Linear Algebra and its Applications 694 (2024) 206–261

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Optimal implementation of quantum gates with two controls

Jens Palsberg [a,*], Nengkun Yu [b]

[a] *Computer Science Department, Eng 6, Lab 486, University of California, Los Angeles, CA 90095, USA*
[b] *Department of Computer Science, Room 153, Stony Brook University, Stony Brook, NY 11794, USA*

ARTICLE INFO

Article history:
Received 21 March 2023
Received in revised form 30 March 2024
Accepted 30 March 2024
Available online 4 April 2024
Submitted by V. Mehrmann

MSC:
15

Keywords:
Quantum computing
Unitary matrices
Optimality

ABSTRACT

We give a detailed proof of a well-known theorem in quantum computing. The theorem characterizes the number of two-qubit gates that is necessary for implementing three-qubit quantum gates with two controls. For example, the theorem implies that five 2-qubit gates are necessary for implementing the Toffoli gate. No detailed proof was available earlier.

1. Introduction

Background. In the circuit model of quantum computing, algorithms frequently use controlled gates. A gate is a unitary matrix and a controlled gate is a particular form of

* Corresponding author.
E-mail addresses: palsberg@ucla.edu (J. Palsberg), nengkun.yu@cs.stonybrook.edu (N. Yu).

https://doi.org/10.1016/j.laa.2024.03.039

unitary matrix. We will focus on controlled gates that operate on three qubits by using two of the qubits as controls and the third qubit as the target. We will write such a gate as $\mathsf{CC}(U)$, where U is a 1-qubit unitary matrix. A well-known example is the Toffoli gate, $\mathsf{CC}(X)$, where X is one of the Pauli gates.

Most quantum computers have no hardware implementation of gates that operate on three qubits. Instead, most quantum computers must implement such gates using gates that operate on one or two qubits. In such implementations, an important goal is to use as few 2-qubit gates as possible to reduce both computation time and error. The reason is that 2-qubit gates are slower and less reliable than 1-qubit gates on current quantum computers.

How many 2-qubit gates do we need to implement $\mathsf{CC}(U)$? Turns out that for many such gates, five 2-qubit gates are necessary [3,4] and sufficient [2,1]. Indeed, the paper [4] shows that at most four 2-qubit gates are sufficient for implementing $\mathsf{CC}(U)$ if and only if either the eigenvalues of U are equal or $\det(U) = 1$. For example, for the Toffoli gate $\mathsf{CC}(X)$, the eigenvalues of X are different and $\det(X) = -1 \neq 1$. So, five 2-qubit gates are necessary for implementing the Toffoli gate. In contrast, if the eigenvalues of U are equal, then a single 2-qubit gate is sufficient for implementing $\mathsf{CC}(U)$. Also, if $\det(U) = 1$, then four 2-qubit gates are sufficient for implementing $\mathsf{CC}(U)$.

The published proof of the theorem is a total of four pages, divided across two papers [3,4] that introduce and combine many ideas in a high-level manner. The purpose of this note is to give a more detailed proof with the following three benefits. First, we provide detailed explanations of many steps that the original proof outlined at a high level. We provide those explanations in the appendix, as proofs of many lemmas. Second, we clarify where the proof about $\mathsf{CC}(U)$ uses the assumptions about U, which is in three specific lemmas. The original proof left this point largely implicit. Third, we use simpler reasoning, as we outline below.

Overview of the proof. The main result is Corollary 7.5, which characterizes the number of two-qubit gates that is necessary for implementing $\mathsf{CC}(U)$. The proof has structure that we illustrate in Fig. 1 and that we outline here, starting at the top of Fig. 1.

The proof of Corollary 7.5 uses the Spectral Theorem to diagonalize $\mathsf{CC}(U)$. This reduces the task of proving Corollary 7.5 to the task of proving Theorem 7.4, which characterizes the number of two-qubit gates that is necessary for implementing the matrix $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. Specifically, Theorem 7.4 says that this number of two-qubit gates is at most four if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$. The matrix $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ is a diagonal matrix, which simplifies the task of managing the large number of cases that arise in the proof. So, the proof of Theorem 7.4 uses a case analysis to show that a couple of cases capture everything. This reduces the task of proving Theorem 7.4 to the task of proving Lemma 5.1 and Lemma 6.4.

Lemma 5.1 and Lemma 6.4 are microcosms of the main result: each one characterizes whether a particular kind of product of four 2-qubit gates implements $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. Specifically, Lemma 5.1 talks about a product of four 2-qubit gates that operate, in order,

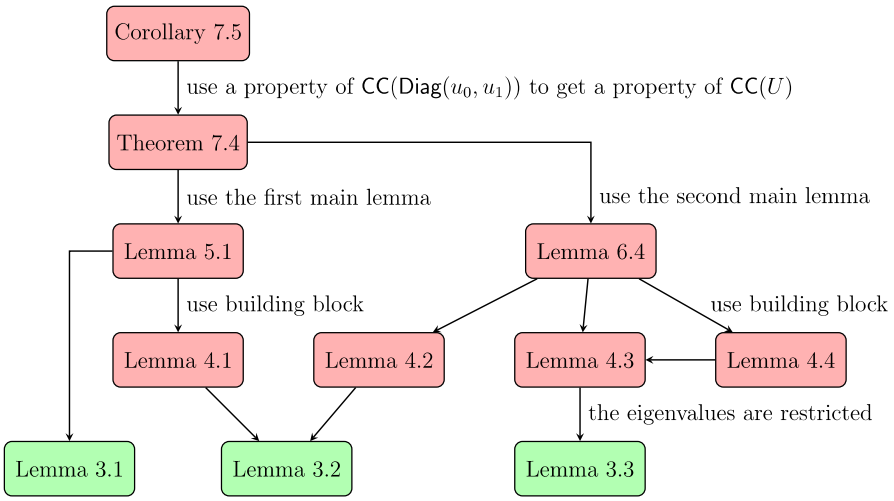

Fig. 1. Proof structure.

on qubits BC, AB, AC, BC, where A and B are the control qubits and C is the target qubit. Similarly, Lemma 6.4 talks about a product of four 2-qubit gates that operate, in order, on qubits BC, AC, BC, AC. In both cases, the lemma states that there exists a product that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

The proofs of the right-to-left directions of Lemma 5.1 and Lemma 6.4 are short and exhibit particular matrix products that are equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. The proofs of the left-to-right directions are longer and more complex. Each of those proofs begins by assuming that a particular product equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and proceeds to use the following three ideas. The first idea is to observe that in a product of four 2-qubit gates that equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, some of those gates must be controlled gates. The second idea is to use the observations about controlled gates to calculate the product in more detail. The third idea is to observe that the more detailed product leads to restrictions on u_0 and u_1. Those observations are made using four key building blocks, provided by Lemmas 4.1, 4.2, 4.3, 4.4, which, in turn, we prove using Lemma 3.2 and Lemma 3.3.

The bottom layer of the proof consists of Lemmas 3.1, 3.2, 3.3, which are the ones whose proofs use the assumptions about u_0 and u_1 in $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. Specifically, under those assumptions, Lemma 3.1 shows that any 3-qubit unitary that commutes with a particular diagonal unitary is actually a controlled unitary, while Lemma 3.2 and Lemma 3.3 show that the eigenvalues of certain unitaries must be of restricted forms.

Simple reasoning. We highlight three aspects in which our proof uses simpler reasoning than the original proof.

The first aspect is the case analysis that reduces the main proof task to just two cases. We give a single case analysis, while the original proof divided the case analysis across two papers [3,4]. In more detail, the paper by Yu and Ying [4] gave a case analysis that

divides into multiple cases, one of which is covered in the other paper [3] that, in turn, has its own case analysis.

The second aspect is the proof of Lemma 6.4. We introduce Lemma 6.3, which derives conclusions from the assumptions of Lemma 6.4 and some additional assumptions, and we introduce Lemma 4.2, which provides a simple way to combine the properties provided by Lemma 6.3.

The third aspect is the proof of Lemma 4.3. We introduce Lemma 3.3, which characterizes the eigenvalues of a family of unitaries and which has an elegant proof that uses the Spectral Theorem.

2. Notation and conventions

Numbers, vectors, and matrices. We will use r to range over real numbers. We will use a, b, c, d, p, q to range over complex numbers. We will use u to range over complex numbers that satisfy $|u| = 1$.

For a complex number c, we will use c^* to denote the conjugate of c.

We will use $|\alpha\rangle, |\beta\rangle, |\gamma\rangle, |\varphi\rangle, |\psi\rangle, |w\rangle, |x\rangle, |z\rangle$ to range over unit vectors of complex numbers. We will call a 2-dimensional unit vector a qubit.

We will use D, E to range over square matrices of complex numbers. We will use I to denote the identity matrix; the size of I will always be clear from the context. We will use X to denote the 2×2 matrix that swaps the components of a 2-dimensional vector and we will use S to denote the 4×4 matrix that swaps the components of a tensor product of two 2-dimensional vectors.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

For a matrix D, we will use $D^\dagger$ to denote the conjugate transpose of D. A unitary matrix U satisfies $U\,U^\dagger = U^\dagger\,U = I$. All of I, X, S are unitary matrices.

We will use *unitary* as a short-hand for *unitary matrix*. We will use the term 1-qubit unitary to refer to a 2×2 unitary matrix of complex numbers, we will use the term 2-qubit unitary to refer to a 4×4 unitary matrix of complex numbers, and we will use the term 3-qubit unitary to refer to a 8×8 unitary matrix of complex numbers. We will use P, Q to range over 1-qubit unitaries, we will use V, W to range over 2-qubit unitaries, and we will use U to sometimes range over 1-qubit unitaries, sometimes range over 2-qubit unitaries, and sometimes range over 3-qubit unitaries.

We will write matrix and vector addition as $+$, we will write tensor product as $\otimes$, and we will write matrix multiplication, including the application of a matrix to a vector as juxtaposition, such as UV and Uv, where U, V are matrices and v is a vector. We will

also write multiplication with a complex number as juxtaposition, such as aU, where a is complex number and U is a matrix.

We will use the convention that, in case of ambiguity, the operators take the following precedence:

Operation	Examples	Precedence
Multiplication with a complex number	aU	apply first
Multiplication of matrices and vectors	UV, $U\|\psi\rangle$	apply second
Tensor product	$U \otimes V$	apply third
Matrix and vector addition	$U + V$, $\|0\rangle + \|1\rangle$	apply last

Eigenvalues. For a unitary U, we use the notation $\mathsf{Eigenvalues}(U)$ to denote the multiset of eigenvalues of U. A multiset set is like a set but each element can occur multiple times. We use $[\ldots]$ to denote a multiset and we use $\sqcup$ to denote union of multisets.

Diagonal matrices. We write a diagonal 2×2 matrix as follows, where c_0, c_1 are complex numbers on the main diagonal:

$$\mathsf{Diag}(c_0, c_1) = c_0\ |0\rangle\langle 0|\ +\ c_1\ |1\rangle\langle 1|$$

Controlled matrices. We say that a square matrix D is controlled if it is of one of the forms

$$D = |0\rangle\langle 0| \otimes E_0\ +\ |1\rangle\langle 1| \otimes E_1$$
$$D = E_0 \otimes |0\rangle\langle 0|\ +\ E_1 \otimes |1\rangle\langle 1|$$

If E is a 2×2 matrix, we define the following controlled matrices:

$$\mathsf{C}(E) = |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes E$$
$$\mathsf{CC}(E) = |0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes \mathsf{C}(E)$$

Notice that $\mathsf{CC}(E) = |0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes E$. Notice also that $\mathsf{C}(\mathsf{Diag}(c_0, c_1)) = \mathsf{Diag}(1, 1, c_0, c_1)$ and $\mathsf{CC}(\mathsf{Diag}(c_0, c_1)) = \mathsf{Diag}(1, 1, 1, 1, 1, 1, c_0, c_1)$.

Qubits and subscripts. Throughout we will work with three qubit registers named A, B, and C, in that order. The state of those qubit registers is an 8-dimensional unit vector of complex numbers.

We will use A and B and C as subscripts of vectors to help remember the three qubits registers. Those subscripts carry no meaning; they are simply helpful reminders. For example, for 2-dimensional unit vectors $|\alpha\rangle, |\beta\rangle, |\gamma\rangle$, we may write $|\alpha\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C$ to suggest that the qubit register A contains $|\alpha\rangle$ and that the qubit register B contains $|\beta\rangle$ and that the qubit register C contains $|\gamma\rangle$. Similarly, for a 4-dimensional unit vector $|w\rangle$ and a 2-dimensional unit vector $|z\rangle$, we may write $|w\rangle_{AB} \otimes |z\rangle_C$ to suggest that the

qubit registers A and B contain $|w\rangle$ and that the qubit register C contains $|z\rangle$. We may also write $|z\rangle_A \otimes |w\rangle_{BC}$ to suggest that the qubit register A contains $|z\rangle$ and that the qubit registers B and C contain $|w\rangle$.

We will use A and B and C as subscripts of unitaries to help remember to which qubit registers they apply. Those subscripts carry no meaning; they are simply helpful reminders. For example, for 1-qubit unitaries P, Q, U, we may write $P_A \otimes Q_B \otimes U_C$ to suggest that the unitary P operates on the A qubit register and that the unitary Q operates on the B qubit register and that the unitary U operates on the C qubit register. Similarly, for 2-qubit unitary V and a 1-qubit unitary P, we may write $V_{AB} \otimes P_C$ to suggest that the unitary V operates on the A and B qubit registers and that the unitary P operates on the C qubit register. We may also write $P_A \otimes V_{BC}$ to suggest that the unitary P operates on the A qubit register and that the unitary V operates on the B and C qubit registers.

Now let us consider what happens if we have two subscripts. For example, suppose we have a 2-qubit unitary V_1 and we want to remind the reader that we are applying V_1 to the A and B qubit registers. For this case, we will use the straightforward notation $V_{1\,AB}$.

Applying a 2-qubit unitary to 3 qubits. We may want to apply a 2-qubit unitary U to two of the three qubit registers, while leaving the third unchanged. In such cases, we may use a short-hand notation that uses a bar over U together with one of the subscripts AB, BC, and AC:

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

The definitions of $\overline{U}_{AB}$ and $\overline{U}_{BC}$ each applies the identity matrix to one of the qubits. So does the definition of $\overline{U}_{AC}$, which we can see as follows. The definition of $\overline{U}_{AC}$ first swaps the B and C qubit registers, which brings the contents of A and C next two each other. Now we can apply U, after which we swap B and C again. Thus, we left B unchanged.

The key point about the notations $\overline{U}_{AB}$ and $\overline{U}_{BC}$ and $\overline{U}_{AC}$ is that the subscripts are meaningful. Specifically, when those subscripts appear in the context of a 2-qubit unitary with a bar over it, those subscripts help define a 3-qubit unitary. Thus, if U is a 2-qubit unitary, then U_{AB} operates on 2 qubits, while $\overline{U}_{AB}$ operates on 3 qubits.

Sets of 3-qubit unitaries. We introduce names for some particular sets of 3-qubit unitaries:

$$\mathcal{G}_{AB} = \{\ \overline{U}_{AB} \mid U \text{ is a 2-qubit unitary } \}$$

$$\begin{aligned}
\mathcal{G}_{BC} &= \{\ \overline{U}_{BC} \mid U \text{ is a 2-qubit unitary }\} \\
\mathcal{G}_{AC} &= \{\ \overline{U}_{AC} \mid U \text{ is a 2-qubit unitary }\} \\
\mathcal{G}_2 &= \mathcal{G}_{AB} \cup \mathcal{G}_{AC} \cup \mathcal{G}_{BC} \\
\mathcal{G}_1 &= \{\ U \otimes I \otimes I \mid U \text{ is a 1-qubit unitary }\} \\
&\quad \cup \{\ I \otimes U \otimes I \mid U \text{ is a 1-qubit unitary }\} \\
&\quad \cup \{\ I \otimes I \otimes U \mid U \text{ is a 1-qubit unitary }\}
\end{aligned}$$

Notice that $\mathcal{G}_1 \subseteq \mathcal{G}_2$.

Traces and partial traces. We use $tr(D)$ to denote the trace of a square matrix D, that is, the sum of the elements on the main diagonal of D.

We will use the technique of tracing out one or more qubits from a unitary. For example, we can consider the case of tracing out the first qubit from a 2-qubit unitary U, the result of which we denote by $tr_A(U)$. The function tr_A is the unique linear function from 2-qubit unitaries to 1-qubit unitaries that, for 1-qubit unitaries P, Q, satisfies

$$tr_A(P \otimes Q) = tr(P)\ Q$$

This generalizes to tracing out multiple qubits from larger unitaries.

The main result, formalized. The main result (Corollary 7.5) says, informally:

> For a 1-qubit unitary U, there exists a product of at most four 2-qubit unitaries and any number of 1-qubit unitaries that is equal to $\mathsf{CC}(U)$ if and only if either the eigenvalues of U are equal or $\det(U) = 1$.

We can formalize the theorem using the notation above. Specifically, the formalized theorem says that:

> For a 1-qubit unitary U, there exists a product of at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ that is equal to $\mathsf{CC}(U)$ if and only if either the eigenvalues of U are equal or $\det(U) = 1$.

For example, for the Toffoli gate, $\mathsf{CC}(X)$, the eigenvalues of X are different and $\det(X) = -1 \neq 1$. So, five 2-qubit gates are necessary for implementing the Toffoli gate.

3. The conditions on the eigenvalues

Theorem 7.4 says that something about $\mathsf{CC}(U)$ is possible if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$. In this section, we will explain the reason for those conditions. Specifically,

we will prove three lemmas that directly use those conditions. Lemmas in later sections use those three lemmas and thus they inherit those conditions.

The first lemma says that if a unitary U commutes with a diagonal unitary $(I_{AB} \otimes \mathsf{Diag}(u_0, u_1))$, then either $u_0 = u_1$ or U is a controlled unitary. We will use this lemma as a key step in the proof of the first main lemma (Section 5).

Lemma 3.1. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. A 3-qubit unitary U commutes with $\mathsf{Diag}(u_0, u_1) \otimes I \otimes I$ if and only if either $u_0 = u_1$ or U is of the form:*

$$U = |0\rangle\langle 0| \otimes V_{00} + |1\rangle\langle 1| \otimes V_{11}$$

where V_{00}, V_{11} are 2-qubit unitaries.

Proof. Let

$$U = \begin{pmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{pmatrix}$$

$$W = \mathsf{Diag}(u_0, u_1) \otimes I \otimes I \;=\; \begin{pmatrix} u_0\ (I \otimes I) & 0 \\ 0 & u_1\ (I \otimes I) \end{pmatrix}$$

Now we calculate both $U\ W$ and $W\ U$, which by assumption are equal:

$$\begin{pmatrix} u_0\ V_{00} & u_1\ V_{01} \\ u_0\ V_{10} & u_1\ V_{11} \end{pmatrix} \;=\; U\ W \;=\; W\ U \;=\; \begin{pmatrix} u_0\ V_{00} & u_0\ V_{01} \\ u_1\ V_{10} & u_1\ V_{11} \end{pmatrix}$$

$$\iff u_1\ V_{01} \;=\; u_0\ V_{01} \;\wedge\; u_0\ V_{10} \;=\; u_1\ V_{10}$$

$$\iff u_0 = u_1 \;\vee\; V_{01} = V_{10} = \mathbf{0}$$

In the second step, in the left-to-right direction, we use $u_0 \neq 0$ and $u_1 \neq 0$. □

Next, we will show that the multisets of eigenvalues of some matrices must be of certain forms, as expressed in Lemma 3.2 and Lemma 3.3. Specifically, the eigenvalues of the tensor product of two 1-qubit unitaries must be of the form $[1, 1, u_0, u_1]$, and for a 1-qubit unitary P, the eigenvalues of $(I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))$ must be of the form $[c, c, d, d]$, in both cases if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$. In Section 4, we will use those lemmas to make conclusions about expressions that equal $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

Lemma 3.2. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 1-qubit unitaries P, Q such that $\mathsf{Eigenvalues}(P \otimes Q) = [1, 1, u_0, u_1]$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose $\mathsf{Eigenvalues}(P \otimes Q) = [1, 1, u_0, u_1]$. From the Spectral Theorem A.3 we have that each of P and Q has two eigenvalues.

Let $\mathsf{Eigenvalues}(P) = [a, b]$ and let $\mathsf{Eigenvalues}(Q) = [p, q]$. From Lemma A.5 we have

$$\mathsf{Eigenvalues}(P \otimes Q) = [ap, aq, bp, bq]$$

From the above two equations for $\mathsf{Eigenvalues}(P \otimes Q)$, we have $[ap, aq, bp, bq] = [1, 1, u_0, u_1]$. For reasons of symmetry, we can focus on two cases that are substantially different.

In the first case, we assume

$$ap = 1 \qquad aq = 1 \qquad bp = u_0 \qquad bq = u_1$$

We have that P is a unitary so each of its eigenvalues is nonzero. In particular, $a \neq 0$. From the first and second equation, we get $p = \frac{1}{a}$ and $q = \frac{1}{a}$, from which we get $p = q$. Now we can combine this with the third and fourth equation and get $u_0 = bp = bq = u_1$.

In the second case, we assume

$$ap = u_0 \qquad aq = 1 \qquad bp = 1 \qquad bq = u_1$$

We calculate

$$u_0 u_1 = (ap)\ (bq) \ = \ (aq)\ (bp) \ = \ 1 \times 1 \ = \ 1$$

In the right-to-left direction, we have two cases. In the first case, suppose $u_0 = u_1$. We pick $P = \mathsf{Diag}(1, u_1)$ and $Q = I$. We see that $\mathsf{Eigenvalues}(P) = [1, u_1]$ and $\mathsf{Eigenvalues}(Q) = [1, 1]$. From Lemma A.5 we have $\mathsf{Eigenvalues}(P \otimes Q) = [1, 1, u_1, u_1] = [1, 1, u_0, u_1]$.

In the second case, suppose $u_0 u_1 = 1$. We pick $P = \mathsf{Diag}(1, u_0)$ and $Q = \mathsf{Diag}(1, u_1)$, and we see that $\mathsf{Eigenvalues}(P) = [1, u_0]$ and $\mathsf{Eigenvalues}(Q) = [1, u_1]$. From Lemma A.5 we have $\mathsf{Eigenvalues}(P \otimes Q) = [1, u_1, u_0, u_0 u_1] = [1, u_1, u_0, 1] = [1, 1, u_0, u_1]$. □

Lemma 3.3. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist a 1-qubit unitary P and complex numbers c, d such that $\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)))\ = [c, c, d, d]$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose $\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)))\ = [c, c, d, d]$. We calculate:

$$\mathsf{C}(\mathsf{Diag}(u_0, u_1)) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \mathsf{Diag}(u_0, u_1)$$

$$(I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)) = |0\rangle\langle 0| \otimes P + |1\rangle\langle 1| \otimes P\ \mathsf{Diag}(u_0, u_1)$$

$$\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))) = \mathsf{Eigenvalues}(P) \sqcup \mathsf{Eigenvalues}(P\ \mathsf{Diag}(u_0, u_1))$$

We use the first equation to prove the second equation, and we use the second equation and Lemma A.6 to prove the third equation.

Suppose $\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))) = [c, c, d, d]$, that is, using the third equation above,

$$\mathsf{Eigenvalues}(P) \sqcup \mathsf{Eigenvalues}(P\ \mathsf{Diag}(u_0, u_1)) = [c, c, d, d]$$

From the Spectral Theorem A.3 we have that P has two eigenvalues and that $P\ \mathsf{Diag}(u_0, u_1)$ has two eigenvalues. We have two cases.

In the first case, suppose $\mathsf{Eigenvalues}(P) = [c, c]$ and $\mathsf{Eigenvalues}(P\ \mathsf{Diag}(u_0, u_1)) = [d, d]$.

From the Spectral Theorem A.3 applied to the unitary P, we get that there exists a 1-qubit unitary Q_0 such that

$$P = Q_0\ \mathsf{Diag}(c, c)\ Q_0^\dagger \quad = \quad c\ Q_0\ \mathsf{Diag}(1, 1)\ Q_0^\dagger \quad = \quad c\ Q_0\ Q_0^\dagger \quad = \quad c\ I$$

Similarly, from the Spectral Theorem A.3 applied to the unitary $P\ \mathsf{Diag}(u_0, u_1)$, we get that there exists a 1-qubit unitary Q_1 such that

$$P\ \mathsf{Diag}(u_0, u_1) = Q_1\ \mathsf{Diag}(d, d)\ Q_1^\dagger \quad = \quad d\ Q_1\ \mathsf{Diag}(1, 1)\ Q_1^\dagger \quad = \quad d\ Q_1\ Q_1^\dagger \quad = \quad d\ I$$

From $\mathsf{Diag}(d, d) = d\ I = P\ \mathsf{Diag}(u_0, u_1) = (c\ I)\ \mathsf{Diag}(u_0, u_1) = c\ \mathsf{Diag}(u_0, u_1) = \mathsf{Diag}(cu_0, cu_1)$, we conclude $cu_0 = d = cu_1$, which combined with $c \neq 0$ gives $u_0 = u_1$.

In the second case, suppose $\mathsf{Eigenvalues}(P) = [c, d]$ and $\mathsf{Eigenvalues}(P\ \mathsf{Diag}(u_0, u_1)) = [c, d]$. We use those equations in the following calculation:

$$cd \quad = \quad \det(P\ \mathsf{Diag}(u_0, u_1)) \quad = \quad \det(P)\ \det(\mathsf{Diag}(u_0, u_1)) \quad = \quad (cd)\ (u_0 u_1)$$

In the second step, we use Lemma A.1.

We have that $c \neq 0$ and $d \neq 0$, so $cd \neq 0$, which together with the above equation implies that $u_0 u_1 = 1$.

In the right-to-left direction, we have two cases. In the first case, suppose $u_0 = u_1$. We pick $P = I$ and $c = 1$ and $d = u_0$. We see that $(I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)) = \mathsf{C}(\mathsf{Diag}(u_0, u_1))$ so $\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))) = \mathsf{Eigenvalues}(\mathsf{C}(\mathsf{Diag}(u_0, u_1))) = [1, 1, u_0, u_1] = [c, c, d, d]$.

In the second case, suppose $u_0 u_1 = 1$. We pick $P = \mathsf{Diag}(1, u_0)$ and $c = 1$ and $d = u_0$. We see that

$$\begin{aligned}(I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)) &= \mathsf{Diag}(1, u_0, 1, u_0)\ \mathsf{Diag}(1, 1, u_0, u_1) \\ &= \mathsf{Diag}(1, u_0, u_0, u_0 u_1) \\ &= \mathsf{Diag}(1, u_0, u_0, 1)\end{aligned}$$

so $\mathsf{Eigenvalues}((I \otimes P)\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))) = [1, u_0, u_0, 1] = [c, c, d, d]$. □

4. Four key building blocks

In Section 5 and Section 6, we will prove two main lemmas (Lemma 5.1 and Lemma 6.4) using the following strategy.

In each case we assume that an expression is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, then show that this implies that some other expression is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, and finally derive properties of u_0 and u_1. The final step of deriving properties of u_0 and u_1 is done using four key building blocks, which are the lemmas we show in this section.

The first two lemmas are about expressions that equal $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and that involve tensor products, which will restrict u_0 and u_1.

Lemma 4.1. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries U, V and 1-qubit unitaries P_0, P_1, Q_0, Q_1 such that*

$$|0\rangle\langle 0| \otimes U_{BC}\ (P_0 \otimes Q_0)\ V_{BC}\ +\ |1\rangle\langle 1| \otimes U_{BC}\ (P_1 \otimes Q_1)\ V_{BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$$

if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

Proof. In the left-to-right direction, suppose

$$|0\rangle\langle 0| \otimes U_{BC}\ (P_0 \otimes Q_0)\ V_{BC}\ +\ |1\rangle\langle 1| \otimes U_{BC}\ (P_1 \otimes Q_1)\ V_{BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$$

From this we have

$$\begin{aligned} U\ (P_0 \otimes Q_0)\ V &= \mathsf{Diag}(1,1,1,1) \\ U\ (P_1 \otimes Q_1)\ V &= \mathsf{Diag}(1,1,u_0,u_1) \end{aligned}$$

We use those two equations in the following calculation:

$$\begin{aligned} \mathsf{Diag}(1,1,u_0,u_1) &= \mathsf{Diag}(1,1,u_0,u_1)\ \mathsf{Diag}(1,1,1,1)^\dagger \\ &= (U\ (P_1 \otimes Q_1)\ V)\ (V^\dagger\ (P_0^\dagger \otimes Q_0^\dagger)\ U^\dagger) \\ &= U\ ((P_1\ P_0^\dagger) \otimes (Q_1\ Q_0^\dagger))\ U^\dagger \end{aligned}$$

From Lemma A.4 we have that the conjugation with U preserves the eigenvalues, so we have that $[1,1,u_0,u_1] = \mathsf{Eigenvalues}(\mathsf{Diag}(1,1,u_0,u_1)) = \mathsf{Eigenvalues}((P_1\ P_0^\dagger) \otimes (Q_1\ Q_0^\dagger))$. From this and Lemma 3.2 we have either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the right-to-left direction, we have two cases. In the first case, suppose $u_0 = u_1$. We pick $U = V = I_{BC}$ and $P_0 = Q_0 = Q_1 = I$ and $P_1 = \mathsf{Diag}(1, u_1)$. We calculate:

$$\begin{aligned} &|0\rangle\langle 0| \otimes U_{BC}\ (P_0 \otimes Q_0)\ V_{BC}\ +\ |1\rangle\langle 1| \otimes U_{BC}\ (P_1 \otimes Q_1)\ V_{BC} \\ &= |0\rangle\langle 0| \otimes I_{BC}\ (I \otimes I)\ I_{BC}\ +\ |1\rangle\langle 1| \otimes I_{BC}\ (\mathsf{Diag}(1,u_1) \otimes I)\ I_{BC} \end{aligned}$$

$$= \mathsf{Diag}(1,1,1,1,0,0,0,0) \ + \ \mathsf{Diag}(0,0,0,0,1,1,u_1,u_1)$$
$$= \mathsf{CC}(\mathsf{Diag}(u_0,u_1))$$

In the third step, we use $u_0 = u_1$.

In the second case, suppose $u_0 u_1 = 1$. We pick

$$U = V \ = \ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and $P_0 = Q_0 = I$ and $P_1 = \mathsf{Diag}(1, u_0)$ and $Q_1 = \mathsf{Diag}(1, u_1)$. We calculate:

$$\begin{aligned}
& |0\rangle\langle 0| \otimes U_{BC} \ (P_0 \otimes Q_0) \ V_{BC} \ + \ |1\rangle\langle 1| \otimes U_{BC} \ (P_1 \otimes Q_1) \ V_{BC} \\
&= |0\rangle\langle 0| \otimes U_{BC} \ (I \otimes I) \ U_{BC} \ + \ |1\rangle\langle 1| \otimes U_{BC} \ (\mathsf{Diag}(1,u_0) \otimes \mathsf{Diag}(1,u_1)) \ U_{BC} \\
&= |0\rangle\langle 0| \otimes (I \otimes I) \ + \ |1\rangle\langle 1| \otimes U_{BC} \ \mathsf{Diag}(1,u_1,u_0,u_0u_1) \ U_{BC} \\
&= |0\rangle\langle 0| \otimes (I \otimes I) \ + \ |1\rangle\langle 1| \otimes U_{BC} \ \mathsf{Diag}(1,u_1,u_0,1) \ U_{BC} \\
&= |0\rangle\langle 0| \otimes (I \otimes I) \ + \ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,1,u_0,u_1) \\
&= \mathsf{Diag}(1,1,1,1,0,0,0,0) \ + \ \mathsf{Diag}(0,0,0,0,1,1,u_0,u_1) \\
&= \mathsf{CC}(\mathsf{Diag}(u_0,u_1))
\end{aligned}$$

In the third step, we use $u_0 u_1 = 1$. □

Lemma 4.2. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. Suppose Q is a 1-qubit unitary and let $|\beta\rangle = Q \ |0\rangle$ and let $|\beta^\perp\rangle = Q \ |1\rangle$. There exist 1-qubit unitaries P_0, P_1 such that*

$$I \otimes I \otimes |\beta\rangle\langle\beta| \ + \ P_0 \otimes P_1 \otimes |\beta^\perp\rangle\langle\beta^\perp| = \mathsf{CC}(\mathsf{Diag}(u_0,u_1)) \tag{1}$$

if and only if $u_0 = 1 = u_1$.

Proof. In the left-to-right direction, suppose Equation (1) holds and let $|\beta\rangle = a|0\rangle + b|1\rangle$. We have three cases.

In the first case, suppose $a \neq 0$ and $b \neq 0$. We multiply each side of Equation (1) with $|1\rangle \otimes |1\rangle \otimes |\beta\rangle$ from the right and, because $|\beta\rangle$ and $|\beta^\perp\rangle$ are orthogonal, we get:

$$|1\rangle \otimes |1\rangle \otimes |\beta\rangle = |1\rangle \otimes |1\rangle \otimes \mathsf{Diag}(u_0,u_1) \ |\beta\rangle$$

which implies $|\beta\rangle = \mathsf{Diag}(u_0,u_1) \ |\beta\rangle$. From this we get $a = u_0 a$ and $b = u_1 b$, which together with $a \neq 0$ and $b \neq 0$ implies $u_0 = 1 = u_1$.

In the second case, suppose $a = 0$. This implies that $|b| = 1$ so $bb^* = 1$, hence $|\beta\rangle\langle\beta| = |1\rangle\langle 1|$. From this and Lemma A.8, we get $|\beta^\perp\rangle\langle\beta^\perp| = I - |\beta\rangle\langle\beta| = I - |1\rangle\langle 1| = |0\rangle\langle 0|$. We have

$$\begin{aligned} & I \otimes I \otimes |1\rangle\langle 1| \ + \ P_0 \otimes P_1 \otimes |0\rangle\langle 0| \\ = \ & I \otimes I \otimes |\beta\rangle\langle\beta| \ + \ P_0 \otimes P_1 \otimes |\beta^\perp\rangle\langle\beta^\perp| \\ = \ & \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \\ = \ & \mathsf{Diag}(1,1,1,u_0) \otimes |0\rangle\langle 0| \ + \ \mathsf{Diag}(1,1,1,u_1) \otimes |1\rangle\langle 1| \end{aligned}$$

From the above we derive

$$\begin{aligned} I \otimes I &= \mathsf{Diag}(1,1,1,u_1) \\ P_0 \otimes P_1 &= \mathsf{Diag}(1,1,1,u_0) \end{aligned}$$

From the first of those equations we have $u_1 = 1$. From the second of those equations we have

$$\mathsf{Eigenvalues}(P_0 \otimes P_1) = \mathsf{Eigenvalues}(\mathsf{Diag}(1,1,1,u_0)) \quad = \quad [1,1,1,u_0]$$

which together with Lemma 3.2 implies $u_0 = 1$. We conclude $u_0 = 1 = u_1$.

In the third case, suppose $b = 0$. This implies that $|a| = 1$ so $aa^* = 1$, hence $|\beta\rangle\langle\beta| = |0\rangle\langle 0|$. From this and Lemma A.8, we get $|\beta^\perp\rangle\langle\beta^\perp| = I - |\beta\rangle\langle\beta| = I - |0\rangle\langle 0| = |1\rangle\langle 1|$. We multiply each side of Equation (1) with $I \otimes I \otimes X$ from both the left and the right, and we get:

$$I \otimes I \otimes |1\rangle\langle 1| \ + \ P_0 \otimes P_1 \otimes |0\rangle\langle 0| = \mathsf{CC}(\mathsf{Diag}(u_1, u_0))$$

From this and the second case, we conclude $u_0 = 1 = u_1$.

In the right-to-left direction, suppose $u_0 = 1 = u_1$. We pick $P_0 = P_1 = I$. We calculate

$$\begin{aligned} I \otimes I \otimes |\beta\rangle\langle\beta| \ + \ P_0 \otimes P_1 \otimes |\beta^\perp\rangle\langle\beta^\perp| &= I \otimes I \otimes |\beta\rangle\langle\beta| \ + \ I \otimes I \otimes |\beta^\perp\rangle\langle\beta^\perp| \\ &= I \otimes I \otimes (|\beta\rangle\langle\beta| \ + \ |\beta^\perp\rangle\langle\beta^\perp|) \\ &= I \otimes I \otimes I \\ &= \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \end{aligned}$$

In the third step, we use Lemma A.8. In the fourth step, we use $u_0 = 1 = u_1$. □

Next, we will prove Lemma 4.3 and Lemma 4.4, which both are special cases of the second main lemma (Lemma 6.4). The idea is that, in a particular kind of matrix product that equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, if the first or last of the unitaries is controlled, then u_0 and u_1 are restricted.

Lemma 4.3. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries V_1, V_2, V_3, V_4 and 1-qubit unitaries P_0, P_1, where $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, such that $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and recall that $\mathsf{CC}(\mathsf{Diag}(u_0, u_1)) = |0\rangle\langle 0| \otimes I_{BC} + |1\rangle\langle 1| \otimes \mathsf{C}(\mathsf{Diag}(u_0, u_1))$. From this and $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$ and Lemma A.27, we have that V_3 is of the following form, where Q_0, Q_1 are 1-qubit unitaries:

$$V_3 = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$$

From the above equations for V_1 and V_3, we have

$$\begin{aligned}
\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC} &= (|0\rangle\langle 0| \otimes I_B \otimes P_0 + |1\rangle\langle 1| \otimes I_B \otimes P_1) \\
&\quad (|0\rangle\langle 0| \otimes V_{2BC} + |1\rangle\langle 1| \otimes V_{2BC}) \\
&\quad (|0\rangle\langle 0| \otimes I_B \otimes Q_0 + |1\rangle\langle 1| \otimes I_B \otimes Q_1) \\
&= |0\rangle\langle 0| \otimes ((I_B \otimes P_0)\ V_{2BC}\ (I_B \otimes Q_0)) + \\
&\quad |1\rangle\langle 1| \otimes ((I_B \otimes P_1)\ V_{2BC}\ (I_B \otimes Q_1))
\end{aligned}$$

From the assumption $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, we can derive the equation $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))\ \overline{V}_{4BC}^{\dagger}$. We have

$$\begin{aligned}
\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC} &= \mathsf{CC}(\mathsf{Diag}(u_0, u_1))\ \overline{V}_{4BC}^{\dagger} \\
&= (|0\rangle\langle 0| \otimes I_{BC} + |1\rangle\langle 1| \otimes \mathsf{C}(\mathsf{Diag}(u_0, u_1))) \\
&\quad (|0\rangle\langle 0| \otimes V_{4BC}^{\dagger} + |1\rangle\langle 1| \otimes V_{4BC}^{\dagger}) \\
&= |0\rangle\langle 0| \otimes V_{4BC}^{\dagger} + |1\rangle\langle 1| \otimes (\mathsf{C}(\mathsf{Diag}(u_0, u_1))\ V_{4BC}^{\dagger})
\end{aligned}$$

In the second step, we use the definition of $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

From the above two equations for $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}$, we have

$$\begin{aligned}
(I \otimes P_0)\ V_2\ (I \otimes Q_0) &= V_4^{\dagger} \\
(I \otimes P_1)\ V_2\ (I \otimes Q_1) &= \mathsf{C}(\mathsf{Diag}(u_0, u_1))\ V_4^{\dagger}
\end{aligned}$$

Now we can combine the above two equations and get:

$$(I \otimes P_1)\ V_2\ (I \otimes Q_1) = \mathsf{C}(\mathsf{Diag}(u_0, u_1))\ (I \otimes P_0)\ V_2\ (I \otimes Q_0)$$

We can rearrange the above as follows:

$$(I \otimes P_1)\ V_2\ (I \otimes Q_1)\ (I \otimes Q_0^{\dagger})\ V_2^{\dagger}\ (I \otimes P_0^{\dagger}) = \mathsf{C}(\mathsf{Diag}(u_0, u_1))$$

For the above equation, we can multiply with $(I \otimes (P_0\ P_1^\dagger))$ on both sides and get:

$$\begin{aligned}&(I \otimes (P_0\ P_1^\dagger))\ (I \otimes P_1)\ V_2\ (I \otimes Q_1)\ (I \otimes Q_0^\dagger)\ V_2^\dagger\ (I \otimes P_0^\dagger)\\ =\ &(I \otimes (P_0\ P_1^\dagger))\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))\end{aligned}$$

Now we can simplify and rearrange the left-hand side and get:

$$((I \otimes P_0)\ V_2)\ (I \otimes (Q_1\ Q_0^\dagger))\ ((I \otimes P_0)\ V_2)^\dagger = (I \otimes (P_0\ P_1^\dagger))\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))$$

We calculate

$$\begin{aligned}&\mathsf{Eigenvalues}(I \otimes (Q_1\ Q_0^\dagger))\\ =\ &\mathsf{Eigenvalues}(((I \otimes P_0)\ V_2)\ (I \otimes (Q_1\ Q_0^\dagger))\ ((I \otimes P_0)\ V_2)^\dagger)\\ =\ &\mathsf{Eigenvalues}((I \otimes (P_0\ P_1^\dagger))\ \mathsf{C}(\mathsf{Diag}(u_0, u_1)))\end{aligned}$$

In the first step, we use Lemma A.4, and in the second step, we use the above equation.

From the Spectral Theorem A.3 we have that $(Q_1\ Q_0^\dagger)$ has two eigenvalues. If $\mathsf{Eigenvalues}((Q_1\ Q_0^\dagger)) = [c, d]$ for some complex numbers c, d, then

$$\mathsf{Eigenvalues}(I \otimes (Q_1\ Q_0^\dagger)) = [c, c, d, d]$$

which together with the above equation implies

$$\mathsf{Eigenvalues}((I \otimes (P_0\ P_1^\dagger))\ \mathsf{C}(\mathsf{Diag}(u_0, u_1))) = [c, c, d, d]$$

which together with Lemma 3.3 gives that either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the right-to-left direction, we have two cases. In the first case, suppose $u_0 = u_1$. Define the 2-qubit unitary $U = \mathsf{C}(\mathsf{Diag}(1, u))$. Now we calculate:

$$\begin{aligned}&\overline{I}_{AC}\ \overline{S}_{BC}\ \overline{U}_{AC}\ \overline{S}_{BC}\\ =\ &\overline{U}_{AB}\ =\ U \otimes I_C\ =\ \mathsf{Diag}(1,1,1,1,1,1,u,u)\ =\ \mathsf{CC}(\mathsf{Diag}(u,u))\end{aligned}$$

In the second case, suppose $u_0 u_1 = 1$. Let $u_0 = e^{-i\theta}$, which together with $u_0 u_1 = 1$ means that $u_1 = e^{i\theta}$. We define the 1-qubit unitary P and the 2-qubit unitaries U and V:

$$\begin{aligned}P &= \mathsf{Diag}(e^{-i\theta/2}, e^{i\theta/2})\\ U &= |0\rangle\langle 0| \otimes X\ +\ |1\rangle\langle 1| \otimes I\\ V &= \mathsf{C}(P)\end{aligned}$$

Notice

$$
\begin{aligned}
P &= e^{-i\theta/2}|0\rangle\langle 0| \ + \ e^{i\theta/2}|1\rangle\langle 1| \\
P^2 &= \mathsf{Diag}(e^{-i\theta}, e^{i\theta}) \ \ = \ \ \mathsf{Diag}(u_0, u_1) \\
\overline{V}_{AC} &= \overline{S}_{BC} \ (V_{AB} \otimes I_C) \ \overline{S}_{BC} \\
&= \overline{S}_{BC} \ (\mathsf{C}(P) \otimes I_C) \ \overline{S}_{BC} \\
&= \overline{S}_{BC} \ ((|0\rangle\langle 0| \otimes I_B \ + \ |1\rangle\langle 1| \otimes P_B) \otimes I_C) \ \overline{S}_{BC} \\
&= \overline{S}_{BC} \ (|0\rangle\langle 0| \otimes I_B \otimes I_C) \ \overline{S}_{BC} \ + \ \overline{S}_{BC} \ (|1\rangle\langle 1| \otimes P_B \otimes I_C) \ \overline{S}_{BC} \\
&= |0\rangle\langle 0| \otimes I_{BC} \ + \ |1\rangle\langle 1| \otimes I_B \otimes P_C
\end{aligned}
$$

In the last step, we use Lemma A.11.

The unitary V is of the form that in the statement of the lemma is required of V_1. Our goal is to show that the product $\overline{V}_{AC} \ \overline{U}_{BC} \ \overline{V}_{AC} \ \overline{U}^\dagger_{BC}$ of four 2-qubit unitaries equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. We calculate; first two expressions that we will need later:

$$
\begin{aligned}
P \ X \ P \ X &= (e^{-i\theta/2}|0\rangle\langle 0| \ + \ e^{i\theta/2}|1\rangle\langle 1|) \ (|0\rangle\langle 1| \ + \ |1\rangle\langle 0|) \\
&\quad\ (e^{-i\theta/2}|0\rangle\langle 0| \ + \ e^{i\theta/2}|1\rangle\langle 1|) \ (|0\rangle\langle 1| \ + \ |1\rangle\langle 0|) \\
&= |0\rangle\langle 0| \ + \ |1\rangle\langle 1| \\
&= I \\
(I \otimes P) \ U \ (I \otimes P) \ U^\dagger &= (|0\rangle\langle 0| \otimes P \ + \ |1\rangle\langle 1| \otimes P) \\
&\quad\ (|0\rangle\langle 0| \otimes X \ + \ |1\rangle\langle 1| \otimes I) \\
&\quad\ (|0\rangle\langle 0| \otimes P \ + \ |1\rangle\langle 1| \otimes P) \\
&\quad\ (|0\rangle\langle 0| \otimes X \ + \ |1\rangle\langle 1| \otimes I) \\
&= |0\rangle\langle 0| \otimes (P \ X \ P \ X) \ + \ |1\rangle\langle 1| \otimes P^2 \\
&= |0\rangle\langle 0| \otimes I \ + \ |1\rangle\langle 1| \otimes P^2 \\
&= \mathsf{C}(P^2) \\
\overline{V}_{AC} \ \overline{U}_{BC} \ \overline{V}_{AC} \ \overline{U}^\dagger_{BC} &= (|0\rangle\langle 0| \otimes I_{BC} \ + \ |1\rangle\langle 1| \otimes I_B \otimes P_C) \\
&\quad\ (|0\rangle\langle 0| \otimes U_{BC} \ + \ |1\rangle\langle 1| \otimes U_{BC}) \\
&\quad\ (|0\rangle\langle 0| \otimes I_{BC} \ + \ |1\rangle\langle 1| \otimes I_B \otimes P_C) \\
&\quad\ (|0\rangle\langle 0| \otimes U^\dagger_{BC} \ + \ |1\rangle\langle 1| \otimes U^\dagger_{BC}) \\
&= |0\rangle\langle 0| \otimes I_{BC} \ + \ |1\rangle\langle 1| \otimes ((I_B \otimes P_C) \ U_{BC} \ (I_B \otimes P_C) \ U^\dagger_{BC}) \\
&= |0\rangle\langle 0| \otimes I_{BC} \ + \ |1\rangle\langle 1| \otimes \mathsf{C}(P^2) \\
&= \mathsf{CC}(P^2) \\
&= \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \quad \square
\end{aligned}
$$

The following lemma follows easily from Lemma 4.3 by exchanging the roles of A and B and considering the conjugate transpose of the product.

Lemma 4.4. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries V_1, V_2, V_3, V_4 and 1-qubit unitaries P_0, P_1, where $V_4 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, such that $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

5. The first main lemma

We will prove that if a particular matrix product equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, then u_0 and u_1 are restricted. The proof uses Lemmas 3.1, 4.1 and also Lemma A.24.

Lemma 5.1 *(The first main lemma). Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries U_1, U_2, U_3, U_4 such that $\overline{U}_{1BC}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose $\overline{U}_{1BC}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. From this we see that

$$\overline{U}_{2AC}\ \overline{U}_{3AB} = \overline{U}_{1BC}^{\dagger}\ \mathsf{CC}(\mathsf{Diag}(u_0, u_1))\ \overline{U}_{4BC}^{\dagger}$$

We have that each of $\overline{U}_{1BC}^{\dagger}$, $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, $\overline{U}_{4BC}^{\dagger}$ commutes with $\mathsf{Diag}(u_0, u_1) \otimes I_{BC}$. In the case of $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, this is because both $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and $\mathsf{Diag}(u_0, u_1) \otimes I_{BC}$ are diagonal matrices. So, $\overline{U}_{2AC}\ \overline{U}_{3AB}$ commutes with $\mathsf{Diag}(u_0, u_1) \otimes I_{BC}$. From this and Lemma 3.1, we have either $u_0 = u_1$ or $\overline{U}_{2AC}\ \overline{U}_{3AB}$ is of the form:

$$\overline{U}_{2AC}\ \overline{U}_{3AB} = |0\rangle\langle 0| \otimes V_{0BC}\ +\ |1\rangle\langle 1| \otimes V_{1BC}$$

where V_0, V_1 are 2-qubit unitaries. In the case where $u_0 = u_1$, we have completed the proof, so let us consider the second case of the disjunction. From the above equation and Lemma A.24 we get that $\overline{U}_{2AC}\ \overline{U}_{3AB}$ is of the form:

$$\overline{U}_{2AC}\ \overline{U}_{3AB} = |0\rangle\langle 0| \otimes P_0 \otimes Q_0\ +\ |1\rangle\langle 1| \otimes P_1 \otimes Q_1$$

where P_0, Q_0, P_1, Q_1 are 1-qubit unitaries. We calculate

$$\begin{aligned}
\mathsf{CC}(\mathsf{Diag}(u_0, u_1)) &= \overline{U}_{1BC}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC} \\
&= (I_A \otimes U_{1BC})\ (\overline{U}_{2AC}\ \overline{U}_{3AB})\ (I_A \otimes U_{4BC}) \\
&= (|0\rangle\langle 0| \otimes U_{1BC}\ +\ |1\rangle\langle 1| \otimes U_{1BC}) \\
&\quad\ (|0\rangle\langle 0| \otimes P_0 \otimes Q_0\ +\ |1\rangle\langle 1| \otimes P_1 \otimes Q_1) \\
&\quad\ (|0\rangle\langle 0| \otimes U_{4BC}\ +\ |1\rangle\langle 1| \otimes U_{4BC})
\end{aligned}$$

$$= |0\rangle\langle 0| \otimes U_{1BC}\ (P_0 \otimes Q_0)\ U_{4BC}\ +\ |1\rangle\langle 1| \otimes U_{1BC}\ (P_1 \otimes Q_1)\ U_{4BC}$$

which together with Lemma 4.1 gives that either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the right-to-left direction, we have two cases. In the first case, suppose $u_0 = u_1$. Define the 2-qubit unitary $U = \mathsf{C}(\mathsf{Diag}(1, u))$. Now we calculate:

$$\begin{aligned}\overline{I}_{BC}\ \overline{I}_{AC}\ \overline{U}_{AB}\ \overline{I}_{BC} &= \overline{U}_{AB}\ =\ U \otimes I_C \\ &= \mathsf{Diag}(1,1,1,1,1,1,u,u)\ =\ \mathsf{CC}(\mathsf{Diag}(u,u))\end{aligned}$$

By the way, notice that $\mathsf{CC}(\mathsf{Diag}(u,u)) = \overline{U}_{AB} \in \mathcal{G}_2$.

In the second case, suppose $u_0 u_1 = 1$. Define

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned} V = \mathsf{Diag}(1,1,1,u_1) &= |0\rangle\langle 0| \otimes \mathsf{Diag}(1,1)\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_1) \\ W = \mathsf{Diag}(1,1,1,u_0) &= |0\rangle\langle 0| \otimes \mathsf{Diag}(1,1)\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_0)\end{aligned}$$

We calculate:

$$\begin{aligned}\overline{U}_{BC}\ \overline{V}_{AC}\ \overline{V}_{AB}\ \overline{U}_{BC} &= \overline{U}_{BC} \\ &\quad (|0\rangle\langle 0| \otimes I \otimes \mathsf{Diag}(1,1)\ +\ |1\rangle\langle 1| \otimes I \otimes \mathsf{Diag}(1,u_1)) \\ &\quad (|0\rangle\langle 0| \otimes \mathsf{Diag}(1,1) \otimes I\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_0) \otimes I) \\ &\quad \overline{U}_{BC} \\ &= \overline{U}_{BC} \\ &\quad (|0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_0) \otimes \mathsf{Diag}(1,u_1)) \\ &\quad \overline{U}_{BC} \\ &= \overline{U}_{BC} \\ &\quad (|0\rangle\langle 0| \otimes \mathsf{Diag}(1,1,1,1)\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_1,u_0,u_0u_1)) \\ &\quad \overline{U}_{BC} \\ &= \overline{U}_{BC} \\ &\quad (|0\rangle\langle 0| \otimes \mathsf{Diag}(1,1,1,1)\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,u_1,u_0,1)) \\ &\quad \overline{U}_{BC} \\ &= |0\rangle\langle 0| \otimes \mathsf{Diag}(1,1,1,1)\ +\ |1\rangle\langle 1| \otimes \mathsf{Diag}(1,1,u_0,u_1) \\ &= \mathsf{CC}(\mathsf{Diag}(u_0,u_1))\quad \square\end{aligned}$$

6. The second main lemma

We will prove that if a particular matrix product equals $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, then u_0 and u_1 are restricted. The proof uses lemmas from Appendix A and Section 4.

Lemma 6.1 enables us to do a case analysis of a unitary, which we will do in the proofs of both Lemma 6.2 and Lemma 6.4. Lemmas 6.2–6.4 form a sequence in which Lemma 6.2 plays major role in the proof of Lemma 6.3, which, in turn, plays a major role in the proof of Lemma 6.4.

Lemma 6.1 *(Case analysis of a unitary). For a 2-qubit unitary V, either*
$\exists|x\rangle : V\ (|x\rangle \otimes |0\rangle)$ *is entangled, or*
$\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$, *or*
$\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$.

Proof. We have that either $\exists|x\rangle : V\ (|x\rangle \otimes |0\rangle)$ is entangled, or $\forall|x\rangle : V\ (|x\rangle \otimes |0\rangle)$ is not entangled. We can subdivide the second disjunct as follows. First recall that if an expression is not entangled, then it is a tensor product. Now from $\forall|x\rangle : V\ (|x\rangle \otimes |0\rangle)$ is not entangled and Lemma A.23, we have that $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$, or $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$. □

Lemma 6.2. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. For 2-qubit unitaries U_1, W_2, V_3, U_4, if*

$$\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$$
$$V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$
$$\text{for any } |x\rangle_A\text{: } \overline{U}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) = \overline{U}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)$$

then either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_3, W_4 and a 1-qubit unitary P_3 such that

$$\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC}$$
$$W_3 = I \otimes |0\rangle\langle 0|\ +\ P_3 \otimes |1\rangle\langle 1|$$

Proof. From Lemma 6.1 we have that we can do a case analysis of $V_3^{\dagger}$ that has three cases.

In the first case, suppose there exists a qubit $|x\rangle$ such that $V_3^{\dagger}\ (|x\rangle \otimes |0\rangle)$ is entangled. From

$$\text{for any } |x\rangle_A\text{: } \overline{U}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) = \overline{U}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)$$

we can derive

$$\begin{aligned}
&\text{for any } |x\rangle_A\text{:}\\
&\overline{S}_{AB}\ \overline{U}_{1AC}\ \overline{S}_{AB}\ \overline{S}_{AB}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)\\
=\ &\overline{S}_{AB}\ \overline{U}_{4BC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{3AC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)
\end{aligned}$$

From the above equation and Lemma A.10 and Lemma A.12, we derive

$$\text{for any } |x\rangle_A\text{: } \overline{U}_{1BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) = \overline{U}_{4AC}^{\dagger}\ \overline{V}_{3BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C)$$

From the above equation and that $V_3^{\dagger}\ (|x\rangle \otimes |0\rangle)$ is entangled and Lemma A.19, we have that $U_4^{\dagger}$ is of the following form, where Q_0, Q_1 are 1-qubit unitaries:

$$U_4^{\dagger} = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$$

This implies

$$U_4 = |0\rangle\langle 0| \otimes Q_0^{\dagger} + |1\rangle\langle 1| \otimes Q_1^{\dagger}$$

From this and the assumption $\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and Lemma 4.4, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the second case, suppose $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V_3^{\dagger}\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$. From Lemma A.31 we have that there exist 2-qubit unitaries W_1, W_3, W_4 and a 1-qubit unitary P_3 such that

$$\begin{aligned}
\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} &= \overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC}\\
W_3 &= I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1|
\end{aligned}$$

In the third case, suppose $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V_3^{\dagger}\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$. From Lemma A.25 we have that we can find a 1-qubit unitary P_0 such that, for any qubit $|x\rangle$:

$$V_3^{\dagger}\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes (P_0\ |x\rangle)$$

Now we have, for any $|x\rangle_A$:

$$\begin{aligned}
\overline{U}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) &= \overline{U}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)\\
&= \overline{U}_{4BC}^{\dagger}\ (|\psi\rangle_A \otimes |0\rangle_B \otimes (P_0\ |x\rangle_C))\\
&= |\psi\rangle_A \otimes (U_{4BC}^{\dagger}\ (|0\rangle_B \otimes (P_0\ |x\rangle_C)))
\end{aligned}$$

From the above equation and Lemma A.22, we have that

$$\forall\ |x\rangle : \exists|w\rangle : U_4^{\dagger}\ (|0\rangle \otimes (P_0\ |x\rangle)) = |0\rangle \otimes |w\rangle$$

We can pick orthogonal qubits $|x_0\rangle$ and $|x_0^{\perp}\rangle$ and calculate:

$$U_4^\dagger\ (|0\rangle \otimes (P_0\ |x_0\rangle)) = |0\rangle \otimes |w_0\rangle$$
$$U_4^\dagger\ (|0\rangle \otimes (P_0\ |x_0^\perp\rangle)) = |0\rangle \otimes |w_1\rangle$$

From Lemma A.17 we have that $U_4^\dagger$ is of the following form, where Q_0, Q_1 are 1-qubit unitaries:

$$U_4^\dagger = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$$

This implies

$$U_4 = |0\rangle\langle 0| \otimes Q_0^\dagger + |1\rangle\langle 1| \otimes Q_1^\dagger$$

From this and the assumption $\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and Lemma 4.4, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$. □

Lemma 6.3. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. For 2-qubit unitaries V_1, V_2, V_3, V_4, if*

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \tag{2}$$
$$\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V_2\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle \tag{3}$$
$$V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \tag{4}$$

then either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_2, W_3, W_4 and 1-qubit unitaries P_1, P_2, P_3, P_4, Q such that

$$\overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$$
$$W_1 = I \otimes |\beta\rangle\langle 0| \ +\ P_1 \otimes |\beta^\perp\rangle\langle 1|$$
$$W_2 = I \otimes |0\rangle\langle 0| \ +\ P_2 \otimes |1\rangle\langle 1|$$
$$W_3 = I \otimes |0\rangle\langle 0| \ +\ P_3 \otimes |1\rangle\langle 1|$$
$$W_4 = I \otimes |0\rangle\langle \beta| \ +\ P_4 \otimes |1\rangle\langle \beta^\perp|$$

where $|\beta\rangle = Q\ |0\rangle$ and $|\beta^\perp\rangle = Q\ |1\rangle$.

Proof. From Equation (3) and Lemma A.30, we have that there exist 2-qubit unitaries U_1, W_2, U_4 and a 1-qubit unitary P_2 such that

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} \tag{5}$$
$$W_2 = I \otimes |0\rangle\langle 0| \ +\ P_2 \otimes |1\rangle\langle 1| \tag{6}$$

From Equations (2) and (5) we have

$$\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \tag{7}$$

From Equation (6) we have $W_2\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$. From this and Equation (7) and Lemma A.29, we have, for any $|x\rangle_A$:

$$U_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) = \overline{U}_{4BC}^{\dagger}\ V_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) \tag{8}$$

From Equations (4), (7), (8), and Lemma 6.2, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_3, W_4 and a 1-qubit unitary P_3 such that

$$\overline{U}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{U}_{4BC} = \overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} \tag{9}$$

$$W_3 = I \otimes |0\rangle\langle 0|\ +\ P_3 \otimes |1\rangle\langle 1| \tag{10}$$

In the cases where either $u_0 = u_1$ or $u_0 u_1 = 1$, we have completed the proof, so let us consider the third case of the disjunction. From Equations (7), (9) we have

$$\overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \tag{11}$$

From Equations (10), (11) and Lemma A.28, we have, for any $|z\rangle_B$:

$$\overline{W}_{1AC}\ \overline{W}_{2BC}\ (|0\rangle_A \otimes |z\rangle_B \otimes |0\rangle_C) = \overline{W}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |z\rangle_B \otimes |0\rangle_C) \tag{12}$$

From Equations (12) and (6) we have, for any $|z\rangle_B$:

$$\overline{W}_{1AC}\ (|0\rangle_A \otimes |z\rangle_B \otimes |0\rangle_C) = \overline{W}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |z\rangle_B \otimes |0\rangle_C)$$

From the above equation and Lemma A.22, we have that:

$$\forall |z\rangle :\ \exists |w\rangle :\ W_4^{\dagger}\ (|z\rangle \otimes |0\rangle) = |z\rangle \otimes |w\rangle$$

From that observation and Lemma A.26, we have that we can pick $|\beta\rangle$ such that, for all $|z\rangle$:

$$W_4^{\dagger}\ (|z\rangle \otimes |0\rangle) = |z\rangle \otimes |\beta\rangle \tag{13}$$

From that observation, we get, for all $|z\rangle$:

$$W_4\ (|z\rangle \otimes |\beta\rangle) = |z\rangle \otimes |0\rangle$$

Let $|\beta^{\perp}\rangle$ be a unit vector that is orthogonal to $|\beta\rangle$. Define a 1-qubit unitary Q:

$$Q = |\beta\rangle\langle 0|\ +\ |\beta^{\perp}\rangle\langle 1|$$

Notice that the columns of Q are orthogonal unit vectors, hence Q is a unitary matrix.

When we combine the above two equations, we get, for all $|z\rangle$:

$$W_4\ (I \otimes Q)\ (|z\rangle \otimes |0\rangle) = W_4\ (|z\rangle \otimes |\beta\rangle) \quad = \quad |z\rangle \otimes |0\rangle$$

From Lemma A.18 we have that $W_4\ (I \otimes Q)$ is of the form:

$$W_4\ (I \otimes Q) = I \otimes |0\rangle\langle 0| \ + \ P_4 \otimes |1\rangle\langle 1|$$

where P_4 is a 1-qubit unitary. The above equation implies the following:

$$W_4 \ = I \otimes |0\rangle\langle \beta| \ + \ P_4 \otimes |1\rangle\langle \beta^{\perp}|$$

From Equation (6) we have $W_2\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$. From this and Equation (11) and Lemma A.29, we have, for any $|x\rangle_A$:

$$\overline{W}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) = \overline{W}_{4BC}^{\dagger}\ \overline{W}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) \tag{14}$$

We have, for any $|x\rangle_A$:

$$\begin{array}{lll}
 & (I_{AB} \otimes Q_C^{\dagger})\ \overline{W}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) & \\
= & (I_{AB} \otimes Q_C^{\dagger})\ \overline{W}_{4BC}^{\dagger}\ \overline{W}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) & \text{(Equation (14))} \\
= & (I_{AB} \otimes Q_C^{\dagger})\ \overline{W}_{4BC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) & \text{(Equation (10))} \\
= & (I_{AB} \otimes Q_C^{\dagger})\ (|x\rangle_A \otimes |0\rangle_B \otimes |\beta\rangle_C) & \text{(Equation (13))} \\
= & |x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C & (Q\ |0\rangle = |\beta\rangle)
\end{array}$$

From the above equation we have, for any $|x\rangle_A$:

$$((I \otimes Q^{\dagger})\ W_1)\ (|x\rangle \otimes |0\rangle) = |x\rangle \otimes |0\rangle$$

From the above equation and Lemma A.18, we have that $(I \otimes Q^{\dagger})\ W_1$ is of the following form, where P_1 is a 1-qubit unitary:

$$(I \otimes Q^{\dagger})\ W_1 = I \otimes |0\rangle\langle 0| \ + \ P_1 \otimes |1\rangle\langle 1|$$

which implies

$$W_1 = I \otimes |\beta\rangle\langle 0| \ + \ P_1 \otimes |\beta^{\perp}\rangle\langle 1| \quad \square$$

Lemma 6.4 *(The second main lemma). Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries U_1, U_2, U_3, U_4, such that $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. From Lemma A.32, we have that there exist unitaries V_1, V_2, V_3, V_4 such that

$$\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} \tag{15}$$

$$V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \tag{16}$$

From the assumption that $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and Equation (15), we have

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \tag{17}$$

From Equations (16) and (17) and Lemma A.28, we have, for all $|x\rangle$:

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) = \overline{V}_{4BC}^{\ \dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \tag{18}$$

From Lemma 6.1 we have that we can do a case analysis of V_2 that has three cases.

In the first case, suppose there exists a qubit $|x\rangle$ such that $V_2\ (|x\rangle \otimes |0\rangle)$ is entangled. From this and Equation (18) and Lemma A.19, we have that V_1 is of the following form, where P_0, P_1 are 1-qubit unitaries: $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. From this and Equation (17) and Lemma 4.3, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the second case, suppose $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V_2\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$. From this and Equation (18) and Lemma A.33, we have that V_1 is of the following form, where P_0, P_1 are 1-qubit unitaries: $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. From this and Equation (17) and Lemma 4.3, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the third case, suppose $\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : V_2\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$. From this, Equations (17), (16), and Lemma 6.3, we conclude that either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_2, W_3, W_4 and 1-qubit unitaries P_1, P_2, P_3, P_4, Q such that

$$\begin{aligned}
\overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} &= \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \\
W_1 &= I \otimes |\beta\rangle\langle 0| \ +\ P_1 \otimes |\beta^{\perp}\rangle\langle 1| \\
W_2 &= I \otimes |0\rangle\langle 0| \ +\ P_2 \otimes |1\rangle\langle 1| \\
W_3 &= I \otimes |0\rangle\langle 0| \ +\ P_3 \otimes |1\rangle\langle 1| \\
W_4 &= I \otimes |0\rangle\langle \beta| \ +\ P_4 \otimes |1\rangle\langle \beta^{\perp}|
\end{aligned}$$

where $|\beta\rangle = Q\ |0\rangle$ and $|\beta^{\perp}\rangle = Q\ |1\rangle$. In the cases where either $u_0 = u_1$ or $u_0 u_1 = 1$, we have completed the proof, so let us consider the third case of the disjunction. From the above equations we calculate:

$$\begin{aligned}
\mathsf{CC}(\mathsf{Diag}(u_0, u_1)) &= \overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} \\
&= (I \otimes I \otimes |\beta\rangle\langle 0| \ +\ P_1 \otimes I \otimes |\beta^{\perp}\rangle\langle 1|)
\end{aligned}$$

$$
\begin{aligned}
&(I \otimes I \otimes |0\rangle\langle 0| \ + \ I \otimes P_2 \otimes |1\rangle\langle 1|) \\
&(I \otimes I \otimes |0\rangle\langle 0| \ + \ P_3 \otimes I \otimes |1\rangle\langle 1|) \\
&(I \otimes I \otimes |0\rangle\langle \beta| \ + \ I \otimes P_4 \otimes |1\rangle\langle \beta^{\perp}|) \\
= I \otimes I \otimes |\beta\rangle\langle \beta| \ + \ &(P_1 \ P_3) \otimes (P_2 \ P_4) \otimes |\beta^{\perp}\rangle\langle \beta^{\perp}|
\end{aligned}
$$

which together with Lemma 4.2 implies $u_0 = u_1$.

In the right-to-left direction, we use the right-to-left direction of Lemma 4.3. □

7. The main theorem

In this section, the only prior lemmas that we will use are Lemma 5.1 (the first main lemma) and Lemma 6.4 (the second main lemma), as well as Lemma A.12 and Lemma A.13.

We say that a product $(\overline{U}_{1 i_1 j_1} \ \overline{U}_{2 i_2 j_2} \ \ldots \ \overline{U}_{m i_m j_m})$ of m 2-qubit unitaries is *canonical* if each $i_k, j_k \in \{A, B, C\}$ and $i_k \neq j_k$ and, for every k, where $1 \leq k < m$, $\{i_k, j_k\} \neq \{i_{k+1}, j_{k+1}\}$.

For two complex numbers u_0, u_1 such that $|u_0| = |u_1| = 1$, we define the set of pairs $R(u_0, u_1) = \{ \ (u_0, u_1), \ (1, u_0^* u_1) \ \}$.

Lemma 7.1 *(Change a diagonal element to one). Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. For a 2-qubit unitary W and a 3-qubit unitary U, if $\mathsf{CC}(\mathsf{Diag}(u_0, u_1)) = \overline{W}_{AB} \ U$, then there exists a 2-qubit unitary V such that $\mathsf{CC}(\mathsf{Diag}(1, u_0^* u_1)) = \overline{V}_{AB} \ U$.*

Proof. Define $V = \mathsf{C}(\mathsf{Diag}(1, u_0^*)) \ W$. We calculate:

$$
\begin{aligned}
\overline{V}_{AB} \ U &= ((\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \ W_{AB}) \otimes I_C) \ U \\
&= ((\mathsf{C}(\mathsf{Diag}(1, u_0^*))) \otimes I_C) \ (W_{AB} \otimes I_C) \ U \\
&= (\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C) \ \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \\
&= \mathsf{Diag}(1,1,1,1,1,1,u_0^*,u_0^*) \ \mathsf{Diag}(1,1,1,1,1,1,u_0,u_1) \\
&= \mathsf{Diag}(1,1,1,1,1,1,1,u_0^* u_1) \\
&= \mathsf{CC}(\mathsf{Diag}(1, u_0^* u_1)) \quad \square
\end{aligned}
$$

Lemma 7.2 *(Reduction). Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. If there exists a product of at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, then either*

there exist 2-qubit unitaries U_1, U_2, U_3, U_4 and complex numbers u_2, u_3 such that $(u_2, u_3) \in R(u_0, u_1)$ and $\overline{U}_{1BC} \ \overline{U}_{2AC} \ \overline{U}_{3AB} \ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_2, u_3))$,

or

there exist 2-qubit unitaries U_1, U_2, U_3, U_4 *and complex numbers* u_2, u_3 *such that* $(u_2, u_3) \in R(u_0, u_1)$ *and* $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_2, u_3))$.

Proof. The proof has four steps. Let E be the product that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

In the first step, we transform E to a product E_2 of at most four elements of $\mathcal{G}_2$ such that $E_2 = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

We have five cases.

In the first case, suppose every factor in E is an element of $\mathcal{G}_1$. In this case, we can condense all the unitaries on qubit A into a single unitary, we can condense all the unitaries on qubit B into a single unitary, and we can condense all the unitaries on qubit C into a single unitary. The result is a product of three unitaries that all are elements of $\mathcal{G}_1$. We have that $\mathcal{G}_1 \subseteq \mathcal{G}_2$, so we have a product of three elements of $\mathcal{G}_2$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

In the second case, suppose every factor in E that is an element of $\mathcal{G}_2 \setminus \mathcal{G}_1$ is actually an element of $\mathcal{G}_{AB} \setminus \mathcal{G}_1$. Now we can absorb each unitary on qubit A into one of the elements of $\mathcal{G}_{AB} \setminus \mathcal{G}_1$. Similarly, we can absorb each unitary on qubit B into one of the elements of $\mathcal{G}_{AB} \setminus \mathcal{G}_1$. After that, we can condense all the unitaries in $\mathcal{G}_{AB} \setminus \mathcal{G}_1$ into a single unitary. Finally, we can condense all the unitaries on qubit C into a single unitary. We have that $\mathcal{G}_C \subseteq \mathcal{G}_2$, so we have a product of two elements of $\mathcal{G}_2$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

In the third case, suppose every factor in E that is an element of $\mathcal{G}_2 \setminus \mathcal{G}_1$ is actually an element of $\mathcal{G}_{AC} \setminus \mathcal{G}_1$. This case is similar to the second case; we omit the details.

In the fourth case, suppose every factor in E that is an element of $\mathcal{G}_2 \setminus \mathcal{G}_1$ is actually an element of $\mathcal{G}_{BC} \setminus \mathcal{G}_1$. This case is similar to the second case; we omit the details.

In the fifth case, suppose E has factors from at least two of the three sets $\mathcal{G}_{AB}, \mathcal{G}_{AC}, \mathcal{G}_{BC}$. Now we can absorb each unitary on qubit A into one of the elements of $\mathcal{G}_{AB} \cup \mathcal{G}_{AC}$, we can absorb each unitary on qubit B into one of the elements of $\mathcal{G}_{AB} \cup \mathcal{G}_{BC}$, and we can absorb each unitary on qubit C into one of the elements of $\mathcal{G}_{AC} \cup \mathcal{G}_{BC}$. We started with a product that contains at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$, so now we have a product of at most four elements of $\mathcal{G}_2$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

This completes the first step of the proof.

In the second step, we transform E_2 to a canonical product E_4 of four elements of $\mathcal{G}_2$ such that $E_4 = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$.

First we observe that if two adjacent unitaries in E_2 operate on the same couple of qubits, we can combine them via multiplication. We can repeat this operation until we

have a canonical product. After that we can pad as needed by multiplying with identity matrices.

In the third step, we transform E_4 to a canonical product E_6 of four elements of $\mathcal{G}_2$ such that the last factor in the product is an element of $\mathcal{G}_{BC}$ and there exist complex numbers u_6, u_7 such that $(u_6, u_7) \in R(u_0, u_1)$ and $E_6 = \mathsf{CC}(\mathsf{Diag}(u_6, u_7))$.

We have three cases.

In the first case, the last unitary in E_4 operates on qubits AB. Thus, we can write $E_4 = \overline{U}_{1i_1j_1}\ \overline{U}_{2i_2j_2}\ \overline{U}_{3i_3j_3}\ \overline{U}_{4AB}$, where each $i_k, j_k \in \{A, B, C\}$ and $i_k \neq j_k$.

Our first goal is to change one of the diagonal elements from u_0 to 1, which we do by multiplying with $\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C$ from the right:

$$\begin{aligned} E_4\ (\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C) &= \mathsf{CC}(\mathsf{Diag}(u_0, u_1))\ (\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C) \\ &= \mathsf{Diag}(1,1,1,1,1,1,u_0,u_1)\ \mathsf{Diag}(1,1,1,1,1,1,u_0^*,u_0^*) \\ &= \mathsf{Diag}(1,1,1,1,1,1,1,u_0^*u_1) \\ &= \mathsf{CC}(\mathsf{Diag}(1,u_0^*u_1)) \end{aligned}$$

Notice that $\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C$ is an element of $\mathcal{G}_{AB}$. So, the product $E_4\ (\mathsf{C}(\mathsf{Diag}(1, u_0^*)) \otimes I_C)$ ends with two elements of $\mathcal{G}_{AB}$ which we can combine into a single unitary $\overline{V}_{AB}$. After this combination, we have a canonical product E_5 of four elements of $\mathcal{G}_2$ where the last factor is an element of $\mathcal{G}_{AB}$ and $E_5 = \mathsf{CC}(\mathsf{Diag}(1, u_0^*u_1))$. Notice that $(1, u_0^*u_1) \in R(u_0, u_1)$.

Our second goal is to swap qubits A and C.

$$\begin{aligned} & \mathsf{CC}(\mathsf{Diag}(1, u_0^*u_1)) \\ = \ & \overline{S}_{AC}\ \mathsf{CC}(\mathsf{Diag}(1, u_0^*u_1))\ \overline{S}_{AC} \\ = \ & \overline{S}_{AC}\ \overline{U}_{1i_1j_1}\ \overline{U}_{2i_2j_2}\ \overline{U}_{3i_3j_3}\ \overline{V}_{4AB}\ \overline{S}_{AC} \\ = \ & \overline{S}_{AC}\ \overline{U}_{1i_1j_1}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{2i_2j_2}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{3i_3j_3}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{V}_{4AB}\ \overline{S}_{AC} \\ = \ & (\overline{S}_{AC}\ \overline{U}_{1i_1j_1}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{2i_2j_2}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{3i_3j_3}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{V}_{4AB}\ \overline{S}_{AC}) \end{aligned}$$

In the first step, we use Lemma A.13. In the second step, we use the assumption about E_5. In the fourth step, we use that matrix multiplication is associative.

The above product has 4 factors that each is of one of the forms $(\overline{S}_{AC}\ \overline{U}_{AB}\ \overline{S}_{AC})$, $(\overline{S}_{AC}\ \overline{U}_{AC}\ \overline{S}_{AC})$, and $(\overline{S}_{AC}\ \overline{U}_{BC}\ \overline{S}_{AC})$. In each case, we can combine the three unitaries into a single unitary. Notice that $(\overline{S}_{AC}\ \overline{U}_{AB}\ \overline{S}_{AC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{AC}\ \overline{U}_{AC}\ \overline{S}_{AC}) \in \mathcal{G}_{AC}$ and $(\overline{S}_{AC}\ \overline{U}_{BC}\ \overline{S}_{AC}) \in \mathcal{G}_{AB}$. In particular, $(\overline{S}_{AC}\ \overline{V}_{4AB}\ \overline{S}_{AC}) \in \mathcal{G}_{BC}$. Thus, after those steps, we arrive at a product E_6 of the required form.

In the second case, the last unitary in E_4 operates on qubits AC. Thus, we can write $E_4 = \overline{U}_{1i_1j_1}\ \overline{U}_{2i_2j_2}\ \overline{U}_{3i_3j_3}\ \overline{U}_{4AC}$, where each $i_k, j_k \in \{A, B, C\}$ and $i_k \neq j_k$. Now we swap A and B:

$$
\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(u_0, u_1)) \\
= \;& \overline{S}_{AB}\ \mathsf{CC}(\mathsf{Diag}(u_0, u_1))\ \overline{S}_{AB} \\
= \;& \overline{S}_{AB}\ \overline{U}_{1 i_1 j_1}\ \overline{U}_{2 i_2 j_2}\ \overline{U}_{3 i_3 j_3}\ \overline{U}_{4AC}\ \overline{S}_{AB} \\
= \;& \overline{S}_{AB}\ \overline{U}_{1 i_1 j_1}\ (\overline{S}_{AB}\ \overline{S}_{AB})\ \overline{U}_{2 i_2 j_2}\ (\overline{S}_{AB}\ \overline{S}_{AB})\ \overline{U}_{3 i_3 j_3}\ (\overline{S}_{AB}\ \overline{S}_{AB})\ \overline{U}_{4AC}\ \overline{S}_{AB} \\
= \;& (\overline{S}_{AB}\ \overline{U}_{1 i_1 j_1}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{U}_{2 i_2 j_2}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{U}_{3 i_3 j_3}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{U}_{4AC}\ \overline{S}_{AB}) \\
= \;& (\overline{S}_{AB}\ \overline{U}_{1 i_1 j_1}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{U}_{2 i_2 j_2}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{U}_{3 i_3 j_3}\ \overline{S}_{AB})\ \overline{U}_{4BC}
\end{aligned}
$$

In the first step, we use Lemma A.13. In the second step, we use the assumption about E_4. In the fourth step, we use that matrix multiplication is associative. In the fifth step, we use Lemma A.12.

In the above product, each of the first three factors is of one of the forms $(\overline{S}_{AB}\ \overline{U}_{AB}\ \overline{S}_{AB})$, $(\overline{S}_{AB}\ \overline{U}_{AC}\ \overline{S}_{AB})$, and $(\overline{S}_{AB}\ \overline{U}_{BC}\ \overline{S}_{AB})$. In each case, we can combine the three unitaries into a single unitary. Specifically, in the first case this is straightforward, while in the second and third case, we use Lemma A.12. Thus, after those steps, we arrive at a product E_6 of the required form. Additionally, we can choose $u_6 = u_0$ and $u_7 = u_1$ and thereby satisfy $(u_6, u_7) \in R(u_0, u_1)$.

In the third case, the last unitary in E_4 operates on qubits BC, which means that we can choose $E_6 = E_4$, and we can choose $u_6 = u_0$ and $u_7 = u_1$ and thereby satisfy $(u_6, u_7) \in R(u_0, u_1)$.

Notice that in each of the three cases, if E_4 is canonical form, then E_6 is in canonical form. This concludes the third step of the proof.

In the fourth step, we transform E_6 to a product of one of the two required forms.

We have eight cases.

In the first case, we can write E_6 as $\overline{U}_{1AB}\ \overline{U}_{2BC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. From Lemma 7.1 we have a 2-qubit unitary V such that $\mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) = \overline{V}_{AB}\ \overline{U}_{2BC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. From $(u_6, u_7) \in R(u_0, u_1)$ we get $(1, u_6^* u_7) \in R(u_0, u_1)$. Now we swap B and C:

$$
\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) \\
= \;& \overline{S}_{BC}\ \overline{V}_{AB}\ \overline{U}_{2BC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}\ \overline{S}_{BC} \\
= \;& \overline{S}_{BC}\ \overline{V}_{AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{2BC}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{3AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{4BC}\ \overline{S}_{BC} \\
= \;& (\overline{S}_{BC}\ \overline{V}_{AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{2BC}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{3AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \\
= \;& \overline{V}_{AC}\ (\overline{S}_{BC}\ \overline{U}_{2BC}\ \overline{S}_{BC})\ \overline{U}_{3AC}\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC})
\end{aligned}
$$

In the first step, we use Lemma A.13. In the third step, we use that matrix multiplication is associative.

Above, $(\overline{S}_{BC}\ \overline{U}_{2BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$. Thus, the product is of one of the required forms.

In the second case, we can write E_6 as $\overline{U}_{1AB}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC}$. From Lemma 7.1 we have a 2-qubit unitary V such that $\mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) = \overline{V}_{AB}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC}$. From $(u_6, u_7) \in R(u_0, u_1)$ we get $(1, u_6^* u_7) \in R(u_0, u_1)$. Now we swap B and C:

$$
\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) \\
= \ & \overline{S}_{BC}\ \overline{V}_{AB}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC}\ \overline{S}_{BC} && \text{(Lemma A.13)} \\
= \ & \overline{S}_{BC}\ \overline{V}_{AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC}\ \overline{S}_{BC} && (\overline{S}_{BC}\ \overline{S}_{BC} = \overline{I}_{BC}) \\
= \ & (\overline{S}_{BC}\ \overline{V}_{AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{2BC})\ \overline{U}_{3AC}\ (\overline{U}_{4BC}\ \overline{S}_{BC}) && \text{(Associativity)} \\
= \ & \overline{V}_{AC}\ (\overline{S}_{BC}\ \overline{U}_{2BC})\ \overline{U}_{3AC}\ (\overline{U}_{4BC}\ \overline{S}_{BC})
\end{aligned}
$$

Here $(\overline{S}_{BC}\ \overline{U}_{2BC}) \in \mathcal{G}_{BC}$ and $(\overline{U}_{4BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$. Thus, the product is of one of the required forms.

In the third case, we can write E_6 as $\overline{U}_{1AB}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. From Lemma 7.1 we have a 2-qubit unitary V such that $\mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) = \overline{V}_{AB}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. From $(u_6, u_7) \in R(u_0, u_1)$ we get $(1, u_6^* u_7) \in R(u_0, u_1)$. Now we do both a swap of B and C and a swap of A and C:

$$
\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(1, u_6^* u_7)) \\
= \ & \overline{S}_{BC}\ \overline{V}_{AB}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}\ \overline{S}_{BC} \\
= \ & \overline{S}_{BC}\ \overline{V}_{AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{2AC}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{3AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{4BC}\ \overline{S}_{BC} \\
= \ & (\overline{S}_{BC}\ \overline{V}_{AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{2AC}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{3AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \\
= \ & \overline{V}_{AC}\ \overline{U}_{2AB}\ \overline{U}_{3AC}\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \\
= \ & \overline{V}_{AC}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{2AB}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{3AC}\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \\
= \ & (\overline{V}_{AC}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{2AB}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{3AC})\ (\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC})
\end{aligned}
$$

In the first step, we use Lemma A.13. In the third step and in the sixth step, we use that matrix multiplication is associative.

Above, $(\overline{V}_{AC}\ \overline{S}_{AC}) \in \mathcal{G}_{AC}$ and $(\overline{S}_{AC}\ \overline{U}_{2AB}\ \overline{S}_{AC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{AC}\ \overline{U}_{3AC}) \in \mathcal{G}_{AC}$ and $(\overline{S}_{BC}\ \overline{U}_{4BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$. Thus, the product is of one of the required forms.

In the fourth case, we can write E_6 as $\overline{U}_{1BC}\ \overline{U}_{2AB}\ \overline{U}_{3AC}\ \overline{U}_{4BC}$. Now we swap B and C:

$$
\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(u_6, u_7)) \\
= \ & \overline{U}_{1BC}\ \overline{U}_{2AB}\ \overline{U}_{3AC}\ \overline{U}_{4BC} \\
= \ & \overline{U}_{1BC}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{2AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{3AC}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{4BC} && (\overline{S}_{BC}\ \overline{S}_{BC} = \overline{I}_{BC}) \\
= \ & (\overline{U}_{1BC}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{2AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{3AC}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{4BC}) && \text{(Associativity)} \\
= \ & (\overline{U}_{1BC}\ \overline{S}_{BC})\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ (\overline{S}_{BC}\ \overline{U}_{4BC})
\end{aligned}
$$

Here $(\overline{U}_{1BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{BC}\ \overline{U}_{4BC}) \in \mathcal{G}_{BC}$. Thus, the product is of one of the required forms.

In the fifth case, we can write E_6 as $\overline{U}_{1BC}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. This is one of the required forms.

In the sixth case, we can write E_6 as $\overline{U}_{1AC}\ \overline{U}_{2AB}\ \overline{U}_{3AC}\ \overline{U}_{4BC}$. Now we swap A and C:

$$\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(u_6, u_7)) \\
= \ & \overline{U}_{1AC}\ \overline{U}_{2AB}\ \overline{U}_{3AC}\ \overline{U}_{4BC} \\
= \ & \overline{U}_{1AC}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{2AB}\ (\overline{S}_{AC}\ \overline{S}_{AC})\ \overline{U}_{3AC}\ \overline{U}_{4BC} && (\overline{S}_{AC}\ \overline{S}_{AC} = \overline{I}_{AC}) \\
= \ & (\overline{U}_{1AC}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{2AB}\ \overline{S}_{AC})\ (\overline{S}_{AC}\ \overline{U}_{3AC})\ \overline{U}_{4BC} && \text{(Associativity)}
\end{aligned}$$

Here $(\overline{U}_{1AC}\ \overline{S}_{AC}) \in \mathcal{G}_{AC}$ and $(\overline{S}_{AC}\ \overline{U}_{2AB}\ \overline{S}_{AC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{AC}\ \overline{U}_{3AC}) \in \mathcal{G}_{AC}$. Thus, the product is of one of the required forms.

In the seventh case, we can write E_6 as $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AB}\ \overline{U}_{4BC}$. Now we swap B and C:

$$\begin{aligned}
& \mathsf{CC}(\mathsf{Diag}(u_6, u_7)) \\
= \ & \overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AB}\ \overline{U}_{4BC} \\
= \ & \overline{U}_{1AC}\ \overline{U}_{2BC}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{3AB}\ (\overline{S}_{BC}\ \overline{S}_{BC})\ \overline{U}_{4BC} && (\overline{S}_{BC}\ \overline{S}_{BC} = \overline{I}_{BC}) \\
= \ & \overline{U}_{1AC}\ (\overline{U}_{2BC}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{3AB}\ \overline{S}_{BC})\ (\overline{S}_{BC}\ \overline{U}_{4BC}) && \text{(Associativity)} \\
= \ & \overline{U}_{1AC}\ (\overline{U}_{2BC}\ \overline{S}_{BC})\ \overline{U}_{3AC}\ (\overline{S}_{BC}\ \overline{U}_{4BC})
\end{aligned}$$

Here $(\overline{U}_{2BC}\ \overline{S}_{BC}) \in \mathcal{G}_{BC}$ and $(\overline{S}_{BC}\ \overline{U}_{4BC}) \in \mathcal{G}_{BC}$. Thus, the product is of one of the required forms.

In the eighth case, we can write E_6 as $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC}$. This is one of the required forms. □

Lemma 7.3. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. Suppose also that $(u_2, u_3) \in R(u_0, u_1)$. If ($u_2 = u_3$ or $u_2 u_3 = 1$), then ($u_0 = u_1$ or $u_0 u_1 = 1$).*

Proof. Suppose ($u_2 = u_3$ or $u_2 u_3 = 1$). We have two cases that each has two subcases.

member of $R(u_0, u_1)$	assumption	consequence	conclusion
$(u_2, u_3) = (u_0, u_1)$	$u_2 = u_3$	$u_0 = u_1$	$u_0 = u_1$
	$u_2 u_3 = 1$	$u_0 u_1 = 1$	$u_0 u_1 = 1$
$(u_2, u_3) = (1, u_0^* u_1)$	$u_2 = u_3$	$1 = u_0^* u_1$	$u_0 = u_1$
	$u_2 u_3 = 1$	$1 \cdot u_0^* u_1 = 1$	$u_0 = u_1$

From the above table we see that, in every case, we reach the desired conclusion. □

Theorem 7.4 *(Main result for a diagonal matrix). Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exists a product of at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. In the left-to-right direction, suppose there exists a product of at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ that is equal to $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. From Lemma 7.2 we have that this implies that either

there exist 2-qubit unitaries U_1, U_2, U_3, U_4 and complex numbers u_2, u_3 such that $(u_2, u_3) \in R(u_0, u_1)$ and $\overline{U}_{1BC}\ \overline{U}_{2AC}\ \overline{U}_{3AB}\ \overline{U}_{4BC} \ = \ \mathsf{CC}(\mathsf{Diag}(u_2, u_3))$,

or

there exist 2-qubit unitaries U_1, U_2, U_3, U_4 and complex numbers u_2, u_3 such that $(u_2, u_3) \in R(u_0, u_1)$ and $\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} \ = \ \mathsf{CC}(\mathsf{Diag}(u_2, u_3))$.

We can apply Lemma 5.1 to the first case and we can apply Lemma 6.4 to the second case, and in both cases we get that the property is true if and only if either $u_2 = u_3$ or $u_2 u_3 = 1$. We have $(u_2, u_3) \in R(u_0, u_1)$ so from Lemma 7.3 we have either $u_0 = u_1$ or $u_0 u_1 = 1$.

In the right-to-left direction, suppose either $u_0 = u_1$ or $u_0 u_1 = 1$. The conclusion follows from Lemma 5.1. □

Corollary 7.5 *(Main result for a gate with two controls). For a 1-qubit unitary U, there exists a product of at most four elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ that is equal to $\mathsf{CC}(U)$ if and only if either the eigenvalues of U are equal or $\det(U) = 1$.*

Proof. Suppose $\mathsf{Eigenvalues}(U) = [u_0, u_1]$. From the Spectral Theorem A.3 we have that there exists unitary matrix V such that $U = V\ \mathsf{Diag}(u_0, u_1)\ V^\dagger$. We calculate

$$\mathsf{CC}(\mathsf{Diag}(u_0, u_1)) = (I_A \otimes I_B \otimes V^\dagger)\ \mathsf{CC}(U)\ (I_A \otimes I_B \otimes V)$$

We have $(I_A \otimes I_B \otimes V^\dagger), (I_A \otimes I_B \otimes V) \in \mathcal{G}_1$. Thus, the number of elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ needed to implement $\mathsf{CC}(U)$ is the same as the number needed to implement $\mathsf{CC}(\mathsf{Diag}(c_0, c_1))$. From Theorem 7.4 we have that this number is at most four if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$. We have $\mathsf{Eigenvalues}(U) = [u_0, u_1]$ so $\det(U) = u_0 u_1$. Thus, (either $u_0 = u_1$ or $u_0 u_1 = 1$) is the same as saying that the eigenvalues of U are equal or that $\det(U) = 1$, as required. □

Notice that Corollary 7.5 implies that five 2-qubit gates are necessary for implementing the Toffoli gate. This is because the Toffoli gate is $\mathsf{CC}(X)$ and the eigenvalues of X are $[1, -1]$, so the eigenvalues of X are different and $\det(X) = -1 \neq 1$.

For completeness, we summarize known results for implementation of $\mathsf{CC}(U)$. The question is whether a product of n elements of $\mathcal{G}_2 \setminus \mathcal{G}_1$ and any number of elements of $\mathcal{G}_1$ is equal to $\mathsf{CC}(U)$. There exists such a product for

- $n \leq 1$ if and only if the eigenvalues of U are equal (see the proof of Lemma 5.1);
- $n \leq 3$ if and only if the eigenvalues of U are equal [4, Lemma 4.1];
- $n \leq 4$ if and only if the eigenvalues of U are equal or $\det(U) = 1$ (Corollary 7.5); and
- $n \leq 5$ always [2,1].

Notice that if the eigenvalues of U are equal, then a single 2-qubit gate is sufficient. Notice also that if the eigenvalues of U are different and $\det(U) = 1$, then four 2-qubit gates are both necessary and sufficient.

8. Conclusion

We have given a detailed proof of a well-known theorem in quantum computing. Our proof has sufficient detail, clarity, and simplicity that it may inspire work on discovering novel, related results.

Declaration of competing interest

No competing interest.

Data availability

No data was used for the research described in the article.

Acknowledgements

We are grateful to the anonymous reviewer for many suggestions that led to significant improvements of the paper. We are also grateful to Kyle Chui, Wenhao Du, Shaviv Hoffman-Lowitz, Keli Huang, Yeon Taek Jeong, Wan-Hsuan Lin, Henry Ma, Landon Miller, Christian Navasca, Nuocheng Pan, Joseph Peetz, Neil Vaishampayan, and Changling Zhao for detailed comments on earlier versions of the proof. Additionally, we are grateful to Kyle Chui, Yeon Taek Jeong, and Neil Vaishampayan for formalizing many of the lemmas and proofs in the Coq proof assistant. Jens Palsberg is supported by the NSF QLCI program through grant number OMA-2016245.

Appendix A. Foundations

Sections A.1–A.4 contain well-known results from linear algebra (or easy consequences thereof), while Sections A.5–A.7 contain lemmas that the original proof [3,4] outlined at a high level.

A.1. Square matrices

We will state properties of determinants and traces of square matrices. We don't give proofs of those properties; proofs are widely available in textbooks on linear algebra.

Lemma A.1. *For square matrices D, E of the same size:* $\det(DE) = \det(D)\ \det(E)$.

Lemma A.2. *For square matrices D, E of the same size:* $tr(DE) = tr(ED)$.

A.2. Unitary matrices

Now we state the Spectral Theorem for the case of a unitary matrix and we state other properties of unitary matrices. We don't give proofs of those properties; proofs are widely available in textbooks on linear algebra.

Theorem A.3 *(Spectral Theorem). For a unitary matrix U, there exists a unitary matrix V and a unitary diagonal matrix W, such that $U = VWV^\dagger$ and the entries on the diagonal of W are the eigenvalues of U.*

Lemma A.4 *(Conjugation preserves eigenvalues). For unitary matrices U, V of the same size, we have* $\mathsf{Eigenvalues}(UVU^\dagger) = \mathsf{Eigenvalues}(V)$.

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

Lemma A.6. *For 1-qubit unitaries P, Q, we have* $\mathsf{Eigenvalues}(|0\rangle\langle 0| \otimes P + |1\rangle\langle 1| \otimes Q) = \mathsf{Eigenvalues}(P) \sqcup \mathsf{Eigenvalues}(Q)$.

We have introduced notation for partial traces in the special case of $tr_A(U)$ where we trace out the first qubit from a 2-qubit unitary U. The following lemma expresses the key property of tr_A. This generalizes to tracing out multiple qubits from larger unitaries.

Lemma A.7. *There exists a unique linear function called tr_A from 2-qubit unitaries to 1-qubit unitaries that, for any 1-qubit unitaries P, Q, satisfies $tr_A(P \otimes Q) = tr(P)\ Q$.*

Lemma A.8. *For a 1-qubit unitary Q, let $|\beta\rangle = Q\ |0\rangle$ and let $|\beta^\perp\rangle = Q\ |1\rangle$. Now $|\beta\rangle\langle\beta| + |\beta^\perp\rangle\langle\beta^\perp| = I$.*

Lemma A.9. *For a 2-qubit unitary V and 2×2 matrices $P_{00}, P_{01}, P_{10}, P_{11}$, where*

$$V = |0\rangle\langle 0| \otimes P_{00} + |0\rangle\langle 1| \otimes P_{01} + |1\rangle\langle 0| \otimes P_{10} + |1\rangle\langle 1| \otimes P_{11}$$

we have $P_{01} = \mathbf{0}$ if and only if $P_{10} = \mathbf{0}$.

A.3. Swaps

Lemma A.10 *(Swap of vectors). For 2-dimensional vectors $|\psi\rangle, |\varphi\rangle$ (not necessarily unit vectors), we have $S\ (|\psi\rangle \otimes |\varphi\rangle) = |\varphi\rangle \otimes |\psi\rangle$.*

Proof. Immediate from the definition of S. □

Lemma A.11 *(Swap of matrices). For 2×2 matrices D, E, we have $S\ (D \otimes E)\ S = E \otimes D$.*

Proof. Immediate from the definition of S. □

Lemma A.12. *For a 2-qubit unitary U, we have $\overline{S}_{AB}\ \overline{U}_{AC}\ \overline{S}_{AB} = \overline{U}_{BC}$.*

Proof. We can write U in the following way:

$$U = |0\rangle\langle 0| \otimes P_{00}\ +\ |0\rangle\langle 1| \otimes P_{01}\ +\ |1\rangle\langle 0| \otimes P_{10}\ +\ |1\rangle\langle 1| \otimes P_{11}$$

where $P_{00}, P_{01}, P_{10}, P_{11}$ are 2×2 matrices.

We calculate:

$$\begin{aligned}
&\overline{S}_{AB}\ \overline{U}_{AC}\ \overline{S}_{AB} \\
&= (S_{AB} \otimes I_C)\ (I_A \otimes S_{BC})\ (U_{AB} \otimes I_C)\ (I_A \otimes S_{BC})\ (S_{AB} \otimes I_C) \\
&= (S_{AB} \otimes I_C)\ (I_A \otimes S_{BC}) \\
&\qquad (|0\rangle\langle 0| \otimes P_{00} \otimes I_C\ +\ |0\rangle\langle 1| \otimes P_{01} \otimes I_C\ +\ |1\rangle\langle 0| \otimes P_{10} \otimes I_C\ +\ |1\rangle\langle 1| \otimes P_{11} \otimes I_C) \\
&\qquad (I_A \otimes S_{BC})\ (S_{AB} \otimes I_C) \\
&= (S_{AB} \otimes I_C) \\
&\qquad (|0\rangle\langle 0| \otimes I_B \otimes P_{00}\ +\ |0\rangle\langle 1| \otimes I_B \otimes P_{01}\ +\ |1\rangle\langle 0| \otimes I_B \otimes P_{10}\ +\ |1\rangle\langle 1| \otimes I_B \otimes P_{11} \\
&\qquad (S_{AB} \otimes I_C) \\
&= I_A \otimes |0\rangle\langle 0| \otimes P_{00}\ +\ I_A \otimes |0\rangle\langle 1| \otimes P_{01}\ +\ I_A \otimes |1\rangle\langle 0| \otimes P_{10}\ +\ I_A \otimes |1\rangle\langle 1| \otimes P_{11} \\
&= I_A \otimes U_{BC} \\
&= \overline{U}_{BC}
\end{aligned}$$

In the first step, we use the definitions of $\overline{S}_{AB}$ and $\overline{U}_{AC}$. In the second step, we use the definition of U. In the third step, we use Lemma A.11. In the fourth step, we use

Lemma A.11. In the fifth step, we use the definition of U. In the sixth step, we use the definition of $\overline{S}_{BC}$. $\square$

Lemma A.13 *(Swap of controlled matrices). Suppose D is a 2×2 matrix and c_1 is a complex number. First, $\overline{S}_{AB}\ \mathsf{CC}(D)\ \overline{S}_{AB} = \mathsf{CC}(D)$. Second, $\overline{S}_{BC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{BC} = \mathsf{CC}(\mathsf{Diag}(1, c_1))$. Third, $\overline{S}_{AC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{AC} = \mathsf{CC}(\mathsf{Diag}(1, c_1))$.*

Proof. We use $\mathsf{CC}(D) = |0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes D$.

First we show $\overline{S}_{AB}\ \mathsf{CC}(D)\ \overline{S}_{AB} = \mathsf{CC}(D)$. We calculate

$$\begin{aligned}
&\overline{S}_{AB}\ \mathsf{CC}(D)\ \overline{S}_{AB} \\
&= \overline{S}_{AB}\ (|0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes D)\ \overline{S}_{AB} \\
&= \overline{S}_{AB}\ (|0\rangle\langle 0| \otimes I \otimes I)\ \overline{S}_{AB}\ +\ \overline{S}_{AB}\ (|1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I)\ \overline{S}_{AB}\ + \\
&\qquad\qquad \overline{S}_{AB}\ (|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes D)\ \overline{S}_{AB} \\
&= I \otimes |0\rangle\langle 0| \otimes I\ \ +\ |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes I\ \ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes D \\
&= \mathsf{Diag}(1,1,0,0,1,1,0,0)\ +\ \mathsf{Diag}(0,0,1,1,0,0,0,0)\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes D \\
&= \mathsf{CC}(D)
\end{aligned}$$

In the third step, we use Lemma A.11.

Second we show $\overline{S}_{BC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{BC} = \mathsf{CC}(\mathsf{Diag}(1, c_1))$. We calculate

$$\begin{aligned}
&\overline{S}_{BC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{BC} \\
&= \overline{S}_{BC}\ (|0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathsf{Diag}(1, c_1))\ \overline{S}_{BC} \\
&= \overline{S}_{BC}\ (|0\rangle\langle 0| \otimes I \otimes I)\ \overline{S}_{BC}\ +\ \overline{S}_{BC}\ (|1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I)\ \overline{S}_{BC}\ + \\
&\qquad\qquad \overline{S}_{BC}\ (|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathsf{Diag}(1, c_1))\ \overline{S}_{BC} \\
&= (|0\rangle\langle 0| \otimes I \otimes I)\ +\ (|1\rangle\langle 1| \otimes I \otimes |0\rangle\langle 0|)\ +\ (|1\rangle\langle 1| \otimes \mathsf{Diag}(1, c_1) \otimes |1\rangle\langle 1|) \\
&= \mathsf{Diag}(1,1,1,1,0,0,0,0) + \mathsf{Diag}(0,0,0,0,1,0,1,0) + \mathsf{Diag}(0,0,0,0,0,1,0,c_1) \\
&= \mathsf{Diag}(1,1,1,1,1,1,1,c_1) \\
&= \mathsf{CC}(\mathsf{Diag}(1, c_1))
\end{aligned}$$

In the third step, we use Lemma A.11.

Third we show $\overline{S}_{AC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{AC} = \mathsf{CC}(\mathsf{Diag}(1, c_1))$. We calculate

$$\begin{aligned}
&\overline{S}_{AC}\ \mathsf{CC}(\mathsf{Diag}(1, c_1))\ \overline{S}_{AC} \\
&= \overline{S}_{AC}\ (|0\rangle\langle 0| \otimes I \otimes I\ +\ |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I\ +\ |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathsf{Diag}(1, c_1))\ \overline{S}_{AC} \\
&= \overline{S}_{AC}\ (|0\rangle\langle 0| \otimes I \otimes I)\ \overline{S}_{AC}\ +\ \overline{S}_{AC}\ (|1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I)\ \overline{S}_{AC}\ + \\
&\qquad\qquad \overline{S}_{AC}\ (|1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \mathsf{Diag}(1, c_1))\ \overline{S}_{AC}
\end{aligned}$$

$$= (I \otimes I \otimes |0\rangle\langle 0|) \ + \ (I \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1|) \ + \ (\mathsf{Diag}(1, c_1) \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1|)$$
$$= \mathsf{Diag}(1,0,1,0,1,0,1,0) + \mathsf{Diag}(0,1,0,0,0,1,0,0) + \mathsf{Diag}(0,0,0,1,0,0,c_1)$$
$$= \mathsf{Diag}(1,1,1,1,1,1,1,c_1)$$
$$= \mathsf{CC}(\mathsf{Diag}(1, c_1))$$

In the third step, we use Lemma A.11. □

A.4. Vectors

We will use the following results in the proofs of Lemma A.19, Lemma A.22, and Lemma A.23. First we state Schmidt decomposition, taken from Nielsen and Chuang [1], Theorem 2.7 and Exercise 2.78.

Theorem A.14 *(Schmidt decomposition). For a unit vector $|\varphi\rangle_{AB}$, there exists a real number r $(0 \leq r \leq 1)$, a pair of orthogonal qubits $|\beta\rangle_A, |\beta^\perp\rangle_A$, and a second pair of orthogonal qubits $|\gamma\rangle_B, |\gamma^\perp\rangle_B$ such that:*

$$|\varphi\rangle_{AB} = \sqrt{r} \ |\beta\rangle_A \otimes |\gamma\rangle_B \ + \ \sqrt{1-r} \ |\beta^\perp\rangle_A \otimes |\gamma^\perp\rangle_B$$

Additionally, $|\varphi\rangle_{AB}$ is a tensor product if and only if $r = 0$ or $r = 1$.

Lemma A.15. *For a 4-dimensional unit vector $|w\rangle$ and orthogonal qubits $|\beta\rangle, |\beta^\perp\rangle$, there exist vectors (not necessarily qubits) $|\psi\rangle, |\varphi\rangle$ such that $|w\rangle = |\beta\rangle \otimes |\psi\rangle + |\beta^\perp\rangle \otimes |\varphi\rangle$.*

Proof. Define a 1-qubit unitary Q:

$$Q = |\beta\rangle\langle 0| \ + \ |\beta^\perp\rangle\langle 1|$$

Notice that the columns of Q are orthogonal unit vectors, hence Q is a unitary matrix.

We can write

$$\begin{aligned}(Q \otimes I)^\dagger \ |w\rangle &= c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \\ &= |0\rangle \otimes (c_{00}|0\rangle + c_{01}|1\rangle) \ + \ |1\rangle \otimes (c_{10}|0\rangle + c_{11}|1\rangle)\end{aligned}$$

Define

$$|\psi\rangle = c_{00}|0\rangle + c_{01}|1\rangle$$
$$|\varphi\rangle = c_{10}|0\rangle + c_{11}|1\rangle$$

We can combine the above observations and get:

$$(Q \otimes I)^\dagger \ |w\rangle = |0\rangle \otimes |\psi\rangle \ + \ |1\rangle \otimes |\varphi\rangle$$

We calculate

$$\begin{aligned}|w\rangle &= (Q \otimes I)\ (Q \otimes I)^\dagger\ |w\rangle \\ &= (Q \otimes I)\ (|0\rangle \otimes |\psi\rangle\ +\ |1\rangle \otimes |\varphi\rangle) \\ &= |\beta\rangle \otimes |\psi\rangle\ +\ |\beta^\perp\rangle \otimes |\varphi\rangle \quad \square\end{aligned}$$

Lemma A.16. *For 2-dimensional vectors $|w_0\rangle, |w_1\rangle$ (not necessarily unit vectors) and for linearly independent qubits $|\alpha_0\rangle, |\alpha_1\rangle$, if $|w_0\rangle \otimes |\alpha_0\rangle + |w_1\rangle \otimes |\alpha_1\rangle = \mathbf{0}$, then $|w_0\rangle = \mathbf{0}$ and $|w_1\rangle = \mathbf{0}$.*

Proof. We pick a qubit $|\alpha_0^\perp\rangle$ such that $|\alpha_0\rangle$ and $|\alpha_0^\perp\rangle$ are orthogonal. From this and that $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are linearly independent, we see that $\langle\alpha_0^\perp|\alpha_1\rangle \neq 0$.

Let us apply $I \otimes \langle\alpha_0^\perp|$ to both sides of $|w_0\rangle \otimes |\alpha_0\rangle + |w_1\rangle \otimes |\alpha_1\rangle = \mathbf{0}$ which gives

$$\langle\alpha_0^\perp|\alpha_1\rangle\ |w_1\rangle = \mathbf{0}$$

From this and $\langle\alpha_0^\perp|\alpha_1\rangle \neq 0$, we conclude $|w_1\rangle = \mathbf{0}$.

From $|w_0\rangle \otimes |\alpha_0\rangle + |w_1\rangle \otimes |\alpha_1\rangle = \mathbf{0}$ and $|w_1\rangle = \mathbf{0}$, we have $|w_0\rangle \otimes |\alpha_0\rangle = \mathbf{0}$. We also have $|\alpha_0\rangle \neq \mathbf{0}$ so we conclude $|w_0\rangle = \mathbf{0}$. $\square$

A.5. Controlled unitaries

We will show that various conditions imply that a unitary is controlled.

Lemma A.17. *If U is a 2-qubit unitary, and $|\beta\rangle, |\beta^\perp\rangle$ are two orthogonal qubits, and we have qubits $|\psi\rangle, |\varphi\rangle$ such that $U\ (|0\rangle \otimes |\beta\rangle) = |0\rangle \otimes |\psi\rangle$ and $U\ (|0\rangle \otimes |\beta^\perp\rangle) = |0\rangle \otimes |\varphi\rangle$, then U is of the form:*

$$U = |0\rangle\langle 0| \otimes P_{00}\ +\ |1\rangle\langle 1| \otimes P_{11}$$

where P_{00}, P_{11} are 1-qubit unitaries.

Proof. We can write

$$U = |0\rangle\langle 0| \otimes P_{00} + |0\rangle\langle 1| \otimes P_{01} + |1\rangle\langle 0| \otimes P_{10} + |1\rangle\langle 1| \otimes P_{11}$$

where $P_{00}, P_{01}, P_{10}, P_{11}$ are 2×2 matrices.

Define a 1-qubit unitary Q:

$$Q = |\beta\rangle\langle 0|\ +\ |\beta^\perp\rangle\langle 1|$$

Notice that the columns of Q are orthogonal qubits so Q is unitary.

Let $|w\rangle$ be a qubit:

$$|w\rangle = a\ |0\rangle\ +\ b\ |1\rangle$$

We calculate $U\ (I \otimes Q)\ (|0\rangle \otimes |w\rangle)$ in two different ways:

$$\begin{aligned}
U\ (I \otimes Q)\ (|0\rangle \otimes |w\rangle) &= U\ (I \otimes Q)\ (|0\rangle \otimes (a\ |0\rangle\ +\ b\ |1\rangle)) \\
&= U\ (a\ |0\rangle \otimes |\beta\rangle\ +\ b\ |0\rangle \otimes |\beta^{\perp}\rangle) \\
&= a\ |0\rangle \otimes |\psi\rangle\ +\ b\ |0\rangle \otimes |\varphi\rangle \\
&= |0\rangle \otimes (a\ |\psi\rangle\ +\ b\ |\varphi\rangle) \\
U\ (I \otimes Q)\ (|0\rangle \otimes |w\rangle) &= U\ (|0\rangle \otimes Q\ |w\rangle) \\
&= |0\rangle \otimes P_{00}\ Q\ |w\rangle\ +\ |1\rangle \otimes P_{10}\ Q\ |w\rangle
\end{aligned}$$

In the third step of the first calculation, we use the $|\psi\rangle, |\varphi\rangle$ from the assumption of the lemma.

From the two calculations of $U\ (I \otimes Q)\ (|0\rangle \otimes |w\rangle)$ we have that

$$|0\rangle \otimes (a\ |\psi\rangle\ +\ b\ |\varphi\rangle) = |0\rangle \otimes P_{00}\ Q\ |w\rangle\ +\ |1\rangle \otimes P_{10}\ Q\ |w\rangle$$

which implies that

$$|1\rangle \otimes P_{10}\ Q\ |w\rangle = \mathbf{0}$$

which implies that

$$P_{10}\ Q\ |w\rangle = \mathbf{0}$$

We have that this is true for any qubit $|w\rangle$, which implies that $P_{10}\ Q = \mathbf{0}$. From this and that Q is unitary, we conclude that $P_{10} = \mathbf{0}$.

From $P_{10} = \mathbf{0}$ and Lemma A.9 we have that $P_{01} = \mathbf{0}$. From this and the assumption that U is unitary, we have that P_{00}, P_{11} are unitary. Thus, U is of the required form. □

Lemma A.18. *If U is a 2-qubit unitary, and $\forall |\beta\rangle : U\ (|\beta\rangle \otimes |0\rangle) = |\beta\rangle \otimes |0\rangle$, then U is of the form:*

$$U = I \otimes |0\rangle\langle 0| + P_1 \otimes |1\rangle\langle 1|$$

where P_1 is a 1-qubit unitary.

Proof. We calculate:

$$(S\ U\ S)\ (|0\rangle \otimes |\beta\rangle) = S\ U\ (|\beta\rangle \otimes |0\rangle)\ \ =\ \ S\ (|\beta\rangle \otimes |0\rangle)\ \ =\ \ |0\rangle \otimes |\beta\rangle$$

In the first and the third step, we use Lemma A.10.

We can pick orthogonal qubits $|\beta\rangle, |\beta^{\perp}\rangle$ and use the above to observe that

$$(S\ U\ S)\ (|0\rangle \otimes |\beta\rangle) = |0\rangle \otimes |\beta\rangle$$
$$(S\ U\ S)\ (|0\rangle \otimes |\beta^{\perp}\rangle) = |0\rangle \otimes |\beta^{\perp}\rangle$$

From Lemma A.17 we have that $(S\ U\ S)$ is of the form

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

where P_0, P_1 are 1-qubit unitaries. From this and Lemma A.11, we have

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

We calculate, for any qubit $|\beta\rangle$:

$$|\beta\rangle \otimes |0\rangle = U\ (|\beta\rangle \otimes |0\rangle) \quad = \quad (P_0 \otimes |0\rangle\langle 0| + P_1 \otimes |1\rangle\langle 1|)\ (|\beta\rangle \otimes |0\rangle) \quad = \quad (P_0\ |\beta\rangle) \otimes |0\rangle$$

In this first step, we use the assumption of the lemma.

From the above we get that, for any qubit $|\beta\rangle$:

$$P_0\ |\beta\rangle = |\beta\rangle$$

Thus, $P_0 = I$, as required. □

Lemma A.19. *If U is a 2-qubit unitary and $|\varphi\rangle_{BC}, |w\rangle_{BC}$ are 4-dimensional unit vectors such that $\overline{U}_{AC}\ (|0\rangle_A \otimes |\varphi\rangle_{BC}) = |0\rangle_A \otimes |w\rangle_{BC}$ and $|\varphi\rangle_{BC}$ is entangled, then U is of the following form, where P_0, P_1 are 1-qubit unitaries:*

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

Proof. We use Schmidt decomposition (Theorem A.14) on $|\varphi\rangle_{BC}$ and get a real number r, a pair of orthogonal qubits $|\beta\rangle_B, |\beta^{\perp}\rangle_B$, and a second pair of orthogonal qubits $|\gamma\rangle_C, |\gamma^{\perp}\rangle_C$ such that:

$$|\varphi\rangle_{BC} = \sqrt{r}\ |\beta\rangle_B \otimes |\gamma\rangle_C\ +\ \sqrt{1-r}\ |\beta^{\perp}\rangle_B \otimes |\gamma^{\perp}\rangle_C$$

We have that $|\varphi\rangle_{BC}$ is entangled so $0 < r < 1$. Now we calculate:

$$\begin{aligned} |0\rangle_A \otimes |w\rangle_{BC} &= \overline{U}_{AC}\ (|0\rangle_A \otimes |\varphi\rangle_{BC}) \\ &= \overline{U}_{AC}\ (|0\rangle_A \otimes (\sqrt{r}\ |\beta\rangle_B \otimes |\gamma\rangle_C\ +\ \sqrt{1-r}\ |\beta^{\perp}\rangle_B \otimes |\gamma^{\perp}\rangle_C)) \\ &= \sqrt{r}\ \overline{U}_{AC}\ (|0\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C)\ +\ \sqrt{1-r}\ \overline{U}_{AC}\ (|0\rangle_A \otimes |\beta^{\perp}\rangle_B \otimes |\gamma^{\perp}\rangle_C) \end{aligned}$$

We can use Lemma A.15 to write $|w\rangle_{BC}$ based on $\{|\beta\rangle_B, |\beta^\perp\rangle_B\}$ as follows, where $|\psi\rangle_C$ and $|\varphi\rangle_C$ are vectors (not necessarily qubits):

$$|w\rangle_{BC} = |\beta\rangle_B \otimes |\psi\rangle_C \ + \ |\beta^\perp\rangle_B \otimes |\varphi\rangle_C$$

We calculate:

$$\begin{aligned}
&|0\rangle_A \otimes |\psi\rangle_B \otimes |\beta\rangle_C \ + \ |0\rangle_A \otimes |\varphi\rangle_B \otimes |\beta^\perp\rangle_C \\
&= \overline{S}_{BC} \ (|0\rangle_A \otimes |\beta\rangle_B \otimes |\psi\rangle_C \ + \ |0\rangle_A \otimes |\beta^\perp\rangle_B \otimes |\varphi\rangle_C) \\
&= \overline{S}_{BC} \ (|0\rangle_A \otimes |w\rangle_{BC}) \\
&= \overline{S}_{BC} \ (\sqrt{r}\ \overline{U}_{AC} \ (|0\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C) \ + \ \sqrt{1-r}\ \overline{U}_{AC} \ (|0\rangle_A \otimes |\beta^\perp\rangle_B \otimes |\gamma^\perp\rangle_C)) \\
&= \sqrt{r}\ \overline{S}_{BC}\ \overline{U}_{AC} \ (|0\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C) \ + \ \sqrt{1-r}\ \overline{S}_{BC}\ \overline{U}_{AC} \ (|0\rangle_A \otimes |\beta^\perp\rangle_B \otimes |\gamma^\perp\rangle_C) \\
&= \sqrt{r}\ \overline{S}_{BC}\ \overline{U}_{AC}\ \overline{S}_{BC}\ \overline{S}_{BC} \ (|0\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C) \ + \\
&\quad \sqrt{1-r}\ \overline{S}_{BC}\ \overline{U}_{AC}\ \overline{S}_{BC}\ \overline{S}_{BC} \ (|0\rangle_A \otimes |\beta^\perp\rangle_B \otimes |\gamma^\perp\rangle_C) \\
&= \sqrt{r}\ \overline{U}_{AB} \ (|0\rangle_A \otimes |\gamma\rangle_B \otimes |\beta\rangle_C) \ + \ \sqrt{1-r}\ \overline{U}_{AB} \ (|0\rangle_A \otimes |\gamma^\perp\rangle_B \otimes |\beta^\perp\rangle_C) \\
&= (\sqrt{r}\ U_{AB} \ (|0\rangle_A \otimes |\gamma\rangle_B)) \otimes |\beta\rangle_C \ + \ (\sqrt{1-r}\ U_{AB} \ (|0\rangle_A \otimes |\gamma^\perp\rangle_B)) \otimes |\beta^\perp\rangle_C
\end{aligned}$$

In the first step, we use Lemma A.10. In the second step, we use the above equation for $|w\rangle_{BC}$. In the third step, we use the equation for $|0\rangle_A \otimes |w\rangle_{BC}$ above. In the sixth step, we use the definition of $\overline{U}_{AC}$ and Lemma A.10.

From this and that $|\beta\rangle, |\beta^\perp\rangle$ are linearly independent and Lemma A.16, we get

$$\begin{aligned}
\sqrt{r}\ U \ (|0\rangle \otimes |\gamma\rangle) &= |0\rangle \otimes |\psi\rangle \\
\sqrt{1-r}\ U \ (|0\rangle \otimes |\gamma^\perp\rangle) &= |0\rangle \otimes |\varphi\rangle
\end{aligned}$$

Now we use $0 < r < 1$ and get:

$$\begin{aligned}
U \ (|0\rangle \otimes |\gamma\rangle) &= |0\rangle \otimes \frac{1}{\sqrt{r}}\ |\psi\rangle \\
U \ (|0\rangle \otimes |\gamma^\perp\rangle) &= |0\rangle \otimes \frac{1}{\sqrt{1-r}}\ |\varphi\rangle
\end{aligned}$$

From the above and Lemma A.17 we have that U is of the form $U = |0\rangle\langle 0| \otimes P_0 \ + \ |1\rangle\langle 1| \otimes P_1$, as required. □

A.6. Tensor products

We will prove seven lemmas about tensor products. First, we will give a necessary and sufficient condition for a vector to be a tensor product (Lemma A.20), we will state conditions under which applying a unitary to two or three qubits is a tensor product

(Lemma A.21 and Lemma A.22), and we will characterize a space that consists entirely of tensor products (Lemma A.23). We also show a case where a controlled unitary turns out to control two tensor products (Lemma A.24), and two cases of deriving conclusions from information about a unitary mapping some tensor products to other tensor products (Lemma A.25 and Lemma A.26).

Lemma A.20. *Suppose* $|w\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ *is a 4-dimensional unit vector where* $a_{00}, a_{01}, a_{10}, a_{11}$ *are complex numbers. Now,* $|w\rangle$ *is a tensor product if and only if* $a_{00}a_{11} = a_{01}a_{10}$.

Proof.

$$
\begin{aligned}
&|w\rangle \text{ is a tensor product} \\
&\iff |w\rangle \;=\; |\psi\rangle \otimes |\varphi\rangle, \text{ for some } |\psi\rangle \text{ and } |\varphi\rangle \\
&\iff \begin{pmatrix} a_{00} \\ a_{01} \end{pmatrix} = b_0|\varphi\rangle \;\;\wedge\;\; \begin{pmatrix} a_{10} \\ a_{11} \end{pmatrix} = b_1|\varphi\rangle, \text{ for some unit vector } b_0|0\rangle + b_1|1\rangle \text{ and } |\varphi\rangle \\
&\iff \left[\exists c: \; \begin{pmatrix} a_{00} \\ a_{01} \end{pmatrix} \;=\; c \begin{pmatrix} a_{10} \\ a_{11} \end{pmatrix}\right] \;\vee\; (a_{10} = a_{11} = 0) \\
&\iff [\exists c: \; a_{00} = ca_{10} \;\wedge\; a_{01} = ca_{11}] \;\vee\; (a_{10} = a_{11} = 0) \\
&\iff a_{00}a_{11} \;=\; a_{01}a_{10}
\end{aligned}
$$

In the fifth step, in the right-to-left direction, we assume $a_{00}a_{11} \;=\; a_{01}a_{10}$ and we consider three cases. First, if $a_{10} = a_{11} = 0$, then that is a separate disjunct in the conclusion. Second, if $a_{10} = 0$ and $a_{11} \neq 0$, then we define $c = \frac{a_{01}}{a_{11}}$. Now, $a_{00} = \frac{a_{01}a_{10}}{a_{11}} = ca_{10}$ and $a_{01} = \frac{a_{01}}{a_{11}}a_{11} = ca_{11}$. Third, if $a_{10} \neq 0$, then we define $c = \frac{a_{00}}{a_{10}}$. Now, $a_{00} = \frac{a_{00}}{a_{10}}a_{10} = ca_{10}$ and $a_{01} = \frac{a_{00}a_{11}}{a_{10}} = ca_{11}$. □

Lemma A.21. *For a 2-qubit unitary* U*, there exists a qubit* $|\psi\rangle$ *such that* $U(|0\rangle \otimes |\psi\rangle)$ *is a tensor product.*

Proof. Suppose

$$
\begin{aligned}
U|00\rangle &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \\
U|01\rangle &= b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle
\end{aligned}
$$

Let $|\psi\rangle = p|0\rangle + q|1\rangle$ be a qubit and let us calculate

$$
\begin{aligned}
U(|0\rangle \otimes |\psi\rangle) &= U(|0\rangle \otimes (p|0\rangle + q|1\rangle)) \\
&= pU|00\rangle + qU|01\rangle \\
&= p(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) + \\
&\quad q(b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle)
\end{aligned}
$$

$$= (pa_{00} + qb_{00})|00\rangle + (pa_{01} + qb_{01})|01\rangle + (pa_{10} + qb_{10})|10\rangle + (pa_{11} + qb_{11})|11\rangle$$

From this and Lemma A.20, we have that $U(|0\rangle \otimes |\psi\rangle)$ is a tensor product if and only if

$$(pa_{00} + qb_{00})\ (pa_{11} + qb_{11}) = (pa_{01} + qb_{01})\ (pa_{10} + qb_{10})$$

We can rearrange the above equation to get:

$$p^2\ (a_{00}a_{11} - a_{01}a_{10})\ + pq\ (a_{00}b_{11} + a_{11}b_{00} - a_{01}b_{10} - a_{10}b_{01}) + q^2\ (b_{00}b_{11} - b_{01}b_{10}) = 0$$

Now we have two cases.

First, if $U|00\rangle$ is a tensor product, then we pick $|\psi\rangle = |0\rangle$, which satisfies the lemma.

Second, if $U|00\rangle$ is not a tensor product, then from $U|00\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ and Lemma A.20, we have that $a_{00}a_{11} - a_{01}a_{10} \neq 0$. Now we pick $q = 1$ and use it to rewrite the above equation to the following equation with the single unknown p:

$$p^2\ (a_{00}a_{11} - a_{01}a_{10})\ + p\ (a_{00}b_{11} + a_{11}b_{00} - a_{01}b_{10} - a_{10}b_{01}) + (b_{00}b_{11} - b_{01}b_{10}) = 0$$

Notice that since $a_{00}a_{11} - a_{01}a_{10} \neq 0$, we have from the quadratic formula that this equation has a solution p_0 given by

$$\begin{aligned} p_0 &= \frac{1}{2a}(-b + \sqrt{b^2 - 4ac}) \qquad \text{where} \\ a &= a_{00}a_{11} - a_{01}a_{10} \\ b &= a_{00}b_{11} + a_{11}b_{00} - a_{01}b_{10} - a_{10}b_{01} \\ c &= b_{00}b_{11} - b_{01}b_{10} \end{aligned}$$

Thus, we have the following solution to the original equation:

$$p_1 = p_0 \qquad q_1 = 1$$

Notice that for any nonzero complex number c, we can scale to a different solution:

$$p_2 = cp_0 \qquad q_2 = c$$

This is a solution because $p_2^2 = c^2p_1^2$ and $p_2q_2 = c^2p_1q_1$ and $q_2^2 = c^2q_1^2$. Thus, each of the three items of the sum in the original equation gets scaled by c^2.

Now we can pick $c_0 = 1/\sqrt{|p_0|^2 + 1}$ and get the following solution:

$$p_3 = c_0p_0 \qquad q_3 = c_0$$

Notice that $|\psi_0\rangle = c_0p_0|0\rangle + c_0|1\rangle$ is a unit vector. Thus we pick $|\psi_0\rangle$, which satisfies the lemma. □

Lemma A.22. *For a 2-qubit unitary U and qubits $|\alpha\rangle, |\beta\rangle, |\gamma\rangle, |\psi\rangle$ and a 4-dimensional unit vector $|\varphi\rangle_{BC}$, if $\overline{U}_{AC}\ (|\alpha\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C) = |\psi\rangle_A \otimes |\varphi\rangle_{BC}$, then there exists a qubit $|w\rangle$ such that $|\varphi\rangle_{BC}$ is a tensor product of the form $|\varphi\rangle_{BC} = |\beta\rangle_B \otimes |w\rangle_C$.*

Proof. From $\overline{U}_{AC}\ (|\alpha\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C) = |\psi\rangle_A \otimes |\varphi\rangle_{BC}$, we will, on each side, form the outer product with itself:

$$\overline{U}_{AC}\ (|\alpha\rangle_A \otimes |\beta\rangle_B \otimes |\gamma\rangle_C)\ (\langle\alpha|_A \otimes \langle\beta|_B \otimes \langle\gamma|_C)\ \overline{U}^{\dagger}_{AC} = (|\psi\rangle_A \otimes |\varphi\rangle_{BC})\ (\langle\psi|_A \otimes \langle\varphi|_{BC})$$

after which we trace out qubits A and C on both sides and get

$$|\beta\rangle\langle\beta| = tr_C(|\varphi\rangle\langle\varphi|) \tag{A.1}$$

Let $|\beta^{\perp}\rangle$ be a qubit that is orthogonal to $|\beta\rangle$. From Lemma A.15 we have vectors $|w\rangle, |z\rangle$ such that

$$|\varphi\rangle = |\beta\rangle \otimes |w\rangle\ +\ |\beta^{\perp}\rangle \otimes |z\rangle \tag{A.2}$$

We calculate

$$\begin{aligned}
|\beta\rangle\langle\beta| &= tr_C(|\varphi\rangle\langle\varphi|) \\
&= tr_C((|\beta\rangle \otimes |w\rangle\ +\ |\beta^{\perp}\rangle \otimes |z\rangle)\ (\langle\beta| \otimes \langle w|\ +\ \langle\beta^{\perp}| \otimes \langle z|)) \\
&= tr_C(|\beta\rangle\langle\beta| \otimes |w\rangle\langle w|\ +\ |\beta\rangle\langle\beta^{\perp}| \otimes |w\rangle\langle z|\ + \\
&\qquad |\beta^{\perp}\rangle\langle\beta| \otimes |z\rangle\langle w|\ +\ |\beta^{\perp}\rangle\langle\beta^{\perp}| \otimes |z\rangle\langle z|) \\
&= |\beta\rangle\langle\beta|\ \langle w|w\rangle\ +\ |\beta\rangle\langle\beta^{\perp}|\ \langle z|w\rangle\ +\ |\beta^{\perp}\rangle\langle\beta|\ \langle w|z\rangle\ +\ |\beta^{\perp}\rangle\langle\beta^{\perp}|\ \langle z|z\rangle
\end{aligned}$$

In the first step, we use Equation (A.1). In the second step, we use Equation (A.2). In the fourth step, we use Lemma A.7 and Lemma A.2.

Now we multiply with $\langle\beta^{\perp}|$ from the left and with $|\beta^{\perp}\rangle$ from the right and we get:

$$0 = \langle z|z\rangle$$

from which we get $|z\rangle = \mathbf{0}$. From this and Equation (A.2), we have

$$|\varphi\rangle = |\beta\rangle \otimes |w\rangle\ +\ |\beta^{\perp}\rangle \otimes |z\rangle\ \ =\ \ |\beta\rangle \otimes |w\rangle$$

and from that $|\varphi\rangle$ and $|\beta\rangle$ are unit vectors, we get that $|w\rangle$ is a unit vector. □

Lemma A.23. *For a 2-qubit unitary U, if $\forall|x\rangle : U\ (|x\rangle \otimes |0\rangle)$ is a tensor product, then either*
$\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : U\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$, *or*
$\exists|\psi\rangle : \forall|x\rangle : \exists|z\rangle : U\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$.

Proof. Let

$$\begin{aligned} U\ (|0\rangle \otimes |0\rangle) &= |\alpha_0\rangle \otimes |\beta_0\rangle \\ U\ (|1\rangle \otimes |0\rangle) &= |\alpha_1\rangle \otimes |\beta_1\rangle \\ U\ (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle) &= |\alpha_+\rangle \otimes |\beta_+\rangle \end{aligned}$$

where $|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_+\rangle, |\beta_0\rangle, |\beta_1\rangle, |\beta_+\rangle$ are qubits. We will show that

$$\text{either } |\alpha_0\rangle \text{ and } |\alpha_1\rangle \text{ are linearly dependent, or } |\beta_0\rangle \text{ and } |\beta_1\rangle \text{ are linearly dependent.} \tag{A.3}$$

We calculate

$$\begin{aligned} U\ (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle) &= \frac{1}{\sqrt{2}}(U(|0\rangle \otimes |0\rangle) + U(|1\rangle \otimes |0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|\alpha_0\rangle \otimes |\beta_0\rangle + |\alpha_1\rangle \otimes |\beta_1\rangle) \end{aligned}$$

From the above two equations for $U\ (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle)$, we see that

$$|\alpha_+\rangle \otimes |\beta_+\rangle = \frac{1}{\sqrt{2}}(|\alpha_0\rangle \otimes |\beta_0\rangle + |\alpha_1\rangle \otimes |\beta_1\rangle) \tag{A.4}$$

Now we pick a qubit $|\beta_0^\perp\rangle$ such that $|\beta_0\rangle$ and $|\beta_0^\perp\rangle$ are orthogonal. Next we multiply on the left with $I \otimes \langle\beta_0^\perp|$ on both sides of Equation (A.4) and we get:

$$(I \otimes \langle\beta_0^\perp|)\ (|\alpha_+\rangle \otimes |\beta_+\rangle) = (I \otimes \langle\beta_0^\perp|)\ (\frac{1}{\sqrt{2}}(|\alpha_0\rangle \otimes |\beta_0\rangle + |\alpha_1\rangle \otimes |\beta_1\rangle))$$

We can simplify both sides of the above equation and get:

$$\langle\beta_0^\perp|\beta_+\rangle\ |\alpha_+\rangle = \frac{1}{\sqrt{2}}\langle\beta_0^\perp|\beta_1\rangle\ |\alpha_1\rangle$$

From the above equation we see that either $|\alpha_+\rangle$ and $|\alpha_1\rangle$ are linearly dependent, or $\langle\beta_0^\perp|\beta_+\rangle = \frac{1}{\sqrt{2}}\langle\beta_0^\perp|\beta_1\rangle = 0$. Let us consider those two cases in turn.

In the first case, if $|\alpha_+\rangle$ and $|\alpha_1\rangle$ are linearly dependent, then we use Equation (A.4) and Lemma A.16 to get that $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are linearly dependent.

In the second case, if $\langle\beta_0^\perp|\beta_+\rangle = \frac{1}{\sqrt{2}}\langle\beta_0^\perp|\beta_1\rangle = 0$, then we have that $|\beta_0^\perp\rangle$ and $|\beta_1\rangle$ are orthogonal, which together with that $|\beta_0^\perp\rangle$ and $|\beta_0\rangle$ are orthogonal gives that $|\beta_0\rangle$ and $|\beta_1\rangle$ are linearly dependent.

This means that we have proved Equation (A.3).

Now we have two cases. In the first case, if $|\alpha_0\rangle$ and $|\alpha_1\rangle$ are linearly dependent, then they are proportional. Thus, we can pick $|\psi\rangle = |\alpha_0\rangle$ and find a constant c and write:

$$|\alpha_1\rangle \otimes |\beta_1\rangle = (c\ |\alpha_0\rangle) \otimes |\beta_1\rangle \quad = \quad |\alpha_0\rangle \otimes (c\ |\beta_1\rangle)$$

In the second case, if $|\beta_0\rangle$ and $|\beta_1\rangle$ are linearly dependent, then they are proportional. Thus, we can pick $|\psi\rangle = |\beta_0\rangle$ and find a constant c and write:

$$|\alpha_1\rangle \otimes |\beta_1\rangle = |\alpha_1\rangle \otimes (c\ |\beta_0\rangle) \quad = \quad (c\ |\alpha_1\rangle) \otimes |\beta_0\rangle$$

Thus, in both cases we have shown that $|\alpha_1\rangle \otimes |\beta_1\rangle$ is of the required form. □

Lemma A.24. *For 2-qubit unitaries 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 unitaries.

Proof. From Lemma A.21 we have that we can pick qubits $|\psi_0\rangle, |\alpha_0\rangle, |\beta_0\rangle$ such that

$$V\ (|0\rangle \otimes |\psi_0\rangle) = |\alpha_0\rangle \otimes |\beta_0\rangle$$

We can also pick a 1-qubit unitary P such that

$$P\ |\alpha_0\rangle = |0\rangle$$

We calculate, for any qubit $|\gamma\rangle$:

$$\begin{aligned}
&\overline{U}_{AC}\ (P^\dagger \otimes I \otimes I)\ (|0\rangle \otimes |\beta_0\rangle \otimes |\gamma\rangle) \\
&= \overline{U}_{AC}\ (P^\dagger \otimes I \otimes I)\ (P \otimes I \otimes I)\ \overline{V}_{AB}\ (|0\rangle \otimes |\psi_0\rangle \otimes |\gamma\rangle) \\
&= \overline{U}_{AC}\ \overline{V}_{AB}\ (|0\rangle \otimes |\psi_0\rangle \otimes |\gamma\rangle) \\
&= |0\rangle \otimes (W_0\ (|\psi_0\rangle \otimes |\gamma\rangle))
\end{aligned}$$

In the first step, we use the above properties of P and V. In the second step, we use that $(P^\dagger \otimes I \otimes I)$ and $(P \otimes I \otimes I)$ cancel out. In the third step, we use the assumption of the lemma.

We have that $\overline{U}_{AC}\ (P^\dagger \otimes I \otimes I)$ has no effect on the B qubit so we can focus on the A and C qubits and get that, for any qubit $|\gamma\rangle$ there exists a qubit $|w\rangle$ such that

$$U\ (P^\dagger \otimes I)\ (|0\rangle \otimes |\gamma\rangle) = |0\rangle \otimes |w\rangle$$

We can pick orthogonal qubits $|\gamma_1\rangle, |\gamma_2\rangle$ and use the above to observe that there exist qubits $|w_1\rangle, |w_2\rangle$ such that:

$$U\ (P^\dagger \otimes I)\ (|0\rangle \otimes |\gamma_1\rangle) = |0\rangle \otimes |w_1\rangle$$
$$U\ (P^\dagger \otimes I)\ (|0\rangle \otimes |\gamma_2\rangle) = |0\rangle \otimes |w_2\rangle$$

From this and Lemma A.17 we have that $U\ (P^\dagger \otimes I)$ is of the following form, where Q_0, Q_1 are 1-qubit unitaries:

$$U\ (P^\dagger \otimes I) = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$$

From this we derive

$$\overline{U}_{AC}\ (P^\dagger \otimes I \otimes I) = |0\rangle\langle 0| \otimes I \otimes Q_0 + |1\rangle\langle 1| \otimes I \otimes Q_1 \tag{A.5}$$

From the assumption of the lemma, we have:

$$\overline{U}_{AC}\ (P^\dagger \otimes I \otimes I)\ (P \otimes I \otimes I)\ \overline{V}_{AB} = |0\rangle\langle 0| \otimes W_0\ +\ |1\rangle\langle 1| \otimes W_1$$

From this we derive:

$$\begin{aligned}
(P \otimes I \otimes I)\ \overline{V}_{AB} &= (\overline{U}_{AC}\ (P^\dagger \otimes I \otimes I))^\dagger\ (|0\rangle\langle 0| \otimes W_0\ +\ |1\rangle\langle 1| \otimes W_1) \\
&= (|0\rangle\langle 0| \otimes I \otimes Q_0\ +\ |1\rangle\langle 1| \otimes I \otimes Q_1)^\dagger\ (|0\rangle\langle 0| \otimes W_0\ +\ |1\rangle\langle 1| \otimes W_1) \\
&= (|0\rangle\langle 0| \otimes I \otimes Q_0^\dagger\ +\ |1\rangle\langle 1| \otimes I \otimes Q_1^\dagger)\ (|0\rangle\langle 0| \otimes W_0\ +\ |1\rangle\langle 1| \otimes W_1) \\
&= |0\rangle\langle 0| \otimes (I \otimes Q_0^\dagger)\ W_0\ +\ |1\rangle\langle 1| \otimes (I \otimes Q_1^\dagger)\ W_1
\end{aligned}$$

In the second step, we use Equation (A.5).

We have that $(P \otimes I \otimes I)\ \overline{V}_{AB}$ has no effect on the C qubit so we can focus on the A and B qubits and get that $(P \otimes I \otimes I)\ \overline{V}_{AB}$ is of the following form, where P_0, P_1 are 1-qubit unitaries:

$$(P \otimes I \otimes I)\ \overline{V}_{AB} = |0\rangle\langle 0| \otimes P_0 \otimes I + |1\rangle\langle 1| \otimes P_1 \otimes I \tag{A.6}$$

We calculate:

$$\begin{aligned}
\overline{U}_{AC}\ \overline{V}_{AB} &= \overline{U}_{AC}\ (P^\dagger \otimes I \otimes I)\ (P \otimes I \otimes I)\ \overline{V}_{AB} \\
&= (|0\rangle\langle 0| \otimes I \otimes Q_0 + |1\rangle\langle 1| \otimes I \otimes Q_1)\ (|0\rangle\langle 0| \otimes P_0 \otimes I + |1\rangle\langle 1| \otimes P_1 \otimes I) \\
&= |0\rangle\langle 0| \otimes P_0 \otimes Q_0\ +\ |1\rangle\langle 1| \otimes P_1 \otimes Q_1
\end{aligned}$$

In the second step, we use Equation (A.5) and Equation (A.6). □

Lemma A.25. *For a 2-qubit unitary V and a qubit $|\psi\rangle$, for which*

$$\forall\ |x\rangle : \exists\ |\varphi\rangle : V\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\varphi\rangle$$

there exists a 1-qubit unitary Q such that

$$\forall\ |x\rangle :\ V\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes (Q\ |x\rangle)$$

Proof. Let $|w_0\rangle$ and $|w_1\rangle$ be unit vectors that exist according to the assumption of the lemma:

$$V\ (|0\rangle \otimes |0\rangle) = |\psi\rangle \otimes |w_0\rangle$$
$$V\ (|1\rangle \otimes |0\rangle) = |\psi\rangle \otimes |w_1\rangle$$

Notice that $(|0\rangle \otimes |0\rangle)$ and $(|1\rangle \otimes |0\rangle)$ are orthogonal and that V is a unitary so it preserves orthogonality, which implies that $|\psi\rangle \otimes |w_0\rangle$ and $|\psi\rangle \otimes |w_1\rangle$ are orthogonal, which implies that $|w_0\rangle$ and $|w_1\rangle$ are orthogonal.

Define a 1-qubit unitary Q:

$$Q = |w_0\rangle\langle 0|\ +\ |w_1\rangle\langle 1|$$

Notice that the columns of Q are orthogonal unit vectors, hence Q is a unitary matrix.

For any qubit $|x\rangle = a|0\rangle + b|1\rangle$, we calculate:

$$\begin{aligned}
Q\ |x\rangle &= (|w_0\rangle\langle 0|\ +\ |w_1\rangle\langle 1|)\ (a|0\rangle + b|1\rangle) \\
&= a|w_0\rangle + b|w_1\rangle \\
V\ (|x\rangle \otimes |0\rangle) &= V\ ((a|0\rangle + b|1\rangle) \otimes |0\rangle) \\
&= V\ (a|0\rangle \otimes |0\rangle\ +\ b|1\rangle \otimes |0\rangle) \\
&= V\ (a|0\rangle \otimes |0\rangle)\ +\ V\ (b|1\rangle \otimes |0\rangle) \\
&= (a|\psi\rangle \otimes |w_0\rangle)\ +\ (b|\psi\rangle \otimes |w_1\rangle) \\
&= |\psi\rangle \otimes ((a|w_0\rangle)\ +\ (b|w_1\rangle)) \\
&= |\psi\rangle \otimes (Q\ |x\rangle) \quad \square
\end{aligned}$$

Lemma A.26. *For a 2-qubit unitary U, if $\forall|z\rangle : \exists|\beta\rangle : U\ (|z\rangle \otimes |0\rangle) = |z\rangle \otimes |\beta\rangle$, then $\exists|\beta\rangle : \forall|z\rangle : U\ (|z\rangle \otimes |0\rangle) = |z\rangle \otimes |\beta\rangle$.*

Proof. Let us consider $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. We can use the assumption of the lemma to find $|\beta_0\rangle, |\beta_1\rangle, |\beta_+\rangle$ such that

$$U\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |\beta_0\rangle$$
$$U\ (|1\rangle \otimes |0\rangle) = |1\rangle \otimes |\beta_1\rangle$$
$$U\ (|+\rangle \otimes |0\rangle) = |+\rangle \otimes |\beta_+\rangle$$

Now we calculate $U\ (|+\rangle \otimes |0\rangle)$ twice.

First we do the calculation based on the first two properties above:

$$\begin{aligned} U\ (|+\rangle \otimes |0\rangle) &= U\ ((\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2}}\ U\ (|0\rangle \otimes |0\rangle)\ +\ \frac{1}{\sqrt{2}}\ U\ (|1\rangle \otimes |0\rangle) \\ &= \frac{1}{\sqrt{2}}\ |0\rangle \otimes |\beta_0\rangle\ +\ \frac{1}{\sqrt{2}}\ |1\rangle \otimes |\beta_1\rangle \end{aligned}$$

Second we do the calculation based on the third property above:

$$\begin{aligned} U\ (|+\rangle \otimes |0\rangle) &= |+\rangle \otimes |\beta_+\rangle \\ &= (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes |\beta_+\rangle \\ &= \frac{1}{\sqrt{2}}\ |0\rangle \otimes |\beta_+\rangle\ +\ \frac{1}{\sqrt{2}}\ |1\rangle \otimes |\beta_+\rangle \end{aligned}$$

From the two calculations of $U\ (|+\rangle \otimes |0\rangle)$ we have that

$$|\beta_0\rangle = |\beta_+\rangle$$
$$|\beta_1\rangle = |\beta_+\rangle$$

From those two properties we conclude $|\beta_0\rangle = |\beta_+\rangle = |\beta_1\rangle$.

Let $|w\rangle = c|0\rangle + d|1\rangle$ be a qubit. We calculate:

$$\begin{aligned} U\ (|w\rangle \otimes |0\rangle) &= U\ ((c|0\rangle + d|1\rangle) \otimes |0\rangle) \\ &= (c\ U\ (|0\rangle \otimes |0\rangle))\ +\ (d\ U\ (|1\rangle \otimes |0\rangle)) \\ &= c\ |0\rangle \otimes |\beta_0\rangle\ +\ d\ |1\rangle \otimes |\beta_1\rangle \\ &= c\ |0\rangle \otimes |\beta_+\rangle\ +\ d\ |1\rangle \otimes |\beta_+\rangle \\ &= (c|0\rangle\ +\ d|1\rangle) \otimes |\beta_+\rangle \\ &= |w\rangle \otimes |\beta_+\rangle \end{aligned}$$

Thus, $|\beta_+\rangle$ has the property that $\forall |z\rangle : U\ (|z\rangle \otimes |0\rangle) = |z\rangle \otimes |\beta_+\rangle$. □

A.7. Other properties

We will prove Lemma A.27 that we use in the proof of Lemma 4.3, and we will prove six other lemmas that we use in the proof of Lemma 6.4 (the second main lemma). All those lemmas are highly specific to the proof tasks that they support.

Lemma A.27. *For 2-qubit unitaries $V_1, V_2, V_3, V_4, U_0, U_1$ and 1-qubit unitaries P_0, P_1, if*

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = |0\rangle\langle 0| \otimes U_{0BC}\ +\ |1\rangle\langle 1| \otimes U_{1BC}$$
$$V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$$

then V_3 is of the following form, where Q_0, Q_1 are 1-qubit unitaries:

$$V_3 = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$$

Proof. We calculate:

$$\begin{aligned}
\overline{V}_{3AC} &= \overline{V}_{2BC}^{\dagger}\ \overline{V}_{1AC}^{\dagger}\ (|0\rangle\langle 0| \otimes U_{0BC}\ +\ |1\rangle\langle 1| \otimes U_{1BC})\ \overline{V}_{4BC}^{\dagger} \\
&= (|0\rangle\langle 0| \otimes V_{2BC}^{\dagger} + |1\rangle\langle 1| \otimes V_{2BC}^{\dagger}) \\
&\quad (|0\rangle\langle 0| \otimes I_B \otimes P_0^{\dagger} + |1\rangle\langle 1| \otimes I_B \otimes P_1^{\dagger}) \\
&\quad (|0\rangle\langle 0| \otimes U_{0BC} + |1\rangle\langle 1| \otimes U_{1BC}) \\
&\quad (|0\rangle\langle 0| \otimes V_{4BC}^{\dagger} + |1\rangle\langle 1| \otimes V_{4BC}^{\dagger}) \\
&= |0\rangle\langle 0| \otimes (V_{2BC}^{\dagger}\ (I_B \otimes P_0^{\dagger})\ U_{0BC}\ V_{4BC}^{\dagger})\ + \\
&\quad |1\rangle\langle 1| \otimes (V_{2BC}^{\dagger}\ (I_B \otimes P_1^{\dagger})\ U_{1BC}\ V_{4BC}^{\dagger}) \\
&= \begin{pmatrix} V_{2BC}^{\dagger}\ (I_B \otimes P_0^{\dagger})\ U_{0BC}\ V_{4BC}^{\dagger} & \mathbf{0} \\ \mathbf{0} & V_{2BC}^{\dagger}\ (I_B \otimes P_1^{\dagger})\ U_{1BC}\ V_{4BC}^{\dagger} \end{pmatrix}
\end{aligned}$$

We can write $\overline{V}_{3AC}$ in the following way:

$$\begin{aligned}
\overline{V}_{3AC} &= |0\rangle\langle 0| \otimes I_B \otimes Q_{00}\ +\ |0\rangle\langle 1| \otimes I_B \otimes Q_{01}\ + \\
&\quad |1\rangle\langle 0| \otimes I_B \otimes Q_{10}\ +\ |1\rangle\langle 1| \otimes I_B \otimes Q_{11} \\
&= \begin{pmatrix} I_B \otimes Q_{00} & I_B \otimes Q_{01} \\ I_B \otimes Q_{10} & I_B \otimes Q_{11} \end{pmatrix}
\end{aligned}$$

where $Q_{00}, Q_{01}, Q_{10}, Q_{11}$ are 2×2 matrices.

From the above two equations for $\overline{V}_{3AC}$, we conclude that V_{3AC} is of the form:

$$\begin{aligned}
\overline{V}_{3AC} &= |0\rangle\langle 0| \otimes I_B \otimes Q_{00}\ +\ |1\rangle\langle 1| \otimes I_B \otimes Q_{11} \\
&= S_{BC}\ (|0\rangle\langle 0| \otimes Q_{00} \otimes I_C\ +\ |1\rangle\langle 1| \otimes Q_{11} \otimes I_C)\ S_{BC} \\
&= S_{BC}\ (\ (|0\rangle\langle 0| \otimes Q_{00}\ +\ |1\rangle\langle 1| \otimes Q_{11}) \otimes I_C\ )\ S_{BC}
\end{aligned}$$

From this we see that $V_3 = |0\rangle\langle 0| \otimes Q_{00} \ + \ |1\rangle\langle 1| \otimes Q_{11}$, which is of the required form. In particular, since V_3 is unitary, Q_{00}, Q_{11} are unitaries. □

Lemma A.28 and Lemma A.29 each embodies a calculation that we need to do twice.

Lemma A.28. *For 2-qubit unitaries V_1, V_2, V_3, V_4 and 1-qubit unitary U, if $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(U)$ and $V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$, then, for any qubit $|x\rangle$:*

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) = \overline{V}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C)$$

Proof. We calculate, for any $|x\rangle$:

$$\begin{aligned}
&\overline{V}_{1AC}\ \overline{V}_{2BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= \overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= \overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ (\overline{V}_{4BC}\ \overline{V}_{4BC}^{\dagger})\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= (\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC})\ (\overline{V}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C)) \\
&= \mathsf{CC}(U)\ \overline{V}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= (|0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes \mathsf{C}(U))\ (|0\rangle_A \otimes (V_4^{\dagger}\ (|x\rangle_B \otimes |0\rangle_C))) \\
&= (|0\rangle_A \otimes (V_4^{\dagger}\ (|x\rangle_B \otimes |0\rangle_C))) \\
&= \overline{V}_{4BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C)
\end{aligned}$$

In the first step, we used the assumption $V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$. In the fourth step, we use the assumption $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{2BC}\ \overline{V}_{4BC} = \mathsf{CC}(\mathsf{Diag}(u_0, u_1))$ and in the fifth step we use the definition of $\mathsf{CC}(\mathsf{Diag}(u_0, u_1))$. □

Lemma A.29. *For 2-qubit unitaries V_1, V_2, V_3, V_4 and a 1-qubit unitary U, if $\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \mathsf{CC}(U)$ and $V_2\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$, then, for any qubit $|x\rangle$:*

$$\overline{V}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) = \overline{V}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)$$

Proof. We calculate, for any $|x\rangle$:

$$\begin{aligned}
&\mathsf{CC}(U^{\dagger}) \\
&= \overline{S}_{AB}\ \mathsf{CC}(U^{\dagger})\ \overline{S}_{AB} \\
&= \overline{S}_{AB}\ \mathsf{CC}(U)^{\dagger}\ \overline{S}_{AB} \\
&= \overline{S}_{AB}\ (\overline{V}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ \overline{V}_{2BC}^{\dagger}\ \overline{V}_{1AC}^{\dagger})\ \overline{S}_{AB} \\
&= \overline{S}_{AB}\ \overline{V}_{4BC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{3AC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{2BC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{1AC}^{\dagger}\ \overline{S}_{AB} \\
&= (\overline{S}_{AB}\ \overline{V}_{4BC}^{\dagger}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{V}_{3AC}^{\dagger}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{V}_{2BC}^{\dagger}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{V}_{1AC}^{\dagger}\ \overline{S}_{AB}) \\
&= \overline{V}_{4AC}^{\dagger}\ \overline{V}_{3BC}^{\dagger}\ \overline{V}_{2AC}^{\dagger}\ \overline{V}_{1BC}^{\dagger}
\end{aligned}$$

In the first step, we use Lemma A.13. In the third step, we use the assumption about $\mathsf{CC}(U)$. In the sixth step, we use Lemma A.12.

Notice that $V_2^\dagger\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$.

From the above two observations and Lemma A.28, we have for any qubit $|x\rangle$:

$$\overline{V}_{4AC}^{\dagger}\ \overline{V}_{3BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) = \overline{V}_{1BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \tag{A.7}$$

We calculate, for any $|x\rangle$:

$$\begin{aligned}
&\overline{V}_{4BC}^{\dagger}\ \overline{V}_{3AC}^{\dagger}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) \\
&= \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{4BC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ \overline{V}_{3AC}^{\dagger}\ \overline{S}_{AB}\ \overline{S}_{AB}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) \\
&= \overline{S}_{AB}\ (\overline{S}_{AB}\ \overline{V}_{4BC}^{\dagger}\ \overline{S}_{AB})\ (\overline{S}_{AB}\ \overline{V}_{3AC}^{\dagger}\ \overline{S}_{AB})\ \overline{S}_{AB}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C) \\
&= \overline{S}_{AB}\ \overline{V}_{4AC}^{\dagger}\ \overline{V}_{3BC}^{\dagger}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= \overline{S}_{AB}\ \overline{V}_{1BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= \overline{S}_{AB}\ \overline{V}_{1BC}\ \overline{S}_{AB}\ \overline{S}_{AB}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\
&= \overline{V}_{1AC}\ (|x\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C)
\end{aligned}$$

In the third step, we use Lemma A.10 and Lemma A.12. In the fourth step, we use Equation (A.7). In the sixth step, we use Lemma A.10 and Lemma A.12. □

Lemma A.30. *For 2-qubit unitaries V_1, V_2, V_3, V_4, for which*

$$\exists\ |\psi\rangle : \forall\ |x\rangle : \exists\ |z\rangle : V_2\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$$

there exist 2-qubit unitaries W_1, W_2, W_4 and a 1-qubit unitary P_2 such that

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \overline{W}_{1AC}\ \overline{W}_{2BC}\ \overline{V}_{3AC}\ \overline{W}_{4BC}$$
$$W_2 = I \otimes |0\rangle\langle 0| + P_2 \otimes |1\rangle\langle 1|$$

Proof. Let $|\psi\rangle$ be a unit vector that satisfies the assumption of the lemma and let $|\psi^\perp\rangle$ be a unit vector that is orthogonal to $|\psi\rangle$.

Let $|w_0\rangle$ and $|w_1\rangle$ be unit vectors that exist according to the assumption of the lemma:

$$V_2\ (|0\rangle \otimes |0\rangle) = |w_0\rangle \otimes |\psi\rangle$$
$$V_2\ (|1\rangle \otimes |0\rangle) = |w_1\rangle \otimes |\psi\rangle$$

Notice that $(|0\rangle \otimes |0\rangle)$ and $(|0\rangle \otimes |1\rangle)$ are orthogonal and that V_2 is a unitary so it preserves orthogonality, which implies that $(|w_0\rangle \otimes |\psi\rangle)$ and $(|w_1\rangle \otimes |\psi\rangle)$ are orthogonal, which implies that $|w_0\rangle$ and $|w_1\rangle$ are orthogonal.

Define 1-qubit unitaries P, Q and then 2-qubit unitaries W_1, W_2, W_4:

$$\begin{aligned}
P &= |\psi\rangle\langle 0| \ + \ |\psi^{\perp}\rangle\langle 1| \\
Q &= |w_0\rangle\langle 0| \ + \ |w_1\rangle\langle 1| \\
W_1 &= V_1 \ (I \otimes P) \\
W_2 &= (I \otimes P)^{\dagger} \ V_2 \ (Q \otimes I)^{\dagger} \\
W_4 &= (Q \otimes I) \ V_4
\end{aligned}$$

Notice that the columns of P are orthogonal unit vectors, and the columns of Q are orthogonal unit vectors, hence P, Q are unitary matrices. We calculate:

$$\begin{aligned}
\overline{W}_{1AC} \ \overline{W}_{2BC} \ \overline{V}_{3AC} \ \overline{W}_{4BC} &= \overline{S}_{BC} \ ((V_{1AB} \ (I_A \otimes P_B)) \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes ((I_B \otimes P_C)^{\dagger} \ V_{2BC} \ (Q_B \otimes I_C)^{\dagger})) \\
&\quad \overline{S}_{BC} \ (V_{3AB} \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes ((Q_B \otimes I_C) \ V_{4BC})) \\
&= \overline{S}_{BC} \ (V_{1AB} \otimes I_C) \ (I_A \otimes P_B \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes I_B \otimes P_C^{\dagger}) \ (I_A \otimes V_{2BC}) \ (I_A \otimes Q_B^{\dagger} \otimes I_C) \\
&\quad \overline{S}_{BC} \ (V_{3AB} \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes Q_B \otimes I_C) \ (I_A \otimes V_{4BC}) \\
&= \overline{S}_{BC} \ (V_{1AB} \otimes I_C) \ \overline{S}_{BC} \ \overline{S}_{BC} \ (I_A \otimes P_B \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes I_B \otimes P_C^{\dagger}) \ (I_A \otimes V_{2BC}) \ (I_A \otimes Q_B^{\dagger} \otimes I_C) \\
&\quad \overline{S}_{BC} \ (V_{3AB} \otimes I_C) \ \overline{S}_{BC} \\
&\quad (I_A \otimes Q_B \otimes I_C) \ (I_A \otimes V_{4BC}) \\
&= \overline{V}_{1AC} \ \overline{V}_{2BC} \ \overline{V}_{3AC} \ \overline{V}_{4BC}
\end{aligned}$$

For any qubit $|\varphi\rangle = a|0\rangle + b|1\rangle$, we calculate:

$$\begin{aligned}
V_2 \ (|\varphi\rangle \otimes |0\rangle) &= V_2 \ ((a|0\rangle + b|1\rangle) \otimes |0\rangle) \\
&= V_2 \ (a|0\rangle \otimes |0\rangle) \ + \ V_2 \ (b|1\rangle \otimes |0\rangle) \\
&= a|w_0\rangle \otimes |\psi\rangle \ + \ b|w_1\rangle \otimes |\psi\rangle \\
&= (a|w_0\rangle + b|w_1\rangle) \otimes |\psi\rangle \\
&= (a \ Q|0\rangle + b \ Q|1\rangle) \otimes |\psi\rangle \\
&= (Q \ (a|0\rangle + b|1\rangle)) \otimes |\psi\rangle \\
&= (Q \ |\varphi\rangle) \otimes |\psi\rangle \\
&= (Q \ |\varphi\rangle) \otimes (P \ |0\rangle)
\end{aligned}$$

For any qubit $|x\rangle$, we calculate:

$$\begin{aligned} W_2\ (|x\rangle \otimes |0\rangle) &= (I \otimes P^\dagger)\ V_2\ (Q^\dagger \otimes I)\ (|x\rangle \otimes |0\rangle) \\ &= (I \otimes P^\dagger)\ V_2\ (Q^\dagger\ |x\rangle \otimes |0\rangle) \\ &= (I \otimes P^\dagger)\ ((Q\ Q^\dagger\ |x\rangle) \otimes P\ |0\rangle) \\ &= (I \otimes P^\dagger)\ (|x\rangle \otimes P\ |0\rangle) \\ &= |x\rangle \otimes |0\rangle \end{aligned}$$

In the third step, we use the above equation for V_2.

From the above and Lemma A.18, we have that W_2 is of the form $W_2 = I \otimes |0\rangle\langle 0| + P_2 \otimes |1\rangle\langle 1|$, where P_2 is a 1-qubit unitary. □

Lemma A.31. *For 2-qubit unitaries V_1, V_2, V_3, V_4, for which*

$$\exists\ |\psi\rangle : \forall\ |x\rangle : \exists\ |z\rangle : V_3^\dagger\ (|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$$

there exist 2-qubit unitaries W_1, W_3, W_4 and a 1-qubit unitary P_3 such that

$$\begin{aligned} \overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} &= \overline{W}_{1AC}\ \overline{V}_{2BC}\ \overline{W}_{3AC}\ \overline{W}_{4BC} \\ W_3 &= I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1| \end{aligned}$$

Proof. We apply Lemma A.30 to $V_4^\dagger, V_3^\dagger, V_2^\dagger, V_1^\dagger$, and we get that there exist 2-qubit unitaries W_4, W_3, W_1 and a 1-qubit unitary P_3 such that

$$\begin{aligned} \overline{V}_{4AC}^{\ \dagger}\ \overline{V}_{3BC}^{\ \dagger}\ \overline{V}_{2AC}^{\ \dagger}\ \overline{V}_{1BC}^{\ \dagger} &= \overline{W}_{4AC}\ \overline{W}_{3BC}\ \overline{V}_{2AC}^{\ \dagger}\ \overline{W}_{1BC} \\ W_3 &= I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1| \end{aligned}$$

From those two equations, we get

$$\begin{aligned} \overline{V}_{1BC}\ \overline{V}_{2AC}\ \overline{V}_{3BC}\ \overline{V}_{4AC} &= \overline{W}_{1BC}^{\ \dagger}\ \overline{V}_{2AC}\ \overline{W}_{3BC}^{\ \dagger}\ \overline{W}_{4AC}^{\ \dagger} \\ W_3^\dagger &= I \otimes |0\rangle\langle 0| + P_3^\dagger \otimes |1\rangle\langle 1| \end{aligned}$$

From the first of those two those equations, we get

$$S_{AB}\ \overline{V}_{1BC}\ \overline{V}_{2AC}\ \overline{V}_{3BC}\ \overline{V}_{4AC}\ S_{AB} = S_{AB}\ \overline{W}_{1BC}^{\ \dagger}\ \overline{V}_{2AC}\ \overline{W}_{3BC}^{\ \dagger}\ \overline{W}_{4AC}^{\ \dagger}\ S_{AB}$$

In the above equation, we add the identity matrix, in the form of $(S_{AB}\ S_{AB})$, in six places and get:

$$\begin{aligned} &S_{AB}\ \overline{V}_{1BC}\ (S_{AB}\ S_{AB})\ \overline{V}_{2AC}\ (S_{AB}\ S_{AB})\ \overline{V}_{3BC}\ (S_{AB}\ S_{AB})\ \overline{V}_{4AC}\ S_{AB} \\ = &\ S_{AB}\ \overline{W}_{1BC}^{\ \dagger}\ (S_{AB}\ S_{AB})\ \overline{V}_{2AC}\ (S_{AB}\ S_{AB})\ \overline{W}_{3BC}^{\ \dagger}\ (S_{AB}\ S_{AB})\ \overline{W}_{4AC}^{\ \dagger}\ S_{AB} \end{aligned}$$

Finally we use that matrix multiplication is associative and Lemma A.12 and get that

$$\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} = \overline{W}_{1AC}^{\dagger}\ \overline{V}_{2BC}\ \overline{W}_{3AC}^{\dagger}\ \overline{W}_{4BC}^{\dagger}$$

as required. □

Lemma A.32. *For 2-qubit unitaries U_1, U_2, U_3, U_4, there exist 2-qubit unitaries V_1, V_2, V_3, V_4 such that*

$$\overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} = \overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC}$$
$$V_3\ (|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$$

Proof. From Lemma A.21 applied to U_3, we have that there exists a qubit $|w\rangle$ and that there exists qubits $|\psi\rangle, |\varphi\rangle$ such that

$$U_3\ (|0\rangle \otimes |w\rangle) = |\psi\rangle \otimes |\varphi\rangle$$

Let $|\psi^{\perp}\rangle_A$ be a unit vector that is orthogonal to $|\psi\rangle_A$, let $|\varphi^{\perp}\rangle_C$ be a unit vector that is orthogonal to $|\varphi\rangle_C$, and let $|w^{\perp}\rangle_C$ be a unit vector that is orthogonal to $|w\rangle_C$. Define 2-qubit unitaries W_0, W_1, W_2 and then 2-qubit unitaries V_1, V_2, V_3, V_4:

$$\begin{aligned}
W_0 &= |\psi\rangle\langle 0| \ + \ |\psi^{\perp}\rangle\langle 1| \\
W_1 &= |\varphi\rangle\langle 0| \ + \ |\varphi^{\perp}\rangle\langle 1| \\
W_2 &= |w\rangle\langle 0| \ + \ |w^{\perp}\rangle\langle 1| \\
V_1 &= U_1\ (W_0 \otimes I) \\
V_2 &= U_2\ (I \otimes W_1) \\
V_3 &= (W_0 \otimes W_1)^{\dagger}\ U_3\ (I \otimes W_2) \\
V_4 &= (I \otimes W_2^{\dagger})\ U_4
\end{aligned}$$

Notice that the columns of W_0 are orthogonal unit vectors, the columns of W_1 are orthogonal unit vectors, and the columns of W_2 are orthogonal unit vectors. Hence W_0, W_1, W_2 are unitary matrices. Now we can check that the two desired properties hold, as follows.

$$\begin{aligned}
&\overline{V}_{1AC}\ \overline{V}_{2BC}\ \overline{V}_{3AC}\ \overline{V}_{4BC} \\
&= \overline{S}_{BC}\ ((U_{1AB}\ (W_0 \otimes I_B)) \otimes I_C)\ \overline{S}_{BC} \\
&\qquad (I_A \otimes (U_{2BC}\ (I_B \otimes W_1))) \\
&\qquad\quad \overline{S}_{BC}\ (((W_0 \otimes W_1)^{\dagger}\ U_{3AB}\ (I_A \otimes W_2)) \otimes I_C)\ \overline{S}_{BC} \\
&\qquad\qquad (I_A \otimes ((I_B \otimes W_2^{\dagger})\ U_{4BC}))
\end{aligned}$$

$$
\begin{aligned}
&= \overline{S}_{BC}\ ((U_{1AB} \otimes I_C)\ (W_0 \otimes I_B \otimes I_C))\ \overline{S}_{BC} \\
&\quad ((I_A \otimes U_{2BC})\ (I_A \otimes I_B \otimes W_1)) \\
&\quad\quad \overline{S}_{BC}\ ((W_0^\dagger \otimes W_1^\dagger \otimes I_C)\ (U_{3AB} \otimes I_C)\ (I_A \otimes W_2 \otimes I_C))\ \overline{S}_{BC} \\
&\quad\quad\quad ((I_A \otimes I_B \otimes W_2^\dagger)\ (I_A \otimes U_{4BC})) \\
&= \overline{S}_{BC}\ ((U_{1AB} \otimes I_C)\ \overline{S}_{BC}\ \overline{S}_{BC}\ (W_0 \otimes I_B \otimes I_C))\ \overline{S}_{BC} \\
&\quad ((I_A \otimes U_{2BC})\ (I_A \otimes I_B \otimes W_1)) \\
&\quad\quad \overline{S}_{BC}\ ((W_0^\dagger \otimes W_1^\dagger \otimes I_C)\ \overline{S}_{BC}\ \overline{S}_{BC}\ (U_{3AB} \otimes I_C)\ \overline{S}_{BC}\ \overline{S}_{BC}\ (I_A \otimes W_2 \otimes I_C))\ \overline{S}_{BC} \\
&\quad\quad\quad ((I_A \otimes I_B \otimes W_2^\dagger)\ (I_A \otimes U_{4BC})) \\
&= \overline{U}_{1AC}\ (W_0 \otimes I_B \otimes I_C)) \\
&\quad \overline{U}_{2BC}\ (I_A \otimes I_B \otimes W_1)) \\
&\quad\quad ((W_0^\dagger \otimes I_B \otimes W_1^\dagger)\ \overline{U}_{3AC}\ (I_A \otimes I_B \otimes W_2)) \\
&\quad\quad\quad ((I_A \otimes I_B \otimes W_2^\dagger)\ \overline{U}_{4BC}) \\
&= \overline{U}_{1AC}\ \overline{U}_{2BC}\ (W_0 \otimes I_B \otimes I_C)\ (W_0^\dagger \otimes I_B \otimes I_C)\ \overline{U}_{3AC}\ \overline{U}_{4BC} \\
&= \overline{U}_{1AC}\ \overline{U}_{2BC}\ \overline{U}_{3AC}\ \overline{U}_{4BC} \\
&\quad V_3\ (|0\rangle \otimes |0\rangle) \\
&= (W_0 \otimes W_1)^\dagger\ U_3\ (I \otimes W_2)\ (|0\rangle \otimes |0\rangle) \\
&= (W_0 \otimes W_1)^\dagger\ U_3\ (|0\rangle \otimes |w\rangle) \\
&= (W_0 \otimes W_1)^\dagger\ (|\psi\rangle \otimes |\varphi\rangle) \\
&= |0\rangle \otimes |0\rangle \quad \square
\end{aligned}
$$

Lemma A.33. *For 2-qubit unitaries V_1, V_2, V_4, if*

$$\forall |x\rangle_C : \overline{V}_{1AC}\ \overline{V}_{2BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) = V_{4BC}^\dagger\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \tag{A.8}$$

$$\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V_2\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle \tag{A.9}$$

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

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

Proof. From Equation (A.9) and Lemma A.25 we have that we can find a 1-qubit unitary Q_0 such that, for any qubit $|x\rangle$:

$$V_2\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes (Q_0\ |x\rangle) \tag{A.10}$$

We calculate, for any qubit $|x\rangle$:

$$\begin{aligned}\overline{V}_{1AC}\ (|0\rangle_A \otimes |\psi\rangle_B \otimes (Q_0\ |x\rangle_C)) &= \overline{V}_{1AC}\ (|0\rangle_A \otimes (V_{2BC}\ (|x\rangle_B \otimes |0\rangle_C))) \\ &= V_4^\dagger{}_{BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C)\end{aligned}$$

In the first step, we use Equation (A.10) and in the second step we use Equation (A.8). From the above equation and Lemma A.22, we have:

$$\forall\ |x\rangle : \exists |w\rangle : V_4^\dagger\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |w\rangle$$

From this and Lemma A.25 we have that we can find a unitary Q_1 such that, for any qubit $|x\rangle$:

$$V_4^\dagger\ (|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes (Q_1\ |x\rangle) \tag{A.11}$$

Now we can continue the above calculation:

$$\begin{aligned}\overline{V}_{1AC}\ (|0\rangle_A \otimes |\psi\rangle_B \otimes (Q_0\ |x\rangle_C)) &= V_4^\dagger{}_{BC}\ (|0\rangle_A \otimes |x\rangle_B \otimes |0\rangle_C) \\ &= |0\rangle_A \otimes |\psi\rangle_B \otimes (Q_1\ |x\rangle_C)\end{aligned}$$

In the second step, we use Equation (A.11). We can pick orthogonal qubits $|x_0\rangle$ and $|x_0^\perp\rangle$ and calculate:

$$\begin{aligned}V_1\ (|0\rangle \otimes (Q_0\ |x_0\rangle)) &= |0\rangle \otimes (Q_1\ |x_0\rangle) \\ V_1\ (|0\rangle \otimes (Q_0\ |x_0^\perp\rangle)) &= |0\rangle \otimes (Q_1\ |x_0^\perp\rangle)\end{aligned}$$

From Lemma A.17 we have that V_1 is of the following form, where P_0, P_1 are 1-qubit unitaries:

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

References

[1] Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[2] Tycho Sleator, Harald Weinfurter, Realizable universal quantum logic gates, Phys. Rev. Lett. 74 (1995).

[3] Nengkun Yu, Runyao Duan, Mingsheng Ying, Five two-qubit gates are necessary for implementing Toffoli gate, Phys. Rev. A (2013).

[4] Nengkun Yu, Mingsheng Ying, Optimal simulation of Deutsch gates and the Fredkin gate, Phys. Rev. A (2015).