Electronic Colloquium on Computational Complexity, Report No. 37 (2023)

Capturing One-Way Functions via NP-Hardness of Meta-Complexity

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

March 27, 2023

Abstract

A one-way function is a function that is easy to compute but hard to invert *on average*. We establish the first characterization of a one-way function by *worst-case* hardness assumptions, by introducing a natural meta-computational problem whose NP-hardness (and the worst-case hardness of NP) characterizes the existence of a one-way function. Specifically, we generalize the notion of time-bounded conditional Kolmogorov complexity to *distributional Kolmogorov complexity*, and prove that a one-way function exists if and only if it is NP-hard to approximate the distributional Kolmogorov complexity under randomized polynomial-time reductions and NP is hard in the worst case. We also propose the *Meta-Complexity Padding Conjecture*, which postulates that distributional Kolmogorov complexity is paddable by an approximation-preserving reduction. Under this conjecture, we prove that the worst-case hardness of an approximate version of the Minimum Circuit Size Problem characterizes the existence of a one-way function.

Our results extend the emerging paradigm of meta-complexity, which suggests that proving NP-hardness of meta-computational problems (i.e., problems that ask to compute complexity) is sufficient to exclude errorless Heuristica and error-prone Pessiland from Impagliazzo's five worlds. The key technical contribution is to conditionally close the gap between errorless and error-prone average-case complexities by combining Nanashima's proof techniques of showing "limits" of black-box reductions (ITCS'21) with non-black-box worst-case-to-average-case reductions of Hirahara (FOCS'18).

ISSN 1433-8092

Contents

1 Introduction

A *one-way function* is a function that is efficiently computable but hard to invert on average. This is one of the most fundamental cryptographic primitives, as the existence of a one-way function is both sufficient and necessary [IL89] for constructing various cryptographic primitives, such as pseudorandom generators [HILL99], pseudorandom function generators [GGM86], digital signatures [Rom90], and commitment schemes [Nao91].

What is a minimal complexity-theoretic assumption that implies the existence of a one-way function? Clearly, no one-way function exists if NP is easy. A major challenge in theoretical computer science is to prove the converse, which would characterize the existence of a one-way function by the worst-case hardness of NP. In an influential paper of Impagliazzo [Imp95], he provided a ramification of this question by proposing the notion of five possible worlds. *Pessiland* is a hypothetical world in which one-way functions do not exist but NP is hard on average. *Heuristica* is a hypothetical world in which NP is hard in the worst case but NP is easy on average. These hypothetical worlds are consistent with our current knowledge of complexity theory and cryptography. The open problem of basing the security of a one-way function on the worst-case hardness of NP is equivalent to excluding both Heuristica and Pessiland from Impagliazzo's five possible worlds—two of the four central challenges in theoretical computer science.[1]

Because of the importance of the questions, a large body of work has been devoted to understanding what types of proof techniques can (or cannot) be used to exclude possible worlds. Standard proof techniques, such as black-box reductions [FF93; BT06b; AGGM06; BB15; HW20], hardness amplification procedures [Vio05] and relativizing proofs [Imp11; HN21], are incapable of excluding Heuristica from Impagliazzo's five worlds. Similarly, a relativizing proof technique is incapable of excluding Pessiland from the five worlds [Wee06].

The main result of this paper is to capture the question of excluding Heuristica and Pessiland by NP-hardness of approximating *distributional Kolmogorov complexity* under randomized reductions. Informally, the distributional Kolmogorov complexity $\mathrm{dK}^{\mathsf{poly}}(x \mid \mathcal{D})$ of a string x given a distribution $\mathcal{D}$ is defined to be the length of an efficient shortest program that prints x given y as input with high probability over a choice of $y \sim \mathcal{D}$. Note that NP-hardness is a notion of *worst-case hardness*. Nevertheless, we present the first characterization of a one-way function, which is a cryptographic primitive based on *average-case hardness*, by worst-case hardness assumptions. Our characterization employs non-relativizing proof techniques and non-black-box reductions; thus, it is unlikely that our proof techniques are subject to the aforementioned limits of the standard proof techniques. The characterization provides a concrete and new approach towards the central challenge of excluding Heuristica and Pessiland.

1.1 Paradigm of Meta-Complexity

Our results are inspired by the emerging paradigm of *meta-complexity* [All21; Hir22a]. Meta-complexity is an informal phrase that refers to the computational complexity of problems that themselves ask to compute complexity. For example, MINKT [Ko91] is the problem of computing the t-*time-bounded Kolmogorov complexity* of a given string x, i.e., the minimum length of a program that prints x in time t. Similarly, the Minimum Circuit Size Problem (MCSP [KC00]) is the problem

[1] The other two challenges are excluding Algorithmica (proving that NP is hard in the worst case; e.g., $\mathsf{P} \neq \mathsf{NP}$) and excluding Minicrypt (proving that the existence of a one-way function implies the existence of a public-key cryptosystem).

of computing the circuit complexity of the truth table of a given Boolean function. It is easy to observe that these meta-computational problems are in NP. Whether they are NP-complete or not is a central open question in the field of meta-complexity.

Based on meta-complexity, Hirahara [Hir18] proposed an approach for excluding Heuristica. He showed that the worst-case and average-case complexities of approximate versions of meta-computational problems, such as MINKT and MCSP, are equivalent. In particular, if these problems are NP-hard, then Heuristica can be excluded from Impagliazzo's five possible worlds, i.e., the worst-case and average-case complexities of NP are equivalent. What makes the approach particularly appealing is that the reductions presented in [Hir18] are *non-black-box*, meaning that the correctness of the reductions can be proved if an oracle is efficient (but may not be proved otherwise). In contrast, in the standard notion of (black-box) reduction, the correctness of reductions can be proved without using the efficiency of an oracle. Bogdanov and Trevisan [BT06b] showed that black-box reductions are too strong to be useful for excluding Heuristica, by proving that NP cannot be reduced to DistNP under randomized nonadaptive polynomial-time reductions unless PH collapses. Here, DistNP is an average-case analogue of NP [BT06a].[2] In a subsequent line of work (e.g., [Hir20a; Hir21; CHV22; GKLO22]), proof techniques that do not rely on hardness amplification procedures were developed, and a strong variant of Heuristica was excluded [Hir21].

Moreover, there is a folklore approach for excluding Pessiland based on NP-hardness of meta-computational problems. Impagliazzo and Levin [IL90, Proposition 1] characterized the existence of a one-way function by the non-existence of an efficient algorithm that approximates a probabilistic variant $\mathrm{q}^t(x)$ of the time-bounded Kolmogorov complexity of an input x drawn from any unknown t'-time samplable distribution, where $t' \ll t$. Here, $\mathrm{q}^t(x)$ is defined to be $-\log \mathrm{Q}^t(x)$, where $\mathrm{Q}^t(x)$ is the *t-time-bounded universal a priori probability* of x, which is the probability that a universal Turing machine produces x given a uniformly random input in time t. In particular, if the problem of approximating $\mathrm{q}^t(x)$ is "NP-hard under t'-time reductions for $t' \ll t$,"[3] then the problem of approximating $\mathrm{q}^t(x)$ with respect to t'-time samplable distributions is DistNP-complete. By the result of [IL90], this implies that Pessiland does not exist, i.e., the average-case hardness of NP implies the existence of a one-way function.

These two results [Hir18; IL90] provide interesting approaches for excluding both Heuristica and Pessiland using the meta-complexity of q^t. Observing that the proof techniques of [Hir18] are applicable to q^t, if the problem of approximating q^t is NP-hard under t'-time reductions for $t' \ll t$, then Heuristica and Pessiland can be excluded simultaneously. This *appears* to be a reasonable approach for basing the security of a one-way function on the worst-case complexity of NP. However, there are two important issues in this approach, as described below.

Errorless vs. error-prone average-case complexities. The first issue is that the notion of average-case complexities of NP used in [Hir18; IL90] are different. On one hand, the result of [IL90] refers to *error-prone average-case complexity*. An error-prone heuristic algorithm A is said to solve a problem L with respect to an input distribution $\mathcal{D}$ if A computes the correct answer $L(x)$ for most instances x drawn from $\mathcal{D}$. On the other hand, the results of [Hir18] refer to *errorless average-case complexity*. An *errorless* heuristic algorithm A is a special case of an error-prone

[2] Specifically, DistNP consists of pairs $(L, \mathcal{D})$ (called *distributional problems*) of languages $L \in \mathsf{NP}$ and polynomial-time samplable distributions $\mathcal{D}$.

[3] More formally, for an NP-complete problem L that is DistNP-complete with respect to the uniform distribution, there exist a polynomial t' and a t'-time reduction that reduces L to the problem of approximating $\mathrm{q}^t(x)$ for all sufficiently large polynomials t.

heuristic algorithm in which for every input x, the algorithm A must output either the correct answer $L(x)$ or a special symbol $\perp$, which indicates the failure of the algorithm A. Whether the error-prone and errorless average-case complexities of NP are equivalent is a long-standing open question [Lev86; Imp95; Imp11; HS22; HN22]. Thus, even if q^t is shown to be NP-hard, the gap between errorless and error-prone complexities prevents us from basing the security of a one-way function on the worst-case complexity of NP.[4]

In terms of Impagliazzo's five worlds, NP-hardness of q^t under efficient reductions excludes an *errorless* variant of Heuristica and an *error-prone* variant of Pessiland according to the results of [Hir18] and [IL90], respectively. There are several ways to define Heuristica and Pessiland, as there are several ways to define average-case complexity. *Errorless Heuristica* refers to a world in which NP is hard in the worst case but easy on average in the sense of errorless average-case complexity (e.g., $\mathsf{DistNP} \subseteq \mathsf{AvgBPP}$). Similarly, one may define errorless and error-prone versions of Pessiland. To base the security of a one-way function on the worst-case complexity of NP, one must exclude both *errorless* Heuristica and *errorless* Pessiland.

A fundamental obstacle. The second issue is that NP-hardness of q^t under t'-time reductions for $t' \ll t$ contradicts plausible complexity assumptions. Saks and Santhanam [SS22] recently presented a significant barrier for proving NP-hardness of t-time-bounded Kolmogorov complexity under efficient reductions. Under plausible complexity-theoretic assumptions, they showed that the problem of approximating $\mathrm{K}^t(x)$ cannot be NP-hard under t'-time reductions if $t' \ll t$. The same proof techniques are applicable to the problem of approximating $\mathrm{q}^t(x)$. Thus, it is unlikely that the folklore approach towards excluding Pessiland can be realized.

In summary, the paradigm of meta-complexity suggests that NP-hardness of meta-computational problems is *sufficient* to exclude errorless Heuristica and error-prone Pessiland. However, important questions remain unanswered.

1. Is an approach based on meta-complexity *necessary* for excluding Heuristica and Pessiland?
2. NP-hardness of q^t under efficient reductions contradicts plausible complexity-theoretic assumptions [SS22]. Is there a variant of time-bounded Kolmogorov complexity whose NP-hardness is plausible and sufficient to exclude Pessiland?
3. Can the gap between errorless and error-prone average-case complexities of NP be closed?

All of these questions are answered in this paper.

1.2 Our Results

We introduce the notion of distributional Kolmogorov complexity—a natural generalization of time-bounded conditional Kolmogorov complexity. Let U be an efficient universal Turing machine. For $t \in \mathbb{N}$ and $d \in \{0,1\}^*$, we define $U^t(d)$ to be the output of the universal Turing machine U on input d if it halts in time t, and a special symbol "$\perp$" otherwise.

[4] In more detail, $\mathsf{NP} \not\subseteq \mathsf{BPP}$ implies $\mathsf{DistNP} \not\subseteq \mathsf{AvgBPP}$, and $\mathsf{DistNP} \not\subseteq \mathsf{HeurBPP}$ implies the existence of a one-way function. However, there is a gap between $\mathsf{DistNP} \not\subseteq \mathsf{AvgBPP}$ and $\mathsf{DistNP} \not\subseteq \mathsf{HeurBPP}$.

Definition 1.1. *For a string $x \in \{0,1\}^*$, a time bound $t \in \mathbb{N}$, a parameter $\lambda \in (0,1]$, and a distribution $\mathcal{D}$ over $\{0,1\}^m$, the* t-time-bounded distributional Kolmogorov complexity of x given $\mathcal{D}$ *is defined to be*

$$\mathrm{dK}^t_\lambda(x \mid \mathcal{D}) := \min\left\{ |d| \;\middle|\; \Pr_{y\sim\mathcal{D}}[U^t(d,y) = x] \geq \lambda \right\},$$

where $|d|$ denotes the length of a string $d \in \{0,1\}^*$. For a function $\tau\colon \mathbb{N} \to \mathbb{N}$, we define

$$\mathrm{dK}^\tau_\lambda(x \mid \mathcal{D}) := \mathrm{dK}^{\tau(n+m)}_\lambda(x \mid \mathcal{D}),$$

where $n := |x|$. For an oracle $A \subseteq \{0,1\}^*$, the notion can be naturally extended to an A-oracle version $\mathrm{dK}^{\tau,A}$ by considering the A-oracle universal Turing machine U^A.

This notion generalizes the notion of time-bounded conditional Kolmogorov complexity. For a distribution $\mathcal{D}_y$ supported only on a string $y \in \{0,1\}^*$, we have

$$\mathrm{dK}^t_\lambda(x \mid \mathcal{D}_y) = \mathrm{K}^t(x \mid y),$$

where $\mathrm{K}^t(x \mid y)$ is the t-time-bounded conditional Kolmogorov complexity of x given y, i.e., the minimum length of a program that prints x on input y in time t. We often identify a string y with the singleton distribution $\mathcal{D}_y$ on y.

The meta-complexity of $\mathrm{dK}^{\mathsf{poly}}$ can be naturally considered as follows. For a polynomial τ, given a string x, a circuit D that represents a distribution $\mathcal{D}$ over $\{0,1\}^m$, a size parameter $s \in \mathbb{N}$, and a "confidence" parameter λ, does $\mathrm{dK}^\tau_\lambda(x \mid \mathcal{D}) \leq s$ hold? Here, we say that an m'-input circuit D *represents* a distribution $\mathcal{D}$ if the distribution of the output $D(r)$ of D over a random input $r \sim \{0,1\}^{m'}$ is identical to $\mathcal{D}$. It is easy to observe that the problem of approximating $\mathrm{dK}^\tau_\lambda(x \mid \mathcal{D})$ (in which λ has a small additive error) is in pr-MA—a randomized and promise variant of NP.

Our main result is to characterize the existence of a one-way function by NP-hardness of approximating $\mathrm{dK}^{\mathsf{poly}}$ under the assumption that NP is hard in the worst case. For a technical reason, we impose a mild restriction on NP-hardness reductions. We say that a reduction to $\mathrm{dK}^{\mathsf{poly}}$ is *parametric honest* [SS20] if there exists a constant $\gamma > 0$ such that the size parameter s in any query of the reduction on inputs of length n satisfies $s \geq n^\gamma$.

Theorem 1.2 (informal; see Theorem 11.1 for a formal statement)**.** *Assume $\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$; i.e., NP cannot be computed by polynomial-size circuits almost everywhere. Then, the following are equivalent.*

1. *There exists a one-way function secure against polynomial-size circuits.*
2. *For some constant $\epsilon > 0$, there exists a parametric-honest randomized polynomial-time non-adaptive reduction from NP to a $(1+\epsilon)$-factor approximation of $\mathrm{dK}^{\tau,A}$ for all large polynomials τ and all oracles $A \in \mathsf{P/poly}$.*
3. *For some $g(n) = n^{1/(\log\log n)^{O(1)}}$, there exists a parametric-honest randomized polynomial-time one-query reduction from NP to a $g(n)$-factor approximation of $\mathrm{dK}^{\tau,A}$ for all large polynomials τ and all oracles $A \in \mathsf{P/poly}$.*

Item 2 states that for every $L \in \mathsf{NP}$, there exists a *single* polynomial-time reduction M (independent of τ and A) that, for all large polynomials τ and all oracles A, reduces L to the problem of

approximating $\mathrm{dK}^{\tau,A}$. Thus, it is implicit that the running time t' of the reduction M is significantly smaller than the time bound τ of $\mathrm{dK}^{\tau,A}$, just as in the folklore approach for excluding Pessiland based on [IL90]. For a technical reason, we consider the A-oracle distributional Kolmogorov complexity for oracles $A \in \mathsf{P/poly}$, which is used to show Item 2 $\Rightarrow$ 1. Note that $\mathrm{dK}^{\tau,A}(x \mid \mathcal{D})$ is approximately equal to $\mathrm{dK}^{\tau}(x \mid \mathcal{D}, C)$, where C is the description of the polynomial-size circuit that computes A.

The assumption that NP is hard in the worst case is necessary for any characterization of a one-way function by NP-hardness. If NP is easy, then every problem in NP (or even PH) is NP-complete, whereas no one-way function exists. This indicates that the existence of a one-way function cannot be equivalent to NP-hardness in the case where NP is easy. Excluding this trivial case (in terms of Impagliazzo's five worlds, Algorithmica) from consideration, Theorem 1.2 shows that a one-way function exists (Heuristica and Pessiland do not exist) if and only if the meta-computational problem of approximating $\mathrm{dK}^{\mathsf{poly}}$ is NP-hard.

Since the existence of a one-way function implies $\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$, Theorem 1.2 can be equivalently rephrased as the following unconditional equivalence: There exists a one-way function if and only if $\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$ and it is NP-hard to approximate $\mathrm{dK}^{\tau,A}$ for any polynomial τ and for any oracle $A \in \mathsf{P/poly}$.

In general, our results suggest that NP-hardness of A-oracle distributional Kolmogorov complexity $\mathrm{dK}^{\mathsf{poly},A}$ is closely related to the existence of a one-way function secure against A. For example, we show that if a probabilistic variant $\mathrm{dpK}^{\mathsf{poly}}$ of $\mathrm{dK}^{\mathsf{poly}}$ is NP-hard to approximate, then $\mathsf{NP} \not\subseteq \mathsf{i.o.BPP}$ implies the existence of a one-way function secure against randomized polynomial-time algorithms. Here, $\mathrm{dpK}^t_\lambda(x \mid \mathcal{D})$ is defined to be $\min\{s \in \mathbb{N} \mid \Pr_{r\sim\{0,1\}^t}[\mathrm{dK}^t_\lambda(x \mid \mathcal{D}, r) \le s] \ge \frac{3}{4}\}$.

1.3 Meta-Complexity Padding Conjecture

Although Theorem 1.2 captures the existence of a one-way function by NP-hardness of $\mathrm{dK}^{\mathsf{poly}}$ under efficient reductions, whether the existence of a one-way function can be characterized by the worst-case intractability of some (natural) computational problem remains an open question. Since the worst-case hardness and errorless average-case hardness of $\mathrm{q}^{\mathsf{poly}}$ are equivalent [Hir18] and the error-prone average-case hardness of $\mathrm{q}^{\mathsf{poly}}$ is equivalent to the existence of a one-way function [IL90], the worst-case intractability of $\mathrm{q}^{\mathsf{poly}}$ would characterize the existence of a one-way function. However, the gap between errorless and error-prone average-case complexities prevents us from obtaining such a characterization. A similar gap exists between [Hir18] and the recent characterization of one-way functions by the error-prone average-case complexity of $\mathrm{K}^{\mathsf{poly}}$ with respect to the uniform distribution [LP20]. The gap can be closed [HS22] if $\mathrm{K}^{\mathsf{poly}}$ is instance-checkable in the sense of Blum and Kannan [BK95], which is open.

Our proof techniques provide a new approach for closing the gap between errorless and error-prone average-case complexities of meta-computational problems. We conjecture that $\mathrm{dK}^{\mathsf{poly}}$ is *paddable* by an approximation-preserving reduction. Specifically, there exists an efficient randomized self-reduction that maps an instance $\varphi = (x, \mathcal{D}, s, \lambda)$ of $\mathrm{dK}^{\mathsf{poly}}_\lambda$ to another instance $(x', \mathcal{D}', s', \lambda)$ of the problem of approximating $\mathrm{dK}^{\mathsf{poly}}_\lambda$ such that $s' \gg |\varphi|$, where $|\varphi|$ denotes the length of the binary encoding of the instance φ. Any natural NP-complete problem is paddable, and the property of being paddable is far weaker than NP-completeness (under honest reductions[5]). Thus, without resolving the NP-hardness of $\mathrm{dK}^{\mathsf{poly}}$, we expect that it is feasible to prove that $\mathrm{dK}^{\mathsf{poly}}$ is paddable

[5] A reduction M is said to be *honest* if the length of any query of M on input length n is at least $n^{\Omega(1)}$.

with current proof techniques. We show that the paddability of $\mathrm{dK}^{\mathsf{poly}}$ is sufficient for closing the gap between errorless and error-prone average-case complexities of $\mathrm{K}^{\mathsf{poly}}$.

In fact, an even weaker property is sufficient: we propose the *Meta-Complexity Padding Conjecture*, which postulates that the problem $\mathrm{Gap}(\mathrm{K}^{\mathsf{poly}}$ vs $\mathrm{K})$ of approximating Kolmogorov complexity is reducible to the problem of approximating $\mathrm{dK}^{\mathsf{poly}}$ via a size-expanding reduction. Here, a reduction to $\mathrm{dK}^{\mathsf{poly}}$ is said to be *size-expanding* [Hir22b] if on input φ, the size parameter s in any query of the reduction satisfies $s = \omega(|\varphi|)$. The problem $\mathrm{Gap}(\mathrm{K}^{\mathsf{poly}}$ vs $\mathrm{K})$ is defined as follows.

Definition 1.3. *For a constant $\epsilon > 0$ and a polynomial p, we define $\mathrm{Gap}_\epsilon(\mathrm{K}^p$ vs $\mathrm{K}) = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ to be the following promise problem.*

$$\Pi_{\mathrm{YES}} := \left\{ x \in \{0,1\}^* \;\middle|\; \mathrm{K}^{p(|x|)}(x) \leq |x|^\epsilon \right\},$$
$$\Pi_{\mathrm{NO}} := \{ x \in \{0,1\}^* \mid \mathrm{K}(x) \geq |x| - 3 \}.$$

Informally, this problem asks to approximate $\mathrm{K}^{p(|x|)}(x)$ to within a factor of $|x|^{1-\epsilon}$. Moreover, in the NO case, the input x has high *resource-unbounded* Kolmogorov complexity, which makes the problem easier. We conjecture that it is feasible to reduce $\mathrm{Gap}_\epsilon(\mathrm{K}^p$ vs $\mathrm{K})$ to $\mathrm{dpK}^{\mathsf{poly}}$ via a size-expanding reduction.

Conjecture 1.4 (The Meta-Complexity Padding Conjecture; informal; see also Conjecture 11.4)**.** *For any polynomial p, there exist constants $\epsilon, \delta > 0$ such that there exists a randomized[6] polynomial-time size-expanding reduction from $\mathrm{Gap}_\delta(\mathrm{K}^p$ vs $\mathrm{K})$ to a $(1+\epsilon)$-factor approximation of dpK^τ for all large polynomials τ.*

This conjecture captures the gap between errorless and error-prone average-case complexities of $\mathrm{q}^{\mathsf{poly}}$, and makes it possible to base the security of a one-way function on the worst-case hardness of approximating $\mathrm{q}^{\mathsf{poly}}$, the circuit complexity, and $\mathrm{rK}^{\mathsf{poly}}$. Here, $\mathrm{rK}^t(x)$ is a randomized variant of $\mathrm{K}^t(x)$, and is defined to be the length of a shortest randomized program that prints x in time t with probability at least $\frac{3}{4}$.

Theorem 1.5 (informal; see Theorem 11.7 for a formal statement)**.** *Under the Meta-Complexity Padding Conjecture, the following are equivalent.*

1. *There exists a one-way function secure against randomized polynomial-time algorithms infinitely often.*
2. *(The Minimum Circuit Size Problem is hard to approximate) For every constant $\epsilon > 0$, no randomized polynomial-time algorithm can approximate the circuit complexity of a given truth table of length 2^n to within a factor of $2^{(1-\epsilon)n}$.*
3. *For every polynomial p, no randomized polynomial-time algorithm can distinguish $\mathrm{q}^t(x) \leq s$ from $\mathrm{q}^{p(t)}(x) > p(s)$ on input $(x, 1^t, 1^s)$ such that $t \geq |x|$.*
4. *For every polynomial p, no randomized polynomial-time algorithm can distinguish $\mathrm{rK}^t(x) \leq s$ from $\mathrm{rK}^{p(t)}(x) > p(s)$ on input $(x, 1^t, 1^s)$ such that $t \geq |x|$.*

[6] The use of randomness is indispensable because there is no deterministic size-expanding reduction from non-trivial languages to dpK^τ.

5. *There exists a pseudorandom generator secure against randomized polynomial-time algorithms infinitely often.*

6. *For every constant $\epsilon > 0$, there exists a hitting set generator*

$$H = \left\{H_n : \{0,1\}^{n^\epsilon} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$$

secure against randomized polynomial-time algorithms infinitely often.

Here, a family H of functions is called a *hitting set generator* against a class $\mathfrak{C}$ if there exists no algorithm $A \in \mathfrak{C}$ that *avoids* H. An algorithm is said to avoid H if A accepts at least half of the strings of length n and rejects every string of length n in the image of H for every $n \in \mathbb{N}$. The complexity of avoiding a hitting set generator is known to be equivalent to the complexity of approximating time-bounded Kolmogorov complexity [Hir20a]. Similarly, the complexity of breaking the security of a pseudorandom generator is equivalent to the error-prone average-case complexity of time-bounded Kolmogorov complexity [LP20]. Theorem 1.5 shows that the gap between these two results can be closed under the Meta-Complexity Padding Conjecture.

It is unlikely that the Meta-Complexity Padding Conjecture can be refuted because $\mathrm{dpK}^{\mathsf{poly}}$ is NP-hard under the existence of a one-way function secure against polynomial-size circuits, in which case $\mathrm{dpK}^{\mathsf{poly}}$ is paddable.

Proposition 1.6. *If there exists a one-way function secure against polynomial-size circuits, then the Meta-Complexity Padding Conjecture is true.*

More broadly, we propose to study whether meta-computational problems are paddable by approximation-preserving reductions. We defer details to Section 3.

2 Overview of Proof Techniques

We explain how to obtain the characterization of the existence of a one-way function by NP-hardness of approximating distributional Kolmogorov complexity.

2.1 Constructing One-Way Functions from NP-Hardness of dK

Here, we explain the construction of a one-way function based on NP-hardness of distributional Kolmogorov complexity under the assumption that NP is hard in the worst case.

The central idea of closing the gap between errorless and error-prone average-case complexities of NP is based on the work of Nanashima [Nan21]. He showed that if there exists a randomized polynomial-time reduction from NP to any oracle that avoids an auxiliary-input hitting set generator, then both Heuristica and Pessiland do not exist. This provide "limits" of black-box reductions in the sense that constructing a black-box reduction from NP to avoiding an auxiliary-input hitting set generator is at least as hard as resolving the central challenge of theoretical computer science. The key insight in his work is to use the fact that a one-way function is *testable* [MX10], which is closely related to the errorless versus error-prone average-case complexities [HS22].[7]

At a high level, we combine Nanashima's "limits" of black-box reductions with the non-black-box worst-case-to-average-case reduction of Hirahara [Hir18]. In fact, there is evidence [Hir18;

[7] More precisely, we use the fact that an auxiliary-input one-way function is instance-checkable.

HW20] that Hirahara's reduction is inherently non-black-box. The reduction of [Hir18] can be seen as a reduction from (approximate variants of) meta-computational problems, such as MINKT and MCSP, to any efficient oracle that avoids a hitting set generator. Hirahara and Watanabe [HW20] showed that any language that can be reducible to any (not necessarily efficient) oracle that avoids a hitting set generator must be in $\mathsf{AM} \cap \mathsf{coAM}$. Since MINKT and MCSP are conjectured to be outside $\mathsf{AM} \cap \mathsf{coAM}$ [Rud97], it is unlikely that the reduction of [Hir18] can be made black-box. Nevertheless, we show that the reduction of [Hir18] is a "mildly" black-box reduction in a certain technical sense, and show that Nanashima's proof techniques are applicable to such a mildly black-box reduction under the assumption that $\mathrm{dK}^{\mathsf{poly}}$ is NP-hard.

2.1.1 New Theory of Non-Black-Box Reductions

To this end, we develop a new theory of mildly black-box reductions (or, equivalently, non-black-box reductions). We introduce the notions of P/poly-*restricted reduction* and *input-aware* P/poly-*restricted reduction*. These are new properties of non-black-box reductions for which proof techniques of [Hir18] and [Nan21], respectively, are applicable.

Before presenting these notions, we explain why new notions are necessary and previous notions are unsatisfactory. Previously, notions called size-restricted reduction [GV08] and class-specific black-box reduction [GT07] were proposed to capture non-black-box reductions in the literature [IW01; GST07]. For example, a *size-restricted reduction from a language L to avoiding a hitting set generator H* is defined to be a reduction R such that for every oracle B that avoids H and is computable by quadratic-size circuits, R^B decides L with oracle access to B. That is, the reduction works if the oracle B can be simulated by an efficient algorithm, but may not work otherwise. Impagliazzo and Wigderson [IW01] used a non-black-box reduction to show that if $\mathsf{EXP} \neq \mathsf{BPP}$, then BPP can be simulated in sub-exponential time on most inputs. It was shown in [GV08] that the reduction of [IW01] is a size-restricted reduction from EXP to avoiding a hitting set generator H_{IW}, whereas there exists a black-box reduction from PSPACE to avoiding a hitting set generator H_{TV} [TV07]. We observe that the notion of size-restricted reduction is mathematically meaningful only if a hitting set generator H is not secure. If there exists no polynomial-size circuit B that avoids H, then the hypothesis of a size-restricted reduction is false; thus, any reduction becomes vacuously a size-restricted reduction.[8] Therefore, the notion of size-restricted reduction is too weak to be useful in a variant of Pessiland in which a hitting set generator is secure (but one-way functions do not exist). Just defining a useful subclass of non-black-box reductions is highly non-trivial. We propose stronger notions of non-black-box reductions that are mathematically meaningful even if a hitting set generator is secure.

For any complexity class $\mathbb{B}$, such as P/poly, and any class $\mathbb{A}$ of problems, we introduce the notion of $\mathbb{B}$-*restricted reduction to* $\mathbb{A}$. We say that an oracle machine M is a $\mathbb{B}$-restricted reduction from a language L to $\mathbb{A}$ if for every oracle $B \in \mathbb{B}$, for all sufficiently long inputs $x \in \{0,1\}^*$, for every problem $A \in \mathbb{A}$,

$$\Pr_M[A(q) = B(q) \text{ for every query } q \text{ of } M \text{ on input } x] \geq \frac{1}{2} \tag{1}$$

implies

$$\Pr_M\left[M^B(x) = L(x)\right] \geq \frac{3}{4}. \tag{2}$$

[8] Observe that a mathematical statement "$\forall B \in \mathbb{B}, P(B)$" is vacuously true if $\mathbb{B} = \emptyset$.

Here, the probabilities are taken over the internal randomness of M. If there exists a randomized polynomial-time nonadaptive $\mathbb{B}$-restricted reduction from L to $\mathbb{A}$, we write[9]

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction \mathbb{B}.$$

An example of $\mathbb{A}$ is $\{A \mid A \text{ avoids } H\}$ for a hitting set generator H, i.e., the class of the problems of avoiding H. The idea behind the definition is that the condition Eq. (1) means that the reduction M cannot distinguish an efficient algorithm B from an oracle A that avoids a hitting set generator, under which the reduction works correctly. Note that the previous notion of size-restricted reduction only considers the situation in which $A = B$, which makes the notion too weak to be useful for our purpose.

This notion can be shown to be robust. For example, the notion remains unchanged even if the constant $\frac{1}{2}$ in Eq. (1) is changed to any constant in $(0, 1)$. Similarly, the constant $\frac{3}{4}$ in Eq. (2) can be changed to any constant in $(\frac{1}{2}, 1)$ by a standard proof technique of amplifying the success probability of BPP algorithms. Moreover, Eq. (2) can be changed to $\Pr_M\left[M^A(x) = L(x)\right] \geq \frac{3}{4}$, i.e., the reduction works under both of the oracles A and B.

A $\mathbb{B}$-restricted reduction may make a query that does not affect the decision of the reduction. For example, by making a uniformly random query $q \sim \{0,1\}^n$, we may assume that $\Pr_{q\sim\{0,1\}^n}[A(q) = B(q)] \geq \frac{1}{2}$ when we prove the correctness of the reduction. Even if the answer $B(q)$ from the oracle B may not be used by the reduction, making such a query is useful for the proof of the correctness of the reduction. This differs from the standard notion of nonadaptive reduction, in which any query that is not used to determine the output of the reduction can be omitted.

The notion of $\mathsf{P/poly}$-restricted reduction captures the non-black-box worst-case-to-average-case reduction of [Hir18]. For example, we can show

$$\mathrm{GapMCSP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \restriction \mathsf{P/poly}$$

for some hitting set generator H.

However, the proof technique of [Nan21] may not be applicable to $\mathsf{P/poly}$-restricted reductions. We need a stronger (i.e., more restrictive) notion, which we call *input-aware* $\mathsf{P/poly}$*-restricted reduction*. In a $\mathsf{P/poly}$-restricted reduction, an efficient oracle $B \in \mathsf{P/poly}$ may not know the input x to the reduction. In an input-aware $\mathsf{P/poly}$-restricted reduction, we allow B to know the input to the reduction.[10] More generally, we provide B with (not only the input but also) *input-dependent advice*, which is a short string that can depend arbitrarily on the input to the reduction. For a function $\alpha\colon \mathbb{N} \to \mathbb{N}$, we write

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction \mathbb{B} /\!/ \alpha(n)$$

if there exists a randomized polynomial-time nonadaptive oracle machine M such that for every oracle $B \in \mathbb{B}$, for all but finitely many inputs $x \in \{0,1\}^*$ and for every advice string $a \in \{0,1\}^{\alpha(|x|)}$,[11] for every problem $A \in \mathbb{A}$, if

$$\Pr_M[A(q) = B(a, q) \text{ for every query } q \text{ of } M \text{ on input } x] \geq \frac{1}{2},$$

[9] The subscript "tt" denotes truth-table reductions, which are equivalent to nonadaptive reductions.

[10] The name is intended to be "(input-aware $\mathsf{P/poly}$)-restricted reduction"; i.e., an efficient oracle in $\mathsf{P/poly}$ is input-aware. Note that a reduction itself is always input-aware, as an input is given to the reduction by definition.

[11] We emphasize that the advice string is given to the oracle but not to the reduction, which makes the reduction less powerful. This is in contrast to a complexity class with advice, in which an advice string is given to an algorithm that computes a problem, which makes the computational model more powerful (e.g., $\mathsf{P} \subseteq \mathsf{P/poly}$).

then

$$\Pr_M\left[M^{B_a}(x) = L(x)\right] \geq \frac{3}{4},$$

where $B_a(q) := B(a, q)$. This notion naturally interpolates between P/poly-restricted reductions and black-box reductions. In the extreme case where α is exponentially large, a $(\mathsf{P}/\mathsf{poly} /\!/ \alpha)$-restricted reduction is equivalent to the standard black-box reduction, as any function can be computed with an exponential amount of advice. Note that an advice string is given to an oracle but not to a reduction; thus, if an advice string becomes longer, the input-aware P/poly-restricted reduction becomes stronger. The notation "$/\!/$" of advice is borrowed from [TV07].[12]

By inspecting the proof of Nanashima [Nan21], we show that his proof is applicable to $(\mathsf{P}/\mathsf{poly} /\!/ 2n)$-restricted reductions. Although the reduction of [Hir18] is not a $(\mathsf{P}/\mathsf{poly} /\!/ 2n)$-restricted reduction, by combining it with a size-expanding reduction from NP to $\mathrm{dK}^{\mathsf{poly}}$, we obtain a $(\mathsf{P}/\mathsf{poly} /\!/ 2n)$-restricted reduction.

2.1.2 Proof Overview

Equipped with the new notions of non-black-box reductions, we now explain our overall proof strategy. The proof consists of three steps.

Step 1. Using the proof techniques of Hirahara [Hir18; Hir22c], we prove

$$\mathrm{dK}^{\mathsf{poly}} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \upharpoonright \mathsf{P}/\mathsf{poly}$$

for a universal hitting set generator H.

By combining this with the assumption that $\mathrm{dK}^{\mathsf{poly}}$ is NP-hard under size-expanding reductions,[13] we obtain an *input-aware* P/poly-restricted reduction that shows

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \upharpoonright \mathsf{P}/\mathsf{poly} /\!/ 2n.$$

Step 2. Using the proof techniques of Nanashima [Nan21] (which employ [IL90]), we prove that if

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \upharpoonright \mathsf{P}/\mathsf{poly} /\!/ 2n,$$

then

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathsf{P}/\mathsf{poly}$$

for some auxiliary-input one-way function f.

Step 3. Using the fact that a one-way function is testable, we prove that if

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathsf{P}/\mathsf{poly},$$

then

$$\mathsf{DistNP} \leq_{\mathrm{tt}}^{\mathsf{AvgBPP}} \{I \mid I \text{ inverts } g\} \upharpoonright \mathsf{P}/\mathsf{poly}$$

for some one-way function g.

[12] In more detail, Trevisan and Vadhan [TV07] introduced the notion of advice that can depend on the internal randomness of a randomized algorithm. Here, we consider the notion of advice that can depend on the input to a reduction.

[13] Since there exists a paddable NP-complete problem, NP-hardness under parametric-honest reductions implies NP-hardness under size-expanding reductions.

To complete the proof, we combine Steps 1 and 3 as follows. Step 1 shows that errorless Heuristica does not exist, i.e., $\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$ implies $\mathsf{DistNP} \not\subseteq \mathsf{i.o.AvgP/poly}$. This follows from the fact that the existence of a hitting set generator implies errorless average-case hardness of MCSP and MINKT [HS17; Hir18]. Step 3 shows that errorless Pessiland does not exist, i.e., $\mathsf{DistNP} \not\subseteq \mathsf{i.o.AvgP/poly}$ implies the existence of a one-way function.

We present details of the steps in the reverse order.

2.1.3 Step 3: Auxiliary-Input One-Way Function to One-Way Function

An *auxiliary-input one-way function* is a cryptographic primitive weaker than a one-way function [Ost91]. For a family

$$f = \left\{ f_x : \{0,1\}^{s(|x|)} \to \{0,1\}^{t(|x|)} \right\}_{x \in \{0,1\}^*}$$

of functions indexed by auxiliary inputs x, we say that an algorithm I *inverts* f *on auxiliary input* x if

$$\Pr_{y \sim \{0,1\}^{s(|x|)}} \left[I(x, f_x(y)) \in f_x^{-1}(f_x(y)) \right] \geq \frac{1}{2}.$$

An algorithm I is said to *invert* f if it inverts f on every auxiliary input x. A family f of functions is said to be an *auxiliary-input one-way function* secure against a class $\mathfrak{C}$ if there exists no algorithm in $\mathfrak{C}$ that inverts f. Note that the standard one-way function corresponds to the special case that the auxiliary input is unary, i.e.,

$$f = \left\{ f_{1^n} : \{0,1\}^{s(n)} \to \{0,1\}^{t(n)} \right\}_{n \in \mathbb{N}}.$$

The existence of a one-way function implies the existence of an auxiliary-input one-way function, but the converse is one of the fundamental open questions in cryptography [Ost91; OW93; Vad06]. However, when an auxiliary input is chosen randomly, the gap can be closed.

Let $\mathcal{D}$ be a polynomial-time samplable distribution. A well-known fact about auxiliary-input one-way functions f is that if it is hard to invert f on an auxiliary input x chosen randomly from $\mathcal{D}$, then this naturally induces a one-way function g: We may define the output of g on input (r, y) to be $(x, f_x(y))$ for randomly chosen $x \sim \mathcal{D}$ and $y \sim \{0,1\}^{s(|x|)}$, where r is a coin flip sequence to generate x. It is not hard to see that if

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \restriction \mathsf{P/poly},$$

then

$$(L, \mathcal{D}) \leq_{\mathrm{tt}}^{\mathsf{HeurBPP}} \{I \mid I \text{ inverts } g\} \restriction \mathsf{P/poly},$$

which means that the distributional problem $(L, \mathcal{D})$ is reduced to inverting the one-way function g via an *error-prone* average-case $\mathsf{P/poly}$-restricted reduction.

We make this average-case reduction *errorless* by using the simple and crucial insight from [Nan21]: a one-way function is testable. The original reduction M from L to $\{I \mid I \text{ inverts } f\}$ is guaranteed to work correctly if the oracle I inverts f on auxiliary input q, where q is a query of M. We can approximately check whether the oracle inverts f on q as follows: Sample $y \sim \{0,1\}^{s(|q|)}$ randomly, and check whether $f_q(I(q, f_q(y))) = y$. If this does not hold, it is an indication that the oracle I fails to invert f on auxiliary input q. Thus, in such a case, our errorless average-case reduction can simply output the special failure symbol "$\perp$." The probability that the reduction

fails is small because we may assume that the oracle inverts f on most auxiliary inputs q by using hardness amplification [Yao82; Gol01]. In summary, we obtain the following result, for which details can be found in Section 10

Theorem 10.3. *Let f be a polynomial-time-computable auxiliary-input family of functions. If*

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathsf{P/poly},$$

then there exists a polynomial-time-computable family $g = \{g_n : \{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$ of functions such that

$$\mathsf{DistNP} \leq_{\mathrm{tt}}^{\mathsf{AvgBPP}} \{I \mid I \text{ inverts } g\} \upharpoonright \mathsf{P/poly}.$$

Remark 2.1. In this step, we do not need our general theory of non-black-box reductions. In fact, using the general notion of P/poly-restricted reduction makes a proof unnecessarily complicated. To simplify the proof, we consider a P/poly-*restricted fixed-auxiliary-input reduction*,[14] i.e., a special case of a P/poly-restricted reduction in which any query of the reduction on input x is of the form (x, z) for some z. See Section 9 for the formal definition.

2.1.4 Step 2: Hitting Set Generator to Auxiliary-Input One-Way Function

It is known that the existence of an auxiliary-input one-way function implies the existence of a hitting set generator [Hir18; Nan21]. Accordingly, any oracle that avoids a hitting set generator can be transformed into an oracle that inverts an auxiliary-input one-way function f. Thus, we see that

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\}$$

implies

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\}$$

for some hitting set generator H. Surprisingly, Nanashima [Nan21] gave the converse for black-box reductions. We show that Nanashima's proof is applicable to non-black-box reductions. More specifically, we show that an input-aware P/poly-restricted reduction to avoiding a hitting set generator can be transformed into a P/poly-restricted reduction to inverting an auxiliary-input one-way function.

Theorem 9.3. *Let L be a language. Let*

$$H = \left\{H_n : \{0,1\}^{s(n)} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$$

be an arbitrary family of functions such that $s(n) < n - \omega(\log n)$. If

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \upharpoonright \mathsf{P/poly} \mathbin{/\!\!/} 2n$$

via an honest reduction, then there exists a polynomial-time-computable auxiliary-input function $f = \{f_x\}_{x\in\{0,1\}^*}$ such that

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathsf{P/poly}$$

[14] The notion of *fixed-auxiliary-input reduction* is due to [ABX08].

The proof of [Nan21] is based on the work of Impagliazzo and Levin [IL90] and Gutfreund and Vadhan [GV08]. We explain the proof idea below and explain a technical challenge for extending [Nan21] to non-black-box reductions.

Gutfreund and Vadhan [GV08] presented a limit of black-box reductions to avoiding a hitting set generator: if there exists an efficient black-box reduction M from a language L to avoiding a hitting set generator, then $L \in \mathsf{BPP}^{\mathsf{NP}}$. In doing so, they presented a generic approach for simulating the reduction to avoiding a hitting set generator. For an input $x \in \{0,1\}^*$, consider an oracle A_x such that $q \in A_x$ if and only if the probability $\mathcal{Q}_x(q)$ that q is queried by the reduction M is at most θ, where θ is some parameter. Here, $\mathcal{Q}_x$ denotes the query distribution of M, and $\mathcal{Q}_x(q)$ denotes the probability that q is sampled from $\mathcal{Q}_x$. Then, they observed that $\mathcal{Q}_x(q)$ can be estimated in $\mathsf{BPP}^{\mathsf{NP}}$. Hirahara and Watanabe [HW20] improved this upper bound to $\mathsf{AM} \cap \mathsf{coAM}$.

Under the non-existence of one-way functions, Impagliazzo and Levin [IL90] showed that for every polynomial-time samplable distribution $\mathcal{D}$, there exists a randomized polynomial-time algorithm T that approximates $\mathcal{D}(x)$ with high probability over a choice of $x \sim \mathcal{D}$ and the internal randomness of T. This lemma was used to characterize the existence of a one-way function by the average-case hardness of $\mathrm{q}^{\mathsf{poly}}$. By extending the lemma of [IL90] to auxiliary-input one-way functions (as in [OW93]), the problem of approximating $\mathcal{Q}_x(q)$ on average over a random choice of $q \sim \mathcal{Q}_x$ for every $x \in \{0,1\}^*$ is reduced to the task of inverting some auxiliary-input one-way function $f = \{f_x\}_{x \in \{0,1\}^*}$. By combining this with [GV08], Nanashima [Nan21] obtained a black-box reduction to inverting an auxiliary-input one-way function.

We now extend this argument to input-aware $\mathsf{P/poly}$ reductions. Observe that the oracle A_x used in [GV08] depends on x; i.e., it is an input-aware oracle. We may simulate this oracle A_x using an efficient algorithm $B \in \mathsf{P/poly}$ if B can invert f on auxiliary input x. In this case, since the oracle A_x cannot be distinguished from some $\mathsf{P/poly}$ algorithm, the $\mathsf{P/poly}$-restricted reduction M to avoiding a hitting set generator works correctly. This is a high-level idea of the proof of Theorem 9.3.

However, there is one important technical detail in the proof. Given a query q as input, it is not possible to check whether $q \in A_x$ or not exactly, as the algorithm of [IL90] cannot compute $\mathcal{Q}_x(q)$ exactly. There are two ways to circumvent this issue.

The first way is to use the idea of Hirahara and Watanabe [HW20]. They employed the proof technique of Bogdanov and Trevisan [BT06b] that selects the threshold θ randomly, which makes it possible to ensure that the probability that $\mathcal{Q}_x(q) \approx \theta$ over a choice of $q \sim \mathcal{Q}_x$ is sufficiently small. We then include θ as an input-dependent advice to the oracle, which costs the length of advice $O(\log n)$ on inputs of length n. In total, the length of input-dependent advice is $|x| + O(\log n) \leq 2n$. The proof is given in Appendix A.

The second way is to use the original idea of Gutfreund and Vadhan [GV08]. They considered a *promise* problem A_x that avoids a hitting set generator, and showed that any oracle that is consistent with A_x can be used to simulate the reduction M. To implement their approach in our setting, we need to extend the notion of $\mathbb{B}$-restricted reduction to $\mathbb{A}$. We consider not only a class of problems but also a class $\mathbb{A}$ of *promise problems*. In addition, we need to consider a class $\mathbb{B}$ of randomized algorithms. The extended definition can be found in Section 8. The details of the proof are presented in Section 9.

2.1.5 Step 1: NP to Hitting Set Generator

By generalizing the worst-case to average-case reduction for MINKT [Hir18], Hirahara [Hir22c] showed that the problem of approximating the *conditional* time-bounded Kolmogorov complexity is easy in Heuristica. We give a further generalization, by showing that approximating $\mathrm{dK}^{\mathsf{poly}}$ is also easy in Heuristica. Moreover, we show that these non-black-box reductions are P/poly-restricted.

Hirahara's reductions are P/poly-restricted. To illustrate that Hirahara's reductions are P/poly-restricted, we review the proof of [Hir18; Hir20b]. Specifically, we reduce the problem of approximating q^t to avoiding a universal hitting set generator. Here, the universal hitting set generator

$$\mathcal{H}^{\mathrm{univ}} = \left\{\mathcal{H}^{\mathrm{univ}}_n \colon \{0,1\}^{s(n)} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$$

is defined as follows. $\mathcal{H}^{\mathrm{univ}}_n$ takes a program of description length $s(n)$, simulates the program for $\mathsf{poly}(n)$ steps (e.g., n^2 steps) and outputs the output of the program. We let $s(n) := n-1$ in this proof overview.[15]

The main technical building block is a pseudorandom generator construction [TV07]. We use a simple pseudorandom generator construction with small advice complexity, which is called the *k-wise direct product generator*

$$\mathrm{DP}_k \colon \{0,1\}^n \times \{0,1\}^{nk} \to \{0,1\}^{nk+k}$$

and is defined as

$$\mathrm{DP}_k(x; z^1, \cdots, z^k) := (z^1, \cdots, z^k, \langle x, z^1\rangle, \cdots, \langle x, z^k\rangle).$$

The pseudorandom generator construction DP_k satisfies the following pseudorandomness property: there exists a polynomial p such that if $\mathrm{q}^{p(n/\epsilon),D}(x) > k + \log p(n/\epsilon)$, then

$$\left|\Pr_z[D(\mathrm{DP}_k(x;z)) = 1] - \Pr_w[D(w) = 1]\right| \le \epsilon.$$

Using this, we present a proof sketch of the following non-black-box worst-case to average-case reduction for the problem of approximating q^t.

Theorem 2.2. *For a polynomial τ and an oracle B, let $\mathrm{Gap}_\tau\mathrm{MqP}^B = (\Pi_{\mathrm{YES}}, \Pi^B_{\mathrm{NO}})$ be the promise problem defined as*

$$\Pi_{\mathrm{YES}} := \left\{(x, 1^t, 1^s) \;\middle|\; t \ge |x| \text{ and } \mathrm{q}^t(x) \le s\right\},$$
$$\Pi^B_{\mathrm{NO}} := \left\{(x, 1^t, 1^s) \;\middle|\; t \ge |x| \text{ and } \mathrm{q}^{\tau(t),B}(x) > s + \log\tau(t)\right\}.$$

Then, there exists a polynomial τ such that for every oracle B,

$$\mathrm{Gap}_\tau\mathrm{MqP}^B \le^{\mathsf{BPP}}_{\mathrm{tt}} \left\{A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\right\} \restriction \{B\}.$$

Here is a proof sketch. Given an instance $(x, 1^t, 1^s)$, consider a reduction M^B that outputs 1 if and only if $B(\mathrm{DP}_k(x;z)) = 0$ for a random $z \sim \{0,1\}^{nk}$, where $n := |x|$ and $k \approx s$. The reduction makes an additional query $w \sim \{0,1\}^{nk+k}$, which ensures that the oracle B accepts many strings.

[15] For Step 2 to work, $s(n) = n - \omega(\log n)$ must be satisfied.

Recall that it suffices to prove the correctness of B-restricted reductions under the assumption that B agrees with an oracle A that avoids $\mathcal{H}^{\mathrm{univ}}$. Let A be an arbitrary oracle that avoids $\mathcal{H}^{\mathrm{univ}}$. We assume that

$$\Pr_M\left[A(q) = B(q) \text{ for every query } q \text{ of } M \text{ on input } (x, 1^t, 1^s)\right] \geq 1 - \epsilon$$

for a small constant $\epsilon > 0$ and prove the correctness of M^B under this assumption. Since M^B makes a query $w \sim \{0,1\}^{nk+k}$, the assumption implies that

$$\Pr_{w \sim \{0,1\}^{nk+k}}[A(w) = B(w)] \geq 1 - \epsilon.$$

Thus, since A accepts at least half of the strings, we obtain

$$\Pr_w[B(w) = 1] \geq \Pr_w[A(w) = 1] - \Pr_w[A(w) \neq B(w)] \geq \frac{1}{2} - \epsilon.$$

This helps us to establish the correctness of M^B in the No case. Assume that $(x, 1^t, 1^s)$ is a No instance, i.e., $\mathrm{q}^{\tau(t),B}(x) > s + \log \tau(t)$. Then, by the pseudorandomness property of DP_k, B cannot distinguish the output distribution of $\mathrm{DP}_k(x;\text{-})$ from the uniform distribution. Thus,

$$\Pr_M\left[M^B(x, 1^t, 1^s) = 0\right] = \Pr_z[B(\mathrm{DP}_k(x; z)) = 1] \approx \Pr_w[B(w) = 1] \geq \frac{1}{2} - \epsilon,$$

which means that M^B rejects with probability $\gtrsim \frac{1}{2}$.

Similarly, since M^B makes a query $\mathrm{DP}_k(x; z)$ for a random z, we have

$$\Pr[B(\mathrm{DP}_k(x; z)) = 1] \leq \Pr[A(\mathrm{DP}_k(x; z)) = 1] + \epsilon.$$

In the Yes case, using the fact that the Kolmogorov complexity of $\mathrm{DP}_k(x; z)$ is small, we can argue that $\mathrm{DP}_k(x; z) \in \mathrm{Im}(\mathcal{H}^{\mathrm{univ}})$.[16] Since A rejects any string in the image of $\mathcal{H}^{\mathrm{univ}}$,

$$\Pr\left[M^B(x, 1^t, 1^s) = 0\right] = \Pr[B(\mathrm{DP}_k(x; z)) = 1] \leq \epsilon,$$

implying that M^B rejects with probability at most ϵ. This completes the proof sketch of Theorem 2.2.

Details can be found in Section 8.

Symmetry of Information for distributional Kolmogorov complexity. Next, we explain how to generalize the result of [Hir22c] to distributional Kolmogorov complexity. The main idea is encapsulated in the following.

Theorem 7.8. *If* $\mathsf{DistNP} \subseteq \mathsf{AvgP}$*, then there exists a polynomial* τ *such that for every* $x \in \{0,1\}^*$*, every distribution* $\mathcal{D}$ *over* $\{0,1\}^m$*, every* $\lambda \in [0,1]$*, every* $\epsilon^{-1} \in \mathbb{N}$*, and every* $t \geq |x| + m + \epsilon^{-1}$*, it holds that*

$$\mathrm{dK}^{\tau(t)}_{\lambda-\epsilon}(x \mid \mathcal{D}) \leq \min\left\{ s \in \mathbb{N} \;\middle|\; \Pr_{y \sim \mathcal{D}}\left[\mathrm{K}^t(x, y) - \mathrm{K}^{\tau(t)}(y) \leq s\right] \geq \lambda \right\} + \log \tau(t).$$

[16] In the actual proof, we show $\mathrm{DP}_k(x; z) \cdot r \in \mathrm{Im}(\mathcal{H}^{\mathrm{univ}})$ for a uniformly random string r.

This generalizes symmetry of information for time-bounded Kolmogorov complexity in Heuristica [Hir22c; GK22]. Here, symmetry of information refers to the statement that for some polynomial τ, for every $x, y \in \{0,1\}^*$ and every $t \geq |x| + |y|$,

$$\mathrm{K}^{\tau(t)}(x \mid y) \leq \mathrm{K}^t(x, y) - \mathrm{K}^{\tau(t)}(y) + \log \tau(t) \tag{3}$$

This is the special case of Theorem 7.8 in which $\mathcal{D}$ is the singleton distribution on y. Symmetry of information enables us to approximate time-bounded conditional Kolmogorov complexity by its unconditional variant. Specifically, observing that (x, y) can be described by a program that prints y and a program that prints x given y as input, we have

$$\begin{aligned} \mathrm{K}^t(x, y) - \mathrm{K}^{\tau(t)}(y) &\leq \mathrm{K}^{t/4}(x \mid y) + \mathrm{K}^{t/4}(y) - \mathrm{K}^{\tau(t)}(y) + O(1) \\ &\leq \mathrm{K}^{t/4}(x \mid y) + \mathrm{cd}_{\mathrm{K}}^{t/4}(y) + O(1), \end{aligned} \tag{4}$$

where $\mathrm{cd}_{\mathrm{K}}^{t/4}(y) := \mathrm{K}^{t/4}(y) - \mathrm{K}(y)$ denotes the computational depth of y [AFMV06], which is known to be small for most strings. By combining this with Eq. (3), the conditional Kolmogorov complexity $\mathrm{K}^{\mathsf{poly}}(x \mid y)$ can be approximated by $\mathrm{K}^{\mathsf{poly}}(x, y) - \mathrm{K}^{\mathsf{poly}}(y)$ to within an additive error of $\mathrm{cd}_{\mathrm{K}}^{\mathsf{poly}}(y)$.

Similarly, Theorem 7.8 makes it possible to reduce the problem of approximating $\mathrm{dK}^{\mathsf{poly}}$ to the problem of approximating $\mathrm{K}^{\mathsf{poly}}$. Let $s = \mathrm{dK}_{\lambda-\epsilon}^{\tau(t)}(x)$ and M be the program of size s that prints x on input $y \sim \mathcal{D}$ with probability at least $\lambda - \epsilon$. Then, for every y such that $M(y) = x$, we have

$$\mathrm{K}^{\mathsf{poly}(t)}(x, y) \leq s + \mathrm{K}^t(y) + O(1).$$

Thus, we obtain the following lower bound on $\mathrm{dK}^{\mathsf{poly}}$:

$$\min\left\{ s \in \mathbb{N} \;\middle|\; \Pr_{y \sim \mathcal{D}}\left[\mathrm{K}^{\mathsf{poly}(t)}(x, y) - \mathrm{K}^t(y) \leq s + O(1)\right] \geq \lambda - \epsilon \right\} \leq \mathrm{dK}_{\lambda-\epsilon}^{\tau(t)}(x \mid \mathcal{D}).$$

Combining this with Theorem 7.8, we see that $\mathrm{dK}^{\mathsf{poly}}$ can be approximated using $\mathrm{K}^{\mathsf{poly}}$.

It is worth mentioning that Theorem 7.8 provides a computational analogue of the theorem of Muchnik [Muc02], which shows that for any strings x, y, and z of length n, the length of a shortest program M such that $M(y) = x$ and $M(z) = x$ is $\max\{\mathrm{K}(x \mid y), \mathrm{K}(x \mid z)\} + \Theta(\log n)$. By considering a distribution $\mathcal{D}_{y,z}$ that outputs y with probability $\frac{1}{2}$ and outputs z with probability $\frac{1}{2}$, Theorem 7.8 shows that

$$\mathrm{dK}_{\frac{3}{4}}^{\tau(t)}(x \mid \mathcal{D}_{y,z}) \leq \max\left\{\mathrm{K}^t(x, y) - \mathrm{K}^{\tau(t)}(y), \mathrm{K}^t(x, z) - \mathrm{K}^{\tau(t)}(z)\right\} + \log \tau(t) =: s'.$$

This implies that there exists a program M of length $s' \approx \max\{\mathrm{K}^t(x \mid y), \mathrm{K}^t(x \mid z)\}$ such that $M(y) = x$ and $M(z) = x$ and that M runs in time $\tau(t)$.

We now explain a high-level proof idea of Theorem 7.8. The key ingredient of the proof is a new property of DP_k. The proof of the pseudorandomness property of DP_k is given by constructing a reconstruction procedure R^D that takes an advice string of length $\approx k$ and reconstructs x. Here, through a careful analysis, we present a reconstruction procedure R^D with the following property: for every D that distinguishes $\mathrm{DP}_k(x; \text{-})$ from the uniform distribution with advantage λ, $R^D(\mathrm{DP}_{k+\ell}(x; z))$ outputs x with probability $\lambda - \epsilon$, where $\ell = O(\log(n/\delta))$. Then, we can construct a program that takes $\mathrm{DP}_{k+\ell}(x; z)$ as hard-wired input and prints x on input $y \sim \mathcal{D}$, which suggests that $\mathrm{dK}_{\lambda-\epsilon}^{\mathsf{poly}}(x \mid \mathcal{D})$ is small.

Details can be found in Section 7.

2.2 Conditional NP-Hardness of dK

We explain how to prove NP-hardness of distributional Kolmogorov complexity under the assumption that a one-way function exists. Our proof is inspired by the recent NP-hardness proofs of learning programs and the partial function variant MCSP* of MCSP [Hir22b].

As in [Hir22c; Hir22b], we reduce the Minimum Monotone Satisfying Assignment problem (MMSA) using a secret sharing scheme. Let φ be a monotone formula on n variables. The goal of MMSA is to approximate the minimum weight of a satisfying assignment of φ by using an oracle for computing $\mathrm{dK}^{\mathsf{poly}}$.

We use the secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$ for the monotone formula φ [BL88]. We say that $T \subseteq [n]$ is *authorized* if the characteristic vector of T satisfies φ. A secret sharing scheme enables sharing a secret $x \sim \{0,1\}^\ell$ among n parties, so that any authorized set of parties can reconstruct the secret, whereas any unauthorized set of parties has no information about the secret. Let $(s_1, \cdots, s_n) := \mathrm{Share}(x)$, where s_i is the share given to the i-th party.

We construct a distribution $\mathcal{D}$ such that φ is satisfiable by an assignment of small weight if and only if $\mathrm{dK}^{\mathsf{poly}}(x \mid \mathcal{D})$ is small. To this end, let $\mathrm{GL}_k \colon \{0,1\}^\lambda \times (\{0,1\}^\lambda)^k \to \{0,1\}^k$ denote the Goldreich–Levin hard-core function [GL89]:

$$\mathrm{GL}_k(f; z^1, \cdots, z^k) := \langle f, z^1 \rangle \cdots \langle f, z^k \rangle,$$

where $\langle a, b \rangle$ denotes the inner product of a and $b \mod 2$. We choose $f_1, \cdots, f_n \sim \{0,1\}^\lambda$ randomly. The distribution $\mathcal{D}$ is constructed as follows. First, $z_1, \cdots, z_n \sim \{0,1\}^{\lambda k}$ is chosen randomly. Let $G_m \colon \{0,1\}^{m^\epsilon} \to \{0,1\}^m$ be a pseudorandom generator. Then, define

$$y := (z_1, \cdots, z_n, G_m(\mathrm{GL}_k(f_1; z_1)) \oplus s_1, \cdots, G_m(\mathrm{GL}_k(f_n; z_n)) \oplus s_n)$$

and the distribution outputs y. Here, we assume that the length of each share is m. This completes the description of $\mathcal{D}$.

To see why this works, let $T \subseteq [n]$ be a small set whose characteristic vector satisfies φ. Consider a program M that takes $\{f_i \mid i \in T\}$ as hard-wired input. Then, the program can compute $G_m(\mathrm{GL}_k(f_i; z_i))$ for each $i \in [n]$. Thus, given y, the program M can compute $\{s_i \mid i \in T\}$, from which the secret x can be reconstructed.

Conversely, assume that there exists a small program M that computes x from $y \sim \mathcal{D}$. Using the algorithmic information extraction lemma of [Hir22b], one can extract from M a small set $T \subseteq [n]$ such that $|T| \leq (1 + o(1)) \cdot |M|/\lambda$ and M cannot distinguish the distribution of $(z_i, \mathrm{GL}_k(f_i; z_i) \oplus s_i)$ for $z_i \sim \{0,1\}^{\lambda k}$ from the uniform distribution for every $i \notin T$. Thus, the only information that M can obtain from y is $\{s_i \mid i \in T\}$. If M can output x from such a set of shares, by the privacy of the secret sharing scheme, T must be authorized. Thus, the characteristic vector of T satisfies φ.

3 Are Meta-Computational Problems Paddable?

Given that an approximation-preserving padding reduction for $\mathrm{dK}^{\mathsf{poly}}$ has a significant consequence (Theorem 1.5), we propose to study whether meta-computational problems are paddable.

For example, consider a formula variant of MCSP. For a Boolean function $f \colon \{0,1\}^n \to \{0,1\}$, let $\mathsf{L}(f)$ denote the minimum number of literals of a De Morgan formula that computes f. The problem Formula-MCSP asks to decide whether $\mathsf{L}(f) \leq s$ for a given truth table of f and a size parameter s. The paddability of Formula-MCSP is closely related to the conjecture of Karchmer,

Raz, and Wigderson [KRW95]. *The KRW conjecture* states that $\mathsf{L}(f \diamond g) \approx \mathsf{L}(f) \cdot \mathsf{L}(g)$ for non-constant functions f and g, where $f \diamond g$ denotes the block-composition of f and g. This provides a way to map f to a function $f \diamond g$ whose complexity is larger than the complexity of f. Using the fact that the special case of the KRW conjecture in which $g = \oplus_m$ is resolved [Hås98; DM18], we observe that Formula-MCSP has an approximation-preserving padding reduction.

Proposition 3.1. *There exists a quasi-polynomial-time algorithm that takes the truth table of a function $f\colon \{0,1\}^n \to \{0,1\}$ and outputs the truth table of a function $f'\colon \{0,1\}^{n'} \to \{0,1\}$ such that*

$$\mathsf{L}(f') = \mathsf{L}(f) \cdot \widetilde{\Theta}(s(n))$$

for some function $s(n) = \mathsf{poly}(n) \geq \omega(1)$.

Proof Sketch. It was shown in [Hås98] (see also [DM18]) that

$$\frac{\mathsf{L}(f) \cdot \mathsf{L}(\oplus_m)}{\mathsf{poly}(\log n, \log m)} \leq \mathsf{L}(f \diamond \oplus_m) \leq \mathsf{L}(f) \cdot \mathsf{L}(\oplus_m).$$

Define $f' := f \diamond \oplus_m$ for a sufficiently large $m = \mathsf{poly}(n)$. Since $\mathsf{L}(\oplus_m) = \Theta(m^2)$, we obtain

$$\mathsf{L}(f) \cdot m^2/\mathsf{poly}(\log n) \leq \mathsf{L}(f \diamond \oplus_m) \leq \mathsf{L}(f) \cdot O(m^2).$$

The input length of f' is $n \cdot m \leq \mathsf{poly}(n)$. Thus, the size of the truth table of f' is a quasi-polynomial in 2^n. □

It is interesting to see whether similar padding reductions exist for other meta-computational problems, such as MCSP. We conjecture that a similar approximation-preserving reduction exists for MCSP.

Conjecture 3.2 (MCSP Padding Conjecture)**.** *There exists an efficient algorithm that takes the truth table of a function $f\colon \{0,1\}^n \to \{0,1\}$ and outputs the truth table of a function $f'\colon \{0,1\}^{n'} \to \{0,1\}$ such that*

$$\mathsf{CC}(f') \approx \mathsf{CC}(f) \cdot s(n)$$

for some function $s(n) = \omega(1)$. Here, $\mathsf{CC}(f)$ denotes the size of a minimum circuit that computes f.

Because paddability is a weaker property than NP-hardness, we expect that investigating Conjecture 3.2 would provide new insight into the complexity of MCSP as well as the Meta-Complexity Padding Conjecture.

4 Related Work

In this section, we mention additional previous results related to our results.

Cryptography from information loss. Ball, Boyle, Degwekar, Deshpande, Rosen, Vaikuntanathan, and Vasudevan [BBDDRVV20] showed that a reduction that loses the information about inputs (a lossy reduction) can be used to construct a one-way function. For example, they showed that if a language L is reduced to another language via a reduction that loses the information about inputs, then there exists a one-way function whose security is based on the worst-case hardness of L. Conceptually, our results are somewhat similar to theirs. A size-expanding reduction for $\mathrm{dK}^{\mathsf{poly}}$ enables us to construct reductions that work correctly under any *input-aware* oracles. This is because a size-expanding reduction enables us to "hide" its input from input-aware oracles. The property of having a lossy reduction is strong: NP-complete problems are unlikely to have a lossy reduction because it implies an upper bound of SZK.

A comparison with the Universality Conjecture. Santhanam [San20] proposed the Universality Conjecture, under which the existence of a one-way function is equivalent to an average-case hardness of MCSP. It is known that the Universality Conjecture cannot be resolved with relativizing proof techniques [RS22]. The consequences of the Universality Conjecture are similar to the consequences of the Meta-Complexity Padding Conjecture (Theorem 1.5). The main question is whether it is feasible to prove these conjectures with current proof techniques. The proof techniques of [San20] are relativizing; thus, the current proof techniques seem to be far from resolving the Universality Conjecture. By contrast, the NP-hardness of $\mathrm{dK}^{\mathsf{poly}}$ under the existence of a one-way function provides evidence of the feasibility of resolving the Meta-Complexity Padding Conjecture—particularly because the proof techniques do not relativize [Hir22b].

NP-complete problems and one-way functions. Allender, Cheraghchi, Myrisiotis, Tirumala, and Volkovich [ACMTV21] and Liu and Pass [LP22] considered whether there exists a natural NP-complete problem whose average-case complexity characterizes the existence of a one-way function, and showed that the problem of computing sublinear-time-bounded conditional Kolmogorov complexity has this property. Note that the *naturalness* of the problem is indispensable for their results to be non-trivial, as the worst-case complexity (NP-completeness) and the average-case complexity can differ significantly for artificial problems. By contrast, it is unclear whether a characterization analogous to ours can be easily proved for artificial problems.

Whether NP-completeness of polynomial-time-bounded conditional Kolmogorov complexity characterizes the existence of a one-way function (if NP is hard in the worst case) is an interesting open question. To answer this question in the affirmative, it suffices to improve our NP-hardness of distributional Kolmogorov complexity under the existence of a one-way function (Section 2.2) to polynomial-time-bounded conditional Kolmogorov complexity. It is worth mentioning that Huang, Ilango, and Ren [HIR23] recently proved NP-hardness of polynomial-time-bounded conditional Kolmogorov complexity under the existence of an indistinguishability obfuscation.

5 Preliminaries

Notation. $[n]$ denotes $\{1, \ldots, n\}$. For n strings $x_1, \cdots, x_n$ and a subset $T \subseteq [n]$, let $x_T := (x_i \mid i \in T)$.

We often identify a language $L \subseteq \{0,1\}^*$ with its characteristic function $L \colon \{0,1\}^* \to \{0,1\}$.

A *promise problem* Π is a pair $(\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ of languages. We identify Π with a function $\Pi \colon \{0,1\}^* \to \{0,1,*\}$ such that $\Pi(x) := 1$ if $x \in \Pi_{\mathrm{YES}}$, $\Pi(x) := 0$ if $x \in \Pi_{\mathrm{NO}}$ and $\Pi(x) := *$

otherwise. If $\Pi_{\mathrm{YES}} = \{0,1\}^* \setminus \Pi_{\mathrm{NO}}$, we identify Π with the language Π_{YES}. A language $L \subseteq \{0,1\}^*$ is said to be *consistent with* Π if $\Pi_{\mathrm{YES}} \subseteq L \subseteq \{0,1\}^* \setminus \Pi_{\mathrm{NO}}$. Similarly, a distribution $\mathcal{A}$ over oracles is said to be consistent with Π if every $A \in \mathcal{A}$ is consistent with Π.

A function $A\colon \{0,1\}^* \to \{0,1,*\}$ is identified with a promise $(A_{\mathrm{YES}}, A_{\mathrm{NO}})$, where $A_{\mathrm{YES}} = A^{-1}(1)$ and $A_{\mathrm{NO}} = A^{-1}(0)$. Let $\mathrm{dom}(A)$ denote the domain of A, i.e., $A^{-1}(\{0,1\})$.

Nonadaptive Reductions. A randomized nonadaptive oracle machine M consists of two randomized machines $M = (Q_M, D_M)$. On input x and a coin flip sequence r, the machine Q_M outputs a sequence $Q_M(x;r)$ of queries.[17] The output $M^A(x;r)$ of the reduction under an oracle A is defined to be $D_M(x, A(q_1), \cdots, A(q_m); r)$, where $(q_1, \cdots, q_m) := Q_M(x;r)$. We often omit the coin flip sequence r from the notations and regard $M^A(x)$ and $Q_M(x)$ as a random variable. For example, $Q_M(x)$ denotes the set of the queries that M makes on input x.

We may assume without loss of generality that for every randomized nonadaptive machine M, there exists a single distribution $\mathcal{Q}_x$ such that the i-th query of M is identically distributed with $\mathcal{Q}_x$ for every $i \in [m]$. This is because the indices of the queries can be shuffled randomly, whose idea is due to Szegedy [FF93]. Throughout this paper, we call the distribution *the query distribution of* M *on input* x and denote it by $\mathcal{Q}_x$.

Randomized oracle. Consider a randomized reduction M and a randomized algorithm A. We often combine them to obtain the randomized algorithm M^A that, on input $x \in \{0,1\}^*$, simulates M on input x by answering any query q to an oracle with $A(q;r)$, where r is a fresh random coin flip sequence and $A(q;r)$ denotes the output of the randomized algorithm A with a coin flip sequence r. To emphasize that a fresh random coin flip is used for each invocation of an oracle,[18] we introduce the notion of *randomized oracle*, which abstracts the property of a randomized algorithm as an oracle.

Definition 5.1. *A* randomized oracle B *is a family of distributions* B_q *over* $\{0,1\}^*$ *for each* $q \in \{0,1\}^*$. *We regard* B *as an oracle that takes a query* q *as input and answers a string a independently drawn from the distribution* B_q. *We identify a randomized algorithm* M *with a randomized oracle* $B = \{B_q\}_{q \in \{0,1\}^*}$, *where* B_q *is the distribution of* $M(q;r)$ *over a random coin flip sequence* r.

To emphasize the difference between the standard complexity class BPP and a class of randomized algorithms that are regarded as randomized oracles, let $\mathbb{BPP}$ denote the class of randomized oracles constructed from randomized (multi-output) polynomial-time algorithms. Similarly, let $\mathbb{BPP}/\mathsf{poly}$ denote the class of randomized oracles constructed from randomized polynomial-time algorithms that take $\mathsf{poly}(n)$ bits of advice on inputs of length n.

Kolmogorov Complexity. We fix an efficient universal Turing machine U. We extend Definition 1.1 to distributional Kolmogorov complexity with randomized oracles.

Definition 5.2. *For a string* $x \in \{0,1\}^*$, *a time bound* $t \in \mathbb{N}$, *a parameter* $\lambda \in (0,1]$, *a distribution* $\mathcal{A}$ *over randomized oracles, and a distribution* $\mathcal{D}$ *over* $\{0,1\}^*$, *the* $\mathcal{A}$-oracle t-time-bounded distributional Kolmogorov complexity of x given $\mathcal{D}$ *is defined to be*

$$\mathrm{dK}^{t,\mathcal{A}}_{\lambda}(x \mid \mathcal{D}) := \min\left\{ |d| \;\middle|\; \Pr_{A\sim\mathcal{A},A,y\sim\mathcal{D}}[U^A \text{ outputs } x \text{ on input } (d,y) \text{ in time } t] \geq \lambda \text{ and } d \in \{0,1\}^* \right\},$$

[17] We often regard $Q_M(x;r)$ as a multiset.

[18] This fact is important for the proof of Proposition 8.2.

where the probability is taken over a choice of $A \sim \mathcal{A}$, the randomness of the randomized oracle A, and $y \sim \mathcal{D}$. For a function $\tau\colon \mathbb{N} \to \mathbb{N}$, we define

$$\mathrm{dK}_\lambda^{\tau,\mathcal{A}}(x \mid \mathcal{D}) := \mathrm{dK}_\lambda^{\tau(n+m),\mathcal{A}}(x \mid \mathcal{D}),$$

where $n := |x|$ and $m := \max\{|y| \mid y \in \mathrm{supp}(\mathcal{D})\}$. For a randomized oracle A, we define $\mathrm{dK}_\lambda^{t,A}(x \mid \mathcal{D}) := \mathrm{dK}_\lambda^{t,\mathcal{A}_A}(x \mid \mathcal{D})$, where $\mathcal{A}_A$ denotes the singleton distribution on A. We omit the superscript A if $A = \emptyset$ and the subscript λ if $\lambda = \frac{1}{10n}$.

The notion of distributional Kolmogorov complexity generalizes the notion of randomized time-bounded Kolmogorov complexity.

Definition 5.3 (Randomized time-bounded Kolmogorov complexity)**.** *For strings $x, y \in \{0,1\}^*$, a time bound $t \in \mathbb{N}$, a distribution $\mathcal{A}$ over randomized oracles, and a parameter $\lambda > 0$, the A-oracle t-time-bounded Kolmogorov complexity of x given y is defined as*

$$\mathrm{rK}_\lambda^{t,\mathcal{A}}(x \mid y) := \mathrm{dK}_\lambda^{t,\mathcal{A}}(x \mid y, \mathcal{U}_t),$$

where $\mathcal{U}_t$ denotes the uniform distribution over $\{0,1\}^t$. We omit the subscript λ if $\lambda = 3/4$.

The following is immediate from the definition.

Fact 5.4. *Let $A \in \mathbb{BPP}$ be a randomized oracle. Then, there exists a polynomial p such that for every $x \in \{0,1\}^*$, every $t \geq |x|$ and every $\lambda \in (0,1]$,*

$$\mathrm{dK}_\lambda^{p(t)}(x) \leq \mathrm{dK}_\lambda^{t,A}(x) + O(1).$$

A simple counting argument implies the following basic fact of Kolmogorov-randomness.

Fact 5.5. *For any integer $s \geq 1$ and any string $y \in \{0,1\}^*$, the number of strings $x \in \{0,1\}^*$ such that $\mathrm{K}(x \mid y) < s$ is less than 2^s.*

Proof. The number of programs of length less than s is at most $\sum_{i=0}^{s-1} 2^i < 2^s$. □

We introduce a variant of computational depth [AFMV06] defined by using the universal a priori probability.

Definition 5.6. *For a time bound $t \in \mathbb{N}$, a string $x \in \{0,1\}^*$, and an oracle A, the* computational depth *of x is defined as*

$$\mathrm{cd}^{t,A}(x) := \mathrm{q}^t(x) - \mathrm{K}^A(x).$$

Here, $\mathrm{q}^t(x) := -\log \Pr_{d \sim \{0,1\}^t}\left[U^t(d) = x\right]$ and $\mathrm{K}^A(x) := \min\left\{|d| \mid U^A(d) = x\right\}$. We omit the superscript A if $A = \emptyset$.

Cryptography. The existence of a one-way function is known to be equivalent to the existence of a pseudorandom generator.

Lemma 5.7 (Håstad, Impagliazzo, Levin, and Luby [HILL99])**.** *There exists a one-way function secure against polynomial-size circuits if and only if for any constant $\epsilon > 0$, there exists a pseudorandom generator*

$$G = \left\{G_n : \{0,1\}^{n^\epsilon} \to \{0,1\}^n\right\}_{n \in \mathbb{N}}$$

secure against polynomial-size circuits.

6 NP-Hardness of Distributional Kolmogorov Complexity

In this section, we prove NP-hardness of distributional Kolmogorov complexity under the existence of a one-way function. We first introduce the notion of reduction to a family of problems.

Definition 6.1 (Reductions to a family of problems)**.** *For a promise problem* Π *and for a family* $\mathbb{F}$ *of promise problems, we say that* Π reduces to $\mathbb{F}$ *and write* $\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{F}$ *if there exists a randomized polynomial-time nonadaptive oracle machine* M *such that for all* $F \in \mathbb{F}$*, for all but finitely many* $x \in \mathrm{dom}(\Pi)$*, for all oracles* A *that are consistent with* F*,*

$$\Pr_M\left[M^A(x) = \Pi(x)\right] \geq \frac{3}{4},$$

where the probability is taken over the internal randomness of M*.*

Definition 6.2. *For a polynomial* $\tau\colon \mathbb{N} \to \mathbb{N}$*, functions* $\epsilon\colon \mathbb{N} \to [0,\infty)$*,* $\delta\colon \mathbb{N} \to (0,1)$*, and an oracle* A*, let*

$$\Pi^A_{\mathrm{YES}} := \left\{(x, \mathcal{D}, 1^s, \lambda) \;\middle|\; \mathrm{dK}^{\tau,A}_\lambda(x \mid \mathcal{D}) \leq s\right\},$$
$$\Pi^A_{\mathrm{NO}} := \left\{(x, \mathcal{D}, 1^s, \lambda) \;\middle|\; \mathrm{dK}^{\tau,A}_{\lambda-\delta(|x|)}(x \mid \mathcal{D}) > (1+\epsilon(|x|)) \cdot s\right\}.$$

We define $\mathrm{Gap}_{\tau,\epsilon,\delta}\mathrm{MdKP}^A$ *to be the promise problem* $(\Pi^A_{\mathrm{YES}}, \Pi^A_{\mathrm{NO}})$*. By default, we assume* $\delta(n) := 1/n$ *and let* $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP} := \mathrm{Gap}_{\tau,\epsilon,1/n}\mathrm{MdKP}$*. The promise problem* $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdpKP}$ *is defined by using* $\mathrm{dpK}^{\tau,A}_\lambda$ *instead of* $\mathrm{dK}^{\tau,A}_\lambda$ *(see Definition 7.2 for the definition of* $\mathrm{dpK}^{\tau,A}_\lambda$*).*

Theorem 6.3. *If a one-way function secure against polynomial-size circuits exists, then*

$$\mathsf{NP} \leq_{\mathrm{m}}^{\mathsf{coRP}} \left\{\mathrm{Gap}_{\tau,\alpha}\mathrm{MdKP}^A \mid \tau\colon \text{a polynomial}, A \in \mathsf{P/poly}\right\}$$

for some $\alpha(n) = n^{1/(\log\log n)^{O(1)}}$*. Here,* $\leq_{\mathrm{m}}^{\mathsf{coRP}}$ *refers to a randomized polynomial-time reduction that maps* YES *instances to* YES *instances with probability 1 and maps* NO *instances to* NO *instances with probability at least* $\frac{1}{2}$*. Moreover, the reduction is size-expanding.*

Here, we say that a function τ is polynomial if $\tau(n) = n^c + c$ for some constant $c \geq 1$. In particular, we assume that $\tau(n) \geq n$ for any $n \in \mathbb{N}$. By padding, we may assume that the time bound τ of dK^τ is sufficiently large.

6.1 Minimum Monotone Satisfying Assignment

We reduce the Minimum Monotone Satisfying Assignment (MMSA) problem to GapMdKP

Definition 6.4 (Minimum Monotone Satisfying Assignment; MMSA)**.** *For a monotone formula* φ *on* n *variables, the* weight *of an assignment* $\alpha \in \{0,1\}^n$ *is defined to be* $\sum_{i=1}^n \alpha_i$*. Let* $\mathrm{MMSA}(\varphi)$ *denote the minimum weight of* $\alpha \in \{0,1\}^n$ *such that* $\varphi(\alpha) = 1$*.*

It is known that MMSA is NP-hard to approximate:

Lemma 6.5 ([DS04; DHK15]). *For some function $g(n) = n^{1/(\log\log n)^{O(1)}}$, it is* NP*-hard under polynomial-time deterministic reductions to solve the promise problem* $\mathrm{Gap}_g\mathrm{MMSA} = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ *defined as follows:*

$$\Pi_{\mathrm{YES}} := \{(\varphi, s) \mid \mathrm{MMSA}(\varphi) \leq s\},$$
$$\Pi_{\mathrm{NO}} := \{(\varphi, s) \mid \mathrm{MMSA}(\varphi) > s \cdot g(|\varphi|)\},$$

where $|\varphi|$ denotes the length of the binary string that represents φ.

6.2 Secret Sharing Scheme

We review the notion of secret sharing scheme. Whether a party is authorized or not is determined by an access structure.

Definition 6.6 (Access Structure). *An* access structure *$\mathcal{A} \subseteq 2^{[n]}$ is a "monotone" collection of subsets of $[n]$; that is, for every $T \supseteq S \in \mathcal{A}$, we have $T \in \mathcal{A}$.*

Definition 6.7 (Secret Sharing [Bei11]). *A* secret sharing scheme *for $\mathcal{A}$ is a pair* $(\mathrm{Share}, \mathrm{Rec})$ *of a randomized algorithm* Share *and a deterministic algorithm* Rec *with the following properties for every $\ell \in \mathbb{N}$:*

1. Correctness: *For every $T \in \mathcal{A}$ and for every string $x \in \{0,1\}^\ell$, any output of* $\mathrm{Share}(x)$ *is a sequence $(y_1, \ldots, y_n)$ of n strings that satisfies*
$$\mathrm{Rec}(T, y_T) = x.$$
2. Privacy: *For every $T \notin \mathcal{A}$ and for every random variable X on $\{0,1\}^\ell$, the random variables X and* $\mathrm{Share}(X)_T$ *are statistically independent.*

The privacy condition can be stated in terms of Kolmogorov complexity.

Lemma 6.8 ([Hir22c, Lemma 6.9]). *Let* $(\mathrm{Share}, \mathrm{Rec})$ *be a secret sharing scheme for an access structure $\mathcal{A}$ over $[n]$. Then, for every ℓ and $k \in \mathbb{N}$, it holds that*

$$\Pr\left[\min_{T \notin \mathcal{A}} \mathrm{K}(X \mid \mathrm{Share}(X)_T) \geq \ell - n - k\right] \geq 1 - 2^{-k},$$

where X is the uniform distribution over $\{0,1\}^\ell$ and the probability is taken over X as well as the internal randomness of Share*.*

The "efficiency" of a secret sharing scheme is defined as follows.

Definition 6.9. *A family $\mathcal{A} = \{\mathcal{A}_\varphi\}_{\varphi \in \{0,1\}^*}$ of access structures is said to* admit efficient secret sharing schemes *if there exists a pair* $(\mathrm{Share}, \mathrm{Rec})$ *of a randomized polynomial-time algorithm* Share *and a deterministic polynomial-time algorithm* Rec *such that for every $\varphi \in \{0,1\}^*$, the pair* $(\mathrm{Share}(\varphi, \text{-}), \mathrm{Rec}(\varphi, \text{-}))$ *is a secret sharing scheme for the access structure $\mathcal{A}_\varphi$.*

Benaloh and Leichter [BL88] showed that access structures represented by monotone formulas admit efficient secret sharing schemes.

Lemma 6.10 ([BL88]). *Let $\mathcal{A} := \{\mathcal{A}_\varphi\}_{\varphi \in \{0,1\}^*}$ be the family of access structures $\mathcal{A}_\varphi := \{T \subseteq [n] \mid \varphi(\chi_T) = 1\}$, where φ is a monotone formula on n variables and $\chi_T \in \{0,1\}^n$ denotes the characteristic vector of $T \subseteq [n]$. Then, $\mathcal{A}$ admits efficient secret sharing schemes.*

6.3 A Proof of NP-Hardness of Distributional Kolmogorov Complexity

Let $A \in \mathsf{P/poly}$ be an oracle and τ be a polynomial. Using Lemma 5.7, let

$$G = \left\{G_n : \{0,1\}^{n^\epsilon} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$$

be a pseudorandom generator secure against polynomial-size circuits, where $\epsilon > 0$ is a parameter chosen later.

It suffices to present a randomized polynomial-time reduction R from MMSA to GapMdKP. Let (φ, s) be an instance of MMSA, where φ is a monotone formula on n variables. Let $(\mathrm{Share}, \mathrm{Rec})$ be the secret sharing scheme of Lemma 6.10.

The reduction first chooses $x \sim \{0,1\}^\ell$ uniformly at random. Then, x is shared to n parties. Let $(s_1, \cdots, s_n) := \mathrm{Share}(\varphi, x)$, where s_i is the share given to the i-th party. Let m be the length of each share. By the efficiency of the secret sharing scheme, there exists a constant $\epsilon^{-1} \in \mathbb{N}$ such that $m \leq (\ell \cdot |\varphi|)^{1/2\epsilon}$. The reduction also chooses $f_1, \ldots, f_n \sim \{0,1\}^\lambda$ uniformly at random.

We now describe the construction of a distribution $\mathcal{D}$. Define $k := m^\epsilon$. Let $\mathrm{GL}_k \colon \{0,1\}^\lambda \times (\{0,1\}^\lambda)^k \to \{0,1\}^k$ be the Goldreich–Levin hard-core function, i.e.,

$$\mathrm{GL}_k(x; (z^1, \cdots, z^k)) := \langle x, z^1\rangle \cdots \langle x, z^k\rangle,$$

where $\langle x, z^i\rangle$ denotes the inner product between x and z^i over $\mathrm{GF}(2)$. To sample a string y from the distribution $\mathcal{D}$, pick uniformly random strings $z_1, \ldots, z_n \sim \{0,1\}^{\lambda k}$ and define

$$y := (z_1, \cdots, z_n, G_m(\mathrm{GL}_k(f_1; z_1)) \oplus s_1, \cdots, G_m(\mathrm{GL}_k(f_n; z_n)) \oplus s_n).$$

This completes the definition of $\mathcal{D}$.

Define $\lambda := n^4 \cdot |\varphi|$, and $\ell := n^6 \cdot |\varphi|$. It is easy to verify that $nk = o(\lambda)$ and $n\lambda = o(\ell)$. Let $\ell' := |x| + |y|$.

We prove the completeness of the reduction.

Claim 6.11. *Assume that there exists a satisfying assignment for φ of weight θ. Then,*

$$\mathrm{dK}^t_1(x \mid \mathcal{D}) \leq 2\theta\lambda,$$

where t is some universal polynomial.

Proof. Let $T \subseteq [n]$ be a set whose characteristic function is a satisfying assignment for φ of weight θ. Let M be a program that takes $\{f_i \mid i \in T\}$ and φ as hard-wired input, takes $y = (z_1, \cdots, z_n, \xi_1, \cdots, \xi_n)$ as input, computes $s_i := \xi_i \oplus G_m(\mathrm{GL}_k(f_i; z_i))$ for every $i \in T$, and outputs $\mathrm{Rec}(\varphi, T, s_T)$. By the correctness of the secret sharing scheme, this program outputs x for every y in the support of $\mathcal{D}$. The size of the program is at most

$$\sum_{i\in T} |f_i| + O(|T| + |\varphi|) \leq \theta\lambda + O(|\varphi|) \leq 2\theta\lambda.$$

◇

To prove the soundness of the reduction, we clarify the condition under which the reduction is successful.

Claim 6.12. *With probability $1-o(1)$ over the internal randomness of the reduction R, it holds that*

$$\mathrm{K}(f_B \mid x, s_{[n]}) \geq \lambda \cdot |B| - 2n$$

for every $B \subseteq [n]$ and

$$\mathrm{K}(x \mid s_T, f_T) \geq \ell - 2n$$

for every $T \notin \mathcal{A}_\varphi$.

Proof. The second item follows from Lemma 6.8. To see the first item, fix any $B \subseteq [n]$. Since $f_{[n]}$ is chosen independently of x and $s_{[n]}$, we obtain

$$\mathrm{K}(f_B \mid x) \geq \lambda \cdot |B| - 2n$$

with probability at least $1 - 2^{-2n}$ over a random choice of f_B. Taking a union bound over all $B \subseteq [n]$, with probability at least $1 - 2^{-n}$, for every B, it holds that $\mathrm{K}(f_B \mid x) \geq \lambda \cdot |B| - 2n$. ◇

Claim 6.13. *Assume* $\mathrm{MMSA}(\varphi) > 2\theta$ *and the event of Claim 6.12 holds. Then,*

$$\mathrm{dK}^{\tau,A}_{1/\tau(\ell')}(x \mid \mathcal{D}) \geq \theta\lambda.$$

To prove this claim, we use the algorithmic information extraction lemma from [Hir22b].

Lemma 6.14 ([Hir22b, Lemma 6.1])**.** *Let $r, k, \epsilon^{-1} \in \mathbb{N}$, $f_1, \cdots, f_n \in \{0,1\}^\lambda$, and $D\colon \{0,1\}^r \times \left(\{0,1\}^{\lambda k}\right)^n \times \left(\{0,1\}^k\right)^n \to \{0,1\}$ be a function. Then, there exists a set $B \subseteq [n]$ such that*

$$\mathrm{K}^D(f_B) \leq |B| \cdot (nk + O(\log(n\lambda kr/\epsilon)))$$

and

$$\left|\Pr[D(R, Z_1, \cdots, Z_n, X_1, \cdots, X_n) = 1] - \Pr\left[D(R, Z_1, \cdots, Z_n, X'_1, \cdots, X'_n) = 1\right]\right| \leq \epsilon.$$

Here, $R \sim \{0,1\}^r$, $Z_i \sim \{0,1\}^{\lambda k}$, $X_i := \mathrm{GL}_k(f_i; Z_i)$, and X'_i is identical to X_i if $i \in B$ and to the uniform distribution if $i \in [n] \setminus B$.

Proof of Claim 6.13. Let M^A be an arbitrary A-oracle $\tau(\ell')$-time program of size $\theta\lambda$. Our goal is to prove

$$\delta := \Pr_{y \sim \mathcal{D}}\left[M^A(y) = x\right] \leq \frac{1}{\tau(\ell')}.$$

Let D be the Boolean function (that depends on M) such that

$$D(z_1, \cdots, z_n, \eta_1, \cdots, \eta_n) = 1$$

if and only if $M(z_1, \cdots, z_n, G_m(\eta_1) \oplus s_1, \cdots, G_m(\eta_n) \oplus s_n)$ outputs x in time $\tau(\ell')$. Let $\epsilon := 1/2\tau(\ell')$. By Lemma 6.14, there exists a set $B \subseteq [n]$ such that

$$\mathrm{K}^D(f_B) \leq |B| \cdot 2nk$$

and

$$\left|\Pr[D(Z_1, \cdots, Z_n, X_1, \cdots, X_n) = 1] - \Pr\left[D(Z_1, \cdots, Z_n, X'_1, \cdots, X'_n) = 1\right]\right| \leq \epsilon,$$

where Z_i, X_i, and X'_i are the random variables defined in Lemma 6.14.

We give an upper bound of the size of B. Since D can be simulated by using M, $s_{[n]}$, and x, we have

$$\mathrm{K}(f_B \mid x, s_{[n]}) - |M| - O(1) \leq \mathrm{K}(f_B \mid M, x, s_{[n]}) \leq \mathrm{K}^D(f_B) + O(1) \leq |B| \cdot 2nk.$$

Thus, we obtain

$$\lambda|B| \leq \mathrm{K}(f_B \mid x, s_{[n]}) + 2n \leq |M| + O(|B| \cdot nk)$$

and therefore

$$|B| \cdot \lambda(1 - o(1)) \leq |B| \cdot (\lambda - O(nk)) \leq |M| \leq \theta\lambda.$$

We conclude that

$$|B| \leq 2\theta.$$

By assumption, this implies that B is not authorized.

Since $X_i = \mathrm{GL}_k(f_i; Z_i)$, we have

$$\Pr[D(Z_1, \cdots, Z_n, X_1, \cdots, X_n) = 1] = \Pr_{y \sim \mathcal{D}}\big[M^A(y) = x\big].$$

On the other hand,

$$\Pr\big[D(Z_1, \cdots, Z_n, X'_1, \cdots, X'_n) = 1\big] = \Pr\big[M^A(Z_1, \cdots, Z_n, G_m(X'_1) \oplus s_1, \cdots, G_m(X'_n) \oplus s_n) = x\big].$$

For every $i \in [n] \setminus B$, X'_i is identical to the uniform distribution; thus, using the security of the pseudorandom generator G_m and a hybrid argument, $G_m(X'_i) \oplus s_i$ is indistinguishable from the uniform distribution Y_i by M^A. It follows that

$$\Big|\Pr\big[M^A(y) = x\big] - \Pr\Big[M^A(Z_{[n]}, Y'_{[n]}) = x\Big]\Big| \leq \epsilon + \frac{1}{m^{\omega(1)}},$$

where Y'_i is identical to the uniform distribution Y_i if $i \in [n] \setminus B$ and is identical to $G_m(\mathrm{GL}_k(f_i; Z_i)) \oplus s_i$ if $i \in B$. Since $Y'_{[n]}$ can be computed from s_B and f_B, the secret x can be described by M^A, s_B and f_B with probability at least $\delta' = \delta - \epsilon - \frac{1}{m^{\omega(1)}}$. Therefore, we obtain

$$\mathrm{K}(x \mid s_B, f_B) \leq |M| + O(\log(1/\delta')) \leq \theta\lambda + O(\log \ell').$$

Since B is not authorized, using Claim 6.12, we have

$$\ell - 2n \leq \mathrm{K}(x \mid s_B, f_B).$$

Combining these inequalities, we conclude that

$$\ell \leq \theta\lambda + O(n) \leq O(n\lambda).$$

This is a contradiction to the choice of ℓ. ◇

We note that the inapproximability factor can be improved by using computational secret sharing schemes. We omit the details in this version.

7 Pseudorandom Generator Constructions

We use two pseudorandom generator constructions. The first one is due to Raz, Reingold, and Vadhan [RRV02], which has small advice complexity with respect to randomized algorithms.

Lemma 7.1 (see the proof of [Hir20a, Theorem 4.7] and [Hir22c])**.** *For all sufficiently large $n, m \in \mathbb{N}$ such that $m \leq 2n$ and for any $\delta \in (0,1)$,*[19] *there exists a family of functions*

$$G_m \colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m,$$

such that for every $x \in \{0,1\}^n$ and every distribution $\mathcal{D}$ over functions $D \colon \{0,1\}^m \to \{0,1\}$ such that

$$\Pr_{\substack{z \sim \{0,1\}^d \\ D \sim \mathcal{D}}}[D(G_m(x;z)) = 1] - \Pr_{\substack{w \sim \{0,1\}^m \\ D \sim \mathcal{D}}}[D(w) = 1] \geq \delta,$$

it holds that

$$\mathrm{drK}^{\mathsf{poly}(n),\mathcal{D}}_{\delta/2m}(x) := \mathrm{dK}^{\mathsf{poly}(n),\mathcal{D}}_{\delta/2m}(x \mid \mathcal{U}_t) \leq m + O(\log^3 n).$$

Here, $d = O(\log^3 n)$ and $\mathcal{U}_t$ denotes the uniform distribution over $\{0,1\}^t$. Moreover, if $\mathcal{D}$ is a randomized oracle, then it holds that

$$\mathrm{rK}^{\mathsf{poly}(n),\mathcal{D}}_{3/4}(x) \leq m + O(\log^3 n).$$

We note that the parameter $\delta/2m$ in $\mathrm{dK}^{\mathsf{poly}(n),\mathcal{D}}_{\delta/2m}(x)$ is significantly smaller than δ. This loss is due to the loss in the hybrid argument, and appears to be inherent for Nisan–Wigderson pseudorandom generator constructions [NW94].

7.1 A New Property of the Direct Product Generator

The second one is the k-wise direct product generator [Hir20c]. Although the seed length of this construction is large, we prove that the construction has a special property that the loss of the parameter λ of $\mathrm{dK}^{\mathsf{poly}}_{\lambda}$ is small.

To state the result, we introduce the notion of distributional probabilistic Kolmogorov complexity, which generalizes probabilistic Kolmogorov complexity [GKLO22].

Definition 7.2. *For parameters $\lambda, \delta \in [0,1]$, for a string $x \in \{0,1\}^*$, a distribution $\mathcal{D}$, and a time bound $t \in \mathbb{N}$, the* t-time-bounded distributional probabilistic Kolmogorov *of x given $\mathcal{D}$ is defined to be*

$$\mathrm{dpK}^t_{\lambda,\delta}(x \mid \mathcal{D}) = \min\left\{ k \in \mathbb{N} \;\middle|\; \Pr_{r \sim \{0,1\}^t}\left[\mathrm{dK}^t_{\lambda}(x \mid \mathcal{D}, r) \leq k\right] \geq \delta \right\}.$$

We omit the subscript δ if $\delta = \frac{3}{4}$.

It is easy to amplify the parameter δ.

Fact 7.3. *There exists a polynomial p such that for every $\delta \in (0,1]$,*

$$\mathrm{dpK}^{p(t/\delta)}_{\lambda}(x \mid \mathcal{D}) \leq \mathrm{dpK}^t_{\lambda,\delta}(x \mid \mathcal{D}) + O(\log(1/\delta)).$$

[19] Note that Lemma 7.1 is interesting only if $m \ll 2n$.

Proof. Let $k := \mathrm{dpK}^t_{\lambda,\delta}(x \mid \mathcal{D})$. With probability at least δ over a coin flip sequence $r \sim \{0,1\}^t$, it holds that $\mathrm{dK}^t(x \mid \mathcal{D}, r) \leq k$. By picking $m = O(1/\delta)$ coin flip sequences $r_1, \cdots, r_m \sim \{0,1\}^t$ independently, with probability at least $\frac{3}{4}$, there exists $i \in [m]$ such that $\mathrm{dK}^t(x \mid \mathcal{D}, r_i) \leq k$. Under this event, there exists a program M of length k that prints x given (y, r_i) as input with probability λ over a choice of $y \sim \mathcal{D}$. Consider a program M' that takes M and i as hard-wired input, $(y, (r_1, \cdots, r_m))$ as input, and simulates M on input (y, r_i). Then, the size of M' is at most $k + O(\log m) = k + O(\log(1/\delta))$ and M' runs in time $p(t/\delta)$ for some polynomial p. Thus, we obtain

$$\mathrm{dpK}^{p(t/\delta)}_{\lambda}(x \mid \mathcal{D}) \leq k + O(\log(1/\delta)).$$

□

Definition 7.4 (k-wise direct product generator [Hir20c; Hir21])**.** *For every $n, k \in \mathbb{N}$, we define the k-wise direct product generator to be a function*

$$\mathrm{DP}_k \colon \{0,1\}^n \times \{0,1\}^{nk} \to \{0,1\}^{nk+k}$$

such that

$$\mathrm{DP}_k(x; z^1, \cdots, z^k) := (z^1, \cdots, z^k, \langle x, z^1\rangle, \cdots, \langle x, z^k\rangle).$$

We also define the Goldreich–Levin hard-core function

$$\mathrm{GL}_k(x; z^1, \cdots, z^k) := \langle x, z^1\rangle, \cdots, \langle x, z^k\rangle.$$

Goldreich and Levin [GL89] showed that the Hadamard code is locally list-decodable.

Lemma 7.5. *There exists a deterministic oracle algorithm M such that for every $n \in \mathbb{N}$, every $x \in \{0,1\}^n$, and every function $f \colon \{0,1\}^n \to \{0,1\}$ such that*

$$\Pr_{z \sim \{0,1\}^n}[f(z) = \langle x, z\rangle] \geq \frac{1}{2} + \epsilon,$$

on input $(\mathrm{DP}_k(x; z), n)$, the algorithm M^f outputs x in time $\mathsf{poly}(n/\epsilon\delta)$ with probability at least $1 - \delta$ over a random choice of $z = (z^1, \cdots, z^k) \sim (\{0,1\}^n)^k$, where $k = O(\log(n/\epsilon\delta))$.

Proof. Fix any $j \in [n]$. Let $\alpha^i := \langle x, z^i\rangle$ be the advice bit for each $i \in [k]$. The j-th bit of the output of the algorithm M^f is defined to be the majority, over all nonempty subsets $T \subseteq [k]$, of $f(z^T \oplus e^j) \oplus \alpha^T$, where $z^T := \sum_{i \in T} z^i$, $\alpha^T := \sum_{i \in T} \alpha^i = \langle x, z^T\rangle$, and $e^j \in \{0,1\}^n$ is the binary string whose j-th entry is 1 and other entries are 0.

Let $K := 2^k - 1$. We assume that $K \geq n/(\epsilon^2\delta)$. For any nonempty subset $T \subseteq [k]$, let y_T be the random variable that takes 1 if $f(z^T \oplus e^j) = \langle x, z^T \oplus e^j\rangle$ and 0 otherwise. Observe that

$$\mathbb{E}[y_T] = \Pr_z[f(z) = \langle x, z\rangle] \geq \frac{1}{2} + \epsilon.$$

Since $\{z^T\}_{\emptyset \subsetneq T \subseteq [k]}$ is pairwise independent, by Chebyshev's inequality, we have $\sum_{T \neq \emptyset} y_T \leq K/2$ with probability at most $1/(K\epsilon^2) \leq \delta/n$. Note that if $y_T = 1$, then $f(z^T \oplus e^j) \oplus \alpha^T = \langle x, z^T \oplus e^j\rangle \oplus \langle x, z^T\rangle = \langle x, e^j\rangle = x_j$, where x_j denotes the j-th bit of x. Under the assumption that $\sum_{T \neq \emptyset} y_T > K/2$, we get that the majority is x_j. □

Theorem 7.6. *For any parameters $n, k \in \mathbb{N}$, and $\epsilon, \delta > 0$ with $k \leq 2n$, there exists a randomized oracle algorithm $R^{(\cdot)}$ satisfying the following: For any string $x \in \{0,1\}^n$ and any distribution $\mathcal{D}$ over functions such that*

$$\Pr_{\substack{z \sim \{0,1\}^{nk} \\ D \sim \mathcal{D}}}[D(\mathrm{DP}_k(x;z)) = 1] - \Pr_{\substack{w \sim \{0,1\}^{nk+k} \\ D \sim \mathcal{D}}}[D(w) = 1] \geq \epsilon,$$

it holds that

$$\Pr_{D \sim \mathcal{D}, z, R}\left[R^D(\mathrm{DP}_{k+\ell}(x;z), n, k) = x\right] \geq \epsilon - \delta$$

for some $\ell = O(\log(n/\delta))$, where R^D runs in time $\mathsf{poly}(n/\delta)$. In particular,

$$\mathrm{dpK}^{\mathsf{poly}(n/\delta), \mathcal{D}}_{\epsilon-\delta}(x) \leq k + O(\log(n/\delta)).$$

Proof. We use a standard hybrid argument (as in [NW94; Vad12]). Fix any string $x \in \{0,1\}^n$. By an averaging argument, with probability at least $\epsilon - \delta$ over a choice of $D \sim \mathcal{D}$, it holds that

$$\Pr_{\bar{z}}[D(z^1, \ldots, z^k, \langle x, z^1\rangle, \ldots, \langle x, z^k\rangle) = 1] - \Pr_{\bar{z}, b}[D(z^1, \ldots, z^k, b_1, \ldots, b_k) = 1] \geq \delta,$$

where $\bar{z} = (z^1, \ldots, z^k) \sim (\{0,1\}^n)^k$ and $b \sim \{0,1\}^k$. For every $i \in \{0, \ldots, k\}$, define the i-th hybrid distribution H_i as the distribution of

$$(z^1, \ldots, z^k, \langle x, z^1\rangle, \ldots, \langle x, z^i\rangle, b_{i+1}, \ldots, b_k),$$

where $\bar{z} = (z^1, \ldots, z^k) \sim (\{0,1\}^n)^k$ and $b_{i+1}, \ldots, b_k \sim \{0,1\}$. By this definition, H_0 is identically distributed with the uniform distribution, and H_k is a distribution identical to $\mathrm{DP}_k(x;\bar{z})$. Thus, there exists $i \in [k]$ such that

$$\Pr_{\bar{z}, b}[D(H_i) = 1] - \Pr_{\bar{z}, b}[D(H_{i-1}) = 1] \geq \frac{\delta}{k}. \tag{5}$$

By a standard calculation (see, e.g., [Vad12, Proposition 7.16]), we prove the following claim.

Claim 7.7. *There exists $i \in [k]$ such that*

$$\Pr_{\bar{z}, b}[D(H_{i-1}) \oplus 1 \oplus b_i = \langle x, z^i\rangle] \geq \frac{1}{2} + \frac{\delta}{k}.$$

Proof. If we pick $b_i \sim \{0,1\}$ randomly, there are two cases: (1) $b_i = \langle x, z^i\rangle$ or (2) $b_i \neq \langle x, z^i\rangle$, each of which happens with probability $\frac{1}{2}$. In particular, we have

$$\Pr[D(H_{i-1}) = 1] = \frac{1}{2} \cdot \Pr[D(H_i) = 1] + \frac{1}{2} \cdot \Pr\left[D(H'_i) = 1\right],$$

where $H'_i := (z^1, \cdots, z^k, \langle x, z^1\rangle, \cdots, \langle x, z^{i-1}\rangle, \langle x, z^i\rangle \oplus 1, b_{i+1}, \cdots, b_k)$. By Eq. (5), we obtain that

$$\frac{\delta}{k} \leq \frac{1}{2} \cdot \Pr[D(H_i) = 1] - \frac{1}{2} \cdot \Pr\left[D(H'_i) = 1\right].$$

Therefore, we conclude that

$$\begin{aligned}
&\Pr_{\bar{z},b}[D(H_{i-1}) \oplus 1 \oplus b_i = \langle x, z^i \rangle] \\
&= \frac{1}{2} \cdot \Pr[D(H_i) = 1] + \frac{1}{2} \cdot \Pr\big[D(H'_i) = 0\big] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \Pr[D(H_i) = 1] - \frac{1}{2} \cdot \Pr\big[D(H'_i) = 1\big] \\
&\geq \frac{1}{2} + \frac{\delta}{k}.
\end{aligned}$$

◇

Let M be the list-decoding algorithm of Lemma 7.5. For each $i \in [k]$ (and $z^1, \ldots, z^{i-1}, z^{i+1}, \ldots, z^k \sim \{0,1\}^n$, $b \sim \{0,1\}^k$), define a function $f_i \colon \{0,1\}^n \to \{0,1\}$ as

$$f_i(z^i) := D(H_{i-1}) \oplus 1 \oplus b_i = D(z^1, \cdots, z^k, \langle x, z^1 \rangle, \cdots, \langle x, z^{i-1} \rangle, b_i, \cdots, b_k) \oplus 1 \oplus b_i$$

for every $z^i \in \{0,1\}^n$. Under the event of Claim 7.7,

$$\Pr_{z'}\Big[M^{f_i}(\mathrm{DP}_{\ell_0}(x; z'), n) = x\Big] \geq 1 - \delta$$

for some $\ell_0 = O(\log(n/\delta))$. Let $\bar{f} := (f_1, \cdots, f_k)$. Consider an algorithm $R_0^{\bar{f}}$ that takes $\mathrm{DP}_{\ell_0}(x; z')$ and $\mathrm{DP}_{\ell_1}(x; z'')$ as input, finds $i \in [k]$ such that $\mathrm{GL}_{\ell_1}(x; z'') = \mathrm{GL}_{\ell_1}(x^i; z'')$, where $x^i := M^{f_i}(\mathrm{DP}_{\ell_0}(x; z''), n)$, and outputs x^i. Since $\mathrm{GL}_{\ell_1}(x; z'')$ serves as a hash function, for $\ell_1 = O(\log(k/\delta))$, with probability at least $1 - \delta$ over $z'' \sim \{0,1\}^{n\ell_1}$, the algorithm R_0 outputs x. Thus, we obtain

$$\Pr_{z', z''}\Big[R_0^{\bar{f}}(\mathrm{DP}_{\ell_0}(x; z'), \mathrm{DP}_{\ell_1}(x; z'')) = x\Big] \geq 1 - 2\delta.$$

Since $\bar{f}$ can be simulated by using $\mathrm{DP}_k(x; z)$, combining these algorithms, we obtain an oracle algorithm R^D that takes $\mathrm{DP}_{k+\ell_0+\ell_1}(x; z)$ as input and prints x. More specifically, since the event of Claim 7.7 holds with probability at least $\epsilon - \delta$ over a choice of $D \sim \mathcal{D}$, we obtain

$$\Pr_{z, D, R}\big[R^D(\mathrm{DP}_{k+\ell_0+\ell_1}(x; z)) = x\big] \geq \epsilon - 3\delta.$$

To see the "In particular" part, by an averaging argument, we also have

$$\Pr_{D \sim \mathcal{D}}\big[R^D(\mathrm{DP}_{k+\ell_0+\ell_1}(x; z)) = x\big] \geq \epsilon - 4\delta$$

with probability at least δ over a choice of z and the internal randomness of R. Under this event, there exists a program (depending on z and the internal randomness of R) that takes $\mathrm{GL}_{k+\ell_0+\ell_1}(x; z)$ as hard-wired input and outputs x given a random oracle $D \sim \mathcal{D}$. The success probability δ can be amplified by Fact 7.3. □

7.2 An Extension of Symmetry of Information

Using the new property of a k-wise direct product generator, we prove "symmetry of information" for $\mathrm{dK}^{\mathsf{poly}}$.

Theorem 7.8. *If* $\mathsf{DistNP} \subseteq \mathsf{AvgP}$*, then there exists a polynomial* τ *such that for every* $x \in \{0,1\}^*$*, every distribution* $\mathcal{D}$ *over* $\{0,1\}^m$*, every* $\lambda \in [0,1]$*, every* $\epsilon^{-1} \in \mathbb{N}$*, and every* $t \geq |x| + m + \epsilon^{-1}$*, it holds that*

$$\mathrm{dK}^{\tau(t)}_{\lambda-\epsilon}(x \mid \mathcal{D}) \leq \min\left\{ s \in \mathbb{N} \;\middle|\; \Pr_{y\sim\mathcal{D}}\left[\mathrm{K}^t(x,y) - \mathrm{K}^{\tau(t)}(y) \leq s\right] \geq \lambda \right\} + \log \tau(t).$$

We first present an algorithmic proof of symmetry of information. Under the assumption that $\mathsf{DistNP} \subseteq \mathsf{AvgP}$, symmetry of information for time-bounded Kolmogorov complexity was proved in [Hir22c]. Here, following [Hir20b], we prove that a "non-disjoint" promise problem can be solved by a meta-computational view of the proof of [Hir22c].

Lemma 7.9 (implicit in [Hir22c])**.** *If* $\mathsf{DistNP} \subseteq \mathsf{AvgP}$*, then* $\mathrm{Gap}_\tau\mathrm{MINcKT} \in \mathsf{P}$ *for some polynomial* τ*. Here, the promise problem* $\mathrm{Gap}_\tau\mathrm{MINcKT} := (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ *is defined as*

$$\Pi_{\mathrm{YES}} := \left\{ (x, y, 1^t, 1^s) \;\middle|\; t \geq |x| + |y| \text{ and } \mathrm{K}^t(x,y) - \mathrm{K}^{\tau(t)}(y) \leq s \right\},$$
$$\Pi_{\mathrm{NO}} := \left\{ (x, y, 1^t, 1^s) \;\middle|\; t \geq |x| + |y| \text{ and } \mathrm{K}^{\tau(t)}(x \mid y) > s + \log \tau(t) \right\}.$$

Observe that the disjointness of $\mathrm{Gap}_\tau\mathrm{MINcKT}$ implies symmetry of information for time-bounded Kolmogorov complexity.

Proof of Lemma 7.9. Using the assumption that $\mathsf{DistNP} \subseteq \mathsf{AvgP}$, by [Hir18; Hir20b], there exist a polynomial-time algorithm $\widetilde{\mathrm{K}}$ and a polynomial τ such that for every $x \in \{0,1\}^*$ and every $t \geq |x|$,

$$\mathrm{K}^{\tau(t)}(x) - \log \tau(t) \leq \widetilde{\mathrm{K}}(x; 1^t) \leq \mathrm{K}^t(x). \tag{6}$$

Let $(x, y, 1^t, 1^s)$ be an input such that $t \geq |x| + |y|$. Let $n := |x|$ and $m := |y|$. Let $k\,(\approx s)$ be a parameter chosen later. By Fact 5.5, we have

$$\mathrm{K}(w, w') \geq |w| + |w'| - \log \tau(t)$$

with probability at least $1 - o(1)$ over a random choice of $w \sim \{0,1\}^{nk+k}$ and $w' \sim \{0,1\}^{m\ell+\ell}$. Since $\widetilde{\mathrm{K}}(w, w'; 1^{t'}) \geq \mathrm{K}(w, w') - \log \tau(t')$, we obtain

$$\Pr_{w,w'}\left[\widetilde{\mathrm{K}}(w, w'; 1^{t'}) \geq |w| + |w'| - 2\log \tau(t')\right] \geq 1 - o(1) \geq \frac{1}{2}, \tag{7}$$

where $t' = \mathsf{poly}(t)$ is a sufficiently large polynomial. Define $\theta_{k,\ell} := |w| + |w'| - 2\log \tau(t') = nk + k + m\ell + \ell - 2\log \tau(t')$.

Next, we define ℓ to be the maximum integer $\ell \in \mathbb{N}$ such that

$$\Pr\left[\widetilde{\mathrm{K}}(w, \mathrm{DP}_\ell(y; z'); 1^{t'}) \geq \theta_{k,\ell}\right] \geq \frac{1}{4}. \tag{8}$$

We claim that ℓ is well defined. Eq. (8) is satisfied for $\ell = 0$ by Eq. (7), and is not satisfied for some $\ell_\infty = m + O(\log t)$ because

$$\begin{aligned}\widetilde{\mathrm{K}}(w, \mathrm{DP}_{\ell_\infty}(y; z'); 1^{t'}) &\leq \mathrm{K}^{t'}(w, \mathrm{DP}_{\ell_\infty}(y; z')) \\ &\leq |w| + |z'| + m + O(\log \ell_\infty). \\ &< |w| + |z'| + \ell_\infty - 2\log \tau(t) = \theta_{k,\ell_\infty},\end{aligned}$$

where the second inequality holds because $(w, \mathrm{DP}_{\ell_\infty}(y; z'))$ can be efficiently computed from w, z', $y \in \{0,1\}^m$, and $\ell_\infty \in \mathbb{N}$.

Since $\ell + 1$ does not satisfy Eq. (8), the negation of Eq. (8) and Eq. (7) indicate that $\mathrm{DP}_{\ell+1}(y; \text{-})$ can be distinguished from the uniform distribution by a circuit D that takes w' and a coin flip sequence w as input and outputs 1 if and only if $\widetilde{\mathrm{K}}(w, w'; 1^{t'}) \geq \theta_{k,\ell}$. It follows from the reconstruction property of $\mathrm{DP}_{\ell+1}$ [Hir21, Theorem 3.2] that

$$\mathrm{K}^{p(t')}(y) \leq \ell + 1 + O(\log t)$$

for some polynomial p.

We now describe a randomized polynomial-time algorithm M that decides the promise problem $\mathrm{Gap}_{\tau'}\mathrm{MINcKT}$ for some polynomial τ'. On input $(x, y, 1^t, 1^s)$, M computes ℓ, picks $z \sim \{0,1\}^{nk}$ and $z' \sim \{0,1\}^{m\ell}$ randomly, and outputs 1 if and only if

$$\widetilde{\mathrm{K}}(\mathrm{DP}_k(x; z), \mathrm{DP}_\ell(y; z'); 1^{t'}) < \theta_{k,\ell}.$$

Consider the case in which the input is a YES instance, i.e., $\mathrm{K}^t(x, y) - \mathrm{K}^{\tau'(t)}(y) \leq s$. Since $(\mathrm{DP}_k(x; z), \mathrm{DP}_\ell(y; z'))$ can be computed from a description for (x, y) and z and z', we obtain

$$\begin{aligned}\widetilde{\mathrm{K}}(\mathrm{DP}_k(x; z), \mathrm{DP}_\ell(y; z'); 1^{t'}) &\leq \mathrm{K}^{t'}(\mathrm{DP}_k(x; z), \mathrm{DP}_\ell(y; z')) \\ &\leq \mathrm{K}^t(x, y) + |z| + |z'| + O(\log t), \\ &\leq s + \mathrm{K}^{\tau'(t)}(y) + |z| + |z'| + O(\log t) \\ &< k + \ell + |z| + |z'| - 2\log \tau(t') = \theta_{k,\ell}\end{aligned}$$

where the last inequality holds by choosing $k := s + O(\log t)$ and $\tau'(t) \geq p(t')$. Thus, M accepts with probability 1.

Conversely, assume that M accepts with probability at least $\frac{7}{8}$. We claim that the input is not a NO instance. Under assumption, we have

$$\Pr_{z,z'}\left[\widetilde{\mathrm{K}}(\mathrm{DP}_k(x; z), \mathrm{DP}_\ell(y; z'); 1^{t'}) \geq \theta_{k,\ell}\right] \leq \frac{1}{8}.$$

Combining this inequality with Eq. (8), we observe that $\mathrm{DP}_k(x; \text{-})$ can be distinguished from the uniform distribution by a circuit D_y that takes w and a coin flip sequence z' and outputs 1 if and only if $\widetilde{\mathrm{K}}(w, \mathrm{DP}_\ell(y; z'); 1^{t'}) \geq \theta_{k,\ell}$. Thus, by the reconstruction property of DP_k, we obtain

$$\mathrm{K}^{\mathsf{poly}(t), D_y}(x) \leq k + O(\log t).$$

Since D_y can be computed from y and $O(\log t)$ bits of information, we conclude that

$$\mathrm{K}^{\tau'(t)}(x \mid y) \leq \mathrm{K}^{\mathsf{poly}(t), D_y}(x) + O(\log t) \leq k + \log \tau'(t)$$

for a sufficiently large polynomial τ'. This means that the input is not a No instance. Taking the contrapositive, any No instance is rejected by M with probability at least $\frac{1}{8}$.

Finally, since pr-P = pr-BPP under the assumption that $\mathsf{DistNP} \subseteq \mathsf{AvgP}$ [BFP05], the randomized algorithm M can be derandomized, which completes the proof. □

Proof of Theorem 7.8. Let M be the polynomial-time algorithm that decides $\mathrm{Gap}_\tau\mathrm{MINcKT}$ for some polynomial τ. Let $s \in \mathbb{N}$ be an integer such that

$$\Pr_{y\sim\mathcal{D}}\left[\mathrm{K}^t(x,y) - \mathrm{K}^{\tau'(t)}(y) \le s\right] \ge \lambda,$$

where τ' is a sufficiently large polynomial chosen later.

We claim that

$$\Pr_{z,y}\left[M(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'+nk}) = 1\right] - \Pr_{w,y}\left[M(w, y, 1^{t'}, 1^{s'+nk}) = 1\right] \ge \lambda - \epsilon, \tag{9}$$

where k, t' and s' are parameters chosen later and $z \sim \{0,1\}^{nk}$, $w \sim \{0,1\}^{nk+k}$, and $y \sim \mathcal{D}$.

By the definition of s, with probability at least λ over a choice of $y \sim \mathcal{D}$, it holds that

$$\mathrm{K}^t(x,y) - \mathrm{K}^{\tau'(t)}(y) \le s$$

Under this event, since $\mathrm{DP}_k(x;z)$ can be computed from x, z, and k in time $t' = \mathsf{poly}(t)$,

$$\mathrm{K}^{t'}(\mathrm{DP}_k(x;z), y) - \mathrm{K}^{\tau(t')}(y) \le \mathrm{K}^t(x,y) + |z| + O(\log n) - \mathrm{K}^{\tau(t')}(y) \le s + |z| + O(\log n),$$

where the last inequality holds for any sufficiently large $\tau'(t) \ge \tau(t')$. By defining $s' := s + O(\log n)$, this shows that $(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'+nk})$ is a Yes instance of $\mathrm{Gap}_\tau\mathrm{MINcKT}$. Thus, we obtain

$$\Pr_{z,y}\left[M(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'+nk}) = 1\right] \ge \lambda.$$

By Fact 5.5, with probability at least $1-\epsilon$ over a choice of $w \sim \{0,1\}^{nk+k}$ and $y \sim \mathcal{D}$, it holds that

$$\mathrm{K}(w \mid y) \ge nk + k - O(\log(1/\epsilon)).$$

Under this event, we have

$$\mathrm{K}^{\tau(t)}(w \mid y) \ge nk + k - O(\log(1/\epsilon)) > nk + s' + \log\tau(t),$$

where the last inequality holds by defining $k := s' + O(\log t)$ and using that $t \ge \epsilon^{-1}$. This shows that $(w, y, 1^{t'}, 1^{s'+nk})$ is a No instance of $\mathrm{Gap}_\tau\mathrm{MINcKT}$. Thus, we obtain

$$\Pr_{w,y}\left[M(w, y, 1^{t'}, 1^{s'+nk}) = 1\right] \le \epsilon.$$

The two inequalities above complete the proof of Eq. (9). Define the function D_y such that $D_y(w) := M(w, y, 1^{t'}, 1^{s'+nk})$. By Theorem 7.6, we obtain

$$\Pr_{y\sim\mathcal{D},z',R}\left[R^{D_y}(\mathrm{DP}_{k+\ell}(x;z'), n, k) = x\right] \ge \lambda - 2\epsilon \tag{10}$$

for some $\ell = O(\log(n/\epsilon))$. By using the pseudorandom generator of logarithmic seed length secure against linear-sized circuits [BFP05], the randomness of R and z' can be replaced with a pseudorandom sequence whose time-bounded Kolmogorov complexity is logarithmic by reducing the success probability of Eq. (10) to $\lambda - 3\epsilon$. For a pseudorandom sequence z', consider a program R' that takes $\mathrm{GL}_{k+\ell}(x; z')$ as hard-wired input and simulates $R^{D_y}(\mathrm{DP}_{k+\ell}(x; z'), n, k)$. The program R' outputs x with probability at least $\lambda - 3\epsilon$ over a choice of $y \sim \mathcal{D}$ and is of length $k + \ell + O(\log t)$. Thus, we obtain

$$\mathrm{dK}^{\tau'(t)}_{\lambda-3\epsilon}(x \mid \mathcal{D}) \leq k + \ell + O(\log t) \leq s + O(\log t).$$

□

8 Input-Aware P/poly-Restricted Reduction

In this section, we present P/poly-restricted reductions to avoiding a hitting set generator.

8.1 Definitions and Basic Properties

Definition 8.1 ($\mathbb{B}$-restricted reductions)**.** *Let Π be a promise problem. Let $\mathbb{A}$ be the class of promise problems. Let $\mathbb{B}$ be the class of randomized oracles. For functions $\epsilon\colon \mathbb{N} \to (0,1)$ and $\delta\colon \mathbb{N} \to (0,1)$, a randomized nonadaptive oracle machine M is said to be a* $\mathbb{B}$-restricted reduction *from Π to $\mathbb{A}$ with parameters (ϵ, δ) if for every $B \in \mathbb{B}$ and for all but finitely many $x \in \mathrm{dom}(\Pi)$, for every $A \in \mathbb{A}$, if*

$$\Pr_{M,B}[A(q) = B(q) \text{ for every } q \in Q_M(x) \cap \mathrm{dom}(A)] \geq \epsilon(n),$$

then

$$\Pr_{M,B}\left[M^B(x) = \Pi(x)\right] \geq 1 - \frac{\delta(n)}{2},$$

where the probabilities are taken over the internal randomness of M. By default, we assume $\epsilon \equiv \frac{1}{2}$ and $\delta \equiv \frac{1}{2}$. If there exists a polynomial-time $\mathbb{B}$-restricted reduction from Π to $\mathbb{A}$, we denote it by $\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction \mathbb{B}$. If $\mathbb{A} = \{\Pi'\}$ for some promise problem Π' and $\mathbb{B} = \{B\}$ for some randomized oracle, then we simply write

$$\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \Pi' \restriction \mathbb{B} \quad \text{and} \quad \Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction B,$$

respectively.

For notational simplicity, we denote the hypothesis in Definition 8.1 by

$$\Pr_{M,B}\left[A\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)}\right] \geq \epsilon(n).$$

This notation can be justified by regarding a partial function $A\colon \{0,1\}^* \to \{0,1,*\}$ as a graph $\{(q, A(q)) \mid q \in \mathrm{dom}(A)\}$.

Proposition 8.2. *The following are equivalent for any polynomials p and q.*

1. $\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction \mathbb{B}$ *with parameters $\epsilon(n) = 1 - 1/p(n)$ and $\delta(n) = 1 - 1/p(n)$.*
2. $\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction \mathbb{B}$ *with parameters $\epsilon(n) = 2^{-q(n)}$ and $\delta(n) = 2^{-q(n)}$.*

Proof. Using $1 - 1/p(n) \geq 2^{-q(n)}$, it is easy to see that the second item implies the first item.

To see the converse, let M be a $\mathbb{B}$-restricted reduction from Π to $\mathbb{A}$. Let $k(n) := 2p(n)q(n)$. We define M' to be a randomized nonadaptive oracle machine that, given $x \in \mathrm{dom}(\Pi)$ as input, simulates M' on input x independently $k(|x|)$ times and outputs the majority vote of the outcome of M'.

We claim that M' is a reduction with exponentially small error parameters. Assume

$$\Pr_{M',B}\Big[A\restriction_{Q_{M'}(x)} \subseteq B\restriction_{Q_{M'}(x)}\Big] \geq 2^{-q(n)}.$$

By the definition of M', we have

$$\Pr_{M',B}\Big[A\restriction_{Q_{M'}(x)} \subseteq B\restriction_{Q_{M'}(x)}\Big] = \Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)}\Big]^{k(n)}.$$

Thus, we have

$$\Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)}\Big] \geq 2^{-q(n)/k(n)} \geq 1 - \frac{1}{p(n)}.$$

By the property of M, we obtain

$$\Pr_{M,B}\big[M^B(x) = \Pi(x)\big] \geq \frac{1}{2} + \frac{1}{2 \cdot p(n)}.$$

It follows from Hoeffding's inequality that

$$\Pr_{M',B}\big[M'^B(x) = \Pi(x)\big] \geq 1 - 2^{-q(n)}.$$

□

Equivalently, we may define the notion of $\mathbb{B}$-restricted reduction as follows.

Proposition 8.3. *For every constant $\delta \in (0, 1/2)$ the following are equivalent.*

1. $\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction \mathbb{B}$.
2. *There exists a randomized nonadaptive oracle machine M such that for every $B \in \mathbb{B}$ and for all sufficiently long $x \in \mathrm{dom}(\Pi)$, for every $A \in \mathbb{A}$, it holds that*

$$\Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)} \Longrightarrow M^B(x) = \Pi(x)\Big] \geq 1 - \delta.$$

Proof. To see the first item implies the second item, let M be a reduction such that if

$$\Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)}\Big] \geq \delta,$$

then

$$\Pr_{M,B}\big[M^B(x) = \Pi(x)\big] \geq 1 - \delta.$$

There are two cases. Either $\Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)}\Big] \geq \delta$ or not. In the former case, we have

$$\Pr_{M,B}\Big[A\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)} \Longrightarrow M^B(x) = \Pi(x)\Big] \geq 1 - \delta$$

because the conclusion in this event is satisfied with probability $1-\delta$. In the latter case, the hypothesis is false with probability $1-\delta$, which means that M satisfies the second item.

To see the converse, let M be the reduction that satisfies the second item. Let $\epsilon := \frac{1-2\delta}{4} > 0$. Assume that

$$\Pr_{M,B}\Big[A\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)}\Big] \geq 1-\epsilon.$$

By the property of M, we have

$$\begin{aligned}
1-\delta &\leq \Pr_{M,B}\Big[A\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)} \Longrightarrow M^B(x) = \Pi(x)\Big] \\
&\leq \Pr_{M,B}\Big[A\restriction_{Q_M(x)} \not\subseteq B\restriction_{Q_M(x)}\Big] + \Pr_{M,B}\big[M^B(x) = \Pi(x)\big] \\
&\leq \epsilon + \Pr_{M,B}\big[M^B(x) = \Pi(x)\big].
\end{aligned}$$

Thus, we obtain

$$\Pr_{M,B}\big[M^B(x) = \Pi(x)\big] \geq 1-\delta-\epsilon = \frac{1}{2}+\epsilon.$$

This success probability can be amplified as in Proposition 8.2. □

$\mathbb{B}$-restricted reductions can be composed naturally.

Proposition 8.4 (composition)**.** *Let B be a randomized oracle, and let Π_1, Π_2 be promise problems. If $\Pi_1 \leq_{\mathsf{tt}}^{\mathsf{BPP}} \Pi_2 \restriction \mathbb{BPP}^B$ and $\Pi_2 \leq_{\mathsf{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction B$, then $\Pi_1 \leq_{\mathsf{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction B$.*

Proof. Let M_1 be the $\mathbb{BPP}^B$-restricted reduction from Π_1 to Π_2, and M_2 be the B-restricted reduction from Π_2 to $\mathbb{A}$. We define a reduction M such that $M^B(x) := M_1^{M_2^B}(x)$ and $Q_M(x) := \bigcup_{q \in Q_{M_1}(x)} Q_{M_2}(q)$.

We claim that M is a B-restricted reduction from Π_1 to $\mathbb{A}$. Let $x \in \mathrm{dom}(\Pi_1)$ be an input of length n. Assume that

$$\Pr_{M,B}\Big[A\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)}\Big] \geq 1-\epsilon$$

for some small constant $\epsilon > 0$. By the definition of the query set $Q_M(x)$, we have

$$\Pr_{M_1,M_2,B}\Big[A\restriction_{Q_{M_2}(q)} \subseteq B\restriction_{Q_{M_2}(q)} \text{ for all } q \in Q_{M_1}(x)\Big] \geq 1-\epsilon.$$

By an averaging argument, with probability at least $1-2\epsilon$ over the internal randomness of M_1, it holds that

$$\Pr_{M_2,B}\Big[A\restriction_{Q_{M_2}(q)} \subseteq B\restriction_{Q_{M_2}(q)} \text{ for all } q \in Q_{M_1}(x)\Big] \geq \frac{1}{2}.$$

By the property of M_2, under this event, if $q \in \mathrm{dom}(\Pi_2)$, then

$$\Pr_{M_2,B}\big[M_2^B(q) = \Pi_2(q)\big] \geq 1-2^{-n}.$$

By a union bound, it holds that

$$\Pr_{M_2,B}\big[M_2^B(q) = \Pi_2(q) \text{ for every } q \in \mathrm{dom}(\Pi_2) \cap Q_{M_1}(x)\big] \geq 1-2^{-n}\cdot n^{O(1)} \geq 1-\epsilon.$$

By regarding M_2^B as a randomized oracle, this means that

$$\Pr_{M_2,B}\left[\Pi_2\restriction_{Q_{M_1}(x)} \subseteq M_2^B\restriction_{Q_{M_1}(x)}\right] \geq 1-\epsilon.$$

Since this holds with probability at least $1-2\epsilon$ over the internal randomness of M_1, we obtain

$$\Pr_{M_1,M_2,B}\left[\Pi_2\restriction_{Q_{M_1}(x)} \subseteq M_2^B\restriction_{Q_{M_1}(x)}\right] \geq 1-3\epsilon \geq \frac{1}{2}.$$

Thus, by the property of M_1, we obtain

$$\Pr_{M_1,M_2,B}\left[M_1^{M_2^B}(x) = \Pi_1(x)\right] \geq \frac{3}{4}.$$

□

We now introduce the notion of input-aware $\mathbb{B}$-restricted reduction.

Definition 8.5. *For a function $\alpha\colon \mathbb{N}\to\mathbb{N}$, a promise problem Π, a class $\mathbb{A}$ of promise problems, and a class $\mathbb{B}$ of randomized oracles, we write $L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{A} \restriction \mathbb{B} /\!\!/ \alpha$ if there exists a randomized nonadaptive oracle machine M such that, for every randomized oracle $B\in\mathbb{B}$, for all but finitely many $x\in\mathrm{dom}(\Pi)$, for every advice string $a\in\{0,1\}^{\alpha(|x|)}$ and every promise problem $A\in\mathbb{A}$, if*

$$\Pr_{M,B}[A(q) = B(a,q) \text{ for every } q\in Q_M(x)\cap\mathrm{dom}(A)] \geq \frac{1}{2},$$

then

$$\Pr_{M,B}\left[M^{B_a}(x) = \Pi(x)\right] \geq \frac{3}{4},$$

where B_a is the randomized oracle such that $B_a(q) := B(a,q)$ and the probabilities are taken over the internal randomness of M and B.

8.2 Reductions to Avoiding the Universal Hitting Set Generator

The universal hitting set generator is formally defined as follows.

Definition 8.6. *We define*

$$\mathcal{H}^{\mathrm{univ}} := \left\{\mathcal{H}_n^{\mathrm{univ}} : \{0,1\}^{n-\log^2 n} \to \{0,1\}^n\right\}_{n\in\mathbb{N}},$$

where $\mathcal{H}_n^{\mathrm{univ}}(d)$ is defined to be the output of the n^2-time simulation of the universal Turing machine on input d (and 1^n if the simulation does not halt in time n^2).

Here, we chose the seed length $s(n) := n - \log^2 n$ because of the following reasons.

1. On one hand, we will need $s(n) = n - \omega(\log n)$ in the transformation from the reduction to avoiding a hitting set generator to inverting an auxiliary-input one-way function (Theorem 9.3).
2. On the other hand, the seed expansion $n - s(n)$ should be small because $n - s(n)$ determines the approximation error of the non-black-box reduction of [Hir18].

Definition 8.7. *For a family* $H = \{H_n : \{0,1\}^{s(n)} \to \{0,1\}^n\}_{n\in\mathbb{N}}$ *of functions, a promise problem* A *is said to* avoid H *if for any* $n \in \mathbb{N}$ *such that* $s(n) \leq n-1$,

$$\Pr[A(w) = 1] \geq \frac{1}{2}$$

and for every $w \in \mathrm{Im}(H_n)$,

$$A(w) = 0,$$

where $\mathrm{Im}(H_n)$ *denotes the image of* H_n, *i.e.,* $\{H_n(z) \mid z \in \{0,1\}^{s(n)}\}$

8.2.1 Meta-complexity reduces to avoiding the universal hitting set generator

We now present the non-black-box worst-case to average-case reduction of [Hir18] in terms of B-restricted reductions.

Theorem 8.8. *Let* $\mathbb{A}$ *denote the class of the promise problems* A *that avoid* $\mathcal{H}^{\mathrm{univ}}$. *There exists a polynomial* τ *such that for every randomized oracle* B, *the promise problem* $\mathrm{Gap}_\tau(\mathrm{q} \text{ vs } \mathrm{rK}^B) = (\Pi_{\mathrm{YES}}, \Pi^B_{\mathrm{NO}})$ *defined as*

$$\Pi_{\mathrm{YES}} := \{(x, 1^t, 1^s) \mid t \geq |x| \text{ and } \mathrm{q}^t(x) \leq s\},$$
$$\Pi^B_{\mathrm{NO}} := \left\{(x, 1^t, 1^s) \;\middle|\; t \geq |x| \text{ and } \mathrm{rK}^{\tau(t),B}(x) > s + \log^3 \tau(t)\right\}$$

satisfies

$$\mathrm{Gap}_\tau(\mathrm{q} \text{ vs } \mathrm{rK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction B.$$

Moreover, the reduction is independent of B.[20]

We need the following lemma for the proof.

Lemma 8.9 ([AF09; AGMMM18]; see also [Hir21, Lemma 9.7])**.** *There exists a polynomial* p *such that for every* $x \in \{0,1\}^*$ *and every* $t \geq |x|$,

$$\Pr_{r\sim\{0,1\}^{p(t)}}\left[\mathrm{K}^{p(t)^2}(x, r) \leq \mathrm{q}^t(x) + |r| + \log p(t)\right] \geq 1 - o(1).$$

Proof of Theorem 8.8. We describe a B-restricted reduction M to $\mathbb{A}$. Let G_k be the pseudorandom generator construction of Lemma 7.1. Let $(x, 1^t, 1^s)$ be an input. The reduction M^B chooses z and $r \sim \{0,1\}^{t'}$ randomly and outputs 1 if and only if

$$B(G_k(x; z) \cdot r) = 0,$$

where $a \cdot b$ denotes the concatenation of two strings a and $b \in \{0,1\}^*$, $t' = \mathsf{poly}(t)$, and k is a parameter chosen later. The reduction also makes an additional query $w \cdot r$ in order to ensure that A and B are close. This completes the description of M.

Assume that

$$\Pr_{M,B}\left[A\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)}\right] \geq 1 - \epsilon$$

[20] That is, there exists a reduction M such that for every B, the reduction M is B-restricted reduction from $\mathrm{Gap}_\tau(\mathrm{q} \text{ vs } \mathrm{rK}^B)$ to $\mathbb{A}$.

for a small constant $\epsilon > 0$ chosen later. Under this assumption, we have

$$\begin{aligned}
&\Pr_{w,r}[A(w \cdot r) = 1] - \Pr_{w,r,B}[B(w \cdot r) = 1] \\
&\leq \Pr_{w,r,B}[w \cdot r \in \mathrm{dom}(A) \text{ and } A(w \cdot r) \neq B(w \cdot r)] \\
&\leq \Pr_{M,B}\left[A\restriction_{Q_M(x)} \not\subseteq B\restriction_{Q_M(x)}\right] \leq \epsilon,
\end{aligned}$$

where the second inequality holds because M makes a query $w \cdot r$. Since A avoids $\mathcal{H}^{\mathrm{univ}}$, it follows that

$$\begin{aligned}
\Pr_{w,r,B}[B(w \cdot r) = 1] &\geq \Pr_{w,r}[A(w \cdot r) = 1] - \epsilon \\
&\geq \frac{1}{2} - \epsilon. \qquad (11)
\end{aligned}$$

Similarly, we have

$$\Pr_{z,r}[A(G_k(x;z), r) = 0] - \Pr_{z,r}[B(G(x;z), r) = 0] \leq \epsilon. \qquad (12)$$

Now, we prove the correctness of M. Let $(x, 1^t, 1^s)$ be a YES instance. Since $\mathrm{q}^t(x) \leq s$ and G_k is efficiently computable, we have

$$\mathrm{q}^{\mathsf{poly}(t)}(G_k(x;z)) \leq s + |z| + O(\log k) \leq k - O(\log^2 t),$$

where we choose a sufficiently large $k = s + |z| + O(\log^2 t)$ so that the last inequality holds. By Lemma 8.9, we obtain

$$\Pr_{r \sim \{0,1\}^{t'}}\left[\mathrm{K}^{t'^2}(G_k(x;z) \cdot r) \leq k + |r| - O(\log^2 t)\right] \geq 1 - \epsilon.$$

Under this event, by the definition of the universal hitting set generator, we have $G_k(x;z) \cdot r \in \mathrm{Im}(\mathcal{H}^{\mathrm{univ}}_{k+t'})$. Since A avoids $\mathcal{H}^{\mathrm{univ}}$, it holds that

$$\Pr_{z,r}[A(G_k(x;z) \cdot r) = 0] \geq 1 - \epsilon.$$

By Eq. (12), we obtain

$$\Pr_{M,B}\left[M^B(x, 1^t, 1^s) = 1\right] = \Pr_{z,r,B}[B(G_k(x;z) \cdot r) = 0] \geq 1 - 2\epsilon.$$

We now prove that any NO instance is accepted by M with probability at most $\frac{3}{4}$. This is sufficient, as the gap between the probabilities $1 - 2\epsilon$ and $\frac{3}{4}$ can be amplified by using a standard technique of repetition. We prove the contrapositive. Assume that

$$\Pr_{M,B}\left[M^B(x, 1^t, 1^s) = 1\right] = \Pr_{z,r,B}[B(G_k(x;z) \cdot r) = 0] \geq \frac{3}{4}.$$

By Eq. (11), we also have

$$\Pr_{w,r,B}[B(w \cdot r) = 0] = 1 - \Pr_{w,r,B}[B(w \cdot r) \neq 0] \leq \frac{1}{2} + \epsilon.$$

These two inequalities indicate that B can distinguish $G_k(x;\text{-})$ from the uniform distribution; thus, by Lemma 7.1, we obtain

$$\mathrm{rK}^{\tau(t),B}(x) \leq k + O(\log^3 n) \leq s + \log^3 \tau(t),$$

where τ is some sufficiently large polynomial. This means that the input is not a NO instance. □

8.2.2 An algorithmic proof of symmetry of information

Hirahara [Hir22c] showed the equivalence between the meta-complexity of the conditional time-bounded Kolmogorov complexity and the (unconditional) time-bounded Kolmogorov complexity via a non-black-box reduction. We show that this reduction can be regarded as a B-restricted reduction.

Theorem 8.10. *For every polynomial p, there exists a polynomial τ such that for any randomized oracles B and B', the promise problem $\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^B \text{ vs } \mathrm{crK}^B) = (\Pi^B_{\mathrm{YES}}, \Pi^B_{\mathrm{NO}})$ defined as*

$$\Pi^B_{\mathrm{YES}} := \left\{(x, y, 1^t, 1^s) \;\middle|\; t \geq |x|+|y| \text{ and } \mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B}(y) \leq s\right\},$$
$$\Pi^B_{\mathrm{NO}} := \left\{(x, y, 1^t, 1^s) \;\middle|\; t \geq |x|+|y| \text{ and } \mathrm{rK}^{\tau(t),B}(x \mid y) > s + \log^3 \tau(t)\right\}$$

satisfies

$$\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^B \text{ vs } \mathrm{crK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_p(\mathrm{q} \text{ vs } \mathrm{rK}^{B'}) \restriction B.$$

Moreover, the reduction is independent of B and B'.[21]

Proof. We describe a B-restricted reduction M to the promise problem $\Pi := \mathrm{Gap}_p(\mathrm{q} \text{ vs } \mathrm{rK}^{B'})$. The reduction M^B takes an instance $(x, \mathcal{D}, 1^t, 1^s)$ of $\mathrm{Gap}_{\tau,\alpha}(\mathrm{q}-\mathrm{rK}^B \text{ vs } \mathrm{crK}^B)$ as input. Let $n := |x|+|y|$. Let $\epsilon > 0$ be a sufficiently small constant. For any randomized oracle B (as well as any promise problem), define $\widehat{B}$ to be the oracle such that $\widehat{B}(w) := B(w, 1^{t'}, 1^{|w|-2\log^3 p(t')})$ for any $w \in \{0,1\}^*$, where $t' = \mathsf{poly}(t)$ is chosen later. Let k ($\approx s$) be a parameter chosen later. Let G_ℓ be the pseudorandom generator construction of Lemma 7.1. For each $\ell \in \mathbb{N}$, the reduction estimates

$$v_\ell := \Pr_{w,z',B}\left[\widehat{B}(w \cdot G_\ell(y; z')) = 0\right]$$

using random sampling, where $w \sim \{0,1\}^k$ and $z' \sim \{0,1\}^{O(\log^3 n)}$. Let $\widehat{v}_\ell$ be the estimated value of v_ℓ. By a concentration inequality, we can make sure that $|\widehat{v}_\ell - v_\ell| \leq \epsilon$ with probability at least $1-2^{-t}$ over the internal randomness of M. Let $\ell^* := \min\left\{\ell \;\middle|\; \widehat{v}_\ell \geq \frac{3}{4}\right\}$. Note that such ℓ^* ($\leq 2|y|$) exists because $\mathrm{q}^{t'}(w \cdot G_\ell(y;z')) \leq |w|+|y| \ll |w|+\ell-2\log^3 p(t')$ for $\ell := 2|y|$. Then, the reduction M^B outputs 1 if and only if $\widehat{B}(G_k(x;z) \cdot G_{\ell^*}(y;z')) = 0$ for random choices of $z, z' \sim \{0,1\}^{O(\log^3 n)}$. Finally, the reduction makes an additional query $w \cdot w'$ to $\widehat{B}$ for $w \sim \{0,1\}^k$ and $w \sim \{0,1\}^{\ell^*-1}$. Note that M can be implemented as a nonadaptive reduction because the number of candidates of the value ℓ is at most $O(n)$.

We prove the correctness of M. Assume that

$$\Pr_{M,B}\left[\Pi\restriction_{Q_M(x)} \subseteq B\restriction_{Q_M(x)}\right] \geq 1-\epsilon.$$

Let $\mathcal{B}$ be any distribution over oracles consistent with B. Let E be the event that $|\widehat{v}_\ell - v_\ell| \leq \epsilon$ for all ℓ. Since the probability that E fails is exponentially small, we assume E in what follows and analyze the success probability of M under the event E.

By a counting argument (Fact 5.5), with probability at least $1-\epsilon$ over a choice of $w \sim \{0,1\}^k, w' \sim \{0,1\}^{\ell^*-1}$, it holds that

$$\mathrm{K}^{B'}(w \cdot w') \geq k + \ell^* - O(1) > k + \ell^* - \log^3 p(t'),$$

[21] crK stands for conditional randomized Kolmogorov complexity.

under which $(w \cdot w', 1^{t'}, 1^{s'})$ is a No instance of Π, where $s' := k + \ell^* - 2\log^3 p(t')$. It follows that

$$\Pr_{w,w',B}\Big[\widehat{B}(w \cdot w') = 1\Big] \le \Pr_{w,w'}\Big[\widehat{\Pi}(w \cdot w') \neq 0\Big] + \Pr\Big[\Pi\restriction_{Q_M(x)} \not\subseteq B\restriction_{Q_M(x)}\Big] \le 2\epsilon,$$

where the first inequality holds because M makes a query $w \cdot w'$. On the other hand, since $\widehat{v}_{\ell^*-1} < \frac{3}{4}$, we have $v_{\ell^*-1} \le \frac{3}{4} + \epsilon$ under the event E; thus,

$$\Pr_{B,w,z'}\Big[\widehat{B}(w \cdot G_{\ell^*-1}(y; z')) = 1\Big] = 1 - v_{\ell^*-1} \ge \frac{1}{4} - \epsilon.$$

These two inequalities indicate that the oracle $\widehat{B}(w \cdot \text{-})$ can distinguish G_{ℓ^*-1} from the uniform distribution. Thus, by Lemma 7.1, we obtain

$$\mathrm{rK}^{\tau(t),B}(y) \le \ell^* + O(\log^3 n) + O(\log t)$$

for a sufficiently large polynomial τ.

Now, assume that $(x, y, 1^t, 1^s)$ is a Yes instance, i.e. $\mathrm{q}^t(x, y) - \mathrm{rK}^{\tau(t),B}(y) \le s$. Since $G_k(x; z) \cdot G_{\ell^*}(y; z')$ can be efficiently computed from (x, y), we have

$$\begin{aligned}
\mathrm{q}^{t'}(G_k(x; z) \cdot G_{\ell^*}(y; z')) &\le \mathrm{q}^t(x, y) + |z| + |z'| + O(\log k\ell^*) \\
&\le s + \mathrm{rK}^{\tau(t),B}(y) + O(\log^3 n) \\
&\le s + \ell^* + O(\log^3 n) \\
&\le k + \ell^* - 2\log^3 p(t'),
\end{aligned}$$

where the last inequality holds by choosing $k := s + O(\log^3 n) + 2\log^3 p(t')$. Thus, $G_k(x; z) \cdot G_{\ell^*}(y; z')$ is a Yes instance of Π with probability 1. It follows that

$$\begin{aligned}
\Pr\big[M^B(x, y, 1^t, 1^s) = 0\big] &= \Pr\Big[\widehat{B}(G_k(x; z) \cdot G_{\ell^*}(y; z')) = 0\Big] \\
&= \Pr\Big[\widehat{\Pi}(G_k(x; z) \cdot G_{\ell^*}(y; z')) = 0\Big] + \Pr\Big[\Pi\restriction_{Q_M(x)} \not\subseteq B\restriction_{Q_M(x)}\Big] \le \epsilon.
\end{aligned}$$

Conversely, assume that M^B accepts with probability at least $\frac{1}{2}$. That is,

$$\Pr\Big[\widehat{B}(G_k(x; z) \cdot G_\ell(y; z')) = 0\Big] \le \frac{1}{2}.$$

By the definition of ℓ^*, we have

$$v_{\ell^*} = \Pr\Big[\widehat{B}(w \cdot G_{\ell^*}(y; z')) = 0\Big] \ge \widehat{v}_{\ell^*} - \epsilon \ge \frac{3}{4} - \epsilon.$$

These two inequalities imply

$$\Pr\Big[\widehat{B}(G_k(x; z) \cdot G_{\ell^*}(y; z')) = 1\Big] - \Pr\Big[\widehat{B}(w \cdot G_{\ell^*}(y; z')) = 1\Big] \ge \frac{1}{4} - \epsilon.$$

This indicates that an oracle $B(\text{-} \cdot G_{\ell^*}(y; z'))$ can distinguish the output distribution of $G_k(x; \text{-})$ from the uniform distribution. Thus, by Lemma 7.1, we obtain

$$\mathrm{rK}^{\tau(t),B}(x \mid y) \le k + O(\log^3 n) \le s + O(\log^3 t) \le s + \log^3 \tau(t)$$

for a sufficiently large polynomial τ. This implies that the input is not a No instance of Π. □

8.2.3 Reductions from distributional Kolmogorov complexity

We reduce a "non-disjoint" promise problem that asks to approximate $\mathrm{dpK}^{\mathsf{poly}}$ to the "non-disjoint" promise problem of approximating conditional Kolmogorov complexity.

Theorem 8.11. *For every polynomial p, there exists a polynomial τ satisfying the following. For randomized oracles B and B', define the promise problem $\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^{B'}$ vs $\mathrm{dpK}^B)$ as follows.*

Input: *a string x, a distribution $\mathcal{D}$ over $\{0,1\}^m$, parameters $t, s, \epsilon^{-1} \in \mathbb{N}$ (encoded in unary), $\lambda \in (0,1)$ (encoded in binary).*

Promise: $t \geq |x| + m + \epsilon^{-1}$.

Yes: $\Pr_{y\sim\mathcal{D}}\Big[\mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B'}(y) \leq s\Big] \geq \lambda$.

No: $\mathrm{dpK}^{\tau(t),B}_{\lambda-\epsilon}(x \mid \mathcal{D}) > s + \log^3 \tau(t)$.

Then, we have

$$\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^{B'} \text{ vs } \mathrm{dpK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_p(\mathrm{q}-\mathrm{rK}^{B'} \text{ vs } \mathrm{crK}^{B'}) \restriction B.$$

Moreover, the reduction is independent of B and B'.

Proof. Let $\Pi := \mathrm{Gap}_p(\mathrm{q}-\mathrm{rK}^{B'}$ vs $\mathrm{crK}^{B'})$. We describe a B-restricted reduction M from $\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^B$ vs $\mathrm{drK}^B)$ to Π. The reduction M^B takes $\varphi = (x, \mathcal{D}, 1^t, 1^s, 1^{\epsilon^{-1}}, \lambda)$ as input. Let $n := |x|$. Define

$$v := \Pr_{z,y}\Big[B(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'}) = 1\Big],$$

where k, t' and s' are parameters chosen later and $z \sim \{0,1\}^{nk}$ and $y \sim \mathcal{D}$. The reduction M^B estimates v by random sampling. Let $\tilde{v}$ be the estimated value of v such that $v \leq \tilde{v} \leq v + \epsilon$ with high probability over the internal randomness of M. The output of the reduction is defined to be 1 if and only if $\tilde{v} \geq \lambda - \epsilon$. The reduction makes an additional query $(w, y, 1^{t'}, 1^{s'})$ for $w \sim \{0,1\}^{nk+k}$.

To prove the correctness of M, assume that

$$\Pr_M\Big[\Pi\restriction_{Q_M(\varphi)} \subseteq B\restriction_{Q_M(\varphi)}\Big] \geq 1 - \epsilon.$$

Consider any YES instance φ of $\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^{B'}$ vs $\mathrm{dpK}^B)$. Then, with probability at least λ over a choice of $y \sim \mathcal{D}$, we have $\mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B'}(y) \leq s$. Under this event, we also have

$$\begin{aligned}\mathrm{q}^{t'}(\mathrm{DP}_k(x;z), y) - \mathrm{rK}^{p(t'),B'}(y) &\leq \mathrm{q}^t(x,y) + |z| + O(\log k) - \mathrm{rK}^{p(t'),B'}(y)\\ &\leq s + nk + O(\log n),\end{aligned}$$

where the last inequality holds for $\tau(t) \geq v(t')$. Choosing $s' := s + nk + O(\log n)$, this implies that $\Pi(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'}) = 1$. It follows that

$$v = \Pr_{z,y\sim\mathcal{D}}\Big[B(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'}) = 1\Big] \geq \Pr_{z,y\sim\mathcal{D}}\Big[\Pi(\mathrm{DP}_k(x;z), y, 1^{t'}, 1^{s'}) = 1\Big] - \epsilon \geq \lambda - \epsilon.$$

With high probability over the internal randomness of M, we have $\tilde{v} \geq v \geq \lambda - \epsilon$, under which M^B accepts.

Conversely, assume that $v \geq \lambda - 2\epsilon$. By a counting argument, for every $y \in \mathrm{supp}(\mathcal{D})$ and every $z \in \{0,1\}^{nk}$, with probability at least $1-\epsilon$ over $w \sim \{0,1\}^{nk+k}$, it holds that

$$\mathrm{K}^{B'}(w \mid y, z) \geq nk + k - O(\log(1/\epsilon)) > s' + \log^3 p(t'),$$

where we choose $k := s' + 2\log^3 p(t')$. Under this event, we have $\Pi(w, y, 1^{t'}, 1^{s'}) = 0$. Thus,

$$\Pr\Big[B(w, y, 1^{t'}, 1^{s'}) = 0\Big] \geq 1 - \epsilon - \Pr\Big[\Pi\restriction_{Q_M(\varphi)} \not\subseteq B\restriction_{Q_M(\varphi)}\Big] \geq 1 - 2\epsilon.$$

Combining this with the assumption that $v \geq \lambda - 2\epsilon$, we obtain

$$\Pr\Big[B(w, y, 1^{t'}, 1^{s'}) = 0\Big] - \Pr\Big[B(\mathrm{DP}_k(x; z), y, 1^{t'}, 1^{s'}) = 0\Big] \geq \lambda - 4\epsilon.$$

By Theorem 7.6, we obtain

$$\mathrm{dpK}^{\mathsf{poly}(t'),B}_{\lambda-5\epsilon}(x \mid \mathcal{D}, r) \leq k + O(\log(n/\epsilon)).$$

This means that the input is not a NO instance. Taking the contrapositive, for any NO instance, we have $v < \lambda - 2\epsilon$. Since $\tilde{v} \leq v + \epsilon \leq \lambda - \epsilon$ holds with high probability over the internal randomness of M^B, any NO instance is rejected with high probability. □

Corollary 8.12. *For a polynomial τ, define the promise problem* $\mathrm{Gap}_\tau(\mathrm{dK}\text{ vs }\mathrm{dpK}^B)$ *as follows.*

Input: *a string x, a distribution $\mathcal{D}$ over $\{0,1\}^m$, parameters $t, s, \epsilon^{-1} \in \mathbb{N}$ (encoded in unary), $\lambda \in (0,1)$ (encoded in binary).*

Promise: $t \geq |x| + m + \epsilon^{-1}$.

Yes: $\mathrm{dK}^t_\lambda(x \mid \mathcal{D}) \leq s - \max\{\mathrm{cd}^{t,B}(y) \mid y \in \mathrm{supp}(\mathcal{D})\}$.

No: $\mathrm{dpK}^{\tau(t),B}_{\lambda-\epsilon}(x \mid \mathcal{D}) > s + \log^3 \tau(t)$.

Then, there exists a polynomial τ such that

$$\mathrm{Gap}_\tau(\mathrm{dK}\text{ vs }\mathrm{dpK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \{A \mid A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\} \restriction B.$$

Similarly, we also have

$$\mathrm{Gap}_\tau(\mathrm{q-rK}^B\text{ vs }\mathrm{dpK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \{A \mid A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\} \restriction B.$$

Moreover, the reduction is independent of B.

Proof. Let $\mathbb{A} = \{A \mid A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\}$. We use Proposition 8.4 to combing the following reductions. We will observe

$$\mathrm{Gap}_\tau(\mathrm{dK}\text{ vs }\mathrm{dpK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_\tau(\mathrm{q-rK}^B\text{ vs }\mathrm{dpK}^B)$$

By Theorem 8.11,

$$\mathrm{Gap}_\tau(\mathrm{q-rK}^B\text{ vs }\mathrm{dpK}^B) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_p(\mathrm{q-rK}^B\text{ vs }\mathrm{crK}^B) \restriction \mathbb{BPP}^B.$$

By Theorem 8.10,

$$\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^B \text{ vs } \mathrm{crK}^B) \le^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_p(\mathrm{q} \text{ vs } \mathrm{rK}^B) \restriction \mathbb{BPP}^B.$$

By Theorem 8.8,

$$\mathrm{Gap}_\tau(\mathrm{q} \text{ vs } \mathrm{rK}^B) \le^{\mathsf{BPP}}_{\mathrm{tt}} \mathbb{A} \restriction B.$$

To show the first reduction, we reduce an instance of $(x, \mathcal{D}, 1^t, 1^s, 1^{\epsilon^{-1}}, \lambda)$ of $\mathrm{Gap}_\tau(\mathrm{dK} \text{ vs } \mathrm{dpK}^B)$ to an instance $(x, \mathcal{D}, 1^t, 1^{s'}, 1^{\epsilon^{-1}}, \lambda)$ of $\mathrm{Gap}_\tau(\mathrm{q}-\mathrm{rK}^B \text{ vs } \mathrm{dpK}^B)$ for some parameter s'. If $\mathrm{dK}^t_\lambda(x \mid \mathcal{D}) \le s - \max\{\mathrm{cd}^{t,B}(y) \mid y \in \mathrm{supp}(\mathcal{D})\}$, then with probability at least λ over a choice of $y \sim \mathcal{D}$, it holds that

$$\mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B}(y) \le s - \mathrm{cd}^{t,B}(y) + \mathrm{q}^t(y) - \mathrm{rK}^{\tau(t),B}(y) + O(\log t) \le s + O(\log t).$$

We define $s' := s + O(\log t)$ so that this can be bounded by s'. □

8.3 Slow Growth Law

Note that the promise problem in Corollary 8.12 has an additive error term of $\mathrm{cd}^{t,B}(y)$. In order to remove the error term, we use the slow growth law of computational depth [Ben88; AFPS12].

Lemma 8.13 (Slow growth law)**.** *Let $f\colon \{0,1\}^* \to \{0,1\}^*$ be a polynomial-time computable function. Let B be any randomized oracle. Then, there exists a polynomial p such that for every $x \in \{0,1\}^*$ and for every $t \ge |x|$,*

$$\mathrm{cd}^{p(t),B}(f(x)) \le \mathrm{cd}^{t,B}(x) + \log p(t).$$

Proof. We extend the notion of the universal a priori probability to a set. For a set $A \subseteq \{0,1\}^*$, let

$$\mathrm{Q}^t(A) := \Pr_{d\sim\{0,1\}^t}\left[U^t(d) \in A\right]$$

and

$$\mathrm{q}^t(A) := -\log \mathrm{Q}^t(A).$$

Consider

$$\frac{\mathrm{Q}^t(x)}{\mathrm{Q}^t(f^{-1}(f(x)))} = \frac{\Pr_{d\sim\{0,1\}^t}\left[U^t(d)=x\right]}{\Pr_{d\sim\{0,1\}^t}[U^t(d)\in f^{-1}(f(x))]} = \Pr_{d\sim\{0,1\}^t}\left[U^t(d)=x \;\middle|\; U^t(d)\in f^{-1}(f(x))\right].$$

Observe that the probability distribution of the random variable $U^t(d)$ under the event that $U^t(d) \in f^{-1}(f(x))$ is computable given $f(x)$ and t. Thus, by a coding theorem,

$$\mathrm{K}(x \mid f(x)) \le -\log \Pr_{d\sim\{0,1\}^t}\left[U^t(d)=x \;\middle|\; U^t(d)\in f^{-1}(f(x))\right] + O(\log t).$$

By the symmetry of information for Kolmogorov complexity [ZL70], we have

$$\mathrm{K}^B(x \mid f(x)) \ge \mathrm{K}^B(x, f(x)) - \mathrm{K}^B(f(x)) - O(\log n) \ge \mathrm{K}^B(x) - \mathrm{K}^B(f(x)) - O(\log n).$$

Observe that $\mathrm{K}^B(x \mid f(x)) \le \mathrm{K}(x \mid f(x)) + O(1)$. Combining these inequalities, we obtain

$$\mathrm{Q}^t(f^{-1}(f(x))) \ge 2^{-\mathrm{q}^t(x)+\mathrm{K}^B(x)-\mathrm{K}^B(f(x))-O(\log t)} =: a.$$

This implies that the output of the universal Turing machine on a random input is in $f^{-1}(f(x))$ with probability a. By applying f to the output of the universal Turing machine, we obtain a constant-size sampling procedure that outputs $f(x)$ with probability a. Thus, we conclude that

$$\mathrm{q}^{p(t)}(f(x)) \le -\log a = \mathrm{q}^t(x) - \mathrm{K}^B(x) + \mathrm{K}^B(f(x)) + O(\log t)$$

for some large polynomial p. □

Corollary 8.14. *Let M be a randomized polynomial-time algorithm. Then, there exists a polynomial p such that for every $x \in \{0,1\}^*$ and every $\epsilon^{-1} \in \mathbb{N}$,*

$$\Pr_M\left[\mathrm{cd}^{p(|x|),B}(M(x)) \le |x| + \log p(|x|) + \log(1/\epsilon)\right] \ge 1 - \epsilon.$$

Proof. Let $M(x;r)$ denote the output of the randomized algorithm M on input x and random bits r. By Fact 5.5, for a uniformly random sequence $r \sim \{0,1\}^m$, we have $\mathrm{K}^B(r) \ge m - \log(1/\epsilon)$ with probability $1-\epsilon$. Under this event, since $\mathrm{q}^{|x|^2}(r) \le m + O(1)$, we obtain

$$\mathrm{cd}^{|x|^2,B}(r) \le m + O(1) - m + \log(1/\epsilon) \le \log(1/\epsilon) + O(1).$$

By Lemma 8.13, for some polynomial p, we have

$$\begin{aligned}\mathrm{cd}^{p(|x|),B}(M(x;r)) &\le \mathrm{cd}^{|x|^3,B}(x,r) + \log p(|x|)\\ &\le |x| + \mathrm{cd}^{|x|^2,B}(r) + O(\log|x|)\\ &\le |x| + \log(1/\epsilon) + O(\log|x|).\end{aligned}$$

□

8.4 Combining Size-Expanding Reductions

We observe that a lower bound for P/poly-oracle $\mathrm{dK}^{\mathsf{poly}}$ implies a lower bound for $\mathrm{dpK}^{\mathsf{poly}}$.

Lemma 8.15. *For every randomized oracle $B \in \mathbb{BPP}/\mathsf{poly}$, there exists an oracle $B' \in \mathsf{P}/\mathsf{poly}$ such that for every $t \ge |x| + \mathrm{K}(\mathcal{D}) + \epsilon^{-1} + \mathrm{K}(\lambda)$,*

$$\mathrm{dK}^{\tau(t),B'}_{\lambda-\epsilon}(x \mid \mathcal{D}) \le \mathrm{dpK}^{t,B}_{\lambda}(x \mid \mathcal{D}) + \log\tau(t).$$

Proof. The idea is to hard-wire a pseudorandom generator secure against linear-size programs in B'. Let $s := \mathrm{dpK}^{t,B}_{\lambda}(x \mid \mathcal{D})$. Then, we have

$$\Pr_{r\sim\{0,1\}^t}\left[\mathrm{dK}^{t,B}_{\lambda}(x \mid \mathcal{D}, r) \le s\right] \ge \frac{3}{4}.$$

Let $f = \{f_n \in \{0,1\}^n\}_{n\in\mathbb{N}}$ be a sequence of strings such that $\mathrm{K}(f_n) \ge n/2$. Such a sequence exists by Fact 5.5. Using [IW97], we construct a pseudorandom generator $G^f_n \colon \{0,1\}^{O(\log n)} \to \{0,1\}^n$ that is computable by an f-oracle polynomial-time deterministic algorithm and is secure against linear-size (time-unbounded) programs. Since $B \in \mathbb{BPP}/\mathsf{poly}$, there exists a polynomial-size circuit C such that C takes q and a coin flip sequence w and the distribution of $C(q;w)$ over $w \sim \{0,1\}^{\mathsf{poly}(|q|)}$ is identical to the distribution of $B(x)$. We define B' to be an oracle that can

answer queries about C and f. Specifically, B' answers the i-th bit of f_n on query $(1^n, i)$, and answers $C(q; w)$ on query $(0, q, w)$.

Consider an arbitrary $r \in \{0,1\}^t$ such that $\mathrm{dK}_{\lambda}^{t,B}(x \mid \mathcal{D}, r) \leq s$. We claim

$$\mathrm{dK}_{\lambda-\epsilon}^{p(t),B'}(x \mid \mathcal{D}, r) \leq s + O(\log t)$$

for some polynomial p. By assumption, there exists a B-oracle program M^B that takes $y \sim \mathcal{D}$ and r and prints x with probability at least λ. Now, we simulate M^B on input (y, r) by a C-oracle algorithm M'^C that takes a coin flip sequence r' as follows. The i-th query q of M^B to B is answered with $C(q; w)$, where w is the i-th block of r'. (In other words, each time B is queried, fresh random bits are used.) Let $M'^C(y, r; r')$ denote the output of this simulation. Since M'^C simulates M^B, with probability at least λ over a random choice of r' and $y \sim \mathcal{D}$, we have $M'^C(y, r; r') = x$. Since this condition can be checked by a $t' = \mathsf{poly}(t)$-size program given r' as input, we can replace r' with $G_{t'}^f(\sigma)$ for some seed σ by reducing the success probability to $\lambda - \epsilon$. Thus, we obtain

$$\Pr_{y \sim \mathcal{D}}\left[M'^C(y, r; G_{t'}^f(\sigma)) = x\right] \geq \lambda - \epsilon.$$

Since $\sigma \in \{0,1\}^{O(\log t')}$ can be hard-wired in a machine, it follows that

$$\mathrm{dK}_{\lambda-\epsilon}^{p(t),B'}(x \mid \mathcal{D}, r) \leq s + O(\log t)$$

for some sufficiently large polynomial p.

Thus, we have

$$\Pr_{r \sim \{0,1\}^t}\left[\mathrm{dK}_{\lambda-\epsilon}^{p(t),B'}(x \mid \mathcal{D}, r) \leq s + O(\log t)\right] \geq \frac{3}{4}.$$

Given $r \in \{0,1\}^t$, it is possible to check whether $\mathrm{dK}_{\lambda-\epsilon}^{p(t),B'}(x \mid \mathcal{D}, r) \leq s$ or not by a program of size $t'' = \mathsf{poly}(t)$. Thus, by the security of the pseudorandom generator $G_{t''}^f$, there exists a seed σ such that

$$\mathrm{dK}_{\lambda-\epsilon}^{p(t),B'}(x \mid \mathcal{D}, G_{t''}^f(\sigma)) \leq s + O(\log t).$$

Let $M^{B'}$ be a B'-oracle program that witnesses this inequality. Consider a B'-oracle program that takes an input $y \sim \mathcal{D}$ and simulates $M^{B'}(y, G_{t''}^f(\sigma))$, where $\sigma \in \{0,1\}^{O(\log t'')}$ is hard-wired. Then, this program outputs x with probability at least $\lambda - \epsilon$. Therefore, we obtain

$$\mathrm{dK}_{\lambda-\epsilon}^{\tau(t),B'}(x \mid \mathcal{D}) \leq s + O(\log t) \leq s + \log \tau(t)$$

for a sufficiently large polynomial τ. □

We note that the reductions presented so far may not be input-aware P/poly-restricted reductions. However, by combining them with a size-expanding reduction, we obtain an input-aware P/poly-restricted reduction.

Theorem 8.16. *Let Π be a promise problem. Assume that*

$$\Pi \leq_{\mathrm{m}}^{\mathsf{BPP}} \left\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^B \;\middle|\; \tau \in \mathsf{poly}, B \in \mathsf{P}/\mathsf{poly}\right\}$$

via a size-expanding reduction for some constant $\epsilon > 0$. Then, it holds that

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{A \;\middle|\; A \textit{ avoids } \mathcal{H}^{\mathrm{univ}}\right\} \restriction \mathbb{BPP}/\mathsf{poly} \mathbin{/\!\!/} 2n.$$

Moreover, the reduction is honest.

Proof. At a high level, we compose the following reductions:

$$\begin{aligned}\Pi &\le_{\mathrm{tt}}^{\mathsf{BPP}} \left\{ \mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{B'} \;\middle|\; \tau\colon \text{a polynomial}, B' \in \mathsf{P/poly} \right\} \\ &\le_{\mathrm{m}}^{\mathsf{BPP}} \mathrm{Gap}_{\tau'}(\mathrm{q}-\mathrm{rK}^{B_a} \text{ vs } \mathrm{dpK}^{B_a}) \\ &\le_{\mathrm{tt}}^{\mathsf{BPP}} \left\{ A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}} \right\} \upharpoonright \mathbb{BPP}/\mathsf{poly} /\!\!/ 2n,\end{aligned}$$

where the first reduction is due to the assumption, the second reduction is a slight modification of the identity map, and the third reduction is due to Corollary 8.12. The randomized oracle B_a denotes an input-aware oracle, and $B' \in \mathsf{P/poly}$ denotes the oracle of Lemma 8.15. Details follow.

Let M be the reduction from Π to $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^B$ for any oracle B and any polynomial τ. Let τ be a polynomial sufficiently larger than the running time of M. Let M' be the reduction of Corollary 8.12.

We describe a $(\mathbb{BPP}/\mathsf{poly} /\!\!/ 2n)$-restricted reduction $\mathcal{M}$ from Π to $\left\{ A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}} \right\}$. Let $B \in \mathbb{BPP}/\mathsf{poly}$ be a randomized oracle. Let $B' \in \mathsf{P/poly}$ be the oracle of Lemma 8.15. Let φ be an input. Let $a \in \{0,1\}^{2n}$ be an advice string, and let $B_a(q) := B(a,q)$. We simulate the reduction M on input φ as follows. Given a query $q = (x, \mathcal{D}, 1^s, \lambda)$ to the oracle $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{B'}$, we reduce q to $q' = (x, \mathcal{D}, 1^{t'}, 1^{s'}, \lambda)$, which we regard as an instance of $\mathrm{Gap}_{\tau'}(\mathrm{q}-\mathrm{rK}^{B_a} \text{ vs } \mathrm{drK}^{B_a})$. (We choose t' and s' later.) Finally, we simulate the reduction M' on input q' using the oracle B_a and answer the query q using the output of M'.

To see the correctness of $\mathcal{M}$, we claim that any instance q of $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{B'}$ is correctly mapped to an instance q' of $\mathrm{Gap}_{\tau'}(\mathrm{q}-\mathrm{rK}^{B_a} \text{ vs } \mathrm{drK}^{B_a})$. Let q be a YES instance of $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{B'}$, i.e., $\mathrm{dK}_\lambda^{\tau,B'}(x \mid \mathcal{D}) \le s$. Then, there exists a B'-oracle program M of size s that outputs x in time t on input $y \sim \mathcal{D}$ with probability λ, where $t := \tau(|x|+|y|)$. In particular, with probability at least λ over a choice of $y \sim \mathcal{D}$, it holds that $\mathrm{q}^{t,B'}(x \mid y) \le s$. Since $\mathrm{q}^t(x,y) = \mathrm{K}^{B'}(x,y) + \mathrm{cd}^{t,B'}(x,y)$ and $\mathrm{K}^{B'}(x,y) \le \mathrm{q}^{t,B'}(y) + \mathrm{q}^{t,B'}(x \mid y) + O(1) \le \mathrm{q}^{t,B'}(y) + s + O(1)$, we obtain

$$\mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B_a}(y) \le s + \mathrm{cd}^{t,B'}(x,y) + \mathrm{q}^{t,B'}(y) - \mathrm{rK}^{\tau(t),B_a}(y)$$

By Corollary 8.14,

$$\mathrm{cd}^{t,B'}(x,y) \le |\varphi| + O(|\varphi|^{1/2})$$

holds with probability $1 - 2^{-|\varphi|^{1/2}}$ over the internal randomness of M. Here, we used that $t = \tau(|x|+|y|)$ is sufficiently larger than the running time of M on input φ.[22] Since

$$\mathrm{K}^{B'}(y) \le \mathrm{rK}^{\tau(t),B_a}(y) + |a| + O(1),$$

we also have

$$\mathrm{q}^{t,B'}(y) - \mathrm{rK}^{\tau(t),B_a}(y) \le \mathrm{cd}^{t,B'}(y) + |a| + O(1),$$

which can be bounded by $|\varphi| + |a| + O(1)$ Thus, we obtain

$$\mathrm{q}^t(x,y) - \mathrm{rK}^{\tau(t),B_a}(y) \le s + O(|\varphi|) \le (1+\epsilon/4)\cdot s =: s'.$$

This shows that q' is a YES instance of $\mathrm{Gap}_{\tau'}(\mathrm{q}-\mathrm{rK}^{B_a} \text{ vs } \mathrm{drK}^{B_a})$.

[22] We may assume without loss of generality that $|x| \ge |\varphi|$ because M is size-expanding.

Conversely, let q be a NO instance of $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{B'}$, i.e., $\mathrm{dK}^{\tau,B'}_{\lambda-\delta}(x \mid \mathcal{D}) \geq (1+\epsilon)\cdot s$. By Lemma 8.15, we have

$$\mathrm{dpK}^{\tau,B}_{\lambda'}(x \mid \mathcal{D}) \geq (1+3\epsilon/4)\cdot s,$$

where $\lambda' := \lambda - \delta/2$. Thus, we obtain

$$\mathrm{dK}^{\tau,B_a}_{\lambda'}(x \mid \mathcal{D}) \geq \mathrm{dK}^{\tau,B}_{\lambda'}(x \mid \mathcal{D}) - O(|\varphi|) \geq (1+\epsilon/2)\cdot s \geq s' + \log^3 \tau(|x|+|y|),$$

which implies that q' is a NO instance of $\mathrm{Gap}_{\tau'}(\mathrm{q}-\mathrm{rK}^{B_a}$ vs $\mathrm{drK}^{B_a})$. □

We also have a $\mathrm{dpK}^{\mathsf{poly}}$ version of Theorem 8.16.

Theorem 8.17. *Let Π be a promise problem. Assume that $\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \left\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdpKP}\right\}_{\tau\in\mathsf{poly}}$ via a size-expanding reduction for some constant $\epsilon > 0$. Then, it holds that*

$$\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \left\{A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\right\} \upharpoonright \mathbb{BPP} /\!\!/ 2n.$$

9 Hitting Set Generator to Auxiliary-Input One-Way Function

In this section, we show that an input-aware P/poly-restricted reduction to an arbitrary oracle that avoids a hitting set generator can be converted into a reduction to an arbitrary inverter of some auxiliary-input one-way function.

Definition 9.1. *Let $s,t\colon \mathbb{N}\to\mathbb{N}$ be polynomials. For an auxiliary-input function*

$$f = \left\{ f_x : \{0,1\}^{s(|x|)} \to \{0,1\}^{t(|x|)} \right\}_{x\in\{0,1\}^*},$$

a randomized oracle I is said to invert *f on auxiliary input x with success probability ϵ if*

$$\Pr_{y\sim\{0,1\}^{s(|x|)},I}\left[I(x,f_x(y)) \in f_x^{-1}(f_x(y))\right] \geq \epsilon,$$

where the probability is over y as well as the randomness of I. By default, we assume $\epsilon := \frac{1}{2}$. We say that I inverts *f if I inverts f on every auxiliary input $x\in\{0,1\}^*$.*

We consider a stronger notion of *fixed-auxiliary-input* reduction.

Definition 9.2. *We say that M is a $\mathbb{I}$-restricted fixed-auxiliary-input reduction from Π to inverting f if for every randomized oracle $I\in\mathbb{I}$, for all but finitely many $x\in\mathrm{dom}(\Pi)$ such that I inverts f on auxiliary input x, it holds that*

$$\Pr_{M,I}\left[M^I(x) = \Pi(x)\right] \geq \frac{3}{4},$$

where the probability is taken over the internal randomness of M and I, and any query of M can be written as (x,q) for some $q\in\{0,1\}^*$. If M is a randomized polynomial-time nonadaptive reduction, then we denote it by

$$\Pi \leq^{\mathsf{BPP}}_{\mathrm{tt}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{I}.$$

Note that we use the same notation with P/poly-restricted reductions. An $\mathbb{I}$-restricted fixed-auxiliary-input reduction is stronger than an $\mathbb{I}$-restricted reduction. Using the stronger notion makes the subsequent proofs simpler.

Theorem 9.3. *Let Π be a promise problem. Let $\mathbb{I}$ be a class of randomized oracles. Let*

$$H = \left\{H_n : \{0,1\}^{s(n)} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$$

be an arbitrary family of functions such that $s(n) < n - \omega(\log n)$. If

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{A \mid A \text{ avoids } H\} \upharpoonright \mathbb{BPP}^{\mathbb{I}} /\!\!/ n$$

via an honest reduction, then there exists a polynomial-time-computable auxiliary-input function $f = \{f_x\}_{x\in\{0,1\}^*}$ such that

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{I}.$$

Under the non-existence of a one-way function, one can estimate the probability that a string is sampled from a polynomial-time samplable distribution. Here, we use its auxiliary-input variant.

Lemma 9.4 (Impagliazzo and Levin [IL90])**.** *Let $\mathcal{Q} = \{\mathcal{Q}_x\}_{x\in\{0,1\}^*}$ be a polynomial-time-samplable family of distributions. Let $\delta\colon \mathbb{N} \to (0,1)$ be a function such that $(\delta(n))^{-1} = n^{O(1)}$. Then, there exist a polynomial-time-computable auxiliary-input function $f = \{f_x\}_{x\in\{0,1\}^*}$ and a randomized polynomial-time nonadaptive oracle machine T such that for every oracle I and every $x \in \{0,1\}^*$ such that I inverts f on auxiliary input x,*

$$\Pr_{q\sim\mathcal{Q}_x,T}\left[(1-\delta(|x|))\cdot\mathcal{Q}_x(q) \leq T^I(x,q) \leq (1+\delta(|x|))\cdot\mathcal{Q}_x(q)\right] \geq 1-\delta(|x|),$$

where the probability is taken over $q \sim \mathcal{Q}_x$ and the internal randomness of T.

We now present a proof of Theorem 9.3.

Proof of Theorem 9.3. Let $\epsilon > 0$ be a sufficiently small constant. By assumption, there exists a randomized polynomial-time nonadaptive machine M such that for any $B \in \mathbb{BPP}^{\mathbb{I}}$ and for all but finitely many $x \in \{0,1\}^*$, for any oracle A that avoids H, if

$$\Pr_{M,B}\left[A\restriction_{Q_M(x)} \subseteq B_x\restriction_{Q_M(x)}\right] \geq \frac{1}{2},$$

where $B_x(q) := B(x,q)$, then

$$\Pr_{M,B}\left[M^B(x) = \Pi(x)\right] \geq 1-\epsilon.$$

Let $p(n)$ be a polynomial that bounds the running time of M on inputs of length n. Let $\delta(n) := \epsilon/2p(n)$.

For any $x \in \{0,1\}^*$, let $\mathcal{Q}_x$ denote the query distribution of M on input x. Applying $\mathcal{Q}_x$ to Lemma 9.4, let f be the auxiliary-input function and let T^I be the approximation algorithm of $\mathcal{Q}_x(\text{-})$ that takes an inverter I of f as oracle.

Fix any input $x \in \mathrm{dom}(\Pi)$ and let $n := |x|$. Let $\theta = \theta(n)$ be a polynomial chosen later. We say that a string $q \in \{0,1\}^*$ is *light* (with respect to $\mathcal{Q}_x$) if

$$\mathcal{Q}_x(q) \leq \theta(n)\cdot 2^{-|q|}.$$

Similarly, we say that q is *heavy* if

$$\mathcal{Q}_x(q) \geq 4\theta(n) \cdot 2^{-|q|}.$$

If q is neither heavy nor light, then q is said to be *undetermined*. Define

$$\mathcal{L} := \{q \in \{0,1\}^* \mid q \text{ is light}\}.$$

We now construct a promise problem A that avoids H. For a query $q \in \{0,1\}^*$, we define the output $A(q)$ of A on input q as follows. Since M is an honest reduction, M makes no query of length n^γ on inputs of length n for some constant $\gamma > 0$. If $|q| < n^\gamma$, then we define $A(q) := 1$ if and only if $q \notin \mathrm{Im}(H)$. If $|q| \geq n^\gamma$, then we define

$$A(q) := \begin{cases} 1 & \text{if } q \text{ is light and } q \notin \mathrm{Im}(H), \\ 0 & \text{if } q \text{ is heavy or } q \in \mathrm{Im}(H), \\ * & \text{otherwise.} \end{cases}$$

For a randomized oracle I and an auxiliary input $x \in \{0,1\}^*$, define R_x^I to be the randomized algorithm that takes q as input, simulates T^I on input (x,q), and outputs 1 if and only if $T^I(x,q) < 2\theta(|x|) \cdot 2^{-|q|}$.

We now describe a reduction M'. The reduction M' takes x as input and oracle access to an inverter I of f, and outputs

$$M'^I(x) := M^{R_x^I}(x).$$

That is, M' simulates M on input x and answers any query q using the randomized algorithm R_x^I.

We establish the correctness of the reduction M' via a sequence of claims. Let $I \in \mathbb{I}$ be any randomized oracle. We define the randomized oracle $B \in \mathbb{BPP}^{\mathbb{I}}$ such that $B(x,q) := R_x^I(q)$ for every $x \in \{0,1\}^*$ and every $q \in \{0,1\}^*$. Fix any input $x \in \mathrm{dom}(\Pi)$ and assume that I inverts f on auxiliary input x.

Claim 9.5. *A avoids H.*

Proof. It is evident from the definition of A that $A(q) = 0$ for every $q \in \mathrm{Im}(H)$. We claim that for every $\ell \in \mathbb{N}$ such that $s(\ell) \leq \ell - 1$, the probability that $A(w) = 1$ over $w \sim \{0,1\}^\ell$ is at least $\frac{1}{2}$. If $\ell < n^\gamma$, the claim is obvious from the definition of A. If $\ell \geq n^\gamma$, then

$$\begin{aligned} \Pr_{w \sim \{0,1\}^\ell}[A(w) \neq 1] &\leq \Pr_w[w \in \mathrm{Im}(H)] + \Pr_w[w \text{ is not light}] \\ &\leq 2^{s(\ell)-\ell} + \frac{1}{\theta} \leq \frac{1}{2}, \end{aligned}$$

where the second inequality holds because

$$\Pr_{w \sim \{0,1\}^\ell}[w \text{ is not light}] \cdot \theta \;\leq \sum_{w \in \{0,1\}^\ell \setminus \mathcal{L}} \mathcal{Q}_x(w) = \Pr_{q \sim Q_x}\left[q \in \{0,1\}^\ell \setminus \mathcal{L}\right] \leq 1.$$

◇

Next, we prove that the reduction M cannot distinguish A from B_x.

Claim 9.6.

$$\Pr_{M,B}\left[A\restriction_{Q_M(x)} \not\subseteq B_x\restriction_{Q_M(x)}\right] \leq \epsilon.$$

Proof. We first bound the probability that a single query $q \sim \mathcal{Q}_x$ satisfies that $q \in \mathrm{dom}(A)$ and $A(q) \neq B_x(q)$. Since M is honest, the length of q is at least n^γ. Thus, if $q \in \mathrm{dom}(A)$ and $A(q) \neq B_x(q)$, then one of the following must be true.

1. $T^I(x,q) \notin (1 \pm \frac{1}{2}) \cdot \mathcal{Q}_x(q)$, or
2. $q \in \mathrm{Im}(H)$ and q is not heavy.

The first event happens with probability at most δ by Lemma 9.4. The probability of the second event is

$$\begin{aligned}
&\Pr_q[q \in \mathrm{Im}(H) \text{ and } q \text{ is not heavy}] \\
&= \Pr_q[q = h \text{ for some } h \in \mathrm{Im}(H) \text{ that is not heavy}] \\
&\leq \sum_{\ell\colon n^\gamma \leq \ell \leq p(n)} |\mathrm{Im}(H)| \cdot 4\theta \cdot 2^{-\ell} \leq p(n) \cdot n^{-\omega(1)} \cdot \theta,
\end{aligned}$$

where the last inequality holds because $\ell - s(\ell) \geq \omega(\log \ell)$.

By a union bound, we obtain

$$\Pr_{M,B}\left[A\restriction_{Q_M(x)} \not\subseteq B_x\restriction_{Q_M(x)}\right] \leq p(n) \cdot \left(\delta + n^{-\omega(1)}\right) \leq \epsilon$$

for all sufficiently large n. ◇

By Claim A.4 and the assumption on M, we obtain

$$\Pr_{M,B}\left[M^{B_x}(x) = \Pi(x)\right] \geq 1 - \epsilon.$$

We conclude that

$$\Pr_{M',I}\left[M'^I(x) \neq \Pi(x)\right] = \Pr_{M,R_x,I}\left[M^{R_x^I}(x) \neq \Pi(x)\right] = \Pr_{M,B}\left[M^{B_x}(x) \neq \Pi(x)\right] \leq \epsilon.$$

□

10 Auxiliary-Input One-Way Function to One-Way Function

We need the notion of errorless average-case easiness. The standard notion of average-case complexity classes is defined only for languages [BT06a]. We extend the notion to promise problems.

Definition 10.1. *Let Π be a promise problem and $\mathcal{D}$ be a family $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ of distributions. We call $(\Pi, \mathcal{D})$ a* distributional (promise) problem. *For a parameter $\epsilon > 0$, we write $(\Pi, \mathcal{D}) \in \mathsf{Avg}_\epsilon\mathsf{BPP}$ if there exists a randomized polynomial-time algorithm M such that for all sufficiently large $n \in \mathbb{N}$,*

$$\Pr_{x\sim\mathcal{D}_n, M}[M(1^n, x) = \bot] \leq \epsilon$$

and for every $x \in \mathrm{supp}(\mathcal{D}_n) \cap \mathrm{dom}(\Pi)$,

$$\Pr_M[M(1^n, x) \in \{\Pi(x), \perp\}] \geq 1 - \epsilon.$$

Similarly, $\mathsf{i.o.Avg}_\epsilon\mathsf{P/poly}$ *denotes the class of distributional problems for which there exists a polynomial-size circuit that computes* Π *with respect to* $\mathcal{D}_n$ *for infinitely many* $n \in \mathbb{N}$.

Using this notion, we may define an average-case analogue of $\mathbb{I}$-restricted reductions.

Definition 10.2. *Let* $\mathbb{I}$ *be a class of randomized oracles. For a family of functions*

$$g = \left\{ g_n : \{0,1\}^{s(n)} \to \{0,1\}^{t(n)} \right\}_{n \in \mathbb{N}},$$

we write

$$(\Pi, \mathcal{D}) \leq_{\mathrm{tt}}^{\mathsf{Avg}_\epsilon\mathsf{BPP}} \{I \mid I \text{ inverts } g\} \restriction \mathbb{I}$$

if there exists a randomized polynomial-time nonadaptive reduction M *such that for any* $I \in \mathbb{I}$*, for all sufficiently large* $n \in \mathbb{N}$*, for all* $x \in \mathrm{supp}(\mathcal{D}_n) \cap \mathrm{dom}(\Pi)$,

$$\Pr_{M,I}\left[M^I(1^n, x) \in \{\Pi(x), \perp\}\right] \geq 1 - \epsilon$$

and if I *inverts* g *on* 1^n*, then*

$$\Pr_{M,I,x \sim \mathcal{D}_n}\left[M^I(1^n, x) = \perp\right] \leq \epsilon.$$

Theorem 10.3. *Let* Π *be a promise problem and* f *be a polynomial-time-computable auxiliary-input family of functions. Let* $\mathbb{I}$ *be a class of randomized oracles. Assume that*

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \restriction \mathbb{BPP}^{\mathbb{I}}.$$

Then, there exists a polynomial-time-computable family $g = \{g_n : \{0,1\}^n \to \{0,1\}^n\}_{n \in \mathbb{N}}$ *of functions such that*

$$(\Pi, \mathcal{D}) \leq_{\mathrm{tt}}^{\mathsf{Avg}_\epsilon\mathsf{BPP}} \{I \mid I \text{ inverts } g\} \restriction \mathbb{I}$$

for every polynomial-time samplable distribution $\mathcal{D}$ *and every constant* $\epsilon > 0$.

Proof. Let

$$f = \left\{ f_x : \{0,1\}^{s(|x|)} \to \{0,1\}^{t(|x|)} \right\}_{x \in \{0,1\}^*}.$$

We construct a candidate one-way function

$$g = \left\{ g_n : \{0,1\}^{s'(n)} \to \{0,1\}^{t'(n)} \right\}_{n \in \mathbb{N}}$$

based on the auxiliary-input one-way function f. Let M be the $\mathbb{I}$-restricted reduction from Π to any inverter for f. For every $n \in \mathbb{N}$, the output of g_n is defined by the following sampling procedure: Pick $x \sim \mathcal{D}_n$ and $z \sim \{0,1\}^{s(|x|)}$ randomly and output $(x, f_x(z))$. The input of g_n is uniformly random bits that are used to simulate this sampling procedure. For an input r of g_n, let $z_r \in \{0,1\}^{s(x)}$ denote the input for $f_x(\text{-})$.

Let g_n^k denote the k-wise direct product of g_n. By the hardness amplification theorem for a one-way function [Yao82; Gol01], there exists a randomized polynomial-time oracle algorithm R such that R^I inverts g_n with success probability $1-\delta(n)^2$ for any randomized oracle I that inverts g_n^k with success probability $\frac{1}{2}$, where $k = k(n) = \mathsf{poly}(1/\delta(n))$. Here, $\delta = \delta(n)$ is a parameter such that $1/\delta(n) \leq n^{O(1)}$. The parameter will be chosen later.

Let $I \in \mathbb{I}$. Fix $n \in \mathbb{N}$ such that I inverts g_n^k. By hardness amplification, R^I inverts g_n with success probability at least $1-\delta(n)^2$. Let $\widehat{I}$ denote R^I. Then, we have

$$\Pr_{r,\widehat{I}}\left[\widehat{I}(1^n, g_n(r)) \in g_n^{-1}(g_n(r))\right] \geq 1-\delta(n)^2.$$

By the definition of g_n, we obtain

$$\Pr_{x\sim\mathcal{D}_n, z\sim\{0,1\}^{s(|x|)}, \widehat{I}}\left[\widehat{I}(1^n, x, f_x(z)) \in f_x^{-1}(f_x(z))\right] \geq 1-\delta(n)^2.$$

We now describe an average-case reduction H from $(\Pi, \mathcal{D})$ to I. On input $(1^n, x)$, where $x \in \mathrm{supp}(\mathcal{D}_n)$, H^I simulates M^I on input x. Let $b \in \{0,1\}$ be the output of $M^I(x)$. Using random sampling, H^I estimates

$$v := \Pr_{z\sim\{0,1\}^{s(|x|)}, \widehat{I}}\left[\widehat{I}(1^n, x, f_x(z)) \in f_x^{-1}(f_x(z))\right].$$

Let $\widetilde{v}$ denote the estimated value. By a concentration inequality, with probability at least $1-\delta$, it holds that $|\widetilde{v} - v| \leq \epsilon$. If $\widetilde{v} \geq 1-2\epsilon$, then H^I outputs b. Otherwise, H^I outputs $\perp$.

Assume that I inverts g^k on 1^n. We claim that

$$\Pr_{x\sim\mathcal{D}_n, H, I}\left[H^I(1^n, x) = \perp\right] \leq 2\delta.$$

By Markov's inequality, with probability at least $1-\delta$ over a choice of $x \sim \mathcal{D}_n$, it holds that

$$v = \Pr_{z,\widehat{I}}\left[\widehat{I}(1^n, x, f_x(z)) \in f_x^{-1}(f_x(z))\right] \geq 1-\delta.$$

Moreover, with probability at least $1-\delta$ over the internal randomness of H, we have $|\widetilde{v} - v| \leq \epsilon$. Thus, with probability at least $1-2\delta$, we have $\widetilde{v} \geq 1-2\epsilon$. The claim follows.

Next, we claim that for every $x \in \mathrm{dom}(\Pi) \cap \mathrm{supp}(\mathcal{D}_n)$, if

$$\Pr_{H,I}\left[H^I(1^n, x) \neq \perp\right] \geq \epsilon,$$

then

$$\Pr_{H,I}\left[H^I(1^n, x) = \Pi(x)\right] \geq 1-\epsilon.$$

Note that $|\widetilde{v} - v| \leq \epsilon$ with probability at least $1-\delta$ over the internal randomness of H. Thus, under assumption, with probability at least $\epsilon - \delta \geq \epsilon/2$, it holds that H^I outputs $\perp$ and $\widetilde{v} - v \leq \epsilon$; thus, $v \geq \widetilde{v} - \epsilon \geq 1-3\epsilon$. Thus,

$$v = \Pr_{z,\widehat{I}}\left[\widehat{I}(1^n, x, f_x(z)) \in f_x^{-1}(f_x(z))\right] \geq 1-3\epsilon.$$

It follows from the property of M that

$$\Pr_{M,I}\bigl[M^I(x) = \Pi(x)\bigr] \geq 1 - \epsilon.$$

Thus, we also have

$$\Pr_{H,I}\bigl[H^I(x) \in \{\Pi(x), \bot\}\bigr] \geq 1 - \epsilon.$$

To complete the proof, we prove

$$\Pr_{H,I}\bigl[H^I(x) \notin \{\Pi(x), \bot\}\bigr] \leq \epsilon$$

by analyzing the following two cases. If $\Pr\bigl[H^I(1^n, x) \neq \bot\bigr] \geq \epsilon$, then the argument above shows $\Pr\bigl[H^I(1^n, x) = \Pi(x)\bigr] \geq 1 - \epsilon$. If $\Pr\bigl[H^I(1^n, x) \neq \bot\bigr] \leq \epsilon$, then we have $\Pr\bigl[H^I(1^n, x) = \bot\bigr] \geq 1 - \epsilon$. □

Corollary 10.4. *Under the same assumption with Theorem 10.3, the following hold for every constant $\epsilon > 0$ and every polynomial-time samplable distribution $\mathcal{D}$.*

1. *If $\mathbb{I} = \mathsf{P/poly}$ and $(\Pi, \mathcal{D}) \notin \mathsf{i.o.Avg}_\epsilon\mathsf{P/poly}$, then there exists a one-way function secure against polynomial-size circuits.*
2. *If $\mathbb{I} = \mathbb{BPP}$ and $(\Pi, \mathcal{D}) \notin \mathsf{Avg}_\epsilon\mathsf{BPP}$, then there exists a one-way function secure against BPP infinitely often.*

Proof. We prove the contrapositive. Since

$$(\Pi, \mathcal{D}) \leq_{\mathrm{tt}}^{\mathsf{Avg}_\epsilon\mathsf{BPP}} \{I \mid I \text{ inverts } g\} \restriction \mathbb{I},$$

if there exists a $\mathsf{P/poly}$ algorithm I that inverts g on 1^n for infinitely many n, then combining I with the reduction, we obtain $(\Pi, \mathcal{D}) \in \mathsf{Avg}_\epsilon\mathsf{P/poly}$.

Similarly, if there exists a randomized polynomial-time algorithm that inverts I on 1^n for all but finitely many n, then $(\Pi, \mathcal{D}) \in \mathsf{Avg}_\epsilon\mathsf{BPP}$. □

11 Proofs of Main Results

The main result of this paper is formally stated as follows.

Theorem 11.1. *The following are equivalent.*

1. *There exists a one-way function secure against polynomial-size circuits.*
2. *$\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$ and $\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \bigl\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^A \mid \tau\colon \text{a polynomial}, A \in \mathsf{P/poly}\bigr\}$ with parametric-honest reductions for some constant $\epsilon > 0$.*
3. *$\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$ and $\mathsf{NP} \leq_{\mathrm{m}}^{\mathsf{coRP}} \bigl\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^A \mid \tau\colon \text{a polynomial}, A \in \mathsf{P/poly}\bigr\}$ with parametric-honest reductions for some $\epsilon(n) = n^{1/(\log\log n)^{O(1)}}$.*

We need a simple proposition that transforms parametric-honest reductions into size-expanding reductions.

Proposition 11.2. *If* $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}$ *is* NP*-hard under parametric-honest reductions, then* $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}$ *is* NP*-hard under size-expanding reductions.*

Proof. Let $L = \left\{\varphi 01^t \;\middle|\; \varphi \in \mathrm{SAT}, t \in \mathbb{N}\right\}$ be a paddable NP-complete problem. By assumption, L is reducible to $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}$ via a parametric-honest reduction M. The size parameter s in any query of M on input $\varphi 01^t$ is at least $|\varphi 01^t|^\gamma$ for some constant $\gamma > 0$. Choosing $t := |\varphi|^{2/\gamma}$, we obtain a size-expanding reduction. □

Proof of Theorem 11.1. Item 1 ⇒ 3 follows from Theorem 6.3. Item 3 ⇒ 2 is obvious.

We prove Item 2 ⇒ 1. By Proposition 11.2, parametric-honest reductions can be made size-expanding reductions. By Theorem 8.16, we have

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\right\} \upharpoonright \mathbb{BPP}/\mathsf{poly} /\!\!/ n.$$

By Theorem 9.3, there exists a polynomial-time-computable auxiliary-input function $f = \{f_x\}_{x\in\{0,1\}^*}$ such that

$$\mathsf{NP} \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{BPP}/\mathsf{poly}.$$

Since $\mathsf{NP} \not\subseteq \mathsf{i.o.P}/\mathsf{poly}$, this induces the existence of an auxiliary-input one-way function. In particular, this implies the existence of a hitting set generator [Hir18; Nan21]. Let L be the image of $\mathcal{H}^{\mathrm{univ}}$. Then, using that the number of YES instances in L is small, we obtain $(L, \mathcal{U}) \notin \mathsf{i.o.Avg}_\epsilon\mathsf{P}/\mathsf{poly}$ for some constant $\epsilon > 0$ [HS17; Hir18] (see also Proposition 11.8). Since $L \in \mathsf{NP}$, we have

$$L \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{BPP}/\mathsf{poly}.$$

By Corollary 10.4, there exists a one-way function secure against polynomial-size circuits.

□

11.1 Generalizing Ostrovsky's Theorem

Ostrovsky [Ost91] showed that for every promise problem $\Pi \in \mathsf{SZK}$, the worst-case hardness of Π implies the existence of an auxiliary-input one-way function. We extend this to every promise problem Π that is reducible to GapMdpKP via a size-expanding reduction.

Theorem 11.3. *Let* Π *be a promise problem such that*

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdpKP}\right\}_{\tau\in\mathsf{poly}}$$

under size-expanding reductions for some constant $\epsilon > 0$*. Then,*

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \textit{ inverts } f\} \upharpoonright \mathbb{BPP}.$$

for some auxiliary-input family f *of functions.*

Proof. By Theorem 8.17, we obtain

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{A \;\middle|\; A \text{ avoids } \mathcal{H}^{\mathrm{univ}}\right\} \upharpoonright \mathbb{BPP} /\!\!/ n.$$

It follows from Theorem 9.3 that

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{BPP}$$

for some auxiliary-input family f of functions. □

Since SZK is reducible to $\mathrm{K}^{\mathsf{poly}}$ [AGHR21], Theorem 11.3 generalizes [Ost91].

11.2 On the Meta-Complexity Padding Conjecture

Next, we give a formal statement of the Meta-Complexity Padding Conjecture.

Conjecture 11.4 (The Meta-Complexity Padding Conjecture)**.** *For any polynomial p, there exist constants $\epsilon, \delta > 0$ such that*

$$\mathrm{Gap}_{\delta}(\mathrm{K}^{p} \text{ vs } \mathrm{K}) \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{ \mathrm{Gap}_{\tau,\epsilon}\mathrm{MdpKP} \;\middle|\; \tau \colon \textit{a polynomial} \right\}$$

via a size-expanding reduction.

Definition 11.5. *For a constant $\epsilon > 0$, the promise problem $\mathrm{Gap}_{\epsilon}\mathrm{MCSP} = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ is defined as follows.*

$$\begin{aligned} \Pi_{\mathrm{YES}} &:= \{(f, 1^s) \mid \mathsf{CC}(f) \leq s\}, \\ \Pi_{\mathrm{NO}} &:= \left\{(f, 1^s) \;\middle|\; \mathsf{CC}(f) \geq s \cdot |f|^{1-\epsilon}\right\}, \end{aligned}$$

where $|f|$ denotes the length 2^n of the truth table of $f \colon \{0,1\}^n \to \{0,1\}$. For a polynomial p, the promise problem $\mathrm{Gap}(\mathrm{q}^t \text{ vs } \mathrm{rK}^{p(t)}) = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ is defined as follows.

$$\begin{aligned} \Pi_{\mathrm{YES}} &:= \left\{(x, 1^t, 1^s) \;\middle|\; t \geq |x| \text{ and } \mathrm{q}^t(x) \leq s\right\}, \\ \Pi_{\mathrm{NO}} &:= \left\{(x, 1^t, 1^s) \;\middle|\; t \geq |x| \text{ and } \mathrm{rK}^{p(t)}(x) \geq p(s)\right\}. \end{aligned}$$

We define $\mathrm{Gap}(\mathrm{q}^t \text{ vs } \mathrm{q}^{p(t)})$ and $\mathrm{Gap}(\mathrm{rK}^t \text{ vs } \mathrm{rK}^{p(t)})$ in a similar way.

These problems can be reduced to DistNP.

Lemma 11.6 ([Hir18])**.** *If there exists no hitting set generator of seed length n^{δ} secure against randomized polynomial-time infinitely often for some constant $\delta > 0$, then $\mathrm{Gap}_{\epsilon}\mathrm{MCSP} \in \text{pr-}\mathsf{BPP}$ for some constant $\epsilon > 0$ and $\mathrm{Gap}(\mathrm{q}^t \text{ vs } \mathrm{rK}^{p(t)}) \in \text{pr-}\mathsf{BPP}$ for some polynomial p.*

We are ready to state the consequence of the Meta-Complexity Padding Conjecture formally.

Theorem 11.7. *Under the Meta-Complexity Padding Conjecture, the following are equivalent.*

1. *There exists a one-way function secure against randomized polynomial-time algorithms infinitely often.*
2. $\mathrm{Gap}_{\epsilon}\mathrm{MCSP} \notin \text{pr-}\mathsf{BPP}$ *for every constant $\epsilon > 0$.*
3. $\mathrm{Gap}(\mathrm{q}^t \text{ vs } \mathrm{rK}^{p(t)}) \notin \text{pr-}\mathsf{BPP}$ *for every polynomial p.*
4. $\mathrm{Gap}(\mathrm{q}^t \text{ vs } \mathrm{q}^{p(t)}) \notin \text{pr-}\mathsf{BPP}$ *for every polynomial p.*
5. $\mathrm{Gap}(\mathrm{rK}^t \text{ vs } \mathrm{rK}^{p(t)}) \notin \text{pr-}\mathsf{BPP}$ *for every polynomial p.*
6. *For every constant $\epsilon > 0$, there exists a polynomial-time-computable hitting set generator*

   $$H = \left\{H_n : \{0,1\}^{n^{\epsilon}} \to \{0,1\}^n\right\}_{n \in \mathbb{N}}$$

   secure against randomized polynomial-time algorithms infinitely often.

7. *There exists a pseudorandom generator secure against randomized polynomial-time algorithms infinitely often.*

8. *Natural properties useful against* $\mathsf{SIZE}(2^{\epsilon n})$ *do not exist for every constant* $\epsilon > 0$.

We recall the fact that the existence of a hitting set generator implies the errorless average-case hardness of $\mathrm{K}^{\mathsf{poly}}$.

Proposition 11.8 ([Hir18])**.** *Let* $H = \left\{H_n : \{0,1\}^{n^{\delta_0}} \to \{0,1\}^n\right\}_{n\in\mathbb{N}}$ *be a polynomial-time computable family of functions for some constant* $\delta_0 \in (0,1)$*. Then, there exist constants* $\delta, \epsilon \in (0,1)$ *and a polynomial* p *such that for any polynomial* $q \geq p$*, if* $(\mathrm{Gap}_\delta(\mathrm{K}^q \text{ vs } \mathrm{K}), \mathcal{U}) \in \mathsf{Avg}_\epsilon\mathsf{BPP}$*, then there exists a promise problem* $\Pi \in \text{pr-}\mathsf{BPP}$ *such that* Π *avoids* H*.*

Proof. Let p be a polynomial such that $\mathrm{K}^{p(n)}(x) \leq n^\delta$ for any $x \in \mathrm{Im}(H_n)$. Let $\epsilon := \frac{1}{16}$.

Let M be the randomized polynomial-time errorless heuristic algorithm for $(\mathrm{Gap}_\delta(\mathrm{K}^q \text{ vs } \mathrm{K}), \mathcal{U})$. Define a randomized algorithm M' as follows. For $n \in \mathbb{N}$ and $x \in \{0,1\}^n$, we define $M'(x) := 1$ if $M(1^n, x) = 0$ and $M'(x) := 0$ if $M(1^n, x) \in \{1, \bot\}$.

Consider any $x \in \mathrm{Im}(H_n)$. Then, x is a YES instance of $\mathrm{Gap}_\delta(\mathrm{K}^p \text{ vs } \mathrm{K})$. Thus, it holds that

$$\Pr_M[M(1^n, x) \in \{1, \bot\}] \geq 1 - \epsilon,$$

which implies that

$$\Pr_{M'}\big[M'(x) = 0\big] \geq 1 - \epsilon.$$

Now, for a random $x \sim \{0,1\}^n$, we would like to bound the probability that $M'(x) = 0$. This event is equivalent to $M(1^n, x) \in \{1, \bot\}$. Thus, we have

$$\Pr_{x\sim\{0,1\}^n, M'}\big[M'(x) = 0\big] \leq \Pr_{x\sim\{0,1\}^n, M}[M(1^n, x) = \bot] + \Pr_{x\sim\{0,1\}^n, M}[M(1^n, x) = 1].$$

The first term is at most ϵ. To bound the second term, observe that the event of the second term happens only if either $\Pi(x) \in \{1, *\}$ or $\Pi(x) = 0$ and $M(1^n, x) = 1$. The first event happens with probability at most $\frac{1}{4}$ by Fact 5.5. The second event happens only if $M(1^n, x) \notin \{\Pi(x), \bot\}$, which happens with probability at most ϵ by the property of M. Overall, we obtain

$$\Pr_{x\sim\{0,1\}^n, M'}\big[M'(x) = 0\big] \leq 2\epsilon + \frac{1}{4} \leq \frac{3}{8}.$$

By an averaging argument, it holds that

$$\Pr_{x\sim\{0,1\}^n}\left[\Pr_{M'}\big[M'(x) = 1\big] \geq \frac{1}{8}\right] \geq \frac{1}{2}. \tag{13}$$

We define a promise problem $\Pi = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$ as follows. Π_{NO} consists of $x \in \{0,1\}^*$ such that $\mathrm{K}^{p(n)}(x) \leq |x|^\delta$. Π_{YES} consists of $x \in \{0,1\}^*$ such that

$$\Pr_{M'}\big[M'(x) = 1\big] \geq \frac{1}{8}.$$

Then, by Eq. (13), we have

$$\Pr_{x\sim\{0,1\}^n}[\Pi(x) = 1] \geq \frac{1}{2}.$$

The arguments above show that any $x \in \Pi_{\mathrm{YES}}$ is accepted by M' with probability at least $\frac{1}{8}$ and that any $x \in \Pi_{\mathrm{NO}}$ is accepted by M' with probability at most ϵ. The gap between ϵ and $\frac{1}{8}$ can be amplified by a standard proof technique. Thus, we obtain $\Pi \in$ pr-BPP. □

Proof of Theorem 11.7. Using the Meta-Complexity Padding Conjecture, let $\Pi := \mathrm{Gap}_{\delta}(\mathrm{K}^t \text{ vs } \mathrm{K})$ such that

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \left\{\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdpKP}\right\}_{\tau \in \mathsf{poly}}.$$

via a size-expanding reduction for some constant $\epsilon > 0$. By Theorem 11.3,

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathbb{BPP}$$

for some auxiliary-input family f of functions. By Theorem 10.3, we obtain

$$(\Pi, \mathcal{U}) \leq_{\mathrm{tt}}^{\mathsf{Avg}_{\epsilon}\mathsf{BPP}} \{I \mid I \text{ inverts } g\} \upharpoonright \mathbb{BPP} \tag{14}$$

for some polynomial-time-computable function g.

Item 1 ⇒ 2 is proved by [ABKMR06] (based on the proof techniques of [GGM86; RR97]). Item 1 ⇒ 4 and Item 1 ⇒ 5 can be proved in a similar way.

Item 4 ⇒ 3 and Item 5 ⇒ 3 are obvious.

Item 2 ⇒ 6 and Item 3 ⇒ 6 is due to Lemma 11.6.

We prove Item 6 ⇒ 1. By Proposition 11.8, for every constant $\epsilon > 0$, $(\mathrm{Gap}_{\epsilon}(\mathrm{K}^t \text{ vs } \mathrm{K}), \mathcal{U}) \notin \mathsf{Avg}_{\epsilon_0}\mathsf{BPP}$. In particular, we have

$$(\Pi, \mathcal{U}) \notin \mathsf{Avg}_{\epsilon_0}\mathsf{BPP}$$

for some constant $\epsilon_0 > 0$. By Eq. (14), this implies that g is a one-way function.

The equivalence between Items 1 and 7 is due to [HILL99]. The equivalence between Items 2 and 8 is due to [Hir18]. □

Finally, we prove the Meta-Complexity Padding Conjecture under the existence of a one-way function.

Reminder of Proposition 1.6. If there exists a one-way function secure against polynomial-size circuits, then the Meta-Complexity Padding Conjecture is true.

Proof Sketch. By Theorem 6.3, $\mathrm{Gap}_{\tau,\alpha}\mathrm{MdKP}^A$ is NP-hard under size-expanding reductions for all polynomials τ, all constants α, and all oracles $A \in \mathsf{P/poly}$. By Lemma 8.15, the same NP-hardness reduction shows NP-hardness of $\mathrm{Gap}_{\tau,\alpha}\mathrm{MdpKP}$ for all polynomials τ and constants α. □

A Another Proof of HSG to Auxiliary-Input OWF

In this appendix, we present an alternative approach of transforming a reduction to avoiding a hitting set generator into a reduction to inverting an auxiliary-input one-way function. Theorem 9.3 shows that a reduction to the class of *promise problems* that avoid a hitting set generator can be transformed. Here, we show that P/poly-restricted reductions to the class of *oracles* that avoid H can be transformed.

Theorem A.1. *Let $\mathbb{A}$ be the class of* oracles $A \subseteq \{0,1\}^*$ *that avoid H. Let Π be a promise problem and*

$$H = \left\{ H_n : \{0,1\}^{s(n)} \to \{0,1\}^n \right\}_{n \in \mathbb{N}}$$

be an arbitrary family of functions such that $s(n) < n - \omega(\log n)$. If

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \mathbb{A} \upharpoonright \mathsf{P/poly} /\!\!/ 2n$$

via an honest reduction, then there exists a polynomial-time-computable auxiliary-input function $f = \{f_x\}_{x \in \{0,1\}^*}$ such that

$$\Pi \leq_{\mathrm{tt}}^{\mathsf{BPP}} \{I \mid I \text{ inverts } f\} \upharpoonright \mathsf{FP/poly}.$$

Here, $\mathsf{FP/poly}$ denotes the class of multi-output polynomial-size circuits.

Proof of Theorem 9.3. Let $\epsilon > 0$ be a sufficiently small constant. Let M be a randomized polynomial-time $\mathbb{B}$-restricted reduction from Π to $\mathbb{A}$ with success probability $1 - \epsilon$. Let $p(n)$ be a polynomial that bounds the running time of M on inputs of length n. Let $\delta(n) := (\epsilon/p(n))^2$.

For any $x \in \{0,1\}^*$, let $\mathcal{Q}_x$ denote the query distribution of M on input x. Applying $\mathcal{Q}_x$ to Lemma 9.4, let f be the auxiliary-input function and let T^I be the approximation algorithm of $\mathcal{Q}_x(\text{-})$ that takes an inverter I of f as oracle.

Fix any input $x \in \mathrm{dom}(\Pi)$ and let $n := |x|$. For a threshold $\theta \in \mathbb{R}$, we say that a string $q \in \{0,1\}^*$ is *θ-light* (with respect to $\mathcal{Q}_x$) if

$$\mathcal{Q}_x(q) \leq \theta \cdot 2^{-|q|}.$$

Otherwise, q is said to be *θ-heavy*.

Let $\theta_0 := p(n)/\epsilon$ and let δ denote $\delta(n)$. Let $\mathcal{A}_n := \left\{ \theta_0 \cdot (1+6\delta)^i \;\middle|\; i \leq 1/\delta \right\}$. We choose a threshold $\theta \sim \mathcal{A}_n$ randomly. Then, as in [BT06b; HW20], it follows from Markov's inequality that with probability at least $1 - \sqrt{\delta}$ over a choice of $\theta \sim \mathcal{A}_n$,

$$\Pr_{q \sim \mathcal{Q}_x} \left[\mathcal{Q}_x(q) \in (1 \pm 2\delta) \cdot \theta 2^{-|q|} \right] \leq \sqrt{\delta}. \tag{15}$$

Note that $\theta \leq O(\theta_0)$. In what follows, we fix θ such that Eq. (15) holds.

Fix any $I \in \mathsf{FP/poly}$. Let $G_I \subseteq \{0,1\}^*$ be the set of instances x such that I inverts f on auxiliary input x.

Claim A.2. *There exists $B \in \mathsf{P/poly}$ such that for every $x \in G_I$, with probability at least $1 - \delta(|x|)$ over a random choice of $q \sim \mathcal{Q}_x$, for every $\theta \in \mathcal{A}_n$,*

1. *if $\mathcal{Q}_x(q) \leq (1-2\delta) \cdot \theta 2^{-|q|}$, then $B(x,\theta,q) = 1$ and*
2. *if $\mathcal{Q}_x(q) \geq (1+2\delta) \cdot \theta 2^{-|q|}$, then $B(x,\theta,q) = 0$.*

Proof. By Lemma 9.4, for every $x \in G$, it holds that

$$\Pr_{q \sim \mathcal{Q}_x, T, I} \left[T^I(x,q) \in (1 \pm \delta(|x|)) \cdot \mathcal{Q}_x(q) \right] \geq 1 - \delta(|x|).$$

Using a standard technique of amplifying the success probability of randomized approximation algorithms, the success probability with respect to the randomness of T can be amplified to exponentially close to 1. By a union bound over all $x \in G$, we obtain a *deterministic* polynomial-size circuit $T_* \in \mathsf{P/poly}$ such that for all $x \in G$,

$$\Pr_{q \sim \mathcal{Q}_x}[T_*(x,q) \in (1 \pm \delta(|x|)) \cdot \mathcal{Q}_x(q)] \geq 1 - \delta(|x|).$$

Define B to be the oracle such that

$$B := \left\{ (x, \theta, q) \;\middle|\; T_*(x,q) \leq \theta \cdot 2^{-|q|} \right\}.$$

Since $T_* \in \mathsf{P/poly}$, we also have $B \in \mathsf{P/poly}$.

Assuming that $T_*(x,q) \in (1 \pm \delta) \cdot \mathcal{Q}_x(q)$, we observe that the two items are satisfied: If $\mathcal{Q}_x(q) \leq (1-2\delta) \cdot \theta 2^{-|q|}$, then we obtain

$$T_*(x,q) \leq (1+\delta) \cdot (1-2\delta) \cdot \theta 2^{-|q|} \leq \theta 2^{-|q|}.$$

Similarly, if $\mathcal{Q}_x(q) \geq (1+2\delta) \cdot \theta 2^{-|q|}$, then we obtain

$$T_*(x,q) \geq (1-\delta) \cdot (1+2\delta) \cdot \theta 2^{-|q|} > \theta 2^{-|q|}.$$

This completes the proof of the claim. ◇

Note that θ can be encoded as a binary string of length $O(\log |\mathcal{A}_n|) = O(\log n)$. Thus, in total, the advice string $a := (x, \theta)$ can be encoded with at most $|x| + O(\log n) \leq 2n$ bits.

Let G'_x denote the set of (θ, q) such that the two items of Claim A.2 are satisfied.

Define

$$\mathcal{L}_\theta := \{q \in \{0,1\}^* \mid q \text{ is } \theta\text{-light } \}.$$

We now construct an oracle A that avoids H. For a query $q \in \{0,1\}^*$, we define the output $A(q)$ of A on input q as follows. Since M is an honest reduction, M makes no query of length n^γ on inputs of length n for some constant $\gamma > 0$. If $|q| < n^\gamma$, then $A(q) := 1$ if and only if $q \notin \mathrm{Im}(H)$. If $|q| \geq n^\gamma$, then we define

$$q \in A \quad \Longleftrightarrow \quad q \in \mathcal{L}_\theta \setminus \mathrm{Im}(H).$$

For a randomized algorithm T_0, define R^{T_0} to be the randomized algorithm that takes q as input, simulates T_0 on input (x,q), and outputs 1 if and only if $T_0(x,q) \leq \theta \cdot 2^{-|q|}$.

We now describe a reduction M'. The reduction M' takes x as input and oracle access to an inverter I of f, and outputs

$$M'^I(x) := M^{R^{T^I}}(x).$$

That is, M' simulates M on input x and answers any query q using the randomized algorithm R^{T^I}.

We establish the correctness of the reduction M' via a sequence of claims.

Claim A.3. *A avoids H.*

Proof. It is evident from the definition of A that $A \cap \mathrm{Im}(H) = \emptyset$. We claim that the size of $A \cap \{0,1\}^\ell$ is at least $2^{\ell-1}$ for every $\ell \in \mathbb{N}$ such that $s(\ell) \le \ell - 1$. If $\ell < n^\gamma$, the claim is obvious from the definition of A. If $\ell \ge n^\gamma$, then

$$\begin{aligned}\Pr_{w \sim \{0,1\}^\ell}[w \notin A] &\le \Pr[w \in \mathrm{Im}(H)] + \Pr[w\colon \theta\text{-heavy}] \\ &\le 2^{s(\ell)-\ell} + \frac{1}{\theta} \le \frac{1}{2},\end{aligned}$$

where the second inequality holds because

$$\Pr_{w \sim \{0,1\}^\ell}[w\colon \theta\text{-heavy}] \cdot \theta \ \le \sum_{w \in \{0,1\}^\ell \setminus \mathcal{L}_\theta} \mathcal{Q}_x(w) = \Pr_{q \sim Q_x}\left[q \in \{0,1\}^\ell \setminus \mathcal{L}_\theta\right] \le 1.$$

◇

Next, we prove that the reduction M cannot distinguish A from $B_{x,\theta}$.

Claim A.4. *If $x \in G$, then*

$$\Pr_M\left[A\restriction_{Q_M(x)} \not\subseteq B_{x,\theta}\restriction_{Q_M(x)}\right] \le \epsilon.$$

Similarly,

$$\Pr_{M,T,I}\left[M^{R^{T^I}}(x) \ne M^A(x)\right] \le \epsilon.$$

Proof. We first bound the probability that a single query $q \sim \mathcal{Q}_x$ satisfies $A(q) \ne B_{x,\theta}(q)$. Let q be any query of length at least n^γ. If $A(q) \ne B_{x,\theta}(q)$, then one of the following must be true.

1. $(\theta, q) \notin G'_x$,
2. $\mathcal{Q}_x(q) \in (1 \pm 2\delta) \cdot \theta 2^{-|q|}$, or
3. $q \in \mathrm{Im}(H)$ and q is θ-light.

The first event happens with probability at most δ by Claim A.2. The second event happens with probability at most $\sqrt{\delta}$ by Eq. (15). The probability of the third event is

$$\begin{aligned}&\Pr_q[q \in \mathrm{Im}(H) \text{ and } q \in \mathcal{L}_\theta] \\ &= \Pr_q[q = h \text{ for some } h \in \mathrm{Im}(H) \cap \mathcal{L}_\theta] \\ &\le \sum_{\ell\colon n^\gamma \le \ell \le p(n)} |\mathrm{Im}(H)| \cdot \theta \cdot 2^{-\ell} \le p(n) \cdot n^{-\omega(1)} \cdot \theta,\end{aligned}$$

where the last inequality holds because $\ell - s(\ell) \ge \omega(\log \ell)$.

By a union bound, we obtain

$$\Pr\left[A\restriction_{Q_M(x)} \not\subseteq B_{x,\theta}\restriction_{Q_M(x)}\right] \le p(n) \cdot \left(\delta + \sqrt{\delta} + n^{-\omega(1)}\right) \le \epsilon$$

for all sufficiently large n.

To see the "similarly" part, observe that the event happens only if $R^{T^I}(q) \ne A(q)$ for some $q \in Q_M(x)$. The probability that this event happens can be bounded in the same way. ◇

By Claim A.4 and the assumption on M, we obtain

$$\Pr_{M}\left[M^{A}(x) = \Pi(x)\right] \geq 1 - \epsilon.$$

Now, we have

$$\begin{aligned}\Pr_{M',I}\left[M'^{I}(x) \neq \Pi(x)\right] &= \Pr_{M,T,I}\left[M^{R^{T^{I}}}(x) \neq \Pi(x)\right] \\ &\leq \Pr_{M,T,I}\left[M^{R^{T^{I}}}(x) \neq M^{A}(x)\right] + \Pr_{M}\left[M^{A}(x) \neq \Pi(x)\right] \\ &\leq 2\epsilon.\end{aligned}$$

□

B Distributional randomized Kolmogorov complexity

In this appendix, we present a non-black-box reduction from the problem of approximating $\mathrm{drK}^{\mathsf{poly}}_{\lambda}$ to $\mathrm{Gap}_{\tau,\alpha}(\mathrm{q}-\mathrm{rK}^{B}\text{ vs }\mathrm{crK}^{B})$. The parameter λ of this reduction has a large error.

Theorem B.1. *For every polynomial p, there exists a polynomial τ such that for any randomized oracles B and B', the promise problem $\mathrm{Gap}_{\tau}(\mathrm{q}-\mathrm{rK}^{B}\text{ vs }\mathrm{drK}^{B}) = (\Pi^{B'}_{\textsc{Yes}}, \Pi^{B}_{\textsc{No}})$ defined as*

$$\begin{aligned}\Pi^{B'}_{\textsc{Yes}} &:= \left\{(x, \mathcal{D}, 1^{t}, 1^{s}) \;\middle|\; t \geq |x| + |y| \text{ and } \mathrm{q}^{t}(x, y) - \mathrm{rK}^{\tau(t),B'}(y) \leq s \text{ for every } y \in \mathrm{supp}(\mathcal{D})\right\}, \\ \Pi^{B}_{\textsc{No}} &:= \left\{(x, \mathcal{D}, 1^{t}, 1^{s}) \;\middle|\; t \geq |x| + |y| \text{ and } \mathrm{drK}^{\tau(t),B}_{1/8|x|}(x \mid \mathcal{D}) > s + \log^{3}\tau(t) \text{ for every } y \in \mathrm{supp}(\mathcal{D})\right\}\end{aligned}$$

satisfies

$$\mathrm{Gap}_{\tau}(\mathrm{q}-\mathrm{rK}^{B}\text{ vs }\mathrm{drK}^{B}) \leq^{\mathsf{BPP}}_{\mathrm{tt}} \mathrm{Gap}_{p}(\mathrm{q}-\mathrm{rK}^{B'}\text{ vs }\mathrm{crK}^{B'}) \restriction B.$$

Moreover, the reduction is independent of B and B'.

Proof. Let $\Pi := \mathrm{Gap}_{p}(\mathrm{q}-\mathrm{rK}^{B'}\text{ vs }\mathrm{crK}^{B'})$. We describe a B-restricted reduction M from $\mathrm{Gap}_{\tau}(\mathrm{q}-\mathrm{rK}^{B}\text{ vs }\mathrm{drK}^{B})$ to Π. The reduction M^{B} takes $(x, \mathcal{D}, 1^{t}, 1^{s})$ as input, picks $y \sim \mathcal{D}$ and $z \sim \{0,1\}^{d}$ randomly, and accepts if and only if

$$B(G_{k}(x; z), y, 1^{t'}, 1^{s'}) = 1$$

for some parameters k, t' and s'. The reduction makes an additional query $(w, y, 1^{t'}, 1^{s'})$ for a random $w \sim \{0,1\}^{k}$.

To prove the correctness of M, assume that

$$\Pr_{M}\left[\Pi\restriction_{Q_{M}(x)} \subseteq B\restriction_{Q_{M}(x)}\right] \geq 1 - \epsilon$$

for a small constant $\epsilon > 0$.

Consider any $\textsc{Yes}$ instance $(x, \mathcal{D}, 1^{t}, 1^{s})$ of $\mathrm{Gap}_{\tau}(\mathrm{q}-\mathrm{rK}^{B}\text{ vs }\mathrm{drK}^{B})$. Then, for every $y \in \mathrm{supp}(\mathcal{D})$, we have $\mathrm{q}^{t}(x, y) - \mathrm{rK}^{\tau(t),B'}(y) \leq s$. Thus, we obtain

$$\begin{aligned}\mathrm{q}^{t'}(G_{k}(x; z), y) - \mathrm{rK}^{p(t'),B'}(y) &\leq \mathrm{q}^{t}(x, y) + |z| + O(\log k) - \mathrm{rK}^{p(t'),B'}(y) \\ &\leq s + O(\log^{3} n),\end{aligned}$$

where the last inequality holds for $\tau(t) \geq p(t')$. Choosing $s' := s + O(\log^3 n)$, this implies that $\Pi(G_k(x;z), y, 1^{t'}, 1^{s'}) = 1$. It follows that

$$\Pr\left[M^B(x, \mathcal{D}, 1^t, 1^s) = 1\right] \geq 1 - \epsilon.$$

Conversely, assume that

$$\Pr\left[M^B(x, \mathcal{D}, 1^t, 1^s) = 1\right] \geq 1 - 2\epsilon.$$

By a counting argument, for every $y \in \mathrm{supp}(\mathcal{D})$, with probability at least $1 - \epsilon$, it holds that

$$\mathrm{K}^{B'}(w \mid y) \geq k - O(1) > s' + \log^3 p(t'),$$

where we choose $k := s' + 2\log^3 p(t')$. Under this event, we have $\Pi(w, y, 1^{t'}, 1^{s'}) = 0$. Thus,

$$\Pr\Big[B(w, y, 1^{t'}, 1^{s'}) = 0\Big] \geq 1 - 2\epsilon.$$

Combining the above inequalities, we get

$$\Pr\Big[B(G_k(x;z), y, 1^{t'}, 1^{s'}) = 1\Big] - \Pr\Big[B(w, y, 1^{t'}, 1^{s'}) = 1\Big] \geq 1 - 4\epsilon.$$

By Lemma 7.1, we obtain

$$\mathrm{drK}^{\mathsf{poly}(t'),B}_{(1-4\epsilon)/2k}(x \mid \mathcal{D}) \leq k + O(\log^3 n).$$

This means that the input is not a NO instance. □

Acknowledgements

I deeply thank Mikito Nanashima for very helpful discussion. This work was supported by JST, PRESTO Grant Number JPMJPR2024, Japan. Parts of this work were completed while the author was a Research Fellow at the University of Warwick supported by the EPSRC New Horizons Grant EP/V048201/1.

References

[ABKMR06] Eric Allender, Harry Buhrman, Michal Koucký, Dieter van Melkebeek, and Detlef Ronneburger. "Power from Random Strings". In: *SIAM J. Comput.* 35.6 (2006), pp. 1467–1493. DOI: 10.1137/050628994.

[ABX08] Benny Applebaum, Boaz Barak, and David Xiao. "On Basing Lower-Bounds for Learning on Worst-Case Assumptions". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2008, pp. 211–220. DOI: 10.1109/FOCS.2008.35.

[ACMTV21] Eric Allender, Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovich. "One-Way Functions and a Conditional Variant of MKTP". In: *Proceedings of the Foundations of Software Technology and Theoretical Computer Science (FSTTCS)*. 2021, 7:1–7:19. DOI: 10.4230/LIPIcs.FSTTCS.2021.7.

[AF09] Luis Filipe Coelho Antunes and Lance Fortnow. "Worst-Case Running Times for Average-Case Algorithms". In: *Proceedings of the Conference on Computational Complexity (CCC)*. 2009, pp. 298–303. DOI: 10.1109/CCC.2009.12.

[AFMV06] Luis Antunes, Lance Fortnow, Dieter van Melkebeek, and N. V. Vinodchandran. "Computational depth: Concept and applications". In: *Theor. Comput. Sci.* 354.3 (2006), pp. 391–404. DOI: 10.1016/j.tcs.2005.11.033.

[AFPS12] Luis Filipe Coelho Antunes, Lance Fortnow, Alexandre Pinto, and Andre Souto. "Low-Depth Witnesses are Easy to Find". In: *Comput. Complex.* 21.3 (2012), pp. 479–497. DOI: 10.1007/s00037-011-0025-1.

[AGGM06] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. "On basing one-way functions on NP-hardness". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2006, pp. 701–710. DOI: 10.1145/1132516.1132614.

[AGHR21] Eric Allender, John Gouwar, Shuichi Hirahara, and Caleb Robelle. "Cryptographic Hardness Under Projections for Time-Bounded Kolmogorov Complexity". In: *Proceedings of the International Symposium on Algorithms and Computation (ISAAC)*. 2021, 54:1–54:17. DOI: 10.4230/LIPIcs.ISAAC.2021.54.

[AGMMM18] Eric Allender, Joshua A. Grochow, Dieter van Melkebeek, Cristopher Moore, and Andrew Morgan. "Minimum Circuit Size, Graph Isomorphism, and Related Problems". In: *SIAM J. Comput.* 47.4 (2018), pp. 1339–1372. DOI: 10.1137/17M1157970.

[All21] Eric Allender. "Vaughan Jones, Kolmogorov Complexity, and the new complexity landscape around circuit minimization". In: *New Zealand journal of mathematics* 52 (2021), pp. 585–604.

[BB15] Andrej Bogdanov and Christina Brzuska. "On Basing Size-Verifiable One-Way Functions on NP-Hardness". In: *Proceedings of the Theory of Cryptography Conference (TCC)*. 2015, pp. 1–6. DOI: 10.1007/978-3-662-46494-6_1.

[BBDDRVV20] Marshall Ball, Elette Boyle, Akshay Degwekar, Apoorvaa Deshpande, Alon Rosen, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan. "Cryptography from Information Loss". In: *Proceedings of the Innovations in Theoretical Computer Science Conference (ITCS)*. 2020, 81:1–81:27. DOI: 10.4230/LIPIcs.ITCS.2020.81.

[Bei11] Amos Beimel. "Secret-Sharing Schemes: A Survey". In: *The Third International Workshop on Coding and Cryptology (IWCC)*. 2011, pp. 11–46. DOI: 10.1007/978-3-642-20901-7_2.

[Ben88] C. H. Bennett. "Logical Depth and Physical Complexity". In: *The universal Turing machine, a half century survey*. Ed. by R. Herken. Oxford University Press, 1988, pp. 227–257.

[BFP05] Harry Buhrman, Lance Fortnow, and Aduri Pavan. "Some Results on Derandomization". In: *Theory Comput. Syst.* 38.2 (2005), pp. 211–227. DOI: 10.1007/s00224-004-1194-y.

[BK95] Manuel Blum and Sampath Kannan. "Designing Programs that Check Their Work". In: *J. ACM* 42.1 (1995), pp. 269–291. DOI: 10.1145/200836.200880.

[BL88] Josh Cohen Benaloh and Jerry Leichter. "Generalized Secret Sharing and Monotone Functions". In: *Proceedings of the International Cryptology Conference (CRYPTO)*. 1988, pp. 27–35. DOI: 10.1007/0-387-34799-2_3.

[BT06a] Andrej Bogdanov and Luca Trevisan. "Average-Case Complexity". In: *Foundations and Trends in Theoretical Computer Science* 2.1 (2006). DOI: 10.1561/0400000004.

[BT06b] Andrej Bogdanov and Luca Trevisan. "On Worst-Case to Average-Case Reductions for NP Problems". In: *SIAM J. Comput.* 36.4 (2006), pp. 1119–1159. DOI: 10.1137/S0097539705446974.

[CHV22] Lijie Chen, Shuichi Hirahara, and Neekon Vafa. "Average-case Hardness of NP and PH from Worst-case Fine-grained Assumptions". In: *Proceedings of the Innovations in Theoretical Computer Science Conference (ITCS)*. 2022, 67:1–67:17.

[DHK15] Irit Dinur, Prahladh Harsha, and Guy Kindler. "Polynomially Low Error PCPs with polyloglog n Queries via Modular Composition". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2015, pp. 267–276. DOI: 10.1145/2746539.2746630.

[DM18] Irit Dinur and Or Meir. "Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity". In: *Comput. Complex.* 27.3 (2018), pp. 375–462. DOI: 10.1007/s00037-017-0159-x.

[DS04] Irit Dinur and Shmuel Safra. "On the hardness of approximating label-cover". In: *Inf. Process. Lett.* 89.5 (2004), pp. 247–254. DOI: 10.1016/j.ipl.2003.11.007.

[FF93] Joan Feigenbaum and Lance Fortnow. "Random-Self-Reducibility of Complete Sets". In: *SIAM J. Comput.* 22.5 (1993), pp. 994–1005. DOI: 10.1137/0222061.

[GGM86] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. "How to construct random functions". In: *J. ACM* 33.4 (1986), pp. 792–807. DOI: 10.1145/6490.6503.

[GK22] Halley Goldberg and Valentine Kabanets. "A Simpler Proof of the Worst-Case to Average-Case Reduction for Polynomial Hierarchy via Symmetry of Information". In: *Electronic Colloquium on Computational Complexity (ECCC)* 007 (2022).

[GKLO22] Halley Goldberg, Valentine Kabanets, Zhenjian Lu, and Igor Carboni Oliveira. "Probabilistic Kolmogorov Complexity with Applications to Average-Case Complexity". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2022, 16:1–16:60. DOI: 10.4230/LIPIcs.CCC.2022.16.

[GL89] Oded Goldreich and Leonid A. Levin. "A Hard-Core Predicate for all One-Way Functions". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 1989, pp. 25–32. DOI: 10.1145/73007.73010.

[Gol01] Oded Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques*. Cambridge University Press, 2001. ISBN: 0-521-79172-3. DOI: 10.1017/CBO9780511546891.

[GST07] Dan Gutfreund, Ronen Shaltiel, and Amnon Ta-Shma. "If NP Languages are Hard on the Worst-Case, Then it is Easy to Find Their Hard Instances". In: *Computational Complexity* 16.4 (2007), pp. 412–441. DOI: 10.1007/s00037-007-0235-8.

[GT07] Dan Gutfreund and Amnon Ta-Shma. "Worst-Case to Average-Case Reductions Revisited". In: *Proceedings of the Approximation, Randomization, and Combinatorial Optimization (APPROX/RANDOM)*. 2007, pp. 569–583. DOI: 10.1007/978-3-540-74208-1_41.

[GV08] Dan Gutfreund and Salil P. Vadhan. "Limitations of Hardness vs. Randomness under Uniform Reductions". In: *Proceedings of the Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*. 2008, pp. 469–482. DOI: 10.1007/978-3-540-85363-3_37.

[Hås98] Johan Håstad. "The Shrinkage Exponent of de Morgan Formulas is 2". In: *SIAM J. Comput.* 27.1 (1998), pp. 48–64. DOI: 10.1137/S0097539794261556.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. "A Pseudorandom Generator from any One-way Function". In: *SIAM J. Comput.* 28.4 (1999), pp. 1364–1396. DOI: 10.1137/S0097539793244708.

[Hir18] Shuichi Hirahara. "Non-Black-Box Worst-Case to Average-Case Reductions within NP". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2018, pp. 247–258. DOI: 10.1109/FOCS.2018.00032.

[Hir20a] Shuichi Hirahara. "Characterizing Average-Case Complexity of PH by Worst-Case Meta-Complexity". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 50–60.

[Hir20b] Shuichi Hirahara. "Non-Disjoint Promise Problems from Meta-Computational View of Pseudorandom Generator Constructions". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2020, 20:1–20:47. DOI: 10.4230/LIPIcs.CCC.2020.20.

[Hir20c] Shuichi Hirahara. "Unexpected hardness results for Kolmogorov complexity under uniform reductions". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2020, pp. 1038–1051. DOI: 10.1145/3357713.3384251.

[Hir21] Shuichi Hirahara. "Average-case hardness of NP from exponential worst-case hardness assumptions". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2021, pp. 292–302. DOI: 10.1145/3406325.3451065.

[Hir22a] Shuichi Hirahara. "Meta-Computational Average-Case Complexity: A New Paradigm Toward Excluding Heuristica". In: *Bull. EATCS* 136 (2022).

[Hir22b] Shuichi Hirahara. "NP-Hardness of Learning Programs and Partial MCSP". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2022.

[Hir22c] Shuichi Hirahara. "Symmetry of Information from Meta-Complexity". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2022, 26:1–26:41. DOI: 10.4230/LIPIcs.CCC.2022.26.

[HIR23] Yizhi Huang, Rahul Ilango, and Hanlin Ren. "NP-Hardness of Approximating Meta-Complexity: A Cryptographic Approach". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2023.

[HN21] Shuichi Hirahara and Mikito Nanashima. “On Worst-Case Learning in Relativized Heuristica”. In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2021, pp. 751–758. DOI: 10.1109/FOCS52979.2021.00078.

[HN22] Shuichi Hirahara and Mikito Nanashima. “Finding Errorless Pessiland in Error-Prone Heuristica”. In: *Proceedings of the Computational Complexity Conference (CCC)*. 2022, 25:1–25:28. DOI: 10.4230/LIPIcs.CCC.2022.25.

[HS17] Shuichi Hirahara and Rahul Santhanam. “On the Average-Case Complexity of MCSP and Its Variants”. In: *Proceedings of the Computational Complexity Conference (CCC)*. 2017, 7:1–7:20. DOI: 10.4230/LIPIcs.CCC.2017.7.

[HS22] Shuichi Hirahara and Rahul Santhanam. “Errorless Versus Error-Prone Average-Case Complexity”. In: *Proceedings of the Innovations in Theoretical Computer Science Conference (ITCS)*. 2022, 84:1–84:23. DOI: 10.4230/LIPIcs.ITCS.2022.84.

[HW20] Shuichi Hirahara and Osamu Watanabe. “On Nonadaptive Security Reductions of Hitting Set Generators”. In: *Proceedings of the Approximation, Randomization, and Combinatorial Optimization (APPROX/RANDOM)*. 2020, 15:1–15:14. DOI: 10.4230/LIPIcs.APPROX/RANDOM.2020.15.

[IL89] Russell Impagliazzo and Michael Luby. “One-way Functions are Essential for Complexity Based Cryptography (Extended Abstract)”. In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 1989, pp. 230–235. DOI: 10.1109/SFCS.1989.63483.

[IL90] Russell Impagliazzo and Leonid A. Levin. “No Better Ways to Generate Hard NP Instances than Picking Uniformly at Random”. In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 1990, pp. 812–821. DOI: 10.1109/FSCS.1990.89604.

[Imp11] Russell Impagliazzo. “Relativized Separations of Worst-Case and Average-Case Complexities for NP”. In: *Proceedings of the Conference on Computational Complexity (CCC)*. 2011, pp. 104–114. DOI: 10.1109/CCC.2011.34.

[Imp95] Russell Impagliazzo. “A Personal View of Average-Case Complexity”. In: *Proceedings of the Structure in Complexity Theory Conference*. 1995, pp. 134–147. DOI: 10.1109/SCT.1995.514853.

[IW01] Russell Impagliazzo and Avi Wigderson. “Randomness vs Time: Derandomization under a Uniform Assumption”. In: *J. Comput. Syst. Sci.* 63.4 (2001), pp. 672–688. DOI: 10.1006/jcss.2001.1780.

[IW97] Russell Impagliazzo and Avi Wigderson. “P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma”. In: *Proceedings of the Symposium on the Theory of Computing (STOC)*. 1997, pp. 220–229. DOI: 10.1145/258533.258590.

[KC00] Valentine Kabanets and Jin-yi Cai. “Circuit minimization problem”. In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 2000, pp. 73–79. DOI: 10.1145/335305.335314.

[Ko91] Ker-I Ko. "On the Complexity of Learning Minimum Time-Bounded Turing Machines". In: *SIAM J. Comput.* 20.5 (1991), pp. 962–986. DOI: 10.1137/0220059.

[KRW95] Mauricio Karchmer, Ran Raz, and Avi Wigderson. "Super-Logarithmic Depth Lower Bounds Via the Direct Sum in Communication Complexity". In: *Computational Complexity* 5.3/4 (1995), pp. 191–204. DOI: 10.1007/BF01206317.

[Lev86] Leonid A. Levin. "Average Case Complete Problems". In: *SIAM J. Comput.* 15.1 (1986), pp. 285–286. DOI: 10.1137/0215020.

[LP20] Yanyi Liu and Rafael Pass. "On One-way Functions and Kolmogorov Complexity". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 1243–1254.

[LP22] Yanyi Liu and Rafael Pass. "On One-Way Functions from NP-Complete Problems". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2022, 36:1–36:24. DOI: 10.4230/LIPIcs.CCC.2022.36.

[Muc02] Andrei A. Muchnik. "Conditional complexity and codes". In: *Theor. Comput. Sci.* 271.1-2 (2002), pp. 97–109. DOI: 10.1016/S0304-3975(01)00033-0.

[MX10] Mohammad Mahmoody and David Xiao. "On the Power of Randomized Reductions and the Checkability of SAT". In: *Proceedings of the Conference on Computational Complexity (CCC)*. 2010, pp. 64–75. DOI: 10.1109/CCC.2010.16.

[Nan21] Mikito Nanashima. "On Basing Auxiliary-Input Cryptography on NP-Hardness via Nonadaptive Black-Box Reductions". In: *Proceedings of the Innovations in Theoretical Computer Science Conference (ITCS)*. 2021, 29:1–29:15. DOI: 10.4230/LIPIcs.ITCS.2021.29.

[Nao91] Moni Naor. "Bit Commitment Using Pseudorandomness". In: *J. Cryptol.* 4.2 (1991), pp. 151–158. DOI: 10.1007/BF00196774.

[NW94] Noam Nisan and Avi Wigderson. "Hardness vs Randomness". In: *J. Comput. Syst. Sci.* 49.2 (1994), pp. 149–167. DOI: 10.1016/S0022-0000(05)80043-1.

[Ost91] Rafail Ostrovsky. "One-Way Functions, Hard on Average Problems, and Statistical Zero-Knowledge Proofs". In: *Proceedings of the Structure in Complexity Theory Conference*. 1991, pp. 133–138. DOI: 10.1109/SCT.1991.160253.

[OW93] Rafail Ostrovsky and Avi Wigderson. "One-Way Fuctions are Essential for Non-Trivial Zero-Knowledge". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 1993, pp. 3–17. DOI: 10.1109/ISTCS.1993.253489.

[Rom90] John Rompel. "One-Way Functions are Necessary and Sufficient for Secure Signatures". In: *Proceedings of the Symposium on Theory of Computing (STOC)*. 1990, pp. 387–394. DOI: 10.1145/100216.100269.

[RR97] Alexander A. Razborov and Steven Rudich. "Natural Proofs". In: *J. Comput. Syst. Sci.* 55.1 (1997), pp. 24–35. DOI: 10.1006/jcss.1997.1494.

[RRV02] Ran Raz, Omer Reingold, and Salil P. Vadhan. "Extracting all the Randomness and Reducing the Error in Trevisan's Extractors". In: *J. Comput. Syst. Sci.* 65.1 (2002), pp. 97–128. DOI: 10.1006/jcss.2002.1824.

[RS22] Hanlin Ren and Rahul Santhanam. "A Relativization Perspective on Meta-Complexity". In: *39th International Symposium on Theoretical Aspects of Computer Science, STACS 2022, March 15-18, 2022, Marseille, France (Virtual Conference)*. 2022, 54:1–54:13. DOI: 10.4230/LIPIcs.STACS.2022.54.

[Rud97] Steven Rudich. "Super-bits, Demi-bits, and NP/qpoly-natural Proofs". In: *Proceedings of the Randomization and Approximation Techniques in Computer Science (RANDOM/APPROX)*. 1997, pp. 85–93. DOI: 10.1007/3-540-63248-4_8.

[San20] Rahul Santhanam. "Pseudorandomness and the Minimum Circuit Size Problem". In: *Proceedings of the Innovations in Theoretical Computer Science Conference (ITCS)*. 2020, 68:1–68:26. DOI: 10.4230/LIPIcs.ITCS.2020.68.

[SS20] Michael Saks and Rahul Santhanam. "Circuit Lower Bounds from NP-Hardness of MCSP Under Turing Reductions". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2020, 26:1–26:13. DOI: 10.4230/LIPIcs.CCC.2020.26.

[SS22] Michael Saks and Rahul Santhanam. "On Randomized Reductions to the Random Strings". In: *Proceedings of the Computational Complexity Conference (CCC)*. 2022, 29:1–29:30. DOI: 10.4230/LIPIcs.CCC.2022.29.

[TV07] Luca Trevisan and Salil P. Vadhan. "Pseudorandomness and Average-Case Complexity Via Uniform Reductions". In: *Computational Complexity* 16.4 (2007), pp. 331–364. DOI: 10.1007/s00037-007-0233-x.

[Vad06] Salil P. Vadhan. "An Unconditional Study of Computational Zero Knowledge". In: *SIAM J. Comput.* 36.4 (2006), pp. 1160–1214. DOI: 10.1137/S0097539705447207.

[Vad12] Salil P. Vadhan. "Pseudorandomness". In: *Foundations and Trends in Theoretical Computer Science* 7.1-3 (2012), pp. 1–336. DOI: 10.1561/0400000010.

[Vio05] Emanuele Viola. "On Constructing Parallel Pseudorandom Generators from One-Way Functions". In: *Proceedings of the Conference on Computational Complexity (CCC)*. 2005, pp. 183–197. DOI: 10.1109/CCC.2005.16.

[Wee06] Hoeteck Wee. "Finding Pessiland". In: *Proceedings of the Theory of Cryptography Conference (TCC)*. 2006, pp. 429–442. DOI: 10.1007/11681878_22.

[Yao82] Andrew Chi-Chih Yao. "Theory and Applications of Trapdoor Functions (Extended Abstract)". In: *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*. 1982, pp. 80–91. DOI: 10.1109/SFCS.1982.45.

[ZL70] Alexander K Zvonkin and Leonid A Levin. "The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms". In: *Russian Mathematical Surveys* 25.6 (1970), pp. 83–124.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il