Minimal universal library for $n \times n$ reversible circuits

Guowu Yang\textsuperscript{a}, Xiaoyu Song\textsuperscript{b,\ast}, Marek A. Perkowski\textsuperscript{b}, William N.N. Hung\textsuperscript{b}, Chang-Jun Seo\textsuperscript{c}

\textsuperscript{a} University of Electronic Science and Technology of China, Sichuan, China
\textsuperscript{b} Department ECE, Portland State University, OR, USA
\textsuperscript{c} Department of EIRE, Inje University, Republic of Korea

Received 29 April 2006; received in revised form 5 November 2007; accepted 17 November 2007

Abstract

Reversible logic plays an important role in quantum computing. Several papers have been recently published on universality of sets of reversible gates. However, a fundamental unsolved problem remains: “what is the minimum set of gates that are universal for $n$-qubit circuits without ancillae bits”. We present a library of 2 gates which is sufficient to realize all reversible circuits of $n$ variables. It is a minimal library of gates for binary reversible logic circuits. We also analyze the complexity of the syntheses.

Keywords: Reversible logic; Syntheses; Permutation

1. Introduction

Reversible logic plays an important role in quantum computing. Several papers have been recently published on universality of sets of reversible gates [1–7], both binary and multiple-valued. However, an important fundamental unsolved problem in binary logic is this: “what is the minimum set of gates that are universal for $n$-qubit circuits without ancillae bits”. (ancillae bits are additional bits added to the circuit and set to initial constant values, they are undesirable in quantum computing where every bit is costly and thus attempted to be spared). In their seminal paper, Shende et al. [1] proved that all those binary reversible circuits that are described by even permutations can be realized using the three gate library. These gates are: Controlled-NOT, Toffoli, and Not. They proved also that exactly one ancillae bit is needed (with a constant input) to be able to realize an arbitrary permutation (even or odd), thus corresponding to arbitrary $n \times n$ reversible circuit. It was next observed that by adding more gates to their library, every circuit can be realized using a library of 4 gates. However, a question arises: what is the minimal library of gates that allows us to realize an arbitrary circuit without ancillae bits. This problem is important for minimal quantum circuit design. We prove below that a library of 2 gates is sufficient to realize all reversible circuits of $n$ variables without additional bits. Also, we prove that no universal library with less than two gates is possible. Thus, our result

\footnote{This work was supported by the NNSF of China under Grant 60773205 and the Fund of Cultivating Leading Scholars in UESTC.}

\ast Corresponding author.

E-mail address: song@ee.pdx.edu (X. Song).
can be compared to proving in past that NAND is a smallest universal library for binary Boolean logic. Although these kinds of results are of theoretical value in practical design since much larger libraries are used, they are nevertheless useful in classical logic theory. Thus we believe that the presented result can be useful to define new, larger families of universal gates for n-bit reversible logic design.

2. Basic definitions

Let $B = \{0, 1\}$. A Boolean logic function $f$ with $n$ input variables, $B_1, \ldots, B_n$, and $n$ output variables, $P_1, \ldots, P_n$, is a function $f: B^n \rightarrow B^n$, where $\langle B_1, \ldots, B_n \rangle \in B^n$ is the input vector and $\langle P_1, \ldots, P_n \rangle \in B^n$ is the output vector. We use lower letters $b_i$ and $p_i$ to represent the variable values.

A Boolean logic function $f$ is a reversible circuit if it is a one-to-one, onto function (bijection). A reversible logic circuit with $n$ inputs and $n$ outputs is also called a $n \times n$ reversible gate.

Now we introduce permutation group and its relationship with reversible circuits. Let $M = \{1, 2, \ldots, m\}$. A bijection (one-to-one, and onto mapping) of $M$ onto itself is called a permutation on $M$. The set of all permutations on $M$ forms a group [8], under composition of mappings, called a symmetric group on $M$, denoted by $S_m$ [9]. If $M$ is a set of all $2^n$ binary vectors with length $n$, the symmetric group on $M$ is denoted by $S_{2^n}$. A permutation group is just a subgroup [8] of a symmetric group.

A mapping $a: M \rightarrow M$ can be written as $a = (1, 2, \ldots, m)$. We use the notation of a product of disjoint cycles [10]. For example, $\langle 1, 2, 3, 4, 5, 6, 7, 8 \rangle$ will be written as $(3, 4)(7, 8)$. The identity mapping “()” (directly wiring) is called the unity element in a permutation group. As convention, a product $^1 a * b$ of two permutations $a$ and $b$ means applying mapping $a$ before $b$, which corresponds to cascading gates $a$ and $b$.

To establish a one-to-one correspondence between a reversible circuit and a permutation, we encode an $n$-bit binary input (output) vector $\langle B_n, B_{n-1}, \ldots, B_1 \rangle_2$ as a unique decimal integer value index $\langle B_n, B_{n-1}, \ldots, B_1 \rangle_2 = 1 + B_1 + B_2 \cdot 2^1 + B_3 \cdot 2^2 + \cdots + B_n \cdot 2^{n-1}$. Using the integer coding, we consider a permutation as a bijection function $f: \{1, 2, 3, \ldots, 2^n\} \rightarrow \{1, 2, 3, \ldots, 2^n\}$. Cascading two gates is equivalent to multiplying two permutations. In what follows, we will not distinguish an $n \times n$ reversible gate from a permutation in $S_{2^n}$. Let $|S|$ be the size of $S$.

A synthesis of a reversible gate $g$ means that there are $m$ known gates such that $g$ is the cascading of these $m$ gates. An $n$-library is the set of $n \times n$ reversible gates which are used to synthesize $n \times n$ reversible gates, denoted as $n_L$, or simply as $L$. We use $T(L)$ to denote a set of all $n \times n$ reversible gates that can be synthesized using gates from library $L$, namely, $T(L) = \{ g \in S_{2^n} | g = () \lor \exists a_i \in L \text{ such that } g = a_1 \cdots a_k \}$. A universal library $L$ satisfies that all $n \times n$ reversible gates can be synthesized by $L$, i.e., $T(L) = S_{2^n}$. A minimal universal library $L$ is a universal library such that there does not exist a universal library $L'$ such that $|L'| < |L|$.

A group $G$ generated by a subset $L$ of $S_{2^n}$ is defined as:

$G = G(L) = \{ g \in S_{2^n} | g = () \lor \exists a_i \in L \text{ such that } g = a_1 \cdots a_k \}$, which is $T(L)$.

3. Minimal universal library

In this section, we construct a new $n$-library and we show that it is minimal universal library. In other words, all $n \times n$ reversible circuits can be synthesized from this library.

From the definitions of $T(L)$ and $G(L)$, we know that a set of all $n \times n$ reversible circuits that can be synthesized using gates from library $L$ is the group generated by $L$, namely $T(L) = G(L)$. For this reason, we can use group theory to prove some properties of reversible logic circuits.

A general Toffoli gate [1,4,6], $T_0$, is defined as: $P_n = B_n, \ldots, P_1 = B_1, \ldots, P_2 = B_2, P_1 = B_1 \oplus B_2 B_3 \cdots B_n$. We introduce a new gate, named full cycle gate (FC), as follows: $P_n = B_n \oplus B_1 \cdots B_{n-1}, \ldots, P_1 = B_1 \oplus B_2 \cdots B_{i-1}, \ldots, P_2 = B_2 \oplus B_1, P_1 = \overline{B_1}$.

Lemma 1. The corresponding permutation of Toffoli gate is: $T_0 = (2^n - 1, 2^n)$.

---

[1] We use * to denote permutation product to differentiate it from other operators, the dot · is used for multiplication.
Proof. Toffoli gate only exchanges the two input values $\langle 1, \ldots, 1, 1, 0 \rangle$ and $\langle 1, \ldots, 1, 1, 1 \rangle$. The remaining values are mapped identically. Notice that index $\langle 1, \ldots, 1, 1, 0 \rangle_2 = 2^n - 1$, index $\langle 1, \ldots, 1, 1, 1 \rangle_2 = 2^n$. Therefore, $To = (2^n - 1, 2^n)$. □

Theorem 1. The corresponding permutation of gate FC is: $FC = (1, 2, 3, \ldots, 2^n)$.

Proof. write $v = \text{index}(b_n, b_{n-1}, \ldots, b_2, b_1)_2$, and suppose that there are $k$ conjunctive 1's from lower bit $b_1$, i.e., $b_1 = \cdots = b_k = 1, b_{k+1} = 0$. $FC(v)$ represents the image of $v$ under $FC$.

Case 1: $k = n$.

Since $v = 2^n$, according to the definition, we have $p_1 = \overline{b_1} = 0, p_i = b_i \oplus b_1 \cdots b_{i-1} = 0$, for $2 \leq i \leq n$. Thus $FC(2^n) = 1$.

Case 2: $1 \leq k < n$.

Like Case 1, we have $p_1 = \cdots = p_k = 0$, but $p_{k+1} = b_{k+1} \oplus b_1 \cdots b_k = 1 = b_{k+1} + 1$, and $p_j = b_j$, for $k + 1 \leq j \leq n$. Therefore, $FC(v) = v + 1$.

Case 3: $k = 0$.

Since $b_1 = 0$, then $p_1 = b_1 = 1 = b_1 + 1$, and $p_j = b_j$, for $2 \leq j \leq n$. Thus, $FC(v) = v + 1$.

Combining these three cases, we have $FC = (1, 2, 3, \ldots, 2^n)$. □

Lemma 2. Let $g = (1, 2, \ldots, m - 1, m)$ and $f = (m - 1, m)$ be two permutations. Then we have $(j, j + 1) = g^{m-(j+1)} * f * g^{j+1}$, for any $1 \leq j \leq m - 2$.

Before proving this Lemma, we give some notations.

$u \rightarrow v \rightarrow w \rightarrow x$ represents number $u$ mapped to number $v$ via $g^{m-(j+1)}$, $v$ mapped to number $w$ via $f$ and $w$ mapped to number $x$ via $g^{j+1}$. So $x$ is the image of $u$ under $g^{m-(j+1)} * f * g^{j+1}$. $u, v, w, x$ are numbers mod $m$ (but we still write $m$ as $m$ not 0), i.e., $m + r = r$.

Proof. We analyze the image of $y$ under $g^{m-(j+1)} * f * g^{j+1}$, for any $1 \leq y \leq m - 2$.

Case 1: $y = j$, then $j \rightarrow j + m - (j + 1) = m - 1 \rightarrow m + j + 1 = j + 1$;

Case 2: $y = j + 1$ then $j + 1 \rightarrow j + 1 + m - (j + 1) = m \rightarrow m - 1 \rightarrow m - 1 + j + 1 = j$;

Case 3: $y \neq j$ and $y \neq j + 1$. These conditions imply that $y + m - (j + 1) \neq m - 1$, and $y + m - (j + 1) \neq m$.

Therefore $y \rightarrow y + m - (j + 1) \rightarrow y + m - (j + 1) \rightarrow y + m - (j + 1) + j + 1 = y + m = y$.

Combining these three cases, we have $g^{m-(j+1)} * f * g^{j+1} = (j, j + 1)$. □

Notice: Lemma 2 tells that any consecutive 2-cycle $(j, j + 1)$ can be represented by $m$ permutations $(1, 2, \ldots, m)$ and one $(m - 1, m)$.

Lemma 3 ([9,10]). $S_m$ can be generated by $(1, 2), (2, 3), \ldots, (m - 1, m)$.

Now we define our new universal library $L = \{To, FC\}$. By the following theorem, we prove that all $n \times n$ reversible circuits can be synthesized from this library.

Lemma 4. $G(L) = S_{2^n}$.

Proof. Set $m = 2^n$. Since Lemma 2, $(1, 2), (2, 3), \ldots, (m - 2, m - 1)$ can be generated by $To$ and $FC$. Using Lemma 3 and $To = (m - 1, m)$, we have $S_{2^n}$ can be generated by $To$ and $FC$. □

Theorem 2. $L = \{To, FC\}$ is a minimal universal library ($n \geq 2$).

Proof. According to the definition of $T(L)$ and $G(L)$, and Lemma 4, $L$ is a universal library.

Suppose that $L$ is not a minimal universal library. Since $|L| = 2$, then there exists a gate $g$ such that $S_{2^n}$ can be generated by $g$. Therefore, there are two integers $r1$ and $r2$ such that $(1, 2) = g^{r1}$, and $(2, 3) = g^{r2}$. Then $(1, 2) * (2, 3) = g^{r1 + r2} = (2, 3) * (1, 2)$. But in fact, $(1, 2) * (2, 3) = (1, 3, 2), (2, 3) * (1, 2) = (1, 2, 3) \neq (1, 2) * (2, 3)$. This contradiction shows that $L$ is a minimal universal library. □

Notice that minimal universal libraries are not unique. For example $\{To * FC, FC\}$ is also a minimal universal library.
4. Complexity of realization

In this section, we will analyze the complexity of realization using the library \(L\) to realize all reversible circuits. We only consider one aspect: the radium of the library \(L\). The radium of a library \(L\) refers to a minimum number \(R(L)\) satisfying that for any reversible circuit \(f\) in \(T(L)\), there exist \(R(L)\) gates or less in \(L\) (can be repeated) such that \(f\) is a cascading of these gates. We denote \(NUM_L(f)\) as a minimum number satisfying that there are at least \(NUM_L(f)\) gates in \(L\) such that \(f\) is a cascading of these gates. Obviously, \(R(L) = \max\{NUM_L(f)\mid f \in T(L)\}\).

Through the direct calculation, we have the following lemma:

**Lemma 5.** 1. \((a_1, a_2, \ldots, a_{s-1}, a_s) = (a_{s-1}, a_s) \ast (a_1, a_2, \ldots, a_{s-1})\), and
2. \((j, j + r) = (j, j + 1) \ast (j + 1, j + 2) \ast \cdots \ast (j + r - 1, j + r) \ast (j + r - 2, j + r - 1) \ast \cdots \ast (j, j + 1)\).

The following proposition is just a different form of a cycle permutation. It will also be repeatedly used in the proof of **Lemma 7**.

**Proposition 1.** \((a_1, a_2, \ldots, a_{s-1}, a_s) = (a_2, \ldots, a_{s-1}, a_s, a_1) = (a_3, \ldots, a_{s-1}, a_s, a_1, a_2) = \cdots = (a_s, a_1, \ldots, a_{s-2}, a_{s-1})\).

**Lemma 6.** For any two permutation \(p_1\) and \(p_2\),

\[NUM_L(p_1 \ast p_2) \leq NUM_L(p_1) + NUM_L(p_2).\]

**Proof.** Directly from the definition of the function \(NUM_L\). \(\square\)

**Lemma 7.** Consider library \(L_1 = \{(1, 2), (2, 3), \ldots, (m-1, m)\}\).

1. Let permutation \(f = (a_1, a_2, \ldots, a_{2k-1}, a_{2k})\) and \([b_1, b_2, \ldots, b_k, \ldots, b_{2k}]\) is the increasing order sorted sequence of \(a_1, a_2, \ldots, a_{2k-1}, a_{2k}\). Then

\[NUM_{L_1}(f) \leq 2[(b_{2k} + b_{2k-1} + \cdots + b_{k+1}) - (b_1 + b_2 + \cdots + b_k)] - k,\]

(1)

2. Let permutation \(h = (a_1, a_2, \ldots, a_{2k+1})\) and \([b_1, b_2, \ldots, b_k, \ldots, b_{2k+1}]\) is the increasing order sorted sequence of \(a_1, a_2, \ldots, a_{2k}, a_{2k+1}\). Then

\[NUM_{L_1}(h) \leq 2[(b_{2k+1} + b_{2k} + \cdots + b_{k+2}) - (b_1 + b_2 + \cdots + b_k)] - (k + 1).\]

(2)

**Proof.** We prove this lemma by induction on \(k\).

First, \(k = 1\). We prove that \(NUM_{L_1}((j, j + r)) = 2r - 1\). For any number from \(1\) to \(m - 1\), under the action of any 2-cycle permutation in \(L_1\), there is at most only one number increasing one. So, in order to increase number \(j\) to \(j + r\) we need \((j, j + 1) \ast (j + 1, j + 2) \ast \cdots \ast (j + r - 1, j + r)\). Similarly, in order to decrease \(j + r\) to \(j\), we need \((j + r - 1, j + r) \ast (j + r - 2, j + r - 1) \ast \cdots \ast (j, j + 1)\). Also \((j, j + r) = (j, j + 1) \ast (j + 1, j + 2) \ast \cdots \ast (j + r - 1, j + r) \ast (j + r - 2, j + r - 1) \ast \cdots \ast (j, j + 1)\). Therefore \(NUM_{L_1}((j, j + r)) = 2r - 1\). Let \(b_1 = j, b_2 = j + r\), then \(NUM_{L_1}(f) = 2(b_2 - b_1) - 1\), i.e., (1) holds. Owing to **Proposition 1**, we can assume that \(a_3 = b_3\), the biggest number. If \(a_2 = b_2\), then \(NUM_{L_1}((a_1, a_2, a_3)) = NUM_{L_1}((b_1, b_2, b_3)) = NUM_{L_1}((b_2, b_3) \ast (b_1, b_2)) \leq NUM_{L_1}((b_2, b_3)) + NUM_{L_1}((b_1, b_2)) = 2(b_3 - b_2) - 1 + 2(b_2 - b_1) - 1 = 2(b_3 - b_1) - 2\). Thus, (2) holds. If \(a_1 = b_2\), then \(NUM_{L_1}((a_1, a_2, a_3)) = NUM_{L_1}((b_2, b_1, b_3)) = NUM_{L_1}((b_2, b_1) \ast (b_2, b_3)) \leq NUM_{L_1}((b_2, b_1)) + NUM_{L_1}((b_2, b_3)) = 2(b_2 - b_1) - 1 + 2(b_3 - b_2) - 1 = 2(b_3 - b_1) - 2\). Thus, (2) holds. Second, suppose that (1) and (2) hold for \(k\). We prove (1) and (2) for \(k + 1\). In \(f = (a_1, a_2, \ldots, a_{2k+1}, a_{2k+2})\), according to **Proposition 1**, we can set \(a_{2k+1} = b_{k+1}\).

**Case 1.** \(a_{2k+2} > b_{k+1}\), then

\[NUM_{L_1}(f) = NUM_{L_1}((a_{2k+1}, a_{2k+2}) \ast (a_1, a_2, \ldots, a_{2k}, a_{2k+1})) \leq NUM_{L_1}((a_{2k+1}, a_{2k+2})) + NUM_{L_1}((a_1, a_2, \ldots, a_{2k}, a_{2k+1})) \leq 2(a_{2k+2} - b_{k+1}) - 1 + \cdots + 2[(b_{2k+2} + b_{2k+1} + \cdots + b_{k+2} - a_{2k+2}) - (b_1 + b_2 + \cdots + b_k)] - k \leq 2[(b_{2k+2} + b_{2k+1} + \cdots + b_{k+2}) - (b_1 + b_2 + \cdots + b_k)] - (k + 1).

Thus (1) holds.
Case 2: $a_{2k+2} < b_{k+1}$, then

$$
\text{NUM}_{L,1}(f) = \text{NUM}_{L,1}((a_{2k+1}, a_{2k+2}) \ast (a_1, a_2, \ldots, a_{2k}, a_{2k+1}))
\leq \text{NUM}_{L,1}((a_{2k+1}, a_{2k+2})) + \text{NUM}_{L,1}((a_1, a_2, \ldots, a_{2k+1}, a_{2k}))
\leq 2(b_{k+1} - a_{2k+2}) - 1 + 2[(b_{2k+2} + b_{2k+1} + \cdots + b_{k+3})
-(b_1 + b_2 + \cdots + b_k + b_{k+1})] - (k + 1).
$$

Thus (1) holds.

Now we prove (2).

In $h = (a_1, a_2, \ldots, a_{2k+2}, a_{2k+3})$, according to Proposition 1, we can set $a_{2k+2} = b_{k+2}$.

Case 1: $a_{2k+3} > b_{k+2}$, then

$$
\text{NUM}_{L,1}(h) = \text{NUM}_{L,1}((a_{2k+2}, a_{2k+3}) \ast (a_1, a_2, \ldots, a_{2k+1}, a_{2k+2}))
\leq \text{NUM}_{L,1}((a_{2k+2}, a_{2k+3})) + \text{NUM}_{L,1}((a_1, a_2, \ldots, a_{2k+1}, a_{2k}))
\leq 2(a_{2k+3} - b_{k+2}) - 1 + 2[(b_{2k+3} + b_{2k+2} + \cdots + b_{k+2} - a_{2k+3})
-(b_1 + b_2 + \cdots + b_k + b_{k+1})] - (k + 1)
\leq 2((b_{2k+2} + b_{2k+1} + \cdots + b_{k+3}) - (b_1 + b_2 + \cdots + b_k + b_{k+1})) - (k + 2).
$$

Thus (2) holds.

Case 2: $a_{2k+3} < b_{k+2}$, then

$$
\text{NUM}_{L,1}(h) = \text{NUM}_{L,1}((a_{2k+2}, a_{2k+3}) \ast (a_1, a_2, \ldots, a_{2k+1}, a_{2k+2}))
\leq \text{NUM}_{L,1}((a_{2k+2}, a_{2k+3})) + \text{NUM}_{L,1}((a_1, a_2, \ldots, a_{2k+1}, a_{2k+2}))
\leq 2(b_{k+2} - a_{2k+3}) - 1 + 2[(b_{2k+3} + b_{2k+2} + \cdots + b_{k+3})
-(b_1 + b_2 + \cdots + b_k + b_{2k+3})] - (k + 1)
\leq 2((b_{2k+2} + b_{2k+1} + \cdots + b_{k+3}) - (b_1 + b_2 + \cdots + b_k + b_{k+1})) - (k + 2).
$$

Thus (2) holds.

Combining these two steps, Lemma 7 is correct. □

**Theorem 3.** Let library $L_1 = \{(1, 2), (2, 3), \ldots, (m - 1, m)\}$, then $R(L_1) \leq (m - 1)m/2$.

**Proof.** Case 1: $m = 2k$ (even number).

For any permutation $g$ in $S_m$, since $g$ is the product of disjoint cycles, using Lemmas 6 and 7, we have:

$$
\text{NUM}_{L,1}(g) \leq [2(m - 1) - 1] + [2((m - 1) - 2) - 1] + \cdots + [2((k + 1) - k) - 1].
$$

(When $g$ is a product of $k$-cycles, the hand reaches maximum. E.g., $g = (1, m) \ast (2, m - 1) \ast \cdots \ast (k, k + 1)) = 2k^2 - k = (m - 1)m/2$.

Case 2: $m = 2k + 1$ (odd number). Similar to case 1,

$$
\text{NUM}_{L,1}(g) \leq [2(m - 1) - 1] + [2(m - 1) - 2] + \cdots + [2(k + 2 - k) - 1]
= 2k^2 + k = (m - 1)m/2. \quad \square
$$

**Theorem 4.** Consider the library $L_2 = \{(1, 2, \ldots, m), (m - 1, m)\}$ and $T(L_2) = S_m$, we have:

$R(L_2) \leq (m - 1)m(m + 1)/2$. Specially, when $m = 2^n$, $L_2 = L$, $R(L) \leq (2^n - 1)2^n(2^n + 1)/2$.

**Proof.** Since Lemmas 2 and 5 (2), we have

$$
\text{NUM}_{L,2}((j, j + 1)) \leq m + 1, \text{ for } 1 \leq j \leq m - 1. \text{ Using Theorem 3,}
$$

$$
R(L_2) \leq ((m - 1)m/2)(m + 1) = (m - 1)m(m + 1)/2.
$$

Specially, when $m = 2^n$, $L_2 = L$, $R(L) \leq (2^n - 1)2^n(2^n + 1)/2. \quad \square$
5. Conclusion

We constructed a new $n \times n$ reversible gate and derived the corresponding permutation. We built a minimal universal library which includes only two gates such that all $n \times n$ reversible circuits can be synthesized by these two gates without ancilla bits. We showed constructively a minimal universal set of reversible binary gates and proved its universality and minimality. We also analyze the complexity of the syntheses.

References