LETTER

A Lower Bound on the Number of Toffoli Gates in Reversible Logic Circuits

Masayuki HIGASHIOHNO[†*], **Takashi HIRAYAMA**[††], ***and*** **Yasuaki NISHITANI**[††], ***Members***

SUMMARY We present a lower bound on the number of gates in reversible logic circuits that represent a given reversible logic function, in which the circuits are assumed to consist of Toffoli gates and have no redundant input/output lines. Experimental results of computing lower bounds on randomly-generated reversible logic functions are also given.

key words: *reversible logic circuits, Toffoli gates, lower bound*

1. Introduction

The synthesis of reversible logic circuits realizing given reversible functions has been studied as the basic research for the quantum logic circuits. For that reason, NOT, CNOT, and Toffoli gates are used for synthesizing reversible logic circuits as well as quantum ones [2], [5]. Figure 1 shows an example of Toffoli gates. In this paper, NOT, CNOT, and k-Toffoli are referred to as Toffoli gates. NOT and CNOT can be considered as 0-Toffoli and 1-Toffoli, respectively. We deal with the synthesis of reversible logic circuits that consist of Toffoli gates and have no redundant input/output lines.

We present a lower bound on the number of Toffoli gates in reversible logic circuits that represent a given reversible logic function. This is the first lower bound for given specific reversible functions although lower bounds for some class of reversible functions have been known [3], [4].

2. Basic Definitions

In this paper, n-input single-output logic functions

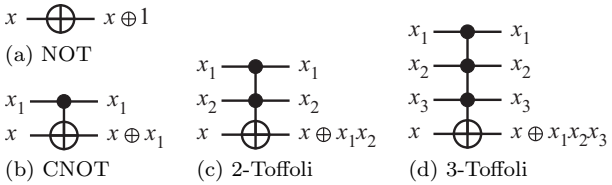

Fig. 1 Example of Reversible Gates.

Manuscript received October 8, 2008.
Manuscript revised December 9, 2008.

[†]Graduate School of Engineering, Iwate University, 4-3-5 Ueda, Morioka, Iwate, 020-8551 Japan
[††]Department of Computer and Information Sciences, Iwate University, 4-3-5 Ueda, Morioka, Iwate, 020-8551 Japan
[*]Presently, Nippon Net Systems, Ltd

("logic functions" for short) are represented by positive polarity Reed-Muller expressions (PPRMs) [1]. It is known that any logic function can be represented by the PPRM uniquely. For example, logic function $x_1\bar{x}_2 + x_2$ is written as $x_1 \oplus x_2 \oplus x_1x_2$ in PPRM.

The composition of an n-input single-output logic function f and an n-input n-output logic function F is denoted by $f \circ F$ and is defined as the mathematical function composition, i.e., the composite function $f' = f \circ F$ is the n-input single-output logic function such that $f'(X) = f(F(X))$ for all the input vectors $X \in \{0,1\}^n$. Similarly, the composite function $F_1 \circ F_2$ of n-input n-output logic functions F_1 and F_2 is the n-input n-output logic function such that $F'(X) = F_1(F_2(X))$ for all $X \in \{0,1\}^n$. Composition of functions is always associative.

Here is the notation of an n-input n-output logic function. Let x_i $(1 \le i \le n)$ be the variable that represents the i-th element of the input vector. By regarding x_i as a logic function, the composition $x_i \circ F$ can be seen as the logic function that represents the i-th output of F. By letting $f_i = x_i \circ F$, F is denoted by f_i and x_i in pairs as follows.

$$[f_1/x_1, f_2/x_2, \ldots, f_n/x_n] \quad \text{where } f_i = x_i \circ F$$

Each f_i/x_i describes the i-th output and input. The trivial case where $f_i = x_i \circ F = x_i$, or x_i/x_i is sometimes omitted in the notation, for simplicity.

Example 1: $\{a, b, c\}$ is a set of variables. $F = [a \oplus bc/a, b \oplus 1/b, c/c]$ is a 3-input 3-output logic function, where f_i is written in PPRM. In this case, F can be also represented as $[a \oplus bc/a, b \oplus 1/b]$ by omitting the notation of c/c. Generally, the composition of n-input single-output logic function f and n-input n-output logic function F can be considered as a substitution in PPRMs, in which each variable x of f is replaced with $x \circ F$. Let $f = c \oplus ab$ and $F = [a \oplus bc/a, b \oplus 1/b]$. The composition $f \circ F$ results in $(c \oplus ab) \circ F = (c \circ F) \oplus (a \circ F)(b \circ F) = c \oplus (a \oplus bc)(b \oplus 1) = c \oplus ab \oplus a$. And let $F' = [a \oplus ab \oplus c/a, c \oplus ab/c]$. The composition $F' \circ F$ results in $[bc \oplus c \oplus ab/a, b \oplus 1/b, c \oplus ab \oplus a/c]$, whose output functions $x \circ (F' \circ F)$ are obtained separately as follows.

$$\begin{aligned} a \circ (F' \circ F) &= (a \circ F') \circ F = (a \oplus ab \oplus c) \circ F \\ &= bc \oplus c \oplus ab \end{aligned}$$

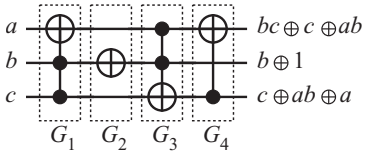

Fig. 2 Example of Reversible Logic Circuit.

$$\begin{aligned} b \circ (F' \circ F) &= (b \circ F') \circ F = b \circ F \\ &= b \oplus 1 \\ c \circ (F' \circ F) &= (c \circ F') \circ F = (c \oplus ab) \circ F \\ &= c \oplus ab \oplus a \end{aligned}$$

Definition 1: An n-input n-output logic function F is called reversible if F is bijective.

Definition 2: The function of a Toffoli gate G is denoted by $[x \oplus p/x]$, where x is a variable and p is a product term without x.

To discuss a lower bound for reversible functions, we regard Toffoli gates as functions rather than devices, hereafter. As functional properties, any Toffoli gate G is reversible, whose inverse function is G itself. For Toffoli gates G_i $(1 \leq i \leq k)$, if $F' = F \circ G_1 \circ G_2 \circ \cdots \circ G_k$, $F' \circ G_k \circ \cdots \circ G_2 \circ G_1 = F$ holds.

Definition 3: A reversible logic circuit is defined by a sequence of Toffoli gates $G_1 G_2 \ldots G_k$, where k is called the number of gates in the circuit. The reversible function realized by the circuit is the composition of gates $G_k \circ G_{k-1} \circ \cdots \circ G_1$.

Example 2: Figure 2 shows a reversible logic circuit with four gates, which is represented by $G_1 G_2 G_3 G_4 = [a \oplus bc/a][b \oplus 1/b][c \oplus ab/c][a \oplus c/a]$. The reversible function F realized by the circuit is the composition of these gates, i.e., $G_4 \circ G_3 \circ G_2 \circ G_1 = [a \oplus c/a] \circ [c \oplus ab/c] \circ [b \oplus 1/b] \circ [a \oplus bc/a] = [a \oplus c/a] \circ [c \oplus ab/c] \circ [a \oplus bc/a, b \oplus 1/b] = [a \oplus c/a] \circ [a \oplus bc/a, b \oplus 1/b, c \oplus ab \oplus a/c] = [bc \oplus c \oplus ab/a, b \oplus 1/b, c \oplus ab \oplus a/c]$.

For a given reversible function F, the synthesis of reversible logic circuits can be seen as the problem of obtaining a sequence of Toffoli gates $G_1 \ldots G_{k-1} G_k$ that satisfies $F = G_k \circ G_{k-1} \circ \cdots \circ G_1$. Since there exist many circuits to realize F, the number of gates k in the resulting circuit varies with the synthesizers. As a theoretical research, we consider a lower bound on k for a given function F.

3. A Lower Bound on the Number of Toffoli Gates in Reversible Logic Circuits

3.1 Lower Bound Theorem

Below, we define the size $\sigma(F)$ of a reversible function F to evaluate the number of gates in the reversible circuits that realize F.

Definition 4: The number of product terms of the PPRM of a logic function f is denoted by $\tau(f)$. We define $\sigma_x(f) = \tau(x \oplus f)$, where x is a variable. Let F be a reversible function, and Var be a set of variables. The size $\sigma(F)$ of F is defined as follows.

$$\sigma(F) = \sum_{x \in Var} \sigma_x(x \circ F)$$

Example 3: For the reversible function $F = [bc \oplus c \oplus ab/a, b \oplus 1/b, c \oplus ab \oplus a/c]$, which was given in Example 2 (Fig. 2), $\sigma_a(a \circ F) = \tau(a \oplus bc \oplus c \oplus ab) = 4$, $\sigma_b(b \circ F) = \tau(b \oplus b \oplus 1) = 1$, and $\sigma_c(c \circ F) = \tau(c \oplus c \oplus ab \oplus a) = 2$. Thus, the size $\sigma(F)$ of F is 7. If F is an identity function, e.g., $[a/a, b/b, c/c]$, the size is $\sigma(F) = 0$.

Lemma 1: For any reversible function F and any Toffoli gate $G = [a \oplus p/a]$, the following inequality holds.

$$2\sigma(F) + 1 \geq \sigma(F \circ G)$$

The proof of Lemma 1 will be given in Section 3.2. In the rest of this section, we discuss a lower bound on the number of gates in reversible circuits by using the above lemma.

Definition 5: Among all reversible circuits that realize reversible function F, those with the minimum number of gates are called the minimum circuits of F. The number of gates in a minimum circuit is denoted by $\gamma(F)$.

Theorem 1 (Lower Bound Theorem): For any reversible function F, the inequality $2^{\gamma(F)} - 1 \geq \sigma(F)$, i.e., $\gamma(F) \geq \lceil \log(\sigma(F) + 1) \rceil$, holds.

(proof) The proof is by mathematical induction on $\gamma(F)$. If $\gamma(F) = 0$, $2^{\gamma(F)} - 1 = 0$ holds. In addition, from $\gamma(F) = 0$, F is the identity function. Then, we have $\sigma(F) = 0$. Thus, the base case is proved.

Assume that the theorem holds for reversible functions F_m such that $\gamma(F_m) = m$ $(m \geq 0)$. It must be shown that the theorem holds for reversible functions F such that $\gamma(F) = m + 1$. Such a function F can be written by the composition of some reversible function F_m with $\gamma(F_m) = m$ and some Toffoli gate $[a \oplus p/a]$, i.e., $F = F_m \circ [a \oplus p/a]$. Then, from Lemma 1, $2\sigma(F_m) + 1 \geq \sigma(F_m \circ [a \oplus p/a]) = \sigma(F)$ holds. Using the induction hypothesis $2^m - 1 \geq \sigma(F_m)$, we have $2^{m+1} - 1 = 2 \cdot (2^m - 1) + 1 \geq 2\sigma(F_m) + 1 \geq \sigma(F)$. □

Example 4: For the reversible function $F = [b \oplus ac \oplus bc/a, 1 \oplus a \oplus c \oplus ab \oplus ac \oplus bc/b, c \oplus 1 \oplus b \oplus ab \oplus ac \oplus bc/c]$, $\sigma(F) = 16$ holds. From the lower bound theorem, $\lceil \log(\sigma(F) + 1) \rceil = \lceil \log 17 \rceil = 5$ or more gates are required in the reversible circuits to realize F. In fact, F is represented by the composition of five gates $[b \oplus c/b] \circ [c \oplus ab/c] \circ [a \oplus bc/a] \circ [b \oplus a/b] \circ [c \oplus 1/c]$, which results in $\gamma(F) = 5$.

3.2 Proof of Lemma 1

As a preliminary to the proof, we define $\delta_x(f) = \sigma_x(f) - \tau(f)$ for logic function f and a variable x. Since $\sigma_x(f) = \tau(x \oplus f)$, $\delta_x(f) = \tau(x \oplus f) - \tau(f)$ holds. Therefore, $\delta_x(f) = -1$ if the product x appears in the PPRM of f, and $\delta_x(f) = 1$ otherwise. Now we give the proof of Lemma 1 in the following.

Lemma 1 is proved if we have two inequalities: $2\sigma_a(a \circ F) - \sigma_a(a \circ F \circ G) \geq -1$ for the variable a used in the Toffoli gate $G = [a \oplus p/a]$, and $2\sigma_x(x \circ F) - \sigma_x(x \circ F \circ G) \geq 0$ for any variable x except a. We prove these inequalities below.

For a variable x, let f be $x \circ F$, where x may be a. From the positive Davio expansion [1], the logic function f can be represented by $f = af_a \oplus f_0$, where f_a and f_0 are logic functions whose PPRMs do not have any products containing a. Then, $f \circ G$ is represented as follows.

$$f \circ G = (a \oplus p)f_a \oplus f_0 = af_a \oplus pf_a \oplus f_0$$

Note that $\tau(af_a) = \tau(f_a)$ and $\tau(f) = \tau(f_a) + \tau(f_0)$ hold as a property of the positive Davio expansion. Let h be the logic function defined as the EXOR combination of common products between PPRMs of pf_a and f_0. Then, we have $\tau(pf_a) = \tau(pf_a \oplus h) + \tau(h)$, $\tau(f_0) = \tau(f_0 \oplus h) + \tau(h)$, and $\tau(pf_a \oplus f_0) = \tau(pf_a \oplus h) + \tau(f_0 \oplus h)$. Since $\tau(f_a) \geq \tau(pf_a)$, the following inequality holds for $2\tau(f) - \tau(f \circ G)$.

$$\begin{aligned}
&2\tau(f) - \tau(f \circ G) \\
&= 2(\tau(f_a) + \tau(f_0)) - (\tau(f_a) + \tau(pf_a \oplus f_0)) \\
&= \tau(f_a) + 2\tau(f_0) - \tau(pf_a \oplus f_0) \\
&\geq \tau(pf_a) + 2\tau(f_0) - \tau(pf_a \oplus f_0) \\
&= 3\tau(h) + \tau(f_0 \oplus h)
\end{aligned}$$

Since $2\sigma_x(f) - \sigma_x(f \circ G) = 2(\tau(f) + \delta_x(f)) - (\tau(f \circ G) + \delta_x(f \circ G))$ holds from the definition of δ_x, we have the following inequality.

$$\begin{aligned}
&2\sigma_x(f) - \sigma_x(f \circ G) \\
&\geq 3\tau(h) + \tau(f_0 \oplus h) + 2\delta_x(f) - \delta_x(f \circ G) \qquad (1)
\end{aligned}$$

We show that the right-hand side of Equation (1) is more than or equal to -1 in the case of $x = a$, and is more than or equal to 0 in the case of $x \neq a$.

(Case $x = a$) $\delta_x(f) = \delta_a(af_a \oplus f_0) = \delta_a(af_a)$ holds in this case. Similarly, $\delta_x(f \circ G) = \delta_a(af_a \oplus pf_a \oplus f_0) = \delta_a(af_a)$ holds. Thus, the right-hand side of Equation (1) is represented by

$$3\tau(h) + \tau(f_0 \oplus h) + \delta_a(af_a).$$

Since the values of τ are always nonnegative and the value of δ_a is either -1 or 1, we have $2\sigma_a(f) - \sigma_a(f \circ G) \geq -1$.

(Case $x \neq a$) In this case, $\delta_x(f) = \delta_x(f_0)$ and $\delta_x(f \circ G) = \delta_x(pf_a \oplus f_0)$ hold. Thus, the right-hand side of Equation (1) is represented by

$$3\tau(h) + \tau(f_0 \oplus h) + 2\delta_x(f_0) - \delta_x(pf_a \oplus f_0) \qquad (2)$$

It is obvious that the formula (2) is more than 0 if $\delta_x(f_0) = 1$, since the values of τ are nonnegative and the values of δ_x are -1 or 1. Therefore, we consider the case of $\delta_x(f_0) = -1$ only, which can be divided into two sub cases: the product x appears in the PPRM of h or $f_0 \oplus h$. If h has the product x, it does not appear in $pf_a \oplus f_0$ from the definition of h. Then, we have $2\delta_x(f_0) - \delta_x(pf_a \oplus f_0) = -3$. Because of $\tau(h) \geq 1$ in this case, the formula (2) is more than or equal to 0. If $f_0 \oplus h$ has the product x, $2\delta_x(f_0) - \delta_x(pf_a \oplus f_0) = -1$ holds since the product also appears in $pf_a \oplus f_0$. Because of $\tau(f_0 \oplus h) \geq 1$ in this case, the formula (2) is more than or equal to 0.

4. Some notes on the lower bound with σ

4.1 Simple lower bound with τ

It is a natural idea to predict the number of gates of a circuit from the size of the function representation. As the size of F, we defined $\sigma(F) = \sum_{x \in Var} \tau(x \oplus x \circ F)$ in the previous section. More simply, the total number of products $\tau(F) = \sum_{x \in Var} \tau(x \circ F)$ can be another measure of size of F. In this section, we compare the two lower bounds with $\sigma(F)$ and $\tau(F)$.

Under the measure of $\tau(F)$, the swap function $S = [b/a, a/b]$ and the identity function $I = [a/a, b/b]$ cannot be distinguished, evaluating to the same, $\tau(S) = \tau(I) = 2$. Meanwhile $\sigma(F)$ can distinguish them as $\sigma(S) = 4$ and $\sigma(I) = 0$. Moreover the lower bound with $\sigma(S)$ tells us that the swap function S requires three or more gates.

As an inequality with $\tau(F)$, $2\tau(F) \geq \tau(F \circ G)$ can be obtained by the similar way of the proof of Lemma 1. Similarly to Theorem 1, the inequality leads to $n \cdot 2^{\gamma(F)} \geq \tau(F)$, i.e., $\gamma(F) \geq \lceil \log(\tau(F)/n) \rceil$, where F is any reversible function with n variables. Considering the values $\sigma(F)$ and $\tau(F)$ are essentially similar, this lower bound $\lceil \log(\tau(F)/n) \rceil$ is inferior to the proposed one $\lceil \log(\sigma(F) + 1) \rceil$.

Furthermore, the maximum $\tau(F)$ is roughly $n2^n$, and the resulting lower bound is $\lceil \log(\tau(F)/n) \rceil = n$. On the other hand, the maximum $\sigma(F)$ is also roughly $n2^n$, and the resulting lower bound is $\lceil \log(\sigma(F)+1) \rceil = n + \log n$. The lower bound with $\sigma(F)$ is larger than that with $\tau(F)$ also in this comparison.

4.2 Comparison with a trivial lower bound

There is a trivial lower bound on the number of gates in reversible circuits. After we describe it, we give the experimental results to compare the trivial lower bound and our proposed one with σ.

Table 1 Average of Lower Bounds.

Reversible functions	$\lceil \log(\sigma(F)+1) \rceil$	$\nu(F)$
3-variable functions	3.88	2.96
4-variable functions	5.36	4.00
5-variable functions	6.99	5.00
6-variable functions	8.00	6.00
8-variable functions	10.44	8.00
10-variable functions	13.00	10.00

Definition 6: For a reversible function F, $\nu(F)$ denotes the number of variables x such that $x \circ F \neq x$.

Suppose that we have a reversible function F and a Toffoli gate $G = [a \oplus p/a]$. For variables x except a, if $x \circ F = x$, then $x \circ F \circ G = x$ holds. If $a \circ F = a$, $a \circ F \circ G \neq a$ holds. Thus, we have the following lemma.

Lemma 2: For any reversible function F and any Toffoli gate G, $\nu(F) + 1 \geq \nu(F \circ G)$ holds.

From the above lemma with $\nu(F)$, we have a trivial lower bound on $\gamma(F)$.

Theorem 2 (Trivial Lower Bound): For any reversible function F, $\gamma(F) \geq \nu(F)$ holds.

The proof can be done simply by mathematical induction on $\gamma(F)$ and omitted in this paper. Since both Theorem 1 with σ and Theorem 2 with ν are lower bounds on $\gamma(F)$, we have a mixed lower bound to pick up a larger one as below.

Theorem 3 (Lower Bound Theorem): For any reversible function F, $\gamma(F) \geq \max\{\nu(F), \lceil \log(\sigma(F) + 1) \rceil\}$ holds.

To make a comparison between the two lower bounds $\nu(F)$ and $\lceil \log(\sigma(F) + 1) \rceil$, we performed experiments on them for reversible functions with various numbers of variables. We computed $\lceil \log(\sigma(F)+1) \rceil$ and $\nu(F)$ for all (40,320) 3-variable functions and 50,000 randomly-generated n-variable functions, where $n = 4$, 5, 6, 8, and 10.

The averages of lower bounds for those functions are given in Table 1. The lower bounds with σ are larger than those with ν; $\lceil \log(\sigma(F)+1) \rceil$ is approaching $n + \log n$ with increasing n while $\nu(F)$ is approaching n.

Table 2 shows the distribution of functions such that the difference between two lower bounds, $\lceil \log(\sigma(F) + 1) \rceil - \nu(F)$, is -1, 0, 1, 2, and 3. In our experiments, $\lceil \log(\sigma(F) + 1) \rceil$ was larger than $\nu(F)$ for almost all functions except for 25 3-variable functions, and the difference increased with the number of variables.

5. Conclusion

We defined the size $\sigma(F)$ of reversible logic functions F, and presented a lower bound on the number of Toffoli gates in reversible logic circuits for F. This is the first non-trivial lower bound for given specific reversible functions. We experimented with randomly-generated reversible functions, and have confirmed that the proposed lower bound is larger than the trivial lower bound in the most cases. As a closing remark, it should be mentioned that Lemma 1 for establishing our lower bound has not used the reversibility of functions. Therefore, a better lower bound may be found by utilizing the reversibility.

Table 2 Number of Functions on the Basis of Difference between Two Lower Bounds.

Diff.	Number of functions					
	3-var.	4-var.	5-var.	6-var.	8-var.	10-var.
-1	25	0	0	0	0	0
0	4,113	15	0	0	0	0
1	35,091	32,104	586	0	0	0
2	1,091	17,881	49,414	50,000	27,957	0
3	0	0	0	0	22,043	50,000
Total	40,320	50,000	50,000	50,000	50,000	50,000

Acknowledgments The authors thank the anonymous reviewer for the suggestions for Section 4.

References

[1] M. Davio, J.P. Deschamps, and A. Thayse, Discrete and Switching Functions, McGraw-Hill, 1978.
[2] P. Gupta, A. Agrawal, and N.K. Jha, "An algorithm for synthesis of reversible logic circuits," *IEEE Trans. CAD*, vol.25, no.11, pp.2317–2330, Nov. 2006.
[3] D. Maslov and G. Dueck, "Reversible cascades with minimal garbage," *IEEE Trans. CAD*, vol.23, no.11, pp.1497–1509, Nov. 2004.
[4] V.V. Shende, A.K .Prasad, I.L. Markov, and J.P. Hayes, "Synthesis of reversible logic circuits," *IEEE Trans. CAD*, vol.22, no.6, pp.710–722, June 2003.
[5] D. Maslov, G. Dueck, and D. Miller, "Toffoli network synthesis with templates," *IEEE Trans. CAD*, vol.24, no.6, pp.807–817, June 2005.