Parity 函數之三層線路下限
A Depth 3 Circuit Lower Bound for the Parity Function

蔡錫鈞
Shi-Chun Tsai
國立暨南國際大學資工系-資管所
Computer Science and Information Engineering Department, and
Information Management Department
National Chi-Nan University
Pu-Li, Nan-Tou 545
Taiwan, ROC
tsai@csie.ncnu.edu.tw

摘要

本文考慮使用AND,OR及NOT等元件來計算Parity函數, 本文証明使用三層線路來計算Parity函數時所須之最少線路數(wires)爲$t2^{\frac{n-1}{t}}$,其中t爲輸出元件的輸入線數.同理可証四層線路之下線.

關鍵字: 計算複雜度;線路複雜度;布林函數複雜度

Abstract

We consider small depth boolean circuits with basis {**AND, OR, NOT**}*. We obtain lower bounds for the parity function with 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

1 Introduction

The goal of computational complexity is to measure the amount of resources needed to perform certain computations. There have 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, circuit model with a complete basis, etc. 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 to prove lower bounds for general computational models in sight , there are some results for simpler and more restrictive computational models, such as small depth circuits, monotone circuits, etc. Restricted models may enable us to constrain the problem and have a clear analysis and derivation of strong lower bounds. We hope that by studying the lower bounds for restricted models will help develop useful tools on attacking the problems for more general models.

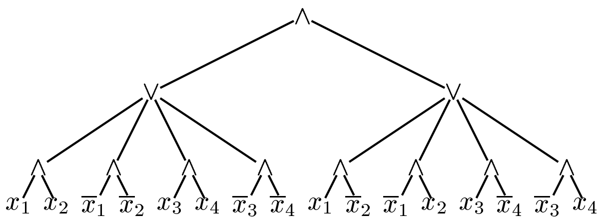

Fig. 1: Depth 3 circuit for PARITY with $n = 4$.

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. For convenience Π_3 is used to denote this type of depth-3 circuits. 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 measurement on edges 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. 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 bound.

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], where super-polynomial and exponential lower bounds on circuit size have been 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 the probabilistic argument.

2 Edge lower bound for depth 3 circuit

Before we discuss depth 3 circuit, we warm up by looking at the complexity of depth 2 circuit for the parity function. Suppose the output is an OR-gate, which takes the outputs of AND-gates as inputs. We claim that the number of AND-gate 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 the 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 for the case AND-OR depth 2 circuit. Next we 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 an identical set. This means 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 in figure 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 input; 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 $|\cap_i A_{i,\ell_i}|$, where $1 \leq \ell_i \leq s_i$, can be 0, 1 or an even number. Since if all the (i,ℓ_i)-th **AND** gates have all the n variables as inputs, then $|\cap_i A_{i,\ell_i}|$ must be 0 or 1; else if these **AND** gates do not have all variables as their inputs, then $|\cap_i A_{i,\ell_i}|$ is even. In the else case, if the size of intersection is non-zero, then $\cap_i A_{i,\ell_i}$ 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 $\vec{x} \in \cap_i A_{i,k_i}$. By the above observation, we have that $|\cap_i A_{i,\ell_i}| \leq 1$, where $1 \leq \ell_i \leq s_i$. In total we have at most $s_1 s_2 \cdots s_t$ intersections of $A_{i,j}$'s, which must be at least 2^{n-1} to guarantee that the circuit computes the parity function correctly. It is clear that the number of edges is at least $s_1 + s_2 + ... + s_t$, which is at least $t(s_1 s_2 \cdots s_t)^{\frac{1}{t}}$, since the arithmetic mean is greater or equal to the geometric mean. Therefore the number of edges is at least $t2^{\frac{n-1}{t}}$. This completes the proof. $\Box$

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 it as following.

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 by Håstad [3], we know that the top fan-in for the optimal depth 3 cricuit must be at least $\sqrt{n}$, which is proved as following.

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

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

Next we extend depth 3 edge lower bound to depth 4 OR-AND-OR-AND circuit. For such a depth 4 circuit that computes the parity function correctly with top fan-in m, we know 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 top fan-in t has at least $t2^{\frac{n-1}{t}}$ edges. The proof technique is by a simple counting argument. An obvious open question is: *can* *we apply this technique to depth* $d(>4)$ *circuits and other boolean functions?* According to our experience, 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, $\sum_1^1$-formula on finite structures, in *Ann. Pure and Appl. Logic 24 (1983)*, 1–48.

[2] M. Furst, J. Saxe and M. Sipser, Parity, circuits and the polynomial time hierarchy. *Math. Systems Theory 17 (1984)*, 13–27.

[3] J. Håstad, *Computational Limitations of Small-Depth Circuits*, MIT PRESS, Cambridge, MA, 1986.

[4] J. Håstad, S. Jukna and R. Pudlák. Top-Down Lower Bounds for Depth 3 Circuits, in *Computational Complexity 5 (1995)*, 99–112.

[5] A. A. Razborov, Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Math. notes of the Academy of Science of the USSR*, 41(4):333–338, 1987.

[6] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. 19th Ann. ACM Symp. Theor. Comput.*, 1987, 77-82.

[7] A. C-C. Yao. Separating the polynomial-time hierarchy by oracles. In *Proc. 26th IEEE Symposium on Foundations of Computer Science*, 1985, 1–10.