Exposition on LP25:

"Hardness along the boundary: Towards one-way functions from the worst-case hardness of time-bounded Kolmogorov complexity"

Hanlin Ren
University of Oxford
hanlin.ren@cs.ox.ac.uk

August 26, 2025

This is an exposition of [LP25].

Definition 1.

$$\mathrm{pK}^t_\delta(x) := \min\Big\{w : \Pr_r[\mathrm{K}^t(x \mid r) \le w] \ge \delta\Big\}.$$

Theorem 2. *Suppose that one-way functions do not exist. Then for every polynomial $t_1(\cdot)$, every function $s(n) \le n-1$, and every $\beta > 1$, there exists a polynomial $t_2(\cdot)$ such that the following promise problem $\Pi := \Pi^{t_1,t_2}_{\mathrm{pK},\beta}[s]$ is in* pr-BPP*:*

$$\begin{aligned}\Pi.\textsc{Yes} &:= \{x \in \{0,1\}^* : \mathrm{pK}^{t_1}_{2/3}(x) \le s(|x|) \text{ and } \mathrm{pK}^{t_2}_{2/3}(x) > \mathrm{pK}^{t_1}_{2/3}(x) - \beta \log |x|\};\\ \Pi.\textsc{No} &:= \{x \in \{0,1\}^* : \mathrm{pK}^{t_1}_{1/3}(x) > s(|x|)\}.\end{aligned}$$

Proof. The proof consists of the following steps.

1. **Defining the one-way function to invert.**

   Let $f(\ell, \Pi', r)$ denote the following one-way function.

   The inputs of f consists of $\ell \in [n]$, $\Pi' \in \{0,1\}^n$, and $r \in \{0,1\}^{t_1(n)}$.

   Let Π be the first ℓ bits of Π', we treat Π as a randomized program Π, run it on randomness r for $t_1(n)$ steps, and record the output y.

   The output of f is (ℓ, y, r).

   Since f is not a one-way function, let Inv be an inverter for f that succeeds w.p. $\ge 1 - n^{-(\beta+2)}$.

2. **Defining the algorithm M for solving Π.**

   On input $z \in \{0,1\}^n$, the algorithm samples $r \leftarrow \{0,1\}^{t_1(n)}$.

   Then, for every $i \in [n]$, the algorithm runs $\mathsf{Inv}(i, z, r)$.

   If Inv ever outputs a program of length at most s that outputs z in $t_1(n)$ steps given randomness r, then we output "Yes". Otherwise we output "No".

3. **The algorithm is correct on No instances.** This is the easier part.

   Suppose that $z \in \Pi.\textsc{No}$, i.e., $\mathrm{pK}^{t_1}_{1/3}(z) > s(|z|)$.

   The probability over r that there *exists* a program of length $s(|z|)$ making M output "Yes" is at most $1/3$, hence the probability that $M(z)$ outputs "Yes" is at most $1/3$.

4. **Defining the distribution $\mathcal{D}$.** Before proceeding to the Yes instances, we define a distribution $\mathcal{D}$ that is concentrated on the inputs (i.e., outputs of f) making Inv fail.

   Repeat the following $n^{\beta+2}$ times until we output an element.

   (a) First, sample (ℓ, Π', r) uniformly at random.

   (b) If Inv succeeds at inverting $f(\ell, \Pi', r)$, repeat.

   (c) Otherwise, output y (the output of Π on randomness r in $t_1(n)$ steps).

   (d) If we have not outputted anything in $n^{\beta+2}$ rounds, we output $\perp$.

5. **The algorithm is correct on Yes instances.** This is the harder part.

   Suppose there is an input $z \in \{0,1\}^n$ such that $\mathrm{pK}^{t_1}_{2/3}(z) = w \leq s(n)$ but the probability that $M(z)$ outputs "Yes" is less than $3/5$.

   Let $S := \{(\ell, z, r) : \ell = \mathrm{K}(z \mid r) \leq w\}$, then $|S| \geq (2/3) \cdot 2^{t_1(n)}$.

   On the other hand, $M(z)$ outputs "Yes" w.p. $< 3/5$, hence Inv fails on at least $F := (2/3 - 3/5) \cdot 2^{t_1(n)}$ inputs in S.

   Hence, the probability that $\mathcal{D}$ outputs z is at least $\frac{F}{n \cdot 2^w \cdot 2^{t_1(n)}} \cdot n^{\beta+2} \geq n^\beta \cdot 2^{-w}$.

   By the coding theorem for pK^t, there is a polynomial $t_2(\cdot)$ such that $\mathrm{pK}^{t_2}_{2/3}(z) \leq w - \beta \log n$.

   Hence $z \notin \Pi.\textsc{Yes}$. In other words, if $z \in \Pi.\textsc{Yes}$ then $M(z)$ outputs "Yes" w.p. at least $3/5$. $\square$

1 Remarks on telescoping

One reason that I was very excited about [LP25] is that, as opposed to its predecessor [LP24], the definition of the worst-case problem now involves *time-bounded computational depth* ($\mathrm{K}^{t_1}(x) - \mathrm{K}^{t_2}(x)$) instead of traditional computational depth ($\mathrm{K}^t(x) - \mathrm{K}(x)$). This opens the way of using a telescoping argument *à la* [Hir21] to base one-way functions on the exponential worst-case hardness of (standard) time-bounded Kolmogorov complexity. However, the results of [LP25] so far falls short of this objective.

Define $\mathrm{cd}^{t_1,t_2}(x) := \mathrm{pK}^{t_1}_{2/3}(x) - \mathrm{pK}^{t_2}_{2/3}(x)$. Using [LP25] we can show that if infinitely-often one-way functions do not exist, then there exists a polynomial $p(\cdot,\cdot)$ such that the following problem is in pr-BPP:

$$\Pi.\textsc{Yes} := \{(x, 1^t, 1^s, 1^{2^d}) : \mathrm{pK}^t_{2/3}(x) \leq s \text{ and } \mathrm{cd}^{t,p(t,2^d)}(x) \leq d\},$$
$$\Pi.\textsc{No} := \{(x, 1^t, 1^s, 1^{2^d}) : \mathrm{pK}^t_{1/3}(x) > s\}.$$

If we could get rid of the 2^d term in the expression $p(t, 2^d)$ above, then we can use a telescoping argument to show that meta-complexity problems admit non-trivial *worst-case* algorithms:

Theorem 3. *Suppose there is a polynomial $p(\cdot)$ such that the following problem is in* pr-BPP*:*

$$\Pi.\textsc{Yes} := \{(x, 1^t, 1^s, 1^{2^d}) : \mathrm{pK}^t_{2/3}(x) \leq s \textit{ and } \mathrm{cd}^{t,p(t)}(x) \leq d\},$$
$$\Pi.\textsc{No} := \{(x, 1^t, 1^s, 1^{2^d}) : \mathrm{pK}^t_{1/3}(x) > s\}.$$

Then for every $a(n) \leq \mathrm{poly}(n)$ and $b(n) \geq 2^{O(n/\log n)}$, given a string $x \in \{0,1\}^n$ and an integer $s \in [n]$, one can distinguish in probabilistic $2^{O(n/\log n)}$ time between the case that $\mathrm{pK}^{a(n)}_{2/3}(x) \leq s$ and the case that $\mathrm{pK}^{b(n)}_{1/3}(x) > s$.

Proof Sketch. Let $I := \varepsilon \log n$ for some constant $\varepsilon > 0$, $t_0 := a(n)$, $t_i := p(t_{i-1})$ for every $i \in [I]$, then $t_I \le b(n)$. Let $d := n/I$, if there is some $i \in [I]$ such that $(x, 1^{t_{i-1}}, 1^s, 1^{2^d}) \in \Pi.\textsc{Yes}$ then we output "Yes"; otherwise we output "No".

If $\mathrm{pK}_{1/3}^{b(n)}(x) > s$, then we would never output "Yes". On the other hand, for every $x \in \{0,1\}^n$, there exists some $i \in [I]$ such that $\mathrm{cd}^{t_{i-1},t_i}(x) \le d$. If $\mathrm{pK}_{2/3}^{a(n)}(x) \le s$, then we will output "Yes" when we enumerate such i. □

That is, the main result of [LP25] is "only" one 2^d factor away from basing one-way functions from the exponential $(2^{\omega(n/\log n)})$ worst-case hardness of the $(\mathrm{pK}^{\mathrm{poly}}$ vs. $\mathrm{pK}^{2^{O(n/\log n)}})$ problem.

References

[Hir21] Shuichi Hirahara. Average-case hardness of NP from exponential worst-case hardness assumptions. In *STOC*, pages 292–302. ACM, 2021.

[LP24] Yanyi Liu and Rafael Pass. On one-way functions and the worst-case hardness of time-bounded Kolmogorov complexity, and computational depth. In *TCC*, 2024.

[LP25] Yanyi Liu and Rafael Pass. Hardness along the boundary: Towards one-way functions from the worst-case hardness of time-bounded Kolmogorov complexity. In *CRYPTO*, 2025.