PAPER

Synthesis of energy-conserving quantum circuits with *XY* interaction

IOP Publishing Quantum Sci. Technol. 9 (2024) 045049 https://doi.org/10.1088/2058-9565/ad53fa

Quantum Science and Technology

RECEIVED
29 January 2024

ACCEPTED FOR PUBLICATION
4 June 2024

PUBLISHED
20 September 2024

PAPER

Synthesis of energy-conserving quantum circuits with *XY* interaction

Ge Bai[1,2,3] **and Iman Marvian**[4,*]

[1] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
[2] QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong Special Administrative Region of China, People's Republic of China
[3] HKU-Oxford Joint Laboratory for Quantum Information and Computation, University of Oxford, Oxford, United Kingdom
[4] Duke Quantum Center, Departments of Electrical and Computer Engineering and Physics, Duke University, Durham, NC 27708, United States of America
[*] Author to whom any correspondence should be addressed.

E-mail: iman.marvian@duke.edu

Keywords: quantum circuits, energy-conserving unitary, *XY* interaction, quantum gates, circuit synthesis, iSWAP gate, symmetry

Abstract

We study quantum circuits constructed from $\sqrt{\text{iSWAP}}$ gates and, more generally, from the entangling gates that can be realized with the $XX+YY$ interaction alone. Such gates preserve the Hamming weight of states in the computational basis, which means they respect the global U(1) symmetry corresponding to rotations around the z axis. Equivalently, assuming that the intrinsic Hamiltonian of each qubit in the system is the Pauli Z operator, they conserve the total energy of the system. We develop efficient methods for synthesizing circuits realizing any desired energy-conserving unitary using $XX+YY$ interaction with or without single-qubit rotations around the z axis. Interestingly, implementing generic energy-conserving unitaries, such as CCZ and Fredkin gates, with two-local energy-conserving gates requires the use of ancilla qubits. When single-qubit rotations around the z-axis are permitted, our scheme requires only a single ancilla qubit, whereas with the $XX+YY$ interaction alone, it requires two ancilla qubits. In addition to exact realizations, we also consider approximate realizations and show how a general energy-conserving unitary can be synthesized using only a sequence of $\sqrt{\text{iSWAP}}$ gates and two ancillary qubits, with arbitrarily small error, which can be bounded via the Solovay–Kitaev theorem. Our methods are also applicable for synthesizing energy-conserving unitaries when, rather than the $XX+YY$ interaction, one has access to any other energy-conserving two-body interaction that is not diagonal in the computational basis, such as the Heisenberg exchange interaction. We briefly discuss the applications of these circuits in the context of quantum computing, quantum thermodynamics, and quantum clocks.

1. Introduction

In the field of quantum computing and other related areas, such as quantum control and quantum thermodynamics, one is often interested in implementing desired unitary transformations on a quantum system, e.g., on a finite number of qubits. Inspired by the classical circuit model, researchers in this field have developed circuit synthesis techniques to implement any desired unitary using elementary gate sets acting on a few qubits in the system [1–7]. For instance, it has been shown that any unitary transformation on n qubits can be implemented exactly with $\mathcal{O}(4^n)$ single-qubit and 2-qubit gates, such as Controlled-NOT (CNOT)gate [8]. However, these general circuit synthesis techniques do not take into account the specific properties of the desired unitaries, such as their symmetries. Such considerations can significantly reduce the number of required gates and also enable circuit realizations that are more noise-resilient. Additionally, the general circuit synthesis techniques do not distinguish between generic gates and the gates that can be

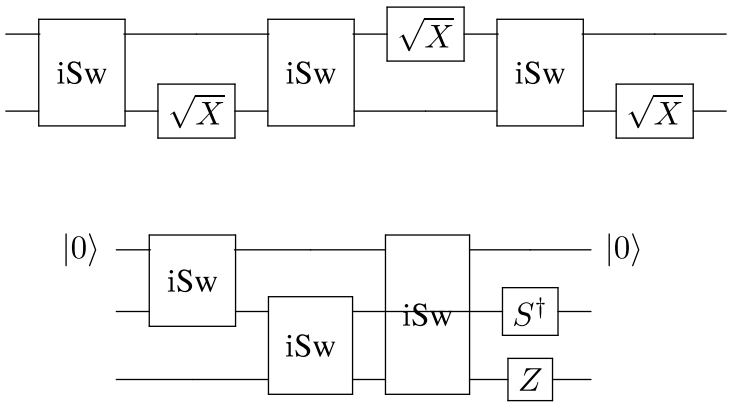


Figure 1. SWAP from iSWAP. The top circuit is the standard way of implementing the SWAP gate using three iSWAP $=\exp(\mathrm{i}R\pi/2)$ gates, also denoted as iSw, where $R=(X\otimes X+Y\otimes Y)/2$ is the XY interaction [22]. (Note that SWAP and iSWAP are indeed equal, up to a global phase in the sector with Hamming weight 1.) This circuit requires three $\sqrt{X}$ gates, which are not energy-conserving. Interestingly, it turns out that even though SWAP is energy-conserving, unless one uses ancilla qubits, such non-energy-conserving gates are unavoidable (see [23] and theorem 5). The bottom circuit realizes SWAP using three iSWAP gates together with two energy-conserving single-qubit gates, namely $S^\dagger$ and Z, and with one ancillary qubit. The lack of non-energy-conserving unitaries makes the bottom circuit more resilient against certain types of noise, such as the fluctuations of the master clock that controls the timing of pulses [23, 24].

realized with native interactions on a particular platform—an important property that makes the gates easier to implement and more robust against noise.

In this work, we study energy-conserving quantum circuits, which are circuits formed from single-qubit rotations around the z-axis and 2-qubit unitary gates U that conserve the sum of Pauli Z operators, such that

$$[U, Z\otimes\mathbb{I}+\mathbb{I}\otimes Z]=0\,. \tag{1}$$

Assuming the qubits have identical intrinsic Hamiltonian, with eigenstates $|0\rangle$ and $|1\rangle$, such gates conserve the total intrinsic energy of the system. Hence, in this paper, we refer to such unitary transformations as energy-conserving unitaries (see section 2 for further details and definitions). Note that this condition can be equivalently understood as a global U(1) symmetry, where the representation of symmetry on each qubit is $\mathrm{e}^{\mathrm{i}\theta Z}:\theta\in(-\pi,\pi]$.

A canonical example of such an energy-conserving gate family, extensively discussed in this paper, is one that can be realized with the Hamiltonian $X\otimes X+Y\otimes Y$, also known as the XY interaction. Besides its fundamental importance in the condensed matter theory, this interaction also plays a crucial role in quantum computing. Namely, it is the native interaction in various solid-state qubits, including quantum dot spins [9–11], as well as some superconducting qubits [12–17]. We also consider quantum circuits that contain other 2-qubit energy-conserving interactions, such as the Heisenberg exchange interaction $X\otimes X+Y\otimes Y+Z\otimes Z$.

It turns out that many useful gates and subroutines in quantum computing are energy-conserving unitaries. This includes the SWAP and controlled-SWAP gates (also know as the Fredkin gate), the controlled-Z (CZ) gate with arbitrary number of control qubits, and the family of unitaries generated by the multi-qubit swap Hamiltonian [18–21]. The standard approaches [2] for implementing such unitaries ignore this conservation law and decomposes the desired unitary to elementary gates that do not conserve the intrinsic energy of qubits, such as CNOT and Hadamard.

In this work, on the other hand, we are interested in the synthesis of energy-conserving unitaries with energy-conserving gates alone. In such circuits, the total energy of the qubits in the system remains conserved throughout the execution of the circuit. As argued in [23], this makes the circuit more resilient against certain types of noise, such as those induced by the instability of the master clock that controls the timing of pulses [24]. As a simple example, in figure 1 we compare two different realizations of a useful and common energy-conserving gate in quantum computing, namely the SWAP gate.

Indeed, even in the cases when the target unitary is not energy-conserving, still, it might be desirable to minimize the use of non-energy-conserving gates. For instance, instead of the standard implementation of the 3-qubit Toffoli gate that requires multiple single and two-qubit non-energy-conserving gates (namely, 6 CNOTs and 2 Hadamards [2, 25, 26]), one can implement this useful gate by sandwiching the energy-conserving controlled-controlled-Z (CCZ) gate between two Hadamards, as shown in figure 2. Then, by realizing CCZ gate with energy-conserving gates, one obtains an implementation of Toffoli, which is more robust against certain fluctuations of the master clock.

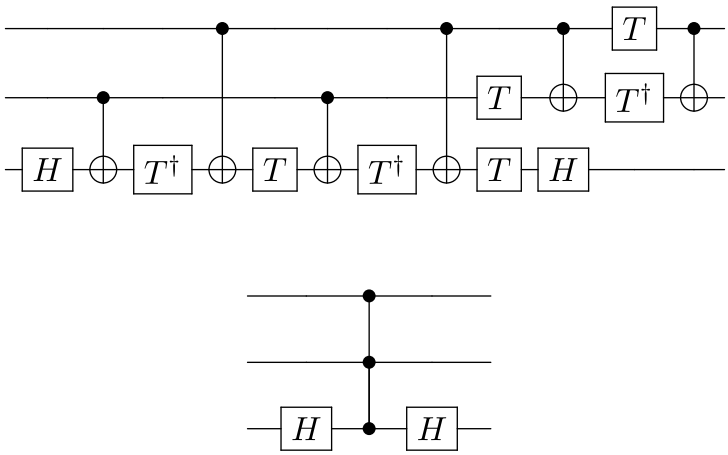


Figure 2. Two different implementations of the Toffoli gate. The top circuit is the standard way of implementing the Toffoli gate [2, 25, 26], which is one of the most useful gates in quantum computing. This circuit contains eight non-energy-conserving gates, namely six CNOTs and two Hadamards. (Indeed, this can be reduced to seven single-qubit non-energy-conserving gates, if one replace each CNOT with a CZ gate sanwhiched with two Hadamards.) The bottom circuit requires a CCZ gate, which is energy-conserving, and two non-energy-conserving gates, namely two Hadamard. Using the techniques developed in this paper, CCZ gate can be realized with XY interaction and local Z with one ancilla qubit, or XY interaction alone with two ancilla qubits. Therefore, in total, it requires only two single-qubit non-energy-conserving gates.

We note that using energy-conserving quantum circuits for suppressing noise has been previously considered in the context of decoherence-free subspaces (DFS) [27–32]. For instance, using the dual-rail encoding, a logical qubit can be encoded in the 2D subspace of a pair of qubits spanned by $|01\rangle$ and $|10\rangle$ states. Then, an encoded version of any desired quantum circuit can be performed in a DFS, i.e., an eigen-subspace of the total intrinsic Hamiltonian $\sum_{j=1}^{n} Z_j$. Indeed, it has been shown that using XY interaction, it is possible to achieve such *encoded universality* [31, 33, 34]. However, a clear downside of this approach is that the encoding reduces the number of logical qubits (e.g., by a factor of 2 in the case of dual-rail encoding), which is undesirable, especially in the NISQ era [35].

On the other hand, in this paper, we do not assume that the global state is restricted to a DFS. Instead, the state of the qubits can be arbitrary. Furthermore, we are interested in a stronger notion of universality, which requires implementing all energy-conserving unitaries. Of course, this notion of universality also implies the encoded universality of XY interaction. In particular, one can use the synthesis techniques developed in this work to find an efficient implementation of the exact gate sequences that are needed to perform an encoded version of a desired circuit in DFS.

Besides quantum computing, the notion of energy-conserving unitaries appears in many broad areas of quantum information science and, therefore, it is crucial to understand how they can be realized with energy-conserving circuits. For instance, in quantum thermodynamics one often assumes energy-conserving unitaries are 'free', i.e. can be realized with negligible cost [36–40]. However, prior to this work, it was not known how a general energy-conserving unitary can be realized, and in particular, how it can be decomposed to a finite sequence of local energy-conserving unitaries. Other areas of applications include quantum clocks, quantum reference frames and the resource theory of asymmetry (see section 8 and [23] for further discussion).

1.1. Summary of the main results: circuit synthesis techniques

It was shown in [23] that it is impossible to implement a generic energy-conserving unitary by applying local energy-conserving gates on the subsystems that form the system (In section 2.2 and theorem 5 we briefly review this result). This is in sharp contrast with the standard universality of 2-qubit gates in the absence of energy conservation [6, 41]. In addition to this result, [23] also shows that this no-go theorem can be circumvented using a single ancilla qubit. In particular, [23] proves that for any desired energy-conserving unitary V on n qubits, there exists an energy-conserving unitary $\widetilde{V}$ on $n+1$ qubits, such that $\widetilde{V}$ can be realized by Hamiltonians $X\otimes X + Y\otimes Y$ and single-qubit Z and

$$\widetilde{V}(|\psi\rangle \otimes |0\rangle_{\text{anc}}) = (V|\psi\rangle) \otimes |0\rangle_{\text{anc}} \,, \tag{2}$$

for all states $|\psi\rangle$ of n qubit system (see the example in figure 1). Subsequently, [42] simplified and generalized this result, to symmetric quantum circuits with arbitrary Abelian symmetries.

Building on the ideas developed in [23] and [42], in this work we go beyond these results and develop various circuit synthesis techniques for constructing explicit circuits with energy-conserving gates. (This is analogous to the development of the theory of quantum circuits: first, the universality of 2-local gates was established mostly using Lie-algebraic arguments [6, 41], and then, building on those results, explicit and efficient circuit synthesis techniques were developed. See, e.g. [3, 43].)

Using these circuit synthesis methods we show that

Theorem 1 (Exact implementation). *Any energy-conserving unitary transformation on n qubits, i.e., a unitary transformation that commutes with $\sum_{j=1}^{n} Z_j$, can be realized exactly, up to a possible global phase, using $\mathcal{O}(4^n n^{3/2})$ gates from any one of the following universal gate sets*

1. $\sqrt{\mathrm{iSWAP}} = \exp(\mathrm{i}\frac{\pi}{4}R)$ *, and* $\exp(\mathrm{i}\phi Z) : \phi \in (-\pi, \pi]$ *gates, with one ancilla qubit, where*

$$R = \frac{1}{2}\left(X \otimes X + Y \otimes Y\right) . \tag{3}$$

2. $\exp(\mathrm{i}\alpha H_{int}) : \alpha \in \mathbb{R}$ *, and* $S = e^{\mathrm{i}\pi/4}\exp(-\mathrm{i}\pi Z/4)$ *gates, with one ancilla qubit, where H_{int} is any energy-conserving 2-qubit Hamiltonian that is not diagonal in the computational basis, such that*

$$[H_{int}, Z \otimes \mathbb{I}] = -[H_{int}, \mathbb{I} \otimes Z] \neq 0 , \tag{4}$$

3. $\exp(\mathrm{i}\alpha R) : \alpha \in (-\pi, \pi]$ *gates, with two ancilla qubits.*

Two canonical examples of non-diagonal energy-conserving Hamiltonians are the XY interaction and the Heisenberg interaction $R_{\mathrm{Heis}} := (X \otimes X + Y \otimes Y + Z \otimes Z)/2$. Then, part 2 of the theorem implies that the following sets are universal:

- $\exp(\mathrm{i}\alpha R) : \alpha \in (-\pi, \pi]$, and S gates, with one ancilla qubit,
- $\exp(\mathrm{i}\alpha R_{\mathrm{Heis}}) : \alpha \in (-\pi, \pi]$, and S gates, with one ancilla qubit.

A few remarks are in order: first, as we show in section 2.1, general energy-conserving unitary transformations on n qubits are smoothly parameterized by $\approx 4^n/\sqrt{\pi n}$ real parameters. Therefore, a simple parameter counting implies that for generic energy-conserving unitaries, the above constructions are close to optimal, by a factor of n^2[5].

Second, note that in part 2 of the theorem the condition that H_{int} is not diagonal is necessary, because otherwise qubits cannot exchange energy with each other, i.e., the overall n-qubit unitary will be also diagonal in the computational basis.

Finally, note that in all the three cases in theorem 1 one needs, at least, one ancilla qubit, which by the argument [23] is unavoidable. However, for the last gate set an extra ancilla is used. This is because XY Hamiltonian has an additional $\mathbb{Z}_2$ symmetry, namely

$$X^{\otimes 2} R X^{\otimes 2} = R . \tag{5}$$

As we further explain in section 6, this $\mathbb{Z}_2$ symmetry can be broken with the extra ancilla qubit. In this case, the ancilla can be interpreted as a quantum reference frame, or asymmetry catalyst [44, 45][6].

In addition to exact implementation, we also investigate the approximate implementation of energy-conserving unitaries using finite gate sets, e.g., $\sqrt{\mathrm{iSWAP}}$ and S gates. Applying the Solovay–Kitaev theorem [1, 50, 51], one can bound the number of such gates that are needed to implement a desired energy-conserving unitary, with any error $\epsilon > 0$ as quantified in terms of the operator norm distance between the desired unitary and the realized unitary (see section 7 for the formal statements). In particular, we show that

Corollary 2 (Approximate implementation). *Any energy-conserving unitary on $n \geqslant 2$ qubits can be realized with an error bounded by $\epsilon > 0$, using $\mathcal{O}(4^n n^{3/2}(n + \log \epsilon^{-1})^{\nu})$ number of gates from either of the following gate sets:*

[5] More generally, we will show in section 5 step 3 that if an energy-conserving unitary acts non-trivially only on a subspace spanned by D elements of the computational basis then it can be realized using $\mathcal{O}(n^2 \times D^2)$ gates from any one of the above gate sets.

[6] It is worth noting that with any finite number of ancilla qubits, it is impossible to implement non-energy-conserving unitaries, using energy-conserving interactions alone. This can be understood as a consequence of the Wigner–Araki–Yanase theorem [46, 47], or equivalently, a consequence of the no-programming theorem [48] (see [49] for the connection).

1. $\sqrt{\text{iSWAP}}$ *gate alone with* 2 *ancilla qubits.*
2. $\sqrt{\text{iSWAP}}$ *and* S *gates with* 1 *ancilla qubit.*

Here, ν *is the exponent for the complexity of Solovay–Kitaev algorithm, and can be chosen as any number greater than* $\log_{(1+\sqrt{5})/2} 2 \approx 1.44042$.

In the above discussions, we did not specify any geometry for the system of qubits and assumed gates can be applied between any pair of qubits. What happens if we assume the qubits form an open chain and gates are allowed only between nearest-neighbor qubits?

As it was noted in [23], this additional restriction does not affect the set of realizable unitaries, provided that the ancilla can be coupled to all the qubits in the chain. This is because interacting two qubits with the ancilla using $X\otimes X+Y\otimes Y$ and Z Hamiltonians, allows us to perform the SWAP gate that exchanges the state of two qubits (see figure 1). Then, applying SWAPs between nearest-neighbor qubits, one can arbitrarily change the order of qubits. On the other hand, if one requires that the ancilla should also be part of the chain and only interact with its nearest neighbors, then the above universality result does not hold anymore. Indeed, in this case, using the Jordan–Wigner transformation [52–54] this system can be mapped to a free fermionic system, which implies that the group of realizable unitaries is significantly smaller than the group of energy-conserving unitaries (namely, it has dimension n^2). Of course, if one is allowed to use the SWAP gate, this restriction can be avoided. That is

Corollary 3 (Approximate implementation with nearest-neighbor gates). *Consider an open chain of* $n+1$ *qubits, where one of the qubits is designated as the ancilla qubit and is initially prepared in state* $|0\rangle$. *Any energy-conserving unitary on the rest of qubits can be realized using* $\mathcal{O}(4^n n^{3/2}(n+\log\epsilon^{-1})^{\nu})$ *number of gates* S, *SWAP, and* $\sqrt{\text{iSWAP}}$ *with two-qubit gates restricted to nearest-neighbor qubits, for any* $\nu > \log_{(1+\sqrt{5})/2} 2$.

Finally, in section 6 we develop circuit synthesis techniques using XY interaction alone and, in particular, without single-qubit Z Hamiltonian and ancilla qubits. It follows that all realizable unitaries should satisfy the $\mathbb{Z}_2$ symmetry of XY interaction in equation (5). However, as the following theorem states, there are more constraints on the realizable unitaries (see section 6 for further details).

Theorem 4 (Circuits with XY interaction alone). *On a system with* $n \geqslant 3$ *qubits, any unitary* V *can be realized with interaction* $R=(X\otimes X+Y\otimes Y)/2$ *alone (without any ancilla qubits) if, and only if,*

1. V *is energy-conserving, i.e.* $[V,\sum_{j=1}^{n} Z_j]=0$.
2. *It satisfies the* $\mathbb{Z}_2$ *symmetry* $X^{\otimes n}VX^{\otimes n}=V$.
3. $det(V^{(m)})=1 : m=0,\cdots,n$, *where* $det(V^{(m)})$ *is the determinant of* $V^{(m)}$, *the component of* $V=\bigoplus_{m=0}^{n} V^{(m)}$ *in the subspace with Hamming weight* m, *that is the eigensubspace of* $\sum_{j=1}^{n} Z_j$ *with eigenvalue* $n-2m$.
4. *When* n *is even,* $det(V^{(n/2,\pm)})=1$, *where* $V^{(n/2,\pm)}$ *is the component of* V *in the joint eigensubspaces of* $\sum_j Z_j$ *and* $X^{\otimes n}$, *with eigenvalues* 0 *and* ± 1, *respectively, such that*

$$V^{(n/2)} = V^{(n/2,+)} \oplus V^{(n/2,-)} \ . \tag{6}$$

Furthermore, any unitary satisfying the above conditions can be realized with $\mathcal{O}(4^n n^{3/2})$ *gates* $\exp(\mathrm{i}\theta R) : \theta \in (-\pi,\pi]$.

This means that the group of unitaries that can be realized with XY interaction alone on $n \geqslant 3$ qubits, denoted by $\mathcal{G}_n$, is isomorphic to

$$\mathcal{G}_n \cong \prod_{m=1}^{\lfloor \frac{n}{2} \rfloor} \mathrm{SU}\left(\binom{n}{m}\right) \qquad : n \text{ is odd}$$

$$\mathcal{G}_n \cong \prod_{m=1}^{\frac{n}{2}-1} \mathrm{SU}\left(\binom{n}{m}\right) \times \left[\mathrm{SU}\left(\frac{1}{2}\binom{n}{\frac{n}{2}}\right)\right]^{\times 2} \qquad : n \text{ is even}$$

where we have used the fact that the dimension of the subspace with Hamming weight m is $\binom{n}{m}$. Note that in the special case of $n=2$, the constraint in condition 4 does not hold and[7]

$$\mathcal{G}_2 \cong \mathrm{U}(1) \ .$$

[7] In this case, the eigen-subspaces of $X^{\otimes 2}$ in the subspace with Hamming weight 1 correspond to vectors $|01\rangle \pm |10\rangle$, which are also eigenvectors of $\exp(\mathrm{i}\theta R)$ with eigenvalues $\mathrm{e}^{\pm \mathrm{i}\theta}$.

It is also worth emphasizing that while the additional constraint in the case of even $n \geqslant 4$, i.e., condition 4, is related to the aforementioned $\mathbb{Z}_2$ symmetry of XY interaction in equation (5), it is not necessarily satisfied by all unitaries that respect the $\mathbb{Z}_2$ symmetry (Namely, it is of the type of constraints discussed in [23] which are the consequence of both locality and symmetry of Hamiltonian). For instance, for a system with $n = 4$ qubits, consider the family of unitaries

$$\exp\left(\mathrm{i}\theta\left[|0011\rangle\langle 1100| + |1100\rangle\langle 0011|\right]\right) \quad : \theta \in (-\pi, \pi]\,,$$

i.e. unitaries generated by Hamiltonian $H = |0011\rangle\langle 1100| + |1100\rangle\langle 0011|$. While these unitaries respect conditions 1–3 of theorem 4, unless $\theta = 0$, they do not satisfy condition 4 of this theorem and therefore they are not realizable with XY interaction alone[8]. Finally, we note that our results on approximate universality imply that the group generated by $\sqrt{\mathrm{iSWAP}}$ gates on $n \geqslant 3$ qubits is a dense subgroup of $\mathcal{G}_n$.

The rest of this paper is organized as follows:

- Section 2 formulates our goal by introducing energy-conserving unitaries and the notion of (semi-)universality. It contains a collection of elementary gates useful for subsequent circuit constructions. In section 2.5, circuits with iSWAP and single-qubit z-rotations are characterized.
- Section 3 discusses the structure of 2-qubit energy-conserving unitaries. It shows the semi-universality of (and thus the equivalence between) the gate sets 1 and 2 in theorem 1 for 2 qubits.
- Section 4 is focused on 3-qubit energy-conserving unitaries. It contains the implementation of controlled-Z and SWAP gates using a single ancilla qubit, as well as circuit identities that are useful afterwards. The construction of 3-qubit 2-level special unitary energy-conserving gates is presented in section 4.2, which serves as a basis for the construction of general n-qubit energy-conserving unitaries.
- Section 5 is dedicated to the construction of n-qubit energy-conserving unitaries, and concludes the proof of theorem 1, for gate sets 1 and 2.
- Section 6 is focused on the set of unitaries that are realizable with XY interaction alone, contains the proof of theorem 4 and completes the proof of theorem 1 for gate set 3.
- Section 7 introduces approximate universality and provides approximate constructions of aforementioned circuits in sections 4–6. It combines a Lie algebraic characterization of unitaries generated by $\sqrt{\mathrm{iSWAP}}$ gates with the Solovay–Kitaev theorem, and proves corollary 2.
- Section 8 contains a short discussion on applications of energy-conserving quantum circuits, in areas such as quantum computing, quantum thermodynamics, and quantum clocks.

2. Preliminaries

2.1. Energy-conserving unitaries

Consider a system with n qubits, each with the intrinsic Hamiltonian $-\Delta E\, Z/2$, where $\Delta E > 0$ is the energy difference between the ground state $|0\rangle$ and the excited state $|1\rangle$ of the qubit. Then, the total intrinsic Hamiltonian of this system is

$$H_{\text{intrinsic}} = -\frac{\Delta E}{2}\sum_{j=1}^{n} Z_j = \Delta E\left(-\frac{n}{2} + \sum_{m=0}^{n} m\,\Pi^{(m)}\right)\,, \tag{7}$$

where Z_j denotes the Pauli Z operator on qubit j tensor product with the identity operator on the rest of qubits, and $\Pi^{(m)}$ is the projector to the eigen-subspace $\mathcal{H}^{(m)}$ of $H_{\text{intrinsic}}$ with energy $(2m - n) \times \Delta E/2$. Then, the total Hilbert space decomposes as

$$\left(\mathbb{C}^2\right)^{\otimes n} \cong \bigoplus_{m=0}^{n} \mathcal{H}^{(m)}\,. \tag{8}$$

Let $\{|0\rangle, |1\rangle\}^{\otimes n}$ be the *computational* basis for n qubits. We will label a vector in this basis with a bit string $\mathbf{b} = b_1 \cdots b_n \in \{0,1\}^n$ as $|\mathbf{b}\rangle$. Then, $\mathcal{H}^{(m)}$ is the subspace spanned by the elements of this basis with Hamming weight m (Recall that the Hamming weight of a bit string is the number of bits with value 1).

We are interested in energy-conserving unitaries on this systems, i.e., those that conserve the total intrinsic Hamiltonian of the qubits in the system. A unitary V on n qubits is energy-conserving if, and only

[8] In particular, in this case, $V^{(2,\pm)} = \exp(\pm \mathrm{i}\theta|\psi_\pm\rangle\langle\psi_\pm|)$ where $|\psi_\pm\rangle = (|0011\rangle \pm |1100\rangle)/\sqrt{2}$ are the eigenvectors of H with eigenvalues ± 1. Then, $\det(V^{(2,\pm)}) = e^{\pm \mathrm{i}\theta}$ which implies, unless $\theta = 0$, this unitary is not realizable with XY interactions alone.

if, it is block-diagonal with respect to the decomposition in equation (8), such that

$$V=\bigoplus_{m=0}^{n} V^{(m)}\,. \tag{9}$$

Following the notation in [23], we denote the set of such unitaries as

$$\begin{aligned}\mathcal{V}_n^{\mathrm{U}(1)} &= \left\{V:[V,H_{\mathrm{intrinsic}}]=0, VV^\dagger=\mathbb{I}^{\otimes n}\right\}\\ &=\bigoplus_{m=0}^{n}\mathrm{U}\left(\mathcal{H}^{(m)}\right)\,,\end{aligned} \tag{10}$$

where $\mathbb{I}$ denotes the identity operator on a single qubit, and $\mathrm{U}(\mathcal{H}^{(m)})$ denotes the group of all unitaries acting on $\mathcal{H}^{(m)}$. Here, the superscript $\mathrm{U}(1)$ refers to the fact that $\mathcal{V}_n^{\mathrm{U}(1)}$ is the set of unitaries that commute with unitaries

$$\left(\exp(\mathrm{i}\theta Z)\right)^{\otimes n}=\exp\left(\mathrm{i}\theta\sum_{j=1}^{n}Z_j\right)\quad:\ \theta\in(-\pi,\pi]\,, \tag{11}$$

which is a representation of the group $\mathrm{U}(1)=\{e^{i\theta}:\theta\in(-\pi,\pi]\}$ that describes the time evolution of a periodic system ([23] studies circuits with general symmetries).

Decomposition in equation (10) implies that energy-conserving unitaries can be smoothly parameterized using

$$\dim\left(\mathcal{V}_n^{\mathrm{U}(1)}\right)=\sum_{m=0}^{n}\binom{n}{m}^2=\binom{2n}{n}\approx\frac{4^n}{\sqrt{\pi n}}\,, \tag{12}$$

real parameters, where by $\approx$ we mean the ratio of two sides goes to 1, in the limit $n\to\infty$, which can be established using the Stirling's approximation for factorials.

As we discuss in the following, it is also useful to consider the subgroup of this group, formed from energy-conserving unitaries $V=\bigoplus_m V^{(m)}$, where in each sector we have $\det(V^{(m)})=1$, i.e.

$$\begin{aligned}\mathcal{SV}_n^{\mathrm{U}(1)} &= \left\{V=\bigoplus_{m=0}^{n}V^{(m)}:V^{(m)}\in\mathrm{SU}\left(\mathcal{H}^{(m)}\right)\right\}\\ &=\bigoplus_{m=0}^{n}\mathrm{SU}\left(\mathcal{H}^{(m)}\right)\,,\end{aligned} \tag{13}$$

where $\mathrm{SU}(\mathcal{H}^{(m)})$ denotes the group of special unitaries acting on $\mathcal{H}^{(m)}$.

With this definition, any element of $\mathcal{V}_n^{\mathrm{U}(1)}$ has a decomposition as

$$V=QD=DQ\,, \tag{14}$$

where unitary $Q\in\mathcal{SV}_n^{\mathrm{U}(1)}$, unitary

$$D=\sum_{m=0}^{n}\exp\left[\mathrm{i}\theta_m\binom{n}{m}^{-1}\right]\Pi^{(m)}\,, \tag{15}$$

is diagonal in the computational basis, and

$$\theta_m=\arg\left(\det\left(V^{(m)}\right)\right)\,, \tag{16}$$

is the phase of the determinant of $V^{(m)}$, and for convenience we assume $\theta_m\in(-\pi,\pi]$. We note that, in general, the decomposition in equation (14) is not unique.

In the following, for any unitary V, $\Lambda^{\mathbf{c}}(V)$ denotes its controlled-version with control string $\mathbf{c}\in\{0,1\}^k$, i.e.

$$\Lambda^{\mathbf{c}}(V):=\sum_{\mathbf{c}'\neq\mathbf{c}}|\mathbf{c}'\rangle\langle\mathbf{c}'|\otimes\mathbb{I}+|\mathbf{c}\rangle\langle\mathbf{c}|\otimes V\,. \tag{17}$$

If $V\in\mathcal{SV}_n^{\mathrm{U}(1)}$, then its controlled version $\Lambda^{\mathbf{c}}(V)$ is in $\mathcal{SV}_{n+k}^{\mathrm{U}(1)}$.

2.2. Semi-universality and universality with *XY* interaction and local Z

Marvian [23] shows that any energy-conserving unitary $V=\bigoplus_{m=0}^{n}V^{(m)}$ can be realized using XY interaction and local Z, up to certain constraints on the relative phases between sectors with different energies. Following [42], we say a set of gates are semi-universal for energy-conserving unitaries, if they generate $\mathcal{SV}_n^{\mathrm{U}(1)}$ for all integer n. Using the notion of semi-universality, the result of [23] can be rephrased as

Theorem 5 (Based on [23]). *For a system with n qubits, the group $G_{XX+YY,Z}$ generated by 2-qubit gates $\exp(\mathrm{i}\alpha[XX+YY])$, single-qubit gates $\exp(\mathrm{i}\beta Z)$, and global phase $e^{\mathrm{i}\phi}\mathbb{I}$ for $\alpha,\beta,\phi\in(-\pi,\pi]$ is equal to the subgroup of all energy-conserving unitaries $V\in\mathcal{V}_n^{U(1)}$ satisfying the extra constraint*

$$\theta_m=\binom{n}{m}\times\left[\frac{m}{n}\times(\theta_n-\theta_0)+\theta_0\right]\ :\ mod\ 2\pi\ , \tag{18}$$

for all $m=0,\cdots,n$, where $\theta_m=arg(det(V^{(m)}))$ and $V^{(m)}$ is the component of V in the sector with Hamming weight m. In particular, $G_{XX+YY,Z}$ contains $\mathcal{SV}_n^{U(1)}$ defined in equation (13) and, therefore, the aforementioned gates are semi-universal.

We note that the circuit synthesis techniques presented in this paper provide an independent proof of the second part of this theorem. In particular, the semi-universality of this gate set is demonstrated in proposition 13. For completeness, in appendix A, we also establish the first part; that is, we show that equation (18) along with the energy conservation condition fully characterizes the group $G_{XX+YY,Z}$[9].

Equation (18) imposes $n-1$ independent constraints on the set of unitaries in $G_{XX+YY,Z}$. Then, it follows from this theorem that the difference between the dimensions of the Lie group of all energy-conserving unitaries and the subgroup $G_{XX+YY,Z}$ is equal to

$$\dim\left(\mathcal{V}_n^{\mathrm{U}(1)}\right)-\dim\left(G_{XX+YY,Z}\right)=n-1\ . \tag{19}$$

Marvian [23] also shows that using a single ancilla qubit, it is possible to circumvent these constraints. That is

Corollary 6 ([23]). *Any energy-conserving unitary can be realized with a single ancillary qubit, and gates $\exp(i\phi Z)$ and 2-local gates $\exp(i\phi[XX+YY])$.*

The proof of this result in Marvian [23] is Lie algebraic. In this work, on the other hand, we give explicit circuit construction methods for realizing general energy-conserving unitaries with a single ancilla qubit.

2.3. 2-level energy-conserving unitaries

A key notion in the quantum circuit theory is the concept of 2-level unitaries, also known as Givens rotations [2]. We say a unitary transformation is 2-level with respect to the computational basis $\{|0\rangle,|1\rangle\}^{\otimes n}$, if it acts trivially (i.e., as the identity operator) on all the basis elements, except, at most 2.

In the following, for any pair of bit strings $\mathbf{b},\mathbf{b}'\in\{0,1\}^n$, $U(\mathbf{b},\mathbf{b}')$ denotes a 2-level unitary acting as $U\in\mathrm{U}(2)$ on the subspace spanned by $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$, and acting trivially on the orthogonal complement of this subspace. More precisely, for a 2×2 unitary

$$U=\begin{pmatrix}u_{11}&u_{12}\\u_{21}&u_{22}\end{pmatrix}, \tag{20}$$

its corresponding 2-level unitary is

$$U\left(\mathbf{b},\mathbf{b}'\right):=u_{11}|\mathbf{b}\rangle\langle\mathbf{b}|+u_{12}|\mathbf{b}\rangle\langle\mathbf{b}'|+u_{21}|\mathbf{b}'\rangle\langle\mathbf{b}|+u_{22}|\mathbf{b}'\rangle\langle\mathbf{b}'|+\sum_{\mathbf{c}\neq\mathbf{b},\mathbf{b}'}|\mathbf{c}\rangle\langle\mathbf{c}|\,. \tag{21}$$

A 2-level unitary $U(\mathbf{b},\mathbf{b}')$ is in $\mathcal{SV}_n^{\mathrm{U}(1)}$ if, and only if $\det(U)=1$ and $w(\mathbf{b})=w(\mathbf{b}')$, where for any bit string $\mathbf{b}=b_1\cdots b_n\in\{0,1\}^n$,

$$w(\mathbf{b})=\sum_{j=1}^{n}b_j\ , \tag{22}$$

denotes the Hamming weight of $\mathbf{b}$.

[9] It is also worth noting that in the context of control theory, using a Lie algebraic argument, [55] shows that in any individual Hamming-weight sector, Hamiltonians $XX+YY$, ZZ, and local Z together generate all unitaries in that sector; a property known as subspace controllability.

2.4. Elementary gates

We mainly study quantum circuits formed from two types of gates. First, single-qubit rotations around z, i.e., unitaries

$$R_z(\phi) = \exp(\mathrm{i}\frac{\phi}{2}Z) = \begin{pmatrix} e^{\mathrm{i}\frac{\phi}{2}} & \\ & e^{-\mathrm{i}\frac{\phi}{2}} \end{pmatrix} \quad : \phi \in (-\pi, \pi] \,. \tag{23}$$

Two important specific cases are

$$T = e^{\frac{\mathrm{i}\pi}{8}} R_z\left(-\frac{\pi}{4}\right) = \begin{pmatrix} 1 & \\ & e^{\mathrm{i}\frac{\pi}{4}} \end{pmatrix} = \sqrt[4]{Z} \tag{24}$$

and

$$S = e^{\frac{\mathrm{i}\pi}{4}} R_z\left(-\frac{\pi}{2}\right) = \begin{pmatrix} 1 & \\ & \mathrm{i} \end{pmatrix} = \sqrt{Z} = T^2 \,. \tag{25}$$

The second type of gates used in our circuits are in the form

$$\exp(\mathrm{i}\alpha R) \quad : \alpha \in (-\pi, \pi] \,, \tag{26}$$

where

$$R := \frac{1}{2}\left(X \otimes X + Y \otimes Y\right) \,. \tag{27}$$

Two important special cases are the iSWAP gate

$$\mathrm{iSWAP} = \mathrm{iSw} = \exp\left(\mathrm{i}\frac{\pi}{2}R\right) = \begin{pmatrix} 1 & & & \\ & & \mathrm{i} & \\ & \mathrm{i} & & \\ & & & 1 \end{pmatrix} , \tag{28}$$

and the square root of iSWAP gate

$$\sqrt{\mathrm{iSWAP}} = \sqrt{\mathrm{iSw}} = \exp\left(\mathrm{i}\frac{\pi}{4}R\right) = \begin{pmatrix} 1 & & & \\ & \frac{1}{\sqrt{2}} & \frac{\mathrm{i}}{\sqrt{2}} & \\ & \frac{\mathrm{i}}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \\ & & & 1 \end{pmatrix} , \tag{29}$$

where the matrices are written in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Note that $\sqrt{\mathrm{iSw}}^\dagger = (\sqrt{\mathrm{iSw}})^7$. See, e.g., [22, 56] for further discussions about the properties and applications of $\sqrt{\mathrm{iSw}}$ and iSw gates for circuit synthesis.

We also consider the SWAP gate

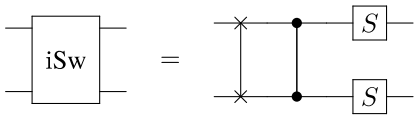
$$\mathrm{SWAP} = \mathrm{Sw} = \begin{pmatrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{pmatrix} = \quad , \tag{30}$$

and the Controlled-Z (CZ) gate

$$CZ = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes Z = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} =$$

2.5. Circuits with iSWAP and single-qubit z rotations

In this paper, we show how a general energy-conserving unitary can be realized with the $\exp(i\alpha R)$ gate and single-qubit rotations around z. However, it is useful to first consider a more restricted family of circuits generated by the single-qubit rotations around z together with iSWAP gate. To analyze such circuits, we consider the useful circuit identity



(31)

Note that the S gate commutes with the controlled-Z gate. Then, using this identity it can be easily seen that

Proposition 7. *Suppose unitary V is realized by a circuit formed from* iSWAP *gates. Then, V has a decomposition as $V = V_3V_2V_1$, where V_1 is a permutation, i.e., is a composition of SWAP gates, V_2 is a composition of controlled-Z gates, and V_3 is a composition of single-qubit S gates. More generally, if in addition to* iSWAP*, the circuit also contains the single-qubit rotations around z, denoted by $R_z(\phi) : \phi \in (-\pi, \pi]$, then the realized unitary V has a similar decomposition, where V_3 is now a product of arbitrary single-qubit rotations around the z axis.*

In particular, note that while iSWAP is an entangling gate, the family of energy-conserving unitaries that can be realized by combining this gate with single-qubit z-rotations, are very limited. Namely, the set of realizable unitaries is specified by n real parameters and they map any element of the computational basis to an element of the computational basis, up to a global phase.

Using this property of iSWAP circuits one can establish several other useful circuit identities, which are summarized in figure 3. Such identities will play a key role for constructions in the following sections.

3. 2-qubit energy-conserving unitaries

3.1. The structure and realization of $\mathcal{V}_2^{\mathrm{U(1)}}$

For $n = 2$ qubits, the energy levels of the intrinsic Hamiltonian $H_{\text{intrinsic}}$ in equation (7) decomposes the Hilbert space into 3 eigen-subspaces corresponding to Hamming weights 0, 1, and 2. Then, a general 2-qubit energy-conserving unitary is specified by $1 + 2^2 + 1 = 6$ real parameters and is in the form

$$V = \begin{pmatrix} e^{i\theta_0} & & \\ & V^{(1)} & \\ & & e^{i\theta_2} \end{pmatrix} = QD = DQ\,. \tag{32}$$

Here, $V^{(1)}$ is an arbitrary 2×2 unitary in the sector with Hamming weight 1 spanned by $|01\rangle$ and $|10\rangle$. Furthermore, D is diagonal in the computational basis and satisfies $[D, V] = 0$, whereas

$$Q = \begin{pmatrix} 1 & & \\ & Q^{(1)} & \\ & & 1 \end{pmatrix} \in \mathcal{S}\mathcal{V}_2^{\mathrm{U(1)}}\,, \tag{33}$$

i.e., has determinant 1 in all sectors with Hamming weights 0, 1, and 2. $Q^{(1)}$ can be written in the basis of $|01\rangle$ and $|10\rangle$ as a single-qubit gate. For example,

$$\begin{aligned} Q = \exp(i\alpha R) \quad &\longrightarrow \quad Q^{(1)} = \exp(i\alpha X) \\ Q = \sqrt{\textbf{iSWAP}} \quad &\longrightarrow Q^{(1)} = \exp(i\pi X/4) \\ Q = \exp(i\alpha[Z_1 - Z_2]) &\longrightarrow \quad Q^{(1)} = \exp(2i\alpha Z)\,. \end{aligned} \tag{34}$$

In particular, using the Euler decomposition for $Q^{(1)}$ as $Q^{(1)} = e^{\mathrm{i}\gamma Z}e^{\mathrm{i}\beta Y}e^{\mathrm{i}\alpha Z}$ for some $\alpha,\beta,\gamma \in (-\pi,\pi]$, we find that Q has a decomposition as

$$Q = e^{\mathrm{i}\frac{\gamma}{2}(Z_1-Z_2)}\sqrt{\mathrm{iSw}}_{12}e^{\mathrm{i}\frac{\beta}{2}(Z_1-Z_2)}\sqrt{\mathrm{iSw}}_{12}^{\dagger}e^{\mathrm{i}\frac{\alpha}{2}(Z_1-Z_2)} . \tag{35}$$

Furthermore,

$$D = e^{i\theta_0}\Pi^{(0)} \pm e^{i\theta_1/2}\Pi^{(1)} + e^{i\theta_2}\Pi^{(2)} \tag{36a}$$

$$= e^{i\,\phi_2 Z_1 Z_2}\; e^{i\,\phi_1(Z_1+Z_2)}\; e^{i\phi_0} , \tag{36b}$$

where $\theta_1 = \arg(\det(V_1))$ and

$$4\phi_0 = \theta_0+\theta_1+\theta_2 =: \Phi_0 , \tag{37a}$$

$$8\phi_1 = 2\theta_0 - 2\theta_2 =: \Phi_1 , \tag{37b}$$

$$4\phi_2 = \theta_0-\theta_1+\theta_2 =: \Phi_2 \;:\; \mathrm{mod}\; 2\pi . \tag{37c}$$

The phases $\Phi_l : l = 0,1,2$ are called the l-body phase associated to the unitary V [23]. It is worth noting that while neither of phases $\theta_0,\theta_1,\theta_2$, or ϕ_0,ϕ_1,ϕ_2 are physically observable, all the l-body phases, except Φ_0, are observable. For instance, when V is the identity operator, equation (36*b*) holds for all

$$\phi_0 = \phi_1 = \phi_2 = \frac{k\pi}{2} \quad : k = 0,\cdots,3 ,$$

whereas for all four cases we have

$$\Phi_0 = \Phi_1 = \Phi_2 = 0 \;:\; \mathrm{mod}\; 2\pi .$$

Note that $\Phi_0 = 4\phi_0$ corresponds to a global phase. Furthermore, $\Phi_1 = 4\phi_1$ can be changed arbitrarily by applying the unitary $\exp(\mathrm{i}\phi_1(Z_1+Z_2))$, which can be realized with local Z interactions. On the other hand, as it follows immediately from equation (18) in theorem 5, a general U(1)-invariant unitary V on a pair of qubits can be realized by XY interaction and local Z if, and only if its 2-body phase is zero, i.e.

$$\Phi_2 = \theta_0-\theta_1+\theta_2 = 0 \;:\; \mathrm{mod}\; 2\pi . \tag{38}$$

This constraint, for instance, excludes the SWAP and CZ gates, because for both of these operators 2-body phase is $\Phi_2 = \pi$.

It is also worth mentioning that the matrices Q and D in decomposition in equation (32) are unique up to a freedom in choosing θ_1 or $\theta_1+\pi$. This freedom is related to the fact that both matrices

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

are in SU(2). Therefore, the component of Q in the sector with Hamming weight 1 is fixed up to a plus/minus sign.

3.2. 2-qubit semi-universality of the gate sets in theorem 1

As we will explain in the following, the above characterization of 2-qubit energy-conserving unitaries immediately implies the semi-universality of gate sets 1 and 2 in theorem 1, for the special case of $n = 2$ qubits. This, in particular, means that using any of these gate sets one can realize the family of unitaries

$$\exp(\mathrm{i}\alpha R) : \alpha = (-\pi,\pi] ,$$

where $R = (X\otimes X + Y\otimes Y)/2$.

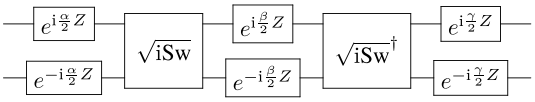
Then, in the rest of the paper, we consider circuits that only contain this family of unitaries as well as the S gate and prove theorem 1 for this gate set, which is a special case of gate set 2 (In other words, we show how a general energy-conserving unitary can be realized with these elementary gates and a single ancilla qubit). This result combined with the following discussion proves theorem 1 for gate sets 1 and 2. Crucially, as we will show below, the gates in each set can be constructed using the other gate set exactly, using a finite $\mathcal{O}(1)$ number of gates. Therefore, to implement a general energy-conserving unitary, the number of required gates from each gate set is the same for all gate sets, up to an $\mathcal{O}(1)$ constant.

Note that, due to $\mathbb{Z}_2$ symmetry of XY interaction in equation (5), the gate set 3, which only includes $\exp(\mathrm{i}\alpha R) : \alpha = (-\pi,\pi]$ without single-qubit rotations around z, is not semi-universal. However, as we will explain in section 6.6, this $\mathbb{Z}_2$ symmetry can be broken using a single ancilla qubit. It follows that in this case semi-universality is achievable with one extra qubit.

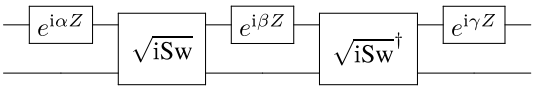
3.2.1. Semi-universality of gate set 1
First, consider the gate set

$$\sqrt{\text{iSWAP}}, \text{and } \exp(\text{i}\phi Z) : \phi \in (-\pi, \pi]\,. \tag{39}$$

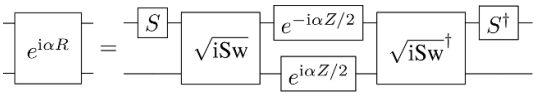
Equation (35) already shows that any unitary in $\mathcal{SV}_2^{\text{U(1)}}$ can be realized exactly with this gate set, using the following circuit:



where α, β and γ come from the Euler decomposition. It is also worth noting that one can save the number of gates at the cost of introducing relative phases between sectors with different Hamming weights, i.e. ,constructing an energy-conserving unitary outside $\mathcal{SV}_2^{U(1)}$. Note that in the decomposition of matrix Q in equation (35) $e^{\text{i}\alpha(Z_1-Z_2)} = e^{\text{i}2\alpha Z_1} e^{-\text{i}\alpha(Z_1+Z_2)}$, and the unitary $e^{-\text{i}\alpha(Z_1+Z_2)}$ commutes with all other unitaries in this decomposition and can be absorbed in the diagonal matrix D. Similar argument works for $e^{\text{i}\beta(Z_1-Z_2)}$ and $e^{\text{i}\gamma(Z_1-Z_2)}$. We conclude that, up to relative phases between sectors with different Hamming weights, any 2-qubit energy-conserving circuit has a decomposition as



For future applications, it is also useful to consider the following realization of the unitary $\exp(\text{i}\alpha R) = \exp(\text{i}\alpha[XX+YY]/2)$:



Therefore, any circuit that involves gates $\exp(\text{i}\alpha R)$ for arbitrary values of $\alpha \in (-\pi, \pi]$, can be transformed to a circuit that only involves gates $\sqrt{\text{iSWAP}}$ and single-qubit rotations around z, and this increases the number of entangling gates by, at most, a factor of 2.

3.2.2. Variation of gate set 1: Heisenberg interaction
A variant of the gate set in equation (39) is

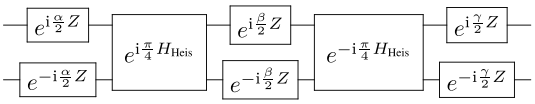
$$\exp(\text{i}\pi R_{\text{Heis}}/4), \text{and } \exp(\text{i}\phi Z) : \phi \in (-\pi, \pi]\,, \tag{40}$$

where $R_{\text{Heis}} := (X\otimes X + Y\otimes Y + Z\otimes Z)/2$ is the Heisenberg interaction. We observe that

$$\exp\left(\text{i}\pi R_{\text{Heis}}/4\right) = \sqrt{\text{iSWAP}}\exp\left(\text{i}\pi Z_1 Z_2/8\right) \tag{41a}$$

$$= \exp\left(\text{i}\pi Z_1 Z_2/8\right)\sqrt{\text{iSWAP}}\,. \tag{41b}$$

Since $\exp(\text{i}\pi Z_1 Z_2/8)$ commutes with the single-qubit rotations around z, in the above circuit we can replace $\sqrt{\text{iSWAP}}$ with $\exp(\text{i}\pi R_{\text{Heis}}/4)$. That is, any $Q \in \mathcal{SV}_2^{\text{U(1)}}$ can be realized with the following circuit



Hence, the gate set in equation (40) is semi-universal.

3.2.3. Semi-universality with gate set 2

Recall the map defined in equation (34), which gives the matrix representation of the component of 2-qubit operators in the sector with Hamming weight 1, relative to $|01\rangle, |10\rangle$ basis. Applying this map we find

$$H_{\text{int}} \longrightarrow H_{\text{int}}^{(1)} \tag{42a}$$

$$S_1 H_{\text{int}} S_1^\dagger \longrightarrow S H_{\text{int}}^{(1)} S^\dagger \tag{42b}$$

where $H_{\text{int}}^{(1)}$ is a 2×2 Hermitian matrix and $S_1 = S\otimes\mathbb{I}$ denotes the S gate on the first qubit. The fact that H_{int} is not diagonal in the computational basis implies that $H_{\text{int}}^{(1)}$ is not diagonal. Then, we apply the following lemma which is shown in appendix B.

Lemma 8. *Suppose H is a 2×2 non-diagonal Hermitian matrix. Then, any unitary $U\in SU(2)$ has a decomposition as*

$$U = \prod_{j=1}^{l} \left[\exp\left(\mathrm{i}\alpha_j H\right) S \exp\left(\mathrm{i}\beta_j H\right) S^\dagger\right] , \tag{43}$$

where $\alpha_j, \beta_j \in \mathbb{R}$, and the length of this sequence, l, is bounded by a constant independent of U.

This lemma together with the correspondence in equation (42) imply that any 2-qubit energy-conserving unitary $Q\in\mathcal{SV}_2^{U(1)}$, has a decomposition as

$$Q = \prod_{j=1}^{l} \left[\exp\left(\mathrm{i}\alpha_j H_{\text{int}}\right) S_1 \exp\left(\mathrm{i}\beta_j H_{\text{int}}\right) S_1^\dagger\right] \tag{44}$$

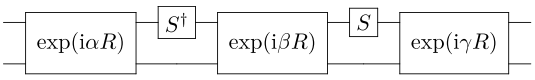
where l, the length of this sequence, does not depend on Q. We conclude that any $Q\in\mathcal{SV}_2^{U(1)}$ can be realized with Hamiltonian H_{int} and S gates, which means gate set 2 is semi-universal on $n=2$ qubits.

3.2.4. Example of gate set 2: XY interaction

For XY interaction, the realization of a general 2-qubit energy-conserving unitary $Q\in\mathcal{SV}_2^{U(1)}$ has a simple form. Applying the Euler decomposition to $Q^{(1)}$ defined in equation (33), this time for the x and y axes, we obtain

$$Q^{(1)} = e^{\mathrm{i}\gamma X} e^{\mathrm{i}\beta Y} e^{\mathrm{i}\alpha X} = e^{\mathrm{i}\gamma X} S e^{\mathrm{i}\beta X} S^\dagger e^{\mathrm{i}\alpha X} , \tag{45}$$

for $\gamma,\beta,\alpha\in(-\pi,\pi]$. Recall that by the correspondence in equation (34), in the subspace with Hamming weight 1 the action of $\exp(\mathrm{i}\alpha R)$ relative to the basis $|01\rangle$ and $|10\rangle$ is described by the unitary $\exp(\mathrm{i}\alpha X)$ and the action of S gate on the first qubit is $S = e^{\frac{\mathrm{i}\pi}{4}}\exp(-\mathrm{i}\pi Z/4)$. It follows that an arbitrary unitary $Q\in\mathcal{SV}_2^{U(1)}$ can be realized as by the circuit

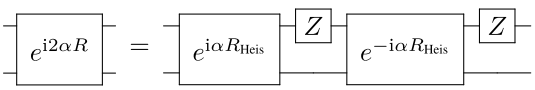


3.2.5. Example of gate set 2: Heisenberg interaction

Another canonical example of non-diagonal energy-conserving Hamiltonians is the Heisenberg interaction $R_{\text{Heis}} = (X\otimes X + Y\otimes Y + Z\otimes Z)/2$. In this case, again the decomposition in equation (44) finds a simple form, which can be seen by noting that

$$\begin{aligned} Z_1 \exp\left(-\mathrm{i}\alpha R_{\text{Heis}}\right) Z_1 \exp\left(\mathrm{i}\alpha R_{\text{Heis}}\right) &= Z_1 \exp\left(-\mathrm{i}\alpha R\right) Z_1 \exp\left(\mathrm{i}\alpha R\right) \\ &= \exp\left(\mathrm{i}2\alpha R\right) , \end{aligned} \tag{46}$$

where we have used the facts that $R_{\text{Heis}} = R + Z\otimes Z/2$, $[R, Z\otimes Z] = 0$, and $(Z\otimes\mathbb{I})R(Z\otimes\mathbb{I}) = -R$. The circuit diagram is shown as follows:



Therefore, gates $\exp(\mathrm{i}\alpha R_{\text{Heis}}) : \alpha\in(-\pi,\pi]$ together with S gate generate all gates in the previous example, which are semi-universal for $n=2$.

3.3. Single-qubit rotations around z (proof of theorem 1 for the special case of $n=1$)

Using the above results, it can be easily shown that any single-qubit rotation around z axis can be realized using the gate set 2 in theorem 1, i.e., S gates and $\exp(\mathrm{i}\alpha H_{\mathrm{int}}) : \alpha \in \mathbb{R}$, and a single ancilla qubit. To see this note that the family of diagonal unitaries

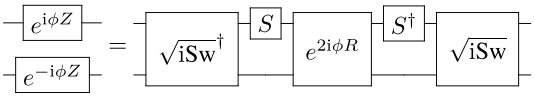
$$e^{\mathrm{i}\phi Z} \otimes e^{-\mathrm{i}\phi Z} \quad : \ \phi \in (-\pi, \pi] \,, \tag{47}$$

are in $\mathcal{SV}_2^{\mathrm{U}(1)}$ and therefore are realizable by the aforementioned gate set. Then, for any single-qubit state $|\psi\rangle \in \mathbb{C}^2$, we have

$$\left(e^{\mathrm{i}\phi Z} \otimes e^{-\mathrm{i}\phi Z}\right) |\psi\rangle \otimes |0\rangle_{\mathrm{anc}} = e^{-\mathrm{i}\phi} e^{\mathrm{i}\phi Z} |\psi\rangle \otimes |0\rangle_{\mathrm{anc}} \,, \tag{48}$$

which means that, up to a global phase, unitary $e^{\mathrm{i}\phi Z}$ can be realized on a system with $n=1$ qubit, using a single ancilla qubit. This proves theorem 1 for gate set 2 in the special case of $n=1$ qubit.

It is worth noting that in the case of XY interaction the following circuit realizes unitaries in equation (47)



4. 3-qubit energy-conserving unitaries

Next, we study 3-qubit energy-conserving unitaries and show how they can be realized with gates $\exp(\mathrm{i}\alpha R) : \alpha \in (-\pi, \pi]$ and S gate. These methods can then be generalized to implement energy-conserving unitaries on an arbitrary number of qubits. We start by constructing a useful 2-level 3-qubit energy-conserving unitary, using only combinations of iSWAP and iSWAP† gates.

4.1. A useful 2-level unitary: two controlled-Z gates

Using equation (31) one can easily show the identities

$$\mathrm{iSw}_{13}\ \mathrm{iSw}_{23}^{\dagger}\ \mathrm{iSw}_{12}\ \mathrm{iSw}_{23} = \exp\left(\mathrm{i}\frac{\pi}{4} Z_2 \left[Z_3 - Z_1\right]\right) \tag{49a}$$

$$\mathrm{iSw}_{13}\ \mathrm{iSw}_{23}\ \mathrm{iSw}_{12}\ \mathrm{iSw}_{23} = -\mathrm{i}\exp\left(\mathrm{i}\frac{\pi}{4} Z_2 \left[Z_1 + Z_3\right]\right) \,, \tag{49b}$$

where iSw_{ij} denotes iSWAP gate on qubits i and j, defined in equation (28). The second identity and similar other identities can be obtained by replacing iSw_{ij} with $\mathrm{iSw}_{ij}^{\dagger}$, or vice versa. It is worth noting that the specific combination of unitaries iSw_{ij} appearing in these identities has a nice interpretation in terms of the permutation group: applying equation (31) to all iSw_{ij} in the left-hand side of equation (49), the left-hand side becomes $\mathrm{Sw}_{13}\mathrm{Sw}_{23}\mathrm{Sw}_{12}\mathrm{Sw}_{23}$, up to a diagonal unitary in the computational basis, where Sw_{ij} denotes the SWAP unitary. However, this combination of swaps is equal to the identity operator, which can be seen from the basic properties of the permutation group. We conclude that $\mathrm{iSw}_{13}\mathrm{iSw}_{23}\mathrm{iSw}_{12}\mathrm{iSw}_{23}$ is equal to a unitary diagonal in the computational basis, that is determined by the right-hand side of equation (49).

The first identity implies that

$$\begin{aligned} \mathrm{iSw}_{13}\mathrm{iSw}_{23}^{\dagger}\mathrm{iSw}_{12}\mathrm{iSw}_{23} S_1^{\dagger} S_3 &= \exp(\mathrm{i}\frac{\pi}{4}\left[(Z_3 - Z_1)(Z_2 - I)\right]) \\ &= |0\rangle\langle 0|_2 \otimes \mathbb{I}_{13} + |1\rangle\langle 1|_2 \otimes Z_1 Z_3 \qquad (50a) \\ &= \mathrm{CZ}_{12}\mathrm{CZ}_{23} \,. \qquad (50b) \end{aligned}$$

See figure 3 for the corresponding circuit identity. This unitary is diagonal in the computational basis and is 2-level, i.e. it acts non-trivially only on states $|011\rangle$ and $|110\rangle$, and it gives -1 sign to both of these states. Note that using the second identity in equation (49) we can obtain a similar construction of this unitary using four iSWAP gates.

For future applications, we also note that equation (49) implies

$$F_{123} := \mathrm{iSw}_{13}\mathrm{iSw}_{23}^{\dagger}\mathrm{iSw}_{12} = \left(S_1 \otimes S_2^{\dagger} \otimes Z_3\right) \mathrm{CZ}_{12}\mathrm{Sw}_{23}. \tag{51}$$

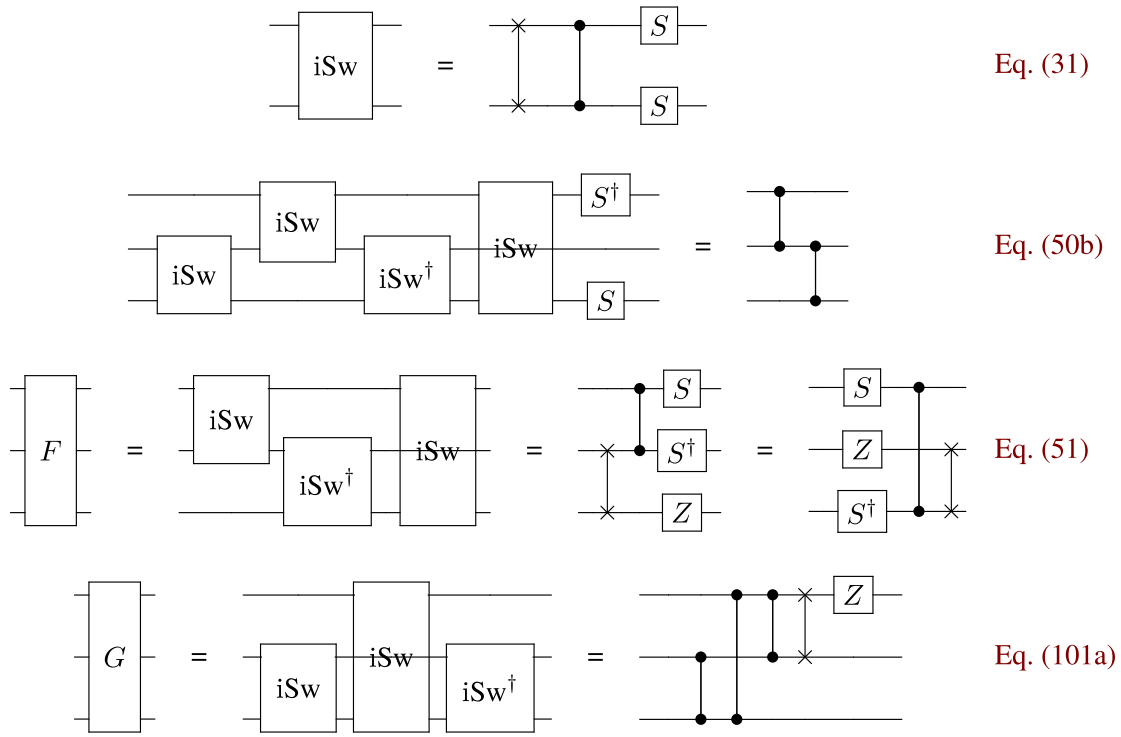


Figure 3. Summary of useful circuit identities involving iSWAP and S gates.

See figure 3 for the corresponding circuit identity. Also, note that changing each iSw gate to $\text{iSw}^\dagger$, or, vice versa, in the circuit on the left-hand side is equivalent to changing S gate to $S^\dagger$ and vice versa in the right-hand side. (This can be seen by considering the complex conjugate of both sides in the computational basis.)

4.1.1. The SWAP and controlled-Z gates with an ancilla qubit

Equation (50*b*) immediately gives a method for realizing the controlled-Z gate: Suppose we prepare qubit 1 in state $|0\rangle$. Then, the overall action of this circuit on qubits 2 and 3 will be CZ gate. Another important unitary transformation that can be realized in this way is the SWAP gate. In figure 1 we compare the circuit obtained in this way (the bottom circuit) with the standard way of implementing the SWAP unitary with 3 iSWAP gates, which is originally presented in [22]. As explained in the caption of figure 1, the realization of the SWAP gate with ancilla is more robust against certain types of errors, such as the fluctuations of the master clock. (It is also worth noting that the use of an ancilla has another advantage: by measuring the ancilla qubit at the end of the process in the z basis, it is possible to detect the presence of certain X errors in the circuit.)

In appendix C we present other examples of identities similar to equation (49). Such identities, for instance, imply that the gate controlled-$R_z(-\frac{\pi}{2})$ can be realized using 3 iSWAP, 3 $\sqrt{\text{iSWAP}}$ gates and an ancilla qubit.

4.2. General 2-level energy-conserving unitaries on 3 qubits

Next, we show how general 2-level energy-conserving unitaries in $\mathcal{SV}_3^{U(1)}$ can be realized. Here, we adapt the approach developed in [42] for quantum circuits with general Abelian symmetries to the case of U(1) symmetry. To achieve this we use the gate F_{123} defined in equation (51).

First, note that sandwiching $\exp(\mathrm{i}\theta R/2)$ on qubits 2 and 3 with F_{123} and $F_{123}^\dagger$ and using the facts that $S^\dagger \otimes S^\dagger$ and SWAP commute with R, we obtain

$$F_{123}^\dagger S_3^\dagger \exp\left(\mathrm{i}\frac{\theta}{2}R_{23}\right) S_3 F_{123} = |0\rangle\langle 0|_1 \otimes \exp\left(\mathrm{i}\frac{\theta}{2}R_{23}\right) + |1\rangle\langle 1|_1 \otimes \exp\left(-\mathrm{i}\frac{\theta}{2}R_{23}\right), \tag{52}$$

or, equivalently, the circuit identity

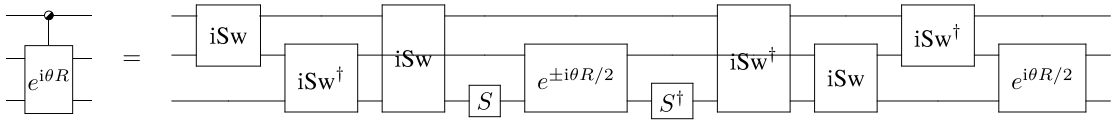
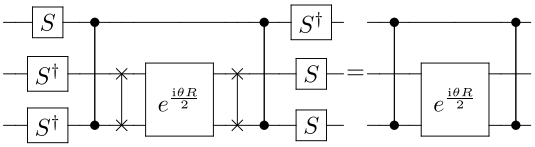


Figure 4. The circuit corresponding to equation (53): Assuming the gate in the middle (the fifth gate) is $\exp(-iR\theta/2)$ with $R=(X\otimes X+Y\otimes Y)/2$, this circuit implements controlled-$\exp(i\theta R)$, i.e. the 2-level 3-qubit unitary U_1 defined in equation (53). This family includes useful unitaries, such as controlled-iSWAP (corresponding to $\theta=\pi/2$, which means the fifth gate is $\sqrt{\text{iSWAP}}^\dagger$ and the tenth gate is $\sqrt{\text{iSWAP}}$) as well as the controlled-$\sqrt{\text{iSWAP}}$ (corresponding to $\theta=\pi/4$, which means the fifth gate is $\exp(-i\pi R/8)$ and the tenth gate is $\exp(i\pi R/8)$). On the other hand, when the gate in the middle is $\exp(+iR\theta/2)$, the circuit realizes U_0 in equation (53), which applies $\exp(i\theta R/2)$ when the control qubit is in state $|0\rangle$ rather than $|1\rangle$. As we explain in the next section, using this construction recursively, we can obtain all energy-conserving 2-level unitaries with determinant 1.



This implies

$$\exp\left(\mathrm{i}\frac{\theta}{2}R_{23}\right)F_{123}^\dagger S_3^\dagger \exp\left(\mathrm{i}\frac{(-1)^b\theta}{2}R_{23}\right)S_3F_{123}=|\bar{b}\rangle\langle\bar{b}|_1\otimes\mathbb{I}_{23}+|b\rangle\langle b|_1\otimes\exp\left(\mathrm{i}\theta R_{23}\right)=:U_b\ :\ b=0,1\,, \tag{53}$$

which corresponds to the circuit in figure 4, where $\bar{b}$ denotes the negation of b. This unitary is 2-level: it acts as $\exp(i\theta X)$ in the 2D subspace

$$\text{span}_{\mathbb{C}}\left\{|\widetilde{0}\rangle\equiv|b01\rangle\,,\ |\widetilde{1}\rangle\equiv|b10\rangle\right\}\ :\ b=0,1\,, \tag{54}$$

whereas it acts as the identity operator elsewhere. By sandwiching the second (or, third) qubit between $S^\dagger$ and S, we obtain the 2-level unitary

$$S_2U_bS_2^\dagger=S_3^\dagger U_bS_3=|b\rangle\langle b|\otimes\mathbb{I}+|\bar{b}\rangle\langle\bar{b}|\otimes\exp\left(\mathrm{i}\theta L_{23}\right)\ :\ b=0,1\,, \tag{55}$$

which acts as $\exp(i\theta Y)$ in the same 2D subspace, where we have defined

$$L=\frac{1}{2}\left(Y\otimes X-X\otimes Y\right)=\left(I\otimes S^\dagger\right)R\left(I\otimes S\right) \tag{56a}$$

$$=\mathrm{i}\left(|10\rangle\langle 01|-|01\rangle\langle 10|\right)\,. \tag{56b}$$

Therefore, we can realize both x and y rotations in the 2D subspace in equation (54). Furthermore, applying the Euler decomposition in equation (45) for SU(2) unitaries, we can obtain a general SU(2) unitary in this 2D subspace.

In conclusion, this way we can realize any 2-level 3-qubit energy-conserving unitary in the form of

$$\Lambda^b(V):=|\bar{b}\rangle\langle\bar{b}|\otimes\mathbb{I}+|b\rangle\langle b|\otimes V\ :\ V=\begin{pmatrix}1 & & \\ & V^{(1)} & \\ & & 1\end{pmatrix}\,, \tag{57}$$

for any $V^{(1)}\in\text{SU}(2)$, with any of the sets 1 and 2 in theorem 1. Here, $\Lambda^b(V)$ denotes a controlled gate that applies V, when the control qubit is b, namely a controlled-V gate for $b=1$ or an anti-controlled-V gate for $b=0$. The number of gates used in this construction is:

1. 32 gates in set 2 (choosing $H_{\text{int}}=R$), if we also allow the application of $S^\dagger$, or 40 gates if we implement $S^\dagger$ as S^3 in set 2;
2. 80 gates in set 1, allowing $\sqrt{\text{iSWAP}}^\dagger$ (one needs 6 gates to implement $\exp(\pm i\theta R)$; see section 3.2.1), or 152 if one implement iSWAP† as $\sqrt{\text{iSWAP}}^6$ and $\sqrt{\text{iSWAP}}^\dagger$ as $\sqrt{\text{iSWAP}}^7$.

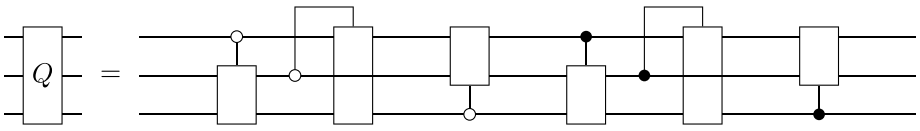


Figure 5. The circuit for implementing arbitrary unitaries in $\mathcal{SV}_3^{\mathrm{U}(1)}$, i.e. all 3-qubit energy-conserving unitaries with the property that the determinant of the component of unitary in each Hamming weight sector is 1. Here, each gate is in the form of equation (57) and hence can be realized by composing 3 circuits in the form of figure 4.

4.2.1. Example: controlled-iSWAP gate

A useful unitary, which plays a crucial role in our construction, is the 3-qubit gate controlled-iSWAP denoted as

$$\Lambda^1\left(\mathrm{iSWAP}\right) = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \mathrm{iSWAP}\ . \tag{58}$$

This unitary can be realized by the circuit in figure 4. In particular, this unitary corresponds to $\theta = \pi/2$, in which case the fifth and tenth gates in the circuit are $\sqrt{\mathrm{iSWAP}}^\dagger$ and $\sqrt{\mathrm{iSWAP}}$ gates, respectively.

In summary, controlled-iSWAP can be realized with

$$3\ \mathrm{iSWAP} + 3\ \mathrm{iSWAP}^\dagger + 1\ \sqrt{\mathrm{iSWAP}} + 1\ \sqrt{\mathrm{iSWAP}}^\dagger + 1S + 1S^\dagger.$$

4.3. Semi-universality on 3 qubits

By composing the above 2-level unitaries one can obtain any unitary $Q \in \mathcal{SV}_3^{\mathrm{U}(1)}$. Recall that any such unitary has a decomposition as

$$Q = \begin{pmatrix} 1 & & & \\ & Q^{(1)} & & \\ & & Q^{(2)} & \\ & & & 1 \end{pmatrix}, \tag{59}$$

where $Q^{(1)}, Q^{(2)} \in \mathrm{SU}(3)$ act on the subspaces with Hamming weights 1 and 2, respectively. According to lemma 12 to be shown later, any unitary in SU(3) can be decomposed into 3 2-level unitaries in SU(3). We conclude that any 3-qubit energy-conserving unitary $Q \in \mathcal{SV}_3^{\mathrm{U}(1)}$ has a decomposition in the form of figure 5, where each gate in this circuit is a 2-level energy-conserving unitary in the form of equation (57).

5. Synthesis of general energy-conserving unitaries with *XY* and *Z* interactions

In this section, we explain how general energy-conserving unitaries can be obtained from 2-level 3-qubit unitaries constructed in section 4.2. In the following, for any pair of bit strings $\mathbf{b}, \mathbf{b}' \in \{0,1\}^n$, $d(\mathbf{b},\mathbf{b}') := \sum_{j=1}^n |b_j - b'_j|$ denotes their Hamming distance, i.e., the number of bits taking different values in $\mathbf{b}$ and $\mathbf{b}'$.

Our construction, which is illustrated in figure 6, is based on the following steps:

1. Synthesizing 2-level special unitaries acting on any two basis elements $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$, with Hamming weights $w(\mathbf{b}) = w(\mathbf{b}')$, and Hamming distance $d(\mathbf{b},\mathbf{b}') = 2$ (see lemma 9).
2. Generalizing the previous step to the case of arbitrary Hamming distance $d(\mathbf{b},\mathbf{b}')$ (see corollary 11).
3. Synthesizing the subgroup $\mathcal{SV}_n^{\mathrm{U}(1)}$, defined in equation (13).
4. Synthesizing the group of all energy-conserving unitaries, denoted by $\mathcal{V}_n^{\mathrm{U}(1)}$.

Note that only in the last step, one needs to use a single ancilla qubit. It is also worth noting that some of the techniques that are used in the proofs of steps 1–3 follow similar constructions that have been developed previously in the quantum circuit theory for circuits without symmetry constraints (see [1, 2]). In step 4, where we use an ancilla qubit, we apply a technique that was developed previously in [42].

Step 1: basis elements with equal Hamming weights and Hamming distance 2

First, we show that by applying the construction in figure 4 recursively, we can realize any unitary in the form $V = U^{(1)}(\mathbf{b},\mathbf{b}')$, defined in equation (21), where $d(\mathbf{b},\mathbf{b}') = 2$, $w(\mathbf{b}) = w(\mathbf{b}')$, and $U^{(1)}(\mathbf{b},\mathbf{b}')$ acts unitarily on the 2-dimensional subspace spanned by $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$ and satisfies

$$\det\left(V\right) = \det\left(U^{(1)}\left(\mathbf{b},\mathbf{b}'\right)\right) = 1\ . \tag{60}$$

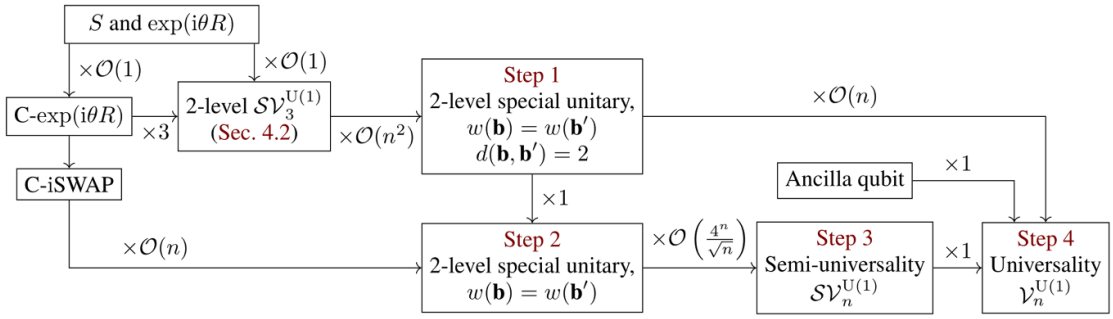


Figure 6. Overview of the method for synthesizing general energy-conserving unitaries. The number on the arrow pointing from one box A to another box B indicates the number of uses of A in the construction of B. C-exp(iθR) denotes controlled-exp(iθR) which can be realized with the circuit in figure 4.

Here, we denote the 2×2 unitary as $U^{(1)}$ since, as we will see below in equation (62), we will think of it as the component of a 2-qubit unitary U in the sector with Hamming weight 1.

For simplicity of presentation, we relabel the qubits such that the common bits of $\mathbf{b}$ and $\mathbf{b}'$ are labeled from 1 to $k=n-2$, and the two different bits of $\mathbf{b}$ and $\mathbf{b}'$ are labeled $n-1$ and n. Rearranging the qubits in this way, noting that $\mathbf{b}$ and $\mathbf{b}'$ have equal Hamming weights and Hamming distance 2, we can write

$$|\mathbf{b}\rangle = |\mathbf{c}\rangle|0\rangle|1\rangle\,, \quad |\mathbf{b}'\rangle = |\mathbf{c}\rangle|1\rangle|0\rangle\,, \tag{61}$$

where $\mathbf{c}\in\{0,1\}^{n-2}$ contains the common bits of $\mathbf{b}$ and $\mathbf{b}'$. With this definition the target gate $U^{(1)}(\mathbf{b},\mathbf{b}')$ can be written as a multi-controlled $\mathcal{SV}_2^{\mathrm{U}(1)}$ gate as

$$U^{(1)}\left(\mathbf{b},\mathbf{b}'\right) = \Lambda^{\mathbf{c}}\left(U\right)\,, \quad U = \begin{pmatrix} 1 & & \\ & U^{(1)} & \\ & & 1 \end{pmatrix}\,, \tag{62}$$

where

$$\Lambda^{\mathbf{c}}\left(U\right) := \sum_{\mathbf{c}'\neq\mathbf{c}} |\mathbf{c}'\rangle\langle\mathbf{c}'|\otimes\mathbb{I} + |\mathbf{c}\rangle\langle\mathbf{c}|\otimes U\,, \tag{63}$$

is a controlled-unitary with control string $\mathbf{c}$.

Now we use a recursive construction of the circuit for $\Lambda^{\mathbf{c}}(U)$. (Here, we are applying a technique that was originally used in [1, 2] for general quantum circuits.) We decompose $\mathbf{c}$ as $\mathbf{c}=\mathbf{c}_1\mathbf{c}_2$, where $\mathbf{c}_1$ has length $\lfloor k/2\rfloor$ and $\mathbf{c}_2$ has length $\lceil k/2\rceil$. Since $U^{(1)}\in\mathrm{SU}(2)$, there exists operators $A^{(1)},B^{(1)}\in\mathrm{SU}(2)$ such that $A^{(1)}B^{(1)}A^{(1)\dagger}B^{(1)\dagger}=U^{(1)}$. (To see this note that a general SU(2) unitary $U^{(1)}$ is equal to $\exp(\mathrm{i}\theta Z)$, up to a change of basis, as $U^{(1)}=W\exp(\mathrm{i}\theta Z)W^\dagger$. Then, one can choose $A^{(1)}=W\exp(\mathrm{i}\theta Z/2)W^\dagger$ and $B^{(1)}=\mathrm{i}WXW^\dagger$.)

Let $A:=1\oplus A^{(1)}\oplus 1$ and $B:=1\oplus B^{(1)}\oplus 1$ be the extensions of $A^{(1)}$ and $B^{(1)}$ to 2-qubit unitaries, in the same way U extends $U^{(1)}$ to a 2-qubit unitary. Then $ABA^\dagger B^\dagger=U$. We can therefore decompose $\Lambda^{\mathbf{c}}(U)$ as

$$\Lambda^{\mathbf{c}}\left(U\right) = \Lambda^{\mathbf{c}_1}\left(A\right)\Lambda^{\mathbf{c}_2}\left(B\right)\Lambda^{\mathbf{c}_1}\left(A^\dagger\right)\Lambda^{\mathbf{c}_2}\left(B^\dagger\right)\,, \tag{64}$$

with the first $\lfloor k/2\rfloor$ qubits being the control qubits for $\Lambda^{\mathbf{c}_1}(A)$ and $\Lambda^{\mathbf{c}_1}(A^\dagger)$, and the next $\lceil k/2\rceil$ qubits being the control qubits for $\Lambda^{\mathbf{c}_2}(B)$ and $\Lambda^{\mathbf{c}_2}(B^\dagger)$, as shown in figure 7.

With this decomposition, we realize $\Lambda^{\mathbf{c}}(U)$ with 4 controlled-unitaries, namely $\Lambda^{\mathbf{c}_1}(A),\Lambda^{\mathbf{c}_2}(B),\Lambda^{\mathbf{c}_1}(A^\dagger)$ and $\Lambda^{\mathbf{c}_2}(B^\dagger)$, each of which has $\lfloor k/2\rfloor$ or $\lceil k/2\rceil$ number of control qubits. We can recursively decompose each of the 4 unitaries into gates with less number of control qubits, and finally reach the $k=1$ case. Note that when $k=1$, the single-controlled gate $\Lambda^{\mathbf{c}}(U)$ is a 2-level $\mathcal{SV}_3^{\mathrm{U}(1)}$ gate whose implementation has been addressed in section 4.2. This gives the base case of the recursion.

The number of 2-level $\mathcal{SV}_3^{\mathrm{U}(1)}$ gates in this recursive construction is given by the following lemma, which applies an argument previously used in the quantum circuit theory [10].

Lemma 9. *For any pair of bit strings $\boldsymbol{b},\boldsymbol{b}'\in\{0,1\}^n$ with equal Hamming weights and Hamming distance 2, any 2-level unitary with determinant 1, which acts non-trivially only in the subspace spanned by $|\boldsymbol{b}\rangle$ and $|\boldsymbol{b}'\rangle$ can be realized with no more than $9n^2/8$ number of 3-qubit controlled gates in equation (53), which all belong to $\mathcal{SV}_3^{\mathrm{U}(1)}$ and can be realized with the circuit in figure 4.*

[10] See chapter 8.1.3 of [1], or exercise 4.30 of [2] .

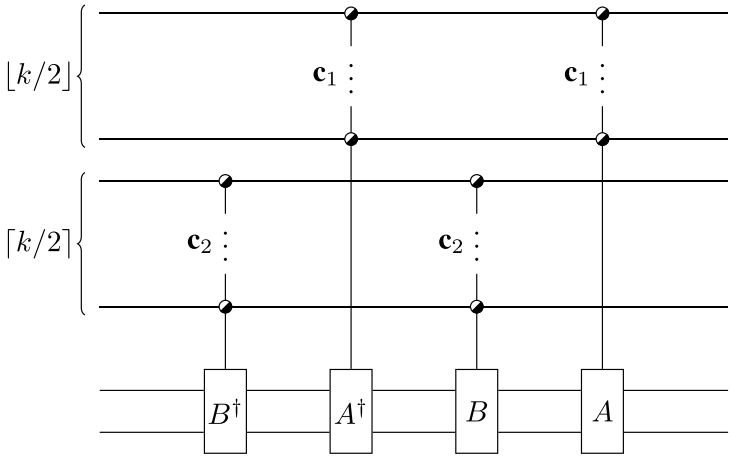


Figure 7. Circuit of a controlled gate with k control qubits (see equation (64)).

Proof. Let $T(k)$ be the number of 3-qubit controlled gates used to implement a gate in the form of $\Lambda^{\mathbf{c}}(U)$ with $|\mathbf{c}| = k$ control qubits. Based on the circuit in figure 7, we obtain the recursive relation:

$$T(k) = 2T\left(\left\lfloor \frac{k}{2} \right\rfloor\right) + 2T\left(\left\lceil \frac{k}{2} \right\rceil\right),\ k \geqslant 2 \tag{65a}$$

$$T(1) = 1. \tag{65b}$$

We will prove by induction that

$$T(k) \leqslant \begin{cases} \left(9k^2 - 1\right)/8 & k \text{ is odd} \\ \left(9k^2 - 4\right)/8 & k \text{ is even.} \end{cases} \tag{66}$$

$T(1) = 1, T(2) = 4$ satisfy the inequality. For $k \geqslant 3$, assuming the inequality holds for all smaller k,

1. If k is even, $T(k) = 4T(k/2) \leqslant 4 \times \frac{9(k/2)^2 - 1}{8} = \frac{9k^2 - 4}{8}$;
2. If k is odd, then one of $\lfloor k/2 \rfloor = \frac{k-1}{2}$ and $\lceil k/2 \rceil = \frac{k+1}{2}$ is even, and the other one is odd. In either case, $T(k) = 2T\left(\frac{k-1}{2}\right) + 2T\left(\frac{k+1}{2}\right) \leqslant 2 \times \left(\frac{9(\frac{k-1}{2})^2}{8} + \frac{9(\frac{k+1}{2})^2}{8} - \frac{1}{8} - \frac{4}{8}\right) = \frac{9k^2-1}{8}$.

Therefore, equation (66) holds for every $k \geqslant 1$.

To implement an n-qubit 2-level gate on the subspace spanned by $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$, we need to implement a controlled gate with $n-2$ control qubits. The number of 3-qubit gates used is therefore $T(n-2) \leqslant 9n^2/8$. □

Step 2: basis elements with equal Hamming weights

Next, using the construction developed in step 1, we show how one can implement general 2-level unitaries that preserve the Hamming weight of states in the computational basis. The technique used here is a variation of a similar technique that has been previously used for general quantum circuits [1].

Lemma 10. *For a system with n qubits, consider a 2-level unitary transformation V that acts trivially on the subspace orthogonal to $|\boldsymbol{b}\rangle, |\boldsymbol{b}'\rangle$, where $\boldsymbol{b}, \boldsymbol{b}' \in \{0,1\}^n$ are a pair of bit strings with equal Hamming weights. Any such unitary can be decomposed as*

$$V = K^\dagger W K\,, \tag{67}$$

where W is also a 2-level unitary that acts on the subspace spanned by $|\boldsymbol{b}'\rangle$ and $|\boldsymbol{b}''\rangle$, where $\boldsymbol{b}', \boldsymbol{b}'' \in \{0,1\}^n$ have equal Hamming weights and have Hamming distance $d(\boldsymbol{b}', \boldsymbol{b}'') = 2$, and unitary K can be realized as a sequence of $d(\boldsymbol{b}, \boldsymbol{b}')/2 - 1$ controlled-iSWAP gates.

We conclude that

Corollary 11. *Any 2-level unitary with determinant 1, acting on a pair of basis elements $|\boldsymbol{b}\rangle$ and $|\boldsymbol{b}'\rangle$ with equal Hamming weights can be realized with $d(\boldsymbol{b}, \boldsymbol{b}')/2 - 1$ controlled-iSWAP, $d(\boldsymbol{b}, \boldsymbol{b}')/2 - 1$ controlled-iSWAP† gates, plus one 2-level gate of the type constructed in step 1. In total this requires $\mathcal{O}(n^2 + d(\boldsymbol{b}, \boldsymbol{b}')) = \mathcal{O}(n^2)$ of gates in any of the gate sets 1 and 2 in theorem 1.*

Proof. (Lemma 10) For any pair of bit strings $\mathbf{b}$ and $\mathbf{b}'$, there exists a sequence of n-bit strings as

$$\mathbf{b} = \mathbf{b}_0 \to \mathbf{b}_1 \to \cdots \to \mathbf{b}_t = \mathbf{b}' \,, \tag{68}$$

such that (i) all bit strings in this sequence have equal Hamming weights, (ii) For any pair of consecutive bit strings $\mathbf{b}_j$ and $\mathbf{b}_{j+1}$ the Hamming distance is 2, and (iii) The length of this sequence is $t+1$, where $t = d(\mathbf{b},\mathbf{b}')/2$.

This sequence of bit strings is realized by applying $t+1$ swaps that can be determined as follows: Suppose we specify each bit by its label (i.e., its location) which is an integer $i \in \{1,\cdots,n\}$, such that $\mathbf{b} = b_1 \cdots b_i \cdots b_n$. Consider the bits in which $\mathbf{b}$ and $\mathbf{b}'$ take different values. There are $d(\mathbf{b},\mathbf{b}')$ such bits, where $d(\mathbf{b},\mathbf{b}')$ is the Hamming distance of $\mathbf{b}$ and $\mathbf{b}'$, which is an even integer because they have equal Hamming weights. These bits can be partitioned into two subsets, each having size $t := d(\mathbf{b},\mathbf{b}')/2$ with the following property: bits in the first subset take value 0 in $\mathbf{b}$ and take value 1 in $\mathbf{b}'$. And, the bits in the second subset take value 1 in $\mathbf{b}$ and take value 0 in $\mathbf{b}'$. More precisely, let

$$l_1, l_2, \cdots, l_t$$

be t distinct integers in $\{1,\cdots,n\}$ where $b_{l_j} = 1$ and $b'_{l_j} = 0$ for $j = 1,\ldots,t$. Similarly, let

$$r_1, r_2, \cdots, r_t$$

be t distinct integers in $\{1,\cdots,n\}$ where $b_{r_j} = 0$ and $b'_{r_j} = 1$ for $j = 1,\ldots,t$. Then, define

$$|\mathbf{b}_j\rangle = \mathrm{SWAP}_{l_j,r_j}|\mathbf{b}_{j-1}\rangle \,, \tag{69}$$

where $|\mathbf{b}_0\rangle = |\mathbf{b}\rangle$, and SWAP_{l_j,r_j} is the SWAP unitary acting on qubits l_j and r_j. In this way, we obtain a sequence of bit strings in the form of equation (68) satisfying the desired properties.

In general, the gate SWAP_{l_j,r_j} acts non-trivially on state $|\mathbf{b}'\rangle$. Now, suppose rather than this gate, we use controlled-iSWAP, with the control qubit chosen to differentiate $|\mathbf{b}'\rangle$ and $|\mathbf{b}_{j-1}\rangle$. Namely, we choose

$$\Lambda^1_{l_{j+1}}\left(\mathrm{iSw}_{l_j,r_j}\right)|\mathbf{b}_{j-1}\rangle = \mathrm{i}|\mathbf{b}_j\rangle \tag{70a}$$

$$\Lambda^1_{l_{j+1}}\left(\mathrm{iSw}_{l_j,r_j}\right)|\mathbf{b}'\rangle = |\mathbf{b}'\rangle \,, \tag{70b}$$

where the unitary in the left-hand side is controlled-iSWAP, i.e.

$$\Lambda^1_{l_{j+1}}\left(\mathrm{iSw}_{l_j,r_j}\right) = |0\rangle\langle 0|_{l_{j+1}} \otimes \mathbb{I}_{l_j,r_j} + |1\rangle\langle 1|_{l_{j+1}} \otimes \mathrm{iSw}_{l_j,r_j} \,, \tag{71}$$

where l_{j+1} is the control qubit, and l_j and r_j are the target qubits. This gate acts trivially on state $\mathbf{b}'$ since by the above definition, $b'_{l_{j+1}} = 0$ for every $j = 0,\ldots,t-1$.

Then, defining

$$K = \Lambda^1_{l_t}\left(\mathrm{iSw}_{l_{t-1},r_{t-1}}\right)\cdots\cdots\Lambda^1_{l_3}\left(\mathrm{iSw}_{l_2,r_2}\right)\Lambda^1_{l_2}\left(\mathrm{iSw}_{l_1,r_1}\right) \,, \tag{72}$$

we find

$$K|\mathbf{b}\rangle = \mathrm{i}^{t-1}|\mathbf{b}_{t-1}\rangle \tag{73a}$$

$$K|\mathbf{b}'\rangle = |\mathbf{b}'\rangle \,. \tag{73b}$$

Therefore, by defining

$$W = KVK^\dagger \,, \tag{74}$$

we find that W is a 2-level unitary acting on the subspace spanned by $|\mathbf{b}''\rangle = |\mathbf{b}_{t-1}\rangle$ and $|\mathbf{b}'\rangle$, where $d(\mathbf{b}',\mathbf{b}'') = 2$. More explicitly, if $V = U(\mathbf{b},\mathbf{b}')$ with

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,, \tag{75}$$

then $W = \widetilde{U}(\mathbf{b}'',\mathbf{b}')$ with

$$\widetilde{U} = \begin{pmatrix} \mathrm{i}^{t-1} & \\ & 1 \end{pmatrix} U \begin{pmatrix} \mathrm{i}^{1-t} & \\ & 1 \end{pmatrix} = \begin{pmatrix} a & \mathrm{i}^{t-1}b \\ \mathrm{i}^{1-t}c & d \end{pmatrix} . \tag{76}$$

This completes the proof of lemma 10. □

Step 3: semi-universality

As defined in equation (13), we call a gate set semi-universal if it generates all unitaries in $\mathcal{SV}_n^{\mathrm{U}(1)}$ for all n, i.e. all energy-conserving unitaries $V=\bigoplus_{m=0}^{n}V^{(m)}$ satisfying the additional constraint $\det(V^{(m)})=1:m=0,\cdots,n$. It can be easily shown that any such unitary can be decomposed into a sequence of 2-level energy-conserving unitaries that satisfy the same constraint. To show this we use the following result.

Lemma 12 ([57]). *Given any basis for $\mathbb{C}^d$, any unitary in $SU(d)$ can be decomposed into a product of no more than $d(d-1)/2$ unitaries in $SU(d)$ that are 2-level with respect to this basis.*

This lemma is a slight variation of a similar result in [57], which does not impose any constraints on the determinant of 2-level unitaries (see also [1, 2]). For completeness, we present the proof in appendix D.

Recall that in the decomposition $V=\bigoplus_{m=0}^{n}V^{(m)}$, unitary $V^{(m)}$ acts on the subspace with Hamming weight m, which has dimension $\binom{n}{m}$. Then, applying this lemma, we find that $V^{(m)}$ can be realized with

$$\frac{1}{2}\binom{n}{m}\times\left[\binom{n}{m}-1\right]$$

2-level energy-conserving unitaries, each of which acts on two computational basis vectors in the subspace of Hamming weight m, has determinant 1, and can be constructed with the method in step 2.

In conclusion, the total number of 2-level gates needed to implement V is

$$\frac{1}{2}\sum_{m=1}^{n-1}\binom{n}{m}\left[\binom{n}{m}-1\right]=\frac{\binom{2n}{n}-2^n}{2}\approx\frac{4^n}{2\sqrt{\pi n}}\,, \tag{77}$$

where $\approx$ means the ratio of two sides goes to 1, in the limit $n\to\infty$.

Combining this with corollary 11 we conclude that

Proposition 13. *Any energy-conserving unitary in $\mathcal{SV}_n^{U(1)}$ can be realized with $\mathcal{O}(4^n n^{3/2})$ gates in any of the gate sets* 1 *and* 2 *in theorem* 1*, without ancillary qubits.*

Here, to count the number of gates, one can use the diagram in figure 6: Recall that controlled-iSWAP can be realized using the circuit in figure 4, which requires $\mathcal{O}(1)$ gates in one of the aforementioned gate sets. Therefore, the total required number of elementary gates is

$$\left[\mathcal{O}\left(n^2\right)+\mathcal{O}\left(n\right)\right]\times\mathcal{O}\left(\frac{4^n}{\sqrt{n}}\right)=\mathcal{O}\left(4^n n^{3/2}\right)\,. \tag{78}$$

Note that, in general, if the desired unitary acts non-trivially only on a subspace spanned by $D\leqslant 2^n$ basis elements, then from lemma 12 it can be decomposed into no more than $D(D-1)=\mathcal{O}(D^2)$ 2-level unitaries. Hence, any such unitary can be implemented with $[\mathcal{O}(n^2)+\mathcal{O}(n)]\times\mathcal{O}(D^2)=\mathcal{O}(n^2D^2)$ elementary gates in theorem 1.

Step 4: universality

Finally, applying a mechanism developed in [42], we show how one can achieve universality using a single ancillary qubit. It is worth noting that this technique can be applied to symmetric circuit with any arbitrary Abelian symmetry (see lemma 5 of [42]).

Let $|\mathbf{b}\rangle$ be an arbitrary element of the computational basis $\{|0\rangle,|1\rangle\}^{\otimes n}$, other than $|0\rangle^{\otimes n}$. Then, there is (at least) one qubit with reduced state $|1\rangle$. Let $|\mathbf{b}'\rangle$ be the n-qubit state obtained from $|\mathbf{b}\rangle$ by changing the state of this qubit from $|1\rangle$ to $|0\rangle$. Define the Hamiltonian

$$\widetilde{H}_{\mathbf{b}}=|\mathbf{b}\rangle\langle\mathbf{b}|\otimes|0\rangle\langle 0|_{\mathrm{anc}}-|\mathbf{b}'\rangle\langle\mathbf{b}'|\otimes|1\rangle\langle 1|_{\mathrm{anc}}\,. \tag{79}$$

Note that $(n+1)$-qubit states $|\mathbf{b}\rangle|0\rangle_{\mathrm{anc}}$ and $|\mathbf{b}'\rangle|1\rangle_{\mathrm{anc}}$ have equal Hamming weights and their Hamming distance is 2. Furthermore, this Hamiltonian is traceless, which means $\exp(\mathrm{i}\widetilde{H}_{\mathbf{b}}\theta)$ has determinant 1. It follows from step 1 that this 2-level energy-conserving unitary can be implemented without ancilla. Implementing this unitary on the system and ancilla we obtain state

$$\exp\left[\mathrm{i}\widetilde{H}_{\mathbf{b}}\theta\right]\left(|\psi\rangle\otimes|0\rangle_{\mathrm{anc}}\right)=\left(\exp\left[\mathrm{i}\theta|\mathbf{b}\rangle\langle\mathbf{b}|\right]|\psi\rangle\right)\otimes|0\rangle_{\mathrm{anc}}\,, \tag{80}$$

where $|\psi\rangle\in(\mathbb{C}^2)^{\otimes n}$ is the initial state of n qubits in the system. Since the state of ancilla qubit remains unchanged, we can reuse again in a similar fashion. Therefore, in this way we can realize the unitary

$\exp(\mathrm{i}|\mathbf{b}\rangle\langle\mathbf{b}|\theta)$. We can apply this procedure to any sector, except the sector with Hamming weight $m=0$, which corresponds to state $|0\rangle^{\otimes n}$. It follows that using $(n-1)$ 2-level unitaries we can realize any unitary in the form

$$D = |0\rangle\langle 0|^{\otimes n} + \sum_{m=1}^{n} \exp(\mathrm{i}\theta_m)\,|\mathbf{b}_m\rangle\langle\mathbf{b}_m|\,, \tag{81}$$

for any arbitrary $\theta_1,\ldots,\theta_n \in (-\pi,\pi]$, where $|\mathbf{b}_m\rangle$ is an arbitrarily selected basis element in the sector with Hamming weight m.

Finally, recall that any energy-conserving unitary V can be decomposed as $V = e^{\mathrm{i}\theta_0} DQ$, where $e^{\mathrm{i}\theta_0} = V^{(0)} = \langle 0|^{\otimes n} V |0\rangle^{\otimes n}$, D is in the form of equation (81), with $\theta_m = \arg(\det(V^{(m)})) - \theta_0$ for $1 \leqslant m \leqslant n$, and $Q \in \mathcal{SV}_n^{\mathrm{U}(1)}$. As mentioned above, D can be implemented with an ancillary qubit. Furthermore, in the previous section we saw how $Q \in \mathcal{SV}_n^{\mathrm{U}(1)}$ can be implemented without ancillary qubits.

Note that the unitary generated by Hamiltonian in equation (79) is of the type we studied in step 1 of this construction, and therefore can be realized with no more than $9(n+1)^2/8$ gates ($n+1$ qubits including one ancilla qubit) in $\mathcal{SV}_3^{\mathrm{U}(1)}$. In total, this step requires $\mathcal{O}(n^2)$ elementary gates.

In conclusion, any energy-conserving unitary can be realized, up to a global phase, with one ancillary qubit. Furthermore, using the diagram in figure 6 and equation (78), we find that this construction requires

$$\mathcal{O}\left(4^n n^{3/2}\right) + \mathcal{O}\left(n^2\right)(n-1) = \mathcal{O}\left(4^n n^{3/2}\right)\,, \tag{82}$$

gates in one of these elementary gate sets, which completes the proof of theorem 1 for sets 1 and 2.

6. Realizing all energy-conserving unitaries with *XY* interaction alone

So far in this paper, we have considered circuits that contain both XY interaction as well as single-qubit rotations around the z axis. In this section, we focus on synthesizing quantum circuits that only contain XY interaction. In this case, the overall realized unitary V on the system respects the $\mathbb{Z}_2$ symmetry corresponding to flipping all the qubits in the system. That is,

$$X^{\otimes n} V X^{\otimes n} = V\,, \tag{83}$$

which follows from the fact that unitary $\exp(\mathrm{i}\theta R_{ij})$ satisfies this symmetry for all qubit pairs i and j and all $\theta \in (-\pi,\pi]$. Interestingly, theorem 4, which is proven below, implies that this $\mathbb{Z}_2$ symmetry together with the U(1) symmetry corresponding to energy conservation, namely

$$\Big[V, \sum_{j=1}^{n} Z_j\Big] = 0\,, \tag{84}$$

characterize the set of realizable unitaries, up to additional constraints on the overall phases in each invariant subspace: First, for any realizable unitary V,

$$\det\left(V^{(m)}\right) = 1 \quad : m = 0,\cdots,n\,, \tag{85}$$

where $V^{(m)}$ is the component of $V = \bigoplus_{m=0}^{n} V^{(m)}$ in the sector with Hamming weight m. Second, in the case of even n,

$$\det\left(V^{(n/2,\pm)}\right) = 1\,, \tag{86}$$

where, as defined in theorem 4, $V^{(n/2,\pm)}$ is the component of $V^{(n/2)}$ in the eigensubspace of $X^{\otimes n}$ with eigenvalue ± 1. In the following, $\mathcal{G}_n$ denotes the group of n-qubit unitaries satisfying these four conditions, i.e., equations (83)–(86).

The necessity of conditions in equations (85) and (86) are discussed in [23, 42] and for completeness is also explained in appendix A and lemma 16. (Briefly, they follow from the fact that $\mathrm{Tr}(\Pi^{(m)}R_{ij})=0$ for all $m=0,\cdots,n$ where $\Pi^{(m)}$ is the projector to the sector with Hamming weight m. Furthermore, for $n\geq 3$, it holds that $\mathrm{Tr}(X^{\otimes n}R_{ij})=0$.)

In the following, we present explicit circuit synthesis methods for implementing general unitary V satisfying the above 4 conditions using XY interaction. This, in particular, completes the proofs of theorem 4 and the main part of theorem 1 for the case of gate set 3.

6.1. Overview of the synthesis method: 4-level unitaries

Recall that the method we used in section 5 decomposes a general energy-conserving unitary to a sequence of 2-level energy-conserving unitaries, which in general do not respect the $\mathbb{Z}_2$ symmetry in equation (83) and hence cannot be realized with XY interaction alone. Hence, we consider a natural extension of 2-level unitaries that satisfy the $\mathbb{Z}_2$ symmetry, namely 4-level unitaries. In the following, for any pair of distinct bit strings $\mathbf{b},\mathbf{b}'\in\{0,1\}^n$, define the Pauli X and Y operators in the subspace spanned by $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$ as

$$X(\mathbf{b},\mathbf{b}'):=|\mathbf{b}\rangle\langle\mathbf{b}'|+|\mathbf{b}'\rangle\langle\mathbf{b}|\,, \tag{87a}$$

$$Y(\mathbf{b},\mathbf{b}'):=\mathrm{i}\left(|\mathbf{b}'\rangle\langle\mathbf{b}|-|\mathbf{b}\rangle\langle\mathbf{b}'|\right)\,. \tag{87b}$$

Let $\overline{\mathbf{b}}$ be the bitwise negation of bit $\mathbf{b}$, which means

$$|\overline{\mathbf{b}}\rangle=X^{\otimes n}|\mathbf{b}\rangle\,. \tag{88}$$

Then, for all $\mathbf{b},\mathbf{b}'\in\{0,1\}^n$ with $\mathbf{b}'\neq\mathbf{b},\overline{\mathbf{b}}$ and $\theta\in(-\pi,\pi]$, consider the following 4-level unitaries

$$\mathbb{R}_x(\theta,\mathbf{b},\mathbf{b}'):=\exp\left[\mathrm{i}\theta X(\mathbf{b},\mathbf{b}')\right]\exp\left[\mathrm{i}\theta X\left(\overline{\mathbf{b}},\overline{\mathbf{b}'}\right)\right] \tag{89a}$$

$$\mathbb{R}_y(\theta,\mathbf{b},\mathbf{b}'):=\exp\left[\mathrm{i}\theta Y(\mathbf{b},\mathbf{b}')\right]\exp\left[\mathrm{i}\theta Y\left(\overline{\mathbf{b}},\overline{\mathbf{b}'}\right)\right]\,. \tag{89b}$$

They clearly respect the $\mathbb{Z}_2$ symmetry in equation (83), and if $\mathbf{b}$ and $\mathbf{b}'$ have equal Hamming weights, i.e.

$$w(\mathbf{b})=w(\mathbf{b}')\,, \tag{90}$$

then they are also energy-conserving.

Note that we have excluded the case of $\mathbf{b}'=\overline{\mathbf{b}}$. In general, $w(\overline{\mathbf{b}})=n-w(\mathbf{b})$, which means unitaries in equation (89) corresponding to the case of $\mathbf{b}'=\overline{\mathbf{b}}$ are not energy-conserving, unless n is even and $w(\overline{\mathbf{b}})=w(\mathbf{b})=n/2$. We call the special case of Hamming weight $m=n/2$ the 'half-filled sector' and study it separately in section 6.4. In this case, indeed there exists a family of 2-level energy-conserving unitaries that respect the $\mathbb{Z}_2$ symmetry, as well as the condition $\det(V^{(n/2)})=1$, namely

$$\exp\left[\mathrm{i}\theta X(\mathbf{b},\overline{\mathbf{b}})\right]=\mathbb{R}_x\left(\frac{\theta}{2},\mathbf{b},\overline{\mathbf{b}}\right)\,, \tag{91}$$

which corresponds to the special case of $\mathbf{b}'=\overline{\mathbf{b}}$ in equation (89*a*). Is this family of unitaries realizable using XY interaction alone?

Interestingly, the answer is no! While the unitary in equation (91) respects the 3 conditions in equations (83)–(85), since $\det(V^{(n/2,\pm)})=e^{\pm\mathrm{i}\theta}$, unless $\theta=0$ it does not respect the condition in equation (86). (Note that this is indeed the generalization of the example we discussed in the introduction, below theorem 4.) It is also worth noting that, unitaries in equation (91) are the only 2-level unitaries that satisfy the 3 conditions in equations (83)–(85). In conclusion, in the following we always restrict our attention to 4-level unitaries in equation (89), i.e.,we impose the condition $\mathbf{b}'\neq\overline{\mathbf{b}}$.

In the following, we first show how the unitaries in equation (89) can be realized with XY interaction alone, and then use them to construct all unitaries respecting the four conditions in theorem 4. In particular, in section 6.2 we show that the circuits for 4-level unitaries in equation (89) can be obtained based on the circuits for 2-level unitaries $\exp[\mathrm{i}\theta X(\mathbf{b},\mathbf{b}')]$ and $\exp[\mathrm{i}\theta Y(\mathbf{b},\mathbf{b}')]$, which were found in section 4.

The restriction to XY interactions alone makes the constructions in this section more complicated and slightly different from the constructions in section 5. However, the presence of $\mathbb{Z}_2$ symmetry also leads to a simplification, which can be understood in terms of the following lemma.

Lemma 14. *Suppose a pair of n-qubit energy-conserving unitaries $V=\bigoplus_{m=0}^{n}V^{(m)}$ and $W=\bigoplus_{m=0}^{n}W^{(m)}$ both respect the $\mathbb{Z}_2$ symmetry in equation (83). Then $V=W$ if, and only if*

$$V^{(m)}=W^{(m)}\qquad:m=0,\cdots,\lfloor\frac{n}{2}\rfloor\,. \tag{92}$$

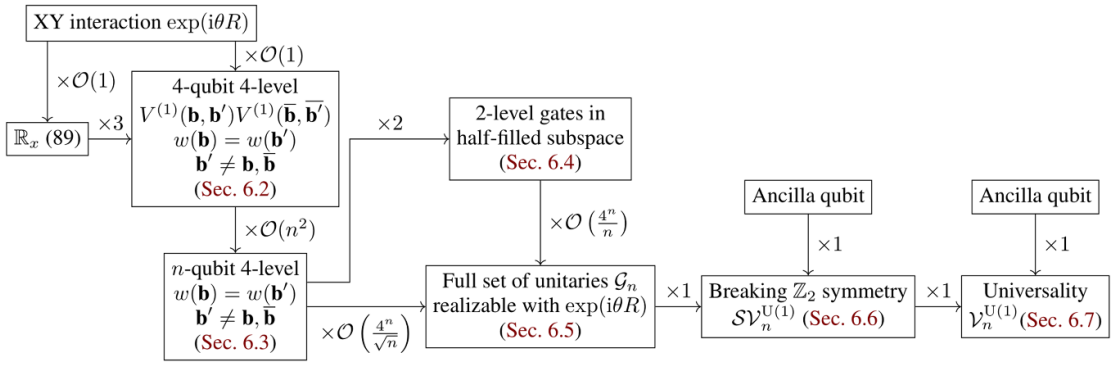


Figure 8. Overview of the method for synthesizing general energy-conserving unitaries with XY interaction alone. The number on the arrow pointing from one box A to another box B indicates the number of uses of A in the construction of B.

Proof. If $W = X^{\otimes n} W X^{\otimes n}$ and $V = X^{\otimes n} V X^{\otimes n}$, then for $m > \lfloor n/2 \rfloor$ it holds that

$$\Pi^{(m)} W \Pi^{(m)} = \Pi^{(m)} X^{\otimes n} W X^{\otimes n} \Pi^{(m)} \tag{93a}$$

$$= X^{\otimes n} \Pi^{(n-m)} W \Pi^{(n-m)} X^{\otimes n} \tag{93b}$$

$$= X^{\otimes n} \Pi^{(n-m)} V \Pi^{(n-m)} X^{\otimes n} \tag{93c}$$

$$= \Pi^{(m)} V \Pi^{(m)} , \tag{93d}$$

where the third line follows from equation (92) since $n - m \leqslant \lfloor n/2 \rfloor$, and we have used the fact that $\Pi^{(m)} X^{\otimes n} = X^{\otimes n} \Pi^{(n-m)}$. Therefore, equation (92) implies $V = W$. The other direction is trivial. □

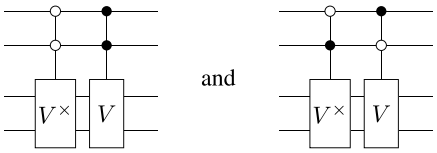
As we further discuss in section 6.4, when n is even, the sector with Hamming weight $m = n/2$ requires special treatment. But, for the rest of the Hilbert space, the above lemma implies a useful simplification. Namely, we can restrict our attention to the subspace

$$\mathcal{H}^{(<n/2)} := \bigoplus_{m=0}^{\lfloor (n-1)/2 \rfloor} \mathcal{H}^{(m)} . \tag{94}$$

Inside this subspace, the unitaries in equation (89) are 2-level and energy-conserving. This fact allows us to use the strategies developed in section 5 based on 2-level unitaries. Figure 8 presents an overview of the workflow in this section.

6.2. A useful family of 4-qubit 4-level energy-conserving $\mathbb{Z}_2$-invariant gates

In this section, we construct a useful family of 4-level unitaries that can be realized using XY interaction alone, namely the following sequences of two controlled unitaries



(95)

where

$$V = \begin{pmatrix} 1 & & \\ & V^{(1)} & \\ & & 1 \end{pmatrix} , \quad V^{\times} = (X \otimes X)\, V\, (X \otimes X) , \tag{96}$$

where $V^{(1)}$ is in SU(2) and acts in the subspace spanned by $|01\rangle$ and $|10\rangle$. The particular pairing of these two controlled unitaries guarantees that this composition respects the $\mathbb{Z}_2$ symmetry of XY interaction. These unitaries then will be used as the building blocks for constructing general unitaries in $\mathcal{G}_n$.

Recall that in the circuit synthesis method developed in section 5, the main building block was the 3-qubit 2-level energy-conserving unitaries in equation (52) (see figure 4). However, this gate does not respect the $\mathbb{Z}_2$

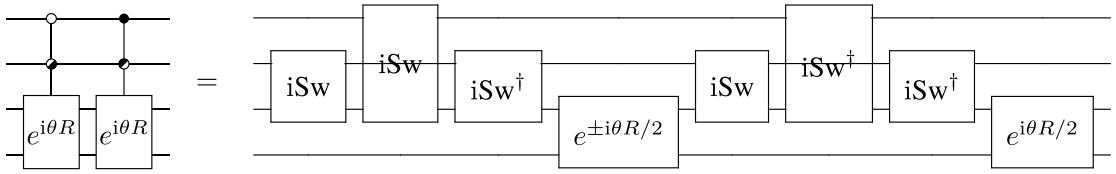


Figure 9. The circuits for implementing $\mathbb{R}_x(\theta,0101,0110)$ and $\mathbb{R}_x(\theta,0001,0010)$, based on equations (100) and (102). The unitary $\mathbb{R}_x(\theta,0101,0110)$ applies $e^{i\theta R}$ on the third and fourth qubits, when the parity of the first two qubits is odd, whereas $\mathbb{R}_x(\theta,0001,0010)$ applies $e^{i\theta R}$ when the parity is even. In the circuit in the right-hand side, these unitaries correspond to choosing the minus sign (odd parity) and plus sign (even parity) in the $e^{\pm i\theta R/2}$ gate, respectively.

symmetry in equation (83), which explains why the single-qubit gates S and $S^\dagger$ appear in this circuit and they cannot be avoided. To construct a gate that respects this symmetry, one may consider a modification of this circuit, obtained by removing S and $S^\dagger$ gates from equation (52). Then, we obtain the 3-qubit gate

$$F_{123}^\dagger \exp\left(\mathrm{i}\frac{\theta}{2}R_{23}\right) F_{123} = |0\rangle\langle 0|_1 \otimes \exp\left(\mathrm{i}\frac{\theta}{2}L_{23}\right) + |1\rangle\langle 1|_1 \otimes \exp\left(-\mathrm{i}\frac{\theta}{2}L_{23}\right) , \tag{97}$$

acting on qubits $1,2,3$, where $L_{jk} := (Y_jX_k - X_jY_k)/2 = \mathrm{i}(|10\rangle\langle 01|_{jk} - |01\rangle\langle 10|_{jk})$ and $F_{ijk} := \mathrm{iSw}_{ik}\mathrm{iSw}_{jk}^\dagger\mathrm{iSw}_{ij}$ as defined in equation (51). While this is a useful unitary, since it always acts non-trivially on qubits 2 and 3, regardless of the state of qubit 1, it can not be easily used in composition with other unitaries.

To overcome this problem, we construct the 4-qubit unitary

$$\begin{aligned}
&\mathbb{R}_x(\theta,0101,0110) \qquad (98)\\
&:= \exp\left[\mathrm{i}\theta\left(|0101\rangle\langle 0110| + |0110\rangle\langle 0101|\right)\right]\\
&\quad \times \exp\left[\mathrm{i}\theta\left(|1010\rangle\langle 1001| + |1001\rangle\langle 1010|\right)\right] ,\\
&= \left(|00\rangle\langle 00|_{12} + |11\rangle\langle 11|_{12}\right)\otimes \mathbb{I}_{34}\\
&\quad + \left(|01\rangle\langle 01|_{12} + |10\rangle\langle 10|_{12}\right)\otimes \exp\left(\mathrm{i}\theta R_{34}\right)\\
&= \sum_{b_1,b_2=0}^{1} |b_1b_2\rangle\langle b_1b_2|_{12}\otimes \exp\left(\mathrm{i}\left[b_1\oplus b_2\right]\theta R_{34}\right)\\
&= \exp\left(\mathrm{i}\frac{\theta}{2}R_{34}\right)\ \mathrm{CZ}_{23}\ \mathrm{CZ}_{13}\ \exp\left(-\mathrm{i}\frac{\theta}{2}R_{34}\right)\ \mathrm{CZ}_{13}\ \mathrm{CZ}_{23} \qquad (99)
\end{aligned}$$

which is obtained from equation (89) by choosing $\mathbf{b} = 0101$ and $\mathbf{b}' = 0110$, and $b_1 \oplus b_2 \in \{0,1\}$ denotes the parity of the bits b_1 and b_2. This unitary applies $\exp(\mathrm{i}\theta R_{34})$ on qubits 3 and 4, when the parity of qubits 1 and 2 is odd. Note that, using equation (50*b*), this unitary can be rewritten as

$$\mathbb{R}_x(\theta,0101,0110) = \exp\left(\mathrm{i}\frac{\theta}{2}R_{34}\right)\ G_{123}^\dagger\ \exp\left(-\mathrm{i}\frac{\theta}{2}R_{34}\right)\ G_{123} , \tag{100}$$

where

$$\begin{aligned}
G_{123} &:= \mathrm{iSw}_{23}^\dagger\mathrm{iSw}_{13}\mathrm{iSw}_{23} &(101a)\\
&= Z_1\mathrm{Sw}_{12}\ \mathrm{CZ}_{12}\ \mathrm{CZ}_{13}\ \mathrm{CZ}_{23} , &(101b)
\end{aligned}$$

and in equation (100) its effect is equivalent to $\mathrm{CZ}_{13}\mathrm{CZ}_{23}$ (see figure 3 for a diagram of the circuit identity in equation (101*a*)). Furthermore, by applying $\exp(\mathrm{i}\frac{\theta}{2}R_{34})$ instead of $\exp(-\mathrm{i}\frac{\theta}{2}R_{34})$ one obtains the gate

$$\mathbb{R}_x(\theta,0001,0010) = \exp\left(\mathrm{i}\frac{\theta}{2}R_{34}\right)\ G_{123}^\dagger\ \exp\left(\mathrm{i}\frac{\theta}{2}R_{34}\right)\ G_{123} . \tag{102}$$

The circuits for unitaries $\mathbb{R}_x(\theta,0101,0110)$ and $\mathbb{R}_x(\theta,0001,0010)$ are presented in figure 9.

Next, we obtain $\mathbb{R}_y$ gates defined in equation (89) from $\mathbb{R}_x$ gates. Note that $\mathbb{R}_y(\theta,0001,0010)$ can be obtained from $\mathbb{R}_x(\theta,0001,0010)$ by sandwiching the third (or the fourth) qubit between S and $S^\dagger$. However, our goal in this section is to avoid single-qubit rotations around the z-axis and realize everything with XY interaction alone.

Hence, to overcome this challenge we use a different approach. Namely, we utilize a 3-qubit sequence introduced by Lidar and Wu in [34, 58] to establish the possibility of universal quantum computing with XY

interaction in a DFS. (It is worth noting that Kempe and Whaley adapt this sequence in [31] to obtain the exact gate sequences for universal quantum computation using the XY interaction alone.) The sequence is given by

$$P_{123}(\phi) = \sqrt{\mathrm{iSw}}_{23}\ \mathrm{iSw}_{12}\ \exp(\mathrm{i}\phi R_{13})\ \mathrm{iSw}_{12}^{\dagger}\ \sqrt{\mathrm{iSw}}_{23}^{\dagger}\ .$$

This gate is diagonal in the computational basis. Indeed, one can show that

$$P_{123}(\phi) = |0\rangle\langle 0|_1 \otimes \exp\left(-\mathrm{i}\frac{\phi}{2}Z_2\right) \otimes \exp\left(\mathrm{i}\frac{\phi}{2}Z_3\right) + |1\rangle\langle 1|_1 \otimes \exp\left(\mathrm{i}\frac{\phi}{2}Z_2\right) \otimes \exp\left(-\mathrm{i}\frac{\phi}{2}Z_3\right)\ , \tag{103}$$

for arbitrary $\phi \in (-\pi, \pi]$. Then, by sandwiching the unitary $\mathbb{R}_x(\theta, 0001, 0010)$ in equation (100) between

$$\begin{aligned} P_{123}\left(\frac{\pi}{2}\right) &= \sqrt{\mathrm{iSw}}_{23}\mathrm{iSw}_{12}\mathrm{iSw}_{13}\mathrm{iSw}_{12}^{\dagger}\sqrt{\mathrm{iSw}}_{23}^{\dagger} && (104a)\\ &= |0\rangle\langle 0|_1 \otimes S_2 \otimes S_3^{\dagger} + |1\rangle\langle 1|_1 \otimes S_2^{\dagger} \otimes S_3 && (104b)\\ &= \mathrm{C}Z_{12}\mathrm{C}Z_{13}S_2S_3^{\dagger}\ , && (104c) \end{aligned}$$

and its inverse we show that

$$P_{123}\left(-\frac{\pi}{2}\right)\mathbb{R}_x(\theta, 0101, 0110)\,P_{123}\left(\frac{\pi}{2}\right) = \mathbb{R}_y(\theta, 0101, 0110)\ . \tag{105}$$

To see this, first recall that $\mathbb{R}_x(\theta, 0101, 0110)$ is defined as

$$\exp\left[\mathrm{i}\theta X(0101, 0110)\right]\exp\left[\mathrm{i}\theta X(1010, 1001)\right]\ .$$

Similarly, $\mathbb{R}_y(\theta, 0101, 0110)$ is defined as

$$\exp\left[\mathrm{i}\theta Y(0101, 0110)\right]\exp\left[\mathrm{i}\theta Y(1010, 1001)\right]\ .$$

Then, we note that

$$\begin{aligned} &P_{123}\left(-\frac{\pi}{2}\right)\exp\left[\mathrm{i}\theta X(0101, 0110)\right]P_{123}\left(\frac{\pi}{2}\right).\\ &= \mathrm{C}Z_{13}S_3\exp\left[\mathrm{i}\theta X(0101, 0110)\right]S_3^{\dagger}\mathrm{C}Z_{13}\\ &= \exp\left[\mathrm{i}\theta Y(0101, 0110)\right]\ , \end{aligned} \tag{106}$$

where we have applied equation (104c). Furthermore, by sandwiching both sides of this equation between $X^{\otimes 4}$ and using the fact that $P_{123}(\phi)$ commutes with $X^{\otimes 4}$, we obtain

$$P_{123}\left(-\frac{\pi}{2}\right)\exp\left[\mathrm{i}\theta X(1010, 1001)\right]P_{123}\left(\frac{\pi}{2}\right) = \exp\left[\mathrm{i}\theta Y(1010, 1001)\right]\ . \tag{107}$$

Then, multiplying the above two equations, we arrive at equation (105).

In summary, in this way we can obtain four families of unitaries

$$\begin{aligned} &\mathbb{R}_x(\theta, 0101, 0110)\ , && (108a)\\ &\mathbb{R}_x(\theta, 0001, 0010) = \mathbb{R}_x(\theta, 1110, 1101)\ , && (108b)\\ &\mathbb{R}_y(\theta, 0101, 0110)\ , && (108c)\\ &\mathbb{R}_y(\theta, 0001, 0010) = \mathbb{R}_y(\theta, 1110, 1101)\ , && (108d) \end{aligned}$$

and their permuted versions, which can all be realized with $\mathcal{O}(1)$ number of $\exp(\mathrm{i}\alpha R)$ gates alone.

As a useful observation, any 4-bit strings $\mathbf{b}$ and $\mathbf{b}'$ satisfying $w(\mathbf{b}) = w(\mathbf{b}')$ and $\mathbf{b}' \neq \mathbf{b}, \bar{\mathbf{b}}$ necessarily have two common bits and two distinct bits, and fit into either equations (108a) and (108c) or equations (108b) and (108d) by permuting the qubits. This means that we can implement $\mathbb{R}_x(\theta, \mathbf{b}, \mathbf{b}')$ and $\mathbb{R}_y(\theta, \mathbf{b}, \mathbf{b}')$ for all $\mathbf{b}, \mathbf{b}' \in \{0,1\}^4$ which satisfy the conditions $w(\mathbf{b}) = w(\mathbf{b}')$ and $\mathbf{b}' \neq \mathbf{b}, \bar{\mathbf{b}}$.

Furthermore, combining these unitaries we can obtain unitaries that act as arbitrary $V^{(1)} \in \mathrm{SU}(2)$ on the subspace spaned by $\{|\mathbf{b}\rangle, |\mathbf{b}'\rangle\}$. In particular, suppose $V^{(1)}$ has the Euler decomposition

$$V^{(1)} = e^{\mathrm{i}\gamma X}e^{\mathrm{i}\beta Y}e^{\mathrm{i}\alpha X}\ . \tag{109}$$

Then, for $\mathbf{b}' \neq \bar{\mathbf{b}}$ the following sequence of unitaries

$$\mathbb{R}_x\left(\gamma, \mathbf{b}, \mathbf{b}'\right) \mathbb{R}_y\left(\beta, \mathbf{b}, \mathbf{b}'\right) \mathbb{R}_x\left(\alpha, \mathbf{b}, \mathbf{b}'\right) = V^{(1)}\left(\mathbf{b}, \mathbf{b}'\right) V^{(1)}\left(\bar{\mathbf{b}}, \overline{\mathbf{b}'}\right) , \tag{110}$$

realize two copies of $V^{(1)}$, namely $V^{(1)}(\mathbf{b}, \mathbf{b}')$ which acts in the subspace spanned by $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$, and $V^{(1)}(\bar{\mathbf{b}}, \overline{\mathbf{b}'})$ which acts in the subspace spanned by $|\bar{\mathbf{b}}\rangle$ and $|\overline{\mathbf{b}'}\rangle$.

Choosing $\mathbf{b}$ and $\mathbf{b}'$ to be bit strings in $\{0,1\}^4$ with Hamming weight 1, we can obtain 4-level unitaries that act as 2-level ones in the sectors with Hamming weights 1 and 3, either of which has dimension 4. Combining such 2-level unitaries, we can realize an arbitrary unitary in SU(4) in the sector with Hamming weight 1. Then, the realized unitary in the sector with Hamming weight 3 is dictated by the $\mathbb{Z}_2$ symmetry. In section 6.4, where we focus on the half-filled sector $m = n/2$, we come back to this example and explain how, in the sector with Hamming weight 2, a general unitary satisfying the condition in equations (83)–(86) can be realized.

We finish this section by rewriting equation (110) in terms of controlled unitaries in the form of equation (95), which will be useful for applications in the next section. Recall that here we consider $\mathbf{b}, \mathbf{b}' \in \{0,1\}^4$ satisfying the constraints $w(\mathbf{b}) = w(\mathbf{b}')$, and $\mathbf{b}' \neq \mathbf{b}, \bar{\mathbf{b}}$. As mentioned above, any such $\mathbf{b}$ and $\mathbf{b}'$ have two common bits and two distinct bits, which means up to a permutation, they can be written as

$$\mathbf{b} = \mathbf{c}01 \quad \text{and} \quad \mathbf{b}' = \mathbf{c}10 ,$$

where $\mathbf{c}$ contains the common bits. Then, we can interpret the unitary in equation (110) as a controlled unitary that acts only when the first two qubits are in $\mathbf{c}$ or $\bar{\mathbf{c}}$. To see this, recall that, as we have seen before in equation (62), the 2-level unitary $V^{(1)}(\mathbf{b}, \mathbf{b}')$ can be written as the controlled gate

$$V^{(1)}\left(\mathbf{b}, \mathbf{b}'\right) = \Lambda^{\mathbf{c}}(V) , \quad V = \begin{pmatrix} 1 & & \\ & V^{(1)} & \\ & & 1 \end{pmatrix} \tag{111}$$

where $\Lambda^{\mathbf{c}}(V)$ is a controlled-V gate with control string $\mathbf{c}$ defined in equation (63). Similarly,

$$V^{(1)}\left(\bar{\mathbf{b}}, \overline{\mathbf{b}'}\right) = \Lambda^{\bar{\mathbf{c}}}\left(V^{\times}\right) , \quad V^{\times} := (X \otimes X)\, V (X \otimes X) . \tag{112}$$

We conclude that the 4-level gate in equation (110) can be rewritten as

$$V^{(1)}\left(\mathbf{b}, \mathbf{b}'\right) V^{(1)}\left(\bar{\mathbf{b}}, \overline{\mathbf{b}'}\right) = \Lambda^{\mathbf{c}}(V)\, \Lambda^{\bar{\mathbf{c}}}\left(V^{\times}\right) , \tag{113}$$

which corresponds to the circuit in equation (95).

6.3. From 4-qubit 4-level gates to *n*-qubit 4-level gates

Next, we use these 4-qubit unitaries to construct general 4-level n-qubit unitaries in the form

$$U^{(1)}\left(\mathbf{b}, \mathbf{b}'\right) U^{(1)}\left(\bar{\mathbf{b}}, \overline{\mathbf{b}'}\right) \quad : U^{(1)} \in \mathrm{SU}(2) , \tag{114}$$

where, $U^{(1)}(\mathbf{b}, \mathbf{b}')$ as defined in equation (21) is a 2-level unitary acting on $|\mathbf{b}\rangle$ and $|\mathbf{b}'\rangle$, and we assume

$$\mathbf{b}' \neq \bar{\mathbf{b}}, \mathbf{b} , \tag{115}$$

and $\mathbf{b}$ and $\mathbf{b}'$ have equal Hamming weights, i.e.

$$w(\mathbf{b}) = w\left(\mathbf{b}'\right) . \tag{116}$$

The assumption that $\mathbf{b}' \neq \bar{\mathbf{b}}$ in equation (115) implies that $\mathbf{b}$ and $\mathbf{b}'$ have, at least, one common bit. Without loss of generality, we assume this common bit is the first bit of $\mathbf{b}$ and $\mathbf{b}'$ and the value of this bit is 1; otherwise, we proceed with $\bar{\mathbf{b}}$ and $\overline{\mathbf{b}'}$ instead. This means

$$|\mathbf{b}\rangle = |1\rangle|\mathbf{c}\rangle, \quad |\mathbf{b}'\rangle = |1\rangle|\mathbf{c}'\rangle , \tag{117}$$

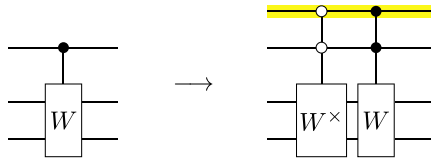
where $\mathbf{c}, \mathbf{c}' \in \{0,1\}^{n-1}$ are the remaining bits of $\mathbf{b}$ and $\mathbf{b}'$, which have equal Hamming weights, i.e. $w(\mathbf{c}) = w(\mathbf{c}')$. With this definition we have

$$U^{(1)}\left(\mathbf{b}, \mathbf{b}'\right) = |0\rangle\langle 0|_1 \otimes \mathbb{I} + |1\rangle\langle 1|_1 \otimes U^{(1)}\left(\mathbf{c}, \mathbf{c}'\right)_{2,\ldots,n} . \tag{118}$$

Now consider the $n-1$ energy-conserving unitary $U^{(1)}(\mathbf{c},\mathbf{c}')_{2,\ldots,n}$. Using the techniques of section 5 steps 1 and 2, we can decompose this unitary as

$$U^{(1)}(\mathbf{c},\mathbf{c}')_{2,\ldots,n} = V_T \cdots V_1 \,, \tag{119}$$

where $T=\mathcal{O}(n^2)$, and each V_j is a gate in the form of $\Lambda^1(W)$ (or $\Lambda^0(W)$). In other words, it is a gate in the form of the left-hand side of the figure below. Note that these gates are not realizable with XY interaction alone, because, in general, they do not commute with $X^{\otimes 3}$, i.e. they break the $\mathbb{Z}_2$ symmetry of this interaction. However, we can extend these 3-qubit gates to 4-qubit gates acting on the original 3 qubits and qubit 1 (i.e. the control qubit in equation (118)) using the following rule:



$$\begin{aligned} V=\Lambda^1(W) \quad &\longrightarrow \quad \Lambda^1(V)\Lambda^0(V^\times) \\ &= \Lambda^{11}(W)\Lambda^{00}(W^\times) \end{aligned} \tag{120}$$

where the highlighted qubit is qubit 1. In other words, we replace each 3-qubit gate V_j in equation (119) with 4-qubit gates

$$\Lambda^1\left(V_j\right)\Lambda^0\left(V_j^\times\right) = \left[|0\rangle\langle 0|_1 \otimes \mathbb{I} + |1\rangle\langle 1|_1 \otimes V_j\right]\left[|1\rangle\langle 1|_1 \otimes \mathbb{I} + |0\rangle\langle 0|_1 \otimes V_j^\times\right] \,, \tag{121}$$

where $V_j^\times = X^{\otimes 3} V_j X^{\otimes 3}$, and the subscript 1 in the right-hand side means the control qubit is qubit 1. Notice that similar to V_j, $V_j^\times$ is also a 2-level 3-qubit unitary. Then, the 4-qubit unitary in equation (121) is in the form of equation (95), which can be realized using XY interaction alone with the methods developed in the previous section. In figure 10 we present an example of this circuit conversion, which is further discussed below (In this figure, we have highlighted qubit 1).

It can be easily shown that the resulting circuit realizes the desired unitary $U^{(1)}(\mathbf{b},\mathbf{b}')U^{(1)}(\overline{\mathbf{b}},\overline{\mathbf{b}'})$: To see this note the resulting circuit has two types of gates: $\Lambda^1(V_j)$, which are activated when the first qubit is $|1\rangle$, and $\Lambda^0(V_j^\times)$, which are activated when it is $|0\rangle$. Clearly, every pair of gates from different types commute with each other. Then, using equation (118) it can be seen that the first family realizes unitary $U^{(1)}(\mathbf{b},\mathbf{b}')$, namely

$$\begin{aligned} U^{(1)}\left(\mathbf{b},\mathbf{b}'\right) &= \Lambda^1\left(U^{(1)}\left(\mathbf{c},\mathbf{c}'\right)\right) \\ &= \Lambda^1\left(V_T \cdots V_1\right) \\ &= \Lambda^1\left(V_T\right)\cdots\Lambda^1\left(V_1\right) \,, \end{aligned} \tag{122}$$

and the second family realizes the unitary

$$\begin{aligned} U^{(1)}\left(\overline{\mathbf{b}},\overline{\mathbf{b}'}\right) &= X^{\otimes n} U^{(1)}\left(\mathbf{b},\mathbf{b}'\right) X^{\otimes n} \\ &= X^{\otimes n}\Lambda^1\left(V_T\right)\cdots\Lambda^1\left(V_1\right) X^{\otimes n} \\ &= \Lambda^0\left(V_T^\times\right)\cdots\Lambda^0\left(V_1^\times\right) \,. \end{aligned} \tag{123}$$

Therefore, we conclude that

Lemma 15. *For any $\boldsymbol{b},\boldsymbol{b}' \in \{0,1\}^n$ with equal Hamming weights, if $\boldsymbol{b}' \neq \overline{\mathbf{b}}, \boldsymbol{b}$, then the 4-level unitary $U^{(1)}(\boldsymbol{b},\boldsymbol{b}')U^{(1)}(\overline{\mathbf{b}},\overline{\mathbf{b}'})$ can be realized with $\mathcal{O}(n^2)$ gates $\exp(\mathrm{i}\alpha R) : \alpha \in (-\pi,\pi]$, without any ancilla qubits.*

6.3.1. Example: a 5-qubit 4-level unitary

Figure 10 shows an example of this circuit conversion where the top is a circuit for the 2-level unitary

$$U^{(1)}\left(1101,1110\right) = \Lambda^{11}\left(U\right) \,, \tag{124}$$

obtained using the techniques of section 5 step 1, and the bottom is the circuit obtained by applying the transformation in equation (120). It can be easily seen that the bottom circuit realizes

$$U^{(1)}\left(11101,11110\right)U^{(1)}\left(00010,00001\right) = \Lambda^{111}\left(U\right)\Lambda^{000}\left(U^\times\right) \,, \tag{125}$$

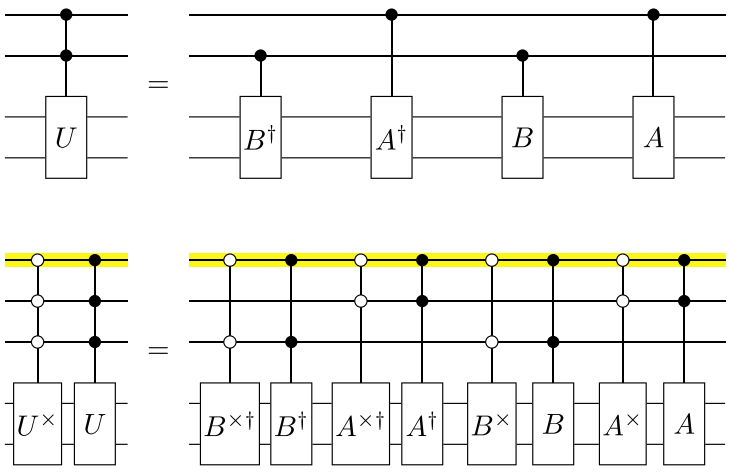


Figure 10. The transformation from the circuit for $\Lambda^{11}(U)$ (upper) to $\Lambda^{111}(U)\Lambda^{000}(U^{\times})$ (lower) using the mapping in equation (120). The highlighted qubit is the extra control qubit.

which corresponds to the unitary in equation (114) with

$$\mathbf{b} = 11101\,, \quad \mathbf{b}' = 11110\,, \tag{126}$$

where

$$U = \begin{pmatrix} 1 & & \\ & U^{(1)} & \\ & & 1 \end{pmatrix}, \quad U^{\times} = (X\otimes X)\,U\,(X\otimes X)\,. \tag{127}$$

6.4. The special case of half-filled sector ($m = n/2$)

Next, we focus on the special case of the sector with Hamming weight $m = n/2$ when n the number of qubits is even. This sector, which can be called the 'half-filled' sector, splits into two equal-sized subspaces corresponding to ± 1 eigenvalues of $X^{\otimes n}$, denoted as

$$\mathcal{H}^{(n/2)} = \mathcal{H}^{(n/2,+)} \oplus \mathcal{H}^{(n/2,-)}\,. \tag{128}$$

The fact XY interaction commutes with $X^{\otimes n}$, means that this Hamiltonian is block-diagonal with respect to the above decomposition. This in turn implies all realizable unitaries with XY interaction are also block-diagonal. That is

$$V^{(n/2)} = V^{(n/2,+)} \oplus V^{(n/2,-)}\,, \tag{129}$$

where $V^{(n/2,\pm)}$ is the component of $V^{(n/2)}$ that acts in the subspace with Hamming weight $n/2$ and eigenvalue ± 1 of $X^{\otimes n}$. We show that

Lemma 16. *For $n \geqslant 4$, consider the unitary $V = V^{(n/2)} \oplus \mathbb{I}_{\perp}$ where $\mathbb{I}_{\perp}$ is the identity operator on the subspace orthogonal to $\mathcal{H}^{(n/2)}$. This unitary can be realized with XY interaction alone (without any ancillary qubit) if, and only if*

$$det\left(V^{(n/2,+)}\right) = det\left(V^{(n/2,-)}\right) = 1\,, \tag{130}$$

where $V^{(n/2,\pm)}$ is the component of $V^{(n/2)}$ in the subspace $\mathcal{H}^{(n/2,\pm)}$, as defined in equation (129). Furthermore, any such unitary can be realized with $\mathcal{O}(n\times 4^n)$ 2-qubit unitaries $\exp(i\theta R)$.

Proof. The necessity of this condition follows from the arguments in [23]: For any pair of qubits i and j and $n > 2$ we have

$$\mathrm{Tr}\left(X^{\otimes n} R_{ij}\right) = \mathrm{Tr}\left(R_{ij}\right) = 0\,, \tag{131}$$

where $R_{ij} = (X_iX_j + Y_iY_j)/2$ is the XY interaction. This, in turn, implies

$$\frac{\mathrm{Tr}\left(R_{ij}\right) \pm \mathrm{Tr}\left(X^{\otimes n} R_{ij}\right)}{2} = \mathrm{Tr}\left(P_{\pm} R_{ij}\right) = 0\,, \tag{132}$$

where $P_\pm = (\mathbb{I} \pm X^{\otimes n})/2$ are the projectors to the subspace with eigenvalue ± 1 of $X^{\otimes n}$. For any unitary W that commutes with $X^{\otimes n}$, let $W = W_+ \oplus W_-$ be the decomposition of W relative to the eigensubspaces of $X^{\otimes n}$. Then, for any unitary W which is decomposable as $W = \prod_k \exp(\mathrm{i}\theta_k R_{i_k j_k})$, equation (132) implies that $\det[P_\pm \exp(\mathrm{i}\theta_k R_{i_k j_k}) P_\pm] = 1$ for every k, where the determinant is calculated over the support of $P_\pm$. Therefore, noting that $R_{i_k j_k}$ and $P_\pm$ commute,

$$\begin{aligned}\det(W_\pm) &= \det\left[\prod_k P_\pm \exp\left(\mathrm{i}\theta_k R_{i_k j_k}\right) P_\pm\right] \\ &= \prod_k \det\left[P_\pm \exp\left(\mathrm{i}\theta_k R_{i_k j_k}\right) P_\pm\right] = 1\,. \end{aligned} \tag{133}$$

This proves the necessity of the condition. In the following, we prove the sufficiency of this condition.

First, for convenience we choose a basis for $\mathcal{H}^{(n/2)}$ which is consistent with the decomposition in equation (128) such that any basis element is either in $\mathcal{H}^{(n/2,+)}$ or $\mathcal{H}^{(n/2,-)}$. To achieve this we define the basis

$$|\mathbf{b},\pm\rangle = \frac{|\mathbf{b}\rangle \pm |\bar{\mathbf{b}}\rangle}{\sqrt{2}} \qquad : w(\mathbf{b}) = \frac{n}{2}\,,\ \ \mathbf{b} < \bar{\mathbf{b}}\,, \tag{134}$$

for $\mathbf{b} = b_1 \cdots b_n \in \{0,1\}^n$, where the first condition means the Hamming weight of $\mathbf{b}$ is $n/2$, and in $\mathbf{b} < \bar{\mathbf{b}}$ we are interpreting $\mathbf{b}$ and $\bar{\mathbf{b}}$ as the binary representations of integers (In other words, this condition means the left-most bit of $\mathbf{b}$ is 0). This condition is imposed to obtain a complete orthonormal basis; otherwise we will consider $|\mathbf{b},+\rangle$ and $|\bar{\mathbf{b}},+\rangle$ as two separate vectors, whereas according to the definition in equation (134) they are indeed equal. (Note that any total order on binary strings can be used here.) Then, it is clear that the set of vectors $|\mathbf{b},\pm\rangle$ with $\mathbf{b}$ defined in equation (134) form a complete orthonormal basis for $\mathcal{H}^{(n/2,\pm)}$.

Next, we show how one can implement unitaries that are 2-level with respect to this basis. Namely, for $\mathbf{b} < \bar{\mathbf{b}}$ and $\mathbf{c} < \bar{\mathbf{c}}$, we consider the unitaries

$$\exp\left(\mathrm{i}2\theta\left[|\mathbf{b},\pm\rangle\langle\mathbf{c},\pm| \ + \ |\mathbf{c},\pm\rangle\langle\mathbf{b},\pm|\right]\right) = \mathbb{R}_x(\theta,\mathbf{b},\mathbf{c})\ \mathbb{R}_x(\pm\theta,\mathbf{b},\bar{\mathbf{c}}) \tag{135a}$$

$$\exp\left(\mathrm{i}2\theta\left[\mathrm{i}|\mathbf{c},\pm\rangle\langle\mathbf{b},\pm| \ - \ \mathrm{i}|\mathbf{b},\pm\rangle\langle\mathbf{c},\pm|\right]\right) = \mathbb{R}_y(\theta,\mathbf{b},\mathbf{c})\ \mathbb{R}_y(\pm\theta,\mathbf{b},\bar{\mathbf{c}}) \tag{135b}$$

where the identities are proven below. Here, $\mathbb{R}_x$ and $\mathbb{R}_y$ are defined in equation (89), namely

$$\mathbb{R}_x(\theta,\mathbf{b},\mathbf{c}) := \exp\left[\mathrm{i}\theta\left(X(\mathbf{b},\mathbf{c}) + X\left(\bar{\mathbf{b}},\bar{\mathbf{c}}\right)\right)\right] \tag{136a}$$

$$\mathbb{R}_y(\theta,\mathbf{b},\mathbf{c}) := \exp\left[\mathrm{i}\theta\left(Y(\mathbf{b},\mathbf{c}) + Y\left(\bar{\mathbf{b}},\bar{\mathbf{c}}\right)\right)\right]\,, \tag{136b}$$

where we have used the fact that $X(\mathbf{b},\mathbf{c})$ and $X(\bar{\mathbf{b}},\bar{\mathbf{c}})$ commute, and the same fact holds for $Y(\mathbf{b},\mathbf{c})$ and $Y(\bar{\mathbf{b}},\bar{\mathbf{c}})$. Note that $\mathbf{b} < \bar{\mathbf{b}}$ and $\mathbf{c} < \bar{\mathbf{c}}$ together imply that $\mathbf{b} \neq \bar{\mathbf{c}}$, because the left-most bit of $\mathbf{b}$ is 0, whereas the left-most bit of $\bar{\mathbf{c}}$ is 1.

To show the identities in equation (135), we note that for $\mathbf{b} < \bar{\mathbf{b}}$ and $\mathbf{c} < \bar{\mathbf{c}}$, it holds that

$$|\mathbf{b}\rangle\langle\mathbf{c}| + |\bar{\mathbf{b}}\rangle\langle\bar{\mathbf{c}}| = |\mathbf{b},+\rangle\langle\mathbf{c},+| + |\mathbf{b},-\rangle\langle\mathbf{c},-| \tag{137}$$

$$|\mathbf{b}\rangle\langle\bar{\mathbf{c}}| + |\bar{\mathbf{b}}\rangle\langle\mathbf{c}| = |\mathbf{b},+\rangle\langle\mathbf{c},+| - |\mathbf{b},-\rangle\langle\mathbf{c},-|\,, \tag{138}$$

which, in turn, implies

$$X(\mathbf{b},\mathbf{c}) + X\left(\bar{\mathbf{b}},\bar{\mathbf{c}}\right) = |\mathbf{b},+\rangle\langle\mathbf{c},+| + |\mathbf{c},+\rangle\langle\mathbf{b},+| + |\mathbf{b},-\rangle\langle\mathbf{c},-| + |\mathbf{c},-\rangle\langle\mathbf{b},-|\,, \tag{139}$$

and

$$X(\mathbf{b},\bar{\mathbf{c}}) + X\left(\bar{\mathbf{b}},\mathbf{c}\right) = |\mathbf{b},+\rangle\langle\mathbf{c},+| + |\mathbf{c},+\rangle\langle\mathbf{b},+| - |\mathbf{b},-\rangle\langle\mathbf{c},-| - |\mathbf{c},-\rangle\langle\mathbf{b},-|\,. \tag{140}$$

Note that the right-hand sides of equations (139) and (140) commute, which using equation (136), implies $\mathbb{R}_x(\theta_1,\mathbf{b},\mathbf{c})$ and $\mathbb{R}_x(\theta_2,\mathbf{b},\bar{\mathbf{c}})$ commute and equation (135*a*) holds. Equation (135*b*) can be shown similarly.

Finally, recall that under the assumption that $\mathbf{b} \neq \mathbf{c},\bar{\mathbf{c}}$ and $w(\mathbf{b}) = w(\mathbf{c})$, the 4-level unitaries in equation (136) can be realized using the method developed previously in section 6.3. We conclude that unitaries in equation (135) can be realized with XY interaction alone. Next, we use these unitaries to construct other unitaries in the half-filled sectors.

Unitaries in equation (135) are 2-level with respect to the basis in equation (134), namely they act non-trivially on the 2D subspace spanned by $|\mathbf{b},+\rangle$ and $|\mathbf{c},+\rangle$ (or $|\mathbf{b},-\rangle$ and $|\mathbf{c},-\rangle$), which is restricted to

the subspace $\mathcal{H}^{(n/2,+)}$ (or $\mathcal{H}^{(n/2,-)}$). Furthermore, relative to the basis $|\mathbf{b},\pm\rangle$ and $|\mathbf{c},\pm\rangle$, the unitaries in equation (135) act as $\exp(\mathrm{i}2\theta X)$ and $\exp(\mathrm{i}2\theta Y)$, i.e. rotations around x and y axes, respectively.

Using the Euler decomposition, one obtains arbitrary 2-level special unitaries (i.e. unitaries with determinant 1) in the subspace spanned by $|\mathbf{b},\pm\rangle$ and $|\mathbf{c},\pm\rangle$. Therefore, using lemma 12, by combining such unitaries we obtain all unitaries acting on $\mathcal{H}^{(n/2,+)}$ and $\mathcal{H}^{(n/2,-)}$ that satisfy the condition in equation (130) of lemma 16. In particular, this requires $\mathcal{O}(D^2)=\mathcal{O}(4^n n^{-1})$ unitaries of the type in equation (135), where

$$D=\dim\left(\mathcal{H}^{(n/2,\pm)}\right)=\frac{1}{2}\binom{n}{n/2}\approx\frac{2^n}{\sqrt{2\pi n}}\,. \tag{141}$$

As we have seen in section 6.3, each 4-level unitary $\mathbb{R}_x(\theta,\mathbf{b},\mathbf{c})$ and $\mathbb{R}_x(\theta,\mathbf{b},\bar{\mathbf{c}})$ can be realized with $\mathcal{O}(n^2)$ gates $\exp(\mathrm{i}\theta R)$. Therefore, we conclude that a general unitary $V^{(n/2)}$ satisfying the condition in equation (130) can be realized with $\mathcal{O}(n^2D^2)=\mathcal{O}(4^n n)$ gates $\exp(\mathrm{i}\theta R)$. This completes the proof of lemma 16. □

6.4.1. Example: the sector with Hamming weight 2 of 4 qubits

In section 6.2, we discussed the implementation of unitaries in sectors with Hamming weights 1 and 3 of 4 qubits. Here, we focus on the sector with Hamming weight 2, and complete the construction of unitaries in $\mathcal{G}_4$.

In this example, the basis defined in equation (134) is the set of vectors

$$|0011,\pm\rangle:=\frac{|0011\rangle\pm|1100\rangle}{\sqrt{2}}, \tag{142a}$$

$$|0101,\pm\rangle:=\frac{|0101\rangle\pm|1010\rangle}{\sqrt{2}}, \tag{142b}$$

$$|0110,\pm\rangle:=\frac{|0110\rangle\pm|1001\rangle}{\sqrt{2}}\,, \tag{142c}$$

which spans the six-dimensional subspace

$$\mathcal{H}^{(2)}=\mathcal{H}^{(2,+)}\oplus\mathcal{H}^{(2,-)}\cong\mathbb{C}^3\oplus\mathbb{C}^3\,.$$

Following the above construction, using the XY interaction alone, we can implement any unitary inside each of these three-dimensional subspaces, provided that it has determinant 1 and is 2-level with respect to the above basis.

For example, consider $U\in\mathrm{SU}(2)$ with the Euler decomposition

$$U=e^{\mathrm{i}\gamma X}e^{\mathrm{i}\beta Y}e^{\mathrm{i}\alpha X}\,.$$

Suppose we want to implement this unitary as a 2-level unitary on the basis vectors $|0011,+\rangle$ and $|0101,+\rangle$, which we denote as unitary $U(0011,+;0101,+)$. Then, using equation (135) we obtain the decomposition

$$\begin{aligned}U(0011,+;0101,+)=&\,\mathbb{R}_x\left(\frac{\gamma}{2},0011,0101\right)\mathbb{R}_x\left(\frac{\gamma}{2},0011,1010\right)\\&\times\mathbb{R}_y\left(\frac{\beta}{2},0011,0101\right)\mathbb{R}_y\left(\frac{\beta}{2},0011,1010\right)\\&\times\mathbb{R}_x\left(\frac{\alpha}{2},0011,0101\right)\mathbb{R}_x\left(\frac{\alpha}{2},0011,1010\right)\,.\end{aligned} \tag{143}$$

Note that applying equations (100) and (105) and their permuted versions, one can implement each unitary in this decomposition using XY interaction alone. Finally, combining such 2-level unitaries on subspace $\mathcal{H}^{(2,+)}$, we obtain the full SU(3) unitary group on this subspace. A similar construction works for $\mathcal{H}^{(2,-)}$. In summary, combined with the results of section 6.2, we obtain the group of all 4-qubit unitaries satisfying conditions in equations (83)–(86), which is isomorphic to the group

$$\mathcal{G}_4\cong\mathrm{SU}(4)\times\mathrm{SU}(3)\times\mathrm{SU}(3)\,.$$

6.4.2. Example: a family of 6-qubit 2-level unitaries

As an example, let us consider the 6-qubit unitary

$$V=\exp\left(i\theta\left[|\mathbf{b},+\rangle\langle\mathbf{b}',+|+|\mathbf{b}',+\rangle\langle\mathbf{b},+|\right]\right)\,, \tag{144}$$

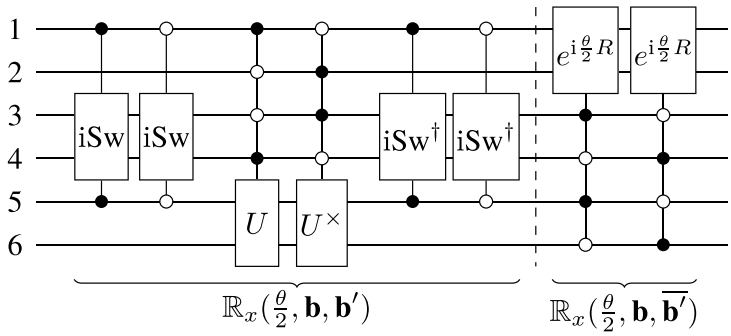


Figure 11. The circuit for realizing the 6-qubit unitary $V = \exp(i\theta[|\mathbf{b},+\rangle\langle\mathbf{b'},+| + |\mathbf{b'},+\rangle\langle\mathbf{b},+|])$, where $|\mathbf{b},+\rangle$ and $|\mathbf{b'},+\rangle$ are defined in equation (145) . The first six gates in the circuit implement $\mathbb{R}_x(\frac{\theta}{2},\mathbf{b},\mathbf{b}')$, and the last two gates implement $\mathbb{R}_x(\frac{\theta}{2},\mathbf{b},\overline{\mathbf{b}'})$. Each of the 4-level gates, namely the pair of controlled-U and $U^\times$ and the pair of controlled-$e^{\mathrm{i}\frac{\theta}{2}R}$, can be implemented with 10 ($T(3) = 10$ in lemma 9) 4-qubit 4-level gates using the construction in section 6.3.

where

$$|\mathbf{b},+\rangle = \frac{|010101\rangle + |101010\rangle}{\sqrt{2}}, \tag{145a}$$

$$|\mathbf{b}',+\rangle = \frac{|100101\rangle + |011010\rangle}{\sqrt{2}}, \tag{145b}$$

and

$$\mathbf{b} = 010101\ ,\ \ \mathbf{b}' = 011010\ .$$

Applying equation (135), the unitary V can be decomposed as

$$V = \mathbb{R}_x\left(\frac{\theta}{2},\mathbf{b},\mathbf{b}'\right)\mathbb{R}_x\left(\frac{\theta}{2},\mathbf{b},\overline{\mathbf{b}'}\right). \tag{146}$$

Then, as we further explain below, applying the above methods we obtain the circuit in figure 11 for implementing the unitary V, where the first part of the circuit, i.e.,the first six unitaries, realizes the unitary

$$\mathbb{R}_x\left(\frac{\theta}{2},\mathbf{b},\mathbf{b}'\right) = \mathbb{R}_x\left(\frac{\theta}{2},\bar{\mathbf{b}},\overline{\mathbf{b}'}\right), \tag{147}$$

and, the second part, i.e. the last two unitaries realizes

$$\mathbb{R}_x\left(\frac{\theta}{2},\mathbf{b},\overline{\mathbf{b}'}\right) = \mathbb{R}_x\left(\frac{\theta}{2},\bar{\mathbf{b}},\mathbf{b}'\right). \tag{148}$$

Note that each consecutive pair of unitaries in figure 11 is an energy-conserving unitary that is 4-level in the computational basis, which can be itself decomposed into a sequence of gates $\exp(\mathrm{i}\alpha R) : \alpha \in (-\pi,\pi]$ using the methods of section 6.3 (In particular, for each of these 4-level unitaries the conditions in equations (115) and (116) hold).

Both parts of this circuit are obtained by applying the method in section 6.3. In particular, the first part of the circuit, which realizes the unitary in equation (147), is obtained by applying the conversion rule in section 6.3 to the 5-qubit circuit in figure 12. This 5-qubit circuit realizes the unitary $\exp\left(\mathrm{i}\frac{\theta}{2}X(\mathbf{c},\mathbf{c}')\right)$, where $\mathbf{c} = 01010$ and $\mathbf{c}' = 00101$, which are obtained by removing the first bit of $\bar{\mathbf{b}}$ and $\overline{\mathbf{b}'}$, i.e.

$$\bar{\mathbf{b}} = 1\mathbf{c} = 101010\ ,\ \ \overline{\mathbf{b}'} = 1\mathbf{c}' = 100101\ .$$

The 5-qubit circuit in figure 12 itself is obtained by the construction in the proof of lemma 10. In particular, this construction gives the decomposition

$$\begin{aligned}\exp\left(\mathrm{i}\frac{\theta}{2}X(\mathbf{c},\mathbf{c}')\right) &= \exp\left(\mathrm{i}\frac{\theta}{2}X(01010,00101)\right)\\ &= \Lambda_5^1\left(\mathrm{iSw}_{34}^\dagger\right)U^{(1)}(00110,00101)\,\Lambda_5^1(\mathrm{iSw}_{34})\end{aligned} \tag{149}$$

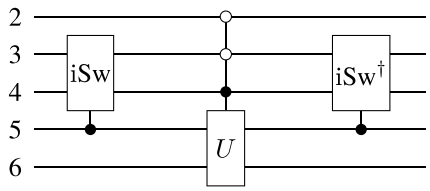


Figure 12. The circuit for realizing the 5-qubit unitary $\exp\left(\mathrm{i}\frac{\theta}{2}X(\mathbf{c},\mathbf{c}')\right)$, where $\mathbf{c}=01010$ and $\mathbf{c}'=00101$. The qubits shown here correspond to the qubits 2 to 6 in figure 11. Based on this circuit, we construct the first part of the circuit in figure 11, which realizes the unitary $\mathbb{R}_x(\frac{\theta}{2},\mathbf{b},\mathbf{b}')=\mathbb{R}_x(\frac{\theta}{2},\bar{\mathbf{b}},\overline{\mathbf{b}'})$ on 6 qubits.

which corresponds to the circuit in figure 12[11]. Here, $U^{(1)}$ and U are defined through equation (76) as

$$U=\begin{pmatrix}1 & & \\ & U^{(1)} & \\ & & 1\end{pmatrix}, \tag{150a}$$

$$U^{(1)}=\begin{pmatrix}\mathrm{i} & \\ & 1\end{pmatrix}e^{\mathrm{i}\frac{\theta}{2}X}\begin{pmatrix}-\mathrm{i} & \\ & 1\end{pmatrix}=\exp\left[\mathrm{i}\frac{\theta}{2}\begin{pmatrix} & \mathrm{i}\\ -\mathrm{i} & \end{pmatrix}\right] \tag{150b}$$

$$U^{\times}:=(X\otimes X)\,U\,(X\otimes X)\ , \tag{150c}$$

where the matrix representation for U is written in the computational basis of qubits 5 and 6 with the ordering $|00\rangle_{65},|01\rangle_{65},|10\rangle_{65},|11\rangle_{65}$, with qubit 6 first.

6.5. The full set of realizable unitaries with *XY* interactions (completing the proof of theorem 4)

Putting everything together, we obtain a method for implementing a general unitary satisfying the conditions in theorem 4, using the XY interaction alone. As emphasized in lemma 14, the additional $\mathbb{Z}_2$ symmetry of XY interaction allows us to restrict our attention to the subspace with Hamming weight $\leqslant n/2$; if the implemented unitary coincides with the desired unitary in this subspace, then it is equal to the desired unitary. In section 6.3, we constructed the 4-level unitary $U^{(1)}(\mathbf{b},\mathbf{b}')U^{(1)}(\bar{\mathbf{b}},\overline{\mathbf{b}'})$, which assuming $w(\mathbf{b})<n/2$ acts as a 2-level unitary in this subspace.

Now, suppose one wants to implement a unitary V satisfying equations (83)–(86), namely $V\in\mathcal{SV}_n^{\mathrm{U}(1)}$ that satisfies the $\mathbb{Z}_2$ symmetry as well as the corresponding determinant constraint in equation (86). Using the techniques of section 5 step 3, we obtain a circuit C containing $\mathcal{O}(4^n/\sqrt{n})$ number of gates $U^{(1)}(\mathbf{b},\mathbf{b}')$ with $w(\mathbf{b})<n/2$ that realizes V in the subspace $\mathcal{H}^{(<n/2)}$. Notice that the resulting unitary acts trivially on the subspace orthogonal to $\mathcal{H}^{(<n/2)}$.

Then, replacing each unitary $U^{(1)}(\mathbf{b},\mathbf{b}')$ in this circuit with 4-level unitaries $U^{(1)}(\mathbf{b},\mathbf{b}')U^{(1)}(\bar{\mathbf{b}},\overline{\mathbf{b}'})$, we obtain a circuit C' that respects the $\mathbb{Z}_2$ symmetry, and behaves identical to C in $\mathcal{H}^{(<n/2)}$, and hence realize the desired unitary V in subspace $\mathcal{H}^{(<n/2)}$. From section 6.3, each unitary $U^{(1)}(\mathbf{b},\mathbf{b}')U^{(1)}(\bar{\mathbf{b}},\overline{\mathbf{b}'})$ with $w(\mathbf{b})=w(\mathbf{b}')$ can be implemented with $\mathcal{O}(n^2)$ gates $\exp(\mathrm{i}\alpha R):\alpha\in(-\pi,\pi]$.

Additionally, if n is even, using the techniques developed in section 6.4, we can construct a circuit with gates $\exp(\mathrm{i}\alpha R):\alpha\in(-\pi,\pi]$ to implement $V^{(n/2)}$, the component of V in the sector with Hamming weight $n/2$. Combining this circuit with C', the resulting circuit implements V in the sectors of Hamming weights $0,\ldots,\lceil n/2\rceil$. By lemma 14, the resulting circuit realizes V in the full n-qubit Hilbert space.

The total number of gates $\exp(\mathrm{i}\alpha R):\alpha\in(-\pi,\pi]$ in this circuit is

$$\mathcal{O}\left(n^2\right)\times\mathcal{O}\left(\frac{4^n}{\sqrt{n}}\right)+\mathcal{O}\left(4^n n\right)=\mathcal{O}\left(4^n n^{3/2}\right)\ . \tag{151}$$

6.6. Breaking the $\mathbb{Z}_2$ symmetry of *XY* interaction with a single ancilla qubit

We have fully characterized $\mathcal{G}_n$, the set of realizable unitary transformations with XY interaction alone (without ancilla qubits). Namely, this is the set of unitaries satisfying all constraints equations (83)–(86),

[11] In particular, the sequence of bit strings in equation (68), which gives the above circuit, is

$$\mathbf{b}=\underset{l_1r_1l_2r_2}{01010}\to 00110\to 00101=\mathbf{b}'\,.$$

The controlled-iSWAP circuit in equation (72) reads $K=\Lambda^1_{l_2}(\mathrm{iSw}_{l_1,r_1})=\Lambda^1_5(\mathrm{iSw}_{34})$, which is the controlled-iSWAP gate acting on qubits 3 and 4 with the control qubit being qubit 5, the second last qubit in figure 11 and in figure 12.

where equation (86) is relevant only in the case of even n. Next, we show that how one can lift the two constraints related to the $\mathbb{Z}_2$ symmetry, i.e. equations (83) and (86), using a single ancilla qubit in the initial state $|0\rangle$ or $|1\rangle$, which fully breaks the symmetry (In this case the ancilla can be interpreted as a quantum reference frame or asymmetry catalyst [45]).

In particular, for any unitary $V \in \mathcal{SV}_n^{\mathrm{U}(1)}$, the unitary

$$V' = V \otimes |0\rangle\langle 0| + \left(X^{\otimes n} V X^{\otimes n}\right) \otimes |1\rangle\langle 1| \,, \tag{152}$$

satisfies

$$V'\left(|\psi\rangle \otimes |0\rangle\right) = \left(V|\psi\rangle\right) \otimes |0\rangle \,, \tag{153}$$

for all n-qubit states $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. In the following, we show that this unitary satisfies all the constraints in equations (83)–(86), and therefore is realizable with XY interaction alone.

First, it is straightforward to see that

$$X^{\otimes(n+1)} V' X^{\otimes(n+1)} = V' \,, \tag{154}$$

and

$$\left(\sum_{j=1}^{n+1} Z_j\right) V' = V' \left(\sum_{j=1}^{n+1} Z_j\right) \,. \tag{155}$$

Next, to verify the constraints in equations (85) and (86), note that the component of V' in the sector with Hamming weight $m = 0, \cdots, n+1$ is

$$V'^{(m)} = V^{(m)} \otimes |0\rangle\langle 0| + X^{\otimes n} V^{(n+1-m)} X^{\otimes n} \otimes |1\rangle\langle 1| \,, \tag{156}$$

where $V^{(m)} = \Pi^{(m)} V \Pi^{(m)}$ is the component of V in the sector with Hamming weight m, and $V'^{(m)}$ and $V^{(n+1-m)}$ are defined in a similar fashion. Then,

$$\det\left(V'^{(m)}\right) = \det\left(V^{(m)}\right) \times \det\left(V^{(n+1-m)}\right) = 1 \,, \tag{157}$$

which implies condition in equation (85) is satisfied. Finally, we show that when $n+1$ is even, V' also satisfies the condition in equation (86). To see this note that

$$V'^{(\frac{n+1}{2})} = V^{(\frac{n+1}{2})} \otimes |0\rangle\langle 0| + X^{\otimes n} V^{(\frac{n+1}{2})} X^{\otimes n} \otimes |1\rangle\langle 1| \,. \tag{158}$$

Suppose $V^{((n+1)/2)}$ has the eigendecompostion

$$V^{(\frac{n+1}{2})} = \sum_j e^{\mathrm{i}\theta_j} |\psi_j\rangle\langle\psi_j| \,, \tag{159}$$

where $\{|\psi_j\rangle\}$ is an orthonormal basis for the subspace of $(\mathbb{C}^2)^{\otimes n}$ with Hamming weight $(n+1)/2$. Then, one can easily see from equations (152) and (159) that $V'^{(\frac{n+1}{2})}$ has the eigen-decomposition

$$\begin{aligned} V'^{(\frac{n+1}{2})} &= \sum_j e^{\mathrm{i}\theta_j} \left(|\psi_j\rangle\langle\psi_j| \otimes |0\rangle\langle 0| + X^{\otimes n}|\psi_j\rangle\langle\psi_j| X^{\otimes n} \otimes |1\rangle\langle 1|\right) \\ &= \sum_j e^{\mathrm{i}\theta_j} \left(|\Psi_j^+\rangle\langle\Psi_j^+| + |\Psi_j^-\rangle\langle\Psi_j^-|\right) \,, \end{aligned} \tag{160}$$

where

$$|\Psi_j^\pm\rangle = \frac{|\psi_j\rangle \otimes |0\rangle \pm X^{\otimes n}|\psi_j\rangle \otimes |1\rangle}{\sqrt{2}} \,, \tag{161}$$

is an orthonormal basis for the eigen-subspace of $(\mathbb{C}^2)^{\otimes(n+1)}$ with Hamming weight $(n+1)/2$, and satisfies

$$X^{\otimes(n+1)} |\Psi_j^\pm\rangle = \pm |\Psi_j^\pm\rangle \,. \tag{162}$$

This immediately implies that

$$V'^{(\frac{n+1}{2})} = V'^{(\frac{n+1}{2},+)} \oplus V'^{(\frac{n+1}{2},-)} \,, \tag{163}$$

where

$$V'^{(\frac{n+1}{2},\pm)} = \sum_j e^{i\theta_j} |\Psi_j^{\pm}\rangle\langle\Psi_j^{\pm}| \,, \tag{164}$$

is the component of $V'^{(\frac{n+1}{2})}$ in the eigen-subspace of $X^{\otimes(n+1)}$ with eigenvalue ± 1. We conclude that

$$\det\left(V'^{(\frac{n+1}{2},\pm)}\right) = \prod_j e^{i\theta_j} = \det\left(V^{(\frac{n+1}{2})}\right) = 1 \,, \tag{165}$$

where here the determinant is the product of non-zero eigenvalues.

We conclude that the condition in equation (86) is also satisfied. In summary, we showed that

Corollary 17. *Any unitary transformation in $\mathcal{SV}_n^{U(1)}$ can be realized using 2-qubit gates $\exp(i\alpha R) : \alpha \in (-\pi, \pi]$ and a single ancilla qubit.*

6.7. All energy-conserving unitaries with 2 ancilla qubits

Finally, combining this with the result of section 5 step 4 that allows us to circumvent the constraints in equation (85) with an ancilla qubit, we can implement a general energy-conserving unitary (up to a global phase) using only XY interaction and 2 ancilla qubits.

In particular, in section 5 step 4 we showed that for any n-qubit energy-conserving unitary $V \in \mathcal{V}_n^{\mathrm{U}(1)}$, there exists a unitary in $\widetilde{V} \in \mathcal{SV}_{n+1}^{\mathrm{U}(1)}$, such that

$$\widetilde{V}(|\psi\rangle \otimes |0\rangle_{\mathrm{anc1}}) = (V|\psi\rangle) \otimes |0\rangle_{\mathrm{anc1}} \,, \tag{166}$$

for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. Furthermore, from section 6.6,

$$\widetilde{V}' = \widetilde{V} \otimes |0\rangle\langle 0| + X^{\otimes(n+1)} \widetilde{V} X^{\otimes(n+1)} \otimes |1\rangle\langle 1| \,, \tag{167}$$

satisfies

$$\widetilde{V}'(|\Psi\rangle \otimes |0\rangle_{\mathrm{anc2}}) = \left(\widetilde{V}|\Psi\rangle\right) \otimes |0\rangle_{\mathrm{anc2}} \,, \tag{168}$$

for all $|\Psi\rangle \in \mathbb{C}^{\otimes(n+1)}$. Moreover, since $\widetilde{V} \in \mathcal{SV}_{n+1}^{\mathrm{U}(1)}$, the argument in the previous section implies that $\widetilde{V}'$ is realizable with XY interaction alone. Choosing $|\Psi\rangle = |\psi\rangle \otimes |0\rangle$ we conclude that

$$\widetilde{V}'(|\psi\rangle \otimes |0\rangle_{\mathrm{anc1}} \otimes |0\rangle_{\mathrm{anc2}}) = (V|\psi\rangle) \otimes |0\rangle_{\mathrm{anc1}} \otimes |0\rangle_{\mathrm{anc2}} \,, \tag{169}$$

for all n qubit state $|\psi\rangle$. This completes the proof of the last part of theorem 1.

7. Approximate universality

For some applications, e.g. in the context of quantum computing, we are interested in the notion of *approximate* universality, where the desired unitary can be implemented using gates from a finite elementary gate set, for instance, S gate and $\sqrt{\mathrm{iSWAP}}$. Clearly, with finite number of gates from this finite gate set, generic energy-conserving unitary V can only be realized with a non-zero error, which can be quantified by the operator norm distance

$$\|V - V'\|_\infty := \sup_{|\psi\rangle : \||\psi\rangle\| = 1} \|(V - V')|\psi\rangle\| \,, \tag{170}$$

where V' is the realized unitary.

In the following we show that for $n = 2$ qubits, any desired energy-conserving unitary in $\mathcal{SV}_2^{U(1)}$ can be realized with arbitrary small error using T and $\sqrt{\mathrm{iSWAP}}$ gates whereas this is not possible if one uses $S = T^2$ instead of T. In the latter case, the generated group is finite, and hence is not dense in $\mathcal{SV}_2^{U(1)}$. On the other hand, in the case of $n \geqslant 3$ qubits T gates are not needed: Any desired element of $\mathcal{SV}_n^{U(1)}$ can be realized with single-qubit S gate and $\sqrt{\mathrm{iSWAP}}$ gate, with arbitrary small error.

The results in this section rely on the Solovay–Kitaev theorem [1, 50]. In particular, we use a recent variant of this result [51], which states that, for any gate set that generates a dense subgroup of $\mathrm{SU}(d)$, if the inverse of each gate is contained in the gate set, then any $V \in \mathrm{SU}(d)$ can be approximated to precision ϵ with

$$N = \mathcal{O}\left(\log^{\nu}\left(\epsilon^{-1}\right)\right) \,, \tag{171}$$

number of gates in the gate set, where

$$\nu > \log_{(1+\sqrt{5})/2} 2 \approx 1.44042\ . \tag{172}$$

Furthermore, the sequences that achieve this bound can be found efficiently.

7.1. Approximate semi-universality of $T + \sqrt{\text{iSWAP}}$ for 2 qubits

Here, we show how a general 2-qubit unitary in $\mathcal{SV}_2^{U(1)}$, i.e. a unitary in the form

$$V = \begin{pmatrix} 1 & & \\ & V^{(1)} & \\ & & 1 \end{pmatrix} : V^{(1)} \in \mathrm{SU}(2)\ ,$$

can be realized with arbitrary small error using T and $\sqrt{\text{iSWAP}}$ gates.

Recall that in the case of 2 qubits, any element of $\mathcal{SV}_2^{U(1)}$ can be realized with S gate and $\exp(i\alpha R) : \alpha \in (-\pi, \pi]$ gate (see the circuit below equation (45)). Luckily equation (32) indicates that the approximate implementation of the gate $\exp(\mathrm{i}\alpha R)$ can be fully characterized using the same techniques and results that have been previously developed in the case of approximate single-qubit unitaries. To see this, recall the correspondence in equation (34) which implies $\sqrt{\text{iSWAP}}$ and $\exp(\mathrm{i}\alpha Z)$ gates acts as $\exp(\mathrm{i}\pi X/4)$ and rotation around z in the subspace spanned by $|01\rangle$ and $|10\rangle$. Using the standard results in quantum computing, one can show that $\exp(\mathrm{i}\pi X/4)$ and $\exp(\mathrm{i}\pi Z/8)$ generate a dense subgroup of SU(2). To see this note that

$$S^\dagger \exp(\mathrm{i}\pi X/4) S^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H\ , \tag{173}$$

which is the Hadamard gate. But, it is well-known that T and H gates together generate a dense subgroup of SU(2) [1, 59]. Combined with the above equation and the fact that $S^\dagger = T^6$, this implies that T and $\exp(\mathrm{i}\pi X/4)$ generate a dense subgroup of SU(2).

We conclude that any $V^{(1)} \in \mathrm{SU}(2)$ can be approximately implemented with T and $\exp(\mathrm{i}\pi X/4)$ gates. By the correspondence in equation (34), this further implies that any $V \in \mathcal{SV}_2^{U(1)}$ can be approximated with the same number of T and $\sqrt{\text{iSWAP}}$ gates. In particular, there exists $\widetilde{V}$, such that $\|V - \widetilde{V}\|_\infty \leqslant \epsilon$ and $\widetilde{V}$ can be realized with $\mathcal{O}(\log^\nu(\epsilon^{-1}))$ of T and $\sqrt{\text{iSWAP}}$ gates, for any $\nu > \log_{(1+\sqrt{5})/2} 2$. Indeed, the above observation implies that one can use the standard existing softwares for approximate implementation of single-qubit gates with H and T gates, to find the sequence of $\sqrt{\text{iSWAP}}$ and T gates that realize any 2-qubit energy-conserving unitary V in the above form.

7.2. Approximate semi-universality of $S + \sqrt{\text{iSWAP}}$ for 3 qubits

Next, we study the case of $n = 3$ qubits. As the first setp, we characterize the group generated by $\sqrt{\text{iSWAP}}$ gates alone. Consider the subgroup of 3-qubit unitaries $\mathcal{SV}_3^{U(1)}$ satisfying the additional $\mathbb{Z}_2$ symmetry in equation (83), i.e.,the group

$$\mathcal{G}_3 = \left\{ U \in \mathcal{SV}_3^{U(1)} : X^{\otimes 3} U X^{\otimes 3} = U \right\}\ . \tag{174}$$

Relative to the computational basis with the following (unconventional) ordering

$$|000\rangle;\ |001\rangle, |010\rangle, |100\rangle;\ |110\rangle, |101\rangle, |011\rangle;\ |111\rangle\ , \tag{175}$$

elements of $\mathcal{G}_3$ are represented as

$$U = \begin{pmatrix} 1 & & & \\ & U^{(1)} & & \\ & & U^{(1)} & \\ & & & 1 \end{pmatrix} : U^{(1)} \in \mathrm{SU}(3)\ . \tag{176}$$

The symmetries of XY interaction imply that any unitary generated by this interaction on 3 qubits, including $\sqrt{\text{iSWAP}}$ on any pair of qubits, is inside $\mathcal{G}_3$. Conversely, we show that the unitaries generated by $\sqrt{\text{iSWAP}}$ on all pairs of qubits generate a dense subgroup of $\mathcal{G}_3$.

Theorem 18. *Consider the group of 3-qubit unitaries generated by gates*

$$\sqrt{\text{iSWAP}}_{12}\ ,\ \sqrt{\text{iSWAP}}_{23}\ ,\ \sqrt{\text{iSWAP}}_{13}\ . \tag{177}$$

This group is a dense subgroup of $\mathcal{G}_3$ defined in equation (174) (or, equivalently, equation (176)). Hence, by the Solovay–Kitaev theorem, for any unitary $U \in \mathcal{G}_3$ and any $\epsilon > 0$, there exists a sequence $V_1, \cdots, V_N$ of length $N = \mathcal{O}(\log^{\nu}(\epsilon^{-1}))$ of these gates such that $\|U - V_N \cdots V_1\|_\infty \leqslant \epsilon$, where ν is given in equation (172). Furthermore, this sequence can be found efficiently.

The proof of this theorem is presented in section 7.4. Before proving this theorem, we discuss two of its important implications. First, combined with theorem 4, this theorem implies that the group generated by $\sqrt{\text{iSWAP}}$ gates on $n \geqslant 3$ qubits is a dense subgroup of the group $\mathcal{G}_n$.

Second, note that by combining $\mathcal{G}_3$ with a generic energy-conserving unitary, one obtains the group $\mathcal{SV}_3^{\text{U}(1)}$, i.e. the group of all unitaries in the form

$$V = \begin{pmatrix} 1 & & & \\ & V^{(1)} & & \\ & & V^{(2)} & \\ & & & 1 \end{pmatrix} \quad : V^{(1)}, V^{(2)} \in \text{SU}(3)\ , \tag{178}$$

with respect to the basis in equation (175).

Lemma 19. *Suppose a 3-qubit energy-conserving unitary J with respect to the basis in equation (175) has the decomposition*

$$J = \begin{pmatrix} e^{i\phi_0} & & & \\ & J^{(1)} & & \\ & & J^{(2)} & \\ & & & e^{i\phi_3} \end{pmatrix}\ . \tag{179}$$

If $J^{(2)} \neq J^{(1)} e^{\text{i}\gamma}$ for some phase $e^{\text{i}\gamma}$, or equivalently, if $|\text{Tr}(J^{(1)\dagger} J^{(2)})| < 3$, then the group generated by J and $\mathcal{G}_3$ contains a dense subgroup of $\mathcal{SV}_3^{\text{U}(1)}$, i.e. all unitaries in the form of equation (178). In particular, this is the case for $J = S \otimes \mathbb{I} \otimes \mathbb{I}$, where $S = e^{\frac{\text{i}\pi}{4}} R_z(-\frac{\pi}{2}) = \begin{pmatrix} 1 & \\ & \text{i} \end{pmatrix}$.

We prove this lemma in appendix E. Note that the assumption that $J^{(2)} \neq J^{(1)} e^{\text{i}\gamma}$, holds for generic energy-conserving unitary J. It is also worth noting that if instead of S gate, one uses Z gate, i.e., $J = Z \otimes \mathbb{I} \otimes \mathbb{I}$, then this assumption is not satisfied, i.e. $|\text{Tr}(J^{(1)\dagger} J^{(2)})| = 3$. Indeed, it turns out that in this case, even though Z gate breaks the $\mathbb{Z}_2$ symmetry, i.e., does not commute with $X^{\otimes 3}$, it cannot extend $\mathcal{G}_3$ to $\mathcal{SV}_3^{\text{U}(1)}$.

Combing this lemma with theorem 18 we conclude that

Corollary 20. *The group generated by unitaries $\sqrt{\text{iSWAP}}_{12}, \sqrt{\text{iSWAP}}_{23}, \sqrt{\text{iSWAP}}_{13}$ and the single-qubit S gates contains a dense subgroup of $\mathcal{SV}_3^{\text{U}(1)}$.*

7.3. Approximate semi-universality of $S + \sqrt{\text{iSWAP}}$ for $n \geqslant 3$ qubits (proof of corollary 2)

Recall that in proposition 13 and theorem 4 we studied unitaries that can be realized with $\exp(\text{i}R\alpha) : \alpha \in (-\pi, \pi]$ gates, with and without S gates, respectively. The above observation in theorem 18 implies that on a system with $n \geqslant 3$ qubits, and for any pair of qubits i and j, the 2-qubit unitary $\exp(\text{i}\alpha R_{ij}) : \alpha \in (-\pi, \pi]$ can be realized with arbitrary small error using gates $\sqrt{\text{iSWAP}}$ that act on qubits i, j and a third different qubit. Therefore, by combining these results we arrive at

Corollary 21. *For any system with $n \geqslant 3$ qubits:*

- *The group generated by $\sqrt{\text{iSWAP}}$ and single-qubit S gates contains a dense subgroup of $\mathcal{SV}_n^{\text{U}(1)}$.*
- *The group generated by $\sqrt{\text{iSWAP}}$ gate is a dense subgroup of $\mathcal{G}_n$, i.e., the group of unitaries satisfying the 4 conditions in theorem 4.*

As we have seen in theorem 1 and its proof in sections 5 and 6, any energy-conserving unitary on n qubits can be implemented using a unitary in $\mathcal{SV}_{n+1}^{\text{U}(1)}$ and one ancilla qubit or a unitary in $\mathcal{G}_{n+2}$ and 2 ancilla qubits. In both cases we need $\mathcal{O}(4^n n^{3/2})$ gates $\exp(\text{i}R\alpha) : \alpha \in (-\pi, \pi]$. Then, to guarantee that the total error in implementing the desired n-qubit unitary is less than ϵ, it suffices to have the error in implementing each single gate $\exp(\text{i}R\alpha) : \alpha \in (-\pi, \pi]$, less than or equal to $\epsilon' = \epsilon/\mathcal{O}(4^n n^{3/2})$. Then, according to our

theorem 18 this can be achieved with $\mathcal{O}(\log^{\nu}(\epsilon'^{-1})) = \mathcal{O}(\log^{\nu}(4^n n^{3/2}\epsilon^{-1})) = \mathcal{O}((n-\log\epsilon)^{\nu})$ number of $\sqrt{\text{iSWAP}}$ gates. Therefore, in total, to achieve the overall error ϵ in implementing the desired n-qubit unitary we need, at most, $\mathcal{O}(4^n n^{3/2}(n-\log\epsilon)^{\nu})$ number of $\sqrt{\text{iSWAP}}$. This completes the proof of corollary 2.

7.4. Proof of theorem 18

Here, we explain the main steps in the proof of theorem 18. Further details and the proof of lemmas can be found in appendices E and F. The first step in the proof of theorem 18 is the following lemma, which fully characterizes the eigen-decomposition of operator

$$W_{123} := \sqrt{\text{iSWAP}}_{23}\sqrt{\text{iSWAP}}_{13}\,. \tag{180}$$

Lemma 22. *The unitary $W_{123} := \sqrt{\text{iSw}}_{23}\sqrt{\text{iSw}}_{13}$ has 3 distinct eigenvalues, namely $\{1, e^{\pm i\theta}\}$, where*

$$\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8} = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\,, \tag{181}$$

and $\theta \approx 0.348886\pi$ is an irrational multiple of π. Each eigenvalue $e^{\pm i\theta}$ has multiplicity two with eigenvectors $|\psi_{\pm\theta}\rangle$ and $X^{\otimes 3}|\psi_{\pm\theta}\rangle$, where

$$|\psi_{+\theta}\rangle := \frac{1}{\sqrt{5-2\sqrt{2}}}\left(|001\rangle + \zeta|010\rangle + \zeta^*|100\rangle\right) \tag{182}$$

$$|\psi_{-\theta}\rangle := \frac{1}{\sqrt{5-2\sqrt{2}}}\left(|001\rangle - \zeta^*|010\rangle - \zeta|100\rangle\right)\,, \tag{183}$$

and

$$\zeta := \frac{\sqrt{5-2\sqrt{2}}}{2} + \frac{\sqrt{2}-1}{2}\mathrm{i}\,. \tag{184}$$

In summary,

$$W_{123} := \sqrt{\text{iSw}}_{23}\sqrt{\text{iSw}}_{13} = \exp\left(\theta A_{123}\right)\,, \tag{185}$$

where $A_{123} := \mathrm{i}(P_+ - P_-)$ and

$$P_{\pm} := |\psi_{\pm\theta}\rangle\langle\psi_{\pm\theta}| + X^{\otimes 3}|\psi_{\pm\theta}\rangle\langle\psi_{\pm\theta}|X^{\otimes 3}\,. \tag{186}$$

See appendix F for the proof of this lemma. The fact that θ/π is an irrational number, i.e., $e^{i\theta}$ is an irrational rotation, follows from the same argument that previously established [59] the universality of H and T gates for a single qubit (see appendix F).

For the following applications, we present the explicit form of A_{123} in the computational basis relative to the order in equation (175):

$$A_{123} = \begin{pmatrix} 0 & & \\ & A^{(1)}_{123} & \\ & & A^{(1)}_{123} \\ & & & 0 \end{pmatrix},\ A^{(1)}_{123} := \begin{pmatrix} 0 & \mathrm{i}\alpha & \mathrm{i}\alpha \\ \mathrm{i}\alpha & 0 & -\beta \\ \mathrm{i}\alpha & \beta & 0 \end{pmatrix},$$
$$\alpha = \left(5-2\sqrt{2}\right)^{-\frac{1}{2}} \approx 0.678598$$
$$\beta = \left(7+4\sqrt{2}\right)^{-\frac{1}{2}} \approx 0.281085. \tag{187}$$

The significance of an irrational rotation is that its repeated application generates a dense subgroup of U(1) (see, e.g. chapter 4.5 of [2]). Applying this result to $W_{123} = e^{\theta A_{123}}$, we conclude that for any $t \in \mathbb{R}$ and any $\delta > 0$, there exists an integer k such that $\|(e^{\theta A_{123}})^k - e^{tA_{123}}\|_{\infty} < \delta$. In other words, any gate in the form of $e^{tA_{123}}$ can be approximated with repeated application of W_{123} to arbitrary precision.

Therefore, applying lemma 22 we know that the group generated by W_{123}, W_{213}, and W_{312} is a dense subgroup of the Lie group generated by unitaries $\exp(tA_{123})$, $\exp(tA_{213})$, $\exp(tA_{312})$, i.e. the group

$$\left\langle \exp\left(tA_{123}\right)\,, \exp\left(tA_{213}\right)\,, \exp\left(tA_{312}\right)\ : t \in \mathbb{R}\right\rangle\,. \tag{188}$$

Clearly, because $A^{(1)}_{123}$ and its permuted versions, $A^{(1)}_{213}$ and $A^{(1)}_{312}$, are traceless and skew-Hermitian, this group is a subgroup of $\mathcal{G}_3$. In the following, we prove that this group is indeed equal to $\mathcal{G}_3$. Since $\mathcal{G}_3$ is a compact connected Lie group, isomorphic to SU(3), it suffices to show that the real Lie algebra generated by $A^{(1)}_{123}$, $A^{(1)}_{213}$, and $A^{(1)}_{312}$, denoted by

$$\mathfrak{h}_3 = \mathfrak{alg}_{\mathbb{R}}\left\{A^{(1)}_{123}, A^{(1)}_{213}, A^{(1)}_{312}\right\}\,, \tag{189}$$

is equal to the Lie algebra $\mathfrak{su}(3)$. First, note that $A^{(1)}_{213}$ can be obtained from $A^{(1)}_{123}$ by exchanging qubits 1 and 2, which results in swapping the last two rows and columns of $A^{(1)}_{123}$ (since the basis vectors are ordered as $|001\rangle, |010\rangle, |100\rangle$) and gives

$$B = \frac{1}{2\beta}\left(A^{(1)}_{123} - A^{(1)}_{213}\right) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathfrak{h}_3\,. \tag{190}$$

Similarly, the permuted versions of this matrix are also in $\mathfrak{h}_3$, i.e.

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathfrak{h}_3\,, \quad \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathfrak{h}_3\,.$$

These matrices generate the Lie algebra $\mathfrak{so}(3)$, i.e. the Lie algebra of real skew-symmetric matrices. Therefore,

$$\mathfrak{so}(3) \subset \mathfrak{h}_3 \subseteq \mathfrak{su}(3)\,. \tag{191}$$

As we explain below, $\mathfrak{h}_3$ has other elements that are still in $\mathfrak{su}(3)$ and not in $\mathfrak{so}(3)$. But, it is well-known that there is no Lie algebra in between $\mathfrak{so}(d)$ and $\mathfrak{su}(d)$, which immediately implies $\mathfrak{h}_3 = \mathfrak{su}(3)$. To show this explicitly, note that

$$C = \frac{1}{2\alpha}\left(A^{(1)}_{123} + A^{(1)}_{213}\right) = \begin{pmatrix} 0 & \mathrm{i} & \mathrm{i} \\ \mathrm{i} & 0 & 0 \\ \mathrm{i} & 0 & 0 \end{pmatrix} \in \mathfrak{h}_3\,. \tag{192}$$

This, in particular, implies

$$\frac{[B,C]+C}{2} = \begin{pmatrix} 0 & 0 & \mathrm{i} \\ 0 & 0 & 0 \\ \mathrm{i} & 0 & 0 \end{pmatrix} \in \mathfrak{h}_3\,. \tag{193}$$

It is straightforward to show that this matrix and its permuted versions, together with matrices in $\mathfrak{so}(3)$ generate the Lie algebra $\mathfrak{su}(3)$.

We conclude that $\mathfrak{h}_3 = \mathfrak{su}(3)$, which in turn implies the group defined in equation (188) is equal to $\mathcal{G}_3$. Combined with lemma 22 this implies that the group generated by W_{123}, W_{312} and W_{231} is a dense subgroup of $\mathcal{G}_3$, which proves the first part of theorem 18.

The second part of the theorem, which bounds the number of the required gates, follows from the Solovay–Kitaev theorem, as stated in equations (171) and (172).

8. Discussion

Building on the previous ideas in the quantum circuit theory [1–3], and, specifically, recent works on symmetric quantum circuits [23, 42], we introduced new circuit synthesis techniques for implementing all energy-conserving unitaries, or, equivalently, all U(1)-invariant unitaries, using XY interaction. We also showed how these techniques can be generalized beyond XY interaction, to all energy conserving interactions that allow qubits to exchange energy (i.e. ,interactions that are not diagonal in the computational basis).

In the introduction, we briefly discussed applications of energy-conserving quantum circuits for suppressing noise in quantum computers. Another important area of application of our results is quantum thermodynamics. In this field, one is often interested in implementing energy-conserving unitaries. Indeed, the resource-theoretic approach to quantum thermodynamics starts with the assumption that all energy-conserving unitaries are free, i.e. ,can be implemented with negligible cost [36–40]. In the context of this resource theory, researchers have developed various protocols utilizing energy-conserving unitaries. However, the problem of implementing energy-conserving unitaries themselves has not been studied much.

In particular, prior to this work, it was not known how a general desired energy-conserving unitary on n qubits can be realized using 2-qubit energy-conserving unitaries.

In addition to quantum thermodynamics, energy-conserving unitaries also play a crucial role in the context of quantum clocks and quantum reference frames [60], covariant error correcting codes [61–63], and the resource theory of asymmetry. (In particular, energy-conserving unitaries are the only unitaries that can be implemented without having access to synchronized clocks.) Other examples of applications of energy-conserving unitaries, or, equivalently circuits with U(1) symmetry, include variational quantum machine learning [64–67], variational quantum eigensolvers for quantum chemistry [68–73], and quantum gravity [74].

Data availability statement

No new data were created or analysed in this study.

Acknowledgment

This work is supported by a collaboration between the US DOE and other Agencies. This material is based upon work supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. Additional support is acknowledged from NSF QLCI Grant OMA-2120757, NSF Phy-2046195, and ARL-ARO QCISS Grant number W911NF-21-1-0005. G B is supported partly by the Hong Kong Research Grant Council (RGC) through the Research Impact Grant R7035-21 F, and partly by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant.

Appendix A. Constraints on the relative phases (proof of equation (18))

In this appendix, we review the argument of [23] that shows how locality restricts realizable unitaries and, in particular, imposes constraints on the relative phases between sectors with different energies. See [23] for further details.

In particular, we show that any unitary V that can be realized with XY interaction local Z Hamiltonian satisfies the constraint

$$\theta_m = \binom{n}{m} \times \left[\frac{m}{n} \times (\theta_n - \theta_0) + \theta_0\right] \ : \ \mathrm{mod}\ 2\pi \ , \tag{18}$$

for all $m = 0, \cdots, n$.

We also show that any energy-conserving unitary V satisfying this constraint has a decomposition as

$$V = e^{\mathrm{i}\alpha} \exp\left(\mathrm{i}\beta Z_j\right) V' \ , \tag{A1}$$

where $\alpha, \beta \in (-\pi, \pi]$, $j \in \{1, \cdots, n\}$ is any arbitrary qubit, and $V' \in \mathcal{SV}_n^{U(1)}$. Recall that according to the first part of theorem 5, which was originally proved in [23] and is also proved using a constructive approach in this paper, we have

$$\mathcal{SV}_n^{\mathrm{U}(1)} \subset G_{XX+YY,Z} \ , \tag{A2}$$

i.e., any unitary in $\mathcal{SV}_n^{\mathrm{U}(1)}$ can be realized with XY and localsingle-qubit Z Hamiltonians. In conclusion, we find that $G_{XX+YY,Z}$ is the subgroup of $\mathcal{V}_n^{\mathrm{U}(1)}$ satisfying equation (18), as stated in theorem 5.

A.1. Proof of equation (18)

Suppose unitary V can be realized with Hamiltonians $H_1, \cdots, H_T$ which all satisfy

$$\left[H_j, \sum_{r=1}^{n} Z_r\right] = 0 \ . \tag{A3}$$

More precisely, assume

$$V = e^{\mathrm{i}\gamma_T H_T} \cdots e^{\mathrm{i}\gamma_1 H_1} \ . \tag{A4}$$

Then, V is energy-conserving, i.e. decomposes as

$$V = \bigoplus_{m=0}^{n} V^{(m)} , \tag{A5}$$

where $V^{(m)}$ is the component of V in the sector with Hamming weight m. Defining

$$\theta_m = \arg\left(\det\left(V^{(m)}\right)\right) , \tag{A6}$$

one can easily show that [23]

$$\theta_m = \sum_{j=1}^{n} \gamma_j \times \mathrm{Tr}\left(\Pi^{(m)} H_j\right) \quad : \mathrm{mod}\ 2\pi . \tag{A7}$$

Suppose each Hamiltonian $H_1, \cdots, H_T$, is either $\mathbb{I}$, $Z_j : j = 1, \cdots n$, or R_{ij}. Then, $\mathrm{Tr}(\Pi^{(m)} H_j)$ is equal to one of the followings

$$\mathrm{Tr}\left(\Pi^{(m)}\right) = \binom{n}{m} \tag{A8a}$$

$$\mathrm{Tr}\left(Z_j \Pi^{(m)}\right) = \frac{n-2m}{n} \times \binom{n}{m} \tag{A8b}$$

$$\mathrm{Tr}\left(R_{ij} \Pi^{(m)}\right) = 0 . \tag{A8c}$$

Here, the second equality follows from

$$\mathrm{Tr}\left(Z_j \Pi^{(m)}\right) = \frac{1}{n} \sum_{j'=1}^{n} \mathrm{Tr}\left(Z_{j'} \Pi^{(m)}\right) \tag{A9}$$

$$= \frac{n-2m}{n} \times \mathrm{Tr}\left(\Pi^{(m)}\right) \tag{A10}$$

$$= \frac{n-2m}{n} \times \binom{n}{m} , \tag{A11}$$

where in the first line we use the permutational symmetry of $\Pi^{(m)}$, and the second line follows from

$$\sum_{j'=1}^{n} Z_{j'} = \sum_{m=0}^{n} (n-2m)\, \Pi^{(m)} . \tag{A12}$$

Finally, note that $\mathrm{Tr}(R_{ij}\Pi^{(m)}) = 0$ follows from the fact that $\langle \mathbf{b}|R_{ij}|\mathbf{b}\rangle = 0$ for all elements of the computational basis.

Then, assuming in decomposition in equation (A4) each Hamiltonian is one of the 3 types $\mathbb{I}$, $Z_r : r = 1, \cdots n$, or R_{ij}, we conclude that

$$\begin{aligned} \theta_m &= \sum_{j=1}^{n} \gamma_j \times \mathrm{Tr}\left(\Pi^{(m)} H_j\right) \\ &= \binom{n}{m} \sum_{j\in A} \gamma_j + \frac{n-2m}{n} \times \binom{n}{m} \sum_{j\in B} \gamma_j \\ &= \binom{n}{m} \left[\alpha + \beta \times (1 - \frac{2m}{n})\right] \quad : \mathrm{mod}\ 2\pi , \end{aligned} \tag{A13}$$

where A and B are subsets of $\{1, \cdots, T\}$ corresponding to all $j \in \{1, \cdots, T\}$, for which $H_j = \mathbb{I}$, and $H_j = Z_r$, respectively, and we have defined

$$\alpha = \sum_{j\in A} \gamma_j \tag{A14a}$$

$$\beta = \sum_{j\in B} \gamma_j . \tag{A14b}$$

Considering $m=0$ and $m=n$, we find

$$\theta_0 = \beta + \alpha \tag{A15}$$
$$\theta_n = -\beta + \alpha\,, \tag{A16}$$

which implies

$$\alpha = \frac{\theta_0+\theta_n}{2} + b\pi \quad : \mathrm{mod}\ 2\pi\,, \tag{A17}$$

and

$$\beta = \frac{\theta_0-\theta_n}{2} + b\pi \quad : \mathrm{mod}\ 2\pi\,, \tag{A18}$$

where $b=0,1$ is unspecified.

Putting these values of α and β in equation (A13) we arrive at

$$\theta_m = \binom{n}{m}\left[\frac{\theta_0+\theta_n}{2} + b\pi + \left(\frac{\theta_0-\theta_n}{2}+b\pi\right)\times\left(1-\frac{2m}{n}\right)\right] \tag{A19}$$
$$= \binom{n}{m}\times\left[\theta_0 - \frac{2m}{n}\left(\frac{\theta_0-\theta_n}{2}+b\pi\right)\right] \quad : \mathrm{mod}\ 2\pi \tag{A20}$$
$$= \binom{n}{m}\times\left[\theta_0\left(1-\frac{m}{n}\right) + \frac{m}{n}\theta_n - b\frac{m}{n}2\pi\right]\,, \tag{A21}$$

where $b=0,1$. Finally, we note that for all $m=1,\cdots,n$, it holds that

$$\binom{n}{m}\times\frac{m}{n}2\pi = \frac{(n-1)!}{(m-1)!\,(n-m)!}2\pi = 0 \quad : \mathrm{mod}\ 2\pi\,. \tag{A22}$$

We conclude that

$$\theta_m = \binom{n}{m}\times\left[\frac{m}{n}\times(\theta_n-\theta_0)+\theta_0\right] \quad : \mathrm{mod}\ 2\pi\,, \tag{A23}$$

which proves equation (18).

Finally, note that multiplying the unitary V with $e^{-\mathrm{i}\alpha}\exp(-\mathrm{i}\beta Z_j)$, where $j=1,\cdots,n$ is an arbitrary qubit, we obtain the energy-conserving unitary

$$V' := e^{-\mathrm{i}\alpha}\exp\left(-\mathrm{i}\beta Z_j\right)V\,, \tag{A24}$$

with the property that $\det(V'^{(m)})=1$, which can be seen by applying equation (A13) to $\theta'_m = \arg(\det(V'^{(m)}))$. Therefore, $V'\in\mathcal{SV}_n^{\mathrm{U}(1)}$, which proves equation (A1).

Appendix B. Proof of lemma 8

First, we show the result for the special case where H is traceless and then extend the result to the general case. Any traceless Hermitian 2×2 matrix can be written as

$$H = \vec{m}\cdot\vec{\sigma} = m_x\sigma_x + m_y\sigma_y + m_z\sigma_z\,, \tag{B1}$$

where $\vec{m}\in\mathbb{R}^3$. Then,

$$SHS^\dagger = m_x\sigma_y - m_y\sigma_x + m_z\sigma_z = \vec{n}\cdot\vec{\sigma}\,, \tag{B2}$$

where $\vec{n}$ is obtained by rotating $\vec{m}$ around the z axis by angle $\pi/2$. Then, unless x and y components of $\vec{m}$ are zero, $\vec{n}\neq\pm\vec{m}$, which in turn implies H does not commute with $SHS^\dagger$. Explicitly, one can check that

$$\mathrm{Tr}\left(\left[H, SHS^\dagger\right]\sigma_z\right) = 4\mathrm{i}\left(m_x^2+m_y^2\right)\,, \tag{B3}$$

which implies the commutator is non-zero, unless $m_x=m_y=0$.

Therefore, $\exp(\mathrm{i}\alpha H)$ and $\exp(\mathrm{i}\alpha SHS^\dagger)$ are rotations around different axes. Then, by Euler decomposition, any special unitary $U \in \mathrm{SU}(2)$ can be realized with a finite sequence of such rotations as

$$U = \prod_{j=1}^{l} \left[\exp\left(\mathrm{i}\alpha_j H\right) S \exp\left(\mathrm{i}\beta_j H\right) S^\dagger\right] , \tag{B4}$$

where $\alpha_j, \beta_j \in \mathbb{R}$, and the length of this sequence, l, is a constant that does not depend on $U \in \mathrm{SU}(2)$.

This proves the lemma when H is traceless. In general, when H is not traceless, the above result implies that for any $U \in \mathrm{SU}(2)$ there exists a sequence in the form of equation (B4) such that

$$\tilde{U} = e^{\mathrm{i}\phi} U = \prod_{j=1}^{l} \left[\exp\left(\mathrm{i}\alpha_j H\right) \exp\left(\mathrm{i}\beta_j SHS^\dagger\right)\right] . \tag{B5}$$

Now recall that any $V \in \mathrm{SU}(2)$ can be decomposed as $V = ABA^\dagger B^\dagger$, for $A, B \in \mathrm{SU}(2)$. Then, from the above result we know that there exists phases $e^{\mathrm{i}\gamma}$ and $e^{\mathrm{i}\delta}$ such that

$$\tilde{A} = e^{\mathrm{i}\gamma} A \quad , \tilde{B} = e^{\mathrm{i}\delta} B, \tag{B6}$$

have decomposition in the form of equation (B4). Then,

$$\tilde{A}\tilde{B}\tilde{A}^\dagger \tilde{B}^\dagger = ABA^\dagger B^\dagger = V . \tag{B7}$$

This implies that when H is not traceless, any element of $V \in \mathrm{SU}(2)$ has a decomposition in the form equation (B4) with $4 \times l$ elements. This completes the proof of the lemma.

Appendix C. Controlled-$R_z(-\frac{\pi}{2})$ using a single ancilla qubit

We saw how based on equation (49) one can obtain a circuit for implementing controlled-Z gate. Other useful unitaries can be obtained in a similar fashion. For instance, one can check the identity

$$\begin{aligned} &\sqrt{\mathrm{iSw}}_{12}\mathrm{iSw}_{13}\sqrt{\mathrm{iSw}}_{23}\mathrm{iSw}_{12}\sqrt{\mathrm{iSw}}_{13}\mathrm{iSw}_{23} \\ &\quad = (-\mathrm{i})\, \exp\left(\mathrm{i}\frac{\pi}{4} Z_1 Z_2\right)\, \exp\left(\mathrm{i}\frac{\pi}{8} Z_3 \left(Z_1 + Z_2\right)\right) , \end{aligned} \tag{C1}$$

where $\sqrt{\mathrm{iSw}}_{ij}$ denotes $\sqrt{\mathrm{iSWAP}}$ gate on qubits i and j. Setting qubit 1 to be $|0\rangle$, and assuming qubits 2 and 3 are in an arbitrary state $|\psi\rangle$, we obtain

$$\begin{aligned} &(-\mathrm{i})\, \exp\left(\mathrm{i}\frac{\pi}{4} Z_1 Z_2\right)\, \exp\left(\mathrm{i}\frac{\pi}{8} Z_3 \left(Z_1 + Z_2\right)\right) \left(|0\rangle_1 |\psi\rangle_{23}\right) \\ &\quad = \left(|0\rangle_1\right) \otimes (-\mathrm{i})\, \exp\left(\mathrm{i}\frac{\pi}{4} Z_2\right)\, \exp\left(\mathrm{i}\frac{\pi}{4} |0\rangle\langle 0|_2 \otimes Z_3\right) |\psi\rangle_{23} . \end{aligned} \tag{C2}$$

Then, one can cancel the unitary $\exp(\mathrm{i}\frac{\pi}{4} Z_2)$ term by applying its inverse. In conclusion, we find that the unitary

$$\exp\left(-\mathrm{i}\frac{\pi}{4} Z_2\right) \sqrt{\mathrm{iSw}}_{12}\mathrm{iSw}_{13}\sqrt{\mathrm{iSw}}_{23}\mathrm{iSw}_{12}\sqrt{\mathrm{iSw}}_{13}\mathrm{iSw}_{23} \tag{C3}$$

implements (up to a global phase) $\exp(\mathrm{i}\frac{\pi}{4}|0\rangle\langle 0|_2 \otimes Z_3)$, the anti-controlled $R_z(\frac{\pi}{2})$ gate on qubits 2 and 3, when qubit 1 is $|0\rangle$. Furthermore, concatenating the above gates with $\exp(-\mathrm{i}\frac{\pi}{4} Z_3)$, one obtain controlled $R_z(-\frac{\pi}{2})$ on qubits 2 and 3.

Appendix D. Proof of lemma 12

Proof. For completeness we include the proof of lemma 12, which follows exactly the proof of a similar result for general unitary transformations (not special unitaries), presented originally in [57] (see also [1, 2]).

The proof is by induction. For $d = 2$, the proposition trivially holds since U itself is in $\mathrm{SU}(2)$. For $d > 2$, assume the proposition holds for any unitary in $\mathrm{SU}(d-1)$. Then, for any $U \in \mathrm{SU}(d)$, let $\mathbf{a} = (a_1, \ldots, a_d)^T$ be its first column of matrix in the basis $|1\rangle, \ldots, |d\rangle$.

For any $a\neq 0$ or $b\neq 0$, define $V(a,b):=(|a|^2+|b|^2)^{-1/2}\begin{pmatrix}a^* & b^*\\ -b & a\end{pmatrix}$, which is an element of SU(2). We define $V(0,0)$ as the identity matrix. This unitary satisfies that

$$V(a,b)\begin{pmatrix}a\\ b\end{pmatrix}=\begin{pmatrix}\sqrt{|a|^2+|b|^2}\\ 0\end{pmatrix}. \tag{D1}$$

Let $V(a,b)_{1,k}$ be the 2-level unitary of $V(a,b)$ acting on the subspace spanned by $|1\rangle$ and $|k\rangle$. If we apply $V(a_1,a_2)$ on the first two components of $\mathbf{a}$, we get

$$V(a_1,a_2)_{1,2}\,\mathbf{a}=\begin{pmatrix}\sqrt{|a_1|^2+|a_2|^2}\\ 0\\ a_3\\ \vdots\\ a_d\end{pmatrix}. \tag{D2}$$

This sets the second component of $\mathbf{a}$ to zero. Further left-multiplying with $V\left(\sqrt{|a_1|^2+|a_2|^2},a_3\right)_{1,3}$, we can set the third component to zero. Repeating this for every other components, we get

$$V\mathbf{a}=(1,0,\ldots,0)^T \tag{D3}$$

$$V:=V\left(\sqrt{\sum_{i=1}^{d-1}|a_i|^2},a_d\right)_{1,d}\ldots V(a_1,a_2)_{1,2} \tag{D4}$$

noting that $\sqrt{\sum_{i=1}^{d}|a_i|^2}=1$. Since U has $\mathbf{a}$ as its first column, VU will be a matrix whose first column is $(1,0,\ldots,0)^T$. Since $VU\in \mathrm{SU}(d)$, its first row must be a unit vector, and thus must be $(1,0,\ldots,0)$. VU therefore has the following block-diagonal form:

$$VU=\begin{pmatrix}1 & \\ & W\end{pmatrix} \tag{D5}$$

where $W\in \mathrm{SU}(d-1)$. By assumption, W can be written as a product of $(d-1)(d-2)/2$ 2-level gates, and V is a product of $d-1$ 2-level gates by definition, thus $U=V^\dagger(1\oplus W)$ can be written as a product of $(d-1)(d-2)/2+d-1=d(d-1)/2$ 2-level unitares in $\mathrm{SU}(d)$. This completes the proof. □

Appendix E. Proof of lemma 19

Recall that

$$\mathcal{G}_3=\left\{U\in \mathcal{SV}_3^{U(1)}: X^{\otimes 3}UX^{\otimes 3}=U\right\}, \tag{E1}$$

and the elements of $\mathcal{G}_3$ have matrix representation

$$U=\begin{pmatrix}1 & & \\ & U^{(1)} & \\ & & U^{(1)}\\ & & & 1\end{pmatrix}\ :U^{(1)}\in \mathrm{SU}(3)\ . \tag{E2}$$

Let $\widetilde{\mathcal{G}}_3$ be the group generated by $\mathcal{G}_3$ and the unitary J. $\mathcal{G}_3$ contains an element U in the form of equation (E1), with $U^{(1)}=e^{i\alpha}J^{(1)\dagger}$, where $e^{i\alpha}$ is a properly chosen phase such that $U^{(1)}$ has determinant 1. It follows that $\widetilde{\mathcal{G}}_3$, being generated by J and $\mathcal{G}_3$, contains UJ, which has the form of

$$UJ=\begin{pmatrix}e^{i\phi_0} & & & \\ & e^{i\alpha}\mathbb{I} & & \\ & & e^{i\alpha}J^{(1)\dagger}J^{(2)} & \\ & & & e^{i\phi_3}\end{pmatrix}. \tag{E3}$$

Furthermore, the assumption of the lemma implies that $e^{i\alpha}J^{(1)\dagger}J^{(2)}$ is not a global phase, i.e. is not in the center of U(3), which means it does not commute with some elements of SU(3). Based on this observation,

we show that the group $\widetilde{\mathcal{G}}_3$ generated by J and $\mathcal{G}_3$ contains $\mathcal{SV}_3^{U(1)}$. (The argument is similar to the proof of Goursat's lemma.)

Consider the elements $\widetilde{\mathcal{G}}_3$ that are in the following form

$$V=\begin{pmatrix} e^{\mathrm{i}\beta_0} & & & \\ & e^{\mathrm{i}\beta_1}\mathbb{I}^{(1)} & & \\ & & V^{(2)} & \\ & & & e^{\mathrm{i}\beta_3} \end{pmatrix} : V\in\widetilde{\mathcal{G}}_3\ , \tag{E4}$$

where $\mathbb{I}^{(1)}$ is the identity operator on the 3D subspace with Hamming weight 1 and $V^{(2)}\in \mathrm{U}(3)$ is an arbitrary unitary on the subspace with Hamming weight 2, and $e^{\mathrm{i}\beta_{0,1,3}}$ are phases. All such unitaries V in the form of equation (E4) constitutes a subgroup of $\widetilde{\mathcal{G}}_3$, denoted as $\widetilde{\mathcal{N}}$. Let $\mathcal{N}$ be the subgroup of U(3) formed from all unitaries $V^{(2)}\in \mathrm{U}(3)$ such that there exists V related to $V^{(2)}$ by equation (E4) and $V\in\widetilde{\mathcal{N}}$. With this definition, equation (E3) implies that

$$e^{\mathrm{i}\alpha}J^{(1)\dagger}J^{(2)}\in\mathcal{N}\ . \tag{E5}$$

Furthermore, it can be easily shown that with this definition, $\mathcal{N}$ is a normal subgroup of U(3). To see this, note that if $V\in\widetilde{\mathcal{N}}$, then for any $U\in\widetilde{\mathcal{G}}_3$, the unitary $UVU^\dagger$ is also in the form given in equation (E4), which means $\widetilde{\mathcal{N}}$ is a normal subgroup of $\widetilde{\mathcal{G}}_3$. Moreover, for any $U^{(1)}\in \mathrm{SU}(3)$ one can choose $U\in\mathcal{G}_3\subset\widetilde{\mathcal{G}}_3$ with decomposition in the form of equation (E2), and $UVU^\dagger\in\widetilde{\mathcal{N}}$ implies $U^{(1)}V^{(2)}U^{(1)\dagger}\in\mathcal{N}$. Finally, we note that any element of U(3) can be written as a global phase times an element of SU(3). In summary, we conclude that if $V^{(2)}\in\mathcal{N}$, then for any $U^{(1)}\in \mathrm{U}(3)$, it holds that $U^{(1)}V^{(2)}U^{(1)\dagger}\in\mathcal{N}$, which means $\mathcal{N}$ is a normal subgroup of U(3).

Next, note that since SU(3) is a simple Lie group, any normal subgroup of U(3) either contains SU(3) or only contains global phases, i.e. is in the center of U(3). But, we just showed that $\mathcal{N}$ contains $e^{\mathrm{i}\alpha}J^{(1)\dagger}J^{(2)}$ and the assumption of lemma implies that this unitary is not in the center of U(3). It follows that $\mathcal{N}$ contains SU(3).

This means that for any $V^{(2)}\in \mathrm{SU}(3)$, there exists $V\in\widetilde{\mathcal{G}}_3$ with decomposition in the form of equation (E4). Furthermore, because SU(3) is a simple Lie group, it is equal to its commutator subgroup. The commutator subgroup generated by elements of $\widetilde{\mathcal{G}}_3$ in the form of equation (E4), contains all elements in the following form

$$\begin{pmatrix} 1 & & & \\ & \mathbb{I}^{(1)} & & \\ & & V^{(2)} & \\ & & & 1 \end{pmatrix} : V^{(2)}\in \mathrm{SU}(3)\ . \tag{E6}$$

Therefore, we find that for any $V^{(2)}\in \mathrm{SU}(3)$, there exists an element of $\widetilde{\mathcal{G}}_3$ with the decomposition in equation (E6). Composing these unitaries with elements of $\mathcal{G}_3$, which are in the form given in equation (E2) one obtains the entire $\mathcal{SV}_3^{U(1)}$, i.e. all unitaries in the form given in equation (178). This completes the proof of the lemma.

Appendix F. Eigenvalues of $W_{123}=\sqrt{\mathrm{iSWAP}}_{23}\sqrt{\mathrm{iSWAP}}_{13}$ (proof of lemma 22)

In this section, we study the eigen-decomposition of operator

$$W_{123}=\sqrt{\mathrm{iSWAP}}_{23}\sqrt{\mathrm{iSWAP}}_{13}\ . \tag{F1}$$

The fact that W_{123} is energy-conserving and respect the $\mathbb{Z}_2$ symetry $X^{\otimes 3}W_{123}X^{\otimes 3}=W_{123}$ implies that with the ordering in equation (175), it has a decomposition as

$$W=\begin{pmatrix} 1 & & & \\ & W_{123}^{(1)} & & \\ & & W_{123}^{(1)} & \\ & & & 1 \end{pmatrix},\quad \text{where}\quad W_{123}^{(1)}=\frac{1}{2}\begin{pmatrix} 1 & \mathrm{i}\sqrt{2} & \mathrm{i} \\ \mathrm{i} & \sqrt{2} & -1 \\ \mathrm{i}\sqrt{2} & 0 & \sqrt{2} \end{pmatrix}. \tag{F2}$$

The eigenvalues of $W_{123}^{(1)}$ are $\{1,e^{\pm\mathrm{i}\,\theta}\}$, where

$$e^{\mathrm{i}\theta}=-\frac{1}{4}+\frac{\sqrt{2}}{2}+\frac{\sqrt{7+4\sqrt{2}}}{4}\mathrm{i}\ , \tag{F3}$$

and θ satisfies equation (181). The eigenvalues of W_{123} are thus the same as $W_{123}^{(1)}$, ignoring multiplicity.

To show that θ/π is an irrational number, i.e. $e^{i\theta}$ is a irrational rotation, we use an argument that was previously used in [59] to show the universality of H and T gates. To link W_{123} with H and T, we compute the characteristic polynomial of $W_{123}^{(1)}$ as

$$\det\left(\lambda\mathbb{I}-W_{123}^{(1)}\right)=(\lambda-1)\left(\lambda^2-\sqrt{2}\lambda+\frac{1}{2}\lambda+1\right). \tag{F4}$$

On the other hand, in the proof of universality of H and T gates, it is shown that the gate sequence $HTHT$ generates an irrational rotation [2]. More specifically, the characteristic polynomial of $e^{i\frac{3}{2}\pi}(HTHT)^2$ (where the global phase $e^{i\frac{3}{2}\pi}$ is added to make the resulting gate in SU(2)) is

$$\det\left(\lambda\mathbb{I}-e^{i\frac{3}{2}\pi}(HTHT)^2\right)=\lambda^2-\sqrt{2}\lambda+\frac{1}{2}\lambda+1\,, \tag{F5}$$

which is a factor of the polynomial in equation (F4). The roots of this polynomial are exactly $e^{\pm i\theta}$.

This shows that the two complex eigenvalues of $W_{123}^{(1)}$ (and thus W), $e^{\pm i\theta}$, are exactly the eigenvalues of $e^{i\frac{3}{2}\pi}(HTHT)^2$. The result that $HTHT$ gives an irrational rotation indicates that $e^{\pm i\theta}$ is an irrational rotation.

The original proof of $e^{\pm i\theta}$ being an irrational rotation uses the following lemma:

Lemma 23 ([59]). *Let $e^{i\theta}$ be the root of a minimum monic polynomial $p(x)$ over the field of rational numbers. Then $e^{i\theta}$ is rational rotation if and only if $p(x)$ is a cyclotomic polynomial.*

The minimum monic polynomial for $e^{i\theta}$ is $x^4+x^3+\frac{1}{4}x^2+x+1$, which is not cyclotomic [59]. Therefore, by lemma 23, $e^{i\theta}$ is an irrational rotation.

ORCID iD

Iman Marvian https://orcid.org/0000-0001-6719-061X

References

[1] Kitaev A Y, Shen A, Vyalyi M N and Vyalyi M N 2002 *Classical and Quantum Computation* (American Mathematical Society)
[2] Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information* (Cambridge University Press)
[3] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev.* A **52** 3457
[4] Deutsch D 1985 Quantum theory, the church–turing principle and the universal quantum computer *Proc. R. Soc.* A **400** 97–117
[5] Deutsch D E, Barenco A and Ekert A 1995 Universality in quantum computation *Proc. R. Soc.* A **449** 669–77
[6] DiVincenzo D P 1995 Two-bit gates are universal for quantum computation *Phys. Rev.* A **51** 1015
[7] Lloyd S 1995 Almost any quantum logic gate is universal *Phys. Rev. Lett.* **75** 346
[8] Möttönen M, Vartiainen J J, Bergholm V and Salomaa M M 2004 Quantum circuits for general multiqubit gates *Phys. Rev. Lett.* **93** 130502
[9] Imamog A, Awschalom D D, Burkard G, DiVincenzo D P, Loss D, Sherwin M and Small A 1999 Quantum information processing using quantum dot spins and cavity QED *Phys. Rev. Lett.* **83** 4204
[10] Warren A, Barnes E and Economou S E 2019 Long-distance entangling gates between quantum dot spins mediated by a superconducting resonator *Phys. Rev.* B **100** 161303
[11] Burkard G, Ladd T D, Pan A, Nichol J M and Petta J R 2023 Semiconductor spin qubits *Rev. Mod. Phys.* **95** 025003
[12] Bialczak R C *et al* 2010 Quantum process tomography of a universal entangling gate implemented with Josephson phase qubits *Nat. Phys.* **6** 409–13
[13] Abrams D M, Didier N, Johnson B R, da Silva M P and Ryan C A 2020 Implementation of *XY* entangling gates with a single calibrated pulse *Nat. Electron.* **3** 744–50
[14] Sung Y *et al* 2021 Realization of high-fidelity CZ and ZZ-free iswap gates with a tunable coupler *Phys. Rev.* X **11** 021058
[15] Houck A A *et al* 2007 Generating single microwave photons in a circuit *Nature* **449** 328–31
[16] Johansson J, Saito S, Meno T, Nakano H, Ueda M, Semba K and Takayanagi H 2006 Vacuum rabi oscillations in a macroscopic superconducting qubit LC oscillator system *Phys. Rev. Lett.* **96** 127006
[17] Abrams D M, Didier N, Johnson B R, da Silva M P and Ryan C A 2019 Implementation of the *XY* interaction family with calibration of a single pulse (arXiv:1912.04424)
[18] Lloyd S, Mohseni M and Rebentrost P 2014 Quantum principal component analysis *Nat. Phys.* **10** 631–3
[19] Marvian I and Lloyd S 2016 Universal quantum emulator (arXiv:1606.02734)
[20] Kimmel S, Yen-Yu Lin C, Hao Low G, Ozols M and Yoder T J 2017 Hamiltonian simulation with optimal sample complexity *npj Quantum Inf.* **3** 1–7
[21] Pichler H, Zhu G, Seif A, Zoller P and Hafezi M 2016 Measurement protocol for the entanglement spectrum of cold atoms *Phys. Rev.* X **6** 041033
[22] Schuch N and Siewert J 2003 Natural two-qubit gate for quantum computation using the *XY* interaction *Phys. Rev.* A **67** 032301
[23] Marvian I 2022 Restrictions on realizable unitary operations imposed by symmetry and locality *Nat. Phys.* **18** 283–89

[24] Ball H, Oliver W D and Biercuk M J 2016 The role of master clock stability in quantum information processing *npj Quantum Inf.* **2** 1–8
[25] DiVincenzo D P 1998 Quantum gates and circuits *Proc. R. Soc.* A **454** 261–76
[26] Shende V V and Markov I L 2008 On the cnot-cost of toffoli gates (arXiv:0803.2316)
[27] Lidar D A, Chuang I L and Birgitta Whaley K 1998 Decoherence-free subspaces for quantum computation *Phys. Rev. Lett.* **81** 2594
[28] Bacon D, Kempe J, Lidar D A and Whaley K B 2000 Universal fault-tolerant quantum computation on decoherence-free subspaces *Phys. Rev. Lett.* **85** 1758–61
[29] DiVincenzo D P, Bacon D, Kempe J, Burkard G and Birgitta Whaley K 2000 universal quantum computation with the exchange interaction *Nature* **408** 339–42
[30] Zanardi P and Rasetti M 1997 Noiseless quantum codes *Phys. Rev. Lett.* **79** 3306
[31] Kempe J and Birgitta Whaley K 2002 Exact gate sequences for universal quantum computation using the *XY* interaction alone *Phys. Rev.* A **65** 052330
[32] Brod D J and Childs A M 2013 The computational power of matchgates and the *XY* interaction on arbitrary graphs (arXiv:1308.1463)
[33] Kempe J, Bacon D, DiVincenzo D P and Whaley K B 2001 Encoded universality from a single physical interaction *Quantum Inf. Comput.* **1** 33–55
[34] Lidar D A and Wu L-A 2001 Reducing constraints on quantum computer design by encoded selective recoupling *Phys. Rev. Lett.* **88** 017905
[35] Preskill J 2018 Quantum computing in the NISQ era and beyond (arXiv:1801.00862)
[36] Horodecki M and Oppenheim J 2013 Fundamental limitations for quantum and nanoscale thermodynamics *Nat. Commun.* **4** 1–6
[37] Brandao F G S L, Horodecki M, Oppenheim J, Renes J M and Spekkens R W 2013 Resource theory of quantum states out of thermal equilibrium *Phys. Rev. Lett.* **111** 250404
[38] Janzing D, Wocjan P, Zeier R, Geiss R and Beth T 2000 Thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the second law *Int. J. Theor. Phys.* **39** 2717–53
[39] Lostaglio M, Korzekwa K, Jennings D and Rudolph T 2015 Quantum coherence, time-translation symmetry and thermodynamics *Phys. Rev.* X **5** 021001
[40] Chitambar E and Gour G 2019 Quantum resource theories *Rev. Mod. Phys.* **91** 025001
[41] Lloyd S 1995 Almost any quantum logic gate is universal *Phys. Rev. Lett.* **75** 346
[42] Marvian I 2023 Theory of Quantum Circuits with Abelian Symmetries (arXiv:2302.12466) (To appear in Physical Review Research)
[43] Vatan F and Williams C 2004 Optimal quantum circuits for general two-qubit gates *Phys. Rev.* A **69** 032315
[44] Gour G and Spekkens R W 2008 The resource theory of quantum reference frames: manipulations and monotones *New J. Phys.* **10** 033023
[45] Marvian I and Spekkens R W 2013 The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations *New J. Phys.* **15** 033001
[46] Wigner E P 1952 *Z. Phys.* **133** 101
[47] Araki H and Yanase M M 1960 Measurement of quantum mechanical operators *Phys. Rev.* **120** 622
[48] Nielsen M A and Chuang I L 1997 Programmable quantum gate arrays *Phys. Rev. Lett.* **79** 321
[49] Marvian I and Spekkens R W 2012 An information-theoretic account of the Wigner-Araki-Yanase theorem (arXiv:1212.3378)
[50] Yu Kitaev A 1997 Quantum computations: algorithms and error correction *Russ. Math. Surv.* **52** 1191–249
[51] Kuperberg G 2023 Breaking the cubic barrier in the Solovay-Kitaev algorithm (arXiv:2306.13158)
[52] Jordan P and Wigner E P 1928 About the pauli exclusion principle *Z. Phys* **47** 14–75
[53] Fradkin E 1989 Jordan-Wigner transformation for quantum-spin systems in two dimensions and fractional statistics *Phys. Rev. Lett.* **63** 322
[54] Nielsen M A *et al* 2005 The fermionic canonical commutation relations and the Jordan-Wigner transform *Sch. Phys. Sci. Univ. Queensland* **59** 75
[55] Wang X, Burgarth D and Schirmer S 2016 Subspace controllability of spin-1/2 chains with symmetries *Phys. Rev.* A **94** 052319
[56] Burkard G, DiVincenzo D P, Loss D and Smolin J A 1999 *Phys. Optim. Quantum Error Correction Circuits* **60** 11404
[57] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 Experimental realization of any discrete unitary operator *Phys. Rev. Lett.* **73** 58
[58] Wu L-A and Lidar D A 2002 Power of anisotropic exchange interactions: universality and efficient codes for quantum computing *Phys. Rev.* A **65** 042318
[59] Oscar Boykin P, Mor T, Pulver M, Roychowdhury V and Vatan F 1999 On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis *40th Annual Symp. on Foundations of Computer Science* (*Cat. No. 99CB37039*) (IEEE) pp 486–94
[60] Bartlett S D, Rudolph T and Spekkens R W 2007 Reference frames, superselection rules and quantum information *Rev. Mod. Phys.* **79** 555
[61] Faist P, Nezami S, Albert V V, Salton G, Pastawski F, Hayden P and Preskill J 2020 Continuous symmetries and approximate quantum error correction *Phys. Rev.* X **10** 041018
[62] Hayden P, Nezami S, Popescu S and Salton G 2021 Error correction of quantum reference frame information *PRX Quantum* **2** 010326
[63] Kong L and Liu Z-W 2021 Charge-conserving unitaries typically generate optimal covariant quantum error-correcting codes (arXiv:2102.11835)
[64] Jakob Meyer J, Mularski M, Gil-Fuster E, Anna Mele A, Arzani F, Wilms A and Eisert J 2023 Exploiting symmetry in variational quantum machine learning *PRX Quantum* **4** 010328
[65] Nguyen Q T, Schatzki L, Braccia P, Ragone M, Coles P J, Sauvage F, Larocca M and Cerezo M 2022 Theory for equivariant quantum neural networks (arXiv:2210.08566)
[66] Sauvage F, Larocca M, Coles P J, and Cerezo M 2022 Building spatial symmetries into parameterized quantum circuits for faster training (arXiv:2207.14413)
[67] Zheng H, Li Z, Liu J, Strelchuk S and Kondor R 2023 Speeding up learning quantum states through group equivariant convolutional quantum ansätze *PRX Quantum* **4** 020327

[68] Barron G S, Gard B T, Altman O J, Mayhall N J, Barnes E and Economou S E 2021 Preserving symmetries for variational quantum eigensolvers in the presence of noise *Phys. Rev. Appl.* **16** 034003
[69] Shkolnikov V O, Mayhall N J, Economou S E and Barnes E 2021 Avoiding symmetry roadblocks and minimizing the measurement overhead of adaptive variational quantum eigensolvers (arXiv:2109.05340)
[70] Gard B T, Zhu L, Barron G S, Mayhall N J, Economou S E and Barnes E 2020 Efficient symmetry-preserving state preparation circuits for the variational quantum eigensolver algorithm *npj Quantum Inf.* **6** 10
[71] Streif M, Leib M, Wudarski F, Rieffel E and Wang Z 2021 Quantum algorithms with local particle-number conservation: Noise effects and error correction *Phys. Rev.* A **103** 042412
[72] Wang Z, Rubin N C, Dominy J M and Rieffel E G 2020 X y mixers: analytical and numerical results for the quantum alternating operator ansatz *Phys. Rev.* A **101** 012320
[73] Kl Barkoutsos P *et al* 2018 Quantum algorithms for electronic structure calculations: particle-hole hamiltonian and optimized wave-function expansions *Phys. Rev.* A **98** 022322
[74] Nakata Y, Wakakuwa E and Koashi M 2023 Black holes as clouded mirrors: the Hayden-Preskill protocol with symmetry *Quantum* **7** 928