Universal Test Sets for Reversible Circuits
(Extended Abstract)

Satoshi Tayu, Shota Fukuyama, and Shuichi Ueno

Department of Communications and Integrated Systems
Tokyo Institute of Technology, Tokyo 152-8550-S3-57, Japan
{tayu,ueno}@lab.ss.titech.ac.jp

Abstract. A set of test vectors is complete for a reversible circuit if it covers all stuck-at faults on the wires of the circuit. It has been known that any reversible circuit has a surprisingly small complete test set, while it is NP-hard to generate a minimum complete test set for a reversible circuit. A test set is universal for a family of reversible circuits if it is complete for any circuit in the family. We show minimum universal test sets for some families of CNOT circuits.

1 Introduction

The power consumption and heat dissipation are major issues for VLSI circuits today. Landauer [3] showed that conventional irreversible circuits necessarily dissipate heat due to the erasure of information. Bennett [1] showed, however, that heat dissipation can be avoided if computation is carried out without losing any information. This motivates the study of reversible circuits. Furthermore, reversible circuits have potential applications in nanocomputing [4], digital signal processing [8], and quantum computing [5].

In order to ensure the functionality and durability of reversible circuits, testing and failure analysis are extremely important during and after the design and manufacturing. It has been known that testing of reversible circuits is relatively easier than conventional irreversible circuits in the sense that few test vectors are needed to cover all stuck-at faults, while it is NP-hard to generate a minimum complete test set for a reversible circuit. This paper considers universal test sets for some families of reversible circuits.

1.1 Reversible Circuits

A function $f{:}\{0,1\}^n \to \{0,1\}^n$ is called a *permutation* if it is bijective. A permutation f is *linear* if $f(\boldsymbol{x} \oplus \boldsymbol{y}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{y})$ for any $\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$, where $\oplus$ is the bitwise XOR operation.

A gate is *reversible* if the Boolean function it computes is a permutation. If a reversible gate has k input and output wires, it is called a $k \times k$ *gate*. A circuit is *reversible* if all gates are reversible and are interconnected without fanout or feedback. If a reversible circuit has n input and output wires, it is called an $n \times n$ *reversible circuit*.

M.T. Thai and S. Sahni (Eds.): COCOON 2010, LNCS 6196, pp. 348–357, 2010.

An $n \times n$ reversible circuit is constructed by starting with n wires, forming the basic circuit, and iteratively concatenating a reversible gate to some subset of the output wires of the previous circuit. Thus, a reversible circuit C can be represented as a sequence of reversible gates G_i: $C = G_1 G_2 \dots G_m$.

1.2 Fault Testing

We focus our attention on detecting stuck-at faults in a reversible circuit C which fix the values of wires to either 0 or 1. Let $W(C)$ be the set of all wires of C. $W(C)$ consists of all output wires of C and input wires to the gates in C. $W(C)$ is the set of all possible fault locations in C. For an $n \times n$ reversible circuit C, a *test* is an input vector in $\{0,1\}^n$. A test set T is said to be *complete* for C if for every possible single or multiple stuck-at fault on $W(C)$, there exists a test $\boldsymbol{t} \in T$ which detects the fault. It is known that there exists a complete test set for any reversible circuit [6]. Let $\tau(C)$ be the minimum size of a complete test set for a reversible circuit C. It is also known that computing $\tau(C)$ is NP-hard [9], while $\tau(C) = O(\log |W(C)|)$ for any reversible circuit C [6], and there exists a reversible circuit C such that $\tau(C) = \Omega(\log \log |W(C)|)$ [9].

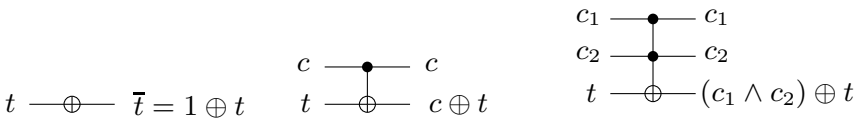
1.3 Universal Test Sets

Let $\mathcal{D}_n$ be the set of all $n \times n$ reversible circuits. A test set $T \subseteq \{0,1\}^n$ is said to be *universal* for $\mathcal{D} \subseteq \mathcal{D}_n$ if T is complete for any circuit in $\mathcal{D}$. It is known that there exists a universal test set for any $\mathcal{D} \subseteq \mathcal{D}_n$[6]. Let $\sigma(\mathcal{D})$ be the minimum size of a universal test set for $\mathcal{D}$. Since the value of a wire of an $n \times n$ reversible circuit is set to 0 by exactly 2^{n-1} input vectors, and to 1 by the remaining 2^{n-1} input vectors, we have the following. (See Theorem IV in Section 2)

Theorem I. [6] $\sigma(\mathcal{D}) \leq 2^{n-1} + 1$ *for any* $\mathcal{D} \subseteq \mathcal{D}_n$. □

1.4 CNOT Circuits

A *k-CNOT gate* is a $(k+1) \times (k+1)$ reversible gate. It passes some k inputs, referred to as control bits, to the outputs unchanged, and inverts the remaining input, referred to as target bit, if the control bits are all 1. The 0-CNOT gate is just an ordinary NOT gate. A *CNOT gate* is a k-CNOT gate for some k. Some CNOT gates are shown in Fig. 1, where a control bit and target bit are denoted by a black dot and ring-sum, respectively. A *CNOT circuit* is a reversible circuit consisting of only CNOT gates. Any Boolean function can be implemented by a CNOT circuit, since the 2-CNOT gate can implement the NAND function. Any permutation can also be implemented by a CNOT circuit. A k-CNOT circuit is a CNOT circuit consisting of only k-CNOT gates. A 1-CNOT circuit is called a *linear reversible circuit*. A linear reversible circuit computes a linear permutation, and any linear permutation can be implemented by a linear reversible circuit [7]. The linear reversible circuits are an important class of reversible circuits with applications to quantum computation [7].



(a) 0-CNOT gate. (b) 1-CNOT gate. (c) 2-CNOT gate.

Fig. 1. CNOT gates

Let $\mathcal{C}_n$ be the set of all $n \times n$ CNOT circuits. Let $\mathcal{C}_{n,k\geq i}$ be the set of all $n \times n$ CNOT circuits consisting of k-CNOT gates for $k \geq i$, $\mathcal{C}_{n,k\leq i}$ be the set of all $n \times n$ CNOT circuits consisting of k-CNOT gates for $k \leq i$, and $\mathcal{C}_{n,k=i} = \mathcal{C}_{n,k\geq i} \cap \mathcal{C}_{n,k\leq i}$. Notice that $\mathcal{C}_n = \mathcal{C}_{n,k\geq 0}$. The following is immediate from Theorem I.

Theorem II. [6] $\sigma(\mathcal{C}_{n,k\leq 2}) \leq \sigma(\mathcal{C}_n) \leq 2^{n-1} + 1$. □

Since the set of n unit vectors is universal for $\mathcal{C}_{n,k\geq 2}$, we have the following.

Theorem III. [2] $\sigma(\mathcal{C}_{n,k\geq 2}) \leq n$. □

1.5 Our Results

We show the following theorems complementing the results in the previous section.

Theorem 1. $\sigma(\mathcal{C}_{n,k=1}) = n + 1$. □

Theorem 2. $\sigma(\mathcal{C}_{n,k\leq 1}) = n + 1$. □

Theorem 3. $\sigma(\mathcal{C}_{n,k\leq 2}) = 2^{n-1} + 1$. □

Corollary 1. $\sigma(\mathcal{C}_n) = 2^{n-1} + 1$. □

Theorem 4. $\sigma(\mathcal{C}_{n,k=b}) = \lceil n/(b-1) \rceil$ *for any* $n \geq 3$ *and* $2 \leq b \leq n-1$. □

Theorem 5. $\sigma(\mathcal{C}_{n,k\geq b}) = \lceil n/(b-1) \rceil$ *for any* $n \geq 3$ *and* $2 \leq b \leq n-1$. □

Corollary 2. $\sigma(\mathcal{C}_{n,k\geq 2}) = n$ *for any* $n \geq 2$. □

Theorem 6. $\sigma(\mathcal{C}_{n,k\geq 1}) = 2^{n-1} + 1$. □

Theorem 1 shows that the linear reversible circuits have a surprisingly small universal test set. Theorem 2 is a generalization of Theorem 1. Theorems 1 and 2 are proved in Sections 3 and 4, respectively.

Corollary 1 is immediate from Theorem 3. Theorem 3 and Corollary 1 show that the equalities hold in the inequalities of Theorem II. They also show that the size of a minimum universal test set for the general CNOT circuits is exponentially large, as suspected. Theorem 3 is proved in Section 5.

Corollary 2 is a special case of Theorem 5 when $b = 2$, which shows that the equality holds in the inequality of Theorem III. Theorems 4 and 5 are proved in Section 6. (An outline of the proof is presented in the extended abstract, due to space limitations.)

Theorem 6 shows that $b \geq 2$ is essential for Theorem 5. Theorem 6 is proved in Section 7.

It is an interesting open question to find a polynomial time algorithm generating a complete test set of size $O(\log |W(C)|)$ for a reversible circuit C.

2 Preliminaries

A wire w of a reversible circuit C is said to be *i-controllable* by a test set T if the value of w can be set to i by a vector of T ($i = 0, 1$). A wire w is said to be *controllable* by T if w is both 0- and 1-controllable by T. A reversible circuit C is said to be *i-controllable* by T if each wire of C is i-controllable by T ($i = 0, 1$). A reversible circuit C is said to be *controllable* by T if C is both 0- and 1-controllable by T. The following characterization for complete test sets is shown in [6].

Theorem IV. [6] *A test set T for a reversible circuit C is complete if and only if C is controllable by T.* □

A test set $T \subseteq \{0, 1\}^n$ is said to be *i-universal* for $\mathcal{D} \subseteq \mathcal{D}_n$ if every circuit of $\mathcal{D}$ is i-controllable by T ($i = 0, 1$). It should be noticed that T is a universal test set for $\mathcal{D}$ if and only if T is both 0- and 1-universal for $\mathcal{D}$.

A family $\mathcal{D}$ of reversible circuits is said to be *hereditary* if $\mathcal{D}$ satisfies the following property: if $C = G_1 G_2 \dots G_m$ is in $\mathcal{D}$ then a subcircuit $C' = G_1 G_2 \dots G_i$ is also in $\mathcal{D}$ for any $i \leq m$. Notice that $\mathcal{C}_{n,k \geq i}$, $\mathcal{C}_{n,k \leq i}$, and $\mathcal{C}_{n,k=i}$ are hereditary for any $n \geq 1$ and $i \geq 0$. Let $C = G_1 G_2 \dots G_m$ be a circuit in a hereditary family $\mathcal{D}$ of reversible circuits, and w be any wire of C. If w is an output wire of gate G_j then w is an output wire of a subcircuit $C' = G_1 G_2 \dots G_j$. Since C' is also in $\mathcal{D}$, we have the following.

Lemma 1. *A test set T is i-universal for a hereditary family $\mathcal{D}$ of reversible circuits if and only if every output wire of any reversible circuit in $\mathcal{D}$ is i-controllable by T ($i = 0, 1$).* □

3 Proof of Theorem 1

We consider that $\{0, 1\}^n$ is an n-dimensional vector space of column vectors over GF(2). The action of an $n \times n$ linear reversible circuit C can be represented by a linear transformation over $\{0, 1\}^n$, and represented as multiplication by a non-singular $n \times n$ matrix $A(C)$ over $\{0, 1\}$:

$$A(C)\boldsymbol{x} = \boldsymbol{y},$$

where $\boldsymbol{x}$ [$\boldsymbol{y}$] is a column vector in $\{0,1\}^n$ whose i-th entry contains the value of the i-th bit of the input [output] of C. A 1-CNOT gate G is denoted by $G[c,t]$, where c and t are the control bit and target bit of G, respectively. The action of a 1-CNOT gate corresponds to multiplication by an elementary matrix, which is the identity matrix with one off-diagonal entry set to one. The elementary matrix $A(G)$ for a 1-CNOT gate $G[c,t]$ is the identity matrix with (t,c)-entry set to one. It should be noted that the multiplication by $A(G)$ performs a row operation, the addition of the c-th row of a matrix to the t-th row. Applying a series of 1-CNOT gates corresponds to multiplying an input vector by a series of elementary matrices, or equivalently to performing a series of row operations on the input vector. Let $C = G_1G_2 \dots G_m$ be an $n \times n$ linear reversible circuit represented as a sequence of 1-CNOT gates G_i, and A_i be an $n \times n$ elementary matrix for G_i. Then the action of C is represented by

$$A_m A_{m-1} \cdots A_1 \boldsymbol{x} = \boldsymbol{y},$$

where $\boldsymbol{x}$ and $\boldsymbol{y}$ are input and output vectors in $\{0,1\}^n$. In other words,

$$A(C) = A_m A_{m-1} \cdots A_1.$$

Let $T = \{\boldsymbol{t}_1, \boldsymbol{t}_2, \dots, \boldsymbol{t}_s\} \subseteq \{0,1\}^n$, and $\boldsymbol{t}_i = (t_{1,i}, t_{2,i}, \cdots, t_{n,i})'$, where $\boldsymbol{v}'$ is the transpose of $\boldsymbol{v}$. Define a matrix

$$M(T) = \begin{bmatrix} t_{1,1} & t_{1,2} & \dots & t_{1,s} \\ t_{2,1} & t_{2,2} & \dots & t_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n,1} & t_{n,2} & \dots & t_{n,s} \end{bmatrix}$$

consisting of column vectors $\boldsymbol{t}_1, \boldsymbol{t}_2, \dots, \boldsymbol{t}_s$.

We prove the theorem by a series of lemmas.

Lemma 2. *A set of tests $T \subseteq \{0,1\}^n$ is 1-universal for $\mathcal{C}_{n,k=1}$ if and only if T contains a basis for $\{0,1\}^n$.*

Proof. Suppose that T contains a basis for $\{0,1\}^n$. Then $r(M(T)) = n$, where $r(B)$ is the rank of a matrix B. Let C be a linear reversible circuit. Then the i-th column of a matrix $A(C)M(T)$ is the output vector for $\boldsymbol{t}_i$. Since $A(C)$ is non-singular, $r(A(C)M(T)) = n$, i.e., every row of $A(C)M(T)$ contains a one element. Therefore, every output wire of C is 1-controllable by T. Thus from Lemma 1, T is 1-universal for $\mathcal{C}_{n,k=1}$.

Suppose contrary that T does not contain a basis for $\{0,1\}^n$. Then, $r(M(T)) < n$, and there exists a sequence of elementary row operations of $M(T)$ resulting in a zero row vector $\mathbf{0} = (0,0,\dots,0)$. Let $A_1, A_2, \dots, A_m$ be elementary matrices corresponding to the sequence of such elementary row operations, and G_i be a 1-CNOT gate corresponding to A_i $(1 \leq i \leq m)$. Then for a linear reversible circuit $C = G_1G_2 \dots G_m$, the i-th column of a matrix $A_m A_{m-1} \cdots A_1 M(T)$ is the output for $\boldsymbol{t}_i$. Since a row of $A_m A_{m-1} \cdots A_1 M(T)$ is a zero row vector, the output wire of C corresponding to the zero row vector is not 1-controllable by T. Thus from Lemma 1, T is not 1-universal for $\mathcal{C}_{n,k=1}$. □

Lemma 3. *No basis for* $\{0,1\}^n$ *is* 0*-universal for* $\mathcal{C}_{n,k=1}$.

Proof. Let T be a basis for $\{0,1\}^n$. Since $M(T)$ is non-singular, there exists a sequence of elementary row operations of $M(T)$ resulting in a sum row vector $\mathbf{1} = (1,1,\ldots,1)$. Let $A_1, A_2, \ldots, A_m$ be elementary matrices corresponding to the sequence of such elementary row operations, and G_i be a 1-CNOT gate corresponding to A_i $(1 \leq i \leq m)$. Then, for a linear reversible circuit $C = G_1 G_2 \ldots G_m$, the i-th column of a matrix $A_m A_{m-1} \ldots A_1 M(T)$ is the output for $\boldsymbol{t}_i$. Since a row of $A_m A_{m-1} \ldots A_1 M(T)$ is a sum row vector, the output wire of C corresponding to the sum row vector is not 0-controllable by T. Thus from Lemma 1, T is not 0-universal for $\mathcal{C}_{n,k=1}$. □

Since a set consisting of just a zero (column) vector is 0-universal for $\mathcal{C}_{n,k=1}$ as easily seen, we have the following.

Lemma 4. *A set of the zero vector and the basis vectors of a basis for* $\{0,1\}^n$ *is a minimum universal test set for* $\mathcal{C}_{n,k=1}$. □

This completes the proof of Theorem 1.

4 Proof of Theorem 2

Since $\sigma(\mathcal{C}_{n,k\leq 1}) \geq \sigma(\mathcal{C}_{n,k=1})$ by definition, $\sigma(\mathcal{C}_{n,k\leq 1}) \geq n+1$ by Theorem 1. Thus, it suffices to show that a set of the zero vector and the basis vectors of a basis for $\{0,1\}^n$ is also a universal test set for $\mathcal{C}_{n,k\leq 1}$.

Let C be a circuit in $\mathcal{C}_{n,k\leq 1}$. We denote a 0-CNOT gate G on bit t by $G[t]$. Let C^+ be a circuit in $\mathcal{C}_{n+1,k=1}$ obtained from C by adding an additional bit $n+1$ and replacing each 0-CNOT gate $G[t]$ of C by a 1-CNOT gate $G[n+1,t]$.

Let $T = \{\boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{t}_2, \ldots, \boldsymbol{t}_n\} \subseteq \{0,1\}^n$, where $\boldsymbol{t}_0 = \mathbf{0}'$, $\{\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots, \boldsymbol{t}_n\}$ is a basis for $\{0,1\}^n$, and $\boldsymbol{t}_i = (t_{1,i}, t_{2,i}, \ldots, t_{n,i})'$. Let $\boldsymbol{t}_i^+ = (t_{1,i}, t_{2,i}, \ldots, t_{n,i}, 1)' \in \{0,1\}^{n+1}$, and $T^+ = \{\boldsymbol{t}_0^+, \boldsymbol{t}_1^+, \boldsymbol{t}_2^+, \ldots, \boldsymbol{t}_n^+\} \subseteq \{0,1\}^{n+1}$. Then

$$M(T^+) = \begin{bmatrix} 0 & t_{1,1} & t_{1,2} & \ldots & t_{1,n} \\ 0 & t_{2,1} & t_{2,2} & \ldots & t_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & t_{n,1} & t_{n,2} & \ldots & t_{n,n} \\ 1 & 1 & 1 & \ldots & 1 \end{bmatrix}.$$

Notice that T^+ is a basis for $\{0,1\}^{n+1}$, since $\{\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots, \boldsymbol{t}_n\}$ is a basis for $\{0,1\}^n$. Notice also that $\boldsymbol{y}_i = (y_{1,i}, y_{2,i}, \ldots, y_{n,i})'$ is the output vector of C for input vector $\boldsymbol{t}_i$ if and only if $\boldsymbol{y}_i^+ = (y_{1,i}, y_{2,i}, \ldots, y_{n,i}, 1)'$ is the output vector of C^+ for input vector $\boldsymbol{t}_i^+$ by the definition of C^+. Thus we have that

$$A(C^+)M(T^+) = \begin{bmatrix} y_{1,0} & y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,0} & y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_{n,0} & y_{n,1} & y_{n,2} & \cdots & y_{n,n} \\ 1 & 1 & 1 & \ldots & 1 \end{bmatrix}.$$

It should be noted that $A(C^+)M(T^+)$ is non-singular since both $A(C^+)$ and $M(T^+)$ are non-singular. It follows that each row of $A(C^+)M(T^+)$ except the last row has a zero element, for otherwise $A(C^+)M(T^+)$ has a sum row vector other than the last row. Thus, every output wire of C is 0-controllable by T, and T is 0-universal for $\mathcal{C}_{n,k\leq 1}$ by Lemma 1. It also follows that each row of $A(C^+)M(T^+)$ has a one element, for otherwise $A(C^+)M(T^+)$ has a zero row vector. Thus, every output wire of C is 1-controllable by T, and T is 1-universal for $\mathcal{C}_{n,k\leq 1}$ by Lemma 1.

Thus, we conclude that T is a universal test set for $\mathcal{C}_{n,k\leq 1}$, which completes the proof of Theorem 2.

5 Proof of Theorem 3

Since $\sigma(\mathcal{C}_{n,k\leq 2}) \leq 2^{n-1}+1$ by Theorem II, it suffices to show the following.

Lemma 5. $\sigma(\mathcal{C}_{n,k\leq 2}) \geq 2^{n-1}+1$.

Proof. Since $\mathcal{C}_{1,k\leq 2} = \mathcal{C}_{1,k=0}$, it is easy to see that $\sigma(\mathcal{C}_{1,k\leq 2}) = 2 = 2^{1-1}+1$. Since $\mathcal{C}_{2,k\leq 2} = \mathcal{C}_{2,k\leq 1}$, we have by Theorem 2 that $\sigma(\mathcal{C}_{2,k\leq 2}) = 2+1 = 2^{2-1}+1$.

We now assume that $n \geq 3$. Let T be a subset of $\{0,1\}^n$ with $|T| \leq 2^{n-1}$. A permutation $f : \{0,1\}^n \to \{0,1\}^n$ is said to be *even* if f can be represented as the product of an even number of transpositions. It is shown in [8] that any even permutation can be implemented by a circuit in $\mathcal{C}_{n,k\leq 2}$. Let $V \subseteq \{0,1\}^n$ be the set of all vectors having one at the n-th entry. Since $|T| \leq 2^{n-1}$ and $|V| = 2^{n-1}$, it is easy to see that there exists an even permutation $f : \{0,1\}^n \to \{0,1\}^n$ such that $f(T) \subseteq V$. Let C be a circuit in $\mathcal{C}_{n,k\leq 2}$ that implements f. Then the n-th bit output wire of C is not 0-controllable by T, and we conclude that T is not a universal test set for $\mathcal{C}_{n,k\leq 2}$ by Lemma 1. Thus, $\sigma(\mathcal{C}_{n,k\leq 2}) \geq 2^{n-1}+1$. □

6 Proof of Theorems 4 and 5

Since $\sigma(\mathcal{C}_{n,k=b}) \leq \sigma(\mathcal{C}_{n,k\geq b})$, it suffices to show the following.

Lemma 6. $\sigma(\mathcal{C}_{n,k\geq b}) \leq \lceil n/(b-1) \rceil$ *for* $n \geq 3$ *and* $2 \leq b \leq n-1$. □

Lemma 7. $\sigma(\mathcal{C}_{n,k=b}) \geq \lceil n/(b-1) \rceil$ *for* $n \geq 3$ *and* $2 \leq b \leq n-1$. □

6.1 Proof of Lemma 6

For $1 \leq j \leq \lceil n/(b-1) \rceil$, define $\boldsymbol{t}_j = (t_{1,j}, t_{2,j}, \ldots, t_{n,j})' \in \{0,1\}^n$ as

$$t_{i,j} = \begin{cases} 1 \text{ if } (j-1)(b-1)+1 \leq i \leq \min\{j(b-1), n\} \\ 0 \text{ otherwise,} \end{cases}$$

and let $T = \{\boldsymbol{t}_j \mid 1 \leq j \leq \lceil n/(b-1) \rceil\} \subseteq \{0,1\}^n$. For any circuit $C \in \mathcal{C}_{n,k\geq b}$, the output vector of C for an input vector $\boldsymbol{t}_j$ is also $\boldsymbol{t}_j$, since any $\boldsymbol{t}_j$ has at most

$b-1$ one elements ($1 \leq j \leq \lceil n/(b-1) \rceil$). By definition, the i-th entry of $\boldsymbol{t}_j$ is one if and only if $j = \lceil i/(b-1) \rceil$. Therefore, for any $1 \leq i \leq n$, there exist $\boldsymbol{t}_j$ and $\boldsymbol{t}_k \in T$ such that $\boldsymbol{t}_j$ and $\boldsymbol{t}_k$ have one and zero at the i-th entry, respectively. Thus the output wires of C are controllable by T, and we conclude that T is a universal test set for $\mathcal{C}_{n,k\geq b}$ by Lemma 1. Since $|T| = \lceil n/(b-1) \rceil$, we have the lemma. □

6.2 Proof of Lemma 7(Sketch)

6.2.1 Proof for the Case of $n = 3$

We have $b = 2$, and will show that $\sigma(\mathcal{C}_{3,k\geq 2}) \geq 3 = \lceil 3/(2-1) \rceil$. We denote by $\overline{\boldsymbol{v}}$ the complement of a vector $\boldsymbol{v}$ such that $\boldsymbol{v} \oplus \overline{\boldsymbol{v}} = \mathbf{1}$. For a gate G of a circuit C, $G(\boldsymbol{v})$ is the output vector of G generated by an input vector $\boldsymbol{v}$ of C. The following lemma is shown in [9].

Lemma I. *A test set $T = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ for a circuit $C \in \mathcal{C}_{n,k\geq 1}$ is complete if and only if T satisfies the following conditions:*

(i) $\boldsymbol{v}_2 = \overline{\boldsymbol{v}_1}$, and
(ii) $G(\boldsymbol{v}_i) = \boldsymbol{v}_i$ $(i = 1, 2)$ for every gate G of C. □

We now prove that $\tau(C) \geq 3$ for circuit C shown in Fig. 2. For any test set $T = \{\boldsymbol{v}, \overline{\boldsymbol{v}}\}$, $\boldsymbol{v}$ or $\overline{\boldsymbol{v}}$ has two one elements. Thus, T does not satisfy condition (ii) of Lemma I, and so T is not complete for C.

Since $C \in \mathcal{C}_{3,k\geq 2}$, we have $\sigma(\mathcal{C}_{3,k\geq 2}) \geq \tau(C) \geq 3$. □

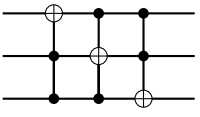


Fig. 2. Reversible circuit C in $\mathcal{C}_{3,k=2}$

6.2.2 Technical Lemmas

Before proving the case of $n \geq 4$, we need some preliminaries. Let $[n] = \{1, 2, \ldots, n\}$, and $X \subsetneq [n]$. For an integer $\tau \in [n] - X$, let $G[X; \tau]$ be the $|X|$-CNOT gate with control bits $c \in X$ and the target bit τ. Such a gate is called an *X-CNOT gate*. For $X_i \subset [n]$, let $\mathcal{C}_n[X_1, X_2, \ldots, X_m]$ be the class of CNOT circuits consisting of only X_i-CNOT gates ($1 \leq i \leq m$). For $\boldsymbol{v} \in \{0,1\}^n$, let $\chi(\boldsymbol{v})$ be the set of integers such that $\boldsymbol{v}$ has one at the i-th entry if and only if $i \in \chi(\boldsymbol{v})$. For a CNOT circuit C, we denote by $C(\boldsymbol{v})$ the output vector of C for input $\boldsymbol{v}$. Since any X-CNOT gate does not change $\boldsymbol{v}$ if $X \not\subseteq \chi(\boldsymbol{v})$, we have the following.

Lemma 8. *Let $X_i \subseteq [n]$ for $1 \leq i \leq m$, and $\boldsymbol{v} \in \{0,1\}^n$ such that $X_i \not\subseteq \chi(\boldsymbol{v})$ for all i with $1 \leq i \leq m$. Then, $C(\boldsymbol{v}) = \boldsymbol{v}$ for $C \in \mathcal{C}_n[X_1, X_2, \ldots, X_m]$.* □

For two vectors $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)'$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)'$, let $\boldsymbol{u} \vee \boldsymbol{v} = (u_1 \vee v_1, u_2 \vee v_2, \ldots, u_n \vee v_n)'$. By definition, $\chi(\boldsymbol{u} \vee \boldsymbol{v}) = \chi(\boldsymbol{u}) \cup \chi(\boldsymbol{v})$.

Lemma 9. *Let $\boldsymbol{u}, \boldsymbol{v} \in T$, $X_1 \subseteq \chi(\boldsymbol{u})$, and $X_2 \subseteq \chi(\boldsymbol{v})$. Then, there exists a circuit $C \in \mathcal{C}_n[X_1, X_2]$ such that $C(\boldsymbol{u}) = \boldsymbol{v}$.*

Proof Sketch. There exist circuits $C_1 \in \mathcal{C}_n[X_1]$ and $C_2 \in \mathcal{C}_n[X_2]$ such that $C_1(\boldsymbol{u}) = \boldsymbol{u} \vee \boldsymbol{v}$ and $C_2(\boldsymbol{u} \vee \boldsymbol{v}) = \boldsymbol{v}$. Thus by concatenating C_1 and C_2, we obtain a desired circuit C. □

For $1 \leq i \leq n - b + 1$, define $\boldsymbol{\beta}_i^{\langle b \rangle} = (\beta_{1,i}, \beta_{2,i}, \ldots, \beta_{n,i})'$ as

$$\beta_{j,i} = \begin{cases} 1 & \text{if } i \leq j \leq i + b - 1, \\ 0 & \text{otherwise.} \end{cases}$$

By definition, $\chi(\boldsymbol{\beta}_i^{\langle b \rangle}) = \{i, i+1, \ldots, i+b-1\}$. For $m \leq n - b + 1$, define that $B_m = \{\boldsymbol{\beta}_i^{\langle b \rangle} \mid 1 \leq i \leq m\}$. Let $\mathcal{T}_{n,b} \subseteq \{0,1\}^n$ be the set of vectors which have at least b one elements.

Lemma 10. *Let $m \leq n - b + 1$, and $\boldsymbol{v}_i \in \{0,1\}^n$ be vectors such that $\boldsymbol{v}_i \in \mathcal{T}_{n,b}$ for $1 \leq i \leq m$. Then, there exists a b-CNOT circuit C_m such that $C_m(\boldsymbol{v}_i) = \boldsymbol{\beta}_i^{\langle b \rangle}$ for $1 \leq i \leq m$.*

Proof Sketch. The proof is done by induction on m. Initially, a circuit C_1 is obtained from Lemma 9. Assume C_j is given. From Lemma 9, there is a $[\chi(\boldsymbol{\beta}_{j+1}^{\langle b \rangle}), \chi(C_j(\boldsymbol{v}_{j+1}))]$-circuit C with $C(C_j(\boldsymbol{v}_{j+1})) = \boldsymbol{\beta}_{j+1}^{\langle b \rangle}$. Since any gate in C does not change $\boldsymbol{\beta}_i^{\langle b \rangle}$ for $i \leq j$, C_{j+1} is obtained by concatenating C_j and C. □

6.2.3 Proof for the Case of $n \geq 4$

We omit the proof for the case of $b = 2$, and assume $b \geq 3$. Let $T \subset \{0,1\}^n$ be any test set consisting of m tests for $m \leq \lceil n/(b-1) \rceil - 1$. Let $T_1 = T \cap \mathcal{T}_{n,b}$ and $T_2 = T - T_1$. Since $|T_1| \leq \lceil n/(b-1) \rceil - 1$, all the vectors in T_1 have zero at the same entry. We assume without loss of generality that all the vector in T_1 have zero at the n-th entry. We can prove that $|T_2| \leq n - b$. Thus by Lemma 9, there is a b-CNOT circuit C with the n-th entry of $C(\boldsymbol{t})$ is zero for all $\boldsymbol{t} \in T_2$. Since any b-CNOT gate does not change $\boldsymbol{t} \in T_1$, the n-th output wire of C is not 1-controllable by $T = T_1 \cup T_2$.

7 Proof of Theorem 6

To prove Theorem 6, it suffices to show $\sigma(\mathcal{C}_{n,k\geq 1}) \geq 2^{n-1} + 1$. Let $\mathrm{val}(\boldsymbol{v}) = \sum_{i=1}^{n} 2^{i-1} v_i$, and $\boldsymbol{r}_m \in \{0,1\}^n$ be the reverse of the n-bit binary representation of integer m. Then, $\mathrm{val}(\boldsymbol{r}_m) = m$. For $\boldsymbol{v}, \boldsymbol{w} \in \{0,1\}^n$, if $\mathrm{val}(\boldsymbol{v}) < \mathrm{val}(\boldsymbol{w})$ then $\chi(\boldsymbol{w}) \not\subseteq \chi(\boldsymbol{v})$. Thus by Lemmas 8 and 9, we have the following.

Lemma 11. *Let $\boldsymbol{u}, \boldsymbol{v} \in \{0,1\}^n$ be non-zero vectors. Then, there exists a circuit C in $\mathcal{C}_n[\chi(\boldsymbol{u}), \chi(\boldsymbol{v})] \subset \mathcal{C}_{n,k\geq 1}$ such that $C(\boldsymbol{u}) = \boldsymbol{v}$, and that $C(\boldsymbol{w}) = \boldsymbol{w}$ for all vectors $\boldsymbol{w}$ with $\mathrm{val}(\boldsymbol{w}) \leq \min\{\mathrm{val}(\boldsymbol{u}), \mathrm{val}(\boldsymbol{v})\} - 1$.* □

Lemma 12. *For $l \leq 2^n - 1$, let $T = \{\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_l\} \subseteq \{0,1\}^n$ with $\boldsymbol{t}_0 = \mathbf{0}$. Then, there exists a circuit C in $\mathcal{C}_{n,k\geq 1}$ such that $C(\boldsymbol{t}_i) = \boldsymbol{r}_i$ for $0 \leq i \leq l$.*

Proof. We show the lemma by induction on l. Initial case is clear since $\boldsymbol{t}_0 = \boldsymbol{r}_0$.

Assume that the lemma holds for $l = l'$ with $l' \leq 2^n - 2$, and we show that the lemma also holds for $l = l' + 1$. By induction hypothesis, there is a circuit $C_{l'}$ satisfying $C_{l'}(\boldsymbol{t}_i) = \boldsymbol{r}_i$ for $0 \leq i \leq l'$. Since $C_{l'}$ implements a permutation, $C_{l'}(\boldsymbol{t}_{l'+1}) \neq \boldsymbol{r}_i$ for $0 \leq i \leq l'$. Thus by Lemma 11, there exists a circuit C in $\mathcal{C}_{n,k\geq 1}$ such that $C(C_{l'}(\boldsymbol{t}_{l'+1})) = \boldsymbol{r}_{l'+1}$ and $C(\boldsymbol{r}_i) = \boldsymbol{r}_i$ for $i \leq l'$. Thus by concatenating $C_{l'}$ and C, we obtain a circuit $C_{l'+1}$ in $\mathcal{C}_{n,k\geq 1}$ satisfying $C_{l'+1}(\boldsymbol{t}_i) = \boldsymbol{r}_i$ for $i \leq l' + 1$. □

Since $\boldsymbol{r}_i$ has 0 at the n-th entry for $i \leq 2^{n-1} - 1$, we have the following by Lemmas 1 and 12.

Corollary 3. *A test set $T \subseteq \{0,1\}^n$ with $\mathbf{0} \in T$ is not 1-universal for $\mathcal{C}_{n,k\geq 1}$ if $|T| \leq 2^{n-1}$.* □

Similarly, we can prove the following by considering $T' = \{\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots, \boldsymbol{t}_{l'}\} = \{0,1\}^n - T$ and a circuit $C \in \mathcal{C}_{n,k\geq 1}$ satisfying $C(\boldsymbol{t}_i) = \boldsymbol{r}_i$ for $i \leq l'$, where $l' = 2^n - 1 - |T|$ and $\boldsymbol{t}_0 = \mathbf{0}$.

Corollary 4. *A test set $T \subseteq \{0,1\}^n$ with $\mathbf{0} \notin T$ is not 0-universal for $\mathcal{C}_{n,k\geq 1}$ if $|T| \leq 2^{n-1}$.* □

From Corollaries 3 and 4, we conclude that $T \subseteq \{0,1\}^n$ is not universal for $\mathcal{C}_{n,k\geq 1}$ if $|T| \leq 2^{n-1}$, and we have Theorem 6.

References

1. Bennett, C.: Logical reversiblity of computation. IBM J. Res. Dev. 17(6), 525–532 (1973)
2. Chakraborty, A.: Synthesis of reversible circuits for testing with universal test set and c-testability of reversible iterative logic array. In: Proc. of the 18th International Conference on VLSI Design, pp.249–254 (2005)
3. Landauer, R.: Irreversibility and heat generation in the computing process. IBM J. Res. Dev. 5(3), 183–191 (1961)
4. Merkle, R.: Two types of mechanical reversible logic. Nanotechnology 4(2), 114–131 (1993)
5. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
6. Patel, K., Hayes, J., Markov, I.: Fault testing for reversible circuits. IEEE Trans. Computer-Aided Design 23(8), 1220–1230 (2004)
7. Patel, K., Markov, I., Hayes, J.: Optimal synthesis of linear reverisible circuits. Quantum Information and Computation 8(3&4), 282–294 (2008)
8. Shende, V., Prasad, A., Markov, I., Hayes, J.: Synthesis of reversible logic circuits. IEEE Trans. Computer-Aided Design 22(6), 710–722 (2003)
9. Tayu, S., Ito, S., Ueno, S.: On fault testing for reversible circuits. IEICE Trans. Inf. & Syst. E91-D(12), 2770–2775 (2008)