On the Grand Challenge

Emanuele "Manu" Viola

Northeastern University

2025 04 22

3

2

1

Book ad

Mathematics of the impossible

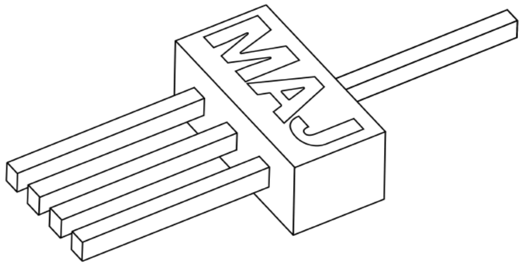
Draft on my homepage

MATHEMATICS OF THE IMPOSSIBLE

THE UNCHARTED COMPLEXITY OF COMPUTATION

Compiled on October 9, 2024

Emanuele "Manu" Viola



Outline

- **The grand challenge, some historical highlights**
- Correlation bounds against polynomials
- Why do known bounds stop “right before” major results?
- A case study: data structures and circuits

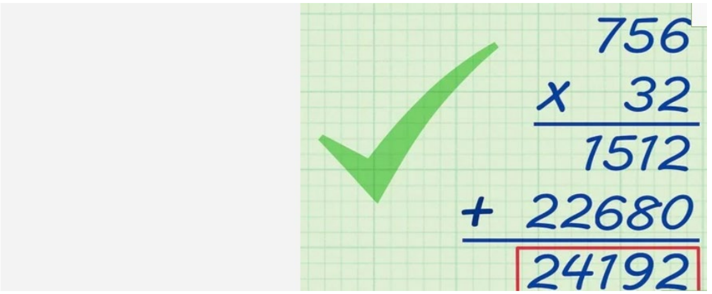
The Grand Challenge (1930 – present)

- **Prove impossibility results in computational models, a.k.a. "lower bounds"**

- **P vs NP is young, prominent special case**

- **Sometimes we say P vs NP to mean the grand challenge**

Multiplication of n-digit integers

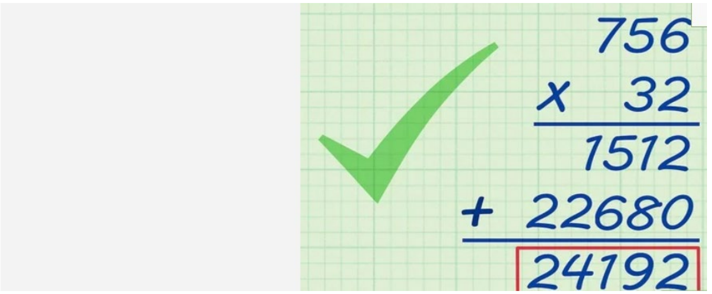


- Feeling: “As regards number systems and calculation techniques, it seems that the final and best solutions were found in science long ago”

- In 1950’s, Kolmogorov conjectured time $\Omega(n^2)$

  Started a seminar with the goal of proving it

Multiplication of n-digit integers



- Feeling: “As regards number systems and calculation techniques, it seems that the final and best solutions were found in science long ago”

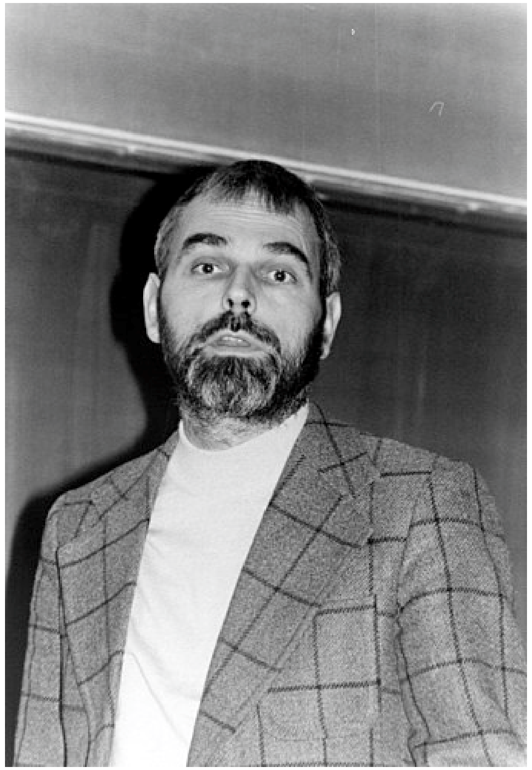
- In 1950’s, Kolmogorov conjectured time $\Omega(n^2)$
  Started a seminar with the goal of proving it

- One week later, $O(n^{1.59})$ time by Karatsuba

- […, 2019] Harvey & van der Hoeven $O(n \cdot log(n))$

Multiplication of nxn matrices

1968 Strassen working to prove $\Omega(n^3)$



Multiplication of nxn matrices

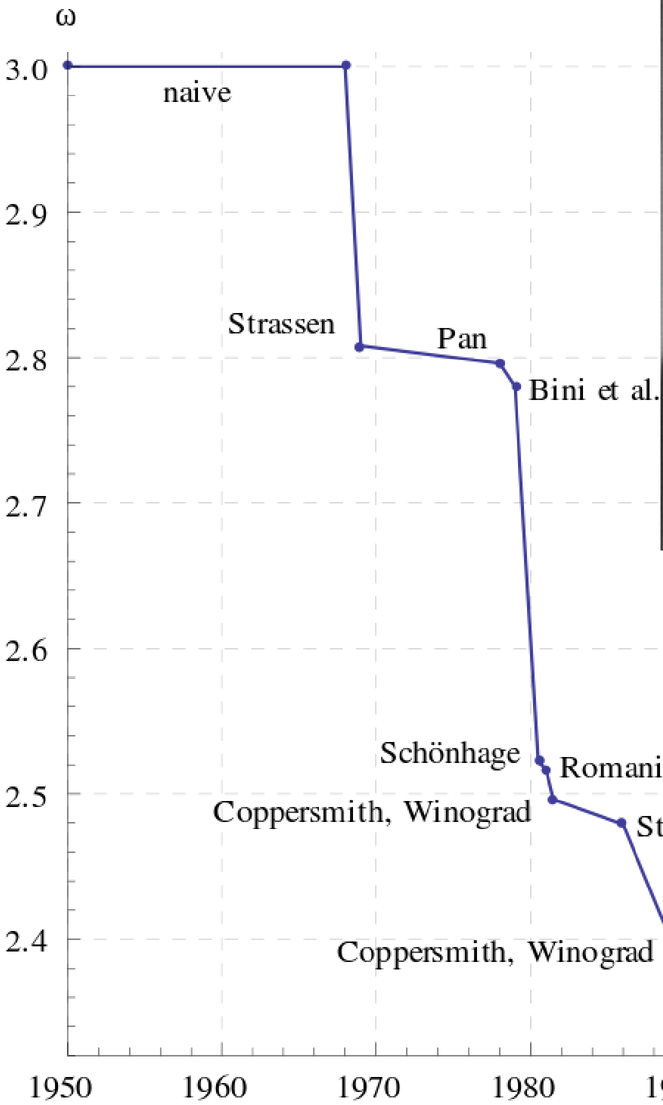
1968 Strassen working to prove $\Omega(n^3)$

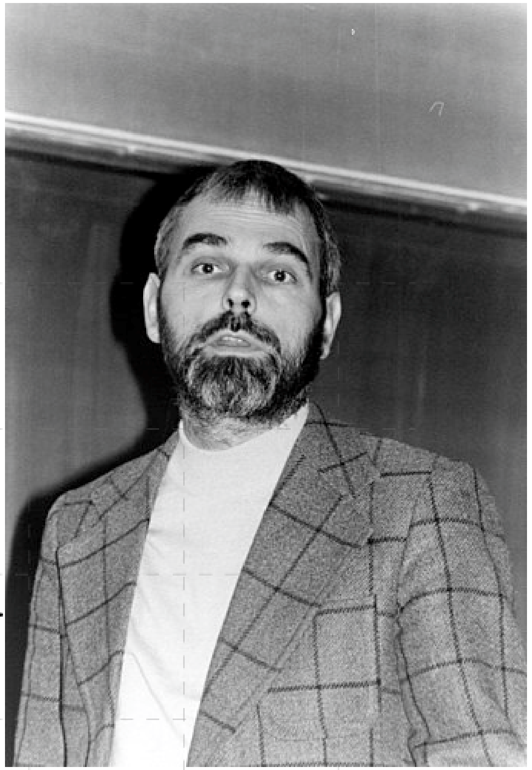
1969: Volker Strassen.

Gaussian elimination is not optimal.

Numer. Math., 13:354–356, 1969.

$O(n^{2.81})$ algorithm





Proving lower bounds for linear transformations

Problem: Give explicit $n \times n$ matrix such that

linear transformation requires $\omega(n)$ size circuits

1970 Valiant:

Fourier transform matrix is a **super-concentrator**

Conjecture: Super-concentrators require $\omega(n)$ wires

Proving lower bounds for linear transformations

Problem: Give explicit $n \times n$ matrix such that

linear transformation requires $\omega(n)$ size circuits

1970 Valiant:

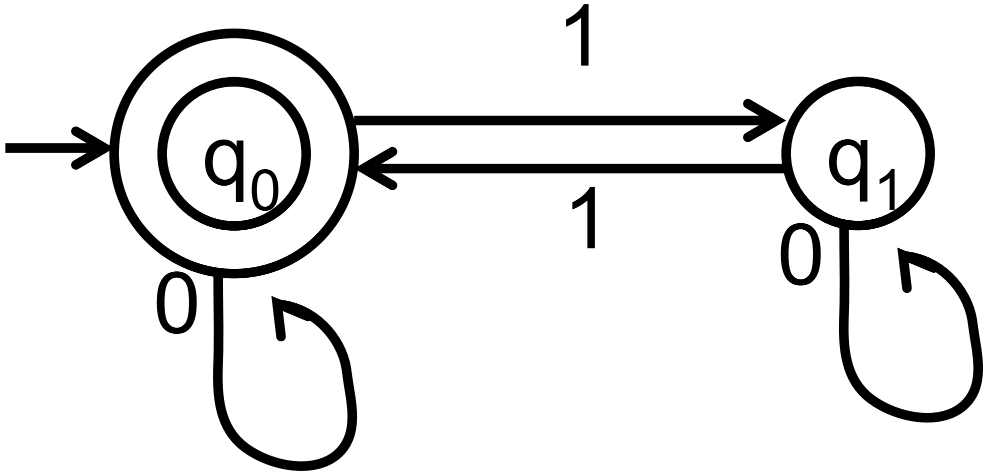
Fourier transform matrix is a **super-concentrator**

Conjecture: Super-concentrators require $\omega(n)$ wires

Later, Valiant: Super-concentrators with $O(n)$ wires exist

Space-bounded

Finite-state automata read input left to right



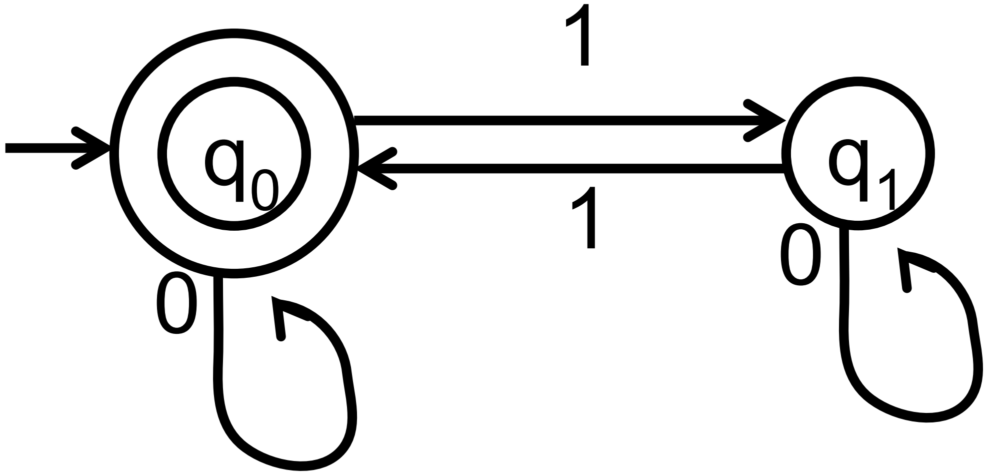
Theorem: Can't recognize palindromes

Let's allow them to read bits multiple times

Conjecture 1983 [Borodin, Dolev, Fich, Paul] Can't compute majority efficiently

Space-bounded

Finite-state automata read input left to right

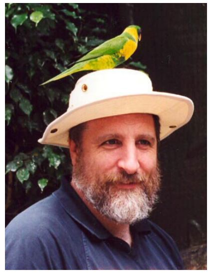


Theorem: Can't recognize palindromes

Let's allow them to read bits multiple times

Conjecture 1983 [Borodin, Dolev, Fich, Paul] Can't compute majority efficiently

Barrington 1989: Can compute Majority (and NC^1)



Boolean circuits

Universal hash functions [Carter Wegman 79]

Conjecture 1990 [Mansour Nisan Tiwari]

Require super-linear size circuits

Boolean circuits

Universal hash functions [Carter Wegman 79]

Conjecture 1990 [Mansour Nisan Tiwari]

Require super-linear size circuits

Theorem 2008 [Ishai Kushilevitz Ostrovsky Sahai]

Linear-size suffices

… many more such examples (see my book)

Next: A “bottleneck” for making progress

Outline

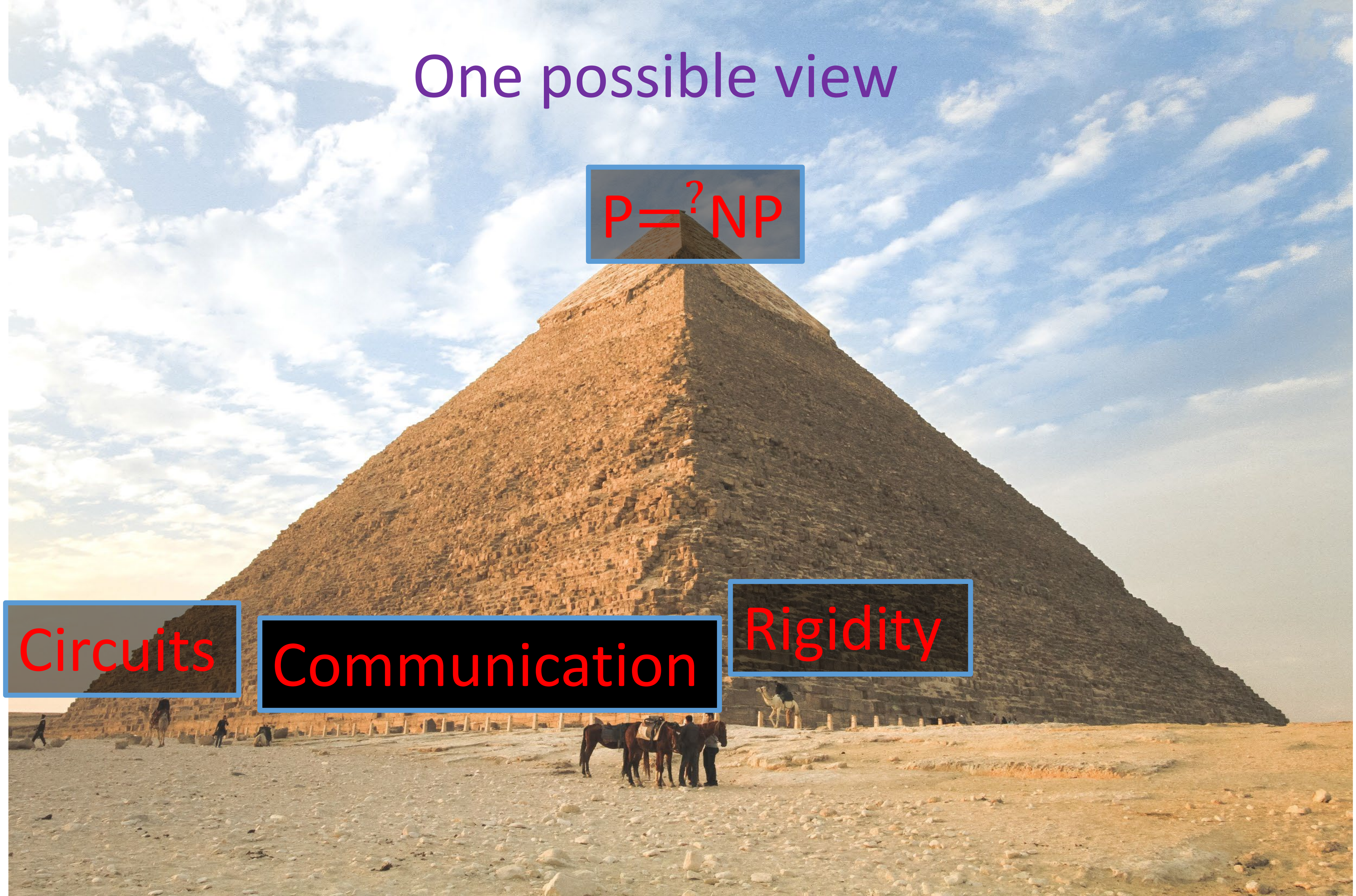
- The grand challenge, some historical highlights
- **Correlation bounds against polynomials**
- Why do known bounds stop “right before” major results?
- A case study: data structures and circuits

One possible view

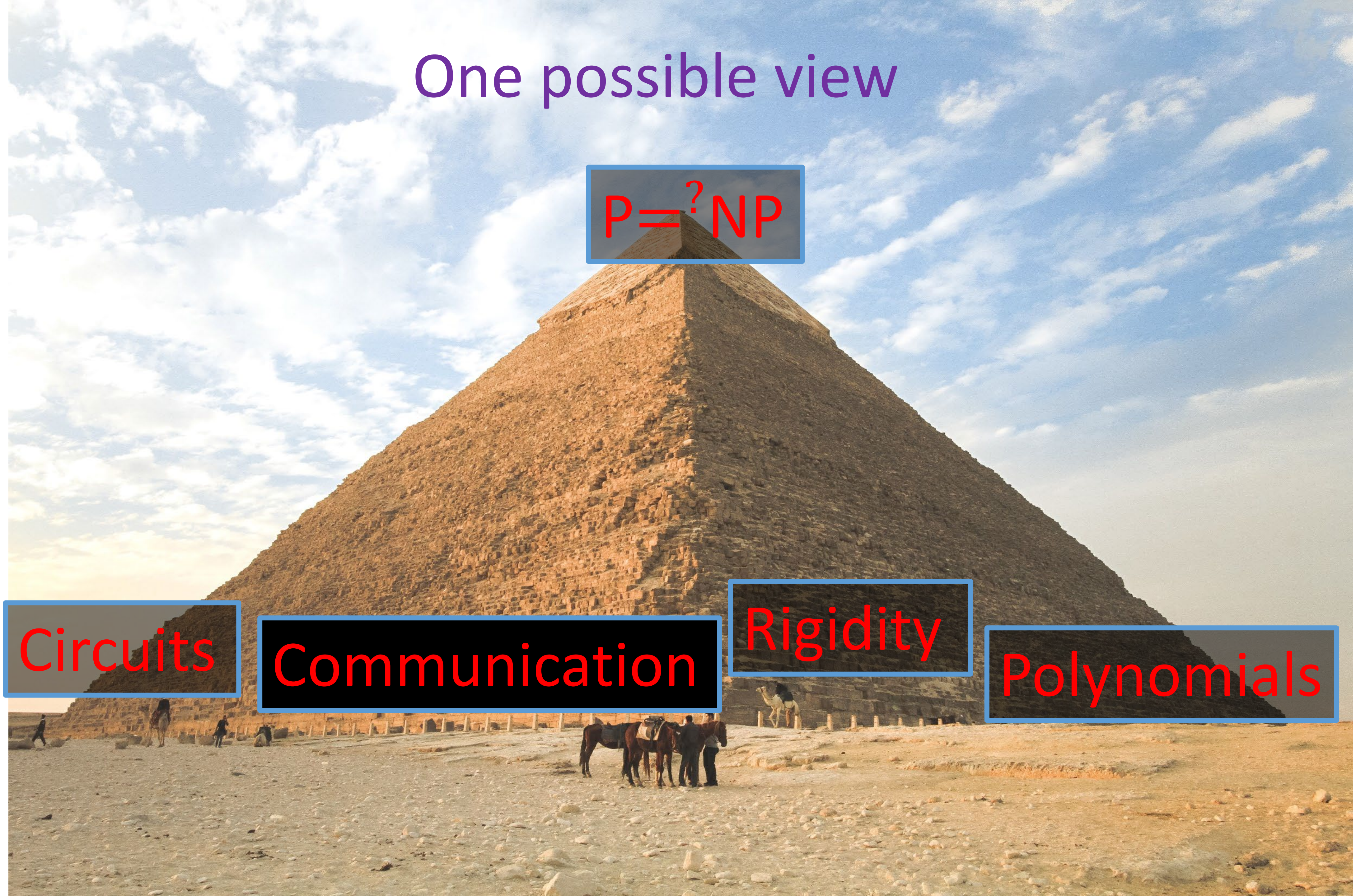
One possible view

One possible view

One possible view



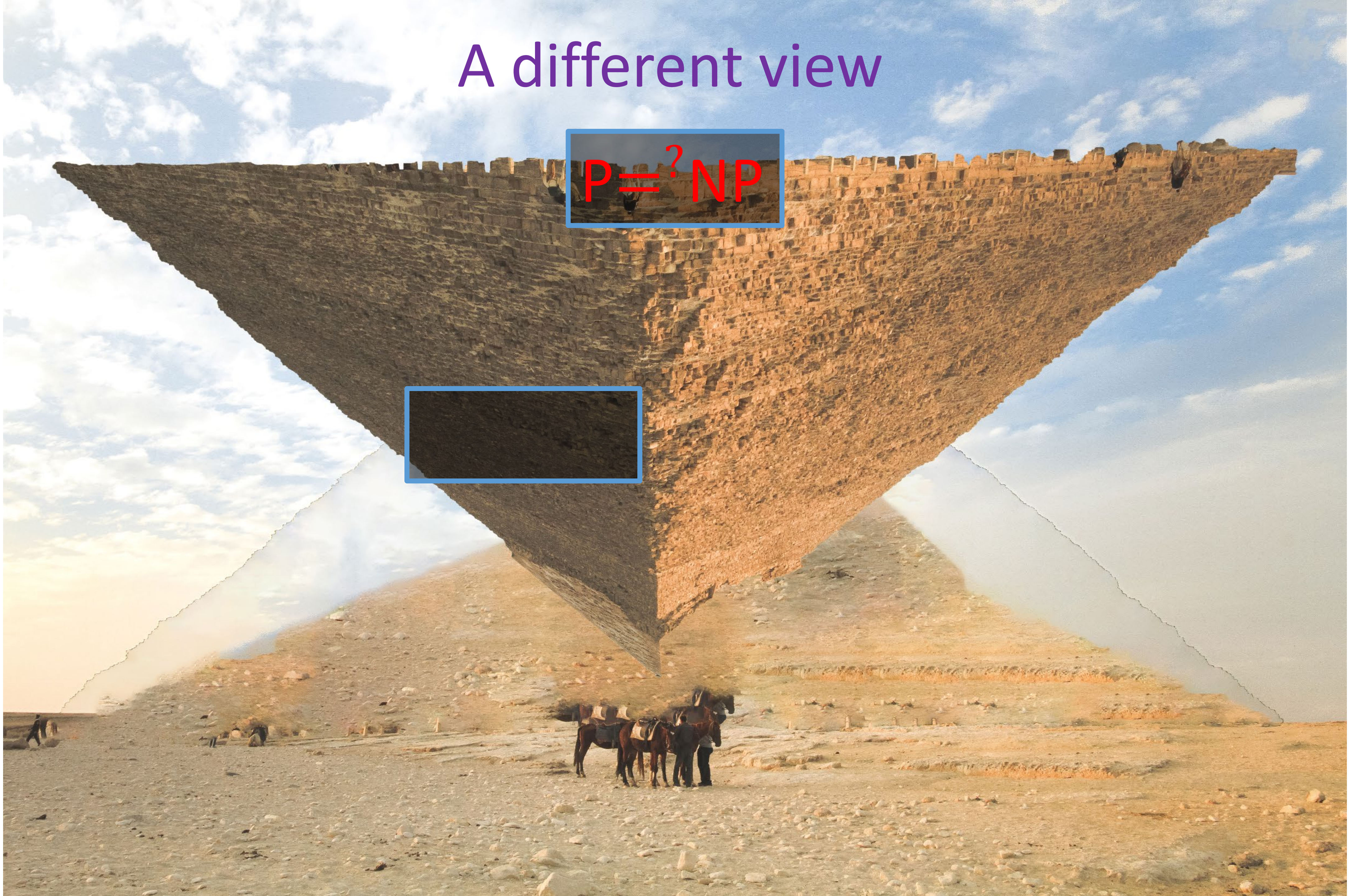
One possible view



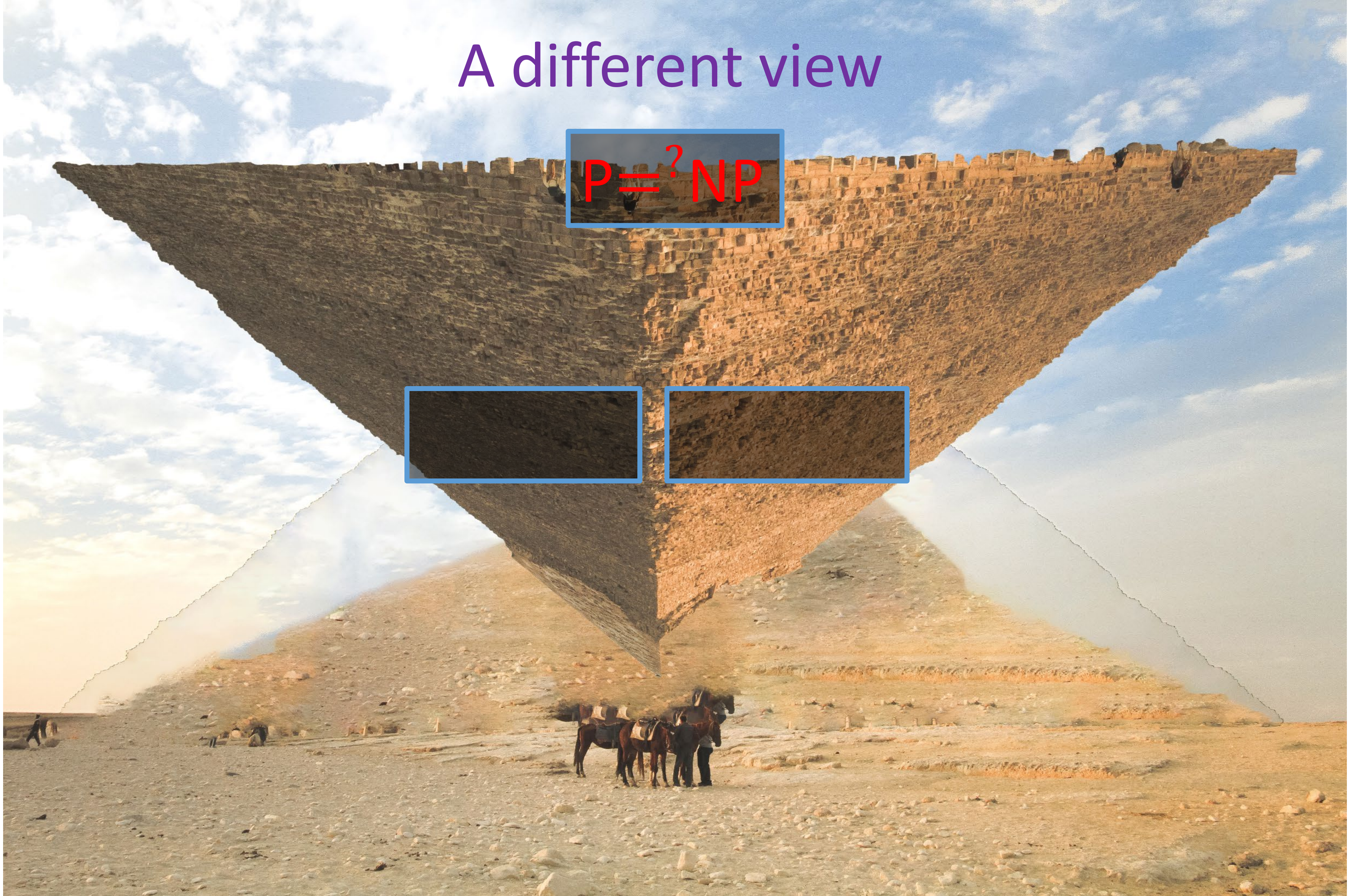
A different view

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

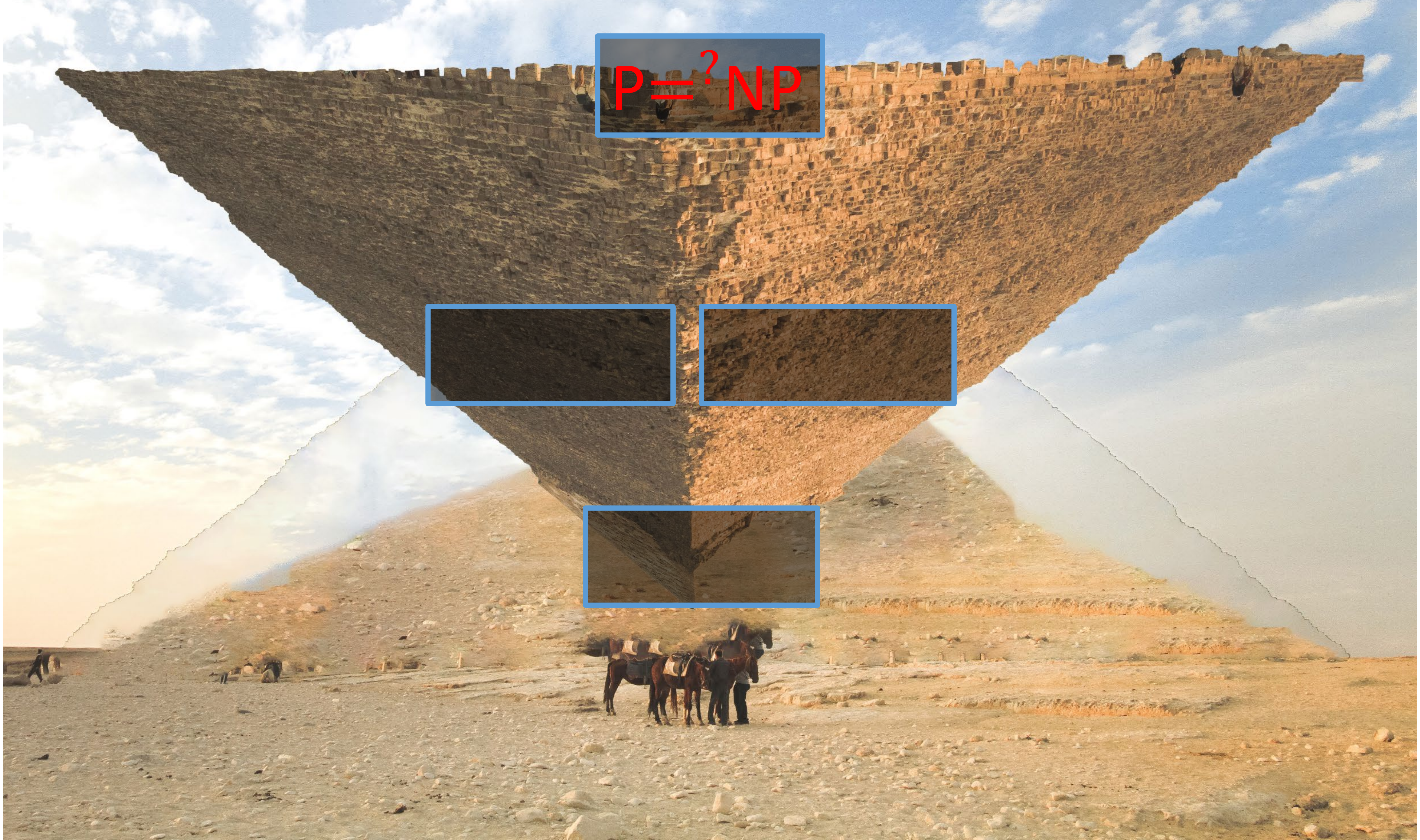
A different view



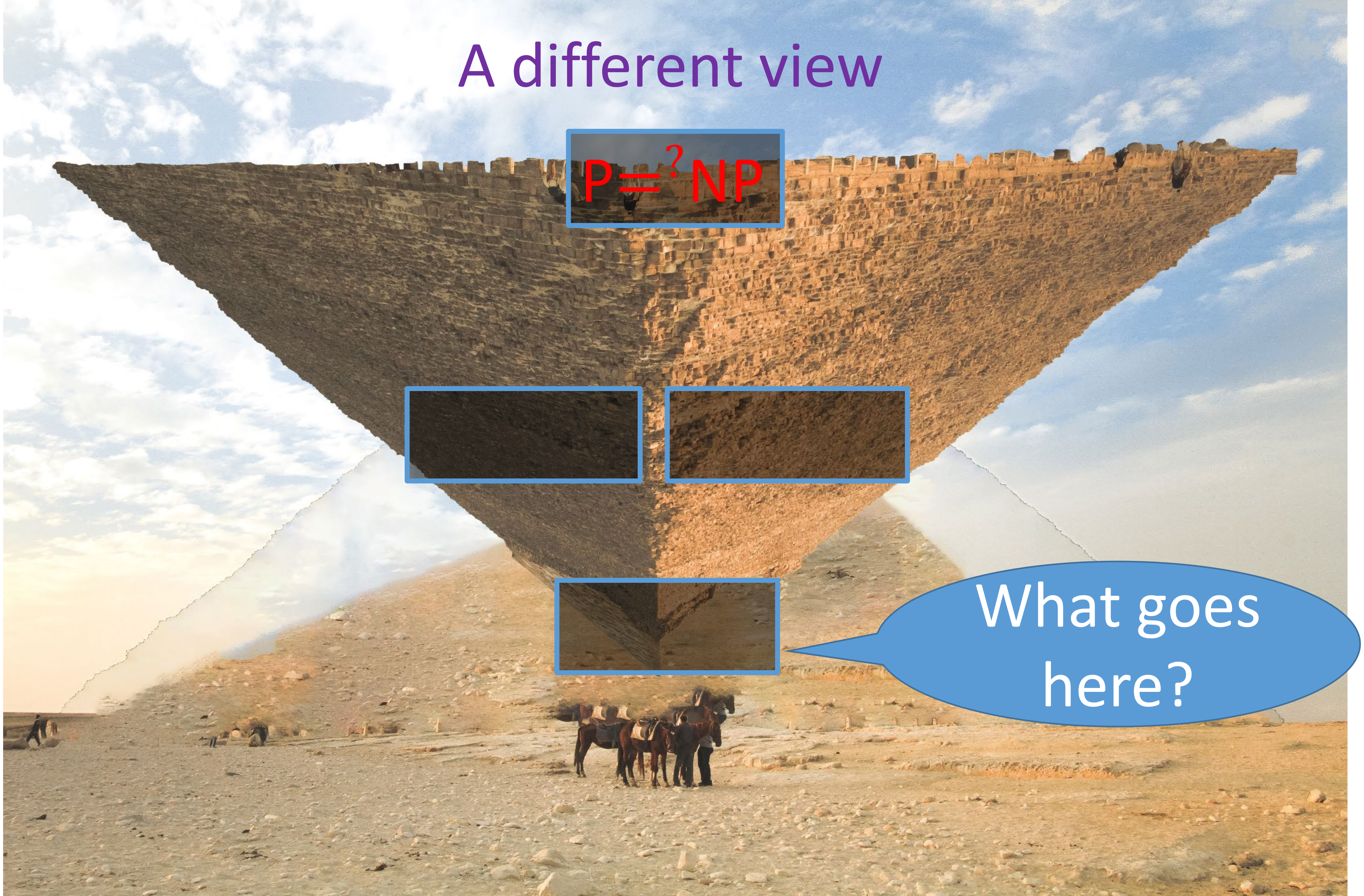
A different view



A different view



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

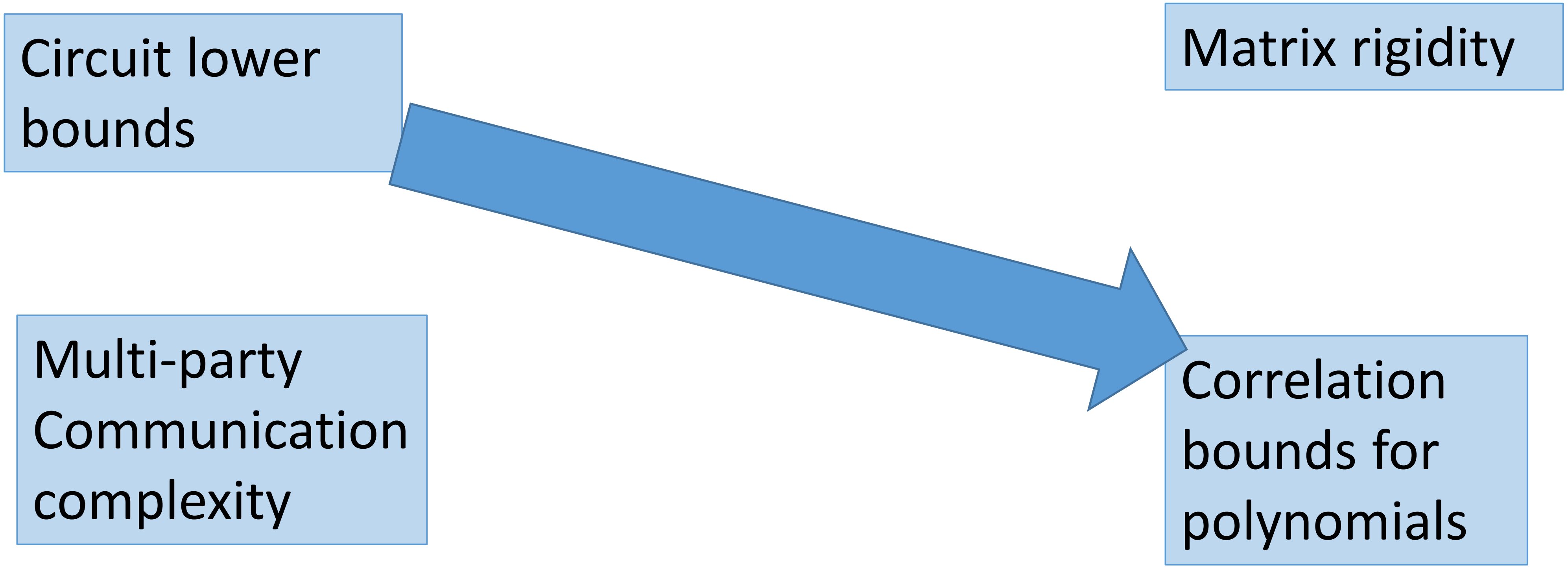
Circuit lower bounds

Matrix rigidity

Multi-party Communication complexity

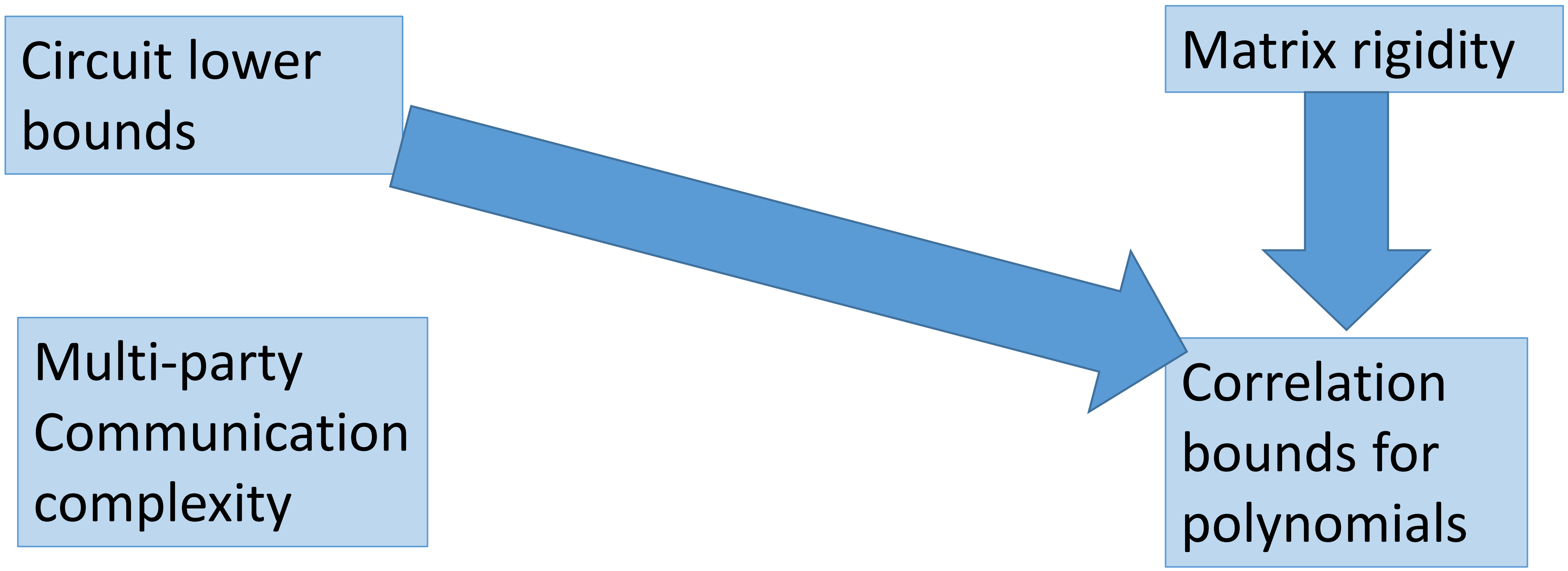
Correlation bounds for polynomials

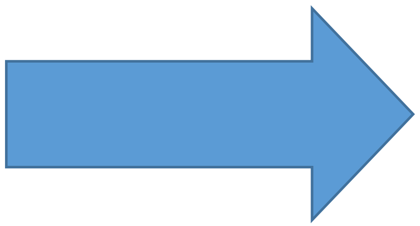
Frontier of P vs. NP



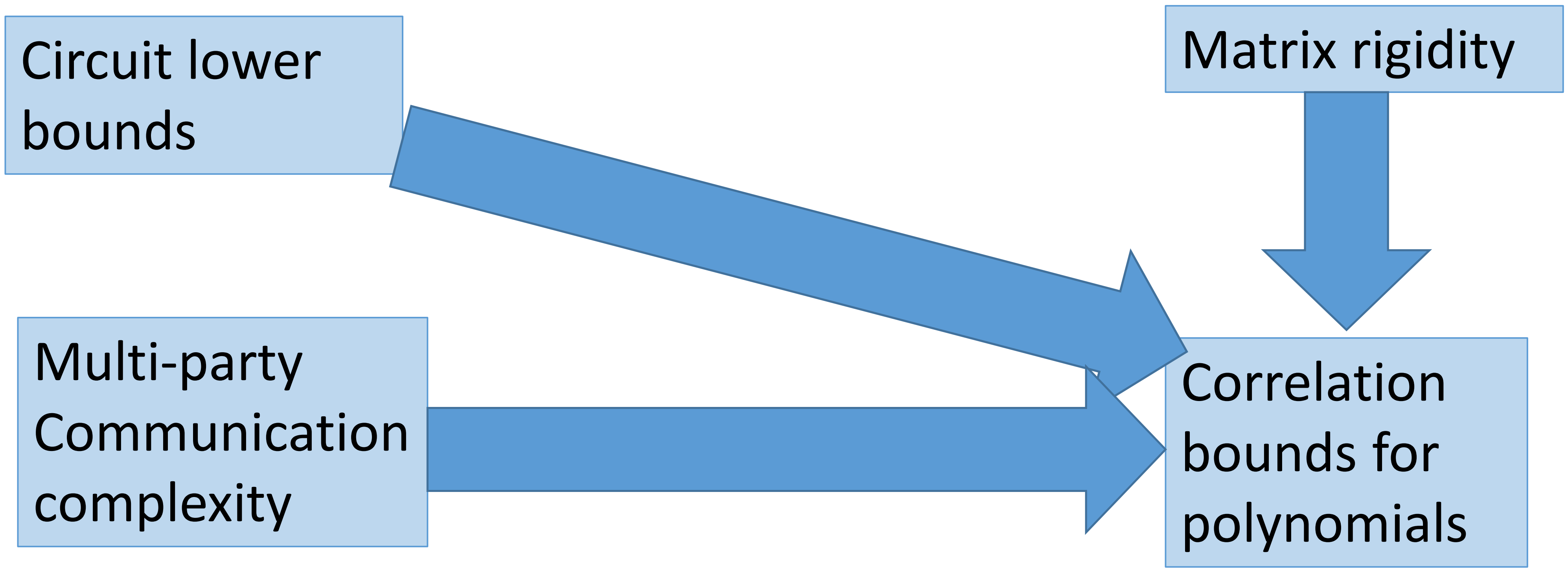
A $\Rightarrow$ B means progress on A requires progress on B

Frontier of P vs. NP



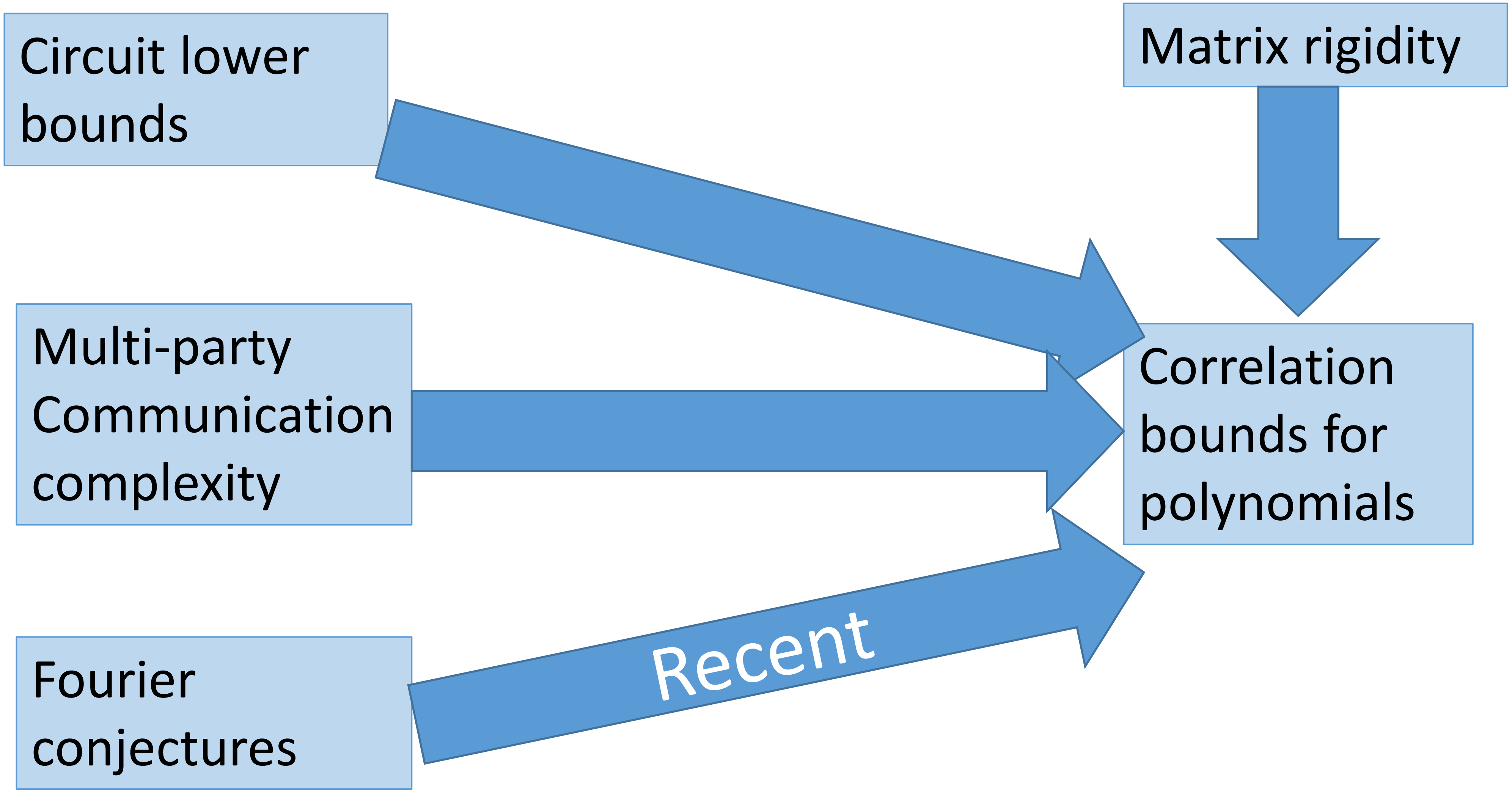
A  B means progress on A requires progress on B

Frontier of P vs. NP



A $\rightarrow$ 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

Survey on my homepage 2008, updated 2022

- Challenge: Find explicit $f: \{0,1\}^n \rightarrow \{0,1\}$ and distribution X such that for every polynomial p of degree d over F_2 (or R)

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

- 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

Next on polynomials

- Some recent results on correlation and pseudorandom generators

[Chattopadhyay Hatami Hosseini Lovett 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

  would imply dream correlation bounds for large degrees

[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] $\geq \Omega(1)$

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

  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 degree 2 by "slowly opening directions"

- Prove the conjecture for special classes of degree 3

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…??

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…
  …over F_2, but recent work covers any d for large fields [Derksen V 2022]

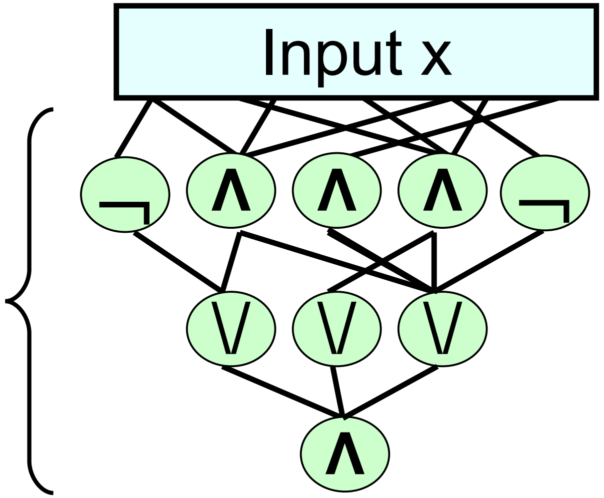
Outline

- The grand challenge, some historical highlights
- Correlation bounds against polynomials
- **Why do known bounds stop "right before" major results?**
- A case study: data structures and circuits

AC^0 circuits

- Depth-d, And-Or-Not circuits (AC^0)

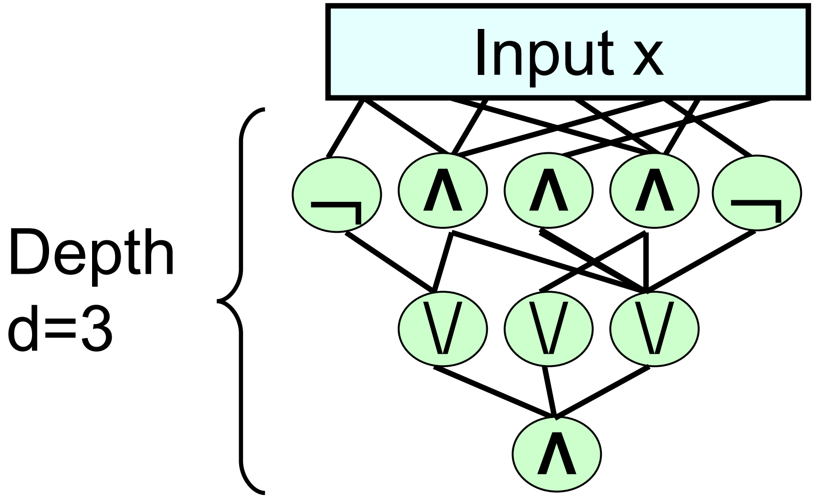
Depth d=3



- $2^{n^{\Omega(\frac{1}{d})}}$ lower bounds [80's: Furst Saxe Sipser, Ajtai, Yao, Hastad,…]

- Why not stronger bounds?

AC^0 circuits



- Depth-d, And-Or-Not circuits (AC^0)

- $2^{n^{\Omega(\frac{1}{d})}}$ lower bounds [80's: Furst Saxe Sipser, Ajtai, Yao, Hastad,…]

- Why not stronger bounds?

- Logarithmic space (L) has circuits of size $2^{n^{O(\frac{1}{d})}}$

  $\Rightarrow$ 80's bounds are best without proving **major result** $(P \neq L)$

- Improvement for $d = 3$ already implies new results for space

Similar phenomenon

- Similar situation in many other models, for example:

- Threshold circuits:

  [90's Impagliazzo Paturi Saks] $n^{1+c^{-d}}$ lower bounds

  [Allender Koucky, 2018 Chen Tell]: best without **major result** ($NC^1 \neq TC^0$)

- Algebraic complexity

  [2013 Gupta Kamath Kayal Saha Saptharishi]

  $n^{\Omega(\sqrt{n})}$ lower bounds for depth-4 homogeneous circuits

  [Agrawal Vinay, Koiran, Tavenas] best without **major result** ($VP \neq VNP$)

Why do current bounds stop “just before” proving major results?

Why do current bounds stop "just before" proving major results?

1. **No reason, it's coincidence**
   I would find this "strange" because same bounds proved with seemingly different techniques

Why do current bounds stop "just before" proving major results?

1. **No reason, it's coincidence**
   I would find this "strange" because same bounds proved with seemingly different techniques

2. **Current techniques are X, for major results need Y**

Why do current bounds stop “just before” proving major results?

1. **No reason, it’s coincidence**
   I would find this “strange” because same bounds proved with seemingly different techniques

2. **Current techniques are X, for major results need Y**

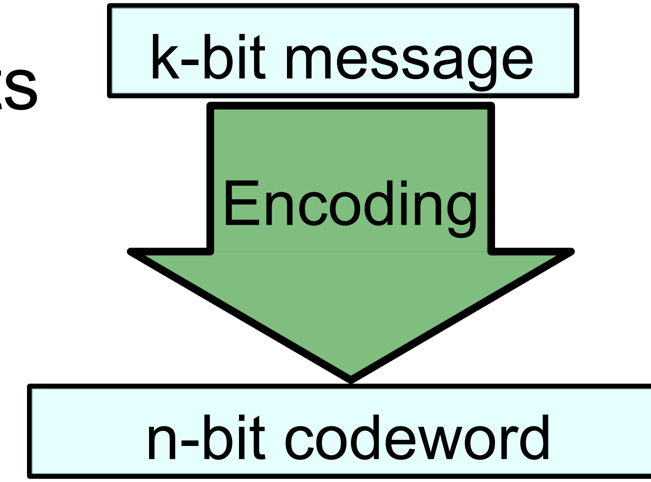
3. **Major results are false**

Outline

- The grand challenge, some historical highlights
- Correlation bounds against polynomials
- Why do known bounds stop “right before” major results?
- **A case study: data structures and circuits**

Complexity of error-correction encoding

- Asymptotically good code over $\{0,1\}$: $C \subseteq \{0,1\}^n$
  rate $\Omega(1)$: $|C| = 2^k$, $k = \Omega(n)$
  distance $\Omega(n)$: $\forall\ x \neq y \in C$, x and y differ in $\Omega(n)$ bits



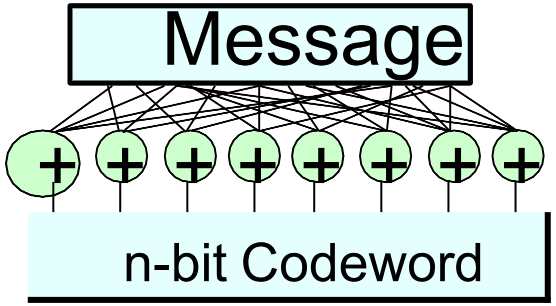
- Consider **encoding function** $f : \{0,1\}^k \to \{0,1\}^n$

- Want to compute f with circuits with **arbitrary** gates;
  only count number of wires

Previous work

Depth 1   Wires $\Theta(n^2)$

Unbounded fan-in

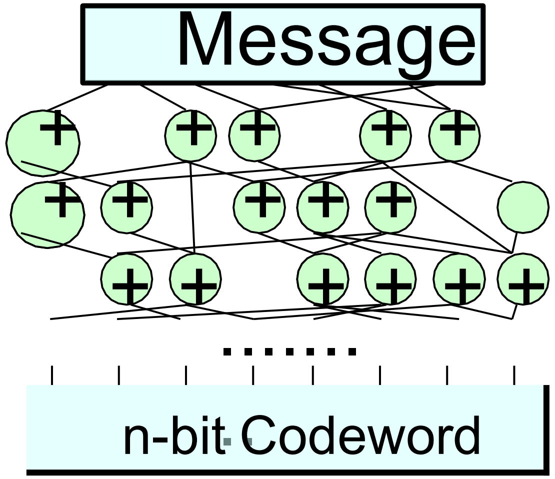


Depth $O(\log n)$ Wires $\Theta(n)$

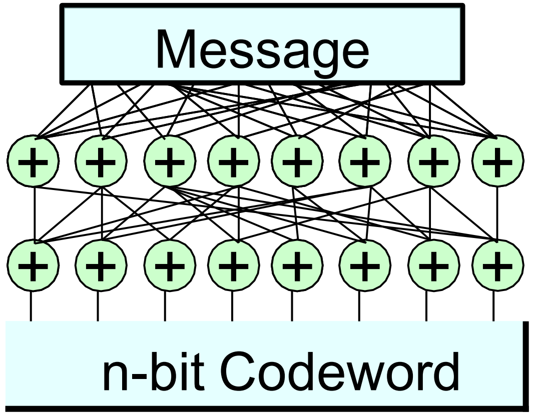
Fan-in 2

[Gelfand Dobrushin Pinsker 73]

[Spielman 95]

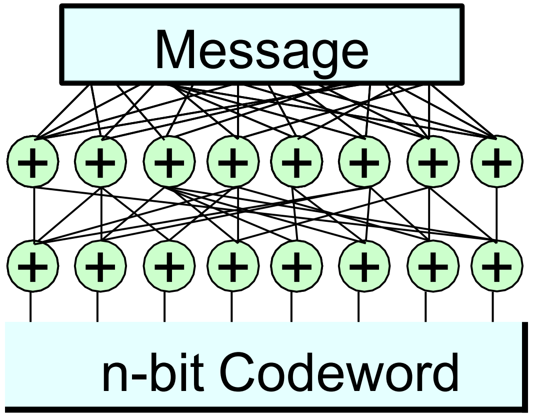


Question: How many wires for depth 2?



[Gál Hansen Koucký Pudlák V 2012]

Depth	Wires
2	$n \cdot \Theta\left(\frac{\log n}{\log\log n}\right)^2$
d > 2	$n \cdot \Theta(\lambda_d(n))$

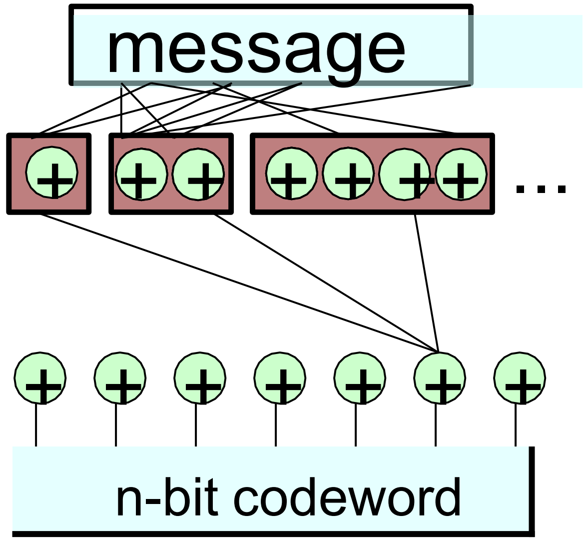


- λ inverse Ackermann: $\lambda_3(n) = \log \log n$, $\lambda_4(n) = \log^* n$, ...
- Best-known bound for linear function in NP

Probabilistic construction

Layer of log n blocks
∀ message ∃ balanced block

Output bit:
XOR one random bit per block



- i-th block balanced for message weight $w = \Theta(n/2^i)$
  Can do with wires $(n/w) \log \binom{n}{w} < n\, i$
- Total wires = $\Sigma_{i < \log n} (n\, i) + n \log n = n \cdot O(\log^2 n)$

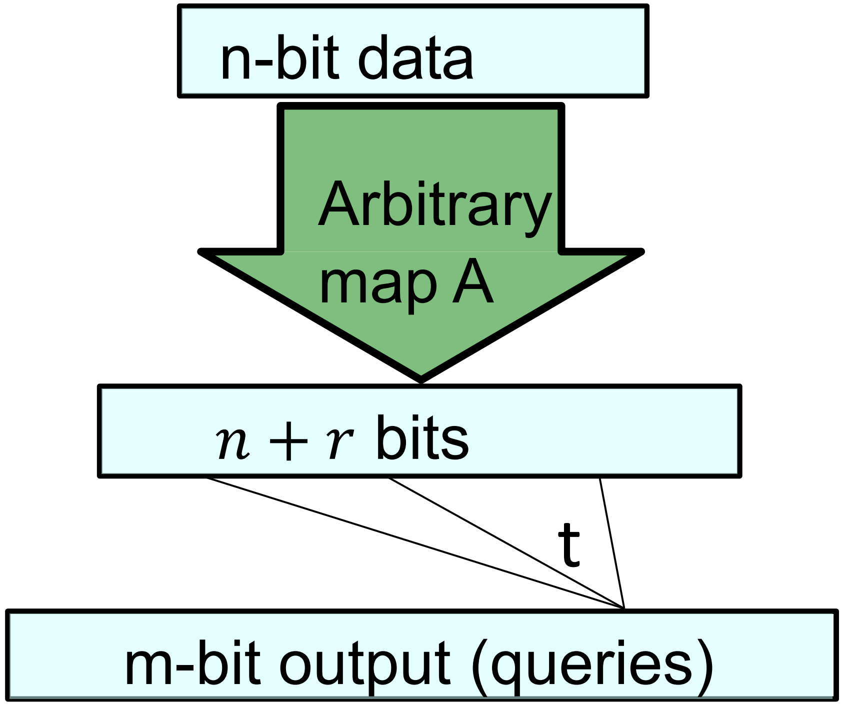
Static data structures

- Store n bits $x \in \{0,1\}^n$ into $n + r$ bits so that each of m queries can be answered reading t bits

- Trivial: $\mathrm{r} = m - n, t = 1 \; or \; r = 0, t = n$

- This talk: Think $r = o(n), m = O(n)$

- Best lower bound:
  $t = \Omega\left(\frac{\mathrm{n}}{\mathrm{r}}\right)$ for Encoding ['07 Gal Miltersen]



From circuits to data structures [V 2018]

- Theorem:
  If $f\colon \{0,1\}^n \to \{0,1\}^m$ computable with w wires in depth d
  then f has data structure with space $n + r$ time $t = \left(\frac{w}{r}\right)^d$ for any r

- Corollaries:
  - f = encoding $\Rightarrow \mathrm{t} = O\left(\frac{\mathrm{n}}{\mathrm{r}}\right) \log^3 n$ [GHKPV], matches [Gal Miltersen] $\Omega\left(\frac{\mathrm{n}}{\mathrm{r}}\right)$
  - $\mathrm{t} > \left(\frac{\mathrm{n}}{\mathrm{r}}\right)^5$ implies new circuit lower bounds

  - [Gal Miltersen] stops “right before” proving **major result**

From circuits to data structures [V 2018]

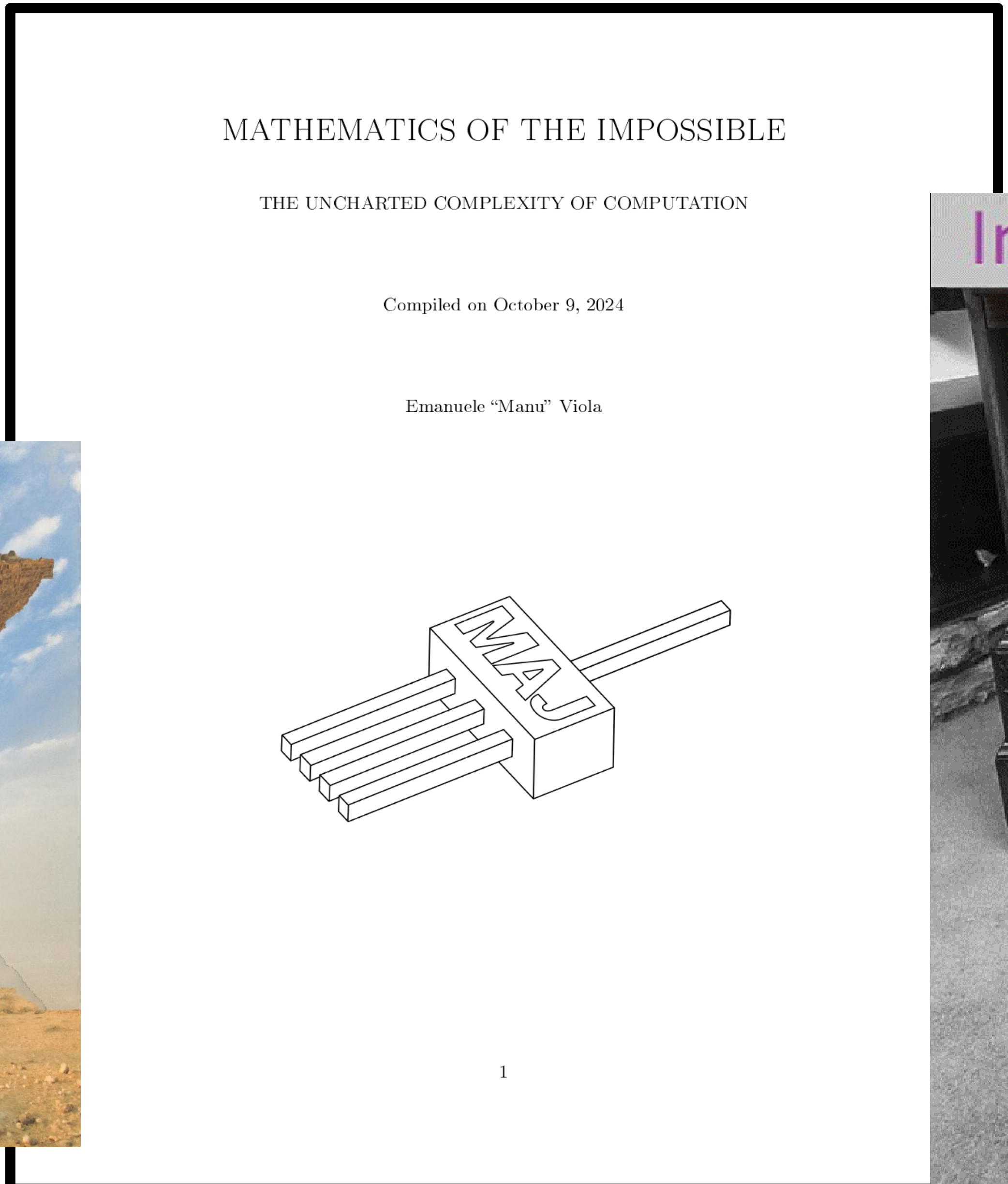
- Theorem:
  If $f: \{0,1\}^n \to \{0,1\}^m$ computable with w wires in depth d
  then f has data structure with space $n + r$ time $t = \left(\frac{w}{r}\right)^d$ for any r

- Proof:
  Store n-bit input and values of gates with fan-in $> w/r$
  Number of such gates is $\leq r$
  To compute any gate: either you have it, or it depends on $\leq w/r$ gates at next layer, repeat. Qed

Open

- Data structures lower bounds for $\mathrm{r} = n^2, m = r^3$ imply anything?

Thanks!


MATHEMATICS OF THE IMPOSSIBLE

THE UNCHARTED COMPLEXITY OF COMPUTATION

Compiled on October 9, 2024

Emanuele “Manu” Viola

1