An Upward Measure Separation Theorem*

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA 50011

Abstract

It is shown that almost every language in ESPACE is very hard to approximate with circuits. It follows that $\mathrm{P} \neq \mathrm{BPP}$ implies that E is a measure 0 subset of ESPACE.

1 Introduction

Hartmanis and Yesha [HY84] proved that P is a proper subset of P/Poly $\cap$ PSPACE if and only if E is a proper subset of ESPACE. (See section 2 for notation and terminology used in this introduction.) This refined the *downward separation* result

$$\mathrm{E} \subsetneqq \mathrm{ESPACE} \Longrightarrow \mathrm{P} \subsetneqq \mathrm{PSPACE}$$

of Book [Boo74] and also led immediately to the *upward separation* result

$$\mathrm{P} \subsetneqq \mathrm{BPP} \Longrightarrow \mathrm{E} \subsetneqq \mathrm{ESPACE} \tag{1.1}$$

of Hartmanis and Yesha [HY84]. (Work of Gill [Gil77], Adleman [Adl78], and Bennett and Gill [BG81] had already established that BPP is contained in P/Poly $\cap$ PSPACE.)

It is reasonable to conjecture that BPP is in fact a *proper* subset of P/Poly $\cap$ PSPACE, and hence that the $\mathrm{P} \subsetneqq \mathrm{BPP}$ hypothesis might yield a stronger conclusion than the separation of E from ESPACE. This paper supports this intuition by proving the following.

Main Theorem. If $\mathrm{P} \subsetneqq \mathrm{BPP}$, then $\mu(\mathrm{E} \mid \mathrm{ESPACE}) = 0$.

The conclusion here states that E is a *measure 0*, i.e., negligibly small, subset of ESPACE in the resource-bounded measure theory of Lutz [Lut89, Lut90]. (This theory, which has the *classical* and *effective* Lebesgue measure theories (cf. Halmos [Hal50], Freidzon [Fre72], Mehlhorn [Meh74]) as special cases,

*This work was supported in part by NSF Grant CCR-8809238.

describes the internal measure-theoretic structure of ESPACE and other complexity classes.) Thus the Main Theorem is an *upward measure separation* result which extends (1.1) by asserting that *any* separation of P from BPP implies a *measure separation* of E from ESPACE.

The proof of the Main Theorem makes essential use of two recent results, presented as Theorems 1 and 2 below. Theorem 1, from Nisan and Wigderson [NW88, NW89], states that P = BPP if E contains any problem "with hardness $2^{\alpha n}$ for some $\alpha > 0$." Theorem 2, from Lutz [Lut89], states that almost every problem in ESPACE has "high selective space-bounded program-size complexity" almost everywhere. Precise statements of these theorems, together with necessary definitions, are given in section 3. The proofs of Theorems 1 and 2, which involve pseudorandom bit generators and resource-bounded measure theory, respectively, are not repeated here. In fact, Theorem 2 captures all the resource-bounded measure theory needed for the Main Theorem, so no measure theory is used in this paper. Details of resource-bounded measure theory may be found in Lutz [Lut89, Lut90], but such details are not needed to follow the argument of this paper.

In section 4, Theorem 2 is used to prove Theorem 3, which states that almost every problem in ESPACE "has hardness greater than $2^{\alpha n}$ for every $0 < \alpha < \frac{1}{3}$," i.e., is very hard to approximate with circuits. The Main Theorem follows immediately from Theorems 1 and 3.

2 Preliminaries

All results in this paper are robust with respect to reasonable choices of the underlying model of computation. Our *machines* can thus be interpreted as Turing machines, pointer machines, random access machines, etc.

All *languages* here are sets $L \subseteq \{0,1\}^*$. We write $L_{=n}$ for $L \cap \{0,1\}^n$. The *characteristic string* of $L_{=n}$ is the 2^n-bit string $\chi_{L_{=n}}$ whose i^{th} bit is 1 iff $w_i \in L$, where w_i is the i^{th} string in the lexicographic enumeration of $\{0,1\}^n$. We write $|x|$ for the *length* of a string $x \in \{0,1\}^*$.

The *symmetric difference* of sets A and B is denoted by $A \triangle B = (A \setminus B) \cup (B \setminus A)$. The *cardinality* of a finite set A is denoted by $|A|$.

Our *circuits* are Boolean, combinational (acyclic) circuits with bounded fan-in, unbounded fan-out, and a single output gate. An n-input circuit γ *computes* the set $L(\gamma)$ of all strings $w \in \{0,1\}^n$ for which $\gamma(w)$, the Boolean value of the output gate on input w, is 1. The *size* of a circuit γ, written size(γ), is the number of gates in γ. The *circuit-size complexity* of a language L is the function $\mathrm{CS}_L : \mathbf{N} \to \mathbf{N}$ defined by

$$\mathrm{CS}_L(n) = \min\{\mathrm{size}(\gamma) \mid L(\gamma) = L_{=n}\}.$$

Further details (which are standard and can be varied in minor ways) may be found in Balcázar, Diáz, and Gabarró [BDG88], Lutz [Lut89], or any standard reference on circuit complexity.

We are interested in the polynomial complexity classes P and PSPACE, the exponential complexity classes E = DTIME(2^{linear}) and ESPACE = DSPACE(2^{linear}), the bounded-error probabilistic time complexity class BPP defined by Gill [Gil77], and the nonuniform complexity class

$$\mathrm{P/Poly} = \{L \mid \mathrm{CS}_L(n) = n^{O(1)}\},$$

consisting of all languages which have polynomial-size circuits.

A property $\varphi(n)$ of natural numbers n holds *infinitely often* (*i.o.*) if it holds for infinitely many $n \in \mathbf{N}$, and *almost everywhere* (*a.e.*) if it holds for all but finitely many $n \in \mathbf{N}$.

In section 4 we use (a special case of) the Chernoff [Che52] bound which can be found in Erdös and Spencer [ES74], Lutz [Lut88], and many other references. This result states that

$$\sum_{0 \leq i \leq aN} \binom{N}{i} p^i (1-p)^{N-i} \leq \rho^N \tag{2.1}$$

for all $0 < a < p < 1$, where

$$\rho = \left(\frac{p}{a}\right)^a \left(\frac{1-p}{1-a}\right)^{1-a}.$$

If we set $p = \frac{1}{2}$, then (2.1) tells us that

$$\sum_{0 \leq i \leq aN} \binom{N}{i} \leq 2^N \rho^N. \tag{2.2}$$

We will use (2.2) in the case where $p = \frac{1}{2}$ and $a = \frac{1}{2}(1-\varepsilon)$ for some $\varepsilon > 0$. In this case,

$$\rho = \left[(1-\varepsilon)^{\varepsilon - 1}(1+\varepsilon)^{-\varepsilon - 1}\right]^{\frac{1}{2}} = \left[\left(1-\varepsilon^2\right)^{-1}\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{\varepsilon}\right]^{\frac{1}{2}}.$$

3 Two Recent Results

This section summarizes two recent results which are used to prove the upward measure separation.

Definition (Nisan and Wigderson [NW88, NW89]). Given $\delta > 0$ and $n, s \in \mathbf{N}$, a language $L \subseteq \{0,1\}^*$ is *(δ, s)-hard at n* if

$$|L(\gamma) \bigtriangleup L_{=n}| > 2^{n-1}(1-\delta)$$

for every n-input circuit γ with $\text{size}(\gamma) \le s$. The *hardness* of a language $L \subseteq \{0,1\}^*$ is the function $\mathrm{H}_L : \mathbf{N} \to \mathbf{N}$ defined by

$$\mathrm{H}_L(n) = \max\{h \in \mathbf{N} \mid L \text{ is } (h^{-1}, h)\text{-hard at } n\}.$$

Thus a language L is (δ, s)-hard at n if every n-input circuit of size s computes L incorrectly on at least $50(1-\delta)$ percent of the inputs in $\{0,1\}^n$. Note that $\mathrm{H}_L(n)$ is bounded above by the size of the smallest circuit which correctly computes $L_{=n}$.

For each $0 < \alpha < 1$, we define the set

$$\mathrm{H}_\alpha = \{L \subseteq \{0,1\}^* \mid \mathrm{H}_L(n) > 2^{\alpha n} \text{ a.e.}\}$$

of languages with hardness greater than $2^{\alpha n}$ almost everywhere.

A new construction of a pseudorandom bit generator was recently used to prove the following:

Theorem 1 (Nisan and Wigderson [NW88, NW89]). If $\mathrm{E} \cap \mathrm{H}_\alpha \neq \emptyset$ for some $\alpha > 0$, then $\mathrm{P} = \mathrm{BPP}$. □

The second result which we review in this section is (a special case of) an almost everywhere lower bound on the space-bounded program-size complexity of languages in ESPACE. (Program-size complexity was originally introduced by Solomonoff [Sol64], Kolmogorov [Kol65], and Chaitin [Cha66]. Time- and space-bounded program-size complexities have since been investigated by Hartmanis [Har83], Sipser [Sip83], Levin [Lev84], Huynh [Huy86], Ko [Ko86], Longpré [Lon86], Lutz [Lut89, Lut90], and many others. For an overview of work in this area, see Kolmogorov and Uspenskii [KU87] or Li and Vitanyi [LV88].)

Definition. Given a machine M, a resource bound $t : \mathbf{N} \to \mathbf{N}$, a language $L \subseteq \{0,1\}^*$, and a natural number n, the *t-space-bounded program-size complexity* of $L_{=n}$ relative to M is

$$\mathrm{KS}_M^t(L_{=n}) = \min\{|\pi| \mid M(\pi, n) = \chi_{L_{=n}} \text{ in } \le t(2^n) \text{ space}\},$$

i.e., the length of the shortest program π such that M, on input (π, n), outputs the characteristic string of $L_{=n}$ and halts without using more than $t(2^n)$ workspace.

Well-known simulation techniques show that there exists a machine U which is *optimal* in the sense that for each machine M there is a constant c such that for all t, L, and n we have

$$\mathrm{KS}_U^{ct+c}(L_{=n}) \leq \mathrm{KS}_M^t(L_{=n}) + c.$$

As usual, we fix an optimal machine U and omit it from the notation.

It can easily be seen that, if $x \in \{0,1\}^\infty$ is the characteristic sequence of $L \subseteq \{0,1\}^*$, then $\mathrm{KS}^t(L_{=n})$ is precisely $\mathrm{KS}^t(x \wedge \hat{\sigma} \mid 2^{n+1} - 1)$, the t-space bounded $\hat{\sigma}$-selective program-size complexity of x, as defined in Lutz [Lut89]. We thus have the following result.

Theorem 2 (Lutz [Lut89]). For any polynomial q and any real $a > 1$, if

$$X = \{L \subseteq \{0,1\}^* \mid \mathrm{KS}^q(L_{=n}) > 2^n - an \text{ a.e.}\},$$

then $\mu(X \mid \mathrm{ESPACE}) = 1$. □

The conclusion of Theorem 2 says that *almost every* language in ESPACE is in X, i.e., has high q-space bounded program-size complexity almost everywhere. A precise definition of the condition $\mu(X \mid \mathrm{ESPACE}) = 1$ may be found in Lutz [Lut89, Lut90], but is not needed here because Theorem 2 gives us the means to prove a variety of measure-theoretic results without explicitly discussing measure.

The only other properties of measure which we use are the following trivial facts.

(i) If $X \subseteq Y$ and $\mu(X \mid \mathrm{ESPACE}) = 1$, then $\mu(Y \mid \mathrm{ESPACE}) = 1$.

(ii) If $X \cap Y = \emptyset$ and $\mu(X \mid \mathrm{ESPACE}) = 1$, then $\mu(Y \mid \mathrm{ESPACE}) = 0$.

Beyond this, we hope that the reader will accept (or acquire from Lutz [Lut89, Lut90]) the intuition that $\mu(X \mid \mathrm{ESPACE}) = 0$ means that $X \cap \mathrm{ESPACE}$ is a very small subset of ESPACE.

4 Upward Measure Separation

The following result is the technical content of this section.

Theorem 3. If $\mathrm{H} = \bigcap_{0<\alpha<\frac{1}{3}} \mathrm{H}_\alpha$, then $\mu(\mathrm{H} \mid \mathrm{ESPACE}) = 1$.

This result is interesting in and of itself, since it says that almost every language in ESPACE is very hard to approximate with circuits. In this paper we are especially interested in the following application.

Main Theorem. If $\mathrm{P} \subsetneqq \mathrm{BPP}$, then $\mu(\mathrm{E} \mid \mathrm{ESPACE}) = 0$.
Proof. Let H be as in Theorem 3. If $\mathrm{P} \subsetneqq \mathrm{BPP}$, then $\mathrm{E} \cap \mathrm{H} = \emptyset$ by Theorem 1. Since $\mu(\mathrm{H} \mid \mathrm{ESPACE}) = 1$, it follows that $\mu(\mathrm{E} \mid \mathrm{ESPACE}) = 0$. □

Thus any separation of P from BPP implies a measure separation of E from ESPACE.

The rest of this section is devoted to the proof of Theorem 3. We use the following lemmas.

Lemma 4. For any real $b < 1$, for all sufficiently small reals $\varepsilon > 0$,

$$\left(1 - \varepsilon^2\right)^{-1} \left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{\varepsilon} < 1 - b\varepsilon^2.$$

Lemma 5. There exist a polynomial q and a constant $c > 0$ with the following property. For every two reals $0 < \alpha < \beta < 1$, for all sufficiently large n, for every language $L \subseteq \{0,1\}^*$, if $\mathrm{H}_L(n) \leq 2^{\alpha n}$, then

$$\mathrm{KS}^q(L_{=n}) < 2^n - c2^{(1-2\alpha)n} + 2^{\beta n}.$$

Proof of Theorem 3. Choose q and c as in Lemma 5 and define X as in Theorem 2, using $a = 2$. We will show that $X \subseteq \mathrm{H}$, whence Theorem 3 follows from Theorem 2.

Assume that $L \notin \mathrm{H}$, i.e., that $L \notin \mathrm{H}_\alpha$ for some $0 < \alpha < \frac{1}{3}$. Fix β such that $\alpha < \beta < 1 - 2\alpha$. Then $\mathrm{H}_L(n) \leq 2^{\alpha n}$ i.o., so the inequality in the conclusion of Lemma 5 holds for infinitely many n. Since $\beta < 1 - 2\alpha$, the right-hand side of this inequality is less than $2^n - 2n$ for all sufficiently large n, so it follows that $L \notin X$. □

Proof of Lemma 4. Calculating with Taylor approximations, we have

$$\begin{aligned}\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{\varepsilon} &= (1-2\varepsilon+o(\varepsilon))^{\varepsilon} = e^{\varepsilon \ln(1-2\varepsilon+o(\varepsilon))} \\ &= e^{-2\varepsilon^2+o(\varepsilon^2)} = 1-2\varepsilon^2+o(\varepsilon^2)\end{aligned}$$

as $\varepsilon \to 0$. Since $b < 1$ and $(1-\varepsilon^2)(1-b\varepsilon^2) = 1-(1+b)\varepsilon^2+o(\varepsilon^2)$ as $\varepsilon \to 0$, it follows that

$$\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{\varepsilon} < (1-\varepsilon^2)(1-b\varepsilon^2)$$

for all sufficiently small ε. □

Proof of Lemma 5. Call an n-input circuit γ *novel* if no n-input circuit which precedes γ (in a standard enumeration of all circuits; no circuit precedes a smaller one in this enumeration) computes the same set as γ. The predicate "γ is a novel n-input circuit" can clearly be tested in space which is polynomial in $n+\text{size}(\gamma)$. Let $\gamma_1, \ldots, \gamma_{J(n)}$ be the enumeration of all novel n-input circuits (in their order of appearance in the standard enumeration). Also, let $N = 2^n$ and let $\Delta_1, \ldots, \Delta_{J(n)}$ be the enumeration of $\{0,1\}^N$ which is lexicographic, except that no string precedes a string which has fewer 1's. (Of course $J(n) = 2^N = 2^{2^n}$ in both cases.) It is routine to design a machine M which takes inputs $\pi \in \{0,1\}^*$ and $n \in \mathbf{N}$ and has the following property. If $\pi = \langle t, d\rangle$, where $t, d \in \{1, \ldots, J(n)\}$ are represented in binary, then $M(\pi, n) = \text{graph}(\gamma_t) \oplus \Delta_d$, where $\text{graph}(\gamma_t)$ is the N-bit characteristic string of the set computed by γ_t, $\oplus$ denotes bitwise exclusive-or, and this computation is carried out in space which is polynomial in 2^n. Since the pairing function can be implemented with $|\langle t, d\rangle| \le |t| + |d| + 2\log|t| + 4$, and since we have fixed an optimal machine in defining KS, it follows that there exist a polynomial q and a constant c_1 such that

$$\text{KS}^q(L_{=n}) \le |t| + |d| + 2\log|t| + c_1 \tag{4.1}$$

whenever $\text{graph}(\gamma_t) \oplus \Delta_d$ is the characteristic string of $L_{=n}$.

Now fix $0 < \alpha < \beta < 1$. A standard counting argument (see, for example, Shannon [Sha49], Balcázar, Diáz, and Gabarró [BDG88], or Lutz [Lut89]) shows that at most $[48e2^{\alpha n}]^{2^{\alpha n}} = [48eN^{\alpha}]^{N^{\alpha}}$ n-input circuits γ are novel and have $\text{size}(\gamma) \le 2^{\alpha n}$. The number $D(n)$ of N-bit strings Δ which have $\frac{N}{2}(1-N^{-\alpha}) = 2^{n-1}(1-2^{-\alpha n})$ or fewer 1's is given by

$$D(n) = \sum_{0 \le i \le aN} \binom{N}{i},$$

where we write $a = \frac{1}{2}(1-\varepsilon)$ and $\varepsilon = N^{-\alpha}$ for convenience. By the Chernoff [Che52] bound discussed in section 2, this implies that

$$D(n) \le 2^N \rho^N,$$

where

$$\rho = \left[\left(1-\varepsilon^2\right)^{-1}\left(\frac{1-\varepsilon}{1+\varepsilon}\right)^{\varepsilon}\right]^{\frac{1}{2}}.$$

It follows by Lemma 4 that

$$D(n) \le 2^N\left(1-\frac{\varepsilon^2}{2}\right)^{\frac{N}{2}} = 2^{N+\frac{N}{2}\log(1-\frac{\varepsilon^2}{2})}$$

for all sufficiently large n. Since

$$\log(1-\frac{\varepsilon^2}{2}) = \frac{1}{\ln 2}\ln(1-\frac{\varepsilon^2}{2}) \le \frac{-\varepsilon^2}{2\ln 2}$$

for all ε, it follows that

$$D(n) \le 2^{N-cN\varepsilon^2} = 2^{N-cN^{1-2\alpha}} \tag{4.2}$$

for all sufficiently large n, where $c = \frac{1}{4\ln 2}$.

Now let n be large enough that (4.2) holds and

$$2 + \log K + 2\log(1+\log K) + c_1 < N^{\beta}, \tag{4.3}$$

where $K = [48eN^{\alpha}]^{N^{\alpha}}$ and c_1 is as in (4.1). Assume that $\mathrm{H}_L(n) \le 2^{\alpha n}$. Then, by (4.2) and our estimate of the number of novel circuits of size $\le 2^{\alpha n}$, there exist $t \le K$ and $d \le 2^{N-cN^{1-2\alpha}}$ such that $\mathrm{graph}(\gamma_t) \oplus \Delta_d$ is the characteristic string of $L_{=n}$. It follows by (4.1) and (4.3) that

$$\begin{aligned}
\mathrm{KS}^q(L_{=n}) &\le |t| + |d| + 2\log|t| + c_1 \\
&\le 1 + \log K + 1 + N - cN^{1-2\alpha} + 2\log(1+\log K) + c_1 \\
&< N - cN^{1-2\alpha} + N^{\beta} \\
&= 2^n - c2^{(1-2\alpha)n} + 2^{\beta n}.
\end{aligned}$$

□

5 Conclusion

This paper refines the picture

$$\mathrm{P} \subsetneq \mathrm{BPP} \Longrightarrow \mathrm{P} \subsetneq \mathrm{P/Poly} \cap \mathrm{PSPACE} \Longleftrightarrow \mathrm{E} \subsetneq \mathrm{ESPACE}$$

to the form

$$\begin{array}{ccc}
\mathrm{P} \subsetneq \mathrm{BPP} & \Longrightarrow & \mu(\mathrm{E} \mid \mathrm{ESPACE}) = 0 \\
\Downarrow & & \Downarrow \\
\mathrm{P} \subsetneq \mathrm{P/Poly} \cap \mathrm{PSPACE} & \Longleftrightarrow & \mathrm{E} \subsetneq \mathrm{ESPACE}.
\end{array}$$

It will be interesting to see the situation clarified further.

Acknowledgments. I thank Noam Nisan, Giora Slutzki, William Schmidt, and David Juedes for helpful discussions.

References

[Adl78] L. Adleman, Two theorems on random polynomial time, *Proceedings of the 19th IEEE Symposium on Foundations of Computer Science*, 1978, pp. 75–83.

[BDG88] J. L. Balcázar, J. Díaz, and J. Gabarró, *Structural Complexity I*, Springer-Verlag, 1988.

[BG81] C. H. Bennett and J. Gill, Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1, *SIAM Journal on Computing* **10** (1981), pp. 96–113.

[Boo74] R. V. Book, Comparing complexity classes, *Journal of Computer and System Sciences* **9** (1974), pp. 213–229.

[Cha66] G. J. Chaitin, On the length of programs for computing finite binary sequences, *Journal of the Association for Computing Machinery* **13** (1966), pp. 547–569.

[Che52] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Annals of Mathematical Statistics* **23** (1952), pp. 493–507.

[ES74] P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, New York, 1974.

[Fre72] R. I. Freidzon, Families of recursive predicates of measure zero, translated in *Journal of Soviet Mathematics* **6** (1976), pp. 449–455.

[Gil77] J. Gill, Computational complexity of probabilistic Turing machines, *SIAM Journal on Computing* **6** (1977), pp. 675–695.

[Hal50] P. R. Halmos, *Measure Theory*, Springer-Verlag, 1950.

[Har83] J. Hartmanis, Generalized Kolmogorov complexity and the structure of feasible computations, *Proceedings of the 24th IEEE Symposium on the Foundations of Computer Science*, 1983, pp. 439–445.

[Huy86] D. T. Huynh, Resource-bounded Kolmogorov complexity of hard languages, *Structure in Complexity Theory*, Springer-Verlag, 1986, pp. 184–195.

[HY84] J. Hartmanis and Y. Yesha, Computation times of NP sets of different densities, *Theoretical Computer Science* **34** (1984), pp. 17–32.

[Ko86] K. Ko, On the notion of infinite pseudorandom sequences, *Theoretical Computer Science* **48** (1986), pp. 9–33.

[Kol65] A. N. Kolmogorov, Three approaches to the quantitative definition of 'information', *Problems of Information Transmission* **1** (1965), pp. 1–7.

[KU87] A. N. Kolmogorov and V. A. Uspenskii, Algorithms and randomness, translated in *Theory of Probability and its Applications* **32** (1987), pp. 389–412.

[Lev84] L. A. Levin, Randomness conservation inequalities; information and independence in mathematical theories, *Information and Control* **61** (1984), pp. 15–37.

[Lon86] L. Longpré, *Resource Bounded Kolmogorov Complexity, a Link Between Computational Complexity and Information Theory*, PhD thesis, Cornell University, 1986. Technical Report TR-86-776.

[Lut88] J. H. Lutz, An elementary combinatorial derivation of "the" Chernoff bound, Technical Report 88-8, Iowa State University, 1988.

[Lut89] J. H. Lutz, Almost everywhere high nonuniform complexity, *Proceedings of the Fourth Structure in Complexity Theory Conference*, 1989, pp. 81–91.

[Lut90] J. H. Lutz, Category and measure in complexity classes, *SIAM Journal on Computing*, 1990, to appear.

[LV88] M. Li and P. M. B. Vitanyi, Two decades of applied Kolmogorov complexity: In memoriam Andrei Nikolaevich Kolmogorov 1903-1987, *Proceedings of the Third Structure in Complexity Theory Conference*, 1988, pp. 80–101.

[Meh74] K. Mehlhorn, The "almost all" theory of subrecursive degrees is decidable, *Proceedings of the Second Colloquium on Automata, Languages, and Programming*, 1974, pp. 317–325.

[NW88] N. Nisan and A. Wigderson, Hardness vs. randomness, *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, 1988, pp. 2-11.

[NW89] N. Nisan and A. Wigderson, Hardness vs. randomness, manuscript.

[Sha49] C. E. Shannon, The synthesis of two-terminal switching circuits, *Bell System Technical Journal* **28** (1949), pp. 59–98.

[Sip83] M. Sipser, A complexity-theoretic approach to randomness, *Proceedings of the 15th ACM Symposium on the Theory of Computing*, 1983, pp. 330–335.

[Sol64] R. J. Solomonoff, A formal theory of inductive inference, *Information and Control* **7** (1964), pp. 1–22, 224–254.