

Short Paper

A Depth 3 Circuit Lower Bound for the Parity Function*

SHI-CHUN TSAI

Information Management Department

National Chi-Nan University

Nantou, 545 Taiwan

E-mail: tsai@csie.ncnu.edu.tw

We consider small depth boolean circuits with basis {AND, OR, NOT}. We obtain lower bounds for the parity function using a relatively simple method. We prove that for any depth 3 circuit with top fan-in t , computing the n -variable parity function must have at least $t2^{\frac{n-1}{t}}$ wires. Similarly, we obtain a lower bound for computing the depth 4 circuits.

Keywords: computational complexity, circuit complexity, boolean function complexity, lower bound, parity

1. INTRODUCTION

The goal of computational complexity is to measure the amount of resources needed to perform certain computations. There has been great progress in finding upper bounds (algorithms) for many problems. However, it is still very difficult to find lower bounds for problems over general computational models, such as Turing machine or the circuit model with a complete basis. Many key open problems in computer science and related areas hinge on finding strong lower bounds. For example, the P v.s. NP problem would be resolved if we could prove an exponential lower bound for any NP-complete problem. While no method for proving lower bounds for general computational models is in sight, there are some results for simpler and more restricted computational models, such as small depth circuits, monotone circuits, etc. Restricted models may enable us to constrain the problem and achieve a clear analysis and derivation of strong lower bounds. We hope that by studying the lower bounds for restricted models, we can help develop useful tools for attacking problems involving more general models.

In this paper, we consider the depth 3 boolean circuit with basis {AND, OR, NOT}, where each level consists of the same type of gate, which can be achieved by adding a small number of extra gates. Without loss of generality, we can push the negation to the input variables. Let AND, OR, AND be the top, middle and bottom gates, respectively.

Received January 7, 2000; revised May 11, 2000; accepted June 1, 2000.

Communicated by Hsu-Chun Yen.

*The work was supported in part by the National Science Council of Taiwan under contract NSC 87-2213-E-260-001.

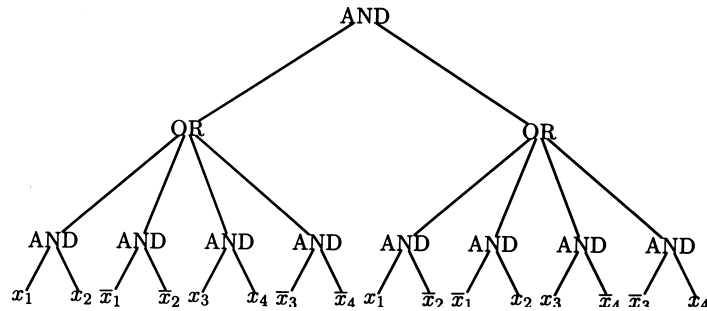


Fig. 1. Depth 3 circuit for PARITY with $n = 4$.

For convenience, Π_3 is used to denote this type of depth-3 circuit. Fig. 1 shows a Π_3 circuit that computes the 4-variable parity function. Here we measure the number of edges that connect the gates. The edge measurement is well justified in VLSI design since the communication edges consume a significant portion of the chip area. We prove that the parity function requires at least $t2^{\frac{n-1}{t}}$ edges, where t is the top fan-in. Note that the same bound holds for OR-AND-OR circuits. This bound is interesting when $t \leq \sqrt{n}$. It is known that the depth-3 circuit size lower bound for PARITY is $\Omega(2^{0.618\sqrt{n}})$ [4]. In the case of $t \leq \sqrt{n}$, we get a large lower bound for the number of edges. The proof is deterministic and very simple. Hopefully, with some extension of this method, we can obtain more general lower bounds.

Small depth circuits have been studied by Ajtai [1], Furst *et al* [2], Yao [7], Håstad [3], Razborov [5], Somlensky [6], and Håstad *et al.* [4], in which superpolynomial and exponential lower bounds on circuit size in terms of gate count were proved for parity and majority functions. Our approach is different from the above. The result is based on the property of the parity function. One major difference is that we prove exponential edge lower bounds by a simple counting argument, instead of size lower bounds and by the probabilistic argument.

2. EDGE LOWER BOUND FOR THE DEPTH 3 CIRCUIT

Before we discuss the depth 3 circuit, we will warm up by looking at the complexity of the depth 2 circuit for the parity function. Suppose the output is an OR-gate and takes the outputs of AND-gates as inputs. We claim that the number of AND-gates for the depth 2 circuit is 2^{n-1} , which gives the exact bound for the depth 2 circuit. For the n -variable parity function, there are 2^{n-1} inputs with odd parity. In the depth 2 circuit, each AND-gate must have all the variables, negated or not, as inputs, i.e., each AND-gate has n inputs; otherwise, there will be an even parity input that makes the AND-gate and the output gate output 1. In other words, each AND-gate recognizes exactly one odd parity input. Therefore, we need exactly 2^{n-1} AND-gates in the depth 2 circuit for the n -variable parity function. Analogously, it is clear that this is also true for the case of the AND-OR depth 2 circuit. Next, we will consider the depth 3 case.

Theorem 1 Any depth 3 circuit computing the parity function with top fan-in t has at least $t2^{\frac{n-1}{t}}$ edges.

Proof: Consider a Π_3 circuit that computes the parity function of n variables, where we label the **OR**-gates from 1 to t and let s_i be the fan-in of the i -th **OR**-gate. Thus, the third level **AND**-gates can be labeled with (i, j) for $1 \leq i \leq t$ and $1 \leq j \leq s_i$. Moreover, let $A_{i,j}$, $1 \leq i \leq t$ be the set of 0-1 assignments that satisfies the (i, j) -th **AND**-gate. Note that different $A_{i,j}$'s may represent the same set. This means that the fan-out of a bottom level **AND**-gate can be greater than 1. Clearly $A_{i,j}$ is determined by its input literals. For instance, as shown in Fig. 1, $A_{1,2} = \{0000, 0001, 0010, 0011\}$. Also, each sub-circuit rooted by an **OR**-gate must have all variables, in negation or not, appear as inputs; otherwise, the circuit would reject an input with odd parity. Observe that $\cup_j A_{i,j}$ is the set of 0-1 assignments satisfying the i -th **OR** sub-circuit. Therefore, $\cap_{i=1}^t \cup_{j=1}^{s_i} A_{i,j}$ is the set of 0-1 assignments with odd parity. By the distributive rule, we know that the set is the union of intersections of the forms $\cap_i A_{i,l_i}$, where $1 \leq l_i \leq s_i$. We claim that $|\cap_i A_{i,l_i}|$ can be 0, 1 or an even number. The reason is that if all the (i, l_i) -th **AND** gates have all the n variables as inputs, then $|\cap_i A_{i,l_i}|$ must be 0 or 1, whereas if these **AND** gates do not have all the variables as their inputs, then $|\cap_i A_{i,l_i}|$ is even. In the latter case, if the size of the intersection is non-zero, then $\cap_i A_{i,l_i}$ contains a 0-1 assignment of even parity.

Let \vec{x} be an assignment with odd parity. Then for each $1 \leq i \leq t$, there must be at least one A_{i,k_i} such that $\vec{x} \in A_{i,k_i}$. Thus, $\vec{x} \in \cap_i A_{i,k_i}$. Based on the above observation, we have that $|\cap_i A_{i,l_i}| \leq 1$, where $1 \leq l_i \leq s_i$. In total, we have at most $s_1 s_2 \dots s_t$ intersections of $A_{i,j}$'s, which must total at least 2^{n-1} to guarantee that the circuit can compute the parity function correctly. It is clear that the number of edges of the circuit is at least $s_1 + s_2 + \dots + s_t$, which is at least $t(s_1 s_2 \dots s_t)^{\frac{1}{t}}$ since the arithmetic mean is greater than or equal to the geometric mean. Therefore the number of edges is at least $t2^{\frac{n-1}{t}}$. This completes the proof. \square

The above also holds for any depth 3 AND-OR-AND circuit that computes the parity function correctly on at least $\epsilon 2^{n-1}$ odd parity inputs, where ϵ is a constant and $0 < \epsilon \leq 1$. We can summarize this as follows:

Corollary 2 Any depth 3 circuit with top fan-in t computing the parity function correctly on at least $\epsilon 2^{n-1}$ odd parity inputs has at least $\epsilon^{\frac{1}{t}} t2^{\frac{n-1}{t}}$ edges.

By applying a result obtained by Håstad [3], we know that the top fan-in for the optimal depth 3 circuit must be at least \sqrt{n} , which is proved as follows:

Corollary 3 The optimal Π_3 circuit for the parity function must have a top fan-in of $\Omega(\sqrt{n})$.

Proof: It is known that PARITY can be computed by a depth 3 circuit of $O(\sqrt{n}2^{\sqrt{n}})$ edges [3]. With the above theorem, we have $t2^{\frac{n-1}{t}} = O(\sqrt{n}2^{\sqrt{n}})$. It follows that $t = \Omega(\sqrt{n})$. \square

Next, we will extend the depth 3 edge lower bound to the depth 4 OR-AND-OR-AND circuit. For such a depth 4 circuit that computes the parity function correctly with a top fan-in of m , we know that at least one of the m subcircuits rooted with OR-gate must compute correctly on at least $2^{n-1}/m$ odd parity inputs. This gives an immediate lower bound for the depth 4 circuit. By Corollary 2, the lower bound is $(\frac{1}{m})^{\frac{1}{t}} t' 2^{\frac{n-1}{t'}}$ where t' is the smallest top fan-in among the depth 3 subcircuits.

3. CONCLUSIONS

In this note, we have proved that any depth 3 circuit computing the parity function with a top fan-in of t has at least $t 2^{\frac{n-1}{t}}$ edges. This has been proved by means of a simple counting argument. An obvious open question is: *Can we apply this technique to depth d (> 4) circuits and to circuits computing other boolean functions?* So far, we don't know how to apply this technique to the majority function, and it is also not clear how to keep the bound from diminishing as the depth increases.

REFERENCES

1. M. Ajtai, " Σ_1^1 -formula on finite structures," *Annals of Pure and Applied Logic*, Vol. 24, No. 1, 1983, pp. 1-48.
2. M. Furst, J. Saxe, and M. Sipser, "Parity, circuits and the polynomial time hierarchy," *Mathematical Systems Theory*, Vol. 17, No. 1, 1984, pp. 13-27.
3. J. Håstad, *Computational Limitations of Small-Depth Circuits*, MIT PRESS, Cambridge, MA, 1986.
4. J. Håstad S. Jukna and R. Rudlák, "Top-down lower bounds for depth 3 circuits," *Computational Complexity*, Vol. 5, No. 2, 1995, pp. 99-112.
5. A. A. Razborov, "Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$," *Mathematical Notes of the Academy of Science of the USSR*, Vol. 41, No. 4, 1987, pp. 333-338.
6. R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *Proceedings of 19th Annual ACM Symposium on Theory of Computing*, 1987, pp. 77-82.
7. A. C-C. Yao, "Separating the polynomial-time hierarchy by oracles," in *Proceedings of 26th IEEE Symposium on Foundations of Computer Science*, 1985, pp. 1-10.

Shi-Chun Tsai (蔡錫鈞) received the B.S. and M.S. degrees in computer science and information engineering in 1984 and 1988, respectively from National Taiwan University, and the Ph.D. degree in computer science from the University of Chicago in 1996. Since then, he joined the department of Information Management of National Chi-Nan University as an associate professor till 2001. Then he joins the Computer Science and Information Engineering Department at NCTU. His research interests focus on theoretical computer science: computational complexity, algorithms design and analysis, randomized computation, discrete mathematics etc. Recently, he is also interested in developing application systems with Java.