Decompositions of reversible logic circuits

Mgr inż. Marek SZYPROWSKI
Received the M.Sc. degree in Computer Science from the Warsaw University of Technology (WUT) in 2008. He is currently a Ph.D. candidate in the Institute of Computer Science, WUT. His research interests include a reversible circuits synthesis, which was also a topic of his M.Sc. thesis.

Dr hab. inż. Paweł KERNOTPF
Received the M.Sc. and Ph.D. degrees in Computer Science from the Warsaw University of Technology (WUT) in 1962 and 1973, respectively. He is currently a professor at the Institute of Computer Science, WUT. His current research interests include logic synthesis, reversible circuits, binary and multi-valued decision diagrams and multi-valued logics.

Abstract
Results of research on decompositions of reversible circuits into blocks are presented where each block is constructed from one kind of gates. The main contribution of this paper consists in discovering that there exist more decompositions than the only one considered in the literature up to now. Moreover, it is shown that all of these decompositions correspond to circuits having different average minimal cost. This fact can be used in the future to guide heuristics in developing better algorithms for reversible logic circuit synthesis.

Keywords: reversible logic circuits, decompositions of reversible circuits.

Dekompozycje odwracalnych układów logicznych

Streszczenie
Układ logiczny jest odwracalny, gdy liczba wejść jest równa liczbie wyjść, a funkcja realizowana przez ten układ jest wzajemnie jednoznaczna. Do tej pory tylko w jednej publikacji rozważano dekompozycję układów odwracalnych na takie bloki, z których każdy jest złożony z bramek odwracalnych jednego typu. W pracy prezentujemy znalezione przez nas trzy inne dekompozycje układów. Dzięki znalezieniu przez nas wszystkich optymalnych układów o trzech wejściach i trzech wyjściach, pokazujemy, że rozpatrywane przez nas nowe dekompozycje prowadzą do układów o mniejszym koszcie niż dla wcześniej rozpatrywanej dekompozycji. Zatem znalezione przez nas dekompozycje mogą mieć duże znaczenie przy konstruowaniu algorytmów syntetyki odwracalnych układów logicznych generujących układy o mniejszym koszcie niż opublikowane dość algorytmy.

Słowa kluczowe: odwracalne układy logiczne, dekompozycje układów odwracalnych.

1. Introduction

A gate (or a circuit) is called reversible if there is a one-to-one (bijective) correspondence between its inputs and outputs. Research on reversible logic circuits is motivated by advances in quantum computing, nanotechnology and low-power design.

Many reversible gate libraries have been examined in the literature, but in this paper we will consider only the most widely used NCT library consisting of NOT, CNOT and Toffoli gates (denoted by N, C, T, respectively). Quality of a library is usually estimated by total number of gates (gate count) [1] or by quantum cost (assuming that the cost of NOT, CNOT and Toffoli gates is 1, 1 and 5, respectively) [1].

Recently, reversible logic synthesis has been extensively studied. Logic synthesis for classical reversible circuits is a first step toward synthesis of quantum circuits. Namely, it has been shown that some important tasks of quantum computing like circuits for implementation of Grover’s quantum search algorithm [2] and stabilizer circuits [3,4] use many NCT gates and contain large parts consisting of classical reversible gates only. Thus, synthesis methods that reduce the size of these sub-blocks would in turn reduce the size of the overall quantum circuit as well.

Different representations of reversible Boolean functions are being used in the reversible logic synthesis algorithms: truth tables, Reed-Muller positive polarity expressions (PPRMs), Reed-Muller spectra, permutation groups, SAT instances, quantified Boolean formulas (QBFs), binary decision diagrams (BDDs) matrices and graphs. Powerful tools, such as modern SAT-solvers, state-of-the-art QBF-provers, BDD manipulation software, and libraries of optimal 3-line and 4-line reversible circuits have been applied to solve the problem. In one of the approaches [5] look-up libraries consisting of millions of 3- and 4-input optimal circuits (only one optimal circuit for each reversible function) is built. However, satisfactory practical solutions for arbitrary libraries of gates and arbitrary cost functions have not yet been found. In addition, even NCT library synthesis techniques developed for such circuits scale not well and optimal circuits not always can be found even for relatively small numbers of inputs and outputs [5-7].

Decomposing a reversible circuit into blocks might help simplifying circuit synthesis. If we consider that each block is constructed only from the gates of the same type then each block can be synthesised separately with simpler algorithms, e.g. optimal synthesis of N-type block is trivial and the algorithm has been constructed for asymptotically optimal synthesis of linear circuits (C-type blocks) [3].

2. Basic notions

Definition 1 A completely specified n-input n-output Boolean function (referred to as $n^n$ function) is called reversible if it maps each input assignment into a unique output assignment.

Since reversible functions are bijective mappings they correspond to permutations of rows in the truth table (see Fig. 1).

![Fig. 1. An example of a reversible Boolean function](image)

Rys. 1. Przykład odwracalnej funkcji boolowskiej

Definition 2 An n-input n-output ($n^n$) gate (or circuit) is reversible if it realizes an $n^n$ reversible function.

Many gate libraries have been examined in the literature. We will consider the most widely used NCT library consisting of NOT, CNOT and Toffoli gates (denoted by N, C, T, respectively), as well as its sublibraries (denoted by NC, NT, CT, N, C, T).

Definition 3 Let $N$ gate performs the operation $(y) = (x \oplus 1)$, $2N$ CNOT gate performs the operation $(y_1,y_2) = (x_1,x_2 \oplus x_3)$, $3N$ TOFFOLI gate performs the operation

$$
$$
$(y_3, y_2, y_1) = (y_3, x_3, x_2 \oplus x_1 y_3)$, where $\oplus$ denotes XOR. Pictorial representations of these gates are shown in Fig. 1.

![Fig. 2. Pictorial representations of reversible gates: a) NOT, b) CNOT, c) Toffoli](image)

All the above defined gates invert one input if and only if all others are 1, passing the other inputs unchanged to corresponding outputs.

**Definition 4** Let $L$ be a reversible gate library. An $L$-circuit is a circuit composed only of gates from $L$. A reversible function is $L$-constructible if it can be computed by an $L$-circuit.

**Definition 5** For any gate libraries $L_1, L_2, \ldots, L_k$, an $L_1 \cup L_2 \cup \cdots \cup L_k$ circuit is a cascade of an $L_1$-circuit followed by an $L_2$-circuit, ..., followed by an $L_k$-circuit. A function computed by an $L_1 \cup L_2 \cup \cdots \cup L_k$-circuit is $L_1 \cup L_2 \cup \cdots \cup L_k$-constructible.

**Definition 6** If a reversible function is $L_1 \cup L_2 \cup \cdots \cup L_k$-constructible and each of the libraries is equal to a sublibrary $N$, $C$ or $T$ than the function has a decomposition $L_1 \cup L_2 \cup \cdots \cup L_k$.

### 3. Circuit decompositions

Circuit decomposition is a special case of general circuit transformation rules (first presented in [8]). A more general framework was presented in [2] for studying possibilities of moving gates along a circuit. A canonical form of an $N$-constructible reversible circuit was pursued in which gates of the same kind are grouped together. By applying transformation rules allowing to push NOT gates towards the end of the circuit it is possible to show that every $N$-constructible function is $C/N$-constructible. However, there exist $C/N$-constructible functions which are not $C/T$-constructible [2], i.e., there exist $N$-constructible functions which are not $C/N$-constructible. Decomposition $C/T[N]$ was introduced in [2] and is the only one considered up to now. An analysis how this decomposition can be applied to larger reversible Boolean functions is also included in [2]. An example of an optimal reversible circuit, implementing the function defined in Table 1, and its $C/T[N]$ decomposition are shown in Fig. 3 and Fig. 4, respectively. As it can be noticed a decomposition of a circuit does not necessarily gives an optimal circuit.

**Tab. 2.** List of all decomposition types with three or four blocks

**Fig. 5.** Example of a $C/T[N]$ decomposition of the reversible circuit from Fig. 3

### 4. Results

We have discovered that besides the $T[N]$ type there exist other decompositions that are interesting for reversible circuit synthesis. To find such decompositions we have prepared a special program. Namely, by exhaustive calculations we have generated minimal size reversible 3*3 circuits under gate count (GC) and quantum cost (QC) minimization for all decompositions with three or four groups of gates of the same kind (under the constraint that each block type appears in a decomposition at most twice). A list of these decomposition types is given in Table 2 (decomposition are shown in pairs together with the inverse ones).

**Tab. 2.** List of all decomposition types with three or four blocks

**Fig. 6.** Example of a $C/T[N]$ decomposition of the reversible circuit from Fig. 3

**Fig. 7.** Example of a $C/T[NC]$ decomposition of the reversible circuit from Fig. 3

Only four of the considered decomposition types have the property that for all reversible 3*3 Boolean functions there exist at least one 3*3 circuit of the specified decomposition type. These decompositions are bolded in Table 2. Examples of minimal such decompositions are presented in Fig. 4-7. It can be noticed that different decompositions result in circuits of different gate count. In this example the $C/T[NC]$ decomposition has the same gate count as the optimal circuit from Fig. 3.
Tables 3 and 4 show how many reversible 3*3 functions can be realized with a specified minimal gate count (column Gate Count in Table 3) or a specified minimal quantum cost (column Quantum Cost in Table 4), depending on one of these four decomposition types (columns 2 to 5). The last column has been obtained by exhaustive construction of all circuits having 1 gate, 2 gates, etc. As the weighted averages (WA) of gate counts of minimal circuits in Table 3 show three decomposition types have advantages over the T|C[N].

The differences between weighted averages are much more substantial when using a quantum cost function (Table 4). This case is of a greater practical interest since quantum cost was defined as to reflect the expected cost of experimental implementation. Moreover, from column 3 and 5 in both Table 3 and Table 4 one can draw the conclusion that we might obtain shorter circuits locating NOT gates at a distance from both ends of the circuit instead of locating all NOT gates at the very end as many existing algorithms do. The types C|T[C[N] / N|C|T] and C|T[N] / C|N[T] have smaller weighted averages than the other two decompositions what suggests that it might be better to put a CNOT gate block as the first or the last one in the circuit.

5. Conclusions

Our experimental data extrapolated to larger circuits can be used in the future to guide some new heuristics. The main problem that arises is how to decompose a reversible function in a way corresponding to a specified decomposition type? This problem is left open. Solving it would be a major step in speeding up reversible circuit synthesis. A circuit designed as a cascade of different optimal blocks might not be optimal as a whole (as shown in the Fig. 3 and Fig. 4), but it can be synthesized faster than with other known methods. Next, it can be reduced by various methods such as using templates [6], peep-hole optimisation and resynthesis approaches [5].

6. References