On the CNOT-cost of the TOFFOLI gate

Vivek V. Shende∗
vshende@princeton.edu

Igor L. Markov†
imarkov@eecs.umich.edu

Abstract

Three-input TOFFOLI gates are heavily used when performing classical logic operations on quantum data, e.g., in reversible arithmetic circuits. However, in physical implementations TOFFOLI gates are decomposed into six CNOT gates and several one-qubit gates. Though this decomposition has been known for at least 10 years, we provide here the first demonstration of its CNOT-optimality.

We first prove that any circuit (i) containing less than six CNOT gates and (ii) implementing a diagonal operator, can be rearranged to form the cosine-sine decomposition of a related operator. Leveraging the canonicity of such decompositions to limit one-qubit gates appearing in respective circuits, we completely classify three-qubit diagonal operators by their CNOT-cost. As a consequence, we deduce that the TOFFOLI cannot be implemented using fewer than six CNOTs. Circuit-analysis techniques developed in our work also produce new lower bounds for related gates and the n-qubit analogue of the TOFFOLI.

1 Introduction

The three-qubit TOFFOLI gate appears in key quantum logic circuits, such as those for modular exponentiation. However, in physical implementations it must be decomposed into one- and two-qubit gates. Figure 1 reproduces the textbook circuit from [13] with six CNOT gates, as well as Hadamard (H), $T = \exp(i\pi\sigma_z/8)$ and $T^\dagger$ gates.

The pursuit of efficient circuits for standard gates has a long and rich history. DiVin-cenzo and Smolin found numerical evidence [4] that five two-qubit gates are necessary and

\[ \text{Figure 1: Decomposing the TOFFOLI gate into one-qubit and six CNOT gates.} \]
sufficient to implement the TOFFOLI. Margolus showed that a phase-modified TOFFOLI gate admits a three-CNOT implementation [6, 5], whose optimality was eventually demonstrated by Song and Klappenecker [19]. Unfortunately, this MARGOLUS gate can replace TOFFOLI only in rare cases. The detailed case analysis used in the optimality proof from [19] does not extend easily to circuits with four or five CNOTs. The omnibus Barenco et al. paper offers circuits for many standard gates, including an eight-CNOT circuit for the TOFFOLI [1, Corollary 6.2], as well as a six-CNOT circuit for the controlled-controlled-σz, which differs from the TOFFOLI only by one-qubit operators [1, Section 7]. Problem 4.4b of the textbook by Nielsen and Chuang asks whether the circuit of Figure 1 could be improved. The problem was marked as unsolved, and we report the following progress.

**Theorem 1** A circuit consisting of CNOT gates and one-qubit gates which implements the n-qubit TOFFOLI gate without ancillae requires at least $2^n$ CNOT gates. For $n = 3$, this bound holds even when ancillae are permitted, and is achieved by the circuit of Figure 1.

Our main tool is the Cartan decomposition in its “KAK” form, which provides a Lie-theoretic generalization of the singular-value decomposition [8]. Several special cases have previously proven useful for the synthesis and analysis of quantum circuits, notably the two-qubit magic decomposition [9, 10, 23, 22, 21, 15, 16], the cosine-sine decomposition [7, 2, 12, 17], and the demultiplexing decomposition [17]. The canonicity of the two-qubit magic decomposition was used previously to perform CNOT-counting for two-qubit operators [15]. The magic decomposition is a two-qubit phenomenon, but the cosine-sine and demultiplexing decompositions hold for $n$-qubit operators ($n \geq 2$) and enjoy similar canonicity. Moreover, the components of these decompositions are *multiplexors* [17] — block-diagonal operators that commute with many common circuit elements. Commutation properties facilitate circuit restructuring that can dramatically reduce the number of circuit topologies to be considered in proofs. These results and observations allow us to perform CNOT-counting using the Cartan decomposition in a divide-and-conquer manner.

In the remaining part of this paper, we first review basic properties of quantum gates in Section 2 and make several elementary simplifications to reduce the complexity of the subsequent case analysis. In particular, we pass from the CNOT and TOFFOLI gates to the symmetric, diagonal CZ and CCZ gates, and recall circuit decompositions which yield operators commuting with $Z$ and CZ gates. We also define qubit-local CZ costs, and observe that the total CZ cost can be lower-bounded by half the sum of the local CZ counts for each qubit. Though weak, this bound suffices for our purposes and we can actually compute it. Section 3 is the heart of the present work, in which we prove our result on the CNOT cost of the TOFFOLI gate. It starts by motivating and outlining the techniques involved, previews key intermediate results, and proves that the CNOT-cost of the TOFFOLI is 6, based on these results. In Section 3.2, we use the canonicity of the cosine-sine decomposition to generalize and extend some circuit simplifications of Klappenecker and Song [18], and also characterize operators with low CZ-costs. Section 3.3, motivated by [16], employs the canonicity of the demultiplexing decomposition, captured by a spectral invariant to lower-bound CZ gates required in circuit implementations of operators. The results apply,

---

1While the Cartan decomposition $SU(n) = SO(n) \cdot [\text{diagonals}] \cdot SO(n)$ is general, the utility of the magic decomposition arises from the the isomorphism $SU(2) \times SU(2) = SO(4)$ being represented as an inner automorphism of $SU(4)$. Such coincidental isomorphisms are few and confined to low dimensions.
2 Preliminaries

We review notation and properties of useful quantum gates, then characterize operators that commute with Z gates placed on multiple qubits. We then review circuit decompositions from [3, 12, 17]. Finally, we introduce terminology appropriate for measuring gate costs of unitary operators in terms of the CNOT and CZ and state elementary but useful observations about these costs.

2.1 Notation and properties of standard quantum gates

We write X, Y, Z for the Pauli operators, and CX, CCX for CNOT, TOFFOLI. Rotation gates \( \exp(i\theta X) \) are denoted by \( R_x(\theta) \), and we analogously use \( R_x, R_y \), omitting the factor of \( \pm 1/2 \) used by other authors. We work throughout on some fixed number of qubits \( N \).

For a one-qubit gate \( g \) and a qubit \( q \), we denote by \( g^{(q)} \) the \( N \)-qubit operator implemented by applying the gate \( g \) on qubit \( q \). Similarly, \( \text{C}^{(i)}X^{(j)} \) is the operator implemented by a controlled-X with the control on qubit \( i \) and target on qubit \( j \).

The controlled-Z being symmetric with respect to exchanging qubits, we do not distinguish control from target in the notation \( \text{CZ}^{(i,j)} \). We similarly denote the operator of a controlled-controlled-Z on qubits \( i, j, k \) by \( \text{CCZ}^{(i,j,k)} \). In choosing qubit labels, we follow throughout the convention that the high-to-low significance order of qubits is the same as the lexicographic order of their labels.

We follow the standard but sometimes confusing convention that typeset operators act on vectors from the left, but circuit diagrams act on inputs from the right. Consistently with the established notation for the CNOT gate, we denote the X gate by “⊕” in circuit diagrams. We denote the Z gate by a “•” symbol, which does not lead to ambiguity in the matching notation for CZ because CZ is symmetric. Thus the following diagram expresses the identity \( \text{CZ}^{(i,m)}X^{(i)} = Z^{(m)}X^{(i)}\text{CZ}^{(i,m)} \) — a de Morgan-like property of the CZ gate.

\[
\begin{align*}
\text{CNOT-}
\begin{array}{c}
\ell \quad \oplus \\
m
\end{array}
&= \\
\text{CNOT-}
\begin{array}{c}
\ell \\
m \\
\end{array}
\end{align*}
\]

Another standard identity relates the X, Z, and one-qubit HADAMARD (H) gates: \( HXH = Z \). By case analysis on control qubits, one obtains the further identities \( H^{(i)}C^{(j)}X^{(i)}H^{(i)} = CZ^{(i,j)} \) and \( H^{(i)}CC^{(j,k)}X^{(i)}H^{(i)} = CCZ^{(j,k)} \). We prefer the X family of gates for some applications, and the Z family for others, as summarized in Table 1.

Circuits consisting entirely of one-qubit gates and CZ (respectively CNOT) gates will be called CZ-circuits (respectively CNOT-circuits). Using the above identities, CZ-circuits and CNOT-circuits can be interchanged at the cost of adding one-qubit H gates. It will also be convenient to consider CZ\(^{(i)}\)-circuits, which by definition are arbitrary circuits where all multi-qubit gates touching qubit \( \ell \) are CZ. While these are not a subclass of CZ-circuits, a CZ\(^{(i)}\)-circuit can be converted into a CZ-circuit without any changes affecting qubit \( \ell \).
CNOT and TOFFOLI

Advantages

- Implement addition and multiplication
- Universal for reversible computation
- Block-diagonal
- Appear in $R_z$-gate decompositions, etc
- Commute with $X$ on target

CZ and CCZ

Symmetric

- Fewer circuit topologies
- Diagonal and subject to general theory
- Commute with $Z$ on target

Other properties

- Change direction after two $H$-conjugations
- One can map back and forth by $H$-conjugation on target

Applications

- Circuit synthesis
- Circuit analysis

Table 1: Relative advantages of standard controlled gates.

2.2 Operators commuting with $Z$

We now recall terminology for operators commuting with $Z$ on some qubits, but possibly not all qubits. Further background on the circuit theory of these quantum multiplexors can be found in [17].

The control-on-box notation of the following diagram indicates that the operator $U$ commutes with $Z^{(ℓ)}$. The backslash on the bottom line indicates an arbitrary number of qubits (a multi-qubit bus).

$$
\begin{array}{c}
\ell \\
\downarrow \\
U
\end{array}
$$

These operators include the commonly-used positively and negatively controlled-$U$ gates, although in our notation $U$ also acts on the control qubits (and is thus “larger than the box in which it is contained”). In general, operators which commute with $Z$ are block-diagonal:

Observation 2 For a unitary operator $Q$ and qubit $ℓ$, the following are equivalent.

- $Q$ commutes with $Z^{(ℓ)}$
- $\langle 0 |^{(ℓ)} Q | 1 \rangle^{(ℓ)} = 0$
- $\langle 1 |^{(ℓ)} Q | 0 \rangle^{(ℓ)} = 0$
- $Q$ admits a decomposition $Q = |0\rangle^{(ℓ)} \otimes Q_0 + |1\rangle^{(ℓ)} \otimes Q_1$

In an appropriate basis, the matrix of $Q$ is block-diagonal with blocks $Q_1$ and $Q_0$, that represent the “then” and “else” branches of the quantum multiplexor $Q$ with select qubit $ℓ$.

Notation. If $Q$ commutes with $Z^{(ℓ)}$ and $ℓ$ is clear from context, we denote by $Q_j$ the operators $\langle j |^{(ℓ)} Q | j \rangle^{(ℓ)}$. Similarly, if $Q$ commutes with with $Z^{ℓ_i}$ for qubits $ℓ_1 \ldots ℓ_k$, then for any bitstring $j_1 \ldots j_k$ we write $Q_{j_1 \ldots j_k}$ for $\langle j_1 \ldots j_k |^{(ℓ_1 \ldots ℓ_k)} Q | j_1 \ldots j_k \rangle^{(ℓ_1 \ldots ℓ_k)}$

We also have the following commutability.

Observation 3 Let $Q, R$ be two gates such that for every qubit $ℓ$, either one of them does not affect $ℓ$, or both of them commute with $Z^{(ℓ)}$. Then $QR = RQ$. In picture:
Dimension-counting shows that roughly this many are necessary for almost all such operators.

Corollary 6 N-qubit operators which commute with Z on k qubits can be implemented using on the order of $2^k 4^{N-k}$ one-qubit and CZ gates.\footnote{Dimension-counting shows that roughly this many are necessary for almost all such operators.}
Proof. This follows from the construction in the proof of Proposition 5 and the known estimates in the cases \( k = 0, N - 1 \) [12] and \( k = N \) [3]. ■

Proposition 5 suggests a difficulty that will arise when dealing with ancilla qubits. If only \( N = 3 \) qubits are available, then \( \det_{1,2} \text{CCZ}^{(1,2,3)} = \text{CZ}^{(1,2)} \), so the \text{CCZ} cannot be implemented in any three-qubit \text{CZ}-circuit in which all gates commute with \( \text{Z}^{(1)}, \text{Z}^{(2)} \). But if \( N = 4 \) qubits are present, \( \det_{1,2} (\text{CCZ}^{(1,2,3)}) = I^{(1,2)} \), so \( \text{CCZ}^{(1,2,3)} \otimes I^{(4)} \) can be implemented in a four-qubit \text{CZ}-circuit in which all one-qubit gates commute with \( \text{Z}^{(1)} \) and \( \text{Z}^{(2)} \). We will discuss these issues further in Section 5.

2.3 Cartan decompositions in quantum logic

This section recalls two important operator decompositions – (cosine-sine and demultiplexing) – and casts them as circuit decompositions. Readers willing to accept their use in our proofs may skip to Section 2.4.

We first make the trivial observation that an operator can be implemented with a single one-qubit gate if and only if it commutes with the Pauli operators \( \text{Z} \) and \( \text{X} \) on all other qubits. Thus to produce a \text{CNOT}-circuit for a given operator \( U \), one may use the following algorithm:

1. Decompose \( U \) into a circuit with only \text{CNOT} gates and operators \( V, W, \ldots \) which commute with \( X \) and \( Z \) on more qubits than \( U \) does.
2. Apply the algorithm recursively to components \( V, W, \ldots \) until one-qubit gates are reached.

As \( Z \) is self-adjoint, the requirement that \( U \) commutes with \( Z^{(i)} \) can be rephrased as the condition that \( U \) is fixed under the involution \( U \mapsto Z^{(i)}UZ^{(i)} \). Given such an involution, a fundamental Lie-theoretic result produces an operator decomposition [8]. Here we recite the result for completeness, but do not require the reader to understand all terminology.

The Cartan Decomposition. Let \( G \) be a reductive Lie group, and \( \theta : G \to G \) an involution. Let \( K = \{ g : \theta(g) = g \} \) and \( A \) be maximal over subgroups contained in \( \{ g : \theta(g) = g^{-1} \} \). Then \( K \) is reductive, \( A \) is abelian, and \( G = KAK \).

In order to restate decompositions of unitary operators as circuit decompositions, we employ the notation of set-valued quantum gates [17]. Completely unlabelled gates denote the set of all gates satisfying all control-on-box commutativity conditions imposed by the diagram, and gates labelled \( R_x, R_y, R_z \) denoted the appropriate set of (possibly multiplexed) rotations. An equivalence of circuits with set-valued gates means that if we pick an element from each set on one side, there is a way to choose elements on the other so that the two circuits compute the same operator. The backslashed wires which usually indicate multiple qubits may also carry zero qubits.

The involution \( \phi_Z : U \mapsto Z^{(i)}UZ^{(i)} \) corresponds to the cosine-sine decomposition.\(^\text{3}\)

\(^{3}\)The terminology comes from the numerical linear algebra literature; see [14] and references therein.
The involution $\phi_X : U \mapsto X^{(\ell)} U X^{(\ell)}$ yields the demultiplexing decomposition [17].

$$\ell \quad = \quad \boxed{\text{}} \quad R_z \quad$$

The map $\phi_X$ restricts to the subgroup of diagonal operators. This group being abelian, the $K$ and $A$ factors commute, leaving the following decomposition of diagonal operators.

$$\ell \quad = \quad \boxed{\text{}} \quad R_z \quad$$

The involution $\phi_X$ further restricts to the subgroup of multiplexed $Z$ rotations, which we can demultiplex again. The $K$ and $A$ factors again commute; the $A$ factor is computed by the last 3 gates in the circuit below.

$$\ell \quad = \quad \boxed{\text{}} \quad R_z \quad R_z \quad R_z \quad R_z \quad$$

To establish the existence of these decompositions, it remains to verify in each case that the purported $K$ and $A$ satisfy the appropriate properties with respect to the relevant involution. This can be checked after passing to the Lie algebra, where it is easy. Alternatively, explicit constructions of the cosine-sine and demultiplexing decompositions are given in [14] and [17], respectively.

To decompose general $n$-qubit operators, Equation 2 can be applied iteratively until all remaining gates are either multiplexed $R_y$ gates or diagonal. The $R_y$ gates can be replaced by $R_z$ gates at the cost of introducing some one-qubit operators; the $R_z$ and other diagonal gates can be decomposed as described above; for details and optimizations see [12]. Smaller circuits are obtained by another algorithm, which alternates cosine-sine decompositions with demultiplexing decompositions; for details and optimizations, see [17].

When circuit decompositions are applied recursively, some gates can be reduced by local circuit transformations. For example, when iteratively demultiplexing multiplexed $R_z$ gates, some $\text{CNOT}$s may be cancelled as shown below.
This technique produces a circuit with $2^n$ CNOT gates for an $n$-ply multiplexed $R_z$ gate. Using Equation 4, we obtain a circuit with $2^n - 2$ CNOT gates for an arbitrary $n$-qubit diagonal operator [3]. Applying this result to CCZ gate leads to the circuit in Figure 1.

### 2.4 Basic facts about CZ-counting

The CZ-cost $|U|_{CZ}$ of an $N$-qubit operator $U$ is the minimum number of CZs which appear in any $N$-qubit CZ-circuit for $U$; we define the CNOT-cost analogously. The identity $H(i)C(i)X(i)H(i) = CZ(i,j)$ ensures that $|U|_{CZ} = |U|_{CNOT}$. The further identity $H(i)CC(i,k)X(i)H(i) = CCZ(i,j,k)$ yields:

**Observation 7** $|CCZ|_{CZ} = |CCZ|_{CNOT} \leq 6$.

By way of illustration, the following modification of the circuit in Figure 1 implements the CCZ in terms of CZs.

\[
\begin{array}{c}
\text{H} & \text{HT} & \text{HTH} & \text{HTH} & \text{H} \\
\end{array}
\]

It shall prove more convenient to compute $|CCZ|_{CZ}$ rather than $|CCZ|_{CNOT}$. Namely, we are going to study the number of CZs which must touch a given qubit in any CZ-circuit for a given operator. More precisely, for a given qubit $\ell$, the $CZ^{(\ell)}$-cost $|U|_{CZ,\ell}$ is the minimum number of CZ gates incident on $\ell$ in any $CZ^{(\ell)}$-circuit for $U$. These cost functions are related through the following estimate.

**Observation 8** For any operator $P$,

\[
|P|_{CZ} \geq \frac{1}{2} \sum_j |P|_{CZ,j}
\]

**Proof.** Each CZ gate touches two qubits. □

For example, in the case of the CCZ, the costs $|CCZ|_{CZ,j}$ are the same for $j = 1, 2, 3$ (by symmetry), thus

\[
|CCZ|_{CZ} \geq 3 \frac{1}{2} |CCZ|_{CZ,j}
\]

(7)

As we show later, $|CCZ|_{CZ,j} = 3$, but no circuit can achieve this lower bound for all qubits $j$ at once. While this bound is very weak in general,\(^4\) it suffices for our purposes.

We emphasize that the number of qubits, $N$, is an unspecified parameter in both $|\cdot|_{CZ}$ and $|\cdot|_{CZ,\ell}$. In the presence of ancillae, we define $|U|_{CZ,\ell}^a := \min |U \otimes I_t^{2^\ell}|_{CZ}$. Obviously $|U|_{CZ}^a \leq |U|_{CZ}$.

\(^4\)Dimension-counting shows that a generic $N$-qubit operator $U$ has $|U|_{CZ} = \Omega(4^N)$, whereas the results of [17] imply that $|U|_{CZ,\ell} < 6N$, so at best we can establish that $|U|_{CZ} \geq N(6N - 1)$.
3 The CNOT cost of the TOFFOLI gate

So far we have reduced CNOT-counting for the TOFFOLI gate to CZ-counting for the CCZ gate, with the latter two being diagonal and symmetric. To show that six CZ gates are required to implement a CCZ gate, we first assume a five-CZ circuit and seek a contradiction, using a divide-and-conquer strategy.

3.1 Outline of the proof

Consider a hypothetical five-CZ implementation of the CCZ, with unspecified one-qubit operators wherever possible. There are many possible arrangements of the CZs, and our proofs will not enumerate over them explicitly, but we fix one here for clarity.

We define $a, b, P, Q$ as follows.

Our circuit decomposition now takes the following form.

Up to some two-qubit diagonal fudge factors, this equation says that the cosine-sine decomposition of $b^\dagger \otimes I$ is $Q^\dagger (a \otimes I) P$.

In Section 3.2, we translate the well-known canonicity of this Cartan decomposition into constraints on the components $a, b, P$ and $Q$. We also consider several related circuit templates and show that constituent gates must often be diagonal or must commute with $Z$ placed on certain qubits; these results will be used repeatedly in the subsequent sections. In particular, we establish that a CZ($\ell$)-circuit for an operator commuting with $Z(\ell)$, containing two or fewer CZs incident to $\ell$, can be restructured to contain only gates commuting with $Z^\ell$.
In Section 3.3 we extend these reductions to a numerical formula characterizing operators $U$ with $|U|_{CZ,\ell} = 0, 1, 2$. The idea is to find an equivalence relation $\sim_\ell$ such that (i) $U \sim_\ell V \implies |U|_{CZ,\ell} = |V|_{CZ,\ell}$ and (ii) the equivalence classes of $\sim_\ell$ are easy to characterize.

**Definition 9** For $P, Q$ commuting with $Z^{(\ell)}$, we write $P \sim_\ell Q$ if there exist $a, b, A, B$ satisfying the following equation.

$$\ell \begin{array}{c} b \hline P \end{array} A = \begin{array}{c} \hline B \end{array} Q$$

(10)

The fact that $| \cdot |_{CZ,\ell}$ is constant on equivalence classes is obvious; the ability to characterize the equivalence classes comes from a comparison between Equation 10 and the demultiplexing decomposition of Equation 3. We construct invariants of the equivalence classes in Theorem 22. The reductions of Section 3.2 provide circuit forms on which the invariants are easy to compute; as a consequence, we arrive at a complete characterization of $| \cdot |_{CZ,\ell} = 0, 1, 2$ in Theorem 23. The CCZ gate falls into none of these classes, and thus each qubit in any circuit computing it must have at least three CZs incident to it.

With this in mind, we return to the constraints of Section 3.2, the pertinence of which to circuits with exactly three CZs incident to some qubit can be seen from Equation 8 and the following discussion. By playing them off the formula of Theorem 23, we derive strong results about the $| \cdot |_{CZ,\ell} = 3$ case. Specifically, we show in Theorem 24 that if $|U|_{CZ,\ell} = 3$ and $\mathcal{C}$ computes $U$ using the minimum required three CZ gates incident on $\ell$, then $\mathcal{C}$ can be arranged to contain no non-diagonal one-qubit gates on $\ell$, possibly at the cost of introducing Z gates elsewhere in the circuit.

This is the last result needed to determine the CZ-cost of the CCZ. From the fact $|CCZ|_{CZ,\ell} > 2$ and Inequality 7, we deduce that any circuit containing fewer than six CZ gates and implementing the CCZ must contain exactly five CZ gates. Moreover two of the qubits, $m, n$ touch exactly three CZ gates and the remaining one touches four. By Theorem 24, we can assume all one-qubit operators on $m, n$ are diagonal. But this contradicts Proposition 5.

**Theorem 10** $|CCZ|_{CZ} = 6$.

We will show in Section 5 that the availability of ancilla qubits does not improve the CZ cost of the CCZ.

### 3.2 Circuit constraints from cosine-sine decomposition

This section is devoted to the study of Equation 9. The one-qubit case of the cosine-sine decomposition guarantees the existence of $4 \times 4$ unitary diagonal matrices $A_1, A_r, B_L, B_r$ and $2 \times 2$ real diagonal matrices with angular parameters $\alpha, \beta$ such that the following equations hold.

$$1 \begin{array}{c} b \hline \end{array} = \begin{array}{c} \hline B_L \end{array} R_y(-\beta) \begin{array}{c} \hline B_R \end{array}$$

(11)

---

5 This is sometimes called the “ZYZ” decomposition.
Define $\hat{P} = A_L P B_R$ and $\hat{Q} = A_R^\dagger Q B_L^\dagger$ to obtain:

\[
\begin{pmatrix}
1 \\
2
\end{pmatrix}
\begin{pmatrix}
R_y(-\beta) & R_y(\alpha) \\
\hat{P} & \hat{Q}
\end{pmatrix}
= \begin{pmatrix}
A_L & R_y(\alpha) \\
A_R & \hat{Q}
\end{pmatrix}
\tag{13}
\]

We rearrange the equation to obtain $\hat{Q}^\dagger (R_y(\alpha) \otimes I) \hat{P} = R_y(\beta) \otimes I$. Transforming the equation by $t \mapsto Z_t^{-1} Z_t^2$, we get $\hat{P}^\dagger (R_y(\alpha) \otimes I) \hat{Q} = R_y(\beta) \otimes I$. Multiplying these equations yields $\hat{P}^\dagger (R_y(2\alpha) \otimes I) \hat{P} = R_y(2\beta) \otimes I$. Thus $R_y(2\alpha)$ and $R_y(2\beta)$ have the same eigenvalues. One can check that in fact they are conjugate under an element of the group $W$ generated by $X^{(2)}$ and $CZ^{(1,2)}$; note that these operators commute with $Z^{(1)}$. That is, there exists $w \in W$ such that $wR_y(2\alpha) w^\dagger = R_y(2\beta)$. Now let $t = wR_y(\alpha) w^\dagger R_y(-\beta)$. We have both $t = R_y(\xi)$ for some $2 \times 2$ real diagonal matrix $\xi$ acting on qubit 2, and $t^2 = I$; it follows that $t = \pm I, \pm \sigma_z^{(2)}$. Thus defining $\hat{P} = \hat{P} \cdot (tw \otimes I)$ and $\hat{Q} = \hat{Q} \cdot (w \otimes I)$, our equation is reduced to:

\[
\begin{pmatrix}
1 \\
2
\end{pmatrix}
\begin{pmatrix}
R_y(-\alpha) & R_y(\alpha) \\
\hat{P} & \hat{Q}
\end{pmatrix}
= \begin{pmatrix}
A_L & R_y(\alpha) \\
A_R & \hat{Q}
\end{pmatrix}
\tag{14}
\]

**Observation 11** The operators $\hat{P}$ and $\hat{Q}$ both commute with $R_y(2\alpha)$. Conjugation by $R_y(\alpha)$ is an involution on the subgroup of such operators. If $\hat{P}$ is fixed by this involution, then $\hat{P} = \hat{Q}$ and the original $a,b$ in Equation 9 may be replaced by diagonal two-qubit operators $a', b'$ such that the equation still holds.

In the most interesting case, the involution is just conjugation by $X^{(1)}$, which leads us later to consider the demultiplexing decomposition. For now, we derive restrictions of $\hat{P}, \hat{Q}$ which follow from the commutability of $\hat{P}, \hat{Q}$ with $R_y(2\alpha)$.

**Lemma 12** Fix distinct qubits $l, m$. Let $U$ be a unitary operator commuting with $Z^{(l)}$, and let $\theta$ be a two-by-two real diagonal matrix of angular parameters which is understood to act on $m$. Then the following are equivalent.

1. $[R_y^{(l)}(\theta), U] = 0$
2. $[U_0, \cos(\theta) \otimes I] = [U_1, \cos(\theta) \otimes I] = 0$ and $U_0(\sin(\theta) \otimes I) = -(\sin(\theta) \otimes I) U_1$
3. One of the following holds
   (a) $\cos(\theta)$ is scalar, and either
      i. $\sin(\theta) = 0$.
      ii. $\sin(\theta)$ is a nonzero scalar and $U_0 = -U_1$.
      iii. $Z \sin(\theta)$ is a nonzero scalar and $U_0 = -Z^{(m)} U_1 Z^{(m)}$.
   (b) $\cos(\theta)$ is not scalar. Then $U$ commutes with $Z^{(m)}$.
      i. $\sin(\theta_0) = 0$ and $\sin(\theta_1) = 0$. 

11
ii. \( \sin(\theta_0) = 0 \) and \( \sin(\theta_1) \neq 0 \) and \( U_{01} = -U_{11} \).

iii. \( \sin(\theta_0) \neq 0 \) and \( \sin(\theta_1) = 0 \) and \( U_{00} = -U_{10} \).

iv. \( \sin(\theta_0) \neq 0 \) and \( \sin(\theta_1) \neq 0 \) and \( U_0 = -U_1 \).

**Proof.** (3) \( \implies \) (1) is trivial. (1) \( \implies \) (2) follows from the expansion \( \exp(iY^{(\ell)} \otimes \theta) = I^{(\ell)} \otimes \cos(\theta) + iY^{(\ell)} \otimes \sin(\theta) \). To see (2) \( \implies \) (3) is just a matter of repeatedly using the observation that the only two-by-two matrices which commute with a two-by-two diagonal matrix with distinct entries are themselves diagonal. \( \blacksquare \)

Translating this back to the original setting:

**Lemma 13** In the situation of Equation 9, at least one of the following must hold.

1. Either \( a, b \) are diagonal or \( aX^{(1)}, bX^{(1)} \) are diagonal.

2. There exists a two-qubit operator \( U \) and two-qubit diagonals \( D, D' \) such that

\[
\begin{array}{c}
P \quad = \quad D' \\
\end{array}
\]

Similarly, there exists a two-qubit operator \( V \) and two-qubit diagonals \( C, C' \) such that

\[
\begin{array}{c}
Q \quad = \quad C' \\
\end{array}
\]

3. Either \( P \) or \( F_X^{(2)} \) commute with \( Z^{(2)} \).

**Proof.** This amounts to unwinding the above discussion in light of Lemma 12. Case I comes from case 3.a.i. of the lemma; the \( X \) appears because of the 2 in \( \theta = 2\alpha \). Case II comes from cases 3.a.ii. and 3.a.iii, and case III is just case 3.b. Here, the \( X \) can arise as a factor of the \( w \) in \( \tilde{P} = \tilde{P}w \) from the discussion above. \( \blacksquare \)

We consider now the special case in which the \( a, b \) operators of Equation 9 do not entangle qubit 2. The following lemma was proven by Klappenecker and Song in the special case \( P = CX \).

**Lemma 14** Suppose the following equation holds.

\[
\begin{array}{c}
1 \quad P \\
\end{array}
\]

Then at least one of the following holds.

1. \( a, b \) are both diagonal or both anti-diagonal.

2. \( P \) takes the form \( d \otimes P_0 \) for some one-qubit diagonal \( d \).
Proof. This follows from the proof of Lemmas 12 and 13, if one notes that (1) the terms extracted in Equations 12 and 11 are one-qubit diagonals and that (2) only cases 3.a.i and 3.a.ii of Lemma 12 can occur. However, it is even easier to give a direct proof:

\[ 0 = \langle 0|^{(1)} a P b|1\rangle^{(1)} = \langle 0|a|0\rangle \langle 0|b|1\rangle P_0 + \langle 0|a|1\rangle \langle 1|b|1\rangle P_1 \]

As the coefficients do not vanish, \(P_0\) and \(P_1\) are linearly dependent. It follows that \(P_0 = \delta \otimes P_0\) for some one-qubit diagonal \(\delta\).

Corollary 15 If \(a^{(i)} CZ^{(i,j)} b^{(j)}\) commutes with \(Z^{(i)}\), then \(a, b\) are both diagonal or anti-diagonal.

Corollary 16 In the situation of Lemma 14, there exist one-qubit operators \(a', b'\) which are either diagonal or anti-diagonal, such that \(a^{(1)} P b^{(1)} = Q\).

Proof. Apply Lemma 14; there only something to prove in case 2. Take \(a' = a \delta b \delta^{-1}\) and \(b' = I\); then \(a^{(1)} P b^{(1)} = a^{(1)} P b^{(1)}\). As \(a^{(1)} = Q P^T\) commutes with \(Z^{(1)}\), it is diagonal.

Corollary 17 Suppose the following equation holds.

\[
\begin{array}{c}
\ell \\
\hline
m \\
\hline
P \\
\hline
\end{array}
\quad = 
\begin{array}{c}
\quad \\
\hline \\
\hline
\quad \\
\hline
Q
\end{array}
\]

Then there exist two-qubit operators \(a', b'\) acting on qubits \(\ell, m\) which (i) commute with with \(Z^{(m)}\), (ii) have block components \(a'_0, a'_1, b'_0, b'_1\) which are each diagonal or anti-diagonal, and (iii) satisfy \((a' \otimes I) P (b' \otimes I) = Q\).

Proof. Every gate in the hypothesis commutes with \(Z^{(m)}\). To find \(a'_i, b'_i\), apply Corollary 16 to \(a^{(i)} P b^{(i)} = Q_i\).

Corollary 17 clarifies the situation of Lemma 13, case 3. The next series of results may be viewed as clarifying case 2.

Lemma 18 Suppose the following equation holds.

\[
\begin{array}{c}
1 \\
\hline
2 \\
\hline
P \\
\hline
\end{array}
\quad = 
\begin{array}{c}
\quad \\
\hline \\
\hline
\quad \\
\hline
Q
\end{array}
\]

Then (I) \(a_i b_j\) is diagonal for all \(i, j\) or (II) one of \(P, X^{(2)} P\) commutes with \(Z^{(2)}\).

Proof. We compute:

\[ 0 = \langle 0|^{(1)} i^{(2)} a P b|1\rangle^{(1)} |j\rangle^{(2)} = \langle 0|^{(1)} a_i b_j|1\rangle^{(1)} |i\rangle^{(2)} P |j\rangle^{(2)} \]

Either \(|i\rangle^{(2)} P |j\rangle^{(2)} = 0\) for some \(i, j\), or \(\langle 0|a_i b_j|1\rangle\) vanishes for all \(i, j\).
Corollary 19 Suppose the following equation holds.

\[
\begin{array}{ccc}
1 & = & 2 \\
M & & T \otimes S \otimes R
\end{array}
\]

Then either (I) an even number of \(r, s, t\) are anti-diagonal, and the remainder diagonal, or (II) \(S\) or \(SX^{(2)}\) commutes with \(Z^{(2)}\).

Proof. In order to apply Lemma 18, we move \(R\) and \(T\) to the other side.

\[
\begin{array}{ccc}
& & T \otimes M \otimes R \otimes T \\
& & S
\end{array}
\]

The cases here will correspond to the cases of Lemma 18. Case II is preserved verbatim. For Case I, the “\(a_i b_j\)” which must be diagonal are \(rst, rsZt, rZst, rsZsZt\). Since \((rst) \otimes rsZt = tZt^\dagger\) is diagonal, we deduce that either \(t\) or \(tX\) is diagonal. Likewise, \(rZst(rst) \otimes rZst = rZt^\dagger\) is diagonal, so either \(r\) or \(rX\) is diagonal. Finally, \(rst\) is diagonal, so from what we know about \(r, t\), either \(s\) or \(sX\) is diagonal, and the number of \(r, s, t\) which are not diagonal is even. ■

The following reformulation will be useful later.

Corollary 20 Fix a qubit \(\ell\), and let \(C\) be a CZ\((\ell)\)-circuit containing two CZ gates incident on \(\ell\). Suppose the operator \(Q\) computed by \(C\) commutes with \(Z^{(\ell)}\). Then there is a CZ\((\ell)\)-circuit \(C'\) computing \(Q\), which contains exactly the same multiqubit gates as \(C\) and moreover contains only a single one-qubit gate on \(\ell\), which is diagonal. The multiqubit gates act on their original wires, with the possible exception that if the other terminals of the two CZ gates touching \(\ell\) had been different, they may now be the same. The one-qubit gates present in \(C'\) but not \(C\) appear along the terminals of the two CZs.

Proof. By hypothesis, \(C\) takes the form

\[
Q = [r \otimes R]CZ^{(\ell, m)}[s \otimes S]CZ^{(\ell, n)}[t \otimes T]
\]

where \(r, s, t\) are subcircuits of one-qubit operators acting on \(\ell\), and \(R, S, T\) are subcircuits containing no gates acting on \(\ell\). We immediately replace \(r, s, t\) by the one-qubit operators they compute. Moreover, if \(m \neq n\), then replace \(S\) and \(T\) by \(\text{SWAP}^{(m, n)}\), where \(\text{SWAP}\) is the gate which exchanges qubits. The swaps will be restored and canceled at the end of the proof. We are in the situation of Lemma 18.

Case I. We are done, with the exception that the \(r, t\) may be anti-diagonal rather than diagonal. In this case, Equation 1 allows the extraneous Xs to be pushed through and cancelled at the cost of introducing Z gates on qubit \(m\). The diagonal gates remaining on qubit \(\ell\) may be commuted through the CZs and conglomerated into one. Finally, the possible swap introduced between the \(S, T\) terms may be cancelled.

Case II. Using Equation 1 and replacing \(s\) by \(sZ\) if necessary, we commute \(S\) past one of the CZs. We now have:

\[
Q = [r \otimes R]CZ^{(\ell, m)}s^{(\ell)}CZ^{(\ell, m)}[t \otimes ST]
\]
Rearranging the equation,
\[ [I \otimes R^\delta]Q[I \otimes T^\dagger] = \ell^{(f)} CZ^{(n,m)}_s P \ell^{(f)} \]

Let \( V \) be the value of either side of the equation above. Then from the LHS we see that \( V \) commutes with \( Z^\ell \), and from the RHS we see that \( V \) is a two-qubit operator commuting with \( Z^{(m)} \). Thus \( V \) is a two-qubit diagonal, and admits the following decomposition.

Substituting this decomposition for the RHS of Equation 15 and restoring the \( R,S,T \) gates completes the proof. ■

3.3 CZ counting via the demultiplexing decomposition

We now turn to the study of \( | \cdot \rangle_{cz,f} \). Recall \( P \sim_{\ell} Q \implies |P|_{cz,f} = |Q|_{cz,f} \); we therefore seek to characterize when \( P \sim_{\ell} Q \). This will be done under the assumption that \( P \) and \( Q \) both commute with \( Z^{(f)} \).

**Definition 21** Let \( U \) commute with \( Z^{(f)} \). Then the \( \ell \)-mux-spectrum \( \mathcal{S}^{(f)}(U) \) is the multi-set of eigenvalues, taken with multiplicity, of \( U^\dagger U_0 \). Two multi-sets \( S,T \) are said to be congruent, \( S \cong T \), if there exists a nonzero scalar \( \lambda \) such that either \( \lambda S = T \) or \( \lambda S = T^\dagger \).

We note that it is necessary to fix the number of qubits on which \( U \) acts before taking its \( \ell \)-mux-spectrum: \( \mathcal{S}^{(f)}(U \otimes I) \) contains \( \dim I \) copies of \( \mathcal{S}^{(f)}(U) \).

**Theorem 22** Suppose \( P,Q \) commute with \( Z^{(f)} \). Then \( P \sim_{\ell} Q \iff \mathcal{S}^{(f)}(P) \cong \mathcal{S}^{(f)}(Q) \).

**Proof.** \((\Rightarrow)\). As \( P \sim_{\ell} Q \), there are gates \( a,b,A,B \) such that

\[ \ell \begin{array}{c} b \\ B \end{array} \oplus \begin{array}{c} a \\ P \end{array} A = \begin{array}{c} a \\ Q \end{array} \]

By Corollary 15, we may assume that either \( a,b \) or \( aX,bX \) are diagonal. In the first case, \( Q_0 = a_0 b_0 A_0 P_0 B \) and \( Q_1 = a_1 b_1 A_1 P_1 B \). Thus \( Q_1^\dagger Q_0 = (a_1 b_1)^\dagger a_0 b_0 B^T P_1^T P_0 B \), which has the same eigenvalues as \( (a_1 b_1)^\dagger a_0 b_0 P_1^T P_0 \). Thus \( \mathcal{S}^{(f)}(P) \cong \mathcal{S}^{(f)}(Q) \).

Otherwise, \( a' = aX \) and \( b' = Xb \) are diagonal. Now \( Q_1^\dagger Q_1 = (a_1 b_1')^\dagger a_0 b_0 B^T P_1^T P_0 B \), which has the same eigenvalues as \( (a_1 b_1')^\dagger a_0 b_0 P_1^T P_1 \), whose eigenvalues in turn are the complex conjugates of those of \( a_0 b_0 P_1^T P_1 \); again \( \mathcal{S}^{(f)}(P) \cong \mathcal{S}^{(f)}(Q) \).

\((\Leftarrow)\). By supposition, the \( \mathcal{S}^{(f)}(P) \cong \mathcal{S}^{(f)}(Q) \). We note \( \mathcal{S}^{(f)}(\chi^{(f)} P \chi^{(f)}) = \mathcal{S}(P) \) and \( \mathcal{S}((R^{(f)}_\lambda P) \mathcal{S}(P) = e^{2i\lambda} \mathcal{S}(P) \). Therefore we can readily find an operator \( P' \sim_{\ell} P \) such that the \( \ell \)-mux-spectrum of \( P' \) is identical, rather than merely congruent, to that of \( Q \). It remains to show that \( P' \sim_{\ell} Q \).

By the demultiplexing decomposition (Equation 3) there exist unitary operators \( M_P,N_P \) and a real diagonal matrix \( \delta_P \), all of which act on the qubits other than \( \ell \), such that \( P' = \ldots \)
Let $P$ commute with $Z^i$. Let $\Phi(\delta)$ by $\Phi(\delta) = R_\ell(\delta)$

$[I \otimes M_P] R_\ell^i(\delta_P)[I \otimes N_P]$. Likewise we decompose $Q = [I \otimes M_Q] R_\ell^i(\delta_Q)[I \otimes N_Q]$. If we let $\Delta_P = \exp(i\delta_P)$ and $\Delta_Q = \exp(i\delta_Q)$, then the $\ell$-mux-spectra of $P'$ and $Q$ are respectively the entries of $\Delta_P^\ell$ and $\Delta_Q^\ell$. Since $\mathbb{Z}(\ell)(P) = \mathbb{Z}(\ell)(Q)$, there must exist a permutation matrix $\pi$ acting on the qubits other than $\ell$ such that $\pi \Delta_P^\ell \pi^\dagger = \Delta_Q^\ell$. Rearranging, we have $\Delta_P^\ell \pi \Delta_Q = \Delta_Q \pi \Delta_P^\ell$. Writing $K$ for this term, $[I \otimes M_Q KM_Q^\dagger P[I \otimes N_P \pi^\dagger N_Q] = Q$. Thus $P' \sim Q$. ■

We now apply Theorem 22 to prove the following result relating $\mathbb{Z}(\ell)(P)$ and $|P|_{\text{CZ, } \ell}$.

We emphasize that the number of qubits on which $P$ acts is an unspecified parameter in both of these functions.

**Theorem 23** Let $P$ commute with $Z^i$.

* $|P|_{\text{CZ, } \ell} = 0$ iff $\mathbb{Z}(\ell)(P) \cong \{1,1,\ldots\}$.

* $|P|_{\text{CZ, } \ell} = 1$ iff $\mathbb{Z}(\ell)(P) \cong \{1,-1,1,-1,\ldots\}$

* $|P|_{\text{CZ, } \ell} \leq 2$ iff $\mathbb{Z}(\ell)(P)$ is congruent to some multi-set $S$ of unit norm complex numbers which come in conjugate pairs.

**Proof.** The first and second statements follow immediately from Theorem 22 and the calculations $\mathbb{Z}(\ell)(I) = \{1,1,\ldots\}$ and $\mathbb{Z}(\ell)(Q^{(\ell,m)}) = \{1,-1,1,-1,\ldots\}$. To perform the relevant calculation for the third statement, we will use Corollary 20.

Let $\ell$ be the highest order qubit. For $\delta$ a diagonal real operator acting on all qubits but $\ell$, define $\Phi(\delta)$ by

$$\Phi(\delta) = R_\ell(\delta)$$

By construction, $|\Phi(\delta)|_{\text{CZ, } \ell} \leq 2$. We compute $\mathbb{Z}(\ell)(\Phi(\delta)) = \{e^{2i\delta_0}, e^{-2i\delta_0}, e^{2i\delta_1}, e^{-2i\delta_1}, \ldots\}$. ($\Rightarrow$) Write the entries of $S$ as $e^{i\theta}, e^{i\theta}, e^{-i\theta}, e^{-i\theta}, \ldots$, and let $\theta$ be the real diagonal operator acting on all qubits but $\ell$ whose diagonal entries are $\theta_0, \theta_1, \ldots$. By construction, $\mathbb{Z}(\ell)(\Phi(\theta/2)) = S$, and $S \cong \mathbb{Z}(\ell)(Q)$ by hypothesis. By Theorem 22, $\Phi(\theta/2) \sim Q$ are $\ell$-equivalent. It follows that $|Q|_{\text{CZ, } \ell} = |(\Phi(\theta/2))|_{\text{CZ, } \ell} \leq 2$.

($\Leftarrow$) By hypothesis $|Q|_{\text{CZ, } \ell} \leq 2.$ If in fact $|Q|_{\text{CZ, } \ell} = 0,1$, note by the first two statements of the Theorem, which have been proven, the $\ell$-mux-spectrum of $Q$ has the desired property. Thus we assume $|Q|_{\text{CZ, } \ell} = 2$. Let $\ell'$ be a circuit in which this minimal CZ count is achieved. By Corollary 20, we can find an equivalent circuit $\ell''$ of the following form.

We have drawn the CZs with different lower contacts, but of course they might be the same. Actually, we prefer the latter case, and ensure it by incorporating swaps into $B, C$ if necessary. We take a cosine-sine decomposition (see Equation 2) of $B$

We have drawn the CZs with different lower contacts, but of course they might be the same. Actually, we prefer the latter case, and ensure it by incorporating swaps into $B, C$ if necessary. We take a cosine-sine decomposition (see Equation 2) of $B$.
Note that the $B_L$ and $B_R$ gates commute with the CZs. Thus $Q \sim \Phi(\beta)$. By Theorem 22, the $\mathcal{Z}^{(i)}(Q) \cong \mathcal{Z}^{(i)}(\Phi(\beta))$. But we have already seen that $\mathcal{Z}^{(i)}(\Phi(\cdot))$ always consists of conjugate pairs of unit-norm complex numbers. ■

While we cannot completely characterize operators with $|\cdot|_{CZ;\ell} = 3$, we can characterize circuits which compute them.

**Theorem 24** Fix a qubit $\ell$, and suppose $M$ commutes with $\mathcal{Z}^{(i)}$. Suppose $|M|_{CZ,j} = 3$, and let $\mathcal{C}$ be a $\mathcal{CZ}^{(j)}$-circuit exhibiting this bound. Then all one-qubit gates of $\mathcal{C}$ on $\ell$ are diagonal or anti-diagonal.

**Proof.** Consider $M, \mathcal{C}$ satisfying the hypothesis. Without loss of generality, $\ell = 1$ and $\mathcal{C}$ takes the form

![Diagram](image)

The CZs may have originally had different terminals, but we can incorporate swaps into $E, F, G, H$ to suppress this behavior. Evidently this will not affect the hypothesis or conclusion.

(*) Define $P$ by

![Diagram](image)

If $PX^{(2)}$ commutes with $\mathcal{Z}^{(2)}$, then return to (*) and replace $G$ by $GX^{(2)}$, $H$ by $X^{(2)}H$, and $h$ by $Z^{(1)}h$. This does not affect the conclusion, and by Equation 1, the resulting circuit still computes $M$. We have ensured that if one of $P, PX^{(2)}$ commutes with $\mathcal{Z}^{(2)}$, then it is $P$.

Define $a, b, Q$ by

![Diagram](image)

Note $|Q|_{CZ,1} = |M|_{CZ,1}$. We also have $Q = [a \otimes I]P[b \otimes I]$, hence are in the situation of Equation 9. Lemma 13 allows us to reduce to the following cases.

**Case I.** $a, b$ are diagonal, or $aX^{(1)}, bX^{(1)}$ are diagonal. In either case, Corollary 15 applied to the circuits defining $a, b$ shows that $e, f, g, h$ are each diagonal or anti-diagonal.

**Case II.** $Q$ takes the form

![Diagram](image)
The cosine-sine decomposition (see Equation 2) of \( V \) along qubit 2 determines unitary operators \( R,S \) and a real diagonal operator \( \delta \) such that:

\[
\begin{array}{cccc}
1 & 2 \\
\downarrow & \downarrow \\
R & S
\end{array}
= \begin{array}{cccc}
2 & 1 \\
\downarrow & \downarrow \\
R_\gamma(\delta) & \ \ \\
S & \ \ \\
\end{array}
\tag{16}
\]

We substitute, commute the \( S,T \) outwards past \( C,C' \), and decompose the diagonals \( C,C' \).

\[
\begin{array}{cccc}
1 & 2 \\
\downarrow & \downarrow \\
R & R_\gamma(\theta) & R_\gamma(\delta) & R_\gamma(\phi) & \ \ \\
S & \ \ \\
\end{array}
\]

Evidently \( S^{(1)}(Q) \) depends only on \( \theta, \delta, \phi \). We calculate that, up to a global scalar multiple, \( S^{(1)}(Q) \) consists of the roots of the following quadratics in \( T \), where

\[
T^2 - 2T(\cos(2\theta + 2\phi) \cos(|i\rangle \langle i|)^2 + \cos(2\theta - 2\phi) \sin(|i\rangle \langle i|)^2) + 1
\]

The equations being real, each has complex conjugate roots. By Theorem 23, \( |M|_{\text{CZ}, \ell} = |Q|_{\text{CZ}, \ell} = 2 \), contrary to hypothesis.

**Case III.** We have already ensured that \( P \), rather than \( PX^{(2)} \), commutes with \( Z^{(2)} \). We replace \( a,b \) by the \( a',b' \) of Corollary 17. We demultiplex \( P \) (see Equation 3) to obtain a decomposition of the following form, where \( D \) is diagonal.

\[
\begin{array}{ccc}
P & = & S \\
\downarrow & & \downarrow \\
D & & R
\end{array}
\]

We have \( |Q|_{\text{CZ}, \ell} = |[a' \otimes I]P[b' \otimes I]|_{\text{CZ}, \ell} = |[a' \otimes I][I \otimes R][I \otimes S][b' \otimes I]|_{\text{CZ}, \ell} = |[I \otimes R][a' \otimes I]D[b' \otimes I][I \otimes S]|_{\text{CZ}, \ell}.

By construction, \( |P|_{\text{CZ}, \ell} = |D|_{\text{CZ}, \ell} = 1 \). Thus if \( D = |0\rangle \langle 0| \otimes D_0 + |1\rangle \langle 1| \otimes D_1 \), then by Theorem 23, the entries of \( D_0D_1 \) are \( e^{i\theta}\{1,-1,1,-1,\ldots\} \). It follows that \( D \) can be written as

\[
\begin{array}{ccc}
D & = & R_\gamma(-\theta/2) \\
\downarrow & & \downarrow \\
\pi & & \pi^\dagger
\end{array}
\]

for some permutation \( \pi \). Evidently \( D_0 \) commutes past \( b' \) and does not affect \( S^{(1)}(a'Db') \); we may as well assume that it is 1.

To compute the invariants, we note that if \( K = |0\rangle \langle 0| \otimes K_0 + |1\rangle \langle 1| \otimes K_1 \) then \( K_1^\dagger K_0 = (x^{(1)} K_1^\dagger x^{(1)} K) |0\rangle \langle 0| \).

We set \( N := x^{(1)}([a' \otimes I]D[b' \otimes I])^\dagger x^{(1)}[a' \otimes I]D[b' \otimes I] \). Applying Equation 1, \( N \) is computed by the following circuit.
The condition on \( a' \) implies that \((a')^\dagger X^{(1)}a'X^{(1)}\) is diagonal. It follows that the subcircuit sandwiched between the two CZs computes a diagonal operator, and so the CZs cancel. Then the \( \pi, \pi^\dagger \) pair on the left cancel. The \( \pi^\dagger Z^{(m)}\pi \) term on the right commutes past the \( (b')^\dagger \). What remains is a circuit of the form

\[
\begin{array}{c}
F \\
\pi \\
\pi^\dagger
\end{array}
\]

By construction, \( N \) commutes with both \( Z^{(1)} \) and \( Z^{(2)} \). It follows that \( F \) is diagonal. Then \( f = \langle 0 |^{(1)} F | 0 \rangle^{(1)} \) is some one-qubit diagonal acting on \( m \). We have \( \langle 0 |^{(1)} N | 0 \rangle^{(1)} = \pi^\dagger Z^{(2)} \pi f^{(2)} \). Denote by \( f_0, f_1 \) the entries of \( f \). Then \( \mathfrak{Z}^{(1)}([a' \otimes I]D[b' \otimes I]) \) is given by the entries of \( \langle 0 |^{(1)} N | 0 \rangle^{(1)} \), which are \( f_0, f_1, -f_0, -f_1 \), and moreover \( f_0 \) will occur with the same multiplicity as \( -f_1 \); likewise \( -f_0 \) will occur with the same multiplicity as \( f_1 \). We see that \( \sqrt{-f_0/f_1} \mathfrak{Z}^{(1)}([a' \otimes I]D[b' \otimes I]) \) come in conjugate pairs. By Theorem 23, \( ||[a' \otimes I]D[b' \otimes I]||_{CZ,1} \leq 2 \). Since \( |M|_{CZ,1} = |Q|_{CZ,1} = ||[a' \otimes I]D[b' \otimes I]||_{CZ,1} \), we are done. ■

3.4 Corollaries

The PERES is a three-qubit operator from classical reversible logic, defined by \( \text{PERES}^{(\ell,m,n)} = C^{(\ell)}X^{(m)} \cdot CC^{(\ell,m)}X^{(n)} \). It can be a useful alternative to the TOFFOLI for implementing classical reversible operators [11].

**Corollary 25** \( |\text{PERES}|_{CZ} = 5 \).

**Proof.** As is clear from its definition, the PERES gate can be implemented by the circuit of Figure 1, save the rightmost CNOT. Thus, \( |\text{PERES}|_{CZ} \leq 5 \). On the other hand, it also follows from the definition that any circuit for the PERES can, with the addition of a single CNOT, become a circuit for the TOFFOLI. Thus \( |\text{PERES}|_{CZ} \geq |\text{TOFFOLI}|_{CZ} - 1 = 5 \), and all inequalities are equalities. ■

In a different direction, we consider below multiply-controlled Z gates:

**Corollary 26** \( |(n - 1) - \text{controlled} - Z|_{CZ} \geq 2n \) for any \( n \geq 3 \).

**Proof.** We proceed by induction on \( n \). Suppose the Corollary is false; choose minimal falsifying \( n \), and a falsifying circuit \( \mathcal{C}' \). By Theorem 10, \( n > 2 \). As before, at least three CZ gates are incident to each qubit, and counting shows that at least one, say \( \ell \) touches exactly three. As before, we can assume that all one-qubit operators which appear on \( \ell \) are diagonal. Form the circuit \( \mathcal{C}' = |1|^{(\ell)} \mathcal{C}^{(\ell)} |1|^{(\ell)} \) by replacing every gate \( g \) of \( \mathcal{C} \) with \( g' = |1|^{(\ell)} g |1|^{(\ell)} \). This has no effect on gates which do not touch \( \ell \); it turns one-qubit gates on \( \ell \) into scalars, and replaces \( CZ^{(\ell,s)} \) with \( Z^{(s)} \). At any rate, \( \mathcal{C}' \) is a CZ-circuit on \( (n - 1) \) qubits which computes the \( (n - 2) \)-controlled-Z. We deduce by induction that it contains at least \( 2(n - 1) \) CZ gates. Adding the (at least) three CZs incident to \( \ell \), there are at least \( 2n + 1 \) total CZs in \( \mathcal{C}' \). ■
4 Three-qubit diagonal operators

We give here a complete classification of three-qubit diagonal operators by their CZ-cost. Throughout this section, we label our qubits 1, 2, 3, from high order to low. In keeping with our usual convention, we abbreviate \( |i\rangle^{(1)} |j\rangle^{(2)} |k\rangle^{(3)} \) by \( D_{ijk} \). We also write \( \Delta(\eta) \) for the one-qubit gate given by \( |0\rangle \langle 0| + |1\rangle \langle 1| \eta \). Define

\[
\lambda_1(D) = \frac{D_{011}D_{000}}{D_{001}D_{010}}, \quad \lambda_2(D) = \frac{D_{101}D_{000}}{D_{100}D_{001}}, \quad \lambda_3(D) = \frac{D_{110}D_{000}}{D_{100}D_{010}}, \quad \xi(D) = \frac{D_{111}D_{000}}{D_{100}D_{010}D_{001}}
\]

Then any three-qubit diagonal \( D \) admits the expansion

\[
D = D_{000} \cdot \Delta(\frac{D_{110}}{D_{000}})^{(1)} \cdot \Delta(\frac{D_{010}}{D_{000}})^{(2)} \cdot \Delta(\frac{D_{001}}{D_{000}})^{(3)} \cdot \text{diag}(1, 1, 1, \lambda_1(D), 1, \lambda_2(D), \lambda_3(D), \xi) \]

The \( \lambda_i(D) \) are multiplicative, \( \lambda_i(DD') = \lambda_i(D)\lambda_i(D') \), and likewise for \( \xi \). We denote by \( S(D) \) the ordered quadruple \( (\lambda_1, \lambda_2, \lambda_3, \xi) \).

**Observation 27** Given two three-qubit diagonals \( D, D' \), we have \( S(D) = S(D') \) iff \( S(D^\dagger D') = (1, 1, 1, 1) \) iff \( D^\dagger D' \) is a tensor product of one-qubit diagonal operators. It follows that \( S(D) = S(D') \implies |D|_{\text{CZ}} = |D'|_{\text{CZ}} \).

**Observation 28** \( \mathcal{Z}(D) = \{1, \lambda_j(D)^\dagger, \lambda_k(D)^\dagger, \xi(D)^\dagger \lambda_i(D)\} \) where \( \{i, j, k\} = \{1, 2, 3\} \).

**Lemma 29** Let \( D \) be a three-qubit diagonal operator. Then \( D \) can be implemented in a three-qubit CZ circuit with:

- 0 CZs on touching qubit 1 iff \( S(D) = (\xi, 1, 1; \xi) \)
- 1 CZ touching qubit 1 iff \( S(D) = (\xi, -1, -1; \xi), (-\xi, 1, -1; \xi), (\xi, 1, 1; -\xi) \)
- 2 CZs touching qubit 1 iff \( S(D) = (a, b, c; abc), (a, b, c; ab/c), (a, b, c; ac/b) \).

**Proof.** This is just a translation of Theorem 23 using Observation 28, involving a straightforward but tedious calculation which we omit. ■

We write \( s(D) \) for \( (\lambda_1(D), \lambda_2(D), \lambda_3(D); \xi(D)) \), where we ignore the order of the \( \lambda_i \).

**Observation 30** Given two three-qubit diagonals \( D, D' \), \( s(D) = s(D') \) if and only if there exist one-qubit diagonals \( d, d', d'' \) and a wire permutation \( \omega \) such that \( D = (d \otimes d' \otimes d'') \cdot \omega D \omega^\dagger \). Thus \( s(D) = s(D') \implies |D|_{\text{CZ}} = |D'|_{\text{CZ}} \).

**Theorem 31** Let \( D \) be a three-qubit diagonal operator. Then there exists a CZ-circuit for \( D \) containing

- 0 CZs iff \( s(D) = (1, 1, 1; 1) \).
- 1 CZ iff \( s(D) = (1, 1, -1; -1) \).
- 2 CZs iff \( s(D) = (1, 1, \xi; \xi), (1, -1, -1; 1) \).
- 3 CZs iff \( s(D) = (1, 1, \xi; \xi), (\xi, -1, -1; \xi), (-\xi, 1, -1; \xi) \).
- 4 CZs iff \( s(D) = (a, b, c; ab/c) \).
- 5 CZs iff \( s(D) = (a, b, c; ab/c), (a, b, c; abc) \).
6 CZs always

**Proof.** We assume without loss of generality that $D$ takes the form $\text{diag}(1, 1, 1, \lambda_1, 1, \lambda_2, \lambda_3, \xi)$. We number the qubits 1, 2, 3 from high-order to low-order.

$(\Leftarrow)$. We can assume that in fact $S(D)$ takes the form given. Our constructions will use the $\text{CX}$, which may be replaced by the $\text{CZ}$ at the cost of inserting HADAMARD gates.

**Case 0.** $S(D) = (1, 1, 1; 1) \implies D = I$.

**Case 1.** $S(D) = (1, 1, -1; -1) \implies D = \text{CZ}^{(1, 2)}$.

**Case 2a.** $S(D) = (\xi, 1, 1; \xi)$. Fix $\eta = \sqrt{\xi}$;

**Case 2b.** $S(D) = (1, -1, -1; 1) \implies D = \text{CZ}^{(1, 3)}\text{CZ}^{(1, 2)}$.

**Case 3a.** $S(D) = (\xi, 1, 1; \xi)$. By Case 2a, the CZ can be implemented in a circuit containing 2 CZs. It follows that any operator that can be implemented with $n > 0$ CZs can be implemented with $n + 1$. Thus since $D$ can be implemented with 2 CZs, it can be implemented with 3.

**Case 3b.** $S(D) = (\xi, -1, -1; \xi)$. Fix $\eta = \sqrt{\xi}$;

**Case 3c.** $S(D) = (-\xi, 1, 1; \xi)$. Fix $\eta = \sqrt{-\xi}$.

**Case 4.** $S(D) = (a, b, c; ab/c)$. Fix square roots $\alpha, \beta, \gamma$ for $a, b, c$;

**Case 5a.** $S(D) = (a, b, c; ab/c)$. As $D$ can be implemented with 4 CZs, it can be implemented with 5.

**Case 5b.** $S(D) = (a, b, c; abc)$. Fix square roots $\alpha, \beta, \gamma$ for $a, b, c$;
Case 6. Any n-qubit diagonal operator has CZ-cost bounded by $2^n - 2$. See [3] or the Appendix.

$\Rightarrow$.

Case 0. $D$ must be locally equivalent to $I$, hence $s(D) = (1, 1, 1; 1)$.

Case 1. $D$ must be locally equivalent to some CZ, hence $s(D) = (1, 1, -1; -1)$

Case 2 Suppose there exists a minimal implementation of $D$ in which both CZ gates connect the same two qubits. Then $D$ is locally equivalent to a two-qubit diagonal; in which case one can compute $s(D) = (\xi, 1, 1; \xi)$

Otherwise, there is a minimal implementation of $D$ in which the two CZ gates are $CZ^{(i,j)}, CZ^{(j,k)}$. By Corollary 20, we may pass to an implementation with only diagonal one-qubit gates along $j$; by Corollary 16, we may pass to an implementation with only diagonal one-qubit gates along $i, k$ as well. But then $D$ is locally equivalent to $CZ^{(i,j)}CZ^{(j,k)}$ and we may compute $s(D) = (1, -1, -1; 1)$.

Case 3. It suffices to show that $|D|_{CZ,j} \leq 1$ for some $j$. For, if $|D|_{CZ,j} = 0$, then $D$ is a two-qubit diagonal, with $s(D) = (\xi, 1, 1; \xi)$, and if $|D|_{CZ,j} = 1$, then by Lemma 29, $s(D) = (\xi, 1, -1; \xi)$ or $(\xi, -1, 1; \xi)$.

Consider an implementation of $D$ containing three CZs. We have $|D|_{CZ,\ell} \leq 1$ for some $\ell$ unless the CZs are distributed so that each qubit touches exactly two. By Corollary 20, we can assume the circuit contains only diagonal gates on qubit $j$; it follows by inspection that $D \sim_j CZ^{(i,j)}CZ^{(j,k)}$. But we have already determined that $|CZ^{(i,j)}CZ^{(j,k)}|_{CZ,j} = 1$.

Case 4. Consider an implementation of $D$ containing four CZs. If any qubit touches fewer than two CZs, we reduce to the previous case and observe that the desired condition on $s$ holds. Thus suppose each qubit touches at least two CZs. Then there are only two possibilities for the number of CZs touched by each qubit: $(2, 2, 4)$ and $(2, 3, 3)$.

For the configuration $(2, 2, 4)$, say qubits $\ell, m$ touch two CZs and qubit $n$ touches four. Note that no CZs connect $\ell, m$. Thus we may assume by Corollary 20 all one-qubit gates on $\ell, m$ are diagonal. By Proposition 5, the desired condition holds.

For the configuration $(2, 3, 3)$, say qubit 1 touches two CZs and qubits 2, 3 touch three. Then there are two CZs connecting qubits 2 and 3, one connecting qubits 1 and 3 and one connecting qubits 1 and 2. By Corollary 20, we ensure that all one-qubit gates on qubit 1 are diagonal. If the CZs connecting qubits 2 and 3 are outermost, $D \sim_\ell CZ^{(1,2)}CZ^{(1,3)}$, hence can be implemented with three CZs by case 3. Thus suppose one of the CZs incident on qubit 1 is outermost; without loss of generality let it be $CZ^{(1,3)}$. Then we have an equation of the form $ACZ^{(1,3)}u^{(3)} = D$ where by construction $|A|_{CZ;\ell} = 1$. We compute $\mathfrak{S}^{(1)}(A) = \mathfrak{S}^{(1)}(D(u^T)^{(3)})CZ^{(1,3)}$. Decompose $u^T = e^{i\theta}R_z(\alpha)R_y(\beta)R_z(\gamma)$; then $\mathfrak{S}^{(\ell)}(A)$ is given by the roots of the equations

$$x^2 - \cos(2\beta)(1 - \lambda_2)x - \lambda_2 = 0$$
$$x^2 - \cos(2\beta)(\lambda_3 - \xi/\lambda_1)x - \lambda_3 \xi/\lambda_1 = 0$$

For these to have any hope of having roots $p, p, -p, -p$, they must at least have the same constant terms – either both $p^2$ or both $-p^2$. In any event, $\lambda_3 \xi = \lambda_2 \lambda_1$ and $S(D) = (\lambda_1, \lambda_2, \lambda_3; \lambda_1 \lambda_2 / \lambda_3)$ as desired.

Case 5. It suffices by Lemma 29 to show that $|D|_{CZ,\ell} \leq 2$ for some $\ell$. Suppose not; then in any five CZ implementation for $D$, each qubit must touch three CZs. It follows that two of the qubits, say $\ell, m$ touch exactly three CZs, and the remaining qubit touches four. By
Theorem 24, all one-qubit gates on \( \ell, m \) are diagonal or anti-diagonal. Enough applications of Equation 1 will ensure that all one-qubit gates on \( \ell, m \) are in fact diagonal. Move the CZ which connects \( \ell, m \) to the edge of the circuit. This yields \( D = \text{CZ}(\ell,m)A \), where \( |A|_{\text{CZ},\ell} \leq 2 \). By Lemma 29, it follows that \( |D|_{\text{CZ},\ell} \leq 2 \) as well.

We have not allowed yet for the possibility of ancillae. However, further analysis, conducted in Section 5, will extend the results on the three-qubit CCZ, TOFFOLI, and PERES to the case when ancillae are allowed.

5 Circuits with ancillae

The proof of Theorem 31\((\Rightarrow)4,5\) made repeated use of the assumption that only three qubits were present. It moreover used in a crucial way the implication \( |D|_{\text{CZ},\ell} \leq 2 \Rightarrow \cdots \) of Lemma 29. This is problematic when ancillae are present: we can have \( |D|_{\text{CZ},\ell} > 2 \) but \( |D \otimes I|_{\text{CZ},\ell} \leq 2 \). In particular, \( S(1) = \{1,1,1,1\} \Rightarrow |\text{CCZ}(1,2,3)|_{\text{CZ},1} \geq 3 \), however, \( S(1)(\text{CCZ}(1,2,3) \otimes I(4)) = \{1,1,1,-1,1,1,-1\} \), so by Theorem 23, \( |\text{CCZ}(1,2,3) \otimes I(4)|_{\text{CZ},1} = 2 \). Indeed:

\[
\begin{array}{c}
\text{Nonetheless, Theorem 10 remains true when ancillae are present, as we show below.}
\end{array}
\]

**Proposition 32** Let \( A \) be a unitary operator; let \( C \) be qubit minimal among CZ-circuits such that \( |C|_{\text{CZ}} = |A|_{\text{CZ}} \) and \( C \) computes \( A \otimes I_2^k \). Then every ancilla in \( C \) touches at least three CZ gates.

**Proof.** Fix an ancilla qubit \( a \). If no CZ gates touch \( a \), then it may be removed. If one (respectively two) CZ touches \( a \), then by Corollary 15 and Equation 1 (respectively Corollary 20), then there is a circuit with no more CZs in which the only one-qubit gates on \( a \) are diagonal.

Now form the circuit \( \langle 0 \rangle^{(a)} C \langle 0 \rangle^{(a)} \) as in the proof of Corollary 26. This circuit computes the operator \( A \) using one fewer ancilla, and has no more CZs than \( C \).

**Proposition 33** For two-qubit operators, \( |\cdot|_{\text{CZ}} = |\cdot|_{\text{CZ}} \).

**Proof.** If no ancillae are needed to minimize CZ-count, then the result holds. Otherwise, each ancilla used in a qubit-minimal CZ-minimal implementation must touch at least three CZ-gates. Thus \( |\cdot|_{\text{CZ}} \geq |\cdot|_{\text{CZ}} \geq 3 \). However it is known that two-qubit operators have \( |\cdot|_{\text{CZ}} \leq 3 \). Thus all the inequalities are equalities.

**Proposition 34** \(|\text{CCZ}|_{\text{CZ}} = 6\).
Proof. The circuit of Equation 6 establishes $|\text{CCZ}|_{\text{CZ}} \leq 6$. Suppose $|\text{CCZ}|_{\text{CZ}}^a = k < 6$, and let $\mathcal{C}$ be a qubit-minimal circuit implementing the CCZ using exactly $k$ CZs. By Proposition 32, every ancilla qubit comes into contact with at least three CZs.

For any non-ancilla $\ell$, we have $\mathcal{Z}(\ell) (\text{CCZ}) = \{1, 1, 1, -1, 1, 1, -1, \ldots\}$. By Theorem 23 at least two CZs must touch each non-ancilla qubit, and we have seen in Proposition 32 that at least three CZs touch each ancilla qubit. Thus if there are $a$ ancillas, then at least $(6 + 3a)/2$ CZs must appear in the circuit. From $(6 + 3a) < 6$ we deduce $a < 2$. We have already dealt with the $a = 0$ case in Theorem 10, and can therefore assume $a = 1$. It follows that at least $9/2$ CZs appear in the circuit; since CZs come in whole numbers, we must have $k = 5$ of them.

The ancilla must touch at least three CZs; each non-ancilla must touch at least two. For the total number to be five, we must have two of the non-ancilla $z$ and the ancilla $a$ touching three. By Corollary 20, we can assume that the only one-qubit operators appearing on $x_1$, $x_2$ are diagonal.

Assume without loss of generality that there are more CZs connecting $x_1$, $z$ than $x_2$, $z$. Then there are only four possibilities regarding which wires are connected by CZs.

<table>
<thead>
<tr>
<th>I</th>
<th>(x_1, x_2)</th>
<th>(x_1, x_2)</th>
<th>(z, a)</th>
<th>(z, a)</th>
<th>(z, a)</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>(x_1, x_2)</td>
<td>(x_1, z)</td>
<td>(x_2, a)</td>
<td>(z, a)</td>
<td>(z, a)</td>
</tr>
<tr>
<td>III</td>
<td>(x_1, z)</td>
<td>(x_1, z)</td>
<td>(x_2, a)</td>
<td>(x_2, a)</td>
<td>(z, a)</td>
</tr>
<tr>
<td>IV</td>
<td>(x_1, z)</td>
<td>(x_1, a)</td>
<td>(x_2, z)</td>
<td>(x_2, a)</td>
<td>(z, a)</td>
</tr>
</tbody>
</table>

Evidently case (I) cannot implement the CCZ, as it does not entangle $x_1$, $x_2$ with $z$. As for the remaining cases, we will show that any circuit with those CZ gates can be transformed so that (*) a CZ which does not touch the ancilla is leftmost among the CZs, and (***) one of the $x$-qubits on which the leftmost CZ gate acts meets only diagonal one-qubit operators.

By Corollary 20, we can assume no non-diagonal one-qubit gates appear on $x_1$. In case (II), the $(x_1, x_2)$ CZ can therefore only be obstructed from moving by the $(x_1, a)$. This can be on only one side, so the $(x_1, x_2)$ can be moved outwards to the other. Similarly, in case (III), an $(x, z)$ can only be obstructed by $(z, a)$ and the other $(x, z)$. In this case, the second $(x, z)$ is obstructed on only one side and can be moved to the edge. In case (IV), we use Corollary 20 to both the $x_1$ and $x_2$ qubits to clear them of non-diagonal gates; the possible additional one-qubit gates will only fall on the $z$ and $a$ qubits. Now the $(x_1, z)$ can only be obstructed by the $(x_2, z)$ and the $(z, a)$, and also the $(x_2, z)$ can only be obstructed by $(z, a)$ and $(x_1, z)$.

Thus one of $(x_1, z)$ and $(x_2, z)$ can be made outermost. Finally, if the gate in question is rightmost rather than leftmost, we may reverse the circuit and invert every gate: the CCZ and CZ are self-adjoint.

Now we derive a contradiction. We have an equation of the form $\text{CCZ}^{(x,z)} = A \cdot \text{CZ}^{(x,z)} u^{(z)}$ where by construction $A$ commutes with $Z^{(z)}$ and $|A|_{\text{CZ}} \leq 1$. On the other hand, we compute $\mathcal{Z}(\ell)(\text{CCZ}^{(x,z)})(u^{(z)})^{(z)} \text{CZ}^{(x,z)}$. Taking a “$\text{XYZ}$” decomposition, $u^{(z)} = R_z(\alpha) R_y(\delta) R_z(\beta)$, we compute $\mathcal{Z}(\ell)(A) = \{1, -1, e^{2i\delta}, e^{-2i\delta}, 1, -1, e^{2i\delta}, e^{-2i\delta}, \ldots\}$, which is not congruent to $\{1, 1, 1, 1, \ldots\}$ or $\{-1, -1, 1, \ldots\}$. By Theorem 23, $|A|_{\text{CZ}} \geq 2$.

Corollary 35 $|\text{TOFFOLI}|_{\text{CZ}}^a = 6$ and $|\text{PERES}|_{\text{CZ}}^a = 5$. 

24
6 Conclusion

While our work is primarily focused on quantum circuit implementations, the TOFFOLI gate originally arose as a universal gate for classical reversible logic [20]. In contrast, the NOT and CNOT gates are not universal for reversible logic: their action on bit-strings is affine-linear over over $\mathbb{F}_2$, and thus the same is true for any operator computed by any circuit containing only these gates.

Augmenting CNOT gates with single-qubit rotations to express the TOFFOLI gate provides the lacking non-linearity. Thus the number of one-qubit gates (excluding inverters) needed to express the TOFFOLI, or more generally any reversible computation, can be thought of as a measure of its non-linearity. It would be interesting to minimize the number of one-qubit gates, rather than CNOTs, which appear in implementations. This inverted cost model is particularly relevant to some quantum implementation technologies. We therefore propose the following challenge: How many one-qubit gates are needed to implement the TOFFOLI? Furthermore, are there circuits that simultaneously minimize the number of CNOT and one-qubit gates?

In a different direction, recall our results showing that diagonality and block-diagonality of an operator impose strong constraints on small circuits that compute this operator. We believe that other conditions may act in a similar way. In particular, we ask what can be said about minimal quantum circuits for operators computable by classical reversible circuits, i.e., operators expressed by 0-1 matrices? We do not know the answer even for three-qubit operators. In particular, the CNOT-cost of the controlled-swap (Fredkin gate) remains unresolved.

Closest to our present work, the exact CNOT-cost of the $n$-qubit analogue of the TOFFOLI gate remains unknown. We have shown that $2n$ CNOTs are necessary if ancillae are not permitted, but already for $n = 4$ we only know $8 \leq |\text{CCCZ}|_\text{CZ} \leq 14$, where the upper bound is provided by a generic decomposition of diagonal operators [3]. Existing constructions of the $n$-qubit TOFFOLI gate require a quadratic number of CNOT gates without the use of ancillae. With one ancilla, such constructions require linearly many CNOTs, but the leading coefficient is in double-digits [1, 11].

Finally, we hope that our proof can be simplified and our techniques generalized. In particular, we have relied on repeated comparisons of various Cartan decompositions to each other. A careful study of the proof will reveal the simultaneous use of six Cartan decompositions — those corresponding to conjugation by $X$ and $Z$ on each of three wires. Keeping track of these decompositions in a more systematic manner may simplify the proof, while using additional decompositions may lead to new results.

A related issue is determining the power of the qubit-by-qubit gate counting we have used. It follows from the results of [17] that, for $U$ an $n$-qubit operator, $|U|_{\text{CZ},\ell} < 6(n - 1)$, so no technique relying solely on this process can achieve better than a quadratic lower bound. On the other hand, we have only been able to characterize when $|U|_{\text{CZ},\ell} > 2$, and thus have achieved only linear lower bounds. Perhaps, these ideas can help toward the questions above.

25
References


