Exact Search-to-Decision Reductions for Time-Bounded Kolmogorov Complexity

Shuichi Hirahara

National Institute of Informatics

Valentine Kabanets

Simon Fraser University

Zhenjian Lu

University of Warwick

Igor C. Oliveira

University of Warwick

CCC 2024

Overview

string x

01001101...0111010111 $\longrightarrow$ 010001110

shortest encoding of x

Suppose given a string x, we can efficiently compute the length of an optimal compression of x.

Can we also efficiently find such a compression?

Kolmogorov Complexity

Kolmogorov Complexity:

$\boxed{\text{K}(x) = \text{“minimum length of a program } M \in \{0,1\}^* \text{ such that } M \text{ outputs } x\text{”}}$

Kolmogorov Complexity

Kolmogorov Complexity:

$\mathrm{K}(x) =$ "minimum length of a program $M \in \{0,1\}^*$ such that M outputs x"

Conditional Kolmogorov Complexity:

$\mathrm{K}(x \mid y) =$ "minimum length of a program $M \in \{0,1\}^*$ such that M outputs x given oracle (query) access to y"

Time-Bounded Kolmogorov Complexity

t-time-bounded Kolmogorov complexity:

$\mathrm{K}^t(x) =$ "minimum length of a program $M \in \{0,1\}^*$ such that M outputs x within time t"

Decision MINKT

Definition (MINKT):

- **Input**: $(x, 1^t, 1^s)$, where $x \in \{0,1\}^*$ and $t, s \in \mathbb{N}$
- **Task**: Decide whether $\mathrm{K}^t(x) \leq s$

Decision MINKT

Definition (MINKT):

- **Input**: $(x, 1^t, 1^s)$, where $x \in \{0,1\}^*$ and $t, s \in \mathbb{N}$
- **Task**: Decide whether $\mathrm{K}^t(x) \leq s$

By trying $s = 1,2,\ldots,|x| + O(1)$, solving MINKT allows us to compute $\mathrm{K}^t(x)$, i.e.,
the length of a shortest t-time program that x

Computing K^t

<u>**Conjecture**</u>: $\boxed{\text{MINKT is NP-complete.}}$

Serach-MINKT

Definition (Search-MINKT):

- **Input**: $(x, 1^t)$, where $x \in \{0,1\}^*$ and $t \in \mathbb{N}$
- **Task**: Find a shortest t-time program that outputs x, i.e.,
    - A program M such that $|M| = \mathrm{K}^t(x)$
    - M outputs x within time t

Search-to-Decision

<u>Question</u>:

MINKT is easy $\overset{?}{\Longrightarrow}$ Search-MINKT is easy

Search-to-Decision

Question:

MINKT is easy $\xrightarrow{?}$ Search-MINKT is easy

A worst-case search-to-decision reduction

Average-Case Search-to-Decision

Question:

MINKT is easy on average $\overset{?}{\Longrightarrow}$ Search-MINKT is easy on average

Average-Case Search-to-Decision

Question:

MINKT is easy on average $\overset{?}{\Rightarrow}$ Search-MINKT is easy on average

Easy on average: For every poly-time samplable distribution D, there is an efficient algorithm that succeeds with high probability over a string $x \sim D$.

Average-Case Search-to-Decision

Question:

MINKT is easy on average $\overset{?}{\Rightarrow}$ Search-MINKT is easy on average

Easy on average: For every poly-time samplable distribution D, there is an efficient algorithm that succeeds with high probability over a string $x \sim D$.

Errorless	Error-Prone
• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm outputs $\perp$.	• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm can output a wrong answer.

Average-Case Search-to-Decision

Question:

MINKT is easy on average $\overset{?}{\Longrightarrow}$ Search-MINKT is easy on average

Easy on average: For every poly-time samplable distribution D, there is an efficient algorithm that succeeds with high probability over a string $x \sim D$.

Errorless	Error-Prone
• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm outputs $\perp$.	• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm can output a wrong answer.

Average-Case Search-to-Decision

Question:

MINKT is easy on average $\xrightarrow{?}$ Search-MINKT is easy on average

Easy on average: For every poly-time samplable distribution D, there is an efficient algorithm that succeeds with high probability over a string $x \sim D$.

Errorless	Error-Prone
• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm outputs $\perp$.	• The algorithm outputs a correct answer for almost all $x \sim D$. • For the other x, the algorithm can output a wrong answer.

Prior Work

Theorem [Liu-Pass'20]:

MINKT is easy on average over the uniform distribution in the error-prone setting	$\Rightarrow$	Search-MINKT is easy on average over the uniform distribution in the error-prone setting

Prior Work

Theorem [Liu-Pass'20]:

MINKT is easy on average over the uniform distribution in the error-prone setting $\Rightarrow$ Search-MINKT is easy on average over the uniform distribution in the error-prone setting

Theorem [Liu-Pass'23]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.NSIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the error-prone setting $\Rightarrow$ Search-MINKT is easy on average over P-samplable distributions in the error-prone setting

Conditional Search-to-Decision

Theorem [Liu-Pass'23]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.NSIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the error-prone setting	$\Rightarrow$	Search-MINKT is easy on average over P-samplable distributions in the error-prone setting

Conditional Search-to-Decision

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{SIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in erroless (resp. error-prone) setting	⇒	Search-MINKT is easy on average over P-samplable distributions in erroless (resp. error-prone) setting

Theorem [Liu-Pass'23]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{NSIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the error-prone setting	⇒	Search-MINKT is easy on average over P-samplable distributions in the error-prone setting

Conditional Search-to-Decision

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{SIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over uniform distribution in erroless (resp. error-prone) setting	$\Rightarrow$	Search-MINKT is easy on average over P-samplable distributions in erroless (resp. error-prone) setting

Theorem [Liu-Pass’23]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{NSIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over uniform distribution in the error-prone setting	$\Rightarrow$	Search-MINKT is easy on average over P-samplable distributions in the error-prone setting

Conditional Search-to-Decision

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{SIZE}\left[2^{o(n)}\right]$

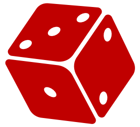
MINKT is easy on average over uniform distribution in erroless (resp. error-prone) setting $\Rightarrow$ Search-MINKT is easy on average over P-samplable distributions in erroless (resp. error-prone) setting

Theorem [Liu-Pass'23]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.}\,\mathbf{NSIZE}\left[2^{o(n)}\right]$

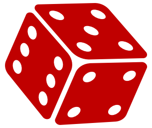
MINKT is easy on average over uniform distribution in the error-prone setting $\Rightarrow$ Search-MINKT is easy on average over P-samplable distributions in the error-prone setting

Can we get rid of the derandomization assumption?

Randomized Kolmogorov Compelxity



Randomized t-time-bounded Kolmogorov complexity:



$\mathrm{rK}^t_\lambda(x) =$ "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Decision MINrKT

Randomized t-time-bounded Kolmogorov complexity:

$\mathrm{rK}_{\lambda}^{t}(x)$ = "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Definition (λ-MINrKT; First Attempt):

- **Input**: $(x, 1^t, 1^s)$, where $x \in \{0,1\}^*$ and $t, s \in \mathbb{N}$
- **Task**: Decide whether
  - $\mathrm{rK}_{\lambda}^{t}(x) \leq s$
  - $\mathrm{rK}_{\lambda}^{t}(x) > s$

Decision MINrKT

Randomized t-time-bounded Kolmogorov complexity:

$\mathrm{rK}^t_\lambda(x)$ = "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Definition (λ-MINrKT; First Attempt):

- **Input**: $(x, 1^t, 1^s)$, where $x \in \{0,1\}^*$ and $t, s \in \mathbb{N}$
- **Task**: Decide whether
  - $\mathrm{rK}^t_\lambda(x) \leq s$
  - $\mathrm{rK}^t_\lambda(x) > s$

This problem is not very natraul and can only be placed in $\exists\cdot\mathbf{PP}$

Decision MINrKT

Randomized t-time-bounded Kolmogorov complexity:

$\mathrm{rK}_{\lambda}^{t}(x) =$ "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Definition (λ-MINrKT):

- **Input**: $(x, 1^t, 1^s, 1^k)$, where $x \in \{0,1\}^*$ and $t, s, k \in \mathbb{N}$
- **Task**: Decide whether
  - $\mathrm{rK}_{\lambda}^{t}(x) \leq s$
  - $\mathrm{rK}_{\lambda-1/k}^{t}(x) > s$

Decision MINrKT

Randomized t-time-bounded Kolmogorov complexity:

$\mathrm{rK}_{\lambda}^{t}(x)$ = "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Definition (λ-MINrKT):

- **Input**: $(x, 1^t, 1^s, 1^k)$, where $x \in \{0,1\}^*$ and $t, s, k \in \mathbb{N}$
- **Task**: Decide whether
  - $\mathrm{rK}_{\lambda}^{t}(x) \leq s$
  - $\mathrm{rK}_{\lambda-1/k}^{t}(x) > s$

This problem is in (promise) **MA**

Search MINrKT

Randomized t-time-bounded Kolmogorov complexity:

$\mathrm{rK}_\lambda^t(x)$ = "minimum length of a randomized program $M \in \{0,1\}^*$ such that M outputs x within time t with probability $\geq \lambda$"

Definition (λ-Search-MINrKT):

- **Input**: $(x, 1^t, 1^k)$, where $x \in \{0,1\}^*$ and $t, s, k \in \mathbb{N}$
- **Task**: Find an $(1/k)$-rK_λ^t witness of x, i.e.,
  - A randomized program M such that $|M| \leq \mathrm{rK}_\lambda^t(x)$
  - M outputs x with probability at least $\lambda - 1/k$

Average-Case Search-to-Decision for rK^t

Theorem [This work]:

λ-MINrKT is easy on average over P-samplable distributions in the erroless setting

$\Rightarrow$

λ-Search-MINrKT is easy on average over P-samplable distributions in the erroless setting

Proof Ideas

Proof Overview

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the erroless setting	$\Rightarrow$	Search-MINKT is easy on average over P-samplable distributions in the erroless setting

Proof Overview

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the erroless setting	$\Rightarrow$	Search-MINKT is easy on average over P-samplable distributions in the erroless setting

High-Level Idea:

- Assume MINKT is easy on average.
- For a typical x from a **P**-samp distribution, there is an optimal t-time program $M \in \{0,1\}^*$ for x that admits a short encoding.
- We can then enumerate all such short encodings (and decode them) to find such an M.

Proof Overview

Theorem [This work]: Assume $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$

MINKT is easy on average over P-samplable distributions in the erroless setting $\Rightarrow$ Search-MINKT is easy on average over P-samplable distributions in the erroless setting

High-Level Idea:

- Assume MINKT is easy on average.
- For a typical x from a **P**-samp distribution, there is an optimal t-time program $M \in \{0,1\}^*$ for x that admits a short encoding.
- We can then enumerate all such short encodings (and decode them) to find such an M.

Proof Overview

High-Level Idea:

- Assume MINKT is easy on average.
- For a typical x from a **P**-samp distribution, there is an optimal t-time program $M \in \{0,1\}^*$ for x that admits a short encoding.
- We can then enumerate all such short encodings (and decode them) to find such an M.

- Consider the lexicographically-first shortest t-time program M for x.
- We know that x has short description given M.
- Here, we want that M has short description given x, so we need some kind of "symmetry of information".

Symmetry of Information

If MINKT is easy on average, then we have symmtry of information for K^t [Hir20, GK22]

Symmetry of Information

If MINKT is easy on average, then we have symmtry of information for K^t [Hir20, GK22]

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

Symmetry of Information

If MINKT is easy on average, then we have symmtry of information for K^t [Hir20, GK22]

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

Symmetry of information for time-unbounded Kolmogorov complexity:

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

Symmetry of Information

If MINKT is easy on average, then we have symmtry of information for K^t [Hir20, GK22]

Symmetry of information for time-unbounded Kolmogorov complexity:

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

Does symmetry of information hold in the time-bounded setting, for K^t?

$$\mathrm{K}^t(x, y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$$

Symmetry of Information

If MINKT is easy on average, then we have symmtry of information for K^t [Hir20, GK22]

Symmetry of information for time-unbounded Kolmogorov complexity:

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

Does symmetry of information hold in the time-bounded setting, for K^t?

$$\mathrm{K}^t(x, y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$$

YES, assuming MINKT is easy on average and $\mathbf{E} \not\subseteq \mathbf{i.o.\,SIZE}\left[2^{o(n)}\right]$

Proof Overview

If MINKT is easy on average, then we have: $\mathrm{K}^t(x,y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$

- Fix x and t, let y_t be a shortest t-time program that outputs x.

Proof Overview

If MINKT is easy on average, then we have: $\mathrm{K}^t(x, y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$

- Fix x and t, let y_t be a shortest t-time program that outputs x.

  - $\mathrm{K}^{\mathrm{poly}(2t)}(y_t \mid x) \lesssim \mathrm{K}^{2t}(x, y_t) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — By SoI for K^t
  - $\lesssim |y_t| - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since given y_t, we can also recover x
  - $= \mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since y_t is a shortest t-time program for x

Proof Overview

If MINKT is easy on average, then we have: $\mathrm{K}^t(x,y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$

- Fix x and t, let y_t be a shortest t-time program that outputs x.

- $\mathrm{K}^{\mathrm{poly}(2t)}(y_t \mid x) \lesssim \mathrm{K}^{2t}(x, y_t) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — By SoI for K^t
- $\lesssim |y_t| - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since given y_t, we can also recover x
- $= \mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since y_t is a shortest t-time program for x

Proof Overview

If MINKT is easy on average, then we have: $\mathrm{K}^t(x, y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$

- Fix x and t, let y_t be a shortest t-time program that outputs x.

- $\mathrm{K}^{\mathrm{poly}(2t)}(y_t \mid x) \lesssim \mathrm{K}^{2t}(x, y_t) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ By SoI for K^t
- $\lesssim |y_t| - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ Since given y_t, we can also recover x
- $= \mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ Since y_t is a shortest t-time program for x

Proof Overview

If MINKT is easy on average, then we have: $\mathrm{K}^t(x, y) \gtrsim \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x)$

- Fix x and t, let y_t be a shortest t-time program that outputs x.

- $\mathrm{K}^{\mathrm{poly}(2t)}(y_t \mid x) \lesssim \mathrm{K}^{2t}(x, y_t) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — By SoI for K^t
- $\lesssim |y_t| - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since given y_t, we can also recover x
- $= \mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(2t)}(x)$ — Since y_t is a shortest t-time program for x

Proof Overview

If MINKT is easy on average, then we have:

- Fix x and t, let y_t be a shortest t-time program that outputs x.

$$\mathrm{K}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$$

If $\mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is small, then y_t admits a short and efficient encoding given x!

Proof Overview

If MINKT is easy on average, then we have:

- Fix x and t, let y_t be a shortest t-time program that outputs x.

$$\mathrm{K}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{K}^{t}(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$$

If $\mathrm{K}^{t}(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is small, then y_t admits a short and efficient encoding given x!

Claim: If MINKT is easy on average, then $\mathrm{K}^{t}(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is at most $O(\log t)$ for an average $x \sim D$

Conding Theorem

If MINKT is easy on average, then we have coding theorem for K^t [Hir18]

Conding Theorem

If MINKT is easy on average, then we have coding theorem for K^t [Hir18]

Coding theorem for time-unbounded Kolmogorov complexity: For every computable distribution D

$$\mathrm{K}(x) \lesssim \log\left(\frac{1}{D(x)}\right)$$

Conding Theorem

If MINKT is easy on average, then we have coding theorem for K^t [Hir18]

Coding theorem for time-unbounded Kolmogorov complexity: For every computable distribution D

$$\boxed{\mathrm{K}(x) \lesssim \log\left(\frac{1}{D(x)}\right)}$$

if MINKT is easy on average, then for every P-samplable dist D and large enough polynomial t

$$\boxed{\mathrm{K}^t(x) \lesssim \log\left(\frac{1}{D(x)}\right)}$$

Proof Overview

<u>Claim</u>: If MINKT is easy on average, then $\mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is small for an average $x \sim D$

Proof Overview

<u>Claim</u>: If MINKT is easy on average, then $\mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is small for an average $x \sim D$

By the coding theorem for K^t, we have

$$\mathrm{K}^t(x) \lesssim \log\left(\frac{1}{D(x)}\right)$$

Proof Overview

Claim: If MINKT is easy on average, then $\mathrm{K}^t(x) - \mathrm{K}^{\mathrm{poly}(t)}(x)$ is small for an average $x \sim D$

By the coding theorem for K^t, we have

$$\boxed{\mathrm{K}^t(x) \lesssim \log\left(\frac{1}{D(x)}\right)}$$

Fact: For every distribution D, with high probability over $x{\sim}D$,

$$\boxed{\mathrm{K}^{\mathrm{poly}(t)}(x) \geq \mathrm{K}(x) \gtrsim \log\left(\frac{1}{D(x)}\right)}$$

What about rK^t?

Proof Overview

If MINKT is easy on average, and $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$, then we have

- symmetry of information for K^t
- coding theorem for K^t

Proof Overview

If MINKT is easy on average, and $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$, then we have

- symmetry of information for K^t
- coding theorem for K^t

We want to say that if MINrKT is easy on average, then we have

- symmetry of information for rK^t
- coding theorem for rK^t

Proof Overview

If MINKT is easy on average, and $\mathbf{E} \not\subseteq \mathbf{i.o.\,SIZE}\left[2^{o(n)}\right]$, then we have

- symmetry of information for K^t
- coding theorem for K^t

We want to say that if MINrKT is easy on average, then we have

- symmetry of information for rK^t
- coding theorem for rK^t

Yes, but...

Proof Overview

If MINKT is easy on average, and $\mathbf{E} \not\subseteq \mathbf{i.o.SIZE}\left[2^{o(n)}\right]$, then we have

- symmetry of information for K^t $\boxed{\mathrm{K}^t(x, y) \geq \mathrm{K}^{\mathrm{poly}(t)}(x) + \mathrm{K}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for K^t $\boxed{\mathrm{K}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

If MINrKT is easy on average, then we have

- symmetry of information for rK^t $\boxed{\mathrm{rK}^t(x, y) \geq \mathrm{rK}^{\mathrm{poly}(t)}(x) + \mathrm{rK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{polylog}(t)}$
- coding theorem for rK^t $\boxed{\mathrm{rK}^t(x) \leq \log(1/D(x)) + \mathbf{polylog}(t)}$

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for rK^t with **polylog** overhead
- coding theorem for rK^t with **polylog** overhead

This will give a quasi-polynomial-time search-to-decision reduction for rK^t

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for rK^t with **polylog** overhead
- coding theorem for rK^t with **polylog** overhead

If MINrKT is easy on average, then we have

- symmetry of information for pK^t with **log** overhead [Goldberg-Kabanets-L.-Oliveira'22]
- coding theorem for pK^t with **log** overhead [L.-Oliveira-Zimand'22]

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t

$$\boxed{\mathrm{pK}^t(x, y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$$

- coding theorem for pK^t

$$\boxed{\mathrm{pK}^t(x) \leq \log\left(1/D(x)\right) + \mathbf{log}(t)}$$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t $\boxed{\mathrm{pK}^t(x,y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for pK^t $\boxed{\mathrm{pK}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

- $\mathrm{pK}^{\mathrm{poly}(2t)}(y_t \mid x) \lesssim \mathrm{pK}^{2t}(x, y_t) - \mathrm{pK}^{\mathrm{poly}(2t)}(x)$
- $\lesssim |y_t| - \mathrm{pK}^{\mathrm{poly}(2t)}(x)$
- $= \mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(2t)}(x)$

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t $\boxed{\mathrm{pK}^t(x, y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for pK^t $\boxed{\mathrm{pK}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

- $\mathrm{pK}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$

We want $\mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$ to be small for an average x.

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t $\quad \boxed{\mathrm{pK}^t(x,y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for pK^t $\quad \boxed{\mathrm{pK}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

- $\mathrm{pK}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$

We want $\mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$ to be small for an average x.

But this requires coding for rK^t...

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t $\boxed{\mathrm{pK}^t(x,y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for pK^t $\boxed{\mathrm{pK}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

- $\mathrm{pK}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$
- $\leq O\big(\mathrm{pK}^t(x) - \mathrm{K}(x)\big)$

via a magical lemma that we proved!

Proof Overview

If MINrKT is easy on average, then we have

- symmetry of information for pK^t $\boxed{\mathrm{pK}^t(x,y) \geq \mathrm{pK}^{\mathrm{poly}(t)}(x) + \mathrm{pK}^{\mathrm{poly}(t)}(y \mid x) - \mathbf{log}(t)}$
- coding theorem for pK^t $\boxed{\mathrm{pK}^t(x) \leq \log(1/D(x)) + \mathbf{log}(t)}$

Fix x and t, let y_t be a shortest t-time randomized program that outputs x.

- $\mathrm{pK}^{\mathrm{poly}(t)}(y_t \mid x) \lesssim \mathrm{rK}^t(x) - \mathrm{pK}^{\mathrm{poly}(t)}(x)$
- $\leq O\big(\mathrm{pK}^t(x) - \mathrm{K}(x)\big)$

via a magical lemma that we proved!

This is small for an average x, by the coding theorem for pK^t

Open Problems

- Can we get worst-case search-to-decision reductions?

Theorem [This work]

MINrKT is easy on average $\Rightarrow$ An algorithm **A** that, given x, runs in $2^{O(n/\log n)}$ time and outputs an $o(1)$-rK^t witness of x, for some $\mathrm{poly}(n) \leq t \leq 2^{n^{\varepsilon}}$

Thank you!