On the Expected Depth of Boolean Circuits

Josep Díaz
María J. Serna
Paul Spirakis
Jacobo Torán

Report LSI–94–7–R

On the expected depth of Boolean circuits *

J.Díaz[†] M.J.Serna[†] P.Spirakis[‡] J.Torán[†]

Abstract

In this paper we analyze the expected depth of a circuit randomly generated from a uniform model. We show that the expected depth of such circuits is polylogarithmic in the number of gates. This result allows us to place the monotone circuit value problem in average NC.

1 Introduction

The *Circuit Value Problem* (CVP) consists in deciding whether a given Boolean circuit with values assigned to the input gates produces value 1 as output. The problem was shown to be P-complete for general circuits by Ladner [Lad75]. Goldschlager proved that the problem remains P-complete for the more restrictive class of monotone circuits with bounded fan-out [Gol77]. These results indicate that the problem is inherently sequential and therefore, assuming that NC $\neq$ P, CVP can not be solved quickly in parallel with a feasible ammount of processors. However it could still be the case that there is an algorithm using a polynomial number of processors that solves the problem in polylogarithmic time for "almost all" instances. This approach has been considered for other P-hard problems, for example in [CRT87] and [CF90].

A natural way to evaluate a circuit consists in computing level by level the values of its gates, evaluating in parallel all the gates at the same level. The time needed to do this is closely related to the circuit's depth; in the worst case, the size and depth of a circuit have the same magnitude, but on the other hand, shallow circuits can be quickly evaluated in parallel using this procedure.

In this article we are interested in the average time needed for this evaluation procedure. We consider two classes BC and UC of monotone bounded/unbounded fan-out circuits, and show that on the average these circuits have polylogarithmic depth with respect to

* This research was supported by the ESPRIT BRA Program of the EC under contract no. 7141,project ALCOM II.

[†] Departament de Llenguatges i Sistemes, Universitat Politècnica Catalunya Pau Gargallo 5, 08028-Barcelona, diaz@lsi.upc.es/mjserna@lsi.upc.es/ jacobo@lsi.upc.es

[‡] Computer Technology Institute, Patras University, spirakis@cti.gr

their size. The average is measured considering a uniform distribution on the circuit descriptions, i.e., every circuit description is counted once. As usual the circuit description will be the sequence of numbered inputs and gates with their respective fan-in connections. This result implies that on the average, the *Circuit Value Problem* for monotone circuits can be computed in polylogarithmic time using a polynomial number of processors.

2 The Uniform Incremental Model

A Boolean circuit α, with n inputs is a finite directed acyclic graph with labelled nodes. Nodes with in-degree 0 are called the *input nodes*, all the remaining nodes are the *gates*. Each gate has associated a function from a given set of boolean functions. A circuit is *monotone* when the set of functions is restricted to the fan-in two $\{\vee, \wedge\}$ gates. Let n be the number of inputs, m the number of gates and $N = n + m$ be the total number of nodes in the circuit. The *depth of a gate* g is defined to be the length of the longest directed path from the inputs (all at depth zero) to g. The *depth of the circuit* is the maximum of the depth of its gates, let d denote the depth of a circuit. Notice that the depth function produces a layering of any circuit. Given a circuit, the *level* L_k will consist of all nodes at depth k. For general background on circuit complexity see [Sav76, Weg87].

A description of a monotone circuit α is a sequence $(\alpha_1, \ldots, \alpha_N)$ where each α_i is either an assignment of a value 1/0 to an input, or $f(\alpha_j, \alpha_k)$ for $f \in \{\wedge, \vee\}$ (gate), with $j, k < i$. The value $v(\alpha_i)$ of a gate α_i in the circuit α, is defined as follows: If α_i is an input 1/0 then $v(\alpha_i) = 1/0$ and if $\alpha_i = f(\alpha_j, \alpha_k)$ then $v(\alpha_i) = f(v(\alpha_j), v(\alpha_k))$. We define the value of the circuit, $v(\alpha)$, to be $v(\alpha_n)$. The fact that every gate is connected only to gates with a smaller number prevents feedback loops. Each description corresponds to a labelled directed acyclic graph of restricted in-degree. We keep n nodes with in-degree 0 and unbounded out-degree correspondig to the n circuit inputs. The remaining m nodes correspond to gates and will have in-degree two. Assuming that circuit gates are only gates $\{\wedge, \vee\}$, each description in which neither the gate functions nor the inputs are fixed, can generate 2^{m+n} different circuits.

We examine circuits w.r.t. their topology, i.e. as labelled directed acyclic graphs of restricted in-degree and/or out-degree.

In order to construct circuits at random, we use an incremental process starting by the inputs, adding a gate at each time. The way each new node randomly chooses its inputs allows us to model different classes of circuits.

A non-input node is defined to be *saturated* when its out-degree (fan-out) is equal to a pre-specified constant (e.g. 2). We consider that all input nodes are always non-saturated.

We start with the n input nodes. When a new node is added, first it selects equiprobably at random non-saturated node as its first input. Again a second node is selected equiprobably at ramdom from the set of non-saturated nodes, as second input.

Let BC denote the class of circuits generated by the above procedure. Notice that all circuits generated in such a way have fan-in two and constant fan-out. Moreover, the incremental procedure provides a topological ordering of the circuit, by assigning to each gate the number of the time step at which it is added.

Consider a second model in which we drop the condition of distinguishability between saturated and non-saturated nodes. Let the class UC be the class of circuits constructed as follows: Start with the n input nodes. When a new node is added, it will have as inputs two different nodes selected uniformly at ramdom among all the nodes in the current graph. Circuits in UC have gates with unbounded fan-out and fan-in two.

Notice that UC and BC are classes of circuits each one with an underlaying probability distribution.

Let us now analyze the probability that a circuit in UC has high out-degree. Given a circuit $C \in UC$ for any node v of C, then

$$\Pr\{v \text{ is selected } k' \text{ times }\} \leq \left(\frac{1}{n}\right)^{k'}$$

Thus

$$\Pr\{\text{ there is a node selected } k' \text{ times }\} \leq (n+m)\left(\frac{1}{n}\right)^{k'}$$

Let $\mathcal{E}$ be the event *"no node is selected more than k' times"* for constant k'. That is the equivalent as the event *"the circuit C has bounded fan-out (k') and fan-in two"*. Thus we have,

Lemma 1 *Any circuit in UC with $O(n^k)$ nodes have constant fan-out k', with probability of $1 - n^{k-k'}$, for $k' > k+2$.*

As it is well known by the Shannon-Lupanov theorem that asymptotically almost all Boolean functions on n variables have circuit complexity $\Theta(2^n/n)$ [Weg87], we shall restrict our models to circuits with at most exponential number of gates in the number of inputs.

Lemma 2 *Any circuit in UC with $N = O(2^n)$ nodes has fan-out $O(\log N)$ with probability at least $1 - N^{-\delta}$ for some constant $\delta > 2$.*

In the next section we will restrict ourselves to UC circuits, as it is easier to work with them, however for circuits with polynomially many gates the expected depth of circuits in the UC and BC models, relates as follows.

Lemma 3 *Let d be the depth of a random circuit with $O(n^k)$ nodes in the UC model, and let d' be the depth of a random circuit of the same size in the BC model. Then we have*

$$(1 - n^{-(k-2)})E[d'] \leq E[d] \leq E[d'] + n^{-2}$$

Proof. Let d be a random variable indicating the depth of a circuit $C \in UC$.

$$E[d] = E[d/\mathcal{E}]P(\mathcal{E}) + E[d/\overline{\mathcal{E}}]P(\overline{\mathcal{E}})$$

thus,

$$E[d] \geq E[d/\mathcal{E}]P(\mathcal{E})$$

and

$$E[d] \leq E[d/\mathcal{E}]P(\mathcal{E}) + n^k P(\overline{\mathcal{E}}) \leq E[d/\mathcal{E}] + n^k P(\overline{\mathcal{E}})$$

therefore

$$(1 - n^{-(k'-k)})E[d/\mathcal{E}] \leq E[d] \leq E[d/\mathcal{E}] + n^k n^{-(k'-k)}$$

Choosing $k' \geq 2k + 2$ we get the result. □

The previous equation tells that in the case of polynomial size circuits, we just need to compute $E[d]$ in the UC model to infer results for the BC model. This allows us to work on the UC model.

3 Analysis of the circuit's depth

Assume that we have a circuit constructed uniformly incrementally in the UC model, consisting of $N = n + m$ nodes. We would like to know how many additional levels $\Delta(N)$ will be created when adding $N/\log(N)$ new nodes. (In other words we wish to study how much the depth increases).

To compute an upper bound $\Delta^*(N)$ for $\Delta(N)$, assume that *all N nodes are at the highest possible level*. Such a case presents the maximum growth in the depth of the new formed circuit. We prove first an upper bound for the $\Delta^*(N)$.

Lemma 4 *For some constants $\gamma > 1$ and $\delta > 2$, with probability at least $1 - N^{-\delta}$ we have $\Delta^*(N) \leq \gamma \log N$.*

Proof. Let L_d be the current highest possible level (before any of the $N/\log N$ nodes were added). Let L_{d+1} be the immediate next new level created.

Assume that a new node goes to L_{d+1} with probability p_1, actually p_1 is a function in the number of currently added nodes, but through the whole process of adding the $N/\log N$ nodes will be bigger than $1 - 2\frac{N/\log N}{N+N/\log N} \geq 1/2$. By the Chernoff bounds (see [HR90]) the maximum size of L_{d+1} is $\mid L_{d+1}^{\max} \mid = \Theta(\frac{N}{\log N})$, with probability at least $1 - \exp(-\frac{\beta^2}{2}\frac{N}{\log N})$, for any $\beta \in (0,1)$.

For $i = 1, 2, \ldots, k$ define $\mathcal{E}_i$ as the event that when adding $N/\log N$ nodes we get that $\mid L_{d+i}^{\max} \mid = \Theta(\frac{N}{\log' N})$.

Conditioning in $\mathcal{E}_1$, a new node goes to L_{d+2} with probability (of success) $p_2 = 2\frac{\lfloor L_{d+1} \rfloor}{N}$. Considering the additions when $\mid L_{d+1}^{\max} \mid /2 \leq \mid L_{d+1} \mid \leq \mid L_{d+1}^{\max} \mid$ we get $p_2 = \Theta(\frac{1}{\log N})$. By the Chernoff bounds the number of nodes added to L_{d+2} will be at most twice $p_2 \mid L_{d+1}^{\max} \mid /2$, which means that

$$\mid L_{d+2}^{\max} \mid = \Theta(\frac{N}{\log^2 N})$$

with probability at least $1 - \exp(-\frac{\beta^2}{2}\frac{N}{\log^2 N})$ for any $\beta \in (0,1)$.

Using the same argument as before, conditioning on the events $\mathcal{E}_1, \ldots, \mathcal{E}_k$, we get that for any $\beta \in (0,1)$,

$$\mid L_{d+k+1}^{\max} \mid = \Theta(\frac{N}{\log^{k+1} N})$$

with probability at least $1 - \exp(-\frac{\beta^2}{2}\frac{N}{\log^{k+1} N})$.

The process can be carried out until the case $k = k_{\max} = \Theta(\dfrac{\log N}{\log\log N})$ where there are at most $a \log N$ remaining nodes to be placed (the last nodes can create at most $a \log N$ additional levels). For this case we get,

$$\begin{aligned}
&\Pr\{\text{all } \mathcal{E}_i \text{ hold for } k = 1, \ldots, k_{\max} - 1\} \\
&= \Pr(\mathcal{E}_1)\Pr(\mathcal{E}_2/\mathcal{E}_1)\ldots\Pr(\mathcal{E}_{k_{\max}-1}/\mathcal{E}_1, \ldots, \mathcal{E}_{k_{\max}-2}) \\
&\geq \textstyle\prod_{k=1}^{k_{\max}-1}(1 - \exp(-\frac{\beta^2}{2}\frac{N}{\log^k N})) \\
&\geq 1 - \textstyle\sum_{k=1}^{k_{\max}-1}\exp(-\frac{\beta^2}{2}\frac{N}{\log^k N}) \\
&\geq 1 - \Theta(\tfrac{\log N}{\log\log N})\exp(-\tfrac{\beta^2}{2}\log N).
\end{aligned}$$

Therefore we can choose a $\delta > 2$ to get this probability at least $1 - N^{-\delta}$, which implies that with high probability, the expected upper bound for the increment of the number of levels is at most

$$\Delta^*(N) = \Theta(\frac{\log N}{\log\log N}) + a \log N \leq (a+1)\log N.$$

Taking $\gamma = a + 1$ the lemma follows. □

As a corollary to the previous lemma, we can obtain the main result.

Theorem 1 *The expected depth of a random circuit in UC with N nodes is at most $\gamma \log^3 N$, for some constant $\gamma > 1$.*

Proof. Let d_N be the random variable denoting the depth of circuits restricted to N nodes. Its expectation $E[d_N]$ satisfy the following recursion,

$$E[d_N] + E[\Delta(N)] = E[d_{N+\frac{N}{\log N}}]$$

using Lemma 4 we get:

$$E[d_{N(1+\frac{1}{\log N})}] \leq E[d_N] + \gamma \log N$$

The solution to the recursion proves the Theorem. □

Using Lemma 3, we also can state the following result,

Theorem 2 *The expected depth of a random circuit with $O(n^k)$ gates in BC is at most $\tau \log^3 n$ for some constant $\tau > 1$.*

4 Average complexity of CVP

Recall that the *Circuit Value Problem* has the following formulation: given an encoding of a boolean circuit α, together with an input assignment $x_1, \ldots x_n$ compute α on $x_1, \ldots x_n$.

The standard encoding of a problem instance is a collection of tuples indicating, gate number, type of gate, together with the gate number of its inputs. Thus each input to the CVP problem incorporates a topological ordering of the circuit. Thus the proposed models UC and BC provides a uniform distribution for the instances to CVP restricted to monotone circuits or fan-out two monotone circuits. As mentioned in the introduction, CVP is P-complete, so there is little hope in finding fast parallel algorithms for the problem. However, based on the results from the previous section we can consider a straightforward parallel algorithm that works fast for most of the possible input instances. Based on the definition of average polynomial time [Gur91], we give the following definition for average NC.

Definition 1 *Let L be a decisional problem and μ_n be a probability distribution that assigns probabilities to strings of length n. We say that L is in average NC (with respect to μ) if there is a parallel algorithm for L running on a polynomial number of processors in time t, and for some constant k and every length n*

$$\sum_{|x|=n} t(x)\mu_n(x) \leq k \log^k(n).$$

We consider the following algorithm for the PRAM models (see for example [JaJ92] for an introduction to the shared memory SIMD). In order to evaluate the circuit on a PRAM we just start evaluating inputs, after that we proceed by levels. Thus the total time (depending on the model of PRAM we use) will depend on the depth of the circuit and the fan-out, fan-in of the gates, while the number of processors is number of gates. Given a circuit with N gates, fan-in p, fan-out q, and depth d, evaluating on a

- CRCW PRAM takes $O(d)$ time
- CREW PRAM takes $O(d)O(\log q)$ time
- ERCW PRAM takes $O(d)O(\log p)$ time
- EREW PRAM takes $O(d)O(\log p)O(\log q)$ time

using $O(N)$ processors.

From Lemma 2, Theorem 1 and the considerations about time bounds for evaluating the circuits, the expected time is polylog in N, and we have

Theorem 3 *CVP for monotone circuits is in average NC (with respect to the uniform distribution).*

Using Theorems 1 and 2, for the BC circuits we get,

Theorem 4 *For each constant k, CVP for bounded fan-out monotone circuits with n inputs and the number of gates bounded by n^k, is in average NC (with respect to the uniform distribution).*

It is easy to see that CVP for bounded fan-out monotone circuits with at most a quadratic number of gates remains P-complete. As a consequence the previous theorem implies that this version of CVP is also in average NC.

5 Conclusions

We have shown that in the uniform model the expected depth for a circuit with N nodes and gates with unbounded fan-out is $O(\log^3 N)$ and this holds with high probability ($\geq 1 - N^{-\delta}$ for some constant $\delta > 2$). This facts imply the monotone circuit value problem can be computed in polylogarithmic expected time with a polynomial number of processors.

The previous result also holds in the uniform model for circuits with polynomially (in the number of inputs) many gates and constant fan-out gates. We conjecture that the expected depth is still polylog for the general case in the BC model.

Something to observe is that in the incremental model studied, we have a uniform distribution over circuit encodings but not over circuits. In other words, a circuit considered as a graph without labels on its gates can be produced many times (one for every possible topological sorting of its gates). The estimation of the depth of a circuit in a model that does not distinguish between different labelings is an interesting open question.

The distribution used is a natural one. However, changing the probability distribution, we can obtain different behaviours on the depth of the circuit. For instance, if Γ denotes the probability that the next node added increases the depth of the circuit, $\Gamma = 1/N$, produces circuits with at most logarithmic expected depth. If we consider the probability distribution given by $\Gamma = 1/|L_d|$ the expected depth of a circuit is clearly polynomial. It is an interesting open question to study the evolution of the expected depth of a random circuit as the Γ changes. these extreme models. In particular it would be interesting to investigate the existence of threshold values for Γ where the expected depth changes from polynomial to polylog.

References

[CF90] N. Calkin and A. Frieze. Probabilistic analysis of a parallel algorithm for finding maximal independent sets. *Random Structures and Algorithms*, 1:39–50, 1990.

[CRT87] D. Coppersmith, P. Raghavan, and M. Tompa. Parallel graph algorithms that are efficient on the average. In *28 IEEE Symposium on Foundations of Computer Science*, pages 260–269. IEEE Society, 1987.

[Gol77] L.M. Goldschlager. The monotone and planar circuit value problems are log space complete for P. *SIGACT News*, 9:25–29, 1977.

[Gur91] Y. Gurevich. Average case analysis. *J. Computer and System Sciences*, 42:346–398, 1991.

[HR90] T. Hagerup and C. Rub. Aguided tour of Chernoff bounds. *Information Processing Letters*, 33:305–308, 1990.

[JaJ92] J. JaJa. *An introduction to parallel algorithms.* Addison-Wesley, 1992.

[Lad75] R.E. Ladner. The circuit value problem is log space complete for P. *SIGACT News*, 7:18–20, 1975.

[Sav76] J. Savage. *The complexity of Computing.* John Wiley, Chichester, 1976.

[Weg87] I. Wegener. *The Complexity of Boolean Functions.* Wiley-Teubner, Chichester-Stuttgart, 1987.

Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya

Recent Research Reports

LSI-93-45-R "Nominalizations in the LKB framework", Irene Castellón Masalles.

LSI-93-46-R "Subcategorization alternances generation via lexical rules", Mariona Taulé Delor, M. Antònia Martí Antonín, and Irene Castellón Masalles.

LSI-93-47-R "Dealing with lexical mismatches", Carmen Soler and Ma. Antònia Martí.

LSI-93-48-R "Translation equivalence via lexicon: a study on tlinks", Anna Samiotou, Irene Castellón, Francesc Ribas, and German Rigau.

LSI-93-49-R "A class-based approach to learn appropriate selectional restrictions from a parsed corpus", Francesc Ribas.

LSI-94-1-R "Logspace and logtime leaf languages", Birgit Jenner, Pierre McKenzie, and Denis Thérien.

LSI-94-2-R "Degrees and reducibilities of easy tally sets", Montserrat Hermo.

LSI-94-3-R "Isothetic polyhedra and monotone boolean formulae", Robert Juan-Arinyo.

LSI-94-4-R "Una modelizaciòn de la incompletitud en los programas" (written in Spanish), Javier Pérez Campo.

LSI-94-5-R "A multiple shooting vectorial algorithm for progressive radiosity", Blanca Garcia and Xavier Pueyo.

LSI-94-6-R "Construction of the Face Octree model", Núria Pla-Garcia.

LSI-94-7-R "On the expected depth of boolean circuits", Josep Díaz, María J. Serna, Paul Spirakis, and Jacobo Torán.

Copies of reports can be ordered from:

Nuria Sánchez
Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028 Barcelona, Spain
`secrelsi@lsi.upc.es`