Canonical Multi-Target Toffoli Circuits

Hans-Jörg Kreowski, Sabine Kuske, and Aaron Lye

University of Bremen, Department of Computer Science
P.O.Box 33 04 40, 28334 Bremen, Germany
{kreo,kuske,lye}@informatik.uni-bremen.de

Abstract. In this paper, we study reversible circuits as cascades of multi-target Toffoli gates. This new type of gates allows to shift parts of a gate to the preceding gate within a circuit provided that a certain independence condition holds. It turns out that shifts decrease the so-called waiting degree such that shifting as long as possible always terminates and yields shift-reduced circuits. As the main result, we show that shift-reduced circuits are unique canonical representatives of their shift equivalence classes. Canonical circuits are optimal with respect to maximal and as-early-as-possible parallelism of targets within gates.

Keywords: canonical form, multi-target Toffoli circuits, reversible computation, shift equivalence

1 Introduction

Reversible computation is an alternative to conventional computing motivated by the fact that the integration density of circuits reaches physical limits in scale and power dissipation. Due to the fact that energy dissipation is significantly reduced or even eliminated in reversible circuits [1], reversible computing is a very promising research area.

Reversible circuits are cascades of reversible gates that compute invertible functions on Boolean vectors. To specify reversible circuits, the gate model introduced by Toffoli [9] is frequently used. In the past this model has been generalized in different ways. In this paper we want to generalize this model further by introducing multi-target Toffoli gates.

A (single-target multi-controlled) Toffoli gate consists of a target line and a set of control lines each of which is different from the target line. The lines represent Boolean variables. The target line gets negated if and only if all control lines are carrying the value 1. All other values are kept invariant by the evaluation of the gate. In particular, a Toffoli gate is reversed by itself. Consider now a set of Toffoli gates such that the target lines are pairwise different and all control lines are disjoint from all target lines. Such gates may be called independent because their evaluation in every sequential order yields the same Boolean function. Moreover, their evaluation can be done in parallel because the various negations cannot interfere with each other. This motivates us to introduce such sets of independent Toffoli gates as a multi-target Toffoli gate.

As the parallel as well as each sequential evaluation of independent gates yield the same result, a multi-target Toffoli gate can be sequentialized with respect to every partition of the set of target lines. Conversely, two gates can be parallelized into one gate if their sets of target lines are disjoint and no target line is control line of the other gate. There is a weaker form of combining two

multi-target Toffoli gates that can be applied much more frequently than the full parallelization: One of the gates is sequentialized first and then only one of the parts is parallelized with the other gate if possible. In this case, a part of a gate is shifted to another gate. The shifts (together with the parallelization) define a relation on multi-target Toffoli circuits with quite significant properties. First of all, the shift relation has the local Church-Rosser property meaning that the circuits resulting from two shifts on a given circuit can be further shifted into a common result. Secondly, shifts decrease the so-called waiting degree. For each target line of some gate, there is a number of preceding gates. If evaluation is done gate by gate, this is the number of steps a negation must wait before it is executed. The waiting degree sums up all these numbers. As the waiting degree decreases with each shift, the lengths of shift sequences are bounded by the maximum waiting degree (which is $\frac{m(m-1)}{2}$ for the number m of target lines of a circuit). In particular, the iteration of shifts as long as possible terminates always with a circuit reduced with respect to shifting. Combining both results, the shift-reduced circuits turn out to be unique normal forms within the classes of shift-equivalent circuits. Therefore, it is justified to call shift-reduced multi-target Toffoli gates canonical. Canonical circuits are optimal with respect to maximal and as-early-as-possible parallelism of targets within gates.

Shifts, shift equivalence and shift-reduced normal forms as unique canonical representatives of their shift equivalence classes were studied by the first author quite some time ago for parallel derivations in graph grammars (see [5–7]). Although multi-target Toffoli circuits as considered in this paper provide a setting quite different from parallel graph grammar derivations, the same ideas work.

The paper is organized as follows. Section 2 introduces the characteristics of reversible functions and circuits. In Section 3 multi-target Toffoli circuits are defined, followed by considering sequentialization, parallelization and shift in Section 4. Section 5 introduces the waiting degree. Section 6 covers our theorem on canonical circuits. Finally, Section 7 contains a conclusion.

2 Reversible Circuits

In this section we introduce the background on reversible functions and their relation to reversible circuits.

2.1 Reversible Functions

Reversible logic can be used for realizing reversible functions. Reversible functions are special multi-output functions and defined as follows.

Definition 1. Let $\mathbb{B} = \{0, 1\}$ be the set of truth values with the negations $\overline{0} = 1$ and $\overline{1} = 0$ and ID be a set of identifiers serving as a reservoir of Boolean variables. Let $\mathbb{B}^X$ be the set of all mappings $a\colon X \to \mathbb{B}$ for some $X \subseteq ID$ where the elements of $\mathbb{B}^X$ are called *assignments*. If the set of variables is ordered, each assignment corresponds to a Boolean vector. Then a bijective Boolean (multi-output) function $f\colon \mathbb{B}^X \to \mathbb{B}^X$ is called *reversible*.

2.2 Reversible Circuits

Reversible circuits are used for representing reversible functions because a reversible function can be realized by a cascade of reversible gates. Reversible

circuits differ from conventional circuits: while conventional circuits rely on the basic binary operations and also fanouts are applied in order to use signal values on several gate inputs, in reversible logic fanouts and feedback are not directly allowed because they would destroy the reversibility of the computation. Also the logic operators AND and OR cannot be used since they are irreversible. Instead a reversible gate library is applied. Since the Boolean operator NOT is inverse, the NOT-gate is part of this reversible library. To increase the expressiveness the universal *Toffoli gate* has been introduced, which is a multi-controlled NOT-gate. Since the Toffoli gate is universal, all reversible functions can be realized by cascades of this gate type alone (cf. [9]).

A (*multiple-control*) *Toffoli gate* consists of a *target line* $t \in ID$ and a set $C \subseteq ID - \{t\}$ of *control lines* and is denoted by $TG(t, C)$. The gate defines the function $f_{t,C} \colon \mathbb{B}^X \to \mathbb{B}^X$ for each $X \subseteq ID$ with $\{t\} \cup C \subseteq X$ which maps an assignment $a \colon X \to \mathbb{B}$ to $f_{t,C}(a) \colon X \to \mathbb{B}$ given by $f_{t,C}(a)(t) = \overline{a(t)}$ if $a(c) = 1$ for all $c \in C$. In all other cases, $f_{t,C}(a)$ is equal to a. Hence, $f_{t,C}(a)$ inverts the value of the target line if and only if all control lines are set to 1. Otherwise the value of the target line is passed through unchanged. The values of all other lines always pass through a gate unchanged. Consequently, $f_{t,C}$ is a mapping on $\mathbb{B}^X$ which is inverse to itself and, therefore, reversible in particular. A multiple-control Toffoli gate can be realized by a sequence of Toffoli gates with two control lines.

Example 2. The four simplest multi-controlled Toffoli gates are NOT, $CNOT$, $CCNOT$, and C^3NOT.

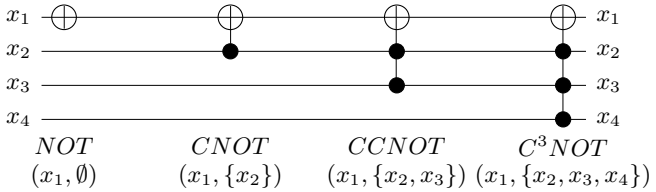


Fig. 1. The four simplest multi-controlled Toffoli gates

In the graphical representation, the target line is indicated by $\oplus$ and the control lines by $\bullet$ vertically connected with their target line (Fig 1).

In addition to positive control lines, in the recent past also negative- and mixed-control Toffoli gates have been considered [8]. This gains smaller circuits in general. Nevertheless, the expressiveness remains the same, since each negative control can be replaced by a positive one with a negation before and after the control. For this reason, in this work we focus on positive control Toffoli gates.

An *extended-target Toffoli gate*, as proposed in [2], with multiple control lines and multiple target lines, denoted by the sets C and T, respectively, holding $C \cup T \subseteq X$, $T \neq \emptyset$ and $C \cap T = \emptyset$, realizes the function $f(a)(x) = \overline{a(x)}$ if $x \in T$ and $a(y) = 1$ for all $y \in C$, and $a(x)$ otherwise. This means that the values of all target lines are negated if the value of each control line is 1. We discuss a further generalization in the following section.

3 Multi-Target Toffoli Circuits

In this section, we introduce the notion of multi-target Toffoli circuits as cascades of multi-target Toffoli gates. Such a gate has a set of target lines where each

target line is controlled by a set of control lines which is disjoint from the set of target lines.

Definition 3. 1. A *multi-target Toffoli gate* over a set X of lines is a pair $mtg = (T, c\colon T \to 2^X)$ with $T \subseteq X$, $T \neq \emptyset$ and $T \cap c(T) = \emptyset$ where $c(T) = \bigcup_{t \in T} c(t)$. T is the *set of target lines*, and $c(t)$ is the *set of control lines* of t for $t \in T$.
2. A multi-target Toffoli gate $mtg = (T, c)$ models the following semantic function f_{mtg} on $\mathbb{B}^X$:

$$f_{mtg}(a)(x) = \begin{cases} \overline{a(x)} & \text{if } x \in T \text{ and } a(y) = 1 \text{ for all } y \in c(x), \\ a(x) & \text{otherwise.} \end{cases}$$

3. A *multi-target Toffoli circuit* $mtc = mtg_1 \dots mtg_n$ is a sequence of multi-target Toffoli gates. Its length n is denoted by $|mtc|$.
4. Let mtc be a multi-target Toffoli circuit. It models the semantic function f_{mtc} defined as the sequential composition of the semantic functions of the gates, i.e.

$$f_{mtc} = f_{mtg_n} \circ \dots \circ f_{mtg_1}.$$

If a multi-target Toffoli gate mtg has the set T of target lines and T' is a subset of T, then mtg can be restricted to T' and its complement $T'' = T - T'$ yielding the multi-target Toffoli gates mtg' and mtg''. It turns out that the sequential composition $mtg'mtg''$ is semantically equivalent to mtg.

Proposition 4. Let $mtg = (T, c)$ be a multi-target Toffoli gate, let $T' \subseteq T$ with $\emptyset \neq T' \neq T$.

1. Then $mtg' = (T', c')$ with $c'(t') = c(t')$ for $t' \in T'$ is a multi-target Toffoli gate. This gate may be denoted by $mtg|_{T'}$, called the *restriction of mtg to* T'.
2. Accordingly, $mtg'' = (T'', c'')$ with $T'' = T - T'$ and $c''(t'') = c(t'')$ for $t'' \in T''$ is also a multi-target Toffoli gate.
3. The sequential composition $mtg'mtg''$ is semantically equivalent to mtg, i.e. $f_{mtg} = f_{mtg'mtg''}$.

Proof. 1. $T' \cap c'(T') = T' \cap \bigcup_{t' \in T'} c'(t') = T' \cap \bigcup_{t' \in T'} c(t') \subseteq T \cap \bigcup_{t \in T} c(t) = T \cap c(T) = \emptyset$.
2. $T' \subseteq T$ and $\emptyset \neq T' \neq T$ imply $T - T' \subseteq T$ and $\emptyset \neq T - T' \neq T$ such that Point 1 applies to $T'' = T - T'$.
3. By definition, we get the following equations for all $a \in \mathbb{B}^X$ and $x \in X$:

$$\begin{aligned} f_{mtg'mtg''}(a)(x) &= (f_{mtg''} \circ f_{mtg'})(a)(x) = f_{mtg''}(f_{mtg'}(a))(x) \\ &= \begin{cases} \overline{f_{mtg'}(a)(x)} & \text{if } x \in T'' \text{ and } f_{mtg''}(a)(y) = 1 \text{ for all } y \in c''(x), \\ f_{mtg'}(a)(x) & \text{otherwise,} \end{cases} \end{aligned}$$

as well as

$$f_{mtg'}(a)(x) = \begin{cases} \overline{a(x)} & \text{if } x \in T' \text{ and } a(y) = 1 \text{ for all } y \in c'(x), \\ a(x) & \text{otherwise.} \end{cases}$$

Combining these results and using $T' \cap T'' = \emptyset$, $T' \cup T'' = T$ and the disjointness of control and target lines, we get:

$$\begin{aligned} f_{mtg'mtg''}(a)(x) &= \begin{cases} \overline{a(x)} & \text{if } x \in T'' \text{ and } a(y) = 1 \text{ for all } y \in c''(x), \\ \overline{a(x)} & \text{if } x \in T' \text{ and } a(y) = 1 \text{ for all } y \in c'(x), \\ a(x) & \text{otherwise,} \end{cases} \\ &= \begin{cases} \overline{a(x)} & \text{if } x \in T \text{ and } a(y) = 1 \text{ for all } y \in c(x), \\ a(x) & \text{otherwise,} \end{cases} \\ &= f_{mtg}(a)(x). \end{aligned}$$

This proves the statement.

Given the situation of Proposition 4, the circuit $mtg'mtg''$ may be seen as a sequentialization of mtg and mtg as a parallelization of $mtg'mtg''$. In the next section, both operations are considered within arbitrary circuits.

4 Sequentialization, Parallelization and Shift

Sequentialization and parallelization can be done within large circuits inducing an equivalence relation on multi-target Toffoli circuits. As parallelization, a particular composition of a sequentialization and a parallelization shifts some target lines of a gate to the preceding gate.

Shifts are defined formally as a generalization of parallelization. The shift operation is quite nondeterministic as there may be many gates within a circuit that allow shifting. But it turns out that shifting has the local Church-Rosser property meaning that two circuits obtained by two shifts on a circuit can always be shifted into a common circuit.

Definition 5. Let $mtg = (T, c)$ be a multi-target Toffoli gate and $T' \subseteq T$ with $\emptyset \neq T' \neq T$. Let mtg' be the restriction of mtg to T' and mtg'' the restriction of mtg to $T'' = T - T'$. Then

1. $mtg'mtg''$ is called *sequentialization* of mtg wrt T' and mtg *parallelization* of $mtg'mtg''$. The parallelization is also denoted by $mtg' + mtg''$.
2. Let $mtc = mtc'mtgmtc''$ be a multi-target Toffoli circuit and $mtg'mtg''$ be the sequentialization of mtg wrt T'. Then mtc and $\overline{mtc} = mtc'mtg'mtg''mtc''$ are in seq-relation wrt T' in gate $i = |mtc'| + 1$, denoted by

$$mtc \xrightarrow[seq(i,T')]{} \overline{mtc}$$

as well as in par-relation after gate $i - 1 = |mtc'|$, denoted by

$$\overline{mtc} \xrightarrow[par(i-1)]{} mtc.$$

Let $\sim_{seq}$ be the equivalence relation induced by seq, i.e. the reflexive, symmetric, and transitive closure of seq and $\sim_{par}$ the corresponding equivalence relation induced by par. Then, obviously, $\sim_{seq}$ and $\sim_{par}$ are equal because seq and par are inverse to each other.

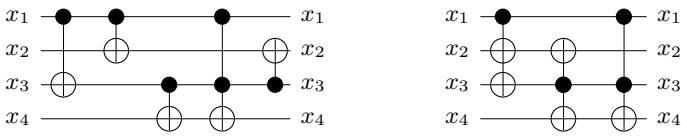
Definition 6. Let mtc and $\widetilde{mtc}$ be two multi-target Toffoli circuits. Then $\widetilde{mtc}$ is a *shift* of mtc if $mtc \xrightarrow[par(i-1)]{} \widetilde{mtc}$ or $mtc \xrightarrow[seq(i+1,T')]{} \overline{mtc} \xrightarrow[par(i-1)]{} \widetilde{mtc}$ for some $i \geq 1$ and $T' \subseteq X$, denoted by

$$mtc \xrightarrow[sh(i,T')]{} \widetilde{mtc}$$

where T' is the set of target lines of the gate $i+1$ in case that the shift is just a parallelization. If i and T' are clear from the context, then we may write $mtc \xrightarrow[sh]{} \widetilde{mtc}$.

Example 7. Consider the mtc over four lines x_1 to x_4 including the gates $mtg_1 = (\{x_3\}, c_1)$ with $c_1(x_3) = \{x_1\}$, $mtg_2 = (\{x_2\}, c_2)$ with $c_2(x_2) = \{x_1\}$, $mtg_3 = (\{x_4\}, c_3)$ with $c_3(x_4) = \{x_3\}$, $mtg_4 = (\{x_4\}, c_4)$ with $c_4(x_4) = \{x_1, x_3\}$ and $mtg_5 = (\{x_2\}, c_5)$ with $c_5(x_2) = \{x_3\}$ as depicted in Fig. 2(a).

Obviously, mtg_1 and mtg_2 can be parallelized because the target line of the one gate is no target or control line of the other gate. The same holds for gates mtg_4 and mtg_5. Hence, we get $mtc \xrightarrow[par(0)]{} mtc' \xrightarrow[par(2)]{} mtc''$ with $mtc' = mtg_1' mtg_3 mtg_4 mtg_5$ and $mtc'' = mtg_1' mtg_3 mtg_4'$ where $mtg_1' = (\{x_2, x_3\}, c_1')$ with $c_1'(x_2) = c_1'(x_3) = \{x_1\}$ and $mtg_4' = (\{x_2, x_4\}, c_4')$ with $c_4'(x_2) = \{x_3\}$ and $c_4'(x_4) = \{x_1, x_3\}$. Afterwards we can apply the shift $sh(2, \{x_2\})$ to mtc'' by sequentializing mtg_4' wrt $\{x_2\}$ and parallelizing the resulting circuit after mtg_1'. This yields the circuit depicted in Fig. 2(b) where $mtg_2' = (\{x_2, x_4\}, c_2')$ with $c_2'(x_2) = c_2'(x_4) = \{x_3\}$.



(a) $mtg_1 mtg_2 mtg_3 mtg_4 mtg_5$ (b) $mtg_1' mtg_2' mtg_4$

Fig. 2. Shifting a multi-target Toffoli circuit

Proposition 8. The shift relation has the local Church-Rosser property meaning that two shifts on a circuit mtc

$$mtc \xrightarrow[sh]{} mtc_1 \quad mtc \xrightarrow[sh]{} mtc_2 \qquad \text{imply} \qquad mtc_1 \xrightarrow[sh]{*} \overline{mtc} \quad mtc_2 \xrightarrow[sh]{*} \overline{mtc}$$

for some circuit $\overline{mtc}$ where $\xrightarrow[sh]{*}$ is the reflexive and transitive closure of the shift relation sh.

Proof. A shift changes two successive gates of a circuit and keeps the rest invariant. Hence two shifts that change four different gates cannot interfere with each other so that they can be applied in any order yielding the same result. The situation becomes more complicated if the two shifts change two or three successive gates. Then various cases can occur. They are listed in Fig. 3.

Let us start with shifts on the same two gates. Then both shifts may be proper shifts of different parts of the second gate or one of the shifts is the

parallelization of the two gates. If both shifts are proper, the parts shifted may be incomparable or one may be a subpart of the other. Hence there are three cases to be considered. As an abbreviation, we write g for mtg.

Case 1: Let $g = (T, c)$ and $g' = (T', c')$. Then the given shifts of $\hat{T}$ and $\hat{\hat{T}}$ in gate $|mtc'| + 2$ with $\hat{T} - \hat{\hat{T}} \neq \emptyset \neq \hat{\hat{T}} - \hat{T}$ are defined because $\hat{T} \cap T = \emptyset = \hat{\hat{T}} \cap T$ and $T \cap c'(\hat{T}) = \emptyset = T \cap c'(\hat{\hat{T}})$. The changed gates after the shifts are:

$$g + g'|_{\hat{T}} = (T \cup \hat{T}, \hat{c}), \qquad g'|_{T-\hat{T}} = (T - \hat{T}, c'|_{T-\hat{T}}),$$
$$g + g'|_{\hat{\hat{T}}} = (T \cup \hat{\hat{T}}, \hat{\hat{c}}), \qquad g'|_{T-\hat{\hat{T}}} = (T - \hat{\hat{T}}, c'|_{T-\hat{\hat{T}}})$$

with $\hat{c}(x) = \hat{\hat{c}}(x) = c(x)$ for $x \in T$, $\hat{c}(x) = c'(x)$ for $x \in \hat{T}$, $\hat{\hat{c}}(x) = c'(x)$ for $x \in \hat{\hat{T}}$. Moreover, the following holds:

$$(\hat{\hat{T}} - \hat{T}) \cap (T \cup \hat{T}) = ((\hat{\hat{T}} - \hat{T}) \cap T) \cup ((\hat{\hat{T}} - \hat{T}) \cap \hat{T}) \subseteq \hat{\hat{T}} \cap T = \emptyset,$$
$$(T \cup \hat{T}) \cap c'(\hat{\hat{T}} - \hat{T}) = (T \cap c'(\hat{\hat{T}} - \hat{T})) \cup (\hat{T}) \cap c'(\hat{\hat{T}} - \hat{T}) \subseteq T \cap c'(\hat{\hat{T}}) = \emptyset.$$

Therefore the shift of $\hat{\hat{T}} - \hat{T}$ in gate $g'|_{T-\hat{T}}$ to the preceding gate $g + g'|_{\hat{T}}$ is defined because $\hat{\hat{T}} - \hat{T} \neq \emptyset$. Analogously the shift of $\hat{T} - \hat{\hat{T}}$ in gate $g'|_{T-\hat{\hat{T}}}$ to the preceding gate $g + g'|_{\hat{T}}$ is defined because $\hat{T} - \hat{\hat{T}} \neq \emptyset$. The changed gates are:

$$(g + g'|_{\hat{T}}) + (g'|_{T-\hat{T}})|_{\hat{\hat{T}}} = g + g'|_{\hat{T} \cup \hat{\hat{T}}}, \qquad (g'|_{T-\hat{T}})|_{(T-\hat{T})-\hat{\hat{T}}} = g'|_{T-(\hat{T} \cup \hat{\hat{T}})},$$
$$(g + g'|_{\hat{\hat{T}}}) + (g'|_{T-\hat{\hat{T}}})|_{\hat{T}} = g + g'|_{\hat{T} \cup \hat{\hat{T}}}, \qquad (g'|_{T-\hat{\hat{T}}})|_{(T-\hat{\hat{T}})-\hat{T}} = g'|_{T-(\hat{T} \cup \hat{\hat{T}})}.$$

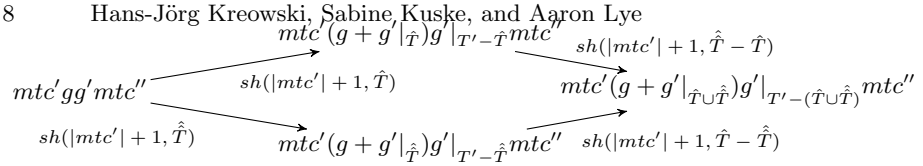
This proves that the two further shifts yield the same circuit.

Case 2: The situation is similar to Case 1 with the exception that $\hat{T} \subseteq \hat{\hat{T}}$ implies $\hat{T} - \hat{\hat{T}} = \emptyset$. But then the shift of $\hat{\hat{T}} - \hat{T}$ after the shift of $\hat{T}$ yields the same result as the shift of $\hat{\hat{T}}$ in the first place using arguments similar to Case 1.

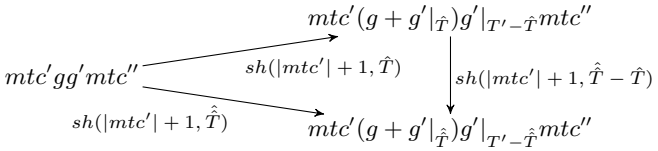
Case 3: Given a shift and a parallelization as in Fig. 3(c), the parallelization after the shift is defined and yields the same result as the parallelization directly using arguments similar to Case 1.

Cases 4-7: Now we consider two shifts changing three successive gates. Then both shifts may be parallelization or one is a parallelization and the other one a proper shift or both are proper shifts.

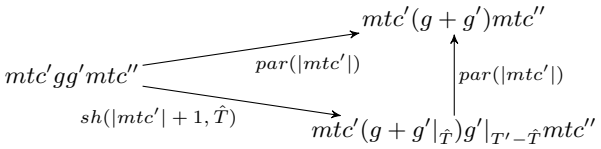
The argumentation that the given shifts can be continued by further shifts into the same result is in all four cases similar to the argumentation in Case 1. Nevertheless, we go into the details of Case 5 because, in this very case, two further shifts are applied after the given proper shift to keep up with the given parallelization. The circuit after the shift has the form $mtc'g(g' + g''|_{\hat{T}})g''|_{T''-\hat{T}}mtc''$ where the gate $|mtc'| + 2$ can be sequentialized wrt T' yielding the circuit $mtc'gg'g''|_{\hat{T}}g''|_{T''-\hat{T}}mtc''$. By assumption g and g' can be parallelized. Both together establish the shift of T' in gate $|mtc'| + 2$ yielding the circuit $mtc'(g + g')g''|_{\hat{T}}g''|_{T''-\hat{T}}mtc''$ where $g''|_{\hat{T}}g''|_{T''-\hat{T}}$ is a sequentialization of g'' so that the parallelization is defined yielding $mtc'(g+g')g''mtc''$ as stated. As there are no cases left, the local Church-Rosser property of shifts is proved.



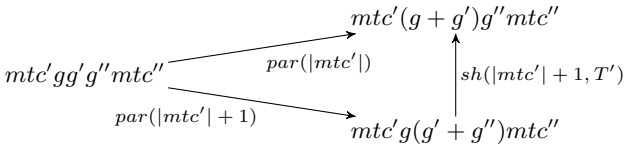
(a) Case 1



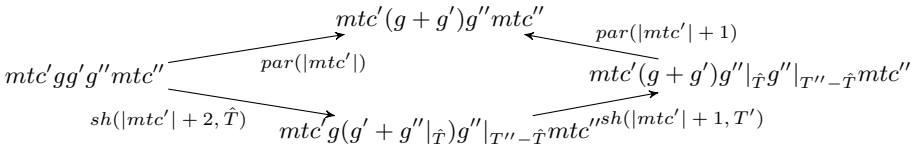
(b) Case 2



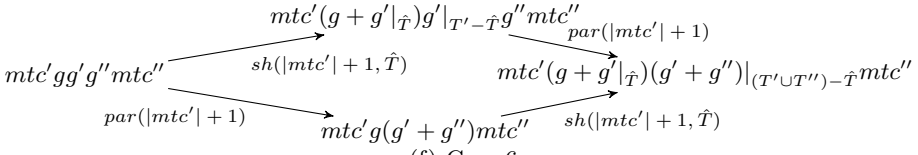
(c) Case 3



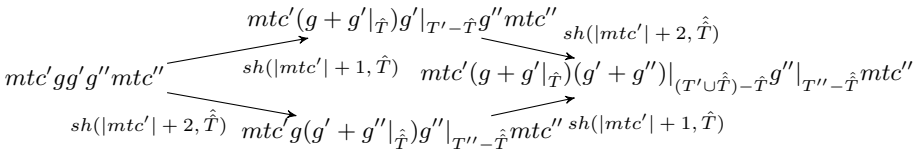
(d) Case 4



(e) Case 5



(f) Case 6



(g) Case 7

Fig. 3. The 7 cases of the shift relation

5 Waiting Degree

Besides the local Church-Rosser property, the shift operation has a second significant property: It does not allow infinite shift sequences. In other words, the lengths of shift sequences starting in some circuit are bounded. Consequently, shifting as long as possible always terminates in a circuit that is reduced with respect to shifting. To prove this, we introduce the waiting degree and show that it decreases with each shift. The waiting degree of a circuit sums up, for each target line, the number of gates that precede the gate of the target line.

Definition 9 (Waiting degree). Let $mtc = (T_1, c_1) \dots (T_n, c_n)$ be a multi-target Toffoli circuit. Then the *waiting degree* of mtc is

$$wait(mtc) = \sum_{j=1}^{n} (j-1) \cdot \#T_j$$

where $\#T_j$ denotes the number of elements of T_j.

Example 10. The waiting degree of the circuit in Fig. 2a is 10 and the waiting degree of the circuit in Fig. 2b is 4.

Proposition 11.

1. If $mtc \xrightarrow[par(i-1)]{} \widetilde{mtc}$, then $wait(\widetilde{mtc}) = wait(mtc) - \sum_{j=i+1}^{n} \#T_j$.
2. If $mtc \xrightarrow[seq(i+1,T')]{} \overline{mtc} \xrightarrow[par(i-1)]{} \widetilde{mtc}$, then $wait(\widetilde{mtc}) = wait(mtc) - \#T'$.

Proof. 1. In this case, $\widetilde{mtc} = (T_1, c_1) \dots (T_{i-1}, c_{i-1})(T_i + T_{i+1}, c)(T_{i+2}, c_{i+2}) \dots (T_n, c_n) = (\widetilde{T}_1, \widetilde{c}_1) \dots (\widetilde{T}_{n-1}, \widetilde{c}_{n-1})$ with $c(x) = c_i(x)$ for $x \in T_i$ and $c(x) = c_{i+1}(x)$ for $x \in T_{i+1}$. Therefore,

$$\begin{aligned}
wait(\widetilde{mtc}) &= \sum_{j=1}^{n-1} (j-1)\#\widetilde{T}_j \\
&= \left(\sum_{j=1}^{i-1} (j-1)\#\widetilde{T}_j \right) + (i-1)\#\widetilde{T}_i + \sum_{j=i+1}^{n-1} (j-1)\#\widetilde{T}_j \\
&= \left(\sum_{j=1}^{i-1} (j-1)\#T_j \right) + (i-1)\#(T_i + T_{i+1}) + \sum_{j=i+1}^{n-1} (j-1)\#T_{j+1} \\
&= \left(\sum_{j=1}^{i-1} (j-1)\#T_j \right) + (i-1)\#T_i + i\#T_{i+1} - \#T_{i+1} + \sum_{j=i+2}^{n} (j-2)\#T_j \\
&= \left(\sum_{j=1}^{i+1} (j-1)\#T_j \right) - \#T_{i+1} + \sum_{j=i+2}^{n} ((j-1)\#T_j - \#T_j) \\
&= \left(\sum_{j=1}^{n} (j-1)\#T_j \right) - \sum_{j=i+1}^{n} \#T_j = wait(mtc) - \sum_{j=i+1}^{n} \#T_j
\end{aligned}$$

2. The proof in this case is analogously.

Proposition 12. Let $mtc = (T_1, c_1) \dots (T_n, c_n)$ be a multi-target Toffoli circuit. Then $wait(mtc) \leq \frac{m(m-1)}{2}$ for $m = \sum_{j=1}^{n} \#T_j$.

Proof. Sequentialize mtc as long as possible. Then the result has length m and waiting degree $\frac{m(m-1)}{2}$. But $wait(mtc)$ is not greater because sequentialization increases the waiting degree.

The two properties imply the following corollary.

Corollary 13. 1. Let $mtc \xrightarrow[sh]{n} \overline{mtc}$ be a shift sequence of n shifts. Then $n \leq wait(mtc)$.
2. Let $mtc = (T_1, c_1) \dots (T_n, c_n)$ be a multi-target Toffoli circuit. Let $m = \sum_{i=1}^{n} \#T_i$. Then shifting as long as possible terminates with a circuit that is reduced wrt shifts after at most $\frac{m(m-1)}{2}$ shifts.

Let $\sim$ be the equivalence relation generated by the shift relation, called shift equivalence. Then $\sim$ is equal to $\sim_{seq} = \sim_{par}$ as $par \subseteq shift$ and $shift \subseteq par \cup par \circ seq \subseteq par \cup (par \circ par^{-1}) \subseteq (par \cup par^{-1})^* = \sim_{par}$.

6 Canonical Circuits

Circuits that are reduced wrt shifts are called canonical. They are local optima wrt the waiting degree. But this result can be tremendously improved by combining the termination with the local Church-Rosser property. The shifting defines an equivalence relation on circuits. Each equivalence class contains only circuits that are semantically equivalent. Moreover, it turns out that each canonical circuit is a unique representative of its shift equivalence class so that it is a global optimum within its class. To show this, we prove first that shift equivalence is confluent meaning that each two equivalent circuits can be shifted into a common circuit.

Theorem 14. Shift-equivalent canonical circuits are equal.

Proof. Let mtc and $\overline{mtc}$ be two shift-equivalent canonical circuits. Due to the following Lemma, there is a circuit $\widetilde{mtc}$ and there are shift sequences from mtc and $\overline{mtc}$ into $\widetilde{mtc}$. Because mtc and $\overline{mtc}$ are canonical and hence shift-reduced, both shift sequences have length 0 yielding $mtc = \widetilde{mtc} = \overline{mtc}$ as stated.

Lemma 15. $mtc \sim \overline{mtc}$ implies $\begin{array}{ccc} mtc & \xrightarrow{*} & \\ & \xrightarrow[sh]{sh\ *} & \widetilde{mtc} \\ \overline{mtc} & & \end{array}$ for some multi-target Toffoli circuit $\widetilde{mtc}$.

Proof. $mtc \sim \overline{mtc}$ iff there is a sequence $zz = mtc_0 \dots mtc_n$ such that $mtc_0 = mtc, mtc_n = \overline{mtc}, mtc_i \xrightarrow[sh]{} mtc_{i+1}$ or $mtc_{i+1} \xrightarrow[sh]{} mtc_i$ for all $i = 0, \dots, n-1$, i.e. a zigzag of shifts.

Let $MTC(zz) = \{mtc_i \mid i = 0, \ldots, n\}$ and let X be a finite set of multi-target Toffoli circuits. Let $reach(X) = \{\overline{mtc} \mid mtc \xrightarrow[sh]{*} \overline{mtc}, mtc \in X\}$. Note that $reach(X)$ is finite. Then, $mtc_i \xrightarrow[sh]{sh} \begin{matrix} mtc_{i-1} \\ mtc_{i+1} \end{matrix}$ is a critical pair of zz if $mtc_i \notin reach(MTC(zz) - \{mtc_i\})$, i.e. mtc_i is a critical element of zz.

Induction on $\#reach(CE(zz))$, where $CE(zz)$ denotes the set of critical elements of zz.

Base: $\#reach(CE(zz)) = 0$. Then there is no critical element because each critical element is reachable by itself by 0 shifts and belongs to $reach(CE(zz))$. Therefore, zz must contain a multi-target Toffoli circuit mtc_{i_0} with $mtc_i \xrightarrow[sh]{} mtc_{i+1}$ for all $i < i_0$ and $mtc_{i+1} \xrightarrow[sh]{} mtc_i$ for all $i \geq i_0$.

Step: Let $\#reach(CE(zz)) = k$ with $k > 0$. Let mtc_i be a critical element of zz i.e. $mtc_i \in CE(zz)$. Then one can replace $mtc_{i-1} \xleftarrow[sh]{} mtc_i \xrightarrow[sh]{} mtc_{i+1}$ in zz by the shifts that make the shift relation locally Church-Rosser due to Proposition 8 defining a new zz'. The new elements of zz' are not critical as none of them has branching shifts. Hence, $CE(zz') \subseteq MTC(zz) \subseteq reach(CE(zz))$. This implies $reach(CE(zz')) \subseteq reach(reach(CE(zz)) = reach(CE(zz))$. The inclusion is proper as $mtc_i \notin reach(CE(zz'))$ because of the following reason. Assuming $mtc_i \in reach(CE(zz'))$ then $mtc_j \xrightarrow[sh]{*} mtc_i$ for some $mtc_j \in CE(zz')$. As $mtc_j \in MTC(zz) - \{mtc_i\}$ we get $mtc_i \in reach(MTC(zz) - \{mtc_i\})$ in contradiction to the choice of mtc_i.

Therefore, $\#reach(CE(zz')) < k$ so that by induction hypothesis, the lemma holds for zz' and therefore for zz too.

7 Conclusion

In this paper, we have studied a generalized class of Toffoli circuits that are sequentially composed of multi-target Toffoli gates. Under certain independence conditions parts of a gate can be shifted to the preceding gate within a circuit. It has turned out that shift-reduced circuits are unique canonical representatives of their shift equivalence classes. To shed more light on the significance of these considerations, further research on the following topics may be helpful.

1. In the case considered in this paper, the negation on a target line takes place if and only if all control lines are 1. More generally, there may be two types of control lines where the lines of one type must be 1 as before, but the other lines must be 0 to trigger the negation (see e.g., [8]). We are confident that all the results in this paper still hold if one considers this more general kind of control with positive and negative control lines.
2. Canonical circuits have minimal waiting degree within their shift equivalence classes. But they may be the starting point for further optimizations. For example, it is clear that the sequential composition of a Toffoli gate with itself yields the identity. Therefore, two identical parts in successive multi-target Toffoli gates can be removed without changing the semantics. Afterwards another round of shift optimization can be started. And there are other operations with such a perspective.
3. Drechsler et al. [4] study exclusive sums of products (ESOPs) which are a special kind of Toffoli circuits where the target lines and the control lines

stem from disjoint sets. Therefore, the independence check for ESOPs concerns only the disjointness of target lines and shifting may become more efficient.
4. Chen et al. [2] and Wille et al. [10] study a special case of our multi-target Toffoli gates where all target lines have the same set of control lines. In both cases, the authors relate the special case with quantum circuits. Hence is may be interesting whether our more general case may yield further improvements in this line of research.
5. As mentioned in the introduction, shifts on parallel graph grammar derivations behave like the shifts on multi-target Toffoli circuits (see, e.g., [5, 3]). Therefore, we wonder whether there is a way to represent Toffoli circuits as parallel derivations.

References

1. Bennett, C.: Logical reversibility of computation. IBM Journal of Research and Development 17(6), 525–532 (1973)
2. Chen, J.-L., Zhang, X.-Y., Wang, L.-L., Wei, X.-Y., Zhao, W.-Q.: Extended Toffoli gate implementation with photons. In: Proceeding of the 9th International Conference on Solid-State and Integrated-Circuit Technology. pp. 575–578. ICSICT (2008)
3. Corradini, A., Montanari, U., Rossi, F., Ehrig, H., Heckel, R., Löwe, M.: Algebraic approaches to graph transformation part I: Basic concepts and double pushout approach. In: Rozenberg, G. (ed.) Handbook of Graph Grammars and Computing by Graph Transformation, Vol. 1: Foundations, pp. 163–245. World Scientific, Singapore (1997)
4. Drechsler, R., Finder, A., Wille., R.: Improving ESOP-based synthesis of reversible logic using evolutionary algorithms. In: Applications of Evolutionary Computation - EvoApplications 2011: EvoCOMNET, EvoFIN, EvoHOT, EvoMUSART, EvoSTIM, and EvoTRANSLOG, Proceedings, Part II. Lecture Notes in Computer Science, vol. 6625, pp. 151–161. Springer (2011)
5. Kreowski, H.-J.: Transformation of derivation sequences in graph grammars. In: Proc. Conference Fundamentals of Computation Theory (Poznan-Kornik, Sept. 1977). Lecture Notes in Computer Science, vol. 56, pp. 275–286. Springer (1977)
6. Kreowski, H.-J.: Manipulationen von Graphmanipulationen. Ph.D. thesis, Technische Universität Berlin (1978), Fachbereich Informatik
7. Kreowski, H.-J.: An axiomatic approach to canonical derivations. In: Proc. IFIP World Computer Congress. IFIP-Transactions, vol. A-51, pp. 348–353. North-Holland (1994)
8. Soeken, M., Thomsen, M. K.: White dots do matter: Rewriting reversible logic circuits. In: Proceedings of the 5th International Conference on Reversible Computation. pp. 196–208. RC'13, Springer-Verlag, Berlin, Heidelberg (2013)
9. Toffoli, T.: Reversible computing. In: de Bakker, W., van Leeuwen, J. (eds.) Automata, Languages and Programming, Lecture Notes in Computer Science, vol. 85, pp. 632–644. Springer (1980)
10. Wille, R., Soeken, M., Otterstedt, C., Drechsler, R.: Improving the mapping of reversible circuits to quantum circuits using multiple target lines. In: Asia and South Pacific Design Automation Conference (ASP-DAC). pp. 145–150. IEEE (2013)