Kolmogorov Complexity Characterizes Statistical Zero Knowledge

Eric Allender
Rutgers University, NJ, USA

Shuichi Hirahara
National Institute of Informatics, Japan

Harsha Tirumala
Rutgers University, NJ, USA

Abstract
We show that a decidable promise problem has a non-interactive statistical zero-knowledge proof system if and only if it is randomly reducible to a promise problem for Kolmogorov-random strings, with a superlogarithmic additive approximation term. This extends recent work by Saks and Santhanam (CCC 2022). We build on this to give new characterizations of Statistical Zero Knowledge $\text{SZK}$, as well as the related classes $\text{NISZKL}$ and $\text{SZKL}$.

2012 ACM Subject Classification Complexity Classes; Problems, reductions and completeness; Circuit complexity

Keywords and phrases Kolmogorov Complexity, Interactive Proofs

Funding Eric Allender: Supported in part by NSF Grants CCF-1909216 and CCF-1909683.
Shuichi Hirahara: Supported in part by JST, PRESTO Grant Number JPMJPR2024, Japan
Harsha Tirumala: Supported in part by NSF Grants CCF-1909216 and CCF-1909683.

1 Introduction

In this paper, we give the first non-trivial characterization of a computational complexity class in terms of reducibility to the Kolmogorov random strings.

Some readers may be surprised that this is possible. After all, the set of Kolmogorov random strings is undecidable, and undecidable sets typically do not figure prominently in complexity-theoretic investigations. But what does it mean to be reducible to the Kolmogorov-random strings? Let us consider the prefix-free Kolmogorov complexity $K$ (which is one of the most-studied types of Kolmogorov complexity), and recall that different universal Turing machines $U$ give a slightly different Kolmogorov measure $K_U$. Then if we say “$A$ is reducible to the $K$-random strings” we probably mean that $A$ is reducible to the $K_U$ random strings, no matter which universal machine $U$ we are using. But it turns out that the class of languages that can be solved in polynomial time with an oracle that returns $K_U(q)$ for any query $q$—regardless of which universal machine $U$ is used—is a complexity class that contains $\text{NEXP}$ and lies in $\text{EXPSPACE}$ [23, 13, 29]. There has been substantial interest in obtaining a precise understanding of which problems can be reduced in this way to the Kolmogorov complexity function under different notions of reducibility [2, 3, 9, 7, 8, 12, 13, 14, 20, 23, 30, 29, 32, 33, 46], but until now, no previously studied complexity class has been characterized in this way, with the exception of $\text{P}$ [8, 46]. (The

---

1 We do wish to highlight the recent work of Ilango, Ren, and Santhanam [37], who related the existence of one-way functions to the average case complexity of computing Kolmogorov complexity.

2 More specifically, it is shown in [13] that all decidable sets with this property lie in $\text{EXPSPACE}$, and it is shown in [23] that there are no undecidable sets with this property. Hirahara shows in [30] that every set in $\text{ExpNP}$ (and hence in $\text{NEXP}$) has this property.
characterizations of $P$ obtained in this way can be viewed as showing that certain limited polynomial-time reductions are useless when using the Kolmogorov complexity function as an oracle.)

Faced with this lack of success, it was proposed in [3, Open Question 4.8] that a more successful approach might be to consider reductions to approximations to the Kolmogorov complexity function. Saks and Santhanam [46] took the first significant step in this direction, by showing the following results:

\[\text{Theorem 1 (Saks & Santhanam [46]).} \]

1. Although (by the work of Hirahara [30]) every language in $\text{EXP}^{\text{NP}}$ is reducible in deterministic polynomial time to any function that differs from $K$ by at most an additive $O(\log n)$ term, no decidable language outside of $P$ is reducible to all approximations to $K$ that differ by an error margin $e(n) = \omega(\log n)$ via an “honest” deterministic polynomial-time nonadaptive reduction.

2. Although (by the work of Hirahara [29]) every language in $\text{NEXP}$ is reducible via randomized nonadaptive reductions to any function that differs from $K$ by at most an additive $O(\log n)$ term, no decidable language outside of $\text{AM} \cap \text{coAM}$ is reducible to all approximations to $K$ that differ by an error margin $e(n) = \omega(\log n)$ via an “honest” probabilistic polynomial-time nonadaptive reduction.

3. No decidable language outside of $\text{SZK}$ is randomly $m$-reducible to each $\omega(\log n)$ approximation to the $K$-random strings.

This is not the first time that the complexity class $\text{SZK}$ (for Statistical Zero Knowledge) has arisen in the context of investigations relating to Kolmogorov complexity. In particular, $\text{SZK}$ and its “non-interactive” subclass $\text{NISZK}$ have been studied in connection with a version of time-bounded Kolmogorov complexity, which in turn is studied because of its connection with the Minimum Circuit Size Problem ($\text{MCSP}$) [11, 14]. These problems lie at the heart of what has come to be called meta-complexity: the study of the computational difficulty of answering questions about complexity.

Allender [2] proposed an intriguing research program towards the $P = \text{BPP}$ conjecture. The class $P$ can be characterized by the class of languages reducible to the set of Kolmogorov-random strings under polynomial-time disjunctive truth-table reductions [8]. Similarly, he conjectured that $\text{BPP}$ can also be characterized by polynomial-time truth-table reductions to the set of Kolmogorov-random strings, and envisioned that such a completely new characterization of complexity classes would give us new insights into $\text{BPP}$, especially from the perspective of computability theory. Unfortunately, his conjecture was refuted by Hirahara [30] under a plausible complexity-theoretic assumption.

In this paper, we show that $\text{SZK}$, $\text{NISZK}$ and their logspace variants $\text{SZKL}$ and $\text{NISZKL}$ can be characterized by reductions to approximations to the Kolmogorov complexity function. We envision that our new characterization of these complexity classes would improve our understanding of zero knowledge interactive proof systems in future. Zero knowledge interactive proof systems have many applications in cryptographic protocols, and they have been studied very widely. We refer the reader to the excellent survey by Vadhan for more background [47]. For our purposes, the complexity classes of interest to us ($\text{SZK}$, $\text{NISZK}$, $\text{SZKL}$, and $\text{NISZKL}$) can be defined in terms of their complete problems. But first, we need to define some basic notions and provide some background.

## 2 Preliminaries

We assume familiarity with basic complexity classes such as $P$, $L$, and $\text{AC}^0$; we view these as classes of functions, as well as of languages. We also will refer to the class of functions...
computed in $\text{NC}^0$, where each output bit depends on at most $O(1)$ input bits. For circuit complexity classes such as $\text{NC}^0_1$, $\text{NC}^0$ and $\text{AC}^0$, by default we assume that the circuit families are “First-Order-uniform” as discussed in [5, 18, 38]. This coincides with Dlogtime-uniform $\text{AC}^0$, and what one might call “Dlogtime-uniform $\text{AC}^0$-uniform” $\text{NC}^0$. (We refer the reader to [49] for more background on circuit uniformity.) When we need to refer to nonuniform circuit complexity, we will be explicit.

All of these classes give rise to restrictions of Karp reducibility $\leq_p$, such as $\leq_m^L \leq_m^{\text{AC}^0}$, and $\leq_m^{\text{NC}^0}$. We will also discuss projections ($\leq_m^{\text{proj}}$), which are $\leq_m^{\text{NC}^0}$ reductions in which each output bit depends on at most one input bit. Thus projections are computed by circuits consisting of constants, wires, and NOT gates.

A promise problem $A$ is a pair of disjoint sets $(Y_A, N_A)$ of YES instances and NO instances, respectively. A solution to a promise problem is any set $B$ such that $Y_A \subseteq B$ and $N_A \subseteq \overline{B}$. A don’t-care instance of $A$ is any string that is not in $Y_A \cup N_A$. A language can be viewed as a promise problem that has no don’t-care instances.

We say that a promise problem $A = (Y, N)$ is decidable if $Y$ and $N$ are decidable sets. Observe that if $B = (Y', N')$ with $Y' \subseteq Y$ and $N' \subseteq N$, then any solution to $A$ is also a solution to $B$. Such subproblems of decidable promise problems are intuitively “decidable”, but are not necessarily decidable according to our definition. Since there are uncountably many subsets of $Y$ and $N$ for any nontrivial promise problem, clearly not every intuitively “decidable” promise problem can be decidable.

When defining reductions between two promise problems $A$ and $B$, there are two options. Either

- for every solution $S$ to $B$ there is a reduction from $A$ to $S$, or
- there is a reduction that correctly decides $A$ when given any solution $S$ for $B$.

As it turns out, these two notions are equivalent [28, 43]. Thus we shall always use the second approach, when defining notions of reducibility between promise problems.

We assume that the reader is familiar with Kolmogorov complexity; more background on this topic can be found in references such as [41, 25]. Briefly, $K_U(x|y) = \min\{ |d| : U(d, y) = x \}$, and $K_U(x) = K(x|\lambda)$ where $\lambda$ denotes the empty string.\(^3\) Although this definition depends on the choice of the Turing machine $U$, we pick some “universal” machine $U'$ and define $K(x|y)$ to be $K_{U'}(x|y)$; for every machine $U$, there is a constant $c$ such that $K(x|y) \leq K_{U'}(x|y) + c$. One important non-trivial fact regarding Kolmogorov complexity is known as symmetry of information:

\begin{theorem} (Symmetry of Information)
\begin{align*}
K(x, y) &= K(x) + K(x|y) \pm O(\log(K(x, y))).
\end{align*}
\end{theorem}

Let $\overline{R}_K$ be the promise problem $(Y_{\overline{R}_K}, N_{\overline{R}_K})$ where $Y_{\overline{R}_K}$ contains all strings $y$ such that $K(y) \geq |y|/2$ and the NO instances $N_{\overline{R}_K}$ consists of those strings $y$ where $K(y) \leq |y|/2 - c(|y|)$ for some approximation error term $e(n)$, where $e(n) = \omega(\log n)$ and $e(n) = n^{o(1)}$. All of our theorems hold for any $e(n)$ in this range. We will sometimes assume that $e(n)$ is computable in $\text{AC}^0$, which is true for most approximation terms of interest.

\(^3\) This is actually the definition of so-called “plain” Kolmogorov complexity, although the letter $K$ is traditionally used for the “prefix-free” Kolmogorov complexity. These two measures differ by at most a logarithmic term, and our theorems hold for either measure. For simplicity, we have presented the simpler definition.
Since the approximation error $e(n)$ is superlogarithmic, it is worth noting that $\tilde{R}_K$ can be defined equivalently either in terms of prefix-free or plain Kolmogorov complexity (because these two measures are within an additive logarithmic term of each other).

Any language that is reducible to $\tilde{R}_K$ via any of the reducibilities that we consider is decidable, by a theorem of [23]. However, it is not known whether this carries over in any meaningful way to promise problems.

The reader may wonder about the justification for the threshold $K(y) \geq |y|/2$ in the definition of $\tilde{R}_K$. The following proposition indicates that, for large error bounds $\epsilon(n)$, using a larger threshold reduces to $\tilde{R}_K$. Later, we show a related result for smaller thresholds.

**Proposition 3.** Let $A = (Y, N)$ be the promise problem where $Y = \{y : K(y) \geq t(|y|)\}$ for some AC$^0$-computable threshold $t(n) \geq n/2$, and where $N = \{y : K(y) \leq t(|y|) - |y|^\epsilon\}$ for some $1 > \epsilon > 0$. Then $A \leq_{m^C}^{N_{\epsilon}} \tilde{R}_K$.

**Proof.** Let $\delta = \frac{\epsilon}{2}$. Given an instance $y$ of length $n$ (for all large $n$), in AC$^0$ we can find the least integer $i < n$ such that $2t(n) - n + 5 \log n + (2(2n)^\delta - n^\delta) \leq i \leq 2t(n) - n - 3 \log n$.

Let $z = y^\delta$. Then $K(z) \leq K(y) + 2 \log i + O(1)$. Similarly, $K(y) \leq K(z) + 2 \log i + O(1)$, and hence $K(z) \geq K(y) - 2 \log i - O(1)$.

Thus if $y \in Y$, then $K(z) \geq t(n) - 2 \log i - O(1) > (t(n) - \frac{n}{2}) + \frac{n}{2} - 3 \log n \geq \frac{n+i}{2} = \frac{|z|}{2}$. And if $y \in N$, then $K(z) < t(n) - n^\delta + 2 \log i + O(1) < (t(n) - \frac{n}{2}) + \frac{n}{2} - n^\delta + 2 \log i + O(1) \leq \frac{n+i}{2} - (n+i)^\delta = \frac{|z|}{2} - |z|^\delta < \frac{|z|}{2} - \epsilon(|z|)$.

Thus $y \in Y$ implies $z \in Y_{\leq R_K}$ and $y \in N$ implies $z \in N_{\geq R_K}$.

Randomized reductions play a central role in the results that we will be presenting. Here is the basic definition:

**Definition 4.** A promise problem $A = (Y, N)$ is $\leq_{m^C}^{\text{RP}}$-reducible to $B = (Y', N')$ with threshold $\theta$ if there is a polynomial $p$ and a deterministic Turing machine $M$ running in time $p$ such that

\[ x \in Y \text{ implies } \Pr_{r \in \{0, 1\}^p(|x|)}[M(x, r) \in Y'] \geq \theta. \]

\[ x \in N \text{ implies } \Pr_{r \in \{0, 1\}^p(|z|)}[M(x, r) \in N'] = 1. \]

Randomized reductions were introduced by Adleman and Manders, as a probabilistic generalization of $\leq_{m}^{\text{P}}$ reducibility\footnote{We assume that the reader is familiar with Karp reducibility $\leq\text{P}_{m}$.} [1]. They used the threshold $\theta = \frac{1}{2}$. One of the most important applications of randomized reductions is the theorem of Valiant and Vazirani [48], where they showed that SAT reduces to Unique Satisfiability (USAT) via a randomized reduction, with threshold $\theta = \frac{1}{4n}$.\footnote{Recently, there have also been several papers showing that certain meta-complexity-theoretic problems are NP-complete under randomized reductions, including [10, 31, 34, 35, 36, 42, 44].} The reader may expect that—as is so often the case with probabilistic notions in computational complexity theory—the choice of threshold is arbitrary, and can be changed with no meaningful consequences. However, this does not appear to be true; we refer the reader to the work of Chang, Kadin, and Rohatgi [24] for a discussion of this point. As they point out, different thresholds are appropriate in different situations. If $A \leq_{m}^{\text{P}} B$ with threshold $\frac{1}{2n}$ (for instance), where the set OR$B = \{(x_1, \ldots, x_k) : \exists i, x_i \in B\} \leq_{m}^{\text{P}} B$, then it is indeed true that $A \leq_{m^C}^{\text{RP}} B$ with threshold $1 - \frac{1}{4n}$ [24]. But Chang, Kadin, and Rohatgi point out that it is far from clear that USAT has this property. We are concerned here with problems that are $\leq_{m^C}^{\text{RP}}$-reducible to $\tilde{R}_K$; just as in the case with randomized reductions to USAT, we must be careful about which threshold $\theta$ we choose. For the remainder of
this paper, we will use the threshold \( \theta = 1 - \frac{1}{n^{1/7}} \). (For a discussion of why we select this
threshold, see Remark 12.)

The following proposition is the counterpart to Proposition 3, for thresholds smaller than
\( \frac{n}{2} \).

**Proposition 5.** Let \( A = (Y, N) \) be the promise problem where \( Y = \{ y : K(y) \geq t(|y|) \} \)
for some polynomial-time computable threshold \( t(n) \leq \frac{n}{2} \), and where \( N = \{ y : K(y) \leq
\langle t(|y|) - |y| \rangle \} \) for some \( 1 > \epsilon > 0 \). Then \( A \leq_{\text{m}} R_{K}^{\text{RP}} \).

**Proof.** Given an instance \( y \) of length \( n \) (for all large \( n \)), in polynomial time we can find the
least integer \( i < n \) such that \( 2t(n) - 2n^\epsilon + 2e(3n) + 4 \log n \leq i \leq 2t(n) - e(n) - 2e \log n \) (for
a constant \( c \) that will be picked later).

Pick a random string \( r \) of length \( n \). Let \( z = yr^0i \). Then \( K(z) \leq K(y) + 2 \log i + |r| \).
Also, by symmetry of information, \( K(z) \geq K(yr^0i0^0i) + K(y0^i) - c' \log n \) (for some fixed
constant \( c' \), and hence with probability at least \( 1 - \frac{1}{n^{\epsilon}} \), \( K(z) \geq (n - \frac{e(n)}{2}) + K(y) - c \log n \)
(for some fixed \( c \), which is the constant \( c \) that we use above in defining \( i \)).

Thus if \( y \in Y \), then with high probability \( K(z) \geq i(n) + (n - \frac{e(n)}{2}) - c \log n > n + \frac{1}{2} = \frac{|z|}{2} \).
And if \( y \in N \), then \( K(z) \geq (t(n) - n^\epsilon) + 2 \log i + |r| \leq n + n^\epsilon - e(3n) \leq \frac{|z|}{2} - e(|z|) \).

Thus \( y \in Y \) implies \( z \in Y_{\frac{n-1}{n^{(1/7)}}} \), and \( y \in N \) implies \( z \in N_{\frac{n-1}{n^{(1/7)}}} \).

We will also need a “two-sided error” version of random reducibility, analogous to the
relationship between RP and BPP.

**Definition 6.** A promise problem \( A = (Y, N) \) is \( \leq_{\text{m}}^{\text{BPP}} \)-reducible to \( B = (Y', N') \) with
threshold \( \theta > \frac{1}{2} \) if there is a polynomial \( p \) and a deterministic Turing machine \( M \) running in
time \( p \) such that

\[
\begin{align*}
&x \in Y \text{ implies } \Pr_{r \in \{0,1\}^p(x)}[M(x, r) \in Y'] \geq \theta. \\
&x \in N \text{ implies } \Pr_{r \in \{0,1\}^p(x)}[M(x, r) \in N'] \geq \theta.
\end{align*}
\]

The complexity classes SZK (Statistical Zero Knowledge) and NISZK (Non-Interactive
Statistical Zero Knowledge) are defined in terms of interactive proof protocols (with a Prover
interacting with a probabilistic polynomial-time Verifier, together with a Simulator that
can produce a distribution on transcripts that is statistically close to the distribution on
messages that would be exchanged by the prover and the verifier on YES instances. But
for our purposes, it will suffice (and be simpler) to present alternative definitions of these
classes, in terms of their standard complete problems.

**Definition 7 (Promise-EA).** Let a circuit \( C : \{0,1\}^m \rightarrow \{0,1\}^n \) represent a probability
distribution \( X \) on \( \{0,1\}^n \) induced by the uniform distribution on \( \{0,1\}^m \). We define Promise-EA
to be the promise problem

\[
Y_{\text{EA}} = \{(C, k) \mid H(X) > k + 1\}
\]

\[
N_{\text{EA}} = \{(C, k) \mid H(X) < k - 1\}
\]

where \( H(X) \) denotes the entropy of \( X \).

**Theorem 8 ([27]).** EA is complete for NISZK under \( \leq_{\text{m}}^{\text{P}} \) reductions.

We will actually take this as a definition; we say that \( (Y, N) \) is in NISZK if and only if
\( (Y, N) \leq_{\text{m}}^{\text{P}} \text{EA} \).
Theorem 10 ([45]). SD is complete for SZK under \( \leq_P \) reductions.

Thus we will define SZK to be the class of promise problems \((Y, N)\) such that \((Y, N) \leq_P \text{SD}^\text{SZK} \).
We have \( \theta > n^k(n-3) \) for all large \( n \), and hence for all large YES instances we have \( KT(y) > n^k(n-3) = \ell - \ell^\delta \) for some \( \delta < 1 \), where \( |y| = tn = \ell \). The focus of [14] was on the measure \( KT \), but (as was previously observed in [4, Theorem 1]) the analysis in Lemma 16 carries over unchanged to the setting of non-resource-bounded Kolmogorov complexity \( K \). Thus, with high probability, the probabilistic routine, when given a YES instance of \( EA \), produces a string \( y \) where \( K(y) > |y| - |y|^\delta \).

On the other hand, if \((C,n−3)\) is a NO instance, then the support of \( C \) has size at most \( 2^{n-n^\epsilon} \), and thus any string \( z \) in the support of \( C \) has \( K(z|C) \leq n-n^\epsilon+O(1) \). Thus any string \( y \) that is produced by \( M \) in this case has \( K(y) \leq t(n-n^\epsilon)+|C|+O(1) \). Since \( t = n^k \) was chosen to be large (with respect to the length of the input instance \((C,n−3)\)), we may assume \( |C| < n^{k+\epsilon} - 4n^k \). Thus if \((C,n−3)\) is any large NO instance, we have \( K(y) < n^k(n−4) = \ell - \ell^{\delta'} \) for some \( \delta' > \delta \). To summarize, with probability 1, the probabilistic routine, when given a NO instance of \( EA \), produces a string \( y \) where \( K(y) \geq |y| - |y|^\delta' \geq (|y| - |y|^\epsilon) - |y|^\epsilon \) for some \( \epsilon > 0 \). We can now conclude that \( EA \leq_{m}^{\text{RP}} \hat{R} \) by appealing to Proposition 3.

To complete the proof of the theorem, we need to show that if \( A \) is any decidable promise problem that has a randomized poly-time \( m \)-reduction \( (\leq_{m}^{\text{BPP}}) \) with error \( 1/n^{o(1)} \) to the promise problem \( \hat{R} \) then \( A \in \text{NISZK} \). This was essentially shown by Saks and Santhanam [46, Theorem 39], but we present a complete argument here. Let \( M \) be the probabilistic machine that computes this \( \leq_{m}^{\text{BPP}} \) reduction.

Let \( y = f(x,r) \in \{0,1\}^m \) denote the output that \( M \) produces, where \( x \) is an instance of \( A \) and \( r \) denotes the randomness used in the reduction. (As in the proof of [46, Theorem 39], we may assume that, for each \( x \), all outputs of the form \( f(x,r) \) have the same length.) Given an \( x \in \{0,1\}^n \), observe that there is a polynomial-sized circuit \( C_x \) such that \( C_x(r) = f(x,r) \).

According to the correctness of the reduction, we have

\[
x \in Y_A \Rightarrow \Pr_r[M(x,r) \in Y_{\hat{R}_K}] \geq 1 - 1/n^{o(1)} \quad \text{and}
\]

\[
x \in N_A \Rightarrow \Pr_r[M(x,r) \in N_{\hat{R}_K}] \geq 1 - 1/n^{o(1)}.
\]

In other words, if \( x \) is a YES instance, then \( K(y) \geq |y|/2 \) with probability at least \( 1 - 1/n^{o(1)} \) and if \( x \) is a NO instance, then \( K(y) \leq |y|/2 - e(|y|) \) with probability at least \( 1 - 1/n^{o(1)} \). (Recall that \( e(n) \) is the error term in the approximation \( \hat{R}_K \).) We will now show that there is an entropy threshold that separates these two distributions, which will provide an \( \text{NISZK} \) upper bound on resolving \( A \).

**Claim:** If \( x \) is a YES instance, then the entropy of the distribution \( C_x(r) \) is at least \( m/2 - e(m)/2 + 1 \) and if \( x \) is a NO instance, then the entropy of \( C_x(r) \) is at most \( m/2 - e(m)/2 - 1 \).

We first show that if the claim holds, then \( A \in \text{NISZK} \). Let \( k = m/2 - e(m)/2 \). The reduction given above reduces membership in \( A \) to the Entropy Approximation (EA) problem on the circuit description \( C_x \) with threshold \( k \). Given \( x \), we can compute the map \( x \mapsto C_x \) in time \( n^{O(1)} \). Recall that \( EA \) is compete for \( \text{NISZK} \). Since \( \text{NISZK} \) is closed under \( \leq_{m}^{\text{P}} \) reductions, we can conclude that \( A \in \text{NISZK} \).

**Proof of claim:**

Assume not and let \( x \) be the lexicographically first string that violates the above claim (for some length \( n \)). Since the reduction is a computable function, and since \( A \) is a decidable promise problem, \( K(x) = O(\log n) \). We have the following two cases to consider:

**Case 1 - \( x \) is a YES instance:** From the correctness of the reduction we have that with probability \( 1 - 1/n^{o(1)} \) the output \( y \) is a string with Kolmogorov complexity at least \( |m|/2 \).
Since $x$ is a violator, we have $H(C_x(r)) < k + 1 = m/2 - e(m)/2 + 1$.

On one hand, the distribution $C_x(r)$ has large enough probability mass on the high-complexity strings. On the other hand, we have that since $x$ is a low-complexity string itself, the elements of $C_x(r)$ with highest mass can be identified by short descriptions. This leads to a contradiction of simultaneously having large enough mass on the low and the high $K$-complexity strings.

Let $t$ be the entropy of the distribution $C_x(r)$. Let $Y = \{y_1 \ldots y_{2t + \log m}\}$ be the heaviest elements (in terms of probability mass) of $C_x(r)$ in decreasing order. Conditioned on $x$, the $K$ complexity of any of these strings $y_i$ is at most $t + O(\log m)$. Since $K(x) = O(\log n) = O(\log m)$, we have $K(y_i) \leq t + O(\log m) < m/2$. Next, we will show that there is at least mass $\frac{1}{m}$ on these strings within $C_x(r)$. This will contradict the correctness of the reduction for $x \in L$ since it cannot output strings with $K$ complexity at most $\lceil m/2 \rceil$ with probability $1/n^{\Omega(1)}$.

Assume not, i.e., the mass on elements of $Y$ is at most $\frac{1}{m}$. Observe that elements of $\text{Sup}(C_x(r)) - Y$ have mass no more than $2^{-(t + \log m)}$ each. Then, the contribution to entropy by these elements is at least $(1 - 1/m)(t + \log m) > t$ (which is a contradiction).

**Case 2 - $x$ is a NO instance:** From the correctness of the reduction we have that with probability at least $1 - 1/n^{\Omega(1)}$ the output $f(x,r)$ is a string with $K$ complexity at most $m/2 - e(m)$. Since $x$ is a violator, we also have $H(C_x(r)) > k - 1 = m/2 - e(m)/2 - 1$.

We claim that the following holds:

$$\Pr_{y \sim f(x,r)}[K(y) > m/2 - e(m)] \geq 1/m.$$ 

Assume not. Then, the entropy of $f(x,r)$ is at most $(1/m)(m) + (1 - 1/m)(m/2 - e(m)) \leq m/2 - e(m) + 1 < m/2 - e(m)/2 - 1$, which contradicts the lower bound on the entropy of $f(x,r)$ above.

Since the claim holds, with probability at least $1/m$ the output of the reduction is not an element of the set $N_{R_K}$. Thus, the reduction fails with probability $1/n^{\Omega(1)}$.

\[\blacktriangle\]

**Remark 12.** The proof of the preceding theorem illustrates why we define the error threshold in our randomized reductions to be $\frac{1}{n^{\Omega(1)}}$. If we assumed that $A$ were $\leq_{\text{BPP}}$-reducible to $\overline{R}_K$ with an inverse polynomial threshold (say $q(n)^{-1}$), then (as in the proof of [46, Theorem 39]) we may modify the reduction so that the length of each output produced has length $\frac{1}{q(n)}Q(n)$ (by padding with some uniformly-random bits). For strings $x$ that are NO instances of $A$, when the reduction to $\overline{R}_K$ fails with probability $1/q(n)$, our calculation of the entropy of $C_x$ will involve a term of $\frac{1}{q(n)}Q(n)$ (because the queries made in this case can have nearly $Q(n)$ bits of entropy). This is more than the entropy gap between the distributions corresponding to the YES and NO outputs.

**Remark 13.** Although our focus in this paper is in $\overline{R}_K$, we note that one can also define an analogous problem $\overline{R}_{K\text{KT}}$ in terms of the time-bounded measure $KT$. The approach used in Theorem 11 also shows that every problem in $\text{NISZK}$ is $\leq_{\text{BPP}}$ reducible to $\overline{R}_{K\text{KT}}$, although we do not know how to show hardness under $\leq_{\text{RP}}$ reductions. (A random sample from the low-entropy distribution is guaranteed to always have low $K$-complexity, but the tools of [14, 16] only guarantee that the output has low $KT$-complexity with high probability.)
4 More Powerful Reductions

Just as $\leq_{\text{m}}^\text{RP}$ and $\leq_{\text{m}}^\text{BPP}$ reducibilities generalize the familiar $\leq_{\text{m}}^\text{P}$ (Karp) reducibility to the setting of probabilistic computation, so also are there probabilistic generalizations of deterministic non-adaptive reductions (also known as truth-table reductions). Before presenting these probabilistic generalizations, let us review the previously-studied deterministic non-adaptive reducibilities that are relevant for this investigation. Some of them may be unfamiliar to the reader.

Ladner, Lynch, and Selman [40] considered several possible ways to define polynomial-time versions of the truth-table reducibility that had been studied in computability theory, before settling on the definition of $\leq_{\text{P}}^\text{tt}$ reducibility below. They considered only reductions between languages; the corresponding generalization to promise problems is due to [45]. In order to state this generalization formally, let us define the characteristic function $\chi_A$ of a promise problem $A = (Y, N)$ to take on the following values in three-valued logic:

- If $x \in Y$, then $\chi_A(x) = 1$.
- If $x \notin N$, then $\chi_A(x) = 0$.
- If $x \notin (Y \cup N)$, then $\chi_A(x) = \ast$.

A Boolean circuit with $n$ variables, when given an assignment in $\{0, 1, \ast\}^n$, can be evaluated using the usual rules of three-valued logic. (See, e.g., [45, Definition 4.6].)

**Definition 14.** Let $A = (Y, N)$ and $B = (Y', N')$ be promise problems. We say $A \leq_{\text{P}}^\text{P} B$ if there is a function $f$ computable in polynomial time, such that, for all $x$, $f(x)$ is of the form $(C, z_1, z_2, \ldots, z_k)$ where $C$ is a Boolean circuit with $k$ input variables, and $(z_1, \ldots, z_k)$ is a list of queries, with the property that

- If $x \in Y$, then $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 1$.
- If $x \notin N$, then $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 0$.

This definition ensures that the circuit $C$, viewed as an ordinary circuit in 2-valued logic, correctly decides membership for all $x \in (Y \cup N)$ when given any solution $S$ for $B$ as an oracle.

If $C$ is a Boolean formula, instead of a circuit, then one obtains the so-called “Boolean formula reducibility” (denoted by $A \leq_{\text{bf}}^\text{P} B$), which was discussed in [40] and studied further in [39, 22]. (See also [21, 6].)

**Theorem 15.** $\text{SZK} = \{ A : A \leq_{\text{bf}}^\text{P} \text{EA} \}$.

**Proof.** $\text{EA} \in \text{NISZK} \subseteq \text{SZK}$. Sahai and Vadhan [45, Corollary 4.14] showed that $\text{SZK}$ is closed under $\text{NC}^1$-truth-table reductions, but the proof carries over immediately to $\leq_{\text{bf}}^\text{P}$ reductions. Thus $\{ A : A \leq_{\text{bf}}^\text{P} \text{EA} \} \subseteq \text{SZK}$. The other inclusion was shown in [27, Proposition 5.4].

Notably, it is still an open question if $\text{SZK}$ is closed under $\leq_{\text{bf}}^\text{P}$ reducibility.

Our characterization of $\text{SZK}$ in terms of reductions to $\text{R}_K$ relies on the following probabilistic generalization of $\leq_{\text{bf}}^\text{P}$:

**Definition 16.** Let $A = (Y, N)$ and $B = (Y', N')$ be promise problems. We say $A \leq_{\text{bf}}^{\text{BPP}} B$ with threshold $\theta > \frac{1}{2}$ if there are functions $f$ and $g$ computable in deterministic polynomial time, and a polynomial $p$, such that, for all $x$, $f(x)$ is a Boolean formula $C$ (with $k = |x|^{O(1)}$ variables), with the property that
If \( x \in Y \), then \( C(g_B(x, 1), \ldots, g_B(x, k)) = 1 \),
if \( x \in N \), then \( C(g_B(x, 1), \ldots, g_B(x, k)) = 0 \),
where
\[
\begin{align*}
\chi_B(x, i) &= 1 \text{ if } \Pr_{r \in \{0, 1\}^{p(|x|)}} [g(x, i, r) \in Y] \geq \theta \\
\chi_B(x, i) &= 0 \text{ if } \Pr_{r \in \{0, 1\}^{p(|x|)}} [g(x, i, r) \in N'] \geq \theta \\
\chi_B(x, i) &= * \text{ otherwise}.
\end{align*}
\]
Intuitively, \( \leq_{\text{BPP}} \) reductions generalize \( \leq_{\text{bf}} \) reductions, in that the queries are now generated probabilistically, and the probability that any query returns a definite YES or NO answer is bounded away from \( \frac{1}{2} \).

The following proposition is immediate from the definitions.

**Proposition 17.** If \( A \leq_{\text{bf}} B \) and \( B \leq_{\text{BPP}} C \) with threshold \( \theta \), then \( A \leq_{\text{BPP}} C \) with threshold \( \theta \).

**Corollary 18.** \( \text{SZK} \subseteq \{ A : A \leq_{\text{BPP}} R \} \) with threshold \( 1 - \frac{1}{n^{\epsilon + 1}} \).

**Proof.** Immediate from Theorem 15 and Theorem 11. □

There are (at least) three other variants of probabilistic nonadaptive reducibility that we should mention. The first of these is the notion that goes by the name “nonadaptive BPP reducibility” or “randomized nonadaptive reductions” in work such as [46, 14, 19] and elsewhere.

**Definition 19.** Let \( A = (Y, N) \) and \( B = (Y', N') \) be promise problems. We say \( A \leq_{\text{BPP}} B \) if there are a function \( f \) computable in polynomial time and a polynomial \( p \) such that, for all \( x \) and all \( r \) of length \( p(|x|) \), \( f(x, r) \) is of the form \( (C, z_1, z_2, \ldots, z_k) \) where \( C \) is a Boolean circuit with \( k \) input variables, and \( (z_1, \ldots, z_k) \) is a list of queries, with the property that
\[
\begin{align*}
\text{If } x \in Y, \text{ then } \Pr_r[C(\chi_B(z_1), \ldots, \chi_B(z_k))] &= 1 \geq \frac{2}{3}.
\end{align*}
\]
\[
\begin{align*}
\text{If } x \in N, \text{ then } \Pr_r[C(\chi_B(z_1), \ldots, \chi_B(z_k))] &= 0 \geq \frac{2}{3}.
\end{align*}
\]
(The threshold \( \frac{2}{3} \) can be replaced by any threshold between \( n^{-k} \) and \( 2^{-n^k} \), by the usual method of taking the majority vote of several independent trials.)

Saks and Santhanam showed that if \( A \leq_{\text{bf}} \tilde{R}_k \) via a reduction that satisfies an additional “honesty” condition, then \( A \in \text{AM} \cap \text{coAM} \) [46]. The most important ways in which \( \leq_{\text{bf}} \) and \( \leq_{\text{BPP}} \) reducibility differ from each other, are (1) in \( \leq_{\text{bf}} \) reducibility, the query evaluation is performed by a Boolean formula, instead of a circuit, and (2) in \( \leq_{\text{BPP}} \) reducibility, the circuit that is chosen, to do the evaluation, depends on the choice of random bits, whereas in \( \leq_{\text{bf}} \) reducibility, the formula is chosen deterministically. Making different choices in these two dimensions gives rise to two other notions:

**Definition 20.** Let \( A = (Y, N) \) and \( B = (Y', N') \) be promise problems. We say \( A \leq_{\text{bf}} B \) if there are a function \( f \) computable in polynomial time and a polynomial \( p \) such that, for all \( x \) and all \( r \) of length \( p(|x|) \), \( f(x, r) \) is of the form \( (C, z_1, z_2, \ldots, z_k) \) where \( C \) is a Boolean formula with \( k \) input variables, and \( (z_1, \ldots, z_k) \) is a list of queries, with the property that
\[
\begin{align*}
\text{If } x \in Y, \text{ then } \Pr_r[C(\chi_B(z_1), \ldots, \chi_B(z_k))] &= 1 \geq \frac{2}{3}.
\end{align*}
\]
\[
\begin{align*}
\text{If } x \in N, \text{ then } \Pr_r[C(\chi_B(z_1), \ldots, \chi_B(z_k))] &= 0 \geq \frac{2}{3}.
\end{align*}
\]
(The threshold \( \frac{2}{3} \) can be replaced by any threshold between \( n^{-k} \) and \( 2^{-n^k} \), simply by incorporating a Boolean formula that takes the majority vote of several independent trials.)
The notation $\leq_{\text{bf}}^{\text{BPP}}$ is intended to suggest “random Boolean formula”, since the Boolean formula is chosen randomly.

**Definition 21.** Let $A = (Y, N)$ and $B = (Y', N')$ be promise problems. We say $A \leq_{\text{circ}}^{\text{BPP}} B$ with threshold $\theta > \frac{1}{2}$ if there are functions $f$ and $g$ computable in deterministic polynomial time, and a polynomial $p$, such that, for all $x$, $f(x)$ is a Boolean circuit (with $k = |x|^{O(1)}$ variables), with the property that

- If $x \in Y$, then $C(\chi_{g,B}(x,1), \ldots, \chi_{g,B}(x,k)) = 1$,
- If $x \in N$, then $C(\chi_{g,B}(x,1), \ldots, \chi_{g,B}(x,k)) = 0$,

where

\[
\begin{align*}
\chi_{g,B}(x,i) &= 1 \text{ if } \Pr_{r \in \{0,1\}^p(|x|)}[g(x,i,r) \in Y'] \geq \theta \\
\chi_{g,B}(x,i) &= 0 \text{ if } \Pr_{r \in \{0,1\}^p(|x|)}[g(x,i,r) \in N'] \geq \theta \\
\chi_{g,B}(x,i) &= * \text{ otherwise.}
\end{align*}
\]

We show in this paper that $\text{SZK}$ is the class of problems $\leq_{\text{bf}}^{\text{BPP}}$ reducible to $\tilde{R}_K$. We are not able to show that the class of problems $\leq_{\text{bf}}^{\text{BPP}}$ reducible to $\tilde{R}_K$ is contained in $\text{SZK}$, although we do observe that $\text{SZK}$ is closed under this type of reducibility.

**Theorem 22.** $\text{SZK} = \{A : A \leq_{\text{bf}}^{\text{BPP}} \text{EA}\}$.

*Proof.* The inclusion of $\text{SZK}$ in $\{A : A \leq_{\text{bf}}^{\text{BPP}} \text{EA}\}$ is immediate from Theorem 15. For the other direction, let $A \leq_{\text{bf}}^{\text{BPP}} \text{EA}$. Thus there are a function $f$ computable in polynomial time, and a polynomial $p$ such that, for all $x$ and all $r$ of length $p(|x|)$, $f(x,r)$ is of the form $(C, z_1, z_2, \ldots, z_k)$, where evaluating the Boolean formula $C(\chi_B(z_1), \ldots, \chi_B(z_k))$ gives a correct answer for all $x \in Y \cup N$ with error at most $2^{-n^2}$. Here is a zero-knowledge interactive protocol for $A$. The verifier sends a random string $r$ to the prover. The prover and the verifier can each compute $f(x,r) = (C, z_1, z_2, \ldots, z_k)$, and then (as in [45, Corollary 4.14]), compute an instance $(D, E)$ of $\text{SD}$ such that $(D, E)$ is a YES instance of $\text{SD}$ if $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 1$, and $(D, E)$ is a NO instance of $\text{SD}$ if $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 0$. The prover and the verifier can then run the $\text{SZK}$ protocol for the $\text{SD}$ instance $(D, E)$. The verifier clearly accepts each YES instance with high probability, and cannot be convinced to accept any NO instance with more than negligible probability. The simulator, given input $x$, will generate the string $r$ uniformly at random, and then compute $f(x,r)$ and compute the instance $(D, E)$ as above, and then produce the transcript that is produced by the $\text{SD}$ simulator on input $(D, E)$. It is straightforward to observe that, if $x \in Y$, then this distribution is very close to the distribution induced by the honest prover and verifier. \hfill \blacksquare

## 5 A New Characterization of $\text{SZK}$

**Theorem 23.** The following are equivalent, for any decidable promise problem $A$:

1. $A \in \text{SZK}$.
2. $A \leq_{\text{bf}}^{\text{BPP}} \tilde{R}_K$ with threshold $1 - \frac{1}{n^{1/2}}$.

*Proof.* Corollary 18 states that all problems in $\text{SZK} \leq_{\text{bf}}^{\text{BPP}}$-reduce to $\tilde{R}_K$. Thus we need only show the converse containment. Let $A \leq_{\text{bf}}^{\text{BPP}} \tilde{R}_K$. As in the proof of Theorem 11, we will build circuits $C_{x,i}(r)$ that model the computation that produces the $i$th query that is asked on input $x$, when using random bits $r$. As in the proof of Theorem 11, we claim that if a $1 - \frac{1}{n^{1/2}}$ fraction of the strings of the form $C_{x,i}(r)$ are in $Y_{\tilde{R}_K}$, then $C_{x,i}$ represents a
distribution with entropy at least \( m/2 - e(m)/2 + 1 \), and if a \( 1 - \frac{1}{n^m} \) fraction of the strings of the form \( C_{x,i}(r) \) are in \( N_{K_x} \), then \( C_{x,i} \) represents a distribution with entropy at most \( m/2 - e(m)/2 - 1 \). Indeed, the proof is essentially identical. Assume that there are infinitely many \( x \) that are not don’t care instances, where replacing the \( K_x \) oracle with the \( EA \) oracle does not yield the correct answer. Given \( n \), we can find the lexicographically-least string \( x \) of length \( n \) for which the reduction fails. Since the reduction fails, there must be some \( i \) such that the \( i^{th} \) query in the formula yields the wrong answer. Thus, given \( (n, i) \), we can find \( x \) and build the circuit \( C_{x,i} \) of Kolmogorov complexity \( O(\log n) \) that yields a correct answer when given \( K_x \) as an oracle, but fails when queries are made to \( EA \) instead. The analysis is identical to the argument in the proof of Theorem 11.

We have nothing to say, regarding the problems that are reducible to \( K_x \) via \( \leq_{tt}^{\text{BPP}} \) or \( \leq_{\text{rd}}^{\text{BPP}} \) reductions, other than to refer to the AM \( \cap \text{coAM} \) upper bound provided by Saks and Santhanam [46]. We do have a somewhat better bound to report, regarding \( \leq_{tt}^{\text{BPP}} \) reducibility.

> **Theorem 24.** The following are equivalent, for any decidable promise problem \( A \):

1. \( A \leq_{tt}^{\text{circ}} \tilde{R}_K \) with threshold \( 1 - \frac{1}{n^m} \).
2. \( A \leq^p_{tt} \text{EA} \).
3. \( A \leq^p_{tt} B \) for some \( B \in \text{SZK} \).

**Proof.** Items 2 and 3 are equivalent, by Theorem 15. Similarly, if \( A \leq^p_{tt} B \) for some \( B \in \text{SZK} \), then we know that \( A \leq_{tt}^P B \leq_{\text{rd}}^{\text{BPP}} \tilde{R}_K \). The composition of a \( \leq_{tt}^P \) reduction with a \( \leq_{\text{rd}}^{\text{BPP}} \) reduction is clearly a \( \leq_{tt}^{\text{BPP}} \) reduction. Finally, the proof of the remaining implication follows along the same lines as the proof of Theorem 23.

### 6 Less Powerful Reductions

The standard complete problems \( \text{EA} \) and \( \text{SD} \) remain complete for \( \text{NISZK} \) and \( \text{SZK} \), respectively, even under more restrictive reductions such as \( \leq_{m}^{\text{L}} \) and \( \leq_{m}^{\text{NC}^0} \). In this section, we show that it is worthwhile considering probabilistic versions of \( \leq_{m}^{\text{L}} \), \( \leq_{m}^{\text{AC}^0} \), and \( \leq_{m}^{\text{NC}^0} \) reducibility to \( \tilde{R}_K \).

> **Definition 25.** For a class \( \mathcal{C} \), a promise problem \( A = (Y, N) \) is \( \leq_{m}^{\text{NC}^0} \)-reducible to \( B = (Y', N') \) with threshold \( \theta \) if there are a function \( f \in \mathcal{C} \) and a polynomial \( p \) such that

\[
\begin{align*}
&\Pr_{r \in \{0,1\}^{\log |x|}} [f(x, r) \in Y'] \geq \theta. \\
&\Pr_{r \in \{0,1\}^{\log |x|}} [f(x, r) \in N'] = 1.
\end{align*}
\]

\( A \) is \( \leq_{m}^{\text{BPC}^c} \)-reducible to \( B \) with threshold \( \theta \) if there are a function \( f \in \mathcal{C} \) and a polynomial \( p \) such that

\[
\begin{align*}
&\Pr_{r \in \{0,1\}^{\log |x|}} [f(x, r) \in Y'] \geq \theta. \\
&\Pr_{r \in \{0,1\}^{\log |x|}} [f(x, r) \in N'] \geq \theta.
\end{align*}
\]

We are particularly interested in the cases \( \mathcal{C} = \text{L} \), \( \mathcal{C} = \text{AC}^0 \), and \( \mathcal{C} = \text{NC}^0 \). Note especially that, in the definitions of \( \leq_{m}^{\text{RL}} \) and \( \leq_{m}^{\text{BPL}} \), the logspace computation has full (two-way) access to the random bits \( r \). This is consistent with the way that probabilistic logspace computation is used in the context of the “verifier” and “simulator” in the complexity classes \( \text{SZK}_L \) and \( \text{NISZK}_L \) [26, 14].

\( \text{SZK}_L \), the “logspace version” of \( \text{SZK} \), was introduced in [26], primarily as a tool to discuss the complexity of problems involving distributions realized by extremely limited circuits (such as \( \text{NC}^0 \) circuits). It is shown in [26] that \( \text{SZK}_L \) contains many of the problems...
of cryptographic significance that lie in $\text{SZK}$. $\text{NISZK}_L$ was introduced in [14] as the “non-
interactive” counterpart to $\text{SZK}_L$, by analogy with $\text{NISZK}$, primarily as a tool to investigate
the complexity of computing time-bounded Kolmogorov complexity. It was subsequently
studied in [15], where it was shown to be robust to several changes to the definition. It
is shown in [26, 14] that complete problems for $\text{SZK}_L$ and $\text{NISZK}_L$ arise by considering
restrictions of the standard complete problems for $\text{SZK}$ and $\text{NISZK}$ where the distributions
under consideration are represented either by branching programs (in $\text{EA}_{\text{BP}}$), or by $\text{NC}^0$
circuits where each output bit depends on at most 4 input bits (in $\text{SD}_{\text{NC}^0}$ and $\text{EA}_{\text{NC}^0}$).

Following the pattern we established in Section 2, we now define $\text{SZK}_L$ and $\text{NISZK}_L$ in
terms of their complete problems, rather than presenting the definitions in terms of interactive
proofs:

$\text{Definition 26.}$ $\text{SZK}_L = \{ A : A \leq \text{proj}^{\text{SD}_{\text{NC}^0}} \} = \{ A : A \leq_{\text{m}} \text{SD}_{\text{BP}} \}$

$\text{NISZK}_L = \{ A : A \leq \text{proj}^{\text{EA}_{\text{NC}^0}} \} = \{ A : A \leq_{\text{m}} \text{EA}_{\text{BP}} \}$.

$\text{Theorem 27.}$ The following are equivalent, for any decidable promise problem $A$:

1. $A \in \text{NISZK}_L$
2. $A \leq_{\text{m}} \text{RNC}^0 \overline{R}_K$
3. $A \leq_{\text{m}} \text{BPNC}^0 \overline{R}_K$
4. $A \leq_{\text{m}} \text{RAC}^0 \overline{R}_K$
5. $A \leq_{\text{m}} \text{BPAC}^0 \overline{R}_K$
6. $A \leq_{\text{m}} \text{RL} \overline{R}_K$
7. $A \leq_{\text{m}} \text{RL} \overline{R}_K$
8. $A \leq_{\text{m}} \text{BPNC}^0 \overline{R}_K$
9. $A \leq_{\text{m}} \text{BPAC}^0 \overline{R}_K$
10. $A \leq_{\text{m}} \text{RL} \overline{R}_K$
11. $A \leq_{\text{m}} \text{RL} \overline{R}_K$

$\text{Proof.}$ The proof that $A \in \text{NISZK}$ implies $A \leq_{\text{m}} \text{RNC}^0 \overline{R}_K$ proceeds as in the proof of Theorem 11,
except that we appeal to [14, Corollary 43] (presenting a nonuniform $\leq_{\text{proj}}^{\text{SD}}$ reduction from
$\text{EA}_{\text{NC}^0}$ to $\overline{R}_K$), instead of Corollary 18 in that paper. In more detail: as in the proof of
Theorem 11, given $x$, the reduction constructs a sequence of independent copies of $\text{EA}$, but
now each distribution is represented by an $\text{NC}^0$ circuit. The proof of Corollary 43 in [14]
shows that these $\text{NC}^0$ circuits can be constructed via uniform projections, and thus each
output bit is computed by a gadget that is connected to $O(1)$ random bits (i.e., the bits that
are fed into the circuit computing the distribution), along with at most one bit from the
input $x$ (determining the circuitry internal to the gadget). The rest of the analysis is similar
to that in the proof of Theorem 11.

If $A$ is decidable and $A \leq_{\text{m}} \text{BPNC}^0 \overline{R}_K$, then, as in the proof of Theorem 11, we build a device
$C_x(r)$ that simulates the computation that produces queries to $\overline{R}_K$ on input $x$. However,
now $C_x$ is a branching program, and thus we replace queries to $\overline{R}_K$ by queries to $\text{EA}_{\text{BP}}$.
Again, the analysis is similar to that in the proof of Theorem 11.

We end this section, with an analogous characterization of $\text{SZK}_L$.

$\text{Definition 28.}$ Let $A = (Y, N)$ and $B = (Y', N')$ be promise problems. We say $A \leq_{\text{m}} B$
if there is a function $f$ computable in logspace such that, for all $x$, $f(x)$ is of the form
$(C, z_1, z_2, \ldots, z_k)$ where $C$ is a Boolean formula with $k$ input variables, and $(z_1, \ldots, z_k)$ is a
list of queries, with the property that

1. If $x \in Y$, then $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 1$.
2. If $x \in N$, then $C(\chi_B(z_1), \ldots, \chi_B(z_k)) = 0$. 
Earlier work that studied $\leq_{bf}^1$ reducibility can be found in [21, 6].

We say $A \leq_{bf}^{\text{BPL}} B$ with threshold $\theta > \frac{1}{2}$ if there are functions $f$ and $g$ computable in deterministic logspace, and a polynomial $p$, such that, for all $x$, $f(x)$ is a Boolean formula (with $k = |x|^{O(1)}$ variables), with the property that

- If $x \in Y$, then $C(x_g,B(x,1),\ldots,x_g,B(x,k)) = 1$,
- If $x \in N$, then $C(x_g,B(x,1),\ldots,x_g,B(x,k)) = 0$,

where

$$
\begin{align*}
\chi_g,B(x,i) &= 1 \text{ if } \Pr_{r \in \{0,1\}^{p(|x|)}} [g(x, i, r) \in Y'] \geq \theta \\
\chi_g,B(x,i) &= 0 \text{ if } \Pr_{r \in \{0,1\}^{p(|x|)}} [g(x, i, r) \in N'] \geq \theta \\
\chi_g,B(x,i) &= \ast \text{ otherwise.}
\end{align*}
$$

(Similarly, one can define $\text{AC}^0$ versions of $\leq_{bf}^1$, although, since an $\text{AC}^0$ circuit cannot evaluate a Boolean formula, we do not pursue that direction here.)

\textbf{Theorem 29.} The following are equivalent, for any decidable promise problem $A$:

\begin{itemize}
  \item $A \in \text{SZK}_L$.
  \item $A \leq_{bf}^1 \text{EA}_{\text{NC}^0}$.
  \item $A \leq_{bf}^{\text{BPL}} \tilde{R}_K$ with threshold $1 - \frac{1}{n^{\log_2 n}}$.
\end{itemize}

\textbf{Proof.} The first two items are equivalent, because (a) $\text{SZK}_L$ is closed under $\leq_{bf}^1$ reducibility [15], and (b) the argument in [27], showing that $\text{SZK} \leq_{bf}^1$-reduces to $\text{NISZK}$ carries over directly to $\text{SZK}_L$ and $\text{NISZK}_L$.

Since $\text{EA}_{\text{NC}^0}$ is complete for $\text{NISZK}_L$, Theorem 27 implies that every $A \in \text{NISZK}_L$ is $\leq_{bf}^{\text{BPL}}$-reducible to $\tilde{R}_K$. The argument that every decidable $A$ that $\leq_{bf}^{\text{BPL}}$-reduces to $\tilde{R}_K$ lies in $\text{SZK}_L$ is similar to the argument in Theorem 23.

\section{Discussion}

There are not many examples of natural computational problems that are known or conjectured to lie outside of $\text{P}$, such that the class of problems reducible to them via $\leq_m^0$ and $\leq_m^1$ (or $\leq_{\text{AC}^0}$) reductions differ (or are conjectured to differ). Is it the case that the problems reducible to $\tilde{R}_K$ via $\leq_m^{\text{RP}}$ and $\leq_m^{\text{RL}}$ (or $\leq_m^{\text{RA} \text{C}^0}$) reductions differ? Or should this be taken as evidence that $\text{NISZK}$ and $\text{NISZK}_L$ coincide?

Similarly, there are not many examples of natural computational problems such that the classes of problems reducible to them via $\leq_{\text{circ}}^0$ and $\leq_{\text{circ}}^1$ reductions differ (or are conjectured to differ). For example, these reducibilities coincide for SAT [22]. Is it the case that $\leq_{\text{BPP}}^m$ and $\leq_{\text{circ}}^1$ reducibilities differ for $\tilde{R}_K$? Or should this be taken as evidence that $\text{SZK}$ is closed under $\leq_{\text{circ}}^1$ reducibility?

Perhaps our new characterizations of statistical zero knowledge classes will be useful in answering these questions.

It is known that every promise problem in $\text{NISZK}_L$ reduces to $\tilde{R}_K$ via nonuniform projections [14, 4]. The following quote from [4] is worth paraphrasing here:

\ldots no complexity class larger than $\text{NISZK}_L$ is known to be (non-uniformly) $\leq_{\text{AC}^0}^m$ reducible to the Kolmogorov-random strings [14]. It seems unlikely that this is optimal.
The discussion in [4] was referring to reductions to an oracle for the exact Kolmogorov-complexity function. Our results show that, for reductions to an approximation to the Kolmogorov-complexity function, NISZKL is essentially “optimal”.

Finally, let us observe that our new characterizations of NISZKL may open new avenues of attack on questions such as whether NP = NL. MKTP, the problem of computing KT complexity, lies in NP and is hard for co-NISZKL under nonuniform projections [14]. If MKTP ∈ NISZKL, then there must be a nonuniform projection f that takes strings of low KT-complexity (and hence low K-complexity) to strings of high K complexity, and simultaneously maps strings of high KT complexity to strings of low K-complexity. It is plausible that one could show unconditionally that no such projection can exist. Among other things, this would show that NP ̸= DET (where DET is the complexity class, containing NL, of problems that reduce to the determinant) since DET ⊆ NISZKL [14]. In this vein, let us also remark that Kolmogorov complexity has already proved useful in developing nonrelativizing proof techniques [31], and also that the machinery of perfect randomized encodings (which were developed in [17] and which are essential to the results of [14]) also does not seem to relativize in any obvious way.

Acknowledgments

EA and HT were supported in part by NSF Grants CCF-1909216 and CCF-1909683. SH was supported in part by JST, PRESTO Grant Number JPMJPR2024, Japan. We thank Sam Buss, Johannes Köbler, and Uwe Schöning for discussions concerning Boolean formula reducibility.

References

Kolmogorov Complexity Characterizes Statistical Zero Knowledge


E. Allender, S. Hirahara, and H. Tirumala


