Information Processing Letters 114 (2014) 282–286

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Upper bounds for reversible circuits based on Young subgroups

Nabila Abdessaied [a,b,*], Mathias Soeken [a,b], Michael Kirkedal Thomsen [a,c], Rolf Drechsler [a,b]

[a] Institute of Computer Science, University of Bremen, Germany
[b] Cyber-Physical Systems, DFKI GmbH, Bremen, Germany
[c] DIKU, Department of Computer Science, University of Copenhagen, Denmark

ARTICLE INFO

Article history:
Received 16 August 2013
Received in revised form 3 January 2014
Accepted 7 January 2014
Available online 20 January 2014
Communicated by J. Torán

Keywords:
Combinatorial problems
Reversible functions
Upper bounds
Synthesis

ABSTRACT

We present tighter upper bounds on the number of Toffoli gates needed in reversible circuits. Both multiple controlled Toffoli gates and mixed polarity Toffoli gates have been considered for this purpose. The calculation of the bounds is based on a synthesis approach based on Young subgroups that results in circuits using a more generalized gate library. Starting from an upper bound for this library we derive new bounds which improve the existing bound by around 77%.

1. Introduction

Reversible computation [1] has proven itself as a very promising research area, especially for applications to emerging technologies. This can be seen 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].

The branch of reversible computations that is most applicable to these areas is the reversible logic models. Here, especially synthesis of reversible logic has become an intensively studied topic and several approaches have been proposed [6–8].

To compare the efficiency of different synthesis approaches it is important to evaluate the resulting circuits. Depending on the target application, different metrics are applied to measure the complexity of a given circuit. Among these metrics we find the number of gates and the gate delay (depth). But also important is the number of elementary quantum gates and the number of lines (width) that describes the number of lines used for temporary computations (called *ancilla* lines). For more details the reader is referred to [9].

In this paper we investigate upper bounds to the number of gates that in general are needed to implement reversible circuits. This is important as a first-approach to understand the complexity of reversible circuits, but, as mentioned, 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 restricted gate library [10,11].

Our work is both an improvement over previous reported upper bounds and an extension of the upper bound to a more general gate library. The improvement shows by combining a synthesis method based on Young subgroups [7] with decomposition of exclusive sum-of-products (ESOP) expressions into the different gate libraries [12,13].

* Corresponding author.

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2014.01.003

2. Background

2.1. Exclusive sum-of-products

Exclusive sum-of-products (ESOPs, [14])

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

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.

Each n-variable function has an infinite number of ESOP representations [14]. As a result, many heuristic minimization approaches have been proposed (e.g. [15,16]) to find the ESOP expression with a small number of product terms. Also, exact ESOP minimization algorithms have been developed (e.g. [17]), which are able to find the ESOP expression with fewest product terms. However, they require a large computation time and are therefore only applicable to relatively small functions.

Several restricted subclasses have been considered in the past, e.g. *positive polarity Reed–Muller expressions* (PPRM [14]), in which all literals are positive, or *fixed polarity Reed–Muller expressions* (FPRMs, [14]), in which each variable must have the same polarity in all product terms. 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 $f_{x_i} = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$.

2.2. Reversible binary functions and circuits

We call a logic function $f : \mathbb{B}^n \to \mathbb{B}^n$ over n bits *reversible*, if it is bijective, i.e. there exists a 1-to-1 mapping from the inputs to the outputs. 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.

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* $g : \mathbb{B}^k \to \mathbb{B}$ 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.

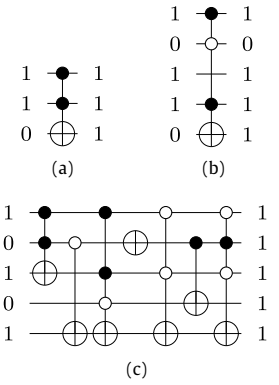

Fig. 1. Reversible circuitry.

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 $g = 1$. *Multiple-control Toffoli gates* (*MCT*) in turn are a subset from MPMCT gates in which the product terms can only consist of positive literals.

In [18], it has been shown that any reversible function $f : \mathbb{B}^n \to \mathbb{B}^n$ 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 [14], 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 negative controls.

Example 1. Fig. 1(a) shows an MCT gate with two positive control lines, while Fig. 1(b) shows an MPMCT gate with mixed polarity control lines. The annotated values demonstrate the computation of the gate for a given input assignment. Fig. 1(c) shows different MPMCT gates in a cascade forming a reversible circuit.

3. General idea

3.1. Existing upper bounds for reversible circuits

Motivated by the fact that upper bounds play a significant role in evaluating the complexity of synthesized reversible circuits, many methods for obtaining the upper bounds for given functions have already been studied. In [10], it has been proven that every reversible function over n variables can be realized with no more than

$$n \cdot 2^n \tag{2}$$

MCT gates. This upper bound was obtained from transformation-based synthesis approaches as initially presented in [19]. The algorithm traverses each of the 2^n rows of the

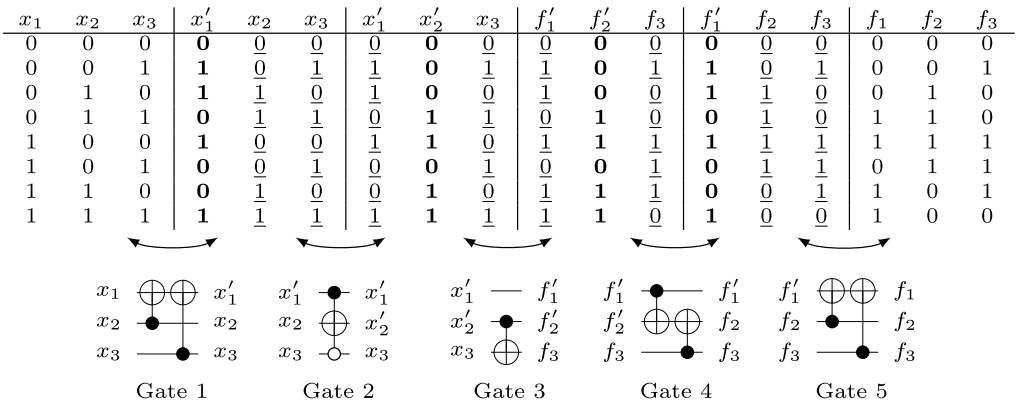

Fig. 2. Synthesis based on Young subgroups.

truth table representation of a function and for each row adds at most one gate per column (i.e. variable).

In [18] an algorithm for the synthesis of optimal circuits based on Toffoli gates with at most two positive control lines has been described. The proposed approach leads to at most

$$n + n^2 + 3\big(2^n + n + 1\big)(3n - 7) \tag{3}$$

gates, with the first, second, and third term referring to the number of NOT, CNOT, and Toffoli gates, respectively. Note that the upper bound only applies to this restricted gate library. Furthermore, many studies have focused on the upper bound of the number of elementary quantum gates in reversible circuits [10,11]. These upper bounds are specific to the special domain of quantum computing, however, reversible logic serves as basis to many other fields as well. To the best of our knowledge, no works thus far have been studying the upper bound on the number of MPMCT gates in reversible circuits and compared them to upper bounds for MCT circuits. However, due to the incorporation of negative control lines in recent synthesis (e.g. [8]) and optimization approaches (e.g. [20]) this consideration becomes important.

3.2. Synthesis based on Young subgroups

We present tighter upper bounds on the maximum number of gates, both for the MCT and MPMCT gate library based on a synthesis algorithm presented in [7]. Applying the algorithm to a reversible function $f(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ leads to circuit with

$$2n - 1 \tag{4}$$

single-target gates.

For this purpose, the algorithm performs the following step for each variable x_j. One single-target gate for the inputs and one single-target gate for the outputs are determined such that applying them to the function leads to a new function which does not change in x_j any longer. These single-target gates can be found by first copying all other variables into a new truth table followed by reassigning x_j and y_j with new values such that they are equal by still ensuring the reversibility of the truth table. If the columns are chosen in ascending order from x_1 to x_n, the targets form a V-shape. A more detailed description of the algorithm can be found in [7].

Example 2. Fig. 2 shows an example application of the synthesis algorithm. First, the columns x_2, x_3 and f_2, f_3 are copied to the second and fifth block of the extended truth table, respectively (the values are underlined). Afterwards, the columns x'_1 and f'_1 are filled in a way such that they have the same values column-wise by still ensuring reversibility. This is e.g. done by filling x'_1 with a 0 in the first row. To ensure reversibility in the fifth row a 1 is inserted since x_2 and x_3 have the same value. After that, the same value of x'_1 is copied as a value to f'_1 in the same row. Again, to ensure reversibility f'_1 is assigned 0 in row 6. This process is repeated until all values of x'_1 and f'_1 have been assigned. Afterwards, the same step is performed for the second column on both sides of the extended truth table. Note that afterwards both middle blocks are equal except for the last column. After the extended truth table has been filled the control functions for the gates can be read. As an example, the first column in the second block changes whenever $\bar{x}_2 x_3$ or $x_2 \bar{x}_3$ holds, hence the control function is $x_2 \oplus x_3$.

Since each reversible function of n variables can be realized as a circuit consisting of $2n - 1$ single-target gates, any Toffoli circuit can be synthesized in $(2n - 1) \cdot u(n)$, where $u(n)$ is the largest number of Toffoli gates required to represent a single-target gate. In the following sections, we describe different techniques to obtain $u(n)$ with respect to the MCT and MPMCT gate libraries.

4. Upper bound based on function decomposition

First, we present a method to obtain upper bounds based on exact synthesis techniques [12,13] which guarantee a minimal circuit representation combined with function decomposition.

Theorem 1. *An n-bit single-target gate can be realized with at most* $u(n) = 3 \cdot 2^{n-3} - 2$ *MCT gates, if* $n \geqslant 5$.

Table 1
Summary of upper bounds for representing one single-target gate and to represent a reversible function.

Method	Single target gate		Reversible circuit	
	MCT	MPMCT	MCT	MPMCT
Decomposition	$3 \cdot 2^{n-3} - 2$	$3 \cdot 2^{n-4}$	$3n2^{n-2} - 4n - 3 \cdot 2^{n-3} + 2$	$3n2^{n-3} - 3 \cdot 2^{n-4}$
ESOP expressions	2^{n-1}	$29 \cdot 2^{n-8}$	$n2^n - 2^{n-1}$	$29n2^{n-7} - 29 \cdot 2^{n-8}$
Existing bound	$\frac{n2^n}{2n-1}$	N/A	$n2^n$	N/A

Table 2
Upper bounds on number of gates.

Upper bound	Number of variables									Average improvement
	2	3	4	5	6	7	8	9	10	
Existing	8	24	64	160	384	896	2048	4608	10 240	
ESOP (MCT)	6	20	56	144	352	832	1920	4352	9728	11%
Decomposition (MCT)	6	20	42	90	242	598	1410	3230	7258	31%
Decomposition (MPMCT)	3	10	21	54	132	312	720	1632	3648	64%
ESOP (MPMCT)	3	10	21	54	99	208	435	986	2204	71%

Proof. 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 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 [12]. The largest circuit required $10 = 3 \cdot 2^{5-3} - 2$ MCT gates.

For the induction step, we assume that the result holds for n variables and consider a single-target gate using $n+1$ lines. By applying the Shannon decomposition the control gate can be decomposed into two n-bit single-target gates and two NOT gates (see Fig. 3). According to the inductive hypothesis, the single-target gates in that circuit can be realized with at most $3 \cdot 2^{n-3} - 2$ gates. Hence, the single-target gate on $n+1$ lines requires

$$2 \cdot \left(3 \cdot 2^{n-3} - 2\right) + 2 = 3 \cdot 2^{(n+1)-3} - 2$$

gates. □

Theorem 2. *An n-bit single-target gate can be realized with at most $u(n) = 3 \cdot 2^{n-4}$ MPMCT gates, if $n \geqslant 5$.*

Proof. We use the same proof as for Theorem 1. In the base case we used an exact synthesis approach that also considers negative control lines [13] and obtained $6 = 3 \cdot 2^{5-4}$ gates for the largest minimal circuit.

In the induction step we used the Shannon decomposition but the circuit construction without the additional two NOT gates (see Fig. 3) resulting in

$$2 \cdot \left(3 \cdot 2^{n-4}\right) = 3 \cdot 2^{(n+1)-4}$$

gates. □

5. Upper bound based on ESOP expressions

Tighter upper bounds for reversible circuits can also be obtained by combining the synthesis approach outlined in Section 3.2 using upper bounds for the size of ESOP expressions.

Theorem 3. *An n-bit single-target gate can be realized with at most $u(n) = 2^{n-1}$ MCT gates.*

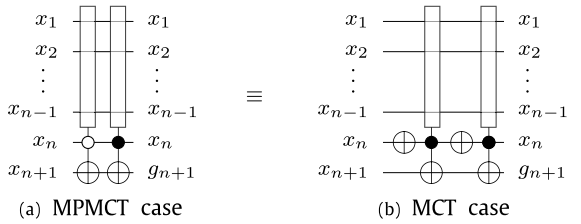

Fig. 3. Single-target gate decomposition.

Proof. 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 $g : \mathbb{B}^{n-1} \to \mathbb{B}$ which PPRM expression consists of all 2^{n-1} product terms. □

Theorem 4. *An n-bit single-target gate can be realized with at most $u(n) = 29 \cdot 2^{n-8}$ MPMCT gates, if $n \geqslant 8$.*

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

$$29 \cdot 2^{n-7} \quad \text{with } n \geqslant 7. \tag{5}$$

This upper bound was presented in [21]. Hence, the ESOP expression of the control function $g : \mathbb{B}^{n-1} \to \mathbb{B}$ consists of at most $29 \cdot 2^{n-8}$ product terms. □

6. Summary and conclusions

Table 1 summarizes the shown tighter upper bounds to represent a single-target gate using Toffoli gates in the MCT and MPMCT gate libraries in the second and third column. One obtains the upper bound for the number of gates in a reversible circuit by multiplying each number by $(2n-1)$. The resulting values are shown in the fourth and fifth column.

To get a better intuition how the new bounds compare to the existing one, we listed their absolute values for up to 10 variables in Table 2. The first row gives the number of lines in the reversible circuits. In the following rows,

the obtained results for the existing upper bound and the proposed upper bounds are presented. For the proposed approaches the average improvement compared to the existing upper bound is given in the last column.

The upper bound for the MCT gates obtained by function decomposition shows better improvements compared to the MCT gate upper bound derived using ESOP minimization. Exploiting the exact synthesis approach in the calculation of the MCT upper bound enables further improvements, which reach 31% on average.

On the other hand, results clearly confirm that the ESOP minimization based upper bound on the number of MPMCT gates is better than the upper bound obtained by the approach using function decomposition. By applying the ESOP based upper bound, an improvement of 71% on average compared to the best known upper bound can be obtained. Furthermore, this is an additional improvement of 31% compared to the best MCT gates upper bound.

For the best upper bound, the overall improvement (with no restriction on the number of variables) is

$$1 - \frac{(2n-1)\cdot 29\cdot 2^{n-8}}{n2^n} = 1 - \frac{29}{128} + \frac{29}{n2^8} > 1 - \frac{29}{128} \approx 77\%. \tag{6}$$

The overall improvement can be calculated in the same way for the remaining bounds as well.

Acknowledgement

This work was partly funded by the European Commission under the *7th Framework Programme* and by the Danish Council for Strategic Research in the framework of the *MicroPower* research project.

References

[1] A. De Vos, Reversible Computing: Fundamentals, Quantum Computing and Applications, Wiley, 2010.
[2] E. Knill, R. Laflamme, G.J. Milburn, A scheme for efficient quantum computation with linear optics, Nature 409 (1) (2001) 46–52.
[3] J. Ren, V.K. Semenov, Y.A. Polyakov, D.V. Averin, J.S. Tsai, Progress towards reversible computing with nSQUID arrays, IEEE Trans. Appl. Supercond. 19 (3) (2009) 961–967.
[4] S. Houri, A. Valentian, H. Fanet, Comparing CMOS-based and NEMS-based adiabatic logic circuits, in: Reversible Computation, in: Lect. Notes Comput. Sci., vol. 7948, 2013, pp. 36–45.
[5] W.C. Athas, L.J. Svensson, Reversible logic issues in adiabatic CMOS, in: Workshop on Physics and Computation, 1994, pp. 111–118.
[6] P. Gupta, A. Agrawal, N.K. Jha, An algorithm for synthesis of reversible logic circuits, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 25 (11) (2006) 2317–2330.
[7] A. De Vos, Y. Van Rentergem, Young subgroups for reversible computers, Adv. Math. Commun. 2 (2) (2008) 183–200.
[8] M. Soeken, R. Wille, C. Hilken, N. Przigoda, R. Drechsler, Synthesis of reversible circuits with minimal lines for large functions, in: Asian South-Pacific Design Automation Conference, 2012, pp. 59–70.
[9] M. Mohammadi, M. Eshghi, On figures of merit in reversible and quantum logic designs, Quantum Inf. Process. 8 (4) (2009) 297–318.
[10] D. Maslov, G.W. Dueck, Reversible cascades with minimal garbage, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 23 (11) (2004) 1497–1509.
[11] M. Saeedi, M.S. Zamani, M. Sedighi, Z. Sasanian, Reversible circuit synthesis using a cycle-based approach, ACM J. Emerg. Technol. Comput. Syst. 6 (4) (2010) 13.
[12] D. Große, R. Wille, G.W. Dueck, R. Drechsler, Exact multiple control Toffoli network synthesis with SAT techniques, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 28 (5) (2009) 703–715.
[13] R. Wille, M. Soeken, N. Przigoda, R. Drechsler, Exact synthesis of Toffoli gate circuits with negative control lines, in: International Symposium on Multiple-Valued Logic, 2012, pp. 69–74.
[14] T. Sasao, AND-EXOR expressions and their optimization, in: T. Sasao (Ed.), Logic Synthesis and Optimization, Kluwer Academic Publisher, 1993, pp. 287–312.
[15] T. Sasao, EXMIN2: A simplification algorithm for exclusive-OR-sum-of-products expressions for multiple-valued-input two-valued-output functions, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 12 (5) (1993) 621–632.
[16] A. Mishchenko, M. Perkowski, Fast heuristic minimization of exclusive-sums-of-products, in: International Workshop on Applications of the Reed–Muller Expansion in Circuit Design, 2001, pp. 242–250.
[17] T. Hirayama, Y. Nishitani, Exact minimization of AND-EXOR expressions of practical benchmark functions, J. Circuits Syst. Comput. 18 (3) (2009) 465–486.
[18] V.V. Shende, A.K. Prasad, I.L. Markov, J.P. Hayes, Synthesis of reversible logic circuits, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 22 (6) (2003) 710–722.
[19] D.M. Miller, D. Maslov, G.W. Dueck, A transformation based algorithm for reversible logic synthesis, in: Design Automation Conference, 2003, pp. 318–323.
[20] M. Soeken, M.K. Thomsen, White dots do matter: Rewriting reversible logic circuits, in: Reversible Computation, in: Lect. Notes Comput. Sci., vol. 7948, 2013, pp. 196–208.
[21] A. Gaidukov, Algorithm to derive minimum ESOP for 6-variable function, in: International Workshop on Boolean Problems, 2002, pp. 141–148.