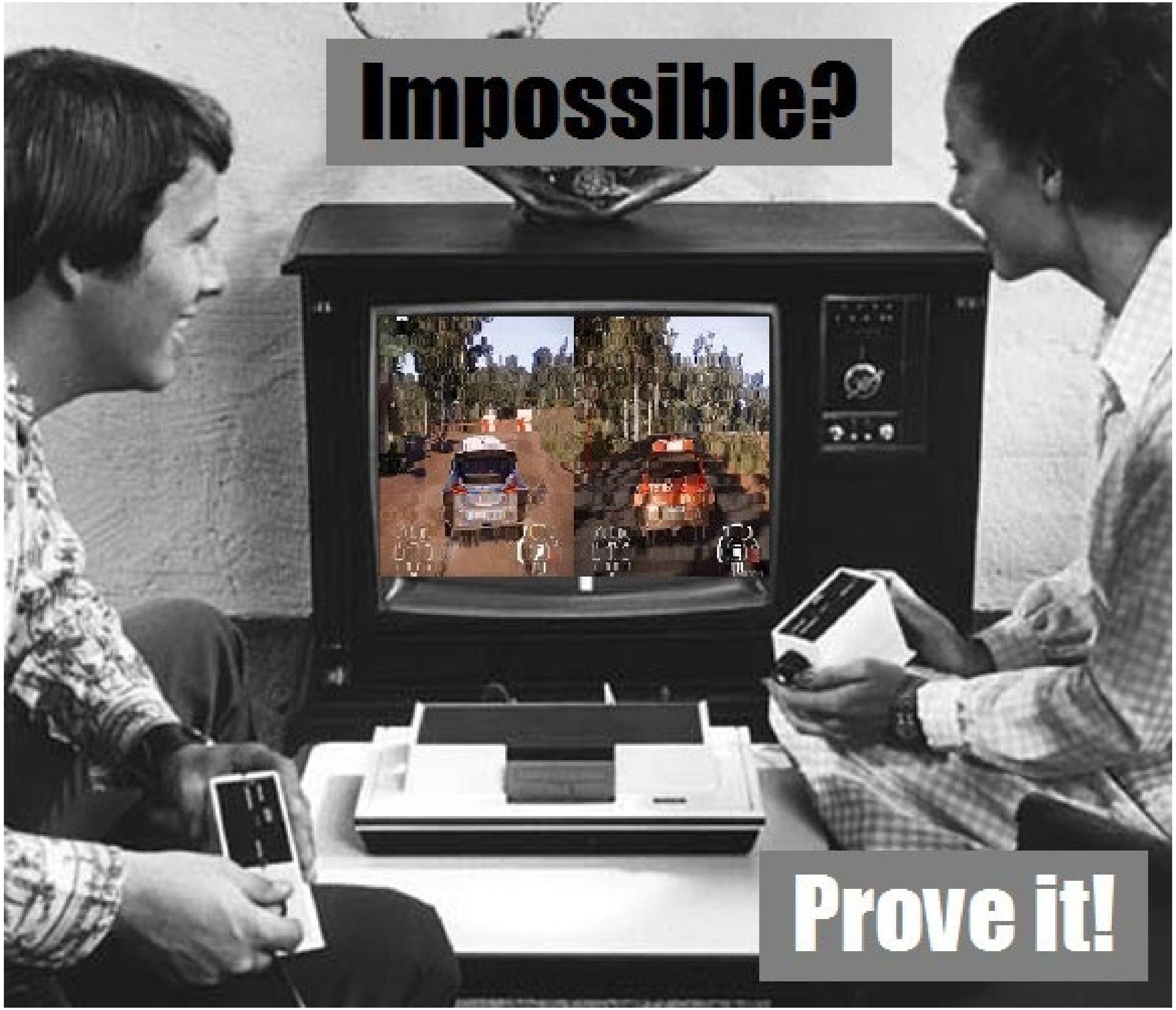
Correlation bounds and all that

Emanuele Viola

Northeastern University

2022 09



3

2

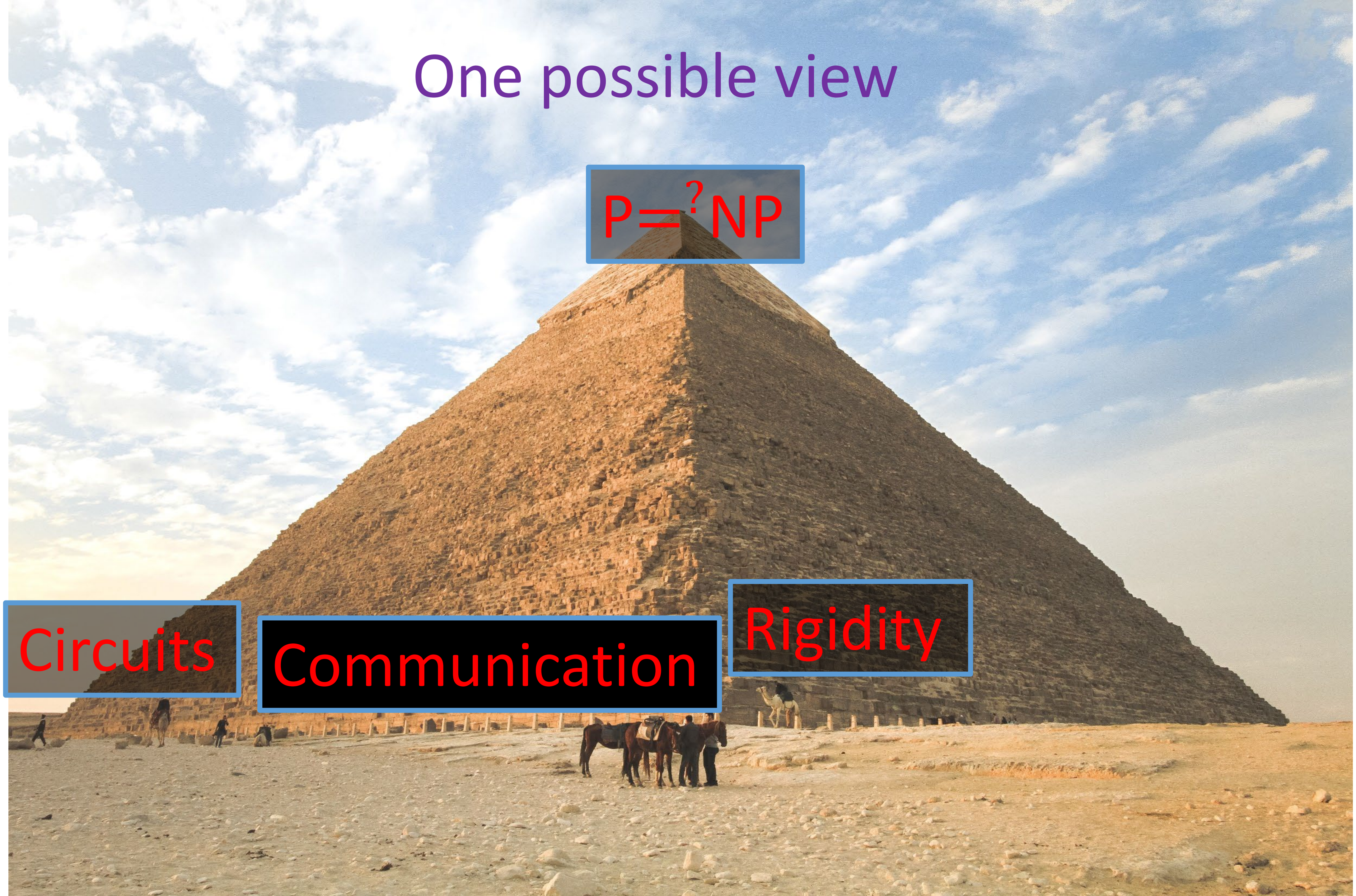
1

One possible view

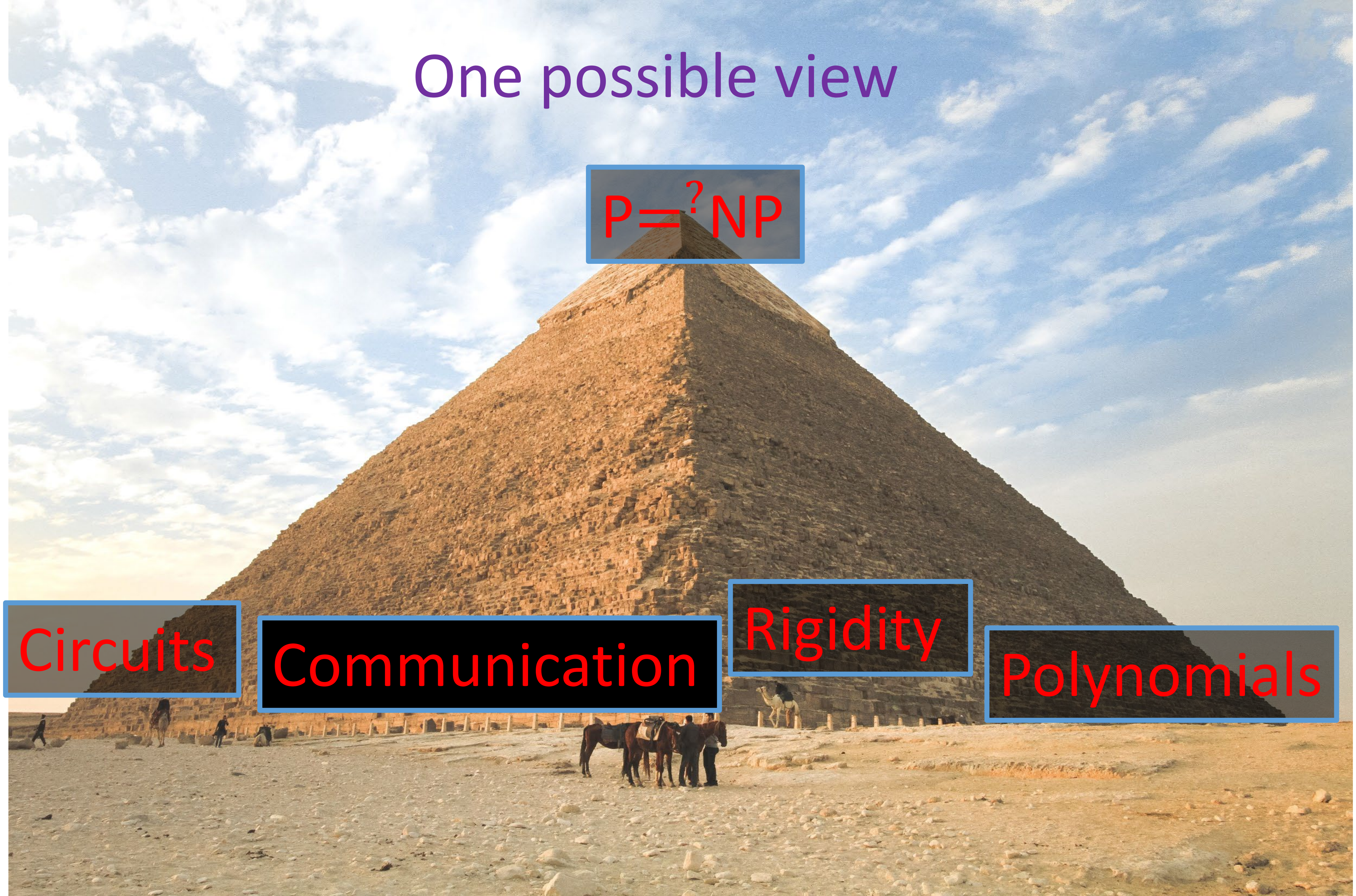
One possible view

One possible view

One possible view

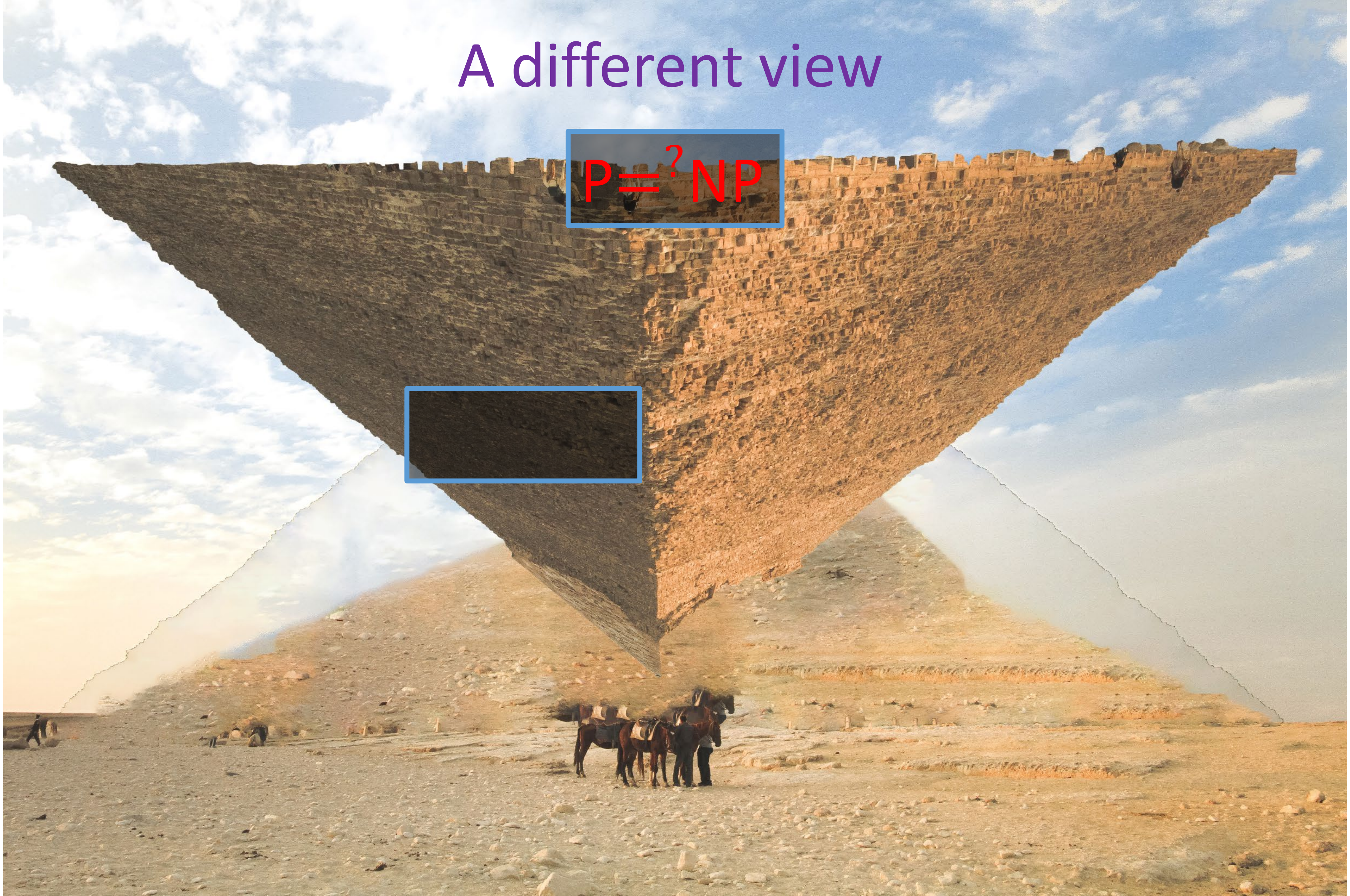


One possible view

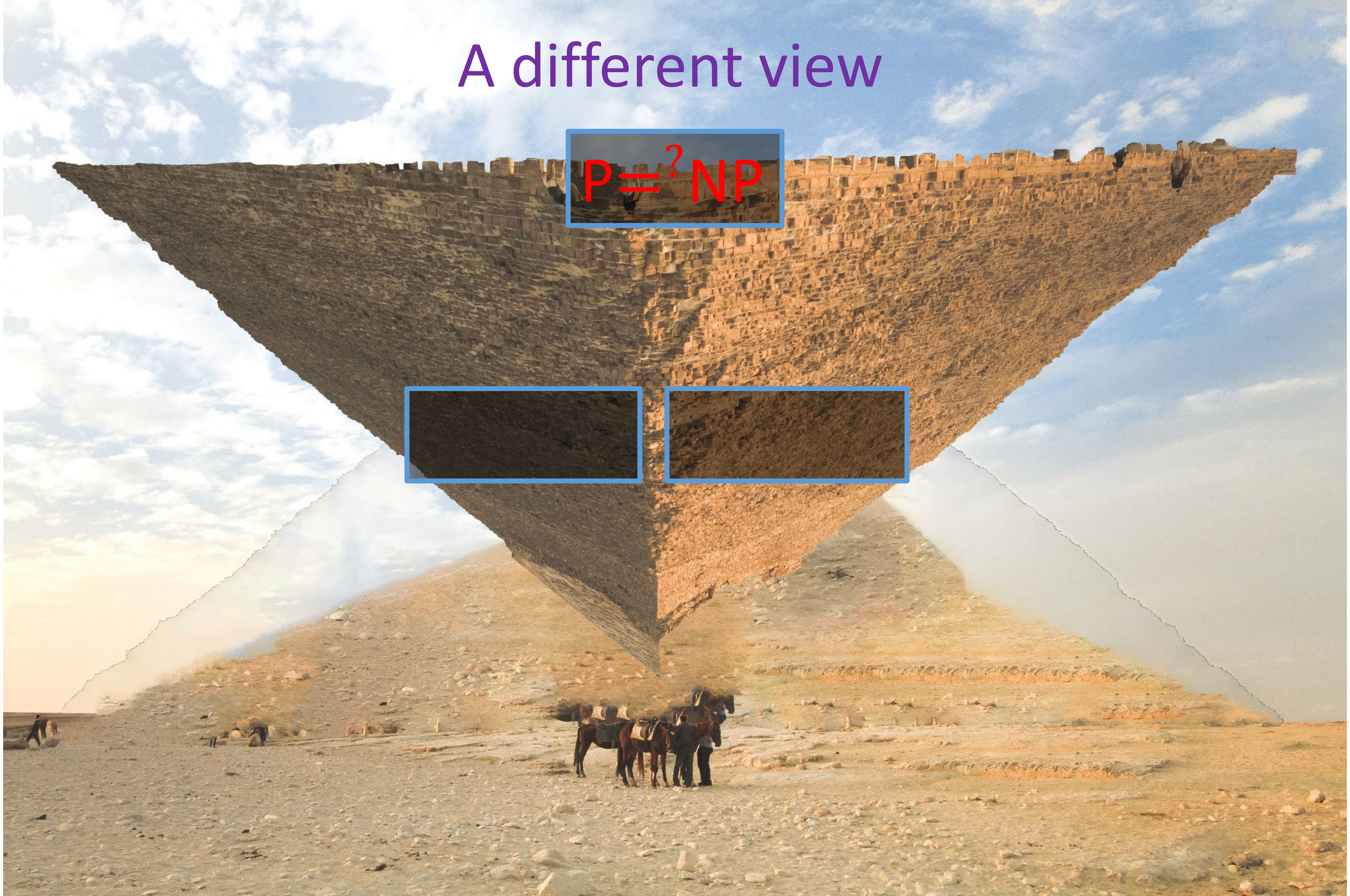


A different view

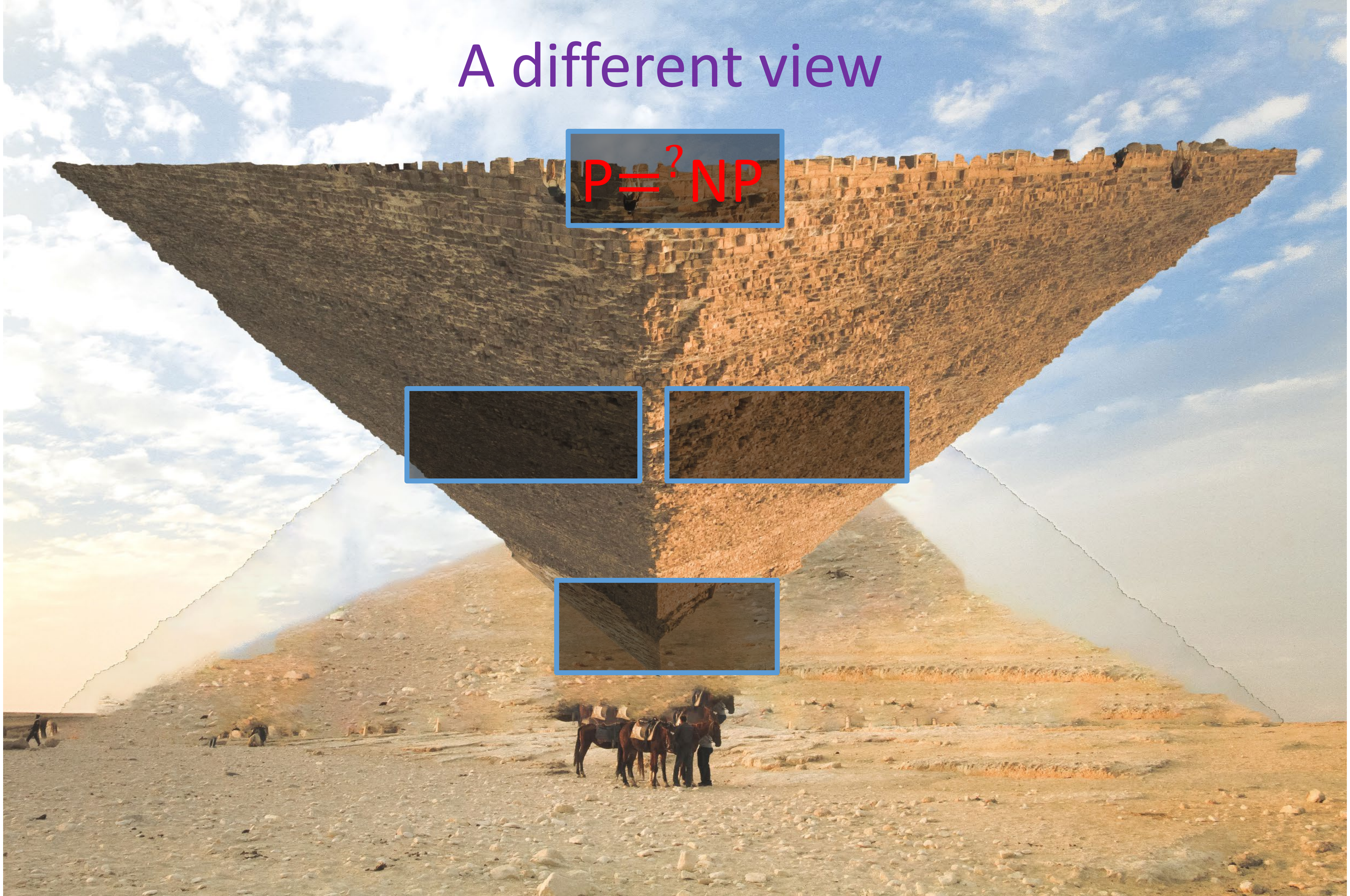
A different view



A different view

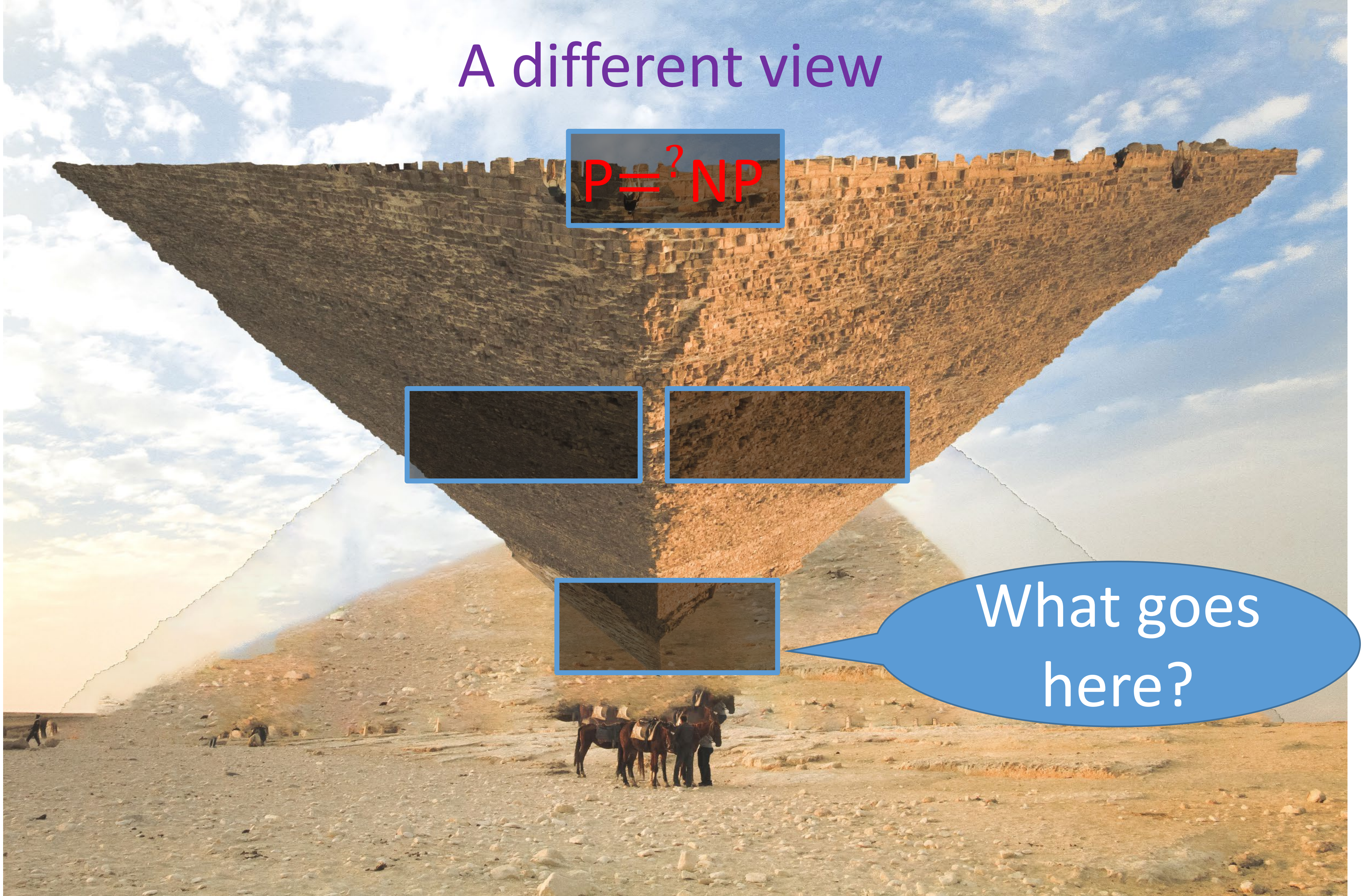


A different view



$P \stackrel{?}{=} NP$

A different view



Frontier of P vs. NP

Circuit lower bounds

Frontier of P vs. NP

Circuit lower bounds

Matrix rigidity

Frontier of P vs. NP

Circuit lower bounds

Matrix rigidity

Correlation bounds for polynomials

Frontier of P vs. NP

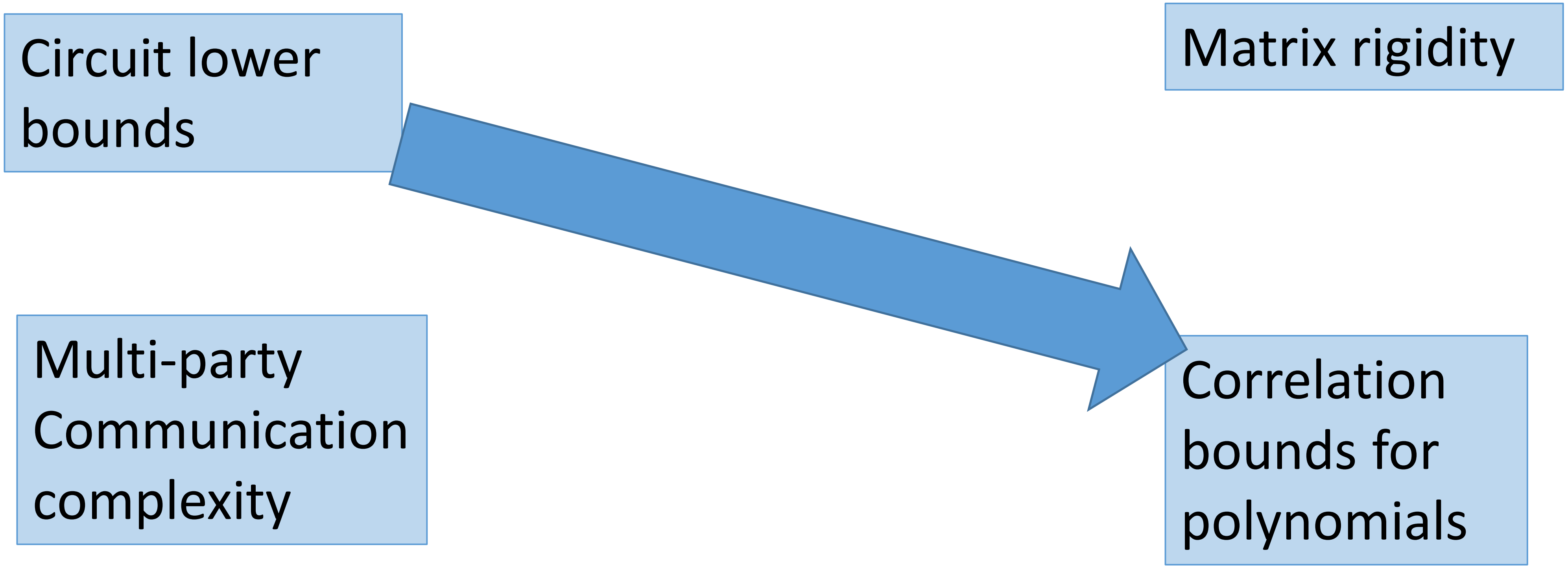
Circuit lower bounds

Matrix rigidity

Multi-party Communication complexity

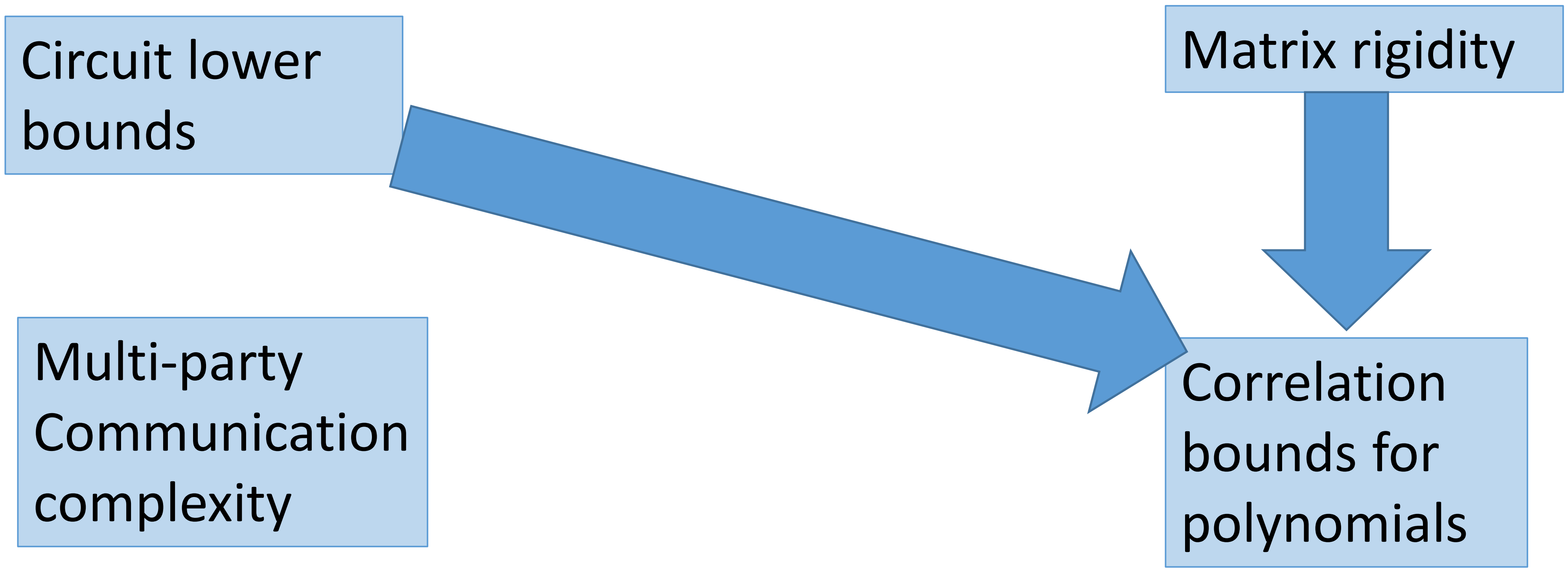
Correlation bounds for polynomials

Frontier of P vs. NP



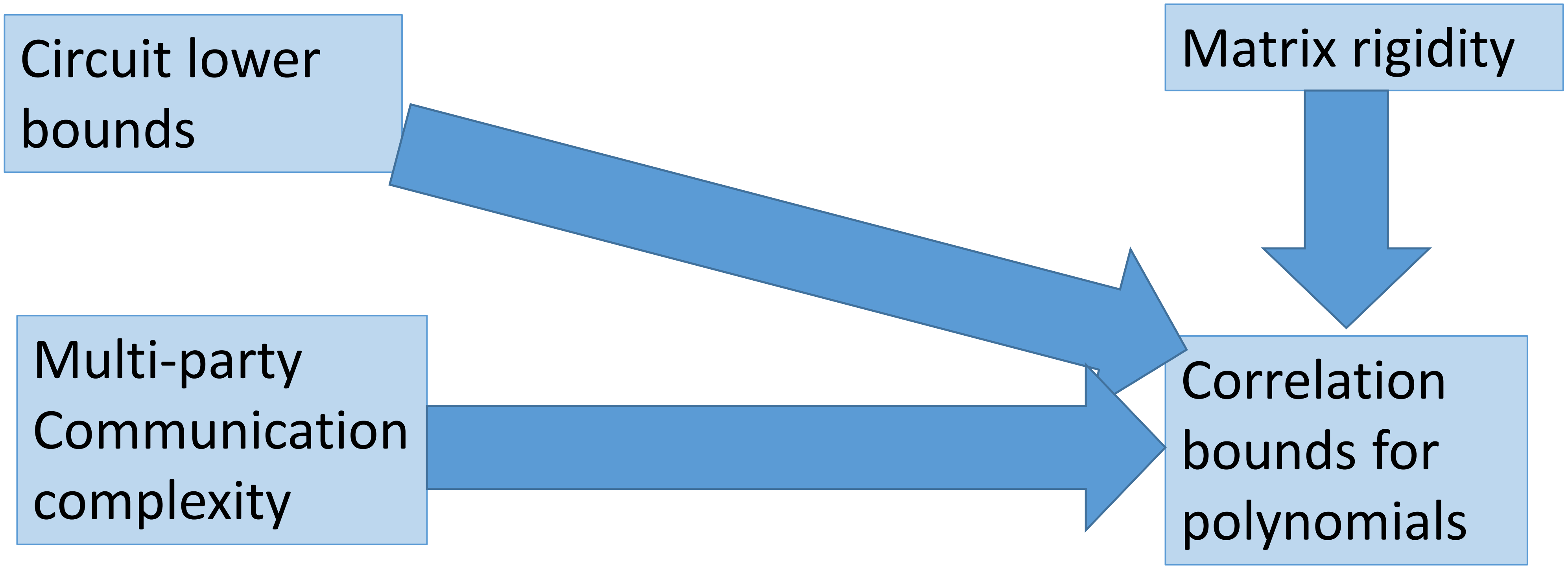
A $\Longrightarrow$ B means progress on A requires progress on B

Frontier of P vs. NP



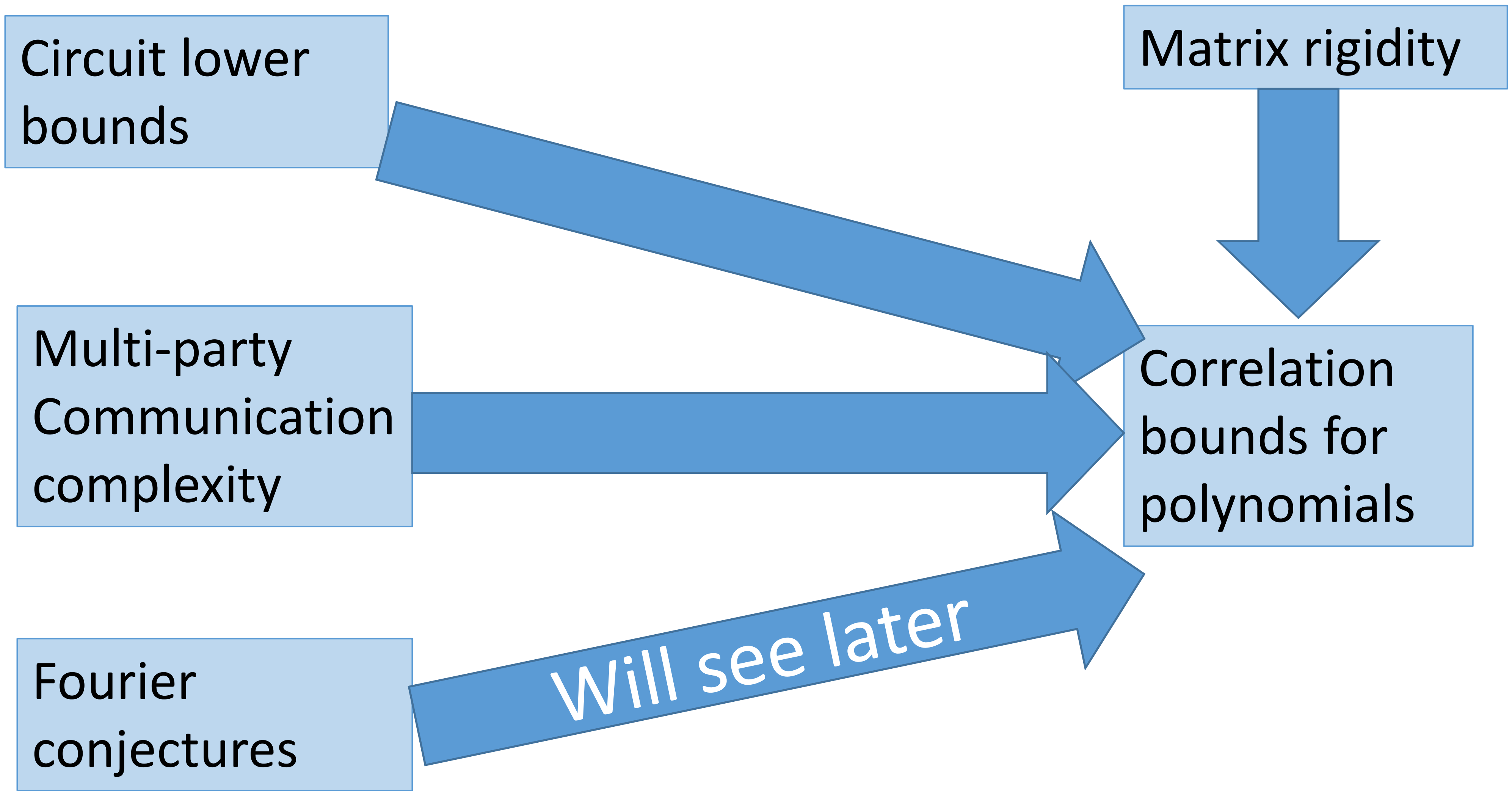
A $\rightarrow$ B means progress on A requires progress on B

Frontier of P vs. NP

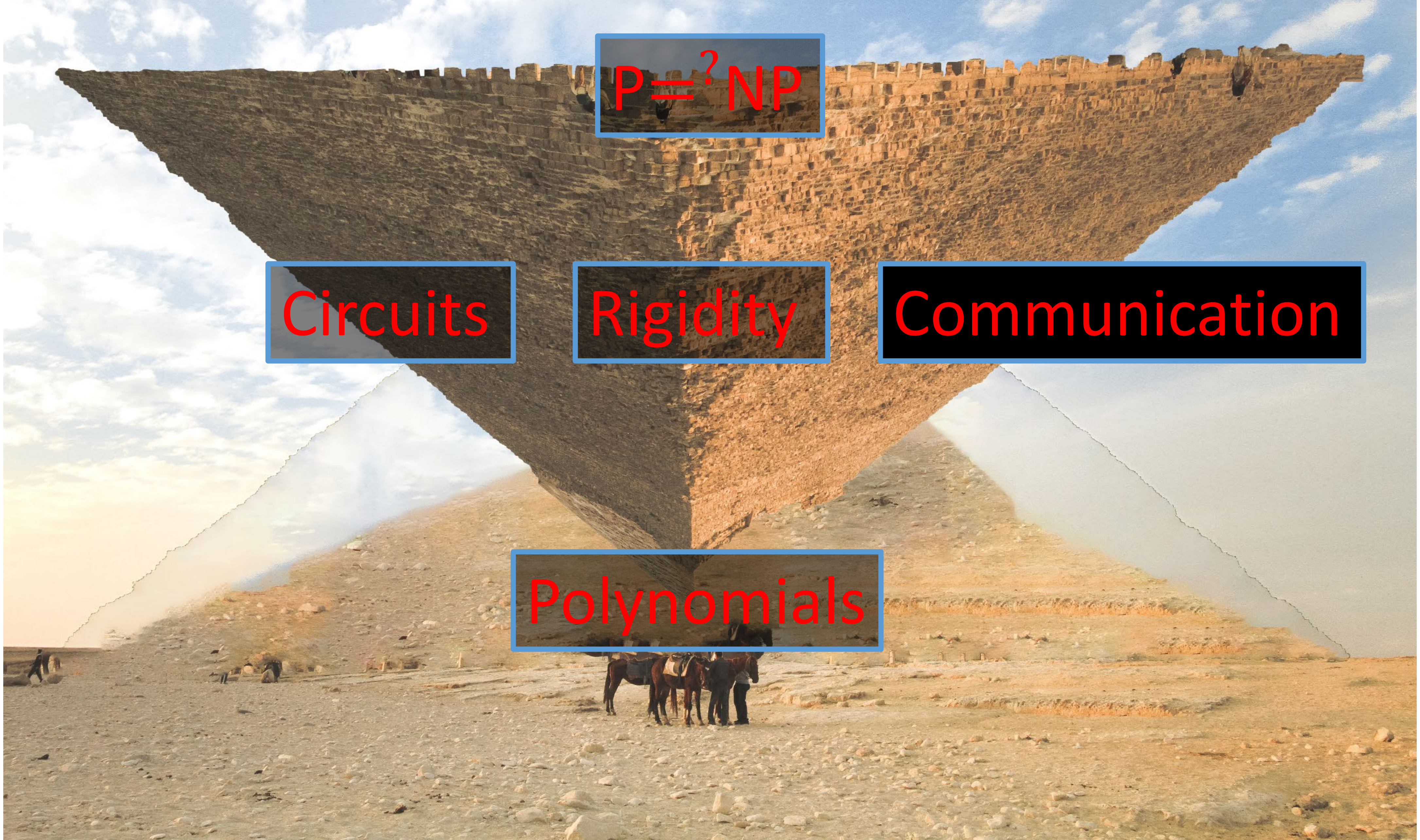


A → B means progress on A requires progress on B

Frontier of P vs. NP



My view


$P \stackrel{?}{=} NP$
Circuits
Rigidity
Communication
Polynomials

Correlation bounds for polynomials [background: survey on V's homepage]

- Challenge: Find explicit $f: \{0,1\}^n \to \{0,1\}$ and distribution X such that for every polynomial p of degree d

$$Correlation(f,p) := Pr[f(X) = p(X)] \leq 1/2 + \epsilon$$

- Razborov, Smolenky, 80's: f = Majority, X = uniform, $\epsilon = O\left(\frac{d}{\sqrt{n}}\right)$
- Babai Nisan Szegedy 90's: f = GIP/Mod_3, $\epsilon = 2^{-\Omega(\frac{n}{2^d})}$
- Open: $\epsilon = 1/\sqrt{n}$ for $d = \log(n)$; required to solve any problem on previous slide

Overview

- Introduction
- A couple of recent results on correlation bounds
- Pseudorandom generators, and more recent results

[Chattopadhyay, Hatami, Hosseini, Lovett, and Zuckerman]
STOC 2020

- Def: Local correlation: $\Delta_S(F) := \boldsymbol{E}_{x_{-S}} \left[\ \boldsymbol{E}_{x_S} [F(x)] \ - E[F] \right]^2$

- Thm : $\forall$ $degree - d \ \ F \quad \exists \ S : |S| \leq 2^{poly(d)}$: $\Delta_S(F)$ small

  $\Rightarrow$ new correlation bounds for small degrees

- Conjecture : $|S| \leq poly(d)$ suffices

[Ivanov Pavlovic V]

- Counterexample to CHHLZ conjecture

- Rules out even weak form, shows what they prove is best possible

- Proof sketch:

  Start with TRIBES DNF

  For any S of size about $n/\log n$: $\boldsymbol{E}_{x-S}$ [TRIBES = 1] $\geq \Omega(1)$

  $\Rightarrow \left[\ \boldsymbol{E}_{x_S}[F(x)] - E[F]\right]^2$ large

  Approximate TRIBES by log(n)-degree polynomial F Qed

[Ivanov Pavlovic V]

- Conjecture: Symmetric polynomials maximize correlation with mod 3; would imply dream correlation bounds

- Prove the conjecture for d = 2 by “slowly opening directions”

- Prove the conjecture for special classes of d = 3

Overview

- Introduction
- A couple of recent results on correlation bounds
- Pseudorandom generators, and more recent results

Pseudorandom generators

- Explicit, low-entropy distributions that “look random” to polynomials

- Equivalent to correlation bounds for small error

- Case of large error remains unclear

- State-of-the-art [Bogdanov V 2007, Lovett, V]:
  To fool degree-d polynomials sum d independent generators for degree 1

- Can analyze up to $d < 0.01 \log n$. Beyond that is unknown (more later)

Fourier conjectures

- Polarizing random walks: Pseudorandom generators from Fourier bounds
  [2018 Chattopadhyay Hatami Hosseini Lovett, …]

- To improve generators for polynomials [2007 Bogdanov V, Lovett, V]
  Fourier Conjectures:

  $\sum_{S:|S|=2} |\hat{p}_S| \quad \leq O(d^2)$ [Chattopadhyay Hatami Lovett Tal]

  $\sum_{S:|S|=k} |\hat{p}_S| \quad \leq 2^{o(dk)}$ [Chattopadhyay Gaitonde Lee Lovett Shetty]

- Theorem[V]: (Even weaker) conjectures
  $\Rightarrow$ correlation bounds beating Razborov-Smolensky,
  for functions related to majority (e.g., $\sum_{i<j} x_i x_j > 0$)

New correlation bounds

- We prove new correlation bounds which aim to, but don't, resolve conjectures
- Note: Correlation with Majority still open!
- Claim: Smolensky $O(\frac{d}{\sqrt{n}})$ bound for Majority tight under uniform distribution
- Claim: Can do $\Omega\left(\frac{d^2}{n}\right)$ for Majority under every distribution
- Conjecture: This is tight
- Claim: Conjecture holds (thus improving Smolensky) for $d = 1$

New pseudorandom generators

- Recall Bogdanov-V paradigm: To fool degree d, sum d generators for degree 1
  Works for d < 0.01 log n, unknown beyond that

- Thm[Derksen V 2022]:
  (Algebraic analogue of) Bogdanov-V works for large degree over large fields
  ⇒ Optimal seed length O(d log n + log q) over large fields.

- Improves on Bogdanov 2005 seminal work which has seed > d^6

- New analysis of Bogdanov-V using invariant theory

- Question: Does this work over small fields?

Thanks!