Complexity of reversible circuits and their quantum implementations

Nabila Abdessaied[a,b], Matthew Amy[c], Rolf Drechsler[a,b], Mathias Soeken[a,b]

[a] *Faculty of Mathematics and Computer Science, University of Bremen, Germany*
[b] *Cyber-Physical Systems, DFKI GmbH, Bremen, Germany*
[c] *Department of Computer Science , Toronto, Canada*

Abstract

We provide an extensive overview of upper bounds on the number of gates needed in reversible and quantum circuits. As reversible gate libraries we consider single-target gates, mixed-polarity multiple-controlled Toffoli gates, and the set consisting of the NOT, the CNOT, and the two-controlled Toffoli gate. As quantum gate libraries we consider the semi-classical NCV library (consisting of NOT, CNOT, and the *square-root* of NOT called *V*) as well as the universal and commonly used Clifford+*T* gate library. Besides a summary of known bounds, the paper provides several new and tighter bounds. Several synthesis approaches and mapping schemes were used to calculate the bounds.

Keywords: Complexity analysis, reversible functions, reversible circuits, quantum circuits, upper bounds, synthesis, technology mapping.

1. Introduction

Reversible circuits and their implementations in quantum computers has attracted many researchers in the last decades. Reversible computation [1] has proven itself as a very promising research area, especially for applications to emerging technologies. This is confirmed by its results in emerging applications such as quantum computation [2], superconducting quantum interference devices (SQUID) [3], and nanoelectromechanical systems (NEMS) [4], but also in low power electronics [1, 5].

As a result of its applicability to such emerging technologies, synthesis of reversible logic has been intensively studied and several approaches have been proposed [6, 7, 8]. To compare the efficacy of different synthesis approaches, the resulting circuits are evaluated in terms of cost metrics which depend on the target application. Standard application-independent metrics used include the number of gates and the gate delay, also called the circuit depth. To further incorporate technology-dependent information, the number of application-specific gates (e.g. quantum phase gates) based on a given library is often compared. Adding helper lines (so-called *ancillas*) to the circuit for temporary computations offers to reduce the gate count and the depth at the expense of space. For more details the reader is referred to [9].

In this paper we derive tighter upper bounds for the number of gates that are required to implement a reversible function in a reversible or quantum circuit. This is important as an approach to understand the complexity of reversible circuits, but also to give an overall quality-measure of the different reversible synthesis methods. Previous research has investigated this topic based on specific synthesis algorithms and using a specific gate library [10, 11]. Further, the exact bounds are known for reversible circuits over up to four variables [12, 13, 14].

Our work is both an improvement over previous reported upper bounds and an extension of the upper bounds to more gate libraries. As reversible gate libraries we consider single-target gates and their specializations. *Single-target gates* (ST) are reversible gates that can invert one line, called the target line, based on the other lines. In the most general case, the target line is inverted, if a control function based on the other lines evaluates to true. The more specialized but still universal *mixed-polarity multiple-controlled Toffoli* (MPMCT) gate library restricts the control function to product terms. Finally, the *NOT, CNOT, Toffoli* (NCT) library restricts the product terms to at most two literals of which all must be of positive polarity. As quantum gate libraries we consider the semi-classical *NCV library* [15] (consisting of NOT, CNOT, and the *square-root* of NOT) as well as the *Clifford+T* gate library. The latter library is of particular interest in the implementation of fault-tolerant quantum circuits [16, 17].

The paper is organized as follows. Section 2 gives a brief background on *exclusive sum-of-products* (ESOP) expressions, reversible circuits, and quantum circuits. Section 3 outlines the general procedure to find the upper bounds and gives an overview of all presented bounds. Sections 4–8 then provide bounds based on the five considered reversible and quantum gate libraries. Section 9 summarizes all results.

2. Background

2.1. Boolean Functions

Let $\mathbb{B} = \{0, 1\}$ denote the *Boolean values*. Then we refer to $\mathcal{B}_{n,m} = \{f \mid f\colon \mathbb{B}^n \to \mathbb{B}^m\}$ as the set of all *Boolean multiple-output functions* with n inputs and m outputs. There are 2^{m2^n} such Boolean functions. We write $\mathcal{B}_n = \mathcal{B}_{n,1}$ and assume that each $f \in \mathcal{B}_n$ is represented by a propositional formula over the variables $x_1, \ldots, x_n$. Furthermore, we assume that each function $f \in \mathcal{B}_{n,m}$ is represented as a tuple $f = (f_1, \ldots, f_m)$ where $f_i \in \mathcal{B}_n$ for each $i \in \{1, \ldots, m\}$ and hence $f(\vec{x}) = (f_1(\vec{x}), \ldots, f_m(\vec{x}))$ for each $\vec{x} \in \mathbb{B}^n$.

2.2. Exclusive Sum-of-Products

Exclusive sum-of-products (ESOPs, [18]) are two-level descriptions of Boolean functions in which a function

$$f = \bigoplus_{i=1}^{k} x_{i_1}^{p_{i_1}} \wedge \cdots \wedge x_{i_{l_i}}^{p_{i_{l_i}}} \tag{1}$$

is composed of k *product terms* that are combined using the exclusive-OR (EXOR, $\oplus$) operation. A product term is the conjunction of literals l_i where a *literal* is either a propositional variable $x^1 = x$ or its negation $x^0 = \bar{x}$. ESOPs are the most general form of two-level AND-EXOR expressions.

Several subclasses have been considered in the past, e.g., *positive polarity Reed-Muller expressions* (PPRM [18]), in which all literals are positive. There are further subclasses, many of which may be defined by applying the following decomposition rules to a Boolean function $f(x_1, x_2, \ldots, x_n)$:

$$f = \bar{x}_i f_{\bar{x}_i} \oplus x_i f_{x_i} \qquad \text{(Shannon)}$$
$$f = f_{\bar{x}_i} \oplus x_i (f_{\bar{x}_i} \oplus f_{x_i}) \qquad \text{(positive Davio)}$$
$$f = f_{x_i} \oplus \bar{x}_i (f_{\bar{x}_i} \oplus f_{x_i}) \qquad \text{(negative Davio)}$$

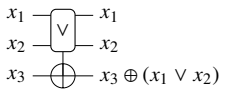
with *co-factors* $f_{\bar{x}_i} = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$ and $f_{x_i} = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$.

2.3. Reversible Circuits

Boolean functions can be realized *reversibly* by circuits that consist of at least n lines and are constructed using cascades of reversible gates from a given gate library. The most common gate libraries are generalizations of the Toffoli gate [19] and are defined in the following.

Definition 1 (Single-target gate)**.** *Given a set of variables $X = \{x_1, \ldots, x_n\}$, a* single-target (ST) gate $\mathrm{T}_c(C, t)$ *with* control lines $C = \{x_{i_1}, \ldots, x_{i_k}\} \subset X$*, a* target line $t \in X \setminus C$*, and a* control function $c \in \mathcal{B}_k$ *inverts the variable on the target line, if and only if $c(x_{i_1}, \ldots, x_{i_k})$ evaluates to true. All other variables remain unchanged. If the definition of c is obvious from the context, it can be omitted from the notation* T_c.

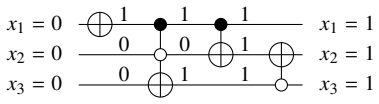
As an example the single-target gate $\mathrm{T}_\vee(\{x_1, x_2\}, x_3)$ acts on three lines x_1, x_2, x_3 and inverts line x_3, if and only if line x_1 or x_2 are set to true. Its graphical representation is:



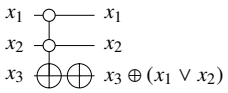
(2)

Definition 2 (Toffoli gate)**.** Mixed-polarity multiple-control Toffoli (MPMCT) gates *are a subset of the single-target gates in which the control function c is represented by one product term or c* = 1*. The literals in the product term are called* control lines *or controls.* Multiple-control Toffoli gates (MCT) *are a subset from the MPMCT gates in which the product terms can only consist of positive literals. The* NCT *gate library refers to MCT gates that have at most two control lines. The name is derived from* NOT *(Toffoli gate with no control line),* CNOT *(controlled NOT: Toffoli gate with one control line), and* Toffoli *(Toffoli gate with two control lines).*

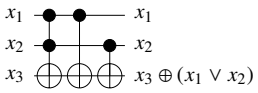
MPMCT gates are drawn by using a dot for each literal that appears in the product term; a solid dot is used for positive literals and a hollow dot for negative literals. Reversible circuits are built by joining them to form a cascade, e.g.:



The circuit shows an example simulation of the input pattern 000, leading to the output pattern 111. Running the circuit from right to left on the pattern 111 likewise leads to 000 at the inputs. Equivalent MPMCT and MCT circuit realizations for the single-target gate in (2) are



and



respectively. Note that both realizations can be derived from the ESOP representations $\bar{x}_1\bar{x}_2 \oplus 1$ and $x_1x_2 \oplus x_1 \oplus x_2$ for $x_1 \vee x_2$.

Every reversible (invertible) function $f \in \mathcal{B}_{n,n}$ can be realized by a reversible circuit over MPMCT or MCT gates using exactly n lines. A synthesis algorithm such as [20] provides a constructive proof. An additional temporary (ancilla) line may need to be added when restricting the number of control lines (see, e.g., [21]). Each single-target gate can be expressed in terms of a cascade of MPMCT or MCT gates, which can be obtained from an ESOP or PPRM expression [18], respectively.

2.4. Quantum Cost Metrics

In order to compute a reversible function on a quantum computer, reversible gates must be mapped into circuits over some library of quantum gates. Such quantum circuits allow the manipulation of classical Boolean values, but also any complex-valued linear combination of them, called a *superposition* of states. In particular, the Boolean values are denoted $|0\rangle$ and $|1\rangle$, and the state of a *qubit* is given by $\alpha|0\rangle + \beta|1\rangle$ for some amplitudes $\alpha, \beta \in \mathbb{C}$. Likewise, we denote a vector of n bits $\vec{x}$ by $|x_1x_2...x_n\rangle$ and describe the state of an n-qubit circuit as a complex combination of n-bit vectors. In general the state of an n-qubit circuit may not be written as n independent qubit states, a phenomenon known as *entanglement*.

A quantum gate acting on n qubits is typically represented by a $2^n \times 2^n$ unitary (norm-preserving) matrix. We denote by $U^\dagger$ the inverse of a gate U, given by the conjugate transpose of U. The subset of unitary matrices that are in fact permutation operators correspond exactly to the (Boolean) reversible functions.

The *quantum cost* of a reversible circuit is measured with respect to the quantum gate library that is used in technology mapping. We consider two quantum gate libraries in this paper: the NCV library and the Clifford+T library. Both libraries are complete for reversible functions.

The NCV gate library consists of the gates NOT, represented by the unitary matrix

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

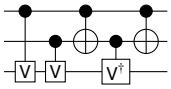
as well as the CNOT and controlled $V/V^\dagger$ gates, where

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$$

Table 1: Overview of the presented bounds

Gate library	1 MPMCT gate	1 Single-target gate	Reversible circuit
Single-target gates (ST)			Section 4
Mixed-polarity multiple-control Toffoli gates (MPMCT)		Section 5.1	Section 5.2
NOT, CNOT, and Toffoli gates (NCT)	Section 6.2	Section 6.3	Section 6.4
NOT, CNOT, V, $V^\dagger$ gates (NCV)	Section 7.1	Section 7.2	Section 7.3
Clifford+T gates	Section 8.1	Section 8.2	Section 8.3

is the "square root" of X. The quantum cost for the NCV gate library is defined as the total number of gates used. We call this number the NCV-cost of a reversible circuit. A possible NCV realization for the Toffoli gate $\mathrm{T}_\wedge(\{x_1, x_2\}, x_3)$ is:

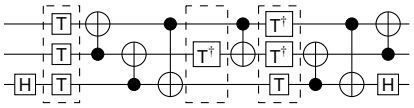


Its NCV-cost is 5 and there exists no realization with fewer costs.

The Clifford+T library consists of CNOT gate, along with the gates H and T, where

$$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

It is typically assumed that this gate set includes the $S = T^2$ and $Z = T^4$ gates, together with the T gate known as *phase gates*. The Clifford+T gate library has grown in popularity due to having known fault-tolerant implementations in most common error correcting codes [17]. These implementations typically have circuit latency proportional to the number of T stages—a group of T gates executed in parallel. This number, called the T-depth [22], defines the quantum cost of the Clifford+T gate library. The number of H gates in a Clifford+T circuit is provided as a secondary cost metric, as this number affects the T-depth optimization possibilities [23]. A T-depth optimal Clifford+T realization of the Toffoli gate is [22]:



Its T-depth is 3 as indicated by the emphasized T stages.

3. Overview

Each of the subsequent five sections provides upper bounds for a reversible or quantum gate library. Table 1 gives an overview of all the considered configurations. The first column lists all the gate libraries while the remaining columns describe the function class for which bounds are given.

For instance, Section 4 discusses how many single-target gates are required to represent any reversible function. Along with the number of gates required for the realization of a reversible function, in the case of MPMCT gates it is further investigated how many of such gates are required to realize one single-target gate.

Fig. 1 illustrates our layered mapping approach from which our upper bounds have been derived. Synthesis approaches allow the realization of a reversible function using ST or MPMCT gates, depending on the approach. ST based circuits can be mapped to MPMCT circuits after synthesis. Different mapping techniques (referred to as B1, NC, and MI and described in detail in Section 6.1) then transform these circuits into circuits that are solely composed of NCT gates which can then be transformed into quantum circuits w.r.t. a quantum gate library.

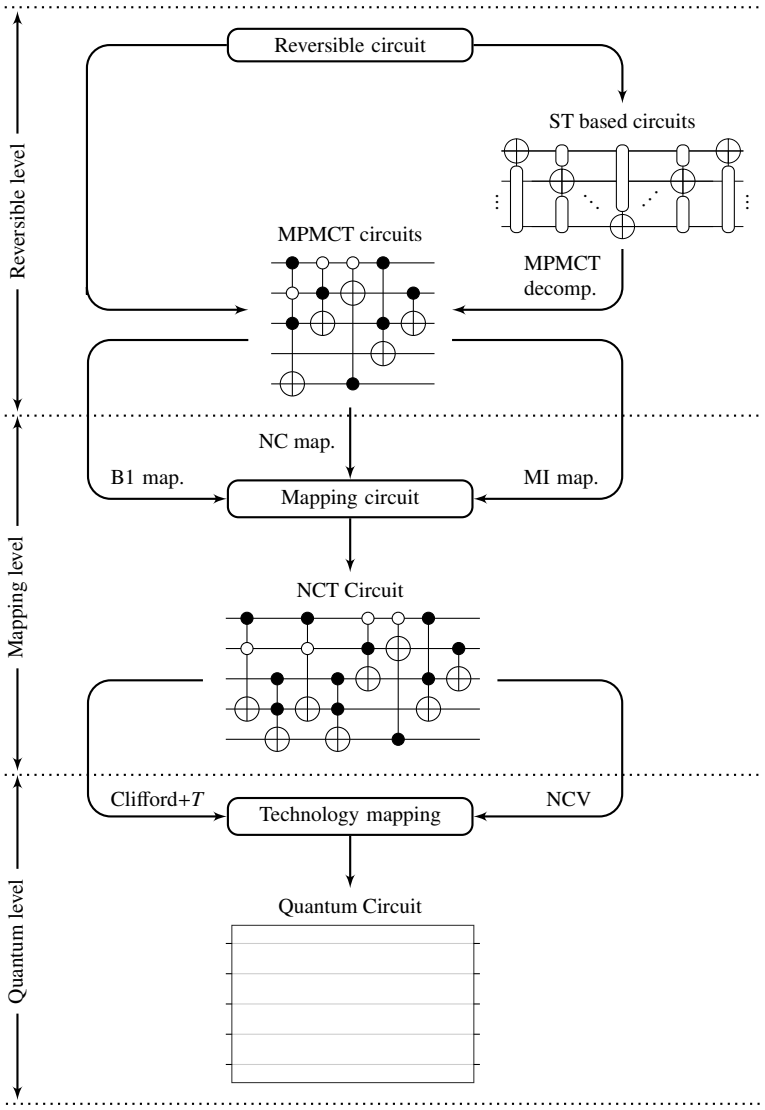


Figure 1: Mapping model

4. Complexity of Single-target Circuits

In this section we review the size of reversible circuits based on single-target gates. Let $X = \{x_1, \ldots, x_n\}$. Given an n-variable reversible function $f(x_1, \ldots, x_n) \in \mathcal{B}_{n,n}$ and a line index $i \in \{1, \ldots, n\}$, one can decompose f into three n-variable reversible functions

$$f = g_1 \circ f' \circ g_2 \tag{3}$$

such that $g_1 = \mathrm{T}_l(X \setminus \{x_i\}, x_i)$ and $g_2 = \mathrm{T}_r(X \setminus \{x_i\}, x_i)$ are single-target gates with control functions l and r, and f' is a reversible function that does not change in line i; in other words $f'_i(\vec{x}) = x_i$. Such a decomposition can always be found for all $1 \leq i \leq n$ [7].

A synthesis algorithm can readily be derived by recursively applying the decomposition to all variables. Eventually f' will be the identity function and the last two single-target gates g_1 and g_2 collapse to one single-target gate with control function $l \oplus r$. This immediately implies a linear upper bound for single-target gates: each n-variable reversible

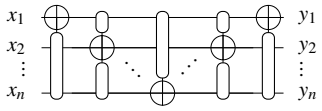
Table 2: Upper bounds for realizing an ST gate

Method	**MCT**	**MPMCT**
Decomposition	$3 \cdot 2^{n-3} - 2$	$3 \cdot 2^{n-4}$
ESOP expressions	2^{n-1}	$29 \cdot 2^{n-8}$

function f can be realized with at most

$$uc_{\mathrm{ST}}(n) = 2n - 1 \tag{4}$$

ST gates [24]. If the decomposition is applied to all lines in numerical order, the resulting circuit is called a *V-shape*



referring to the distribution of the target lines. The above synthesis approach, called the *Young subgroup synthesis*, was initially proposed in [7], then later reimplemented based on binary decisions diagrams (BDD) and presented in [25].

5. Complexity of MPMCT Circuits

This section first gives upper bounds for the realization of single-target gates in terms of MPMCT gates and then gives upper bounds for reversible circuits in general.

5.1. Upper Bounds for Single-target Gates

The complexity of ST gates was studied in [26] and upper bounds were derived based on functional decomposition and ESOP upper bounds. In particular, it was proven that an ST gate can be realized with at most

$$us_{\mathrm{MPMCT}}(n) \leq 3 \cdot 2^{n-4} \tag{5}$$

MPMCT gates. Table 2 summarizes all derived upper bounds for ST gates based on MCT and MPMCT gates.

5.2. Upper Bounds for Reversible Circuits

In [10], based on the transformation-based synthesis approach [20], it has been proven that every reversible function over n variables can be realized with no more than

$$uc_{\mathrm{MPMCT}}(n) \leq n \cdot 2^n \tag{6}$$

MPMCT gates. The algorithm proceeds by traversing each of the 2^n rows of the truth table and for each row adds at most one gate per column, giving a worst case of $n \cdot 2^n$ gates.

The authors in [11] derived a weaker upper bound based on a cycle-based synthesis approach. Their synthesis algorithm produces circuits with at most

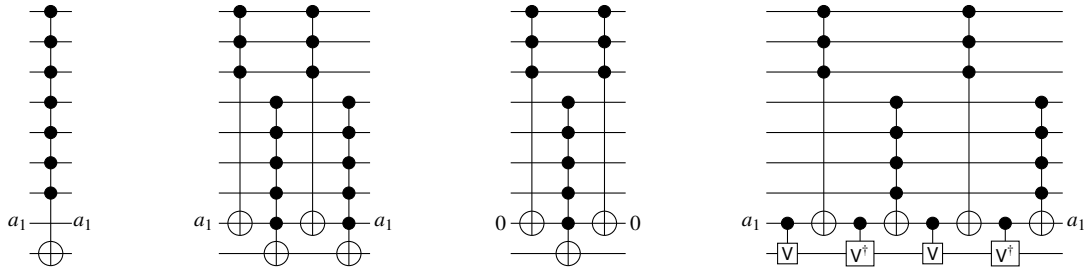
$$uc_{\mathrm{MPMCT}}(n) \leq \left(3n + \tfrac{1}{2}\right) \cdot 2^n \tag{7}$$

MPMCT gates. Although the bound is weaker, the authors are able to decompose the formula to use a fewer number of NOTs, CNOTs, and Toffoli gates. This can have an influence on the quantum cost metric.

Using the complexity of a single-target gate (see previous section), in [26] a better upper bound is derived for MPMCT circuits. Based on the Young subgroup synthesis approach it is shown that any reversible function over n variable can be implemented with at most

$$uc_{\mathrm{MPMCT}}(n) \leq 3(2n-1) \cdot 2^{n-4} \leq 3n \cdot 2^{n-3} \tag{8}$$

MPMCT gates.



(a) MCT gate (b) Barenco et al. mapping (Lemma 7.3) (c) Nielsen and Chuang mapping (d) Miller et al. mapping

Figure 2: Different types of mapping an MCT into smaller MCT gates using one ancilla

6. Complexity of NCT Circuits

This section first gives an overview of the approaches considered for mapping MPMCT gates to NCT circuits. Upper bounds on the number of NCT gates needed to realize MPMCT gate, ST gate, and general reversible circuits are then studied.

6.1. Technology Mapping for Reversible Circuits

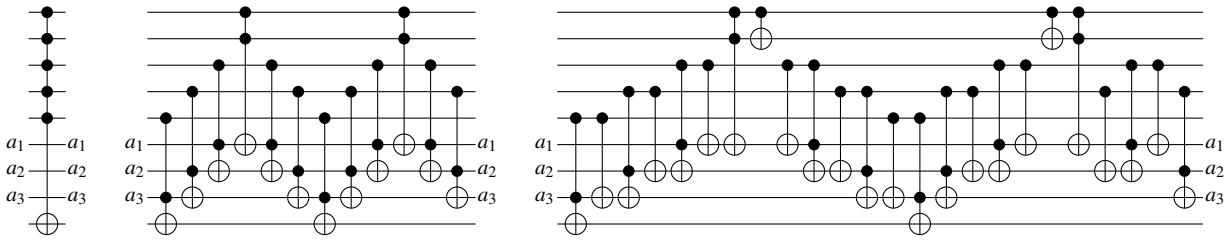
In order to derive a quantum circuit for a reversible function, the following approach is typically applied: (i) use synthesis to obtain a reversible circuit description, e.g., based on MPMCT gates; (ii) transform the circuit into one that consists only of NCT gates; (iii) map each Toffoli gate to a quantum circuit. Different approaches have been proposed for the second step:

1. *Barenco et al. (Lemma 7.3)*: According to [15, Lemma 7.3] a Toffoli gate $\mathrm{T}(C, t)$ with $|C| \geq 3$ is mapped to a cascade
$$\mathrm{T}(C_1, a_1) \circ \mathrm{T}(C_2 \cup \{a_1\}, t) \circ \mathrm{T}(C_1, a_1) \circ \mathrm{T}(C_2 \cup \{a_1\}, t) \tag{9}$$
where $C = C_1 \cup C_2$ and $C_1 \cap C_2 = \emptyset$. The *helper line* a_1 can neither be in C, nor can it be t. If no free line is available, an additional line must be added to the circuit. Note that the cascade restores the value on a_1 and therefore it can be reused for all gates. Fig. 2(b) shows the cascade for a 7 controlled MCT gate.

2. *Nielsen and Chuang,* [27]: If the helper line in the previous transformation is assigned to the 0 state, the fourth gate in (9) can be omitted. This approach leads to circuits with cheaper quantum cost, however, if no free lines are in the 0 state an additional line is needed. Fig. 2(c) illustrates the resulting circuit after applying this transformation.

3. *Miller et al.,* [28]: An MPMCT gate can be mapped directly to a quantum circuit in a more efficient way by making use of controlled V gates. In particular, a Toffoli gate $\mathrm{T}(C, t)$ may be mapped to the following circuit:
$$V(a_1, t) \circ \mathrm{T}(C_1, a_1) \circ V^\dagger(a_1, t) \circ \mathrm{T}(C_2, a_1) \circ V(a_1, t) \circ \mathrm{T}(C_1, a_1) \circ V^\dagger(a_1, t) \circ \mathrm{T}(C_2, a_1) \tag{10}$$
In this case, the control set C_2 has one fewer line, at the expense of 4 controlled $V/V^\dagger$ gates. A helper line is required, but as in the Barenco et al. approach any free line may be used rather than one in the 0 state. An example of this transformation is illustrated in Fig. 2(d).

4. *Barenco et al. (Lemma 7.2)*: According to [15, Lemma 7.2] a second step can be applied to the circuits obtained from the previous algorithms or directly when the number of helper lines is $|C| - 2$. The resulting cascade consists of NCT gates and is illustrated in Fig. 3(b). In [29], Maslov et al. have optimized this algorithm to improve the quantum cost of NCV based quantum circuits. The network depicted in Fig. 3(c) presents the optimized transformation for the 5-controlled gate with 3 helper lines. Each Toffoli gate is combined with a CNOT gate to form a Peres gate, which uses 4 instead of 5 NCV gates.



(a) MCT gate (b) Barenco et al. mapping (Lemma 7.2) (c) Optimized Barenco et al. mapping (Lemma 7.2) by Maslov et al.

Figure 3: Different types of mapping an MCT gate into smaller NCT gates using $(c-2)$ ancillas

In the rest of the paper we denote the one ancilla mapping algorithms of Barenco et al. (Lemma 7.3), Nielsen and Chuang, and Miller et al. by B1, NC, and MI, respectively. Also, we refer to the $c-2$ ancillas mapping algorithm from Barenco et al. (Lemma 7.2) as B2.

6.2. Upper Bounds for MPMCT Gates

Theorem 1. *A c-control MPMCT gate can be realized, if* $c \geq 5$*, with at most*

- $um_{\mathrm{NCT}_{\mathrm{B1}}}(c) \leq 8(c-3)$
- $um_{\mathrm{NCT}_{\mathrm{NC}}}(c) \leq 6(c-3)$
- $um_{\mathrm{NCT}_{\mathrm{MI}}}(c) \leq 8(c-4)+4$
- $um_{\mathrm{NCT}_{\mathrm{B2}}}(c) \leq 4(c-2)$

NCT gates. Note that these bounds are upper bounds.

Proof. The upper bounds for B1 and B2 are proven in [15].

In the NC mapping two of the three resulting MPMCT gates have $\left\lceil \frac{c}{2} \right\rceil$ controls while the third one has $c+1-\left\lceil \frac{c}{2} \right\rceil$ controls. Each of these gates is mapped with respect to the B2 mapping, giving

$$\begin{aligned} um_{\mathrm{NCT}_{\mathrm{NC}}}(c) &\leq 2 \cdot 4\left(\left\lceil \tfrac{c}{2} \right\rceil - 2\right) + 4\left(c+1-\left\lceil \tfrac{c}{2} \right\rceil - 2\right) \\ &\leq 4\left(c + \left\lceil \tfrac{c}{2} \right\rceil - 5\right) \end{aligned}$$

For even c, we have $um_{\mathrm{NCT}_{\mathrm{NC}}}(c) \leq 6\left(c-\frac{10}{3}\right) \leq 6(c-3)$, and for odd c, we have $um_{\mathrm{NCT}_{\mathrm{NC}}}(c) \leq 6(c-3)$.

In the MI mapping two of the resulting four MPCMCT gates have $\left\lceil \frac{c}{2} \right\rceil$ controls while the other two have $c-\left\lceil \frac{c}{2} \right\rceil$ controls. Applying B2 mapping yields

$$um_{\mathrm{NCT}_{\mathrm{MI}}}(c) \leq 2 \cdot 4\left(\left\lceil \tfrac{c}{2} \right\rceil - 2\right) + 2 \cdot 4\left(c - \left\lceil \tfrac{c}{2} \right\rceil - 2\right) \leq 8(c-4)$$

Toffoli gates. In addition, four NCV gates are required. □

Table 3 summarizes these upper bounds for the number of Toffoli gates given by each mapping from the previous section when applied to an MPMCT gate with $c \geq 5$ control lines. Note that for the MI mapping four additional NCV gates are included and that four additional NOT gates need to be added in the case that all control lines in the MPMCT gate are negative.

Table 3: Number of NCT gates for an MPMCT gate with c controls

Mapping	Ancillas	NCT
B1 (Barenco et al. (Lemma 7.3 [15]))		$8(c-3)$
NC (Nielsen and Chuang [27])	1	$6(c-3)$
MI (Miller et al. [28])		$8(c-4)+4$ [a]
B2 (Barenco et al. (Lemma 7.2 [15])	$c-2$	$4(c-2)$

[a] 4 NCV gates

6.3. Upper Bounds for Single-target Gates

6.3.1. Upper Bounds Based on PPRM Expressions

Tighter upper bounds for reversible circuits can be obtained by combining the synthesis approach outlined in the previous section using MCT gates and upper bounds for the size of PPRM expressions. We will make use of the following lemma and corollary which are proven in Appendices A and B, respectively.

Lemma 1.

$$\sum_{1\le i\le\left\lceil\frac{n}{2}\right\rceil} i\binom{n}{i} = \begin{cases} n\cdot 2^{n-2} & n \text{ even} \\ n\cdot 2^{n-2} + \frac{n+1}{4}\binom{n}{\frac{n+1}{2}} & n \text{ odd} \end{cases} \quad \text{and} \quad \sum_{\left\lceil\frac{n}{2}\right\rceil<i\le n} i\binom{n}{i} = \begin{cases} n\cdot 2^{n-2} & n \text{ even} \\ n\cdot 2^{n-2} - \frac{n+1}{4}\binom{n}{\frac{n+1}{2}} & n \text{ odd.} \end{cases}$$

Corollary 1. *From Lemma 1, we derive the following inequations for $n \ge 6$:*

$$4\cdot\sum_{i=0}^{\left\lceil\frac{n}{2}\right\rceil}(i-2)\binom{n}{i} + 8\cdot\sum_{i=\left\lceil\frac{n}{2}\right\rceil+1}^{n}(i-3)\binom{n}{i} \le (6n-24)\cdot 2^{n-1} \tag{11}$$

$$4\cdot\sum_{i=0}^{\left\lceil\frac{n}{2}\right\rceil}(i-2)\binom{n}{i} + 6\cdot\sum_{i=\left\lceil\frac{n}{2}\right\rceil+1}^{n}(i-3)\binom{n}{i} \le (5n-21)\cdot 2^{n-1} \tag{12}$$

$$4\cdot\sum_{i=0}^{\left\lceil\frac{n}{2}\right\rceil}(i-2)\binom{n}{i} + 8\cdot\sum_{i=\left\lceil\frac{n}{2}\right\rceil+1}^{n}(i-4)\binom{n}{i} \le (6n-28)\cdot 2^{n-1} \tag{13}$$

Theorem 2. *An n-variable single-target gate with $n \ge 7$ can be realized with at most*

- $us_{\mathrm{NCT_{B1}}}(n) \le (6n-30)\cdot 2^{n-2}$
- $us_{\mathrm{NCT_{NC}}}(n) \le (5n-26)\cdot 2^{n-2}$
- $us_{\mathrm{NCT_{MI}}}(n) \le (6n-34)\cdot 2^{n-2}$

NCT gates.

Proof. An n-variable single-target gate can be realized with at most $us_{\mathrm{MCT}}(n) = 2^{n-1}$ MCT gates. This follows from the PPRM representation, which is canonical for a given function when disregarding the order of product terms. Hence, there exists a control function $c \in \mathcal{B}_{n-1}$ for which the PPRM expression consists of all 2^{n-1} product terms, and therefore

$$us_{\mathrm{MCT}}(n) \le 2^{n-1} \le \sum_{i=0}^{n-1}\binom{n-1}{i} \tag{14}$$

with $\binom{n-1}{i}$ being the total number of product terms that have i literals, i.e., the total number of Toffoli gates that have i controls. Let's now consider the number of gates after mapping to the NCT gate library: In [30], it has been shown that each MPMCT gate, with i controls and $i \leq \left\lceil \frac{n-1}{2} \right\rceil$, can be decomposed to $4(i-2)$ Toffoli gates. Otherwise, it can be decomposed to a cascade using one of the mapping algorithms that require one ancilla.

When the B1 mapping is chosen as a one ancilla mapping algorithm, each i-control MPMCT gate with $i > \left\lceil \frac{n-1}{2} \right\rceil$ can be decomposed to $8(i-3)$ Toffoli gates. We thus have

$$us_{\mathrm{NCT_{B1}}}(n) \leq 4 \cdot \sum_{i=0}^{\left\lceil \frac{n-1}{2} \right\rceil} (i-2)\binom{n-1}{i} + 8 \cdot \sum_{i=\left\lceil \frac{n-1}{2} \right\rceil + 1}^{n-1} (i-3)\binom{n-1}{i} \overset{\text{Corollary 1}}{\leq} (6(n-1)-24) \cdot 2^{(n-1)-1} \leq (6n-30) \cdot 2^{n-2}$$

When the NC mapping is applied,

$$us_{\mathrm{NCT_{B1}}}(n) \leq 4 \cdot \sum_{i=0}^{\left\lceil \frac{n-1}{2} \right\rceil} (i-2)\binom{n-1}{i} + 6 \cdot \sum_{i=\left\lceil \frac{n-1}{2} \right\rceil + 1}^{n-1} (i-3)\binom{n-1}{i} \overset{\text{Corollary 1}}{\leq} (5(n-1)-21) \cdot 2^{(n-1)-1} \leq (5n-26) \cdot 2^{n-2}$$

Finally, when the MI mapping is adopted,

$$us_{\mathrm{NCT_{B1}}}(n) \leq 4 \cdot \sum_{i=0}^{\left\lceil \frac{n-1}{2} \right\rceil} (i-2)\binom{n-1}{i} + 8 \cdot \sum_{i=\left\lceil \frac{n-1}{2} \right\rceil + 1}^{n-1} (i-4)\binom{n-1}{i} \overset{\text{Corollary 1}}{\leq} (6(n-1)-28) \cdot 2^{(n-1)-1} \leq (6n-34) \cdot 2^{n-2}$$

□

6.3.2. Upper Bounds Based on General ESOP Expressions

Even tighter bounds can be obtained when using general ESOP expressions instead of PPRM expressions. Note that this includes the consideration of negative control lines.

Theorem 3. *An n-variable single-target gate can be realized, if $n \geq 6$, with at most*

- $us_{\mathrm{NCT_{B1}}}(n) \leq 29(n-4) \cdot 2^{n-5}$
- $us_{\mathrm{NCT_{NC}}}(n) \leq \frac{87}{4}(n-4) \cdot 2^{n-5}$
- $us_{\mathrm{NCT_{MI}}}(n) \leq 29(n-5) \cdot 2^{n-5}$

NCT gates.

Proof. The best known upper bound on the number of product terms in a minimum ESOP form for an n-variables Boolean function is [31]

$$29 \cdot 2^{n-7} \quad \text{with} \quad n \geq 7. \tag{15}$$

Hence, the ESOP expression of the control function $c \in \mathcal{B}_{n-1}$ consists of at most $29 \cdot 2^{n-8}$ product terms. Each product term has at most $n-1$ terms in the worst case, and so mapping a product term (i.e., MPMCT gate with at most $n-1$ controls) using the B1 mapping gives at most $8(n-4)$ Toffoli gates. Hence at most $29(n-4) \cdot 2^{n-5}$ Toffoli gates when the B1 mapping is applied, so $us_{\mathrm{NCT_{B1}}}(n) \leq 29(n-4) \cdot 2^{n-5}$ as required. The remaining upper bounds are derived using the same argument. □

6.3.3. Upper Bounds Based on Functional Decomposition

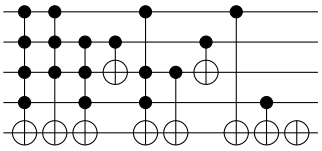
In this section, we derive upper bounds based on functional decomposition in an induction proof. We use exact bounds for the base case that were found using exhaustive search in combination with optimal synthesis [32].

Theorem 4. *For an n-variable single-target gate we have for $n \geq 6$:*

- $us_{\mathrm{NCT_{B1}}}(n) \leq (5n - 31) \cdot 2^{n-1} + (2^{n-4} - 2)$
- $us_{\mathrm{NCT_{NC}}}(n) \leq (15n - 93) \cdot 2^{n-3} + (2^{n-4} - 2)$
- $us_{\mathrm{NCT_{MI}}}(n) \leq (5n - 36) \cdot 2^{n-1} + (2^{n-4} - 2)$

NCT gates, where the first term in each bound refers to the number of Toffoli gates and the second term refers to the number of NOT gates.

Proof. We first show an upper bound of $us_{\mathrm{MCT}}(n) = 2^{n-5} \cdot 10 + 2^{n-4} - 2$ for the number of MCT gates if $n \geq 5$. The proof is obtained by induction on n. For the base case let $n = 5$. Using exhaustive search we enumerated all 65,536 Boolean functions over 4 variables that can be represented by a 5-bit single-target gate and for each one we obtain the minimal circuit using an exact synthesis approach [32]. The largest circuit requires 10 MCT gates:

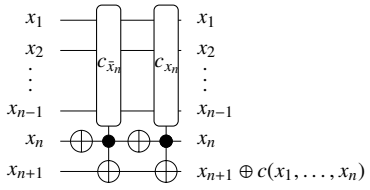


Therefore, we have

$$us_{\mathrm{MCT}}(5) = 1 + 3 + 0 + 5 + 1 = 10, \tag{16}$$

where the terms partition the Toffoli gates by their number of controls from 4 controls to 0 controls.

In the induction step, let's consider an $(n+1)$-bit single-target gate $\mathrm{T}_c(\{x_1, \ldots, x_n\}, x_{n+1})$. By applying the Shannon decomposition the gate can be decomposed into two n-bit single-target gates and 2 NOT gates:



With this, we obtain

$$us_{\mathrm{MCT}}(n+1) = 2 \cdot us_{\mathrm{MCT}}(n) + 2 = 2(2^{n-5} \cdot 10 + 2^{n-4} - 2) + 2 = 2^{n-4} \cdot 10 + 2^{n-3} - 4 + 2 = 2^{(n+1)-5} \cdot 10 + 2^{(n+1)-4} - 2.$$

Hence, a single-target gate on n lines requires at most $2^{n-5} \cdot 10 + 2^{n-4} - 2$ MCT gates.

For the mapping to NCT gates we need to take a closer look at the number of controls for each MCT gate. According to (16) we have the following distribution for each n-bit single-target gate:

#controls	$n-1$	$n-2$	$n-3$	$n-4$	$n-5$	0
#gates	2^{n-5}	$3 \cdot 2^{n-5}$	0	$5 \cdot 2^{n-5}$	2^{n-5}	$2^{n-4} - 2$

(17)

As an example, consider now the B1 mapping which requires $8(n-3)$ NCT gates for a MCT gate with n controls. Therefore:

$$\begin{aligned} us_{\mathrm{NCT_{B1}}}(n) =& 2^{n-5}(8(n-4) + 3 \cdot 8(n-5) + 5 \cdot 8(n-7) + 8(n-8)) + (2^{n-4} - 2) \\ =& 2^{n-2}((n-4) + 3(n-5) + 5(n-7) + (n-8)) + (2^{n-4} - 2) \\ =& 2^{n-1}(5n - 31) + (2^{n-4} - 2) \end{aligned}$$

The bounds based on the other mappings can be derived analogously. □

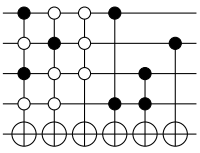
Better bounds can be found when extending the decomposition-based approach for MPMCT gates.

Theorem 5. *An n-variable single-target gate can be realized, if $n \geq 6$, with at most*

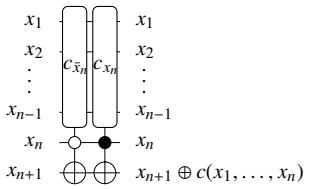
- $us_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq (3n - 16) \cdot 2^{n-1}$
- $us_{\mathrm{NCT}_{\mathrm{NC}}}(n) \leq (\frac{9}{4}n - 12) \cdot 2^{n-1}$
- $us_{\mathrm{NCT}_{\mathrm{MI}}}(n) \leq (3n - 19) \cdot 2^{n-1}$

NCT gates.

Proof. We are using the same idea for the proof as for Theorem 4. The largest minimal circuit contains 6 MPMCT gates:



Together with the decomposition



and an updated distribution of gates as in (18), an upper bound for the number of gates $us_{\mathrm{MPMCT}}(n) = 2^{n-5} \cdot 6$ is obtained for $n \geq 5$.

As an example, consider again the B1 mapping which requires $8(n - 3)$ NCT gates for an MPMCT gate with n controls. Based on the new bound for MPMCT gates and the following distribution for each n-bit single-target gate:

$$\begin{array}{rccccc} \#\text{controls} & n-1 & n-2 & n-3 & n-4 & n-5 \\ \#\text{gates} & 2 \cdot 2^{n-5} & 2^{n-5} & 2 \cdot 2^{n-5} & 2^{n-5} & 0 \end{array} \tag{18}$$

We have

$$us_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq 2^{n-5}(2 \cdot 8(n-4) + 8(n-5) + 2 \cdot 8(n-6) + 8(n-7)) \leq (6n - 32)2^{n-2} \leq (3n - 16)2^{n-1}$$

NCT gates. The bounds based on the other mappings can be derived analogously. □

Comparing the upper bounds for single-target gates based on ESOPs and function decomposition, we observe that general PPRM expressions give the best upper bounds. In fact, it gives the exact number of MCT gates and their exact number of controls. In the remainder of the paper, we will focus on the upper bounds that are derived from PPRM expressions.

6.4. Upper Bounds for NCT Circuits

The synthesis algorithm presented by Shende *et al.* in [21] provides a constructive upper bound: a reversible function over n variables can be realized with at most

$$uc_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq 9n \cdot 2^n + o(n \cdot 2^n) \tag{19}$$

NCT gates. A stronger upper bound can be found using the transformation based synthesis algorithm. In [10] it has been proven that an n-variable reversible function can be realized with at most

$$uc_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq 5n \cdot 2^n + o(n \cdot 2^n) \tag{20}$$

NCT gates. In the following we give new upper bounds on the size of NCT circuits for general reversible functions using the transformation based synthesis approach with different mapping strategies:

Theorem 6. *Using the transformation based synthesis algorithm, if $n \geq 6$, an NCT based circuit has at most*

- $uc_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq (10n - 28) \cdot 2^{n-1}$
- $uc_{\mathrm{NCT}_{\mathrm{NC}}}(n) \leq (9n - 25) \cdot 2^{n-1}$
- $uc_{\mathrm{NCT}_{\mathrm{MI}}}(n) \leq (10n - 32) \cdot 2^{n-1}$

NCT gates.

Proof. A reversible circuit synthesized with the transformation based approach will have at most n NOT gates, $(n - 1) \cdot 2^{n+1} - n^2 + 4$ CNOT gates, and $\sum_{i=2}^{n-1} \binom{n}{i}$ MCT gates where i denotes the number of controls on each gate.

Based on the B1 mapping, after mapping the $\sum_{i=2}^{n-1} \binom{n}{i}$ MCT gates, we get

$$4 \cdot \sum_{i=2}^{\lceil \frac{n}{2} \rceil} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n-1} (i-3)\binom{n}{i}$$

NCT gates. Hence:

$$uc_{\mathrm{NCT}_{\mathrm{B1}}}(n) \leq n + (n-1) \cdot 2^{n+1} - n^2 + 4 + 4 \cdot \sum_{i=2}^{\lceil \frac{n}{2} \rceil} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n-1} (i-3)\binom{n}{i}$$

$$\overset{\text{Corollary 1}}{\leq} n + (n-1) \cdot 2^{n+1} - n^2 + 4 + (6n-24) \cdot 2^{n-1} \leq (10n-28) \cdot 2^{n-1} + n - n^2 + 4 \leq (10n-28) \cdot 2^{n-1}$$

Using the NC mapping,

$$uc_{\mathrm{NCT}_{\mathrm{NC}}}(n) \leq n + (n-1) \cdot 2^{n+1} - n^2 + 4 + 4 \cdot \sum_{i=2}^{\lceil \frac{n}{2} \rceil} (i-2)\binom{n}{i} + 6 \cdot \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n-1} (i-3)\binom{n}{i}$$

$$\overset{\text{Corollary 1}}{\leq} n + (n-1) \cdot 2^{n+1} - n^2 + 4 + (5n-21) \cdot 2^{n-1} \leq (9n-25) \cdot 2^{n-1} + n - n^2 + 4 \leq (9n-25) \cdot 2^{n-1}$$

Using the MI mapping,

$$uc_{\mathrm{NCT}_{\mathrm{MI}}}(n) \leq n + (n-1) \cdot 2^{n+1} - n^2 + 4 + 4 \cdot \sum_{i=2}^{\lceil \frac{n}{2} \rceil} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n-1} (i-4)\binom{n}{i}$$

$$\overset{\text{Corollary 1}}{\leq} n + (n-1) \cdot 2^{n+1} - n^2 + 4 + (6n-28) \cdot 2^{n-1} \leq (10n-32) \cdot 2^{n-1} + n - n^2 + 4 \leq (10n-32) \cdot 2^{n-1}$$

□

7. Complexity of NCV Quantum Circuits

This section first gives upper bounds for the realization of MPMCT and ST gates in terms of NCV gates and then gives upper bounds for reversible circuits based on NCV gates.

Table 4: NCV-cost for an MPMCT gate with c controls

Mapping	**Ancillas**	**NCV**
B1 (Barenco et al. (Lemma 7.3 [15]))		$24(c-3)+12$ ([30])
NC (Nielsen and Chuang [27])	1	$18(c-3)+10$
MI (Miller et al. [28])		$24(c-4)+16$
B2 (Barenco et al. (Lemma 7.2 [15]))	$c-2$	$12(c-2)+2$ ([30])

7.1. NCV-cost for MPMCT Gates

Theorem 7. *A c-control MPMCT gate can be realized, if $c \geq 5$, with at most*

- $um_{\mathrm{NCV}_{\mathrm{B1}}}(c) \leq 24(c-3)+12$
- $um_{\mathrm{NCV}_{\mathrm{NC}}}(c) \leq 18(c-3)+10$
- $um_{\mathrm{NCV}_{\mathrm{MI}}}(c) \leq 24(c-4)+16$
- $um_{\mathrm{NCV}_{\mathrm{B2}}}(c) \leq 12(c-2)+2$

NCV gates. When the MPMCT gate has only negative controls four additional NOT gates are needed.

Proof. The first and last upper bounds have been already proven in [30], while the second and the third bounds are calculated using the circuit structure for each mapping approach.

In the NC mapping two of the three resulting MPMCT gates have $\lceil \frac{c}{2} \rceil$ controls while the third one has $c+1-\lceil \frac{c}{2} \rceil$ controls. Each of these gates is mapped with respect to the B2 mapping, giving

$$\begin{aligned} um_{\mathrm{NCV}_{\mathrm{NC}}}(c) &\leq 2\left(12\left(\left\lceil \tfrac{c}{2} \right\rceil - 2\right)+2\right) + 12\left(c+1-\left\lceil \tfrac{c}{2} \right\rceil - 2\right)+2+4 \\ &\leq 12\left(c+\left\lceil \tfrac{c}{2} \right\rceil - 5\right)+10 \end{aligned}$$

For even c, we have $um_{\mathrm{NCT}_{\mathrm{NC}}}(c) \leq 18\left(c-\frac{10}{3}\right)+10 \leq 18(c-3)+10$, and for odd c, we have $u(c) \leq 18(c-3)+10$.

In the MI mapping two of the resulting four MPCMCT gates have $\lceil \frac{c}{2} \rceil$ controls while the other two have $c-\lceil \frac{c}{2} \rceil$ controls. Applying B2 mapping yields

$$\begin{aligned} um_{\mathrm{NCT}_{\mathrm{MI}}}(c) &\leq 2\left(12\left(\left\lceil \tfrac{c}{2} \right\rceil - 2\right)+2\right) + 2\left(12\left(c-\left\lceil \tfrac{c}{2} \right\rceil - 2\right)+2\right)+4+4 \\ &\leq 24(c-4)-16 \end{aligned}$$

Toffoli gates. □

Table 3 summarizes the above theorem, along with the number of ancillas used by each mapping approach.

7.2. NCV-cost for Single-target Gates

The following corollary is proven in Appendix C.

Corollary 2. *From Lemma 1, we derive the following inequations for $n \geq 6$:*

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil+1}^{n} (24(i-3)+12) \cdot \binom{n}{i} \leq (18n-63) \cdot 2^{n-1} \tag{21}$$

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil+1}^{n} (18(i-3)+10) \cdot \binom{n}{i} \leq (15n-55) \cdot 2^{n-1} \tag{22}$$

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil+1}^{n} (24(i-4)+16) \cdot \binom{n}{i} \leq (18n-72) \cdot 2^{n-1} \tag{23}$$

Theorem 8. *An n-variable single-target gate can be realized, if $n \geq 6$, with at most*

- $us_{\mathrm{NCV}_{\mathrm{B1}}}(n) \leq (18n-81) \cdot 2^{n-2}$
- $us_{\mathrm{NCV}_{\mathrm{NC}}}(n) \leq (15n-70) \cdot 2^{n-2}$
- $us_{\mathrm{NCV}_{\mathrm{MI}}}(n) \leq (18n-90) \cdot 2^{n-2}$

NCV gates.

Proof. We have

$$us_{\mathrm{NCV}_{\mathrm{B1}}}(c) \leq \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil} (12(i-2)+2) \cdot \binom{n-1}{i} + \sum_{i=\lceil \frac{n-1}{2} \rceil+1}^{n-1} (24(i-3)+12) \cdot \binom{n-1}{i}$$

$$\overset{\text{Corollary 2}}{\leq} (18(n-1)-63) \cdot 2^{n-2} \leq (18n-81) \cdot 2^{n-2}$$

The other upper bounds are proven using the same argument. □

7.3. NCV-cost for Quantum Circuits

Many studies have focused on the upper bound of the number of elementary quantum gates in quantum circuits. The transformation based algorithm as mentioned in [10] leads to quantum circuits over the NCV library with the following upper bound on NCV-cost:

$$uc_{\mathrm{NCV}_{\mathrm{B1}}}(n) \leq 11n \cdot 2^n + o(n \cdot 2^n) \tag{24}$$

Comparatively, in [11] the authors have confirmed that using a cycle based synthesis approach, any reversible function over n variable can be realized with at most

$$uc_{\mathrm{NCV}_{\mathrm{B1}}}(n) \leq 8.5n \cdot 2^n \tag{25}$$

NCV gates. In the following we present the complexity of NCV circuits using the transformation based synthesis approach with different mapping strategies.

Theorem 9. *Using the transformation based synthesis algorithm, an NCV circuit has the following upper bound on the number of NCV gates:*

- $uc_{\mathrm{NCV}_{\mathrm{B1}}}(n) \leq (11n-33) \cdot 2^n$
- $uc_{\mathrm{NCV}_{\mathrm{NC}}}(n) \leq (9.5n-29.5) \cdot 2^n$
- $uc_{\mathrm{NCV}_{\mathrm{MI}}}(n) \leq (11n-38) \cdot 2^n$

Table 5: T-depth for an MPMCT gate with c controls

Mapping	**Ancillas**	**Clifford+T**
B1 (Barenco et al. (Lemma 7.3 [15]))		$24(c-3)$
NC (Nielsen and Chuang [27])	1	$18(c-3)$
MI (Miller et al. [28])		$24(c-4)+8$
B2 (Barenco et al. (Lemma 7.2 [15]))	$c-2$	$12(c-2)$

Proof. A reversible circuit synthesized with the transformation based approach will have at most n NOT gates, $(n-1)\cdot 2^{n+1} - n^2 + 4$ CNOT gates, and $\sum_{i=2}^{n-1}\binom{n}{i}$ MCT gates where i denotes the number of controls on each gate.

Based on the B1 mapping, we see that

$$uc_{\mathrm{NCT_{B1}}}(n) \leq n + (n-1)\cdot 2^{n+1} - n^2 + 4 + \sum_{i=2}^{\lceil \frac{n}{2} \rceil}(12(i-2)+2)\cdot\binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil+1}^{n-1}(24(i-3)+12)\cdot\binom{n}{i}$$

$$\overset{\text{Corollary 2}}{\leq} n + (n-1)\cdot 2^{n+1} - n^2 + 4 + (18n-63)\cdot 2^{n-1} \leq (11n-33)\cdot 2^n + n - n^2 + 4 \leq (11n-33)\cdot 2^n$$

□

The other upper bounds are calculated using the same method.

8. Complexity of Clifford+T Quantum Circuits

This section first presents the existing upper bounds on the T-depth of MPMCT gates. New upper bounds on the T-depth required to realize MPMCT gates, ST gates, and quantum circuits are then given.

8.1. T-depth for MPMCT Gates

Table 5 summarizes the upper bounds for the T-depth for each mapping defined in Section 6.1 when applied to an MPMCT gate with c control lines for $c \geq 5$. These upper bounds are obtained by directly mapping each two-control Toffoli to an (optimal) T-depth 3 circuit. Likewise, we map the controlled V to an optimal T-depth 2 circuit. In the following we derive better upper bounds by making use of T gate cancellations.

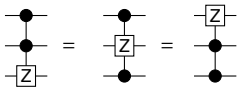
Theorem 10. *A c-control MPMCT gate with $c \geq 4$ can be realized with T-depth at most*

$$4(c-1)$$

using the B2 mapping.

Proof. We first note that the T-depth for a c-control MPMCT gate is the same as the T-depth for a c-control MCT gate. In particular, we may write the MPMCT gate as an MCT gate, conjugated on some bits by NOT gates. Since the NOT gates are irrelevant to the T-depth, the T-depth for an MPMCT gate is given by the T-depth of an MCT gate with the same number of controls.

Consider the c-control MCT gate mapped using the B2 algorithm as shown in Figure 3(b). We first rewrite every Toffoli with a doubly-controlled Z gate and a Hadamard gate on either side of the target line. As Hadamard gates are self-inverse, we remove two H gates for every pair of Toffolis having the same target and nothing in between (see Fig. 4(a)). Now recall that controlled phase gates are symmetric in that the target behaves like a control [33], i.e.,



By applying this fact (see Fig. 4(b)), we may observe that each doubly-controlled Z gate now shares exactly two controls with another gate, a fact that can be used to eliminate T gates by using the iZ-gate [34], defined as

$$iZ : |xyz\rangle \mapsto \omega^{4xyz-2xy}|xyz\rangle$$

where $\omega = e^{\frac{i\pi}{4}}$. We further denote by $iZ^\dagger$ its inverse. The iZ gate implements the doubly-controlled Z gate up to some phase and uses only 4 T-gates:

For each pair of doubly-controlled Z gates which share two controls, one is written as an iZ gate and a singly-controlled $S^\dagger$ gate, and the other is written as an $iZ^\dagger$ and a singly-controlled S gate (see Fig. 4(c)) – the controlled $S/S^\dagger$ gates then cancel (see Fig. 4(d)).

To further optimize this mapping, we define a refinement of the iZ gate – the $i\omega Z$ gate

$$i\omega Z : |xyz\rangle \mapsto \omega^{4xyz-2xy-z}|xyz\rangle$$

where $\omega = e^{\frac{i\pi}{4}}$ and $i\omega Z^\dagger$ is its inverse This gate may be implemented in T-depth 1, as below, and together with a $T^\dagger$ gate on the target implements the iZ gate:

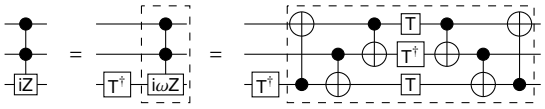


Fig. 5(a) shows the B2 mapping of the 5 control MCT gate where iZ gates have been replaced with $i\omega Z/i\omega Z^\dagger$ gates, and the T gates cancelled or otherwise parallelized (see Fig. 5(b)). Note that the 4 "points" of the cascade are left as iZ gates since they cannot be parallelized further. The extra phase gates from the outermost cascades (see Fig. 5(b)) also cancel despite being physically separated in the circuit, since each ancilla is returned to its initial state as in Figure 5(c).

To complete the analysis, we note that each $iZ/iZ^\dagger$ gate can be mapped to 4 T gates in depth 2 [34], while each $i\omega Z/i\omega Z^\dagger$ gate can be mapped in T-depth 1 as above. This gives a total T-depth of

$$4(c-2)+4 = 4(c-1).$$

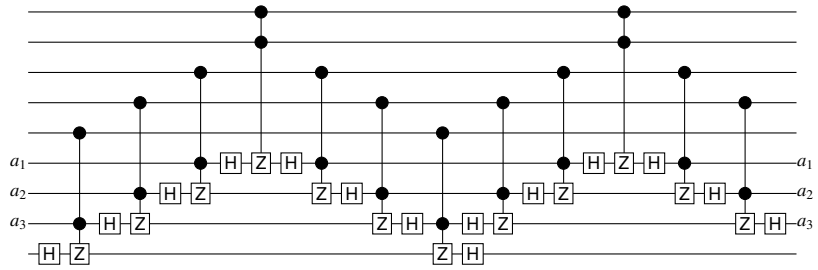
□

Note that this bound beats out the T-depths achieved by T-par [35], showing that their heuristic approach is non-optimal in some cases. Moreover, using a single 0-valued ancilla, the T-depth may be reduced to $4(c-2)$. Specifically, using a single ancilla in the zero state, the $iZ/iZ^\dagger$ gates may be mapped to a T-depth 1 circuit [34], giving a total T-depth of 1 for each two-control Toffoli in the original mapping – i.e. $4(c-2)$.

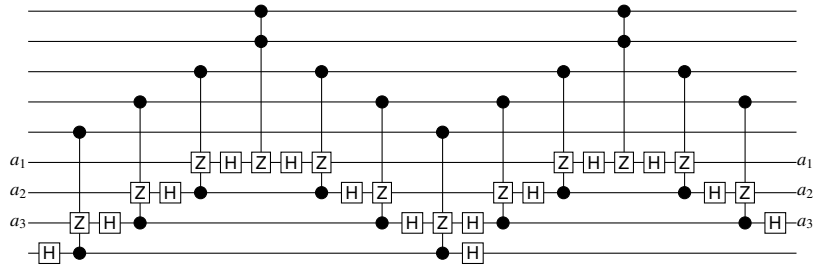
Next we give upper bounds on the T-depth of MPMCT gate mappings using a single helper line. For each single ancilla mapping (B1, NC, MI), a c-control MPMCT gate is broken down into m-control and $c-m+1$ or $c-m$-control MPMCT gates, which are further decomposed using the B2 mapping. In addition to the optimized B2 mapping above, we further reduce the T-depth bounds by using the *self-inverse* property of MPMCT gates to cancel additional $T/T^\dagger$ gates.

Theorem 11. *An c-control MPMCT gate with $c \geq 5$ controls can be realized with T-depth at most*

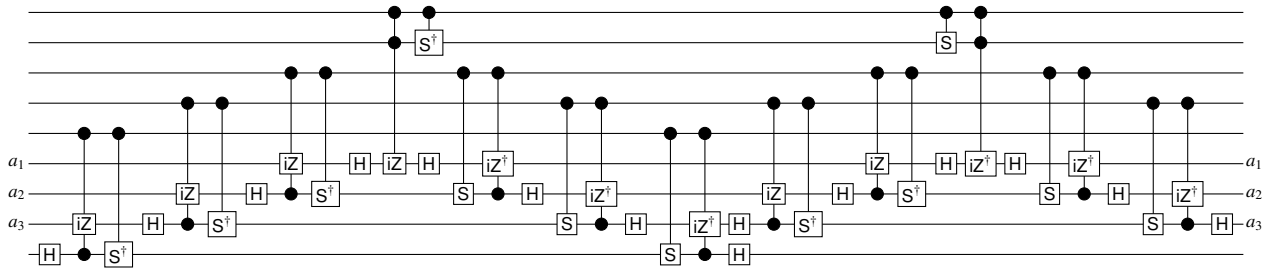
- $um_{\mathrm{CLF}_{\mathrm{B1}}}(c) \leq 8(c-2)$
- $um_{\mathrm{CLF}_{\mathrm{NC}}}(c) \leq 6(c-2)+2$
- $um_{\mathrm{CLF}_{\mathrm{MI}}}(c) \leq 8(c-3)+4$



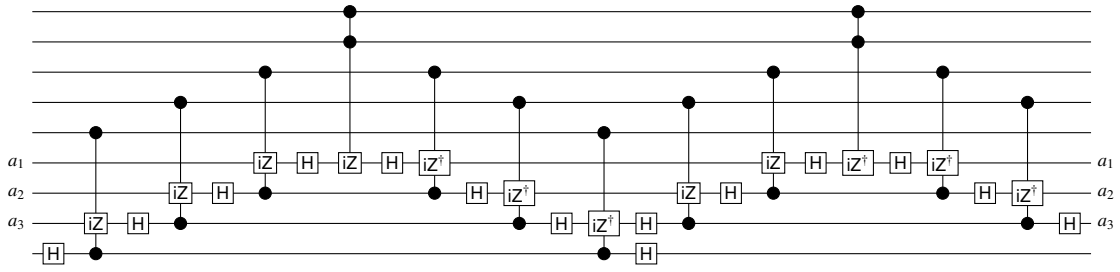
(a)



(b)



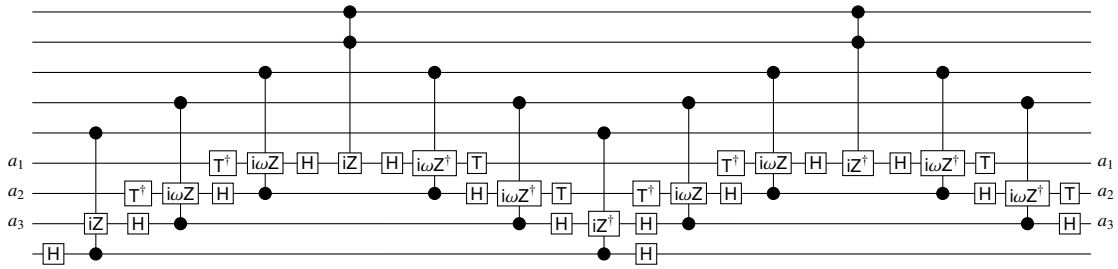
(c)



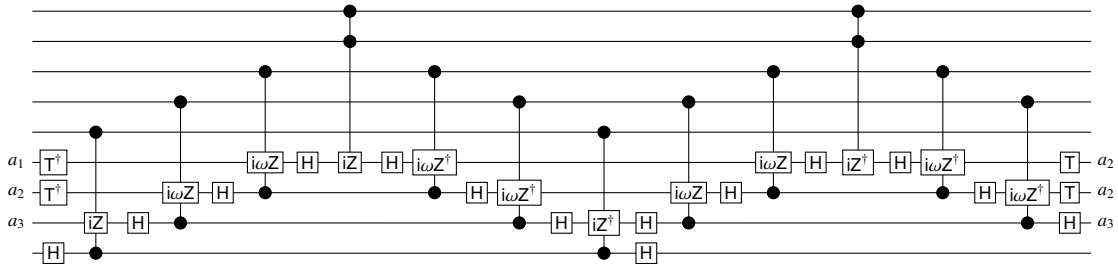
(d)

Figure 4: Optimization of B2 mapping w.r.t. T-depth

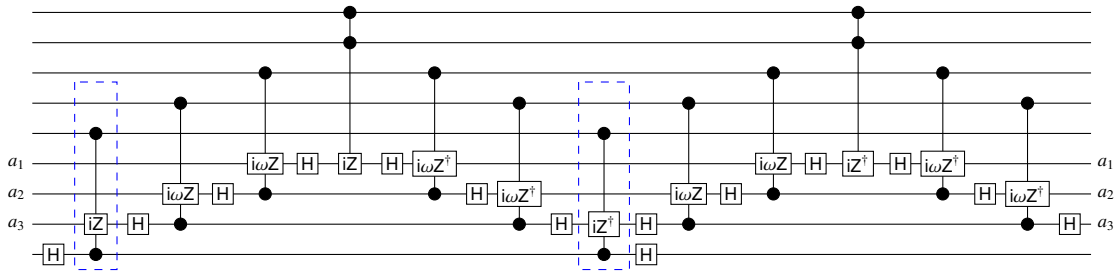
Proof. Consider the B1 mapping, as in Figure 2(b). If we map the first two MPMCT gates using the B2 mapping above, then use the *inverse* (obtained by reversing the circuit and replacing each T gate with $T^\dagger$) of the B2 mapping for the remaining MPMCT gates, we can cancel an additional 8 T gates. Specifically, for each pair of MPMCT gates



(a)



(b)



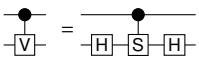
(c)

Figure 5: T-depth 17 implementation of the 5 control MCT gate using the B2 mapping

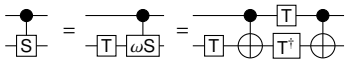
(first and third or second and fourth), the value on the target line of either dashed iZ gate shown in Figure 5(c) is constant. As in the proof of Theorem 10, we may then replace each dashed iZ gate with an $i\omega Z$ gate and cancel the extra T gates. The result is a total reduction of 8 levels of T-depth, giving a total T-depth for a c-control MPMCT gate of $2 \cdot 4(m-1) + 2 \cdot 4(c+1-m-1) - 8 = 8(c-2)$.

Using the same argument for the NC mapping, additional $T/T^\dagger$ gate (and layer of T-depth) from the first and third MPMCT gates. The resulting mapping has T-depth of $6(c-2)$ when c is even and $6(c-2)+2$ when c is odd.

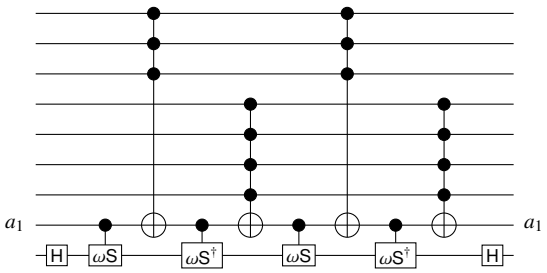
Finally consider the MI mapping. We use the same argument to reduce each of the 4 multiple control Toffolis by one layer of T-depth. We further note that each controlled V gate may be mapped in T-depth 1. In particular, we first map each controlled V to controlled S gates conjugated by Hadamards, as below:



then cancel adjacent Hadamards. The controlled S gates are then mapped alternately into $\omega S/\omega S^\dagger$ gates using



where ωS maps $|xy\rangle$ to $\omega^{2xy-y}|xy\rangle$. As shown in the following:



the additional $T/T^\dagger$ gates cancel, leaving 4 $\omega S/\omega S^\dagger$ gates, each of which is mapped to two $T/T^\dagger$ gates in T-depth 1. The total T-depth for the MI mapping scheme is then at most $2 \cdot 4(m-1) + 2 \cdot 4(c-m-1) - 8 + 4 = 8(c-3) + 4$. □

8.2. T-depth for Single-target Gates

The following corollary is proven in Appendix C.

Corollary 3. *From Lemma 1, we derive the following inequations for $n \geq 6$:*

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} 4(i-1) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n} 8(i-2) \cdot \binom{n}{i} \leq (6n-14) \cdot 2^{n-1} \tag{26}$$

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} 4(i-1) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n} (6(i-2)+2) \cdot \binom{n}{i} \leq (5n-11) \cdot 2^{n-1} \tag{27}$$

$$\sum_{i=0}^{\lceil \frac{n}{2} \rceil} 4(i-1) \cdot \binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil + 1}^{n} (8(i-3)+4) \cdot \binom{n}{i} \leq (6n-16) \cdot 2^{n-1} \tag{28}$$

Theorem 12. *An n-variable single-target gate can be realized, if $n \geq 6$, with T-depth at most*

- $us_{\mathrm{CLF_{B1}}}(n) \leq (6n-20) \cdot 2^{n-2}$
- $us_{\mathrm{CLF_{NC}}}(n) \leq (5n-16) \cdot 2^{n-2}$
- $us_{\mathrm{CLF_{MI}}}(n) \leq (6n-22) \cdot 2^{n-2}$

Proof. We have

$$us_{\mathrm{CLF_{B1}}}(n) \leq \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil} 4(i-1) \cdot \binom{n-1}{i} + \sum_{i=\lceil \frac{n-1}{2} \rceil + 1}^{n-1} 8(i-2) \cdot \binom{n-1}{i} \overset{\text{Corollary 3}}{\leq} (6(n-1)-14) \cdot 2^{n-2} \leq (6n-20) \cdot 2^{n-2}$$

The other upper bounds are proven using the same argument. □

Table 6: Updated T-depth for an MPMCT gate with c controls

Mapping	**Ancillas**	**Clifford+T**
B1 (Barenco et al. (Lemma 7.3 [15]))		$8(c-2)$
NC (Nielsen and Chuang [27])	1	$6(c-2)+2$
MI (Miller et al. [28])		$8(c-3)+4$
B2 (Barenco et al. (Lemma 7.2 [15]))	$c-2$	$4(c-1)$

Table 7: Complexity of reversible and quantum circuits

MPMCT Complexity Sect. 5.2	**Technology Mapping**	**NCT Complexity** Sect. 6.4	**NCV Complexity** Sect. 7.3	**Clifford+T Complexity** Sect. 8.3
$3(2n-1)\cdot 2^{n-4}$ [26]	B1 [15]	$(10n-28)\cdot 2^{n-1}$	$(11n-33)\cdot 2^{n}$	$(6n-14)\cdot 2^{n-1}$
	NC [27]	$(9n-25)\cdot 2^{n-1}$	$(9.5n-29.5)\cdot 2^{n}$	$(5n-11)\cdot 2^{n-1}$
	MI [28]	$(10n-32)\cdot 2^{n-1}$	$(11n-38)n\cdot 2^{n}$	$(6n-16)\cdot 2^{n-1}$

8.3. T-depth for Quantum Circuits

To the best of the authors' knowledge, no works thus far have studied the upper bounds on reversible quantum circuits over the Clifford+T library. In this section we study and compare the T-depth of such circuits using different kinds of synthesis approaches.

Theorem 13. *Using the transformation based synthesis approach, an n-variable reversible function can be realized over Clifford+T with a T-depth at most*

- $uc_{\mathrm{CLF}_{\mathrm{B1}}}(n) \leq (6n-14)\cdot 2^{n-1}$
- $uc_{\mathrm{CLF}_{\mathrm{NC}}}(n) \leq (5n-11)\cdot 2^{n-1}$
- $uc_{\mathrm{CLF}_{\mathrm{MI}}}(n) \leq (6n-16)\cdot 2^{n-1}$

Proof. For an n-variable reversible function, the synthesis approach produces a circuit with at most n NOT gates, $((n-1)\cdot 2^{n+1}-n^2+4)$ CNOT gates, and $\sum_{i=2}^{n-1}\binom{n}{i}$ MCT gates where i denotes the number of controls on each gate. The T-depth of a NOT or a CNOT gate is 0.

Based on the B1 mapping, we obtain at most

$$uc_{\mathrm{CLF}_{\mathrm{B1}}}(n) \leq \sum_{i=2}^{\lceil \frac{n}{2} \rceil} 4(i-1)\cdot\binom{n}{i} + \sum_{i=\lceil \frac{n}{2} \rceil+1}^{n-2} 8(i-2)\cdot\binom{n}{i} \overset{\text{Corollary 3}}{\leq} (6n-14)\cdot 2^{n-1}$$

The other upper bounds are obtained using the same argument. □

9. Summary and Conclusions

Table 7 outlines the upper bounds for reversible and quantum circuits using the mapping methods B1, NC, and MI. Note that the table sketches the circuit upper bounds derived from the transformation based synthesis approach [20]. Table 8 summarizes the best known upper bounds to represent an MPMCT gate (first column), a single-target gate (second column), and a circuit (third column) using single-target gates, MPMCT gates, NCT gates, NCV gates, and Clifford+T gates.

As can be seen from the tables, a comprehensive overview of upper bounds for the most commonly used reversible and quantum gate libraries has been proposed in this paper. Most of the bounds are tighter compared to the previously known ones. The bounds can be used to evaluate the quality of synthesis approaches. Although several bounds have been proposed, concrete circuit realizations for worst case functions are still missing. Knowing such functions would be very helpful for evaluating the limitations of known and new synthesis approaches.

Table 8: Summary for gate and circuit complexity

Gate library	MPMCT gate	ST gate	Circuit
ST	0	1	$2n-1$
MPMCT	1	$3 \cdot 2^{n-4}$	$3(2n-1) \cdot 2^{n-4}$
NCT	$6(c-3)$	$(5n-26) \cdot 2^{n-2}$	$(9n-25) \cdot 2^{n-1}$
NCV	$18(c-3)+6$	$(15n-70) \cdot 2^{n-2}$	$8.5n \cdot 2^n$ [11]
Clifford+T	$6(c-2)+2$	$(5n-16) \cdot 2^{n-2}$	$(5n-11) \cdot 2^{n-1}$

[1] De Vos, A.. Reversible Computing: Fundamentals, Quantum Computing and Applications. Wiley; 2010.
[2] Knill, E., Laflamme, R., Milburn, G.J.. A scheme for efficient quantum computation with linear optics. Nature 2001;409(1):46–52.
[3] Ren, J., Semenov, V.K., Polyakov, Y.A., Averin, D.V., Tsai, J.S.. Progress towards reversible computing with nSQUID arrays. IEEE Trans on Applied Superconductivity 2009;19(3):961–967.
[4] Houri, S., Valentian, A., Fanet, H.. Comparing CMOS-based and NEMS-based adiabatic logic circuits. In: Reversible Computation. Springer; 2013, p. 36–45.
[5] Athas, W.C., Svensson, L.J.. Reversible logic issues in adiabatic CMOS. In: Workshop on Physics and Computation. 1994, p. 111–118.
[6] Gupta, P., Agrawal, A., Jha, N.K.. An algorithm for synthesis of reversible logic circuits. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2006;25(11):2317–2330.
[7] De Vos, A., Van Rentergem, Y.. Young subgroups for reversible computers. Advances in Mathematics of Communications 2008;2(2):183–200.
[8] Soeken, M., Wille, R., Hilken, C., Przigoda, N., Drechsler, R.. Synthesis of reversible circuits with minimal lines for large functions. In: Asia and South Pacific Design Automation Conference, on. 2012, p. 85–92.
[9] Mohammadi, M., Eshghi, M.. On figures of merit in reversible and quantum logic designs. Quantum Information Processing 2009;8(4):297–318.
[10] Maslov, D., Dueck, G.W.. Reversible cascades with minimal garbage. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2004;23(11):1497–1509.
[11] Saeedi, M., Zamani, M.S., Sedighi, M., Sasanian, Z.. Reversible circuit synthesis using a cycle-based approach. Journal of Emerging Technologies 2010;6(4):13.
[12] Maslov, D., Miller, D.M.. Comparison of the cost metrics through investigation of the relation between optimal ncv and optimal nct 3-qubit reversible circuits. IET Computers & Digital Techniques 2007;1(2):98–104.
[13] Li, Z., Chen, H., Xu, B., XIAO, F.y., XUE, X.l.. Fast algorithms for 4-qubit reversible logic circuits synthesis. Acta Electronic Sinica 2008;36(11):2081–2089.
[14] Golubitsky, O., Maslov, D.. A study of optimal 4-bit reversible toffoli circuits and their synthesis. Computers, IEEE Transactions on 2012;61(9):1341–1353.
[15] Barenco, A., Bennett, C.H., Cleve, R., DiVinchenzo, D., Margolus, N., Shor, P., et al. Elementary gates for quantum computation. The American Physical Society 1995;52:3457–3467.
[16] Steane, A.M.. Efficient fault-tolerant quantum computing. Nature 1999;399(6732):124–126.
[17] Jones, N.C.. Logic synthesis for fault-tolerant quantum computers. arXiv preprint arXiv:13107290 2013;.
[18] Sasao, T.. AND-EXOR expressions and their optimization. In: Sasao, T., editor. Logic Synthesis and Optimization. Kluwer Academic Publisher; 1993, p. 287–312.
[19] Toffoli, T.. Reversible computing. Springer; 1980,.
[20] Miller, D.M., Maslov, D., Dueck, G.W.. A transformation based algorithm for reversible logic synthesis. In: Design Automation Conference. 2003, p. 318–323.
[21] Shende, V.V., Prasad, A.K., Markov, I.L., Hayes, J.P.. Synthesis of reversible logic circuits. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2003;22(6):710–722.
[22] Amy, M., Maslov, D., Mosca, M., Roetteler, M.. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. IEEE Trans on CAD of Integrated Circuits and Systems 2013;32(6):818–830.
[23] Abdessaied, N., Soeken, M., Drechsler, R.. Quantum circuit optimization by Hadamard gate reduction. In: Reversible Computation. Springer; 2014, p. 149–162.
[24] Soeken, M., Abdessaied, N., Drechsler, R.. A framework for reversible circuit complexity. arXiv preprint arXiv:14075878 2014;.
[25] Soeken, M., Tague, L., Dueck, G.W., Drechsler, R.. Ancilla-free synthesis of large reversible functions using binary decision diagrams. Journal of Symbolic Computation 2015;.
[26] Abdessaied, N., Soeken, M., Thomsen, M.K., Drechsler, R.. Upper bounds for reversible circuits based on young subgroups. Information Processing Letters 2014;114(6):282 – 286.
[27] Nielsen, M., Chuang, I.. Quantum Computation and Quantum Information. Cambridge Univ. Press; 2000.
[28] Miller, D.M., Wille, R., Sasanian, Z.. Elementary quantum gate realizations for multiple-control Toffolli gates. In: International Symposium on Multiple-Valued Logic, on. 2011, p. 217–222.
[29] Maslov, D., Dueck, G.. Improved quantum cost for n-bit Toffoli gates. Electronics Letters 2003;39:1790.
[30] Maslov, D., Dueck, G., Miller, D., Negrevergne, C.. Quantum circuit simplification and level compaction. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2008;27(3):436–444.
[31] Gaidukov, A.. Algorithm to derive minimum ESOP for 6-variable function. In: International Workshop on Boolean Problems. 2002, p. 141–148.

[32] Große, D., Wille, R., Dueck, G.W., Drechsler, R.. Exact multiple control Toffoli network synthesis with SAT techniques. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2009;28(5):703–715.
[33] Soeken, M., Miller, D.M., Drechsler, R.. Quantum circuits employing roots of the pauli matrices. Physical Review A 2013;88:042322.
[34] Selinger, P.. Quantum circuits of t-depth one. Physical Review A 2013;87(4):042302.
[35] Amy, M., Maslov, D., Mosca, M.. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on 2014;33(10):1476–1489.
[36] Graham, R.L., Knuth, D.E., Patashnik, O.. Concrete Mathematics. Addison-Wesley; 1994.

Appendix A. Proof of Lemma 1

This and the following proofs use many identities that can be found in [36].

Proof. Taking into conservation that

$$\sum_{i=1}^{n} i\binom{n}{i} = n \cdot 2^{n-1} \qquad \text{and} \qquad i\binom{n}{i} = (n-(i+1))\binom{n}{n-(i+1)},$$

we consider the cases when n is even and n is odd. If n is even, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n}{2}$. Then

$$\sum_{i=1}^{\frac{n}{2}} i\binom{n}{i} + \sum_{i=\frac{n}{2}+1}^{n} i\binom{n}{i} = n \cdot 2^{n-1} \qquad \text{and} \qquad 2\sum_{i=\frac{n}{2}+1}^{n} i\binom{n}{i} = n \cdot 2^{n-1},$$

and therefore

$$\sum_{i=\frac{n}{2}+1}^{n} i\binom{n}{i} = n \cdot 2^{n-2} \qquad \text{and} \qquad \sum_{i=1}^{\frac{n}{2}} i\binom{n}{i} = n \cdot 2^{n-2}$$

If n is odd, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n+1}{2}$. Then

$$\sum_{i=1}^{\frac{n+1}{2}} i\binom{n}{i} + \sum_{i=\frac{n+3}{2}}^{n} i\binom{n}{i} = n \cdot 2^{n-1} \qquad \text{and} \qquad \frac{n+1}{2}\binom{\frac{n+1}{2}}{n} + 2\sum_{i=\frac{n+3}{2}}^{n} i\binom{n}{i} = n \cdot 2^{n-1},$$

and therefore

$$\sum_{i=\frac{n+3}{2}}^{n} i\binom{n}{i} = n \cdot 2^{n-2} - \frac{n+1}{4}\binom{\frac{n+1}{2}}{n} \qquad \text{and} \qquad \sum_{i=1}^{\frac{n+1}{2}} i\binom{n}{i} = n \cdot 2^{n-2} + \frac{n+1}{4}\binom{\frac{n+1}{2}}{n}.$$

The other inequations are derived using the same argument. □

Appendix B. Proof of Corollary 1

Proof. We consider the cases when n is even and n is odd. If n is even, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n}{2}$. Then

$$\sum_{i=0}^{\frac{n}{2}} \binom{n}{i} = 2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}} \qquad \text{and} \sum_{i=\frac{n}{2}+1}^{n} \binom{n}{i} = 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}},$$

and therefore

$$\begin{aligned}
&4 \cdot \sum_{i=1}^{\frac{n}{2}} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\frac{n}{2}+1}^{n} (i-3)\binom{n}{i} \\
&= 4 \cdot \sum_{i=1}^{\frac{n}{2}} i\binom{n}{i} - 8 \cdot \sum_{i=1}^{\frac{n}{2}} \binom{n}{i} + 8 \cdot \sum_{i=\frac{n}{2}+1}^{n} i\binom{n}{i} - 24 \cdot \sum_{i=\frac{n}{2}+1}^{n} \binom{n}{i} \\
&\overset{\text{Lemma 1}}{=} 4n \cdot 2^{n-2} - 8\left(2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}\right) + 8n \cdot 2^{n-2} - 24\left(2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}}\right) \\
&= (6n-32) \cdot 2^{n-1} + 8\binom{\frac{n}{2}}{n}
\end{aligned}$$

Since $\binom{\frac{n}{2}}{n} \leq 2^{n-1}$, we get

$$4 \cdot \sum_{i=1}^{\frac{n}{2}} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\frac{n}{2}+1}^{n} (i-3)\binom{n}{i} \leq (6n-32) \cdot 2^{n-1} + 8.2^{n-1} = (6n-24) \cdot 2^{n-1}$$

If n is odd, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n+1}{2}$. Then

$$\sum_{i=0}^{\frac{n+1}{2}} \binom{n}{i} = 2^{n-1} + \binom{\frac{n+1}{2}}{n} \qquad \text{and} \qquad \sum_{i=\frac{n+3}{2}}^{n} \binom{n}{i} = 2^{n-1} - \binom{\frac{n+1}{2}}{n},$$

and therefore

$$\begin{aligned}
&4 \cdot \sum_{i=1}^{\frac{n+1}{2}} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\frac{n+3}{2}}^{n} (i-3)\binom{n}{i} \\
&= 4 \cdot \sum_{i=1}^{\frac{n+1}{2}} i\binom{n}{i} - 8 \cdot \sum_{i=1}^{\frac{n+1}{2}} \binom{n}{i} + 8 \cdot \sum_{i=\frac{n+3}{2}}^{n} i\binom{n}{i} - 24 \cdot \sum_{i=\frac{n+3}{2}}^{n} \binom{n}{i} \\
&\overset{\text{Lemma 1}}{=} 4\left(n \cdot 2^{n-2} + \frac{n+1}{4}\binom{\frac{n+1}{2}}{n}\right) - 8\left(2^{n-1} + \binom{\frac{n+1}{2}}{n}\right) + 8\left(n \cdot 2^{n-2} - \frac{n+1}{4}\binom{\frac{n+1}{2}}{n}\right) - 24\left(2^{n-1} - \binom{\frac{n+1}{2}}{n}\right) \\
&= (6n-32) \cdot 2^{n-1} - (n-15)\binom{\frac{n+1}{2}}{n}
\end{aligned}$$

Since $\binom{\frac{n+1}{2}}{n} \leq 2^{n-3}$, we get

$$\begin{aligned}
4 \cdot \sum_{i=1}^{\frac{n+1}{2}} (i-2)\binom{n}{i} + 8 \cdot \sum_{i=\frac{n+3}{2}}^{n} (i-3)\binom{n}{i} &\leq (6n-32) \cdot 2^{n-1} - (n-15) \cdot 3 \cdot 2^{n-1} \\
&= (6n-24) \cdot 2^{n-1} - 8 \cdot 2^{n-1} - (n-15) \cdot 3 \cdot 2^{n-3} \\
&= (6n-24) \cdot 2^{n-1} - (3n-13) \cdot 2^{n-3} \leq (6n-24) \cdot 2^{n-1}
\end{aligned}$$

The other inequations are derived using the same argument. □

Appendix C. Proof of Corollaries 2 and 3

We give the proof for Corollary 2, the proof for Corollary 3 follows the same argument.

Proof. We consider the cases when n is even and n is odd. If n is even, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n}{2}$. Then

$$\sum_{i=0}^{\frac{n}{2}} \binom{n}{i} = 2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}} \qquad \text{and} \qquad \sum_{i=\frac{n}{2}+1}^{n} \binom{n}{i} = 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}},$$

and therefore

$$\begin{aligned}
&\sum_{i=1}^{\frac{n}{2}} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\frac{n}{2}+1}^{n} (24(i-3)+12) \cdot \binom{n}{i} \\
&= 12 \cdot \sum_{i=1}^{\frac{n}{2}} i\binom{n}{i} - 22 \cdot \sum_{i=1}^{\frac{n}{2}} \binom{n}{i} + 24 \cdot \sum_{i=\frac{n}{2}+1}^{n} i\binom{n}{i} - 60 \cdot \sum_{i=\frac{n}{2}+1}^{n} \binom{n}{i} \\
&\overset{\text{Lemma 1}}{=} 12n \cdot 2^{n-2} - 22\left(2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}\right) + 24n \cdot 2^{n-2} - 60\left(2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}}\right) \\
&= (18n-82) \cdot 2^{n-1} + 19\binom{\frac{n}{2}}{n}
\end{aligned}$$

Since $\binom{\frac{n}{2}}{n} \leq 3 \cdot 2^{n-1}$, we get

$$\sum_{i=1}^{\frac{n}{2}} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\frac{n}{2}+1}^{n} (24(i-3)+12) \cdot \binom{n}{i} \leq (18n-82) \cdot 2^{n-1} + 19.2^{n-1} = (18n-63) \cdot 2^{n-1}$$

If n is odd, we have $\left\lceil \frac{n}{2} \right\rceil = \frac{n+1}{2}$. Then

$$\sum_{i=0}^{\frac{n+1}{2}} \binom{n}{i} = 2^{n-1} + \binom{\frac{n+1}{2}}{n} \qquad \text{and} \qquad \sum_{i=\frac{n+3}{2}}^{n} \binom{n}{i} = 2^{n-1} - \binom{\frac{n+1}{2}}{n},$$

and therefore

$$\begin{aligned}
&\sum_{i=1}^{\frac{n+1}{2}} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\frac{n+3}{2}}^{n} (24(i-3)+12) \cdot \binom{n}{i} \\
&= 12 \cdot \sum_{i=1}^{\frac{n+1}{2}} i\binom{n}{i} - 22 \cdot \sum_{i=1}^{\frac{n+1}{2}} \binom{n}{i} + 24 \cdot \sum_{i=\frac{n+3}{2}}^{n} i\binom{n}{i} - 60 \cdot \sum_{i=\frac{n+3}{2}}^{n} \binom{n}{i} \\
&\overset{\text{Lemma 1}}{=} 12\left(n \cdot 2^{n-2} + \frac{n+1}{4}\binom{\frac{n+1}{2}}{n}\right) - 22\left(2^{n-1} + \binom{\frac{n+1}{2}}{n}\right) + 24\left(n \cdot 2^{n-2} - \frac{n+1}{4}\binom{\frac{n+1}{2}}{n}\right) - 60\left(2^{n-1} - \binom{\frac{n+1}{2}}{n}\right) \\
&= (18n-82) \cdot 2^{n-1} - (3n-35)\binom{\frac{n+1}{2}}{n}
\end{aligned}$$

Since $\binom{\frac{n+1}{2}}{n} \leq 3 \cdot 2^{n-3}$, we get

$$\begin{aligned}
\sum_{i=1}^{\frac{n+1}{2}} (12(i-2)+2) \cdot \binom{n}{i} + \sum_{i=\frac{n+3}{2}}^{n} (24(i-3)+12) \cdot \binom{n}{i} &\leq (18n-63) \cdot 2^{n-1} - 19 \cdot 2^{n-1} - (3n-35) \cdot 3 \cdot 2^{n-3} \\
&= (18n-63) \cdot 2^{n-1} - (9n-29) \cdot 2^{n-3} \leq (18n-63) \cdot 2^{n-1}
\end{aligned}$$

The other inequations are derived using the same argument. □