Electronic Colloquium on Computational Complexity, Report No. 13 (2018)

Nondeterminisic Sublinear Time Has Measure 0 in P

John M. Hitchcock and Adewale Sekoni

Department of Computer Science
University of Wyoming

Abstract

The measure hypothesis is a quantitative strengthening of the P $\neq$ NP conjecture which asserts that NP is a nonnegligible subset of EXP. Cai, Sivakumar, and Strauss (1997) showed that the analogue of this hypothesis in P is false. In particular, they showed that NTIME$[n^{1/11}]$ has measure 0 in P. We improve on their result to show that the class of all languages decidable in nondeterministic sublinear time has measure 0 in P. Our result is based on DNF width and holds for all four major notions of measure on P.

1 Introduction

A central hypothesis of resource-bounded measure [7,9] is that NP does not have measure 0 in EXP [11,12]. Cai, Sivakumar, and Strauss [5] proved the surprising result that NTIME$[n^{1/11}]$ has measure 0 in P. This implies the analogue of the measure hypothesis in P fails, because NTIME$[\log n]$ has nmeasure 0 in P.

We improve the result of Cai et al. by showing that the class of all languages that can be decided in nondeterministic time at most

$$n\left(1 - \frac{2\lg\lg n}{\lg n}\right)$$

has measure 0 in P. In particular, the nondeterministic sublinear time class

$$\mathrm{NTIME}[o(n)]$$

has measure 0 in P.

Resource-bounded measure was initially defined for exponential-time and larger classes [8]. Defining measure within subexponential- and polynomial-time complexity classes has been challenging [2] and there are several notions [13, 15] The result of Cai et al. holds for

ISSN 1433-8092

a notion of measure on P we will refer to as Γ_d(P)-measure. Moser [13] developed a new notion of measure called F-measure. It is the only notion of measure that allows for defining resource-bounded dimension [10] at P. It was unknown whether or not the result of Cai et al. also holds for F-measure. Our result holds for Γ(P) measure (defined in [2]) and therefore for F-measure and all the notions of measure at P considered in [13,15].

Our stronger result also has a much easier proof than the proof in [5]. Cai et al. use Håstad's switching lemma and pseudorandom generators to show that the set of languages with nearly exponential size circuits has Γ_d(P)-measure 0 [5]. We use DNF width rather than the circuit size to improve their result. It is well known that a random Boolean function has DNF width close to n (see [6]). In Section 3, we show that the class of languages with sublinear DNF width has measure 0 in P. This is then applied in Section 4 to show that nondeterministic sublinear time also has measure 0 in P.

2 Preliminaries

2.1 Languages and Boolean functions

The set of all binary strings is $\{0,1\}^*$. The length of a string $x \in \{0,1\}^*$ is denoted by $|x|$. The empty string is denoted by λ. For $n \in \mathbb{N}$, $\{0,1\}^n$ is the set of strings of length n. $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, ...$ is the standard lexicographic enumeration of $\{0,1\}^*$. A language L is a subset of $\{0,1\}^*$. The set of length n strings of a language L is $L^{=n} = L \cap \{0,1\}^n$. Associated with every language L is its characteristic sequence $\chi_L \in \{0,1\}^\infty$. It is defined as

$$\chi_L[i] = 1 \iff s_i \in L \text{ for } i \in \mathbb{N},$$

where $\chi_L[i]$ is the i^{th} bit of χ_L. We also index χ_L with strings i.e. for $i \in \mathbb{N}$, $\chi_L[s_i] = \chi_L[i]$. $\chi_L[i,j]$ denotes the i^{th} through j^{th} bits of χ_L, while $\chi_L[\text{length } n]$ denotes $\chi_L[2^n - 1, 2^{n+1} - 2]$, i.e. the substring of the characteristic string of L corresponding to the strings in $L^{=n}$.

A Boolean function is any $f : \{0,1\}^n \longrightarrow \{0,1\}$. A DNF (disjunctive normal form) formula of f over the variables $x_1, x_2, \cdots, x_n$ is the logical OR of terms. A term is a logical AND of literals, where a literal is either a variable x_i or its logical negation $\overline{x}_i$. We require that no term contains a variable and its negation [14]. Also the logical OR of the empty term computes the constant $\mathbf{1}$ function while the the empty DNF computes the constant $\mathbf{0}$ function. A term's width is the number of literals in it. The size of a DNF computing f is the number of terms in it, while its width is the length of its longest term. The DNF width of f is the shortest width of any DNF computing f. We note that the width of the constant $\mathbf{0}$ and $\mathbf{1}$ functions is 0. For any term T we say that T fixes a bit position i if either x_i or its negation appear in T. The bit positions that aren't fixed by T are called free bit positions. For example the term $x_1 x_3 \bar{x}_4 : \{0,1\}^4 \longrightarrow \{0,1\}$, fixes the first, third and fourth bit positions, while the second bit position is free. We say that T covers a subset of $\{0,1\}^n$ if it evaluates to true on only the elements of the subset. The subset covered by T is the set of all strings that agree with T on all its fixed bit positions. A string $x \in \{0,1\}^n$ agrees with T if, for any fixed bit position i of T, the ith bit of x is 1 if and only if x_i appears in

T. We call the subset covered by T a subcube of dimension $n-k$, where k is the number of literals in T. It is called a subcube because it is a dimension $n-k$ hamming cube contained in the dimension n hamming cube.

Associated with any Boolean function is its characteristic string $\chi_f \in \{0,1\}^{2^n}$ defined as

$$f(w) = 1 \iff \chi_f[w] = 1 \text{ for } w \in \{0,1\}^n.$$

For any language L we view $L^{=n}$ as the Boolean function $\chi_{L^{=n}}$ defined as

$$\chi_{L^{=n}}(w) = 1 \iff L[w] = 1 \text{ for all } w \in \{0,1\}^n.$$

We can then define $\mathrm{DNF}_{\mathrm{width}}(L^{=n})$ to be the DNF width of $\chi_{L^{=n}}$.

2.2 Resource-bounded Measure at P

Resource-bounded measure was introduced by Lutz [8]. He used martingales and a resource bound $\Delta \supseteq \mathrm{p}$ to characterize classes of languages as either "big" or "small". Here p is the class of functions computable in polynomial time. Resource-bounded measure is a generalization of classical Lebesgue measure. For a given resource bound $\Delta \supseteq \mathrm{p}$ we get a "nice" characterization of sets of languages as having measure 0, measure 1 or being immeasurable with respect to Δ. Associated with each resource bound Δ is a class $R(\Delta)$ that does not have Δ-measure 0. We can then use Δ-measure to define a measure on classes within $R(\Delta)$. For example, p-measure yields a measure on the exponential-time class $R(\mathrm{p}) = \mathrm{E} = \mathrm{DTIME}[2^{O(n)}]$. For the class p_2 of quasipolynomial-time computable functions, p_2-measure yields a measure on $R(\mathrm{p}_2) = \mathrm{EXP} = \mathrm{DTIME}[2^{n^{O(1)}}]$. See [4, 9] for a survey of resource-bounded measure in $\Delta \supseteq \mathrm{p}$.

An apparently more difficult task is developing a notion of resource-bounded measure on subexponential classes, in particular developing a measure on P [2]. There are at least four notions of measure defined on P. Three of these are due to Strauss [15] and one is due to Moser [13]. None of them are quite as "nice" as measures on $R(\Delta) \supseteq \mathrm{E}$, each one of them having some limitations. See [3, 13, 15] for a more detailed discussion of the limitations of these notions of measure. In this paper we only consider one notion of measure on P we call $\Gamma(\mathrm{P})$-measure. $\Gamma(\mathrm{P})$-measure was introduced in [2]. We use $\Gamma(\mathrm{P})$-measure for two reasons. First, it is the simplest of the four notions of measure on P. Second, the martingales considered in $\Gamma(\mathrm{P})$-measure can be easily shown to be martingales in the other notions of measure at P [13, 15].

2.3 $\Gamma(\mathrm{P})$-measure

A martingale is a function $d : \{0,1\}^* \longrightarrow [0, \infty)$ that satisfies the the following averaging condition:

$$d(w) = \frac{d(w1) + d(w0)}{2}, \forall w \in \{0,1\}^*.$$

Intuitively, the input $w \in \{0,1\}^*$ to the martingale d is a prefix of the characteristic sequence of a language. The martingale starts with initial capital $d(\lambda)$. More generally, $d(w)$ is the martingale's current capital after betting on the strings $s_0, s_1, \cdots, s_{|w|-1}$ in the standard ordering. The martingale d tries to predict the membership of string $s_{|w|}$ when given input w. If d chooses to bet on $s_{|w|}$ and is successful in predicting its membership, then its current capital increases, otherwise it decreases. The martingale d can also choose to not risk its current capital $d(w)$ by not betting on $s_{|w|}$. The goal is to make d grow without bound on some subset of $\{0,1\}^\infty$. We say a martingale d succeeds on a language L if

$$\limsup_{n\to\infty} d(\chi_L[0, n-1]) = \infty.$$

We say d succeeds on a class $C \subseteq \{0,1\}^\infty$ if it succeeds on every language in C. It is easy to see that the probability a martingale d succeeds on a randomly selected language is 0. A language L is randomly selected by adding each string to L with probability 1/2. It can be shown that any class $C \subseteq \{0,1\}^\infty$ has measure 0 under the probability measure if and only if some martingale d succeeds on C. If d can be computed in some resource bound Δ then we say that C has Δ-measure 0 if d succeeds on C.

A $\Gamma(\mathrm{P})$-martingale is a martingale d such that:

- $d(w)$ can be computed by a Turing machine M with oracle access to w and input $s_{|w|}$. We denote this computation as $M^w(s_{|w|})$.
- $M^w(s_{|w|})$ is computed in time polynomial in $\lg(|w|)$. In other words, the computation is polynomial in the length of $s_{|w|}$.
- d only bets on strings in a P-printable set denoted G_d.

The input string $s_{|w|}$ to $M^w(s_{|w|})$ allows the Turing machine to compute the length of w without reading all of w whose length is exponential in the length of $s_{|w|}$. A set $S \subseteq \{0,1\}^*$ is P-printable [1] if $S \cap \{0,1\}^n$ can be printed in time polynomial in n. A class $C \subseteq \{0,1\}^\infty$ has $\Gamma(\mathrm{P})$-measure 0 zero if there is some $\Gamma(\mathrm{P})$-martingale that succeeds on it [15].

3 Measure and DNF Width

In this section we show that the class of languages with sublinear DNF width has measure 0 in P. Recall that for a language L, $\mathrm{DNF}_{\mathrm{width}}(L^{=n})$ denotes the DNF width of the characteristic string of L at length n.

Theorem 3.1. *The class*

$$X = \left\{ L \in \{0,1\}^\infty \;\middle|\; \mathrm{DNF}_{\mathrm{width}}(L^{=n}) \le n\left(1 - \frac{2\lg\lg n}{\lg n}\right) \text{ i.o.} \right\}$$

has $\Gamma(\mathrm{P})$*-measure 0.*

Proof. For clarity we omit floor and ceiling functions.

The Martingale

Consider the following martingale d that starts with initial capital 4. Let L be the language d is betting on. d splits its initial capital capital into portions $C_{i,1}, C_{i,2}, i \in \mathbb{N}$, where $C_{i,1} = C_{i,2} = 1/n^2$. $C_{n,1}$ and $C_{n,2}$ are reserved for betting on strings in $\{0,1\}^n$. For each length n, d only risks $C_{n,1}$ and $C_{n,2}$. Thus, d never runs out of capital to bet on $\{0,1\}^n$ for all $n \in \mathbb{N}$.

Now we describe how d bets on $\{0,1\}^n$ with $C_{n,1}$. d uses $C_{n,1}$ to bet that the first n strings of $\{0,1\}^n$ don't belong to L. If d makes no mistake then the capital $C_{n,1}$ grows from $1/n^2$ to $2^n/n^2$. But once d makes a mistake it loses all of $C_{n,1}$, i.e. $C_{n,1}$ becomes 0.

Next we describe how d bets on $\{0,1\}^n$ with $C_{n,2}$. The martingale d only bets with capital $C_{n,2}$ if it loses $C_{n,1}$, i.e. the martingale d makes a mistake on the first string of length n that belongs to L. Let us call this string w. Let $w_1, w_2, \cdots, w_{n/\lg n}$ be a partition of w into $n/\lg n$ substrings, such that $w = w_1 w_2 \cdots w_{n/\lg n}$ and each w_i has length $\lg n$. Furthermore d splits $C_{n,2}$ into $\binom{\lg n}{2\lg\lg n}\frac{n}{\lg n}$ equal parts, i.e. $n^{1+o(1)}$ many parts. We refer to each of them as $C_{n,2,i}$, for $i \in [1, 2, \cdots, \binom{\lg n}{2\lg\lg n}]$. Each one is reserved for betting according to the prediction of some dimension $2\lg\lg n$ subcube that contains w. We only consider subcubes containing w whose free bits lie completely in one of the w_i's. Let us call these subcubes the boundary subcubes of w. It is easy to see that there are $\binom{\lg n}{2\lg\lg n}\frac{n}{\lg n}$ boundary subcubes of w.

Finally, to completely specify d, we describe how it bets with each $C_{n,2,i}$ on any string $x \in \{0,1\}^n$ that comes after w, the string d lost all of $C_{n,1}$ on. d bets as follows:

for *each boundary subcube* B_i *of* w **do**
  $C_{n,2,i} \leftarrow$ capital reserved for betting on B_i;
  if $x \in B_i$ **then**
    verify that if $y < x$ and $y \in B_i$, then $y \in L$;
    proceed to next B_i if the verification fails;
    bet all of $C_{n,2,i}$ on x being in L;
  end
end

Algorithm 1: How d bests on $x \in \{0,1\}^n$ that comes after w.

Intuitively, each $C_{n,2,i}$ is reserved for betting on a boundary subcube of w. The martingale predicts that each subcube is contained in $L^{=n}$. If the subcube B_i which contains w is really contained in $L^{=n}$, then the capital reserved for betting on this subcube grows from $C_{n,2,i}$ to $2^{2^{2\lg\lg n}-1}C_{n,2,i}$. This follows because we don't make any mistakes while betting on the $2^{2\lg\lg n} - 1$ strings in $B_i \setminus \{w\}$, and each of these bets doubles $C_{n,2,i}$.

The Martingale's Winnings on X

We now show that d succeeds on any $L \in X$ by examining its winnings on $L^{=n}$. In the first case, suppose the first n strings of $\{0,1\}^n$ are all not contained in L. In this case we bet with $C_{n,1}$ and raise this capital from $1/n^2$ to $2^n/n^2$. In the second case, suppose $\mathrm{DNF}_{\mathrm{width}}(L^{=n}) \le n(1 - \frac{2\lg\lg n}{\lg n})$ and one of the first n strings of $\{0,1\}^n$ is in L. Let us denote the first such string by w. In this case d will lose all of $C_{n,1}$ and have to bet with $C_{n,2}$. Since $\mathrm{DNF}_{\mathrm{width}}(L^{=n}) \le n(1 - \frac{2\lg\lg n}{\lg n})$, w must be contained in a subcube of dimension at least $(\frac{2\lg\lg n}{\lg n})n$. By a simple averaging argument it can be seen that there must be at least one boundary subcube of w that has dimension at least $2\lg\lg n$. Since d must bet on such a subcube, its capital reserved for this subcube rises from $C_{n,2,i}$ to $2^{2^{2\lg\lg n}-1}C_{n,2,i} = \Theta(n^{\lg n})$. Since any $L \in X$ satisfies the above two cases infinitely often, d's capital rises by $\Omega(n^{\lg n})$ infinitely often. Thus, d succeeds on X.

The Martingale is a $\Gamma(\mathrm{P})$-Martingale

Now we need to show d is a $\Gamma(\mathrm{P})$-martingale. It is easy to see that d is computable in time polynomial in n. Since for each $x \in \{0,1\}^n$ we bet on, we iterate though $n^{1+o(1)}$ sububes of dimension $2\lg\lg n$, and each subcube contains $O(\lg^2 n)$ points. Also the set of strings that d bets on in $\{0,1\}^n$ is P-printable since it only bets on the $n^{2+o(1)}$ points in the boundary subcubes of the first n strings of length n. □

4 Measure and Nondeterministic Time

The following lemma is a generalization of an observation made in [5].

Lemma 4.1. *If L can be decided by a nondeterministic Turing machine in time $f(n) \le n$, then L has DNF width at most $f(n)$.*

Proof. We will show that for all n, $L^{=n}$ is covered by a DNF of width at most $f(n)$. If $L^{=n} = \emptyset$, then it is covered by the empty DNF which has width 0. All that's left is to show that $L^{=n}$ is covered by subcubes of dimension at least $n - f(n)$ whenever $L^{=n} \ne \emptyset$. This is sufficient because every subcube of dimension at least $n - f(n)$ is covered by a width $f(n)$ term, so L can be covered by a width $f(n)$ DNF. Let M be a nondeterministic Turing machine that decides L in time at most $f(n)$ and $x \in L^{=n}$. Thus, there is a nondeterministic computation of M on input x that accepts. Since M uses at most $f(n)$ time it can only examine at most $f(n)$ bits of x. So there are at least $n - f(n)$ bits of x that aren't examined by M on some accepting computation of M on x. Therefore the set of all strings $y \in \{0,1\}^n$ that agree with x in all the bit positions examined by an accepting computation must also be accepted by the same computation. This set of strings is precisely a subcube of dimension at least $n - f(n)$; therefore, it is covered by a DNF term of width at most $f(n)$. Since $x \in L^{=n}$ was arbitrary, it follow that $L^{=n}$ can be covered by DNF term(s) of width at most $f(n)$; therefore, $L^{=n}$ has DNF width at most $f(n)$. □

Theorem 4.2. *The class of all languages decidable in nondeterministic time at most $n(1 - \frac{2\lg\lg n}{\lg n})$ infinitely often has $\Gamma(\mathrm{P})$-measure 0.*

Proof. By lemma 4.1, any language decidable in nondeterministic time at most $n(1 - \frac{2\lg\lg n}{\lg n})$ has DNF width at most $n(1 - \frac{2\lg\lg n}{\lg n})$ for all but finitely many n. Therefore it follows by theorem 3.1 that the set of all such languages have $\Gamma(\mathrm{P})$-measure 0. □

We now have the main result of the paper:

Corollary 4.3. NTIME $\left[n(1 - \frac{2\lg\lg n}{\lg n})\right]$ *has* $\Gamma(\mathrm{P})$*-measure 0.*

Corollary 4.4. NTIME$[o(n)]$ *has* $\Gamma(\mathrm{P})$*-measure 0.*

Because $\Gamma(\mathrm{P})$ measure 0 implies measure 0 in the other notions of measure on P [13,15], Theorem 4.2 and its corollaries extend to these measures as well.

Corollary 4.5. *The class of all languages decidable in nondeterministic time at most* $n(1 - \frac{2\lg\lg n}{\lg n})$ *infinitely often has* F*-measure 0,* $\Gamma_d(\mathrm{P})$*-measure 0, and* $\Gamma/(\mathrm{P})$*-measure 0.*

A language L has decision tree depth $f(n) : \mathbb{N} \longrightarrow \mathbb{N}$ infinitely often if $\chi_{L^{=n}}$ has decision tree depth at most $f(n)$ for infinitely many n. It is easy to show and well known that a function with decision tree depth k has DNF width at most k. See [14] for the definition of decision tree depth and a proof of the previous statement. Therefore Theorem 4.2 immediately implies the following corollary.

Corollary 4.6. *The set of all languages with decision tree depth at most* $n(1 - \frac{2\lg\lg n}{\lg n})$ *infinitely often has* $\Gamma(\mathrm{P})$*-measure 0.*

References

[1] E. Allender and R. Rubinstein. P-printable sets. *SIAM Journal on Computing*, 17:1193–1202, 1988.

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

[3] Eric Allender and Martin Strauss. Measure on p: Robustness of the notion. In *International Symposium on Mathematical Foundations of Computer Science*, pages 129–138. Springer, 1995.

[4] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. Marcel Dekker, New York, N.Y., 1997.

[5] J. Cai, D. Sivakumar, and M. Strauss. Constant-depth circuits and the Lutz hypothesis. In *Proceedings of the 38th Symposium on Foundations of Computer Science*, pages 595–604. IEEE Computer Society, 1997.

[6] Y. Crama and P. L. Hammer. *Boolean Functions - Theory, Algorithms, and Applications*, volume 142 of *Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, 2011.

[7] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992.

[8] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992.

[9] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–254. Springer-Verlag, 1997.

[10] J. H. Lutz. Dimension in complexity classes. *SIAM Journal on Computing*, 32(5):1236–1259, 2003.

[11] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164(1–2):141–163, 1996.

[12] J. H. Lutz and E. Mayordomo. Twelve problems in resource-bounded measure. *Bulletin of the European Association for Theoretical Computer Science*, 68:64–80, 1999. Also in *Current Trends in Theoretical Computer Science: Entering the 21st Century*, pages 83–101, World Scientific Publishing, 2001.

[13] Philippe Moser. Martingale families and dimension in p. *Theoretical Computer Science*, 400(1-3):46–61, 2008.

[14] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[15] M. Strauss. Measure on P: Strength of the notion. *Information and Computation*, 136(1):1–23, 1997.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il