On the Depth of Randomly Generated Circuits*

Tatsuie Tsukiji (築地 立家)
Dept. of Computer Science, Tokyo Institute of Technology
Meguro-ku Ookayama, Tokyo 152, Japan
Email: tsukiji@cs.titech.ac.jp

Fatos Xhafa
Dept. of LSI, Faculty of Informatics, UPC
Pau Gargallo 5, 08028 Barcelona, Spain
Email: fatos@goliat.upc.es

Abstract

This research is motivated by the Circuit Value Problem; this problem is well known to be inherently sequential. We consider Boolean circuits with descriptions length d that consist of gates with a fixed fan-in f and a constant number of inputs. Assuming uniform distribution of descriptions, we show that such a circuit has expected depth $O(\log d)$. This improves on the best known result. More precisely, we prove for circuits of size n their depth is asymptotically $ef \ln n$ with extremely high probability. Our proof uses the coupling technique to bound circuit depth from above and below by those of two alternative *discrete-time* processes. We are able to establish the result by embedding the processes in suitable *continuous-time* branching processes. As a simple consequence of our result we obtain that monotone CVP is in the class average NC.

Key Words: random circuits, depth, recursive trees, domination by coupling, continuous Poisson process.

1 The Problem and Motivation

A circuit is a directed acyclic graph whose nodes are labeled from a given set: the nodes with in-degree 0 are called inputs and all the remaining nodes are gates. Circuits are a widely used model for both sequential and parallel computations by giving appropriate labels to nodes. For parallel computations, the size of a circuit – the number of its gates – corresponds to the cost of the structure, while its depth – the length of a longest path – corresponds to its computation time. Furthermore, circuits consist an excellent model for computation of Boolean functions, namely, if inputs are labeled by Boolean variables and gates by Boolean functions, then Boolean circuits are obtained (see e.g., [BDG95, page 106]).

Our model of circuit comes from the Circuit Value Problem (CVP) in which the instance of the problem is a description $(\alpha_1, \ldots, \alpha_a, \alpha_{a+1}, \ldots, \alpha_{a+n})$ where $\alpha_1, \ldots, \alpha_a$ are inputs and each α_i with $i > a$ is a gate $\alpha_i = (\alpha_{j_1}, \ldots, \alpha_{j_f})$ with $j_k < i$, $1 \leq k \leq f$. A simple parallel algorithm to decide

*This research was supported by ESPRIT Long Term Research Project 20244-ALCOM-IT.

the output value of the circuit is: compute the gates level by level, where all the gates of one level are computed in parallel. Thus, the parallel time depends on the depth of the circuit. We assume uniform distribution of descriptions and show that the depth of size $n$ circuits (with a constant number of inputs) converges to $ef \ln n$ in probability, i.e., for any $\varepsilon > 0$, the probability that it is between $(ef - \varepsilon) \ln n$ and $(ef + \varepsilon) \ln n$ tends to 1 as $n \to \infty$. For simplicity we will consider Boolean circuits with binary gates ($f = 2$); the result can be easily extended to the general case.

Díaz et al. [DSS$^+$94] study the average NC complexity[1] of monotone CVP. They use the following incremental process to generate at random a circuit $C_{a,n}$ beginning with $a$ inputs. Generally, $C_{a,n}$ is a circuit on the set of $n+a$ nodes $1, \ldots, n+a$. $C_{a,0}$ consists simply of $a$ input nodes, labeled by $1, \ldots, a$. To obtain $C_{a,n+1}$ from $C_{a,n}$, the gate $n+1$ is joined by edges to two nodes chosen from $\{1, \ldots, n\}$ uniformly at random with replacement. We refer to these circuits as *random recursive circuits*. In [DSS$^+$94], the authors gave two upper bounds for the depth of $C_{a,n}$. The first one is $O(\log^3 n)$ and is easy to understand while the second one shows a more tight bound $4e \ln n$. Both of these bounds were proved by straightforward methods. They also presented a lower bound $e \ln n$, which was derived easily by a result of [Pit94] on recursive trees. As a simple consequence of our result for $f = 2$, we are able to decide the constant, i.e., the depth of $C_{a,n}$ converges to $2e \ln n$ in probability. Thus, in terms of parallel time computation, we have that the expected time to decide the output of a monotone CVP is $2e \ln n$, asymptotically.

Another interesting related work in this line is that of Codenotti et al. [CGS95], where strong lower bounds on the expected parallel time to compute Boolean functions by circuits are given. They consider self-time circuits – a model in which gates compute their output as soon as it is determined (possibly by a subset of the inputs to the gate).

2 Proof Outline, Definitions and Notations

Instead of handling a random recursive circuit $C_{1,n}$, we consider alternative incremental processes B_n and $D_n^{(k)}$ which are easier to analyze, and such that their depths bound that of $C_{1,n}$ from above and below (we only consider the case $a = 1$ since similar arguments hold also for general $C_{a,n}$ with a fixed $a$.) We then prove that their depths converge to $2e \ln n$, in probability. Following, we give an alternative notation for circuits and then a more precise sketch of the proof. For a circuit $C$, $depth(i)$ denotes the depth of the node $i$, i.e., the length of a longest path from an input to it. Since we concern the depth, we may look a circuit $C$ on the set of nodes $\{1, \ldots, n\}$ as a string of non-negative integers $depth(1) depth(2) \cdots depth(n)$. Thus, a recursive circuit is an incremental string, whose tail component takes a random value according to the inherent distribution. When dealing with strings, we use subscripts and superscripts to denote different components and strings, respectively. Thus, s_i^j is the $i$th component (or its value) of string s^j. For convention, we give a total order to the components of a string $s$ by taking $s_i + (i-1)/n$, and denote by $s(i)$ the value of the $i$th smallest component of $s$. For example, if $s = 0121$ then $s(1) = 0$, $s(2) = s(3) = 1$ and $s(4) = 2$ (by convention the second

[1] The average NC is the class of the problems that admit parallel algorithms with *polylog* expected running time and use a *polynomial* number of processors.

smallest component is s_2 while the third smallest one is s_4.)

An *incremental string* X_n with a *transition distribution* $\{P_{ni}\}$, $P_{n1} + P_{n2} + \cdots + P_{nn} = 1$ for any $n = 1, 2, \ldots$, is the output of a discrete-time Markov process at time $t = n$: the process starts from $X_1 = 0$. Generally, the length of X_n is $n$. At time $t = n$, it gives to the $n$th component the value $X_{n-1}(i) + 1$, where $i$ is randomly chosen from $\{1, \ldots, n-1\}$ according to the distribution $\Pr[i = x] = P_{nx}$. Since a recursive circuit $C_n := C_{1,n-1}$ decides its $n$th component as $\max\{C_{n-1}(i), C_{n-1}(j)\} + 1$, where $i, j$ are chosen from $\{1, \ldots, n\}$ uniformly at random with replacement, it is an incremental string with transition distribution $M_{ni} = (2i-1)/n^2$.

Note that the depth of C_n is $\max(C_n) := \max_i C_n(i)$. More generally, for any incremental string of integers X_n, we consider the depth of X_n the maximum of any integer in X_n. In order to establish an upper bound for the depth of C_n, we propose an alternative incremental string B_n such that $\max(B_n)$ stochastically dominates $\max(C_n)$, i.e.,

$$\Pr[\max(B_n) \geq i] \geq \Pr[\max(C_n) \geq i] \quad \text{for any } i \ . \tag{1}$$

The transition distribution of B_n is given by $L$: $L_{ni} = 2/n$ if $n/2 \leq i \leq n$ and 0 otherwise. So, the $n$th component of B_n is $B_{n-1}(i) + 1$, where $i$ is chosen uniformly from the half largest components of B_n. Clearly, $L$ dominates $M$, i.e.,

$$\sum_{i \leq x \leq n} L_{nx} \geq \sum_{i \leq x \leq n} M_{nx} \quad \text{for any } n \text{ and } i \ . \tag{2}$$

Therefore, intuitively, the intensity of growth of $\max(C_n)$ is smaller than or equal to that of $\max(B_n)$ for each discrete-time $t = n$. Moreover, since both processes start from the same state 0, $\max(B_n)$ may dominate $\max(C_n)$ at any time. This intuition is formally proved due to the existence theorem of a coupling for a pair of general Markov chains (see, e.g., [Lin92, pp 127–131]). We will give, however, an elementary proof of this theorem for incremental strings. First, for the completeness of the paper; secondly, our simple case may illuminate the general theorem (i.e., Strassen's theorem [Str65]) with a short proof; and finally, we actually exhibit an algorithm which inputs a pair of transition distributions and outputs a coupling of them.

To show a lower bound on $\max(C_n)$, we consider the incremental string $D_n^{(k)}$, with a parameter $k = 1, 2, \ldots$, whose transition distribution is the following $k$-step staircase distribution $N^{(k)}$: $N_{ni}^{(k)} = 2(x+0.5)/kn$ if $xn/k < i \leq (x+1)n/k$. Then, for any $k$, $M$ dominates $N^{(k)}$, hence $\max(C_n)$ dominates $\max(D_n^{(k)})$.

We prove, for any $\varepsilon > 0$, with probability one, that $(2e + \varepsilon)\ln n$ and $(2e - \varepsilon)\ln n$ are upper and lower bound for B_n and $D_n^{(k)}$ (for sufficiently large $k$), respectively. These bounds imply that $\max(C_n) \to 2e \ln n$, in probability. To show this, we follow Pittel's proof for the height of random recursive trees. A size $n$ recursive tree has $n$ nodes labeled by $1, \ldots, n$. The root is 1, and the labels increase along every path leading away from 1. Several measures of (uniformly distributed) random recursive trees are well understood, including depth of nodes [Szy90, Mah91], the distribution of leaves in a rooted subtree [MS91], and the height [Pit94], which we use in our proof. (We suggest to the reader the survey by Smythe and Mahmoud [SM95].) Pittel proves this strong law for $\max(R_n)$: $\max(R_n) \to e \ln n$ in probability. He considers a continuous-time birth process R_t. The initial ancestor is born at time $t = 0$, producing its children according to a Poisson process with rate 1 (a pure birth process with independent $Exp(1)$ inter-birth times); each child mimics its parents, producing their children independently according to the (time shifted) Poisson process. Consider the chronological sequence of birth times $t_1 < t_2 < \cdots$ so that t_n is the moment when the $n$th child is born ($t_1 := 0$). A remarkable thing is that, for each $n$, R_{t_n} has the same distribution as R_n, and therefore Kingman's theorem [Kin75] is applicable to R_n.

An (*continuous-time*) *incremental string* X_t with a *transition rate* $\{P_{ni}\}$ is the output of a continuous-time Markov process; the process begins at time $t = t_1 := 0$ with $X_{t_1} = 0$. Immediately after the moment $t = t_n$ when the $n$th component decides its value, the $n$ components of X_{t_n} raise their hands independently at random and the fastest component wins to decide the $(n+1)$th component of X_t as one more than its value, where the $i$th smallest component of X_{t_n} raises his hand according to a Poisson process with rate $P_{ni}$. We sometimes say that the $i$th smallest component produces the $(n+1)$th component if it is the winner to decide the value of the component. Notice that we can ignore the possibility that plural components raise their hands at the same moment. Therefore, as a string of depths, R_t is an incremental string with the transition rate $P_{ni} = 1$ (which does not depend on $n$ nor on $i$). Moreover, any discrete-time incremental string X_n can be embedded in a continuous-time process X_t by letting the transition rate of X_t be proportional to the transition distribution of X_n. Thus, B_n and $D_n^{(k)}$ can be embedded in continuous-time processes as continuously increasing strings B_t and $D_t^{(k)}$ by appropriately deciding their transition rates $J$ and $K^{(k)}$, respectively: $J_{ni} = 1$ if $n/2 \le i \le n$ and 0 otherwise; $K_{ni}^{(k)} = (x + 0.5)/(k - 0.5)$ if $xn/k < i \le (x+1)n/k$.

Neither B_t nor $D_t^{(k)}$ is a pure birth process (as opposed to R_t), since their transition rates depend on both population and position ($n$ and $i$). We have, however, a natural coupling of each of them with the recursive tree $R_{t'}$ for some $t' > t$. More generally, let X_t be an incremental string with the transition rate $P$ such that $P_{ni} \le 1$ for all n, i. Then we observe that X_t and a substring of R_t generated by the following process, referred to as $(X, R)_t$, are equally distributed. We basically simulate R_t, namely producing components with the transition rate 1, but some components are killed and the alive components at time $t$ form the substring $(X, R)_t$. Only the surviving components give birth to new alive components. The initial component is not killed (alive). At the moment when the $n$th alive component is produced, say from the $i$th smallest alive component, we flip the coin and decide with probability $1 - P_{ni}$ to kill it.

Now, for the upper bound case, we can work with $(B, R)_t$ instead of B_t, since they have the same distrituiton, and we let t'_n be the moment when the $n$th component is produced in $(B, R)_t$. Due to the coupling $(B, R)_t$, we have that $\max(B_{t'_n})$ is stochastically dominated by $\max(R_{t'_n})$. Then we apply Pittel's limit theorem for the height of a random recursive tree, which derives $\max(R_{t'_n}) \to 2e \ln n$ in probability. However, in order to obtain the upper bound we still need to prove that both $B_{t'_n}$ and B_n have the same distribution. This also holds and is proved in Lemma 2. The proof for the lower bound uses the coupling $(D^{(k)}, R)_t$, as well as Szymańki's result [Szy90] about the probability distribution of depths of the nodes in a random recursive tree. The proof for the lower bound is the most nontrivial part of the paper.

3 Domination by Coupling

In this section we prove the dominations for B_n, C_n and $D_n^{(k)}$.

Theorem 1 *max(B_n) dominates max(C_n), and max(C_n) dominates max($D_n^{(k)}$).*

In fact, this theorem is a corollary of the next proposition.

Proposition 1 *Let X_n and Y_n be two random strings of integers with transition distributions P and Q, respectively. If Q dominates P, then max(Y_n) dominates max(X_n) for each n.*

Proof. It is sufficient to construct, for each n, a finite set of triples (p_i, s^i, u^i), where $p_i \in [0,1]$ and s^i, u^i are strings of length n, such that

(a) $\sum_i p_i = 1$,

(b) $\Pr[X_n = i] = \sum_{\{s^j(n)=i\}} p_j$,

(c) $\Pr[Y_n = i] = \sum_{\{u^j(n)=i\}} p_j$,

(d) $\max(s^i) \leq \max(u^i)$.

To prove it, we use the Strassen's theorem for random variables taking a finite number of values. In the general setting, Strassen's theorem is quite complicated, but in our case, however, we can prove it easily. We sate it in Lemma 1 (the proofs of Proposition 1 and Lemma 1 are omitted).

Lemma 1 *Let X and Y be two random variables, taking values in $\{1, \ldots, n\}$. If Y dominates X, i.e., $\Pr[Y \geq i] \geq \Pr[X \geq i]$ for any i, then there is a coupling of X and Y with respect to the standard order of integers.*

4 The Depth of Circuits

In this section we establish the main result of the paper, namely a probability convergence for the depth of randomly generated circuits.

Theorem 2 *The depth of random recursive circuits satisfies*

$$\frac{max(C_n)}{\ln n} \longrightarrow 2e \quad \textit{in probability} . \tag{3}$$

This is shown by proving an upper and lower bound for $\max(B_n)$ and $\max(D_n^{(k)})$, respectively, by embedding them into continuous-time branching processes. Here we give justification of our embeddings.

Lemma 2 *Let X_n be a discrete-time incremental string with a transition distribution $\{P_{ni}\}$, and let X_t be a continuous time incremental string with transition rate $\{Q_{ni}\}$. If Q is proportional to P, namely there is a positive constant c such that $Q_{ni} = cP_{ni}$ for all i, then X_{t_n} has the same distribution as X_n, where t_n is the moment of time when the nth component of X_t is decided.*

4.1 Upper Bound

The following lemma gives the proof for the upper bound.

Lemma 3 *For any $\varepsilon > 0$,*

$$max(B_n) \;\le\; (2e+\varepsilon)\ln n \quad \textit{with probability one} \ . \tag{4}$$

Proof. We work on continuous-time branching processes R_t and $(B,R)_t$. Recall that t'_n is the moment when the $n$th component is produced in $(B,R)_t$, and $(B,R)_{t'_n}$ is distributed as $B_{t'_n}$, hence as B_n by Lemma 2. We know that $\max(R_t)$ dominates $\max((B,R)_t)$, so it suffices to prove the upper bound for $H_n := \max(R_{t'_n})$, i.e., for the depth of $R_{t'_n}$.

We first compute t'_n. The birth rate of $(B,R)_t$ is given by $J$. Therefore, its transition rate at any time, when the length of a string is $n$, equals

$$\sum_{i=1}^{n} J_{ni} = \lceil n/2 \rceil \ . \tag{5}$$

At this point, we follow Pittel's proof for the height of a random recursive tree to derive

$$\frac{t'_n}{\ln n} \longrightarrow 2 \quad \text{in probability} \ . \tag{6}$$

Indeed, note that the transition rate of $(B,R)_t$ depends only on $n$. Then,

$$t'_n = \sum_{k=1}^{n-1} \tau_k \ , \tag{7}$$

where $\tau_1, \dots, \tau_{n-1}$ are independent and $\tau_k \sim \mathrm{Exp}(\lambda_k)$, $\lambda_k = \lceil k/2 \rceil$. Therefore, the mean and the variance of t_n are calculated as

$$E(t'_n) = \sum_{k=1}^{n-1} 1/\lambda_k = (1+o(1))2\ln n \ , \tag{8}$$

and

$$\mathrm{var}(t'_n) = \sum_{k=1}^{n-1} (1/\lambda_k)^2 = O(1) \ . \tag{9}$$

Thus, Chebysheff's inequality as well as Borel-Cantelli lemma deduce

$$\lim_{n\to\infty} t'_n/E(t'_n) = 1, \quad \text{almost surely} \ , \tag{10}$$

deriving (6). Now we compute H_n. Let $T(k)$ be the moment when the first member of the kth generation is produced in the recursive tree R_t. Pittel proves that

$$\frac{T(k)}{k} \longrightarrow \frac{1}{e}, \quad \text{in probability} \ , \tag{11}$$

by using Kingman's theorem [Kin75]. Since $T(H_n)$ and $T(H_n+1)$ are the first moments when the depth of R_t becomes equal to H_n and H_n+1, we have

$$T(H_n) \le t'_n \le T(H_n+1) \ . \tag{12}$$

Therefore, dividing by H_n and letting $n \to \infty$ implies, due to (11),

$$\frac{H_n}{t'_n} \to e, \quad \text{in probability} \ . \tag{13}$$

By combining with (6) we conclude

$$\frac{H_n}{\ln n} \to 2e, \quad \text{in probability} \ ,$$

and this proves the lemma. □

4.2 Lower Bound

The proof for the lower bound uses the coupling $(D^{(k)}, R)_t$, as well as Szymańki's result [Szy90] about the probability distribution of depths of the nodes in a random recursive tree. The result is stated and proved in the following lemma.

Lemma 4 *For any $\varepsilon > 0$, there is an integer k such that*

$$max(D_n^{(k)}) \ \geq \ (2e - \varepsilon) \ln n, \quad \textit{with probability one} \ . \tag{14}$$

Proof. Omitted.

5 Further Research

It would be interesting to study the expected number of gates in a level of the circuit. This would give us an estimation for the (expected) number of processors needed to compute the circuit in parallel. Another interesting problem is that of finding the distribution of gates in levels. This is related somehow to the *shape* of the circuit.

Acknowledgments

We wish to thank Josep Díaz for encouragement and helpful comments. We also thank Maria Serna and Hosam Mahmoud for helpful discussions. We are very greatful to anonymous referees for many useful comments.

References

[BDG95] Balcázar, J.L., Díaz, J. and Gabarró, J.: *Structural Complexity I.* Springer Verlag (1995)

[CGS95] Codenotti, B., Gemmell, P., and Simon, J.: Average Circuit Depth and Average Communication Complexity. In *Third European Symposium on Algorithms*, Lecture Notes in Comp. Sc. Springer-Verlag (1995) 102–112

[DSS$^+$94] Díaz, J., Serna, M.J., Spirakis, P., Torán, J. and Tsukiji, T.: On the expected depth of Boolean circuits. Technical Report **LSI-94-7-R** Univ. Politèc. de Catalunya Dept. LSI (1994)

[Kin75] Kingman, J.: The first birth problem for an edge-dependent branching process. *Ann. Prob.* **3** (1975) 790–801

[Lin92] Lindvall, T.: *Lectures on the Coupling Method.* Wiley Interscience Pub., (1992)

[Mah91] Mahmoud, H.: Limiting distributions for path lengths in recursive trees. *Prob. in the Eng. and Inf. Sc.* **5** (1991) 53–59

[MS91] Mahmoud, H.M. and Smythe, R.T.: On the Distribution of Leaves in Rooted Subtrees of Recursive Trees. *The Ann. of Appl. Prob.* **1** (3) (1991) 406–418

[Pit94] Pittel, B.: Note on the Heights of Random Recuresive Trees and Random m-ary Search Trees. *Random Struct. and Alg.* **5** (1994) 337–347

[SM95] Smythe, R.T. and Mahmoud, H.M.: *A Survey of Recursive Trees. Teorya Imovirnosty ta Mat. Stat. (in Ukrainian)* **51** (1994) 1–29

[Str65] Strassen, V.: The existence of probability measures with given marginals. *Ann. Math. Stat.* **36** (1965) 423–439

[Szy90] Szymański, J.: *On the maximum degree and height of a random recursive tree.* Wiley New York (1990)