A framework for reversible circuit complexity

Mathias Soeken[1,2] Nabila Abdessaied[2] Rolf Drechsler[1,2]
[1] Faculty of Mathematics and Computer Science, University of Bremen, Germany
[2] Cyber-Physical Systems, DFKI GmbH, Bremen, Germany
{msoeken,nabila,drechsle}@informatik.uni-bremen.de

Abstract

Reversible single-target gates are a generalization of Toffoli gates which are a helpful formal representation for the description of synthesis algorithms but are too general for an actual implementation based on some technology. There is an exponential lower bound on the number of Toffoli gates required to implement any reversible function, however, there is also a linear upper bound on the number of single-target gates which can be proven using a constructive proof based on a former presented synthesis algorithm. Since single-target gates can be mapped to a cascade of Toffoli gates, this synthesis algorithm provides an interesting framework for reversible circuit complexity. The paper motivates this framework and illustrates first possible applications based on it.

1 Introduction

In this paper we concern ourselves with a special class of Boolean multiple-output functions called *reversible functions* which are those functions $f : \mathbb{B}^n \to \mathbb{B}^m$ that are bijective, i.e. there exists a 1-to-1 mapping from the inputs to the outputs. Clearly, if f is reversible, then $n = m$. Boolean multiple-output functions that are not reversible are called irreversible. Reversible functions can be implemented in terms of reversible circuits. Reversible functions and circuits play an important role in quantum computation [3] and low-power computing [4].

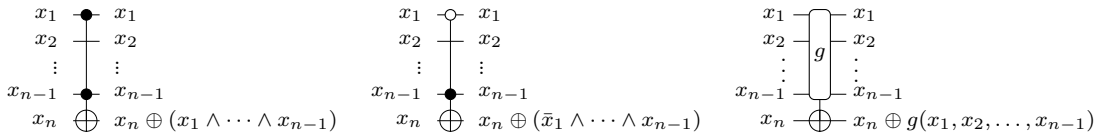
A lot of research has been investigating the complexity of Boolean functions and Boolean circuits in the past [12, 11], however, no thorough considerations have been made for reversible functions and circuits so far. Recently the complexity of synthesis [2] and equivalence checking [7] have individually been investigated. Based on two bounds for the number of gates in reversible circuits, in this paper we propose a general framework that is helpful for the analysis of reversible circuit complexity. The first bound is a linear upper bound with respect to single-target gates [6], the second one is an exponential lower bound with respect to Toffoli gates [8]. Single-target gates are convenient to be used as a model for analysis of reversible functions as well as for the description of synthesis algorithms [6, 1], whereas Toffoli gates have been used in practical implementations [5]. Single-target gates can be mapped to a cascade of Toffoli gates using exclusive sum-of-products (ESOP) mapping.

The paper is structured as follows. We first review ESOP mapping and reversible circuits. Afterwards, we prove the two bounds that are discussed above. Section 5 describes the framework for complexity analysis and Sect. 6 illustrates an application based on the framework for a better than optimal embedding strategy. The paper concludes in Sect. 7.

2 Notation and Definitions

2.1 Boolean Functions

Let $\mathbb{B} \stackrel{\text{def}}{=} \{0, 1\}$ denote the *Boolean values*. Then we refer to $\mathcal{B}_{n,m} \stackrel{\text{def}}{=} \{f \mid f \colon \mathbb{B}^n \to \mathbb{B}^m\}$ 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 $\mathcal{B}_n \stackrel{\text{def}}{=} \mathcal{B}_{n,1}$ 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 $\vec{x} \in \mathbb{B}^n$.



(a) MCT gate (b) MPMCT gate (c) Single target gate

Figure 1: Reversible gates

2.2 Exclusive Sum of Products

Exclusive sum-of-products (ESOPs, [9]) are two-level descriptions for Boolean functions in which a function is composed of k *product terms* that are combined using the exclusive-OR (EXOR, $\oplus$) operation. A product term is the conjunction of l_i literals 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:

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

Several restricted subclasses have been considered in the past, e.g. *positive polarity Reed-Muller expressions* (PPRM [9]), in which all literals are positive. There are further subclasses and most of them can be defined based on applying the following decomposition rules. An arbitrary Boolean function $f(x_1, x_2, \ldots, x_n)$ can be expanded as

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

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

Reversible functions can be realized by reversible circuits that consist of at least n lines and are constructed as cascades of reversible gates that belong to a certain gate library. The most common gate library consists of Toffoli gates or single-target gates.

Definition 1 (Reversible single-target gate)**.** *Given a set of variables $X = \{x_1, \ldots, x_n\}$, a* reversible single-target gate $\mathrm{T}_g(C, t)$ *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 $g \in \mathcal{B}_k$ *inverts the variable on the target line, if and only if $g(x_{i_1}, \ldots, x_{i_k})$ evaluates to true. All other variables remain unchanged. If the definition of g is obvious from the context, it can be omitted from the notation T_g.*

Definition 2 (Toffoli gate)**.** Mixed-polarity multiple-control Toffoli (MPMCT) gates *are a subset of the single-target gates in which the control function g can be represented with one product term or $g = \bigwedge_{k=i}^{j} x_i^p = 1$.* Multiple-control Toffoli gates (MCT) *in turn are a subset from MPMCT gates in which the product terms can only consist of positive literals.*

Using synthesis algorithms it can easily been shown that any reversible function $f \in \mathcal{B}_{n,n}$ can be realized by a reversible circuit with n lines when using MCT gates. That is, it is not necessary to add any temporary lines (ancilla) to realize the circuit. This can be the case if the MCT (or MPMCT) gates are restricted to a given size, e.g. three bits. Note that 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 [9], respectively. For drawing circuits, we follow the established conventions of using the symbol $\oplus$ to denote the target line, solid black circles to indicate positive controls and white circles to indicate negated controls.

Example 1. *Figure 1a shows a Toffoli gate with n positive controls, Fig. 1b shows a Toffoli gate with mixed polarity control lines, and Fig. 1c shows the diagrammatic representation of a*

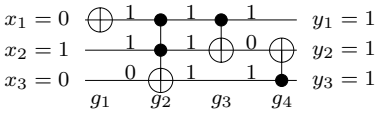


Figure 2: Reversible circuit

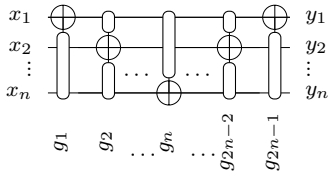


Figure 3: Synthesis based on Young subgroups

single-target gate based on Feynman's notation. Fig. 2 shows different Toffoli gates in a cascade forming a reversible circuit. The annotated values demonstrate the computation of the gate for a given input assignment.

3 Upper bound for Single-Target Gate Circuits

Theorem 1. *Let $f \in \mathcal{B}_{n,n}$ be reversible and x a variable in f. Then, f can be decomposed as $f = g_2 \circ f' \circ g_1$ into three functions $g_1, f', g_2 \in \mathcal{B}_{n,n}$ such that f' is a reversible function that does not change x, and g_1 and g_2 can each be realized as a single-target gate that acts on x.*

Proof. Reversible functions of n variables are isomorphic to the symmetric group S_{2^n}. Consequently, f corresponds to an element $a \in S_{2^n}$. The element a can be decomposed as $a = h_2 v h_1$, where both h_1 and h_2 are members of the Young subgroup $S^2_{2^{n-1}}$ and v is a member of $S_2^{2^{n-1}}$ [10]. From h_1, h_2, and v one can derive g_1, g_2, and f' [6]. □

Corollary 1. *Each reversible function $f \in \mathcal{B}_{n,n}$ can be implemented as a reversible circuit with at most $2n - 1$ single-target gates.*

Proof. When applying Theorem 1 to all variables in an iterative manner, f' will be the identity function after at most n steps and at most $2n$ gates have been collected. Since f' is the identity function in the last step, the last two gates can be combined into one single-target gate. □

A truth table based algorithm that makes use of the results of Theorem 1 and Corollary 1 has been presented in [6]. Since the variables are selected in a decreasing order, the target lines of the resulting single-target gates are aligned on a V-shape (cf. Fig. 3).

4 Lower Bound for Toffoli Gate Circuits

Reversible circuits with n inputs that consist of only one MCT gate can represent $n \cdot 2^{n-1}$ reversible functions. There are n possible positions to fix the target line and then $n-1$ positions remain to either put or not put a control line. If one has two Toffoli gates one can represent at most $(n \cdot 2^{n-1})(n \cdot 2^{n-1})$ functions. The actual number is smaller, since for some circuits the order of gates does not matter or both gates are equal which corresponds to the empty circuit. In general, one can represent at most $(n \cdot 2^{n-1})^k$ reversible functions with a circuit that consists of k Toffoli gates. Since there are $2^n!$ reversible functions one can derive that there is at least one function that requires

$$\left\lceil \frac{\log(2^n!)}{\log(n2^{n-1})} \right\rceil \tag{2}$$

gates.

Theorem 2. *There exist a reversible function which smallest circuit realization requires an exponential number of Toffoli gates.*

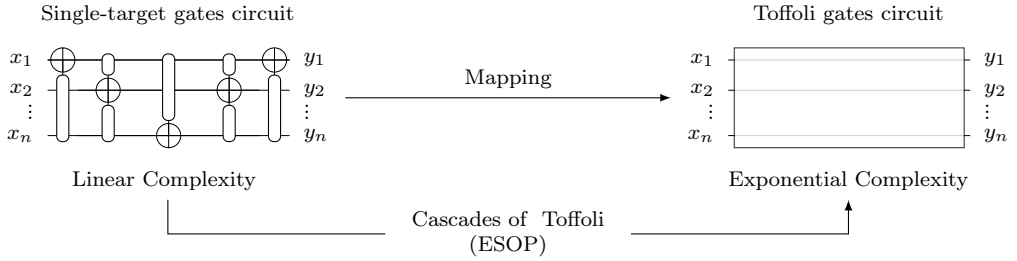


Figure 4: Reversible circuit complexity

Proof. We show that there exist a constant c such that $\left\lceil \frac{\log(2^n!)}{\log(n2^{n-1})} \right\rceil \geq c \cdot 2^n$. We have

$$\left\lceil \frac{\log(2^n!)}{\log(n2^{n-1})} \right\rceil \geq \frac{\log(2^n!)}{\log(n2^{n-1})} = \frac{\log_2(2^n!)}{\log_2(n2^{n-1})} \geq c \cdot 2^n$$

which can be rewritten to

$$\log_2(2^n!) \geq c \cdot 2^n \log_2(n2^{n-1}) = c \cdot 2^n \left(\log_2 n + (n-1)\right).$$

Since $(\log_2 n + (n-1)) < 2n$ we are left to prove that $\log_2(2^n!) \geq c_0 \cdot 2^n n$ for some constant c_0, which we do using induction on n. From the base case we obtain $c_0 = \frac{1}{2}$. Assume for some n we have $\log_2(2^n!) \geq \frac{1}{2} \cdot 2^n n$, then in the induction step we get

$$\log_2(2^{n+1}!) = \sum_{k=1}^{2^{n+1}} \log_2 k = \sum_{k=1}^{2^n} \log_2 k + \sum_{k=1}^{2^n} \log_2(k+2^n) = \log_2(2^n!) + \sum_{k=1}^{2^n} \log_2(k+2^n). \quad (3)$$

We will now derive a lower bound for the second term in the last expression of (3). We have

$$\sum_{k=1}^{2^n} \left(\log_2(k+2^n) - \log_2 k\right) = \sum_{k=1}^{2^n} \log_2 \frac{k+2^n}{k} = \sum_{k=1}^{2^n} \log_2 \left(1 + \frac{2^n}{k}\right) \geq \sum_{k=1}^{2^n} 1 = 2^n$$

from which we derive

$$\sum_{k=1}^{2^n} \log_2(k+2^n) \geq \sum_{k=1}^{2^n} \log_2 k + 2^n = \log_2(2^n!) + 2^n.$$

Plugging this into (3) we get

$$\log_2(2^{n+1}!) \geq \log_2(2^n!) + \log_2(2^n!) + 2^n \geq 2 \cdot \left(\frac{1}{2} \cdot 2^n n\right) + 2^n = \frac{1}{2} \cdot 2^{n+1}(n+1). \qquad \square$$

The proof for Theorem 2 in [8] uses mEXOR gates as underlying gate library, which generalize MCT gates to have more than one target line. The proof can be carried out analogously for MPMCT gates.

5 Framework for Circuit Complexity Analysis

Both bounds that have been presented in the previous section are used to motivate a framework for reversible circuit complexity analysis that is illustrated in Fig. 4. If only considering single-target gates, one knows that at most linear many gates are required. When being restricted to Toffoli gates, there are functions that need at least an exponential number of gates. Since single-target gates can be translated to cascades of Toffoli gates, there must be control functions which require exponential many product terms when being decomposed into ESOP expressions.

However, when restricting the ESOP mapping interesting cases arise. Let us first consider that we only allow single-target target gates which control function can be mapped to ESOP expressions that have a constant number of product terms, e.g. 1 or 2. Then the resulting Toffoli

circuits are of linear size. The most interesting and important question is how to determine which class of reversible functions can be represented using these circuits when applying this restriction. We experienced this to be a difficult research problem in our investigations on this topic. The same idea can be extended to other cases. If e.g. we allow those single-target gates which control functions can be mapped to linear size ESOP expressions, one obtains Toffoli circuits of quadratic size.

6 Application: "Better than Optimal" Embedding

In this section we consider half of the V-shaped circuit that has been considered in the previous section. That is, we consider reversible circuits with n variables and n single-target gates that have their target lines in subsequent order from the top line to the bottom line. Also, no two single-target gates have the target line in common. It can easily be seen that at most $\left(2^{2^{n-1}}\right)^n$ different reversible functions can be realized with such circuits.

We will now show that in fact exactly $\left(2^{2^{n-1}}\right)^n$ different functions can be realized, which implies that these circuits are a canonical representation for this subset of reversible functions.

Lemma 1. *Reversible circuits with $k \geq n$ lines that have n single-target gates with pairwise different target lines in increasing order on lines 1 to n can realize exactly $\left(2^{2^{k-1}}\right)^n$ reversible functions.*

Proof. We prove this using induction on n. The base case is simple since each single-target gate realizes a different function and since the target line is fixed on the first line, there are $2^{2^{k-1}}$ possibilities to choose the control function. Assuming the claim holds for all circuits with up to n gates, we consider a circuit that has $n+1$ gates. The subcircuit C' consisting of the first n gates realizes $\left(2^{2^{k-1}}\right)^n$ functions due to the induction hypothesis. Since the $(n+1)th$ gate has its target line on a line that has not been used as target line in C' and since there are no two gates that realize the same function, the statement follows. □

Corollary 2. *Reversible circuits with n lines that have n single-target gates with their targets being on increasing lines (from the top to the bottom) can realize exactly $\left(2^{2^{n-1}}\right)^n$ reversible functions.*

There are also $\left(2^{2^{n-1}}\right)^n$ Boolean multiple-output functions in $\mathcal{B}_{n-1,n}$. When realizing these functions as reversible circuits one needs to embed them first into reversible functions, which will have up to $2n-1$ variables. The additional variables are required to ensure that the function is bijective. However, since there is a 1-to-1 correspondence between the number of half V-shaped circuits on n lines and the number of functions in $\mathcal{B}_{n-1,n}$, a "better than optimal" embedding is possible because in the conventional case there are functions that require at least $2n-1$ lines (e.g. the constant functions). One only needs to define a mapping function from the multiple-output function to the reversible one as well as an interpretation function for the computed outputs. Based on Lemma 1 this embedding technique can be extended to functions in $\mathcal{B}_{k-1,n}$ with $k \geq n$.

7 Conclusions

We have motivated a framework for the analysis of complexity of reversible circuits based on two bounds. As one first application of this framework we have presented an idea for a better than optimal embedding. The research in this area is still in its infancy so far, however, the discussions started in this paper provide a starting point to tackle the open problems. One direction for future work is to find a way to derive function classes from a subset of reversible circuits. It is also open whether these will be function classes known from the literature or whether new ones for the special case of reversible functions need to be defined.

Acknowledgments. We thank Eugenia Rosu for her help with the proof to Theorem 2. We also thank Amatulwaseh Hayat for many interesting discussions.

References

[1] N. Abdessaied, M. Soeken, M. K. Thomsen, R. Drechsler: Upper bounds for reversible circuits based on Young subgroups, in: *Information Processing Letters* **114**, 2014, 282–286.

[2] A. Chattopadhyay, C. Chandak, and K. Chakraborty: Complexity analysis of reversible logic synthesis, in: *arXiv:1402.0491*, 2014.

[3] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter: Elementary gates for quantum computation, in: *Physical Review A* **52**, 1995, 3457.

[4] A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, E. Lutz: Experimental verification of Landauer's principle linking information and thermodynamics, in: *Nature* **483**, 2012, 187–189.

[5] B. Desoete, A. De Vos: A reversible carry-look-ahead adder using control gates, in: *INTEGRATION* **33**, 2002, 89–104.

[6] A. De Vos, Y. Van Rentergem: Young subgroups for reversible computers, in: *Advances in Mathematics of Communications* **2**, 2008, 183–200.

[7] S. P. Jordan: Strong equivalence of reversible circuits is coNP-complete, in: *arXiv:1307.0836*, 2013.

[8] D. Maslov, G. W. Dueck, D. M. Miller: Toffoli network synthesis with templates, in: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **24**, 2005, 807–817.

[9] T. Sasao: AND-EXOR expressions and their optimization, in: T. Sasao (Ed.) *Logic Synthesis and Optimization*, Kluwer Academic Publisher, 1993, 287–312.

[10] Y. Van Rentergem, A. De Vos, L. Storme: Implementing an arbitrary reversible logic gate, in: *Journal of Physics A: Mathematical and General* **38**, 2005, 3555–3577.

[11] H. Vollmer: *Introduction to Circuit Complexity: A Uniform Approach*, Springer, 1999.

[12] I. Wegener: *The complexity of Boolean functions*, Wiley-Teubner, 1987.