One-Way functions and Polynomial Time Dimension

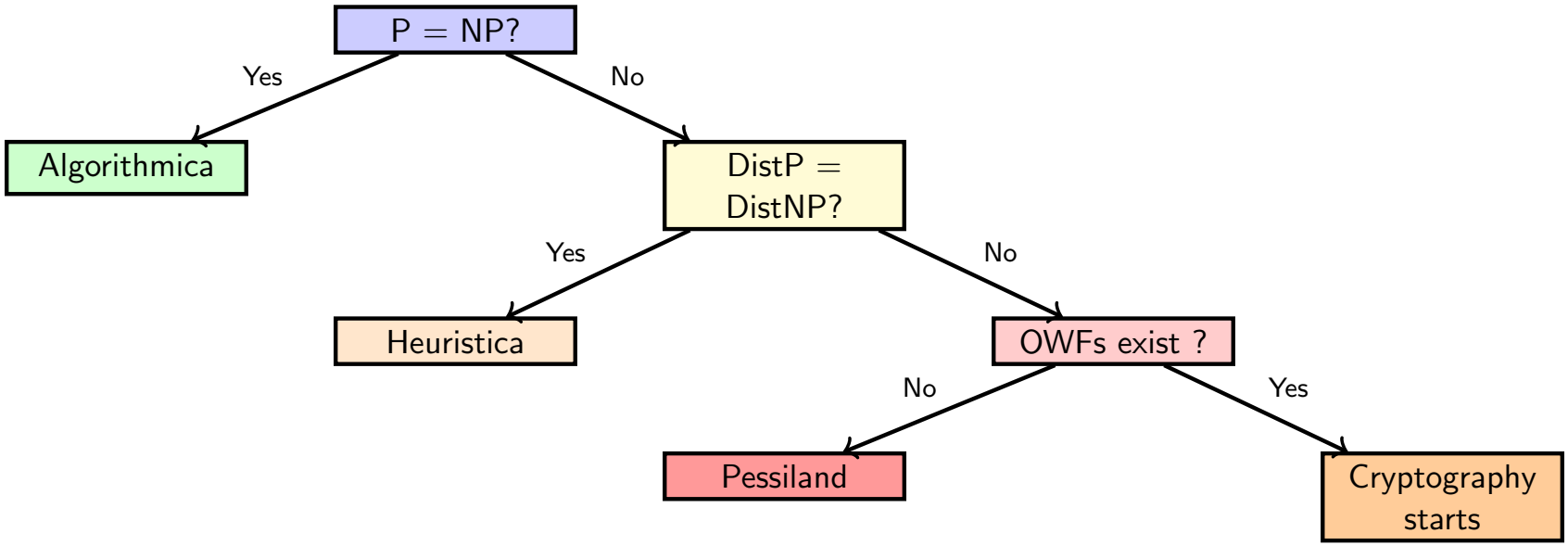
Satyadev Nandakumar, Subin Pulari, Akhil S, Suronjona Sarma

January 21, 2025

Overview

- Polynomial time dimension ($\mathrm{cdim_P}$) : quantifies information density in infinite binary strings.
  - Measured using betting algorithms called *s*-gales.
- Time-bounded Kolmogorov complexity ($\mathcal{K}_{\mathrm{poly}}$) measures compressibility of finite prefixes of sequences.
- Long-standing open question: Is $\mathrm{cdim_P} = \mathcal{K}_{\mathrm{poly}}$? [Hitchcock, Vinodchandran CCC 2004]
  - We show : OWF $\implies \mathrm{cdim_P} \neq \mathcal{K}_{\mathrm{poly}}$.

Impagliazzo's Five Worlds



Meta-Complexity

Minimum Circuit Size Problem (MCSP)

Given a Boolean function f, and an integer s,

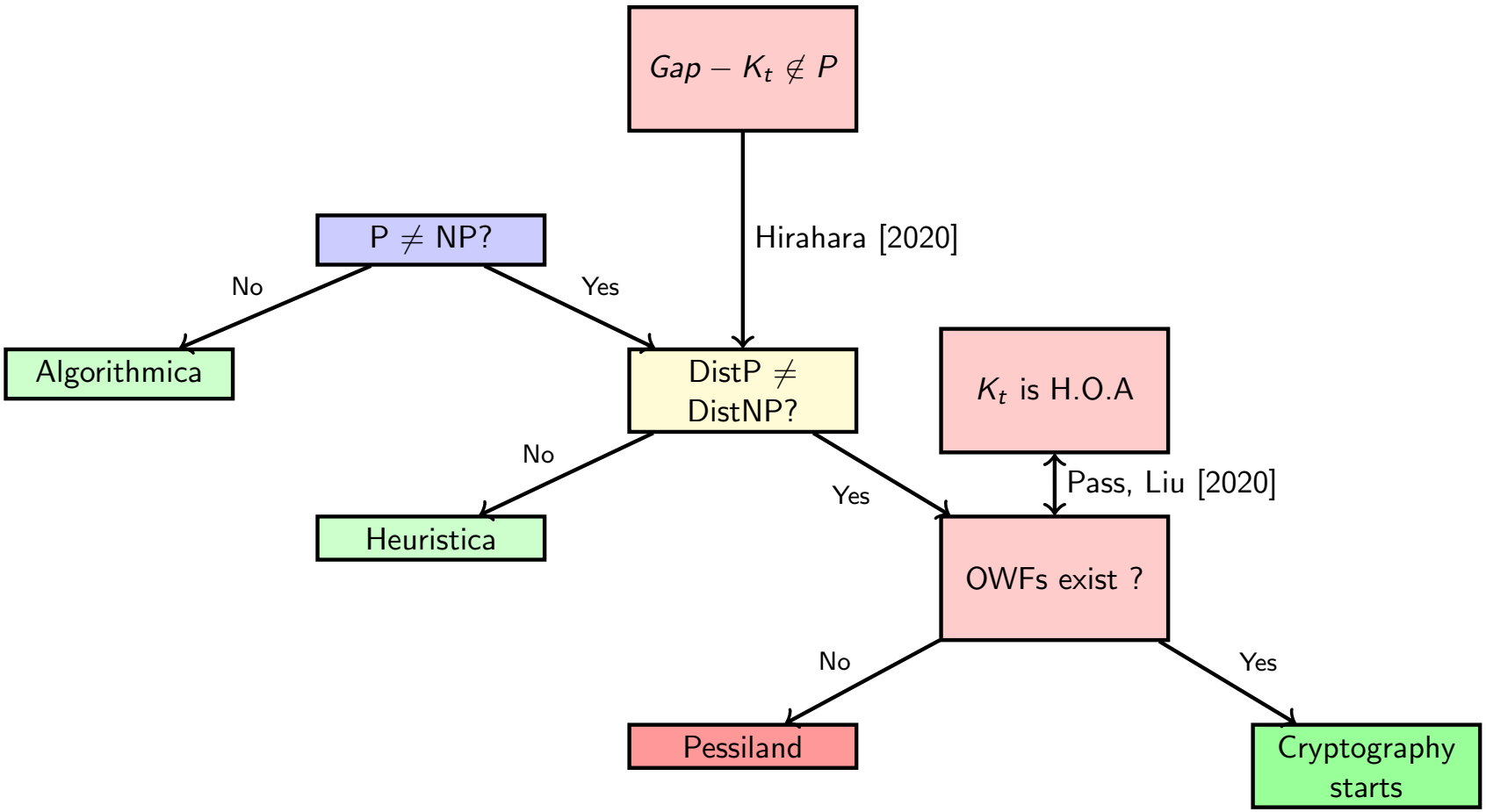
Is there a circuit of size $\leq s$ that can compute f ?

Poly-time Kolmogorov Complexity (MK_tP)

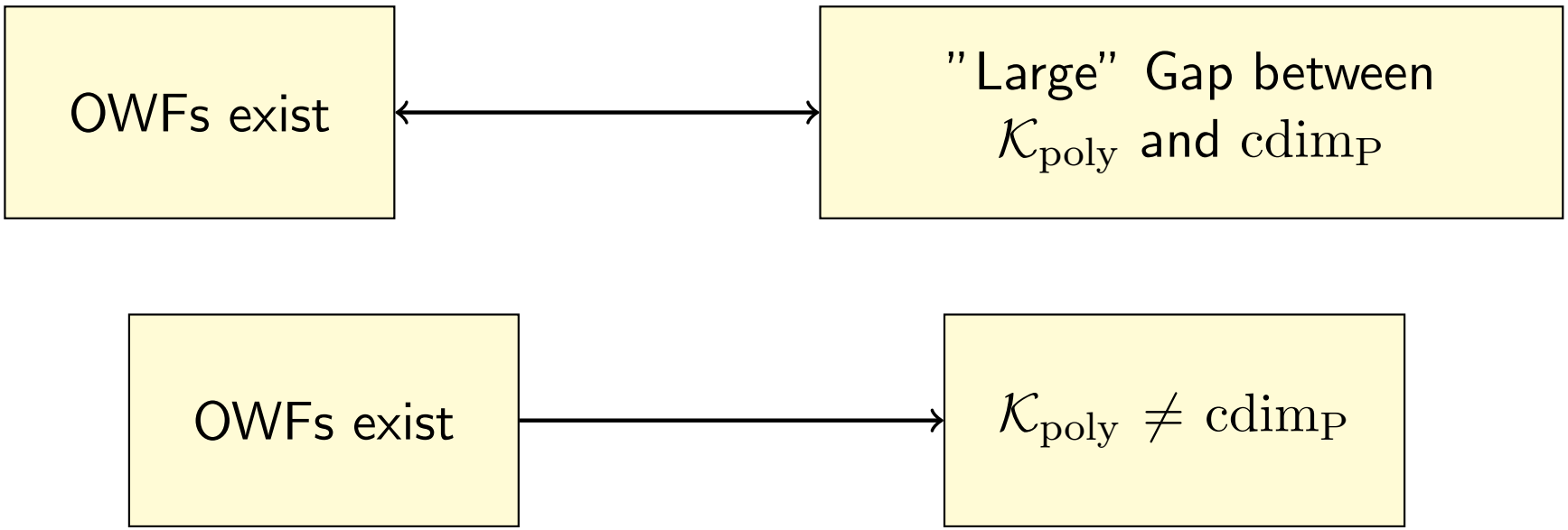
Given a string x , and an integer s,

Is there a $t(n)$-time program p of size $\leq s$ that outputs x ?

Meta-Complexity : Some results

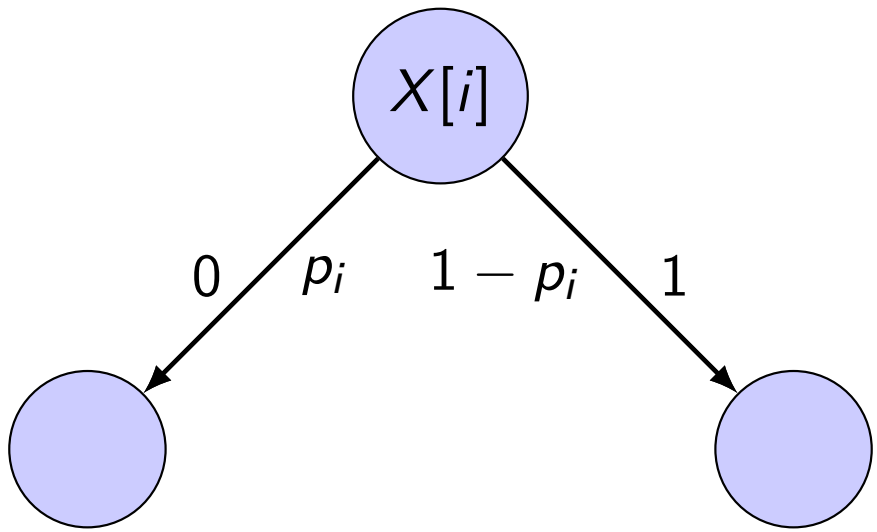


Our Results


OWFs exist
"Large" Gap between $\mathcal{K}_{\text{poly}}$ and cdim_{P}
OWFs exist
$\mathcal{K}_{\text{poly}} \neq \text{cdim}_{\text{P}}$

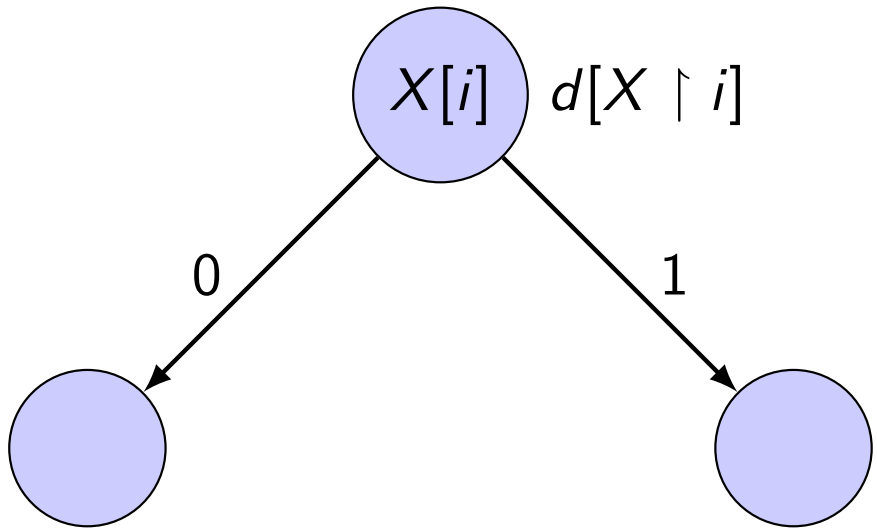
$\mathrm{cdim}_{\mathrm{P}}$

- Defined using **s-gales**: betting algorithms.



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

- Defined using **s-gales**: betting algorithms.



$d[X \upharpoonright i+1] =$

$2^s.p_i.d[X \upharpoonright i]$

$d[X \upharpoonright i+1] =$

$2^s.(1-p_i).d[X \upharpoonright i]$

$\mathrm{cdim_P}$

- Defined using **s-gales**: betting algorithms.

$$\mathrm{cdim_P}(X) = \inf_s \{\exists \text{ poly-time } s-\textit{gale } d \text{ s.t } \limsup_n d(X \upharpoonright n) = \infty\}.$$

Time-Bounded Kolmogorov Complexity (K_t)

- *Compressibility* rate of finite prefixes of a sequence.

$$K_t(x) = \min_p \{|p| : U_{t(|x|)}(p) = x.\}$$

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

Unbounded Time Setting

- Mayordomo and Lutz (2002): Unbounded time notions of information density are equivalent.
- Similar equivalences at PSPACE, finite-state levels.

Question [Hitchcock, Vinodchandran 2005]

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

OWF, $\mathrm{cdim}_{\mathrm{P}}$ and $\mathcal{K}_{\mathrm{poly}}$

Theorem [Akhil, Nandakumar, Pulari, Sharma 2025]

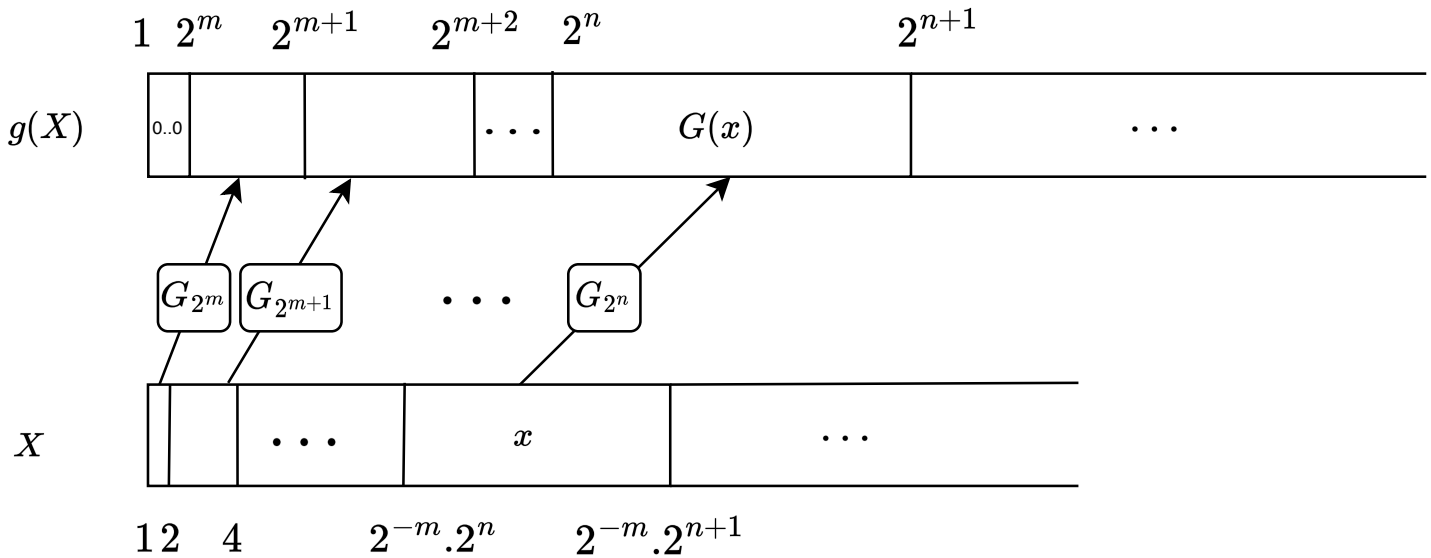
$$\text{OWF exist} \implies \exists X \in \Sigma^{\infty},\ \mathrm{cdim}_{\mathrm{P}}(X) \neq \mathcal{K}_{\mathrm{poly}}(X).$$

Proof Outline

- OWFs $\leftrightarrow$ PRGs [HILL 99] $\quad G_n : sn \to n, s < 1.$
- PRG outputs have **low** K_t by design. $\quad K_t(G_n(x)) \leq |x| = sn.$
- $\mathrm{cdim}_{\mathrm{P}} = \mathcal{K}_{\mathrm{poly}} \implies$ PTIME s-gale d that win on concatenation of PRG outputs.

Proof Outline 2

- $\mathrm{cdim}_{\mathrm{P}} = \mathcal{K}_{\mathrm{poly}} \implies$ PTIME s-gale d that $\limsup d(g(X) \upharpoonright n) = \infty$.



- Use distinguishers A derived from s-gale d to break G.

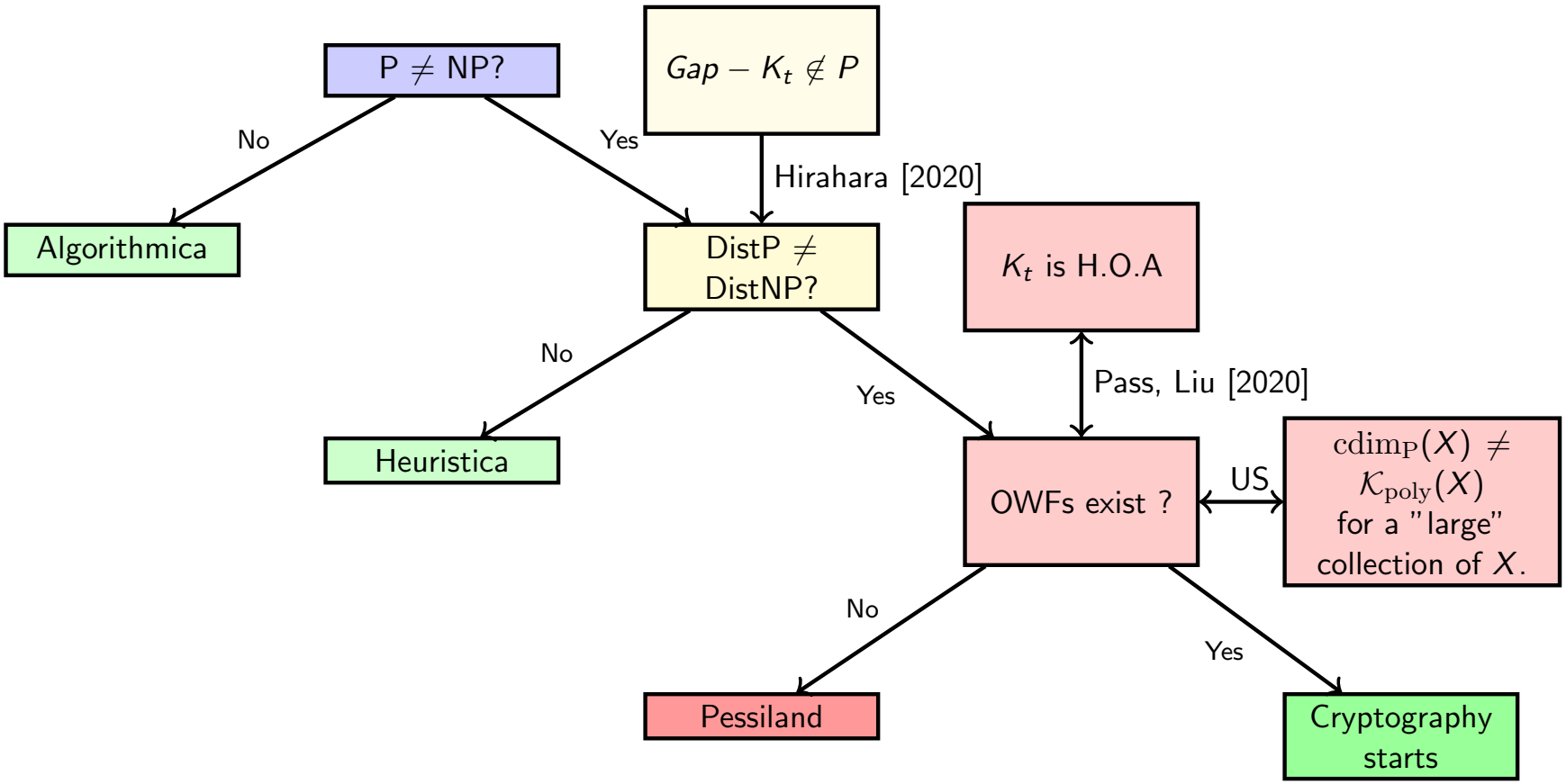
Tools used

- Standard s-gale techniques.
- $\Pr[A(PRG) = 1]$ is high : **Borel-Cantelli Lemma**.
- $\Pr[A(Random) = 1]$ is low : **Kolmogorov Inequality**.

Conclusion

- A characterisation of existence of OWFs using Information theoretic formulation.
- cdimP and Kpoly are distinct under the assumption of OWFs.
- Hope to inspire new connections between meta-complexity, cryptographic theory and information theory.

Meta-Complexity : Some results



Thank you!