Information and Computation 222 (2013) 80–92

Contents lists available at SciVerse ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Limits on the computational power of random strings

Eric Allender [a], Luke Friedman [a], William Gasarch [b,*]

[a] Dept. of Computer Science, Rutgers University, New Brunswick, NJ 08855, USA
[b] Dept. of Computer Science, University of Maryland, College Park, MD 20742, USA

ARTICLE INFO

Article history:
Available online 26 October 2012

Keywords:
Kolmogorov complexity
Prefix complexity
Uniform derandomization
Complexity classes

ABSTRACT

How powerful is the set of random strings? What can one say about a set A that is efficiently reducible to R, the set of Kolmogorov-random strings? We present the first *upper bound* on the class of computable sets in P^R and NP^R.

The two most widely-studied notions of Kolmogorov complexity are the "plain" complexity $C(x)$ and "prefix" complexity $K(x)$; this gives rise to two common ways to define the set of random strings "R": R_C and R_K. (Of course, each different choice of universal Turing machine U in the definition of C and K yields another variant R_{C_U} or R_{K_U}.) Previous work on the power of "R" (for *any* of these variants) has shown:

- $\mathrm{BPP} \subseteq \{A\colon\ A \leqslant_{tt}^{\mathrm{p}} R\}$.
- $\mathrm{PSPACE} \subseteq \mathrm{P}^R$.
- $\mathrm{NEXP} \subseteq \mathrm{NP}^R$.

Since these inclusions hold irrespective of low-level details of how "R" is defined, and since BPP, PSPACE and NEXP are all in Δ_1^0 (the class of decidable languages), we have, e.g.: $\mathrm{NEXP} \subseteq \Delta_1^0 \cap \bigcap_U \mathrm{NP}^{R_{K_U}}$.

Our main contribution is to present the first upper bounds on the complexity of sets that are efficiently reducible to R_{K_U}. We show:

- $\mathrm{BPP} \subseteq \Delta_1^0 \cap \bigcap_U \{A\colon\ A \leqslant_{tt}^{\mathrm{p}} R_{K_U}\} \subseteq \mathrm{PSPACE}$.
- $\mathrm{NEXP} \subseteq \Delta_1^0 \cap \bigcap_U \mathrm{NP}^{R_{K_U}} \subseteq \mathrm{EXPSPACE}$.

Hence, in particular, PSPACE is sandwiched between the class of sets polynomial-time Turing- and truth-table-reducible to R.

As a side-product, we obtain new insight into the limits of techniques for derandomization from uniform hardness assumptions.

1. Introduction

In this paper, we take a significant step toward providing characterizations of some important complexity classes in terms of efficient reductions to *noncomputable* sets. Along the way, we obtain new insight into the limits of techniques for derandomization from uniform hardness assumptions.

Our attention will focus on the set of Kolmogorov random strings:

* Corresponding author. Fax: +1 301 405 6707.
E-mail addresses: allender@cs.rutgers.edu (E. Allender), lbfried@cs.rutgers.edu (L. Friedman), gasarch@cs.umd.edu (W. Gasarch).

0890-5401/$ – see front matter
http://dx.doi.org/10.1016/j.ic.2011.09.008

Definition 1. Let $K(x)$ be the prefix Kolmogorov complexity of the string x. Then

$$R_K = \{x\colon\ K(x) \geqslant |x|\}.$$

(More complete definitions of Kolmogorov complexity can be found in Section 2. Each universal prefix Turing machine U gives rise to a slightly different measure K_U, and hence to various closely-related sets R_{K_U}.)

The first steps toward characterizing complexity classes in terms of efficient reductions to R_K came in the form of the following curious inclusions:

Theorem 2. *The following inclusions hold*:

- $\mathrm{BPP} \subseteq \{A\colon\ A \leqslant^{\mathrm{p}}_{tt} R_K\}$ [11].
- $\mathrm{PSPACE} \subseteq \mathrm{P}^{R_K}$ [2].
- $\mathrm{NEXP} \subseteq \mathrm{NP}^{R_K}$ [1].

We call these inclusions "curious" because the upper bounds that they provide for the complexity of problems in BPP, PSPACE and NEXP are not even computable; thus at first glance these inclusions may seem either trivial or nonsensical.

A key step toward understanding these inclusions in terms of standard complexity classes is to invoke one of the guiding principles in the study of Kolmogorov complexity: The choice of universal machine should be irrelevant. Theorem 2 actually shows that problems in certain complexity classes are *always* reducible to R_K, no matter *which* universal machine is used to define $K(x)$. That is, combining this insight with the fact that BPP, PSPACE, and NEXP are all contained in Δ^0_1 (the class of decidable languages), we have:

- $\mathrm{BPP} \subseteq \Delta^0_1 \cap \bigcap_U \{A\colon\ A \leqslant^{\mathrm{p}}_{tt} R_{K_U}\}$.
- $\mathrm{PSPACE} \subseteq \Delta^0_1 \cap \bigcap_U \mathrm{P}^{R_{K_U}}$.
- $\mathrm{NEXP} \subseteq \Delta^0_1 \cap \bigcap_U \mathrm{NP}^{R_{K_U}}$.

The question arises as to how powerful the set $\Delta^0_1 \cap \bigcap_U \{A\colon\ A \leqslant_r R_{K_U}\}$ is, for various notions of reducibility $\leqslant_r$. Until now, no computable upper bound was known for the complexity of any of these classes. (Earlier work [1] did give an upper bound for a related class defined in terms of a very restrictive notion of reducibility: $\leqslant^{\mathrm{p}}_{dtt}$ reductions – but this only provided a characterization of P in terms of a class of polynomial-time reductions, which is much less compelling than giving a characterization where the set R_K is actually providing some useful computational power.)

Our main results show that the class of problems reducible to R_K in this way *does* have bounded complexity; hence it is at least plausible to conjecture that some complexity classes can be characterized in this way:

Main results.

- $\Delta^0_1 \cap \bigcap_U \{A\colon\ A \leqslant^{\mathrm{p}}_{tt} R_{K_U}\} \subseteq \mathrm{PSPACE}$.
- $\Delta^0_1 \cap \bigcap_U \mathrm{NP}^{R_{K_U}} \subseteq \mathrm{EXPSPACE}$.

A stronger inclusion is possible for "monotone" truth-table reductions ($\leqslant^{\mathrm{p}}_{mtt}$). We show that:

- $\Delta^0_1 \cap \bigcap_U \{A\colon\ A \leqslant^{\mathrm{p}}_{mtt} R_{K_U}\} \subseteq \mathrm{coNP} \cap \mathrm{P/poly}$.

Combining our results with Theorem 2 we now have:

- $\mathrm{BPP} \subseteq \Delta^0_1 \cap \bigcap_U \{A\colon\ A \leqslant^{\mathrm{p}}_{tt} R_{K_U}\} \subseteq \mathrm{PSPACE} \subseteq \Delta^0_1 \cap \bigcap_U \mathrm{P}^{R_{K_U}}$.
- $\mathrm{NEXP} \subseteq \Delta^0_1 \cap \bigcap_U \mathrm{NP}^{R_{K_U}} \subseteq \mathrm{EXPSPACE}$.

In particular, note that PSPACE is sandwiched in between the classes of computable problems that are reducible to R_K via polynomial-time truth-table and Turing reductions.

Our results bear a superficial resemblance to results of Book et al. [8–10], who also studied decidable sets that are reducible in some sense to algorithmically random sets. However, there is really not much similarity at all. Book et al. studied the class **ALMOST-R**:

Definition 3. Let **R** be a reducibility (e.g., $\leqslant^p_m$ or $\leqslant^p_T$). Then **ALMOST-R** is the class of all B such that $\{A\colon\ B$ is **R**-reducible to $A\}$ has measure 1.

Book et al. showed that **ALMOST-R** can be characterized as the class of decidable sets that are **R**-reducible to sets whose characteristic sequences are (for example) Martin-Löf random. Thus using such sets as oracles is roughly the same