ROBDDs Application for Finding the Shortest Transfer Sequence of Sequential Circuit or Only Revealing Existence of this Sequence without Deriving the Sequence itself

A. Matrosova, V. Andreeva, A. Melnikov
Tomsk state university, *Russia*
mau11@yandex.ru, *avv.21@mail.ru*, *alexey.ernest@gmail.com*

Abstract

Methods of revealing of transfer sequence existence of the length not more l for a set of states (internal states) without deriving the sequence itself and finding the shortest transfer sequence of the length not more l for a sequential circuit are developed. The methods are based on applying operations either on full ROBDDs, representing transition functions or fragments of these ROBDDs. Multiplications of the proper ROBDDs are executed with using full ROBDDs but summations - with using ROBDDs fragments. It is setup that for revealing transfer sequence existence we may use ROBDDs fragments depending on only state variables. When finding the shortest sequence we use ROBDDs so that each path originated by state variables has the only prolongation among input variables. The initial state of a sequential circuit is given. Set M^0 of states one of which has to be reached is represented by the ROBDD.

1. Introduction

The problem of finding transfer sequences for sequential circuits is connected with providing reliability of their functioning. We need solve this problem, for example, when finding test sequence for hard detectable faults. In this case, we may represent all test patterns of such fault [1] with ROBDD using a combinational part of a sequential circuit and extract set M^0 of internal states from these test patterns. Then any transfer sequence into M^0 is the test sequence for the hard detectable fault. Hardware Trojan Circuits [2] may be included in sequential circuit and triggered when reaching an internal state from set M^0. If suspicious poles for including Trojan Circuits are found, it may be enough to reveal transfer sequences existence into the proper set of internal states without finding sequences themselves. In this paper methods of revealing of transfer sequence existence of the length not more l for set M^0 of internal states and finding the shortest transfer sequence of the length not more l for a sequential circuit are developed. The methods are based on applying operations either on ROBDDs (full ROBDDs), representing transition functions or fragments of these ROBDDs. Multiplications of the proper ROBDDs are executed with using full ROBDDs but summations - with using the ROBDD fragments. It is setup that for revealing transfer sequence existence we may use the ROBDDs fragments depending on only state variables. When we find the shortest sequence we may use ROBDDs for which a path originated by state variables has the only prolongation among input variables. Note that set M^0 of internal states is represented by the ROBDD.

In Section 2 a method of revealing transfer sequence existence is represented. In Section 3 an algorithm of finding the shortest transfer sequence for a sequential circuit is suggested.

2. Revealing of transfer sequence existence

Let set M^0 of internal states be represented by ROBDD R^{s_0}. Try to reveal transfer sequence existence into M^0 of the length not more l. We mean a sequence that reaches some state from M^0.

Let ROBDD R^{z_i} represents transition function of a sequential circuit corresponding to state (internal) variable z_i. When deriving R^{z_i}, we first execute Shannon decomposition for state variables $z_1,\ldots, z_p$ and then for input variables $x_1,\ldots,x_n$. ROBDD R^{kj} is obtained by a multiplication of ROBDDs corresponding to state variables of product k_j originated by ROBDD R^{s_0} path .We take into consideration signs of inversion of k_j variables.

Remind that mutually inversion ROBDDs differ by

This work is partly supported by the Tomsk State University Competitiveness Improvement Program.
Participation in EWDTS2016 is partially supported within the "Program of increase of the international competitiveness of Tomsk State University for 2013-2020"
978-1-5090-0693-9/16/$31.00 ©2016 IEEE

a permutation of their terminal nodes.

Present full state of sequential circuit by Boolean vector depending on input and state variables. First input variables are enumerated.

Denote $M(k_j)$ as a set of internal states represented by k_j .

ROBDD R^{kj} presents all full states from which one step transitions into states of $M(k_j)$ are executed.

Let $M(R^{kj})$ be a set of internal states reachable by one step transition from full states represented by ROBDD R^{kj}.

Proposal 1. $M(k_j)$ contains $M(R^{kj})$.

Proof. Based on the construction of ROBDD R^{kj}, we conclude that any Boolean vector representing full state of sequential circuit and turning the product originated by the path connecting ROBDD R^{kj} root with its 1 terminal node into1, provides the one step transition in one of states of $M(k_j)$. It means that $M(k_j)$ contains $M(R^{kj})$. The proposal is proved.

Proposal 2. Initial fragment δ of a path connecting ROBDD R^{kj} root with its first internal node marked by input variable represents a set of internal states from which some states of $M(k_j)$ are reachable by one step transition.

Proof. Fragment δ originates some full states providing transitions into states of $M(k_j)$. The proposal is proved.

Note that correspondence between a previous internal state and the next internal state (reachable by one step transition) is provided by the previous full state. We are not interested in this correspondence but only in a set of previous internal states so that each its element guarantees one step transition into states of $M(k_j)$. That is why we may consider only δ fragments which contains ROBDD R^{kj}. Extract these fragments from R^{kj} as follows.

1). Exclude from R^{kj} internal nodes marked by input variables.

2). Hanging edges connect with 1 terminal node.

3). Simplify the obtained graph in a conventional way.

As a result we derive ROBDD R^{kj*}. This ROBDD presents all internal states providing one step transitions into next internal states from $M(k_j)$ at the expense of the proper input states.

Consider an example to illustrate deriving ROBDD R^{kj*}.

We have Sum of Products (SoP) depending on input and state variables.

$$\bar{x}_1\bar{x}_2\bar{z}_1z_2 \vee x_1\bar{x}_2z_1z_2 \vee x_1x_2\bar{z}_1z_2 \vee x_1x_2z_1\bar{z}_2 \vee \bar{x}_1x_2z_1z_2$$

The ordering set of variables is as follows: z_1,z_2,x_1,x_2.
The corresponding ROBDD is shown in Fig.1.

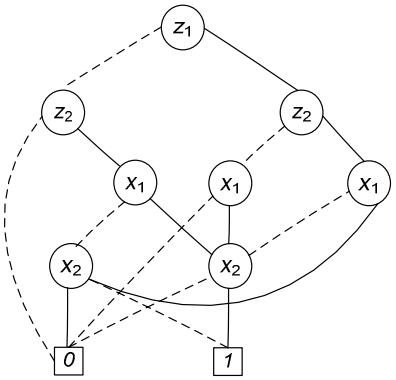

Figure 1. ROBDD implementing SoP

Executing points 1-3 we have the following sequence of graphs (Fig.2a-c).

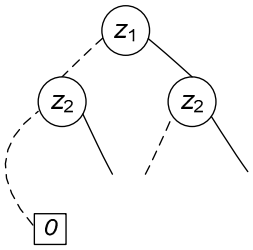

Figure 2a. Excluding nodes

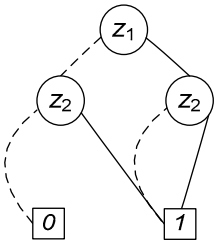

Figure 2b. Connecting of hanging edges

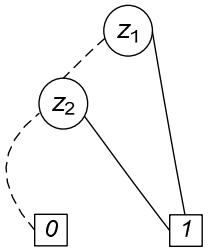

Figure 2c. ROBDD

Note that we simplify the graph obtained in point 2. Fig. 2c represents the result.

Derive ROBDDs R^{kj*} for all paths connecting ROBDD R^{s_0} root with its 1 terminal node. As only a fact of one step transition into internal states of set M^0 it is important for us, and we are not interested in correspondence between a previous and the next internal states we may summarize all ROBDDs R^{kj*} to get resulting ROBDD R^{s_1}.

Having got R^{s_1} we then get ROBDDs R^{s_2}, R^{s_3} ,…,R^{s_l} in a similar way.

Let α presents an initial internal state of a sequential circuit.

Proposal 3. If a substitution of vector α into ROBDD R^{s_1} turns this ROBDD into1, then there exists one step transition from α into some internal state from M^0.

Proof. Turning ROBDD R^{s_1} into 1 means that one product originated by the path of the ROBDD is turned into 1. Consequently, there exists at least one transition from α into some states from M^0 (different inputs vectors may provide reaching several states from M^0).The proposal is proved.

For current ROBDD R^{s_i} we execute a substitution of vector α. If α turns R^{s_i} into1, we stop calculations. Show that then value i is the length of the shortest sequence that guarantees reaching some state from M^0.

Proposal 4. If a substitution of vector α into ROBDD R^{s_i} turns the ROBDD into 1then there exists a sequence of the length i that guarantees reaching some state from M^0.

Proof. Turning ROBDD R^{s_i} into 1on α means that there exists one step transition from α into one of states represented by ROBDD R^{s_i-1} , then - into one of states represented by R^{s_i-2} and so on until we get one of state from M^0. The proposal is proved.

When current $i=l$ but ROBDD R^{s_1} can not be turned into 1 on α we conclude that there is no a sequence of the length not more l that reaches a state from M^0.

3. Finding the shortest transfer sequence into M^0.

We use the same set of states M^0 represented with ROBDD R^{s_0}. It is necessary to find the shortest transfer sequence of the length not more l. It does not matter which internal state from M^0 is reached.

Derive ROBDD R^{k_j} for each product k_j originated by the path from R^{s_0} in the above mentioned way. For each internal state represented by initial fragment δ of a path connecting ROBDD R^{k_j} root with 1 terminal node we provide existence at least one full state. From such full state there exists one step transition into the state from M^0. (ROBDD R^{k_j} represents all such full states).

Proposal 5. Initial fragment δ of a path connecting ROBDD R^{k_j} root with its first internal node marked by any input variable represents a set of internal states from which there exist one step transitions into the states from $M(k_j)$. A prolongation of δ till 1-terminal node of R^{k_j} originates full states providing such transitions.

Proof. The proof is similar to that of Proposal 2.

Taking into consideration proposal 5 we simplify ROBDD R^{k_j} as follows. .

1. Separate a set of internal nodes marked by input variables that are connected at least with one internal node marked by a state variable.

2. For each separated node find one path connecting it with 1 terminal node of R^{k_j}, the shorter path the better.

3. If in obtained graph there are nodes from which only one edge runs, we connect the second edge with 0 terminal node.

The simplification procedure is illustrated in Fig. 3a-3b. Initial ROBDD is represented in Fig. 1.

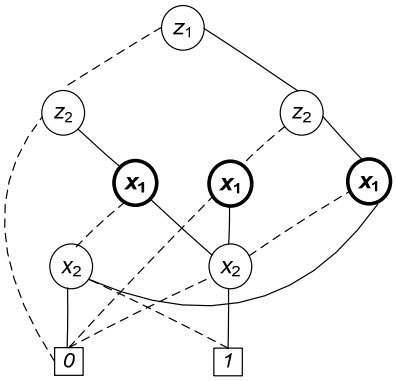

Figure 3a. ROBDD with separated nodes

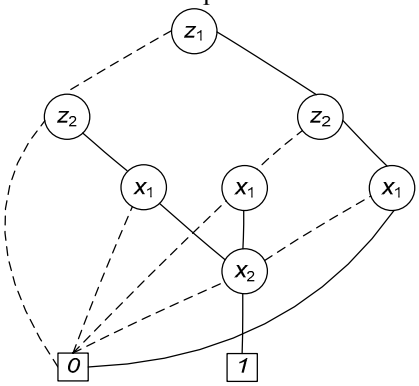

Figure 3b. Simplified ROBDD

The simplified graph is denoted as R^{k_j**}. Take into consideration that different δ fragments of ROBDD R^{k_j**} are pairwise orthogonal but prolongations of these fragments may be not orthogonal.

Let $M(R^{k_j**})$ be a set of internal states that are one step reachable from full states represented by ROBDD R^{k_j**}.

Proposal 6. $M(k_j)$ contains $M(R^{k_j**})$.

Proof. Under construction of R^{k_j**} we have the following. Any Boolean vector of input and state variables of a sequential circuit that turns the product originated by the path connecting ROBDD R^{k_j**} root with 1 terminal node into 1 provides one step transition into the internal state from $M(k_j)$. The proposal is proved .

Corollary. $M(R^{k_j**}) \subseteq M(R^{k_j}) \subseteq M(k_j)$

Remind that p is the number of state variables of a sequential circuit. After completing all δ fragments of

ROBDD R^{k_j**}till products of rank p we get products representing all internal states from which there exist one step transitions into internal states of a set $M(k_j)$. Moreover for each such internal state there is at least one full state providing this transition,

Derive R^{k_j**} in a similar way for each path connecting ROBDD R^{s_0} root with 1 terminal node.

Summarize all ROBDDs R^{k_j**} to get resulting ROBDD R^{s_1*}.

Derive $R^{s_1}$from R^{s_1*} in the way suggested in Section 2.

Then in the above mentioned way we get ROBDDs R^{s_2*}, R^{s_3*} ,…,R^{s_l*}.

Remind that α is an initial internal state of a sequential circuit.

Proposal 7. If a substitution of vector α into ROBDD R^{s_1*} turns one of fragment δ of this ROBDD into1, then there exists one step transition from α into some internal state from M^0 by input state represented with the Boolean vector turning the prolongation of δ into1.

Proof. It means that there exists the full state providing one step transition into the internal state from M^0. The proposal is proved.

For current ROBDD R^{s_i*} execute a substitution of vector α. If α turns some fragment δ of R^{s_i*} into 1, we stop calculations. Then i is the length of the shortest sequence that guarantees reaching some state from M^0.

Proposal 8. If a substitution of vector α into ROBDD R^{s_i*} turns some fragment δ of this ROBDD into 1 then there exists a sequence of the length i that guarantees reaching some state from M^0.

Proof. It means that there exists the full state providing one step transition into the internal state from a set represented by R^{s_i-1} , then - into one of states represented by R^{s_i-2} and so on when we get one of state from M^0. The proposal is proved.

When current i is equal to l and any fragment δ of ROBDD R^{s_1*} cannot be turned into 1 on α we conclude that there is no a transfer sequence of the length not more l that reaches a state from M^0.

Algorithm of finding the shortest transfer sequence into M^0

Let keep R^{s_0}, R^{s_1*},…,R^{s_i*}. Here i is the length of the shortest transfer sequence into M^0. Find one of these sequence. For that we find a prolongation (product of input variables) of fragment δ from R^{s_i**} where δ is turned into 1 on vector α. The Boolean vector of input variables that turns the product originated by the prolongation into 1 call ε_1, and vector α overcall α_1. Form the Boolean vector representing the full state of a sequential circuit and denote it as $\varepsilon_1{:}\alpha_1$.

1. Having substituted vector $\varepsilon_1{:}\alpha_1$ into transition functions of the sequential circuit we find the internal state α_2.

2. Find fragment δ from R^{s_i-1*}, that is turned on vector α_2 into 1 and the corresponding full state $\varepsilon_2{:}\alpha_2$ from $R^{s_i-1*}$and so on till finding vector $\varepsilon_i{:}\alpha_i$ that turns ROBDD R^{s_1*} into 1. This Boolean vector provides one step transition in the state from M^0.

Input sequence ε_1, ε_2,…,ε_i is the shortest transfer sequence into M^0.

4. Conclusion

New approach to revealing existence of a transfer sequence into M^0 of the length not more l and finding the shortest transfer sequence into M^0 of the length not more l for a sequential circuit is suggested. The approach is based on applying operations either on ROBDDs (full ROBDDs), representing transition functions of a sequential circuit or fragments of these ROBDDs. Multiplications of the proper ROBDDs are executed with using full ROBDDs, but summations-with using the ROBDDs fragments. The operations on ROBDDs have a polynomial complexity.

5. References

[1] A.Yu Matrosova , S.A Ostanin, A.I Bucharov, I.E Kirienko I. “Generating all test patterns for a given stuck-at fault of a logical circuit and its ROBDD implementation,” *Tomsk State University, Journal of Control and Computer Science*, N 2 (27), 2014, pp. 77-86 (In Russian)

[2]. Masoyoshi Yoshimura, Tomohiro Bouyashiki, Toshinori Hosokawa. A sequence Generation Method to detect Hardware Trojan Circuits//16-th IEEE Workshop on RTL and High Level Testing, 2015, IIT, Mumbai, India, 25-26 November, 2015, pp.84-89.