Combinatorics, Probability and Computing (1999) 8, 209–228. Printed in the United Kingdom
© 1999 Cambridge University Press

On the Expected Depth of Random Circuits

SUNIL ARYA[1]†, MORDECAI J. GOLIN[2]‡
and KURT MEHLHORN[3]

[1] Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong
(e-mail: arya@cs.ust.hk)

[2] Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong
(e-mail: golin@cs.ust.hk)

[3] Max-Planck-Institut für Informatik,
D-66123 Saarbrücken, Germany
(e-mail: mehlhorn@mpi-sb.mpg.de)

Received 21 September 1996; revised 14 July 1998

In this paper we analyse the expected depth of random circuits of fixed fanin f. Such circuits are built a gate at a time, with the f inputs of each new gate being chosen randomly from among the previously added gates. The depth of the new gate is defined to be one more than the maximal depth of its input gates. We show that the expected depth of a random circuit with n gates is bounded from above by $ef \ln n$ and from below by $2.04\ldots f \ln n$.

1. Introduction

Recently, Diaz, Serna, Spirakis and Toran [1], motivated by the problem of discovering how quickly a circuit could be evaluated in parallel, posed the question of calculating the depth of a random circuit. They described a model for the generation of random circuits in which each gate has fanin two and showed an upper bound of $O(\ln^3 n)$ on the circuit's expected depth, where n is the number of nodes in the circuit. In this paper we extend their problem by investigating random circuits of fixed fanin f where f can be any integer greater than 0 and tighten their bound by showing the existence of constants c_1 and c_2 such that

$$c_1 f \ln n \leqslant \text{Expected Depth} \leqslant c_2 f \ln n.$$

† Partially supported by HKUST grant DAG95/96.EG01.
‡ Partially supported by HK RGC CRG grants 181/93E and 652/95E.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

We use straightforward methods to prove that $c_2 \leqslant e$. To evaluate c_1 we develop a new technique that constructs a Markov chain that approximates (and understates) the growth of the circuit and are able to lower bound c_1 as a function of the values of the stationary distribution of the chain. Using this technique we can analytically bound $1.39\ldots \leqslant c_1$. The technique allows us to do better, though. By constructing a more complicated Markov chain and using a linear equation solver to find its stationary distribution we are able to prove that $2.0479\ldots \leqslant c_1$.

As an interesting philosophical aside we point out that our technique also seems to provide a good indication (although not a formal proof) that $2.44 \leqslant c_1$. The idea is this. We show that c_1 is bounded from below by a function of the values of a stationary distribution of an extremely complicated Markov chain, a chain so large that with our computer resources we were unable to calculate its stationary distribution explicitly. We were easily able to simulate the action of this chain, though, and did so for a very large number of steps. The number of times a state was reached divided by the number of steps the process was run should, with high confidence, closely approach the stationary distribution of the state. Plugging the values found into our equations we are thus able to say that we believe with high confidence that $2.44 \leqslant c_1$.

1.1. Problem definition and history

For any integer $f \geqslant 1$, a *circuit of fanin* f is an acyclic graph where the in-degree of each node is bounded by f. Circuits are among the most useful structures in computer science. Depending on the application, different structural parameters of circuits are important. For example, when a circuit is used as a computational device the length of a longest and a shortest path from a source (= node with in-degree 0) to a node measures the minimum and maximum delay of an input signal to reach the node.

We study structural parameters of *random circuits*. A random circuit of maximal fanin f is constructed node-by-node by starting with node 0 and defining its *depth* or *level*, $d_0 = 0$. The f inputs of the nth† gate are chosen at random (with repetition) from the first $n-1$ gates; the depth of the nth gate is defined to be 1 plus the maximum depth of its inputs. Formally, random circuits are built a gate at a time by the process $\mathscr{P}$ defined in Figure 1.

Process $\mathscr{P}$:

- $d_0 = 0$
- For each n choose f integers $i_n^1, \ldots, i_n^f$ where each i_n^j is chosen randomly from $\{0, 1, 2, \ldots, n-1\}$.
  1. The multiset $S_n = \{i_n^1, \ldots, i_n^f\}$ contains the *inputs* to gate n.
  2. $d_n = 1 + \max_{j \leqslant f} d_{i_n^j}$ is the *depth* of gate n.

Figure 1 The random process $\mathscr{P}$ that generates random circuits

† The *nth gate* refers to the nth gate added to the circuit. Because gate numbering starts at 0, the circuit actually contains the $n+1$ gates $0, 1, \ldots, n$ after the nth gate is added.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

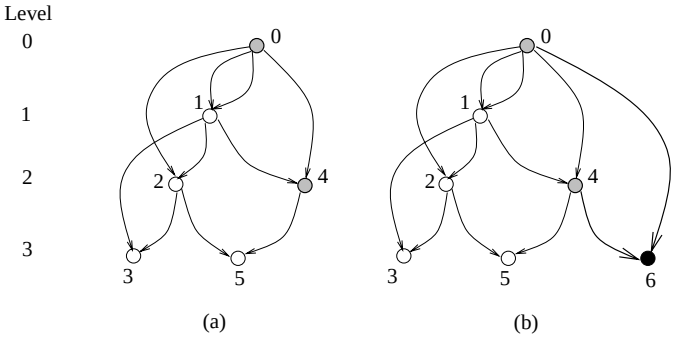


Figure 2 Random circuit of fanin two. Black node 6 has inputs 0 and 4 and therefore has depth $d_6 = \max(d_0, d_4) + 1 = 3$

In what follows we will use the following notation.

Definition 1.1.

$$\begin{aligned} L(d,n) &= \text{number of nodes at depth } d \text{ at time } n \\ &= |\{i \,:\, i \leqslant n,\, d_i = d\}|, \\ E(d,n) &= \mathrm{E}\,(L(d,n))\,, \\ \mathrm{Depth}_n(P) &= \text{depth of the circuit at time } n \;=\; \max_{i \leqslant n} d_i. \end{aligned}$$

Note that if $f = 1$ the random circuit process reduces to picking a node at random and making the new node its child. This is a very standard and well studied technique for creating random trees. The expected depth of a random tree of n nodes was shown by Pittel [7] to be $e \ln n$. We refer the reader to papers by Mahmoud and Smythe [3], Meir and Moon [4], Moon [5], Na and Rapaport [6], and Szymanski [8] for more results on random trees.

In Section 2 we present an upper bound on the expected depth of random circuits of $ef \ln n = 2.718\ldots f \ln n$, where f is the fanin. Our approach is based on first computing an upper bound on the expected number of nodes at any level and then arguing that the probability that the tree is so deep that the expected number of nodes at the deepest level is less than one is small. Note that, for $f = 1$, Pittel's result implies that this bound is tight. In Section 3 we present lower bounds on the expected depth. The first lower bound we find, one which we present for pedagogical reasons because it illustrates the technique used, is $1.39\ldots f \ln n$. To compute the lower bound, we define a modified random circuit which is guaranteed always to have a depth smaller than the original circuit. The advantage of the modified circuit is that it is mathematically easier to analyse than the original circuit. We model the modified circuit by a Markov chain whose analysis yields the above-mentioned lower bound. By using a more accurate model, we are able to prove a better lower bound of $2.04\ldots f \ln n$. As we attempt to use still more accurate models, it turns out that the Markov chain has too many states and we are not able to solve the equations owing to the large computational resources needed. We are, however, able to simulate the Markov chain directly leading to a possible lower bound of $2.44\ldots f \ln n$.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Note. Tsukiji and Xhafa have just released a new paper [9] in which they analyse the same problem and actually prove a stronger result, namely that the circuit depth actually converges to $ef \ln n$ in probability. Their paper, though, uses much more sophisticated and specialized tools as 'subroutines', namely Kingman's theorem and Pittel's analysis [7] of the height of random trees (actually the case $f = 1$). This paper, while presenting a weaker result, does so in a fully self-contained manner, its main tool being the convergence theorem for homogeneous Markov chains.

2. An upper bound on the expected circuit depth

In this section we derive an upper bound on the expected circuit depth. We start by establishing a recurrence inequality describing the growth of $E(d,n)$, the expected number of nodes on level d at time n.

Lemma 2.1. *Consider a random circuit of fanin f. Then*

$$\begin{aligned} E(0,n) &= 1, && \text{for } n \geqslant 0, \\ E(d,0) &= 0, && \text{for } d \geqslant 1, \\ E(d,n) &\leqslant E(d,n-1) + f \cdot \tfrac{E(d-1,n-1)}{n}, && \text{for } n \geqslant 1,\ d \geqslant 1. \end{aligned} \tag{2.1}$$

Proof. The first and the second statements follow directly from the way the random circuit is constructed. To prove the third equation note that

$$L(d,n) = L(d,n-1) + \delta(d,n), \tag{2.2}$$

where $\delta(d,n) = 1$, if $d_n = d$, and 0 otherwise. Taking expectations of both sides of the equation yields

$$\begin{aligned} E(d,n) &= E(d,n-1) + \Pr(\delta(d,n) = 1) \\ &= E(d,n-1) + \\ &\quad \sum_{i \geqslant 1} \Pr(L(d-1,n-1) = i) \cdot \Pr\left(\delta(d,n) = 1 \,\middle|\, L(d-1,n-1) = i\right) \end{aligned}$$

Observe that if $d_n = d$ this implies that at least one of the nth gate's f inputs is at depth $d-1$. Thus

$$\Pr\left(\delta(d,n) = 1 \,\middle|\, L(d-1,n-1) = i\right) \leqslant 1 - (1 - i/n)^f \leqslant fi/n. \tag{2.3}$$

Substituting this back we have

$$\begin{aligned} E(d,n) &\leqslant E(d,n-1) + \sum_{i \geqslant 1} \Pr(L(d-1,n-1) = i) \cdot fi/n \\ &\leqslant E(d,n-1) + fE(d-1,n-1)/n, \end{aligned} \tag{2.4}$$

establishing the third equation of the lemma. □

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

The inequalities just derived can now be used to upper bound $E(d,n)$. In what follows $H_n = \sum_{1 \leqslant i \leqslant n} 1/i$ is the nth *harmonic number*.

Lemma 2.2. $$E(d,n) \leqslant (f \cdot H_n)^d / d!.$$

Proof. Define $\overline{E}(d,n)$ using the same relation as in the statement of Lemma 2.1 except with the inequality in the third equation being replaced by equality. We compute an upper bound for $\overline{E}(d,n)$ defined by this new relation; clearly this upper bound also applies to $E(d,n)$.

Let $\overline{E}_d(x) = \sum_{n \geqslant 0} \overline{E}(d,n) x^n$ be the generating function for the $\overline{E}(d,n)$. Then

$$\overline{E}_0(x) = 1 + x + x^2 + \cdots = \frac{1}{1-x}, \tag{2.5}$$

$$\overline{E}_d(x) = \frac{f}{1-x} \int \overline{E}_{d-1}(x)dx, \qquad \text{for } d \geqslant 1. \tag{2.6}$$

The latter equation follows easily from the recurrence relation on $\overline{E}(d,n)$ (multiply both sides by x^n and then sum over n). The constant of integration in equation (2.6) must be chosen to satisfy the boundary condition $\overline{E}_d(0) = 0$. It is now easy to prove by induction that $\overline{E}_d(x)$ is given by

$$\overline{E}_d(x) = \frac{f^d}{d!} \cdot \frac{1}{1-x} \cdot (-\ln(1-x))^d. \tag{2.7}$$

We can extract $\overline{E}(d,n)$, the coefficient of x^n in the series expansion of $\overline{E}_d(x)$, as follows. Using the expansion $-\ln(1-x) = \sum_{i \geqslant 1} x^i/i$ and the convolution theorem of ordinary generating functions it is seen that the coefficient of x^r in $(-\ln(1-x))^d$ is given by

$$\sum_{\substack{i_1,\ldots,i_d \geqslant 1 \\ i_1+\cdots+i_d = r}} \frac{1}{i_1 i_2 \cdots i_d}. \tag{2.8}$$

The coefficient of x^n in $(1/(1-x)) \cdot (-\ln(1-x))^d$ can be computed by summing the coefficients of x^r in $(-\ln(1-x))^d$ over r ranging from 0 to n. Thus, $\overline{E}(d,n)$, the coefficient of x^n in $\overline{E}_d(x)$, is given by

$$\overline{E}(d,n) = \frac{f^d}{d!} \left(\sum_{\substack{i_1,\ldots,i_d \geqslant 1 \\ i_1+\cdots+i_d \leqslant n}} \frac{1}{i_1 i_2 \cdots i_d} \right). \tag{2.9}$$

We can compute an upper bound on $\overline{E}(d,n)$ by relaxing the summation,

$$\overline{E}(d,n) \leqslant \frac{f^d}{d!} \left(\sum_{1 \leqslant i_1,\ldots,i_d \leqslant n} \frac{1}{i_1 i_2 \cdots i_d} \right) = \frac{f^d}{d!} \left(\sum_{1 \leqslant i \leqslant n} \frac{1}{i} \right)^d = \frac{(f \cdot H_n)^d}{d!}. \tag{2.10}$$

Since this is also an upper bound on $E(d,n)$, this completes the proof. □

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Theorem 2.1. *The expected depth of the random circuit after n gates are added satisfies*

$$\mathtt{E}\left(\mathrm{Depth}_n(P)\right) \leqslant f \cdot e \cdot H_n + O(1).$$

Proof. Observe that, for any d, $\mathrm{Depth}_n(P) \geqslant d$ implies $L(d,n) \geqslant 1$. Thus

$$\Pr\left(\mathrm{Depth}_n(P) \geqslant d\right) \leqslant E(d,n) \leqslant \frac{(f \cdot H_n)^d}{d!}, \tag{2.11}$$

where the last inequality follows from Lemma 2.2. Inserting Stirling's formula $d! = (d/e)^d\sqrt{2\pi d}(1 + O(1/d))$ into this equation yields

$$\Pr\left(\mathrm{Depth}_n(P) \geqslant d\right) \leqslant \left(\frac{feH_n}{d}\right)^d \frac{1}{\sqrt{2\pi d}}\left(1 + O\left(\frac{1}{d}\right)\right). \tag{2.12}$$

Thus, for any $x > 0$,

$$\begin{aligned} \mathtt{E}\left(\mathrm{Depth}_n(P)\right) &\leqslant x + \sum_{d>x} \Pr\left(\mathrm{Depth}_n(P) \geqslant d\right) \qquad (2.13)\\ &\leqslant x + \sum_{d>x} \left(\frac{feH_n}{d}\right)^d \frac{1}{\sqrt{2\pi d}}\left(1 + O\left(\frac{1}{d}\right)\right) \end{aligned}$$

We will now show that, for any $x > 0$,

$$\sum_{d>x} \left(\frac{x}{d}\right)^d = O(1). \tag{2.14}$$

Setting $x = \lceil feH_n \rceil$ and inserting the last inequality into the one that precedes it will conclude the proof of the lemma. To show (2.14) note that

$$\begin{aligned} \sum_{d>x} \left(\frac{x}{d}\right)^d &\leqslant \sum_{0\leqslant i\leqslant x} \left(\frac{1}{1+\frac{i}{x}}\right)^x + \sum_{d>2x} \left(\frac{x}{d}\right)^d \\ &\leqslant \sum_{0\leqslant i\leqslant x} e^{-i/2} + \sum_{d>2x} \left(\frac{1}{2}\right)^d = O(1) \end{aligned}$$

where the second inequality follows from the fact that $(1+u)^{-1} \leqslant e^{-u/2}$ for $0 \leqslant u \leqslant 1$. □

3. Lower bounds on the expected circuit depth

In this section we describe how to derive lower bounds on the expected depths of random circuits. Our approach will be to construct various modified random circuits P', such that $\mathtt{E}\left(\mathrm{Depth}_n(P')\right) \leqslant \mathtt{E}\left(\mathrm{Depth}_n(P)\right)$. Because of the way that they are constructed we will easily be able to lower bound $\mathtt{E}\left(\mathrm{Depth}_n(P')\right)$, thus effectively bounding $\mathtt{E}\left(\mathrm{Depth}_n(P)\right)$ as well.

More specifically we will show how to construct a Markov chain that approximates P' where the state of the Markov chain is the number of gates on the deepest level of P'. Calculating the stationary probabilities of the Markov chain will then permit finding out how often a new level is started, letting us in turn calculate the expected depth of P'.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Process $\mathscr{P}'$:

- $d'_0(0) = 0$
- For each n
  1. Choose f integers $i_n^1, \ldots, i_n^f$ where each i_n^j is chosen randomly from $\{0, 1, 2, \ldots, n-1\}$.
  2. The multiset $S_n = \{i_n^1, \ldots, i_n^f\}$ contains the *inputs* to gate n.
  3. Set the depth of the gate $d'_n(n-1)$ to $1 + \max_{j \leqslant f} d'_{i_n^j}(n-1)$.
  4. For all $i \leqslant n$ set $d'_i(n)$ to some value $\leqslant d'_i(n-1)$ using some arbitrary rule.

Figure 3 A process $\mathscr{P}'$ that generates modified random circuits

This section is split into three parts. In the first we prove two lemmas that will be crucial for establishing the lower bound. In the second we describe a family of modified circuit processes, P_ϕ, $\phi > 1$ and analytically calculate $\mathtt{E}\left(\mathrm{Depth}_n(P_\phi)\right)$ as a function of ϕ. We then figure out the best lower bound that this approach can yield. In the third part we extend our techniques to examine more complicated modified circuits, again parametrized by some variable.

3.1. Basic lemmas

In this subsection we present two lemmas upon which our analysis will be based. We say that P' is a process that generates a *modified random circuit* if it is defined as in Figure 3.

Note that this process generates random circuits a gate at a time in the same way that $\mathscr{P}$ does. The difference between $\mathscr{P}$ and $\mathscr{P}'$ is that $\mathscr{P}'$ sometimes, in step 4, decreases the depths of some gates using some arbitrary rule. Since gates can have their depths decreased at any time we can no longer talk about the absolute depth d_i of gate i but instead must specify $d'_i(n)$, the depth of gate i after the nth step of the modified process.

Because gates can only have their depths decreased and not increased it is natural to suspect that, for any modified circuit P', $\mathrm{Depth}(P') \leqslant \mathrm{Depth}(P)$. In fact this is true, as stated in the next lemma.

Lemma 3.1. $$\mathtt{E}\left(\mathrm{Depth}_n(P')\right) \leqslant \mathtt{E}\left(\mathrm{Depth}_n(P)\right).$$

Proof. Let $C = (S_1, S_2, \ldots, S_n)$ be a sequence of multisets in which $S_i \in \{0, 1, \ldots, i-1\}^f$. Fixing C actually fixes the action of the first n steps of both $\mathscr{P}$ and $\mathscr{P}'$. We can therefore, for $j \leqslant n$, talk about $d_i(C)$ and $d'_i(j, C)$, the depths of the gates (at time j) given C, and similarly, $\mathrm{Depth}_j(P, C)$ and $\mathrm{Depth}_j(P', C)$. We will show by induction that

$$\forall j \leqslant n, \forall i \leqslant j, \quad d'_i(j, C) \leqslant d_i(C). \tag{3.1}$$

This is obviously true for the base case $n = 1$. Assume, then, it is true for $C = (S_1, S_2, \ldots, S_{n-1})$. To prove it is true for $C = (S_1, S_2, \ldots, S_n)$ first note that the induction hypothesis immediately tells us that

$$\forall j \leqslant n-1, \forall i \leqslant j, \quad d'_i(j, C) \leqslant d_i(C).$$

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Thus

$$\forall i \leqslant n-1, \quad d'_i(n, C) \leqslant d'_i(n-1, C) \leqslant d_i(C)$$

and

$$d'_n(n, C) = 1 + \max_{j \leqslant f} d'_{i_n^j}(n-1, C) \leqslant 1 + \max_{j \leqslant f} d_{i_n^j}(C) = d_n(n, C),$$

proving (3.1). This equation then implies

$$\mathrm{Depth}_n(P', C) \leqslant \mathrm{Depth}_n(P, C).$$

Let $\mathscr{C}$ be the collection of all possible sequences C. Then

$$\begin{aligned} \mathtt{E}\left(\mathrm{Depth}_n(P')\right) &= \frac{1}{|\mathscr{C}|} \sum_{C \in \mathscr{C}} \mathrm{Depth}_n(P', C) \\ &\leqslant \frac{1}{|\mathscr{C}|} \sum_{C \in \mathscr{C}} \mathrm{Depth}_n(P, C) = \mathtt{E}\left(\mathrm{Depth}_n(P)\right). \end{aligned}$$

□

The second lemma we will need generalizes the ergodic theory of homogeneous Markov chains to special time-dependent ones.

In what follows, if $M = (m_{i,j})$ is a matrix then $|M| = \sup_j \sum_i |m_{i,j}|$, that is, the supremum of the column (absolute value) sums, and, if $\pi = (\pi(1), \pi(2), \ldots)$ is a vector, then $|\pi| = \sup_j \pi(j)$.

Lemma 3.2. *Let M be a Markov chain with time-dependent transition probabilities. Let A_r be the transition matrix for the rth step. Suppose A is the transition matrix for some irreducible aperiodic time-independent chain and A has a stationary distribution π. Suppose further that $|A_r - A| = O(\phi^{-r})$ for some $\phi > 1$. Let π_0 be any distribution and, for $r > 0$, set $\pi_r = A_{r-1}\pi_{r-1}$. Then*

$$|\pi_r - \pi| \to 0.$$

Proof. We will prove the lemma by showing that $\forall \epsilon > 0$, $\exists m, K$ such that $\forall r > m + K$, $|\pi_r - \pi| < \epsilon$.

Let $\epsilon > 0$. First note that, since A is irreducible and has a stationary distribution, standard theorems on Markov chains [2, p. 208] imply that all the states in A are non-null and persistent. Now, since A is non-null persistent, irreducible and aperiodic, other standard theorems, for instance, [2, p. 214, note (c)], then tell us that, given any initial distribution $\overline{\pi}$, $A^k\overline{\pi} \to \pi$ so

$$|A^k(\overline{\pi} - \pi)| \to 0 \tag{3.2}$$

Next note that, $\forall m > 0$,

$$\begin{aligned} \pi_{m+1} - \pi &= A_m\pi_m - A\pi \\ &= A_m\pi_m - A\pi_m + A\pi_m - A\pi \\ &= (A_m - A)\pi_m + A(\pi_m - \pi). \end{aligned}$$

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Iterating this equation yields

$$\pi_{m+k} - \pi = \sum_{l=0}^{k-1} A^{k-1-l}(A_{m+l} - A)\pi_{m+l} + A^k(\pi_m - \pi). \tag{3.3}$$

We now show that the sum on the right side of this equation tend, componentwise, to 0 as $k \to \infty$.

First suppose r is fixed and $B = A_r - A$; denote the components of B by $b_{i,j}$. The lemma condition $|A_r - A| = O(\phi^{-r})$ translates into $\forall j, \sum_i |b_{i,j}| = O(\phi^{-r})$, where the constant implicit in the $O(\cdot)$ is independent of j. Now, given *any* distribution $\pi' = (\pi'(1), \pi'(2) \ldots)$, set $\sigma = (A_r - A)\pi' = B\pi'$. We then find that

$$\begin{aligned}
\sum_i |\sigma(i)| &\leqslant \sum_{i,j} |b_{i,j}|\pi'(j) \\
&= \sum_j \pi'(j) \left(\sum_i |b_{i,j}| \right) \\
&= \sum_j \pi'(j) O(\phi^{-r}) \\
&= O(\phi^{-r}),
\end{aligned}$$

where the last equality follows from the fact that $\sum_j \pi'(j) = 1$.

Now let $r = m + l$, $\pi' = \pi_{m+l}$ and set

$$\delta = A^{k-1-l}(A_{m+l} - A)\pi' = A^{k-1-l}\sigma.$$

Since every entry in A^{k-1-l} has absolute value at most 1 we find that $\forall j, \delta(j) \leqslant \sum_i |\sigma(i)| = O(\phi^{-(m+l)})$. Thus

$$\begin{aligned}
\left| \sum_{l=0}^{k-1} A^{k-1-l}(A_{m+l} - A)\pi_{m+l} \right| &\leqslant \sum_{l=0}^{k-1} \left| A^{k-1-l}(A_{m+l} - A)\pi_{m+l} \right| \\
&= \sum_{l=0}^{k-1} O(\phi^{-(m+l)}) = O(\phi^{-m}),
\end{aligned}$$

where the constant implicit in the $O(\phi^{-m})$ term is *independent of* k. Thus

$$|\pi_{m+k} - \pi| \leqslant O(\phi^{-m}) + |A^k(\pi_m - \pi)|. \tag{3.4}$$

Given ϵ we can therefore find m such that the $O(\phi^{-m})$ term is less that $\epsilon/2$. Once m is fixed equation (3.2) tells us that $\exists K$ such that $\forall k > K$, $|A^k(\pi_m - \pi)| < \epsilon/2$. Thus $\forall r > m + K$, $|\pi_r - \pi| < \epsilon/2 + \epsilon/2 = \epsilon$, proving the theorem. □

3.2. The first lower bound

In this subsection we describe our first method of calculating lower bounds. We create a family of processes $\mathscr{P}_\phi$, $\phi > 1$ that create modified random circuits P_ϕ and bound the expected depths of the P_ϕ. This will permit us to prove the following theorem.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Theorem 3.1. *Let P be a random circuit grown by process $\mathscr{P}$. Then, for every $\epsilon > 0$,*

$$\mathtt{E}(\mathrm{Depth}_n(P)) \geqslant \left(\frac{f}{e-2} - \epsilon\right) \ln n + O(1).$$

Note that $1/(e-2) = 1.39\ldots$.

For a given fixed $\phi > 1$ the process $\mathscr{P}_\phi$ works in stages, during stage r adding gates n, $\lceil \phi^r \rceil < n \leqslant \lceil \phi^{r+1} \rceil$. Within a stage, while adding the gates, process $\mathscr{P}_\phi$ behaves exactly the same as process $\mathscr{P}$, picking the inputs of the gates at random and placing a gate one level deeper than the maximum depth of its parents. It is only at the end of a stage that the process will modify the circuit, decreasing the depths of some gates using a rule to be described below. The essential fact about the process P_ϕ is that its 'level-decreasing' rule will be defined so that between any two consecutive stages exactly one of the following transitions must occur.

T1 The depth of P_ϕ increases by one and the new deepest level contains only one gate.
T2 The depth of P_ϕ remains the same and the number of gates on the deepest level increases by one.
T3 The depth of P_ϕ remains the same and the number of gates on the deepest level does not change.

Because of this fact we will be able to define a Markov chain whose state at time r is the number of nodes on the deepest level of P_ϕ after the conclusion of stage r. Calculating the stationary distribution of this chain will permit us to calculate how often a new level is added to P_ϕ, letting us lower bound $\mathtt{E}\left(\mathrm{Depth}_n(P_\phi)\right)$ and thus, via Lemma 3.1, lower bounding $\mathtt{E}(\mathrm{Depth}_n(P))$ as well. We now describe the process P_ϕ in detail.

It starts in stage 0 by placing gate 0 at depth 0 and gate 1 at depth 1.

At the end of stage $r-1$ the process knows three pieces of information describing the result of stage $r-1$:

(i) $l_{r-1} = \mathrm{Depth}_{\lceil \phi^r \rceil}(P_\phi)$,
(ii) $S_{r-1} = \{i \leqslant \lceil \phi^r \rceil \ : \ d'_i\left(\lceil \phi^r \rceil\right) = l_{r-1}, \quad \text{and}$
(iii) some gate g_{r-1} such that $d'_{g_{r-1}}\left(\lceil \phi^r \rceil\right) = l_{r-1} - 1$.

Before starting stage $r = 1$ the process thus sets $l_0 = 0$, $g_0 = 0$ and $S_0 = \{1\}$.

Assume now that the process knows l_{r-1}, g_{r-1} and S_{r-1} and is ready to start stage r. It then adds gates n, $\lceil \phi^r \rceil < n \leqslant \lceil \phi^{r+1} \rceil$ in the same way as $\mathscr{P}$ would. When it completes the stage there are three possibilities.

1. Some gate $g' \in S_{r-1}$ was chosen as the parent of one of the newly created gates, call it g'', added during the stage. In this case, the depth of g'' is at least $l_{r-1} + 1$.
2. The first case did not hold but g_{r-1} was the parent of some gate, call it g'. Note that the depth of g' is at least l_r.
3. Neither of the first two cases occurs.

The corresponding actions taken by $\mathscr{P}_\phi$ are as follows.

1. Move g'' to depth $l_{r-1} + 1$. Set $l_r = l_{r-1} + 1$, $g_r = g'$, and $S_r = \{g''\}$.
2. Move g' to depth l_{r-1}. Set $l_r = l_{r-1}$ and $S_r = S_{r-1} \cup \{g'\}$.
3. Nothing.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

After completing these actions the process then moves *all* gates at level l_r or greater except for those in S_r to level $l_r - 1$. Note that after these modifications the circuit P_ϕ knows the correct values for l_r, g_r, and S_r as defined in (i), (ii) and (iii). Also note that, by definition, the process $\mathscr{P}_\phi$ makes exactly one of the transitions **T1**, **T2**, or **T3** each time it advances from one state to the next.

We now define L to be the random process $L = (l_0, l_1, l_2, l_3, \ldots)$ where $l_r = \mathrm{Depth}_{\lceil \phi^{r+1} \rceil}(P_\phi)$ as defined above. We also set $|S_r| = i$ and

$$\begin{aligned} p_i^r &= \Pr\left(\text{transition } \mathbf{T1} \text{ occurs after stage } r+1 \;\middle|\; |S_r| = i\right), \\ q_i^r &= \Pr\left(\text{transition } \mathbf{T2} \text{ occurs after stage } r+1 \;\middle|\; |S_r| = i\right), \\ z_i^r &= \Pr\left(\text{transition } \mathbf{T3} \text{ occurs after stage } r+1 \;\middle|\; |S_r| = i\right), \end{aligned} \tag{3.5}$$

and let

$$\pi_i^r = \Pr\left(|S_r| = i\right).$$

Since the depth of P_ϕ increases (by one) during stage r if and only if transition **T1** occurs, this means

$$\Pr\left(P_\phi \text{ increases by one during stage } r\right) = \sum_{j \geqslant 1} \pi_j^{r-1} p_j^{r-1}.$$

However, because

$$\mathtt{E}\left(\mathrm{Depth}_n(P)\right) \geqslant \mathtt{E}\left(\mathrm{Depth}_{\phi\lfloor \log_\phi n \rfloor}(P_\phi)\right),$$

this implies that

$$\mathtt{E}\left(\mathrm{Depth}_n(P)\right) \geqslant \sum_{1 \leqslant r \leqslant \log_\phi n} \left(\sum_{j \geqslant 1} \pi_j^{r-1} p_j^{r-1} \right). \tag{3.6}$$

The remainder of this subsection is devoted to proving Theorem 3.1 by evaluating the right-hand side of the last equation. We start by showing that p_i^r, q_i^r and z_r^i converge rather quickly to constants.

Lemma 3.3.

$$p_i^r = 1 - \phi^{-if} + O\left(\phi^{-r}\right), \tag{3.7}$$

$$q_i^r = \phi^{-if}\left(1 - \phi^{-f}\right) + O\left(\phi^{-r}\right), \tag{3.8}$$

$$z_i^r = \phi^{-(i+1)f} + O\left(\phi^{-r}\right), \tag{3.9}$$

where the constants implicit in the $O(\cdot)$ notation are independent of i.

Proof. First note that $|S_r| \leqslant r + 1$ because $|S_0| = 1$ and the value of S_r can only increase by 1 between a stage and the one following it. This means that p_i^r, q_i^r and z_i^r are undefined for $i = |S_r| > r + 1$ and we are able to set their values to whatever we want. For convenience, we set their values to be, respectively, $1 - \phi^{-if}$, $\phi^{-if}\left(1 - \phi^{-f}\right)$, and $\phi^{-(i+1)f}$.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Thus we will only be interested in analysing situations in which $i \leqslant r+1$. For technical reasons our proofs will require i/ϕ^r and i^2/ϕ^r to be bounded by a constant, say $1/2$. To ensure this we will therefore assume that r is taken large enough so that $\frac{i^2}{\phi^r} \leqslant \frac{(r+1)^2}{\phi^r} < \frac{1}{2}$.

To prove (3.7) it now suffices to note that if $i = |S_r|$ then **T1** *does not* occur only if all of the i gates on level l_r are never chosen during the $(r+1)$st stage. Thus

$$1 - p_i^r = \prod_{\lceil \phi^{r+1} \rceil < m \leqslant \lceil \phi^{r+2} \rceil} \left(1 - \frac{i}{m}\right)^f = \exp\left(\sum_m f \cdot \ln\left(1 - \frac{i}{m}\right)\right). \tag{3.10}$$

However,

$$\begin{aligned} \sum_m \ln(1 - i/m) &= -\sum_m i/m + O\left(i^2/m^2\right) \\ &= -i \ln \frac{\lceil \phi^{r+2} \rceil}{\lceil \phi^{r+1} \rceil + 1} + O\left(i^2 \phi^{-r}\right) = -i \ln \phi + O\left(i^2 \phi^{-r}\right), \end{aligned}$$

where the constant implicit in the $O(\cdot)$ on the right side of the first equality is independent of i because $i/m < 1/2$.

Thus

$$1 - p_i^r = \exp\left(-if \ln \phi + O\left(fi^2\phi^{-r}\right)\right) = \phi^{-if}\left[1 + O\left(fi^2\phi^{-r}\right)\right] = \phi^{-if} + O\left(\phi^{-r}\right) \tag{3.11}$$

where the second equality follows from (recall our assumption) $i^2\phi^{-r} < 1/2$ so $e^{O\left(fi^2\phi^{-r}\right)} = 1 + O\left(fi^2\phi^{-r}\right)$ with the constant implicit in the $O(\cdot)$ on the right-hand side independent of r; the last equality follows from the fact that $\phi^{-if} i^2 f = O(1)$.

To prove (3.9) a similar calculation shows that

$$z_i^r = \prod_{\lceil \phi^{r+1} \rceil < m \leqslant \lceil \phi^{r+2} \rceil} \left(1 - \frac{i+1}{m}\right)^f = \phi^{-(i+1)f} + O\left(\phi^{-r}\right).$$

Equation (3.8) then follows from $q_i^r = 1 - p_i^r - z_i^r$. □

Recall that process L is a time-dependent Markov chain with transition probabilities p_i^r, q_i^r, z_i^r as defined in (3.5) and initial distribution $\pi^0 = (1, 0, 0, \ldots)$. Thus

$$\pi_i^{r+1} = \begin{cases} \sum_{j \geqslant 1} \pi_j^r p_j^r + \pi_1^r z_1^r, & \text{for } i = 1, \\ \pi_{i-1}^r q_{i-1}^r + \pi_i^r z_i^r, & \text{for } i \geqslant 2. \end{cases} \tag{3.12}$$

For use below we also define A_r to be the transition matrix for L at time r. We now define a *new* time-*independent* Markov chain M as follows.

Set

$$p_i = 1 - \phi^{-if}, \qquad q_i = \phi^{-if}\left(1 - \phi^{-f}\right), \qquad z_i = \phi^{-(i+1)f},$$

and let M be the homogeneous (time-independent) Markov chain with transition matrix A given by

$$a_{ij} = \begin{cases} p_i, & \text{if } j = 1, \\ q_i, & \text{if } j = i+1, \\ z_i, & \text{if } j = i, \\ 0, & \text{otherwise.} \end{cases} \tag{3.13}$$

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

If we let $B = A_r - A$ and set the entries of B to be $b_{i,j}$, then we find from Lemma 3.3 that

$$\sum_j |b_{i,j}| = (p_i - p_i^r) + (q_i - q_i^r) + (z_i - z_i^r) = O(\phi^{-r}).$$

This simply says that

$$|A_r - A| = O(\phi^{-r}).$$

We now show, by calculation, that A has a stationary distribution. We will then use this fact to permit the application of Lemma 3.2. Suppose then that A has some stationary distribution, π, that is, there exists a distribution $\pi = (\pi_1, \pi_2, \pi_3, \ldots)$ satisfying

$$\pi_1 = \sum_{j \geqslant 1} \pi_j p_j + \pi_1 z_1 \tag{3.14}$$

and

$$\pi_i = \pi_{i-1} q_{i-1} + \pi_i z_i, \quad \text{for } i \geqslant 2. \tag{3.15}$$

Then, for $i \geqslant 2$,

$$\pi_i = \frac{\pi_{i-1} q_{i-1}}{1 - z_i} = \frac{s^{i-1}(1-s)}{1 - s^{i+1}} \pi_{i-1} \tag{3.16}$$

where $s = \phi^{-f}$. We unwind this last equation to find

$$\pi_i = \frac{s^{i-1}(1-s)}{1 - s^{i+1}} \cdot \frac{s^{i-2}(1-s)}{1 - s^i} \cdots \frac{s(1-s)}{1 - s^3} \cdot \pi_1, \tag{3.17}$$

which can be rewritten as

$$\pi_i = s^{(i^2-i)/2} \left[\frac{1-s}{1-s^{i+1}} \cdot \frac{1-s}{1-s^i} \cdots \frac{1-s}{1-s^3} \right] \cdot \pi_1. \tag{3.18}$$

Recalling that $\sum_i \pi_i = 1$ we find

$$\pi_1 = \left[1 + \sum_{i \geqslant 2} \left(s^{(i^2-i)/2} \left[\frac{1-s}{1-s^{i+1}} \cdot \frac{1-s}{1-s^i} \cdots \frac{1-s}{1-s^3} \right] \right) \right]^{-1},$$

and for $i \geqslant 2$ define π_i by equation (3.18). By substitution we find that this distribution satisfies (3.14) and (3.15) and is therefore a stationary one for A.

We have just proven that A has a stationary distribution. It is easy to see that A is irreducible and aperiodic and thus we may apply Lemma 3.2 to find that $|\pi^r - \pi| \to 0$.

Now set

$$c_\phi = \pi_1 - \pi_1 z_1 = \sum_{j \geqslant 1} \pi_j p_j.$$

Note that $\sum_{j \geqslant 1} \pi_j p_j \leqslant 1$, and $\forall r\, p_j, p_j^{r-1} \leqslant 1$. Furthermore, $\forall j, p_j^r \to p_j$ and, because $|\pi^r - \pi| \to 0$, $\forall j, \pi_j^r \to \pi_j$. Thus $\pi_j^{r-1} p_j^{r-1} \to \pi_j p_j$ and the Lebesgue-dominated convergence theorem implies that

$$\lim_{r \to \infty} \left(\sum_{j \geqslant 1} \pi_j^{r-1} p_j^{r-1} \right) = \left(\sum_{j \geqslant 1} \pi_j p_j \right) = c_\phi.$$

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Substituting into equation (3.6) we find that, for every $\epsilon > 0$,

$$\mathrm{E}(\mathrm{Depth}_n(P)) \geqslant \frac{\ln n}{\ln \phi}(c_\phi - \epsilon) + O(1). \tag{3.19}$$

To prove Theorem 3.1 it will therefore suffice to show that $\lim_{\phi \to 1}(c_\phi / \ln \phi) = f/(e-2)$.

Let $\tilde{\pi}_i = \lim_{\phi \to 1} \pi_i$ (we omit the straightforward but tedious formal justification of the existence of $\tilde{\pi}_i$). Taking the limit as $\phi \to 1$ of equation (3.18) yields

$$\tilde{\pi}_i = \left[\frac{1}{i+1} \cdot \frac{1}{i} \cdots \frac{1}{3}\right] \cdot \tilde{\pi}_1 = \frac{2}{(i+1)!} \cdot \tilde{\pi}_1. \tag{3.20}$$

Equating the sum of the steady state probabilities to one, we get

$$2\tilde{\pi}_1 \sum_{i \geqslant 1} \frac{1}{(i+1)!} = 1 \tag{3.21}$$

or

$$\tilde{\pi}_1 = \frac{1}{2(e-2)}. \tag{3.22}$$

For any specific ϕ we can rewrite equation (3.14) as follows:

$$c_\phi = \sum_{j \geqslant 1} \pi_j p_j = \pi_1(1 - z_1) = \pi_1(1 - s^2). \tag{3.23}$$

Thus, recalling that $s = \phi^{-f}$ we find that

$$\lim_{\phi \to 1} \frac{c_\phi}{\ln \phi} = \lim_{\phi \to 1} \pi_1 \frac{1 - s^2}{\ln \phi} = -f\tilde{\pi}_1 \lim_{s \to 1} \frac{1 - s^2}{\ln s} = 2f\tilde{\pi}_1 = \frac{f}{e-2}, \tag{3.24}$$

completing the proof of the theorem. □

3.3. Improved lower bounds

The modified random circuit process $\mathscr{P}_\phi$ analysed in the previous subsection keeps track of the number of gates at the deepest level of the random circuit $\mathscr{P}$; the number of gates at the second-deepest level is essentially assumed to be one; and the gates at all other levels are ignored. In the event that a new level is not added during a given stage, this has the effect of underestimating the likelihood that a new gate is added to the deepest level; in turn, this results in underestimating the likelihood of adding a new level in the next stage. This suggests that we might obtain a better lower bound on the expected circuit depth by considering modified random circuits that keep track of the number of gates at two, three, or more of the deepest levels.

We first illustrate the idea for a modified process with two levels: the generalization to more than two levels will be obvious. As before, the process $\mathscr{P}_\phi$ works in stages, operating exactly like process $\mathscr{P}$ within a stage, but activating level-decreasing rules at the end of each stage. These ensure that, between two stages, exactly one of the following transitions occurs.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

T1 The depth of P_ϕ increases by one and the new deepest level contains only one gate. The number of gates on the second-deepest level (the old deepest one) remains the same.

T2 The depth of P_ϕ remains the same and the number of gates on the deepest level increases by one. The number of gates on the second-deepest level remains the same.

T3 The depth of P_ϕ and the number of gates on the deepest level remains the same and the number of gates on the second-deepest level increases by one.

T4 The depth of P_ϕ and the number of gates on the deepest and second-deepest levels all remain the same.

As before, we can model process $\mathscr{P}_\phi$ by a Markov chain. The state of the Markov chain at time r is given by the number of nodes at the deepest and second-deepest levels of P_ϕ at the end of stage r. The details are similar to those developed for the one level Markov chain and are given in the Appendix (Section 4).

It follows that, for every $\epsilon > 0$,

$$\mathrm{E}(\mathrm{Depth}_n(P)) \geqslant \frac{\ln n}{\ln \phi}(c_\phi - \epsilon) + O(1), \tag{3.25}$$

where c_ϕ is a function of the steady state probabilities of this chain. This can be done not only for the two level process but also for processes with three, four, or more levels. However, unlike the Markov chain for the one level process, we do not know how to analytically compute the steady state probabilities for the infinite Markov chains corresponding to two or more levels as functions of ϕ and to take the limit as $\phi \to 1$. Our approach, therefore, is to modify the process further by limiting the maximum number of gates allowed at each of the deepest levels. The resulting process can be modelled by a finite Markov chain. We are then able to compute the steady state probabilities of the finite Markov chain using an equation solver (Maple). In fact, we can directly obtain the value of $\lim_{\phi \to 1}(c_\phi / \ln \phi)$ by solving the equations.

We used Maple to solve the equations for a finite Markov chain corresponding to a five level process for various numbers of states permitted at each level. The results are shown in Table 1. Each entry of the table shows the maximum number of gates allowed at the five deepest levels along with the lower bound achieved. To choose the number of gates permitted on each level, we started with at most one gate allowed on each of the five deepest levels. Each subsequent entry was obtained by looking at the previous entry and attempting to increase the maximum number of gates allowed by one in exactly one out of the five deepest levels. The choice that led to the best lower bound is the one shown in the table. The last row of the table shows the best lower bound of $2.04\ldots f \ln n$ obtained by using this approach. Of course, by building larger Markov chains we could improve this lower bound at the expense of requiring more computer time to solve the equations. We note that every 'solution' is actually a proof of a lower bound. The way we build the Markov chains tells us that the lower bound to the circuit depth can actually be expressed as a function of the steady state probabilities of the Markov chain. Solving the equations to find the steady state probabilities is therefore actually a *proof* of a lower bound. The results in the table can therefore be viewed as the results of a heuristic search for better proofs.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

Table 1 Lower bounds on expected circuit depth (to 4 decimal places). B_i is the maximum number of gates allowed on depth l_{r-i} in the modified random circuit process

B_0	B_1	B_2	B_3	B_4	Lower bound
1	1	1	1	1	$1.0000\, f \ln n$
2	1	1	1	1	$1.3333\, f \ln n$
2	2	1	1	1	$1.4545\, f \ln n$
3	2	1	1	1	$1.5673\, f \ln n$
3	3	1	1	1	$1.6510\, f \ln n$
4	3	1	1	1	$1.6896\, f \ln n$
4	4	1	1	1	$1.7337\, f \ln n$
4	4	2	1	1	$1.7896\, f \ln n$
4	4	3	1	1	$1.8201\, f \ln n$
4	5	3	1	1	$1.8479\, f \ln n$
5	5	3	1	1	$1.8819\, f \ln n$
5	5	4	1	1	$1.9072\, f \ln n$
5	6	4	1	1	$1.9295\, f \ln n$
5	6	5	1	1	$1.9491\, f \ln n$
6	6	5	1	1	$1.9652\, f \ln n$
6	7	5	1	1	$1.9817\, f \ln n$
6	7	6	1	1	$1.9970\, f \ln n$
6	7	6	2	1	$2.0120\, f \ln n$
6	7	7	2	1	$2.0231\, f \ln n$
6	7	7	3	1	$2.0352\, f \ln n$
6	8	7	3	1	$2.0479\, f \ln n$

Table 2 Simulated lower 'bounds' on expected circuit depth. These 'bounds' have not been proven but are suggested by the results of Markov chain simulations

Levels	Simulated lower bound
1	$1.39\, f \ln n$
2	$1.78\, f \ln n$
3	$2.08\, f \ln n$
4	$2.26\, f \ln n$
5	$2.37\, f \ln n$
10	$2.44\, f \ln n$
20	$2.44\, f \ln n$

Since the computer time needed to solve equations quickly becomes enormous, we also directly simulated the Markov chains to compute the steady state probabilities. This was done as follows. Since the best lower bound is obtained in the limiting case as $\phi \to 1$, we chose $s = \phi^{-f} = 0.999$. We started the simulation from the state of the Markov chain that corresponds to having one gate at each of the deepest levels. At each step, using a random number generator, we carried out a transition to another state in accordance with the probabilities of the Markov chain. This step was repeated 10^8 times to get rid of any biases introduced by the initial probability distribution. Then the process was continued for another 10^8 steps, during which the time spent in each state was recorded;

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

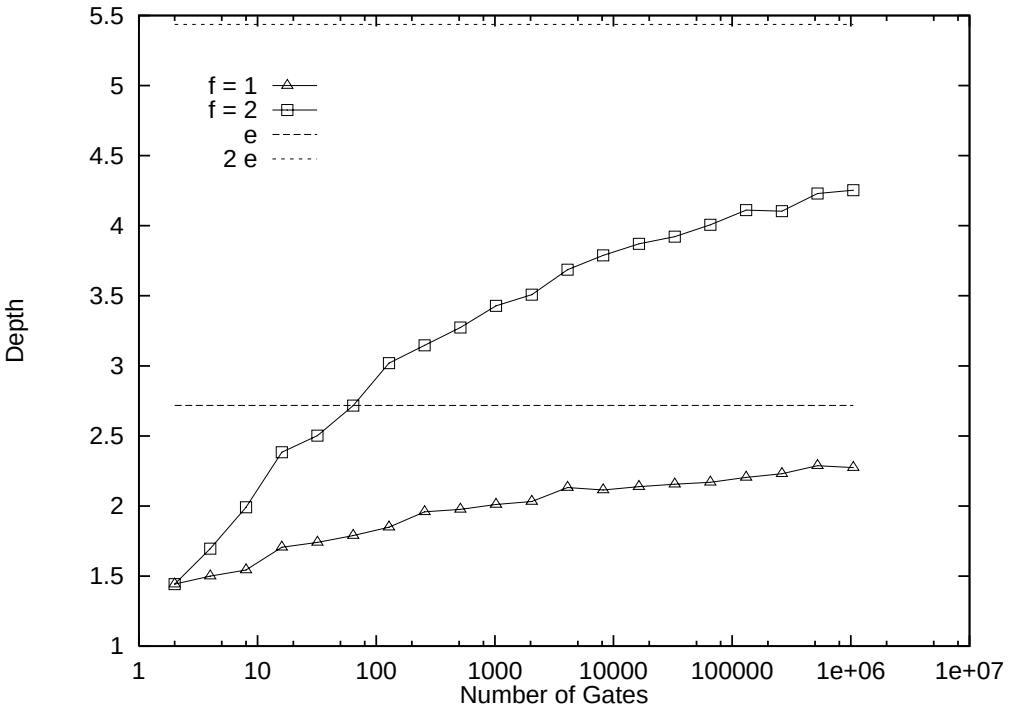


Figure 4 Ratio of circuit depth divided by $\ln n$ for fanins $f = 1$ and $f = 2$

the time spent in a state as a fraction of the total number of steps should approach the steady state probability. In order to obtain the best results, we did not place any limit on the maximum number of gates allowed at each level. We did the simulation for Markov chains corresponding to 1, 2, 3, 4, 5, 10 and 20 level processes. The corresponding lower bounds are shown in Table 2. The best lower bound we obtained is $2.44\ldots f \ln n$ for a 10 level Markov chain; using more levels than 10 barely improved the lower bound. Note that these are not really lower bounds: these are the simulation results for the Markov chains which should be telling us with great accuracy (but not total certainty) the values of the stationary probability distribution, which in turn give us the lower bound. If the stationary distribution values are accurate, then using a Markov chain equation solver will yield these values, formally proving the lower bounds.

We conclude by noting that we attempted to check our results and derive intuition as to the actual upper bound by simulating the random circuit process for fanin $f = 2$. In our experiments, we computed the average depth of the circuit over 100 different trials (see Figure 4). Unfortunately, the process, if it does converge, seems to do so very slowly, with the depth of the circuit divided by $\ln n$ still growing at $n = 1,000,000$ nodes. As a second check on our work we also simulated the random circuit process for fanin $f = 1$, the random tree, for which it is known that the depth converges to $e \ln n$. The depth of our generated trees divided by $\ln n$, even with n approaching $1,000,000$ nodes, did not appear to exhibit convergent behaviour. It seems that processes of this type possess very slow convergence, a property that deserves further examination.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

4. Appendix

We present more details on how to model the two level modified random circuit process using a Markov chain (see Section 3.3). The process $\mathscr{P}_\phi$ knows four pieces of information at the end of stage $r-1$: the depth of the modified circuit l_{r-1}; sets $S_{1,r-1}$ and $S_{2,r-1}$ of gates at depths l_{r-1} and $l_{r-1}-1$, respectively; some gate g_{r-1} at depth $l_{r-1}-2$. On completing a stage there are four possibilities, as follows.

1. Some gate $g' \in S_{1,r-1}$ was chosen as the parent of one of the newly created gates, call it g'', added during the stage. In this case, the depth of g'' is at least $l_{r-1}+1$.
2. The first case did not hold but some gate $g' \in S_{2,r-1}$ was chosen as the parent of one of the newly created gates, call it g'', added during the stage. In this case the depth of g'' is at least l_{r-1}.
3. The first two cases did not hold but g_{r-1} was the parent of some gate, call it g'. Note that the depth of g' is at least $l_{r-1}-1$.
4. None of the first three cases occur.

The corresponding actions taken by $\mathscr{P}_\phi$ are as follows.

1. Move g'' to depth $l_{r-1}+1$. Set $l_r = l_{r-1}+1$, g_r to be any gate from $S_{2,r-1}$, $S_{2,r} = S_{1,r-1}$ and $S_{1,r} = \{g''\}$.
2. Move g'' to depth l_{r-1}. Set $l_r = l_{r-1}$ and $S_{1,r} = S_{1,r-1} \cup \{g''\}$.
3. Move g' to depth $l_{r-1}-1$. Set $l_r = l_{r-1}$ and $S_{2,r} = S_{2,r-1} \cup \{g'\}$.
4. Nothing.

After completing these actions the process then moves *all* gates at level $l_r - 1$ or greater except for those in $S_{1,r}$ and $S_{2,r}$ to level $l_r - 2$. The probabilities of the transitions are defined as follows:

$$\begin{aligned}
p^r_{i,j} &= \Pr\left(|S_{1,r}| = i, |S_{2,r}| = j \text{ and transition } \mathbf{T1} \text{ occurs after stage } r+1\right),\\
q^r_{i,j} &= \Pr\left(|S_{1,r}| = i, |S_{2,r}| = j \text{ and transition } \mathbf{T2} \text{ occurs after stage } r+1\right),\\
t^r_{i,j} &= \Pr\left(|S_{1,r}| = i, |S_{2,r}| = j \text{ and transition } \mathbf{T3} \text{ occurs after stage } r+1\right),\\
z^r_{i,j} &= \Pr\left(|S_{1,r}| = i, |S_{2,r}| = j \text{ and transition } \mathbf{T4} \text{ occurs after stage } r+1\right),
\end{aligned}$$

and let

$$\pi^r_{i,j} = \Pr\left(|S_{1,r}| = i, |S_{2,r}| = j\right).$$

We can derive the transition probabilities using the same method as for the one level Markov chain.

Lemma 4.1.

$$p^r_{i,j} = 1 - \phi^{-if} + O\left(\phi^{-r}\right), \tag{4.1}$$

$$q^r_{i,j} = \phi^{-if}\left(1 - \phi^{-jf}\right) + O\left(\phi^{-r}\right), \tag{4.2}$$

$$t^r_{i,j} = \phi^{-(i+j)f}\left(1 - \phi^{-f}\right) + O\left(\phi^{-r}\right), \tag{4.3}$$

$$z^r_{i,j} = \phi^{-(i+j+1)f} + O\left(\phi^{-r}\right). \tag{4.4}$$

We let $p_{i,j}, q_{i,j}, t_{i,j}$, and $z_{i,j}$ denote the limit values of these transition probabilities. Arguing exactly as for the one level Markov chain we can show that, for every $\epsilon > 0$,

$$\mathrm{E}\left(\mathrm{Depth}_n(P)\right) \geqslant \frac{\ln n}{\ln \phi}(c_\phi - \epsilon) + O(1), \tag{4.5}$$

where $c_\phi = \sum_{i,j} \pi_{i,j} p_{i,j}$.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press

References

[1] Diaz, J., Serna, M. J., Spirakis, P. and Toran, J. (1994) On the expected depth of Boolean circuits. Report LSI-94-7-R, Departament de Llenguatges i Sistemes, Universitat Politècnica Calalunya Pau Gargallo 5, Barcelona.

[2] Grimmett, G. R. and Stirzaker, D. R. (1992) *Probability and Random Processes* (2nd edn), Clarendon Press, Oxford.

[3] Mahmoud, H. and Smythe, R. T. (1991) On the distribution of leaves in rooted subtrees of recursive trees. *Ann. Appl. Probab.* **1** 406–418.

[4] Meir, A. and Moon, J. (1974) Recursive trees with no nodes of outdegree one. *Congr. Numer.* **66** 49–62.

[5] Moon, J. (1974) The distance between nodes in recursive trees. In Vol. 13 of *London Math. Soc. Lecture Notes*, Cambridge University Press, pp. 125–132.

[6] Na, H. and Rapaport, A. (1970) Distribution of nodes of a tree by degree. *Math. Biosci.* **6** 313–329.

[7] Pittel, B. (1994) Notes on the heights of random recursive trees and random *m*-ary search trees, *Random Struct. Alg.* **5** 337–347.

[8] Szymanski, J. (1990) On the maximum degree and the height of a random recursive tree. In *Random Graphs '87* (M. Karoński, J. Jaworski and A. Ruciński, eds), Wiley, New York, pp. 431–524.

[9] Tsukiji, T. and Xhafa, F. (1996) On the depth of randomly generated circuits. In *Proc. 4th Annual Symposium on Algorithms*, Springer, pp. 208–220.

https://doi.org/10.1017/S096354839900382X Published online by Cambridge University Press