-local. The ancillary qubits are initially prepared in states $|0\rangle$ and $|1\rangle$, and at the end of process they return to the same states. The above figure demonstrates implementation of the family $\{e^{i\theta Z^{\otimes 4}}\}$ using the nearest neighbor interactions $X_r X_s + Y_r Y_s$, and local Z on one of the ancillary qubits.

To see how such ancillary qubits can be useful, note that according to Eq.(15) and Eq.(16), using 2-local $U(1)$ -invariant Hamiltonians $\{R_{rs} : r, s \in \{1, \dots, n\} \cup \{a, \bar{a}\}\}$ together with local Z_a (or $Z_{\bar{a}}$) one can implement the family of unitaries generated by the Hamiltonian $\mathbf{Z}^{\mathbf{b}} \otimes (Z_a - Z_{\bar{a}})$, for any bit string $\mathbf{b} \in \{0, 1\}^n$. Under this Hamiltonian, any arbitrary initial $|\psi\rangle$ of n qubits, evolves to

$$e^{i\theta \mathbf{Z}^{\mathbf{b}} \otimes (Z_a - Z_{\bar{a}})} \left(|\psi\rangle |0\rangle_a |1\rangle_{\bar{a}} \right) = (e^{i2\theta \mathbf{Z}^{\mathbf{b}}} |\psi\rangle) |0\rangle_a |1\rangle_{\bar{a}}. \quad (18)$$

Note that at the end of the process, the ancillary qubits go back to their initial states. Therefore, combining these unitaries, one can generate all Hamiltonians $\{\mathbf{Z}^{\mathbf{b}} : \mathbf{b} \in \{0, 1\}^n\}$, and hence all diagonal unitaries on n qubits. Then, as we show in the Supplementary Material, combining these Hamiltonians with Hamiltonians $\{R_{rs} : r, s \in \{1, \dots, n\}\}$, one can generate all $U(1)$ -invariant Hamiltonians. To summarize

Theorem 3. *Using a pair of ancillary qubits prepared in states $|0\rangle$ and $|1\rangle$, any unitary which is invariant under rotations around z can be implemented using 2-local Hamiltonians $\{X_r X_s + Y_r Y_s\}$, together with the single-qubit Z Hamiltonian on one of the ancillary qubits.*

Discussion— The long-term dynamics of quantum many-body systems with generic local Hamiltonians are intractable. In the absence of symmetries, there are no constraints on the possible unitary evolution of the system. In many cases, the conservation laws imposed by the symmetries of Hamiltonian provide the only tractable constraints on the long-term behavior: For any time t , the unitary evolution $U(t)$ of system commutes with the generators of the symmetries. Our first result implies that locality and symmetry together yield stronger constraints on the long-term dynamics. Such constraints could be useful, for instance, for understanding scrambling in many-body systems with conserved charges [10]. It is worth noting that these constraints hold, even if the interactions are long-

range, provided that each term in the Hamiltonian acts non-trivially on a finite number of sites.

Our second result, implies that using ancillary qubits, one can circumvent these constraints in the case of the group $U(1)$. This result justifies the framework of the resource theory of quantum thermodynamics, which allows arbitrary energy-conserving unitaries on a composite system. Our technique for implementing arbitrary phase-insensitive unitaries using the phase-insensitive interaction $XX + YY$ and ancillary qubits, can have further applications in the context of quantum computing.

Acknowledgements: I am grateful to Austin Hulse, David Jennings, and Hadi Salmasian for reading the manuscript carefully and providing many useful comments.

-
- [1] E. H. Lieb and D. W. Robinson, in *Statistical mechanics* (Springer, 1972), pp. 425–431.
 - [2] S. Lloyd, Physical Review Letters **75**, 346 (1995).
 - [3] D. P. DiVincenzo, Physical Review A **51**, 1015 (1995).
 - [4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Physical review A **52**, 3457 (1995).
 - [5] D. E. Deutsch, A. Barenco, and A. Ekert, Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences **449**, 669 (1995).
 - [6] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth, Int. J. Theor. Phys. **39**, 2717 (2000).
 - [7] M. Horodecki and J. Oppenheim, Nature communications **4** (2013).
 - [8] F. G. Brandao, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Physical review letters **111**, 250404 (2013).
 - [9] P. Zanardi and S. Lloyd, Physical Review A **69**, 022313 (2004).
 - [10] V. Khemani, A. Vishwanath, and D. A. Huse, Physical Review X **8**, 031057 (2018).

Supplementary Material

Charge vectors and their Fourier Transform

Consider the decomposition of the representation $\{U(g) : g \in G\}$ to the irreducible representations (irreps) of G . If G is a finite or compact Lie group, then every representation is completely reducible, i.e., there exists a unitary W such that

$$WU(g)W^\dagger = \bigoplus_{\mu \in \text{irrep}(U)} u^{(\mu)}(g) \otimes I_{m_\mu}, \quad \forall g \in G \quad (19)$$

and the Hilbert space \mathcal{H} decomposes as

$$\mathcal{H} \cong \bigoplus_{\mu \in \text{irrep}(U)} \mathbb{C}^{d_\mu} \otimes \mathbb{C}^{m_\mu}, \quad (20)$$

where $\text{irrep}(U)$ is the set of inequivalent irreps of G appearing in the representation U , $\{u^{(\mu)}(g) : g \in G\}$ is the irreducible representation which acts irreducibly on \mathbb{C}^{d_μ} , d_μ is the dimension of irrep μ and m_μ is its multiplicity, and I_{m_μ} is the identity operator on \mathbb{C}^{m_μ} . Using Schur's lemmas, one can show that in this basis any G -invariant operator A can be written as

$$WAW^\dagger = \bigoplus_{\mu \in \text{irrep}(U)} I_{d_\mu} \otimes A^{(\mu)}, \quad (21)$$

where I_{d_μ} is the identity operator on \mathbb{C}^{d_μ} , and $A^{(\mu)}$ is an operator acting on \mathbb{C}^{m_μ} . Using this decomposition, the charge vector of operator A is

$$|\chi_A\rangle = \sum_{\mu \in \text{irrep}(U)} \text{Tr}(\Pi_\mu A) |\mu\rangle = \sum_{\mu \in \text{irrep}(U)} d_\mu \times \text{Tr}(A^{(\mu)}) |\mu\rangle. \quad (22)$$

Next, consider the function $\chi_A : G \rightarrow \mathbb{C}$ defined by equation

$$\chi_A(g) = \text{Tr}(AU(g)) = \sum_{\mu \in \text{irrep}(U)} \text{Tr}(u^{(\mu)}(g)) \times \text{Tr}(A^{(\mu)}) = \sum_{\mu \in \text{irrep}(U)} \text{Tr}(A^{(\mu)}) \chi^{(\mu)}(g). \quad (23)$$

where $\chi^{(\mu)}$ is the character of irrep μ . The fact that characters of inequivalent irreps are linearly independent, immediately implies that for G -invariant operators there is a linear invertible map between function χ_A and the charge vector $|\chi_A\rangle$. In particular, using the orthogonality relation, $\int_G dg \chi^{(\nu)}(g) \overline{\chi^{(\mu)}(g)} = \delta_{\mu,\nu}$, we find

$$|\chi_A\rangle = \int_G dg \chi_A(g) \sum_{\mu \in \text{irrep}(U)} d_\mu \overline{\chi^{(\mu)}(g)} |\mu\rangle, \quad (24)$$

where dg is the uniform (Haar) measure, and $\overline{\chi^{(\mu)}(g)}$ is the complex conjugate of $\chi^{(\mu)}(g)$. The inverse transformation is

$$\chi_A(g) = \sum_{\mu \in \text{irrep}(U)} \langle \mu | \chi_A \rangle \frac{\chi^{(\mu)}(g)}{d_\mu}. \quad (25)$$

Note that for a Hermitian operator, all coefficients $\{\text{Tr}(A^{(\mu)})\}$ are real numbers. Furthermore, for any choice of real number $\{a_\mu \in \mathbb{R}\}$, the Hermitian G -invariant operator $A = \sum a_\mu \Pi_\mu / \text{Tr}(\Pi_\mu)$, has the charge vector $|\chi_A\rangle = \sum_\mu a_\mu |\mu\rangle$. Therefore,

$$\left\{ \chi_A : A = A^\dagger, [A, U(g)] = 0, \forall g \in G \right\} = \left\{ \sum_{\mu \in \text{irrep}(U)} a_\mu \chi^{(\mu)} : a_\mu \in \mathbb{R} \right\}, \quad (26)$$

where the summation is over the set of all irreps of G which appear in the representation $\{U(g) : g \in G\}$.

Lie algebra generated by local symmetric Hamiltonians (Proof of theorem 1)

First, we consider the special case of identical systems. Consider a system formed from n local *sites*, each with a finite-dimensional Hilbert space

$$\mathcal{H}_i \cong \mathbb{C}^d : i = 1, \dots, n. \quad (27)$$

Let $\mathcal{H} \cong \bigotimes_{i=1}^n \mathcal{H}_i$ be the joint Hilbert space. Assume all sites have the same representation of symmetry, namely $\{u(g) \in \mathcal{L}(\mathbb{C}^d) : g \in G\}$, and therefore $\{U(g) = u(g)^{\otimes n} : g \in G\}$ is the representation of symmetry on the total system.

Let

$$\mathfrak{a} \equiv \{A \in \mathcal{L}((\mathbb{C}^d)^{\otimes n}) : A + A^\dagger = 0, [A, U(g)] = 0 : \forall g \in G\}, \quad (28)$$

be the set of all G -invariant anti-Hermitian operators, which form a Lie algebra.

Consider the sub-algebra of \mathfrak{a} generated by G -invariant anti-Hermitian k -local operators, denoted by

$$\mathfrak{h}_k \equiv \text{alg}\{A \in \mathcal{L}((\mathbb{C}^d)^{\otimes n}) : A \in \mathfrak{a}, A \text{ is } k\text{-local}\} \quad (29)$$

$$= \text{alg}\{A \in \mathcal{L}((\mathbb{C}^d)^{\otimes n}) : A + A^\dagger = 0, [A, U(g)] = 0 \forall g \in G, A \text{ is } k\text{-local}\}. \quad (30)$$

Define \mathcal{S}_k to be the charge vector for all Hamiltonians C with the property that $iC \in \mathfrak{h}_k$, i.e.

$$\mathcal{S}_k \equiv \{|\chi_C\rangle : iC \in \mathfrak{h}_k\} = \text{Span}_{\mathbb{R}}\{|\chi_C\rangle : iC \in \mathfrak{a}, C \text{ is } k\text{-local}\}, \quad (31a)$$

where in the right-hand side we have the linear combinations of charge vectors of k -local G -invariant Hamiltonians, and the equality follows from Eq.(6).

To determine the dimension of the subspace \mathcal{S}_k , it is useful to consider the Fourier transform of the charge vectors. For any operator C , let $\chi_C : G \rightarrow \mathbb{C}$ be the function defined by equation $\chi_C(g) = \text{Tr}(CU(g))$. Consider the subspace

$$\tilde{\mathcal{S}}_k \equiv \{\chi_C : iC \in \mathfrak{h}_k\}. \quad (32)$$

As we have seen before χ_C is related to $|\chi_C\rangle$ via Fourier transform, and therefore subspaces \mathcal{S}_k and $\tilde{\mathcal{S}}_k$ have equal dimension, i.e.

$$\dim(\mathcal{S}_k) = \dim(\tilde{\mathcal{S}}_k). \quad (33)$$

Next, note that up to a permutation any k -local operator C has a decomposition as

$$C = \tilde{C} \otimes I_d^{\otimes(n-k)}, \quad (34)$$

where $\tilde{C} \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$ acts on k sites, and I_d is the identity operator on \mathbb{C}^d . Then,

$$\chi_C(g) = \text{Tr}(CU(g)) = [\text{Tr}(u(g))]^{n-k} \times \text{Tr}(\tilde{C}u(g)^{\otimes k}). \quad (35)$$

The first factor $[\text{Tr}(u(g))]^{n-k}$ is independent of C . Therefore, the dimension of $\tilde{\mathcal{S}}_k$ is equal to the dimension of the subspace spanned by functions $\text{Tr}(\tilde{C}u(g)^{\otimes k})$ for G -invariant Hermitian operators \tilde{C} , which act on k systems, i.e.

$$\text{Span}_{\mathbb{R}}\left\{\chi_{\tilde{C}} : \tilde{C} \in \mathcal{L}((\mathbb{C}^d)^{\otimes k}), \tilde{C} = \tilde{C}^\dagger, \forall g : [\tilde{C}, u(g)^{\otimes k}] = 0\right\} = \left\{\sum_{\mu \in \text{irrep}(\tilde{U})} a_\mu \chi^{(\mu)} : a_\mu \in \mathbb{R}\right\}, \quad (36)$$

where $\text{irrep}(\tilde{U})$ is the set of irreps of G that appear in representation $\{\tilde{U}(g) = u^{\otimes k}(g) : g \in G\}$, and the equality follows from Eq.(26). Clearly, the dimension of this subspace is equal to $N_{\text{irrep}}(k)$, the number of distinct irreps of G that appearing in representation $\{\tilde{U}(g) = u^{\otimes k}(g) : g \in G\}$. Together with lemma 1, this proves theorem 1.

The general case of non-identical subsystems

Next, consider the more general case where the subsystems are not identical. Assume there are a finite number of *types* of sites, where each type carries a particular representation of group G . More precisely, suppose each site has one of T possible rep-

representations $\{v^{(1)}, \dots, v^{(T)}\}$, where for each $t \in \{1, \dots, T\}$, $\{v^{(t)}(g) : g \in G\}$ is a finite-dimensional unitary representation of group G .

Then, our previous argument can be easily generalized to show that \mathcal{S}_k , the set of charge vectors for k -local G -invariant Hamiltonians, is a finite-dimensional subspace, whose dimension is bounded by a number which is independent of n , the total number of sites. In fact, the dimension of \mathcal{S}_k is upper bounded by the total number of inequivalent irreps of G , which appear in all tensor product representations

$$\left\{ \bigotimes_{i=1}^k v^{(t_i)} : t_1, \dots, t_k \in \{1, \dots, T\} \right\}. \quad (37)$$

This follows from the fact that any k -local operator can act non-trivially on at most k sites, and the representation of group G on those k sites is equivalent to one of the representations listed above. Therefore, the charge vector of any such operator can only contain components in irreps $\{\mu\}$ which appear in one of these representations. Clearly, the total number of inequivalent irreps appearing in the above representations, is independent of n , the total number of sites.

On the other hand, let $\bigotimes_{i=1}^n v^{(t_i)}$ be the representation of group G on the total system, where $v^{(t_i)}$ is the representation of group G on site i and $t_i \in \{1, \dots, T\}$. For a compact connected Lie group G , such as $U(1)$ and $SO(3)$, as the number of sites which carry a non-trivial representation of G increases, the number of distinct irreps which appear in this representation also increases unboundedly, and for sufficiently large n , this will be larger than the dimension of \mathcal{S}_k . Therefore, by lemma 1 we conclude that for sufficiently large n , there are G -invariant unitaries which cannot be implemented using k -local G -invariant Hamiltonians.

Proof of theorem 2

Consider the symmetry transformation

$$U(e^{i\theta}) = (e^{i\theta Z})^{\otimes n} = e^{i\theta \sum_r Z_r} = \sum_{q=-n}^n e^{iq\theta} \Pi_q, \quad (38)$$

where Π_q is the projector to the subspace corresponding to eigenvalue q of operator $\sum_r Z_r$. Then, the charge vector associated to any operator A is

$$|\chi_A\rangle = \sum_{q=-n}^n \text{Tr}(\Pi_q A) |q\rangle, \quad (39)$$

and its Fourier transform is the function

$$\chi_A(e^{i\theta}) = \text{Tr}(AU(e^{i\theta})) = \text{Tr}(A(e^{i\theta Z})^{\otimes n}) = \sum_{q=-n}^n e^{iq\theta} \text{Tr}(\Pi_q A). \quad (40)$$

Let \mathfrak{h}_k be the Lie algebra generated by k -local $U(1)$ -invariant Hamiltonians, and $\tilde{\mathcal{S}}_k$ be the subspace

$$\tilde{\mathcal{S}}_k \equiv \{\chi_A : iA \in \mathfrak{h}_k\}. \quad (41)$$

First, using Eq.(6), we find

$$\tilde{\mathcal{S}}_k \equiv \{\chi_A : iA \in \mathfrak{h}_k\} = \text{Span}_{\mathbb{R}} \left\{ \chi_A : A = A^\dagger, [A, \sum_r Z_r] = 0, A \text{ is } k\text{-local} \right\}, \quad (42)$$

i.e. $\tilde{\mathcal{S}}_k$ is the span of functions χ_A for all k -local Hermitian, $U(1)$ -invariant operators. We claim that this subspace is equal to

$$\tilde{\mathcal{S}}_k = \text{Span}_{\mathbb{R}} \{\xi_v : 0 \leq v \leq k\}, \quad \text{where } \xi_v(e^{i\theta}) = (\cos \theta)^{n-v} (i \sin \theta)^v. \quad (43)$$

To prove Eq.(43) first note that

$$\chi_A(e^{i\theta}) = \text{Tr}(\mathcal{D}(A)U(e^{i\theta})), \quad (44)$$

where

$$\mathcal{D}(A) \equiv \sum_{\mathbf{b} \in \{0,1\}^n} |\mathbf{b}\rangle\langle\mathbf{b}| A |\mathbf{b}\rangle\langle\mathbf{b}| = \sum_{b_1, \dots, b_n \in \{0,1\}} (|b_1\rangle\langle b_1| \otimes \dots \otimes |b_n\rangle\langle b_n|) A (|b_1\rangle\langle b_1| \otimes \dots \otimes |b_n\rangle\langle b_n|), \quad (45)$$

is the diagonal part of A . This definition immediately implies that if A is k -local, then $\mathcal{D}(A)$ is also k -local, i.e., acts non-trivially on, at most, k sites. Furthermore, any diagonal operator can be written as a linear combination of operators $\{\mathbf{Z}^{\mathbf{b}} : \mathbf{b} \in \{0,1\}^n\}$. We conclude that

$$\tilde{\mathcal{S}}_k = \text{Span}_{\mathbb{R}} \left\{ \chi_A : A = \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}, a_{\mathbf{b}} \in \mathbb{R}, A \text{ is } k\text{-local} \right\}. \quad (46)$$

Next, using the fact that operators $\{\mathbf{Z}^{\mathbf{b}} : \mathbf{b} \in \{0,1\}^n\}$ are linearly independent, and pairwise orthogonal relative to the Hilbert-Schmidt inner product, we find that any k -local operator $A = \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}$ can be written as

$$A = \sum_{\mathbf{b}: w(\mathbf{b}) \leq k} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}. \quad (47)$$

This immediately implies

$$\tilde{\mathcal{S}}_k = \text{Span}_{\mathbb{R}} \left\{ \chi_{\mathbf{Z}^{\mathbf{b}}} : w(\mathbf{b}) \leq k \right\}, \quad (48)$$

where

$$\chi_{\mathbf{Z}^{\mathbf{b}}}(e^{i\theta}) \equiv \text{Tr}(\mathbf{Z}^{\mathbf{b}}(e^{i\theta Z})^{\otimes n}) = 2^n (\cos \theta)^{n-w(\mathbf{b})} (i \sin \theta)^{w(\mathbf{b})}, \quad (49)$$

$w(\mathbf{b}) = \sum_{l=1}^n b_l$ is the Hamming weight of the bit string $\mathbf{b} = b_1 \dots b_n$, and the summation is over all bit strings with Hamming weight $w(\mathbf{b}) \leq k$. Here, the equality follows from the fact that $\text{Tr}(e^{i\theta Z}) = 2 \cos \theta$ and $\text{Tr}(Z e^{i\theta Z}) = 2i \sin \theta$. This proves our claim in Eq.(43).

Similarly, using Eq.(49), for any operator $A = \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}$, we have

$$\chi_A(e^{i\theta}) = \text{Tr}(A(e^{i\theta Z})^{\otimes n}) = \sum_{\mathbf{b}} a_{\mathbf{b}} \text{Tr}(\mathbf{Z}^{\mathbf{b}}(e^{i\theta Z})^{\otimes n}) = 2^n \sum_{v=0}^n \xi_v(e^{i\theta}) \times \sum_{\mathbf{b} \in \{0,1\}^n: w(\mathbf{b})=v} a_{\mathbf{b}}. \quad (50a)$$

By the second part of lemma 1, an operator $iA = i \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}$ with real coefficients $\{a_{\mathbf{b}}\}$ is in \mathfrak{h}_2 only if χ_A is in the subspace $\tilde{\mathcal{S}}_k$. Since functions $\{\xi_v : v = 0, \dots, n\}$ are linearly independent, and subspace $\tilde{\mathcal{S}}_k$ is the linear span of $\{\xi_v : 0 \leq v \leq k\}$, χ_A is in the subspace $\tilde{\mathcal{S}}_k$, only if the coefficients of ξ_v for $v > k$ is zero, i.e.

$$\sum_{\mathbf{b}: w(\mathbf{b})=v} a_{\mathbf{b}} = 0 : \quad \forall v > k, \quad (51)$$

where the summation is over all bit strings with Hamming weight v , and the condition should hold for all $v > k$. This proves the necessity of condition in Eq.(14) in theorem 2. Next, we prove the sufficiency of this condition.

Sufficiency of condition in Eq.(14) of theorem 2

As we discuss in the main part of the paper, for any subset $v+1 \leq n$ distinct qubits $l_1, l_2, \dots, l_{v+1} \in \{1, \dots, n\}$, we have

$$\begin{aligned} ic_v \times (Z_{l_1} \dots Z_{l_v} - Z_{l_2} \dots Z_{l_{v+1}}) = & \quad (52) \\ \left[[\dots [iR_{l_1 l_2}, iR_{l_2 l_3}], \dots, iR_{l_v, l_{v+1}}], iR_{l_{v+1}, l_1} \right] & : v \text{ even}, \\ \left[[\dots [iR_{l_1 l_2}, iR_{l_2 l_3}], \dots, iR_{l_v, l_{v+1}}], iT_{l_{v+1}, l_1} \right] & : v \text{ odd}, \end{aligned}$$

where $c_v = \pm 1$, depending on v . Therefore, for any pair of bit strings $\mathbf{b}_1, \mathbf{b}_2 \in \{0,1\}^n$, the operator $i(\mathbf{Z}^{\mathbf{b}_1} - \mathbf{Z}^{\mathbf{b}_2})$ can be obtained from these commutators, provided that \mathbf{b}_1 and \mathbf{b}_2 have equal Hamming weights, i.e. $w(\mathbf{b}_1) = w(\mathbf{b}_2) = v$, and their Hamming distance $d(\mathbf{b}_1, \mathbf{b}_2) = 2$ (Recall that the Hamming distance is the number of bits that should be flipped to transform

one bit string to another).

Next, we prove that the linear span of operators in Eq.(52) for a fixed $v < n$ is

$$\text{Span}_{\mathbb{R}} \left\{ i(\mathbf{Z}^{\mathbf{b}_1} - \mathbf{Z}^{\mathbf{b}_2}) : w(\mathbf{b}_1) = w(\mathbf{b}_2) = v, d(\mathbf{b}_1, \mathbf{b}_2) = 2 \right\} = \text{Span}_{\mathbb{R}} \left\{ i(\mathbf{Z}^{\mathbf{b}_1} - \mathbf{Z}^{\mathbf{b}_2}) : w(\mathbf{b}_1) = w(\mathbf{b}_2) = v \right\}, \quad (53)$$

i.e. the restriction $d(\mathbf{b}_1, \mathbf{b}_2) = 2$ can be removed. To prove this we use the fact that any pair of bit strings $\mathbf{c}_1, \mathbf{c}_2 \in \{0, 1\}^n$ with equal Hamming weights $w(\mathbf{c}_1) = w(\mathbf{c}_2) = v$ are related to each other by a permutation of bits. Furthermore, any permutation can be realized by a sequence *transpositions*, i.e., 2-bit permutations, which only exchange the value of two-bits. It follows that for any pair of bit strings $\mathbf{c}_1, \mathbf{c}_2 \in \{0, 1\}^n$ with equal Hamming weights $w(\mathbf{c}_1) = w(\mathbf{c}_2) = v$, there is a path in the space of bit strings with Hamming weight v from \mathbf{c}_1 to \mathbf{c}_2 , i.e.

$$\mathbf{f}_1, \dots, \mathbf{f}_L \in \{0, 1\}^n : w(\mathbf{f}_k) = v, \quad \mathbf{f}_1 = \mathbf{c}_1, \mathbf{f}_L = \mathbf{c}_2, \quad (54)$$

where each consecutive pair of bit strings have Hamming distance 2, i.e.

$$d(\mathbf{f}_r, \mathbf{f}_{r+1}) = 2 : 1 \leq r \leq L - 1. \quad (55)$$

Therefore, $i(\mathbf{Z}^{\mathbf{c}_1} - \mathbf{Z}^{\mathbf{c}_2})$ can be obtained using the linear combination

$$i(\mathbf{Z}^{\mathbf{c}_1} - \mathbf{Z}^{\mathbf{c}_2}) = i(\mathbf{Z}^{\mathbf{f}_1} - \mathbf{Z}^{\mathbf{f}_L}) = i(\mathbf{Z}^{\mathbf{f}_1} - \mathbf{Z}^{\mathbf{f}_2}) + i(\mathbf{Z}^{\mathbf{f}_2} - \mathbf{Z}^{\mathbf{f}_3}) + \dots + i(\mathbf{Z}^{\mathbf{f}_{L-1}} - \mathbf{Z}^{\mathbf{f}_L}). \quad (56)$$

This proves Eq.(53). Next, it can be easily seen that

$$\text{Span}_{\mathbb{R}} \left\{ i(\mathbf{Z}^{\mathbf{b}_1} - \mathbf{Z}^{\mathbf{b}_2}) : w(\mathbf{b}_1) = w(\mathbf{b}_2) = v \right\} = \left\{ i \sum_{\mathbf{b}:w(\mathbf{b})=v} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}} : a_{\mathbf{b}} \in \mathbb{R}, \sum_{\mathbf{b}:w(\mathbf{b})=v} a_{\mathbf{b}} = 0 \right\}, \quad (57)$$

where the right-hand side is the subspace of all linear combinations $i \sum_{\mathbf{b}:w(\mathbf{b})=v} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}}$ for bit strings with Hamming weight v , which satisfy the linear constraint $\sum_{\mathbf{b}:w(\mathbf{b})=v} a_{\mathbf{b}} = 0$.

Next, considering the linear combinations of subspaces with different Hamming weights $v < n$, we obtain the subspace

$$\left\{ i \sum_{\mathbf{b}} a_{\mathbf{b}} \mathbf{Z}^{\mathbf{b}} : a_{\mathbf{b}} \in \mathbb{R}, \forall v < n : \sum_{\mathbf{b}:w(\mathbf{b})=v} a_{\mathbf{b}} = 0 \right\}. \quad (58)$$

Recall that this subspace is obtained from linear combination of commutators in Eq.(52), which only involve 2-local U(1)-invariant operators $\{iR_{lm}, iT_{lm}\}$. Therefore, this subspace is a subspace of \mathfrak{h}_k for $k \geq 2$, where \mathfrak{h}_k is the Lie algebra generated by k -local U(1)-invariant anti-Hermitian operators.

By definition, in addition to this subspace, \mathfrak{h}_k also includes arbitrary linear combinations of operators $\{i\mathbf{Z}^{\mathbf{b}} : w(\mathbf{b}) \leq k\}$. Linear combinations of these operators with the set of operators in Eq.(58), yield all diagonal Hamiltonians which satisfy condition in Eq.(51). This proves the sufficiency of this condition and completes the proof of theorem 2.

Proof of theorem 3

Let \mathfrak{a} be the set of $U(1)$ -invariant anti-Hermitian operators,

$$\mathfrak{a} \equiv \left\{ A \in \mathcal{L}((\mathbb{C}^2)^{\otimes n}) : A + A^\dagger = 0, \left[A, \sum_{r=1}^n Z_r \right] = 0 \right\}. \quad (59)$$

Any arbitrary operator $A \in \mathcal{L}((\mathbb{C}^2)^{\otimes n})$ can be written as

$$A = \sum_{\mathbf{b}, \mathbf{b}' \in \{0,1\}^n} a_{\mathbf{b}, \mathbf{b}'} |\mathbf{b}\rangle \langle \mathbf{b}'|. \quad (60)$$

Using the fact that

$$\left(\sum_{r=1}^n Z_r \right) |\mathbf{b}\rangle = [n - 2w(\mathbf{b})] |\mathbf{b}\rangle, \quad (61)$$

we find that

$$\left[A, \sum_{r=1}^n Z_r \right] = 2 \sum_{\mathbf{b}, \mathbf{b}'} a_{\mathbf{b}, \mathbf{b}'} [w(\mathbf{b}') - w(\mathbf{b})] |\mathbf{b}\rangle \langle \mathbf{b}'|. \quad (62)$$

This implies that if $[A, \sum_{r=1}^n Z_r] = 0$, then

$$a_{\mathbf{b}, \mathbf{b}'} = 0 \quad \text{for } w(\mathbf{b}) \neq w(\mathbf{b}'). \quad (63)$$

In other words, the off-diagonal terms for bit strings with different Hamming weights vanish.

Therefore, the space of $U(1)$ -invariant operators is spanned by

$$\{ |\mathbf{b}\rangle \langle \mathbf{b}'| : w(\mathbf{b}) = w(\mathbf{b}'); \mathbf{b}, \mathbf{b}' \in \{0,1\}^n \}. \quad (64)$$

This implies that \mathfrak{a} , the space of anti-Hermitian $U(1)$ -invariant operators is spanned by

$$\mathfrak{a} = \text{Span}_{\mathbb{R}} \left\{ i(|\mathbf{b}\rangle \langle \mathbf{b}'| + |\mathbf{b}'\rangle \langle \mathbf{b}|), |\mathbf{b}\rangle \langle \mathbf{b}'| - |\mathbf{b}'\rangle \langle \mathbf{b}| : w(\mathbf{b}) = w(\mathbf{b}'); \mathbf{b}, \mathbf{b}' \in \{0,1\}^n \right\}. \quad (65)$$

Using the fact that for any pair of bit strings $\mathbf{b}, \mathbf{b}' \in \{0,1\}^n$,

$$\left[i|\mathbf{b}\rangle \langle \mathbf{b}|, (|\mathbf{b}\rangle \langle \mathbf{b}'| - |\mathbf{b}'\rangle \langle \mathbf{b}|) \right] = i(|\mathbf{b}\rangle \langle \mathbf{b}'| + |\mathbf{b}'\rangle \langle \mathbf{b}|), \quad (66)$$

we find that the Lie algebra \mathfrak{a} is generated by

$$\mathfrak{a} = \text{alg} \left\{ i|\mathbf{b}\rangle \langle \mathbf{b}|, |\mathbf{b}\rangle \langle \mathbf{b}'| - |\mathbf{b}'\rangle \langle \mathbf{b}| : w(\mathbf{b}) = w(\mathbf{b}'); \mathbf{b}, \mathbf{b}' \in \{0,1\}^n \right\}. \quad (67)$$

Next, we prove that this algebra is generated by the following set of operators

$$\{ i|\mathbf{b}\rangle \langle \mathbf{b}| \} \cup \{ iR_{lr} = i(X_l X_r + Y_l Y_r)/2 : l, r \in \{1, \dots, n\} \}, \quad (68)$$

i.e., we prove that

$$\text{alg} \left\{ i|\mathbf{b}\rangle \langle \mathbf{b}|, iR_{lr} = i(X_l X_r + Y_l Y_r)/2 : l, r \in \{1, \dots, n\}, \mathbf{b} \in \{0,1\}^n \right\} \quad (69a)$$

$$= \text{alg} \left\{ i|\mathbf{b}\rangle \langle \mathbf{b}|, |\mathbf{b}\rangle \langle \mathbf{b}'| - |\mathbf{b}'\rangle \langle \mathbf{b}| : w(\mathbf{b}) = w(\mathbf{b}'); \mathbf{b}, \mathbf{b}' \in \{0,1\}^n \right\} = \mathfrak{a}. \quad (69b)$$

To prove this claim, first note that for any bit string $\mathbf{b} \in \{0,1\}^n$, and any pair of distinct qubits $l, r \in \{1, \dots, n\}$, it holds that

$$[i|\mathbf{b}\rangle \langle \mathbf{b}|, iR_{lr}] = |\mathbf{b}'\rangle \langle \mathbf{b}| - |\mathbf{b}\rangle \langle \mathbf{b}'| \equiv F(\mathbf{b}', \mathbf{b}), \quad (70)$$

where \mathbf{b}' is the bit string obtained by exchanging bits l and r of bit string \mathbf{b} , and

$$F(\mathbf{d}, \mathbf{e}) \equiv |\mathbf{d}\rangle\langle\mathbf{e}| - |\mathbf{e}\rangle\langle\mathbf{d}|. \quad (71)$$

Next, note that

$$F(\mathbf{b}, \mathbf{b}'') = \left[F(\mathbf{b}, \mathbf{b}'), F(\mathbf{b}', \mathbf{b}'') \right]. \quad (72)$$

By combining these two steps, we can obtain $F(\mathbf{c}_1, \mathbf{c}_2) = |\mathbf{c}_1\rangle\langle\mathbf{c}_2| - |\mathbf{c}_2\rangle\langle\mathbf{c}_1|$, for any pair of bit strings $\mathbf{c}_1, \mathbf{c}_2 \in \{0, 1\}^n$ with equal Hamming weights: Recall that any pair of bit strings with equal Hamming weights are related via a permutation and any such permutation can be realized by combining *transpositions*, i.e., 2-bit permutations. Therefore, there exists a sequence $\mathbf{b}_1, \dots, \mathbf{b}_L$, such that $\mathbf{b}_1 = \mathbf{c}_1$, $\mathbf{b}_L = \mathbf{c}_2$, $d(\mathbf{b}_k, \mathbf{b}_{k+1}) = 2$ for $1 \leq k \leq L$. Then, using Eq.(72) we have

$$F(\mathbf{c}_1, \mathbf{c}_2) = F(\mathbf{b}_1, \mathbf{b}_L) = \left[\dots \left[\left[F(\mathbf{b}_1, \mathbf{b}_2), F(\mathbf{b}_2, \mathbf{b}_3) \right], F(\mathbf{b}_3, \mathbf{b}_4) \right], F(\mathbf{b}_4, \mathbf{b}_5) \right] \dots, F(\mathbf{b}_{L-1}, \mathbf{b}_L) \right]. \quad (73)$$

This proves Eq.(69), i.e., the Lie algebra \mathfrak{a} is generated by operators $\{i|\mathbf{b}\rangle\langle\mathbf{b}|, iR_{lr}\}$.

Finally, as we have seen in Eq.(18), if one has access to two ancillary qubits initially prepared in states $|0\rangle$ and $|1\rangle$, then using interactions $\{R_{lr} : l, r \in \{1 \dots, n\} \cup \{a, \bar{a}\}\}$ and a single Z term on an ancillary qubit, one can implement all Hamiltonians $\{|\mathbf{b}\rangle\langle\mathbf{b}|\}$. Combining these two results, we conclude that any $U(1)$ -invariant unitary can be implemented using interactions $\{R_{lr} : l, r \in \{1 \dots, n\} \cup \{a, \bar{a}\}\}$ and local Z on an ancillary qubit a or \bar{a} . This completes proof of theorem 3.