On the Behavior of Substitution-based Reversible Circuit Synthesis Algorithms: Investigation and Improvement

Mehdi Saeedi, Morteza Saheb Zamani, Mehdi Sedighi
Email: {msaeedi, szamani, msedighi}@aut.ac.ir

Quantum Design Automation Group
Computer Engineering Department - Amirkabir University of Technology
Tehran, Iran

Presented by:
Mahtab Niknahad (Amirkabir University of Technology)

ANNUAL Symposium ON VLSI 2007
PORTO ALEGRE, BRAZIL
Outline

- Introduction
- Basic concept
- Previous work
- Search-based method
- Proposed method
  - DFS and BFS synthesis methods
  - Hybrid synthesis method
- Experimental results
- Conclusion
- References
Introduction

- Reversible function
- Landauer’s paper about energy dissipation
- Bennett’s paper about the power dissipation of reversible gates
- The applications of reversible circuits
  - Low power CMOS design
  - Optical computing
  - Quantum computing
  - Synthesis

QDA Group, Amirkabir University of Technology, Tehran, Iran
Basic Concept (1)

- Reversible Function
- A new notation for reversible function
- Reversible gate
- various reversible gates
  - NOT, CNOT, C2NOT, ...
- \( x_i (\text{out}) = x_i \) \((i < n)\), \( x_n (\text{out}) = x_1 x_2 ... x_{n-1} \oplus x_n \).
- PPRM (Positive polarity Reed-Muller) expansion.
  \[
  f(x_1, x_2, ..., x_n) = a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n \\
  \oplus a_{12} x_1 x_2 \oplus ... \oplus a_{n,n-1} x_{n-1} x_n \oplus \\
  ... \oplus a_{12...n} x_1 x_2 ... x_n
  \]

QDA Group, Amirkabir University of Technology, Tehran, Iran
Basic Concept (2)

- Gate Complexity
  - The number of terms in PPRM expansion
  - The number of non-zero coefficients in previous equation

- gate cost
  - The number of elementary operations required to realize a gate

- Reducing the number of cascaded gates and the number of gate control lines are always preferred
Previous Work

- Two type of algorithms:
  - Transformation-based algorithms
  - Synthesis Algorithms (constructive algorithm)
- The size of a reversible circuit can be very large
  - A practical algorithm may become extremely difficult
- Search-based algorithms
  - Extensive exploration is required
Search-based method (1)

- PPRM expansion
- common sub-expressions
  - common sub-expressions between the PPRM expansions of multiple outputs are identified
- Primary objective
  - Minimize the number of gates (i.e. factors) needed to transform a PPRM expansion into the identity function.
- Secondary objective
  - Minimize the size of the individual gates (i.e. the number of literals in each factor) which is related to the number of control lines for each CNOT-based gate.

QDA Group, Amirkabir University of Technology, Tehran, Iran
Search-based method (2)

- While common sub-expressions seem to be good candidates for current substitution, there is no guarantee that the resulted PPRM expression contains fewer terms.
  - Example 1 (common sub-expression)
  - \( a_{out} = a \oplus b, \quad b_{out} = b \oplus bc \oplus ac, \quad c_{out} = 1 \oplus c \).
  - \( b = b \oplus ac \) (common factor)
  - \( a_{out} = a \oplus b \oplus ac, \quad b_{out} = b \oplus bc \oplus ac, \quad c_{out} = 1 \oplus c \)
  - Not only this common factor dose not decrease the number of terms in its original expression (i.e. \( b \)), but also it increases the number of terms in the other expression (i.e. \( a \)).

QDA Group, Amirkabir University of Technology, Tehran, Iran
Search-based method (3)

- Therefore, **greedy** common sub-expression selection may not result in a better expression.
- Greedy disregard of non-common factors.
- Example 2 (non-common sub-expression):
  - $a_{out} = 1 \oplus a \oplus b \oplus c \oplus ac$, $b_{out} = b \oplus bc \oplus ac$, $c_{out} = c$
  - $b_{out} = b \oplus a$ (non-common factor)
  - Using this factor will result in an optimized CNOT-based circuit with the cost of 8.
- The best report result is a circuit with the cost of 16.
Search-based method (4)

- An important result:
  - Based on the previous two examples, it can be concluded that the selection metric of common sub-expressions may result in poor results. Therefore, there is a clear advantage to use other factors as well as common factors to simplify a reversible circuit.
Search-based method (5)

- The only sub-expression that can increase the number of terms in PPRM expansions is $v_{i,\text{out}} = v_i \oplus \overline{I}$

- Any increase in the number of PPRM terms is discarded

- However, there is no direct correlation between local increase or decrease in the number of PPRM terms and the final synthesized result. (The next slide)
Search-based method (6)

- \( a_{out} = 1 \oplus a \oplus c \oplus ab \oplus ac, \quad b_{out} = 1 \oplus b \oplus ab \oplus ac, \quad c_{out} = a \oplus 1 \)
- \( a_{out} = a \oplus c \) (Common factor)
- \( a_{out} = 1 \oplus a \oplus c \oplus ab \oplus bc \oplus ac, \quad b_{out} = 1 \oplus b \oplus c \oplus ab \oplus bc \oplus ac, \quad c_{out} = 1 \oplus a \oplus c \)
- The number of term eliminations is (-1,-2,-1)
- Using this factor as an initial substitution will result in better-synthesized result

- The greedy substitution of factors, which results in fewer PPRM terms, may not lead to solution at all

QDA Group, Amirkabir University of Technology, Tehran, Iran
Proposed Method (1)

- DFS and BFS synthesis algorithm
- DFS algorithm
  - It considers the results of previously substituted factors before examining any new substitutions
- BFS Algorithm
  - It considers all new factors before using the results of previously substituted factors
- Deeper nodes are more likely to be close to a solution
- The authors of [12] used a DFS-based search method.
- Using a new previously unconsidered factor to synthesize a circuit

QDA Group, Amirkabir University of Technology, Tehran, Iran
Proposed Method (2)

- **Example 4 (DFS vs. BFS synthesis methods)**
  - \[ a_{out} = 1 \oplus ab \oplus bc \oplus ac, \quad b_{out} = 1 \oplus a \oplus bc \oplus ac, \]
  - \[ c_{out} = 1 \oplus a \oplus b \oplus ab \oplus bc \oplus ac \]

- **BranchNo** is the maximum number of acceptable substitutions at each node

- **MaxDepth** is the maximum tree depth at which PPRM terms can still be increased.

- Please see the paper for more details.

- Testing more factors will always lead to better results.

- Efficient method to synthesize

QDA Group, Amirkabir University of Technology, Tehran, Iran
Hybrid synthesis method

- In the first \textit{MaxDepth} levels, a BFS algorithm is used to evaluate all of the possible factors including common sub-expressions.
- After that, a DFS algorithm is used to evaluate the previously considered nodes, as we believe that deeper nodes have more opportunities to lead a result.
- By using a hybrid DFS & BFS method, the benefits of both algorithm are used.
- Several notations and theorems are proposed in this paper which were omitted due to the lack of time.

QDA Group, Amirkabir University of Technology, Tehran, Iran
Experimental results (1)

☐ The first eight examples are come from literature.

☐ The second eight examples are introduced for the first time.

☐ Please note that the second examples are not synthesized using the previously published paper (Search-based method)

☐ Pentium IV 3.0GHz computer with 1GB memory
Experimental results (2)

- Cost as the total cost of final circuit and SNd as the number of searched nodes

Table 1. The results of using our method on examples of [12]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cost</td>
<td>SNd</td>
<td>Cost</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>11</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>761</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>156</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>51</td>
<td>9515</td>
<td>27</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>20</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>12</td>
<td>230</td>
<td>12</td>
</tr>
<tr>
<td>Average</td>
<td>24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. The results of using our method for eight new examples where the method of [12] can not produce any circuit

<table>
<thead>
<tr>
<th>Our Circuits</th>
<th>No. of Gates</th>
<th>Cost</th>
<th>SNd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>19</td>
<td>66</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>14</td>
<td>77</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>11</td>
<td>4387</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>19</td>
<td>352</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>51</td>
<td>678</td>
</tr>
<tr>
<td>6</td>
<td>14</td>
<td>62</td>
<td>9712</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>73</td>
<td>74521</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>72</td>
<td>85191</td>
</tr>
</tbody>
</table>
# Experimental results (3)

## Table 3. Our synthesized circuits for the attempted examples

<table>
<thead>
<tr>
<th>Circuit#</th>
<th>Description</th>
<th>Our synthesized circuits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(4,5,6,1,0,7,2,3)</td>
<td>b=b, a=a, b=b, a=a, b=b, a=a, b=b</td>
</tr>
<tr>
<td>2</td>
<td>(7,6,4,5,0,1,2,3)</td>
<td>a=a, b=b, a=a, b=b, a=a, b=b</td>
</tr>
<tr>
<td>3</td>
<td>(0,1,2,3,5,4,3,8,7)</td>
<td>b=b, a=a, b=b, a=a, b=b, a=a</td>
</tr>
<tr>
<td>4</td>
<td>(0,6,2,3,4,5,1,7)</td>
<td>a=a, b=b, c=c, b=b, a=a, b=b, a=a</td>
</tr>
<tr>
<td>5</td>
<td>(0,1,4,2,3,4,5,6,7,8,9,10,11,12,13,1,15)</td>
<td>a=a, b=b, c=c, b=b, a=a, b=b, c=c, b=b, a=a, b=b, c=c, b=b, a=a, b=b, c=c, b=b, a=a</td>
</tr>
<tr>
<td>6</td>
<td>(4,5,6,7,2,3,1,0)</td>
<td>c=c, c=c, b=b, a=a, b=b, a=a, b=b, a=a</td>
</tr>
<tr>
<td>7</td>
<td>(8,9,10,11,12,13,14,15,4,5,6,7,2,3,1,0)</td>
<td>d=d, d=d, b=b, a=a, b=b, a=a, b=b, a=a, b=b, a=a</td>
</tr>
<tr>
<td>8</td>
<td>(0,1,2,3,6,7,5,4,14,15,13,12,9,8,11,10)</td>
<td>d=d, d=d, b=b, a=a, b=b, a=a, b=b, a=a, b=b, a=a, b=b, a=a, b=b, a=a, b=b, a=a</td>
</tr>
</tbody>
</table>

QDA Group, Amirkabir University of Technology, Tehran, Iran
Conclusion

- A more efficient search-based synthesis method is proposed.
- There is no direct correlation between local common sub-expression factors and the final circuit.
- A new hybrid DFS/BFS reversible circuit synthesis algorithm is proposed.
- Experimental results demonstrated that using our method can lead to better synthesis circuits with respect to the total circuit cost as well as the probability of leading to a synthesized circuit.

QDA Group, Amirkabir University of Technology, Tehran, Iran
References


Thanks for your attentions.

Any question?

(msaeedi@aut.ac.ir)