A Duality between One-Way Functions and Average-Case Symmetry of Information

A Duality between One-Way Functions and Average-Case Symmetry of Information*

Shuichi Hirahara†
National Institute of Informatics
Japan
s_hirahara@nii.ac.jp

Rahul Ilango‡
Massachusetts Institute of Technology
USA
rilango@mit.edu

Zhenjian Lu
University of Oxford
United Kingdom
zhenjian.lu@cs.ox.ac.uk

Mikito Nanashima
Tokyo Institute of Technology
Japan
nanashima.m.aa@is.c.titech.ac.jp

Igor C. Oliveira§
University of Warwick
United Kingdom
igor.oliveira@warwick.ac.uk

ABSTRACT

Symmetry of Information (SoI) is a fundamental property of Kolmogorov complexity that relates the complexity of a pair of strings and their conditional complexities. Understanding if this property holds in the *time-bounded* setting is a longstanding open problem. In the nineties, Longpré and Mocas (1993) and Longpré and Watanabe (1995) established that if SoI holds for time-bounded Kolmogorov complexity then cryptographic one-way functions do not exist, and asked if a converse holds.

We show that one-way functions exist *if and only if* (probabilistic) time-bounded SoI fails on average, i.e., if there is a samplable distribution of pairs (x, y) of strings such that SoI for pK^t complexity fails for many of these pairs. Our techniques rely on recent perspectives offered by probabilistic Kolmogorov complexity and meta-complexity, and reveal further equivalences between inverting one-way functions and the validity of key properties of Kolmogorov complexity in the time-bounded setting: (average-case) language compression and (average-case) conditional coding.

Motivated by these results, we investigate correspondences of this form for the worst-case hardness of NP (i.e., $\mathsf{NP} \not\subseteq \mathsf{BPP}$) and for the average-case hardness of NP (i.e., $\mathsf{DistNP} \not\subseteq \mathsf{HeurBPP}$), respectively. Our results establish the existence of similar *dualities* between these computational assumptions and the failure of results from Kolmogorov complexity in the time-bounded setting. In particular, these characterizations offer a novel way to investigate the main hardness conjectures of complexity theory (and the relationships among them) through the lens of Kolmogorov complexity and its properties.

CCS CONCEPTS

• **Theory of computation → Computational complexity and cryptography**.

KEYWORDS

Kolmogorov complexity, symmetry of information, one-way functions, average-case complexity

ACM Reference Format:
Shuichi Hirahara, Rahul Ilango, Zhenjian Lu, Mikito Nanashima, and Igor C. Oliveira. 2023. A Duality between One-Way Functions and Average-Case Symmetry of Information. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23), June 20–23, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3564246.3585138

1 INTRODUCTION

1.1 Context and Motivation

A basic and fundamental property in Shannon's information theory is *Symmetry of Information* (SoI). Informally, SoI says that for any two random variables X and Y the amount of information that X reveals about Y is the same as the amount of information that Y reveals about X. Formally, it says that

$$I(X;Y) \;=\; H(Y) - H(Y \mid X) \;=\; H(X) - H(X \mid Y)\,,$$

where H denotes the entropy function. Equivalently, symmetry of information is often written as:

$$H(X,Y) \;=\; H(Y) + H(X \mid Y) \;=\; H(X) + H(Y \mid X)\,,$$

where $H(X,Y)$ denotes the entropy of the jointly distributed random variable (X,Y).

Symmetry of information is also a basic and fundamental property of Kolmogorov complexity, which can be viewed as an algorithmic analogue of information theory. The Kolmogorov complexity $\mathsf{K}(x)$ of a string x is the length of the smallest program p that outputs x (when p is fed to an a priori fixed universal Turing machine). The conditional Kolmogorov complexity of x given y, written $\mathsf{K}(x \mid y)$, is defined similarly, with the difference that y is provided as input to the universal machine. Zvonkin and Levin [50]

*The full version of the paper is available at [18].

†Supported by JST, PRESTO Grant Number JPMJPR2024, Japan.
‡Supported by an NSF Graduate Research Fellowship and NSF CCF-1909429.
§This work received support from the Royal Society University Research Fellowship URF\R1\191059, the EPSRC New Horizons Grant EP/V048201/1, and the Centre for Discrete Mathematics and its Applications (DIMAP) at the University of Warwick.

STOC '23, June 20–23, 2023, Orlando, FL, USA

ACM ISBN 978-1-4503-9913-5/23/06…$15.00
https://doi.org/10.1145/3564246.3585138

(actually, [50] credits Levin and Kolmogorov independently) show that the SoI property from information theory also holds for Kolmogorov complexity, with an additive logarithmic loss. Formally, for any strings x and y,

$$\mathrm{K}(x, y) \approx \mathrm{K}(y) + \mathrm{K}(x \mid y) \approx \mathrm{K}(x) + \mathrm{K}(y \mid x) ,$$

up to an additive factor of order $\pm O(\log(|x|+|y|))$ in each equation. Written this way, symmetry of information roughly says that: (*i*) to describe both x and y it suffices to first describe y optimally without considering x and then describe x optimally assuming access to a description of y; and (*ii*) there is no significantly better way to describe a pair of strings x, y. Note that (*i*) is easily seen to hold, while (*ii*) is non-trivial and states that

$$\mathrm{K}(x, y) \geq \mathrm{K}(x \mid y) + \mathrm{K}(y) - O(\log(|x| + |y|)) .$$

Symmetry of information has found numerous applications in a variety of areas (see the textbooks [27, 45] for a comprehensive introduction) and is widely regarded as one of the main pillars of the theory of Kolmogorov complexity (see, e.g., [25]).

Time-Bounded Kolmogorov Complexity. A disadvantage of Kolmogorov complexity is that it does not take into account the complexity of generating the string x. This issue is particularly significant in applications to algorithms and complexity theory, where the running time is a crucial parameter. Remarkably, in his seminal paper [23, Section 4], Kolmogorov also proposed the study of *t-time-bounded Kolmogorov complexity*, denoted by $\mathrm{K}^t(x)$, which is the shortest size of a program that prints x in time at most t. Similarly to Kolmogorov complexity, the theory of time-bounded Kolmogorov complexity has been widely investigated and has led to several influential results and applications (see, e.g., [2, 3, 14, 15, 22, 28, 40, 46]).

Motivated by the prominent role of symmetry of information in Kolmogorov complexity, the existence of a *time-bounded* symmetry of information principle has been considered since the early years of algorithmic information theory. According to Levin (see [26]), already in the sixties Kolmogorov suggested time-bounded versions of symmetry of information as an interesting research question [24]. Unfortunately, the classical proof that SoI holds for (time-unbounded) Kolmogorov complexity requires an exhaustive search, and as such, the same argument is not applicable in the time-bounded setting.

One-Way Functions and Time-Bounded Symmetry of Information. In the nineties, Longpré and Mocas [32] and Longpré and Watanabe [33] established a connection between time-bounded SoI and the existence of cryptographic one-way functions. More precisely, they proved that if SoI holds for time-bounded Kolmogorov complexity then one-way functions do not exist. Since one-way functions are both necessary and sufficient for the existence of a variety of fundamental cryptographic primitives, such as private-key encryption [12], pseudorandom generators [13], digital signatures [43], and commitment schemes [38], their result further highlights the significance of understanding the validity of SoI in the time-bounded setting.

Longpré and Mocas [32] asked if a converse result holds, i.e., if time-bounded symmetry of information characterizes the non-existence of one-way functions. Similarly, Longpré and Watanabe [33] mentioned that their ultimate goal would be to prove some if and only if statement regarding symmetry of information. In the same paper, they showed that time-bounded SoI holds if $\mathrm{P} = \mathrm{NP}$, which is stronger than the assumption that one-way functions do not exist. Recent papers (Hirahara [17], Goldberg and Kabanets [8], and Goldberg, Kabanets, Lu, and Oliveira [9]) improved this by deriving time-bounded SoI from weaker assumptions on average-case complexity of NP. However, establishing a *characterization* of the existence of one-way functions (or of any other computational assumption) through SoI has remained elusive.

1.2 Results

We confirm the existence of a tight relationship between symmetry of information and cryptography, by establishing the first *characterization* of one-way functions using SoI. More precisely, our results show that one-way functions exist if and only if time-bounded SoI fails on average, i.e., if there is a samplable distribution of pairs (x, y) of strings such that time-bounded SoI fails for many of these pairs.

In order to state unconditional characterizations, we work in the setting of probabilistic Kolmogorov complexity, i.e., our results are stated for the measures rK^t and pK^t. These measures naturally extend the theory of time-bounded Kolmogorov complexity to the realm of probabilistic algorithms. Intuitively, this is a more suitable perspective in our context, given that the security of a one-way function refers to probabilistic polynomial-time adversaries. Nevertheless, under standard derandomization assumptions our results can also be stated for the classical notion of K^t complexity employed in early papers in the area.

Before formally stating our results, we briefly review the necessary notions from probabilistic Kolmogorov complexity. We discuss additional related work in Section 1.5.

Probabilistic Kolmogorov Complexity. Thanks to the ubiquitous role of randomness in algorithms and complexity, probabilistic Kolmogorov complexity has found a number of applications in recent years (e.g., [9, 17, 34, 36, 37, 39]). As alluded to above, we consider two notions that extend (deterministic) time-bounded Kolmogorov complexity K^t to the setting of randomized algorithms: rK^t complexity and pK^t complexity. We briefly review these notions below, referring to Section 2 for their formal definitions.

For a string x, we let $\mathrm{rK}^t(x)$ denote the shortest size of a randomized program that prints x with probability at least $2/3$ when running for at most t steps. We refer to $\mathrm{rK}^t(x)$ as the *randomized t-time bounded Kolmogorov complexity of* x. Intuitively, there is a short and efficient randomized program that prints x with high probability. The code of this program serves as a description of x.

On the other hand, we let $\mathrm{pK}^t(x)$ denote the smallest integer k such that, with probability at least $2/3$ over the choice of a random string $w \sim \{0,1\}^t$, there is a (deterministic) program that when given w prints x within at most t steps. In other words, for a typical random string w, the string x has a t-time bounded description of length at most k given w. We refer to $\mathrm{pK}^t(x)$ as the *probabilistic*

t-time bounded Kolmogorov complexity of x. Informally, this notion can be interpreted as K^t in the presence of a random string shared by all parties involved in a computation.

Under a standard derandomization assumption, Goldberg, Kabanets, Lu, and Oliveira [9] proved that, for every string x, $\mathsf{K}^t(x)$, $\mathsf{rK}^t(x)$, and $\mathsf{pK}^t(x)$ are the same up to an additive factor of $O(\log |x|)$ and at most a polynomial overhead in the running time t. (Roughly speaking, this is similar in nature to the conjectured collapse NP = MA = AM.) For this reason, the results presented next also hold for K^t complexity, under a standard derandomization assumption. However, as in previous works, probabilistic Kolmogorov complexity allows us to obtain unconditional statements. We refer to the survey [35] for more information about rK^t and pK^t and their applications in algorithms and complexity theory.

1.2.1 One-Way Functions, Symmetry of Information, and Kolmogorov Complexity. As alluded to above, our main results establish a *duality* between the (non-)existence of one-way functions and the validity of the symmetry of information principle in the time-bounded setting for most pairs of strings. More generally, we establish that the preservation in the time-bounded setting of average-case versions of other key principles from Kolmogorov complexity is completely captured by one-way functions.

Theorem 1 (Duality Between One-way Functions and Properties of pK). *The following are equivalent.*

(1) *Infinitely-often one-way functions do not exist.*
(2) **(Average-Case Symmetry of Information)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every polynomial q, there exists a polynomial p such that for every computable time bound $t\colon \mathbb{N} \to \mathbb{N}$ with $t(n) \geq p(n)$ and for all large enough n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathsf{pK}^{t(n)}(x,y) \geq \mathsf{pK}^{t(n)}(x \mid y) + \mathsf{pK}^{t(n)}(y) - \log t(n)\right] \geq 1 - \frac{1}{q(n)}$$

(3) **(Average-Case Conditional Coding)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every polynomial q, there exists a polynomial p such that for all large enough n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathsf{pK}^{p(n)}(x \mid y) \leq \log \frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(4) **(Average-Case Language Compression)** *For every recursively enumerable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_{n\in\mathbb{N}}$, every polynomial time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and every polynomial q, there exists a polynomial p such that for all large enough n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[x \in L_y \implies \mathsf{pK}^{p(n)}(x \mid y) \leq \log |L_y| + \log p(n)\right] \geq 1 - \frac{1}{q(n)},$$

where $L_y = \{x \in \{0,1\}^n \mid (x,y) \in L\}$.

Observe that a coding theorem for pK^t with optimal parameters is known to hold unconditionally [37]. In contrast, Theorem 1 Item 3 considers *conditional* coding, where we relate conditional pK^t complexity and conditional probability. This exhibits a contrast between (time-unbounded) Kolmogorov complexity, where coding and conditional coding can be established, and time-bounded Kolmogorov complexity, where coding holds but conditional coding does not hold under a cryptographic assumption.

Note that in Theorem 1 (Items 2-4) we stated high probability versions of each property of Kolmogorov complexity. As a consequence of our proof, we can show that the low probability (i.e., non-negligible) and high probability versions of these statements are all equivalent (see Section 3). The result is also robust with respect to almost-everywhere versus infinitely-often statements, i.e., it is possible to prove that one-way functions do not exist if and only if the average-case Kolmogorov complexity properties hold infinitely often.

An interesting aspect of the average-case setting is that we can employ a statement of symmetry of information where the same time bound $t(n)$ appears on both sides of the inequality (Theorem 1 Item 2). In recent papers that establish worst-case SoI under an easiness assumption (e.g., [8, 9, 17]), there is a loss of parameters and the inequalities are of the form $\mathsf{pK}^{t(n)}(x,y) \geq \mathsf{pK}^{p(t(n))}(x \mid y) + \mathsf{pK}^{p(t(n))}(y) - \log p(t(n))$, for some polynomial $p(\cdot)$.

Relevance to the Foundations of Cryptography. Our result reveals a deep relationship between the existence of secure cryptography and the failure of the symmetry of information principle for efficient computations. We discuss this in more detail now.

Consider the output of a polynomial-time computable function $y = f(x)$, and assume for simplicity that f is an injective function. Since given x we can efficiently recover y, x contains all the necessary information about y. On the other hand, intuitively, we can break a candidate one-way function f if $y = f(x)$ contains sufficient information for us to efficiently recover x from it. Longpré and Watanabe [33] made this intuition formal in the context of an arbitrary polynomial-time computable function f, i.e., they proved that if SoI holds in the time-bounded setting then secure one-way functions do not exist. In other words, the existence of one-way functions necessarily breaks the symmetry of information between y and x in the time-bounded setting. Indeed, this must hold for a non-negligible fraction of such pairs of strings.

Our result completes the picture by showing that a failure of symmetry of information for a non-negligible fraction of pairs (x,y) of strings produced by a samplable distribution is all we need to construct key cryptographic primitives such as one-way functions, private-key encryption, digital signatures, commitment schemes, etc. In other words, the existence of secure cryptography can be formally characterized by a break of the computational/information symmetry between the input and output of an efficiently computable function with respect to polynomial-time computations.

In our next result, we consider two natural questions posed to us by Watanabe [49]:

- Is it possible to get an unconditional equivalence between the non-existence of a one-way function and symmetry of information for rK?
- The usual notions of time-bounded Kolmogorov complexity do not refer to the complexity of producing a succinct encoding. Can we efficiently compute a short program that "witnesses" the symmetry of information inequality $\mathsf{rK}^t(x \mid y) \lesssim \mathsf{rK}^t(x,y) - \mathsf{rK}^t(y)$?

We are able to answer these questions in the quasi-polynomial-time regime. In the statement below, a quasi-polynomial is a function of the form $\exp(\log^c n)$, for some constant $c \in \mathbb{N}$.

Theorem 2 (Duality Between One-way Functions and Properties of rK). *The following are equivalent.*

(1) *Infinitely-often polynomial-time-computable one-way functions secure against quasi-polynomial-time randomized algorithms do not exist.*
(2) **(Average-Case Symmetry of Information)** *For every polynomial time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every quasipolynomial q, there exists a quasipolynomial p such that for every computable time bound $t\colon \mathbb{N} \to \mathbb{N}$ with $t(n) \geq p(n)$ and for all large enough n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathsf{rK}^{t(n)}(x,y) \geq \mathsf{rK}^{t(n)}(x \mid y) + \mathsf{rK}^{t(n)}(y) - \log t(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(3) **(Average-Case Symmetry of Information with an Efficient Encoder)** *In addition to Item 2, there exists a quasi-polynomial-time randomized algorithm M that takes $(x,y) \sim \mathcal{D}_n$ and, with probability $\geq 1 - 1/q(n)$ over the choice of (x,y) and the internal randomness of M, outputs the description of a randomized program of length $\leq \mathsf{rK}^{t(n)}(x,y) - \mathsf{rK}^{t(n)}(y) + \log t(n)$ that takes y as input and outputs x with high probability in time $p(n)$.*
(4) **(Average-Case Approximation of K by $\mathsf{rK}^{\mathsf{quasipoly}}$)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every quasi-polynomial q, there exists a quasi-polynomial p such that for all large enough n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathsf{rK}^{p(n)}(x \mid y) \leq \mathsf{K}(x \mid y) + \log p(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(5) **(Average-Case Approximation of K by $\mathsf{rK}^{\mathsf{quasipoly}}$ with an Efficient Encoder)** *In addition to Item 4, there exists a quasi-polynomial-time randomized algorithm M that takes $(x,y) \sim \mathcal{D}_n$ as input and, with probability $\geq 1 - 1/q(n)$ over the choice of (x,y) and the internal randomness of M, outputs the description of a randomized program of length $\leq \mathsf{K}(x \mid y) + \log p(n)$ that takes y as input and outputs x with high probability in time $p(n)$.*

In our opinion, Theorem 2 Item 4 is particularly striking. It shows that, under the ability to invert one-way functions, time-bounded Kolmogorov complexity and Kolmogorov complexity essentially coincide for most strings generated by a samplable distribution. In a sense, this explains why all key properties of Kolmogorov complexity survive on average if one-way functions do not exist.

An unexpected consequence of the equivalences in Theorem 2 is that if time-bounded SoI holds on average then time-bounded SoI holds on average with an efficient encoder.

For succinctness, we emphasized different aspects of Kolmogorov complexity in the equivalences appearing in Theorem 1 and Theorem 2. We stress that it is not difficult to adapt our techniques so that in both statements we obtain the same set of results (e.g., an average-case conditional coding statement in Theorem 2 or the approximation of K by pK in Theorem 1). The only fundamental difference between these characterizations is that for rK our techniques can only be applied in the quasi-polynomial regime.

1.2.2 Complexity Theory Through the Lens of Kolmogorov Complexity. Inspired by these results, we begin investigating whether other central questions in complexity theory could also be captured through structural properties of time-bounded Kolmogorov complexity. First, we consider the average-case complexity of NP. Since the assumption that NP is easy on average is stronger than the assumption that one-way functions do not exist, it is natural to suspect that a stronger form of the aforementioned average-case principles might hold in this case.

While in Theorem 1 Items 2-4 we sampled a pair (x,y) of strings from $\mathcal{D}$, our next result will consider a more general way of sampling (x,y). In more detail, we consider a distribution C supported over $\{0,1\}^n$ and a distribution $\mathcal{D}$ supported over $\{0,1\}^n \times \{0,1\}^n$. In order to sample a pair (x,y), we first sample $y \sim C$, then sample $x \sim \mathcal{D}(\cdot \mid y)$. It turns out that such a change completely captures the difference between inverting one-way functions and solving problems in NP on average.

Theorem 3 (Duality Between DistNP vs HeurBPP and Kolmogorov Complexity). *The following are equivalent.*

(1) $\mathsf{DistNP} \subseteq \mathsf{HeurBPP}$.
(2) **(Independent Average-Case Conditional Coding)** *For every polynomial-time samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over the support of the second half of $\mathcal{D}_n$, and for every polynomial q, there exists a polynomial p such that for all large enough n,*

$$\Pr_{y\sim C_n, x\sim\mathcal{D}_n(\cdot\mid y)}\left[\mathsf{pK}^{p(n)}(x \mid y) \leq \log\frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(3) **(Independent Average-Case Language Compression)** *For every recursively enumerable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_{n\in\mathbb{N}}$, for every polynomial-time samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over the support of the second half of $\mathcal{D}_n$, and for every polynomial q, there exists a polynomial*

p such that for all large enough n,

$$\Pr_{y\sim C_n, x\sim \mathcal{D}_n(\cdot|y)}[x \in L_y \implies \mathsf{pK}^{p(n)}(x \mid y) \leq \log|L_y| + \log p(n)] \geq 1 - \frac{1}{q(n)}.$$

We also show that the assumption that DistNP $\subseteq$ HeurBPP implies a stronger form of Average-Case Symmetry of Information called Independent Average-Case Symmetry of Information (see Theorem 13 in Section 5). However, this result is not yet an equivalence. We discuss this in more detail in Section 1.4.

Finally, we consider the worst-case complexity of NP, and the possibility of capturing this setting through Kolmogorov complexity.

Theorem 4 (Duality Between NP vs BPP and Kolmogorov Complexity). *The following are equivalent.*

(1) NP $\subseteq$ BPP.
(2) **(Worst-Case Conditional Coding)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, there exists a polynomial p such that for all large enough n and $(x,y) \in \mathsf{Support}(\mathcal{D}_n)$,*
$$\mathsf{pK}^{p(n)}(x \mid y) \leq \log \frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n).$$
(3) **(Worst-Case Language Compression)** *For every polynomial time computable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_{n\in\mathbb{N}}$, there exists a polynomial p such that for all large enough n and all $x, y \in \{0,1\}^n$,*
$$x \in L_y \implies \mathsf{pK}^{p(n)}(x \mid y) \leq \log|L_y| + \log p(n).$$

Moreover, the above equivalence continues to hold if we replace pK *with* rK *in Item 2 and Item 3.*

Similarly to Theorem 3, the role of symmetry of information in the setting of Theorem 4 remains unclear. We refer to Section 1.4 for a discussion on this.

These duality results uncover a far-reaching correspondence between computational assumptions and key aspects of time-bounded Kolmogorov complexity. In particular, these characterizations offer a novel way to investigate the main hardness conjectures of complexity theory (and the relationships among them) through the lens of Kolmogorov complexity and its properties.

1.3 Techniques

In this section, we explain the main ideas behind our proofs. We focus on Theorems 1, 2, and 3.

Theorem 1: OWFs vs Average-Case SoI for pK^t via Conditional Coding. The equivalence between the non-existence of one-way functions and average-case symmetry of information is proved via average-case conditional coding. That is, we first show that one-way functions do not exist if and only if average-case conditional coding holds. We then argue that symmetry of information and conditional coding are equivalent in the average-case setting.

Part 1: OWFs vs Conditional Coding. First, we explain how the non-existence of one-way functions implies average-case conditional coding. Consider an arbitrary samplable distribution $\{\mathcal{D}_n\}_n$ over $\{0,1\}^n \times \{0,1\}^n$ and assume one-way functions do not exist. Our goal is to, on average when (x,y) is sampled from $\mathcal{D}_n$, give a short (length roughly $\log \frac{1}{\mathcal{D}_n(x|y)}$) and efficient (time at most $p(n)$) description of x given access to y.

To gain some intuition, let us ignore the efficient part for now and recall how to prove the conditional coding theorem in the time-unbounded setting. First, we can assume without loss of generality that $D_n(x \mid y) \geq 2^{-n}$, since otherwise the desired bound on the complexity of x given y is trivial. One description of x would be to first describe the probability $p = \mathcal{D}_n(x \mid y)$ that x is sampled from $\mathcal{D}_n(\cdot \mid y)$ and then describe the index of x in the set $\{x' : \mathcal{D}_n(x' \mid y) \geq p\}$, which contains at most $1/p = 1/\mathcal{D}_n(x \mid y)$ elements. In general, this gives an (inefficient) description for x of length at least n bits (to describe the value $\mathcal{D}_n(x \mid y)$) plus $\log \frac{1}{\mathcal{D}_n(x|y)}$ bits (to describe the index). Thus, this description's length is worse than the trivial bound of $n + O(1)$ for x! To improve this, one uses a standard trick in Kolmogorov complexity: instead of describing $\mathcal{D}_n(x \mid y)$, one describes the largest power of two less than or equal to $\mathcal{D}_n(x \mid y)$. Let α be this value. Then, given α, one can also specify the index of x in the set $\{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$. This gives a description for x given y of length at most $\log n$ (to describe α) plus at most $\log \frac{1}{\alpha} = O(1) + \log \frac{1}{D_n(x|y)}$, as desired. However, this description is not an efficient one. Indeed, even assuming one-way functions do not exist, it is unclear how to easily compute the i-th element of the set $\{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$ on average.

Instead, we take a different approach that relies on hashing. Our description of x given y will still include α, but instead of specifying the index of x in the set $\{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$, we will specify the hash value $v = H(x)$ of x where H is a randomly chosen pairwise independent hash function. Setting parameters appropriately, we can guarantee that with high probability that v is of length $\log \frac{1}{\mathcal{D}_n(x|y)} + O(1)$ and that $v \neq H(x')$ for all $x' \in \{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$. Thus, the value v uniquely specifies x in the set $\{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$ and so this gives a description of x given y of length $(\log \frac{1}{\mathcal{D}_n(x|y)} + O(1)) + \log n + \log n$ (the first term comes from specifying v, the second from specifying α, and the third from specifying H).

We show that this description is also efficient on average assuming one-way functions do not exist. A first attempt might be to consider the candidate one-way function that takes as input randomness r, a parameter α, and a random hash function H, and outputs $(H(x), y, H, \alpha)$ where (x,y) is sampled from $\mathcal{D}_n$ using the randomness r. Since one-way functions do not exist, this function can be inverted on average. Thus, to try to go from the description (v, α, H) back to x one could try to run the inverter to find an x' such that $H(x') = v$. The difficulty is that x' is not guaranteed to be in the set $\{x' : \mathcal{D}_n(x' \mid y) \geq \alpha\}$ and so x' might not equal x, even though they both hash to v!

To get around this, we show that, assuming one-way functions do not exist, there exists an efficient algorithm B such that on average $B(x,y)$ outputs a constant factor approximation of $\mathcal{D}_n(x \mid y)$. Crucially, however $B(x,y)$ *never overestimates* $\mathcal{D}_n(x \mid y)$ (even in the worst-case). To prove the existence of B we build on [20, 21]. Assuming we have B, we can then consider the candidate one-way function that takes as input randomness r, a parameter α, and a

random hash function H, then samples (x, y) from $\mathcal{D}_n$ using the randomness r and outputs $\perp$ if $B(x, y) \le \alpha$ and otherwise outputs $(H(x), y, H, \alpha)$. This means that the one-way function always outputs $\perp$ on any x' where $\mathcal{D}_n(x' \mid y) < \alpha$. Using this new candidate one-way function, we can fix the aforementioned difficulty in the previous paragraph and efficiently go from the description (v, α, H) back to x, as desired.

We note that pK complexity is particularly useful when implementing the plan described above, since we need random bits (e.g., to obtain H) and additional information that depends on the choice of these random bits (e.g., the hash value $v = H(x)$ once we have H).

To show that average-case conditional coding theorem allows us to break any candidate one-way function $f\colon \{0,1\}^n \to \{0,1\}^n$, we consider a (polynomial-time samplable) distribution $\mathcal{D}$ which samples $(x, f(x))$, where x is uniformly random. Note that this distribution can be equivalently viewed as first sampling $y := f(z)$ for a uniformly random z and then sampling $x \sim \mathcal{D}(\cdot \mid y)$, where, crucially, $\mathcal{D}(\cdot \mid y)$ is uniformly distributed on $f^{-1}(y)$. Now assuming that average-case conditional coding holds, we have for most pairs (x, y) sampled from $\mathcal{D}$,

$$\mathsf{pK}^{\mathrm{poly}(n)}(x \mid y) \lesssim \log \frac{1}{\mathcal{D}(x \mid y)}.$$

Then, by an averaging argument, for most $y := f(z)$ (where z is uniformly random) the above condition holds with high probability over x sampled from $\mathcal{D}(\cdot \mid y)$. Since $\mathcal{D}(\cdot \mid y)$ is uniformly distributed on $f^{-1}(y)$, this means that for most (say at least half) $x \in f^{-1}(y)$, it is the case that

$$\mathsf{pK}^{\mathrm{poly}(n)}(x \mid y) \lesssim \log \frac{1}{\mathcal{D}(x \mid y)} = \log |f^{-1}(y)|. \tag{1}$$

A useful property of probabilistic Kolmogorov complexity is that if $\mathsf{pK}^{\mathrm{poly}(n)}(a \mid b)$ is at most k, where $a, b \in \{0,1\}^n$, then there is a universal randomized algorithm USamp that, given b as input, runs in $\mathrm{poly}(n)$ time and outputs a with probability at least $1/O\left(n \cdot 2^k\right)$. Then combining this fact with Equation (1), we get that for at least half of the $x \in f^{-1}(y)$, $\mathrm{USamp}(y)$ outputs x with probability at least $1/O\left(n \cdot |f^{-1}(y)|\right)$, which implies that it outputs *some* $x' \in f^{-1}(y)$ with probability at least $1/O(n)$. This gives an efficient algorithm that finds a pre-image of y with high probability, for most y.

Part 2: Conditional Coding vs Symmetry of Information. It remains to show the equivalence between average-case conditional coding and average-case symmetry of information. We describe how to get the latter from the former. Roughly speaking, if average-case conditional coding holds, then we have for every polynomial-time samplable distribution $\mathcal{D}$ over $\{0,1\}^n \times \{0,1\}^n$ and for almost all pairs (x, y) sampled from $\mathcal{D}$,

$$\mathsf{pK}^{\mathrm{poly}(n)}(x \mid y) \lesssim \log \frac{1}{\mathcal{D}(x \mid y)}.$$

By the fact that $\mathcal{D}(x \mid y) = \mathcal{D}(x, y)/\mathcal{D}'(y)$, where $\mathcal{D}'$ is the marginal distribution of $\mathcal{D}$ on the second half, we can rewrite the above as

$$\mathsf{pK}^{\mathrm{poly}(n)}(x \mid y) \lesssim \log \frac{1}{\mathcal{D}(x, y)} - \log \frac{1}{\mathcal{D}'(y)}. \tag{2}$$

Remember that for symmetry of information, we aim to show

$$\mathsf{pK}^{\mathrm{poly}(n)}(x \mid y) \lesssim \mathsf{pK}^{\mathrm{poly}(n)}(x, y) - \mathsf{pK}^{\mathrm{poly}(n)}(y). \tag{3}$$

Therefore, it suffices to show that $\mathsf{pK}^{\mathrm{poly}(n)}(x, y) \gtrsim \log \frac{1}{\mathcal{D}(x,y)}$ and that $\mathsf{pK}^{\mathrm{poly}(n)}(y) \lesssim \log \frac{1}{\mathcal{D}'(y)}$. Note that the second inequality is exactly the (ordinary) coding theorem for $\mathsf{pK}^{\mathrm{poly}}$, which holds unconditionally thanks to [37]. For the first inequality, we use an "incompressibility" property of Kolmogorov complexity, which says that for every distribution $\mathcal{E}$, almost all elements z sampled from $\mathcal{E}$ have (resource-unbounded) Kolmogorov complexity at least $\log \frac{1}{\mathcal{E}(z)}$ minus some small additive term (see Lemma 7). Since it can be shown that $\mathsf{pK}^{\mathrm{poly}(n)}(x, y)$ is lower bounded by $\mathsf{K}(x, y)$ (modulo some additive logarithmic term), we get that the first inequality holds for almost all (x, y) sampled from $\mathcal{D}$.

Similarly, to show that average-case symmetry of information implies average-case conditional coding, we can "reverse" the above argument and show Equation (2) from Equation (3), in which case we need to show $\mathsf{pK}^{\mathrm{poly}(n)}(x, y) \lesssim \log \frac{1}{\mathcal{D}(x,y)}$ and $\mathsf{pK}^{\mathrm{poly}(n)}(y) \gtrsim \log \frac{1}{\mathcal{D}'(y)}$. These again follow from the coding theorem and the "incompressibility" property for $\mathsf{pK}^{\mathrm{poly}}$.

Theorem 2: OWFs & Average-Case SoI for rK^t. To show the equivalence between average-case SoI for rK^t and the non-existence of quasi-polynomial-time variants of one-way functions, we employ a general approach of showing symmetry of information from meta-complexity [17]. It was shown in [17] that the existence of an efficient algorithm that approximates resource-bounded Kolmogorov complexity implies a corresponding version of SoI. We apply a similar proof technique to the average-case setting, and show that Item 1 implies Item 4 in Theorem 2, i.e., $\mathsf{rK}^{\mathrm{poly}}$ is approximated by K if a one-way function does not exist. For simplicity, we consider polynomial-time bounds in this proof overview.

The key technical ingredient is a *pseudorandom generator construction* $G_k\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^k$ [47]. A pseudorandom generator construction takes a "hard" string $x \in \{0,1\}^n$ and a seed $z \in \{0,1\}^d$ and outputs a pseudorandom sequence $G_k(x; z)$ with the following reconstruction property. If a function D distinguishes the output distribution of $G_k(x; \text{-})$ from the uniform distribution, then the D-oracle Kolmogorov complexity of x is small. In other words, if the D-oracle Kolmogorov complexity of x is large, then the output distribution $G_k(x; \text{-})$ looks pseudorandom to D. Following [17], we use the specific pseudorandom generator construction of [41], which satisfies the reconstruction property that

$$\mathsf{rK}^{\mathrm{poly}(n),D}(x) \le k + O(\log^3 n) \tag{4}$$

and the seed length is $d = O(\log^3 n)$. Moreover, a pseudorandom generator construction has an "advice function", which outputs the witness for Equation (4), namely, the description of a D-oracle randomized program of length $k + O(\log^3 n)$ that prints x with high probability. This property enables us to show SoI with an efficient encoder.

We instantiate the approach of [17] using the approximation algorithm of [19]. Under the assumption that there is no one-way

function, it was shown in [19] that for every polynomial-time samplable distribution $\mathcal{D}$, there exists an efficient average-case algorithm A that approximates the *resource-unbounded* Kolmogorov complexity $\mathsf{K}(x)$ of a string $x \sim \mathcal{D}$. We observe that this algorithm enables us to approximate the conditional Kolmogorov complexity $\mathsf{K}(x \mid y)$ as well because

$$\mathsf{K}(x \mid y) \approx \mathsf{K}(x, y) - \mathsf{K}(y)$$

by the symmetry of information for K. Let A be an average-case algorithm that approximates $\mathsf{K}(x \mid y)$ on input $(x, y) \sim \mathcal{D}$.

Using the algorithm A, let us explain how to prove $\mathsf{rK}^{\mathsf{poly}}(x \mid y) \approx \mathsf{K}(x \mid y)$ for most $(x, y) \sim \mathcal{D}$. The idea is to try to distinguish the pseudorandom generator construction $G_k(x;\text{-})$ from the uniform distribution by using the approximation algorithm A. On the one hand, observe that

$$A(G_k(x;z), y) \approx \mathsf{K}(G_k(x;z) \mid y) \lesssim \mathsf{K}(x \mid y) + |z|$$

because $G_k(x;z)$ is computable given x, z and k as input. Note that $|z| = O(\log^3 n)$, which is negligible. On the other hand, by a standard counting argument, we have

$$A(w, y) \approx \mathsf{K}(w \mid y) \gtrsim k$$

for a random $w \sim \{0,1\}^k$. These two inequalities show that when $k \gtrsim \mathsf{K}(x \mid y)$, the algorithm $A(\text{-}, y)$ can distinguish $G_k(x;\text{-})$ from the uniform distribution. By the reconstruction property from Equation (4), we obtain $\mathsf{rK}^{\mathsf{poly}(n)}(x \mid y) \le k \approx \mathsf{K}(x \mid y)$, which completes the proof.

In fact, there are important technical details hidden in the outline above. We need to choose $k \approx \mathsf{K}(x \mid y)$ depending on (x, y), which is chosen randomly from a distribution $\mathcal{D}$. Thus, the distribution $(G_k(x;z), y)$ may not be polynomial-time samplable in general. This is problematic for us because A is guaranteed to work correctly only with respect to polynomial-time samplable distributions. The issue is not present in the worst-case setting [17]. Fortunately, it turns out that there is a simple way to circumvent this issue. We consider a distribution that randomly chooses $k \sim [2n]$ as the input distribution of A. Using that A works correctly with high probability, we can use A to approximate $\mathsf{K}(G_k(x;z) \mid y)$ for *every* $k \in [2n]$ for a randomly chosen $(x, y) \sim \mathcal{D}$.

Once we obtain the approximation of $\mathsf{rK}^{\mathsf{poly}}$ by K, SoI for $\mathsf{rK}^{\mathsf{poly}}$ easily follows from SoI for K.

To prove that SoI for $\mathsf{rK}^{\mathsf{poly}}$ implies the non-existence of one-way functions, a natural idea is to try to follow our approach for Theorem 1. However, an unconditional (ordinary) coding theorem for rK is currently unknown, and this was an important ingredient in that argument. Instead, we adapt the proof ideas of [33] to the average-case setting. In general, they proved that if SoI for $\mathsf{K}^{\mathsf{poly}}$ holds with an additive error of $e(n)$, then any one-way function can be inverted in time $n^{O(1)} \cdot 2^{O(e(n))}$. In our case, the reconstruction property of Equation (4) incurs an additive error of $O(\log^3 n)$, which makes the running time of the inverter quasi-polynomial. More generally, this is why the equivalence is proved in the quasi-polynomial time regime.

This completes our sketch of the proof of Theorem 2.

The proof overviews presented above highlight two perspectives that can be leveraged to obtain a characterization of the existence one-way functions via average-case symmetry of information: (*i*) employing conditional coding as a bridge between the two statements, and (*ii*) a meta-computational approach through meta-complexity. The two approaches come with different benefits, and shed light on distinct aspects of the duality between the statements. In terms of generality, we note that the meta-computational approach can also be implemented in the setting of pK^t, which provides a different proof of Theorem 1. On the other hand, the same method does not seem to work in a worst-case complexity setting, since in the worst-case the time-unbounded and time-bounded Kolmogorov complexities of a string can be quite far from each other. In contrast, the conditional coding perspective can be employed to prove Theorem 4 (see Section 6).

Theorem 3: Characterizing DistNP vs HeurBPP via Conditional Extrapolation. The average-case easiness of NP is derived from the *independent* version of conditional coding and language compression in a way that is similar to the other characterization results for one-way functions and the worst-case complexity of NP. Remember that the *independent* version of the statements comes with two samplable distributions C and $\mathcal{D}$, where $\mathcal{D}$ is over $\{0,1\}^n \times \{0,1\}^n$, and C is over conditionings of the second half element of $\mathcal{D}$. To solve an NP problem L on average under a samplable distribution $\mathcal{E}$, we set $\mathcal{D}$ to the distribution of $(x, y \circ b)$, where $x \sim \{0,1\}^n$, $y \sim \mathcal{E}$, and $b = 1$ if and only if x is a witness for $y \in L$ (otherwise, $b = 0$).[1] By letting C be the distribution of $y \circ 1$ for $y \sim \mathcal{E}$, a pair (x, y) selected as $y \circ 1 \sim C$ and $x \sim \mathcal{D}(\cdot \mid y \circ 1)$ is distributed over the witness-instance pairs for L. Crucially, the marginal distribution of y corresponds to $\mathcal{E}$, and in case y is a positive instance, the marginal distribution of x is uniform over the witnesses for y. Using this, the average-case easiness of L follows from the observation that the efficient search of witness from the language compression holds even in the average-case settings with respect to witness-instance pairs.

To show the opposite direction, we introduce a new concept of *conditional extrapolation*, which may be of independent interest. The conditional extrapolation for a joint distribution $\mathcal{D}$ over $\{0,1\}^* \times \{0,1\}^*$ is a probabilistic algorithm CondExt that is given a string y in the support of the second half of $\mathcal{D}$ and selects a sample x according to $\mathcal{D}(\cdot \mid y)$ with a small statistical error (note that $\mathcal{D}(\cdot \mid y)$ is not efficiently samplable in general even if $\mathcal{D}$ is samplable). We are interested in achieving this when y is sampled from a *different* distribution C. In more detail, we consider the following statement involving distributions C and $\mathcal{D}$:

Conditional Extrapolation. There exists a probabilistic polynomial time algorithm CondExt such that for all $\varepsilon^{-1}, \delta^{-1} \in \mathbb{N}$,

$$\Pr_{y \sim C}\left[\mathsf{L}_1\Big(\mathsf{CondExt}(y; 1^{\varepsilon^{-1}}, 1^{\delta^{-1}}), \mathcal{D}(\cdot \mid y)\Big) \le \varepsilon\right] \ge 1 - \delta,$$

where we use the notation L_1 to refer to the total variation distance between two distributions.

[1] The actual construction is a little more involved in order to meet the conditions in the statement; e.g., C is over the support of the second half of $\mathcal{D}$.

As a key lemma in our proof of equivalence, we show that DistNP $\subseteq$ HeurBPP holds if and only if conditional extrapolation is feasible for every samplable joint distribution $\mathcal{D}$ *on average* over the choice of the conditional string y, where y is selected according to an arbitrary samplable distribution C. The proof of the lemma is based on an adaptation of the proof of the well-known equivalence result between one-way functions and distributional one-way functions [21], where we apply a heuristic scheme for the search version of the circuit SAT problem instead of an inverting algorithm.

Conditional extrapolation yields the implication from the average-case easiness of NP to the *independent* version of conditional coding, language compression, and symmetry of information. More specifically, we apply the conditional extrapolation to join two independent samplable distributions C and $\mathcal{D}$ and make a *samplable* distribution of (x, y) for $y \sim C$ and $x \sim \mathcal{D}(\cdot \mid y)$ by regarding the sampling process as $y \sim C$ and $x \sim \mathsf{CondExt}(y)$. Namely, by conditional extrapolation, we can derive the *independent* version of the statements from the corresponding average-case statements for joint samplable distributions. Since the latter is shown under the non-existence of one-way functions (a consequence of DistNP $\subseteq$ HeurBPP), we obtain the *independent* version of the statements from DistNP $\subseteq$ HeurBPP.

1.4 Open Problems

Note that in the context of one-way functions we have obtained a precise characterization through average-case symmetry of information, average-case conditional coding, and average-case language compression. On the other hand, the exact role of symmetry of information remains mysterious in the correspondences for the worst-case easiness of NP and for the average-case easiness of NP. In light of Theorem 3 and Theorem 13, we ask the following question.

Problem 5. *Is Independent Average-Case Symmetry of Information* equivalent *to* DistNP $\subseteq$ HeurBPP*?*

Next, we consider *worst-case* (time-bounded) symmetry of information. Hirahara [17], Goldberg and Kabanets [8], and Goldberg, Kabanets, Lu, and Oliveira [9] showed that the *errorless* average-case easiness of DistNP implies worst-case symmetry of information. For instance, [9] proved that worst-case symmetry of information holds for pK^t under the assumption that DistNP $\subseteq$ AvgBPP. While we believe that some of our results can be adapted to show correspondences between DistNP $\subseteq$ AvgBPP and certain "certified" average-case versions of key principles from Kolmogorov complexity, a proof that worst-case symmetry of information implies a corresponding easiness assumption for NP remains elusive.

Problem 6. *Is there a natural computational assumption that is equivalent to Worst-Case Symmetry of Information?*

It would also be interesting to obtain an unconditional analogue of Theorem 2 in the polynomial time regime. This is connected to the advice complexity of the reconstruction procedure from [41], which incurs a poly-logarithmic additive factor in our bounds on Kolmogorov complexity.

1.5 Related Work

In this section we discuss the broader context surrounding our results, providing pointers to related research directions and the most relevant recent developments.

As mentioned above, Longpré and Watanabe [33] showed that if P = NP then worst-case time-bounded SoI holds. This result has been improved by [8, 17] (see also the subsequent paper [9]), where it was shown that the same conclusion holds under the weaker assumption that NP admits errorless heuristic schemes. In contrast, our results establish the first equivalence between a natural computational assumption (inverting one-way functions) and average-case time-bounded SoI.

Longpré [31] proved that symmetry of information holds for a space-bounded notion of Kolmogorov complexity, while Ronneburger [44] established that it fails for Levin's Kt complexity. Lee and Romashchenko [26] investigate symmetry of information for variants of distinguishing complexity (CD^t), including non-deterministic distinguishing complexity and non-deterministic distinguishing complexity with randomness. On the other hand, here we are concerned with variants of time-bounded Kolmogorov complexity that are equivalent to K^t under standard hardness assumptions. Liu and Pass [30] proved that a general form of time-bounded symmetry of information for strings x and y of different lengths fails when K^t complexity is defined with respect to RAM-machines (as opposed to Turing machines).

Liu and Pass [28] (see also [19, 29, 42]) showed an equivalence between inverting one-way functions and the error-prone average-case easiness of computing K^t complexity. Our results (Theorem 1 and Theorem 2) are incomparable to theirs, as we do not consider an equivalence between two computational assumptions (inverting one-way functions and easiness of computing K^t), i.e., we relate instead one-way functions and the validity of key principles from Kolmogorov complexity in the time-bounded setting. It is worth noting that several additional characterizations of one-way functions are known, e.g., [10, 13, 20, 21].

Several papers have considered coding [3, 34, 37] and language compression [5–7, 15] in the time-bounded setting. While an optimal coding theorem for pK^t is known unconditionally [37], the existence of a result of this form for rK^t and K^t is currently only known under a derandomization assumption (see, e.g., [3]). Weak forms of language compression hold for variants of distinguishing complexity (see [7]). In general, our results and the literature on this topic indicate that language compression most likely does not hold for time-bounded Kolmogorov complexity measures.

One of the proofs discussed in Section 1.3 relies on techniques from meta-complexity, a rapidly developing area which investigates the complexity of computational problems and tasks that are themselves about computations and their complexity. We refer to the surveys [1, 16] for an overview of recent results in this area.

1.6 Organization

Due to space constraints, we state but do not prove our main theorems in the subsequent sections. We refer the interested reader to the full version [18] of the paper for more details.

2 PRELIMINARIES

2.1 Basic Definitions and Notation

For a string $w \in \{0,1\}^*$, we use $|w| \in \mathbb{N}$ to denote its length. The empty string is denoted by ϵ. For any $w \in \{0,1\}^*$ and any $i \le |w|$, we let $w_{[i]}$ denote the i-bit prefix of w.

Probability Distributions. Due to our investigation of conditional coding, we will be mostly interested in distributions supported over pairs of strings. Unless stated otherwise, we use $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ to denote an ensemble of polynomial-time samplable distributions, where each $\mathcal{D}_n$ is supported over $\{0,1\}^{\ell_1(n)} \times \{0,1\}^{\ell_2(n)}$, and ℓ_1 and ℓ_2 are polynomials satisfying $\ell_1(n), \ell_2(n) \ge n$.[2] We let PSamp be the collection of ensembles of distributions that can be sampled in polynomial time. When n is clear from context, we might simply write $\mathcal{D}$ instead of $\mathcal{D}_n$. We use $\mathcal{D}^{(2)}$ to refer to the marginal distribution of the second half element of $\mathcal{D}$.

We use $\mathcal{D}_n(x,y)$ to denote the probability that the pair (x,y) is sampled from $\mathcal{D}_n$. Similarly, $\mathcal{D}_n(x \mid y)$ denotes the probability x is sampled from $\mathcal{D}_n$ given y is sampled.

One-Way Functions. We will be concerned with one-way functions that are secure against uniform probabilistic polynomial-time algorithms (PPTs). As usual, we say that an efficiently computable collection $f = \{f_n\}_{n\ge1}$ satisfying $f_n \colon \{0,1\}^n \to \{0,1\}^{\mathsf{poly}(n)}$ is a *one-way function* (OWF) if for every PPT algorithm A and constant $c \ge 1$ and for every sufficiently large n, we have

$$\Pr_{x\sim\{0,1\}^n}[f(A(1^n, f(x))) = f(x)] \le n^{-c}. \tag{5}$$

It is well known that the existence of one-way functions does not crucially depend on the success probability in this definition (i.e., weak and strong one-way functions are equivalent) and on the output length of each f_n (we can assume output length $m = n$ without loss of generality). We refer to [11] for more details.

Similarly, we say that f is an *infinitely-often one-way function* (i.o. OWF) if for every PPT A and constant $c \ge 1$ as above, there are infinitely many values of n such that Equation (5) holds.

Time-Bounded Kolmogorov Complexity. Let U be a Turing machine. Given a positive integer t and a string $x \in \{0,1\}^*$, we let

$$\mathsf{K}^t_U(x) = \min_{p\in\{0,1\}^*}\left\{|p| \;\middle|\; U(p,\epsilon) \text{ outputs } x \text{ in at most } t \text{ steps}\right\}.$$

We say that $\mathsf{K}^t_U(x)$ is the *t-time-bounded Kolmogorov complexity of x* (with respect to U). As usual, we fix U to be a time-optimal machine [27], and drop the index U when referring to time-bounded Kolmogorov complexity measures. In addition, we use $\mathsf{K}(x)$ to denote the (time-unbounded) Kolmogorov complexity of x.

It will be useful to consider a randomized variant of K^t where instead of having a deterministic machine that prints x, we consider a randomized machine that generates x with high probability. Given a probability parameter $\delta \in [0,1]$ and a positive integer t, we let $\mathsf{rK}^t_\delta(x)$ denote the *t-time-bounded randomized Kolmogorov complexity of x* where $\mathsf{rK}^t_\delta(x)$ equals

$$\min_{p\in\{0,1\}^*}\left\{|p| \;\middle|\; \Pr_{r\sim\{0,1\}^t}[U(p,r) \text{ outputs } x \text{ in at most } t \text{ steps}] \ge \delta\right\}.$$

For simplicity, we omit δ when $\delta = 2/3$, i.e., when x is printed with high probability.

We also make use of another probabilistic variant of $\mathsf{K}^t(x)$ introduced by Goldberg, Kabanets, Lu, and Oliveira [9], which we define next. For a string x, the *probabilistic t-time-bounded Kolmogorov complexity of x*, denoted $\mathsf{pK}^t(x)$, is equal to the minimum $k \in \mathbb{N}$ such that

$$\Pr_{r\sim\{0,1\}^{t(|x|)}}\left[\exists\, p \in \{0,1\}^k \text{ s.t. } U(p,r) = x \text{ in } t(|x|) \text{ steps}\right] \ge \frac{2}{3}.$$

It is known that the deterministic and probabilistic time-bounded Kolmogorov complexities of a string essentially coincide, under a plausible circuit lower bound assumption: for every string x and time bound $t(n) \ge n$, $\mathsf{pK}^t(x) \le \mathsf{K}^t(x)$ and $\mathsf{K}^{\mathsf{poly}(t)}(x) \le \mathsf{pK}^t(x) + O(\log|x|)$ [9]. We refer to [35] for more background on probabilistic time-bounded Kolmogorov complexity and its applications.

These definitions can be extended to *conditional* Kolmogorov complexity in the natural way. For instance, in $\mathsf{pK}^t(x \mid y)$ the machine U is also given access to the input string y. For concreteness, we assume that y is given in a separate input tape.

Average-case Complexity. Recall that a pair $(L,\mathcal{D})$ is a *distributional problem* if $L \subseteq \{0,1\}^*$ and $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ is a distribution family, where each $\mathcal{D}_n$ is over $\{0,1\}^*$.

We let DistNP denote the set of distributional problems $(L,\mathcal{D})$ with $L \in \mathsf{NP}$ and $\mathcal{D} \in \mathsf{PSamp}$.

A distributional problem $(L,\mathcal{D})$ is said to admit a (error-prone) *heuristic scheme* if there exists a probabilistic polynomial-time algorithm A such that for every $n,k \in \mathbb{N}$,

$$\Pr_{x\sim\mathcal{D}_n, A}\left[A(x;1^n,1^k) \ne L(x)\right] \le 1/k.$$

We let HeurBPP denote the set of distribution problems that admit a heuristic scheme. For more information about average-case complexity, we refer to [4].

2.2 Technical Lemmas

Kolmogorov Complexity and Coding Results. We will need the following results.

Lemma 7. *The following two hold.*

(1) *For any distribution family $\{\mathcal{D}_n\}_n$ over $\{0,1\}^n$,*

$$\Pr_{x\sim\mathcal{D}_n}\left[\mathsf{K}(x) < \log\frac{1}{\mathcal{D}_n(x)} - \alpha\right] < \frac{1}{2^\alpha}.$$

(2) *For any distribution family $\{\mathcal{D}_n\}_n$ over $\{0,1\}^n \times \{0,1\}^n$ and any $y \in \mathsf{support}(\mathcal{D}^{(2)}_n)$, where $\mathcal{D}^{(2)}_n$ is the marginal distribution of $\mathcal{D}_n$ on the second half,*

$$\Pr_{x\sim\mathcal{D}_n(\cdot\mid y)}\left[\mathsf{K}(x \mid y) < \log\frac{1}{\mathcal{D}_n(x \mid y)} - \alpha\right] < \frac{1}{2^\alpha}.$$

Pairwise Independent Hash Family. We review below the definition of pairwise independent hash functions.

[2] Recall that $\mathcal{D}$ can be sampled in polynomial time if there is a polynomial-time algorithm Samp such that $\mathsf{Samp}(1^n, r)$ is distributed according to $\mathcal{D}_n$ when r is a uniformly random string of length $\mathsf{poly}(n)$.

Definition 8 (Pairwise Independent Hash Family)**.** For $m, n \in \mathbb{N}$, a family of hash functions $\mathcal{H} := \{h\colon \{0,1\}^n \to \{0,1\}^m\}$ is called *pairwise independent* if, for any distinct $x, x' \in \{0,1\}^n$, and any $y, y' \in \{0,1\}^m$, we have

$$\Pr_{h\sim\mathcal{H}}\left[h(x) = y \wedge h(x') = y'\right] = \frac{1}{2^{2m}}.$$

Theorem 9 (See e.g., [48, Problem 3.3]). *Let $m, n \in \mathbb{N}$. There is a family of pairwise independent hash functions*

$$H_{n,m} := \{h_w\colon \{0,1\}^n \to \{0,1\}^m\}_w,$$

where each h_w is indexed by a $w \in \{0,1\}^{n+m}$. Moreover, given n, m, w, and x, $h_w(x)$ can be computed in time $\mathrm{poly}(n, m)$.

3 ONE-WAY FUNCTIONS, AVERAGE-CASE CONDITIONAL CODING, LANGUAGE COMPRESSION AND SYMMETRY OF INFORMATION

In this section, we give equivalences between the existence of one-way functions and average-case properties of $\mathrm{pK}^{\mathrm{poly}}$.

Theorem 10. *The following are equivalent.*

(1) *Infinitely-often one-way functions do not exist.*
(2) **(Strong Average-Case Conditional Coding)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every polynomial q, there exists a polynomial p such that for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{pK}^{p(n)}(x \mid y) \le \log \frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n)\right] \ge 1 - \frac{1}{q(n)}.$$

(3) **(Weak Average-Case Conditional Coding)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, there exists polynomials p and q such that for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{pK}^{p(n)}(x \mid y) \le \log \frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n)\right] \ge \frac{1}{q(n)}.$$

(4) **(Strong Average-Case Language Compression)** *For every recursive enumerable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_n$, every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and every polynomial q, there exists a polynomial p such that for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[x \in L_y \implies \mathrm{pK}^{p(n)}(x \mid y) \le \log |L_y| + \log p(n)\right] \ge 1 - \frac{1}{q(n)}.$$

(5) **(Weak Average-Case Language Compression)** *For every polynomial-time recursive enumerable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_n$ and every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, there exist polynomials p and q such that for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[x \in L_y \implies \mathrm{pK}^{p(n)}(x \mid y) \le \log |L_y| + \log p(n)\right] \ge \frac{1}{q(n)}.$$

(6) **(Strong Average-Case Symmetry of Information)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every polynomial q, there exists a polynomial p such that for all computable time bound t with $t(n) \ge p(n)$ and for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{pK}^{t(n)}(x, y) \ge \mathrm{pK}^{t(n)}(x \mid y) + \mathrm{pK}^{t(n)}(y) - \log t(n)\right] \ge 1 - \frac{1}{q(n)}.$$

(7) **(Weak Average-Case Symmetry of Information)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, there exist polynomials p and q such that for all computable time bound t with $t(n) \ge p(n)$ and for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{pK}^{t(n)}(x, y) \ge \mathrm{pK}^{t(n)}(x \mid y) + \mathrm{pK}^{t(n)}(y) - \log t(n)\right] \ge \frac{1}{q(n)}.$$

4 ONE-WAY FUNCTIONS AND AVERAGE-CASE SYMMETRY OF INFORMATION FOR $\mathrm{rK}^{\mathrm{quasipoly}}$

We present the characterization of the existence of a one-way function secure against quasipolynomial time adversaries by average case symmetry of information for $\mathrm{rK}^{\mathrm{poly}}$.

Theorem 11. *The following are equivalent.*

(1) *Infinitely-often polynomial-time-computable one-way functions secure against quasi-polynomial-time randomized algorithms do not exist.*
(2) **(Approximation of K by $\mathrm{rK}^{\mathrm{quasipoly}}$)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every quasi-polynomial q, there exists a quasi-polynomial p such that for all n,*

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{rK}^{p(n)}(x \mid y) \le \mathrm{K}(x \mid y) + \log p(n)\right] \ge 1 - \frac{1}{q(n)}.$$

(3) **(Approximation of K by $\mathrm{rK}^{\mathrm{quasipoly}}$ with an Efficient Encoder)** *In addition to Item 2, there exists a quasi-polynomial-time randomized algorithm M that takes $(x, y) \sim \mathcal{D}_n$ as input and, with probability $1 - 1/q(n)$ over the choice of (x, y) and the internal randomness of M, outputs the description of a randomized program of length $\mathrm{K}(x \mid y) + \log p(n)$ that takes y as input and outputs x in time $p(n)$.*
(4) **(Average-Case Symmetry of Information)** *For every polynomial time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and for every quasi-polynomial q, there exists a quasi-polynomial p such that for all computable*

time bounds t with $t(n) \geq p(n)$ and for all n,

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{rK}^{t(n)}(x,y) \geq \mathrm{rK}^{t(n)}(x \mid y) + \mathrm{rK}^{t(n)}(y) - \log t(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(5) **(Average-Case Symmetry of Information with an Efficient Encoder)** *In addition to Item 4, there exists a quasi-polynomial-time randomized algorithm M that takes $(x,y) \sim \mathcal{D}_n$ and, with probability $1 - 1/q(n)$ over the choice of (x,y) and the internal randomness of M, outputs the description of a randomized program of length $\mathrm{rK}^{t(n)}(x,y) - \mathrm{rK}^{t(n)}(y) + \log t(n)$ that takes y as input and outputs x in time $p(n)$.*

5 DistNP VS HeurBPP, INDEPENDENT AVERAGE-CASE CONDITIONAL CODING AND LANGUAGE COMPRESSION

In this section, we show the following relationships between the average-case easiness of NP and the *independent* variants of average-case conditional coding, language compression, and symmetry of information.

Theorem 12. *The following are equivalent.*

(1) $\mathsf{DistNP} \subseteq \mathsf{HeurBPP}$.

(2) **(Independent Average-Case Conditional Coding)** *For every samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over $\mathsf{Support}(\mathcal{D}_n^{(2)})$, and for every polynomial q, there exists a polynomial p such that for all large enough $n \in \mathbb{N}$,*

$$\Pr_{y\sim C_n, x\sim\mathcal{D}_n(\cdot|y)}\left[\mathrm{pK}^{p(n)}(x \mid y) \leq \log\frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(3) **(Independent Average-Case Language Compression)** *For every computable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_n$, for every samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over $\mathsf{Support}(\mathcal{D}_n^{(2)})$, and for every polynomial q, there exists a polynomial p such that for all n,*

$$\Pr_{y\sim C_n, x\sim\mathcal{D}_n(\cdot|y)}\left[x \in L_y \implies \mathrm{pK}^{p(n)}(x \mid y) \leq \log|L_y| + \log p(n)\right] \geq 1 - \frac{1}{q(n)}.$$

(4) **(Conditional Extrapolation)** *For every samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over $\mathsf{Support}(\mathcal{D}_n^{(2)})$, there exists a probabilistic polynomial-time algorithm $\mathsf{CondExt}$ such that for all $n, \varepsilon^{-1}, \delta^{-1} \in \mathbb{N}$,*

$$\Pr_{y\sim C_n}\left[\mathsf{L}_1\left(\mathsf{CondExt}(y; 1^{\varepsilon^{-1}}, 1^{\delta^{-1}}), \mathcal{D}_n(\cdot \mid y)\right) \leq \varepsilon\right] \geq 1 - \delta.$$

Theorem 13. *If $\mathsf{DistNP} \subseteq \mathsf{HeurBPP}$ holds, then the following holds:*

(5) **(Independent Average-Case Symmetry of Information)** *For every samplable distribution families $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ and $\{C_n\}_{n\in\mathbb{N}}$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, and each C_n is over $\mathsf{Support}(\mathcal{D}_n^{(2)})$, and for every polynomial q, there exists a polynomial p such that for all enough large $n \in \mathbb{N}$ and for all computable time bound $t\colon \mathbb{N} \to \mathbb{N}$ with $t(n) \geq p(n)$ and for all n,*

$$\Pr_{\substack{y\sim C_n,\\ x\sim\mathcal{D}_n(\cdot|y)}}\left[\mathrm{pK}^{t(n)}(x,y) \geq \mathrm{pK}^{t(n)}(x \mid y) + \mathrm{pK}^{t(n)}(y) - \log t(n)\right] \geq 1 - \frac{1}{q(n)}.$$

6 NP VS BPP, WORST-CASE CONDITIONAL CODING AND LANGUAGE COMPRESSION

Theorem 14. *The following are equivalent.*

(1) $\mathsf{NP} \subseteq \mathsf{BPP}$.

(2) **(Worst-Case Conditional Coding)** *For every polynomial-time samplable distribution family $\{\mathcal{D}_n\}_n$, where each $\mathcal{D}_n$ is over $\{0,1\}^n \times \{0,1\}^n$, there exists a polynomial p such that for all large enough n, and $(x,y) \in \mathsf{Support}(\mathcal{D}_n)$*

$$\mathrm{pK}^{p(n)}(x \mid y) \leq \log\frac{1}{\mathcal{D}_n(x \mid y)} + \log p(n).$$

(3) **(Worst-Case Language Compression)** *For every polynomial time computable set $L \subseteq \{\{0,1\}^n \times \{0,1\}^n\}_n$, there exists a polynomial p such that for all n and all $x, y \in \{0,1\}^n$,*

$$x \in L_y \implies \mathrm{pK}^{p(n)}(x \mid y) \leq \log|L_y| + \log p(n).$$

Moreover, the above holds if we replace pK *with* rK.

ACKNOWLEDGMENTS

We thank the anonymous STOC reviewers for their comments and suggestions. We would like to thank Hanlin Ren for asking a question about conditional coding that led to part of these investigations and for initial discussions. We are grateful to Osamu Watanabe for conversations that motivated Theorem 2. We also thank Rahul Santhanam for related discussions.

REFERENCES

[1] Eric Allender. 2021. Vaughan Jones, Kolmogorov Complexity, and the new complexity landscape around circuit minimization. *New Zealand journal of mathematics* 52 (2021), 585–604. https://doi.org/10.53733/148

[2] Eric Allender, Harry Buhrman, Michal Koucký, Dieter van Melkebeek, and Detlef Ronneburger. 2006. Power from Random Strings. *SIAM J. Comput.* 35, 6 (2006), 1467–1493. https://doi.org/10.1137/050628994

[3] Luis Filipe Coelho Antunes and Lance Fortnow. 2009. Worst-Case Running Times for Average-Case Algorithms. In *Conference on Computational Complexity* (CCC). 298–303. https://doi.org/10.1109/CCC.2009.12

[4] Andrej Bogdanov and Luca Trevisan. 2006. Average-Case Complexity. *Found. Trends Theor. Comput. Sci.* 2, 1 (2006). https://doi.org/10.1561/0400000004

[5] Harry Buhrman, Lance Fortnow, and Sophie Laplante. 2001. Resource-Bounded Kolmogorov Complexity Revisited. *SIAM J. Comput.* 31, 3 (2001), 887–905. https://doi.org/10.1137/S009753979834388X

[6] Harry Buhrman, Sophie Laplante, and Peter B. Miltersen. 2000. New bounds for the language compression problem. In *Conference on Computational Complexity* (CCC). 126–130. https://doi.org/10.1109/CCC.2000.856742

[7] Harry Buhrman, Troy Lee, and Dieter van Melkebeek. 2005. Language compression and pseudorandom generators. *Comput. Complex.* 14, 3 (2005), 228–255.

[8] Halley Goldberg and Valentine Kabanets. 2022. A Simpler Proof of the Worst-Case to Average-Case Reduction for Polynomial Hierarchy via Symmetry of Information. *Electron. Colloquium Comput. Complex.* 7 (2022), 1–14. https://eccc.weizmann.ac.il/report/2022/007/

[9] Halley Goldberg, Valentine Kabanets, Zhenjian Lu, and Igor C. Oliveira. 2022. Probabilistic Kolmogorov Complexity with Applications to Average-Case Complexity. In *Computational Complexity Conference* (CCC). 16:1–16:60. https://doi.org/10.4230/LIPIcs.CCC.2022.16

[10] Oded Goldreich. 1990. A Note on Computational Indistinguishability. *Inf. Process. Lett.* 34, 6 (1990), 277–281. https://doi.org/10.1016/0020-0190(90)90010-U

[11] Oded Goldreich. 2001. *The Foundations of Cryptography - Volume 1: Basic Techniques*. Cambridge University Press. https://doi.org/10.1017/CBO9780511546891

[12] Shafi Goldwasser and Silvio Micali. 1984. Probabilistic Encryption. *J. Comput. Syst. Sci.* 28, 2 (1984), 270–299. https://doi.org/10.1016/0022-0000(84)90070-9

[13] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. 1999. A Pseudorandom Generator from any One-way Function. *SIAM J. Comput.* 28, 4 (1999), 1364–1396. https://doi.org/10.1137/S0097539793244708

[14] Shuichi Hirahara. 2018. Non-Black-Box Worst-Case to Average-Case Reductions within NP. In *Symposium on Foundations of Computer Science* (FOCS). 247–258. https://doi.org/10.1109/FOCS.2018.00032

[15] Shuichi Hirahara. 2021. Average-case hardness of NP from exponential worst-case hardness assumptions. In *Symposium on Theory of Computing* (STOC). 292–302. https://doi.org/10.1145/3406325.3451065

[16] Shuichi Hirahara. 2022. Meta-Computational Average-Case Complexity: A New Paradigm Toward Excluding Heuristica. *Bull. EATCS* 136 (2022). http://bulletin.eatcs.org/index.php/beatcs/article/view/688

[17] Shuichi Hirahara. 2022. Symmetry of Information from Meta-Complexity. In *Computational Complexity Conference* (CCC). 26:1–26:41. https://doi.org/10.4230/LIPIcs.CCC.2022.26

[18] Shuichi Hirahara, Rahul Ilango, Zhenjian Lu, Mikito Nanashima, and Igor C. Oliveira. 2023. A Duality Between One-Way Functions and Average-Case Symmetry of Information. Cryptology ePrint Archive, Paper 2023/424. https://eprint.iacr.org/2023/424

[19] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. 2021. Hardness on any Samplable Distribution Suffices: New Characterizations of One-Way Functions by Meta-Complexity. *Electron. Colloquium Comput. Complex.* (2021), 82. https://eccc.weizmann.ac.il/report/2021/082

[20] Russell Impagliazzo and Leonid A. Levin. 1990. No Better Ways to Generate Hard NP Instances than Picking Uniformly at Random. In *Symposium on Theory of Computing* (STOC). 812–821. https://doi.org/10.1109/FSCS.1990.89604

[21] Russell Impagliazzo and Michael Luby. 1989. One-way Functions are Essential for Complexity Based Cryptography (Extended Abstract). In *Symposium on Theory of Computing* (STOC). 230–235. https://doi.org/10.1109/SFCS.1989.63483

[22] Ker-I Ko. 1991. On the Complexity of Learning Minimum Time-Bounded Turing Machines. *SIAM J. Comput.* 20, 5 (1991), 962–986. https://doi.org/10.1137/0220059

[23] Andrey N. Kolmogorov. 1965. Three approaches to the quantitative definition of information. *Problems of information transmission* 1, 1 (1965), 1–7.

[24] Andrey N. Kolmogorov. 1968. Several Theorems about Algorithmic Entropy and Algorithmic Amount of Information (a talk at a Moscow Math. Soc. meeting on 10/31/67). In Usp. Mat. Nauk, Vol. 23. 201.

[25] Troy Lee. 2006. *Kolmogorov complexity and formula lower bounds*. Ph. D. Dissertation. University of Amsterdam.

[26] Troy Lee and Andrei E. Romashchenko. 2005. Resource bounded symmetry of information revisited. *Theor. Comput. Sci.* 345, 2-3 (2005), 386–405. https://doi.org/10.1016/j.tcs.2005.07.017

[27] Ming Li and Paul M. B. Vitányi. 2019. *An Introduction to Kolmogorov Complexity and Its Applications, 4th Edition*. Springer. https://doi.org/10.1007/978-3-030-11298-1

[28] Yanyi Liu and Rafael Pass. 2020. On One-way Functions and Kolmogorov Complexity. In *Symposium on Foundations of Computer Science* (FOCS). 1243–1254. https://doi.org/10.1109/FOCS46700.2020.00118

[29] Yanyi Liu and Rafael Pass. 2021. On the Possibility of Basing Cryptography on EXP≠BPP. In *International Cryptology Conference* (CRYPTO). 11–40. https://doi.org/10.1007/978-3-030-84242-0_2

[30] Yanyi Liu and Rafael Pass. 2022. On One-Way Functions from NP-Complete Problems. In *Computational Complexity Conference* (CCC). 36:1–36:24. https://doi.org/10.4230/LIPIcs.CCC.2022.36

[31] Luc Longpré. 1986. *Resource bounded Kolmogorov complexity, a link between computational complexity and information theory*. Ph. D. Dissertation. Cornell University.

[32] Luc Longpré and Sarah Mocas. 1993. Symmetry of Information and One-Way Functions. *Inf. Process. Lett.* 46, 2 (1993), 95–100. https://doi.org/10.1016/0020-0190(93)90204-M

[33] Luc Longpré and Osamu Watanabe. 1995. On Symmetry of Information and Polynomial Time Invertibility. *Inf. Comput.* 121, 1 (1995), 14–22. https://doi.org/10.1006/inco.1995.1120

[34] Zhenjian Lu and Igor Carboni Oliveira. 2021. An Efficient Coding Theorem via Probabilistic Representations and Its Applications. In *48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference)*, Vol. 198. 94:1–94:20. https://doi.org/10.4230/LIPIcs.ICALP.2021.94

[35] Zhenjian Lu and Igor C. Oliveira. 2022. Theory and Applications of Probabilistic Kolmogorov Complexity. *Bull. EATCS* 137 (2022). http://bulletin.eatcs.org/index.php/beatcs/article/view/700

[36] Zhenjian Lu, Igor C. Oliveira, and Rahul Santhanam. 2021. Pseudodeterministic algorithms and the structure of probabilistic time. In *Symposium on Theory of Computing* (STOC). 303–316. https://doi.org/10.1145/3406325.3451085

[37] Zhenjian Lu, Igor Carboni Oliveira, and Marius Zimand. 2022. Optimal Coding Theorems in Time-Bounded Kolmogorov Complexity. In *International Colloquium on Automata, Languages, and Programming* (ICALP). 92:1–92:14. https://doi.org/10.4230/LIPIcs.ICALP.2022.92

[38] Moni Naor. 1991. Bit Commitment Using Pseudorandomness. *J. Cryptol.* 4, 2 (1991), 151–158. https://doi.org/10.1007/BF00196774

[39] Igor C. Oliveira. 2019. Randomness and Intractability in Kolmogorov Complexity. In *International Colloquium on Automata, Languages, and Programming* (ICALP). 32:1–32:14. https://doi.org/10.4230/LIPIcs.ICALP.2019.32

[40] Igor C. Oliveira, Ján Pich, and Rahul Santhanam. 2019. Hardness Magnification near State-Of-The-Art Lower Bounds. In *Computational Complexity Conference* (CCC). 27:1–27:29. https://theoryofcomputing.org/articles/v017a011/

[41] Ran Raz, Omer Reingold, and Salil P. Vadhan. 2002. Extracting all the Randomness and Reducing the Error in Trevisan's Extractors. *J. Comput. Syst. Sci.* 65, 1 (2002), 97–128. https://doi.org/10.1006/jcss.2002.1824

[42] Hanlin Ren and Rahul Santhanam. 2021. Hardness of KT Characterizes Parallel Cryptography. In *Computational Complexity Conference* (CCC). 35:1–35:58. https://doi.org/10.4230/LIPIcs.CCC.2021.35

[43] John Rompel. 1990. One-Way Functions are Necessary and Sufficient for Secure Signatures. In *Symposium on Theory of Computing* (STOC). 387–394. https://doi.org/10.1145/100216.100269

[44] Detlef Ronneburger. 2004. *Kolmogorov Complexity and Derandomization*. Ph. D. Dissertation. Rutgers University.

[45] Alexander Shen, Vladimir A. Uspensky, and Nikolay Vereshchagin. 2017. *Kolmogorov complexity and algorithmic randomness*. American Mathematical Society.

[46] Michael Sipser. 1983. A Complexity Theoretic Approach to Randomness. In *Symposium on Theory of Computing* (STOC). 330–335. https://doi.org/10.1145/800061.808762

[47] Luca Trevisan and Salil P. Vadhan. 2007. Pseudorandomness and Average-Case Complexity Via Uniform Reductions. *Computational Complexity* 16, 4 (2007), 331–364. https://doi.org/10.1007/s00037-007-0233-x

[48] Salil P. Vadhan. 2012. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science* 7, 1-3 (2012), 1–336. https://doi.org/10.1561/0400000010

[49] Osamu Watanabe. 2022. Personal Communication.

[50] Alexander K. Zvonkin and Leonid A. Levin. 1970. The complexity of finite objects and the algorithmic concepts of randomness and information. *UMN (Russian Math. Surveys)* 25, 6 (1970), 83–124.

Received 2022-11-07; accepted 2023-02-06