An Exponential Lower Bound of the Size of OBDDs Representing Division

4 B − 2

Takashi HORIYAMA and Shuzo YAJIMA

Graduate School of Engineering, Kyoto University

1 Introduction

The size of an OBDD [1] largely depends on the variable ordering. It is important to clarify the lower bounds of OBDDs representing arithmetic functions. In this report, we investigate a lower bound of the size of OBDDs representing integer division. More precisely, we focus on each bit of the output of the n-bit / n-bit division, and prove that the size of OBDDs representing the i-th bit is $\Omega(2^{(n-i)/8})$. We also prove the same lower bound on $\vee$-OBDDs [3], $\wedge$-OBDDs [3] and $\oplus$-OBDDs. To prove this lower bound, we introduce a strong fooling set, which has a more restricted property than a fooling set [4].

2 Preliminaries

2.1 Ordered Binary Decision Diagrams

An Ordered Binary Decision Diagram (OBDD) is a directed acyclic graph which represents a Boolean function. It has two sink nodes labeled by 0 and 1, called the 0-node and the 1-node. The other nodes are called variable nodes, labeled by input variables. Each variable node has exactly two outgoing edges, called 0-edge and 1-edge. A unique source is called the root node. On every path from the root node to a sink node, each variable appears at most once in the same order. Each node represents a Boolean function. If node v is a sink node, $func(v)$ equals the label. If node v is a variable node, $func(v) = \overline{x} \cdot func(0\text{-}succ(v)) + x \cdot func(1\text{-}succ(v))$, where x is the label of v, $0\text{-}succ(v)$ ($1\text{-}succ(v)$) is the node pointed by the 0-edge (1-edge) of v. The function represented by an OBDD is the one represented by the root node.

Two nodes u and v of same label and representing the same function are called to be equivalent. A node whose 0-edge and 1-edge point to the same node is called a redundant node. Here we consider reduced OBDDs which have node no equivalent nodes and no redundant nodes. The size is the number of nodes in the OBDD.

An $\vee$-OBDD is defined as an OBDD with '$\vee$' symbols. On every path from the node to a constant node, only '$\vee$' can appear more than once. If the node v is labeled by an '$\vee$', $func(v) = func(0\text{-}succ(v)) + func(1\text{-}succ(v))$. Similarly, $\wedge$-OBDDs and $\oplus$-OBDDs can be defined as OBDDs with '$\wedge$' symbols and '$\oplus$' symbols respectively.

2.2 Strong Fooling Sets

Let $f_n(X)$ be a single output Boolean function where the number of input variables is parameterized by n. A partition for f_n is a partition of X into two disjoint sets L and R. From an input assignment $l_i \cdot r_i$, we obtain a partial assignment l_i (r_i) which is an assignment to all variables in L (R). A fooling set of f_n is the set $\mathcal{A}$ of input assignments having the following properties.

There is some $z \in \{0,1\}$, such that $f_n(l_i \cdot r_i) = z$ for all $l_i \cdot r_i \in \mathcal{A}$, but for any two distinct assignments $l_i \cdot r_i$ and $l_j \cdot r_j \in \mathcal{A}$, either $f_n(l_i \cdot r_j) \neq z$ or $f_n(l_j \cdot r_i) \neq z$.

We introduce more restricted fooling sets, named strong fooling sets. A strong fooling set $\mathcal{A}$ has the property that $f_n(l_i \cdot r_j) \neq z$ for any two distinct assignments $l_i \cdot r_i$ and $l_j \cdot r_j \in \mathcal{A}$ $(i < j)$. The set is called a 0-strong fooling set when $z = 0$, and a 1-strong fooling set when $z = 1$.

Theorem 1 [2] *Let the function f_n have a fooling set $\mathcal{A}$ containing at least c elements for every balanced partition (L, R). The size of the OBDD representing f_n is $\Omega(c)$ for any variable ordering. A balanced partition is a partition of X such that $\lfloor \omega|Y| \rfloor \leq |Y \cap L| \leq \lceil \omega|Y| \rceil$ for some ω, $Y(\subseteq X)$.*

3 OBDDs Representing Division

n-bits / n-bits division is described as follows. Find the value of $Q = (q_{n-1} \ldots q_0)$ such that $\sum_{i=0}^{n-1} x_i \cdot 2^i = (\sum_{i=0}^{n-1} q_i \cdot 2^i)(\sum_{i=0}^{n-1} y_i \cdot 2^i) + R$ and $R < (\sum_{i=0}^{n-1} y_i \cdot 2^i)$, when an assignment of inputs $X = (x_{n-1} \ldots x_0)$ and $Y = (y_{n-1} \ldots y_0)$ is given. Let a function Div_i^n denote the output q_i of n-bits / n-bits division.

Lemma 1 *For every balanced partition for the set of inputs, the function Div_0^n has a 0-strong fooling set containing at least $2^{n/8-1}$ elements.*

除算を表現する二分決定グラフの指数下界
堀山 貴史　矢島 脩三
京都大学大学院工学研究科

Sketch of Proof: Let X_U denote the upper half $(x_{n-1} \ldots x_{n/2})$, and X_D denote the lower half $(x_{n/2-1} \ldots x_0)$. Then, X is partitioned into four sets, $X_{UL} = X_U \cap L$, $X_{DL} = X_D \cap L$, $X_{UR} = X_U \cap R$, $X_{DR} = X_D \cap R$. For an integer p $(-n/2 < p < n/2)$, define the set $Args_p = \{\langle x_{i+n/2}, x_{i+p}\rangle | 0 \leq i < n/2 - p\}$ if $p \geq 0$, and $Args_p = \{\langle x_{i+n/2-p}, x_i\rangle | 0 \leq i < n/2 + p\}$ if $p < 0$.

Let $Split_p = Args_p \cap [(X_{UL} \times X_{DR}) \cup (X_{UR} \times X_{DL})]$. $Split_p$ contains at least $n/8$ elements for some p [2]. Then, for every balanced partition, there exists some $Split_p$ which have at least $n/8$ elements. Define $U = (u_{m-1} \ldots u_0), V = (v_{m-1} \ldots v_0)$ as follows, where $m = n/2 - |p|$. If $p \geq 0$, $u_i = x_{i+n/2}$ and $v_i = x_{i+p}$. If $p < 0$, $u_i = x_{i+n/2-p}$ and $v_i = x_i$. The set $Args_p$ consists of all pairs $\langle u_i, v_i\rangle$ for $0 \leq i < m$.

For above p, construct a set $\mathcal{A}$ of input assignments, such that each assignment satisfies the following. The set contains at least $2^{n/8-1}$ elements.

1) If $p \geq 0$, y_i is assigned 1 for each $p \leq i < n/2$, and assigned 0 for each $0 \leq i < p$, $n/2 \leq i < n$. If $p < 0$, y_i is assigned 1 for each $0 \leq i < n/2 - p$, and assigned 0 for each $n/2 - p \leq i < n$.

2) If $p \geq 0$, x_i is assigned 0 for each $0 \leq i < p$, $n - p \leq i < n$. If $p < 0$, x_i is assigned 1 for each $n/2 + p \leq i < n/2 - p$.

3) For each $\langle u_i, v_i\rangle \in Args_p - Split_p$, u_i is assigned 1 and v_i is assigned 0

4) Whether $\langle u_0, v_0\rangle$ is in $(Args_p - Split_p)$ or not, u_0 is assigned 1 and v_0 is assigned 0.

5) For each i $(0 \leq i < m)$, $u_i = \overline{v_i}$.

We consider the case $p \geq 0$. One property of a strong fooling set is that the output of Div_0^n is 0 for all assignments in $\mathcal{A}$. As $X = U2^{n/2} + V2^p$ and $Y = 2^{n/2} - 2^p$, $X = YU + (U + V)2^p = Y(U + 1)$. This means that the output of Div_0^n is 0 for all assignments in $\mathcal{A}$.

Another property is that $Div_0^n(l_i \cdot r_j) = 1 (\neq 0)$ for any two distinct assignments $l_i \cdot r_i$ and $l_j \cdot r_j$ in $\mathcal{A}$ $(i < j)$. Let $g[l_i \cdot r_j]$ denote $U + V$ for the assignments $l_i \cdot r_j$. As is shown above, $g[l_i \cdot r_i] = g[l_j \cdot r_j] = Y$. However, $g[l_i \cdot r_j]$ and $g[l_j \cdot r_i]$ can not be equivalent to Y. Hence, $g[l_i \cdot r_j] < g[l_j \cdot r_i]$ or $g[l_j \cdot r_i] < g[l_i \cdot r_j]$ holds. Let $l_1 \cdot r_1, l_2 \cdot r_2, \cdots$ denote all assignments in $\mathcal{A}$. Without loss of generality, $g[l_{i+1} \cdot r_i] > g[l_i \cdot r_{i+1}]$ holds for any i. As $g[l_{i+1} \cdot r_i] > Y[l_i \cdot r_i] = g[l_i \cdot r_i]$, $g[l_{i+1} \cdot r_k] > g[l_i \cdot r_k]$ holds for any k. Therefore $g[l_j \cdot r_j] = Y[l_j \cdot r_j] > g[l_i \cdot r_j]$ holds. For $l_i \cdot r_j$, the quotient is U and the remainder is $(U + V)2^p$. This means that the output of Div_0^n is 1 for all assignments $l_i \cdot r_j$ $(i < j)$.

In the case $p < 0$, $\mathcal{A}$ is similarly proved to be a strong fooling set. It is shown that there exists a 0-strong fooling set $\mathcal{A}$ containing at least $2^{n/8-1}$ elements for every balanced partition. □

Theorem 2 *The size of the OBDD representing Div_0^n is $\Omega(2^{n/8})$ for any variable ordering.*

Corollary 1 *The size of the OBDD representing Div_i^n is $\Omega(2^{(n-i)/8})$ for any variable ordering, where $0 \leq i < n$.*

4 ∨-OBDDs, ∧-OBDDs and ⊕-OBDDs Representing Division

Theorem 3 *Let a function f_n have a fooling set containing at least c elements for every balanced partition. If the set is a 1-fooling set (a 0-fooling set), the size of the ∨-OBDD (∧-OBDD) representing f_n is $\Omega(c)$ for any variable ordering.*

Sketch of Proof: Suppose the set $\mathcal{A}$ is a 1-fooling set. Assume that the size is less than c. Then there exist two distinct assignments $l_i \cdot r_i$ and $l_j \cdot r_j$ in $\mathcal{A}$, such that a single node v is led from the root node by both l_i and l_j, and the 1-node is led from the node v by both r_i and r_j. This breaks the property of a 1-fooling set. □

Theorem 4 *Let a function f_n have a strong fooling set containing at least c elements for every balanced partition. The size of the ⊕-OBDD representing f_n is $\Omega(c)$ for any variable ordering.*

Sketch of Proof: Suppose the set $\mathcal{A}$ is a 1-strong fooling set. Assume that the size is c' $(c' < c)$. Define a matrix $\mathbf{A} = [a_{ij}]_{1 \leq i,j \leq c}$ representing $\mathcal{A}$, where $a_{ij} = f_n(l_i \cdot r_j)$. Also define two matrices $\mathbf{B} = [b_{ik}]_{1 \leq i \leq c, 1 \leq k \leq c'}$ and $\mathbf{C} = [c_{kj}]_{1 \leq k \leq c', 1 \leq j \leq c}$, where b_{ik} $(c_{kj}) = 1$ if and only if an assignment l_i (r_j) gives an odd number of paths from the root node (the node v_k) to the node v_k (the 1-node). As $\mathbf{A} = \mathbf{B} \cdot \mathbf{C}$ over $\mathbf{GF}(2)$, $c \leq c'$ holds when the rank of the matrices are considered. A contradiction occurs. □

Corollary 2 *The size of the ∨-OBDD representing Div_i^n is $\Omega(2^{(n-i)/8})$ for any variable ordering. The same lower bound holds on the ∧-OBDD and the ⊕-OBDD.*

5 Conclusion

In this report, we proved that the size of OBDDs, ∨-OBDDs, ∧-OBDDs and ⊕-OBDDs representing division has an exponential lower bound.

References

[1] R.E.Bryant: IEEE Trans. Compt., C-35(8), pp.667-691, 1986.

[2] R.E.Bryant: IEEE Trans.Compt., 40(2), pp.205-213, 1991.

[3] K.Takagi and S.Yajima: KUIS Technical report, KUIS-95-0005,1995.

[4] C.D.Thompson: in Proc. 11th STOC,pp.81-88,1979.