Probabilistic $\text{NC}^1$-Circuits Equal Probabilistic Polynomial Time

Marek Karpinski
Rutger Verbeek

Abstract We prove that probabilistic $\text{NC}^1$ ($\text{PrNC}^1$) circuits (i.e. uniform log-depth poly-size circuits with unbounded error probability) are computationally exactly as powerful as probabilistic polynomial time. This entails that the probabilistic $\text{NC}^k$-hierarchy collapses at the $\text{NC}^1$ level; if unbounded fan-in is allowed it collapses even at the level $0$. As a side effect we prove the identity $\text{PrNC} = \text{Pr}_2\text{SC} = \text{Pr}_2\text{SC}^1$ ($\text{Pr}_2\text{SC}^k$ meaning simultaneous polynomial time and $\log n$ space bounded machines with two-way random tape [KV 84]). The central problems in computational complexity theory are whether $\text{NC} = \text{P}$ [Co 83], $\text{NC}^2 = \text{NC}$ and $\text{SC} = \text{NC}$ [Co 79, Ru 81] and the most classical problem whether $\text{LOGSPACE} = \text{P}$. Surprisingly the results of the present paper and [KV 84] give affirmative answer to all these questions in the probabilistic case.

* Dept. of Computer Science, University of Bonn, Wegelerstraße 6, 5300 Bonn 1 W.-Germany (mailing address)
† Dept. of Computer Science, University of Dortmund, 4600 Dortmund 5o, W.-Germany
1. Probabilistic uniform circuits

The reader is referred to [Co 83] for an extended exposition on uniform circuits. The main definitions are given below.

A circuit $C$ with $n$ inputs is a finite directed acyclic graph, such that each node has a label from $\{x_1, \ldots, x_n\} \cup \{\Lambda, \nu, \tau\}$. A node labelled $x_i$ has indegree (fan-in) 0 and is called an input node. A node $\nu$ with label from $\{\Lambda, \nu\}$ must have indegree 2, whereas $\tau$ with label $\tau$ has indegree 1. Exactly one node does have outdegree (fan-out) 0; we call it the output node $y$. The fan-out of the other nodes is unbounded.

The size of $C$ ($s(C)$) is the number of nodes in $C$, the depth $d(C)$ is the length of the longest path in $C$. Every 0-1 assignment to the input nodes (interpreted as boolean variables) yields unique 0-1 assignment to all the remaining nodes (including $y$). In this way one defines a boolean function $f_C : \{0, 1\}^n \rightarrow \{0, 1\}$, called the function computed by $C$.

A function $f : \{0, 1\}^* \rightarrow \{0, 1\}$ is computed by a circuit family $<$ of $\nu$, $n \in \mathbb{N}$, if for every $n$, $f_C \equiv f \mid \{0, 1\}^n$. A circuit family $<$ is called uniform, if $C_n$ can be constructed from $n$ in $O(\log n)$ space [Bo 77, Ru 81].

$\text{NC}^k$ is the class of all functions computable by a uniform circuit family with $s(C_n) = O(1)$ and $d(C_n) = O(\log^kn)$, $\text{NC} = \bigcup_k \text{NC}^k$.

We shall extend the notion of a circuit to circuits with unbounded fan-in for 'AND' and 'OR' gates [SSF 81]. The corresponding classes of functions will be denoted by $\text{QNC}^k$ and $\text{QNC}$.

A probabilistic circuit [Co 83] is a circuit $C$ with ordinary inputs $x_1, \ldots, x_n$ and designated coin-tossing inputs $z_1, \ldots, z_m$. The probability that the output $y$ is one (on input $x_1, \ldots, x_n$) is the fraction of input bit-vectors $z_1, \ldots, z_m$ for which $f_C(x_1, \ldots, x_n, z_1, \ldots, z_m) = 1$. We say a function $f$ is probabilistically computed by $<$, if for all $n$ and all $x_1, \ldots, x_n$

$$\Pr[f_C(x_1, \ldots, x_n, z_1, \ldots, z_m) = f(x_1, \ldots, x_n)] > \frac{1}{2}. \quad \text{(When } \frac{1}{2} \text{ in the definition above is replaced by } \frac{3}{4}, f \text{ is Monte-Carlo computable by } C [Co 83]).$$

$\text{PrNC}^k$ is the class of all functions probabilistically computable by a uniform circuit family with depth $O(\log^kn)$ and polynomial size, $\text{PrNC} = \bigcup_k \text{PrNC}^k$; for unbounded fan-in $\text{PrQNC}^k$ and $\text{PrQNC}$ is defined analogously. (The class $\text{PrNC}$ is the probabilistic version of S. Cook's Monte-Carlo $\text{RNC-class} [Co 83].$)
2. Uniform circuits and two-way random generators

For an exact definition of two-way random-tape and the corresponding complexity classes see [KV 84].

Informally, a language in $\Pr_2 \text{SPACE}(f(n))$ is recognized by a probabilistic $f(n)$-space bounded machine with two-way access to a random sequence. The following depends on the fact that circuits have multiple access to the random input.

Theorem 1 [KV 84] Probabilistic machines with two-way random-tape that are simultaneously log $n$-space and polynomial-time bounded are as powerful as those without restriction on space:

$$\Pr_2 \text{SC}^1 = \text{PP}.$$  

The proof of Theorem 1 is based on the following construction (Lemmas 1 and 2) which is adapted from the proof of Lemma 5 of [KV 84] and modified now for application in uniform circuits.

Let $M$ be a probabilistic strictly $n^k$-time bounded one-tape machine. (For every $f \in \text{PP}$ there exists $k$, such that $f$ is strictly $n^k$-time computable [Gl 77].) Denote by $\text{comp}_M(x)$ the set of $M$-computations on input $x$ encoded by $c_0 \leq c_1 \leq \ldots \leq c_n \in \mathbb{E}^*$, where the $c_i$'s are encodings of IDs padded with blanks to exactly the same length $n^k$ and the $a_i$'s are the random bits of the computation, such that $c_i M c_{i+1}$ for the random bit $a_i$. A stopping ID $c_i, i < n^k$, is identically repeated up to the step $n^k$ with arbitrary random bits $a_i$.

We encode now the computations in binary using a coding function $h : \Sigma \rightarrow \{0,1\}^*$ for an appropriate $l$. Denote $\text{bincomp}_M(x) = h(\text{comp}_M(x))$ (for $h$ naturally extended over $\mathbb{E}^*$).

Lemma 1 Given an arbitrary probabilistic strictly $n^k$-time bounded one-tape machine $M$, there exists a deterministic log-space bounded machine $\overline{M}$ such that $\overline{M}$ computes the function $f : \Sigma^* x \{0,1\}(0,1)^* \rightarrow \{0,1\}$:

$$f(x,y) = \begin{cases} 1 & \text{if } y \in \text{bincomp}_M(x) \text{ and } h^{-1}(y) \text{ is accepting} \\ 0 & \text{if } y \in \text{bincomp}_M(x) \text{ and } h^{-1}(y) \text{ is rejecting} \\ a & \text{if } y \notin \text{bincomp}_M(x) \end{cases}$$

for $x \in \Sigma^*, a \in \{0,1\}, y \in \{0,1\}^*, (h : \Sigma^* \rightarrow \{0,1\}^* \text{ as above}).$
Proof. Standard construction as for deterministic machines
(cf. [HU 79]).

For a deterministic log \( n \)-space bounded machine \( M \) with binary input
\( \text{bincomp}_M(x) \) will denote now the binary encoding of the computation of \( M \) on \( x \),
such that the codes of single configurations have the same length \( 1 \cdot \log n \)
for an appropriate fixed \( 1 \). We denote by \( c_i \) the code of the \( i \)th configuration
consisting of \( s_i, p_i, y_i \) denoting \( s_i \), the contents of the worktapes and the
state, \( p_i \), the binary code of the input position, \( y_i \), the input symbol
(i.e. \( y_i = x_{p_i} \)). Define \( \text{TEST}_M(x,y) = 1 \) if \( y = \text{bincomp}_M(x) \) and
0 if \( y \neq \text{bincomp}_M(x) \).

Lemma 2. Given arbitrary log \( n \)-space bounded machine \( M \) with binary input,
\( \text{TEST}_M(x,y) \) is computed by uniform poly-size constant-depth unbounded
fan-in circuits,
\( \text{TEST}_M \in \text{QNC}^0 \).

Proof. (cf. Figure 1)

Let \( t \) denote an upper bound on the running time of \( M \), i.e.
\( t = n^k \) for an appropriate \( k \) depending on \( M \).

The circuits \( A_i (1 \leq i \leq t) \) compare the configurations \( c_{i-1} \) and \( c_i \)
and generate a "correctness bit" \( r_i \), which is set to 1 iff
\( (s_{i-1}, p_{i-1}) \sim (s_i, p_i) \). \( A_0 \) checks, whether \( c_0 \) is a legal initial
configuration. Furthermore \( A_i (0 \leq i \leq t) \) outputs \( y_i \) and an unary
representation of \( p_i \), i.e. \( v_{ij} = 1 \) iff \( j = p_i \). To do this, it
compares (in parallel) \( p_i \) with \( \beta_j \) (1 \leq j \leq n), \( \beta_j \) denoting the
binary code of \( j \).

The circuits \( B_i (0 \leq i \leq t) \) select the \( p_i \)'s input bit (using \( v_{ij} \)'s),
compare it with \( y_i \) and set the output bit \( q_i \) to 1 iff \( r_i = 1 \) and
\( y_i = x_{p_i} \). If all \( q_i \)'s are 1, the whole circuit outputs 1.
Since the circuits $A_i$ have only $O(\log n)$ inputs and $O(n)$ outputs, the standard depth 3 CNF-representation of their functions have polynomial size; since the $B_i$'s have constant depth and polynomial size, this is true for the whole circuit.

Uniformity of our circuit family is guaranteed by the fact that $A_i$'s (for all $i$) are all identical and the same holds for all $B_i$'s.

**Theorem 2** Any boolean function computed by a polynomial-time bounded machine is computed by some uniform family of probabilistic circuits $\langle C_n \rangle$ with polynomial size, constant depth, and unbounded fan-in:

$$\Pr[\text{QNC}^0] \subseteq \text{PP}.$$  

**Proof** (cf. Figure 2)

Let $M$ be a probabilistic poly-time machine, $M^\prime$ the log-space machine of Lemma 1. The circuit $C_n$ has inputs $x,y,z,a$ ($x$ is an ordinary input of size $n$; $y,z$ are random inputs of appropriate polynomial size; $a$ is a single random bit).

![Diagram](Figure 1)

![Diagram](Figure 2)
Using the circuit of Lemma 2 it computes $\text{TEST}_M^{\overline{M}}(xy, z)$ and in addition
the output of $\overline{M}$ called $\gamma$ (which can be found at a fixed position
in $z$, if $z = \text{bincomp}_M(xy)$. If $\text{TEST}_M^{\overline{M}}(xy, z) = 1$, then $C_n$ outputs $\gamma$,
otherwise $C_n$ outputs $a$.

Let $p$ denote the probability that $M$ outputs 1 on $x$, $n := |x|,
q := \Pr[y \in \text{bincomp}_M(x)]$ and $z = \text{bincomp}_M(x, y)$.
Then $\Pr[C_n$ outputs 1] $= p \cdot q + \frac{1}{2} \cdot \Pr[y \notin \text{bincomp}_M(x) \text{ or } z \notin \text{bincomp}_M(xy)]$
$= p \cdot q + \frac{1}{2} \cdot (1-q) = \frac{1}{2} + \left(p - \frac{1}{2}\right) \cdot q > \frac{1}{2} \iff p > \frac{1}{2}$
$\iff M$ accepts $x$.

PC will stand for the class of boolean functions computed by uniform polynomial-
size circuits.

Lemma 3 The probabilistic uniform poly-size circuit class is included in
probabilistic polynomial time,
$\text{PrPC} \subseteq \text{PP}$.

Proof Given uniform family of probabilistic circuits $\langle C_n \rangle$, the simulating
poly-time bounded machine constructs the circuit $C_n$ in its memory,
using its random generator to assign values to the random inputs of $C_n$.
Since the circuit with the random bits fixed behaves deterministically
we can simulate it in deterministic polynomial time (cf. [Bo 77]).
Since the random pads required for the circuit and the machine have
the same length, the probabilities for accepting and rejecting are
identical in both models.

Theorem 3 The following classes of 0-1-valued functions are all equivalent:

1. $\text{PrNC}^1$ (probabilistic log depth)
2. $\text{PrNC}$ (probabilistic poly-log depth, poly-size)
3. $\text{PrQNC}^0$ (probabilistic constant depth, poly-size)
4. $\text{Pr}_2\text{SC}^1$ (probabilistic log-space poly-time with two-way
   random tape, cf. [KV 84])
5. $\text{PrPC}$ (probabilistic poly-size)
6. $\text{PP}$ (probabilistic poly-time)

$\text{PrNC}^1 = \text{PrNC} = \text{PrQNC}^0 = \text{Pr}_2\text{SC}^1 = \text{PrPC} = \text{PP}$. 
Proof. The equalities follow from Theorem 1, Theorem 2, Lemma 3 and the fact that for all $k$, $\PrQNC^k \subseteq \PrNC^{k+1}$ (decompose a gate with unbounded fan-in $n > 2$ into a log $n$-depth circuit, cf. [Co 83]).

We define the classes of probabilistic $k$-bounded alternation-depth circuits as uniform circuit families with $O(\log^k n)$ levels of AND and OR gates with unbounded fan-ins and negations pushed to the inputs (cf. [Co 83]). Denote the corresponding classes of functions by $\PrADC^k$, $k = 1, \ldots$, $\PrADC = \bigcup_k \PrADC^k$. □

Theorem 4. The probabilistic alternation-depth hierarchy collapses at level 1, $\PrADC^1 = \PrADC = \PP$.

Proof. By Theorem 2, $\PP \subseteq \PrQNC^0$ and this is contained in $\PrADC^1$.

On the other hand $\PrADC^k \subseteq \PrQNC^k$.

□

It is well known [BG 81], [AB-O 84] that nonuniform deterministic poly-size circuits are as powerful as Monte-Carlo ones. By [AB-O 84] the same is true for corresponding deterministic and Monte-Carlo classes of unbounded fan-in.

By [FSS 84] and Theorem 3, the class of uniform probabilistic circuits of constant depth ($\PrQNC^0$) is not included in the class of nonuniform deterministic polynomial size circuits of constant depth (the parity function is in $\P$ and therefore in $\PrQNC^0$, but not in nonuniform $\QNC^0$).

Theorem 5. $\PrQNC^0 \nsupseteq$ nonuniform $\QNC^0$.

□

3. Conclusion

There are natural functions in $\PrQNC^0$, which are not in $\QNC^0$, e.g. majority and parity. The positive answer to the question "are the probabilistic uniform log-depth circuits equivalent to the Monte-Carlo uniform log-depth circuits" would require a breakthrough in complexity theory since $\PrNC^1 \neq \RNC^1 \subseteq \BPP$ unless Monte-Carlo poly-time equals probabilistic poly-time. One level higher a negative answer to the same question (with $\log n$ replaced by $\log^2 n$), i.e. $\PrNC^2 \neq \RNC^2$ would imply probabilistic $\LOGSPACE$ is unequal to probabilistic polynomial time.
Finally we indicate another application of our result towards probabilistic versions of the parallel WRAMs of [CSV 82]: any such (both deterministic and probabilistic) WRAM with a polynomial number of processors can be simulated by some PrWRAM with a polynomial number of processors in $\log n$ parallel time.

References

[AB-O 84] Ajtai, M., and Ben-Or, M.,
A theorem on probabilistic constant depth computations,

[Bo 77] Borodin, A.,
On relating time and space to size and depth,
SIAM Journal on Computing 6 (1977), pp. 733-744

[BCP 83] Borodin, A., Cook, S., and Pippenger, N.,
Parallel computation for well endowed rings and space-bounded probabilistic machines,
Information and Control 58 (1983), 96-114

[BG 81] Benett, C., and Gill, J.,
Relative to a random oracle $A$, $P^A \neq NP^A \neq co-NP^A$ with probability 1,

[Co 83] Cook, S.
The classification of Problems which have fast parallel algorithms,

[CSV 82] Chandra, A.K., Stockmeyer, L.J., and Vishkin, U.,
A complexity theory for unbounded fan-in parallelism,

[FSS 81] Furst, M., Saxe, J.B., and Sipser, M.,
Parity, Circuits, and the polynomial time hierarchy,

[Gi 77] Gill, J.,
Computational complexity of probabilistic Turing machines,
SIAM Journal on Computing 6 (1977), pp. 675-694
Hopcroft, J., and Wilber, J.,
Introduction to automata theory, languages, and computation,
Addison-Wesley, Reading (1979).

Karpinski, M., and Verheek, R.,
There is no polynomial deterministic space simulation of probabilistic
space with two-way random-tape generator,
Interne Bericht 1/4 des Instituts für Informatik, Universität Bonn
(1984), submitted to Information Control

Karpinski, M., and Verheek, R.,
On the power of two-way random generators and the impossibility
of deterministic poly-space simulation,
Interne Bericht 1/5 des Instituts für Informatik, Universität Bonn
(1984)

Pippenger, N.,
On simultaneous resource bounds (preliminary version),
Proc. 20th IEEE FOCS (1979), 307-311

Ruzzo, W.L.,
On uniform circuit complexity,

Sipser, M.,
A complexity theoretic approach to randomness,

Stockmeyer, L.J.,
The complexity of approximate counting,
Proc. 15th ACM STOC (1983), pp. 118-126