A Small Span Theorem within P

Wolfgang Lindner and Rainer Schuler*

Abteilung Theoretische Informatik, Universität Ulm,
Oberer Eselsberg, 89069 Ulm, GERMANY

Abstract

The development of Small Span Theorems for various complexity classes and reducibilities plays a basic role in (resource bounded) measure-theoretic investigations of efficient reductions. A Small Span Theorem for a complexity class $\mathcal{C}$ and reducibility $\leq_r$ is the assertion that, for all sets A in $\mathcal{C}$, at least one of the cones below or above A is a negligible small class with respect to $\mathcal{C}$, where the cones below or above A refer to the sets $\{B : B \leq_r A\}$ and $\{B : A \leq_r B\}$, respectively. That is, a Small Span Theorem rules out one of the four possibilities of the size of upper and lower cones for a set in $\mathcal{C}$.

Here we use the recent formulation of resource-bounded measure of Allender and Strauss which allows meaningful notions of measure on polynomial-time complexity classes. We show two Small Span Theorems for polynomial-time complexity classes and sublinear-time reducibilities, namely a Small Span Theorem for P and Dlogtime-uniform NC^0-computable reductions, and for P^{NP} and Dlogtime-transformations. Furthermore, we show that, for every fixed k, the hard set for P under Dlogtime-uniform AC^0-reductions of depth k and size n^k is a small class. In contrast, we show that every upper cone under P-uniform NC^0-reductions is not small.

1 Introduction

Resource-bounded measure [18] provides a tool to investigate abundance phenomena in complexity classes. Besides insights in the measure-theoretic structure of complexity classes, resource-bounded measure also enriches the measure-theoretic investigations of efficient reductions with its origin in the work of Bennet and Gill [13, 19, 14, 4, 6]

A unifying theme in this area is the development of *Small Span Theorems* for various complexity classes and reducibilities. A first Small Span Theorem for EXP and polynomial-time many-one reductions was shown by Juedes and Lutz [17], and has subsequently extended to other reducibilities (e.g. [9, 20]). Briefly, a Small Span Theorem for a complexity class $\mathcal{C}$ is the assertion that, for all sets A in $\mathcal{C}$, at least one of the cones below or above A

*{lindner,schuler}@informatik.uni-ulm.de

is a negligible small class with respect to $\mathcal{C}$, where the cones below or above A refer to the sets reducible to A, and the sets to which A can be reduced, respectively. That is, a Small Span Theorem rules out one of the four possibilities of the size of upper and lower cones for a set in $\mathcal{C}$. As an immediate consequence, the hard sets for $\mathcal{C}$ is a negligible small class with respect to $\mathcal{C}$. Furthermore, there are sets for all of the three possibilities not ruled out by a Small Span Theorem, which has been further studied in [10, 15, 8, 23]. (For a recent overview, we refer to [7, 21].)

The formulation of resource-bounded measure given by Lutz applies only to complexity classes at least containing E. Recently, Allender and Strauss [4, 5, 3] provided meaningful notions of measure on P. Here we concentrate on the most restricted notion, the conservative $\Gamma(\mathrm{P})$-measure. Though some of intuitively small subclasses of P are in fact not measurable, notably the *p-printable sets* and hence all sparse sets in P, it satisfies all basic properties required by a reasonable notion of measure in P. In particular, it is possible to define *pseudo-random* sets and to show that the majority of sets in P is pseudo-random [3]. Furthermore, all proofs in this context relativize, that is, the definitions immediately apply to classes like P^{NP}.

In order to have a non-trivial degree structure in P without unproven assumptions we consider reductions computed by Dlogtime-uniform constant depth circuits (see e.g. [1]). We show a Small Span Theorem for Dlogtime-uniform NC^0-reductions in P. In contrast, we show that every upper cone under P-uniform NC^0-reductions is not small. It follows that a Small Span Theorem for P-uniform NC^0-reductions does not hold.

A consequence of the Small Span Theorem is that the hard sets for P under Dlogtime-uniform NC^0-reductions is a small class. We also show that this can be improved to a restricted version of Dlogtime-uniform AC^0-reductions of depth k.

As in the proofs in [17, 9] the main technical step in the proof of the Small Span Theorem is to show that every reduction from a pseudo-random set can not decrease the length of its value to much. In the case of polynomial-time reductions and exponential-time classes this involves inverting polynomial-time functions, which can be done in exponential time. But even Dlogtime-uniform NC^0-computable functions can not be inverted in polynomial time, unless $\mathrm{P} = \mathrm{NP}$. Thus, we merely explore the fact that for a NC^0-computable function there is some constant c such that each output bit depends on at most c different input bits. In contrast, we use the exponential lower bound on the size of a constant depth circuit for the parity function [25, 16] to show the result concerning the hard sets for P under (restricted) AC^0-reductions.

However, in the presence of an NP-oracle, Dlogtime-transformations are invertible. This allows us to show a Small Span Theorem for Dlogtime-transformations within P^{NP} with an adaption of the proofs in [17, 9].

2 Preliminaries

A *circuit family* is a sequence $\{C_n\}$, $n \in N$ where each C_n is an acyclic circuit with n Boolean inputs $x_1, \ldots, x_n$ (as well as the constants 0 and 1 allowed as inputs) and some number of output gates $y_1, \ldots, y_m$. $\{C_n\}$ has *size* $s(n)$ if each circuit C_n has at most $s(n)$ gates; it has *depth* $d(n)$ if the length of the longest path from input to output in C_n is at most $d(n)$. A family $\{C_n\}$ is *uniform* if the function $n \mapsto C_n$ is easy to compute in some sense. We will consider Dlogtime-uniformity [12] and P-uniformity [2].

A function f is said to be AC^0*-computable* if there is a circuit family $\{C_n\}$ of polynomial size and constant depth consisting of unbounded fan-in AND and OR and NOT gates such that for each input x of length n, the output of C_n on input x is $f(x)$.

A function f is said to be NC^0*-computable* if there is a circuit family $\{C_n\}$ of polynomial size and constant depth, consisting of fan-in two AND and OR and NOT gates. Note that for any NC^0 circuit family, there is some constant c such that each output bit depends on at most c different input bits.

Note that a NC^0-(AC^0)-computable function f satisfies the restriction that $|x| = |y| \implies |f(x)| = |f(y)|$.

A function g is an *inverse* of a function f, if, for all strings y, $y \in \mathit{range}\ f \implies f(g(y)) = y$. A proof of the following can be found in e.g. [1].

1. Proposition. P = NP *if and only if every length increasing Dlogtime-uniform* NC^0*-computable function has a polynomial-time computable inverse.*

A set A is NC^0*-(*AC^0*-)reducible* to a set B if A is many-one reducible to B via a polynomially length bounded NC^0-(AC^0-)computable function.

A function f is a *Dlogtime-transformation* if f is polynomially length bounded and the set $\{(x, i, b) : \text{the } i\text{-th bit of } f(x) \text{ is } b \in \{0, 1\}\ \}$ is decidable in logarithmic time.

A set A is *r-printable* if there is a function computable within the resources specified by r, which, on input 0^n, prints out the whole set of strings in A up to length n.

3 Measure on P

In order to define a reasonable notion of measure within subexponential time classes, Allender and Strauss [4, 5] consider *sublinear* computations. Here the underlying computation model is a Turing machine with random-access to its input via a special index tape. When M enters a special query state, M receives the i-th bit of the input, where i is the content of the index tape. Furthermore, M is given both w and the length of w as the input.

Given such a machine M and a string w, let $I_M(w)$ denote the set of bits queried by M to the input w. We assume that M queries the bits of the input w in *parallel*, that is, the bits queried by M do not depend on the actual input w but only on the length $|w|$. Define the *dependency set* $D_M(w) \subset \{0, 1, \ldots, n\}$ be the unique minimal set containing $I_M(w)$

and satisfying

$$i \in D_M(w) \Longrightarrow I_M(w[0..i]) \subseteq D_M(w)$$

Note that the queries to the length of w are *not* content of the dependency set.

A function f is $\Gamma(n^c)$-*computable* if it is computable by a machine M such that M runs in time $O(\log^c |w|)$ and has dependency sets $D_M(w)$ with size bounded by $O(\log^c |w|)$. A function $f : \Sigma^\star \to \Sigma^\star$ is $\Gamma(\mathrm{P})$-*computable* if f is $\Gamma(n^c)$-computable for some $c \in N$.

A *martingale* is a function $d : 2^{<\omega} \to \mathrm{R}^+$ satisfying the *average law* $d(x0) + d(x1) = 2d(x)$ for all $x \in 2^{<\omega}$. A martingale *succeeds* on a set $A \subseteq \Sigma^\star$ if $\limsup_n d(A|z_n) = \infty$. A class $\mathcal{X}$ is a $\Gamma(n^c)$-*nullset* if there is a $\Gamma(n^c)$-computable martingale d which succeeds on every set in $\mathcal{X}$. A class $\mathcal{X}$ is a $\Gamma(\mathrm{P})$-*nullset* if $\mathcal{X}$ is a $\Gamma(n^c)$-nullset for some $c \in N$.

Allender and Strauss show that the $\Gamma(\mathrm{P})$-nullsets define a reasonable notion of nullsets. That is, the $\Gamma(\mathrm{P})$-measure corresponds to P in the sense that all singletons of P are $\Gamma(\mathrm{P})$-nullsets, but the whole space P is not a $\Gamma(\mathrm{P})$-nullsets. Moreover, the collection of $\Gamma(\mathrm{P})$-nullsets is closed under subsets, finite unions, and arbitrary unions over the sub-collection of $\Gamma(n^c)$-nullsets.

The latter permits the definition of pseudo-random sets as the "typical" sets within P in the sense of [24]. More precisely, define a set A to be $\Gamma(n^c)$-*random* if no $\Gamma(n^c)$-computable martingale succeeds on A. Equivalently, A is $\Gamma(n^c)$-random if and only if the singleton $\{A\}$ is a $\Gamma(n^c)$-nullset. Then, for each fixed c, all sets in P but a $\Gamma(\mathrm{P})$-nullset are $\Gamma(n^c)$-random, but no $\Gamma(n^c)$-random set possesses any property which is specific for only a $\Gamma(n^c)$-nullset.

This gives us the following characterization of $\Gamma(\mathrm{P})$-nullsets in terms of $\Gamma(n^c)$-random sets.

2. Proposition. *Let $\mathcal{X}$ any class of sets. The following are equivalent.*

1. *$\mathcal{X}$ is a $\Gamma(\mathrm{P})$-nullset.*
2. *For some $c \geq 1$, $\mathcal{X}$ contains no $\Gamma(n^c)$-random set.*

Mayordomo [22] showed that, for every fixed c, the class of non-Dtime(n^c)-bi-immune sets is small in exponential time. The same proof can be used to show the following.

3. Proposition. *If A is a $\Gamma(n^c)$-random set then A is bi-immune for the class of* Dtime(n^c)*-printable sets.*

4 The Small Span Theorem

4. Lemma. *Let A be a $\Gamma(n^3)$-random set reducible to some set B via a function f computable by a Dlogtime-uniform* NC^0*-circuit family of depth d. Then $|f(x)| \geq |x|/2^d$.*

Proof. Suppose f maps strings of length n to strings of length less than $n/2^d$ for infinitely many n. Fix such an n. Then there is at least one input bit which is ignored by the circuit computing f. Let y be the string of length n, where all the ignored bits are set to 1, and the remaining bits are set to 0. Then $f(0^n) = f(y)$, and therefore, $A(0^n) = A(y)$, that is, the membership of y in A can be predicted from the membership of 0^n in A. Since y can be computed in time $O(n \log n)$, it follows that there is a $\Gamma(n^3)$-martingale which succeeds on A. □

5. Theorem. *Let A be a $\Gamma(n^3)$-random set in* $\mathrm{Dtime}(n^c)$*, for some $c \geq 1$. Let A be reducible to some set B via a Dlogtime-uniform* NC^0*-reduction f. Then B has an infinite* $\mathrm{Dtime}(n^{c+3})$*-printable subset.*

Proof. Since A is $\Gamma(n^3)$-random, $A \cap 0^\star$ is infinite. Hence, by Lemma 4, $f(A \cap 0^\star)$ is a infinite $\mathrm{Dtime}(n^{c+3})$-printable subset of B. □

6. Corollary (Small Span Theorem). *For every set A in* P*, either its upper or its lower cone under Dlogtime-uniform* NC^0*-reductions is a* $\Gamma(\mathrm{P})$*-null set.*

Proof. Fix a set A in P. If the lower cone of A is a $\Gamma(\mathrm{P})$-nullset then the assertion follows vacuously. So assume that the lower cone of A is not a $\Gamma(\mathrm{P})$-nullset. Hence, by Proposition 2, the lower cone of A contains a $\Gamma(n^3)$-random set in $\mathrm{Dtime}(n^c)$, for some $c \geq 1$. From Proposition 3, Theorem 5 and the transitivity of uniform projections, it follows that the upper cone of A contains no $\Gamma(n^{c+3})$-random set. Hence, again by Proposition 2, the upper cone of A is a $\Gamma(\mathrm{P})$-null set. □

7. Remark. We note that there are sets in P for all three cases not ruled out by the Small Span Theorem. First, every set in NC^0 can be reduced to all sets, hence its upper cone is not small. Second, the lower cone of any complete set in P is not small. Finally, consider the set $A = \{x : |x| = 2^k, k \geq 1,$ and x has an even number of 1's$\}$. Using similar arguments as in Lemma 4 and Theorem 5 its not hard to see that the upper cone of A is small. Moreover, for every set B reducible to A, $0^{2^k} \in B$ is decidable in linear time, whence B is not bi-immune for the class of $\mathrm{Dtime}(n)$-printable sets. Hence the lower cone of A is small as well.

8. Theorem. *(1) Every upper cone under* P*-uniform* NC^0*-computable reductions is not a* $\Gamma(\mathrm{P})$*-nullset.*
(2) Every degree under P*-uniform* AC^0*-computable reductions is not a* $\Gamma(\mathrm{P})$*-nullset.*

Proof. Fix any set A. In order to proof that the p-printable sets do not form a $\Gamma(\mathrm{P})$-nullset Allender and Strauss [4] show the following.

Let d be a $\Gamma(\mathrm{P})$-martingale. Then there are p-printable sets D and D_1, with $D_1 \subseteq D$, such that, for all set B, if B satisfies $x \in D \implies B(x) = D_1(x)$ then d does not succeed on B.

Since D is sparse, for every n there is some string x of length n such that $\{yx_n : |x| = |y| = n\} \cap D = \emptyset$. Let x_n be the smallest such x. Since D is p-printable, x_n can be obtained from n in time polynomial in n.

Define a set A' by

$$z \in A' \iff \begin{cases} z \in D_1 & \text{if } z \in D \\ z = yx_n \text{ and } y \in A & \text{if } z \notin D \end{cases}$$

By the definition, d does not succeed on A'. The set A is reducible to A' via a P-uniform NC^0-function $y \mapsto yx_n$. This shows (1).

For (2) note that A' is reducible to A via a P-uniform AC^0-function. □

9. Remark. Let A be a complete for P under P-uniform NC^0-reductions. Then the lower cone of A is P, hence not a $\Gamma(\mathrm{P})$-nullset. By Theorem 8, the upper cone of A is not a $\Gamma(\mathrm{P})$-nullset as well. Thus, in contrast to Dlogtime-uniform NC^0-reductions, a Small Span Theorem for P and P-uniform NC^0-reductions does not hold.

In the following we show that each output-bit of a reduction may depend on all of the input-bits when considering only the hard sets for P.

Let us call a AC^0-function *k-bounded* if the circuit computing f has depth $\leq k$, and every output-bit is determined by a circuit of size $\leq n^k$.

10. Theorem. *Let $k \geq 1$ some fixed constant. The upper cone of PARITY under Dlogtime-uniform k-bounded* AC^0*-reductions is a* $\Gamma(\mathrm{P})$*-nullset.*

Proof. Let *PARITY* be reducible to some set B via a function f computable by an AC^0 circuit of depth k.

Let C_n be the circuit which, for strings x of length n, compares $f(x)$ with all strings of length $|f(x)|$ and accepts x if and only if $f(x) \in B$. Since f is a reduction from *PARITY* to B, C_n computes the parity function. The size of C_n is $O(n^k + 2^{|f(x)|})$. From the lower bound $2^{n^{\Omega(1/d)}}$ on the *PARITY* function [25, 16], it follows that $|f(x)| \geq |x|^{(1/ck)}$, where c can be chosen independently of B and f.

Hence, $f(1 \cdot 0^\star)$ is an infinite $\mathrm{Dtime}(n^{ck+2})$-printable subset of B. The assertion follows from Proposition 2. □

5 A Small Span Theorem in P^{NP}

As already observed in [4] all basic properties hold also in the presence of an NP oracle, if we consider $\Gamma(n^c)^{\mathrm{NP}}$-computable functions where the machine computing f may ask queries to *SAT* of length bounded by $O(\log^c n)$.

As in [17, 10] we adapte the version of the strongly P-bi-immune sets [11] in order to proof the following lemma.

11. Lemma. *There is a constant $c \geq 1$ such that, if A is a $\Gamma(n^c)^{SAT}$-random set reducible to some set B via a Dlogtime-transformation f, then $|f(x)| \geq |x|$ for infinitely many x.*

Proof. Define f's *collision set* $C_f \subseteq \Sigma^\star \times \Sigma^\star$ by

$$C_f = \{(x, y) : x < y \text{ and } f(x) = f(y)\},$$

and its *bounded collision set* $\hat{C}_f \subseteq \Sigma^\star \times \Sigma^\star$ by

$$\hat{C}_f = \{(x, y) : x < y \text{ and } f(x) = f(y) \text{ and } |f(y)| \leq |y|\}.$$

First we show that if the bounded collision set $\hat{C}_f$ is finite, then $|f(x)| \geq |x|$ for infinitely many x. Consider the following two cases:

- If the collision set C_f is finite, then $|f(x)| \geq |x|$ i.o. follows from an easy counting argument.
- Otherwise the collision set C_f is infinite. Since $\hat{C}_f \subseteq C_f$ and $\hat{C}_f$ is finite, for almost all pairs (x, y) in C_f, $|f(y)| > |y|$.

Thus it suffices to show that f's bounded collision set $\hat{C}_f$ is finite. So assume that $\hat{C}_f$ is infinite. Hence there are infinitely many n and pairs (x_n, y_n) such that y_n is the lex. smallest string of length n such that there is some string $x' < y$ with $f(x') = f(y)$, and x_n is the lex smallest such x'. Every pair (x_n, y_n) can be generated by prefix search and $O(n)$ adaptive queries to an NP oracle. Since $f(x_n) = f(y_n)$, $A(x_n) = A(y_n)$. It follows that there is a martingale succeeding on A which is $\Gamma(n^c)$-computable relative to SAT, for some c which can be chosen independently of the transformation f. □

12. Theorem. *There are constants* $c, c' \geq 1$ *such that, if* A *is a* $\Gamma(n^c)^{SAT}$*-random set in* $\mathrm{Dtime}(n^d)^{SAT}$ *reducible to some set* B *via a Dlogtime-transformation* f*, then* B *is not bi-immune for the class of sets* $\mathrm{Dtime}(n^{\max(c',d)})$*-printable relative to* SAT*.*

Proof. Let c be as in Lemma 11. Let I be the infinite set of strings x such that x is the lex smallest string of the strings x' of length $|x|$ with $|f(x')| \geq |x'|$. Then $f(I \cap A)$ or $f(I \cap \overline{A})$ is a infinite set of B or $\overline{B}$, respectively, which is printable in time $O(n^{\max(c',d)})$ relative to SAT, where c' can be chosen independently of the transformation f. □

13. Corollary. *For every set* A *in* P^{NP}*, either its upper or its lower cone under Dlogtime-transformations is a* $\Gamma(\mathrm{P}^{\mathrm{NP}})$*-nullset.*

Acknowledgment. The authors would like to thank Johannes Köbler for many helpful discussions.

References

[1] M. Agrawal and E. Allender. An isomorphism theorem for circuit complexity. Technical Report TR96-002, ECCC, 1996.

[2] E. Allender. P-uniform circuit complexity. *Journal of the ACM*, 36:912–928, 1989.

[3] E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. Journal version; in preparation.

[4] E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. In *Proc. 35th IEEE Symposium on Foundations of Computer Science*, pages 807–818. 1994.

[5] E. Allender and M. Strauss. Measure on P: Robustness of the notion. In *Proc. 20th Mathematical Foundations of Computer Science*. Springer-Verlag, 1995.

[6] K. Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. In *Proceedings of the 1st Structure in Complexity Theory* LNCS 223, Springer Verlag, pages 23-34, 1986.

[7] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. Technical Report 22, Universität Heidelberg, 1996. to appear.

[8] K. Ambos-Spies, E. Mayordomo, and X. Zheng. A comparison of weak completeness notions. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, pages 171–178. IEEE Computer Society Press, 1996.

[9] K. Ambos-Spies, H.-C. Neis, and S.A. Terwijn. Genericity and measure for exponential time. In *Proc. 19th Mathematical Foundations of Computer Science*, volume 841 of *LNCS*, pages 221–232, 1994.

[10] K. Ambos-Spies, S.A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. In *Proc. 5th International Symposium on Algorithms and Computation*, volume 834 of *LNCS*, pages 369–377, 1994.

[11] J.L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Math. Systems Theory*, 18:1–10, 1985.

[12] D.A.M. Barrington, N. Immmerman and H. Straubing. On uniformity within NC^1. *J. Comput. System Sci.*, 41:274–306, 1990.

[13] C.H. Bennet and J. Gill. Relative to a random oracle A, $P(A) \neq NP(A) \neq$ co-NP(A) with probability 1. *SIAM Journal on Computing*, 10:69–113, 1981.

[14] R. Book, J. Lutz, and K. Wagner. An observation on probability versus randomness with applications to complexity classes. *Mathematical Systems Theory*, 26:201–209, 1994.

[15] H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proceedings of the 10th Annual Structure in Complexity Theory Conference*, pages 197–203. IEEE Computer Society Press, 1995.

[16] J. Håstad. Almost optimal lower bounds for small depth circuits. In *Proc. 18th ACM Symposium on Theory of Computing*, pages 6–20, 1986.

[17] D. Juedes and J.H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24:279–295, 1995.

[18] J.H. Lutz. Almost everywhere high nonuniform complexity. *J. Comput. System Sci.*, 44:220–258, 1992.

[19] J. Lutz. A pseudorandom oracle characterization of BPP. *SIAM Journal on Computing*, 22:1075–1086, 1993.

[20] J.H. Lutz. A small span theorem for P/Poly-Turing reductions. In *Proc. 10th Structure in Complexity Theory Conference*. 1995.

[21] J. Lutz. The quantitative structure of exponential time. In A. Selman and L. Hemaspaandra, editors, *Complexity Theory Retrospective II*. Springer Verlag, 1996. to appear.

[22] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136:487–506, 1992.

[23] R. Schuler. Truth-table closure and Turing closure of average polynomial time have different measures in EXP. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, pages 190-195. IEEE Computer Society Press, 1996.

[24] V.A. Uspenskii, A.L. Semenov, and A.Kh. Shen'. Can an individual sequence of zeros and ones be random? *Russian Math. Surveys*, 45:121–189, 1990.

[25] A.C-C Yao. Separating the polynomial hierarchy by oracles. In *Proc. 26th IEEE Symposium on Foundations of Computer Science*, pages 1-10. 1985.