Toffoli Requires Six Quantum Neighbor Gates

KELI HUANG, University of California, Los Angeles, USA
JENS PALSBERG, University of California, Los Angeles, USA

Toffoli gates are key building blocks in quantum programs, and on most current quantum computers, they must be implemented with smaller gates. Such an implementation requires five 2-qubit gates if we assume that each gate can operate on any two qubits. However, many current quantum computers have only 2-qubit gates that operate on neighboring qubits; we call them neighbor gates. How many neighbor gates are required to implement a Toffoli gate? In this paper, we show that six neighbor gates are necessary and sufficient, and we generalize to a characterization of all 3-qubit diagonal gates.

CCS Concepts: • **Computer systems organization → Quantum computing**; • **Software and its engineering → Compilers**.

Additional Key Words and Phrases: quantum computing, compilers, code size

ACM Reference Format:
Keli Huang and Jens Palsberg. 2025. Toffoli Requires Six Quantum Neighbor Gates. 1, 1 (December 2025), 37 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Background. Researchers are designing quantum algorithms that, in some cases, have an exponential advantage over classical algorithms. They describe their algorithms in the form of quantum circuits that use quantum gates. In a recent trend, many of their papers [Berry et al. 2019, 2024; Goings et al. 2022; Lee et al. 2021; Rubin et al. 2024; Su et al. 2021] express an algorithm's execution time in terms of the number of Toffoli gates. They do that because they anticipate error-corrected quantum computers on which the execution of Toffoli gates will be a bottleneck. Thus, they use Toffoli gates as building blocks that must be compiled to hardware gates.

Toffoli gates are 3-qubit gates and on most current quantum computers, they must be implemented with smaller gates. Thus, the implementation of a Toffoli gate on a given quantum computer has a direct impact on the execution time of quantum algorithms. For such an implementation, five 2-qubit gates are necessary and sufficient, as shown by [Palsberg and Yu 2024; Yu et al. 2013; Yu and Ying 2015], assuming that a 2-qubit gate can operate on any two qubits. In our terminology, such an implementation uses *unrestricted* gates.

Current quantum computers rarely support that a 2-qubit gate can operate on any two qubits. For example, IBM Condor (1,121 qubits) and IBM Osprey (433 qubits) support that a 2-qubit gate operates only on some pairs of qubits. In particular, for any three qubits, they support 2-qubit gates on at most two of the three possible pairs of qubits. They do that because supporting a 2-qubit gate is easier when the two qubits are neighbors on the chip. In our terminology, current quantum computers tend to support *neighbor* gates.

Authors' addresses: Keli Huang, University of California, Los Angeles, USA, kelihuang@cs.ucla.edu; Jens Palsberg, University of California, Los Angeles, USA, palsberg@ucla.edu.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM XXXX-XXXX/2025/12-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

In this paper, we focus on the question of how many 2-qubit neighbor gates are required to implement a Toffoli gate and, more generally, any 3-qubit diagonal gate.

Question: Five or Six? We can implement a Toffoli gate both using five unrestricted gates [Yu et al. 2013], and using six neighbor gates, as we show in Section 3. Here we arrive at our central question: *five or six?* Specifically, can we improve the implementation of a Toffoli gate from using five unrestricted gates to using five neighbor gates? Or, are we forced to use a sixth neighbor gate?

Our Results. We show that six neighbor gates are necessary and sufficient to implement a Toffoli gate. We also generalize this to a characterization of the number of neighbor gates (Theorem 7.1) and the number of unrestricted gates (Theorem 7.2) that are sufficient to implement 3-qubit diagonal gates. In Corollary 7.3, we prove that these upper bounds are indeed least upper bounds.

Our Proof Technique. Figure 1 shows our proof structure. The lower bound for implementations

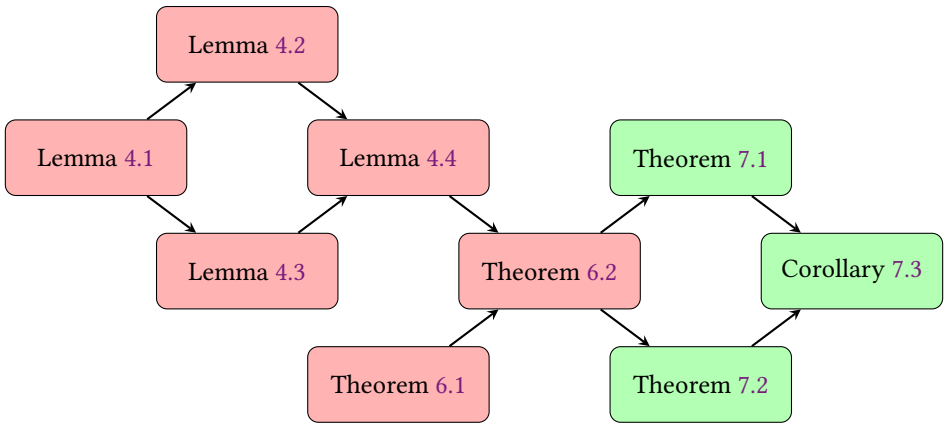


Fig. 1. Proof structure.

of a Toffoli gate is a corollary of Theorem 6.2, which is a novel equivalence between the expressive power of unrestricted gates and the expressive power of neighbor gates. Specifically, Theorem 6.2 says that three classes of quantum circuits implement the same 3-qubit diagonal gates; those classes are (1) four neighbor gates, (2) five neighbor gates, and (3) four unrestricted gates. The most surprising aspect of Theorem 6.2 is the implication (2) $\Rightarrow$ (1), which says that we can transform any circuit with five neighbor gates into an equivalent circuit with four neighbor gates. This may seem like a magic trick: a gate disappeared! We prove Theorem 6.2 by proving the chain of implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

The proof of the implication (2) $\Rightarrow$ (3) is the main technical innovation in this paper: we transform an implementation of a 3-qubit diagonal gate using five neighbor gates into an implementation using four unrestricted gates. We devote Section 4 to proving one particular form of this result (Lemma 4.4), which uses Lemmas 4.1–4.3, and then we use it in Section 6 in the proof of Theorem 6.2 which relies on Theorem 6.1. Our proofs in Section 4 and Section 6 rely on a suite of known lemmas that we list in Appendix A. In particular, we use Lemma A.9 ([Palsberg and Yu 2024, Lemma 6.4]), which characterizes the 3-qubit quantum gates with two controls that can be implemented with four neighbor gates.

A surprising corollary of Theorem 6.2 is that while *four* unrestricted gates and *four* neighbor gates have the *same* expressive power, *five* unrestricted gates have *strictly more* expressive power

than *five* neighbor gates. In particular, five unrestricted gates are sufficient to implement a Toffoli gate, while five neighbor gates are insufficient. Another surprising finding is that, in some cases, the qubit layout affects the optimal number of neighbor gates (Theorem 6.1).

The Rest of the Paper. In Section 2, we recall key quantum concepts, and in Section 3, we show implementations of the Toffoli gate and two other gates. In Section 5, we define some sets of 3-qubit diagonal gates that we use to state our results, and in Sections 4–7, we state and prove our theorems, with the exception of some proofs that we relegated to the appendices. In Section 8, we use our theorems to show that our implementations in Section 3 are optimal, and in Section 9, we discuss related work.

2 QUANTUM CONCEPTS

Qubits, Quantum States, and Quantum Gates. A qubit is a two-dimensional unit vector of complex numbers. An n-qubit quantum state is a 2^n-dimensional unit vector of complex numbers. We use lower-case letters a, b, d, p, q to represent complex numbers. Furthermore, we use lowercase letters, enclosed in Dirac notation, as $|x\rangle$, $|y\rangle$, $|z\rangle$ to range over 1-qubit quantum states.

A quantum gate is a unitary matrix. A matrix U is unitary if $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ is the conjugate transpose of U, and I is the identity matrix. We use uppercase letters, such as U, to range over quantum gates. We will use the following gates.

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$R_z(\alpha) = \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix} \qquad R_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \qquad P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Notice that S is the 2-qubit swap gate, while the others are 1-qubit gates. Also, we have that $HZH = X$, $HXH = Z$, and $H^\dagger = H$. We use Greek letters α, β, γ, φ, and θ to stand for angles ranging from 0 to 2π.

We write an n-qubit diagonal gate with 2^n complex-number entries as $\mathrm{Diag}(d_0,\ d_1,\ \ldots\ , d_{2^n-1})$, where d_i is the $(i+1)^{th}$ element on the diagonal.

For an n-qubit gate U, we define its $(n+1)$-qubit zero-controlled gate as $|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes I$, which applies U to the target qubits when the control qubit is $|0\rangle$ and applies the identity matrix if it is $|1\rangle$. Also, we define its $(n+1)$-qubit one-controlled gate as $\mathrm{C}(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$. which applies U to the target qubits when the control qubit is $|1\rangle$ and applies the identity matrix if it is $|0\rangle$.

We use $\mathsf{Eigenvalues}(U)$ to denote the multiset of eigenvalues of the unitary matrix U, and we use $\sqcup$ to denote the multiset-union operator.

Quantum Circuit Diagrams. In a circuit diagram, each qubit has its own line, and we use the symbol / to denote that a diagram represents multiple qubits in a single line. We display the X gate as $\oplus$, and we display the S gate as two $\times$'s connected by a line. In such a diagram, we have three special notations. We display a zero-controlled operation as $\circ$ and a one-controlled operation as $\bullet$, as shown in Figure 2.

If there exist two n-qubit gates V_0 and V_1, such that an $(n+1)$-qubit gate V can be written as $V = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1$, then, in a diagram, we use $\square$ on a line to emphasize such a qubit, as shown in Figure 3. We borrow this notation from [Shende and Markov 2008].

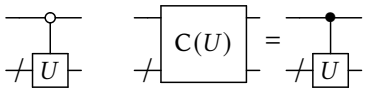


Fig. 2. Circuits for controlled gates.

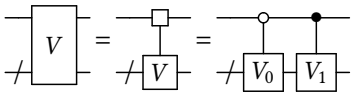


Fig. 3. Zero-one-controlled circuits.

For a 3-qubit diagonal gate $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7)$, there exist four 1-qubit gates $D_{00} = \mathrm{Diag}(d_0, d_1)$, $D_{01} = \mathrm{Diag}(d_2, d_3)$, $D_{10} = \mathrm{Diag}(d_4, d_5)$, and $D_{11} = \mathrm{Diag}(d_6, d_7)$, such that $D = |00\rangle\langle 00| \otimes D_{00} + |01\rangle\langle 01| \otimes D_{01} + |10\rangle\langle 10| \otimes D_{10} + |11\rangle\langle 11| \otimes D_{11}$. This enables us to think of D in terms of two control qubits, and we display D as shown in Figure 4.

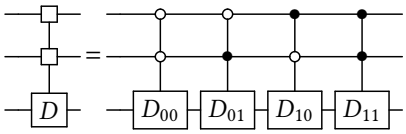


Fig. 4. A gate with two zero-one-controlled qubits.

Applying a 2-qubit Gate to 3 Qubits. Because we focus on 3-qubit circuits, we use three uppercase letters A, B, C to represent these three different qubits. An unrestricted 2-qubit gate can operate on any pair of qubits: AB, BC, and AC. However, neighbor gates can operate on only two of the three pairs. Following [Palsberg and Yu 2024], we define a 3-qubit gate $\overline{U}_{ij}$, where $ij \in \{AB, BC, AC\}$, to represent that a 2-qubit gate U is implemented on the qubits i and j in a 3-qubit circuit, with the third qubit remaining unchanged. In this notation, if U is a 2-qubit unitary, then U_{ij} operates on 2 qubits, while $\overline{U}_{ij}$ operates on 3 qubits. We define $\overline{U}_{ij}$ as follows.

$$\overline{U}_{AB} \;=\; U \otimes I, \qquad \overline{U}_{BC} \;=\; I \otimes U, \qquad \overline{U}_{AC} \;=\; \overline{S}_{BC}\, \overline{U}_{AB}\, \overline{S}_{BC}$$

Notice the use of the swap gate S in $\overline{S}_{BC}$. We have that $\overline{S}_{AB}\, \overline{U}_{AC}\, \overline{S}_{AB} = \overline{U}_{BC}$ [Palsberg and Yu 2024, Lemma A.12]. Furthermore, we can easily check that $\overline{S}_{BC}\, \overline{S}_{AC}\, \overline{U}_{AB}\, \overline{S}_{AC}\, \overline{S}_{BC} = \overline{U}_{BC}$. If we have qubit indices $ij \in \{BA, CB, CA\}$, then the qubit order must be reversed by sandwiching two swap gates. Thus, we write $\overline{U}_{ij}$ as $(\overline{S}_{ji}\, \overline{U}_{ji}\, \overline{S}_{ji})$ or $\overline{SUS}_{ji}$. We write $\overline{UVW}_{ij}$ as an abbreviation for $\overline{U}_{ij}\, \overline{V}_{ij}\, \overline{W}_{ij}$.

Sets of Gates. If U, V are 3-qubit gates, and $\mathcal{S}$ is a set of 3-qubit diagonal gates, then we define:

$$U\, \mathcal{S}\, V \;=\; \{\, U\, D\, V \mid D \in \mathcal{S} \,\}$$

3 PROGRAMMING WITH NEIGHBOR GATES

In this section, we present five example circuits that implement the Toffoli gate (Examples 3.1–3.2) and other diagonal gates (Examples 3.3–3.5). They all have the optimal numbers of 2-qubit gates, as we will show in Section 8.

Qubit Layout. If we have three qubits A, B, and C, and only two of the pairs are neighbors, the qubit layout is one of the ones in Figure 5. We will study all three layouts.

The Toffoli Gate. The Toffoli gate can be written $\mathrm{CC}(X)$, and it can be depicted as the left-hand-side of Circuit (1). Here, A, B, C are qubits, and the idea is that if both A and B are 1, then the gate will flip C by applying an X gate. The usual terminology is that A, B are the control qubits, while C is the target qubit. The notation $\mathrm{CC}(X)$ signals that the gate has two control qubits and that we may apply an X gate to the target qubit. Below is an implementation of a Toffoli gate that uses five

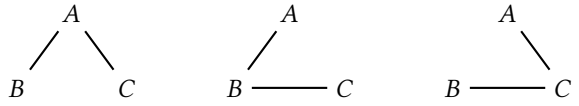
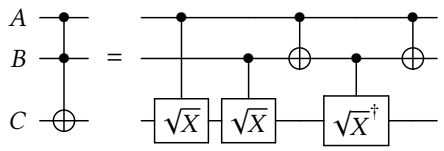


Fig. 5. Three qubit layouts.

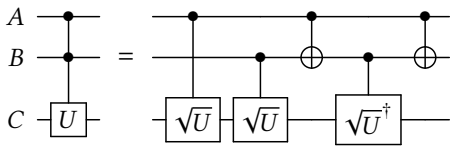
unrestricted gates, which is the optimal number of such gates. Those gates are all conditional gates that each has a single control.



(1)

Notice that in Circuit (1), the gates are applied to all possible qubit pairs AC, BC, and AB.

A Gate with Two Controls. We can generalize $\mathrm{CC}(X)$ to $\mathrm{CC}(U)$ where U is a 1-qubit unitary, and we can implement it by a straightforward generalization of the scheme above.



(2)

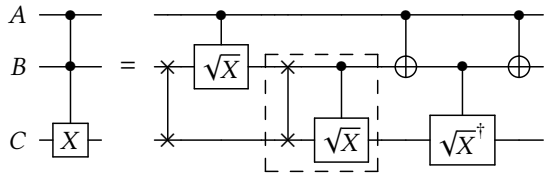
In Table 1, we walk through the effect of Circuit (2) on $|AB\rangle|C\rangle$, and we see that the circuit implements $\mathrm{CC}(U)$ correctly: the final state is $|AB\rangle\ U|C\rangle$ if and only if $|AB\rangle = |11\rangle$, and $|AB\rangle\ |C\rangle$ otherwise.

Table 1. The effect of the circuit in (2) on $|AB\rangle\ |C\rangle$.

Input	$\mathrm{C}(\sqrt{U})_{AC}$	$\mathrm{C}(\sqrt{U})_{BC}$	$\mathrm{C}(X)_{AB}$	$\mathrm{C}(\sqrt{U}^\dagger)_{BC}$	$\mathrm{C}(X)_{AB}$
$\|00\rangle\ \|C\rangle$	$\|00\rangle\ \|C\rangle$	$\|00\rangle\ \|C\rangle$	$\|00\rangle\ \|C\rangle$	$\|00\rangle\ \|C\rangle$	$\|00\rangle\ \|C\rangle$
$\|01\rangle\ \|C\rangle$	$\|01\rangle\ \|C\rangle$	$\|01\rangle\ (\sqrt{U}\|C\rangle)$	$\|01\rangle\ (\sqrt{U}\|C\rangle)$	$\|01\rangle\ \|C\rangle$	$\|01\rangle\ \|C\rangle$
$\|10\rangle\ \|C\rangle$	$\|10\rangle\ (\sqrt{U}\|C\rangle)$	$\|10\rangle\ (\sqrt{U}\|C\rangle)$	$\|11\rangle\ (\sqrt{U}\|C\rangle)$	$\|11\rangle\ \|C\rangle$	$\|10\rangle\ \|C\rangle$
$\|11\rangle\ \|C\rangle$	$\|11\rangle\ (\sqrt{U}\|C\rangle)$	$\|11\rangle\ (U\|C\rangle)$	$\|10\rangle\ (U\|C\rangle)$	$\|10\rangle\ (U\|C\rangle)$	$\|11\rangle\ (U\|C\rangle)$

Example 3.1 ($\mathrm{CC}(X)$ using 2-qubit gates only on AB and BC). Now let us move from using unrestricted gates to using neighbor gates. We ask: can we improve the implementation of $\mathrm{CC}(X)$ from using five unrestricted gates to using five neighbor gates? The answer is No, and we need six neighbor gates to make a Toffoli. Let us assume that a 2-qubit gate can operate on qubits AB, and on qubits BC, but not AC. In other words, a 2-qubit gate can operate on the two control qubits but on only one of the pairs of a control qubit and the target qubit. Circuit (1) for $\mathrm{CC}(X)$ violates this assumption because the first gate operates on AC. We can fix that by (i) changing the first gate's

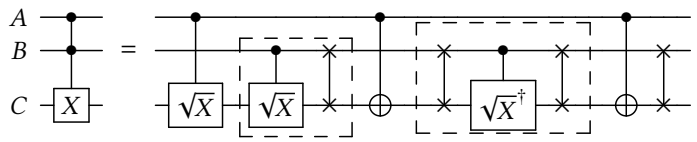
target qubit from C to B and (ii) inserting two swap gates.



The above circuit uses neighbor gates entirely, but, at first, it appears to use seven gates. However, the third and fourth gates both operate on qubits BC so they can be combined by matrix multiplication, as indicated by the dashed lines above. The result is a total of six neighbor gates.

A similar situation to the one above arises when we assume that a 2-qubit gate can operate on qubits AB, and on qubits AC, but not BC. Notice that also in this case, a 2-qubit gate can operate on the two control qubits and on one of the control qubits and the target qubit. We can handle this situation as we did above.

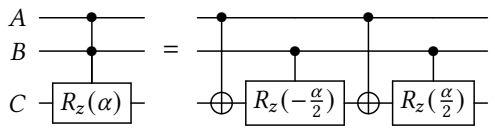
Example 3.2 ($\mathrm{CC}(X)$ using 2-qubit gates only on AC and BC). A rather different situation arises when we assume that a 2-qubit gate can operate on qubits AC and on BC, but not on AB. In other words, a 2-qubit gate can operate on both pairs of a control qubit and the target qubit, while it cannot operate on the two control qubits. Circuit (1) for $\mathrm{CC}(X)$ violates this assumption because the third gate and the fifth gate operate on AB. However, we can fix that by (i) changing the third gate's target qubit from B to C and (ii) inserting two swap gates, and (iii) doing steps (i)–(ii) for the fifth gate.



The above circuit uses neighbor gates entirely, but, at first, it appears to use nine gates. However, the second and third gates operate on qubits BC so they can be combined by matrix multiplication, as indicated by the dashed lines above. Similarly, the fifth, sixth, and seventh gates all operate on qubits BC so they can be combined as well. The result is a total of six neighbor gates.

In summary, the optimal number of 2-qubit gates for implementing $\mathrm{CC}(X)$ depends on whether we allow unrestricted gates or limit ourselves to neighbor gates.

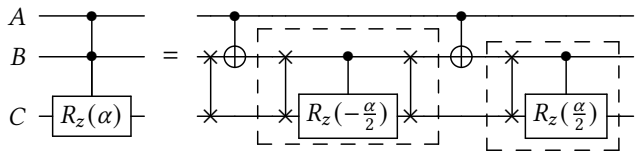
Example 3.3 ($\mathrm{CC}(R_z(\alpha))$ using 2-qubit gates only on AC and BC). The example above illustrates that five unrestricted gates have strictly more expressive power than five neighbor gates. In contrast, four unrestricted gates have the same expressive power as four neighbor gates if the qubit layout can be chosen to be any one of the three cases in Figure 5. Let us examine a case that can be implemented with four unrestricted gates, namely $\mathrm{CC}(R_z(\alpha))$:



Notice that the above circuit uses four neighbor gates: it uses no 2-qubit gates on qubits AB.

Example 3.4 ($\mathrm{CC}(R_z(\alpha))$ using 2-qubit gates only on AB and BC). Now we can ask the question of whether we can also implement $\mathrm{CC}(R_z(\alpha))$ by four neighbor gates that cannot operate

on qubits AC. Surprisingly, the answer is No! Rather, we have to use five neighbor gates, for example, as follows.

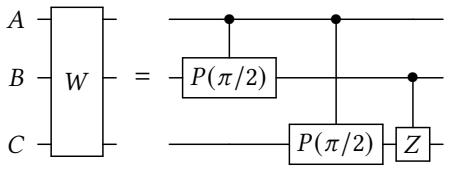


Similarly, if we cannot operate a 2-qubit gate on BC, we must use five neighbor gates to implement $\mathrm{CC}(R_z(\alpha))$. Thus, while we can implement $\mathrm{CC}(R_z(\alpha))$ using four neighbor gates, we can do it only in the case where a 2-qubit gate can operate on both pairs of a control qubit and the target qubit.

One can wonder whether we can implement $\mathrm{CC}(R_z(\alpha))$ either using three unrestricted gates or using four neighbor gates that cannot operate on A and C. The answer to both questions is No, as we will show later in the paper.

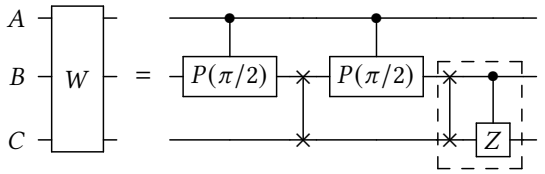
In summary, the optimal number of 2-qubit neighbor gates for the implementation of $\mathrm{CC}(R_z(\alpha))$ depends on the layout of the qubit.

Example 3.5 ($\mathrm{Diag}(1,\ 1,\ 1,\ -1,\ 1,\ i,\ i,\ 1)$ using 2-qubit gates only on AB and BC). Five unrestricted gates have strictly more expressive power than five neighbor gates while four unrestricted gates have the same expressive power as four neighbor gates if the qubit layout can be chosen to be any one of the three cases in Figure 5. What about three unrestricted gates? Consider the 3-qubit diagonal gate $W = \mathrm{Diag}(1,\ 1,\ 1,\ -1,\ 1,\ i,\ i,\ 1)$, which we can implement with three unrestricted gates as follows.



(3)

Now we can ask: can we improve the implementation of W from using three unrestricted gates to using three neighbor gates? Or, does the focus on neighbor gates force us to use additional gates? The answer is that we need four neighbor gates to make a W gate. For example, here is an implementation of W with four neighbor gates, specifically on AB and BC.



Similarly, we can implement W with four neighbor gates on AB and AC by adding swap gates on qubits AC before and after $\mathrm{C}(Z)$ gate in Equation (3). We can also implement W with four neighbor gates on AC and BC by adding swap gates on qubits AC before and after $\mathrm{C}(P(\pi/2))$ in Equation (3).

In Section 8, we show that all our circuits above are optimal.

4 FROM FIVE NEIGHBOR GATES TO FOUR UNRESTRICTED GATES

Here, we present the main technical innovation in this paper: an implementation of a 3-qubit diagonal gate using five 2-qubit neighbor gates can be transformed into an implementation using four 2-qubit unrestricted gates. In Lemma 4.1, we prove this for a subset of such circuits of five

2-qubit neighbor gates, and then in Lemma 4.4, we generalize to a wider subset, and ultimately in Theorem 6.2 (in Section 6), we generalize to all such circuits, as illustrated in Figure 1.

The proof of Lemma 4.1 transforms the implementation of a diagonal gate into a form that uses 1) a 3-qubit gate with a single control qubit and two target qubits, and 2) two 2-qubit gates. Fortunately, the 3-qubit gate in 1) can be implemented with four 2-qubit gates, two of which can be combined with the two 2-qubit gates in 2). The net result is a circuit with four 2-qubit gates.

The proof of Lemma 4.4 uses Lemma 4.2 and Lemma 4.3 to transform an implementation of a diagonal gate to the simpler form covered by Lemma 4.1.

Lemma 4.1. *Suppose D is a 3-qubit diagonal gate. If there exist two 1-qubit gates P and Q and three 2-qubit gates U_1, U_3, and U_5, such that $\overline{U_1}_{BC}\,\overline{\mathsf{C}(P)}_{AC}\,\overline{U_3}_{BC}\,\overline{\mathsf{C}(Q)}_{AC}\,\overline{U_5}_{BC} = D$, then there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC} = D$.*

Proof. Suppose that $\overline{U_1}_{BC}\,\overline{\mathsf{C}(P)}_{AC}\,\overline{U_3}_{BC}\,\overline{\mathsf{C}(Q)}_{AC}\,\overline{U_5}_{BC} = D$. We calculate as shown in Figure 6, and we justify each step as follows. Notice that in Figure 6, we order the qubits as A, C, B, which simplifies the circuit diagrams, and we will continue to use this qubit order in the circuit diagrams throughout this section. In contrast, the calculations in the text will use the qubit order A, B, C.

In the first step, we use the assumption about D.

In the second step, for $\mathsf{C}(P)$ and $\mathsf{C}(Q)$, according to Lemma A.3, there exist four complex numbers d_{p_0}, d_{p_1}, d_{q_0}, and d_{q_1} and two 1-qubit gates K and L, such that the second step is valid.

In the third step, for $\mathsf{C}(\mathsf{Diag}(d_{p_0},\ d_{p_1}))$ and $\mathsf{C}(\mathsf{Diag}(d_{q_0},\ d_{q_1}))$, according to Lemma A.6, there exist two 1-qubit gates $P(\varphi_p)$ and $P(\varphi_q)$ and two 2-qubit gates $\mathsf{C}(R_z(\alpha))$ and $\mathsf{C}(R_z(\beta))$, such that the third step is valid.

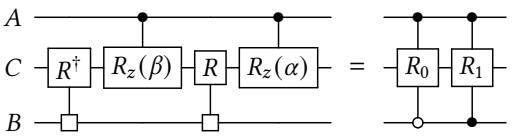
In the fourth step, because $P(\varphi_q)$ commutes with $\mathsf{C}(R_z(\beta))$, we define one 1-qubit gate $P(\varphi) = P(\varphi_p + \varphi_q)$ and three 2-qubit gates $W_1 = U_1\,(I \otimes K)$, $W_3 = (I \otimes K^\dagger)\,U_3\,(I \otimes L)$, and $W_5 = (I \otimes L^\dagger)\,U_5$.

In the fifth step, for W_3, according to Lemma A.4, there exist six 1-qubit gates M_0, M_1, $R_y(\theta_0)$, $R_y(\theta_1)$, N_0, and N_1 and three 2-qubit gates $M = M_0 \otimes |0\rangle\langle 0| + M_1 \otimes |1\rangle\langle 1|$, $R = |0\rangle\langle 0| \otimes R_y(\theta_0) + |1\rangle\langle 1| \otimes R_y(\theta_1)$, and $N = N_0 \otimes |0\rangle\langle 0| + N_1 \otimes |1\rangle\langle 1|$, such that the fifth step is valid.

In the sixth step, we use that M commutes with $\mathsf{C}(R_z(\alpha))$ and N commutes with $\mathsf{C}(R_z(\beta))$ while $R^\dagger = |0\rangle\langle 0| \otimes R_y(-\theta_0) + |1\rangle\langle 1| \otimes R_y(-\theta_1)$ cancels out with R in the circuit.

In the seventh step, we define two 2-qubit gates $G_1 = W_1\,M$ and $G_5 = R\,N\,W_5$.

In the eighth step, we need multiple substeps of reasoning to derive the desired equation. We first rearrange the result of the first seven steps to give the first equation in (4):



(4)

In Equation (4), the right-hand-side circuit equals the left-hand-side circuit for the following reasons. If qubit A is $|0\rangle$, then we implement I on qubits B and C. If qubit A is $|1\rangle$ and qubit B is $|0\rangle$, then we implement $R_0 = R_z(\alpha)\,R_y(\theta_0)\,R_z(\beta)\,R_y(-\theta_0)$ on qubit C. If qubit A is $|1\rangle$ and qubit B is $|1\rangle$, then we implement $R_1 = R_z(\alpha)\,R_y(\theta_1)\,R_z(\beta)\,R_y(-\theta_1)$ on qubit C. Because $R_z(\alpha)$, $R_z(\beta)$, $R_y(\pm\theta_0)$, and $R_y(\pm\theta_1)$ all have determinant 1, according to Lemma A.10, we conclude that $\det(R_0) = \det(R_1) = 1$. From this, there exist two complex numbers $e^{i\gamma_0}$ and $e^{i\gamma_1}$, such that $\mathsf{Eigenvalues}(R_0) = (e^{i\gamma_0}, e^{-i\gamma_0})$ and $\mathsf{Eigenvalues}(R_1) = (e^{i\gamma_1}, e^{-i\gamma_1})$. From the above observations, according to Lemma A.12 and Lemma A.3, there exists one 2-qubit gate F, such that

$$\mathsf{C}\left(\begin{bmatrix} R_0 & 0 \\ 0 & R_1 \end{bmatrix}\right) = (I \otimes F) \cdot \mathsf{C}(\mathsf{Diag}(e^{-i\gamma_1},\ e^{-i\gamma_0},\ e^{i\gamma_0},\ e^{i\gamma_1})) \cdot (I \otimes F^\dagger) \tag{5}$$

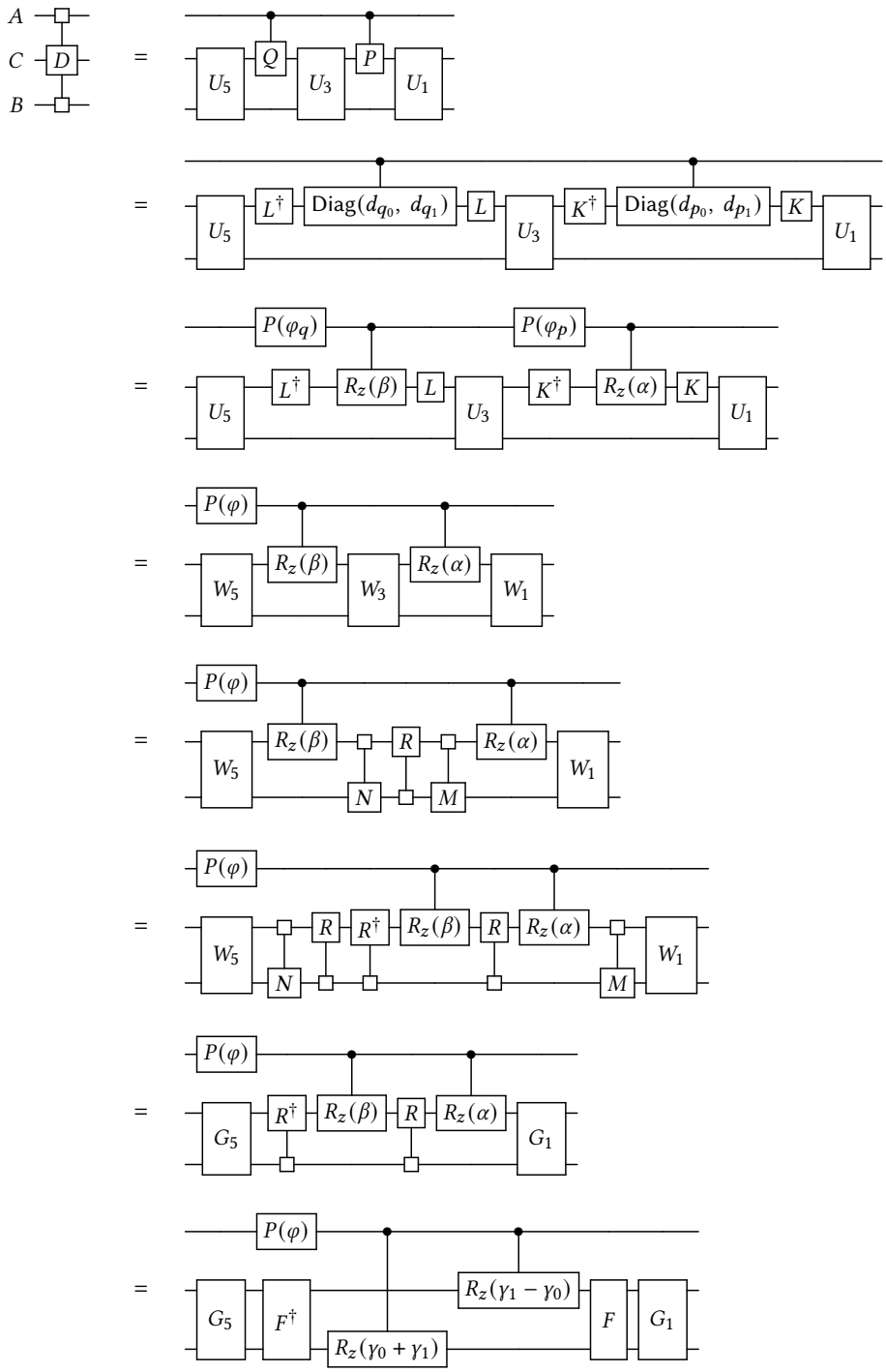


Fig. 6. The key calculation in Lemma 4.1.

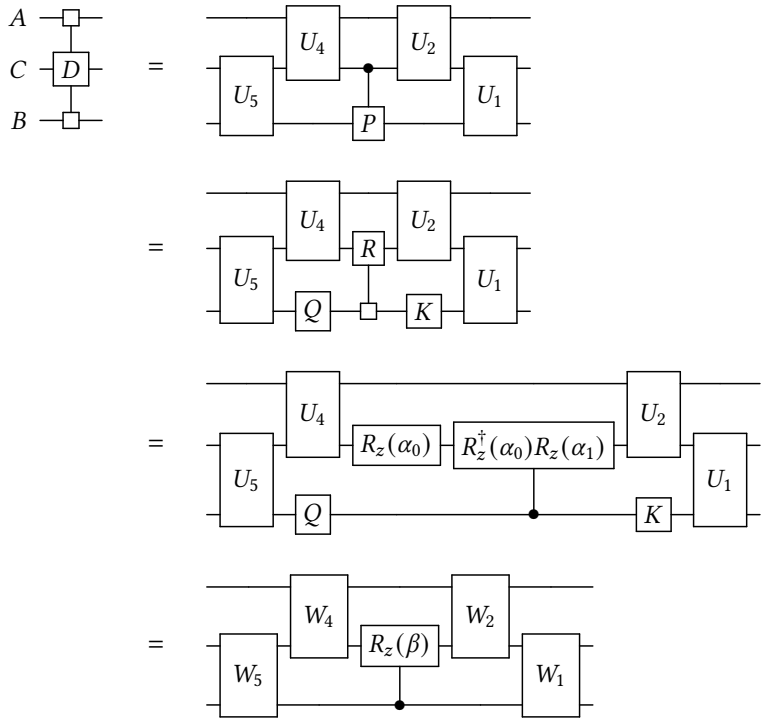
Now we plug Equations (4)–(5) into in Figure 6, which completes the eighth step.

From Figure 6 we conclude that there exist four 2-qubit gates $V_1 = G_1 F$, $V_2 = \mathrm{C}(R_z(\gamma_1 - \gamma_0))$, $V_3 = \mathrm{C}(R_z(\gamma_0 + \gamma_1))\ (P(\varphi) \otimes I)$, and $V_4 = F^\dagger G_5$, such that $\overline{V_1}_{BC}\ \overline{V_2}_{AC}\ \overline{V_3}_{AB}\ \overline{V_4}_{BC} = D$. □

Lemma 4.2. *Suppose D is a 3-qubit diagonal gate. If there exist one 1-qubit gate P and five 2-qubit gates U_1, U_2, U_3, U_4, U_5, where $U_3 = I \otimes |0\rangle\langle 0| + P \otimes |1\rangle\langle 1|$, such that $\overline{U_1}_{BC}\ \overline{U_2}_{AC}\ \overline{U_3}_{BC}\ \overline{U_4}_{AC}\ \overline{U_5}_{BC} = D$, then there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\ \overline{V_2}_{AC}\ \overline{V_3}_{AB}\ \overline{V_4}_{BC} = D$.*

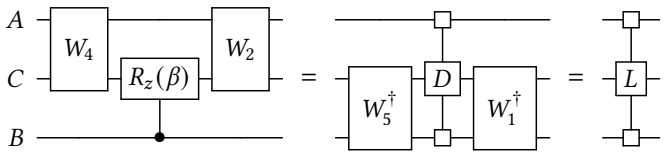
Proof. Suppose that $\overline{U_1}_{BC}\ \overline{U_2}_{AC}\ \overline{U_3}_{BC}\ \overline{U_4}_{AC}\ \overline{U_5}_{BC} = D$, where $U_3 = I \otimes |0\rangle\langle 0| + P \otimes |1\rangle\langle 1|$. We calculate as Equation (6).

In the first step, we use the assumptions about D and U_3. In the second step, for $\mathrm{C}(P)$, according to Lemma A.5, there exist four 1-qubit gates K, Q, $R_z(\alpha_0)$, and $R_z(\alpha_1)$ and one 2-qubit gate $R = |0\rangle\langle 0| \otimes R_z(\alpha_0) + |1\rangle\langle 1| \otimes R_z(\alpha_1)$, such that the second step is valid. In the third step, we use Lemma A.7. In the fourth step, we define one 1-qubit gate $R_z(\beta) = R_z(\alpha_1 - \alpha_0)$ and four 2-qubit gates $W_1 = U_1\ (K \otimes I)$, $W_2 = U_2$, $W_4 = (I \otimes R_z(\alpha_0))\ U_4$, and $W_5 = (Q \otimes I)\ U_5$.



(6)

From the result, by moving W_1 and W_5 to the left-hand side of the equation, we have that



(7)

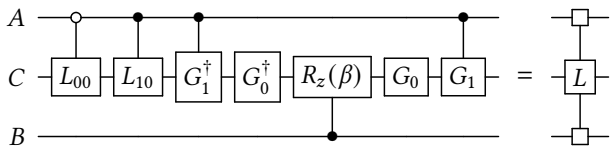
In Equation (7), the right two circuits equal the left-hand-side circuit. This is because the left-hand-side circuit commutes with Z gates on qubit B and the middle-hand-side circuit commutes with Z gates on qubit A, and according to Lemma A.1, there exist four 1-qubit gates L_{00}, L_{01}, L_{10}, and L_{11}, such that both circuits can be written as one 3-qubit gate $L = |00\rangle\langle 00| \otimes L_{00} + |01\rangle\langle 01| \otimes L_{01} + |10\rangle\langle 10| \otimes$

$L_{10} + |11\rangle\langle 11| \otimes L_{11}$. For Equation (7), we have the following two observations: If qubit B is $|0\rangle$, then $|0\rangle\langle 0| \otimes L_{00} + |1\rangle\langle 1| \otimes L_{10} = W_2\, W_4$; If qubit B is $|1\rangle$, then $|0\rangle\langle 0| \otimes L_{01} + |1\rangle\langle 1| \otimes L_{11} = W_2\, (I \otimes R_z(\beta))\, W_4$. From this, we know that

$$\text{Eigenvalues}(\begin{bmatrix} L_{01}L_{00}^\dagger & 0 \\ 0 & L_{11}L_{10}^\dagger \end{bmatrix}) = \text{Eigenvalues}((W_2\, (I \otimes R_z(\beta))\, W_2^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{-i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$$

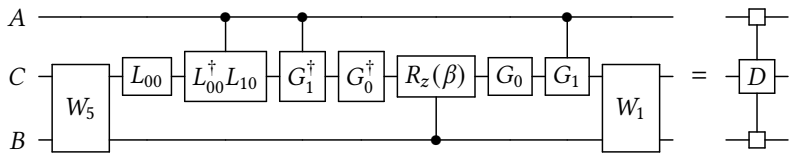
From the above and according to Lemma A.12, we have three cases: (1) $\text{Eigenvalues}(L_{01}L_{00}^\dagger) = \text{Eigenvalues}(L_{11}L_{10}^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$, (2) $\text{Eigenvalues}(L_{01}L_{00}^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{-i\frac{\beta}{2}})$, $\text{Eigenvalues}(L_{11}L_{10}^\dagger) = (e^{i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$, and (3) $\text{Eigenvalues}(L_{01}L_{00}^\dagger) = (e^{i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$ and $\text{Eigenvalues}(L_{11}L_{10}^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{-i\frac{\beta}{2}})$. The proof of case (3) is similar to that of case (2) by symmetry, and the proofs of case (1) and case (2) go as follows.

For case (1), because $\text{Eigenvalues}(L_{01}L_{00}^\dagger) = \text{Eigenvalues}(L_{11}L_{10}^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$, according to Lemma A.2, there exist two 1-qubit gates G_0 and G_1, such that $L_{01} = G_0\, R_z(\beta)\, G_0^\dagger\, L_{00}$ and $L_{11} = G_1\, G_0\, R_z(\beta)\, G_0^\dagger\, G_1^\dagger\, L_{10}$, and we can rewrite L in Equation (7) as



(8)

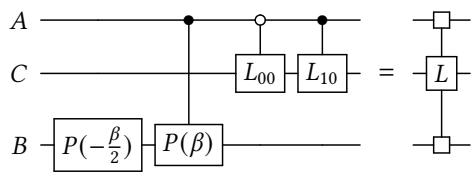
From Equations (7)–(8), by moving $W_5^\dagger$ and $W_1^\dagger$ back, according to Lemma A.7, we have that



(9)

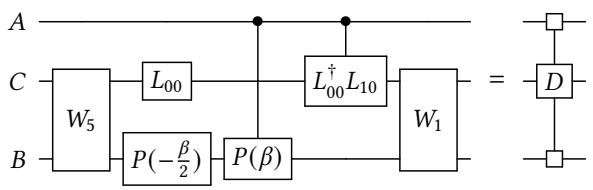
According to Equation (9), we know that there exist two 1-qubit gates $M = G_1$ and $N = G_1^\dagger\, L_{10}\, L_{00}^\dagger$ and three 2-qubit gates $F_1 = W_1$, $F_3 = (I \otimes G_0)\, \text{C}(R_z(\beta))\, (I \otimes G_0^\dagger)$, and $F_5 = (I \otimes L_{00})\, W_5$, such that $\overline{F_1}_{BC}\, \overline{\text{C}(M)}_{AC}\, \overline{F_3}_{BC}\, \overline{\text{C}(N)}_{AC}\, \overline{F_5}_{BC} = D$. According to Lemma 4.1, there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{AB}\, \overline{V_4}_{BC} = D$.

For case (2), if $\text{Eigenvalues}(L_{01}L_{00}^\dagger) = (e^{-i\frac{\beta}{2}},\ e^{-i\frac{\beta}{2}})$ and $\text{Eigenvalues}(L_{11}L_{10}^\dagger) = (e^{i\frac{\beta}{2}},\ e^{i\frac{\beta}{2}})$, we have that $L_{01}L_{00}^\dagger = e^{-i\frac{\beta}{2}} I$ and $L_{11}L_{10}^\dagger = e^{i\frac{\beta}{2}} I$, and we conclude that $L_{01} = e^{-i\frac{\beta}{2}} L_{00}$ and $L_{11} = e^{i\frac{\beta}{2}} L_{10}$. From the above, we can rewrite L in Equation (7) as



(10)

From Equations (7) and (10), by moving $W_5^\dagger$ and $W_1^\dagger$ back, according to Lemma A.7, we have that



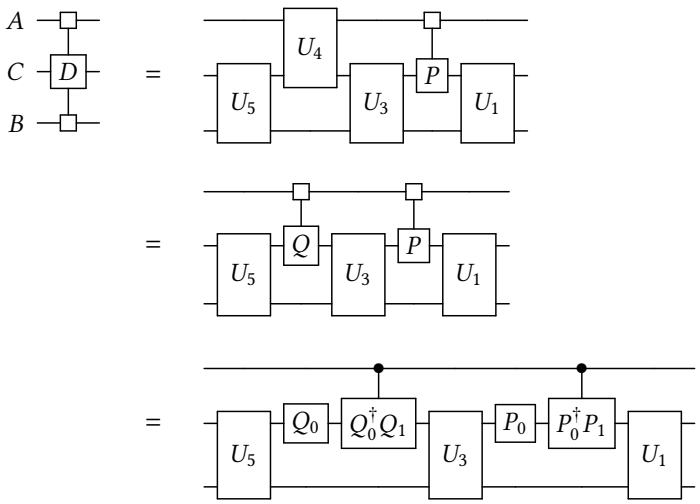
(11)

By Equation (11), there exist four 2-qubit gates $V_1 = W_1$, $V_2 = \mathrm{C}(L_{10}L_{00}^\dagger)$, $V_3 = \mathrm{C}(P(\beta))$, and $V_4 = (P(-\frac{\beta}{2}) \otimes L_{00})\, W_5$, such that $\overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{AB}\, \overline{V_4}_{BC} = D$. □

Lemma 4.3. *Suppose D is a 3-qubit diagonal gate. If there exist two 1-qubit gates P_0 and P_1 and five 2-qubit gates U_1, U_2, U_3, U_4, and U_5, where $U_2 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, such that $\overline{U_1}_{BC}\, \overline{U_2}_{AC}\, \overline{U_3}_{BC}\, \overline{U_4}_{AC}\, \overline{U_5}_{BC} = D$, then there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{AB}\, \overline{V_4}_{BC} = D$.*

Proof. Suppose that $\overline{U_1}_{BC}\, \overline{U_2}_{AC}\, \overline{U_3}_{BC}\, \overline{U_4}_{AC}\, \overline{U_5}_{BC} = D$, where $U_2 = P = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. We calculate as shown in Equation (12).

In the first step, we use the assumptions about D and U_2. From these assumptions, according to Lemma A.1, we have that both D and U_2 commute with Z gates on qubit A. From this, we conclude that U_4 also commutes with Z gates on qubit A. As a result, according to Lemma A.1, we conclude that there exist two 1-qubit gates Q_0 and Q_1, such that $U_4 = Q = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$. In the second step, we use this observation. In the third step, we use Lemma A.7.



(12)

From Equation (12), we have that there exist two 1-qubit gates $M = P_1 P_0^\dagger$ and $N = Q_1 Q_0^\dagger$ and three 2-qubit gates $W_1 = U_1$, $W_3 = (I \otimes P_0)\, U_3$, and $W_5 = (I \otimes Q_0)\, U_5$, such that

$$\overline{W_1}_{BC}\, \overline{\mathrm{C}(M)}_{AC}\, \overline{W_3}_{BC}\, \overline{\mathrm{C}(N)}_{AC}\, \overline{W_5}_{BC} \quad = \quad D$$

From this and Lemma 4.1, we conclude that there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{AB}\, \overline{V_4}_{BC} = D$. □

Lemma 4.4. *Suppose D is a 3-qubit diagonal gate. If there exist five 2-qubit gates U_1, U_2, U_3, U_4, U_5, such that $\overline{U_1}_{BC}\, \overline{U_2}_{AC}\, \overline{U_3}_{BC}\, \overline{U_4}_{AC}\, \overline{U_5}_{BC} = D$, then there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{AB}\, \overline{V_4}_{BC} = D$.*

Proof. Suppose that $D = |0\rangle\langle 0| \otimes D_0 + |1\rangle\langle 1| \otimes D_1$. For U_2, U_3, U_4, and U_5, according to Lemma A.16, there exist four 2-qubit gates W_2, W_3, W_4, and W_5, such that

$$\overline{U_2}_{AC}\, \overline{U_3}_{BC}\, \overline{U_4}_{AC}\, \overline{U_5}_{BC} \quad = \quad \overline{W_2}_{AC}\, \overline{W_3}_{BC}\, \overline{W_4}_{AC}\, \overline{W_5}_{BC} \tag{13}$$

$$W_4\, (|0\rangle \otimes |0\rangle) \quad = \quad |0\rangle \otimes |0\rangle \tag{14}$$

By Equation (13) and the assumptions of D, if we define $W_1 = U_1$, we have that

$$\overline{W_1}_{BC}\,\overline{W_2}_{AC}\,\overline{W_3}_{BC}\,\overline{W_4}_{AC}\,\overline{W_5}_{BC} = D \tag{15}$$

By Equations (14)-(15), we conclude that, for all $|y\rangle$, we have that

$$\begin{aligned} & \overline{W_2}_{AC}\,\overline{W_3}_{BC}\,(|0\rangle_A \otimes |y\rangle_B \otimes |0\rangle_C) \\ = \; & \overline{W_1}^{\dagger}_{BC}\,D\,\overline{W_5}^{\dagger}_{BC}\,\overline{W_4}^{\dagger}_{AC}\,(|0\rangle_A \otimes |y\rangle_B \otimes |0\rangle_C) \\ = \; & \overline{W_1}^{\dagger}_{BC}\,\overline{D_0}_{BC}\,\overline{W_5}^{\dagger}_{BC}\,(|0\rangle_A \otimes |y\rangle_B \otimes |0\rangle_C) \end{aligned} \tag{16}$$

According to Lemma A.8, W_3 has three cases. In the first case, suppose that there exists a qubit $|y\rangle$, such that $W_3\,(|y\rangle \otimes |0\rangle)$ is entangled. From this and Equation (16), for W_2, according to Lemma A.13, we conclude that there exist two 1-qubit gates P_0 and P_1, such that $W_2 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. From this and Equation (15), according to Lemma 4.3, we conclude that there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC} = D$.

In the second case, suppose that $\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : W_3\,(|y\rangle \otimes |0\rangle) = |x\rangle \otimes |z\rangle$. From this and Equation (16), for W_2, according to Lemma A.17, we conclude that there exist two 1-qubit gates P_0 and P_1, such that $W_2 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. From this and Equation (15), according to Lemma 4.3, we conclude that there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC} = D$.

In the third case, suppose that $\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : V_3\,(|y\rangle \otimes |0\rangle) = |z\rangle \otimes |x\rangle$. From this, for W_2, W_3, W_4, and W_5, according to Lemma A.15, we conclude that there exist one 1-qubit gate P and three 2-qubit gates K_2, K_3, and K_5, such that $\overline{W_2}_{AC}\,\overline{W_3}_{BC}\,\overline{W_4}_{AC}\,\overline{W_5}_{BC} = \overline{K_2}_{AC}\,\overline{K_3}_{BC}\,\overline{W_4}_{AC}\,\overline{K_5}_{BC}$ and $K_3 = I \otimes |0\rangle\langle 0| + P \otimes |1\rangle\langle 1|$. From this and Equation (15), according to Lemma 4.2, we conclude that there exist four 2-qubit gates V_1, V_2, V_3, and V_4, such that $\overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC} = D$. □

5 SETS OF 3-QUBIT DIAGONAL GATES

In this section, we define the sets $\mathcal{S}_1, \ldots, \mathcal{S}_6$ of 3-qubit diagonal gates. For each $\mathcal{S}_i$, we will prove the least upper bounds shown in Table 2 on the number of 2-qubit neighbor gates and on the number of 2-qubit unrestricted gates needed to implement *any* 3-qubit diagonal gate D in $\mathcal{S}_i$. In more detail, we will prove those upper bounds in Theorem 7.1 and Theorem 7.2, and we will prove Corollary 7.3 which states that the upper bounds in Table 2 are indeed least upper bounds, as illustrated in Figure 1. In the first row of Table 2, the least upper bounds are based on picking the qubit layout, among three cases in Figure 5, that minimizes the number of 2-qubit gates. We borrow the notions of $\mathcal{S}_1$, $\mathcal{S}_4$, $\mathcal{S}_5$, and $\mathcal{S}_6$ from Shende and Markov [2008], though we state their definitions in a different way. In contrast, $\mathcal{S}_2$ and $\mathcal{S}_3$ are new. The interesting cases are $\mathcal{S}_4$ and $\mathcal{S}_6$ for which we need an additional neighbor gate, compared to the number of unrestricted gates.

Table 2. Least upper bounds on the number of 2-qubit gates needed to implement any gate in $\mathcal{S}_i$.

# of 2-qubit gates	$\mathcal{S}_1$	$\mathcal{S}_2$	$\mathcal{S}_3$	$\mathcal{S}_4$	$\mathcal{S}_5$	$\mathcal{S}_6$
Neighbor gates	1	2	3	**4**	4	**6**
Unrestricted gates	1	2	3	**3**	4	**5**

The Idea. Table 2 shows that when i increases, the number of 2-qubit gates needed to implement a gate in $\mathcal{S}_i$ increases or stays the same. Thus, when i increases, the gates in $\mathcal{S}_i$ become more resource-intensive to implement. Intuitively, this is because, when i increases, the gates in $\mathcal{S}_i$ must satisfy fewer constraints on its eight diagonal elements. Specifically, the gates in $\mathcal{S}_1$ must satisfy

three constraints, while the gates in $\mathcal{S}_2 \cup \mathcal{S}_3$ must satisfy two constraints, and the gates in $\mathcal{S}_4 \cup \mathcal{S}_5$ must satisfy a single constraint. Ultimately, $\mathcal{S}_6$ is the set of all diagonal 3-qubit gates.

The Definition. Each $\mathcal{S}_i$ is a union of three sets: $\mathcal{S}_i = \mathcal{S}_i^1 \cup \mathcal{S}_i^2 \cup \mathcal{S}_i^3$. We give the definitions of the sets $\mathcal{S}_i^j$ in Figure 7. For most i, the three sets $\mathcal{S}_i^1, \mathcal{S}_i^2, \mathcal{S}_i^3$ are different and reflect different ways of imposing constraints on the diagonal elements of a gate.

Intuition. The definition of sets $\mathcal{S}_i^j$ contains many constraints that equate products of diagonal elements. A key intuition behind the definition lies in a property that we will state as Lemma 5.3 below: $D \in \mathcal{S}_i^j$ if and only if $D^\dagger \in \mathcal{S}_i^j$. For example, the definition of $\mathcal{S}_1^1$ contains the constraint $d_0 d_5 = d_1 d_4$. For $D \in \mathcal{S}_1^1$, we see that every diagonal element of $D^\dagger$ is the one from D but conjugated. So, when we have $d_0 d_5 = d_1 d_4$ and we conjugate all four factors, we see that the equation still holds.

Each $\mathcal{S}_i$ is a union of three sets: $\mathcal{S}_i = \mathcal{S}_i^1 \cup \mathcal{S}_i^2 \cup \mathcal{S}_i^3$. We define each $\mathcal{S}_i^j$ as follows.

$$\mathcal{S}_1^1 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_5 = d_1d_4 \ \wedge\ d_0d_6 = d_2d_4 \ \wedge\ d_0d_7 = d_3d_4 \,\}$$
$$\mathcal{S}_1^2 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_3 = d_1d_2 \ \wedge\ d_0d_6 = d_2d_4 \ \wedge\ d_0d_7 = d_2d_5 \,\}$$
$$\mathcal{S}_1^3 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_3 = d_1d_2 \ \wedge\ d_0d_5 = d_1d_4 \ \wedge\ d_0d_7 = d_1d_6 \,\}$$

$$\mathcal{S}_2^1 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_3 = d_1d_2 \ \wedge\ d_4d_7 = d_5d_6 \,\}$$
$$\mathcal{S}_2^2 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_5 = d_1d_4 \ \wedge\ d_2d_7 = d_3d_6 \,\}$$
$$\mathcal{S}_2^3 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_6 = d_2d_4 \ \wedge\ d_1d_7 = d_3d_5 \,\}$$

$$\mathcal{S}_3^1 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_7 = d_3d_4 \ \wedge\ d_1d_6 = d_2d_5 \,\}$$
$$\mathcal{S}_3^2 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_7 = d_2d_5 \ \wedge\ d_1d_6 = d_3d_4 \,\}$$
$$\mathcal{S}_3^3 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_7 = d_1d_6 \ \wedge\ d_2d_5 = d_3d_4 \,\}$$

$$\mathcal{S}_4^1 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_3d_5d_6 = d_1d_2d_4d_7 \,\} = \mathcal{S}_4^2 = \mathcal{S}_4^3$$

$$\mathcal{S}_5^1 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_3d_4d_7 = d_1d_2d_5d_6 \,\}$$
$$\mathcal{S}_5^2 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_2d_5d_7 = d_1d_3d_4d_6 \,\}$$
$$\mathcal{S}_5^3 = \{\, \mathrm{Diag}(d_0,d_1,d_2,d_3,d_4,d_5,d_6,d_7) \mid d_0d_1d_6d_7 = d_2d_3d_4d_5 \,\}$$

$$\mathcal{S}_6^1 = \text{the set of all 3-qubit diagonal unitaries} = \mathcal{S}_6^2 = \mathcal{S}_6^3$$

Fig. 7. The definition of $\mathcal{S}_1, \ldots, \mathcal{S}_6$.

Properties. We can show, through a tedious case analysis, that $\mathcal{S}_1 \subseteq \mathcal{S}_2 \subseteq \mathcal{S}_4 \subseteq \mathcal{S}_6$, $\mathcal{S}_1 \subseteq \mathcal{S}_3 \subseteq \mathcal{S}_5 \subseteq \mathcal{S}_6$, and $\mathcal{S}_2 \subset \mathcal{S}_5$, while $\mathcal{S}_2 \not\subset \mathcal{S}_3$ and $\mathcal{S}_3 \not\subset \mathcal{S}_4$ and $\mathcal{S}_4 \not\subset \mathcal{S}_5$. Figure 8 shows the inclusion relations among the $\mathcal{S}_i$ sets, and Figure 9 shows detailed inclusion relations among some of the $\mathcal{S}_i^j$ sets. In particular, each set $\mathcal{S}_1^j$ is included in two sets $\mathcal{S}_2^j$ and one set $\mathcal{S}_3^j$. In addition, each set $\mathcal{S}_2^j$ is included in one set $\mathcal{S}_5^j$, and each set $\mathcal{S}_3^j$ is included in two sets $\mathcal{S}_5^j$.

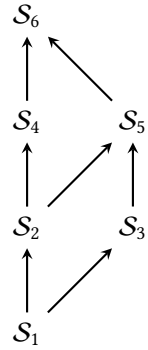


Fig. 8. Inclusion relations among the $\mathcal{S}_i$ sets.

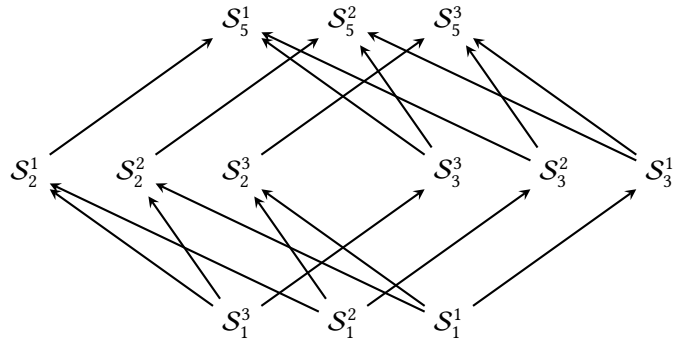


Fig. 9. Inclusion relations among some of the $\mathcal{S}_i^j$ sets.

The sets $\mathcal{S}_i^j$ satisfy three key properties that we state as Lemma 5.1, Lemma 5.2, and Lemma 5.3 and that we prove in Appendix B. First, Lemma 5.1 says that we can map a gate from one of $\mathcal{S}_i^1, \mathcal{S}_i^2, \mathcal{S}_i^3$ to another by conjugating the gate with a swap gate.

Lemma 5.1. *For all $i \in 1..6$, (1) $\overline{S}_{BC}\,\mathcal{S}_i^1\,\overline{S}_{BC} = \mathcal{S}_i^1$, (2) $\overline{S}_{AB}\,\mathcal{S}_i^1\,\overline{S}_{AB} = \mathcal{S}_i^2$, (3) $\overline{S}_{AC}\,\mathcal{S}_i^1\,\overline{S}_{AC} = \mathcal{S}_i^3$, (4) $\overline{S}_{AC}\,\mathcal{S}_i^2\,\overline{S}_{AC} = \mathcal{S}_i^2$, (5) $\overline{S}_{BC}\,\mathcal{S}_i^2\,\overline{S}_{BC} = \mathcal{S}_i^3$, and (6) $\overline{S}_{AB}\,\mathcal{S}_i^3\,\overline{S}_{AB} = \mathcal{S}_i^3$.*

Second, Lemma 5.2 says that conjugating a gate with a swap gate preserves the number of 2-qubit neighbor gates and the number of 2-qubit unrestricted gates used in an implementation. Lemma 5.2 also states how to change each component gate when conjugating with a swap gate.

Lemma 5.2. *For $k \in \{ AB, AC, BC \}$, a 3-qubit gate D can be implemented with m 2-qubit gates as $D = \overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\ldots\,\overline{U_{mi_m}}$ if and only if $\overline{S}_k\,D\,\overline{S}_k$ can be implemented with m 2-qubit gates as $\overline{S}_k\,D\,\overline{S}_k = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\ldots\,\overline{V_{mj_m}}$. Specifically, we have the following table.*

For mapping a product D to:	map each factor in D as follows:
$\overline{S}_{BC}\ D\ \overline{S}_{BC}$	$\overline{U}_{BC} \rightarrow \overline{S\ U\ S}_{BC}$ $\overline{U}_{AC} \rightarrow \overline{U}_{AB}$ $\overline{U}_{AB} \rightarrow \overline{U}_{AC}$
$\overline{S}_{AC}\ D\ \overline{S}_{AC}$	$\overline{U}_{BC} \rightarrow \overline{S\ U\ S}_{AB}$ $\overline{U}_{AC} \rightarrow \overline{S\ U\ S}_{AC}$ $\overline{U}_{AB} \rightarrow \overline{S\ U\ S}_{BC}$
$\overline{S}_{AB}\ D\ \overline{S}_{AB}$	$\overline{U}_{BC} \rightarrow \overline{U}_{AC}$ $\overline{U}_{AC} \rightarrow \overline{U}_{BC}$ $\overline{U}_{AB} \rightarrow \overline{S\ U\ S}_{AB}$

When we combine Lemma 5.1 and Lemma 5.2, we see that for a given i, the least upper bounds for neighbor gates and unrestricted gates are the same across $\mathcal{S}_i^1$, $\mathcal{S}_i^2$, and $\mathcal{S}_i^3$.

Third, the dagger operation will not change the set to which a 3-qubit diagonal gate belongs.

Lemma 5.3. *A 3-qubit diagonal gate $D \in \mathcal{S}_i^j$ if and only if $D^\dagger \in \mathcal{S}_i^j$.*

Examples. Here are examples of elements of the sets $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$. First, for the 3-qubit gate $\mathrm{CC}(-I) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ -1,\ -1)$, we have that $d_0 d_3 = d_1 d_2$, $d_0 d_5 = d_1 d_4$, and $d_0 d_7 = d_1 d_6$. From this, we conclude that $\mathrm{CC}(-I) \in \mathcal{S}_1$.

For the gate $\mathrm{C}(Z \otimes Z) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ -1,\ -1,\ 1)$, we have that $d_0 d_3 = d_1 d_2$ and $d_4 d_7 = d_5 d_6$. Also, we have that $d_0 d_7 = d_3 d_4$ and $d_1 d_6 = d_2 d_5$. From this, we conclude that $\mathrm{C}(Z \otimes Z) \in \mathcal{S}_2 \cap \mathcal{S}_3$, but also that $\mathrm{C}(Z \otimes Z) \notin \mathcal{S}_1$.

If we change -1 to i in $\mathrm{C}(Z \otimes Z)$, we get the gate $D_3 = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ i,\ i,\ 1)$, and we have $d_0 d_7 = d_3 d_4$ and $d_1 d_6 = d_2 d_5$. From this, we conclude that $D_3 \in \mathcal{S}_3$. Similarly, we can easily check that $D_3 \notin \mathcal{S}_2$.

For the gate $\mathrm{C}(S \otimes S^\dagger) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ -i,\ i,\ 1)$, and we have $d_0 d_3 = d_1 d_2$ and $d_4 d_7 = d_5 d_6$. From this, we conclude that $\mathrm{C}(S \otimes S^\dagger) \in \mathcal{S}_2$. Similarly, we can easily check that $\mathrm{C}(S \otimes S^\dagger) \notin \mathcal{S}_3$.

Examples from Section 3. Now we turn to the gates from Section 3. In Examples 3.1 and 3.2 we considered the 3-qubit gate $\mathrm{CC}(X)$, which can be conjugated with $I \otimes I \otimes H$ to give the diagonal gate $\mathrm{CC}(Z) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ -1)$. We have $\mathrm{CC}(Z) \notin \mathcal{S}_4$ because $d_0 d_3 d_5 d_6 = 1 \neq -1 = d_1 d_2 d_4 d_7$. Also, $\mathrm{CC}(Z) \notin \mathcal{S}_5^1$ because $d_0 d_3 d_4 d_7 = -1 \neq 1 = d_1 d_2 d_5 d_6$. Similarly, we can easily check that $\mathrm{CC}(Z) \notin \mathcal{S}_5^2$ and $\mathrm{CC}(Z) \notin \mathcal{S}_5^3$. So, $\mathrm{CC}(Z) \notin \mathcal{S}_4 \cup \mathcal{S}_5$.

In Examples 3.3 and 3.4 we considered $\mathrm{CC}(R_z(\alpha)) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ e^{-i\frac{\alpha}{2}},\ e^{i\frac{\alpha}{2}})$. We have $\mathrm{CC}(R_z(\alpha)) \in \mathcal{S}_5^3 \subseteq \mathcal{S}_5$ because $d_0 d_1 d_6 d_7 = d_2 d_3 d_4 d_5$. Similarly, we can easily check that $\mathrm{CC}(R_z(\alpha)) \notin \mathcal{S}_3 \cup \mathcal{S}_4 \cup \mathcal{S}_5^1 \cup \mathcal{S}_5^2$.

In Example 3.5 we considered the 3-qubit diagonal gate $W = \mathrm{Diag}(1,\ 1,\ 1,\ -1,\ 1,\ i,\ i,\ 1)$. We have $W \in \mathcal{S}_4 \cap \mathcal{S}_5$ because $d_0 d_3 d_5 d_6 = d_1 d_2 d_4 d_7$, and also $d_0 d_3 d_4 d_7 = d_1 d_2 d_5 d_6$. Similarly, we can easily check that $W \notin \mathcal{S}_2 \cup \mathcal{S}_3$.

6 THE EXPRESSIVENESS OF FOUR NEIGHBOR GATES

In this section, we state two theorems on the expressiveness of four neighbor gates. We begin with Theorem 6.1, which says that a 3-qubit diagonal gate D belongs to subsets of $\mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented using particular products of four neighbor gates. This is significant because some 3-qubit diagonal gates, such as $\mathrm{CC}(R_z(\alpha))$, are in one of the subsets of $\mathcal{S}_4 \cup \mathcal{S}_5$ but not the others, as we saw in Section 5.

Theorem 6.1. *Suppose D is a 3-qubit diagonal gate.*

(1) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5^1$ if and only if there exist four 2-qubit gates U_1, U_2, U_3, U_4, such that $\overline{U_1}_{AC}\,\overline{U_2}_{AB}\,\overline{U_3}_{AC}\,\overline{U_4}_{AB} = D$.*
(2) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5^2$ if and only if there exist four 2-qubit gates U_1, U_2, U_3, U_4 such that $\overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{U_3}_{BC}\,\overline{U_4}_{AB} = D$.*
(3) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5^3$ if and only if there exist four 2-qubit gates U_1, U_2, U_3, U_4 such that $\overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{BC}\,\overline{U_4}_{AC} = D$.*

We prove Theorem 6.1 by first proving Property (3) through a sequence of if-and-only-if statements. First, $D \in \mathcal{S}_4 \cup \mathcal{S}_5^3$ if and only if for particular d_0', d_1', we have that $\mathrm{CC}(\mathrm{Diag}(d_0', d_1'))$ satisfies $d_0' d_1' = 1$ or $d_0' = d_1'$. Then we use Lemma A.9 to see that $\mathrm{CC}(\mathrm{Diag}(d_0', d_1'))$ satisfies this constraint if and only if $\mathrm{CC}(\mathrm{Diag}(d_0', d_1'))$ can be implemented by a particular combination of four neighbor gates. Finally, we use Lemma 5.2 to transform this combination of neighbor gates to a product that both has the desired form and equals D. After we are done with proving Proving (3), we use Lemma 5.1 and Lemma 5.2 to derive Properties (1)–(2) from Property (3).

Proof. (Theorem 6.1) Suppose we have a 3-qubit diagonal gate $D = \mathrm{Diag}(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7)$. We will prove the three properties in the order (3), (2), (1).

Property (3). We reason as follows.

$$
\begin{aligned}
D \in \mathcal{S}_4 \cup \mathcal{S}_5^3 \quad &\Longleftrightarrow \quad d_0 d_3 d_5 d_6 = d_1 d_2 d_4 d_7 \quad \vee \quad d_0 d_1 d_6 d_7 = d_2 d_3 d_4 d_5 \\
&\Longleftrightarrow \quad \frac{d_6\, d_0}{d_2\, d_4} = \frac{d_7\, d_1}{d_3\, d_5} \quad \vee \quad \frac{d_6\, d_0}{d_2\, d_4} \cdot \frac{d_7\, d_1}{d_3\, d_5} = 1 \\
&\Longleftrightarrow \quad \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad\qquad \overline{V_1}_{AC}\,\overline{V_2}_{BC}\,\overline{V_3}_{AC}\,\overline{V_4}_{BC} = \mathrm{CC}(\mathrm{Diag}(\frac{d_6\, d_0}{d_2\, d_4}, \frac{d_7\, d_1}{d_3\, d_5})) \\
&\Longleftrightarrow \quad \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad\qquad \overline{S}_{AB}\,\overline{V_1}_{AC}\,\overline{V_2}_{BC}\,\overline{V_3}_{AC}\,\overline{V_4}_{BC}\,\overline{S}_{AB} = \overline{S}_{AB}\,\mathrm{CC}(\mathrm{Diag}(\frac{d_6\, d_0}{d_2\, d_4}, \frac{d_7\, d_1}{d_3\, d_5}))\,\overline{S}_{AB} \\
&\Longleftrightarrow \quad \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad\qquad \overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{BC}\,\overline{V_4}_{AC} = \mathrm{CC}(\mathrm{Diag}(\frac{d_6\, d_0}{d_2\, d_4}, \frac{d_7\, d_1}{d_3\, d_5})) \\
&\Longleftrightarrow \quad \exists \text{ 2-qubit gates } U_1, U_2, U_3, U_4 : \\
&\qquad\qquad \overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{BC}\,\overline{U_4}_{AC} = D
\end{aligned}
\tag{17}
$$

In the first step, we use the definitions of D, $\mathcal{S}_4$, $\mathcal{S}_5^3$. In the third step, we use Lemma A.9. In the fifth step, we use Lemma 5.2. In the sixth step, we define $W_1 = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3)$ and $W_4 = \mathrm{Diag}(1,\ 1,\ d_4/d_0,\ d_5/d_1)$, and then we use $U_1 = W_1 V_1$ and $U_2 = V_2$ and $U_3 = V_3$ and $U_4 = V_4 W_4$. This is sufficient to complete the proof of Property (3) because we have:

$$
\begin{aligned}
\overline{W_1}_{BC}\,\mathrm{CC}(\mathrm{Diag}(\frac{d_6\, d_0}{d_2\, d_4}, \frac{d_7\, d_1}{d_3\, d_5}))\,\overline{W_4}_{AC} \quad &= \quad \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3,\ d_0,\ d_1,\ d_2,\ d_3) \\
&\qquad\quad \mathrm{Diag}(1, 1, 1, 1, 1, 1, \frac{d_6\, d_0}{d_2\, d_4}, \frac{d_7\, d_1}{d_3\, d_5}) \\
&\qquad\quad \mathrm{Diag}(1, 1, 1, 1, d_4/d_0,\ d_5/d_1,\ d_4/d_0,\ d_5/d_1) \\
&= \quad \mathrm{Diag}(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7) \\
&= \quad D
\end{aligned}
$$

Property (2). We reason as follows.

$$\begin{aligned}
D \in \mathcal{S}_4 \cup \mathcal{S}_5^2 &\iff \overline{S}_{BC}\, D\, \overline{S}_{BC} \in \mathcal{S}_4 \cup \mathcal{S}_5^3 \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{BC}\, \overline{V_4}_{AC} = \overline{S}_{BC}\, D\, \overline{S}_{BC} \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{S}_{BC}\, \overline{V_1}_{BC}\, \overline{V_2}_{AC}\, \overline{V_3}_{BC}\, \overline{V_4}_{AC}\, \overline{S}_{BC} = D \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{S\, V_1\, S}_{BC}\, \overline{V_2}_{AB}\, \overline{S\, V_3\, S}_{BC}\, \overline{V_4}_{AB} = D \\
&\iff \exists \text{ 2-qubit gates } U_1, U_2, U_3, U_4 : \\
&\qquad \overline{U_1}_{BC}\, \overline{U_2}_{AB}\, \overline{U_3}_{BC}\, \overline{U_4}_{AB} = D
\end{aligned} \tag{18}$$

In the first step, we use Lemma 5.1. In the second step, we use Property (3). In the fourth step, we use Lemma 5.2.

Property (1). We reason as follows.

$$\begin{aligned}
D \in \mathcal{S}_4 \cup \mathcal{S}_5^1 &\iff \overline{S}_{AB}\, D\, \overline{S}_{AB} \in \mathcal{S}_4 \cup \mathcal{S}_5^2 \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{V_1}_{BC}\, \overline{V_2}_{AB}\, \overline{V_3}_{BC}\, \overline{V_4}_{AB} = \overline{S}_{AB}\, D\, \overline{S}_{AB} \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{S}_{AB}\, \overline{V_1}_{BC}\, \overline{V_2}_{AB}\, \overline{V_3}_{BC}\, \overline{V_4}_{AB}\, \overline{S}_{AB} = D \\
&\iff \exists \text{ 2-qubit gates } V_1, V_2, V_3, V_4 : \\
&\qquad \overline{V_1}_{AC}\, \overline{S\, V_2\, S}_{AB}\, \overline{V_3}_{AC}\, \overline{S\, V_4\, S}_{AB} = D \\
&\iff \exists \text{ 2-qubit gates } U_1, U_2, U_3, U_4 : \\
&\qquad \overline{U_1}_{AC}\, \overline{U_2}_{AB}\, \overline{U_3}_{AC}\, \overline{U_4}_{AB} = D
\end{aligned}$$

In the first step, we use Lemma 5.1. In the second step, we use Property (2). In the fourth step, we use Lemma 5.2. □

Next, we state Theorem 6.2, which says that the following four classes of 3-qubit diagonal gates are equivalent: (1) $\mathcal{S}_4 \cup \mathcal{S}_5$, (2) those implemented with four neighbor gates, (3) those implemented with five neighbor gates, and (4) those implemented with four unrestricted gates.

Theorem 6.2. *Suppose D is a 3-qubit diagonal gate. The following conditions on D are equivalent.*

(1) $D \in \mathcal{S}_4 \cup \mathcal{S}_5$.
(2) *There exist four 2-qubit gates U_1, U_2, U_3, U_4, such that $\overline{U_1}_{i_1}\, \overline{U_2}_{i_2}\, \overline{U_3}_{i_1}\, \overline{U_4}_{i_2} = D$, where $i_1, i_2 \in \{ AB, AC, BC \}$.*
(3) *There exist five 2-qubit gates W_1, W_2, W_3, W_4, W_5, such that $\overline{W_1}_{j_1}\, \overline{W_2}_{j_2}\, \overline{W_3}_{j_1}\, \overline{W_4}_{j_2}\, \overline{W_5}_{j_1} = D$, where $j_1, j_2 \in \{ AB, AC, BC \}$.*
(4) *There exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{V_1}_{k_1}\, \overline{V_2}_{k_2}\, \overline{V_3}_{k_3}\, \overline{V_4}_{k_4} = D$, where $k_1, k_2, k_3, k_4 \in \{ AB, AC, BC \}$.*

Notice that in Theorem 6.2, each of Properties (2)–(3) uses just two indices, which means that the matrix products use neighbor gates. In contrast, Property (4) uses four indices.

We give the proof of Theorem 6.2 below, but first we outline the idea of the proof. The centerpiece of the proof is Table 3, which summarizes key properties that we prove in a suite of lemmas. Notice that in Table 3, each row has a structure that is similar to the four items in Theorem 6.2. Specifically,

the first column of Table 3 has a subset of $\mathcal{S}_4 \cup \mathcal{S}_5$, the third column has a product of four neighbor gates, the fourth column has a product of five neighbor gates, and the fifth column has a product of four unrestricted gates. Additionally, the second column lists the two qubits that the first gate in each of the products in columns 3–5 works on.

Table 3. Summary of our lemmas in Theorem 6.2.

D	1^{st} gate	Four neighbor gates	Five neighbor gates	Four gates
$\mathcal{S}_4 \cup \mathcal{S}_5^3$	BC	$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}\,\overline{U_{4AC}}$	$\overline{W_{1BC}}\,\overline{W_{2AC}}$	$\overline{V_{1BC}}\,\overline{V_{2AC}}$
$\mathcal{S}_4 \cup \mathcal{S}_5^2$		$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3BC}}\,\overline{U_{4AB}}$	$\overline{W_{3BC}}\,\overline{W_{4AC}}\,\overline{W_{5BC}}$	$\overline{V_{3AB}}\,\overline{V_{4BC}}$
$\mathcal{S}_4 \cup \mathcal{S}_5^2$	AB	$\overline{U_{1AB}}\,\overline{U_{2BC}}\,\overline{U_{3AB}}\,\overline{U_{4BC}}$	$\overline{W_{1AB}}\,\overline{W_{2BC}}$	$\overline{V_{1AB}}\,\overline{V_{2BC}}$
$\mathcal{S}_4 \cup \mathcal{S}_5^1$		$\overline{U_{1AB}}\,\overline{U_{2AC}}\,\overline{U_{3AB}}\,\overline{U_{4AC}}$	$\overline{W_{3AB}}\,\overline{W_{4BC}}\,\overline{W_{5AB}}$	$\overline{V_{3AC}}\,\overline{V_{4AB}}$
$\mathcal{S}_4 \cup \mathcal{S}_5^3$	AC	$\overline{U_{1AC}}\,\overline{U_{2BC}}\,\overline{U_{3AC}}\,\overline{U_{4BC}}$	$\overline{W_{1AC}}\,\overline{W_{2BC}}$	$\overline{V_{1AC}}\,\overline{V_{2BC}}$
$\mathcal{S}_4 \cup \mathcal{S}_5^1$		$\overline{U_{1AC}}\,\overline{U_{2AB}}\,\overline{U_{3AC}}\,\overline{U_{4AB}}$	$\overline{W_{3AC}}\,\overline{W_{4BC}}\,\overline{W_{5AC}}$	$\overline{V_{3AB}}\,\overline{V_{4AC}}$

The key idea of Table 3 is to show different approaches to implementing gates in the three sets $\mathcal{S}_4 \cup \mathcal{S}_5^1$, $\mathcal{S}_4 \cup \mathcal{S}_5^2$, and $\mathcal{S}_4 \cup \mathcal{S}_5^3$. For example, if we want to consider an implementation of a gate in $\mathcal{S}_4 \cup \mathcal{S}_5^3$, and we want the first gate to operate on qubits BC, then Table 3 suggests three different ways of doing it. The first implementation uses four neighbor gates, and the second uses five neighbor gates, while the third, in column "Four gates", uses four unrestricted gates.

Table 3 is based on two key lemmas. First, in Appendix C, Lemma C.1 shows a reduction from arbitrary products of four 2-qubit unrestricted gates to the nine cases listed in the third and fifth columns of Table 3. Lemma C.2 shows a reduction from arbitrary products of five 2-qubit neighbor gates to the three cases listed in the fourth column of Table 3. Together, Lemma C.1 and Lemma C.2 enable us to focus on the products listed in Table 3 when we discuss a product using four or five 2-qubit gates in Theorem 6.2.

Proof. (Theorem 6.2) We will prove (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

Condition (1) $\Rightarrow$ Condition (2). Immediate from Theorem 6.1, using $\mathcal{S}_5 = \mathcal{S}_5^1 \cup \mathcal{S}_5^2 \cup \mathcal{S}_5^3$.

Condition (2) $\Rightarrow$ Condition (3). We use I as the fifth gate.

Condition (3) $\Rightarrow$ Condition (4). Suppose there exist five 2-qubit gates W_1, W_2, W_3, W_4, W_5, such that $\overline{W_1}_{j_1}\,\overline{W_2}_{j_2}\,\overline{W_3}_{j_1}\,\overline{W_4}_{j_2}\,\overline{W_5}_{j_1} = D$, where $j_1, j_2 \in \{ AB, AC, BC \}$. According to Lemma C.2, we can assume that the product is one of the three cases in the fourth column in Table 3. We will consider each of those three cases in turn.

First, if $j_1 = BC$ and $j_2 = AC$, then from Lemma 4.4, we have that there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC} = D$.

Second, if $j_1 = AB$ and $j_2 = BC$, then according to Lemma 5.2, we know that $\overline{S}_{BC}\,\overline{S}_{AC}\,D\,\overline{S}_{AC}\,\overline{S}_{BC} = \overline{W_1}_{BC}\,\overline{S\,W_2\,S}_{AC}\,\overline{W_3}_{BC}\,\overline{S\,W_4\,S}_{AC}\,\overline{W_5}_{BC}$. According to Lemma 4.4, there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{S}_{BC}\,\overline{S}_{AC}\,D\,\overline{S}_{AC}\,\overline{S}_{BC} = \overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC}$. From this, according to Lemma 5.2, we know that $D = \overline{V_1}_{AB}\,\overline{S\,V_2\,S}_{BC}\,\overline{S\,V_3\,S}_{AC}\,\overline{V_4}_{AB}$.

Third, if $j_1 = AC$ and $j_2 = BC$, then according to Lemma 5.2, we know that $\overline{S}_{AB}\,D\,\overline{S}_{AB} = \overline{W_1}_{BC}\,\overline{W_2}_{AC}\,\overline{W_3}_{BC}\,\overline{W_4}_{AC}\,\overline{W_5}_{BC}$. According to Lemma 4.4, there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{S}_{AB}\,D\,\overline{S}_{AB} = \overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{V_3}_{AB}\,\overline{V_4}_{BC}$. From this, according to Lemma 5.2, we know that $D = \overline{V_1}_{AC}\,\overline{V_2}_{BC}\,\overline{S\,V_3\,S}_{AB}\,\overline{V_4}_{AC}$.

Thus, in all three cases, we get the desired conclusion.

Condition (4) ⇒ Condition (1). Suppose there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{V_1}_{k_1}\,\overline{V_2}_{k_2}\,\overline{V_3}_{k_3}\,\overline{V_4}_{k_4} = D$, where $k_1, k_2, k_3, k_4 \in \{\ AB,\ AC,\ BC\ \}$. From Lemma C.1 we have that we can assume that the product is one of the nine cases in the third and fifth columns in Table 3. We will show the three cases in the fifth column in detail here. The first case we will consider is the one where $k_1 = BC$, $k_2 = AC$, $k_3 = AB$, and $k_4 = BC$. Let us write $D = \mathsf{Diag}(d_0, d_1, \ldots, d_7)$ as $D = |0\rangle\langle 0| \otimes D_0 + |1\rangle\langle 1| \otimes D_1$, where $D_0 = \mathsf{Diag}(d_0, d_1, d_2, d_3)$ and $D_1 = \mathsf{Diag}(d_4, d_5, d_6, d_7)$. From the assumption about D, we have that

$$\overline{V_2}_{AC}\,\overline{V_3}_{AB} = |0\rangle\langle 0| \otimes (V_1^\dagger\, D_0\, V_4^\dagger) + |1\rangle\langle 1| \otimes (V_1^\dagger\, D_1\, V_4^\dagger) \tag{19}$$

By Equation (19), according to Lemma A.14, there exist four 1-qubit gates P_0, P_1, Q_0, Q_1, such that $\overline{V_2}_{AC}\,\overline{V_3}_{AB} = |0\rangle\langle 0| \otimes P_0 \otimes Q_0 + |1\rangle\langle 1| \otimes P_1 \otimes Q_1$, and we have that

$$D_0 = V_1\,(P_0 \otimes Q_0)\,V_4 \qquad D_1 = V_1\,(P_1 \otimes Q_1)\,V_4 \tag{20}$$

By Equation (20), we conclude that

$$D_0^\dagger\, D_1 = V_4^\dagger\,(P_0^\dagger P_1 \otimes Q_0^\dagger Q_1)\,V_4 \tag{21}$$

By Lemma A.11, there exist four complex numbers a, b, p, q, such that $\mathsf{Eigenvalues}(P_0^\dagger P_1 \otimes Q_0^\dagger Q_1) = (ap,\ bp,\ aq,\ bq)$. From this and by Equation (21), we have that

$$\begin{aligned} \mathsf{Eigenvalues}(D_0^\dagger\, D_1) &= (\frac{d_4}{d_0},\ \frac{d_5}{d_1},\ \frac{d_6}{d_2},\ \frac{d_7}{d_3}) \\ = \mathsf{Eigenvalues}(V_4^\dagger\,(P_0^\dagger P_1 \otimes Q_0^\dagger Q_1)\,V_4) &= (ap,\ bp,\ aq,\ bq) \end{aligned} \tag{22}$$

According to Equation (22), we conclude that for $\mathsf{Eigenvalues}(D_0^\dagger\, D_1)$, there exists the multiplication of two eigenvalues equal to the multiplication of the other two eigenvalues. Thus, we have the following three cases. (1) If $d_0 d_1 d_6 d_7 = d_2 d_3 d_4 d_5$, we conclude that $D \in \mathcal{S}_5^3$. (2) If $d_0 d_2 d_5 d_7 = d_1 d_3 d_4 d_6$, we conclude that $D \in \mathcal{S}_5^2$. (3) If $d_0 d_3 d_5 d_6 = d_1 d_2 d_4 d_7$, we conclude that $D \in \mathcal{S}_4$. As a result, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^2 \cup \mathcal{S}_5^3 \subseteq \mathcal{S}_4 \cup \mathcal{S}_5$.

For the second case where $k_1 = AB$, $k_2 = BC$, $k_3 = AC$, and $k_4 = AB$, according Lemma 5.2, we have that $\overline{S}_{BC}\,\overline{S}_{AC}\,D\,\overline{S}_{AC}\,\overline{S}_{BC} = \overline{V_1}_{BC}\,\overline{S\,V_2\,S}_{AC}\,\overline{S\,V_3\,S}_{AB}\,\overline{V_4}_{BC}$. From the analysis of the first case, we conclude that $\overline{S}_{BC}\,\overline{S}_{AC}\,D\,\overline{S}_{AC}\,\overline{S}_{BC} \in \mathcal{S}_4 \cup \mathcal{S}_5^2 \cup \mathcal{S}_5^3$. According to Lemma 5.1, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^1 \cup \mathcal{S}_5^2 \subseteq \mathcal{S}_4 \cup \mathcal{S}_5$.

For the third case where $k_1 = AC$, $k_2 = BC$, $k_3 = AB$, and $k_4 = AC$, according Lemma 5.2, we have that $\overline{S}_{AB}\,D\,\overline{S}_{AB} = \overline{V_1}_{BC}\,\overline{V_2}_{AC}\,\overline{S\,V_3\,S}_{AB}\,\overline{V_4}_{BC}$. From the analysis of the first case, we conclude that $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_4 \cup \mathcal{S}_5^2 \cup \mathcal{S}_5^3$. According to Lemma 5.1, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^1 \cup \mathcal{S}_5^3 \subseteq \mathcal{S}_4 \cup \mathcal{S}_5$.

For the other six cases in the third column, three of them can be derived according to Theorem 6.1, and the other three cases can be derived by symmetry. For the first case where $k_1 = AB$, $k_2 = AC$, $k_3 = AB$, and $k_4 = AC$, if $D = \overline{V_1}_{AB}\overline{V_2}_{AC}\overline{V_3}_{AB}\overline{V_4}_{AC}$, then we have that $D^\dagger = \overline{V_4^\dagger}_{AC}\overline{V_3^\dagger}_{AB}\overline{V_2^\dagger}_{AC}\overline{V_1^\dagger}_{AB}$. According to Theorem 6.1 property (1), we conclude that $D^\dagger \in \mathcal{S}_4 \cup \mathcal{S}_5^1$. According to Lemma 5.3, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^1$.

For the second case where $k_1 = AB$, $k_2 = BC$, $k_3 = AB$, and $k_4 = BC$, if $D = \overline{V_1}_{AB}\overline{V_2}_{BC}\overline{V_3}_{AB}\overline{V_4}_{BC}$, then we have that $D^\dagger = \overline{V_4^\dagger}_{BC}\overline{V_3^\dagger}_{AB}\overline{V_2^\dagger}_{BC}\overline{V_1^\dagger}_{AB}$. According to Theorem 6.1 property (2), we conclude that $D^\dagger \in \mathcal{S}_4 \cup \mathcal{S}_5^2$. According to Lemma 5.3, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^2$.

For the third case where $k_1 = AC$, $k_2 = BC$, $k_3 = AC$, and $k_4 = BC$, if $D = \overline{V_1}_{AC}\overline{V_2}_{BC}\overline{V_3}_{AC}\overline{V_4}_{BC}$, then we have that $D^\dagger = \overline{V_4^\dagger}_{BC}\overline{V_3^\dagger}_{AC}\overline{V_2^\dagger}_{BC}\overline{V_1^\dagger}_{AC}$. According to Theorem 6.1 property (3), we conclude that $D^\dagger \in \mathcal{S}_4 \cup \mathcal{S}_5^3$. According to Lemma 5.3, we conclude that $D \in \mathcal{S}_4 \cup \mathcal{S}_5^3$.

The above three cases, along with six others that can be derived according to Theorem 6.1, lead to the overall conclusion that $D \in \mathcal{S}_4 \cup \mathcal{S}_5$. □

7 CHARACTERIZATION OF ALL 3-QUBIT DIAGONAL GATES

In this section, we first state two theorems that give upper bounds on the number of 2-qubit gates needed to implement a 3-qubit diagonal gate. We begin with Theorem 7.1, which focuses on neighbor gates.

Theorem 7.1. *Suppose D is a 3-qubit diagonal gate.*

(1) *We have $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit neighbor gate.*
(2) *We have $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit neighbor gates.*
(3) *We have $D \in \mathcal{S}_2 \cup \mathcal{S}_3$ if and only if D can be implemented with three 2-qubit neighbor gates.*
(4) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit neighbor gates.*
(5) *We have $D \in \mathcal{S}_6$ if and only if D can be implemented with six 2-qubit neighbor gates.*

Notice that $\mathcal{S}_2$ appears twice in Theorem 7.1 because we state if-and-only-if properties. Specifically, in the forwards direction, both 2 and 3 are upper bounds for $\mathcal{S}_2$, while in the backwards direction, we characterize accurately which gates can be implemented with two 2-qubit neighbor gates and with three 2-qubit neighbor gates. In Appendix D, we prove each if-and-only-if property by proving the two directions separately. For the left-to-right direction, we pick a 3-qubit diagonal gate from the given subset and then implement it with neighbor gates. For the right-to-left direction, we first assume that a three-qubit diagonal gate D equals the product of some 2-qubit neighbor gates. Then we discuss which restrictions each neighbor gate must satisfy to make this equation valid. The neighbor gates satisfy those restrictions simultaneously, which let us derive the subset to which D belongs.

Next, we state Theorem 7.2, which focuses on unrestricted gates.

Theorem 7.2. *Suppose D is a 3-qubit diagonal gate.*

(1) *We have $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit unrestricted gate.*
(2) *We have $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit unrestricted gates.*
(3) *We have $D \in \mathcal{S}_3 \cup \mathcal{S}_4$ if and only if D can be implemented with three 2-qubit unrestricted gates.*
(4) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit unrestricted gates.*
(5) *We have $D \in \mathcal{S}_6$ if and only if D can be implemented with five 2-qubit unrestricted gates.*

Notice that $\mathcal{S}_4$ appears twice in Theorem 7.2, which is because we state if-and-only-if properties. In Appendix E, we prove Theorem 7.2. In the left-to-right direction, the cases of $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, and $\mathcal{S}_5$ are immediate from Theorem 7.1. In contrast, we give a separate proof of the case of $\mathcal{S}_4$, akin to the proof of the case of $\mathcal{S}_4$ in Theorem 7.1, and we also give a separate proof of the case of $\mathcal{S}_6$. In the right-to-left direction, we do the proof in a manner similar to that of Theorem 7.1, but without neighbor restrictions.

Now we use the upper bounds in Theorem 7.1 and Theorem 7.2, along with examples from Section 5, to prove Corollary 7.3, which states least upper bounds.

Corollary 7.3. *Table 2 states the least upper bounds on the number of 2-qubit gates needed to implement any gate in $\mathcal{S}_1, \ldots, \mathcal{S}_6$.*

Proof. For $\mathcal{S}_1$, according to Theorem 7.1.(1), the upper bound on the number of 2-qubit neighbor gates is 1, and according to Theorem 7.2.(1), the upper bound on the number of 2-qubit unrestricted gates is 1. Because there exists a 3-qubit diagonal gate $\mathrm{CC}(-I) = \mathrm{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ -1,\ -1) = \mathrm{C}(Z) \otimes I$, such that $\mathrm{CC}(-I) \in \mathcal{S}_1$ and $\mathrm{CC}(-I)$ cannot be implemented without 2-qubit gates, we

conclude that for $\mathcal{S}_1$, the least upper bound on the number of 2-qubit neighbor gates is 1, and the least upper bound on the number of 2-qubit unrestricted gates is 1.

For $\mathcal{S}_2$, according to Theorem 7.1.(2), the upper bound on the number of 2-qubit neighbor gates is 2, and according to Theorem 7.2.(2), the upper bound on the number of 2-qubit unrestricted gates is 2. Because there exists a 3-qubit diagonal gate $\mathsf{C}(Z \otimes Z) = \mathsf{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ -1,\ -1,\ 1)$, such that $\mathsf{C}(Z \otimes Z) \in \mathcal{S}_2$ and $\mathsf{C}(Z \otimes Z) \notin \mathcal{S}_1$, we conclude that $\mathsf{C}(Z \otimes Z)$ cannot be implemented with one 2-qubit neighbor gate according to Theorem 7.1.(1) or one 2-qubit unrestricted gate according to Theorem 7.2.(1). Thus, for $\mathcal{S}_2$, the least upper bound on the number of 2-qubit neighbor gates is 2, and the least upper bound on the number of 2-qubit unrestricted gates is 2.

For $\mathcal{S}_3$, according to Theorem 7.1.(3), the upper bound on the number of 2-qubit neighbor gates is 3, and according to Theorem 7.2.(3), the upper bound on the number of 2-qubit unrestricted gates is 3. Because there exists a 3-qubit diagonal gate $D_3 = \mathsf{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ i,\ i,\ 1)$, such that $D_3 \in \mathcal{S}_3$ and $D_3 \notin \mathcal{S}_2$, we conclude that D_3 cannot be implemented with two 2-qubit neighbor gates according to Theorem 7.1.(2) or two 2-qubit unrestricted gates according to Theorem 7.2.(2). Thus, for $\mathcal{S}_3$, the least upper bound on the number of 2-qubit neighbor gates is 3, and the least upper bound on the number of 2-qubit unrestricted gates is 3.

For $\mathcal{S}_4$, according to Theorem 7.1.(4), the upper bound on the number of 2-qubit neighbor gates is 4, and according to Theorem 7.2.(3), the upper bound on the number of 2-qubit unrestricted gates is 3. Because there exists a 3-qubit diagonal gate $W = \mathsf{Diag}(1,\ 1,\ 1,\ -1,\ 1,\ i,\ i,\ 1)$ as shown in Example 3.5, such that $W \in \mathcal{S}_4$ and $W \notin \mathcal{S}_2 \cup \mathcal{S}_3$, we conclude that W cannot be implemented with three 2-qubit neighbor gates according to Theorem 7.1.(3) or two 2-qubit unrestricted gates according to Theorem 7.2.(2). Thus, for $\mathcal{S}_4$, the least upper bound on the number of 2-qubit neighbor gates is 4, and the least upper bound on the number of 2-qubit unrestricted gates is 3.

For $\mathcal{S}_5$, according to Theorem 7.1.(4), the upper bound on the number of 2-qubit neighbor gates is 4, and according to Theorem 7.2.(4), the upper bound on the number of 2-qubit unrestricted gates is 4. Because there exists a 3-qubit diagonal gate $\mathsf{CC}(R_z(\alpha)) = \mathsf{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ e^{-i\frac{\alpha}{2}},\ e^{i\frac{\alpha}{2}})$ as shown in Examples 3.3 and 3.4, such that $\mathsf{CC}(R_z(\alpha)) \in \mathcal{S}_5$ and $W \notin \mathcal{S}_3 \cup \mathcal{S}_4$, we conclude that $\mathsf{CC}(R_z(\alpha))$ cannot be implemented with three 2-qubit neighbor gates according to Theorem 7.1.(3) or three 2-qubit unrestricted gates according to Theorem 7.2.(3). Thus, for $\mathcal{S}_5$, the least upper bound on the number of 2-qubit neighbor gates is 4, and the least upper bound on the number of 2-qubit unrestricted gates is 4.

For $\mathcal{S}_6$, according to Theorem 7.1.(5), the upper bound on the number of 2-qubit neighbor gates is 6, and according to Theorem 7.2.(5), the upper bound on the number of 2-qubit unrestricted gates is 5. Because there exists a 3-qubit diagonal gate $\mathsf{CC}(Z) = \mathsf{Diag}(1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ -1)$, such that $\mathsf{CC}(Z) \in \mathcal{S}_6$ and $W \notin \mathcal{S}_4 \cup \mathcal{S}_5$, we conclude that $\mathsf{CC}(Z)$ cannot be implemented with four 2-qubit unrestricted gates according to Theorem 7.2.(4). Also, according to Theorem 6.2, we conclude that $\mathsf{CC}(Z)$ cannot be implemented with five 2-qubit neighbor gates. Thus, for $\mathcal{S}_6$, the least upper bound on the number of 2-qubit neighbor gates is 6, and the least upper bound on the number of 2-qubit unrestricted gates is 5.

In summary, we have proved that Table 2 states the least upper bounds on the number of 2-qubit gates needed to implement any gate in $\mathcal{S}_1, \ldots, \mathcal{S}_6$. □

8 OUR EXAMPLE CIRCUITS IN SECTION 3 ARE OPTIMAL

The Circuits in Examples 3.1 and 3.2 are optimal. Each of our circuits in Examples 3.1 and 3.2 implements $\mathsf{CC}(X)$ using six neighbor gates. Because $\mathsf{CC}(X)$ can be diagonalized using 1-qubit gates to $\mathsf{CC}(Z)$, the number of two-qubit neighbor gates needed to implement $\mathsf{CC}(X)$ is the same as for $\mathsf{CC}(Z)$. From Section 5, we have that $\mathsf{CC}(Z) \notin \mathcal{S}_4 \cup \mathcal{S}_5$. From this and Theorem 6.2, specifically

(3) $\Rightarrow$ (1), we conclude that five 2-qubit neighbor gates cannot make a Toffoli gate, so six neighbor gates are needed.

The Circuit in Example 3.3 is optimal. Our circuit in Example 3.3 implements $\mathrm{CC}(R_z(\alpha))$ using four neighbor gates. From Section 5, we have that $\mathrm{CC}(R_z(\alpha)) \in \mathcal{S}_5^3 \subseteq \mathcal{S}_5$, but $\mathrm{CC}(R_z(\alpha)) \notin \mathcal{S}_3 \cup \mathcal{S}_4 \cup \mathcal{S}_5^1 \cup \mathcal{S}_5^2$. From this, because $\mathcal{S}_2 \subseteq \mathcal{S}_4$, according to Theorem 7.1.(3), we conclude that three 2-qubit neighbor gates cannot make a $\mathrm{CC}(R_z(\alpha))$ gate, so four neighbor gates are needed.

The Circuit in Example 3.4 is optimal. Our circuit in Example 3.4 implements $\mathrm{CC}(R_z(\alpha))$ using five neighbor gates on AB and BC. From Section 5, we have that $\mathrm{CC}(R_z(\alpha)) \in \mathcal{S}_5^3$, but $\mathrm{CC}(R_z(\alpha)) \notin \mathcal{S}_3 \cup \mathcal{S}_4 \cup \mathcal{S}_5^1 \cup S_5^2$. From Theorem 6.1.(2) and $\mathrm{CC}(R_z(\alpha)) \notin \mathcal{S}_4 \cup \mathcal{S}_5^2$, we have that we cannot implement $\mathrm{CC}(R_z(\alpha))$ on AB and BC using four neighbor gates, so five neighbor gates on AB and BC are needed.

The Circuits in Example 3.5 is optimal. Our circuits in Example 3.5 implements W using three unrestricted gates and four neighbor gates, respectively. From Section 5, we have that $W \in \mathcal{S}_4 \cap \mathcal{S}_5$, but $W \notin \mathcal{S}_2 \cup \mathcal{S}_3$. From this and according to Theorem 7.2.(2), we conclude that two 2-qubit unrestricted gates cannot make a W gate, so three unrestricted gates are needed. Also, according to Theorem 7.1.(3), we conclude that three 2-qubit neighbor gates cannot make a W gate, so four neighbor gates are needed.

The impact of qubit layout. Examples 3.1 and 3.2 along with Equation (1) illustrate that the optimal number of 2-qubit gates for implementing a 3-qubit diagonal gate outside $\mathcal{S}_4 \cup \mathcal{S}_5$, depends on whether we allow unrestricted gates or only neighbor gates. Similarly, Example 3.5 illustrates that the optimal number of 2-qubit gates for implementing a gate in $\mathcal{S}_4$, but outside $\mathcal{S}_2 \cup \mathcal{S}_3$, depends on whether we allow unrestricted gates or only neighbor gates. Examples 3.3 and 3.4 illustrate that the optimal number of 2-qubit neighbor gates for implementing a gate in $\mathcal{S}_5$, but outside $\mathcal{S}_3 \cup \mathcal{S}_4$, depends on the qubit layout.

9 RELATED WORK

Least upper bounds for 3-qubit Diagonal Gates. [Palsberg and Yu 2024; Yu et al. 2013; Yu and Ying 2015] studied 3-qubit diagonal gates of the form $\mathrm{CC}(\mathrm{Diag}(d_0,\ d_1))$. They proved the following least upper bounds on the number of unrestricted gates needed in an implementation. If $\mathrm{CC}(\mathrm{Diag}(d_0,\ d_1)) \in \mathcal{S}_1$, which happens when $d_0 = d_1$, then it can be implemented using one 2-qubit gate. If $\mathrm{CC}(\mathrm{Diag}(d_0,\ d_1)) \in \mathcal{S}_5$ which happens when $d_0\, d_1 = 1$ or $d_0 = d_1$, then it can be implemented using four 2-qubit gates. In general, if $\mathrm{CC}(\mathrm{Diag}(d_0,\ d_1)) \in \mathcal{S}_6$, then it can be implemented using five 2-qubit gates. Our Theorem 7.2 generalizes their results.

For any 3-qubit diagonal gate D, [Shende and Markov 2008] proved the following least upper bounds on the number of unrestricted $\mathrm{C}(X)$ gates needed in an implementation. If $D \in \mathcal{S}_1$, then it can be implemented with two $\mathrm{C}(X)$ gates. If $D \in \mathcal{S}_4$, then it can be implemented with five $\mathrm{C}(X)$ gates, a remarkable jump from the three gates that are sufficient if we can freely pick the 2-qubit gates. If $D \in \mathcal{S}_5$, then it can be implemented with four $\mathrm{C}(X)$ gates. Notice that elements of $\mathcal{S}_4$ require as most as many 2-qubit unrestricted gates as elements of $\mathcal{S}_5$ according to Theorem 7.2, while, perhaps surprisingly, elements of $\mathcal{S}_4$ require at least as many unrestricted $\mathrm{C}(X)$ gates as elements of $\mathcal{S}_5$. This is possible in part because $\mathcal{S}_4 \not\subseteq \mathcal{S}_5$ and $\mathcal{S}_5 \not\subseteq \mathcal{S}_4$. If $D \in \mathcal{S}_6$, then it can be implemented with six $\mathrm{C}(X)$ gates.

Mapping Circuits to Neighbor Gates. [Wille et al. 2014] presented strategies for mapping a quantum circuit to a nearest-neighbor architecture by inserting swap gates. Many papers on this mapping problem have followed, including [Farghadan and Mohammadzadeh 2017] for a two-dimensional

grid, [Bhattacharjee et al. 2018; Hattori and Yamashita 2019] for a two-dimensional architecture, and [Chang and Lee 2021; Datta et al. 2022a,b] for a two-dimensional hexagonal architecture. [Zhao et al. 2020] studied how to map a variety of controlled gates to a nearest-neighbor architecture. [Duckering et al. 2021] showed how to implement a Toffoli gate using eight $\mathrm{C}(X)$ neighbor gates. [Park and Ahn 2023] constructed a one-dimensional nearest-neighbor circuit for the quantum Fourier transform. None of those papers show optimality.

10 CONCLUSION

The Toffoli gate is a key building block for error-corrected quantum computers, and it is a key component of many quantum algorithms. For implementing a Toffoli gate, we consider common quantum architectures that have only neighbor gates, and we prove that six 2-qubit neighbor gates are necessary and sufficient. Moreover, we prove least upper bounds for implementing 3-qubit diagonal gates using neighbor gates and using unrestricted gates, respectively. We find that while the expressive power of four 2-qubit unrestricted gates is the same as four 2-qubit neighbor gates, the expressive power of five 2-qubit unrestricted gates is strictly more than five 2-qubit neighbor gates.

Our results are independent of specific gate sets. This implies that there is no gate set with 2-qubit gates and 1-qubit gates that supports that we use just five neighbor gates to implement a Toffoli gate. Rather, for any specific gate set, we must use at least six neighbor gates.

We see at least six directions for future work, which we discuss below.

Automation. Is it possible to automate our analysis by an SMT-solver or an automated theorem prover? Such an automation could provide more general insights for larger and more complex configurations that might be intractable to analyze manually.

ZX-calculus. Can some of our proofs be given more easily using ZX-calculus or ZH-calculus?

Limited gate sets. Actual quantum hardware typically supports only a limited gate set. How many neighbor gates are required to implement a Toffoli gate under such hardware constraints?

Asymptotic lower bounds. How many neighbor gates are required to implement an n-qubit Toffoli gates with $(n-1)$ controls? Shende and Markov [2008] showed that we need at least $2n$ unrestricted $\mathrm{C}(X)$ gates, and we speculate that a lower bound on the number of neighbor $\mathrm{C}(X)$ gates will be even higher.

General 3-qubit gates. How many neighbor gates are required to implement any 3-qubit gate? [Chen et al. 2024] showed that 11 unrestricted gates are sufficient, and we speculate that we need even more neighbor gates.

Non-neighbors. How many neighbor gates are required to implement a Toffoli gate on three qubits that are connected but where either none of them are neighbors or only two of them are neighbors? One way to approach this case might be to use swap gates to bring two pairs of the qubits to be neighbors, resulting in the situation in Figure 5.

Qubit mapping. How can our results be integrated into an algorithm for qubit mapping?

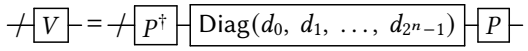
Different qubit technologies. Different qubit technologies have different constraints on "which qubits are neighbors?" In this paper, we have taken our motivation from a leading kind of quantum computer that uses superconducting qubits. However, quantum computers based on trapped-ion qubits, spin qubits, and neutral-atom qubits come with different constraints. This opens the question of how many 2-qubit gates are needed to implement a Toffoli gate on such computers. For example, we can ask how many Mølmer-Sørensen gates are needed.

Acknowledgements. We are grateful to the anonymous reviewers for their many helpful suggestions that led us to improve the paper. We are supported by the NSF QLCI program: grant number OMA-2016245.

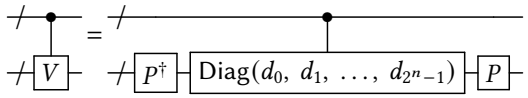
A KNOWN LEMMAS

Lemma A.1. [Shende and Markov 2008, Observation 2] *For an $(n+1)$-qubit gate V, it commutes with Z gates on qubit i if and only if there exist two n-qubit gates V_0 and V_1, such that $V = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1$ on qubit i.*

Lemma A.2. [Horn and Johnson 2012, Theorem 2.5.3] *For an n-qubit gate V, there exist 2^n complex numbers $d_0, d_1, \ldots, d_{2^n-1}$ and one n-qubit gate P, where* Eigenvalues$(V) = (d_0,\ d_1,\ \ldots,\ d_{2^n-1})$*, such that*

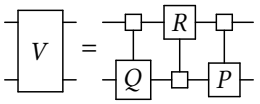


Lemma A.3. *For an n-qubit gate V, there exist 2^n complex numbers $d_0, d_1, \ldots, d_{2^n-1}$ and one n-qubit gate P, where* Eigenvalues$(V) = (d_0,\ d_1,\ \ldots,\ d_{2^n-1})$*, such that*

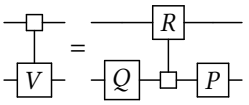


Proof. One can easily prove this according to Lemma A.2. □

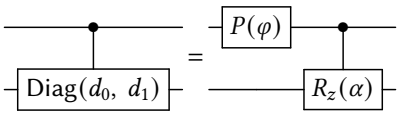
Lemma A.4. [Paige and Wei 1994] *For a 2-qubit gate V, there exist six 1-qubit gates P_0, P_1, $R_y(\theta_0)$, $R_y(\theta_1)$, Q_0, and Q_1 and three 2-qubit gates $P = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, $R = R_y(\theta_0) \otimes |0\rangle\langle 0| + R_y(\theta_1) \otimes |1\rangle\langle 1|$, and $Q = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$, such that*



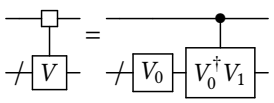
Lemma A.5. [Shende et al. 2005] *For two 1-qubit gates V_0 and V_1 and one 2-qubit gate $V = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1$, there exist four 1-qubit gates P, Q, $R_z(\alpha_0)$, and $R_z(\alpha_1)$ and one 2-qubit gate $R = R_z(\alpha_0) \otimes |0\rangle\langle 0| + R_z(\alpha_1) \otimes |1\rangle\langle 1|$, such that*



Lemma A.6. [Shende and Markov 2008, Equation 4] *Suppose d_0, d_1 are two complex numbers. For* C(Diag$(d_0,\ d_1)$)*, there exist one 1-qubit gate $P(\varphi)$ and one 2-qubit gate* C$(R_z(\alpha))$*, such that*



Lemma A.7. *For two n-qubit gates V_0 and V_1, we have $V = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1 =$* C$(V_1 V_0^\dagger)$ $(I \otimes V_0)$.



Proof. C$(V_1 V_0^\dagger)$ $(I \otimes V_0) = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes V_1 V_0^\dagger)$ $(I \otimes V_0) = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1$. □

Lemma A.8. [Palsberg and Yu 2024, Lemma 6.1] *For a 2-qubit gate V, either*

- $\exists|y\rangle : V(|y\rangle \otimes |0\rangle)$ *is entangled, or*
- $\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : V(|y\rangle \otimes |0\rangle) = |x\rangle \otimes |z\rangle$*, or*
- $\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : V(|y\rangle \otimes |0\rangle) = |z\rangle \otimes |x\rangle$.

Lemma A.9. [Palsberg and Yu 2024, Lemma 6.4] *Suppose d_0, d_1 are complex numbers such that $|d_0| = |d_1| = 1$. There exist 2-qubit unitaries U_1, U_2, U_3, U_4, such that $\overline{U_1}_{AC}\,\overline{U_2}_{BC}\,\overline{U_3}_{AC}\,\overline{U_4}_{BC} = \mathsf{CC}(\mathsf{Diag}(d_0, d_1))$ if and only if either $d_0 = d_1$ or $d_0 d_1 = 1$.*

Lemma A.10. *For square matrices U, V of the same size, we have that* $\det(U\,V) = \det(U)\det(V)$.

Lemma A.11. [Palsberg and Yu 2024, Lemma A.5] *For 1-qubit gates P and Q and complex numbers a, b, p, q, if* $\mathsf{Eigenvalues}(P) = (a, b)$ *and* $\mathsf{Eigenvalues}(Q) = (p, q)$*, then* $\mathsf{Eigenvalues}(P \otimes Q) = (ap, aq, bp, bq)$.

Lemma A.12. [Palsberg and Yu 2024, Lemma A.6] *For 1-qubit gates P, Q, we have that* $\mathsf{Eigenvalues}(|0\rangle\langle 0| \otimes P + |1\rangle\langle 1| \otimes Q) = \mathsf{Eigenvalues}(P) \sqcup \mathsf{Eigenvalues}(Q)$.

Lemma A.13. [Palsberg and Yu 2024, Lemma A.19] *If V is a 2-qubit gate and $|\phi\rangle_{BC}$, $|\omega\rangle_{BC}$ are 4-dimensional unit vectors, such that $\overline{V}_{AC}(|0\rangle_A \otimes |\phi\rangle_{BC}) = |0\rangle_A \otimes |\omega\rangle_{BC}$ and $|\phi\rangle_{BC}$ is entangled, then V is of the following form, where P_0 and P_1 are 1-qubit gates*

$$V = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$$

Lemma A.14. [Palsberg and Yu 2024, Lemma A.24] *For 2-qubit gates U, V, W_0, W_1, if*

$$\overline{U}_{AC}\,\overline{V}_{AB} = |0\rangle\langle 0| \otimes W_0 + |1\rangle\langle 1| \otimes W_1$$

then

$$\overline{U}_{AC}\,\overline{V}_{AB} = |0\rangle\langle 0| \otimes P_0 \otimes Q_0 + |1\rangle\langle 1| \otimes P_1 \otimes Q_1$$

, where P_0, Q_0, P_1, Q_1 are 1-qubit gates.

Lemma A.15. [Palsberg and Yu 2024, Lemma A.30] *For 2-qubit gates U_1, U_2, U_3, U_4, for which*

$$\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : U_2(|y\rangle \otimes |0\rangle) = |z\rangle \otimes |x\rangle$$

there exist 2-qubit gates V_1, V_2, V_4 and a 1-qubit gate P such that

$$\overline{U_1}_{AC}\,\overline{U_2}_{BC}\,\overline{U_3}_{AC}\,\overline{U_4}_{BC} = \overline{V_1}_{AC}\,\overline{V_2}_{BC}\,\overline{U_3}_{AC}\,\overline{V_4}_{BC}$$
$$V_2 = I \otimes |0\rangle\langle 0| + P \otimes |1\rangle\langle 1|$$

Lemma A.16. [Palsberg and Yu 2024, Lemma A.32] *For 2-qubit gates U_1, U_2, U_3, U_4, there exist 2-qubit gates V_1, V_2, V_3, V_4, such that*

$$\overline{U_1}_{AC}\,\overline{U_2}_{BC}\,\overline{U_3}_{AC}\,\overline{U_4}_{BC} = \overline{V_1}_{AC}\,\overline{V_2}_{BC}\,\overline{V_3}_{AC}\,\overline{V_4}_{BC}$$
$$V_3(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$

Lemma A.17. [Palsberg and Yu 2024, Lemma A.33] *For 2-qubit gates V_1, V_2, V_4, if*

$$\forall|y\rangle : \overline{V_1}_{AC}\overline{V_2}_{BC}(|0\rangle_A \otimes |y\rangle_B \otimes |0\rangle_C) = \overline{V_4}^{\dagger}_{BC}(|0\rangle_A \otimes |y\rangle_B \otimes |0\rangle_C)$$
$$\exists|x\rangle : \forall|y\rangle : \exists|z\rangle : V_2(|y\rangle \otimes |0\rangle) = |x\rangle \otimes |z\rangle$$

then V_1 is of the following form, where P_0, P_1 are 1-qubit gates:

$$V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$$

B CHARACTERISTICS OF $\mathcal{S}_i^j$ SETS

In this section, we prove two characteristics of $\mathcal{S}_i^j$ sets mentioned in Section 5. Lemma 5.1 states that $\mathcal{S}_i^j$ sets can be transformed to another one with the same i index after swap transformations. Lemma 5.2 states that both the number of unrestricted 2-qubit gates and the number of neighbor 2-qubit gates stay the same after swap transformations. Lemma 5.3 states that the dagger operation will not change the set to which the 3-qubit diagonal gate belongs.

Lemma 5.1. *(1) $\overline{S}_{BC}\,\mathcal{S}_i^1\,\overline{S}_{BC} = \mathcal{S}_i^1$, (2) $\overline{S}_{AB}\,\mathcal{S}_i^1\,\overline{S}_{AB} = \mathcal{S}_i^2$, (3) $\overline{S}_{AC}\,\mathcal{S}_i^1\,\overline{S}_{AC} = \mathcal{S}_i^3$, (4) $\overline{S}_{AC}\,\mathcal{S}_i^2\,\overline{S}_{AC} = \mathcal{S}_i^2$, (5) $\overline{S}_{BC}\,\mathcal{S}_i^2\,\overline{S}_{BC} = \mathcal{S}_i^3$, and (6) $\overline{S}_{AB}\,\mathcal{S}_i^3\,\overline{S}_{AB} = \mathcal{S}_i^3$.*

Proof. Suppose we have that $D = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3,\ d_4,\ d_5,\ d_6,\ d_7)$. For property (1), we suppose $\overline{S}_{BC}\,D\,\overline{S}_{BC} = \mathrm{Diag}(d_0,\ d_2,\ d_1,\ d_3,\ d_4,\ d_6,\ d_5,\ d_7) = \mathrm{Diag}(d_0',\ d_1',\ d_2',\ d_3',\ d_4',\ d_5',\ d_6',\ d_7')$. From this, we know that: (1) If $D \in \mathcal{S}_1^1$, then $d_0d_5 = d_1d_4$, $d_0d_6 = d_2d_4$, and $d_0d_7 = d_3d_4$. Thus, we have $d_0'd_6' = d_2'd_4'$, $d_0'd_5' = d_1'd_4'$, and $d_0'd_7' = d_3'd_4'$ and $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_1^1$. (2) If $D \in \mathcal{S}_2^1$, then $d_0d_3 = d_1d_2$ and $d_4d_7 = d_5d_6$. Thus, we have $d_0'd_3' = d_1'd_2'$ and $d_4'd_7' = d_5'd_6'$ and $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_2^1$. (3) If $D \in \mathcal{S}_3^1$, then $d_0d_7 = d_3d_4$ and $d_1d_6 = d_2d_5$. Thus, we have $d_0'd_7' = d_3'd_4'$ and $d_2'd_5' = d_1'd_6'$ and $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_3^1$. (4) If $D \in \mathcal{S}_4^1$, then $d_0d_3d_5d_6 = d_1d_2d_4d_7$. Thus, we have $d_0'd_3'd_5'd_6' = d_1'd_2'd_4'd_7'$ and $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_4^1$. (5) If $D \in \mathcal{S}_5^1$, then $d_0d_3d_4d_7 = d_1d_2d_5d_6$. Thus, we have $d_0'd_3'd_4'd_7' = d_1'd_2'd_5'd_6'$ and $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_5^1$. (6) If $D \in \mathcal{S}_6^1$, then $\overline{S}_{BC}\,D\,\overline{S}_{BC} \in \mathcal{S}_6^1$ by definition.

For property (2), we suppose $\overline{S}_{AB}\,D\,\overline{S}_{AB} = \mathrm{Diag}(d_0,\ d_1,\ d_4,\ d_5,\ d_2,\ d_3,\ d_6,\ d_7)$ and D is equal to $\mathrm{Diag}(d_0',\ d_1',\ d_2',\ d_3',\ d_4',\ d_5',\ d_6',\ d_7')$. From this, we know that: (1) If $D \in \mathcal{S}_1^1$, then $d_0d_5 = d_1d_4$, $d_0d_6 = d_2d_4$, and $d_0d_7 = d_3d_4$. Thus, we have $d_0'd_3' = d_1'd_2'$, $d_0'd_6' = d_2'd_4'$, and $d_0'd_7' = d_2'd_5'$ and $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_1^2$. (2) If $D \in \mathcal{S}_2^1$, then $d_0d_3 = d_1d_2$ and $d_4d_7 = d_5d_6$. Thus, we have $d_0'd_5' = d_1'd_4'$ and $d_2'd_7' = d_3'd_6'$ and $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_2^2$. (3) If $D \in \mathcal{S}_3^1$, then $d_0d_7 = d_3d_4$ and $d_1d_6 = d_2d_5$. Thus, we have $d_0'd_7' = d_2'd_5'$ and $d_1'd_6' = d_3'd_4'$ and $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_3^2$. (4) If $D \in \mathcal{S}_4^1$, then $d_0d_3d_5d_6 = d_1d_2d_4d_7$. Thus, we have $d_0'd_3'd_5'd_6' = d_1'd_2'd_4'd_7'$ and $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_4^2$. (5) If $D \in \mathcal{S}_5^1$, then $d_0d_3d_4d_7 = d_1d_2d_5d_6$. Thus, we have $d_0'd_2'd_5'd_7' = d_1'd_3'd_4'd_6'$ and $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_5^2$. (6) If $D \in \mathcal{S}_6^1$, then $\overline{S}_{AB}\,D\,\overline{S}_{AB} \in \mathcal{S}_6^2$ by definition.

For property (3), we suppose $\overline{S}_{AC}\,D\,\overline{S}_{AC} = \mathrm{Diag}(d_0,\ d_4,\ d_2,\ d_6,\ d_1,\ d_5,\ d_3,\ d_7)$ and D is equal to $\mathrm{Diag}(d_0',\ d_1',\ d_2',\ d_3',\ d_4',\ d_5',\ d_6',\ d_7')$. From this, we know that: (1) If $D \in \mathcal{S}_1^1$, then $d_0d_5 = d_1d_4$, $d_0d_6 = d_2d_4$, and $d_0d_7 = d_3d_4$. Thus, we have $d_0'd_5' = d_1'd_4'$, $d_0'd_3' = d_1'd_2'$, and $d_0'd_7' = d_1'd_6'$ and $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_1^3$. (2) If $D \in \mathcal{S}_2^1$, then $d_0d_3 = d_1d_2$ and $d_4d_7 = d_5d_6$. Thus, we have $d_0'd_6' = d_2'd_4'$ and $d_1'd_7' = d_3'd_5'$ and $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_2^3$. (3) If $D \in \mathcal{S}_3^1$, then $d_0d_7 = d_3d_4$ and $d_1d_6 = d_2d_5$. Thus, we have $d_0'd_7' = d_1'd_6'$ and $d_3'd_4' = d_2'd_5'$ and $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_3^3$. (4) If $D \in \mathcal{S}_4^1$, then $d_0d_3d_5d_6 = d_1d_2d_4d_7$. Thus, we have $d_0'd_3'd_5'd_6' = d_1'd_2'd_4'd_7'$ and $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_4^3$. (5) If $D \in \mathcal{S}_5^1$, then $d_0d_3d_4d_7 = d_1d_2d_5d_6$. Thus, we have $d_0'd_1'd_6'd_7' = d_2'd_3'd_4'd_5'$ and $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_5^3$. (6) If $D \in \mathcal{S}_6^1$, then $\overline{S}_{AC}\,D\,\overline{S}_{AC} \in \mathcal{S}_6^3$ by definition.

For property (4), we have $\overline{S}_{AC}\,\mathcal{S}_i^2\,\overline{S}_{AC} = \overline{S}_{AC}\,\overline{S}_{AB}\,\mathcal{S}_i^1\,\overline{S}_{AB}\,\overline{S}_{AC} = \overline{S}_{AB}\,\overline{S}_{BC}\,\mathcal{S}_i^1\,\overline{S}_{BC}\,\overline{S}_{AB} = \mathcal{S}_i^2$.

For property (5), we have $\overline{S}_{BC}\,\mathcal{S}_i^2\,\overline{S}_{BC} = \overline{S}_{BC}\,\overline{S}_{AB}\,\mathcal{S}_i^1\,\overline{S}_{AB}\,\overline{S}_{BC} = \overline{S}_{AC}\,\overline{S}_{BC}\,\mathcal{S}_i^1\,\overline{S}_{BC}\,\overline{S}_{AC} = \mathcal{S}_i^3$.

For property (6), we have $\overline{S}_{AB}\,\mathcal{S}_i^3\,\overline{S}_{AB} = \overline{S}_{AB}\,\overline{S}_{AC}\,\mathcal{S}_i^1\,\overline{S}_{AC}\,\overline{S}_{AB} = \overline{S}_{AC}\,\overline{S}_{BC}\,\mathcal{S}_i^1\,\overline{S}_{BC}\,\overline{S}_{AC} = \mathcal{S}_i^3$. □

Lemma 5.2. *For $k \in \{ AB, AC, BC \}$, a 3-qubit gate D can be implemented with m 2-qubit gates as $D = \overline{U_{1i_1}}\,\overline{U_{2i_2}} \ldots \overline{U_{mi_m}}$ if and only if $\overline{S}_k D \overline{S}_k$ can be implemented with m 2-qubit gates as $\overline{S}_k D \overline{S}_k = \overline{V_{1j_1}}\,\overline{V_{2j_2}} \ldots \overline{V_{mj_m}}$. Specifically, for p ranging from 1 to m,*

(1) *for $k = BC$, we have if $i_p = BC$ then $V_p = S U_p S$ and $j_p = BC$, if $i_p = AC$ then $V_p = U_p$ and $j_p = AB$, and if $i_p = AB$ then $V_p = U_p$ and $j_p = AC$.*
(2) *for $k = AC$, we have if $i_p = BC$ then $V_p = S U_p S$ and $j_p = AB$, if $i_p = AC$ then $V_p = S U_p S$ and $j_p = AC$, and if $i_p = AB$ then $V_p = S U_p S$ and $j_p = BC$.*
(3) *for $k = AB$, we have if $i_p = BC$ then $V_p = U_p$ and $j_p = AC$, if $i_p = AC$ then $V_p = U_p$ and $j_p = BC$, and if $i_p = AB$ then $V_p = S U_p S$ and $j_p = AB$.*

Proof. Suppose we have that $D = \mathrm{Diag}(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7)$ and that D can be implemented with m 2-qubit gates $U_1, U_2, \ldots, U_m$ as $D = \overline{U_{1i_1}}\,\overline{U_{2i_2}} \ldots \overline{U_{mi_m}}$, where $i_1, i_2, \ldots, i_m \in \{ AB, AC, BC \}$.

If $k = BC$, then we have that $\overline{S}_{BC} D \overline{S}_{BC} = \mathrm{Diag}(d_0, d_2, d_1, d_3, d_4, d_6, d_5, d_7)$. From this, we conclude that $\overline{S}_{BC}\,\overline{U_{1i_1}}\,\overline{U_{2i_2}} \ldots \overline{U_{mi_m}}\,\overline{S}_{BC} = (\overline{S}_{BC}\,\overline{U_{1i_1}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2i_2}}\,\overline{S}_{BC}) \ldots (\overline{S}_{BC}\,\overline{U_{mi_m}}\,\overline{S}_{BC})$. For p ranging from 1 to m, if $i_p = BC$, we define $V_p = S U_p S$ and $j_p = BC$. If $i_p = AC$, we define $V_p = U_p$ and $j_p = AB$. If $i_p = AB$, we define $V_p = U_p$ and $j_p = AC$. From the above, according to Section 2, we have that $(\overline{S}_{BC}\,\overline{U_{1i_1}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2i_2}}\,\overline{S}_{BC}) \ldots (\overline{S}_{BC}\,\overline{U_{mi_m}}\,\overline{S}_{BC}) = \overline{V_{1j_1}}\,\overline{V_{2j_2}} \ldots \overline{V_{mj_m}}$.

If $k = AC$, then we have that $\overline{S}_{AC} D \overline{S}_{AC} = \mathrm{Diag}(d_0, d_4, d_2, d_6, d_1, d_5, d_3, d_7)$. From this, we conclude that $\overline{S}_{AC}\,\overline{U_{1i_1}}\,\overline{U_{2i_2}} \ldots \overline{U_{mi_m}}\,\overline{S}_{AC} = (\overline{S}_{AC}\,\overline{U_{1i_1}}\,\overline{S}_{AC})\,(\overline{S}_{AC}\,\overline{U_{2i_2}}\,\overline{S}_{AC}) \ldots (\overline{S}_{AC}\,\overline{U_{mi_m}}\,\overline{S}_{AC})$. For p ranging from 1 to m, if $i_p = BC$, we define $V_p = S U_p S$ and $j_p = AB$. If $i_p = AC$, we define $V_p = S U_p S$ and $j_p = AC$. If $i_p = AB$, we define $V_p = S U_p S$ and $j_p = BC$. From the above, according to Section 2, we have that $(\overline{S}_{AC}\,\overline{U_{1i_1}}\,\overline{S}_{AC})\,(\overline{S}_{AC}\,\overline{U_{2i_2}}\,\overline{S}_{AC}) \ldots (\overline{S}_{AC}\,\overline{U_{mi_m}}\,\overline{S}_{AC}) = \overline{V_{1j_1}}\,\overline{V_{2j_2}} \ldots \overline{V_{mj_m}}$.

If $k = AB$, then we have that $\overline{S}_{AB} D \overline{S}_{AB} = \mathrm{Diag}(d_0, d_1, d_4, d_5, d_2, d_3, d_6, d_7)$. From this, we conclude that $\overline{S}_{AB}\,\overline{U_{1i_1}}\,\overline{U_{2i_2}} \ldots \overline{U_{mi_m}}\,\overline{S}_{AB} = (\overline{S}_{AB}\,\overline{U_{1i_1}}\,\overline{S}_{AB})\,(\overline{S}_{AB}\,\overline{U_{2i_2}}\,\overline{S}_{AB}) \ldots (\overline{S}_{AB}\,\overline{U_{mi_m}}\,\overline{S}_{AB})$. For p ranging from 1 to m, if $i_p = BC$, we define $V_p = U_p$ and $j_p = AC$. If $i_p = AC$, we define $V_p = U_p$ and $j_p = BC$. If $i_p = AB$, we define $V_p = S U_p S$ and $j_p = AB$. From the above, according to Section 2, we have that $(\overline{S}_{AC}\,\overline{U_{1i_1}}\,\overline{S}_{AC})\,(\overline{S}_{AC}\,\overline{U_{2i_2}}\,\overline{S}_{AC}) \ldots (\overline{S}_{AC}\,\overline{U_{mi_m}}\,\overline{S}_{AC}) = \overline{V_{1j_1}}\,\overline{V_{2j_2}} \ldots \overline{V_{mj_m}}$.

From the above, we conclude that D can be implemented with m 2-qubit gates if and only if $\overline{S}_k D \overline{S}_k$ can be implemented with m 2-qubit gates. Also, if we fix k, then each j_p after adding swap gates has a one-to-one correspondence to i_p before adding swap gates. Thus, these m 2-qubit gates are 2-qubit neighbor (unrestricted) gates before the swap transformations if and only if these m 2-qubit gates are 2-qubit neighbor (unrestricted) gates before the swap transformations. □

Lemma 5.3. *A 3-qubit diagonal gate $D \in \mathcal{S}_i^j$ if and only if $D^\dagger \in \mathcal{S}_i^j$.*

Proof. For two 3-qubit diagonal gate $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7)$ and $D^\dagger = \mathrm{Diag}(d_0^\dagger, d_1^\dagger, \ldots, d_7^\dagger)$, we have that $D \in \mathcal{S}_i^j$ if and only if $D^\dagger \in \mathcal{S}_i^j$. This is because all the equations needed are still valid after the dagger operation. □

C REDUCTION TO A FEW CASES IN THEOREM 6.2

In Table 3, we list six implementations using four neighbor gates, three implementations using five 2-qubit neighbor gates, and three implementations using four 2-qubit unrestricted gates. This is sufficient because of the following two lemmas. Lemma C.1 reduces the number of implementations using four 2-qubit unrestricted gates to nine, and Lemma C.2 reduces the number of implementations using five 2-qubit neighbor gates to three.

Lemma C.1. *For four 2-qubit gates U_1, U_2, U_3, U_4, there exist 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_3}}\,\overline{U_{4i_4}} = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_3}}\,\overline{V_{4j_4}}$, where $i_1, i_2, i_3, i_4 \in \{ AB, AC, BC \}$ and j_1, j_2, j_3, j_4 satisfy one of the following cases:*

(1) $j_1 = BC$, $j_2 = AC$, $j_3 = BC$, $j_4 = AC$.
(2) $j_1 = BC$, $j_2 = AB$, $j_3 = BC$, $j_4 = AB$.
(3) $j_1 = BC$, $j_2 = AC$, $j_3 = AB$, $j_4 = BC$.
(4) $j_1 = AB$, $j_2 = BC$, $j_3 = AB$, $j_4 = BC$.
(5) $j_1 = AB$, $j_2 = AC$, $j_3 = AB$, $j_4 = AC$.
(6) $j_1 = AB$, $j_2 = BC$, $j_3 = AC$, $j_4 = AB$.
(7) $j_1 = AC$, $j_2 = BC$, $j_3 = AC$, $j_4 = BC$.
(8) $j_1 = AC$, $j_2 = AB$, $j_3 = AC$, $j_4 = AB$.
(9) $j_1 = AC$, $j_2 = BC$, $j_3 = AB$, $j_4 = AC$.

Proof. For products using four 2-qubit gates U_1, U_2, U_3, U_4, we first restrict $i_1 = BC$. We examine all products as shown in Table 4. We see that three of the products are already among the nine cases in the lemma, so we copy them straight to the third column and add the case number. For each one of the five remaining products, we map the first column to the second column by inserting S gates that cancel out and by using associativity. The result is an expression that we simplify to the expression in the third column, using the properties of S gates listed in Section 2. The expression in the third column can easily be seen as one of the first three cases in the lemma.

By defining $A' = C$, $B' = A$, and $C' = B$, for $i_1 = B'C'$, according to Table 4, we have that for four 2-qubit gates U_1, U_2, U_3, U_4, there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_3}}\,\overline{U_{4i_4}} = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_3}}\,\overline{V_{4j_4}}$, where $i_2, i_3, i_4 \in \{ A'B', A'C', B'C' \}$ and j_1, j_2, j_3, j_4 satisfy case (4), case (5), or case (6).

By defining $A' = B$, $B' = A$, and $C' = C$, for $i_1 = B'C'$, according to Table 4, we have that for four 2-qubit gates U_1, U_2, U_3, U_4, there exist four 2-qubit gates V_1, V_2, V_3, V_4, such that $\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_3}}\,\overline{U_{4i_4}} = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_3}}\,\overline{V_{4j_4}}$, where $i_2, i_3, i_4 \in \{ A'B', A'C', B'C' \}$ and j_1, j_2, j_3, j_4 satisfy case (7), case (8), or case (9).

From the above, we conclude that all products using four 2-qubit gates can be implemented with nine specific products using four 2-qubit gates. □

Lemma C.2. *For five 2-qubit gates U_1, U_2, U_3, U_4, U_5, there exist five 2-qubit gates V_1, V_2, V_3, V_4, V_5, such that $\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_1}}\,\overline{U_{4i_2}}\,\overline{U_{5i_1}} = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_1}}\,\overline{V_{4j_2}}\,\overline{V_{5j_1}}$, where $i_1, i_2 \in \{ AB, AC, BC \}$ and j_1, j_2 satisfy one of the following cases:*

(1) $j_1 = BC$, $j_2 = AC$.
(2) $j_1 = AB$, $j_2 = BC$.
(3) $j_1 = AC$, $j_2 = BC$.

Proof. For products using five 2-qubit neighbor gates U_1, U_2, U_3, U_4, U_5, we first restrict $i_1 = BC$. We examine all products and summarize them in Table 5. We see that one of the products is already among the three cases in the lemma, so we copy them directly to the third column and add the case number. For the one remaining gate combination, we do the following calculations, we map the first column to the second column by inserting S gates that cancel out and by using associativity. The result is an expression that we simplify to the expression in the second column, using the properties of S gates listed in Section 2. The expression in the third column can easily be seen as the first case in the lemma.

By defining $A' = C$, $B' = A$, and $C' = B$, for $i_1 = B'C'$, according to Table 5, we have that for five 2-qubit neighbor gates U_1, U_2, U_3, U_4, U_5, there exist five 2-qubit neighbor gates V_1, V_2, V_3, V_4, V_5,

Table 4. Implement products using four 2-qubit gates within a few combinations

when $i_1 = BC$.

$\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_3}}\,\overline{U_{4i_4}}$	$\overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_3}}\,\overline{V_{4j_4}}$		
$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3AC}}\,\overline{U_{4AB}}$	$\overline{U_{1BC}}\,(\overline{U_{2AB}}\,\overline{S}_{AB})$ $(\overline{S}_{AB}\,\overline{U_{3AC}}\,\overline{S}_{AB})\,(\overline{S}_{AB}\,\overline{U_{4AB}})$	(2)	$\overline{U_{1BC}}\,\overline{U_2\,S}_{AB}\,\overline{U_{3BC}}\,\overline{S\,U_{4AB}}$
$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3AC}}\,\overline{U_{4BC}}$	$(\overline{U_{1BC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2AB}}\,\overline{S}_{BC})$ $(\overline{S}_{BC}\,\overline{U_{3AC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{4BC}})$	(3)	$\overline{U_1\,S}_{BC}\,\overline{U_{2AC}}\,\overline{U_{3AB}}\,\overline{S\,U_{4BC}}$
$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3BC}}\,\overline{U_{4AB}}$		(2)	$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3BC}}\,\overline{U_{4AB}}$
$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3BC}}\,\overline{U_{4AC}}$	$(\overline{U_{1BC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2AB}}\,\overline{S}_{BC})$ $(\overline{S}_{BC}\,\overline{U_{3BC}})\,\overline{U_{4AC}}$	(1)	$\overline{U_1\,S}_{BC}\,\overline{U_{2AC}}\,\overline{S\,U_{3BC}}\,\overline{U_{4AC}}$
$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3AB}}\,\overline{U_{4AC}}$	$\overline{U_{1BC}}\,(\overline{U_{2AC}}\,\overline{S}_{AC})$ $(\overline{S}_{BC}\,\overline{S}_{BC}\,\overline{S}_{AC}\,\overline{U_{3AB}}\,\overline{S}_{AC}\,\overline{S}_{BC}\,\overline{S}_{BC})$ $(\overline{S}_{AC}\,\overline{U_{4AC}})$	(1)	$\overline{U_{1BC}}\,\overline{U_2\,S}_{AC}\,\overline{S\,U_3\,S}_{BC}\,\overline{S\,U_{4AC}}$
$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3AB}}\,\overline{U_{4BC}}$		(3)	$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3AB}}\,\overline{U_{4BC}}$
$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}\,\overline{U_{4AB}}$	$(\overline{U_{1BC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2AC}}\,\overline{S}_{BC})$ $(\overline{S}_{BC}\,\overline{U_{3BC}})\,\overline{U_{4AB}}$	(2)	$\overline{U_1\,S}_{BC}\,\overline{U_{2AB}}\,\overline{S\,U_{3BC}}\,\overline{U_{4AB}}$
$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}\,\overline{U_{4AC}}$		(1)	$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}\,\overline{U_{4AC}}$

Table 5. Implement products using five 2-qubit neighbor gates within a few combinations

when $i_1 = BC$.

$\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_1}}\,\overline{U_{4i_2}}\,\overline{U_{5i_1}}$	$\overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_1}}\,\overline{V_{4j_2}}\,\overline{V_{5j_1}}$		
$\overline{U_{1BC}}\,\overline{U_{2AB}}\,\overline{U_{3BC}}\,\overline{U_{4AB}}\,\overline{U_{5BC}}$	$(\overline{U_{1BC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{2AB}}\,\overline{S}_{BC})$ $(\overline{S}_{BC}\,\overline{U_{3BC}}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_{4AB}}\,\overline{S}_{BC})$ $(\overline{S}_{BC}\,\overline{U_{5BC}})$	(1)	$\overline{U_1\,S}_{BC}\,\overline{U_{2AC}}\,\overline{S\,U_3\,S}_{BC}$ $\overline{U_{4AC}}\,\overline{S\,U_{5BC}}$
$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}\,\overline{U_{4AC}}\,\overline{U_{5BC}}$		(1)	$\overline{U_{1BC}}\,\overline{U_{2AC}}\,\overline{U_{3BC}}$ $\overline{U_{4AC}}\,\overline{U_{5BC}}$

such that $\overline{U_{1i_1}}\,\overline{U_{2i_2}}\,\overline{U_{3i_1}}\,\overline{U_{4i_2}}\,\overline{U_{5i_1}} = \overline{V_{1j_1}}\,\overline{V_{2j_2}}\,\overline{V_{3j_1}}\,\overline{V_{4j_2}}\,\overline{V_{5j_1}}$, where $i_2 \in \{A'B',\ A'C'\}$ and j_1, j_2 satisfy case (2).

By defining $A' = B$, $B' = A$, and $C' = C$, for $i_1 = B'C'$, according to Table 5, we have that for five 2-qubit neighbor gates U_1, U_2, U_3, U_4, U_5, there exist five 2-qubit neighbor gates V_1, V_2, V_3, V_4, V_5,

such that $\overline{U_1}_{i_1}\ \overline{U_2}_{i_2}\ \overline{U_3}_{i_1}\ \overline{U_4}_{i_2}\ \overline{U_5}_{i_1} = \overline{V_1}_{j_1}\ \overline{V_2}_{j_2}\ \overline{V_3}_{j_1}\ \overline{V_4}_{j_2}\ \overline{V_5}_{j_1}$, where $i_2 \in \{\ A'B',\ A'C'\}$ and j_1, j_2 satisfy case (3).

From the above, we conclude that all products using five 2-qubit neighbor gates can be implemented with three specific products using 2-qubit neighbor gates. □

D PROOF OF THEOREM 7.1

Here, we prove Theorem 7.1 from Section 7. Theorem 7.1 shows the tight bounds on the number of needed neighbor 2-qubit gates of 3-qubit diagonal gates.

Lemma D.1. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit neighbor gate.*

Proof. ($\Rightarrow$). If $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7) \in \mathcal{S}_1$, then we suppose that $D \in \mathcal{S}_1^1$. This is valid because according Lemma 5.1 and Lemma 5.2, $\mathcal{S}_1^1$, $\mathcal{S}_1^2$, and $\mathcal{S}_1^3$ have the same upper bound on the number of of 2-qubit neighbor gates. From this, we have that

$$d_0 d_5 = d_1 d_4, \quad d_0 d_6 = d_2 d_4, \quad d_0 d_7 = d_3 d_4$$

From the above, there exists one 2-qubit gate $U_1 = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3)$ and one 1-qubit gate $\mathrm{Diag}(1,\ d_4/d_0)$, such that $D = \mathrm{Diag}(1,\ d_4/d_0) \otimes U_1$.

($\Leftarrow$). If $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7)$ can be implemented with one 2-qubit gate U_1 and one 1-qubit gate P, then we suppose the first 2-qubit gate operates on the BC qubits as $D = P \otimes U_1$. This is valid because the other two cases, where the first 2-qubit gate operates on the AC qubits and AB qubits, lead to the same sets $\mathcal{S}_i$, according to Lemma 5.1 and Lemma 5.2. Because D commutes with Z gates on qubits A, B, and C, we know that P is a 1-qubit diagonal gate, and there exists two complex numbers a_0 and a_1, such that $P = \mathrm{Diag}(a_0, a_1)$. Similarly, we know that U_1 is a 2-qubit diagonal gate, and there exists four complex numbers b_0, b_1, b_2, and b_3, such that $U_1 = \mathrm{Diag}(b_0, b_1, b_2, b_3)$. From this, we have that $d_0 = a_0 b_0$, $d_1 = a_0 b_1$, $d_2 = a_0 b_2$, $d_3 = a_0 b_3$, $d_4 = a_1 b_0$, $d_5 = a_1 b_1$, $d_6 = a_1 b_2$, $d_7 = a_1 b_3$, from which we conclude

$$\begin{aligned} d_0 d_5 &= (a_0 b_0)\ (a_1 b_1) = (a_0 b_1)\ (a_1 b_0) = d_1 d_4 \\ d_0 d_6 &= (a_0 b_0)\ (a_1 b_2) = (a_0 b_2)\ (a_1 b_0) = d_2 d_4 \\ d_0 d_7 &= (a_0 b_0)\ (a_1 b_3) = (a_0 b_3)\ (a_1 b_0) = d_3 d_4 \end{aligned}$$

As a result, we have that $D \in \mathcal{S}_1^1 \subset \mathcal{S}_1$. □

Lemma D.2. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit neighbor gates.*

Proof. ($\Rightarrow$). If $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7) \in \mathcal{S}_2$, then we suppose that $D \in \mathcal{S}_2^3$. This is valid because according Lemma 5.1 and Lemma 5.2, $\mathcal{S}_2^1$, $\mathcal{S}_2^2$, and $\mathcal{S}_2^3$ have the same upper bound on the number of of 2-qubit neighbor gates. From this, we conclude that

$$d_0 d_6 = d_2 d_4, \quad d_1 d_7 = d_3 d_5$$

Thus, there exist 2-qubit gates $U_1 = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3)$ and $U_2 = \mathrm{Diag}(1,\ 1,\ d_4/d_0,\ d_5/d_1)$, such that $D = \overline{U_1}_{BC}\ \overline{U_2}_{AC}$.

($\Leftarrow$). If $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7)$ can be implemented with two 2-qubit gates U_1 and U_2, then we suppose the first 2-qubit gate operates on the BC qubits as $D = \overline{U_1}_{BC}\ \overline{U_2}_{AC}$ or $D = \overline{U_1}_{BC}\ \overline{U_2}_{AB}$. This is valid because the other two cases where the first 2-qubit gate operates on the AC qubits and AB qubits lead to the same sets $\mathcal{S}_i$ according to Lemma 5.1 and Lemma 5.2. For the first case, because D commutes with Z gates on qubits A and B, we conclude that U_1 commutes with Z gates on qubit B, and U_2 commutes with Z gates on qubit A. From this, according to Lemma A.1, there exist four

1-qubit gates P_0, P_1, Q_0, and Q_1, such that U_1 can be written as $U_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$ and U_2 can be written as $U_2 = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$. As a result, we have that $P_0\,Q_0 = \mathsf{Diag}(d_0,\ d_1)$, $P_1\,Q_0 = \mathsf{Diag}(d_2,\ d_3)$, $P_0\,Q_1 = \mathsf{Diag}(d_4,\ d_5)$, and $P_1\,Q_1 = \mathsf{Diag}(d_6,\ d_7)$. Because we have that $P_0\,Q_0\,Q_0^\dagger\,P_1^\dagger = P_0\,Q_1\,Q_1^\dagger\,P_1^\dagger$, we conclude that

$$\mathsf{Diag}(d_0/d_2,\ d_1/d_3) = (P_0\,Q_0)(Q_0^\dagger\,P_1^\dagger) = (P_0\,Q_1)(Q_1^\dagger\,P_1^\dagger) = \mathsf{Diag}(d_4/d_6,\ d_5/d_7)$$

From the above, we have that

$$d_0d_6 = d_2d_4, \quad d_1d_7 = d_3d_5$$

From this, we have that $D \in \mathcal{S}_2^3 \subset \mathcal{S}_2$.

For the second case, by applying the S gates, from Section 2, we have $\overline{S}_{BC}\,\overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{S}_{BC} = (\overline{S}_{BC}\,\overline{U_1}_{BC}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_2}_{AB}\,\overline{S}_{BC}) = \overline{S\,U_1\,S}_{BC}\,\overline{U_2}_{AC} = \overline{S}_{BC}\,D\,\overline{S}_{BC} = D'$. From Lemma 5.1 and Lemma 5.2 and the discussion for the first case, we conclude $D' \in \mathcal{S}_2$. □

Lemma D.3. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_2 \cup \mathcal{S}_3$ if and only if D can be implemented with three 2-qubit neighbor gates.*

Proof. ($\Rightarrow$). For $D = \mathsf{Diag}(d_0, d_1, \ldots, d_7)$, suppose that either $D \in \mathcal{S}_2$ or $D \in \mathcal{S}_3$. If $D \in \mathcal{S}_2$, then according to Lemma D.2, we can implement D by three 2-qubit neighbor gates. If $D \in \mathcal{S}_3$, we suppose that $D \in \mathcal{S}_3^1$. This is valid because according Lemma 5.1 and Lemma 5.2, $\mathcal{S}_3^1$, $\mathcal{S}_3^2$, and $\mathcal{S}_3^3$ have the same upper bound on the number of of 2-qubit neighbor gates. From this, we have that

$$d_0d_7 = d_3d_4, \quad d_1d_6 = d_2d_5$$

Thus, there exist three 2-qubit gates $U_1 = \mathsf{Diag}(d_0,\ d_1,\ d_2,\ d_3) \cdot \mathsf{C}(X)$ and additionally $U_2 = \mathsf{Diag}(1,\ 1,\ d_4/d_0,\ d_5/d_1)$ with $U_3 = \mathsf{C}(X)$, such that $D = \overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{BC}$.

($\Leftarrow$). If $D = \mathsf{Diag}(d_0, d_1, \ldots, d_7)$ can be implemented with three 2-qubit gates U_1, U_2, U_3, then we suppose the first 2-qubit gate operates on the BC qubits as $D = \overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{BC}$ or $D = \overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{U_3}_{BC}$. This is valid because the other two cases where the first 2-qubit gate operates on the AC qubits and AB qubits lead to the same sets $\mathcal{S}_i$ according to Lemma 5.1 and Lemma 5.2. For the first case, because D commutes with Z gates on qubit A, we conclude that U_2 commutes with Z gates on qubit A. From this, according to Lemma A.1, there exist two 1-qubit gates P_0 and P_1, such that U_2 can be written as $U_2 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. From this, we have that $U_1\,(I \otimes P_0)\,U_3 = \mathsf{Diag}(d_0,\ d_1,\ d_2,\ d_3)$, $U_1\,(I \otimes P_1)\,U_3 = \mathsf{Diag}(d_4,\ d_5,\ d_6,\ d_7)$, and

$$\mathsf{Eigenvalues}(U_3^\dagger\,(I \otimes P_0^\dagger P_1)\,U_3) = (\frac{d_4}{d_0},\ \frac{d_5}{d_1},\ \frac{d_6}{d_2},\ \frac{d_7}{d_3})$$

From the above, according to Lemma A.11, we conclude that there are two pairs of the same eigenvalues among four eigenvalues. As a result, we have the following three cases: (a) $d_0d_5 = d_1d_4$ and $d_2d_7 = d_3d_6$, (b) $d_0d_6 = d_2d_4$ and $d_1d_7 = d_3d_5$, and (c) $d_0d_7 = d_3d_4$ and $d_1d_6 = d_2d_5$. By calculation, we conclude that for case (a), we have $D \in \mathcal{S}_2^2 \subset \mathcal{S}_2$, for case (b), we have $D \in \mathcal{S}_2^3 \subset \mathcal{S}_2$, and for case (c), we have $D \in \mathcal{S}_3^1 \subset \mathcal{S}_3$.

For the second case, according to Section 2, by inserting the S gates, we have $\overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{U_3}_{BC} = (\overline{U_1}_{BC}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_2}_{AB}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_3}_{BC}) = \overline{U_1\,S}_{BC}\,\overline{U_2}_{AC}\,\overline{S\,U_3}_{BC} = D$. From this and the discussion for the first case, we conclude that either $D \in \mathcal{S}_2$ or $D \in \mathcal{S}_3$. □

Lemma D.4. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit neighbor gates.*

Proof. According to Theorem 6.2, we have that $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit neighbor gates. □

Lemma D.5. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_6$ if and only if D can be implemented with six 2-qubit neighbor gates.*

Proof. For $D = \mathrm{Diag}(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7)$, we define $a = \sqrt{(d_6/d_2)(d_0/d_4)(d_7/d_3)(d_1/d_5)}$, $b = \sqrt{(d_2/d_6)(d_4/d_0)(d_7/d_3)(d_1/d_5)}$. From this, we define $U_1 = \mathrm{Diag}(d_0, d_1, d_2, d_3)\,\mathrm{C}(X)$, $U_2 = \mathrm{Diag}(1, 1, \sqrt{b}, 1/\sqrt{b})$, $U_3 = S$, and additionally $U_4 = \mathrm{Diag}(1, 1, 1, a)$, $U_5 = S\mathrm{C}(X)$, and $U_6 = \mathrm{Diag}(1, 1, d_4/(d_0\sqrt{b}), (d_5\sqrt{b})/d_1)$. We can see that $\overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{BC}\,\overline{U_4}_{AC}\,\overline{U_5}_{BC}\,\overline{U_6}_{AC} = D$. □

Theorem 7.1. *Suppose D is a 3-qubit diagonal gate.*

(1) *We have $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit neighbor gate.*
(2) *We have $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit neighbor gates.*
(3) *We have $D \in \mathcal{S}_2 \cup \mathcal{S}_3$ if and only if D can be implemented with three 2-qubit neighbor gates.*
(4) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit neighbor gates.*
(5) *We have $D \in \mathcal{S}_6$ if and only if D can be implemented with six 2-qubit neighbor gates.*

Proof. We have property (1) according to Lemma D.1, property (2) according to Lemma D.2, property (3) according to Lemma D.3, property (4) according to Lemma D.4, and property (5) according to Lemma D.5. □

E PROOF OF THEOREM 7.2

Here, we prove Theorem 7.2 from Section 7. Theorem 7.2 shows the tight bounds on the number of needed unrestricted 2-qubit gates of 3-qubit diagonal gates.

Lemma E.1. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit unrestricted gate.*

Proof. Using one 2-qubit unrestricted gate to implement D is the same as using one 2-qubit neighbor gate, and we have discussed this in Lemma D.1 in Appendix D. □

Lemma E.2. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit unrestricted gates.*

Proof. Using two 2-qubit unrestricted gates to implement D is the same as using two 2-qubit neighbor gates, and we have discussed this in Lemma D.2 in Appendix D □

Lemma E.3. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_3 \cup \mathcal{S}_4$ if and only if D can be implemented with three 2-qubit unrestricted gates.*

Proof. ($\Rightarrow$). For $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7)$, suppose that $D \in \mathcal{S}_3$ or $D \in \mathcal{S}_4$. If $D \in \mathcal{S}_3$. Then, according to Lemma D.3, we can implement D by three 2-qubit neighbor gates. If $D \in \mathcal{S}_4$, then we have that

$$d_0 d_3 d_5 d_6 = d_1 d_2 d_4 d_7$$

Thus, there exist three 2-qubit gates $U_1 = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3)$, $U_2 = \mathrm{Diag}(1,\ 1,\ d_4/d_0,\ d_5/d_1)$, and $U_3 = \mathrm{Diag}(1,\ 1,\ 1,\ (d_6\, d_0)/(d_4\, d_2))$, such that $D = \overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{AB}$.

($\Leftarrow$). Suppose that $D = \mathrm{Diag}(d_0, d_1, \ldots, d_7) = |0\rangle\langle 0| \otimes D_0 + |1\rangle\langle 1| \otimes D_1$. We have two scenarios as D is implemented with 2-qubit neighbor gates or not. If D can be implemented with three 2-qubit neighbor gates, then according to Lemma D.3, we conclude that either $D \in \mathcal{S}_2 \subset \mathcal{S}_4$ or $D \in \mathcal{S}_3$.

If D can be implemented with three 2-qubit gates U_1, U_2, U_3, and they are not neighbor gates, then we suppose the first 2-qubit gate operates on the BC qubits as $D = \overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{AB}$ or $D = \overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{U_3}_{AC}$. This is valid because the other two cases where the first 2-qubit gate operates on the AC qubits and AB qubits lead to the same sets $\mathcal{S}_i$ according to Lemma 5.1 and Lemma 5.2.

According to Lemma A.14, we conclude that there exist four 1-qubit gates P_0, P_1, Q_0, Q_1, such that $U_2 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$ and $U_3 = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$. From this, we have $U_1\,(Q_0 \otimes P_0) = \mathrm{Diag}(d_0,\ d_1,\ d_2,\ d_3)$, $U_1\,(Q_1 \otimes P_1) = \mathrm{Diag}(d_4,\ d_5,\ d_6,\ d_7)$, and

$$Q_0^\dagger Q_1 \otimes P_0^\dagger P_1 = \mathrm{Diag}(\frac{d_4}{d_0},\ \frac{d_5}{d_1},\ \frac{d_6}{d_2},\ \frac{d_7}{d_3})$$

From the above, we know that both $P_0^\dagger P_1$ and $Q_0^\dagger Q_1$ commute with Z gates, and there exist four complex numbers a, b, p, q, such that $P_0^\dagger P_1 = \mathrm{Diag}(a,\ b)$, $Q_0^\dagger Q_1 = \mathrm{Diag}(p,\ q)$, and

$$\mathrm{Diag}(\frac{d_4}{d_0},\ \frac{d_5}{d_1},\ \frac{d_6}{d_2},\ \frac{d_7}{d_3}) = \mathrm{Diag}(ap,\ bp,\ aq,\ bq)$$

From the above, we have that

$$d_0 d_3 d_5 d_6 = d_1 d_2 d_4 d_7$$

By calculation, we conclude that $S \in \mathcal{S}_4$.

For the second case, by using S gates, from Section 2, we have $\overline{S}_{BC}\,\overline{U_1}_{BC}\,\overline{U_2}_{AB}\,\overline{U_3}_{AC}\,\overline{S}_{BC} = (\overline{S}_{BC}\,\overline{U_1}_{BC}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_2}_{AB}\,\overline{S}_{BC})\,(\overline{S}_{BC}\,\overline{U_3}_{AC}\,\overline{S}_{BC}) = \overline{S\,U_1\,S}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{AB} = \overline{S}_{BC}\,D\,\overline{S}_{BC} = D'$. According to Lemma 5.1 and Lemma 5.2 and the discussion for the first case, we conclude that both D' and D satisfy $\mathcal{S}_4$. □

Lemma E.4. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit unrestricted gates.*

Proof. According to Theorem 6.2, we have that $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit unrestricted gates. □

Lemma E.5. *Suppose D is a 3-qubit diagonal gate. $D \in \mathcal{S}_6$ if and only if D can be implemented with five 2-qubit unrestricted gates.*

Proof. For $D = \mathrm{Diag}(d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7)$, we define $a = \sqrt{(d_6/d_2)(d_0/d_4)(d_7/d_3)(d_1/d_5)}$, $b = \sqrt{(d_2/d_6)(d_4/d_0)(d_7/d_3)(d_1/d_5)}$. From this, we define $U_1 = \mathrm{Diag}(d_0, d_1, d_2, d_3)\,\mathrm{C}(X)$, $U_2 = \mathrm{Diag}(1, 1, \sqrt{b}, 1/\sqrt{b})$, $U_3 = \mathrm{Diag}(1, 1, 1, a)$, $U_4 = \mathrm{C}(X)$, $U_5 = \mathrm{Diag}(1, 1, d_4/(d_0\sqrt{b}), (d_5\sqrt{b})/d_1)$. We can see that $\overline{U_1}_{BC}\,\overline{U_2}_{AC}\,\overline{U_3}_{AB}\,\overline{U_4}_{BC}\,\overline{U_5}_{AC} = D$. □

Theorem 7.2. *Suppose D is a 3-qubit diagonal gate.*

(1) *We have $D \in \mathcal{S}_1$ if and only if D can be implemented with one 2-qubit unrestricted gate.*
(2) *We have $D \in \mathcal{S}_2$ if and only if D can be implemented with two 2-qubit unrestricted gates.*
(3) *We have $D \in \mathcal{S}_3 \cup \mathcal{S}_4$ if and only if D can be implemented with three 2-qubit unrestricted gates.*
(4) *We have $D \in \mathcal{S}_4 \cup \mathcal{S}_5$ if and only if D can be implemented with four 2-qubit unrestricted gates.*
(5) *We have $D \in \mathcal{S}_6$ if and only if D can be implemented with five 2-qubit unrestricted gates.*

Proof. We have property (1) according to Lemma E.1, property (2) according to Lemma E.2, property (3) according to Lemma E.3, property (4) according to Lemma E.4, and property (5) according to Lemma E.5. □

REFERENCES

Dominic W Berry, Craig Gidney, Mario Motta, Jarrod R McClean, and Ryan Babbush. 2019. Qubitization of arbitrary basis quantum chemistry leveraging sparsity and low rank factorization. *Quantum* 3 (2019), 208. https://doi.org/10.22331/q-2019-12-02-208

Dominic W Berry, Yuan Su, Casper Gyurik, Robbie King, Joao Basso, Alexander Del Toro Barba, Abhishek Rajput, Nathan Wiebe, Vedran Dunjko, and Ryan Babbush. 2024. Analyzing prospects for quantum advantage in topological data analysis. *PRX Quantum* 5, 1 (2024), 010319. https://doi.org/10.1103/PRXQuantum.5.010319

Anirban Bhattacharjee, Chandan Bandyopadhyay, Robert Wille, Rolf Drechsler, and Hafizur Rahaman. 2018. A novel approach for nearest neighbor realization of 2D quantum circuits. In *2018 IEEE computer society annual symposium on VLSI (ISVLSI)*. IEEE, 305–310. https://doi.org/10.1109/ISVLSI.2018.00063

Kuan-Yu Chang and Chun-Yi Lee. 2021. Mapping nearest neighbor compliant quantum circuits onto a 2-D hexagonal architecture. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 41, 10 (2021), 3373–3386. https://doi.org/10.1109/TCAD.2021.3127868

Jianxin Chen, Dawei Ding, Weiyuan Gong, Cupjin Huang, and Qi Ye. 2024. One gate scheme to rule them all: Introducing a complex yet reduced instruction set for quantum computing. In *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2*. 779–796. https://doi.org/10.1145/3620665.3640386

Kamalika Datta, Abhoy Kole, Indranil Sengupta, and Rolf Drechsler. 2022a. Mapping quantum circuits to 2-dimensional quantum architectures. In *Lecture Notes in Informatics (LNI)*. Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/inf2022_94

Kamalika Datta, Abhoy Kole, Indranil Sengupta, and Rolf Drechsler. 2022b. Nearest neighbor mapping of quantum circuits to two-dimensional hexagonal qubit architecture. In *2022 IEEE 52nd International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 35–42. https://doi.org/10.1109/ISMVL52857.2022.00013

Casey Duckering, Jonathan M Baker, Andrew Litteken, and Frederic T Chong. 2021. Orchestrated trios: compiling for efficient communication in quantum programs with 3-qubit gates. In *Proceedings of the 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. 375–385. https://doi.org/10.1145/3445814.3446718

Azim Farghadan and Naser Mohammadzadeh. 2017. Quantum circuit physical design flow for 2D nearest-neighbor architectures. *International Journal of Circuit Theory and Applications* 45, 7 (2017), 989–1000. https://doi.org/10.1002/cta.2335

Joshua J Goings, Alec White, Joonho Lee, Christofer S Tautermann, Matthias Degroote, Craig Gidney, Toru Shiozaki, Ryan Babbush, and Nicholas C Rubin. 2022. Reliably assessing the electronic structure of cytochrome P450 on today's classical computers and tomorrow's quantum computers. *Proceedings of the National Academy of Sciences* 119, 38 (2022), e2203533119. https://doi.org/10.1073/pnas.2203533119

Wakaki Hattori and Shigeru Yamashita. 2019. Mapping a quantum circuit to 2D nearest neighbor architecture by changing the gate order. *IEICE TRANSACTIONS on Information and Systems* 102, 11 (2019), 2127–2134. https://doi.org/10.1587/transinf.2018EDP7439

Roger A Horn and Charles R Johnson. 2012. *Matrix analysis*. Cambridge university press.

Joonho Lee, Dominic W Berry, Craig Gidney, William J Huggins, Jarrod R McClean, Nathan Wiebe, and Ryan Babbush. 2021. Even more efficient quantum computations of chemistry through tensor hypercontraction. *PRX Quantum* 2, 3 (2021), 030305. https://doi.org/10.1103/PRXQuantum.2.030305

Christopher C Paige and Musheng Wei. 1994. History and generality of the CS decomposition. *Linear Algebra Appl.* 208 (1994), 303–326. https://doi.org/10.1016/0024-3795(94)90446-4

Jens Palsberg and Nengkun Yu. 2024. Optimal Implementation of Quantum Gates with Two Controls. *Linear Algebra Appl.* (2024). https://doi.org/10.1016/j.laa.2024.03.039

Byeongyong Park and Doyeol Ahn. 2023. Reducing CNOT count in quantum Fourier transform for the linear nearest-neighbor architecture. *Scientific Reports* 13, 1 (2023), 8638. https://doi.org/10.1038/s41598-023-35625-3

Nicholas C Rubin, Dominic W Berry, Alina Kononov, Fionn D Malone, Tanuj Khattar, Alec White, Joonho Lee, Hartmut Neven, Ryan Babbush, and Andrew D Baczewski. 2024. Quantum computation of stopping power for inertial fusion target design. *Proceedings of the National Academy of Sciences* 121, 23 (2024), e2317772121. https://doi.org/10.1073/pnas.2317772121

Vivek V Shende, Stephen S Bullock, and Igor L Markov. 2005. Synthesis of quantum logic circuits. In *Proceedings of the 2005 Asia and South Pacific Design Automation Conference*. 272–275. https://doi.org/10.1145/1120725.1120847

Vivek V Shende and Igor L Markov. 2008. On the CNOT-cost of TOFFOLI gates. *arXiv preprint arXiv:0803.2316* (2008). https://doi.org/10.48550/arXiv.0803.2316

Yuan Su, Dominic W Berry, Nathan Wiebe, Nicholas Rubin, and Ryan Babbush. 2021. Fault-tolerant quantum simulations of chemistry in first quantization. *PRX Quantum* 2, 4 (2021), 040332. https://doi.org/10.1103/PRXQuantum.2.040332

Robert Wille, Aaron Lye, and Rolf Drechsler. 2014. Optimal SWAP gate insertion for nearest neighbor quantum circuits. In *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 489–494. https://doi.org/10.1109/ASPDAC.2014.6742939

Nengkun Yu, Runyao Duan, and Mingsheng Ying. 2013. Five Two-Qubit Gates Are Necessary for Implementing Toffoli Gate. *Physical Review A* (2013). https://doi.org/10.1103/PhysRevA.88.010304

Nengkun Yu and Mingsheng Ying. 2015. Optimal simulation of Deutsch gates and the Fredkin gate. *Physical Review A* (2015). https://doi.org/10.1103/PhysRevA.91.032302

Peng Zhao, Peng Xu, Dong Lan, Xinsheng Tan, Haifeng Yu, and Yang Yu. 2020. Switchable next-nearest-neighbor coupling for controlled two-qubit operations. *Physical review applied* 14, 6 (2020), 064016. https://doi.org/10.1103/PhysRevApplied.14.064016