Consequently,

$$\begin{aligned}
[\textstyle\sum_{i=0}^{\infty}(I-B)^i]_{1,m} &= [\textstyle\sum_{i=0}^{\infty} C^i]_{1,m} + [\textstyle\sum_{i=0}^{\infty} C^i C']_{1,m} \\
&= [\textstyle\sum_{i=0}^{\infty} C^i]_{1,m} + \textstyle\sum_{i=0}^{\infty}(\sum_{j=1}^{m}[C^i]_{1,j}[C']_{j,m}) \\
&= [\textstyle\sum_{i=0}^{\infty} C^i]_{1,m} + \textstyle\sum_{i=0}^{\infty}[C^i]_{1,m-1}[C']_{m-1,m} \\
&= [\textstyle\sum_{i=0}^{\infty} C^i]_{1,m} + (1-\frac{1}{2^{q(n)}})\textstyle\sum_{i=0}^{\infty}[C^i]_{1,m-1}
\end{aligned}$$

End of Proof of Claim.

To complete the proof of the theorem, it will suffice to show that $w \in S$ if and only if $\sum_{i=0}^{\infty}[C^i]_{1,m} \geq (1-\frac{1}{2^{q(n)}})\sum_{i=0}^{\infty}[C^i]_{1,m-1}$.

If w is in S, then

$$\begin{aligned}
\textstyle\sum_{i=0}^{\infty}[C^i]_{1,m} &\geq \textstyle\sum_{i=0}^{2^{p(n)}}[C^i]_{1,m} \\
&= \textstyle\sum_{i=0}^{2^{p(n)}}[(1-\frac{1}{2^{q(n)}})A^i]_{1,m} \\
&\geq (1-\frac{1}{2^{q(n)}})^{2^{p(n)}}\textstyle\sum_{i=0}^{2^{p(n)}}[A^i]_{1,m} \\
&> (1-\frac{1}{2^{p(n)}})\textstyle\sum_{i=0}^{2^{p(n)}}[A^i]_{1,m} > \frac{1}{2} \\
&> (1-\frac{1}{2^{q(n)}})\frac{1}{2} \\
&> (1-\frac{1}{2^{q(n)}})\textstyle\sum_{i=0}^{\infty}[A^i]_{1,m-1} \\
&\geq (1-\frac{1}{2^{q(n)}})\textstyle\sum_{i=0}^{\infty}[C^i]_{1,m-1}.
\end{aligned}$$

If w is not in S, then

$$\begin{aligned}
(1-\tfrac{1}{2^{q(n)}})\textstyle\sum_{i=0}^{\infty}[C^i]_{1,m-1} &\geq (1-\frac{1}{2^{q(n)}})\textstyle\sum_{i=0}^{2^{p(n)}}(1-\frac{1}{2^{q(n)}})^i[A^i]_{1,m-1} \\
&> (1-\frac{1}{2^{q(n)}})^{1+2^{p(n)}}\textstyle\sum_{i=0}^{2^{p(n)}}[A^i]_{1,m-1} \\
&> (1-\frac{1}{2^{p(n)}})(\frac{1}{2}+\frac{1}{2^{p(n)}}) > \frac{1}{2} \\
&> \textstyle\sum_{i=0}^{\infty}[A^i]_{1,m} \\
&\geq \textstyle\sum_{i=0}^{\infty}[C^i]_{1,m}.
\end{aligned}$$

■

First note that summing the absolute values of the entries of any column of $I - B$ yields a number strictly less than one. That is, there is a number $g < 1$ such that each entry of $(I-B)^i$ is less than g^i, and thus $\sum_{i=0}^{\infty}(I-B)^i$ converges. (Since this sum converges, it must therefore be equal to the unique solution of the equation $X = I - BX + X$, which is equal to B^{-1}.)

Claim:

$$\sum_{i=0}^{\infty}[(I-B)^i]_{1,m} = \sum_{i=0}^{\infty}[C^i]_{1,m} - (1 - \frac{1}{2^{q(n)}})\sum_{i=0}^{\infty}[C^i]_{1,m-1}$$

Note that this claim says that the question of whether or not $\sum_{i=1}^{\infty}(I-B)^i \geq 0$ is roughly the same as the question of whether the probability that M accepts x is greater than the probability that M rejects x (since C differs from the transition matrix of M only by a multiplicative constant that is very close to 1).

Proof of Claim: First we show that for all $i \geq 1$,

$$(I-B)^i = C^{i-1}(I-B).$$

This is trivially true for $i = 1$. The induction hypothesis yields that $(I-B)^{i+1} = (I-B)^i(I-B) = C^{i-1}(I-B)(I-B)$. Thus entry (h,j) of $(I-B)^{i+1}$ is equal to

$$\begin{aligned}
&\sum_{k=1}^{m}(\sum_{l=1}^{m}[C^{i-1}]_{h,l}[I-B]_{l,k})[I-B]_{k,j} \\
&= \sum_{k=1}^{m-1}(\sum_{l=1}^{m}[C^{i-1}]_{h,l}[I-B]_{l,k})[I-B]_{k,j} + (\sum_{l=1}^{m}[C^{i-1}]_{h,l}[I-B]_{l,m})[I-B]_{m,j} \\
&= \sum_{k=1}^{m-1}(\sum_{l=1}^{m}[C^{i-1}]_{h,l}[C]_{l,k})[I-B]_{k,j} + (\sum_{l=1}^{m}[C^{i-1}]_{h,l}[C]_{l,m})[I-B]_{m,j} \\
&= [C^i(I-B)]_{h,j}.
\end{aligned}$$

(The next-to-last equality holds since $[I-B]_{l,k} = [C]_{l,k}$ for $k \neq m$, and $[I-B]_{m,j} = 0$). Thus for all $i \geq 1$,

$$(I-B)^i = C^{i-1}(I-B).$$

Hence,

$$\begin{aligned}
\textstyle\sum_{i=0}^{\infty}(I-B)^i &= I + \textstyle\sum_{i=1}^{\infty} C^{i-1}(I-B) \\
&= I + \textstyle\sum_{i=1}^{\infty} C^{i-1}(C+C') \\
&= I + \textstyle\sum_{i=1}^{\infty} C^i + C^{i-1}C' \\
&= \textstyle\sum_{i=0}^{\infty} C^i + \sum_{i=0}^{\infty} C^iC'
\end{aligned}$$

[Va92] L. Valiant, *Why is Boolean complexity theory difficult?* in *Boolean Function Complexity*, edited by M. S. Paterson, London Mathematical Society Lecture Notes Series 169, Cambridge University Press, 1992.

[Vi91] V. Vinay, *Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits*, Proc. 6th IEEE Structure in Complexity Theory Conference (1991) 270–284.

[Wa86] K. Wagner, *The complexity of combinatorial problems with succinct input representation*, Acta Informatica 23 (1986) 325–356.

[Wi87] C. Wilson, *Relativized NC*, Math. Systems Theory 20 (1987) 13–29.

[Wi90] C. B. Wilson, *Decomposing NC and AC*, SIAM J. Comput. 19 (1990) 384–396.

[Za91] V. Zankó, *#P-completeness via many-one reductions*, International Journal of Foundations of Computer Science 2 (1991) 77–82.

[Zu93] D. Zuckerman, personal communication.

8 Appendix

In the proof of Theorem 6, we required the following lemma, which is essentially from [Ju84] (see also [Ju86]).

Lemma 20 *Let matrix B and language S be as in the proof of Theorem 6. Then*

$$x \in L \Leftrightarrow \ \textit{entry } 1,m \textit{ of } (\sum_{i=1}^{\infty}(I-B)^i) \geq 0.$$

Proof. Recall that A is a matrix and p is a polynomial such that

- $x \in S \Rightarrow \sum_{i=0}^{2^{p(n)}}[A^i]_{1,m} > \frac{1}{2} + \frac{1}{2^{p(n)}} \wedge \sum_{i=0}^{2^{p(n)}}[A^i]_{1,m-1} < \frac{1}{2}$.
- $x \notin S \Rightarrow \sum_{i=0}^{2^{p(n)}}[A^i]_{1,m-1} > \frac{1}{2} + \frac{1}{2^{p(n)}} \wedge \sum_{i=0}^{2^{p(n)}}[A^i]_{1,m} < \frac{1}{2}$,

$q(n)$ is a polynomial such that $(1-\frac{1}{2^{q(n)}})^{1+2^{p(n)}} > 1-\frac{1}{2^{p(n)}}$, and B is the matrix $I-(C+C')$, where C' is the all zero matrix, except that entry $m-1,m$ has value $-(1-\frac{1}{2^{q(n)}})$, and $C = (1-\frac{1}{2^{q(n)}})A$. That is, $I-B = C+C'$.

[Ju85] H. Jung, *On probabilistic time and space*, Proc. 12th ICALP, Lecture Notes in Computer Science 194, 1985, pp. 310–317.

[Ju86] H. Jung, *Stochastische Turingmaschinen und die Kompliziertheit arithmetischer Probleme*, doctoral dissertation, Humboldt-Universität, East Berlin.

[LL76] R. Ladner and N. Lynch, *Relativization of questions about log space computability*, Mathematical Systems Theory 10 (1976) 19–32.

[LLS75] R. Ladner, N. Lynch, and A. Selman, *A comparison of polynomial-time reducibilities*, Theoretical Computer Science 1 (1975) 103–123.

[Ni92] N. Nisan, $RL \subseteq SC$, Proc. 24th STOC, 1992, pp. 619–623.

[Og93] M. Ogiwara, $NC^k(NP) = AC^{k-1}(NP)$, manuscript.

[OH91] M. Ogiwara and L. Hemachandra, *A complexity theory for feasible closure properties*, Proc. 6th IEEE Structure in Complexity Theory Conference, 1991, pp. 16–29.

[Ro93] P. Rossmanith, personal communication.

[RST84] W. Ruzzo, J. Simon, and M. Tompa, *Space-bounded hierarchies and probabilistic computation*, J. Comput. and System Sci. 28 (1984) 216–230.

[Si81] J. Simon, *On tape-bounded probabilistic Turing machine acceptors*, Theoretical Computer Science 16 (1981) 158–167.

[To91] S. Toda, *Counting problems computationally equivalent to the determinant*, Technical Report CSIM 91-07, Dept. Comp. Sci. and Inf. Math., Univ. of Electro-Communications, Tokyo, 1991.

[To92] S. Toda, *Classes of arithmetic circuits capturing the complexity of computing the determinant*, IEICE Trans. Inf. and Syst., vol. E75-D (1992) 116–124.

[Tor91] J. Torán, *Complexity classes defined by counting quantifiers*, J. ACM 38 (1991) 753–774.

[Va79] L. Valiant, *The complexity of computing the Permanent*, Theoret. Comput. Sci. 8 (1979) 189–201.

[BH93] A Ben-Dor and S. Halevi, *Zero-one permanent is #P-complete, a simpler proof*, to appear in Proc. 2nd Israel Symposium on Theory of Computing and Systems (ISTCS93), IEEE press.

[BIS90] D. Barrington, N. Immerman, and H. Straubing, *On uniformity within NC^1*, J. Comput. System Sci. 41 (1990) 274–306.

[BRS91] R. Beigel, N. Reingold, and D. Spielman, *PP is closed under intersection*, Proc. 23rd STOC, 1991, pp. 1–9.

[BDHM92] G. Buntrock, C. Damm, U. Hertrampf, and C. Christoph, *Structure and Importance of Logspace MOD-Classes*, Mathematical Systems Theory 25 (1992) 223–237.

[Co85] S. Cook, *A taxonomy of problems with fast parallel algorithms*, Information and Control 64 (1985) 2–22.

[Da91] C. Damm, *$DET = L^{\#L}$?*, Informatik-Preprint 8, Fachbereich Informatik der Humboldt-Universität zu Berlin, 1991.

[FFK91] S. Fenner, L. Fortnow, and S. Kurtz, *Gap-definable counting classes*, Proc. 6th IEEE Structure in Complexity Theory Conference, 1991, pp. 30–42.

[FR91] L. Fortnow and N. Reingold, *PP is closed under truth-table reductions*, Proc. 6th IEEE Structure in Complexity Theory Conference, 1991, pp. 13–15.

[Gi77] J. Gill, *Computational complexity of probabilistic Turing machines*, SIAM J. Comput. 6 (1977) 675–695.

[Gu93] S. Gupta, *The power of witness reduction*, to appear in SIAM J. Comput. A preliminary version appeared in Proc. 6th IEEE Structure in Complexity Theory Conference, 1991, pp. 43–59.

[Je91] B. Jenner, personal communication.

[Ju84] H. Jung, *On probabilistic tape complexity and fast circuits for matrix inversion problems*, Proc. 11th ICALP, Lecture Notes in Computer Science 172, 1984, pp. 281–291.

have recently shown that no "black-box" simulation of PL can yield a bounded-error probabilistic logspace algorithm for PL [Zu93].

- Can anything more be said about the relationship between PLH and $NC^1(PL)$ (or #LH and $NC^1(\#L)$)? Note that for many classes $\mathcal{C}$ of interest (including AC^k, NC^k, NL, L, NP [ABJ91, Og93]), $AC^0(\mathcal{C})$ is equal to $NC^1(\mathcal{C})$.

Acknowledgments. The first author thanks Birgit Jenner for several motivating and informative discussions. Dave Barrington, Michelangelo Grigni, Sanjeev Saluja, and Pierre McKenzie also provided helpful information. We thank Carsten Damm for constructive comments on an earlier draft.

References

[Al90] E. Allender, *Oracles vs Proof techniques that do not relativize*, Proc. SIGAL International Symposium on Algorithms, 1990, Lecture Notes in Computer Science 450, pp. 39–52.

[AJi93] E. Allender and J. Jiao, *Depth reduction for noncommutative arithmetic circuits*, Proc. 25th STOC, 1993.

[ABJ91] C. Àlvarez, J. Balcázar, and B. Jenner, *Adaptive logspace reducibility and parallel time*, to appear in Mathematical Systems Theory. Preliminary version appeared in Proc. 8th STACS, Lecture Notes in Computer Science 480, pp. 422–433.

[AJe93] C. Àlvarez and B. Jenner, *A very hard log-space counting class*, Theoretical Computer Science 107 (1993) 3–30.

[Ba91] J. Balcázar, *Adaptive logspace and depth-bounded reducibilities*, Proc. 6th IEEE Structure in Complexity Theory Conference, 1991, pp. 240–254.

[BCP83] A. Borodin, S. Cook, and N. Pippenger, *Parallel computation for well-endowed rings and space-bounded probabilistic machines*, Information and Control 48 (1983) 113–136.

[BCGR92] S. Buss, S. Cook, A. Gupta, and V. Ramachandran, *An optimal parallel algorithm for formula evaluation*, SIAM J. Comput. 21 (1992) 755–780.

Then the function f defined by

$$\sum_{j=0}^{n^k} \sum_{i=1}^{n^l} (g(h(x,i)) + 2^{|y_i|^{c'}+1}) 2^{jn^c+i}$$

is in #L.

Note that $f(x)$, viewed as a binary string, consists of n^k repetitions of a string containing n^l fields, where each field is of length n^c, consisting of leading zeros, followed by a one, followed by the encoding of $g(y_i)$ for some query y_i that could be asked on input x. If a machine asks the query $f(x)$ at the beginning of its computation, then it can simulate M on input x, moving one block to the right for each step of M that is simulated, and keeping track of which cell of M's oracle tape is being scanned at any particular moment. ∎

7 Conclusion

By making use of recent theorems relating #L and the determinant, we have given simplified proofs of some facts concerning PL, and we have proved new results concerning the classes of sets reducible to PL and to the determinant. A number of open questions remain. Among them:

- Is L^{PL} equal to PL? Note that logspace Turing reducibility is a non-adaptive (i.e., truth-table) reducibility (see [LL76]). Thus L^{PL} is the class of sets logspace truth-table reducible to PL. The proof in [FR91] that PP is closed under truth-table reductions relies on the fact that if f is in GapP, then so is $\sum_{i=0}^{2^{|x|^c}} f(x,i)$; however if this closure property holds for GapL, then #P = P. Thus if L^{PL} is equal to PL, it seems that a very different proof will be needed.

- What closure properties can be established for #L and GapL? In regard to this question, it is appropriate to mention that GapL can be characterized as the class of functions computed by "skew" arithmetic circuits [To92]. Related results regarding arithmetic circuits and certain subclasses of TC^1 may be found in [AJi93].

- Can any relationship be established between PL or #L and AC^1 (or logCFL)?

- Can any any relationship be established between PL (or $C_=L$) and bounded-error probabilistic logspace? Note in this regard that David Zuckerman and Mauricio Karchmer

in logspace from x. Let $g'(x,i) = g(y_i)$, and note that g' is also in $\#\mathrm{LH}_i$, and by induction has $\mathrm{AC}^0_i(h)$ circuits for some $h \in \#\mathrm{L}$. Let $k(0,z) = h(z)$, and $k(1,z) = f'(z)$. Our $\mathrm{AC}^0_{i+1}(k)$ circuits for f consist of subcircuits computing $g(y_i) = k(0,x,i)$, followed by a gate computing $f(x) = k(1,x,g(y_1),\ldots,g(y_{n^k}))$ at the root.

(We remark that, with a little more effort, $\#\mathrm{LH}_i$ functions can be computed by circuits consisting of exactly i #L oracle gates, where the outputs of one gate feed directly into the gate on the next layer.)

The proof of the second inclusion is quite similar to the proof of the forward inclusion in the preceding theorem. ∎

Corollary 18

- $\#\mathrm{LH} = \mathrm{AC}^0(\#\mathrm{L}) = \mathrm{AC}^0(\mathrm{DET})$
- $\mathrm{PLH} = \mathrm{AC}^0(\mathrm{PL})$

(Part 2 of this corollary was previously observed by Carsten Damm and Peter Rossmanith [Je91, Ro93].)

The reader should not be alarmed by the fact that L^{PL} is contained in $\mathrm{AC}^0(\mathrm{PL})$ (and in fact the containment may even be proper), even though AC^0 is properly contained in L; we refer the reader to the discussion in [Wi87, Wi90].

Some of the motivation for this study came from the question of whether or not $\mathrm{L}^{\#\mathrm{L}} = \mathrm{L}^{\mathrm{DET}} = \mathrm{L}^{\mathrm{PL}}$, by analogy to the equalities that are known to hold for the related classes #P and PP. The reader should be able to see that $\mathrm{L}^{\#\mathrm{L}}$ and $\mathrm{L}^{\mathrm{DET}}$ are indeed equal and contain L^{PL}, but we do not see how to compute the low-order or middle bits of a #L function in L^{PL} or even in $\mathrm{NC}^1(\mathrm{PL})$. We close this section with an observation showing that $\mathrm{L}^{\#\mathrm{L}}$ can be defined using very restricted access to the oracle. (For related observations, see [AJe93, Proposition 2 and Section 6].)

Proposition 19 *Let $\mathcal{C}$ be any of the classes* L, NL, PL, or #L. *Then the class $\mathcal{C}^{\#\mathrm{L}}$ remains unchanged even when the oracle Turing machines defining the class are restricted to make at most one query to the oracle, and to read the answer just once from left to right.*

Proof. Let an oracle Turing machine M be given, and let the oracle be the function g. Let the run time of M be n^k, let the possible queries on an input x of length n be contained in the set $\{h(x,1),\ldots,h(x,n^l)\}$ (where h is logspace-computable), and let the number of bits in $g(y)$ be $|y|^{c'}$. Let c be greater than k and c'.

matrix showing, for all configurations of a logspace-bounded machine, the probability of getting from one configuration to another, such that the machine accepts z}.)

The $\mathrm{AC}^0_{i+1}(C)$ circuit accepting A consists of $\mathrm{AC}^0_i(C)$ circuits computing membership of (x,i) in B', followed by a layer of AND and OR gates computing the transition matrix Y of M on input x with oracle answers given by the subcircuits for B', followed by one more oracle gate, checking if (Y,x) is in C.

($\subseteq$) We prove only the induction step ($\mathrm{AC}^0_i(\mathrm{PL}) \subseteq \mathrm{PLH}_i$ implies $\mathrm{AC}^0_{i+1}(\mathrm{PL})$ ($\subseteq$) PLH_{i+1}); the proof for the basis is essentially identical.

Let A be accepted by an $\mathrm{AC}^0_{i+1}(B)$ circuit family $\{C_n\}$ for some B in PL. We describe the behavior of a probabilistic oracle machine M accepting A. On input x, M looks at circuit C_n. If the output gate of C_n is an oracle gate, then M accepts iff y is in B, where $y = y_1 y_2 \ldots y_r$ is the word input to the oracle gate. The subcircuit computing each bit y_i is an $\mathrm{AC}^0_i(B)$ circuit, and by induction hypothesis can be simulated using an oracle from PLH_i.

On the other hand, if the output gate is an AND, OR, or NOT gate, then the output of the circuit can be computed by a constant number of applications of $\leq^{\log}_{\mathrm{ctt}}$ or $\leq^{\log}_{\mathrm{dtt}}$ reductions to a set in PLH_{i+1}. But this also defines a set in PLH_{i+1}, by the closure properties established in the preceding section.

(Alternatively, one may observe that $\mathrm{AC}^0_1(\mathrm{PL}) = \mathrm{PL}$, and that an $\mathrm{AC}^0_i(\mathrm{PL})$ circuit may be viewed as consisting of i layers of $\mathrm{AC}^0_1(\mathrm{PL})$ subcircuits.) ∎

Theorem 17 $\#\mathrm{LH}_i \subseteq \mathrm{AC}^0_i(\#\mathrm{L}) \subseteq \mathrm{L}^{\#\mathrm{LH}_i}$.

(We remark that $\#\mathrm{LH}_i$ is defined as a class of *functions*, while $\mathrm{AC}^0_i(\#\mathrm{L})$ is defined as a class of *languages*. Note however that it is quite natural to view a circuit as computing a function; moreover, it is well-known that the set of functions defined in this way is exactly the same as the set of functions f such that the language $\{(x,i,b) : \text{bit } i \text{ of } f(x) \text{ is } b\}$ is in the associated language class. It follows from the proof below that $\#\mathrm{LH}_i$ is actually equal to the class of functions computed by $\mathrm{AC}^0_i(\#\mathrm{L})$ circuits, with the added restriction that the output gate be an oracle gate.)

Proof. The first inclusion is obvious when $i = 1$; thus assume the induction hypothesis for i and let f be in $\#\mathrm{L}^g$ for some $g \in \#\mathrm{LH}_i$. Thus there is some $f' \in \#\mathrm{L}$ such that $f(x) = f'(x, g(y_1), \ldots, g(y_{n^k}))$, where (as in the proof of the previous theorem) the list of y_i's contains all possible queries that could be asked on input x, and this list can be generated

input x with oracle g. Let #LH *denote* $\bigcup_i$#LH$_i$.

(The PL *Hierarchy) Define* PLH$_1$ *to be* PL*, and let* PLH$_{i+1}$ *be the class of languages A such that, for some logspace-bounded probabilistic oracle Turing machine M, and some language $B \in$ PLH$_i$, A is the language accepted by M with oracle B (where acceptance is defined using the* PL *acceptance criterion). Let* PLH *denote* $\bigcup_i$PLH$_i$.

In both of these definitions, the "Ruzzo-Simon-Tompa" relativization method is used (cf. Section 3).

We will show that PLH and #LH can be defined in terms of AC^0 reductions to PL and #L, respectively. An AC^0 reduction is a uniform family of constant-depth circuits of unbounded-fan-in AND and OR gates, NOT gates, and "oracle" gates. If the oracle is a function $f : \{0,1\}^* \to \{0,1\}^*$, then an oracle gate has some number m of inputs $x_1, \ldots, x_m$ and some number of outputs, representing $f(x_1, \ldots, x_m)$. If the function f does not always take inputs of length m to outputs of the same length, then it may be necessary to assume some sort of "end-of-string" encoding; our theorems do not depend on these details. If the oracle is a language, then the oracle gate computes the characteristic function of the language. Our results do not depend very much on the particular uniformity condition used. Logspace-uniformity is sufficient, although the theorems also hold if more restrictive uniformity conditions are used; see [BIS90, BCGR92] for discussions of uniformity issues involved in low-level circuit complexity.

It will turn out to be useful to consider certain refinements of AC^0 reducibility. Following [ABJ91] (see also [Ba91]), define AC$^0_i(f)$ to be the class of languages accepted by AC^0 circuits with oracle gates for f, where no path from input to output goes through more than i oracle gates. If $\mathcal{C}$ is a class of functions (languages), then AC$^0_i(\mathcal{C})$ is equal to the union over all (characteristic) functions f in $\mathcal{C}$ of AC$^0_i(f)$.

Theorem 16 *For all i,* AC^0_i(PL) = PLH$_i$.

Proof. ($\supseteq$) Any set $A \in$ PL = PLH$_1$ can be accepted with a single oracle gate. Thus assume that PLH$_i \subseteq$ AC^0_i(PL), and let A be the language accepted by M^B for some B in PLH$_i$ and some probabilistic logspace-bounded oracle Turing machine M. Since M makes queries using the Ruzzo-Simon-Tompa restriction, there is a list $y_1, \ldots, y_{n^k}$ computable in logspace from x such that all queries of M on input x come from the set $\{y_1, \ldots, y_{n^k}\}$. The set $B' = \{(x,i) : y_i \in B\}$ is also in PLH$_i \subseteq$ AC^0_i(PL). (Without loss of generality, $B' \in$ AC$^0_i(C)$, where C is the "canonical complete set" for PL: $C = \{(Y,z) : Y$ is a transition

6 Reductions to #L and PL

Corollary 10 raises the obvious question of whether the low-order or middle bits of a #L function can be computed using the power of PL. At present, we see no reason to believe that this is possible; it seems plausible that $\oplus$L (i.e., determining the low-order bit of a #L function) is not NC^1-reducible to PL. Any attempt to investigate this question must first make precise what it should mean to try to compute something "using the power of PL."

It is a pleasing fact of complexity theory that most of the "natural" complexity classes can be defined as the class of problems "reducible" to some important problem, where the definition does *not* depend on the particular notion of reduction that is used. For example, nondeterministic logspace can be defined as the class of problems reducible to transitive closure (or $s-t$-connectivity) using any of the notions of reducibility that have been considered (e.g., $\leq_m^{\log}$, AC^0, NC^1, first-order projections, etc.).

However, the class of problems reducible to the determinant and to PL seem to be exceptions to this rule. As an extreme example, consider the class of functions that are logspace many-one reducible to the determinant; by Theorem 1 this is GapL. The zero-one functions (i.e., languages) in this class are determined by logspace-bounded nondeterministic Turing machines, where the number of accepting and rejecting computations differ by either zero or one; there seems to be no reason to believe that all of nondeterministic logspace is contained in that class. On the other hand, it is obvious that nondeterministic logspace can be reduced to the determinant if less restrictive reductions are used (since all that is required is to check if a #L function is non-zero).

When Cook [Co85] considered the class of problems reducible to the determinant, he framed his definition using NC^1 reducibility. Alternatively, one could consider the class of things AC^0-reducible to the determinant; we show that this class corresponds to a logspace-analog of the counting hierarchy. (We do not know if this class is equal to the class considered by Cook.)

The counting hierarchy (see [Wa86, Tor91]) consists of sets in the classes PP, $\mathrm{PP}^{\mathrm{PP}}$, $\mathrm{PP}^{\mathrm{PP}^{\mathrm{PP}}}$, etc. One obtains a computationally-equivalent class of functions if one considers #P, $\#\mathrm{P}^{\#\mathrm{P}}$, etc. Let us now consider the analogous classes defined in terms of #L and PL.

Definition 2 *(The #L Hierarchy) Define* $\#\mathrm{LH}_1$ *to be* #L*, and let* $\#\mathrm{LH}_{i+1}$ *be the class of functions* f *such that, for some logspace-bounded nondeterministic oracle Turing machine* M*, and some function* $g \in \#\mathrm{LH}_i$*,* $f(x)$ *is the number of accepting computations of* M *on*

Proof. Let $A \in \mathrm{C_=L}$, and let $B \leq^{\log}_{\mathrm{dtt}} A$ via reduction f (so $x \in B$ iff there is an $i \leq n^k$ such that $f(x,i) \in A$. Let g be the GapL function defining A. Then $x \in B$ iff $\prod_{i=1}^{n^k} g(x,i) = 0$. Theorem 8 now shows that $B \in \mathrm{C_=L}$.

Similarly, if $B \leq^{\log}_{\mathrm{ctt}} A$ via reduction f, then $x \in B$ iff $\sum_{i=1}^{n^k} g(x,i)^2 = 0$. ∎

It remains unknown if $\mathrm{C_=L}$ is closed under complement.

Closure of $\mathrm{C_=L}$ under $\leq^{\log}_{\mathrm{dtt}}$ reductions is also sufficient to show that $\mathrm{C_=L}$ contains the class LogFew that was defined and studied in [BDHM92]. (We refer the reader to [BDHM92] for the definition of this class.)

Theorem 14 $\mathrm{LogFew} \subseteq \mathrm{C_=L}$.

Proof. The definition of LogFew makes it clear that if $A \in \mathrm{LogFew}$, then there is a logspace-computable function f and a #L function g such that $x \in A$ iff $\exists i \leq |x|^c \;\; g(x) = f(x,i)$. Clearly, then, A is $\leq^{\log}_{\mathrm{dtt}}$ reducible to a set in $\mathrm{C_=L}$. ∎

We have one more result that makes mention of $\mathrm{C_=L}$. The motivation for this result came not so much from any question about $\mathrm{C_=L}$ itself, but rather from a question about the relationship between #L and GapL. As these classes are defined, it is obvious that #L is properly contained in GapL, because GapL contains negatively-valued functions. However, if we choose any natural binary representation of GapL and #L functions (such as sign-magnitude or two's complement, etc.), it is natural to ask if GapL, viewed as a set of functions from Σ^* to Σ^*, contains any functions that are not in #L.

Theorem 15 *If every function $f : \Sigma^* \to \Sigma^*$ in GapL is also in #L, then $C_=L = NL$.*

Proof. Let $A \in \mathrm{C_=L}$, and let g be the GapL function that defines A. Let $g' = -g^2$. That is, $x \in A \Longrightarrow g'(x) = 0$, and $x \notin A \Longrightarrow g'(x) < 0$.

Let $f : \Sigma^* \to \mathbf{N}$ be the function defined on the natural numbers so that $f(x)$ is the natural number whose binary representation is given by the representation of $g'(x)$. (All that we assume about the the representation chosen for g' is that zero be represented as a string of zeros.) Then it follows that $x \in A \Longrightarrow f(x) = 0$, and $x \notin A \Longrightarrow f(x) > 0$. If $f \in \#\mathrm{L}$, then $A \in \mathrm{NL}$. ∎

Definition 1 *$C_=L$ is the class of languages A for which there is a function $g \in GapL$ such that $x \in A$ iff $g(x) = 0$.*

As is the case with C$_=$P, there are several equivalent ways of defining C$_=$L.

Proposition 11 *The following are equivalent:*

1. *$A \in C_=L$.*
2. *There is a function $f \in FL$ and a function $g \in GapL$ such that $x \in A$ iff $f(x) = g(x)$.*
3. *There is a function $f \in FL$ and a function $g \in \#L$ such that $x \in A$ iff $f(x) = g(x)$.*

Proof. ((1) $\Longrightarrow$ (2)) and ((3) $\Longrightarrow$ (2)) are immediate from the definitions.

For ((2) $\Longrightarrow$ (3)), let f and g be the functions in FL and GapL, respectively, defining language A. By Proposition 2, there are functions $f_1 \in$ FL and $f_2 \in \#$L such that $g(x) = f_2(x) - f_1(x)$. Thus $g' = f_2 + f_1$ is a function in #L and $f' = f_1 + f$ is a function in FL such that $x \in A$ iff $g'(x) = f'(x)$.

For ((2) $\Longrightarrow$ (1)), let f and g be as above, and note that $g - f$ is in GapL, and $x \in A$ iff $g(x) - f(x) = 0$. ∎

The proof of Proposition 4 shows that C$_=$L can also be characterized by probabilistic polynomial-time logspace-bounded machines where the probability of accepting and of rejecting are both exactly $\frac{1}{2}$.

Theorem 12 *The set of all singular integer matrices is complete for $C_=L$ under $\leq_m^{\log}$ reductions.*

Proof. The proof is immediate from Theorem 1. ∎

More generally, the set $\{(A, r) :$ the determinant of matrix A is $r\}$ is complete for C$_=$L, just as the set $\{(A, r) :$ the determinant of matrix A is $\geq r\}$ is complete for PL.

Note that NL is contained in C$_=$L. (This is because NL is closed under complement, and membership in a coNL set is equivalent to having zero accepting computations.)

Proposition 13 *$C_=L$ is closed under $\leq_{\rm dtt}^{\log}$ and $\leq_{\rm ctt}^{\log}$ reductions. (In particular, it is closed under union and intersection.)*

Proof. We present the proof for $\leq^{\log}_{\rm ctt}$ reductions. The proof of the other claim is analogous. Let $C \leq^{\log}_{\rm ctt} B$ via a reduction g, so that $x \in C$ iff $\forall i \leq n^c \;\; g(x,i) \in B$. Let h be the GapL function such that $h(y) > 0$ if $y \in B$, and $h(y) < 0$ otherwise. Let $H(x,i)$ denote $h(g(x,i))$.

The definition of the following sequence of polynomials follows the presentation in Section 2 of [BRS91]. Define

$$\begin{aligned}
P^+(x,i) &= [(H(x,i)-1)\textstyle\prod_{j=1}^{n^k}(H(x,i)-2^j)^2]^{2^{\lceil c\log n\rceil+1}} \\
P^-(x,i) &= [(-H(x,i)-1)\textstyle\prod_{j=1}^{n^k}(-H(x,i)-2^j)^2]^{2^{\lceil c\log n\rceil+1}} \\
N(x,i) &= P^-(x,i) - P^+(x,i) \\
D(x,i) &= P^-(x,i) + P^+(x,i) \\
S(x,i) &= \tfrac{N(x,i)}{D(x,i)} \\
A(x) &= (\textstyle\sum_{i=1}^{n^c} S(x,i)) - (n^c-1) \\
A'(x) &= (\textstyle\prod_{i=1}^{n^c}(D(x,i)))(\sum_{i=1}^{n^c}(N(x,i)\prod_{l\neq i} D(x,l))) - (\prod_{i=1}^{n^c}(D(x,i)))^2(n^c-1)
\end{aligned}$$

$S(x,i)$ is equivalent to the function that is called $S^{(n^c)}_{n^k}(H(x,i))$ in [BRS91]; it is proved there that $A(x)$ is positive if all of the $H(x,i)$ are positive, and $A(x)$ is negative otherwise. Observe that $A'(x)$ is positive if and only if $A(x)$ is, and note also that A' may be seen to be in GapL because of the closure properties established above. This shows that $C \in$ PL. ∎

Corollary 10 *Language A is in* PL *if and only if there is a logspace-computable function $b(x) = O(\log|x|)$ and a* GapL *function f such that [$x \in A$ if and only if the high-order $b(x)$-th bit of $f(x)$ is 1].*

Proof. The forward direction is obvious from the foregoing, with $b(x) = 1$.

For the converse, note that the language $B = \{(x,y) : y \leq f(x)\}$ is in PL (since $(x,y) \in B$ iff the GapL function $f(x) - y \geq 0$). Thus the language $C = \{(z,x,y) : z \leq f(x) \leq y\}$ is also in PL, by Corollary 9. Let $u_1, u_2, \ldots, u_r$ be the $2^{b(x)-1}$ strings of length $(b(x)-1)$, and note that x is in A iff $\bigvee_i u_i 10^{n^k - b(x)} \leq f(x) \leq u_i 11^{n^k - b(x)}$. By corollary 9, A is in PL. ∎

5 Exact Counting in Logspace

In this section, we introduce the class C$_=$L as the logspace-analog of the class C$_=$P. We do this in order to characterize the complexity of the class of singular matrices, which is arguably a much more natural problem than the complete sets for PL that have been presented above. The set of integer matrices with determinant zero is a natural complete set for C$_=$L.

First, we need to present some definitions.

4 Closure Properties of GapL and PL

One way of interpreting the results of the previous section is that PL is the class of languages that are reducible to the high-order bit of a #L function. In this section, we will improve this, to show that PL is the class of languages that are reducible to any of the high-order $O(\log n)$ bits of a #L function. Along the way, we will establish some closure properties of PL and of GapL.

The following theorem and its proof are logspace-analogues of results concerning GapP that were proved in [FFK91].

Theorem 8 *Let f be any function in* GapL.

1. *Let g be a function in* FL. *Then $f(g(\cdot))$ is in* GapL.
2. $\sum_{i=0}^{|x|^c} f(x,i)$ *is in* GapL.
3. $\prod_{i=0}^{|x|^c} f(x,i)$ *is in* GapL.
4. *Let g be a function in* FL *such that $g(x) = O(1)$. Then $\binom{f(x)}{g(x)}$ is in* GapL.

Proof. The proofs of the first three closure properties may be taken essentially word-for-word from [FFK91].

For the fourth closure property, observe, as in [FFK91] that if f is the difference of two #L functions h and h', then

$$\binom{f(x)}{g(x)} = \sum_{i=0}^{g(x)} (-1)^i \binom{h(x)+i}{i} \binom{h'(x)+1}{g(x)-i}.$$

The result now follows from the first three closure properties and from [BDHM92, Lemma 2], where it is shown that if a is in #L and b is in FL with $b(x) = O(1)$, then $\binom{a(x)}{b(x)}$ is in GapL. ∎

A *logspace conjunctive truth-table reduction* of one set A to another set B (denoted $A \leq_{\mathrm{ctt}}^{\log} B$) is a logspace-computable function $f(x) = y_1, \ldots, y_r$ for some r such that x is in A if and only if *all* of the y_i are in B. Logspace disjunctive truth-table reductions ($\leq_{\mathrm{dtt}}^{\log}$) are defined similarly, with "all" replaced by "at least one." For more formal definitions, see [LLS75].

Corollary 9 PL *is closed under $\leq_{\mathrm{ctt}}^{\log}$ and $\leq_{\mathrm{dtt}}^{\log}$ reductions. (In particular,* PL *is closed under intersection and union.)*

We provide a complete proof of this fact in the Appendix.[3]

Now note that

$$\begin{aligned} x \in L &\Leftrightarrow [(\textstyle\sum_{i=1}^{\infty}(I-B)^i)]_{1,m} \geq 0 \\ &\Leftrightarrow [B^{-1}]_{1,m} \geq 0 \\ &\Leftrightarrow [D^{-1}]_{1,m} \geq 0 \\ &\Leftrightarrow \mathrm{DET}(D')/\mathrm{DET}(D) \geq 0 \\ &\Leftrightarrow \mathrm{DET}(D')\mathrm{DET}(D) \geq 0 \\ &\Leftrightarrow \mathrm{DET}(D'' \times D) \geq 0 \end{aligned}$$

where D' is the $(1,m)$ minor of D, and D'' is the matrix with 1 in the (1,1) position, 0 in all other positions in the first row and column, and D' in the lower left $(m-1) \times (m-1)$ submatrix.

Note that $D'' \times D$ can be constructed in logspace from A (and hence from x). The theorem now follows immediately from Corollary 5. ∎

The proof given above makes it clear that the result "PL = PL(poly)" *relativizes* using the appropriate notion of "relativized PL." (This was not so clear from the proof in [Ju85].) We will need this fact in later sections. First, however, we must define what is meant by "relativized PL."

The question of what is an appropriate (or even meaningful) way to provide space-bounded machines with an oracle has been the subject of some debate. For a discussion of some of the issues involved and a list of references, see [Al90]. It turns out that a simple and useful notion of relativization is the so-called Ruzzo-Simon-Tompa relativization [RST84]; briefly, using this notion of relativization, a set is in PL^A if there is a probabilistic logspace machine M with an oracle tape and query states (as is usual in the definition of oracle Turing machines) along with the restriction that the machine act *deterministically* when it is writing on its oracle tape. Note that this forces the property that each query that can be asked during a computation on input x is described completely by x and by M's configuration when the query starts to be written. In particular, only a polynomial number of queries can possibly be asked over all of M's computations on x.

Corollary 7 *For any set S,* $\mathrm{PL}^S = \mathrm{PL(poly)}^S$.

Proof. The only modification that needs to be made to the proof of Theorem 6 is that the matrix A needs to record the transition matrix of machine M on input x with oracle S. This can clearly be computed in logspace, relative to oracle S. ∎

[3]The argument presented thus far (along with the Appendix) is closely patterned after an argument in [Ju84]. (The paper [Ju84] presents a complete set for PL; the PL=PL(poly) theorem was not presented until [Ju85].)

3 A simple proof of Jung's Theorem

Theorem 6 PL = PL(poly).

Proof. We will use the fact that PL is closed under complement; an easy proof may be found in [RST84]. We will also use the fact that this proof (similar to a result in [Gi77]) shows that for any set S in PL, there is a probabilistic logspace-bounded Turing machine M and a polynomial p such that, for any string x, if x is in S, then the probability that M reaches the unique accepting configuration of M in time $2^{p(|x|)}$ is at least $\frac{1}{2} + \frac{1}{2^{p(|x|)}}$, and if x is not in S, then the probability that M reaches the unique rejecting configuration of M in time $2^{p(|x|)}$ is at least $\frac{1}{2} + \frac{1}{2^{p(|x|)}}$.

Given such a machine M, we will show how a PL(poly) machine M' can be constructed, accepting S.

Given input x of length n, the first step is to build an $m \times m$ matrix A such that

- $x \in L \Rightarrow \sum_{i=0}^{2^{p(n)}} [A^i]_{1,m} > \frac{1}{2} + \frac{1}{2^{p(n)}} \wedge \sum_{i=0}^{2^{p(n)}} [A^i]_{1,m-1} < \frac{1}{2}$.
- $x \notin L \Rightarrow \sum_{i=0}^{2^{p(n)}} [A^i]_{1,m-1} > \frac{1}{2} + \frac{1}{2^{p(n)}} \wedge \sum_{i=0}^{2^{p(n)}} [A^i]_{1,m} < \frac{1}{2}$.

(In this expression, the notation $[D]_{i,j}$ denotes the (i,j)-th entry of matrix D, and A^i denotes the ith power of matrix A under usual matrix multiplication.)

This matrix A is just the transition matrix of M on input x, with one row and column for each of the polynomially-many configurations of M, where m is the accept configuration, $m-1$ is the reject configuration, and all entries are 0, 1 or $\frac{1}{2}$, recording the probability of getting from one configuration to another in one step. (For the conditions above to hold, note that m and $m-1$ must have outdegree zero; i.e., M enters *no* state after halting.)

Now let $q(n)$ be a polynomial sufficiently greater than $p(n)$ so that $(1 - \frac{1}{2^{q(n)}})^{1+2^{p(n)}} > 1 - \frac{1}{2^{p(n)}}$.

Let B be the matrix $I - ((1 - \frac{1}{2^{q(n)}})A + C')$, where C' is the all zero matrix, except that entry $m-1, m$ has value $-(1 - \frac{1}{2^{q(n)}})$, and I denotes the identity matrix. Note that B can be computed in logspace from A.

Let $D = 2^{q(n)+1}B$. Note that D is an integer matrix.

Intuitively, $(1 - \frac{1}{2^{q(n)}})A + C'$ may be thought of as subtracting Prob[M rejects] from Prob[M accepts]. Thus it is not too surprising that one can show that

$$x \in L \Leftrightarrow \text{ entry } 1, m \text{ of } (\sum_{i=1}^{\infty}(I - B)^i) \geq 0.$$

Proposition 4 *The following are equivalent:*

1. $A \in$ PL(poly).
2. $\exists f \in$ #L *such that* $x \in A$ *iff the high order bit of* $f(x)$ *is 1.*
3. $\exists f \in$ GapL *such that* $x \in A$ *iff* $f(x) \geq 0$.

Proof. (1 implies 2): Let M be the probabilistic logspace machine accepting L in polynomial time; thus M halts on all inputs. Without loss of generality, M flips a coin on each step, so the total number of computations is a power of two. Input x is accepted iff at least half of these computations accept, which happens iff the high-order bit of the #L function counting the number of accepting computations of M on input x is one.[2]

(2 implies 3): #L is contained in GapL by Proposition 2.

(3 implies 1): Let f be a GapL function such that $x \in L$ iff $f(x) \geq 0$. By Proposition 2 there is a FL function g and a #L function h such that $f(x) = g(x) - h(x)$. Let $p(|x|)$ be greater than the running time of the #L machine defining h (call this machine M) and greater than the number of bits in $g(x)$. Now let M' be a Turing machine that flips a coin and, if it is heads, flips $p(|x|)$ coins and accepts if the sequence obtained is one of the first $g(x)$ strings in lexicographic order. (This can be done since FL $\subseteq$ #L.) If, on the other hand, the first coin flipped is tails, then M' flips $p(|x|)$ coins, simulating M (using coin flips to simulate the nondeterministic moves of M), and M' accepts iff the path simulated on M rejects *and* all of the "unused" remaining coin flips (out of the original $p(|x|)$) are heads.

It is easy to verify that, out of the $2^{p(|x|)+1}$ probabilistic sequences, exactly $g(x) + (2^{p(|x|)} - h(x))$ are accepting. This number is less than half iff $f(x) < 0$. ∎

Corollary 5 *Nonneg.DET* $\in$ PL(poly)*, where Nonneg.DET is the set of all integer matrices with determinant* ≥ 0.

Proof. Immediate from Theorem 1 and Proposition 4. ∎

It will follow from the proof of Theorem 6 in the next section that Nonneg.DET is in fact complete for PL under $\leq_m^{\log}$ reductions.

[2] There is some need to be careful here. We have defined a #L function to be a function mapping Σ^* to the naturals; however, it is convenient, for this proposition and elsewhere, to assume that the #L function is written in binary. Clearly, if leading zeros are not written, then it is pointless to talk about the "high-order bit" of a #L function. Thus we assume that there is some constant k such that a #L function is always represented in binary, using exactly n^k bits. One could devise other conventions, but they would not affect the theorems in any interesting way. GapL functions will be encoded similarly, where the high-order bit records the sign.

gardless of the notion of reducibility that is used. For instance, NL is the class of languages reducible to s-t-connectivity under logspace many-one or Turing reductions, or under 1-L reductions or quantifier-free projections or NC^1 or AC^0 reductions or under any of the many other low-level reductions that have been studied in the literature. However, DET does not seem to have this property. In Section 6 we present characterizations of the classes reducible to PL and #L under various notions of reducibility. For example, $AC^0(PL)$ is equal to the hierarchy $PL^{PL^{\cdot^{\cdot^{PL}}}}$.

2 Basic Facts about GapL

The following definitions are adapted from [FFK91]. Given a nondeterministic Turing machine M that halts on all computation paths on all inputs, let $\mathrm{gap}_M(x)$ be [number of accepting paths of M on input x] − [number of rejecting paths of M on input x]. Let GapL be $\{\mathrm{gap}_M : M \text{ is a nondeterministic logspace-bounded Turing machine}\}$. Let FL denote the class of functions computed in (deterministic) logspace.

Given function classes $\mathcal{C}$ and $\mathcal{D}$, let $\mathcal{C} - \mathcal{D}$ be the class of functions $\{f - g : f \in \mathcal{C} \text{ and } g \in \mathcal{D}\}$.

Proposition 2 GapL = #L − #L = #L − FL = FL − #L.

The proof of this proposition is almost word-for-word the same as the proof of Proposition 3.5 in [FFK91]. The only observation that is required in order to translate the proof of [FFK91] into this setting is that every function in FL is in #L. Although this fact is implicit in [AJe93], we make it explicit here.

Proposition 3 *FL ⊆ #L*

Proof. Let f be any function in FL, $f : \Sigma^* \to \mathbf{N}$, and assume that the output of f is written in binary. If $m = |f(x)|$, let us number the bit positions of $f(x)$ so that $f(x) = y_{m-1}y_{m-2}\ldots y_2y_1y_0$. Consider a nondeterministic machine N that, on input x, computes $m = |f(x)|$, nondeterministically chooses i such that $0 \le i \le m-1$, rejects if $y_i = 0$, and otherwise forms 2^i accepting paths. Clearly $f(x)$ is the number of accepting paths of N on input x, and N uses space $\log n$. ∎

Let PL(poly) denote the class of sets accepted by PL machines with the restriction that the machines run in polynomial time. In the next section, we will show that this class is equal to PL.

reaches an accepting configuration is greater than one half. Although the definition of PL is straightforward, it turns out that the complexity of PL is rather difficult to analyze, in part because probabilistic logspace machines can perform useful work after exponentially many computation steps. An easy way to see this is to note that the s-t connectivity problem (a standard NL-complete set) can be accepted with *zero error* by a PL machine that follows a randomly-chosen path from vertex s, accepting if vertex t is reached, and otherwise trying another randomly-chosen path, and so on; if a path exists, it will eventually be found (with probability one).

Gill showed in [Gi77] that PL is contained in PSPACE. In [Si81], this was improved to DSPACE($\log^6 n$), but it was not until the appearance of [BCP83] that it was even known that PL is contained in P; [BCP83] shows that PL is contained in NC^2, and this can be improved slightly to TC^1 (the class computed by logarithmic-depth threshold circuits). The source of this difficulty was the fact, already alluded to, that probabilistic logspace machines cannot obviously be restricted to run in polynomial time without loss of computational power. However, Jung showed in [Ju85] that, at least in the *unbounded error* model (which defines the class PL), the polynomial-time restriction causes no loss of power. The proof presented in [Ju85] is complicated; we present an easy proof in Section 3.

Note that it would be remarkable if an analogous theorem could also be proved in the *bounded error* case. We have already seen that NL can be accepted with bounded (in fact zero) error; thus this would in some sense provide a non-uniform version of L=NL (i.e., L/poly = NL/poly). Furthermore, Nisan [Ni92] has shown that bounded-error, polynomial-time logspace can be simulated in polynomial time and space $\log^2 n$; hence extending Jung's theorem to bounded error would provide a small-space polynomial-time algorithm for transitive closure. All of these consequences would be surprising.

Let DET denote the determinant function. (Do not confuse this with the definition of [Co85], where DET is used to denote the class of functions NC^1-reducible to the determinant.) Theorem 1 allows one to show that $\mathrm{L}^{\mathrm{DET}} = \mathrm{L}^{\#\mathrm{L}}$, as well as $\mathrm{AC}^0(\mathrm{DET}) = \mathrm{AC}^0(\#\mathrm{L})$ and $\mathrm{NC}^1(\mathrm{DET}) = \mathrm{NC}^1(\#\mathrm{L})$, etc. However, no logspace-analog of the theorem $\mathrm{P}^{\mathrm{PP}} = \mathrm{P}^{\#\mathrm{P}}$ is known, and we suspect that no such analog exists. For example, although we show that any of the high-order $O(\log n)$ bits of a #L function can be computed in L^{PL}, we know of no reason to suspect that the middle or low-order bit of a #L function can be computed in this way.

For most natural problems A, the class of things reducible to A remains the same re-

1 Introduction

One of the most important and influential early results of complexity theory is the theorem of [Va79] showing that the complexity of computing the permanent of an integer matrix is characterized by the complexity class #P of functions that count the number of accepting computation paths of a nondeterministic polynomial-time machine. It is perhaps surprising that well over a decade passed before it was discovered that an equally-close connection exists between the complexity of computing the determinant of a matrix and the class #L (defined in [AJe93]) of functions that count the number of accepting computation paths of a nondeterministic logspace-bounded machine. In order to state this connection more precisely, let us define GapL to be $\{f : f(x) = g(x) - h(x)$ for some g and h in #L$\}$. (This definition is by analogy to the class GapP, consisting of the difference of #P functions, which is defined and studied in [FFK91, OH91, Gu93].)

Although stated in different ways, the results of [Vi91, Theorem 6.5], [To91, Theorem 2.1], [Da91], and [Va92, Theorem 2] show the following fact:

Theorem 1 *[To91, Da91, Vi91, Va92] A function f is in* GapL *iff f is logspace many-one reducible to the determinant.*

(A function f is logspace many-one reducible to the determinant if there is a function g computable in logspace such that $f(x)$ (viewed as a number written in binary) is equal to the determinant of matrix $g(x)$.)[1] The proof given in [To91] is particularly clear and direct. We remark that the logspace many-one reductions presented in, for example, the proof of [To91], can in fact be computed by uniform AC^0 circuits; we will use this fact later.

In this paper we use Theorem 1 to give a very simple proof of a theorem of Jung [Ju85], concerning the complexity class PL. PL is defined to be the class of languages A for which there exists a probabilistic Turing machine (in the sense of [Gi77]; that is, a Turing machine with access to a source of unbiased random bits), such that on input x the machine never uses more than $\log |x|$ space, and $x \in A$ if and only if the probability that the machine

[1]This definition of "functional many-one reducibility" is from [AJe93]. It should be noted that the notion of one function being "many-one reducible" to another is sometimes defined in a much less restrictive way. For example, it is shown in [Za91, BH93] that the permanent of zero-one matrices is "many-one complete" for #P, using a less restrictive version of "many-one reductions." On the other hand, it follows from [Va79] that the permanent of integer matrices cannot be complete for #P or GapP using our definition of "many-one reduction" unless P = $\oplus$P (since the permanent and the determinant are equal mod 2). That is, the relationship between the determinant and #L is even *closer* than the relationship that is known to exist between the permanent and #P.

ABSTRACT

Recent results by Toda, Vinay, Damm, and Valiant have shown that the complexity of the determinant is characterized by the complexity of counting the number of accepting computations of a nondeterministic logspace-bounded machine. (This class of functions is known as #L.) Using that characterization, we give a very simple proof of a theorem of Jung, showing that probabilistic logspace-bounded (PL) machines lose none of their computational power if they are restricted to run in polynomial time.

We also present new results comparing and contrasting the classes of functions reducible to PL, #L, and the determinant, using various notions of reducibility.

DIMACS Technical Report 93-43
July 1993

Relationships Among PL, #L, and the Determinant

by

Eric Allender[1,2]
Department of Computer Science
Rutgers University
New Brunswick, NJ 08903

Mitsunori Ogiwara[3]
Department of Computer Science
University of Electro-Communications
Chofu-shi, Tokyo 182, JAPAN

[1]Permanent Member
[2]Supported in part by NSF grant CCR-9204874. This work was done while on sabbatical at Princeton University.
[3]Supported in part by the NSF under grant CCR-9002292. Work done in part while visiting SUNY-Buffalo.

DIMACS is a cooperative project of Rutgers University, Princeton University, AT&T Bell Laboratories and Bellcore.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.