One-Way functions and Polynomial Time Dimension

Satyadev Nandakumar, Subin Pulari, Akhil S, Suronjona Sarma

February 27, 2025

Outline

Introduction and Motivation

- Polynomial-time Dimension:
  Quantifies **information density** of infinite binary strings.
  With polynomial-time resource bounds.
- Two approaches:
  1. $\mathrm{cdim}_{\mathrm{P}}$: Defined using *s-gales* (betting strategies).
  2. $\mathcal{K}_{\mathrm{poly}}$: Using *time-bounded Kolmogorov complexity*.
- Robustness question: *Are these two notions equivalent?*
- Our Result :
  One-way functions $\iff$ Dimension gaps for a "Large" collection of sequences.

Polynomial Time Dimension ($\mathrm{cdim}_{\mathrm{P}}$)

- s-gale : $d : \Sigma^* \to [0, \infty)$ such that
$$d(w0) + d(w1) = 2^s \cdot d(w).$$
- Poly-time s-gale : $d : \Sigma^* \to \mathbb{Q}$ such that
$$d(w) \text{ runs in time } |w|^k.$$

$\mathrm{cdim}_{\mathrm{P}}$

For an infinite binary sequence $X \in \Sigma^\infty$, define

$$\mathrm{cdim}_{\mathrm{P}}(X) = \inf_s \{\exists \text{ poly-time } s\text{-gale } d \ : \ \limsup_n d(X \upharpoonright n) = \infty\}.$$

Polynomial Time Dimension ($\mathrm{cdim}_{\mathrm{P}}$)

For an infinite binary sequence $X \in \Sigma^\infty$, define

$$\mathrm{cdim}_{\mathrm{P}}(X) = \inf_s \{\exists \text{ poly-time } s\text{-gale } d \quad : \quad \limsup_n d(X \upharpoonright n) = \infty\}.$$

For a set of sequences $\mathcal{F} \subseteq \Sigma^\infty$, define

$$\mathrm{cdim}_{\mathrm{P}}(\mathcal{F}) = \inf_s \{\exists \text{ poly-time } s\text{-gale } d : \forall X \in \mathcal{F}, \limsup_n d(X \upharpoonright n) = \infty\}.$$

Kolmogorov Complexity approach ($\mathcal{K}_{\mathrm{poly}}$)

For a finite string $x \in \Sigma^*$, for a time function $t(n)$,

$$K_t(x) = \min\{|\Pi| \ : \ \mathcal{U}_t(\Pi) = x\}.$$

- Length of the shortest description of x from which a $t(n)$-time algorithm can recover x.

$\mathcal{K}_{\mathrm{poly}}$

For an infinite string $X \in \Sigma^\infty$:

$$\mathcal{K}_{\mathrm{poly}}(\mathcal{F}) = \inf_{t \in \mathrm{poly}} \liminf_{n \to \infty} \frac{K_t(X \restriction n)}{n}.$$

Kolmogorov Complexity approach ($\mathcal{K}_{\text{poly}}$)

For an infinite string $X \in \Sigma^\infty$:

$$\mathcal{K}_{\text{poly}}(\mathcal{F}) = \inf_{t \in \text{poly}} \liminf_{n \to \infty} \frac{K_t(X \upharpoonright n)}{n}.$$

For a set of infinite strings $\mathcal{F} \subseteq \Sigma^\infty$:

$$\mathcal{K}_{\text{poly}}(\mathcal{F}) = \inf_{t \in \text{poly}} \sup_{X \in \mathcal{F}} \liminf_{n \to \infty} \frac{K_t(X \upharpoonright n)}{n}.$$

Robustness in the Classical Setting

Theorem (Mayordomo, Lutz)

For all $\mathcal{F} \subseteq \Sigma^\infty$,

$$\mathrm{cdim}(\mathcal{F}) = \sup_{X \in \mathcal{F}} \liminf_{n \to \infty} \frac{K(X \upharpoonright n)}{n}.$$

Theorem (Hitchcock , Vinodchandran)

For every $\mathcal{F} \subseteq \Sigma^\infty$,

$$\mathrm{cdim}_{\mathrm{PSPACE}}(\mathcal{F}) = \mathcal{K}_{\mathrm{PSPACE}}(\mathcal{F}).$$

Robustness in the Polynomial-Time Setting ?

- Hitchcock, Vinodchandran [2005] : For all $\mathcal{F} \subseteq \Sigma^\infty$,

$$\mathcal{K}_{\text{poly}}(\mathcal{F}) \leq \text{cdim}_{\text{P}}(\mathcal{F}).$$

- However, the reverse inequality remains elusive.

Question

Is it true that, for every sequence $X \in \Sigma^\infty$,

$$\text{cdim}_{\text{P}}(X) = \mathcal{K}_{\text{poly}}(X)?$$

Our Main Results

- We resove this by relating it to the existence of one-way functions.
- One-way functions $\implies \mathrm{cdim}_{\mathrm{P}} \neq \mathcal{K}_{\mathrm{poly}}$.

Our Main Results

- We resove this by relating it to the existence of one-way functions.
- One-way functions $\implies \mathrm{cdim}_{\mathrm{P}} \neq \mathcal{K}_{\mathrm{poly}}$.
- OWF $\implies \nu \{X : \mathrm{cdim}_{\mathrm{P}}(X) \neq \mathcal{K}_{\mathrm{poly}}(X)\} = 1$,
- (Converse) Dimension gap $\implies$ (infinitetly-often) OWF.

Dimension Gaps from One-Way Functions

Lemma

If one-way functions exist, then for all $s < 1/2$, there exists a set $\mathcal{F} \subseteq \Sigma^\infty$ such that:

$$\mathcal{K}_{\mathrm{poly}}(\mathcal{F}) \leq s \quad \textit{and} \quad \mathrm{cdim}_{\mathrm{P}}(\mathcal{F}) \geq 1/2.$$

Proof Ideas: Overview

- Assume one-way functions exist.
- For all $s < 1$, this implies the existence of pseudorandom generators

  $$\text{(PRGs) } \{G_n : \Sigma^{sn} \to \Sigma^n\}_{n\in\mathbb{N}}$$

  running in polynomial time.
- We use these PRG's to construct a *short seed map*

  $$g : \Sigma^\infty \to \Sigma^\infty.$$

Construction of g

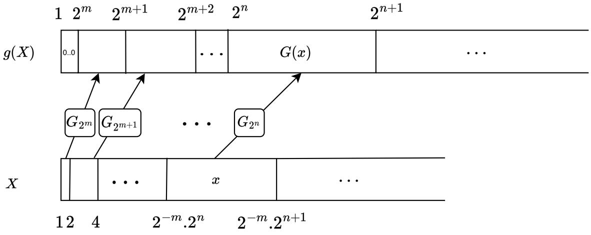


Figure: Illustration of $g(X)$.

Proof Ideas: Overview

- We use these PRG's $G_n : \Sigma^{sn} \to \Sigma^n$ to construct a *short seed map*

$$g : \Sigma^\infty \to \Sigma^\infty.$$

- We show :
  1. $\mathcal{K}_{\text{poly}}(\mathcal{F} = g(\Sigma^\infty)) \leq s$.
  2. For any $s' \in (s, 1/2)$,
     exists an s'-gale d that succeeds on $\mathcal{F} \implies$
     exists a *distinguisher* A that breaks the PRG

     $\therefore$ *OWF* $\implies \text{cdim}_{\text{P}}(\mathcal{F}) \geq 1/2$.

Breaking a PRG

- The PRG $\{G_n\}_n$ is broken if there exists
A polynomial-time algorithm $\mathcal{A}$ (Distinguisher) such that
for infinitely many n and some constant c:

$$\left| \Pr_{x \sim U_{s.n}} [\mathcal{A}(G_n(y)) = 1] - \Pr_{r \sim U_n} [\mathcal{A}(r) = 1] \right| \geq 1/n^c.$$

Breaking the PRG via gales

- We have an s'-gale d that succeeds on all $Y \in g(\Sigma^\infty)$.
- Using standard techniques, convert d into a martingale $\tilde{d}$ such that for all $Y \in g(\Sigma^\infty)$:

$$\tilde{d}(Y \upharpoonright 2^{n+1}) > 2^{(1-\tilde{s})2^n} \tilde{d}(Y \upharpoonright 2^n),$$

for infinitely many n and some $\tilde{s} \in (2s', 1)$.

The Distinguisher Algorithm

- Construct a polynomial-time distinguisher A:
  1. On an input w of length 2^n, randomly choose $r \in \Sigma^{s \cdot 2^n}$.
  2. Compute $w' = g(r)$.
  3. Output 1 if
  $$\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w'),$$
  and output 0 otherwise.

Performance of A on PRG Outputs

- Use Borell-Cantelli Lemma to get a uniform bound over a positive measure-subset.

$$\nu(\mathcal{F}) = \mu(g^{-1}(\mathcal{F})).$$

$\nu(g(\Sigma^\infty)) = 1.$

Borel Cantelli:

$$\nu(\{Y : \tilde{d}(Y \upharpoonright 2^{n+1}) > 2^{(1-\tilde{s})2^n}\tilde{d}(Y \upharpoonright 2^n)\}) \geq 1/n^2.$$

Borel Cantelli Lemma

Define

- $f_n(Y) = 1$ iff $\tilde{d}(Y \upharpoonright 2^{n+1}) > 2^{(1-\tilde{s})2^n} \tilde{d}(Y \upharpoonright 2^n)$.
- $A_n = \{Y : f_n(Y) = 1\}$

We have :

- For all $Y \in g(\Sigma^\infty)$, $\exists^\infty n$ s.t $f_n(Y) = 1$.
- $\nu(\limsup A_n) = 1$.
- Borel Cantelli : $\sum_n \nu(A_i) = \infty$.

$$\exists^\infty n \text{ s.t } \nu(A_n) > 1/n^2.$$

Performance of A on PRG Outputs

Let n be such that $\nu(A_n) > 1/n^2$.

$$\Pr_{x\sim U_{s.2^n}}[\mathcal{A}(G(x)) = 1] = \Pr_{x\sim U_{s.2^n}} \Pr_{r\sim U_{s.2^n}}[\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w')]$$
$$= \nu(\{Y : \tilde{d}(Y \restriction 2^{n+1}) > 2^{(1-\tilde{s})2^n}\tilde{d}(Y \restriction 2^n)\})$$
$$\geq 1/n^2.$$

$\exists^\infty n$ s.t $\quad \Pr_{x\sim U_{s.2^n}}[\mathcal{A}(G_n(x)) = 1] \geq 1/n^2$.

Performance of A on random inputs

Kolmogorov inequality : For any $w' \in \Sigma^{2^n}$,

the number of $w \in \Sigma^{2^n}$ such that $\tilde{d}(w'w) \geq 2^{(1-\tilde{s})|w|} \cdot \tilde{d}(w')$

is less than $2^n / 2^{-(1-\tilde{s})|w|}$

$$\forall n, \qquad \Pr_{y \sim U_{2^n}}[\mathcal{A}(y) = 1] \leq 1/2^{(1-\tilde{s}).2^n}.$$

OWF's and roboustness

There exists infintely many n such that

$$\Pr_{x \sim U_{s.2^n}}[\mathcal{A}(G(x)) = 1] - Pr_{y \sim U_{2^n}}[\mathcal{A}(y) = 1] \geq 1/n^2.$$

- Thus if $\forall \mathcal{F} \subseteq \Sigma^{\infty},\ \mathrm{cdim}_{\mathrm{P}}(\mathcal{F}) = \mathcal{K}_{\mathrm{poly}}(\mathcal{F})$,

  $\implies$ PRGs $\{G_n : \Sigma^{sn} \to \Sigma^n\}$ do not exist

  $\implies$ OWF's do not exist.

Main Theorem

Theorem

Suppose that one-way functions exist. Then, for every $s < \frac{1}{2}$, there exists a short seed polynomial-time samplable distribution ν over Σ^∞ such that:

1. *For every $s' \in (s, \frac{1}{2})$ and every polynomial-time ν-approximable s'-supergale d,*

$$\nu(S^\infty(d)) = 0.$$

Furthermore, this implies the existence of infinitely-often one-way functions.

Polynomial Time Samplable Distribution

Definition (Polynomial Time Samplable Distribution)

A measure ν over Σ^{∞} is *short seed polynomial time samplable* if : there exists a Turing machine M that uses $s.n$ random bits, where $s < 1$, such that for every n and $w \in \Sigma^n$,

$$\Pr_{r \sim \Sigma^{q(n)}}[M(1^n, r) = w] = \nu_n(w).$$

OWF's and roboustness of sequences

We now extend the result to sequences :

- If $\forall X \in \Sigma^\infty, \;\; \mathrm{cdim}_{\mathrm{P}}(X) = \mathcal{K}_{\mathrm{poly}}(X)$,

  $\implies$ PRGs $\{G_n : \Sigma^{sn} \to \Sigma^n\}$ do not exist

  $\implies$ OWF's do not exist.

OWF's and roboustness of sequences

We construct an (almost) Universal polytime-gale .

Poly-time gale combination :

Theorem

There exist a $t(n) \cdot n \log(n)$-time s-gale d s.t
for all $t(n)$-time s-gales d', there exist a constant $c_{d'}$ s.t

$$\forall X \in \Sigma^{\infty}, n \in \mathbb{N}, \qquad d(X \upharpoonright n) \geq c_d' \cdot d(X \upharpoonright n).$$

Corollary : There exists a poly-time s-gale d that succeeds on a ν-positive measure subset of $g(\Sigma^{\infty})$.

Converse

Theorem

If, for some $s < 1$, there exists a polynomial-time samplable distribution ν over Σ^∞ such that:

1. *The number of random bits used by the sampler for ν on input 1^n is at most sn.*
2. *For every $s' \in (s, \frac{1}{2})$ and every polynomial-time ν-approximable s'-supergale d,*

$$\nu(S^\infty(d)) = 0.$$

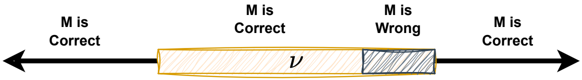
Then infinitely-often one-way functions exist.

ν-approximable supergale

Let $d : \Sigma^* \to [0, \infty) \cap \mathbb{Q}$ be an s-supergale and ν be any probability distribution over Σ^∞.

d is $t(n)$-time ν-approximable if for $\forall k$ $\exists$ probabilistic $t(n)$-time machine M and constant $c < 1$, s.t $\forall n$,

- $\{w \in \Sigma^n : M(w) \notin [c \cdot d(w), d(w)]\} \subseteq \mathrm{supp}(\nu_n)$
- $\nu_n\{w \in \Sigma^n : M(w) \notin [c \cdot d(w), d(w)]\} \leq n^{-k}$.



Proof Overview:

Construct d such that $\nu(S^{\infty}(d)) = 1$

$\neg$i. o. OWFs $\implies$ we can ν approximate d

Contradiction to (2)

Proof: Construct gale d s.t. $\nu(\mathbf{S^\infty(d)}) = \mathbf{1}$

Let there be ν such that condition (1) and (2) holds.

Construct supergale: $d(w) = 2^{s'|w|}\nu(w)$
Property: From (1), we have, $\nu_n(w) \geq \frac{1}{2^{|w|\cdot s}}$
$\implies d(w) \geq 2^{|w|(s'-s)}$ ....$(*)$

Claim: $\nu(\mathbf{S^\infty(d)}) = \mathbf{1}$
Proof: $\forall X \in supp(\nu)$
$(*) \implies d(X \restriction n) \geq 2^{n(s'-s)} > 1$
$\implies \lim_{n\to\infty} d(X \restriction n) = \infty$

$\{X : \lim_{n\to\infty} d(X \restriction n) = \infty\} \supseteq supp(\nu)$
$\implies \nu\{X \in \Sigma^\infty : \limsup_{n\to\infty} d(X \restriction n) > \nu\{supp(\nu)\}\infty\} = 1.$

$\neg$ i.o. OWF $\implies$

Let S be a machine s.t. $\forall n\ \forall w \in \Sigma^n$,
$\Pr_{r \leftarrow U_{n^{c'}}} [S(1^n, r) = w] = \nu_n(w)$
Let $f(w) = S(1^{|w|^{c'}}, w)$

$\neg$ i.o. OWF $\implies$

- **Inverter for sampler f:** f can be inverted by $\mathcal{I}$ w.p. $\geq 1 - O\left(\frac{1}{n^q}\right)$ for any $q > 1$
- **Approximating algo for $\nu_\mathbf{n}$:** $\exists$ PPT algo $\mathcal{A}$ and $c < 1$, s.t.

$\Pr_{w \sim \nu_n}[c \cdot \nu_n(w) \leq \mathcal{A}(w) \leq \nu_n(w)] \geq 1 - O\left(\frac{1}{n^q}\right)$. [IRS]

Lemma from [IRS'22]

Theorem

Assume i.o. one-way functions do not exist. Let $\mathcal{D} = \{\mathcal{D}_n\}$ be a poly time samplable distribution and $q \geq 1$. Then, $\exists$ PPT algo $\mathcal{A}$ and constant $c < 1$ such that $\forall n$,

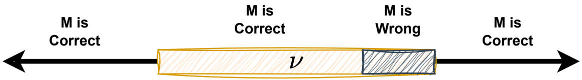
$$\Pr_{x \sim \mathcal{D}_n}[c \cdot \mathcal{D}_n(x) \leq \mathcal{A}(x) \leq \mathcal{D}_n(x)] \geq 1 - O\left(\frac{1}{n^q}\right).$$

Use inverter $\mathcal{I}$ and approximating algo $\mathcal{A}$ to ν-approximate d

Construct $M(w)$ s.t.:

- Run $\mathcal{I}(w)$
- If $(f(\mathcal{I}(w)) \neq w)$:
  - Output 0
- Else:
  - Run $\mathcal{A}(w)$
  - Output $2^{s'|w|}\mathcal{A}(w)$

Conditions for ν-approximation



- **Condition 1.** If $\nu(w) = 0 \implies w \notin \mathrm{supp}(\nu_n)$
  $\implies \mathcal{I}$ doesn't invert $f \implies M$ outputs 0
  $\implies \{w : M(w) \notin [c \cdot d(w), d(w)]\} \subseteq \mathrm{supp}(\nu_n)$

- **Condition 2.** [IRS] $\implies \mathcal{A}$ approximates ν_n
  $\implies M$ approximates d w.p. $\geq 1 - O\left(\frac{1}{n^q}\right)$
  $\implies \forall n, \nu\{w : M(w) \notin [c \cdot d(w), d(w)]\} \leq O\left(n^{-q}\right)$

Therefore, machine M ν-approximates d. [Contradiction]

Conclusion and Future Work

- We showed that (i.o) One-way functions exist $\iff$ dimension gaps for a "Large" collection of sequences.
- **Future Directions:**
  - Dimension separation from milder assumptions. DistP $\neq$ DistNP $\implies \mathrm{cdim}_{\mathrm{P}} \neq \mathcal{K}_{\mathrm{poly}}$?

Thank You!

Questions?