Circuit depth relative to a random oracle

Peter Bro Miltersen
Aarhus University, Computer Science Department
Ny Munkegade, DK 8000 Aarhus C, Denmark.
bromille@daimi.aau.dk

August 1991

Keywords: Computational complexity, random oracles, circuit depth.

Introduction

The study of separation of complexity classes with respect to random oracles was initiated by Bennett and Gill [1] and continued by many authors.

Wilson [5, 6] defined relativized circuit depth and constructed various oracles $A$ for which $P^A \neq NC^A$, $NC^A_k \neq NC^A_{k+\epsilon}$, $AC^A_k \neq AC^A_{k+\epsilon}$, $AC^A_k \not\subseteq NC^A_{k+1-\epsilon}$ and $NC^A_k \not\subseteq AC^A_{k-\epsilon}$ for all positive rational $k$ and $\epsilon$, thus separating those classes for which no trivial argument shows inclusion. In this note we show that as a consequence of a single lemma, these separations (or improvements of them) hold with respect to a random oracle $A$.

The results

Let $\Sigma = \{0, 1\}$ and let $\log n$ denote $\log_2 n$. Recall the following definitions by Wilson [4, 5, 6].

---

*This research was partially supported by the ESPRIT II Basic Research actions Program the EC under contract No. 3075 (project ALCOM).
Definition 1 A bounded fan-in oracle circuit $C$ is a circuit containing negation gates of indegree 1, and and or gates of indegree 2 as well as of unspecified oracle gates of various indegrees, giving a single boolean output. Given an oracle $A$, i.e. a subset of $\Sigma^*$, $C^A$ denotes the circuit, where each oracle gate of indegree $m$ in $C$ has been replaced by a gate computing $\chi_A : \Sigma^m \to \Sigma$, where $\chi_A(x)$ is 1 if $x \in A$ and 0 otherwise. The depth of an oracle gate with $n$ inputs is $\lceil \log n \rceil$. The size of an oracle gate with $n$ inputs is $n - 1$. The boolean gates have size and depth 1. The size of an oracle circuit is the sum of the sizes of its gates. The depth of a path in the circuit is the sum of the depths of the gates along the path. The depth of the circuit is the depth of its deepest path.

Definition 2 An unbounded fan-in oracle circuit $C$ is defined as in the bounded fan-in case, except that and and or gates of arbitrary indegree are allowed, and each oracle gate is only charged a depth of 1. The depth of an unbounded fan-in circuit is thus simply the length of its longest path.

Definition 3 DEPTH$_{1,0}^A(d)$ is the class of functions $f$ so that for infinitely many integers $n$ a bounded fan-in oracle circuit $C_n$ with $n$ inputs of depth at most $d$ exists, so that $C_n^A(x) = f(x)$ for all $x \in \Sigma^n$, where $C_n^A(x)$ denotes the output of $C_n^A$ when $x$ is given as input.

Let $k$ be a positive rational number. NC$_k^A$ is the class of functions $f$ for which a logspace-uniform family of polynomial size, $O(\log^k n)$-depth bounded fan-in circuits $C_n$ with $n$ inputs exists, so that $C_n^A(x) = f(x)$. AC$_k^A$ is the class of functions $f$ for which a logspace-uniform family of polynomial size, $O(\log^k n)$-depth unbounded fan-in circuits $C_n$ with $n$ inputs exists, so that $C_n^A(x) = f(x)$.

Let $A$ be an oracle. Let $t_1^n, \ldots, t_n^n$ be the $n$ lexicographically first strings of length $\lceil \log n \rceil$. Let $f_n^A : \{0,1\}^n \to \{0,1\}^n$ be the function $f_n^A(x) = \chi_A(xt_1^n)\chi_A(xt_2^n)\cdots\chi_A(xt_n^n)$.

Lemma 4 Let $n$ and $d$ be positive integers. Let $C$ be a fixed oracle circuit with $n$ boolean inputs and $n$ boolean outputs containing at most $s = 2^{n+2-\log d}$ oracle gates of indegree exactly $n + \lceil \log n \rceil$ so that no path in $C$ contains more than $d$ oracle gates of indegree exactly $n + \lceil \log n \rceil$ (no restric-
tions is made on gates of other indegrees). Then, for a random oracle \( A \), the probability that \( C^A \) computes \((f^n_A)^{d+1}\), i.e. the composition of \( f^n_A \) with itself \( d + 1 \) times, is at most \( 2^{-2^n} \).

**Proof** Let us call the oracle gates of indegree \( n + \lceil \log n \rceil \) for interesting. We partition the gates of \( C \) into \( d \) levels 0, 1, \ldots, \( d - 1 \), such that no path exists from the output of any interesting gate at level \( i \) to the input of any interesting gate at level \( j \) if \( j \leq i \). The idea of the proof is to show that with high probability, \((f^n_A)^{i+1}(x)\) is not computed before level \( i \). Given an oracle \( A \) and a vector \( x \in \Sigma^n \), let \( I^A_x(i) \) denote the set of strings \( y \) for which some string \( t \) of length \( \lceil \log n \rceil \) exists, so that \( yt \) is given as input to some interesting gate at level \( i \), when \( C^A \) is given \( x \) as an input. For convenience, let \( I^A_x(d) = \{C^A(x)\} \).

Consider the following procedure for finding an \( x \) so that \( C^A(x) \neq (f^n_A)^{d+1}(x) \).

1. \( L := \emptyset \).
2. if \( \Sigma^n \subseteq L \) then abort, we were not successful.
3. select any \( x \in \Sigma^n \setminus L \).
4. \( x_0 := x \).
5. for \( i := 0 \) to \( d \) do
6. compute \( I^A_x(i) \) by simulating the necessary parts of the circuit.
7. \( L := L \cup I^A_x(i) \cup \{x_i\} \).
8. \( x_{i+1} := f^n_A(x_i) \).
9. if \( x_{i+1} \in L \) then goto 2.
10. od.
11. return \( x \).

Let us first observe that the protocol indeed returns an \( x \) with the desired property in case it does not abort. This is so, because \( x_{d+1} = (f^n_A)^{d+1}(x) \), and
the algorithm makes sure that \( x_{d+1} \notin L \) at a time when \( I^A_x(d) \subseteq L \) and by
definition \( C^A(x) \in I^A_x(d) \). Let us then estimate the probability of abortion.
We will first give an upper bound on the probability of leaving the for-loop
at line 9. For convenience, let us assume that the membership of a string in
\( A \) is not determined until the algorithm asks for it. It is easy to see that the
protocol makes sure that no bit of the value of \( f^A_n(x_i) \) has been determined
previous to line 8. Hence, all \( 2^n \) values are equally likely. Of these values, \( |L| \)
causes the algorithm to leave the for-loop in the next line. Hence, each time
line 9 is encountered, the probability of leaving the loop is exactly \( \frac{|L|}{2^n} \).
If we assume that \( m \) values of \( x \) has been tried so far (including the current value),
an upper bound of this is \( \frac{m(s+d+1)}{2^n} \leq \frac{3dms}{2^n} \). Thus, each time the for-loop
is executed, an upper bound of the probability of leaving it prematurely is
\( (d+1)\frac{3dms}{2^n} \leq \frac{6d^2ms}{2^n} \). Since the algorithm will try different values of \( x \) at least
until this upper bound is 1 and the above argument applies to all of them,
we have that for any positive integer \( k \):

\[
Pr(\text{abortion}) \leq \frac{6d^2ms}{2^n} \leq \frac{3dms}{2^n} k.
\]

Putting \( k = \lceil 2^n \rceil \), we get:

\[
Pr(\text{abortion}) \leq 2^{-2^\frac{n}{2}}.
\]

\[\square\]

**Theorem 5** For \( \alpha < \frac{1}{2} \), \( P^A \not\subseteq \text{DEPTH}^A_{\text{i.o.}}(\alpha n) \) for a random oracle \( A \) with
probability 1.

**Proof** Let \( d_n = [\alpha n] \). The family of functions \( g^A_n = (f^A_n)^d_n+1 \) is clearly
in \( P^A \). Fix \( n \) and let \( C \) be a fixed bounded fan-in oracle circuit of depth
\( d_n \). It is easy to see that the size of \( C \) is at most \( 2^{d_n} \), so by the lemma,
the probability that \( C^A \) computes \( g^A_n \) is at most \( 2^{-2^\frac{n}{2}} \). There are at most
\( 2^{2^d_n+o(d_n)} \) bounded fan-in oracle circuits of depth \( d_n \), so the probability that
some such circuit computes \( g^A_n \) with \( A \) as oracle is at most \( 2^{2^d_n+o(d_n)} \cdot 2^{-2^\frac{n}{2}} \) which
is less than \( 2^{-n} \) for sufficiently large \( n \). Thus, for fixed \( N \), the probability
that for some \( n \) greater than \( N \), \( g^A_n \) has \( A \)-circuits of depth at most \( \alpha n \), is
at most \( \sum_{n=N}^\infty 2^{-n} = 2^{-N+1} \). The probability that for all \( N \), an \( n \) greater
than \( N \) exists, so that \( g^A_n \) has circuits of depth at most \( \alpha n \), is thus at most
\[ \inf_N 2^{-N+1} = 0. \]

The theorem is an improvement of Wilson’s result [5] that oracles \( A \) exists, so that \( P^A \neq NC^A \). Since every function has unrelativized depth at most \( n + o(n) \), the result is optimal, up to a multiplicative constant of \( 2 + \epsilon \).

Similar results about circuit size were obtained by Lutz and Schmidt [3] who showed that for small \( \alpha \) and a random oracle \( A \), \( NP^A \not\subseteq SIZE_{i.o.}^A(2^{\alpha n}) \) and by Kurtz, Mosey and Royer [2], who proved \( NP^A \not\subseteq co-NSIZE_{i.o.}^A(2^{\alpha n}) \).

**Theorem 6** For rational \( k \geq 0 \) and \( \epsilon > 0 \), \( AC^A_k \not\subseteq NC^A_{k+1-\epsilon} \) for random \( A \) with probability 1.

**Proof** Let \( d_n = \lfloor \log^k n \rfloor \) and \( g_n^A = (f_n^A)^{d_n+1} \). \( g_n^A \) is in \( AC^A_k \). It is sufficient to prove that with probability 1, \( g_n^A \) is not computed by a family of bounded fan-in circuits \( C_n \) of depth \( O(\log^{k+1-\epsilon} n) \). Fix an \( n \) and a circuit \( C_n \) within this bound. Observe that \( C_n \) can not contain a path with more than \( O(\log^{k-\epsilon} n) \) oracle gates of indegree \( n + \lceil \log n \rceil \) and that \( C_n \) satisfies the size bound of the lemma. Thus, the probability that \( C_n \) computes \( g_n^A \) is at most \( 2^{-2^{\frac{n}{2}}} \). Now proceed as in the previous proof.

It is easy to see from the proof that we actually get the stronger result that there are functions in \( AC^A_n \) which can not be computed in depth \( o(\log^{k+1} n) \) by bounded fan-in \( A \)-circuits.

**Theorem 7** For rational \( k > 0 \) and \( \epsilon > 0 \), \( NC^A_k \not\subseteq AC^A_{k-\epsilon} \) for random \( A \) with probability 1.

**Proof** The proof is bred upon the idea behind the corresponding oracle construction by Wilson [6]. Let \( d_n = \lfloor \log^k n \rfloor \), \( m_n = \lfloor \log^2 n \rfloor \) and let \( g_n^A(x_1x_2\ldots x_n) = (f_{mn}^A)^{d_n+1}(x_1x_2\ldots x_{m_n}) \). \( g_n^A \) is in \( NC^A_k \), since we are only charged depth \( O(\log \log n) \) for computing \( f_{mn}^A \). The probability that \( g_n^A \) is computed by a specific circuit of size \( O(n^l) \), depth \( O(\log^{k-\epsilon} n) \), even with unbounded fan-in, is, by the lemma, at most \( 2^{-2\frac{mn}{2}} \leq 2^{-n - \frac{\log n}{2}} \). Now proceed as in the previous proofs.

The proof actually gives us functions in \( NC^A_k \) which require superpolynomial size to be computed in depth \( o(\log^k n/\log \log n) \) with unbounded fan-in \( A \)-
circuits. This is optimal, since standard techniques provide a simulation of $NC_k^A$ by polynomial size, depth $O(\log^k n/\log \log n)$, unbounded fan-in $A$-circuits.

**Corollary 8** For rational $k \geq 0$ and $\epsilon > 0$, $NC_k^A \neq NC_{k+\epsilon}^A$ and $AC_k^A \neq AC_{k+\epsilon}^A$ for random $A$ with probability 1.

**References**


