# A Circuit-Based Proof of Toda's Theorem


Ravi Kannan *
School of Computer Science
Carnegie-Mellon University
Pittsburgh, Pennsylvania 15213

H. Venkateswaran †
College of Computing
Georgia Institute of Technology
Atlanta, Georgia 30332-0280

V.Vinay *
Department of Computer Science and Automation
Indian Institute of Science
Bangalore 560012, India

Andrew C. Yao ‡
Department of Computer Science
Princeton University
Princeton, New Jersey 08544



*Supported in part by SFB 303.

†Supported in part by NSF grant CCR-8711749.

‡Supported in part by NSF grant CCR-8813283.

Running Head: CIRCUIT PROOF OF TODA'S THEOREM

Address for correspondence:

H. Venkateswaran

College of Computing

Georgia Institute of Technology

Atlanta, Georgia 30332-0280.

## ABSTRACT

We present a simple proof of Toda's result (Toda, 1989) which states that $\oplus P$ is hard for the Polynomial Hierarchy under randomized reductions. Our approach is circuit-based in the sense that we start with uniform circuit definitions of the Polynomial Hierarchy and apply the Valiant-Vazirani (1986) lemma on these circuits.

**List of symbols used**

| | |
|---|---|
| $O$ | upper case oh |
| 0 | zero |
| 1 | one |
| $v$ | vee |
| $\vert$ | vertical bar |
| $\in$ | set membership |
| $'$ | prime |
| $k$ | lower case kay |
| $\times$ | times |
| [ | left square bracket |
| ] | right square bracket |

# 1 Introduction

In this paper we give a simple proof of Toda's result (Toda, 1989) which states that $\oplus P$ is hard for the Polynomial Hierarchy ($PH$) under randomized reductions. The class $\oplus P$ is the class of all languages $L$ such that $L$ is accepted by a polynomial time nondeterministic Turing machine that accepts an input iff it has an odd number of accepting computations (Papadimitriou and Zachos, 1983). The original proof of this theorem is by Toda (1989) who uses it to prove the result that $PH \subseteq P^{PP}$. Our approach is circuit-based in the sense that we start with uniform circuit definitions of $PH$ (Vinay, Venkateswaran and Veni Madhavan, 1990) and apply the Valiant-Vazirani (1986) lemma on these circuits.

Our results demonstrate the usefulness of uniform circuit characterizations of standard complexity classes such as $NP$ . These circuit definitions served as a motivation to investigate the applicability of recent circuit complexity results to exponential size circuits. We claim that such characterizations have made it possible to isolate the combinatorial essence of Toda's proof more clearly. We also give new uniform circuit characterizations of the class $\oplus P$ and BP.$\oplus P$ . Here BP.$\oplus P$ is the class of all languages $L$ for which there exists a language $A \in \oplus P$ and a constant $\delta > 0$ such that, for any randomly chosen polynomial length string $y$, the probability that $[(x, y) \in A$ iff $x \in L]$ is at least $1/2 + \delta$. These circuit characterizations provide a combinatorial and algebraic framework to study the properties of these classes.

Allender (1989) motivated by Toda's proof technique, studied the simulation of constant depth polynomial size circuits by threshold circuits. Later, this result was extended in (Allender and Hertrampf, 1990) to uniform circuits. Our results, which were discovered independently, are proved for exponential size circuits. Considering exponential size circuits makes it possible to present Toda's proof in a circuit framework. The uniformity condition used here is also different and is based on recognition of the connection language of the circuits rather than generating circuit descriptions. The language recognition version of the uniformity condition is used since the circuits considered have exponential size. The focus of the results in (Allender and Hertrampf, 1990) is on depth reduction for unbounded fan-in circuits whereas our focus was on providing a simple proof of Toda's theorm using well known circuit techniques. Although it is not too difficult to derive our results and the simulation in (Allender and Hertrampf, 1990) of $AC^0$ by a uniform family of constant depth threshold circuits as corollaries of a general theorem, we believe that an explicit proof of Toda's theorem will be quite useful. Both our results use a lemma from Valiant and Vazirani (1986) to achieve uniformity.

## 2 Preliminaries

The Boolean circuits that we consider are, in general, uniform unbounded or semi-unbounded fan-in circuits. It is assumed that the negations appear only at the inputs. By semi-unbounded fan-in circuits we mean circuits where there is an asymmetry in the fan-in of the gates depending on the gate type. The uniformity condition for the circuit families considered is based on the recognition of the direct connection language defined as follows (Ruzzo, 1981): The *direct connection language* $L_{DC}$ of a family $\{G_n\}$ of Boolean circuits is the set of strings of the form $\langle n, g, y\rangle$ such that either (i) $g$ and $y$ are gate names and $y$ is an input of the gate $g$, or (ii) $g$ is a gate name and $y$ is the type of the gate $g$. A family $\{G_n\}$ of Boolean circuits of size $C(n)$ is said to be *uniform* if its direct connection language can be recognized by a deterministic Turing machine in time $O(\log C(n))$.

We will say that a language is recognized by a uniform family of randomized circuits $\{G_n\}$ if,

- the circuit $G_n$ has exactly $q(n)$ random (supplementary) inputs ($q$ is a polynomial), in addition to the original $n$ inputs.
- for all inputs of length $n$ in the language, $G_n$ evaluates to 1 for more than two-thirds of the random inputs, and
- for all inputs of length $n$ not in the language, $G_n$ evaluates to 1 for less than one-third of the random inputs.

Our results use uniform circuit characterizations of $NP$, $PH$ and $\oplus P$. It is known (Venkateswaran, 1988) that $NP$ is the class of languages recognized by a uniform family of semi-unbounded fan-in circuits of exponential size and constant depth with the restriction that the OR gates can have exponential ($2^{n^{O(1)}}$) fan-in but AND gates can have only polynomial fan-in. The characterizations of $PH$ and $\oplus P$ given below can all be obtained in a straightforward manner from the results in (Venkateswaran, 1988; Vinay, Venkateswaran and Veni Madhavan, 1990). We sketch their proofs for completeness. It should be noted here that this characterization of *PH* also follows from a parallel random access machine characterization of *PH* in (Immerman, 1989) and the well known correspondence between such machines and unbounded fan-in Boolean circuits (Stockmeyer and Vishkin, 1984).

**Lemma 1** *PH is exactly the class of languages recognized by a uniform family of constant depth, exponential size unbounded fan-in circuits over* {AND ,OR }. *( We call such circuits PH -circuits.)*

**Proof.** From the above definition of *NP* , it follows that *Co-NP* is the class of languages accepted by a uniform family of exponential size and constant depth semi-unbounded fan-in circuits with AND -gates with exponential fan-in and OR -gates with polynomial fan-in. A simple induction on $k$ can then be used to prove that $\Sigma_k^p$ is characterized by a uniform family of exponential size and constant depth circuits with alternating layers of *NP* and *Co-NP* circuits, beginning with an *NP* -layer.□

**Lemma 2** $\oplus P$ *is exactly the class of languages recognized by a uniform family of constant depth, exponential size unbounded fan-in circuits over* { XOR ,AND ,OR } *with the restriction that the* XOR *gates can have exponential fan-in but the other gates have polynomial fan-in. ( We call such circuits* $\oplus P$ *-circuits.)*

**Proof.** One direction follows from the fact that PARITY–SAT(the set of all conjunctive normal form formulas with an odd number of satisfying assignments) is complete for $\oplus P$ . For the other direction, note that it is sufficient to consider a circuit with XOR and AND gates only. A simulation of such a circuit by a polynomial time nondeterministic Turing machine can be done as described in lemma 15 in (Venkateswaran, 1988). The machine maintains a stack to do the circuit evaluation. At an XOR gate, the machine existentially guesses and recursively simulates an immediate predecessor. At an AND gate, the machine guesses the input gate names of the gate in order and pushes them on the stack. (The uniformity machine can be easily modified to verify the order of the inputs of an AND gate.) The machine then recursively simulates the first input of the AND gate. At a circuit input, the machine rejects if the input has value zero. If the circuit input has value one the machine either accepts or pops the gate on the top of the stack and recursively simulates it depending on whether the stack is empty or not. It is not difficult to see that the time taken by this machine is at most the maximum AND fan-in raised to the depth and that the machine accepts if and only if the $\oplus P$ circuit evaluates to a one.□

**Corollary 3** *BP.$\oplus P$ is exactly the class of languages recognized by a uniform family of randomized $\oplus P$ -circuits.*□

## 3 The Result

The lemmas in the previous section together with the following theorem prove Toda's theorem.

**Theorem 4** *Let $\{G_r\}$ be a family of uniform PH - circuits. Then, there is a uniform family of randomized $\oplus P$ -circuits that recognize the same language as $\{G_r\}$.*

**Proof.** We assume that the fan-in of all the gates is exactly $2^p$. We will replace every unbounded fan-in gate, $v$, by a randomized $\oplus P$ -circuit $F_v$. Consider an OR gate $v$ in $G_r$. We use the following lemma by Valiant and Vazirani (1986). Note that the inner product used is over (XOR , AND ).

**Lemma 5** *Let $S$ be a nonempty subset of $\{0,1\}^p$. Let $w_1, \cdots, w_p$ be random $p$ bit vectors, and let $S_i = \{j \mid j \in S, j \cdot w_1 = \cdots = j \cdot w_i = 0\}$ for each $1 \leq i \leq p$. Then, the probability that $|S_i| = 1$ for some $1 \leq i \leq p$ is at least $1/4$.*□

Our randomized circuit has a random $d(r) \times p$ matrix $W$ as supplementary input ($d(r)$ to be determined later). For $1 \leq i \leq d(r)$, row $i$ of this matrix consists of $p$ entries $w_{i,1}, \cdots, w_{i,p}$, each of which is a $p$-bit vector. **All $F_v$ receive the same set of random bits as supplementary input.**

Replace $v$ by an OR gate $v'$ with $d(r)$ input gates. Let these input gates be denoted as $u_1, \cdots, u_{d(r)}$. Each of the gates $u_i$ of $v'$ is an OR gate. For $1 \leq i \leq d(r)$, the gate $u_i$ has as inputs $p$ XOR gates $u_{ik}$, $1 \leq k \leq p$. Each of these XOR gates $u_{ik}$ have as inputs $2^p$ AND gates $u_{ikj}$ for $0 \leq j \leq 2^p - 1$. An AND gate $u_{ikj}$ has two inputs: (a) the gate that is the $j$-th input of $v$, and

(b) a subcircuit that verifies that, for all $1 \leq h \leq k$, the inner product of the $p$-bit binary vector representing $j$ with the $p$-bit vector $w_{ih}$ is zero.

If the chosen gate $v$ were an AND gate in $G_r$, the above construction is used after transforming $v$ into an OR gate using DeMorgan's law and XOR gates. It is easy to check that the final circuit so obtained is a $\oplus P$ -circuit if $d(r)$ is chosen to be a polynomial.

Let $\mathcal{H}_r$ denote the constructed circuit. We first show that the circuit family $\{\mathcal{H}_r | r \geq 1\}$ is uniform by giving a scheme to label the gates of $\mathcal{H}_r$. The labeling is illustrated for the circuit replacing the gate $v$.

Let $v$ be labeled as $L(v)$ in $G_r$. The output gate $v'$ is labeled $L(v)$ also. For $1 \leq i \leq d(r)$, let $u_i$ be labeled as $[L(v), i]$. For $1 \leq i \leq d(r)$, $1 \leq k \leq p$, let $u_{ik}$ be labeled as $[L(v), i, k]$. For $1 \leq i \leq d(r)$, $1 \leq k \leq p$, $0 \leq j \leq 2^p - 1$, let $u_{ikj}$ be labeled as $[L(v), i, k, j]$.

To complete the proof, we have to show that the error committed by the resulting circuit is quite small. Let $C$ be the size of the circuit $\mathcal{H}_r$ and let $depth(u)$ denote the depth of the gate $u$ in this circuit. By choosing the set $S$ in lemma 5 to be $\{j \mid j\text{th input of } v \text{ in } G_r \text{ evaluates to } 1\}$, it can be verified that the error committed at any gate $u$ in $\mathcal{H}_r$ is at most $C^{depth(u)} * (\frac{3}{4})^{d(r)}$. So choosing $d(r)$ to be a suitably large polynomial we can make this error as small as possible. It should be noted that the number of random bits used is $p^2 \times d(r)$ which is a polynomial since $d(r)$ is. □

The corollary below shows that unboundedness does not help over semi-unboundedness for certain uniform families of circuits. The proof follows from the characterization of BP.$\oplus P$ in corollary 3 and the proof of theorem 4, which shows how to replace unbounded fan-in OR and AND gates by randomized $\oplus P$ -circuits.

**Corollary 6** *BP.$\oplus P$ is exactly the class of languages recognized by a uniform family of constant depth, exponential size unbounded fan-in randomized circuits over the basis* {XOR , OR , AND }.□

**Acknowledgements:** The first and the third author thank the Forschungsinstitut für Discrete Mathematik and Institut für Operations Research of the University of Bonn. The second author is thankful to Gil Neiger, Gary Peterson, Larry Ruzzo and Martin Tompa for some very useful comments.

## References


E. Allender (1989), A note on the power of threshold circuits, *in* "Proceedings, 30th Annual IEEE Symposium on Foundations of Computer Science", pp. 580-584.

E. Allender and U. Hertrampf (1990), On the power of uniform families of constant depth threshold circuits, *in* "Proceedings, 15th International Symposium on Mathematical Foundations of Computer Science", pp. 158-164, Lecture Notes in Computer Science, Vol. 452, Springer-Verlag, New York/Berlin.

N. Immerman (1989), Expressibility and parallel complexity, *SIAM J. Comput.* **18**, 625-638.

C.H. Papadimitriou and S. Zachos (1983), Two remarks on the power of counting, *in* "Proceedings, 6th GI Conference on Theoretical Computer Science", pp.269-276, Lecture Notes in Computer Science, Vol. 145, Springer-Verlag, New York/Berlin.

W.L. Ruzzo (1981), On uniform circuit complexity, *J. Comput. System Sci.* **22**,365-383.

L. Stockmeyer and U. Vishkin (1984), Simulation of parallel random access machines by circuits, *SIAM J. Comput.* **13**, 409-422.

S. Toda (1989), On the computational power of PP and $\oplus P$ , *in* "Proceedings, 30th Annual IEEE Symposium on Foundations of Computer Science", pp. 514-519.

L.G. Valiant and V.V. Vazirani (1986), NP is as easy as detecting unique solutions, *Theoretical Comput. Sci.* **47**, 85-93.

H. Venkateswaran (1988), Circuit definitions of nondeterministic complexity classes, *in* "Proceedings, 8th Annual Foundations of Software Technology aand Theoretical Computer Science Conference", pp. 175-192, Lecture Notes in Computer Science, Vol.338, Springer-Verlag, New York/Berlin.

V.Vinay, H.Venkateswaran, C.E.Veni Madhavan (1990), Circuits, Pebbling and Expressibility, *in* "Proceedings, 5th Annual Conference on Structure in Complexity Theory", Barcelona, Spain, pp. 223-230.