To the University of Wyoming:

The members of the Committee approve the thesis of Adewale Sekoni presented on 12/10/2014.

Dr. John Hitchcock, Chairperson

Dr. Eric Moorhouse, External Department Member

Dr. Thomas Bailey

Dr. James Caldwell

APPROVED:

Dr. James Caldwell, Head, Department of Computer Science

Dr. Al Rodi, Dean, College of Engineering and Applied Science

Sekoni, Adewale, Polynomial-Space Randomness and DNF Complexity, M.S., Department of Computer Science, December, 2014.

We study the nonuniform complexity of problems decidable in exponential space (ESPACE). Lutz showed that almost every problem in ESPACE has circuit-size complexity $\Omega(2^n/n)$. We investigate the more restrictive model of disjunctive normal form (DNF) complexity. We prove that almost every problem in ESPACE has DNF complexity $\Theta(\frac{2^n}{\lg n \lg\lg n})$. Every pspace-random sequence must have DNF complexity $\Theta(\frac{2^n}{\lg n \lg\lg n})$.

POLYNOMIAL-SPACE RANDOMNESS AND DNF COMPLEXITY

by

Adewale Sekoni, BSc Computer Science

A thesis submitted to the
Department of Computer Science
and the
University of Wyoming
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE
in
COMPUTER SCIENCE

Laramie, Wyoming
December 2014

To my mother Adetoun Sekoni

Contents

Acknowledgments

I would like to thank my adviser Dr. John Hitchcock for the supervision and support he offered me during the research. I would also like to extend my thanks to my committee members Dr. Eric Moorhouse, Dr. Thomas Bailey, Dr. James Caldwell for accepting to be on my committee.

This research was supported in part by NSF grant 0917417 and a University of Wyoming Graduate Mentoring Initiative assistantship.

Adewale Sekoni

University of Wyoming

December 2014

Chapter 1

Introduction

The disjunctive normal form (DNF) complexity of Boolean functions has been extensively studied with many fundamental results obtained. Of particular importance to us is the Korshunov-Kuznetsov theorem [1]. It states that the optimal DNF size for a random Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is

$$(K + o(1))(2n/\lg n \lg\lg n), \text{where } 1 \leq K \leq 1.54169.$$

Nigmatullin showed that for almost all Boolean functions $f : \{0,1\}^n \longrightarrow \{0,1\}$ and $\epsilon > 0$

$$(1-\epsilon)\overline{\ell}(n) \leq \ell(f) \leq (1+\epsilon)\overline{\ell}(n).$$

Here $\ell(f)$ is the number of terms in the smallest DNF that computes f and $\overline{\ell}(n)$ is the average of $\ell(f)$ when f is uniformly selected form the set of all Boolean functions from $\{0,1\}^n$ to $\{0,1\}$. We extend the knowledge of DNF complexity to the resource-bounded measure framework. Similar work has been carried out by Lutz [2], in the more general setting of circuit-size complexity.

Circuit-size complexity has also been extensively studied. Shannon [3] showed that every Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ can be computed by a circuit of size $O(2^n/n)$. Lupanov [4] showed that every Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is computed by a circuit of size $(2^n/n)(1 + O(1/\sqrt{n}))$. Using resource-bounded measure Lutz [2] showed that almost every language in exponential space has circuit-size complexity $\Omega(2^n/n)$. We show

that the DNF complexity of almost every language is within a constant factor of the average DNF complexity of a random Boolean function. We prove that all pspace-random languages have DNF complexity $\Theta(\frac{2^n}{\lg n \lg\lg n})$.

Using infinite binary strings to represent languages, we prove our main result by establishing a lower bound on space-bounded Kolmogorov complexity of languages with nonuniform DNF complexity $\Theta(\frac{2^n}{\lg n \lg\lg n})$. A language L has nonuniform DNF complexity $NDC : \mathbb{N} \longrightarrow \mathbb{R}$, if for all but finite n we can construct a DNF formula of size $\leq NDC(n)$ such that $s \in L \cap \{0,1\}^n \iff \gamma(s) = 1$.

A major component of our proof is bounding the probability that the DNF complexity of a random function deviates from $\Theta(\frac{2^n}{\lg n \lg\lg n})$. We do this by considering two cases for some parameter $k \in \mathbb{N}$. The first case is that a random function has a subcube of dimension k and the second case is that it doesn't have any subcube of dimension k and has size $\Theta(\frac{2^n}{\lg n \lg\lg n})$. Both probabilities are inversely related so we need to choose k in such a way that both events have a "small enough" probability. For instance in the proof of R. G. Nigmatullin's theorem in [5], $\lceil 2 \lg n \rceil$ is chosen for k. But this value doesn't work for our purposes and leads to a probability bound on the first case that is too big. We show that choosing k to be ϵn for small enough ϵ leads to a better probability for the first case and doesn't make the second case too bad.

1.1 Preliminaries

The set of all binary strings is $\{0,1\}^*$. The length of a string $x \in \{0,1\}^*$ is $|x|$. The empty string is denoted as λ. For $n \in \mathbb{N}$, $\{0,1\}^n$ is the set of strings of length n and $\{0,1\}^{\leq n}$ is the set of strings of length at most n. We write $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, ...$ for the standard lexicographic enumeration of $\{0,1\}^*$.

A *language* is a subset $L \subseteq \{0,1\}^*$. We write $L_{=n} = L \cap \{0,1\}^n$ and $L_{\leq n} = L \cap \{0,1\}^{\leq n}$. 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 can also index χ_L with strings as in $\chi_L[s_i] = \chi_L[i]$ for $i \in \mathbb{N}$. $\chi_L[i,j]$ denotes the i^{th} through j^{th} bits of χ_F inclusive while $\chi_{L_{=n}}$ denotes $\chi_L[2^n-1, 2^{n+1}-2]$, i.e. the substring of χ_L corresponding to the strings in $L_{=n}$.

We say that a statement $P(n)$ holds almost everywhere if it is true for all but finitely many $n \in \mathbb{N}$. It is denoted by $P(n)$ *a.e.* Similarly we write $P(n)$ *i.o.* to say that $P(n)$ holds for infinitely many n.

1.2 Boolean Functions

A Boolean function is any $f : \{0,1\}^n \longrightarrow \{0,1\}$. Associated with any Boolean function is its characteristic sequence $\chi_f \in \{0,1\}^{2^n}$ defined as

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

equivalently

$$\chi_f = f(s_{2^n-1})f(s_{2^n}) \dots f(s_{2^{n+1}-2})$$

Besides its characteristic sequence a Boolean function can be represented in other ways. In this paper we also represent them in *disjunctive normal form* (DNF). A DNF representation is the *disjunction* (logical **OR**) of zero or more terms; a term is the *conjunction* (logical **AND**) of zero or more literals; a literal is either a Boolean variable or its negation (logical **NOT**). Given a Boolean function f we use D_f to denote a DNF representation of f and $size(D_f)$ for the number of terms in D_f. We write $\ell(f)$ or $\ell(\chi_f)$ for

$$min\{size(D) | D \text{ is a DNF representation of } f\},$$

$\overline{\ell}(n)$ for

$$E[\ell(f)].$$

In the second definition the expectation is taken over the random uniform selection from the set of all Boolean functions from $\{0,1\}^n$ to $\{0,1\}$. Thus $\overline{\ell}(n)$ is the average DNF complexity of a random Boolean function on n variables.

The *DNF-size* complexity of a language L is the function

$$DS_L : \mathbb{N} \longrightarrow \mathbb{N}$$
$$DS_L(n) = \ell(\chi_{L=n}).$$

I.e. $DS_L(n)$ is the size of the smallest DNF whose characteristic sequence is $\chi_{L=n}$.
Similarly, we can define the DNF complexity DS_x for $x \in \{0,1\}^\infty$

$$DS_x : \mathbb{N} \longrightarrow \mathbb{N}$$
$$DS_x(n) = DS_L(n),$$

where L is the language whose characteristic sequence is x.

1.2.1 Hypercube

An n-cube is an undirected graph whose vertex set is $\{0,1\}^n$ and has an edge between any two vertices that differ in one bit position. Sometimes we view a Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ as a covering the n-cube. We say f covers some vertex set S of an n-cube if $S = f^{-1}(1)$. Given an n-cube we refer to its subgraphs that are also k-cubes for $k \in \{0,1,\cdots,n\}$ as subcubes. It is easy to see that every subcube corresponds to some term, i.e it is covered by a term.

1.3 Resource-Bounded Measure

A set $X \subseteq \{0,1\}^\infty$ has pspace measure zero, denoted by $\mu_{\text{pspace}}(X) = 0$, if there is a pspace-computable martingale that attains arbitrarily large values on it. X has measure one if it is the complement of a measure zero set. Similarly we say that X has measure zero in ESPACE, denoted by $\mu(X|\text{ESPACE}) = 0$, if there is a pspace-computable martingale that attains arbitrarily large values on $X \cap \text{ESPACE}$. X has measure one in ESPACE if its complement has measure zero in ESPACE. We say $x \in \{0,1\}^\infty$ is pspace-random if there is no pspace-computable martingale that attains arbitrarily large values on it. We do not go into the full definition of pspace measure as Theorem 1.1 suffices for our purpose. For a review of resource-bounded measure see [2].

1.4 Space-Bounded Kolmogorov Complexity

Given a Turing machine M and "program" $\pi \in \{0,1\}^*$ for M we say that "$M(\pi, n) = w$ in $\leq s$ space" if M, on input (π, n), outputs the string $w \in \{0,1\}^*$ and halts without using more than s cells of workspace. We are only interested in the situation where the output has the from $\chi_{L_{=n}}$, i.e., the characteristic sequence of $L_{=n}$, for some language L.

Given a Turing machine M, a space bound $s : \mathbb{N} \longrightarrow \mathbb{N}$, a language L, and a natural number n, the $s(n)$-*space-bounded Kolmogorov complexity* of $L_{=n}$ relative to M is

$$KS_M^{s(n)}(L_{=n}) = min\{|\pi| \ | M(\pi, n) = \chi_{L_{=n}} in \leq s(n) \text{ space}\}$$

Intuitively $KS_M^{s(n)}(L_{=n})$ is the length of the shortest program that causes the Turing machine M to halt with output $\chi_{L_{=n}}$ in $\leq s(n)$ space. Using standard efficient simulation techniques we can show that there is a universal machine U such that for each machine M there is a constant c such that for all s, L and n, we have

$$KS_U^{c.s(n)+c}(L_{=n}) \leq KS_M^{s(n)}(L_{=n}) + c.$$

Henceforth we fix such a Turing machine U and omit it from the notation.

Theorem 1.1. *Lutz [6] Let $c \in \mathbb{N}$ and $\epsilon > 0$.*
If

$$X = \{L \subseteq \{0,1\}^* | \ KS^{2^{cn}}(L_{=n}) > 2^n - 2^{\epsilon n} \ a.e.\},$$

then $\mu_{pspace}(X) = \mu(X|\text{ESPACE}) = 1$.

Chapter 2

Resource-Bounded Measure of Nonuniform DNF complexity of Languages

In this section we prove our main result and its corollary:

Theorem 2.1. *The set of all $x \in \{0,1\}^\infty$ such that $DS_x(n) = \Theta(\frac{2^n}{\lg n \lg\lg n})$ has pspace-measure 1 and measure 1 in ESPACE.*

Corollary 2.2. *Every pspace-random language has DNF complexity $\Theta(\frac{2^n}{\lg n \lg\lg n})$*

We treat n/k where $n, k \in \mathbb{N}$ as integers. We don't include floors or ceilings because they don't affect our results but make things messy. We make use of the following bound

$$\binom{n}{n/k} \leq 2^{nH(1/k)}, \text{where } H(\alpha) = \alpha \lg \frac{1}{\alpha} + (1-\alpha) \lg \frac{1}{1-\alpha}.$$

Analogous to $\ell(f)$ and $\overline{\ell}(n)$ we define $\ell_k^+(f)$ and $\overline{\ell_k^+}(n)$, where k is a positive integer. $\ell_k^+(f)$ denotes the size of the smallest DNF computing f in which no term has as few as $\frac{k-1}{k}n$ literals. $\overline{\ell_k^+}(n)$ denotes the expectation of $\ell_k^+(f)$ over the uniform random distribution on Boolean functions from $\{0,1\}^n$ to $\{0,1\}$.

What follows are six claims that build up to our main result. The first claim establishes an upper bound on the probability that the augmented DNF size $\overline{\ell_k^+}(f)$ of a random Boolean function f deviates from its average $\overline{\ell_k^+}(n)$.

The proof of the following claim is based on the proof of Theorem 2.1 in [5].

Claim 2.1. *$Pr[|\ell_k^+(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n}] \leq 2\exp(-2^{n/6})$ for sufficiently large k.*

Proof. A sequence $X_0, X_1, \cdots$ of random variables is a martingale with respect to the sequence $Z_0, Z_1, \cdots$ if, for all $n \geq 0$, the following conditions hold:

- X_n is a function of $Z_0, Z_1, \cdots, Z_n$;
- $E[|X_n|] < \infty$;
- $E[X_{n+1}|Z_0, \cdots, Z_n] = X_n$.

A *Doob martingale* is a martingale constructed in the following way. Let $Z_0, Z_1, \cdots, Z_n$ be a sequence of random variables, and let Y be a random variable with $E[|Y|] < \infty$. Then

$$X_i = E[Y|Z_0, \cdots, Z_i], \quad i = 0, 1, \cdots, n$$

gives a martingale with respect to $Z_0, Z_1, \cdots, Z_n$. [7]

Azuma's inequality [8] states that if $0 = X_0, X_1, \cdots, X_N$ is a martingale with respect to the sequence $Z_0, Z_1, \cdots, Z_N$ and if $|X_{i+1} - X_i| \leq C \neq 0$ for $0 \leq i \leq N-1$, then

$$Pr[|X_N| > \lambda] \leq 2\exp\left(\frac{-\lambda^2}{2C^2N}\right).$$

We now construct a *Doob martingale* as follows. Let $N = 2^n$, and let $s_1, s_2, \cdots, s_{2^n}$ be the strings of $\{0,1\}^n$, in some arbitrary order. Let $X_i = Y_i - \overline{\ell_k^+}(n)$ where Y_i is the expectation of $\overline{\ell_k^+}(f)$ conditioned on the values of f on the strings $s_1, s_2, \cdots, s_i$. It is easy to see that $X_0 = 0$ and $X_N = \overline{\ell_k^+}(f) - \overline{\ell_k^+}(n)$. We choose C to be the maximum of $|\overline{\ell_k^+}(f) - \overline{\ell_k^+}(g)|$ over all Boolean functions f and g that differ only on a single string in $\{0,1\}^n$. If we flip the bit of a Boolean function on some string from a 0 to 1, then the resulting function has at most one more term in its shortest DNF formula than the original formula. On the other hand if we flip from 1 to 0 then we may have to add more terms. For sufficiently large k the changed string can lie in at most $\binom{n}{(n/k)-1}$ terms in any shortest disjunctive normal form in which no term has as few as $\frac{k-1}{k}n$ literals. Each of these terms can be replaced by $(n/k) - 1$ terms that cover all the strings of the original term with the exception of the string whose value

was changed to 0. Thus the number of terms added is at most $\frac{n-k}{k}\binom{n}{(n/k)-1} \leq 2^{nH(1/k)+\lg\frac{n-k}{k}}$. Now we apply Azuma's inequality with $N = 2^n$, $\lambda = 2^{2n/3}$ and $C = 2^{n/12}$ by choosing k sufficiently large. We get

$$Pr[|\ell_k^+(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n}] \leq 2\exp(-2^{n/6}), \text{ for sufficiently large } k.$$

□

The following claim shows that substituting DNF size $\ell(f)$ for the augmented DNF size $\overline{\ell_k^+}(f)$ doesn't significantly change the probability bound of the previous claim.

Claim 2.2. *For sufficiently large k and $\epsilon(k) > 0$,*

$$Pr[|\ell(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n}] \leq 2^{-2^{\epsilon(k)n}} \ a.e$$

Proof. Since $\overline{\ell_k^+}(f) = \ell(f)$, unless f covers a subcube of dimension n/k we see that

$$Pr[\overline{\ell_k^+}(f) \neq \ell(f)] \leq Pr[f \text{covers a subcube of dimension } n/k].$$

The probability that a random Boolean function has a particular subcube of dimensions n/k is $2^{-2^{n/k}}$. There are $\binom{n}{n/k}2^{\frac{k-1}{k}n}$ subcubes of dimension n/k. By the union bound the probability that a random Boolean function has a subcube of dimension n/k is at most

$$2^{-2^{n/k}}\binom{n}{n/k}2^{\frac{k-1}{k}n} \leq 2^{-2^{n/k}+n(H(1/k)+\frac{k-1}{k})}.$$

Hence

$$\begin{aligned}
Pr[|\ell(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n}] &= Pr[|\ell(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n} \wedge \ell(f) = \ell_k^+(f)] + \\
&\quad Pr[|\ell(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n} \wedge \ell(f) \neq \ell_k^+(f)] \\
&= Pr[|\ell_k^+(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n} \wedge \ell(f) = \ell_k^+(f)] + \\
&\quad Pr[|\ell(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n} \wedge \ell(f) \neq \ell_k^+(f)] \\
&\leq Pr[|\ell_k^+(f) - \overline{\ell_k^+}(n)| > 2^{\frac{2}{3}n}] \ + \ Pr[\ell(f) \neq \ell_k^+(f)] \\
&\leq 2\exp(-2^{n/6}) + 2^{-2^{n/k}+n} \ \text{ a.e, for sufficiently large } k \\
&\leq 2^{-2^{\epsilon(k)n}} \ \text{ a.e, for sufficiently large } k \text{ and } \epsilon(k) = \frac{1}{2k}.
\end{aligned}$$

From here onwards we set k to k_0 and ϵ to $\epsilon(k_0)$ such that

$$Pr[|\ell(f) - \overline{\ell^+_{k_0}}(n)| > 2^{\frac{2}{3}n}] \leq 2^{-2^{\epsilon n}} \text{ a.e.}$$

□

Using the previous probability bound, the next claim establishes an upper bound on the number of Boolean functions $f : \{0,1\} \longrightarrow \{0,1\}$ that deviate a "little" from $\overline{\ell^+_{k_0}}(n)$. This bound will be used in computing an upper bound on the space-bounded Kolmogorov complexity of

$$\{x \in \{0,1\}^\infty | \ |DS_x(n) - \overline{\ell^+_{k_0}}(n)| > 2^{\frac{2}{3}n} \ i.o.\}$$

in Claim 2.5.

Claim 2.3. *The number of Boolean functions $f : \{0,1\}^n \longrightarrow \{0,1\}$ such that $|\ell(f) - \overline{\ell^+_{k_0}}(n)| > 2^{\frac{2}{3}n}$ is at most $2^{2^n - 2^{\epsilon n}}$ for sufficiently large n.*

Proof. This follows directly from Claim 2.1. Since the probability distribution we used on the 2^{2^n} Boolean functions is the uniform distribution, there are at most $2^{2^n - 2^{\epsilon n}}$ such functions. □

Now we present two algorithms that will be used in Claim 2.5 to bound the space-bounded Kolmogorov complexity of the languages in

$$\{x \in \{0,1\}^\infty | \ |DS_x(n) - \overline{\ell^+_{k_0}}(n)| > 2^{\frac{2}{3}n} \ i.o.\}.$$

Consider the following algorithms, the first computes $\overline{\ell^+_{k_0}}(n)$ and the second takes in two non-negative integer arguments i, n and outputs χ_f. Here χ_f is the characteristic string of the i^{th} Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ with size $\ell(f)$ such that $|\ell(f) - \overline{\ell^+_{k_0}}(n)| \leq 2^{\frac{2}{3}n}$.

Algorithm 1.

Input: n

Output: $\overline{\ell^+_{k_0}}(n)$

$total = 0$

for all *Boolean function* $f : \{0,1\}^n \longrightarrow \{0,1\}$ ***do***

  $min = 2^n$

  for all *DNF formulae* D *with no subcube of dimension* n/k *and size* $\leq 2^n$ ***do***

    if D *computes* f ***then***

      $min = minimum\{min, size(D)\}$

    end if

  end for

  $total = total + min$

end for

$\overline{\ell^+_{k_0}}(n) = total/2^{2^n}$

return $\overline{\ell^+_{k_0}}(n)$

Algorithm 2.

1: *Input:* i, n
2: *Output:* χ_f *where* f *is the* i^{th} *Boolean function with* n *arguments such that* $|\ell(f) - \overline{\ell^+_{k_0}}(n)| \leq 2^{\frac{2}{3}n}$
3: *compute* $\overline{\ell^+_{k_0}}(n)$
4: $count = 0$
5: ***for all*** *Boolean function* $f : \{0,1\}^n \longrightarrow \{0,1\}$ ***do***
6: $min = 2^n$
7: ***for all*** *DNF formala* D *with size* $\leq 2^n$ ***do***
8: ***if*** D *computes* f ***then***
9: $min = minimum\{min, size(D)\}$
10: ***end if***
11: ***end for***
12: ***if*** $|min - \overline{\ell^+_{k_0}}(n)| > 2^{\frac{2}{3}n}$ ***then***
13: $count = count + 1$
14: ***end if***
15: ***if*** $count = i$ ***then***
16: ***return*** χ_f
17: ***end if***
18: ***end for***

Claim 2.4. *Algorithm 1 and Algorithm 2 use space polynomial in* 2^n.

Proof. Because of the similarity of both algorithms we'll only consider algorithm 1.
The for-loop of line 4 iterates for exactly 2^{2^n} times thus we need 2^n bits to implement its counter. The inner for-loop of line 6 iterates for at most 2^{3^n} times since there are 3^n possible terms which occurs at most once in any DNF formula. Therefore this loop requires at most 2^{nlg3} bits to implement its counter. The predicate $D\ computes f$ of line 8 can also be easily

implement in space polynomial in 2^n. The variables $total, min, \overline{\ell_{k_0}^+}(n)$ are bounded above by $2^n * 2^{2^n}$ and thus each uses at most $2^n + n$ bits.

□

Claim 2.5. *Let* $X = \{x \in \{0,1\}^\infty |\ |DS_x(n) - \overline{\ell_{k_0}^+}(n)| > 2^{\frac{2}{3}n}\ i.o.\}$. *Then there is a constant* $c_0 > 0$ *such that for all* $x \in X$,

$$KS^{2^{cn}}(L_{=n}) \leq 2^n - 2^{\epsilon n} + c_0 \quad i.o., \text{ where } \chi_L = x.$$

Proof. Given $x \in X$ let f be the Boolean function associated with the characteristic sequence $x[length\ n]$ and L be the language whose characteristic sequence is x. Claim 2.3 tells us that for sufficiently large n there are at most $2^{2^n - 2^{\epsilon n}}$ Boolean functions $f : \{0,1\}^n \longrightarrow \{0,1\}$ such that $|\ell(f) - \overline{\ell_{k_0}^+}(n)| > 2^{\frac{2}{3}n}$. Since by definition $\ell(f) = DS_x(n)$, there exists a positive $i \leq 2^{2^n - 2^{\epsilon n}}$ such that Algorithm 2 outputs $x[length\ n]$. Since we need at most $2^n - 2^{\epsilon n}$ bits to represent i and Algorithm 2 uses at most 2^{cn} space, for some constant c, the definition of space-bounded Kolmogorov complexity implies that $KS^{2^{cn}}(L_{=n}) \leq 2^n - 2^{\epsilon n}$ i.o. here c_0 is the length of the string used to encode a universal Turing machine. □

The following claim is a minor extension of results proved by Pippenger [5]. It shows that $\overline{\ell_k^+}(n) \approx \ell(n) = \Theta(\frac{2^n}{\lg n \lg\lg n})$.

Claim 2.6. $\overline{\ell_k^+}(n) = \Theta(\frac{2^n}{\lg n \lg\lg n})$.

Proof.

$$(1 + o(1))\frac{2^n}{\lg n \lg\lg n} \leq \overline{\ell}(n) \tag{2.1}$$

$$\overline{\ell}(n) \leq (1 + o(1))\frac{2^{n+1}}{\lg n \lg\lg n} \tag{2.2}$$

(2.1) and (2.2) are due to Kuznetsov and Pippenger respectively [5].

We make use of the following observations:

$\overline{\ell_k^+}(f) = \ell(f)$, unless f covers a subcube of dimension n/k.

$\ell(f) \leq \overline{\ell_k^+}(f)$

$\overline{\ell_k^+}(f) - \ell(f) \leq |\{x \in \{0,1\}^n | x \text{ is contained in a subcube of dimension } n/k \text{ covered by } f\}|$

$E[\overline{\ell_k^+}(f) - \ell(f)] \leq \binom{n}{n/k} 2^{(\frac{k-1}{k})n} 2^{-2^{n/k}} 2^{n/k} \leq 2^{-2^{n/k} + (H(1/k)+1)n}$

The last inequality follows because there are $\binom{n}{n/k}2^{(\frac{k-1}{k})n}$ subcubes of dimension n/k. Each dimension n/k cube is included with probability $2^{-2^{n/k}}$ and contains $2^{n/k}$ points. By the linearity of expectations we also see that $\overline{\ell_k^+}(n) \leq \overline{\ell}(n) + 2^{-2^{n/k}+(H(1/k)+1)n}$. The second observation implies that $\overline{\ell_k^+}(n) \geq \overline{\ell}(n)$. Thus $\overline{\ell_k^+}(n)$ is arbitrarily close to $\overline{\ell}(n)$. Therefore $\overline{\ell_k^+}(n) = \Theta(\frac{2^n}{\lg n \lg\lg n})$. □

We now bring everything together using Claim 2.5 & 2.6 and Theorem 1.1 to show that

$$\{x \in \{0,1\}^\infty | DS_x = \Theta(\frac{2^n}{\lg n \lg\lg n})\}$$

is a measure 1 set by showing that it is a superset of a measure 1 set.

Theorem 2.1. *The set of all $x \in \{0,1\}^\infty$ such that $DS_x(n) = \Theta(\frac{2^n}{\lg n \lg\lg n})$ a.e. has pspace-measure 1 and measure 1 in ESPACE.*

Proof. It follows from claim 2.5 that

$$\begin{aligned} X &= \{x \in \{0,1\}^\infty |\ |DS_x(n) - \overline{\ell_{k_0}^+}(n)| > 2^{\frac{2}{3}n}\ i.o.\} \\ &\subseteq \{x \in \{0,1\}^\infty |\ \left(KS^{2^{cn}}(L_{=n}) \leq 2^n - 2^{\epsilon n} + c_0\ \text{ i.o.}\right) \wedge (\chi_L = x)\} \\ \implies & \\ X^c &= \{x \in \{0,1\}^\infty |\ |DS_x(n) - \overline{\ell_{k_0}^+}(n)| \leq 2^{\frac{2}{3}n}\ a.e.\} \\ &\supseteq \{x \in \{0,1\}^\infty |\ (KS^{2^{cn}}(L_{=n}) > 2^n - 2^{\epsilon n} + c_0\ \text{ a.e.}) \wedge (\chi_L = x)\} \end{aligned}$$

Theorem 1.1 tells us that

$$\{x \in \{0,1\}^\infty |\ (KS^{2^{cn}}(L_{=n}) > 2^n - 2^{\epsilon n} + c_0\ \text{ a.e.}) \wedge (\chi_L = x)\}$$

has pspace-measure 1 and hence measure one in ESPACE. Since X^c is a superset of a pspace-measure 1 set, it follows that $\mu_{\text{pspace}}(X^c) = \mu(X^c|\text{ESPACE}) = 1$.
Similarly since $Y = \{x \in \{0,1\}^\infty | DS_x = \Theta(\frac{2^n}{\lg n \lg\lg n})\}$ is a superset of X^c. Therefore, it follows that
$\mu_{\text{pspace}}(Y) = \mu(Y|\text{ESPACE}) = 1$. □

References

[1] E. Blais and L.-Y. Tan, "Approximating boolean functions with depth-2 circuits," *Electronic Colloquium on Computational Complexity*, 2013. [Online]. Available: http://eccc.hpi-web.de/report/2013/051/

[2] J. H. Lutz, "Almost everywhere high nonuniform complexity," *jcss*, vol. 44, no. 2, pp. 220–258, 1992.

[3] C. E. Shannon, "The synthesis of two-terminal switching circuits," *Bell System Technical Journal*, vol. 28, no. 1, pp. 59–98, 1949.

[4] O. B. Lupanov, "On the synthesis of contact networks," *Doklady Akademii Nauk SSSR*, vol. 119, no. 1, pp. 23–26, 1958.

[5] N. Pippenger, "The shortest disjunctive normal form of a random boolean function," *Random Structures & Algorithms*, pp. 161–186, 2003. [Online]. Available: http://dx.doi.org/10.1002/rsa.10065

[6] D. W. Juedes and J. H. Lutz, "Completeness and weak completeness under polynomial-size circuits," *Information and Computation*, vol. 125, no. 1, pp. 13–31, 1996.

[7] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. New York, NY, USA: Cambridge University Press, 2005.

[8] F. Chung and L. Lu, "Concentration inequalities and martingale inequalities: a survey," *Internet Mathematics*, vol. 3, no. 1, pp. 79–127, 2006. [Online]. Available: http://projecteuclid.org/euclid.im/1175266369